NEC

IX2000/IX3000 シリーズ
機能説明書

日本電気株式会社

ご注意

- 本書は内容の一部または全部を無断で転載することは禁止されています。
- 本書の内容については、将来予告なしに変更することがあります。
- 本書の内容について万全を期しておりますが、万一ご不審な点や誤り、記載もれなど、お気付きのことがありましたら、ご一報くださいますようお願いいたします。
- 運用した結果については、上項に関わらず責任を負いかねますので、ご了承ください。
- 「βリリース」と記載されている機能は、その機能の動作検証や実験を目的として実装されているものであり、動作保証およびユーザサポートの対象外となります。

商標について

- 本マニュアルに記載されている会社名、製品・サービス名は、各社の登録商標、または商標です。

対象装置

本マニュアルで対象とする装置は以下となります。

- IX3315
- IX3110、IX3110-Z
- IX3015
- IX2215、IX2215-Z
- IX2207
- IX2107
- IX2106、IX2106-Z
- IX2105、IX2105-Z
- IX2235
- IX2310

目次

1 章 機能概要 1-1
■1.1 IX2000/IX3000 シリーズの機能の特徴 1-1
■1.2 諸元 1-4
1.2.1 IX2000/IX3000 ソフトウェア仕様 1-4
1.2.2 IX2000/IX3000 ソフトウェア諸元 1-7
■1.3 ハードウェア仕様 1-22
1.3.1 装置対応バージョン 1-22
1.3.2 ハードウェア諸元 1-23
■1.4 制限事項 1-25
2 章 ルータの設定 2-1
■2.1 基本操作 2-1
2.1.1 装置の起動 2-1
2.1.2 コマンド入力 2-2
2.1.3 実行モード 2-4
2.1.4 設定の確認 2-6
2.1.5 設定の保存 2-6
2.1.6 設定の削除 2-7
2.1.7 スーパーリセット 2-7
2.1.8 Web コンソールの設定 2-7
2.1.9 設定例 2-8
■2.2 システムの設定 2-9
2.2.1 システムの設定 2-9
2.2.2 パスワード情報の暗号化表示設定 2-10
2.2.3 バナー表示設定 2-10
■2.3 設定準備 2-12
■2.4 物理、リンクレイヤの設定 2-14
2.4.1 デバイス、インタフェース名表記法 2-14
2.4.2 FastEthernet/GigaEthernet インタフェースの設定 2-15
2.4.3 FastEthernet/GigaEthernet インタフェース（スイッチング HUB）の設定 2-17
2.4.4 BRI インタフェースの設定 2-21
2.4.5 Serial インタフェースの設定 2-28
2.4.6 Loopback インタフェースの設定 2-32
2.4.7 Null インタフェースの設定 2-32
2.4.8 トンネルインタフェースの設定 2-32
■2.5 ループガード機能 2-33
2.5.1 ループガード機能の概要 2-33
2.5.2 ループになる構成 2-33
2.5.3 ループガード機能の設定 2-34
■2.6 端末認証の設定 2-36
2.6.1 端末認証機能の概要 2-36
2.6.2 機能ブロック 2-38
2.6.3 IEEE802.1X 機能の設定 2-39
2.6.4 検疫機能の設定 2-49
2.6.5 MAC 認証機能の設定 2-53
2.6.6 Web 認証機能の設定 2-55
2.6.7 端末認証機能の併用 2-57

2.6.8 端末認証機能とフィルタ機能の併用 2-57
2.6.9 その他のプロトコルとの同時使用 2-58
2.6.10 注意事項 2-59
2.6.11 補足 2-60
■2.7 VLAN の設定 2-65
2.7.1 VLAN タギングの設定 2-65
2.7.2 ポート VLAN の設定 2-68
2.7.3 VLAN の特徴と注意事項 2-69
■2.8 ダイナミック VLAN 機能の設定 2-72
2.8.1 ダイナミック VLAN 機能の概要 2-72
2.8.2 ダイナミック VLAN の設定 2-73
2.8.3 端末認証機能の併用 2-77
2.8.4 注意事項 2-77
■2.9 ブリッジの設定 2-78
2.9.1 ブリッジの基本設定 2-79
2.9.2 制限事項 2-86
2.9.3 フィルタ 2-87
2.9.4 TCP-MSS 調整 2-90
2.9.5 QoS 2-90
2.9.6 VLAN 2-98
2.9.7 パススルー 2-103
■2.10 Ether over IP の設定 2-104
2.10.1 EtherIP 機能 2-104
2.10.2 ネットワーク設計の注意事項 2-109
2.10.3 制限事項 2-111
2.10.4 注意事項 2-111
■2.11 PPP の設定 2-112
2.11.1 PPP プロファイルの設定 2-113
2.11.2 LCP の設定 2-114
2.11.3 NCP の設定 2-116
2.11.4 TCP の設定 2-117
2.11.5 無通信切断の設定 2-117
2.11.6 マルチリンク PPP の設定 2-117
■2.12 PPPoE の設定 2-121
2.12.1 PPPoE クライアントの設定 2-123
2.12.2 PPPoE クライアントの応用 2-125
2.12.3 PPPoE サーバの設定 2-128
■2.13 ダイアラの設定 2-129
2.13.1 基本設定 2-129
2.13.2 複数対地の設定 2-134
2.13.3 発信抑止設定 2-136
2.13.4 自動切断 2-137
2.13.5 優先接続 2-138
■2.14 データコネクト対応オンデマンド VPN 機能の設定 2-142
2.14.1 データコネクト機能概要 2-142
2.14.2 契約条件 2-142
2.14.3 制限事項 2-143
2.14.4 注意事項 2-143
2.14.5 データコネクトサービスの概要 2-143
2.14.6 基本設定（IKEv1/Ver8.8 以降） 2-145

2.14.7 基本設定（IKEv2/Ver9.5 以降） 2-149
2.14.8 RADIUS 連携の設定（IKEv2/Ver9.5 以降） 2-150
2.14.9 QoS の詳細設定 2-153
2.14.10 動作確認方法 2-154
2.14.11 ひかり電話ナンバーゲート対応 2-156
2.14.12 ホームゲートウェイ/オフィスゲートウェイ配下での接続 2-157
2.14.13 最大接続数設定(Ver.9.6 以降) 2-158
2.14.14 死活監視機能(Ver.9.6 以降) 2-159
■2.15 USB データ通信端末の設定 2-160
2.15.1 対応するデータ通信端末 2-160
2.15.2 USB データ通信端末の基本設定 2-164
2.15.3 回線接続中の電波レベル 2-167
2.15.4 LED 2-169
2.15.5 デバイス状況の表示 2-170
2.15.6 統計情報の表示 2-172
2.15.7 電波レベル・回線接続履歴表示 2-173
2.15.8 活線挿抜（ホットプラグ） 2-174
2.15.9 PIN 認証 2-174
2.15.10 QoS 設定時の注意事項 2-176
2.15.11 MIB 2-178
2.15.12 異常検出・リカバリ機能 2-179
■2.16 IPv4 の設定 2-184
2.16.1 IPv4 アドレスの設定 2-184
2.16.2 unnumbered アドレスの設定 2-185
2.16.3 MTU の変更 2-185
2.16.4 TCP MSS 調整 2-186
2.16.5 ICMP リダイレクトメッセージの送信制御設定 2-188
2.16.6 ARP の設定 2-189
2.16.7 プロキシ ARP の設定 2-191
2.16.8 ダイレクトブロードキャスト 2-194
■2.17 VRF-Lite の設定 2-195
2.17.1 機能概要 2-195
2.17.2 注意事項 2-195
2.17.3 基本設定 2-196
2.17.4 VRF 対応機能の設定 2-197
2.17.5 対応状況 2-198
2.17.6 多対地 IPsec 構成 2-201
2.17.7 多対地 BGP 構成 2-204
2.17.8 ダイナミック VPN 構成 2-205
2.17.9 NetMeister VRF 接続構成 2-206
■2.18 DHCP の設定 2-209
2.18.1 DHCP サーバ機能 2-209
2.18.2 DHCP クライアントの設定 2-212
2.18.3 DHCP リレーエージェントの設定 2-213
2.18.4 不正端末検知機能の設定 2-214
■2.19 NAT/NAPT の設定 2-216
2.19.1 NAT の設定 2-217
2.19.2 NAPT の設定 2-220
2.19.3 対応アプリケーション 2-228
2.19.4 アクセスログ機能 2-229

2.19.5 パケット評価フロー 2-232
2.19.6 MAP-E(動的 IP アドレス)トンネルでの NAPT 動作モードについて 2-233
■2.20 IPv6 の設定 2-238
2.20.1 IPv6 の有効設定 2-238
2.20.2 IPv6 アドレスの設定 2-239
2.20.3 リンクローカルアドレスの補足 2-240
2.20.4 MTU の変更 2-240
2.20.5 TCP MSS 調整 2-241
2.20.6 強制リアセンブリ 2-242
2.20.7 RA の設定 2-242
2.20.8 ND プロキシの設定 2-245
2.20.9 ローカル ND プロキシの設定 2-247
2.20.10 ICMPv6 リダイレクトメッセージの送信制御設定 2-248
2.20.11 サイトの設定 2-248
■2.21 DHCPv6 の設定 2-249
2.21.1 サポートメッセージ 2-249
2.21.2 Prefix Delegation クライアントの設定 2-250
2.21.3 Prefix Delegation サーバの設定 2-255
2.21.4 PD/RA 自動判別 2-258
2.21.5 Prefix Delegation 再配布の設定 2-260
2.21.6 接続情報の保持時間設定 2-263
■2.22 ルーティングの設定 2-264
2.22.1 経路制御とディスタンス 2-264
2.22.2 イコールコストマルチパス 2-267
2.22.3 スタティックルート 2-269
2.22.4 RIP/RIPng 2-271
2.22.5 OSPFv2/OSPFv3 2-280
2.22.6 BGP4 2-295
2.22.7 ポリシールーティング 2-315
■2.23 マルチキャストの設定 2-320
2.23.1 機能概要 2-320
2.23.2 IPv4 マルチキャスト機能 2-322
2.23.3 IGMP プロキシ機能 2-322
2.23.4 スタティック設定 2-323
2.23.5 PIM-SM 機能 2-324
2.23.6 IPv6 マルチキャスト機能 2-332
2.23.7 制限事項・注意事項・サポート構成 2-335
2.23.8 IGMP スヌーピング機能 2-341
■2.24 DNS の設定 2-342
2.24.1 プロキシ DNS の設定 2-342
2.24.2 DNS リゾルバの設定 2-346
2.24.3 DNS キャッシュの設定 2-348
2.24.4 FQDN 指定対応 2-349
2.24.5 DNS サーバアクセス振り分け 2-350
2.24.6 ローカル DNS サーバ 2-351
■2.25 ダイナミック DNS 機能の設定 2-352
2.25.1 ダイナミック DNS 機能 2-352
2.25.2 ダイナミック DNS の設定 2-352
2.25.3 ダイナミック DNS の動作 2-355
2.25.4 注意事項 2-355

■2.26 NTP の設定 2-356
2.26.1 NTP クライアントの設定 2-356
2.26.2 NTP サーバの設定 2-359
2.26.3 NTP アクセスリスト 2-360
■2.27 VRRP の設定 2-361
2.27.1 基本設定 2-361
2.27.2 ルータバックアップ 2-364
2.27.3 ロードバランシング 2-366
2.27.4 プリエンプトモードとノンプリエンプトモード 2-368
2.27.5 VR IP アドレス宛のパケット処理 2-370
2.27.6 タイマ設定 2-370
2.27.7 ネットワークモニタ機能との組み合わせ 2-371
2.27.8 VRRP 使用時の注意点 2-372
■2.28 ネットワークモニタの設定 2-373
2.28.1 ネットワークモニタ機能の概要 2-373
2.28.2 ネットワークモニタの基本動作 2-374
2.28.3 イベントの設定 2-375
2.28.4 アクションの設定 2-387
2.28.5 watch グループ毎の設定 2-397
2.28.6 その他の動作モード 2-399
2.28.7 使用例 2-404
2.28.8 ネットワークモニタ機能の注意事項 2-412
■2.29 スケジューラ機能の設定 2-414
2.29.1 スケジューラ機能 2-414
2.29.2 スケジューラ機能の設定 2-414
2.29.3 スケジューラ機能の時刻指定と NTP による時刻変更 2-416
2.29.4 コマンドリストの一時停止 2-417
2.29.5 コンフィグモードで作業中の場合のスケジューラ機能の影響 2-417
2.29.6 スケジューラ機能・コマンドリストの注意事項 2-418
■2.30 パケットフィルタの設定 2-419
2.30.1 スタティックフィルタ 2-419
2.30.2 ダイナミックフィルタ 2-422
2.30.3 強制リアセンブリ 2-429
2.30.4 MAC フィルタ 2-429
2.30.5 パケットフィルタのロギング 2-430
■2.31 URL フィルタリング 2-432
2.31.1 注意事項 2-432
2.31.2 内部 URL フィルタリング機能 2-433
2.31.3 外部 URL フィルタリング機能 2-434
2.31.4 URL フィルタリング対象外の設定 2-436
2.31.5 ブロック画面の設定 2-436
2.31.6 URL フィルタキャッシュの設定 2-437
2.31.7 URL フィルタリング機能の処理順序 2-437
2.31.8 その他の設定 2-437
2.31.9 ブロック画面のカスタマイズ 2-437
■2.32 不正アクセス検知（IDS）の設定 2-438
2.32.1 不正アクセス検知条件 2-438
2.32.2 不正アクセス検知条件の設定 2-439
■2.33 トンネルの設定 2-441
2.33.1 トンネル機能の概要 2-441

2.33.2 トンネルの設定 2-442
2.33.3 フラグメントの設定 2-442
2.33.4 IPv6 over IPv4 トンネルの設定 2-443
2.33.5 IPv4 over IPv6 トンネルの設定 2-444
2.33.6 IPv4 over IPv4 トンネルの設定 2-445
2.33.7 IPv6 over IPv6 トンネルの設定 2-446
2.33.8 GRE（Generic Routing Encapsulation）トンネルの設定 2-447
2.33.9 IPv4 over IPv6 トンネル(冗長)の設定 2-453
2.33.10 MAP-E の設定 2-454
2.33.11 IPv6 国内標準プロビジョニング方式の設定 2-466
■2.34 IKE の設定 2-468
2.34.1 IKE の基本設定 2-469
2.34.2 対向装置の監視 2-471
2.34.3 commit-bit 対応 2-472
2.34.4 Dangling SA 型/Continuous-channel SA 型 2-474
2.34.5 リキー設定 2-476
2.34.6 DELETE 送信抑止設定 2-476
■2.35 IPsec の設定 2-477
2.35.1 IPsec の基本設定 2-477
2.35.2 トンネルモード 2-485
2.35.3 IPsec リモートアクセス機能 2-489
2.35.4 IPsec トンネル二重化対応 2-491
2.35.5 IPsec と NAT/NAPT の連携 2-493
2.35.6 トランスポートモード 2-495
2.35.7 NAT トラバーサル機能 2-497
2.35.8 IPsec のネスト時の注意 2-501
■2.36 スマートデバイス対応（L2TP LNS 機能）の設定 2-502
2.36.1 L2TP LNS 機能の概要 2-502
2.36.2 動作確認端末 2-502
2.36.3 注意事項 2-502
2.36.4 L2TP LNS/IPsec の基本設定 2-503
2.36.5 接続情報の取得 2-505
2.36.6 Radius 連携 2-505
■2.37 L2TP LAC 機能によるリモートアクセス設定 2-506
2.37.1 L2TP LAC 機能の概要 2-506
2.37.2 注意事項 2-506
2.37.3 L2TP LAC および PPPoE サーバ機能の基本設定 2-507
2.37.4 接続情報の取得 2-508
■2.38 IKEv2/IPsec の設定 2-509
2.38.1 IKEv2/IPsec の概要 2-509
2.38.2 事前共有鍵による設定例 2-511
2.38.3 NAT トラバーサル機能 2-518
2.38.4 DELETE・REKEY 送信抑止設定 2-518
2.38.5 注意事項 2-519
2.38.6 複数ポリシーの設定 2-520
2.38.7 IPsec リモートアクセス機能(拠点側動的アドレス対応) 2-520
2.38.8 その他の認証方式 2-522
2.38.9 表示コマンド/イベントログ 2-524
■2.39 ダイナミック VPN の設定 2-526
2.39.1 ダイナミック VPN の概要 2-526

2.39.2 設定例 2-527
2.39.3 各機能の設定 2-531
2.39.4 動作 2-534
2.39.5 状態確認 2-535
2.39.6 ダイナミック VPN の VRF 構成 2-536
■2.40 QoS の設定 2-539
2.40.1 優先制御/帯域制御の動作 2-540
2.40.2 優先制御/帯域制御の設定方法 2-545
2.40.3 帯域制御/優先制御設定の注意事項 2-549
2.40.4 マーキング・カラーリングの設定 2-555
2.40.5 qos-group 値の付与 2-558
2.40.6 SW-HUB の優先制御（Ver.8.3 以降） 2-560
2.40.7 ダイナミック QoS の設定 2-562
■2.41 VoIP のフォワーディング設定 2-567
2.41.1 VoIP のフォワーディングのための実現機能 2-567
2.41.2 RTP の QoS 設定 2-567
2.41.3 マルチリンク PPP インタリーブの設定 2-568
2.41.4 ヘッダ圧縮 2-570
2.41.5 RTP ヘッダ圧縮（CRTP） 2-570
2.41.6 TCP ヘッダ圧縮（CTCP） 2-571
2.41.7 送出遅延制御 2-572
■2.42 AAA の設定 2-573
2.42.1 AAA の有効化 2-573
2.42.2 認証（Authentication）の設定 2-574
2.42.3 許可（Authorization）の設定 2-581
2.42.4 アカウンティング（Accounting）の設定 2-583
2.42.5 AAA の使用例 2-585
2.42.6 RADIUS クライアント 2-586
2.42.7 サーバの設定 2-590
■2.43 Web コンソールの設定 2-592
2.43.1 Web コンソール機能の特徴 2-592
2.43.2 注意事項 2-592
2.43.3 Web コンソールを利用する設定 2-593
2.43.4 対応ブラウザ 2-595
2.43.5 Web コンソールの操作 2-595
2.43.6 Web コンソールの保守管理 2-596
2.43.7 かんたん設定 2-601
2.43.8 詳細設定 2-603
2.43.9 拡張ページ 2-626
2.43.10 WebAPI 機能 2-627
2.43.11 その他 2-628
■2.44 Wake on LAN の設定 2-629
2.44.1 Wake on LAN 機能概要 2-629
2.44.2 制限事項 2-629
2.44.3 コマンドラインからの利用 2-629
2.44.4 Web コンソールからの利用 2-630
■2.45 URL リダイレクトの設定 2-631
2.45.1 URL リダイレクト機能概要 2-631
2.45.2 注意事項 2-633
■2.46 URL オフロードの設定 2-634

2.46.1 URL オフロード機能概要 2-635
2.46.2 制限事項 2-636
2.46.3 基本設定 2-636
2.46.4 基本動作 2-640
2.46.5 構成別設定例 2-641
2.46.6 プロキシ例外設定の自動化 2-644
2.46.7 運用情報 2-649
■2.47 リンクマネージャの設定 2-650
2.47.1 機能概要 2-650
2.47.2 注意事項 2-651
2.47.3 Web コンソールからの利用方法 2-651
2.47.4 コマンドラインでの利用方法 2-655
2.47.5 主な利用方法 2-658
2.47.6 リンクマネージャの通信制御機能 (Ver.9.6 以降) 2-659
2.47.7 処理順序 2-661
■2.48 NetMeister の設定 2-662
2.48.1 利用方法 2-663
2.48.2 利用環境 2-663
2.48.3 注意事項 2-665
2.48.4 基本設定 2-665
2.48.5 NetMeister との接続 2-668
2.48.6 ダイナミック DNS 2-675
2.48.7 アラーム通知 2-676
2.48.8 NetMeister 通信冗長化 2-678
2.48.9 アクション実行 2-681
2.48.10 デバイスリスト 2-681
2.48.11 UTM 統計レポート 2-681
2.48.12 URL オフロード拡張 2-681
2.48.13 他機種収容 2-681
2.48.14 UTM 脅威分析 2-681
2.48.15 リモートログイン 2-682
2.48.16 ダイナミック VPN 設定 2-682
2.48.17 メトリクス 2-682
2.48.18 ポート情報 2-683
2.48.19 Find Your Device 2-684
2.48.20 NetMeister Prime 2-684
2.48.21 イベントログ送信機能 2-684
■2.49 アプリケーション解析機能の設定 2-686
2.49.1 アプリケーション解析機能概要 2-686
2.49.2 機能一覧 2-686
2.49.3 注意事項 2-686
2.49.4 WAN・LAN インタフェースの指定 2-687
2.49.5 トラフィックのローカルブレイクアウトについて 2-689
2.49.6 URL オフロード併用 2-689
2.49.7 情報の確認 2-690
■2.50 ゼロコンフィグの設定 2-693
2.50.1 ゼロコンフィグ 2-693
2.50.2 SMF とは？ 2-693
2.50.3 自動コンフィグレーション機能（ゼロコンフィグ機能） 2-693
2.50.4 リモートメンテナンス 2-694

2.50.5 起動時バージョン固定（PULL バージョンアップ・ダウン）（Ver.8.4 以降） 2-694
2.50.6 死活監視・運用監視（Heartbeat） 2-695
2.50.7 ゼロコンフィグ適用環境 2-696
■2.51 sFlow の設定 2-697
2.51.1 sFlow エージェント機能概要 2-697
2.51.2 sFlow エージェント設定 2-699
2.51.3 sFlow エージェントの設定調整 2-700
2.51.4 IPsec 利用時の監視方法 2-700
■2.52 アクセスリストの設定 2-701
2.52.1 IPv4/IPv6 アクセスリスト 2-701
2.52.2 ドメイン名指定 2-707
2.52.3 ダイナミックアクセスリスト 2-707
2.52.4 MAC アクセスリスト 2-708
■2.53 ルートマップの設定 2-709
■2.54 プレフィックスリストの設定 2-710
■2.55 UFS キャッシュの設定 2-711
2.55.1 概要 2-711
2.55.2 動作原理 2-712
2.55.3 UFS キャッシュの設定 2-714
2.55.4 UFS キャッシュの表示 2-714
2.55.5 消費メモリ量 2-715
2.55.6 ハッシュテーブルサイズの拡張について 2-716
■2.56 OpenFlow の設定 2-717
2.56.1 OpenFlow 機能概要 2-717
2.56.2 注意事項・制限事項 2-718
2.56.3 OpenFlow ポート機能 2-718
2.56.4 OpenFlow テーブル機能 2-719
2.56.5 OpenFlow Channel 機能 2-723
2.56.6 OpenFlow 機能の基本設定 2-726
2.56.7 ProgrammableFlow 対応 2-731
2.56.8 高速転送機能 2-732
2.56.9 Packet-In 抑止機能 2-735
2.56.10 QoS 対応 2-736
2.56.11 ルータ機能との併用 2-736
2.56.12 VLAN タグ制御補助機能 2-737
2.56.13 フローエントリ コンフィグ制御機能 2-738
2.56.14 表示コマンド 2-740
2.56.15 イベントログの設定 2-741
■2.57 キーテレフォンシステム連携機能の設定 2-742
2.57.1 機能概要 2-742
2.57.2 インタフェースの設定 2-742
2.57.3 グローバルアドレス通知機能の設定 2-743
2.57.4 NAT/NAPT の設定 2-745
2.57.5 フィルタの設定 2-746
2.57.6 設定例 2-747
2.57.7 制限事項 2-749
■2.58 設定パラメータの一覧 2-750
3 章 UTM 機能の設定 3-1
■3.1 はじめに 3-1
3.1.1 UTM 概要 3-1

3.1.2 機能一覧 3-1
3.1.3 UTM ライセンス 3-2
■3.2 注意事項 3-3
3.2.1 IPv4 インターネット接続の必要性 3-3
3.2.2 セキュリティ・スキャン対象外のトラフィック 3-3
3.2.3 メモリについて 3-3
3.2.4 UTM と併用できない機能 3-4
3.2.5 UTM が動作しないインタフェース 3-4
3.2.6 内蔵 SSL 証明書について 3-4
3.2.7 最大セッション数に達した場合の動作について 3-4
■3.3 基本設定 3-5
■3.4 脅威検出の通知と情報の取得について 3-7
■3.5 セキュリティ・スキャン 3-8
3.5.1 アンチウイルス（AV） 3-8
3.5.2 不正侵入防止（IPS） 3-10
3.5.3 Web ガード（WG） 3-14
3.5.4 URL フィルタリング（UF） 3-16
■3.6 運用・保守 3-20
3.6.1 イベントログ 3-20
3.6.2 エラーログ 3-20
3.6.3 統計情報 3-21
3.6.4 LED 通知 3-21
■3.7 NetMeister 連携 3-22
3.7.1 アラーム通知 3-22
3.7.2 UTM 脅威レポート通知 3-23
3.7.3 UTM 脅威分析通知 3-23
3.7.4 UTM ライセンス自動設定機能 3-23
■3.8 詳細設定 3-24
3.8.1 UTM サーバとの接続 3-24
3.8.2 UFS キャッシュ 3-24
3.8.3 ライセンス登録・ライセンス延長 3-25
3.8.4 リダイレクトページ設定 3-27
3.8.5 グループ別ポリシーの設定 3-27
3.8.6 ホワイトリスト設定 3-29
3.8.7 通知の設定 3-30
3.8.8 NetMeister 連携 3-31
■3.9 情報の確認 3-32
3.9.1 CLI 表示 3-32
3.9.2 セキュリティログ 3-37
4 章 ゼロタッチプロビジョニング 4-1
■4.1 はじめに 4-1
4.1.1 ゼロタッチプロビジョニング（ZTP）概要 4-1
4.1.2 用語の定義 4-1
4.1.3 適用範囲 4-2
4.1.4 制限事項 4-2
■4.2 設定の流れ 4-3
4.2.1 NetMeister への装置登録 4-3
4.2.2 ZTP の有効化設定 4-3
4.2.3 子機 ZTP の有効化設定 4-4
4.2.4 ZTP 起動後の動作 4-4

4.2.5 ZTP の動作パターン 4-5
4.2.6 ZTP の運用フロー 4-6
■4.3 LED 4-8
4.3.1 MODE スイッチ LED 4-8
4.3.2 VPN、PPP、BAK、の LED 4-9
■4.4 統計情報・メッセージ 4-10
4.4.1 エラーログ 4-10
4.4.2 ZTP 処理中の無条件表示ログ 4-11
5 章 保守・運用 5-1
■5.1 設定の変更 5-1
5.1.1 再起動が必要なコマンド 5-1
5.1.2 操作が必要なコマンド 5-2
5.1.3 インタフェース一括設定 5-3
■5.2 設定の保存 5-5
5.2.1 スタートアップコンフィグ 5-5
5.2.2 デフォルトコンフィグ 5-7
■5.3 設定値の調整 5-9
5.3.1 送受信処理のスケジューリング 5-9
5.3.2 ルートキャッシュ数 5-11
5.3.3 ルートエントリ数 5-12
5.3.4 OSPFv2 ルートエントリ数 5-13
5.3.5 NAT/NAPT エントリ数 5-13
■5.4 LED 状態 5-15
■5.5 IX3315 の注意事項 5-16
5.5.1 10G インタフェースについて 5-16
5.5.2 インタフェース数の調整 5-16
5.5.3 受信パケットの優先制御 5-17
5.5.4 IPsec の注意事項 5-17
5.5.5 QoS クラス数の設定 5-18
5.5.6 レイテンシ制限機能の無効化 5-18
5.5.7 SW-HUB での送信レート制限無効化 5-18
■5.6 起動時コンフィグダウンロード 5-20
5.6.1 動作 5-20
5.6.2 設定 5-22
■5.7 USB メモリの利用 5-23
5.7.1 対応機能 5-23
5.7.2 対応 USB メモリ 5-23
5.7.3 USB メモリのマウント 5-24
5.7.4 USB メモリデバイスの確認 5-25
5.7.5 USB メモリのファイル、ディレクトリ指定方法 5-25
5.7.6 USB メモリが使用可能なコマンド 5-26
5.7.7 かんたん操作ボタン（SEL／ENT ボタン） 5-27
5.7.8 イジェクト機能（USB ボタン機能） 5-28
5.7.9 コピー機能（USB ボタン機能） 5-29
5.7.10 リストア機能（USB ボタン機能） 5-30
5.7.11 コマンドバッチ機能（USB ボタン機能） 5-34
5.7.12 工場出荷状態装置のリストア機能 5-36
5.7.13 USB メモリ認証・セキュリティ 5-38
5.7.14 スケジューラ機能と連携したログの保存 5-40
■5.8 コンフィグ引継ぎ 5-41

5.8.1 IX2004/IX2005 コンフィグ引継ぎ 5-41
6 章 ルーティング状態確認 6-1
■6.1 物理/リンクレイヤの状態確認 6-1
■6.2 IPv4 レイヤの状態確認 6-1
6.2.1 IPv4 レイヤの状態確認 6-1
6.2.2 ARP 情報の確認 6-1
■6.3 IPv6 レイヤの状態確認 6-2
6.3.1 IPv6 レイヤの状態確認 6-2
6.3.2 近隣探索情報の確認 6-2
6.3.3 マルチキャストリスナ情報の確認 6-2
■6.4 ルーティング情報の状態確認 6-3
6.4.1 ルーティングテーブルの確認 6-3
6.4.2 RIPv1/v2 プロトコルの状態確認 6-3
6.4.3 RIPng プロトコルの状態確認 6-4
6.4.4 OSPFv2 プロトコルの状態確認 6-4
6.4.5 OSPFv3 プロトコルの状態確認 6-5
6.4.6 BGP4 プロトコルの状態確認 6-5
■6.5 到達および経路確認 6-6
6.5.1 IPv4 到達および経路確認 6-6
6.5.2 IPv6 到達および経路確認 6-8
■6.6 隣接ノードのアドレス調査方法 6-10
7 章 遠隔設定と監視 7-1
■7.1 telnet を利用した遠隔設定 7-1
■7.2 SSH を利用した遠隔設定 7-2
7.2.1 SSH サーバの設定 7-2
7.2.2 秘密鍵の操作 7-3
7.2.3 仕様 7-4
■7.3 SNMP を利用した監視 7-5
7.3.1 Trap と管理オブジェクト 7-5
7.3.2 SNMP バージョン 7-11
7.3.3 SNMP の設定 7-13
■7.4 ロギング 7-18
7.4.1 ロギングの取得 7-18
7.4.2 ロギングの出力 7-23
7.4.3 ロギングの出力制御 7-24
■7.5 syslog を利用した監視 7-27
8 章 統計情報 8-1
■8.1 統計情報一覧 8-1
■8.2 統計情報詳細 8-4
8.2.1 デバイス関連 8-4
8.2.2 インタフェース関連 8-16
8.2.3 PPP 関連 8-18
8.2.4 ブリッジ関連 8-21
8.2.5 IPv4 関連 8-21
8.2.6 IPv6 関連 8-27
8.2.7 ルーティング関連 8-31
8.2.8 マルチキャスト関連 8-37
8.2.9 トンネル関連 8-38
8.2.10 IKE/IPsec 関連 8-40
8.2.11 QoS 関連 8-47

8.2.12 CRTP 関連 8-49
8.2.13 VLAN 関連 8-50
8.2.14 VRRP 関連 8-51
8.2.15 ネットワークモニタ関連 8-53
8.2.16 アクセスリスト関連 8-55
8.2.17 トラフィックフィルタ関連 8-57
8.2.18 プレフィックスリスト関連 8-58
8.2.19 SNMP 関連 8-58
8.2.20 NTP 関連 8-59
8.2.21 ロギング 8-59
8.2.22 UFS キャッシュ 8-61
8.2.23 SIP-NAT 関連 8-63
8.2.24 IEEE802.1X 関連 8-71
8.2.25 HTTP サーバ関連 8-74
8.2.26 グローバルアドレス通知機能関連 8-75
8.2.27 NGN 機能関連 8-76
8.2.28 ループガード関連機能 8-76
8.2.29 sFlow 関連機能 8-77
8.2.30 IDS 関連機能 8-78
8.2.31 L2TP 関連 8-79
8.2.32 URL リダイレクト関連 8-81
8.2.33 OpenFlow 関連 8-81
8.2.34 URL オフロード関連 8-83
8.2.35 URL フィルタリング関連 8-85
8.2.36 UTM 関連 8-86
9 章 ベンチマークテストのための設定 9-1
■9.1 ARP エントリの固定設定 9-1
■9.2 近隣エントリの固定設定 9-2
10 章 ファームウェアインストール 10-1
■10.1 2 面管理対応版でのバージョンアップ方法 10-1
10.1.1 格納されているプログラムの確認方法 10-1
10.1.2 バージョンアップの手順 10-1
10.1.3 起動ファームウェアの選択 10-4
■10.2 2 面管理対応版以外のバージョンアップ方法 10-4
■10.3 起動時の自動バージョンアップ 10-5
■10.4 正常に立ち上がらない場合のファームウェアインストール 10-8
■10.5 コンフィグファイルのダウンロード方法 10-11
■10.6 工場出荷値設定へのもどし方 10-12
■10.7 ブートできない場合の処置 10-12
11 章 障害発生時の処置ガイドライン 11-1
■11.1 イベント表示による解析 11-1
■11.2 システムロードアベレージ 11-1
11.2.1 システムロードアベレージ 11-1
11.2.2 システムロードアベレージ履歴表示 11-3
■11.3 回線使用率の解析 11-4
■11.4 送受信パケットの解析 11-4
■11.5 装置異常時の解析 11-5
11.5.1 装置電圧状態の確認 11-5
11.5.2 装置温度状態の確認 11-5
11.5.3 装置 FAN 状態の確認 11-6

11.5.4 メモリの状態確認 11-7
11.5.5 バッファの状態確認 11-9
11.5.6 キューの状態確認 11-9
11.5.7 uptime の確認 11-9
11.5.8 エラーログの確認 11-9
11.5.9 プログラムおよびハードウェア情報の確認 11-9
■11.6 テクニカルサポートのための状態収集 11-10
11.6.1 テクニカルサポート送付用情報の確認 11-10
11.6.2 ロギング情報の確認 11-10
■11.7 インタフェースの確認 11-12
11.7.1 PPPoE インタフェースの状態確認 11-12
11.7.2 トンネルインタフェースの確認 11-14
12 章 パケット評価フロー 12-1
■12.1 IPv4 パケット評価 12-1
■12.2 IKEv1/IPsec 送信評価フロー 12-2
■12.3 IKEv1/IPsec 受信評価フロー 12-3
■12.4 IKEv2/IPsec 送信評価フロー 12-4
■12.5 IKEv2/IPsec 受信評価フロー 12-5
■12.6 アクセスリスト評価フロー 12-7
13 章 バージョンアップにおける諸注意 13-1
■13.1 Ver.8.1 コンフィグ 13-1
13.1.1 自動コンフィグ継承 13-1
13.1.2 コンフィグ継承の注意事項 13-1
■13.2 Ver.8.2 コンフィグ 13-2
13.2.1 自動コンフィグ継承 13-2
13.2.2 コンフィグ継承の注意事項 13-2
■13.3 Ver.8.3 コンフィグ 13-2
13.3.1 自動コンフィグ継承 13-2
13.3.2 コンフィグ継承の注意事項 13-2
■13.4 Ver.8.4 コンフィグ 13-3
13.4.1 自動コンフィグ継承 13-3
13.4.2 コンフィグ継承の注意事項 13-3
■13.5 Ver.8.5 コンフィグ 13-3
13.5.1 自動コンフィグ継承 13-3
13.5.2 コンフィグ継承の注意事項 13-3
■13.6 Ver.8.6 コンフィグ 13-3
13.6.1 自動コンフィグ継承 13-3
13.6.2 コンフィグ継承の注意事項 13-3
■13.7 Ver.8.7 コンフィグ 13-4
13.7.1 自動コンフィグ継承 13-4
13.7.2 コンフィグ継承の注意事項 13-4
■13.8 Ver.8.8 コンフィグ 13-4
13.8.1 自動コンフィグ継承 13-4
13.8.2 コンフィグ継承の注意事項 13-4
■13.9 Ver.8.9 コンフィグ 13-5
13.9.1 自動コンフィグ継承 13-5
13.9.2 コンフィグ継承の注意事項 13-5
■13.10 Ver.8.10 コンフィグ 13-5
13.10.1 自動コンフィグ継承 13-5
13.10.2 コンフィグ継承の注意事項 13-5

■13.11 Ver.8.11 コンフィグ 13-6
13.11.1 自動コンフィグ継承 13-6
13.11.2 コンフィグ継承の注意事項 13-6
■13.12 Ver.9.0 コンフィグ 13-6
13.12.1 自動コンフィグ継承 13-6
13.12.2 コンフィグ継承の注意事項 13-6
■13.13 Ver.9.1 コンフィグ 13-6
13.13.1 自動コンフィグ継承 13-6
13.13.2 コンフィグ継承の注意事項 13-6
■13.14 Ver.9.2 コンフィグ 13-7
13.14.1 自動コンフィグ継承 13-7
13.14.2 コンフィグ継承の注意事項 13-7
■13.15 Ver.9.3 コンフィグ 13-8
13.15.1 自動コンフィグ継承 13-8
13.15.2 コンフィグ継承の注意事項 13-8
■13.16 Ver.9.4 コンフィグ 13-9
13.16.1 自動コンフィグ継承 13-9
13.16.2 コンフィグ継承の注意事項 13-9
■13.17 Ver.9.5 コンフィグ 13-9
13.17.1 自動コンフィグ継承 13-9
13.17.2 コンフィグ継承の注意事項 13-9
■13.18 Ver.9.6 コンフィグ 13-10
13.18.1 自動コンフィグ継承 13-10
13.18.2 コンフィグ継承の注意事項 13-10
■13.19 Ver.9.7 コンフィグ 13-11
13.19.1 自動コンフィグ継承 13-11
13.19.2 コンフィグ継承の注意事項 13-11
■13.20 Ver.10.0 コンフィグ 13-11
13.20.1 自動コンフィグ継承 13-11
13.20.2 コンフィグ継承の注意事項 13-11
■13.21 Ver.10.1 コンフィグ 13-12
13.21.1 自動コンフィグ継承 13-12
13.21.2 コンフィグ継承の注意事項 13-12
■13.22 Ver.10.2 コンフィグ 13-12
13.22.1 自動コンフィグ継承 13-12
13.22.2 コンフィグ継承の注意事項 13-12
■13.23 Ver.10.3 コンフィグ 13-13
13.23.1 自動コンフィグ継承 13-13
13.23.2 コンフィグ継承の注意事項 13-13
■13.24 Ver.10.4 コンフィグ 13-13
13.24.1 自動コンフィグ継承 13-13
13.24.2 コンフィグ継承の注意事項 13-13
■13.25 Ver.10.5 コンフィグ 13-14
13.25.1 自動コンフィグ継承 13-14
13.25.2 コンフィグ継承の注意事項 13-14
■13.26 Ver.10.6 コンフィグ 13-14
13.26.1 自動コンフィグ継承 13-14
13.26.2 コンフィグ継承の注意事項 13-14
■13.27 Ver.10.7.17 コンフィグ 13-15
13.27.1 自動コンフィグ継承 13-15

13.27.2 コンフィグ継承の注意事項 13-15
■13.28 Ver.10.7.18 コンフィグ 13-17
13.28.1 自動コンフィグ継承 13-17
13.28.2 コンフィグ継承の注意事項 13-17
■13.29 Ver.10.8 コンフィグ 13-17
13.29.1 自動コンフィグ継承 13-18
13.29.2 コンフィグ継承の注意事項 13-18
■13.30 Ver.10.9 コンフィグ 13-18
13.30.1 自動コンフィグ継承 13-18
13.30.2 コンフィグ継承の注意事項 13-18
14 章 付録 14-1
■14.1 関連 RFC 一覧 14-1
■14.2 ソースアドレスセレクション 14-11
■14.3 ルータ ID セレクション 14-13
■14.4 キューイング処理 14-14
■14.5 インタフェースの特性 14-16
■14.6 インタフェースの MTU 値 14-19
■14.7 TCP-MSS 調整値 14-20
■14.8 ソフトウェア起動プロセス 14-22
■14.9 マルチパス 14-23
■14.10 FIB と RIB 14-24
■14.11 デフォルト開設ポート番号 14-26
■14.12 インタフェース内部構成 14-27
■14.13 ソフトウェア構造 14-30
■14.14 ISDN 発信シーケンス 14-40
■14.15 プライベート MIB 詳細 14-54
■14.16 Trap 詳細 14-71
■14.17 ISDN 切断理由コード一覧 14-75
■14.18 アカウンティングリスト 14-79
■14.19 INS1500 サービスの利用可否 14-81
■14.20 ルータメッセージ一覧 14-82
■14.21 Ver.9.5 以前のソフトウェア諸元値 14-86
■14.22 Ver.9.6 以降 販売終了製品ソフトウェア諸元値 14-98
■14.23 Ver.9.6 以降 販売終了製品ハードウェア仕様 14-110
■14.24 Ver.9.1 以前の Web コンソールの設定 14-112

1章 機能概要

本章では、IX2000/IX3000 シリーズの機能の特徴、諸元および制限事項について示します。

■1.1 IX2000/IX3000 シリーズの機能の特徴

IX2000/IX3000 シリーズの機能の特徴は、次に示すとおりです。

ソフトウェアによる高性能フォワード処理

- 通常パケット高速フォワーディング処理
- フィルタ設定時の高速フォワーディング処理
- NAT/NAPT 使用時の高速フォワーディング処理
- IPsec/トンネル使用時の高速フォワーディング処理
- PPPoE 使用時の高速フォワーディング処理
- VLAN タグ使用時の高速フォワーディング処理
- レイヤ 2 高速フォワーディング処理

ルーティングプロトコル

- スタティックルーティング
- RIP/RIPv2
- RIPng
- OSPFv2
- OSPFv3
- BGP4
- ポリシールーティング

サポートインタフェース

- 2.5GBASE-T
- 5GBASE-T
- 10GBASE-SR/LR（Ver.9.4 以降）
- 10GBASE-T（Ver.9.4 以降）
- 1000BASE-SX/LX（Ver.8.0 以降）
- 1000BASE-T
- 100BASE-TX
- 10BASE-T
- SW-HUB（IX2000/IX3000 シリーズ）
- 専用線 BRI（I.430a）
- ISDN BRI（I.430）
- ISDN PRI
- Serial
- USB（Ver.8.8 以降）

IPv6 対応

- 標準機能サポート
- DHCPv6（Prefix Delegation 機能のみ）
- プロキシ DNS6

IPv4 環境から IPv6 環境への移行期に対応

- IPv4/IPv6 デュアルスタック
- 各種 IP トンネル機能をサポート
- IPv6 over IPv4、IPv6 over IPv6、IPv4 over IPv6、IPv4 over IPv4

ブロードバンド対応

- PPPoE 対応により、複数プロバイダからのプロバイダ選択可能

NGN 対応

- データコネクトサービス対応（Ver.8.6 以降）
- ナンバーゲートサービス対応（Ver.8.7 以降）
- ホームゲートウェイ・オフィスゲートウェイ対応（Ver8.7 以降）

セキュリティ機能

- パケットフィルタによるパケット単位のアクセス制限
- IPsec によるパケット単位の暗号化、認証サポート
- 動的アドレス環境での IPsec のサポート
- 冗長構成での IPsec のサポート
- IEEE802.1X による端末認証
- MAC 認証機能による端末認証（Ver.8.0 以降）
- IDS 機能（Ver.8.10 以降）
- UTM 機能（Ver.10.0 以降）

QoS 制御機能

- クラスベースキュー（CBQ）による優先制御
- プライオリティキューイング（PQ）
- IP precedence（TOS 操作）、Diffserv（DSCP 操作）
- トラフィックシェーピングによる流量制御
- ローレイテンシキューイング（LLQ）
- SW-HUB ポート入力優先制御（Ver.8.3 以降）

信頼性向上

- VRRPv2（IPv4）によるルータ二重化機能
- VRRPv3（IPv6）によるルータ二重化機能（Ver.8.6 以降）
- ネットワークモニタ機能によるエンド・ツー・エンドのパス監視
- ISDN との組み合わせによるネットワーク信頼性向上
- IPsec トンネル冗長化機能

マルチキャスト機能

- IGMP プロキシによる IPv4 マルチキャストフォワーディング
- MLD プロキシによる IPv6 マルチキャストフォワーディング
- PIM-SM（Ver.8.4 以降）

■1.2 諸元

1.2.1 IX2000/IX3000 ソフトウェア仕様

Ver9.0 以前の対応バージョンは明記しません。

分類	機能	備考
サポートプロトコル	IPv4 / IPv6	
VRF 機能	VRF-Lite（Ver9.5 以降）	
ルーティング プロトコル	RIP, RIPv2, RIPng, OSPFv2,OSPFv3, BGP4, ポリシールーティング	
拡張機能（IPv4）	DHCP サーバ DHCP クライアント DHCP リレーエージェント プロキシ DNS ダイナミック DNS NAT/NAPT IPsec パススルー PPTP マルチパススルー（Ver9.3） プロキシ ARP TCP MSS 調整、 URL リダイレクト URL オフロード（Ver9.4 以降）	
拡張機能（IPv6）	DHCPv6 PD サーバ DHCPv6 PD クライアント プロキシ DNS ダイナミック DNS TCP MSS 調整 URL リダイレクト	
リンクレイヤ機能	PPP、マルチリンク PPP PPPoE クライアント PPPoE サーバ（Ver9.7 以降） PPPoE パススルー ポートミラーリング ループガード リンクマネージャ	
ISDN	ISDN 迂回 ISDN 複数対地接続	
ブリッジ機能	トランスペアレントブリッジ ブルータ Integrated Routing and Bridging Ether over IP（EtherIP） Ether over GRE	
トンネル機能	IPv6 over IPv6 IPv6 over IPv4 IPv4 over IPv6 IPv4 over IPv4 GRE L2TPv2（LNS）（Ver8.10 以降） L2TPv2（LAC）（Ver9.7 以降） MAP-E（Ver10.1 以降）	
OpenFlow	OpenFlow スイッチ機能 （OpenFlow Switch Specification 1.3.1）	

分類	機能	備考
IPsec 機能	IPsec(AH, ESP) IKE(メインモード/アグレッシブモード) IKEv2 手動鍵 IPsec 高速処理対応 NAT トラバーサル機能 ダイナミック VPN	
FireWall 機能	IPv4/IPv6 スタティックフィルタ IPv4/IPv6 ダイナミックフィルタ MAC フィルタ IDS URL フィルタリング（ver9.5 以降）	
認証機能	AAA RADIUS クライアント(IPv4) PAP/CHAP IEEE802.1X MAC アドレス認証 Web 認証（Ver9.5 以降）	
QoS 制御機能	ToS/Traffic Class/COS 制御 送信優先制御（PQ, CBQ, LLQ） 帯域制御（トラフィックシェーピング）	
マルチキャスト機能	IPv4 IGMP プロキシ（IGMPv1,v2 のみ） IGMP スヌーピング（IX2215 のみ） IPv6 MLD プロキシ（MLDv1,v2） PIM-SM（IPv4 のみ）	
冗長構成	VRRPv2 VRRPv3 ネットワークモニタ リンクアグリゲーション	
時刻同期機能	SNTP クライアント/サーバ	
保守管理機能	Ping, Traceroute、nslookup telnet サーバ/クライアント SSHv2 サーバ TFTP クライアント SNMPv1/v2c SNMPv3（ver10.4 以降） sFlow syslog 自動バージョンアップ スケジューラ プログラムファイル 2 面管理	
Web コンソール機能	かんたん設定 詳細設定 保守管理 拡張ページ（Ver9.3） WebAPI 機能（Ver9.6）	Ver9.2 以降リニューアル

分類	機能	備考
NetMeister	DDNS 設定（Ver9.7） NetMeister Ver2.0 対応（Ver10.0） NetMeister Ver3.0 対応（Ver10.1） NetMeister Ver4.0 対応（Ver10.2） NetMeister Ver5.0 対応（Ver10.3） NetMeister Ver6.0 対応（Ver10.4） NetMeister Ver7.0 対応（Ver10.5）	
UTM 機能	アンチウィルス（AV） 不正侵入防止（IPS） Web ガード（WG） URL フィルタリング（UF）	

1.2.2 IX2000/IX3000 ソフトウェア諸元

※下記数値は、各機能の諸元を表すものであり、組み合わせによりすべてを満足できない場合があります。
※「仕様」は各装置の推奨最大値，「default」は未設定状態での設定値，「制限値」はソフトウェア上の最大値となります。
※Ver.9.7 以降の販売終了製品、Ver.9.5 以前のバージョンのソフトウェア諸元は付録 21 を参照してください。

1.2.2.1 Ver.9.6 以降のソフトウェア諸元

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
VLAN タギング	VLAN 設定数 （1 物理インタフェース当たり）	32	32	32	32	32	1000 ※1	32	32 1000※2
	VLAN 設定数 （1 ポート VLAN インタフェース当たり）	8	8	8	8	-	8	-	同左
PPP	マルチリンク PPP 最大リンク数	-	-	2	-	-	-	2	同左
PPPoE	PPPoE 同時接続数 （1 物理インタフェース当たり）	8	8	8	8	8	8	-	32
	PPPoE サーバ同時接続数 （装置あたり）	32	32	32	32	32	32	-	32
ISDN	自己電話番号設定数	-	-	2	-	-	-	-	2
	SPID 設定数	-	-	2	-	-	-	-	2
	宛先/発信者番号認証用電話番号設定数 （1 対地当たり）	-	-	8	-	-	-	-	8
	登録対地数	-	-	96	-	-	-	-	同左
	同時接続対地数	-	-	2	-	-	-	-	同左
	無通信時間の設定最大値	-	-	86400	-	-	-	120	86400
データコネクト(NGN)	設定インタフェース数	1	1	1	1	1	1	-	1
	対地数（同時接続数）	16	16	32	32	32	300	-	なし
	対地数（設定数）	16	16	100	100	100	5000	-	なし

（注）PPPoE と VLAN タギングの制限値は両方合わせた値となります。
※1 システム全体で 1000 まで
※2 IX3315 のみ

分類	項目 （Ver.9.6 以降のソフトウェア諸元）		IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
ブリッジ	グループ当たりのインタフェース数		10	10	10	50※1	50※1	200	-	なし
	ブリッジグループ数		255	255	255	255	255	1000	-	同左
	BVI インタフェース数		64	64	64	64	64	64	8	64
	学習アドレスエントリ数		4096	4096	4096	10000	10000	20000	10000※4 20000※5 4096	なし
EtherIP Ether over GRE （ブリッジ機能）	対地数 （ブリッジグループ当たり）		10	10	10	50※1	50※1	300※1	-	Tunnel 数
	対地数 （1 対地当たり 1 ブリッジグループの場合）		10	10	10	50※1	50※1	1000 ※1※2	-	Tunnel 数
IEEE802.1X	サプリカント数 （インタフェース当たり）※3	EAP-MD5 使用時	64	64	64	64	64	128	32	256
		EAP-PEAP/TLS 使用時	32	32	32	32	32	64	32	256
	検疫許可フィルタ ID 設定数 （インタフェース当たり）		3	3	3	3	3	3	-	なし
MAC 認証	収容端末数（インタフェース当たり）		512	512	512	512	512	512	-	なし
Web 認証	認証端末数		2048	2048	2048	2048	2048	2048	-	65535
	認証パスワード設定数		32	32	32	32	32	32	-	なし
リンクマネージャ機能	登録端末数		4096	4096	4096	4096	4096	4096	-	4096
MAP-E	収容回線数（Ver.10.7 まで） 収容回線数(Ver10.8 以降)		1 2	1 2	1 2	1 2	1 2	1 2	- -	1 なし

※1 使用する条件によって、最大値は異なります。Ether over IP の項を参照してください。
※2 フレームのコピーが発生しない条件下の値です。
※3 IEEE802.1X の認証確立時間は主に Supplicant と認証サーバの性能に依存します。特に電子証明書を利用する認証方式でその特性が顕著に現れるため、注意してください。
※4 IX2235、IX2310
※5 IX3315

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
IPv4	ARP エントリ数	2048	2048	2048	2048	2048	2048	2048	65536
	インタフェースアドレス数（セカンダリ）	16	16	16	16	16	16	-	16
	スタティックルート数	1024	1024	1024	2048	2048	10000	-	なし
	ルート数	4096	4096	4096	8192	8192	100000	2048 100000※3	なし
	ルートキャッシュエントリ数	65535	65535	65535	100000	100000	200000	65535※1 100000※2 200000※3	65535 200000※5
	マルチパス数	4	4	4	4	4	4	-	4
	マルチキャストスタティックルート数	64	64	64	64	64	256	-	なし
VRF	VRF 数	32	32	32	32	32	32 512※4	-	なし
NAT	静的 NAT 数	2048	2048	2048	8192	8192	16384	-	なし
	静的 NAT 設定数	256	256	1024	2048	2048	2048	-	なし
	動的 NAT 数	2048	2048	2048	2048	2048	2048	-	なし
	キャッシュサイズ	2048	2048	2048	8192	8192	16384	512	65535
NAPT	キャッシュサイズ	250000	250000	250000	250000	250000	500000	65535	諸元値と同じ
	静的 NAPT/サービス数	255	255	255	255	255	255	-	なし
	アクセスログの保存サイズ	128	128	128	128	128	128	-	128
DHCP サーバ	プロファイル設定数	64	64	64	64	64	64	-	なし
	インタフェース当たりのプロファイル 割り当て数	1	1	1	1	1	1	-	1
	グローバルでのプロファイル割り当て数	4	4	4	4	4	4	-	なし
	アドレスプール設定数 （インタフェース当たり）	1	1	1	1	1	1	-	1
	クライアント設定数 （装置当たり）	512	512	512	512	512	1024	-	65535
	固定クライアント設定数	32	32	32	32	32	32	-	なし
DHCP リレーエージェント	リレー先サーバ数	4	4	4	4	4	4	-	なし

※1 IX2215/IX2207/IX2107/IX2106
※2 IX2235/IX2310
※3 IX3315 のみ
※4 Ver.10.2 以降
※

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
IPv6	スタティックルート設定数	1024	1024	1024	2048	2048	10000	-	なし
	ルート数	2048	2048	2048	4096	4096	20000	-	なし
	リアセンブルバッファサイズ[byte]	65535	65535	65535	65535	65535	65535	65535	65535
	インタフェースアドレス数 （インタフェース当たり）	16	16	16	16	16	16	-	なし
	ルートキャッシュエントリ数	4096	4096	4096	8192	8192	20000	4096 20000 ※2	※3
	マルチパス数	16	16	16	16	16	16	-	16
ICMPv6	メッセージ送出間隔 [msec]	1000	1000	1000	1000	1000	1000	1000	10000
ND （近隣探索）	ルータ通知用プレフィックス数 （装置当たり）	16	16	16	16	16	16	-	なし
	近隣キャッシュ数 【Ver9.6】 （装置当たり）	1024	1024	1024	1024	1024	1024	1024 ※1	8192 ※1
	近隣キャッシュ数 【Ver9.7】 （装置当たり）	16384	16384	16384	16384	16384	16384	1024 ※1	16384 ※1
DHCPv6 サーバ	接続 PD クライアント数	128	128	256	256	256	256	-	なし
DHCPv6 クライアント	PD 再配布プール設定数	128	128	256	256	256	256	-	なし

※1 default,制限値はインタフェース当りの値となります。
※2 IX3315 のみ
※3 機種によって上限が異なります。コマンドリファレンスマニュアルを参照してください。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
RIP/RIPv2	受信ルート数	2048	2048	2048	2048	2048	4096	-	なし
	ネイバ数	512	512	512	512	512	512	-	なし
	同時送信経路数（装置当たり）	1000	1000	1000	1000	1000	1000	-	なし
	設定インタフェース数	64	64	64	64	64	64	-	なし
RIPng	受信ルート数	1000	1000	1000	1000	1000	2048	-	なし
	ネイバ数	64	64	64	64	64	64	-	なし
	同時送信経路数（装置当たり）	1000	1000	1000	1000	1000	1000	-	なし
OSPFv2	プロセス数	1	1	1	1	1	1	-	1
	エリア数	16	16	16	16	16	16	-	なし
	バーチャルリンク数	16	16	16	16	16	16	-	16
	ネットワーク登録数	64	64	64	64	64	64	-	同左
	AS 外部 LSA 数	1000	1000	1000	4000	4000	20000	-	65535
	Type7 LSA（NSSA）数	1000	1000	1000	4000	4000	20000	-	65535
	ルートエントリ数	2048	2048	2048	4096	4096	20000	2048	65535
	ネイバ数	128	128	128	128	128	128	-	なし
OSPFv3	プロセス数	4	4	4	4	4	4	-	なし
	エリア数	16	16	16	16	16	16	-	なし
	ネットワーク登録数	64	64	64	64	64	64	-	同左
	AS 外部 LSA 数	1000	1000	1000	1000	1000	1000	-	1000
	ルートエントリ数	2048	2048	2048	2048	2048	2048	2048	65535
	ネイバ数	64	64	64	64	64	64	-	なし
BGP4	ルートエントリ数（パス数）	4096	4096	4096	8192	8192	100000	-	なし
	ピア数	64	64	64	128	128	1000	-	なし
	ダイナミックネイバ数	64	64	64	128	128	1000	64	65535
ポリシー ルーティング	1 インタフェース当たりの条件数 （参照する access-list の行数）※1	96	96	96	96	96	256	-	なし
VRRPv2 VRRPv3	VRRP グループ設定数 （装置当たり）	32	32	32	32	32	32	-	なし
	参加可能な VRRP ルータ数 （1VR グループ当たり）	4	4	4	4	4	4	-	なし

※1 Ver9.6 以降はアクセスリストの最適化コマンドにより、より多くの条件を指定可能です。詳細はアクセスリストの章を参照してください。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
PIM-SM	ネイバ数	128	128	128	128	128	256	-	なし
	マルチキャストグループ数	128	128	128	128	128	255	-	255
	マルチキャストエントリ数	256	256	256	256	256	256	-	なし
	ダウンストリームインタフェース数	16	16	16	16	16	64	-	なし
IGMP プロキシ	リスナキャッシュ数	32	32	32	32	32	32	-	なし
	アップストリームインタフェース	1	1	1	1	1	1	1	1
	ダウンストリームインタフェース	16※1	16※1	16※1	16※1	16※1	32※1	-	なし
MLD プロキシ	リスナキャッシュ数	32	32	32	32	32	32	-	なし
	アップストリームインタフェース	1	1	1	1	1	1	1	1
	ダウンストリームインタフェース	16※1	16※1	16※1	16※1	16※1	32※1	-	なし
	MLDv2 のソースアドレス数 （マルチキャストグループ当たり）	64	64	64	64	64	64	-	128
ネットワーク モニタ	監視プロファイル（watch-group）の最大数	128	128	128	256	256	5000	-	なし
	1 プロファイル当たりのイベント数	96	96	96	96	96	96	-	なし
	1 プロファイル当たりのアクション数	16	16	16	16	16	16	-	なし
	装置全体のイベント数	128	128	128	256	256	5000	-	なし

※1 ダウンストリーム数は固定ビットレート、2Mbps のストリーミング時の推奨値です。ストリーミング量により最大値が異なります。詳細はマルチキャストの設定の項を参照してください。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）			IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
トンネル	トンネル数		IPv4 over IPv4 IPv4 over IPv6 IPv4 over GRE L2TP	128	128	128	256	256	5000	-	同左
			IPv6 over IPv4 IPv6 over IPv6 IPv6 over GRE	128	128	128	256	256	1024	-	IPv4 overIPv4 トンネル数
	多段トンネル終端段数※3,※5			3	3	3	3	3	3	-	3
IKE/IKEv2※1	対地数	MD5 SHA-1		128	128	128	256	256	5000※2	-	なし
		SHA-256（Ver.8.6 以降）		128	128	128	256	256	5000※2	-	なし
		SHA-384（Ver.8.6 以降） SHA-512（Ver.8.6 以降）		128	128	128	256	256	5000	-	なし
IPsec※1	対地数	MD5 SHA-1	トンネル IPv4 over IPv4 IPv4 over IPv6	128	128	128	256	256	5000※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	128	128	256	256	1024	-	トンネル数
			トランスポート	32	32	32	32	32	64	-	なし
		SHA-256 ※4	トンネル IPv4 over IPv4 IPv4 over IPv6	128	128	128	256	256	5000※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	128	128	256	256	1024	-	トンネル数
			トランスポート	32	32	32	32	32	64	-	なし
		SHA-384 SHA-512 ※4	トンネル IPv4 over IPv4 IPv4 over IPv6	128	128	128	256	256	5000※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	128	[128	256	256	1024	-	トンネル数
			トランスポート	32	32	32	32	32	64	-	なし
	ポリシーに対応するプロポーザル設定数			4	4	4	4	4	4	-	4
	自動鍵マップに対応する自動鍵 プロポーザル設定数			8	8	8	8	8	8	-	8
ダイナミック VPN	接続対地数			128	128	128	256	256	5000	同左※7	同左※7
	接続対地数（BGP 使用時）			64	64	64	128	128	1000	同上※7	同上※7

※1 [ ]内はソフトウェア暗号認証処理の場合の対地数、[ ]なしはハードウェア暗号認証処理の場合の対地数を表します。ソフトウェア暗号認証処理の場合は、IKE の DH グループおよび IPsec の PFS はデフォルト値を使用してください。
※2 トンネル種別が混在する場合の最大数は、以下のトンネル数を 2 として計算してください。
- IPv6 over IPv4, IPv6 over IPv6
- IPv6 over IPv4 IPsec,IPv6 over IPv6 IPsec,EtherIP with IPsec

※3 SHA-256、SHA-384、SHA-512 のソフトウェア暗号認証処理による IPsec トンネルの場合、最大のトンネル段数は 1 となります。
※4 マルチリンク PPP では利用できません。
※5 L2TP では多段トンネルは利用できません。
※6 拠点間の動的接続は諸元値で制限されます。センタでの拠点からの接続数の制限を設定できます。デフォルト値は諸元値となります。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
AAA/Radius	RADIUS サーバ設定数	4	4	4	4	4	4	-	なし
SNMP エージェント	TRAP 送信先マネージャ設定数	8	8	8	8	8	8	-	なし
	コミュニティ登録件数	253	253	253	253	253	253	-	なし
	グループ登録件数 ※5	253	253	253	253	253	253	-	なし
	ユーザ登録件数 ※5	253	253	253	253	253	253	-	なし
プロキシ DNS	ipv4 固定/動的サーバ設定数	各 2	各 2	各 2	各 2	各 2	各 2	-	なし
	ipv4 セッション数 ※1	254	254	254	254	254	254	254	1024
	ipv6 固定/動的サーバ設定数	各 2	各 2	各 2	各 2	各 2	各 2	-	なし
	ipv6 セッション数 ※1	254	254	254	254	254	254	254	1024
DNS リゾルバ	固定/動的サーバ設定数	6	6	6	6	6	6	-	なし
SNTP クライアント	サーバ設定数	3	3	3	3	3	3	-	なし
MAC フィルタ	MAC フィルタ設定数 （インタフェース当たり）	in 3 out 3	in 3 out 3	in 3 out 3	in 3 out 3	in 3 out 3	in 3 out 3	-	なし
MAC アクセスリスト	アクセスリスト名の数	1024	1024	1024	1024	1024	1024	-	なし
	１アクセスリスト当たりの各エントリ数	1024	1024	1024	1024	1024	1024	-	なし
	アクセスリスト総エントリ数	1024	1024	1024	1024	1024	1024	-	なし
	アクセスリストキャッシュ数	8192	8192	8192	8192	8192	8192	8192	65535
トラフィック フィルタ	スタティックフィルタ設定数※2 （インタフェース当たり）	64	64	64	64	64	128	-	なし
	ダイナミックフィルタ設定数 （インタフェース当たり）	in 8 out 8	in 8 out 8	in 8 out 8	in 8 out 8	in 8 out 8	in 8 out 8	-	なし
IP アクセス リスト	アクセスリスト名の数	256	256	256	256	256	5120	-	なし
	１アクセスリスト当たりの各エントリ数	256	256	256	256	256	2048	-	なし
	アクセスリスト総エントリ数	512	512	512	512	512	10000	-	なし
	アクセスリストキャッシュ数	8192	8192	8192	20000	20000	100000	8192 20000※3	65535 100000※3
	ダイナミックアクセスリスト名の数	64	64	64	64	64	256	-	なし
	ダイナミックアクセスリスト １アクセスリスト当たりの各エントリ数	256	256	256	256	256	512	-	なし
	ダイナミックアクセスリスト キャッシュ数	65535 100000 ※4	65535 100000 ※4	65535 100000 ※4	100000	100000	65535 250000 ※4	8192 32768※3	諸元値と同じ
URL フィルタリング	内部 URL フィルタリング数	256	256	256	256	256	256	-	なし
	登録インタフェース数	4	4	4	4	4	4	-	なし

※1 IPv4/IPv6 は問い合わせ元のプロトコルとなります。
※2 最大数まで使用する場合は、UFS キャッシュを併用してください。
※3 IX3315 のみ
※4 Ver.10.3 以降
※5 Ver10.4 以降

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
QoS	ポリシーマップ数 （インタフェース当たり）	in 1 out 1	in 1 out 1	in 1 out 1	in 1 out 1	in 1 out 1	in 1 out 1	-	in 1 out 1
	1 クラス当たりの優先キュー数	8	8	8	8	8	8	8	8
VoIP 関連	RTP ヘッダ圧縮接続数	-	-	16	-	-	-	-	255
	TCP ヘッダ圧縮接続数	-	-	16	-	-	-	-	255
クラスマップ ※1 ※2	クラスマップ数 （Ethernet インタフェースのみ）	16	16	16	32	32	128 512※5	-	128 256※6 5000※4
	クラスマップ数 （データコネクトのみ利用する場合）	16	16	100	100	100	1000	-	128 256※6 5000※4
	クラスマップ数 （上記以外）	-	-	8	-	-	-	-	62
ルートマップ	ルートマップ数	128※3	128※3	128※3	128※3	128※3	256※3	-	なし
プレフィックスリスト	プレフィックスリスト数	1024	1024	1024	1024	1024	1024	-	なし
	1 リストのエントリ数	256	256	256	256	256	1024	-	なし
	総エントリ数	512	512	512	512	512	2048	-	なし
UFS キャッシュ	最大キャッシュ数（IPv4）	40000	40000	40000	40000	60000	200000	8192 100000 ※4	100000 500000 ※4
	最大キャッシュ数（IPv6）	10000	10000	10000	20000	30000	100000	4096 50000 ※4	65535 500000 ※4
	ハッシュサイズ	8192	8192	8192	8192	8192	8192	1024 2048※4	65536
ロギング	ロギングバッファサイズ（byte） （保持件数：1 件 80byte の場合）	8000000 （100000）	8000000 （100000）	8000000 （100000)	8000000 （100000）	40000000 （5000000）	40000000 （5000000）	131072 （1638） 819200 ※7 （10240）	8388608 （104857） 83886080 ※7 （1048576）
syslog	syslog 送信先設定数	8	8	8	8	8	8	-	なし

※1 クラスマップの仕様値は帯域制御を含む場合です。カラーリングのみで利用する場合は制限値まで利用可能です。クラスマップ数に class-local, class-default は含みません。
※2 データコネクト利用時は同時利用されるクラスマップが NGN の同時接続数で制限されるため、仕様値まで設定可能となっています。
※3 最大数まで使用する場合は、UFS キャッシュを併用してください。
※4 IX3315 のみ
※5 Ver.10.2 以降
※6 IX2235,IX2310
※7 IX2310,IX3315

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
URL リダイレクト	端末登録エントリ数	2048	2048	2048	2048	2048	2048	-	2048
	同時セッション受信数	64	64	64	64	64	64	-	64
スケジューラ	最大アクションリスト数	128	128	128	128	128	1024	-	なし
	最大コマンド数	512	512	512	512	512	1024	-	なし
	最大タイマ数	128	128	128	128	128	1024	-	なし
Wake on LAN	端末情報登録数	128	128	128	128	128	256	-	なし
システム	プログラム世代管理数	2	2	2	2	2	2	-	なし
	ログインアカウント設定数	8	8	8	8	8	8	-	50
	ユーザ名長	16	16	16	16	16	16	-	16
	パスワード長	80	80	80	80	80	80	-	249
	telnet 同時ログイン数	4	4	4	4	4	4	-	4
	SSH 同時ログイン数	4	4	4	4	4	4	-	4
	コンソール同時ログイン数	1	1	1	1	1	1	-	1
	enable-config 同時操作数	1	1	1	1	1	1	-	1
	ブートエントリ数	4	4	4	4	4	4	-	4
	格納ファイル数	19	19	19	19	19	19	19	19

分類	項目	IX2106 IX2107 仕様	IX2207 仕様	IX2215 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様	default	制限値
OpenFlow	フローエントリ数※1	8192	8192	8192	8192	8192	65535	-	なし
	フローテーブル数	255	255	255	255	255	255	-	255
	ポート数	128	128	128	128	128	1024	-	なし
	フローキャッシュ数	65535	65535	65535	65535	65535	65535	-	65535
	コントローラ設定数	4	4	4	4	4	4	-	なし
	コントローラ同時接続数	1	1	1	1	1	1	-	1
Ether over GRE（ OpenFlow 機能）	対地数	10	10	10	10	10	100 1024※2	-	なし
UTM	同時セッション数※3	10000	10000	10000	10000	15000	25000	10000	65535

※1 ハッシュ機能の利用が前提です。
※2 フラッディング処理がない場合のみです。
※3 IPv4 と IPv6 を両方合わせたセッション数です。

■1.3 ハードウェア仕様

1.3.1 装置対応バージョン

IX2000/IX3000 シリーズの各装置は、以下のバージョンのソフトウェアから使用可能です。

装置名（IX2000 シリーズ）	ソフトウェア対応バージョン
IX2106	Ver.9.6～
IX2106-Z	Ver.9.6～
IX2107	Ver.10.7～
IX2207	Ver.9.0～
IX2215	Ver.8.8～
IX2215-Z	Ver.8.9～
IX2235	Ver.10.4～
IX2310	Ver.10.5～

装置名（IX3000 シリーズ）	ソフトウェア対応バージョン
IX3315	Ver.9.4～

1.3.2 ハードウェア諸元

分類	項目		IX2106 IX2106-Z 仕様	IX2107 仕様	IX2207 仕様	IX2215 IX2215-Z 仕様	IX2235 仕様	IX2310 仕様	IX3315 仕様
インタフェース	GigaEthernet（10G:RJ45/SFP）		-	-	-	-	-	-	2
	GigaEthernet（10G:RJ45）		-	-	-	-	-	4	-
	GigaEthernet		1	1	2	2	2	-	-
	GigaEthernet（RJ45/SFP）		-	-	-	-	-	-	2
	GigaEthernet（HUB ポート）		4	4	4	8	8	-	8 x 2
	FastEthernet		-	-	-	-	-	-	-
	FastEthernet（HUB ポート）		-	-	-	-	-	-	-
	BRI		-	-	-	1	-	-	-
	T1		-	-	-	-	-	-	-
	USB		-	-	2	1	1	1	1
メモリ	ヒープメモリ		256MB	512MB	256MB	256MB	1GB	4GB※2	4GB※2
	コンフィグメモリ		1024KB	1024KB	1024KB	1024KB	1024KB	1024KB	10MB
電源ユニット			-	-	-	-	-	-	2※1
FAN			-	-	-	-	-	2	2
装置監視	温度	アラーム発生（高温）	76	76	76	76	81	66	66
		アラーム発生（低温）	-1	-1	-1	-1	-1	-1	-1
		アラーム復旧（高温）	70	70	70	70	75	60	60
		アラーム復旧（低温）	5	5	5	5	5	5	5
	監視電圧（正常範囲：±10%）		+1.0V +1.35V +2.5V +3.3V +5V	+1.0V +1.35V +2.5V +3.3V +5V	+1.0V +1.5V +2.5V +3.3V +5V	+1.0V +1.5V +2.5V +3.3V +5V	+1.0V +1.5V +2.5V +3.3V +5V	+2.5V +3.3V +5V +12V	+2.5V +3.3V +5V +12V
LED	PWR		○	○	○	○	○	○	○
	ALM		○	○	○	○	○	○	○
	BUSY/BSY		○	○	○	○	○	○	○
	VPN		○	○	○	○	○	○	○
	PPP		○	○	○	○	○	○	○
	BAK		○	○	○	○	○	○	○
	1		-	-	○	○	○	○	○
	2		-	-	○	○	○	○	○
	3		-	-	○	○	○	○	○
MODE スイッチ, MODE LED			-	○	-	-	○	○	-
暗号/認証処理	DES/3DES/AES(128,192,256) MD5/SHA		○	○	○	○	○	○	○
	SHA2	256	○	○	○	○	○	○	○
		384,512	○	○	○	○	○	○	○

※1：オプション利用時。標準では 1 個。
※2：4GB 中 1GB はシステムで予約済のため、実質 3GB となります。

■1.4 制限事項

IX2000/IX3000 シリーズにおいて、以下の機能制限がありますので、ご注意願います。詳細については、各項目の章も参照してください。

IPv4 プロトコル関連

- セカンダリアドレスで動作する機能については、IPv4 の章を参照してください。
- マルチキャストの制限事項は、マルチキャストの章を参照してください。
- ポリシールーティング、フィルタ、QoS 等でアクセスリストを大量に設定する場合は、Ver9.6 以降推奨です。詳細はアクセスリストの章を参照してください。

IPv6 プロトコル関連

- IPv6 は、MLD プロキシのみで PIM には対応しておりません。

ブリッジ関連

- スパニングツリーはサポートしておりません。
- リンクアグリゲーションはサポートしておりません（対応は SWHUB のみ）。
- Ethernet over IP, Ethernet over GRE に対応しています。

Ethernet over IP 関連

- L2TPv3 は対応しておりません。

IEEE802.1X 関連

- サプリカント機能はサポートしておりません。

RIP、RIPng 関連

- RIPng におけるタイマ値変更はサポートしておりません。

OSPFv2

- 複数プロセスには対応しておりません。
- External の経路は、集約できません。

OSPFv3

- NSSA（Not So Stubby Area）はサポートしておりません。
- バーチャルリンクはサポートしておりません。
- External の経路は、集約できません。

BGP4 関連

- BGP4+には対応しておりません。
- 4 バイト AS には対応しておりません。

トンネル関連（IKE/IPsec, L2TP）

- IKEv1, IKEv2 の制限事項は、IKE の章を参照してください。
- IX3315 で 1000 対地以上設定する場合は、IX3315 の章を参照してください。
- IKEv1 は、preshared-key のみのサポートです。
- IKEv1 では同じピアに対して複数の IKE ポリシーは設定できません。
- SHA2 はハードウェア諸元を参照して、H/W 対応しているものをご利用ください。
- L2TP(LNS)機能は IPsec（IKEv1 かつ IPv4）との併用が必須です。また設定後再起動が必要です。

MAP-E 関連

- MAP-E の章を参照してください。

NAT、NAPT 関連

- ヘアピン NAT は Ver9.3 以降の対応で、1 インタフェースのみ設定できます。

DHCPv6（PD）関連

- Ver.8.7 までは、NTP サーバオプションはサポート対象外です。

DNS 関連

- ローカル DNS サーバ機能（Ver.10.3 以降）による IP アドレスレコードの名前解決応答を除き、DNS サーバ機能はサポートしておりません。
- DNS サーバへの問い合わせは TCP 非対応です。
- Ver.10.2 以前のプロキシ DNS は TCP による問い合わせに対応しておりません。

ネットワークモニタ関連

- 隠蔽できる経路は Static、Connected、ポリシールーティングの経路のみです。
- 多対地で利用する場合は、Ver8.5 以降を推奨します。

VRRP 関連

- VRRPv3 の MIB/Trap は対応しておりません。

QoS 関連

- 入力廃棄のポリシング機能はサポートしておりません。
- イーサネットインタフェース以外では、LLQ はサポートしておりません。

CRTP 関連

- CTCP は、BRI 以外では動作しません。
- CRTP、CTCP は、IPv4 のみの対応です。

ゼロコンフィグ機能

- ゼロコンフィグ専用装置でのみ動作します。

ISDN

- 発信と同時に着信した場合は、34 秒から 3 分程データ通信を確立できない場合があります。
- IX3010,IX3015 において、T1 カードでの ISDN-PRI モードと 4BRI-ST カードとの併用はサポートしておりません。
- INS1500 以外は、PRI 複数ポートの使用はサポートしておりません。

T1

- CTCP はサポートしておりません。
- Channelized は IX3010,IX3015 のみのサポートとなります。

BRI

- BRI デバイスモードで reset コマンドは使用しないでください。インタフェースモードでの reset コマンドを使用してください。

GigaEthernet 関連

- 10Gbps 対応のインタフェースが 10Gbps 以外のリンク速度でリンクアップしたとき、最大スループットが帯域の 90%～97%程度になります（5Gbps などリンク速度が速いほどさらにスループットが低下します)。[理由]Ether デバイスの制限事項により、パケット間の間隔(IPG：Inter-Packet Gap)を通常よりも 32byte 多く挿入しているためです。【回避策】IX3315 で 1Gbps のリンク速度でご利用する場合、GE0,GE1 ポートをお使いください。

NGN 関連

- NGN の章を参照してください。

OpenFlow 関連

- OpenFlow の章を参照してください。

UTM 関連

- UTM の章を参照してください。

ゼロタッチプロビジョニング関連

- ゼロタッチプロビジョニングの章を参照してください。

2章 ルータの設定

本章では、IX2000/IX3000 シリーズを使用するために最低限必要な設定について説明するとともに、より有効に機能させるために必要となる情報を提供いたします。

■2.1基本操作

2.1.1 装置の起動

電源 ON 時に、ハードウェアの自己診断を行い、その後プログラムファイルを起動します。
ハードウェアの診断で Fail と表示された場合は装置交換が必要です。温度異常の場合は設置環境の見直しが必要です。起動時に異常がある場合は show error-log コマンドでも確認可能です。

```
NEC Diagnostic Software
Copyright (c) NEC Corporation 2001-2018. All rights reserved.

%DIAG-INFO: Starting System POST(Power On Self Test)

                    DRAM TEST 1: Pass
                    DRAM TEST 2: Pass
<省略>
          TEMPERATURE STATUS: +51.0degC Pass

NEC Bootstrap Software
Copyright (c) NEC Corporation 2001-2018. All rights reserved.

%BOOT-INFO: Trying flash load, exec-image [（プログラムファイル名）].
Loading: ############（中略）############### [OK]


Starting at 0x20000

Loading configuration file: startup-configuration.
Configuring router subsystems (before IDB proc): done.
Constructing IDB(Interface Database): done.
Configuring router subsystems (after IDB proc): done.
Initializing router subsystems: done.
Starting router subsystems: done.

All router subsystems coming up.
<省略>

Router#
```

ルータが正常に起動するとプロンプトが表示されます。（アカウント登録後は「login:」を表示し、ログイン後にプロンプトが表示されます。）

2.1.2 コマンド入力

本装置は、CLI（Command Line Interface）でコマンドを受け付けます。

```
Router# help
```

コマンドは、表示されているプロンプトに続けて、1 つまたは複数のコマンドをスペースで区切って入力します。パラメータが必要なコマンドも、コマンドとパラメータの間をスペースで区切って入力します。エンターキーで 1 行ずつコマンドを実行します。

入力は、1 バイト文字（半角英数時と記号）で行います。一部のコマンドを除いて、大文字小文字の区別はありません。なお、任意の文字列を入力するコマンドで「"」や「?」は利用できません。

コマンドが間違っている場合には、エラーメッセージを出力します。

```
Router# halp [Enter]
% halp    -- Invalid command.
```

2.1.2.1 補完機能・省略機能

本装置の CLI には補完・省略機能があります。

数文字入力して [TAB] キーを押すことで、完全な形のコマンドに補完することが可能です。

```
選択肢が 1 つしかない場合は、コマンドが補完されます。
Router# en [TAB]
Router# enable-config

選択肢が複数ある場合は、入力可能なコマンドが表示されます。（「?」でも同じ効果）
Router# e [TAB]
   enable-config    -- Enter configuration mode
   exit             -- Exit from the router
```

入力した文字列で始まるコマンド・パラメータが 1 つだけの場合は、省略したまま [Enter] キーで実行することも可能です。

```
Router# en [Enter]
enable-config を実行

Router# sh run [Enter]
show running-config を実行
```

2.1.2.2 その他の便利機能

他にもヘルプやコマンド履歴などの便利な機能があります。

「?」キー	ヘルプを表示します。
「↑」「↓」キー	最近実行したコマンドの履歴を表示
「Ctrl」+「c」キー	コマンドライン上の入力文字をキャンセル
「Ctrl」+「z」キー	オペレーションモードに遷移（後述）
「Ctrl」+「a」キー	行の先頭にジャンプ
「Ctrl」+「e」キー	行の末尾にジャンプ

これ以外にも help コマンドで表示されるショートカットキーに対応しています。

2.1.2.3 表示コマンド

show で始まる表示コマンドを実行すると、画面上に結果を表示します。表示が 1 画面に収まらない場合は、表示の途中で「--More---」を表示します。

```
--More--
```

More が表示されて表示が停止している間、以下の操作が可能です。

スペースキー	次の数行を表示します。
「Enter」キー	1 行ずつ表示します。
「q」キー、「Ctrl」+「c」キー	表示を中止します。
「/」キー	指定文字列を検索します。次の項目で説明します。

大量のログ収集を行う場合、表示が More で停止しないほうが便利です。「terminal length 0」コマンドを設定することで、一度に全て表示させることができます。この設定は、ログアウトまたは「terminal length 22」で元に戻ります。

2.1.2.4 表示内容の検索

画面表示の検索を行うことができます。

（1）「--More--」が表示されている状態で「/」キーを押してください。

```
--More--  「/」を入力
```

（2）「Search:」が表示されるので、検索文字列を入力してください。

```
Search: GigaEthernet「Enter」を入力
```

（3）検索対象文字は反転して表示されます。「--More--」表示されるので、
さらに、次の候補を検索する場合は「n」キーを入力してください。

```
--Skip--
        Tx errors:
          0 single collisions, 0 multiple collisions
          0 excessive collisions, 0 late collisions
          0 deferred transmissions
          0 heart beat errors, 0 underflows
Interface GigaEthernet1.0 is up
  Fundamental MTU is 1500 octets
  Current bandwidth 1G b/s, QoS is disabled
        :
--More--  「n」を入力
```

（4）通常の表示と同様に、「Space」キーで次の 1 画面分表示、「Enter」キーで 1 行表示、「Q」キーで表示を中止することもできます。

検索した文字列は反転して表示されますが、ターミナルの種類によっては、正しく表示されない場合があります。そのような場合は、反転表示抑止の設定を行ってください。

terminal suppress-highlight	反転表示抑止の設定

2.1.3 実行モード

本装置は、モードコンフィグを採用しています。全てのコマンドは、適切なモードに遷移して実行する必要があります。現在のモードはプロンプトでも確認できます。

※以下、プロンプトの「Router」部分は、hostname コマンドで変更されます。設定した文字列に切り替わります。

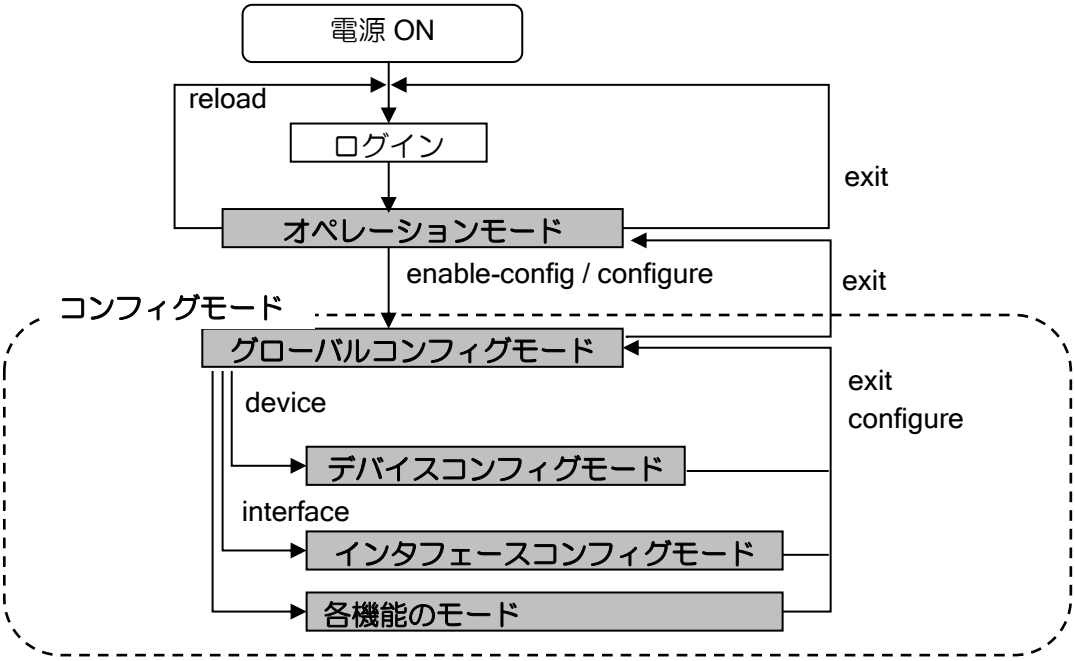
- オペレーションモード
  - ログインして最初に入るモードです。ルータの状態表示や telnet クライアント機能、装置の再起動（reload）コマンドを利用できます。
  - ルータの設定変更を行う場合は、最初に enable-config または configure コマンドを入力してグローバルコンフィグモードに移動してください。
  - プロンプトは「Router# 」です。

- グローバルコンフィグモード（enable-config, configure）
  - ルータの設定変更を行う基本のモードです。ルータ全体に関わる設定、確認等ができます。
  - プロンプトは「Router(config)# 」です。

- デバイスコンフィグモード（device）
  - インタフェース配下のデバイスの設定、確認等を行うためのモードです。
  - プロンプトは「Router(config-GigaEthernet0)# 」のようにデバイス名を表示します。

- インタフェースコンフィグモード（interface）
  - インタフェース単位の設定、確認等を行うためのモードです。
  - プロンプトは「Router(config-GigaEthernet0.0)# 」のようにインタフェース名を表示します。

その他、PPP や DHCP、OSPF、BGP、IKEv2 など、さまざまな機能が専用のモードを用意しています。詳細はそれぞれの機能の説明を参照してください。



すべてのモードは、exit コマンドで抜けることができます。「Ctrl」+「z」キーで、どのモードからでもオペレーションモードに遷移したり、configure コマンドで、どのモードからでもグローバル

コンフィグモードに遷移することも可能です。
このほか特殊なブートモニタモードがあります。スーパーリセットの項目で確認してください。

2.1.3.1 デバイスコンフィグモードとインタフェースコンフィグモード

装置全体で有効な設定はグローバルコンフィグモードで行いますが、装置前面に記載されている GE0, GE1 などへの設定は、以下のモードで行います。

デバイスの設定

GE0 などのデバイスを設定したい場合は、以下のコマンドで該当のデバイスコンフィグモードに移動します。

※GE1 の場合は GigaEthernet1 のように読み替えてください。

device GigaEthernet0 :	装置前面の GE0 ポートのデバイス設定。 speed, duplex, SWHUB のポート VLAN の設定やリンクアグリゲーションの設定などを行います。
device BRI0	装置前面の BRI0 ポートのデバイス設定
device USB0	装置前面の USB0 ポートのデバイス設定

インタフェース設定

GE0 などのデバイス上のインタフェースを設定したい場合は、以下のコマンドで該当のインタフェースコンフィグモードに移動します。

※GE1 の場合は GigaEthernet1.0 のように読み替えてください。SWHUB デバイスは装置によって番号が異なります。

GigaEthernet0.0	GE0 の基本インタフェース設定 GE0 に接続する装置との IPv4, IPv6 設定や DHCP、HTTP などの主に L3 以上の設定
GigaEthernet0.1～	GE0 のサブインタフェース設定 PPPoE やタグ VLAN など、複数設定可能なインタフェースの設定
GigaEthernet2:1.0	ポート VLAN 時の基本インタフェース設定 SW-HUB デバイスでポート VLAN を設定した場合
GigaEthernet2:1.1～	ポート VLAN 時のサブインタフェース設定 SW-HUB デバイスでポート VLAN を設定した場合

「.0」で終わるインタフェースを基本インタフェース、「.1 以上」で終わるインタフェースをサブインタフェースと呼びます。一部設定できるコマンドが異なります。

このほかにも、Loopback や Null、Tunnel、BVI などのインタフェース設定があります。

2.1.4 設定の確認

本装置では、装置起動時に読み込む設定（startup-config）と、現在動作中の設定（running-config）の 2 つの設定があります。他に default-config もありますが、詳細は保守・運用の章を参照してください。

2.1.4.1 running-config の確認

running-config は以下のコマンドで表示することができます。

```
Router(config)# show running-config
! NEC Portable Internetwork Core Operating System Software
! IX Series IXxxxx (magellan-sec) Software, Version X.X.X
      :
```

何も設定していない状態でも、デバイスと基本インタフェースは表示されます。また Web コンソール機能が有効ないくつかの装置では、工場出荷状態で Web コンソール機能に必要な設定が登録されています。詳しくは Web コンソールまたは各機能の章で確認してください。

2.1.4.2 startup-config の確認

startup-config は、以下のコマンドで表示することができます。
設定を保存している場合は、保存したときの running-config が表示されます。

```
Router(config)# show startup-config
Using 1468 out of 1048576 bytes

! NEC Portable Internetwork Core Operating System Software
! IX Series IXxxxx (magellan-sec) Software, Version X.X.X
      :
```

工場出荷時には設定は保存されていないため、以下のように表示します。

```
Router(config)# show startup-config
% Non-volatile configuration memory is not present
```

2.1.5 設定の保存

設定コマンドは全て running-config を変更するコマンドです。変更した設定を確定し、装置の電源を OFF/ON しても設定変更が反映されているようにするには、設定の保存が必要です。

設定の保存はグローバルコンフィグモードで、以下のコマンドで行います。
保存中は装置の電源を落としたり、コマンドを入力したりしないようにしてください。

```
Router(config)# write memory（または copy running-config startup-config）
Building configuration...
% Warning: do NOT enter CNTL/Z while saving to avoid config corruption.
Router(config)#
```

その他の保存コマンドとして、以下も可能です。

```
(1) startup-config を装置内にバックアップする。
Router(config)# copy startup-config <ファイル名>

(2) startup-config を指定の TFTP サーバにバックアップ
Router(config)# copy startup-config <TFTP サーバのアドレス>:<ファイル名>

(3) startup-config を指定の TFTP サーバから取得
Router(config)# copy <TFTP サーバのアドレス>:<ファイル名> startup-config
```

2.1.6 設定の削除

設定の削除はグローバルコンフィグモードで、以下のコマンドで行います。

```
Router(config)# erase startup-config
Are you sure you want to erase the startup-configuration? (Yes or [No]): yes
```

設定を削除しても、running-config は変更されません。
工場出荷状態に戻すためには、コンフィグを削除したあと、そのまま再起動してください。

```
Router(config)# reload
% Warning: do NOT enter CNTL/Z while saving to avoid config corruption.
Notice: The router will be RELOADED. This is to ensure that
        the peripheral devices are properly initialized.
Are you sure you want to reload the router? (Yes or [No]): yes
```

2.1.7 スーパーリセット

パスワードを忘れてしまった場合に、全ての設定を消去することができます。
これには、以下の特殊なモードを使用します。

- ブートモニタモード

ルータとして動作する前のモードです。このモードでは、ルータの立ち上げ設定およびハードウェア情報の確認等ができます。起動時のプログラムファイル読み込み中（「#」表示中）に [Ctrl] + [c] キーを押すことで遷移することができます。

cc コマンドで全ての設定を削除したあと、b コマンドで起動すると工場出荷状態に戻ります。

cc	コンフィグを消去します。
b	装置の起動

2.1.8 Web コンソールの設定

工場出荷状態で Web コンソール機能が有効な装置では、Web コンソールのみでルータの設定変更が可能です。詳細は Web 設定マニュアルを参照してください。工場出荷状態で Web コンソール機能が無効の装置でも、Web コンソール機能を有効化して利用することができます。詳細は Web コンソールの章を参照してください。

2.1.9 設定例

グローバルコンフィグモードでアカウントと装置名を設定し、インタフェースコンフィグモードで GE0 と GE1 に IP アドレスを設定して有効化するときの設定例です（各設定の説明は別途）。
最後に設定を保存しています。

```
【設定例】
Router# enable-config
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# username admin password plain 1 *********
Router(config)# hostname HOST1
HOST1(config)# interface GigaEthernet0.0
HOST1(config-GigaEthernet0.0)# ip address 192.168.0.254/24
HOST1(config-GigaEthernet0.0)# no shutdown
HOST1(config-GigaEthernet0.0)# exit
HOST1(config)# interface GigaEthernet1.0
HOST1(config-GigaEthernet1.0)# ip address 192.168.1.254/24
HOST1(config-GigaEthernet1.0)# no shutdown
HOST1(config-GigaEthernet1.0)# exit
HOST1(config)# write memory
```

以降の章の設定例では、プロンプトは省略して表示します。

■2.2 システムの設定

2.2.1 システムの設定

初期導入時、アカウント、パスワード、システム情報、日付時刻等の設定を行ってください。
工場出荷時にはアカウント設定されておりませんので、認証なくログインされます。
なお、設定完了後は、write memory コマンドで必ず設定情報を保存してください。保存していない設定情報は、装置を再起動すると消えます。

2.2.1.1 アカウントの登録

工場出荷時にはアカウント設定されておりませんので、必要に応じてユーザ名とパスワード、ユーザレベルの登録を行ってください。

username	アカウント設定

パスワードは、hash で Ver8.7 以降、従来よりもセキュリティの高い hash 化を行うことができます。Ver8.7 以降でも既存のコマンドは利用可能ですが、新方式の設定が推奨です。

【設定例】

Ver8.6 までの方式
username USERNAME password plain PASSWORD administrator

Ver8.7 以降の方式
username USERNAME password plain 1 PASSWORD administrator

ユーザレベルは、次の 3 種類が設定できます。

- administrator：全てのコマンドを実行できます。
  プロンプトの末尾は # です。
- operator：ほとんどの show コマンドと、ping などの保守コマンドを実行できます。
  show ikev2 sa のような暗号化の鍵を含む show コマンドは実行できません。
  プロンプトの末尾は $ です。
- monitor：show running-config, show startup-config, show tech-support 以外は
  operator と同様のコマンドを実行できます。
  プロンプトの末尾は % です。

2.2.1.2 システム情報の登録

必要に応じて以下の設定も変更してください。

hostname	ホスト名の設定
timezone	タイムゾーンの設定（Ver4.3 以降）
clock	時刻の設定
show clock	時刻情報の表示

2.2.2 パスワード情報の暗号化表示設定

PPP のパスワード情報等を show コマンド表示する際、暗号化して表示することが可能です。コマンドは以下の通りです。

パスワード情報を設定時、暗号化した情報を設定した場合は、以下のコマンドに関係なく暗号化表示されます。また、一旦暗号化表示された情報は、平文で表示することはできません。暗号化コマンド削除後も平文で表示されず、暗号化表示のままとなります。

service password-encryption	暗号化コマンド

以下のコマンドで設定する情報を暗号化表示することができます。

authentication secret-password	PPP 認証パスワード
ike policy	IKE 事前共有鍵
ipsec manualkey	IPsec 固定鍵
radius host	共有秘密鍵
ip dhcp-client authentication delayed-auth	DHCP クライアント認証設定（Ver.8.3 以降）
startup software-update	自動ファームウェア更新（Ver.8.7 以降）
ikev2 authentication	IKEv2 認証設定（Ver.8.7 以降）
password	ダイナミック DNS パスワード設定（Ver.8.8 以降）（ダイナミック DNS コンフィグモード）
startup config-download	起動時コンフィグダウンロード（Ver.8.8 以降）
usbmem authentication	USB メモリ認証（Ver.9.0 以降）
ngn radius-auth password	RADIUS 認証パスワード（Ver9.5 以降）

※username で設定したパスワードは、暗号化表示設定に関わらず、ハッシュ表示されます。

以下の show コマンドにおいて、情報を暗号化して表示します。

show running-config	ランニングコンフィグレーションの表示
show ppp password	CHAP/PAP パスワードの表示
show ppp control authentication	CHAP/PAP 運用情報の表示
show ike policy	IKE ポリシー設定の表示
show ipsec policy	IPsec ポリシー設定の表示
show tech-support	テクニカルサポート情報の表示

2.2.3 バナー表示設定

Ver.8.10 以降、ログイン時にバナーメッセージを表示することができます。以下の操作で装置に接続した場合に、メッセージを表示します。

- コンソール
- telnet
- SSH

バナーメッセージの表示契機は以下の 3 種類があります。

種別	表示契機
motd	ログイン時、ログインプロンプト表示前
login	ログイン時、ログインプロンプト表示前 （username 設定時のみ表示、SSH ログイン時は表示されません）
exec	ログイン成功直後、コマンドプロンプト表示前

以下のコマンドでバナー設定を行います。

banner	バナー設定

バナー入力は通常のコマンドとは異なり、1 コマンドで表示メッセージを複数行設定できます。行の先頭に‘.’（ピリオド）のみ入力し改行することにより、入力が終了します。途中で入力を中断する場合は[ctrl]+[c]を入力してください。

```
【入力例】
(config)# banner motd
Enter TEXT message. Input line with only '.' to exit (abort with CNTL/C).
**Router-banner**
[motd banner]
.      ＜＜ピリオドを入力し改行で入力終了＞＞

(config)# banner login
Enter TEXT message. Input line with only '.' to exit (abort with CNTL/C).
**Router-banner2**
[login banner]
.      ＜＜ピリオドを入力し改行で入力終了＞＞

(config)# banner exec
Enter TEXT message. Input line with only '.' to exit (abort with CNTL/C).
**Router-banner3**
[exec banner]
.      ＜＜ピリオドを入力し改行で入力終了＞＞

【表示例】
All router subsystems coming up.

**Router-banner**
[motd banner]

**Router-banner2**
[login banner]
login: admin
Password:
NEC Portable Internetwork Core Operating System Software
Copyright Notices:
Copyright (c) NEC Corporation 2001-2013. All rights reserved.
Copyright (c) 1985-1998 OpenROUTE Networks, Inc.
Copyright (c) 1984-1987, 1989 J. Noel Chiappa.
**Router-banner3**
[exec banner]
#
```

■2.3 設定準備

ルータとしての設定を行う前に、次の情報について整理してください。

各インタフェースの物理、リンクレイヤに関する設定情報の決定

- 10BASE-T/100BASE-TX/1000BASE-T
- 10BASE-T/100BASE-TX/1000BASE-T/10GBase-T ポートの Rate/Duplex（固定としたい場合）
- I.430/I.430a
- BRI ポートの HSD128kbps/HSD64kbps/INS64 選択
- T1
- 各種設定の選択
- PPPoE
- ポート VLAN（SW-HUB 使用時のみ）
- 各種パラメータ

トンネル設定に必要な情報の決定

- トンネルもインタフェースの 1 つつに位置づけられています。
  - IPv4 over IPv4
  - IPv6 over IPv4
  - IPv4 over IPv6
  - IPv6 over IPv6
  - GRE
  - IPsec
  - EtherIP
  - L2TPv2（LNS）（Ver.8.10 以降）
  - L2TPv2（LAC）（Ver.9.7 以降）

各インタフェースの設定情報の決定

- IPv4
  - サブネットワーク
  - IP アドレス
    - ✧ DHCP クライアント、PPP によるアドレス自動割当を含みます。
  - NAT の使用、停止
    - ✧ 各種パラメータ
  - NAPT の使用、停止
    - ✧ 各種パラメータ
  - DHCP サーバの使用、停止
    - ✧ 各種パラメータ
  - DHCP リレーエージェントの使用、停止
    - ✧ 各種パラメータ
  - プロキシ DNS、DNS リゾルバの使用、停止
    - ✧ 各種パラメータ

- IPv6
  - リンクのプレフィックス
  - RA の送信、停止
  - ND の各種パラメータ（通常変更の必要はありません）
  - RA 送出時の各種パラメータ（通常変更の必要はありません）
  - DHCPv6 PD の使用、停止
    - 各種パラメータ
  - プロキシ DNS、DNS リゾルバの使用、停止
    - 各種パラメータ

ルーティング関係の設定情報の決定

- スタティックルート
- デスティネーションプレフィックス
- ネクストホップアドレス
- ダイナミックルーティングプロトコル
- 使用ルーティングプロトコルとその設定
- 経路制御
- メトリック（必要な場合のみ）
- ディスタンス（必要な場合のみ）
- 経路再配信に関する情報

■2.4物理、リンクレイヤの設定

物理、リンクレイヤの設定について必要なコマンドは次のとおりです。インタフェースのそれぞれの特性については、付録を参照してください。

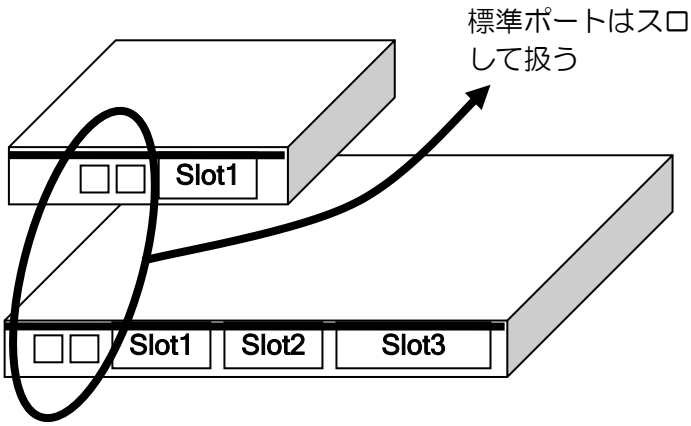
2.4.1 デバイス、インタフェース名表記法

デバイスおよびインタフェース名の表記方法について説明します。

(a) IX3015

IX3015 でのデバイス、インタフェース名表記法は以下のようになります。

スロット番号



IX3015
※IX3015 は slot1 に HUB が実装されているものとして扱います。

デバイス名表記法

[DEVICE][slot]/[port]

- [port] → ポート番号（種別ごとに 0 からカウント）
- [slot] → スロット番号（標準ポートはスロット 0）

【表記例】
IX3015 Slot2 の T1 カードのポート 1：Serial2/0

インタフェース名表記法（一般）

[INTERFACE][slot]/[port].[sub-interface]

- [sub-interface] → サブインタフェース番号（基本インタフェースは 0）

【表記例】
IX2025 の BRI,基本：BRI1/0.0
IX3015 Slot2 の T1 カードのポート 1,基本：Serial2/0.0

インタフェース名表記法（ポート VLAN、チャネライズド T1 のみ）

[INTERFACE][slot]/[port]:[group].[sub-interface]

- チャネライズド時は 0
- チャネライズド、ポート VLAN グループ番号

✧ Serial の場合、チャネルグループ 0 はグループ指定なしの場合と同じになります。Serial1/0.0 と Serial1/0:0.0 は同じインタフェースを表します。コマンドはどちらの形式でも入力可能ですが、表示は Serial1/0.0 の形式となります。

【表記例】
IX3015 Slot3 の T1 カードのチャネルグループ 10：Serial3/0:10.0

(b) その他の装置

(a)以外の装置でのデバイス、インタフェース名表記法は以下のようになります。

デバイス名表記法

[DEVICE][port]

- ポート番号（種別ごとに 0 からカウント）

【表記例】
IX2215 の BRI ポート：BRI0
IX3110 の GE2 ポート：GigaEthernet2

インタフェース名表記法（一般）

[INTERFACE][port].[sub-interface]

- サブインタフェース番号（物理インタフェースは 0）

【表記例】
IX2215 の BRI 基本：BRI0.0
IX3110 の GE2 ポート基本：GigaEthernet2.0

インタフェース名表記法（ポート VLAN）

[INTERFACE][port]:[group].[sub-interface]

- ポート VLAN グループ番号

【表記例】
IX2105 の SW-HUB 部分の VLAN グループ 2：GigaEthernet1:2.0

2.4.2 FastEthernet/GigaEthernet インタフェースの設定

IX2000/IX3000 シリーズでは、FastEthernet（100/10Mbps）インタフェースと GigaEthernet（1000/100/10Mbps、10Gbps（Ver.9.4 以降）、2.5/5Gbps（Ver.10.5 以降））をサポートします。

インタフェースの設定

speed	Rate の設定 （デバイスコンフィグモード）
duplex	Duplex の設定 （デバイスコンフィグモード）
no shutdown	デバイスの有効設定 （デバイスコンフィグモード）
no shutdown	インタフェースの有効設定 （インタフェースコンフィグモード）
auto-connect	PPP 切断時、自動再接続有効設定 PPPoE インタフェースのときに有効 （インタフェースコンフィグモード）
encapsulation	サブインタフェースのカプセル化方式設定 PPP または VLAN タギングの設定で使用 （インタフェースコンフィグモード）
keepalive	デバイス（インタフェース）ダウン検出時間の設定 （デバイスコンフィグモード）
show interfaces	インタフェースの動作状態表示
show devices	デバイスの動作状態表示

2.4.2.1 コネクタ種別の変更

メタル（RJ-45）のコネクタと光ファイバ（SFP）のコネクタをサポートしている機種では、使用するコネクタ種別の設定はポート毎に行います。両方のコネクタを同時に使用することはできません。なお、IX3315 では SFP 指定時の速度の固定設定は未サポートです。

コマンドは以下のとおりです。

connector-type	コネクタ種別の設定 （デバイスコンフィグモード）

【設定例】
IX3110 の GE2,3 を SFP で使用

```
device GigaEthernet2
   connector-type sfp
device GigaEthernet3
   connector-type sfp
```

コネクタ種別が SFP の場合、レーザー出力を行います。レーザー出力を停止する場合、デバイスコンフィグモードで shutdown を行ってください。

【設定例】
IX3110 の GE1 のレーザー出力を停止

```
(config)# device GigaEthernet1
(config- GigaEthernet1)# shutdown
```

2.4.2.2 MDI/MDI-X 指定設定（Ver.8.4 以降）

IX シリーズのイーサネットポートは、MDI/MDI-X 指定設定をサポートしています。

当該ポートは Auto-MDI/MDI-X 機能をサポートしていますが、speed と duplex がともに固定設定である場合、Auto-MDI/MDI-X 機能は無効となります。この時、ポートが MDI/MDI-X のどちらの接続方式で固定動作するかを、デバイスコンフィグモードによって指定できます。

コマンドは以下のとおりです。

mdi-mdix	固定動作時の MDI/MDI-X の設定 （デバイスコンフィグモード）
port mdi-mdix	固定動作時の MDI/MDI-X の設定（指定ポート） （デバイスコンフィグモード） ※SW-HUB ポートでのみ実行可能

【設定例】
IX2025 の FE1/0 の接続方式を MDI に指定

```
(config)# device FastEthernet1/0
(config-FastEthernet1/0)# speed 100
(config-FastEthernet1/0)# duplex full
(config-FastEthernet1/0)# mdi-mdix mdi
```

MDI/MDI-X 指定設定については、以下の注意事項があります。

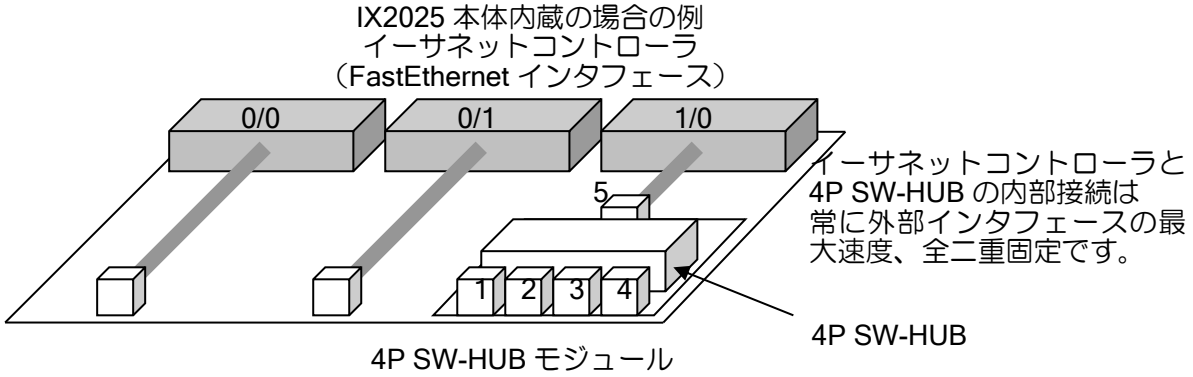
- speed か duplex がオート設定の場合、本機能で指定した値に関わらず、ポートの接続方式は Auto-MDI/MDI-X 機能によって決定されます。
- IX3010 の内蔵ポートは、Auto-MDI/MDI-X 機能と MDI/MDI-X 指定設定をサポートしていません。

2.4.3 FastEthernet/GigaEthernet インタフェース（スイッチング HUB）の設定

スイッチング HUB（SW-HUB）をサポートしている装置の設定方法について説明します。

スイッチング HUB モジュールは、Ethernet インタフェースに繋がる外付けハブと同様に考えることができます。
ポート VLAN では、運用の際にはいくつかの注意が必要です。詳細はポート VLAN の設定の項を参照してください。

内部的には以下の図のようになっています。



2.4.3.1 ポートの設定

特定ポートを指定しない duplex, speed コマンドは、SW-HUB ポート全体に直接作用します。ただし、speed コマンドでインタフェース速度を 10Mbps とした場合でも、Ethernet コントローラと SW-HUB は外部インタフェースの最大速度と同じ速度（IX3315 は 10Gbps、その他のギガ対応装置の場合 1Gbps,それ以外は 100Mbps）で接続されています。このため、QoS や OSPF のコスト計算でインタフェース速度の値を使用する場合には注意が必要です。

設定および表示コマンドは以下のとおりです。

スイッチング HUB の設定

speed	Rate の設定（全ポート） （デバイスコンフィグモード）
duplex	Duplex の設定（全ポート） （デバイスコンフィグモード）
shutdown	デバイスの停止設定（全ポート） （デバイスコンフィグモード）
port speed	Rate の設定（指定ポート） （デバイスコンフィグモード）
port duplex	Duplex の設定（指定ポート） （デバイスコンフィグモード）
port shutdown	デバイスの停止設定（指定ポート） （デバイスコンフィグモード）
show devices	デバイスの動作状態表示

show interfaces の表示例です。

【表示例】

```
Router(config)# show interfaces FastEthernet1/0.0
Interface FastEthernet1/0.0 is administratively down
   Fundamental MTU is 1500 octets
   Current bandwidth 100000000 b/s
   ARP subsystem disabled, physical layer is down, 0 requests queued
   Logical interface statistics:
      0 packets input, 0 bytes
      0 overflows, 0 errors, 0 unknown protos, 0 drops
      0 output requests, 0 bytes
      0 overflows, 0 errors
      1 self-test oks, 1 fails, 0 maintenance fails
   IEEE-802.3 status:
      State is initialized
   FastEthernet statistics:
      Physical address 00:00:4c:64:62:aa
      Full-Duplex, 100Mb/s, 100BaseTX
                          :
                          :
      Extended card is Switching Hub(4 port)
         Hub Port 1 is up
            Full-Duplex, 100Mb/s, 100BaseTX
            0 CRC errors, 0 collisions
         Hub Port 2 is down
            Full-Duplex, 100Mb/s, 100BaseTX
            0 CRC errors, 0 collisions
         Hub Port 3 is down
            Full-Duplex, 100Mb/s, 100BaseTX
            0 CRC errors, 0 collisions
         Hub Port 4 is down
            Full-Duplex, 100Mb/s, 100BaseTX
            0 CRC errors, 0 collisions
```

デバイスコンフィグモードでの speed コマンドによって、以下のように変更されます。

```
【表示例】

1) device - speed 100/auto の場合

    Interface FastEthernet1/0.0
      Current bandwidth 100000000 b/s              ... 100Mbps
                        :
      FastEthernet statistics:
          Full-duplex, 100Mb/s, 100BaseTX          ... 100Mbps
                        :
      Extended card is Switching Hub(4 port)
        Hub Port 1 is up
          Full-duplex, 100Mb/s, 100BaseTX          ... 100Mbps or 10Mbps

2) device - speed 10 の場合

    Interface FastEthernet1/0.0
      Current bandwidth 10000000 b/s               ... 10Mbps
                        :
      FastEthernet statistics:
        Full-duplex,   10Mb/s, 100BaseTX           ... 10Mbps
                        :
      Extended card is Switching Hub(4 port)
        Hub Port 1 is up
          Full-duplex, 10Mb/s, 100BaseTX           ... 10Mbps
```

2.4.3.2 ポートモニタ設定

SW-HUB の指定したポートにて送受信したパケットを、SW-HUB 内の別のポートに送信することができます（Ver.8.3 以降）。

```
【設定例】
ポート 1 で送受信したパケットをポート 4 に送信。

device FastEthernet1/0
  port 1 mirror-port 4 both
  vlan-group 4 port 4

interface FastEthernet1/0.0
  ip address 10.0.0.1/24
  no shutdown
```

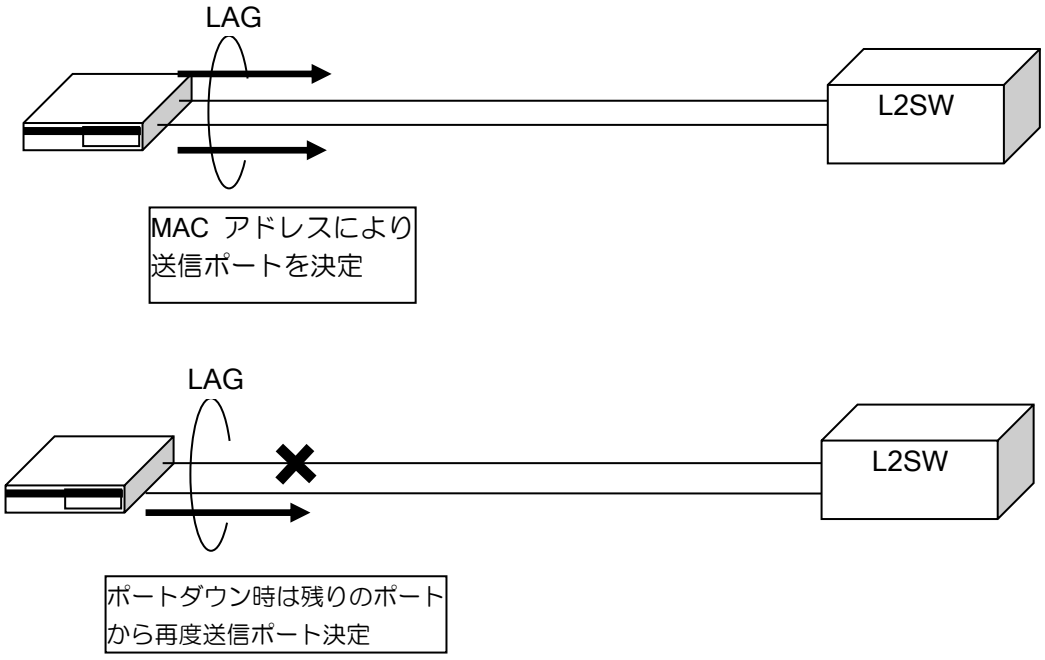
ポートモニタについては、以下の注意事項があります。

- 複数ポートのパケットを 1 つのポートに送信することはできません。
- IX2215 は複数のモニタポートを 1 つのポートに送信可能です（Ver.8.11 以降）。
- 送信先として指定したポートは、通常のパケットの送受信はできません。
- SW-HUB とイーサネットコントローラ間のモニタはできません。
- ミラーポートに設定したポートは、モニタポートとは別な VLAN に設定してください。（ミラーポートとモニタポートが同じ VLAN に設定されている場合、ミラーポートがリンクアップしている際に、モニタポートを含むインタフェース（上記設定例の場合 FastEthernet1/0.0）のダウンが検出できません）
- IX2105, IX2106,IX2107,IX2207,IX2235 では、モニタポートを 1 つのみ設定可能です。
- IX3315 では、SW-HUB 毎にモニタポートを 1 つ設定可能です。また、別 SW-HUB 間のポートモニタ設定はできません。

2.4.3.3 リンクアグリゲーションの設定

IX2000/IX3000 シリーズでは、リンクアグリゲーション機能に対応しています（Ver.8.8 以降）。リンクアグリゲーション機能を使用することにより、複数のポートを 1 つの論理ポートとして利用することが可能となります。

同一リンクアグリゲーショングループ（LAG）に属しているポートに対して、アップしているポートの中から、送信先 MAC アドレス、送信元 MAC アドレスを元に送信ポートを決定します。ポートがダウンした場合、MAC アドレスを元に残りのアップしているポートの中から再度送信ポートを決定します。



リンクアグリゲーション機能には以下の制限があります。

- HUB ポートでのみ使用可能です。
- 静的設定のみ対応しています。LACP 等の動的設定には対応していません。
- リンクアグリゲーション機能を使用して回線の増速（例えば 1G ポートを 2 ポート使用して 2Gbps の通信を行う）はできません。
- モニタポート・ミラーポートとの併用はできません。

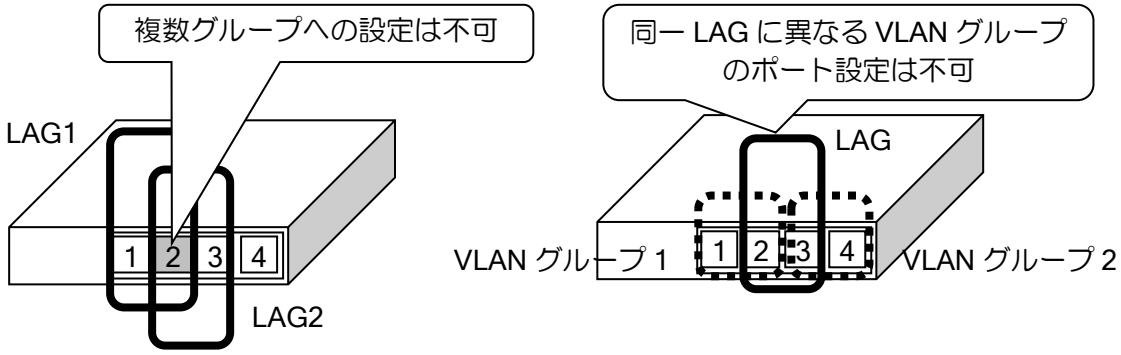
リンクアグリゲーションの設定は以下の通りです。

port link-aggregation	リンクアグリゲーションの有効設定 （デバイスコンフィグモード）

【設定例】
ポート 1 とポート 2 を LAG1 に設定

```
device GigaEthernet1
  port 1 link-aggregation 1
  port 2 link-aggregation 1
```

1 つの LAG に対して、複数の物理ポートを指定することができます。ただし、1 つの物理ポートに対して複数の LAG を設定することはできません。また、ポート VLAN を併用する場合、同一 LAG に指定するポートは全て同一ポート VLAN に指定する必要があります。



2.4.4 BRI インタフェースの設定

IX2000/IX3000 シリーズでは、専用線（I.430a）および ISDN（I.430）をサポートします。IX3015 シリーズでは 4BRI-ST カードを使用することにより、サポートします。

2.4.4.1 専用線の設定

IX2000/IX3000 シリーズでの専用線インタフェースの設定は次のとおりです。

BRI インタフェースの設定

isdn switch-type	交換機種別の設定 （デバイスコンフィグモード）
no shutdown	インタフェースの有効設定 （インタフェースコンフィグモード）
show interfaces	動作状態の表示

【設定例】

```
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix2010-1
   authentication password ix2010-1 ix2010-1
   authentication password ix2010-2 ix2010-2
device BRI1/0
   isdn switch-type hsd128k
interface FastEthernet0/0.0
   ip address 172.18.1.1/24
   no shutdown
interface BRI1/0.0
   ppp binding bri1/0.0
   ip unnumbered FastEthernet0/0.0
   no shutdown
```

2.4.4.2 ISDN の設定

IX2000/IX3000 シリーズでの ISDN インタフェース（オプション機能）の設定は次のとおりです。

なお、IX2000/IX3000 シリーズの ISDN インタフェースについては、バックアップ回線用としての使用を考慮しているため、ISDN 事業者の種々のサービスに対応できない場合がありますのでご注意ください。

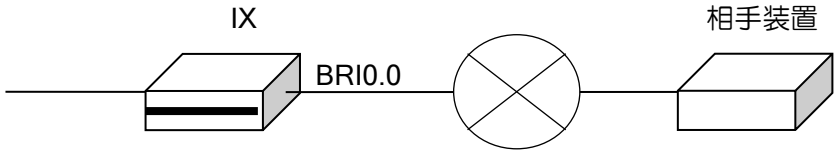
デバイスコンフィグモードでは以下の設定を行います。

その他の設定は、インタフェースコンフィグモードで行います。インタフェースコンフィグモードの設定はダイアラの設定の項を参照してください。

IX3015 の場合は、Dialer インタフェースのみ使用可能です。

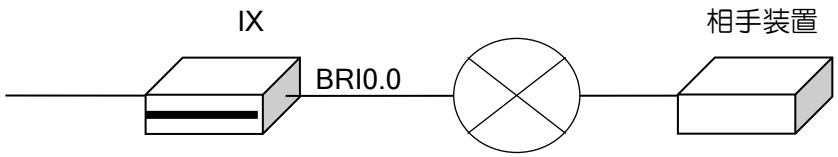
isdn switch-type	交換機種別の設定 （デバイスコンフィグモード）
isdn answer1	着信電話番号の登録 （デバイスコンフィグモード）
isdn answer2	着信電話番号の登録 （デバイスコンフィグモード）

発信時の answer1/answer2 動作



address 宛てに発呼しますが、その際に自分の電話番号として answer1 を使用して発呼します。
answer2 は使用しません。

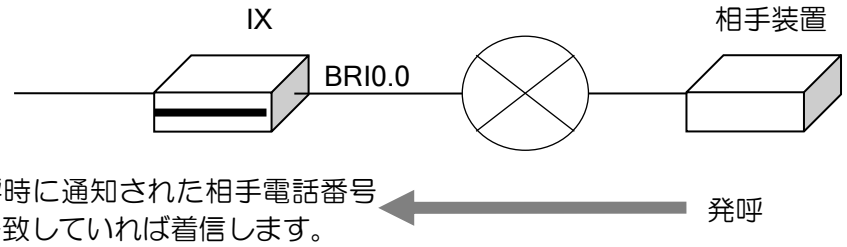
着信時の answer1/answer2 動作



answer1 または answer2
に対する発呼のみ着信します。
SETUP に番号が設定されていない場合は、
answer2 は設定しないでください。

※destination が設定されている相手からの着信しか受け付けません。

着信時の caller 動作



※発信者番号認証はサブアドレスまで含めた番号が対象となります。サブアドレスを省略し、電話番号のみでの認証はできません。
※destination が設定されている相手からの着信しか受け付けません。

ISDN（I.430）の設定例

```
【設定例】
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix2010-1
   authentication password ix2010-1 ix2010-1
   authentication password ix2010-2 ix2010-2
device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567
interface FastEthernet0/0.0
   ip address 172.18.1.1/24
   no shutdown
interface BRI1/0.0
   encapsulation ppp
   no auto-connect
   dialer string 81-123-4568
   ppp binding bri1/0.0
   ip unnumbered FastEthernet0/0.0
   no shutdown
```

- 代表電話番号

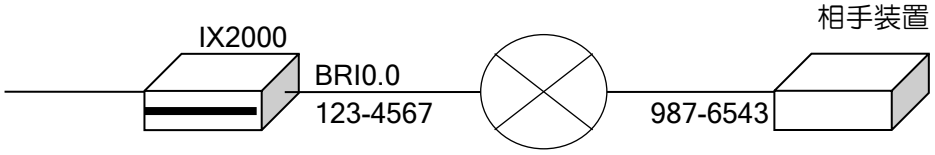
複数の ISDN 回線に対して、代表電話番号を契約することにより、その番号に対して複数の着呼が可能となります。

```
【設定例】

device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-111-0001          ：代表番号
device BRI1/1
   isdn switch-type ins64
   isdn answer1 81-111-0001          ：代表番号
device BRI1/2
   isdn switch-type ins64
   isdn answer1 81-111-0001          ：代表番号
device BRI1/3
   isdn switch-type ins64
   isdn answer1 81-111-0001          ：代表番号
```

2.4.4.3 サポートしていない BRI 構成

以下の BRI 構成は、サポートしていません。

(1)destination を設定していない ISDN インタフェース



【未サポートの設定例】

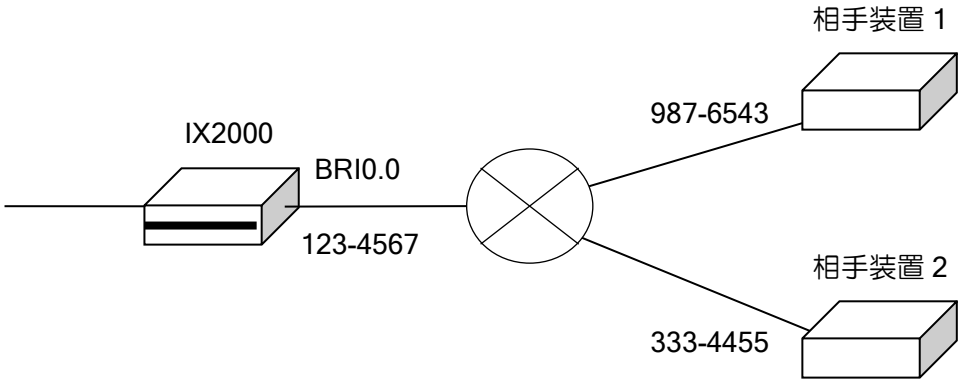
```
device BRI0
   isdn switch-type ins64
   isdn answer1 123-4567

interface BRI0.0
   no auto-connect
   ppp binding bri0.0
   ip unnumbered FastEthernet0.0
   no shutdown
```

次のように、isdn address,destination を設定してください。

【サポート可能な設定例】

```
device BRI0
   isdn switch-type ins64
   isdn answer1 123-4567
   isdn address backup1 987-6543

interface BRI0.0
   no auto-connect
   destination backup1
   ppp binding bri0.0
   ip unnumbered FastEthernet0.0
   no shutdown
```

(2)複数装置（対地）への ISDN 発着信



【未サポートの設定例】

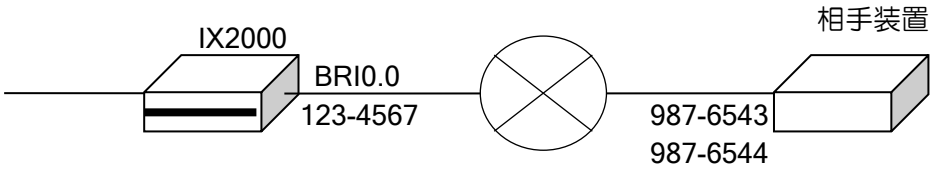
```
device BRI0
   isdn switch-type ins64
   isdn answer1 123-4567
   isdn address backup1 987-6543
   isdn address backup1 333-4455

interface BRI0.0
   no auto-connect
   destination backup1
   ppp binding bri0.0
   ip unnumbered FastEthernet0.0
   no shutdown
```

次のように、1 つの装置へのみ発着信を行うように設定してください。

【サポート可能な設定例】

```
device BRI0
   isdn switch-type ins64
   isdn answer1 123-4567
   isdn address backup1 987-6543


interface BRI0.0
   no auto-connect
   destination backup1
   ppp binding bri0.0
   ip unnumbered FastEthernet0.0
   no shutdown
```

(3)isdn caller と isdn address の組み合わせが合わない ISDN 構成



【未サポートの設定例】

```
device BRI0
   isdn switch-type ins64
   isdn answer1 123-4567
   isdn address backup1 987-6543
   isdn address backup1 987-6544
   isdn caller 987-6543

interface BRI0.0
   no auto-connect
   destination backup1
   ppp binding bri0.0
   ip unnumbered FastEthernet0.0
   no shutdown
```

isdn caller を設定する際は、次のように isdn address に設定した全ての電話番号を設定してください。また、isdn address に設定されていない電話番号を isdn caller に設定しないでください。

【サポート可能な設定例】

```
device BRI0
   isdn switch-type ins64
   isdn answer1 123-4567
   isdn address backup1 987-6543
   isdn address backup1 987-6544
   isdn caller 987-6543
   isdn caller 987-6544

interface BRI0.0
   no auto-connect
   destination backup1
   ppp binding bri0.0
   ip unnumbered FastEthernet0.0
   no shutdown
```

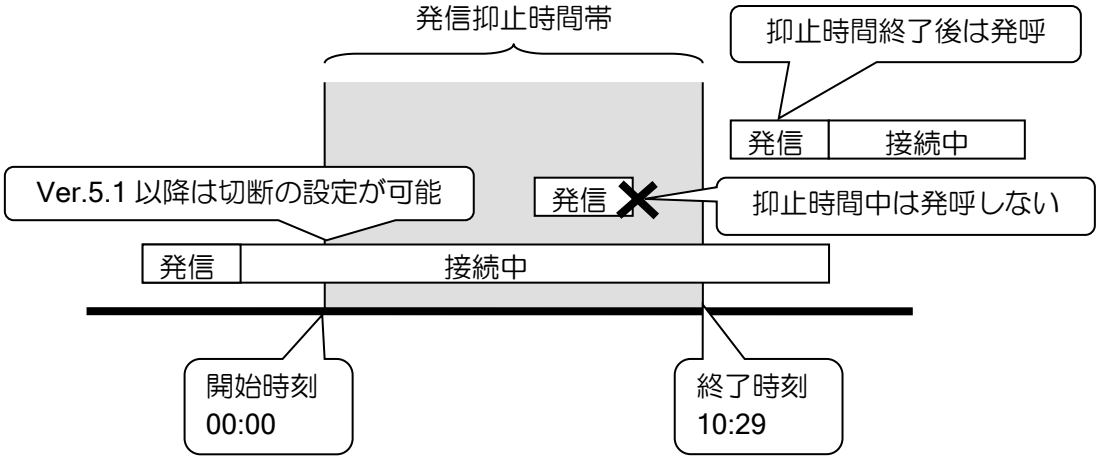
2.4.4.4 自動発信抑止機能

指定された時間帯に、自動発信を抑止する機能を設定します。

dialer restraint one-shot	自動発信抑止（指定時間帯）の設定
dialer restraint week	自動発信抑止（毎週指定曜日/時間帯）の設定
dialer restraint day	自動発信抑止（毎日指定時間帯）の設定

設定した時間帯には、自動発信を行いません。ただし、オンデマンド帯域制御を使用している場合、2B 目以降の発信は抑止されません。Ver.5.1 以降は、自装置から発呼した接続中の回線については、切断するかどうかの設定が可能です。設定方法には、特定した日の特定の時間帯、毎日特定の時間帯、毎週特定の時間帯の 3 種類あります。1 つのインタフェースに対して、複数の条件を設定することができます。複数の条件を設定した場合は、条件のいずれかが抑止時間帯であれば、発信を抑止します。

no dod-restraint コマンドは、全ての自動発信抑止設定を無効にします。

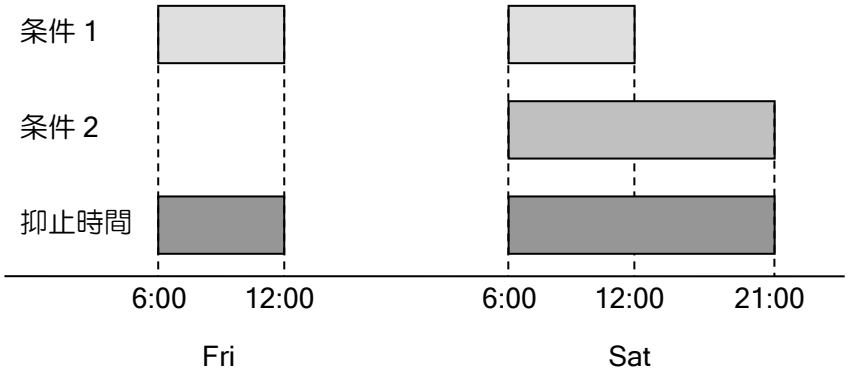


【設定例】

```
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix2010-1
   authentication password ix2010-1 ix2010-1
```

```
   authentication password ix2010-2 ix2010-2
device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567
interface FastEthernet0/0.0
   ip address 172.18.1.1/24
   no shutdown
interface BRI1/0.0
   encapsulation ppp
   no auto-connect
   dialer restraint day start 0 0 end 10 29
   dialer string 81-123-4568
   ppp binding bri1/0.0
   ip unnumbered FastEthernet0/0.0
   no shutdown
```

複数条件設定時の動作例




```
【設定例】
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix2010-1
   authentication password ix2010-1 ix2010-1
   authentication password ix2010-2 ix2010-2
device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567
interface FastEthernet0/0.0
   ip address 172.18.1.1/24
   no shutdown
interface BRI1/0.0
   encapsulation ppp
   no auto-connect
   dialer restraint week start sat 6 0 end sat 21 0
   dialer restraint day start 6 0 end 12 0
   dialer string 81-123-4568
   ppp binding bri0.0
   ip unnumbered FastEthernet0/0.0
   no shutdown
```

2.4.4.5 4BRI-ST の動作

(a) デバイスの使用順序

最も若番のデバイスから、ラウンドロビンで使用します。以下の場合、次のデバイスを使用します。

- B チャネルに空きが無い場合
- 発呼に失敗した場合

(b)クロックマスタ回線の切り替え

4BRI-ST カードでは、クロックマスタ回線から供給されるクロックを全てのポートで使用します。クロックマスタ回線は、以下の条件で切り替えが行われます。コマンドによる切り替えはできません。

- 装置起動直後のクロックマスタ回線は、ポート 0 になります。
- 最初に up したポートにクロックマスタ回線が切替わります。
- 複数ポートが同時に up した場合は、元のクロックマスタ回線に最も近い老番ポートに切替わります。
- クロックマスタ回線が down した場合は、最も近い老番ポートに切替わります。
- クロックマスタ回線が down しても、他に up しているポートが存在しない場合、クロックマスタ回線は切替わりません。
- ポート 3 がクロックマスタ回線の時に切替が発生した場合は、ポート 0 にローテーションします。

2.4.5 Serial インタフェースの設定

IX2000/IX3000 シリーズでは、以下の Serial インタフェースをサポートしています。

サポートする Serial インタフェースの種類

T1	

Serial インタフェースの設定は次のとおりです。

Serial インタフェースの設定

t1	T1 の設定
no shutdown	インタフェースの有効設定 （インタフェースコンフィグモード）
keepalive	デバイス（インタフェース）ダウン検出時間の設定 （デバイスコンフィグモード）
down-notify	デバイス（インタフェース）ダウン検出時間の設定 （グローバルコンフィグモード）
show interfaces	動作状態の表示

2.4.5.1 T1 の設定

IX2000/IX3000 シリーズでの T1 インタフェースの設定は次のとおりです。

t1 clock source	クロック供給モードの設定※ （Ver.5.0 以降客先限定リリース）
t1 fdl	Facility Data Link（FDL）の設定 （デバイスコンフィグモード）

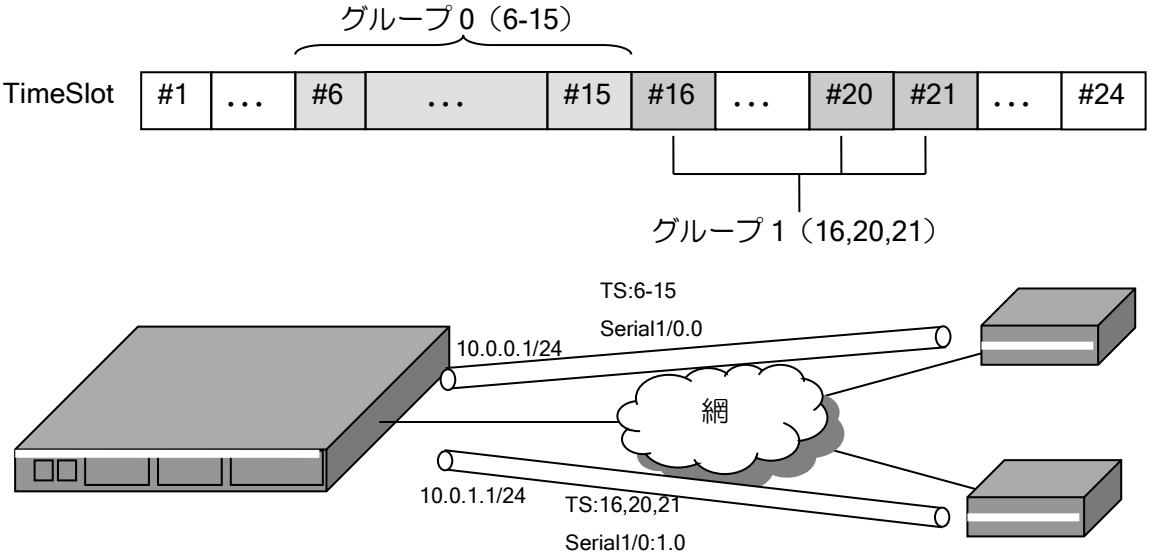
t1 linecode	T1 符号化タイプの設定 （デバイスコンフィグモード）
t1 lbo	CSU/DSU 受信装置の期待信号範囲の設定 （デバイスコンフィグモード）
t1 loopback	ループバックの設定 （デバイスコンフィグモード）
t1 timeslots	タイムスロットの設定 （デバイスコンフィグモード）
t1 channel-group	チャネライズドのグループ設定 （デバイスコンフィグモード）
t1 di-group	DI ポートの設定 （デバイスコンフィグモード）
no shutdown	インタフェースの有効設定 （インタフェースコンフィグモード）
show interfaces	動作状態の表示

※クロック供給モードの internal 指定は、ハードウェアが internal 指定に対応している必要があります。そのハードウェアが internal 対応しているかどうかは、show interfaces コマンドにて確認することができます（show devices でも可能）。

```
【表示例】
Router(config)# show interfaces Serial0
      :
T1 status:
   Current clock source is line(only)        ←(only)の場合、そのハードウェアは
                                               対応されておりません。
```

(a)チャネライズド T1 ポートの設定

T1 カードを使用することにより、チャネライズドポートとして使用できます。設定はグループと使用するタイムスロットを指定します。同一グループには、不連続なタイムスロットを割り当てることもできます。



【設定例】

グループ 0 にタイムスロット 6-15 の 10 チャネル分を割り当て
グループ 1 にタイムスロット 16,20,21 の 3 チャネル分を割り当て

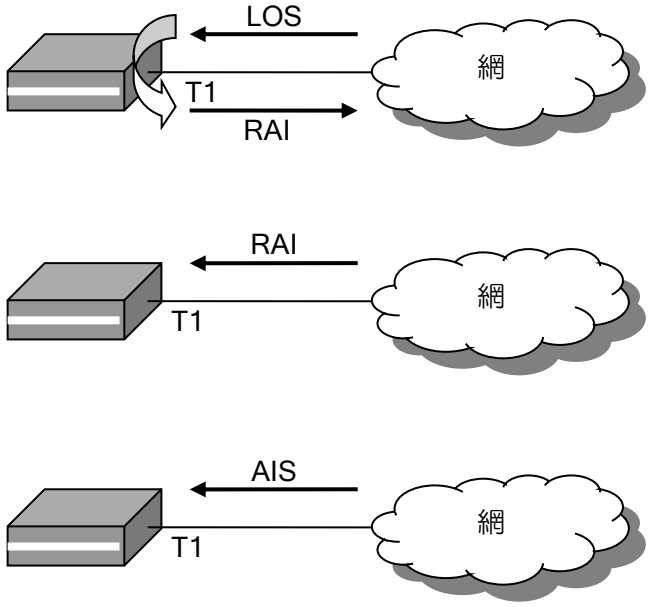
```
device Serial1/0
   t1 channel-group 0 timeslots 6-15
   t1 channel-group 1 timeslots 16,20,21

interface Serial1/0.0
   encapsulation ppp
   ppp binding profile1
   ip address 10.0.0.1/24
   no shutdown

interface Serial1/0:1.0
   encapsulation ppp
   ppp binding profile2
   ip address 10.0.1.1/24
   no shutdown
```

(d)物理リンク警報処理

IX2000/IX3000 シリーズの T1 インタフェースでは、物理リンク警報は次のように処理されます。

- IX3015（T1 カード）の場合

受信警報の種別	動作
LOS 受信時	RAI を網に送信
RAI 受信時	受信のみ
AIS 受信時	受信のみ



2.4.5.2 ISDN-PRI の設定

IX3000 シリーズでは、T1 を使用することにより、PRI（Primary Rate Interface）を使用することができます。

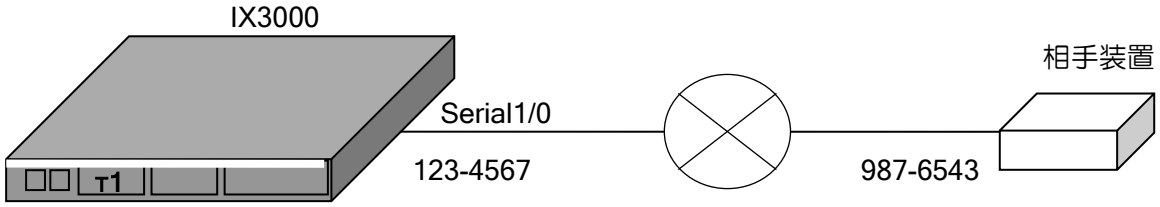
デバイスコンフィグモードでは以下の設定を行います。

t1 pri-group	ISDN-PRI 有効 （デバイスコンフィグモード）
isdn bchan-number-order	B チャンネル選択方式の設定 （デバイスコンフィグモード）
isdn switch-type	交換機種別の設定 （デバイスコンフィグモード）
isdn answer1	着信電話番号の登録 （デバイスコンフィグモード）
isdn answer2	着信電話番号の登録 （デバイスコンフィグモード）

※マルチリンク PPP は 46B までのサポートとなります。

その他の設定はインタフェースコンフィグモードで行います。PRI の場合は、インタフェースの設定は Dialer インタフェースのみ使用可能です。SerialX/0.0 のインタフェースは使用できません。不特定着信設定については Dialer0 のみ設定可能です。

それ以外については、BRI の場合の設定と同様になります。設定方法については、BRI の設定、ダイアラの設定の項を参照してください。



【設定例】老番の空チャンネルから使用

```
ppp profile pri-01
   authentication request chap-pap
   authentication myname IX1
   authentication password IX1 pri-01
   authentication password IX2 pri-01

device Serial1/0
   t1 pri-group
   isdn switch-type ins1500
   isdn answer1 123-4567
   isdn bchan-number-order descending

interface Dialer0
   encapsulation ppp
   no auto-connect
   dialer string 987-6543
   ppp binding pri-01
   ip address 10.0.0.1/30
   no shutdown
```

- ISDN-PRI の複数ポート対応について
  INS1500 の場合のみ複数ポートに対応しています。NI-PRI では 1 ポートのみ使用可能となります。

2.4.6 Loopback インタフェースの設定

IX2000/IX3000 シリーズでは、ループバックインタフェースをサポートしています。

ループバックインタフェースは内部的なインタフェースであり、直接外部には見えないインタフェースです。絶対に落ちないインタフェースとして利用することができます。
どのインタフェースにも属さない IPv4 アドレスまたは IPv6 アドレスを付加し、他のインタフェースから参照（unnumbered）させるなどの利用方法があります。
Loopback インタフェースと Null インタフェースの相違点は、Loopback インタフェースに対してパケットを送出した場合、自分自身に対してパケットが再帰的にもどってきますが、Null インタフェースはそのパケットを廃棄します。この動作以外は、同等の動作が可能です。
なお、Loopback インタフェースには Loopback0.0 と Loopback1.0 の 2 つのインタフェースが用意されています。これらのインタフェースは IPv6 のスコープゾーンの扱いに関して違いがありますので、IPv6 の章のスコープゾーンとインタフェースの項を参照してください。

2.4.7 Null インタフェースの設定

IX2000/IX3000 シリーズでは、Null インタフェースをサポートしています。
Null インタフェースは内部的なインタフェースであり、直接外部には見えないインタフェースです。絶対に落ちないインタフェースとして利用することができます。
Null インタフェースの利用方法としては、正常にルーティングできないパケットについて、スタティックルートを Null インタフェースに設定しておくことで、不要なパケットを明示的に廃棄することができます。
Loopback インタフェースと Null インタフェースの相違点は、Loopback インタフェースに対してパケットを送出した場合、自分自身に対してパケットが再帰的にもどってきますが、Null インタフェースはそのパケットを廃棄します。この動作以外は、同等の動作が可能です。
Null0.0 は、設定の有無に関わらずインタフェースが up となります。そのため、何も設定せずに使用することができます。

2.4.8 トンネルインタフェースの設定

IX2000/IX3000 シリーズでは、種々のトンネル機能をサポートしています。詳細はトンネルの節にて説明します。トンネルも、通常のインタフェースの 1 つとして振舞います。

■2.5 ループガード機能

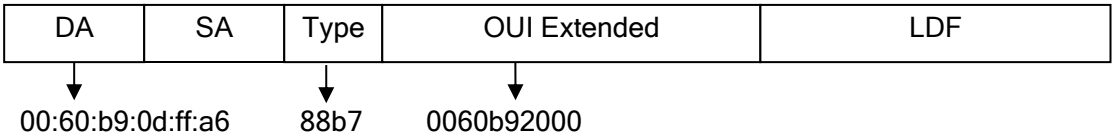
IX2215（Ver.8.9 以降）,IX3315（Ver.9.4 以降）,IX2106/IX2207(Ver.9.6 以降),IX2235,IX2107 の SW-HUB ではループガード機能をサポートしています。

ループを検出したポートを自動的に shutdown することが可能で、ケーブルの接続誤りによるブロードキャストストームなどの被害を最小限にすることができます。

2.5.1 ループガード機能の概要

ループガード機能は、SW-HUB 上に設定したインタフェースから、以下の IX ルータ専用の特殊フレームをフラッディングして送信します。このフレームが折り返されて SW-HUB の別ポートで受信した場合にループと判定し、受信したポートを自動的に shutdown することができます（shutdown せず、検出のみとすることも可能です）。

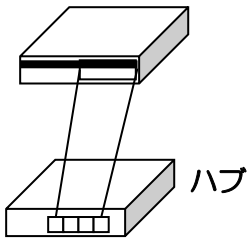
ループ検出用フレーム



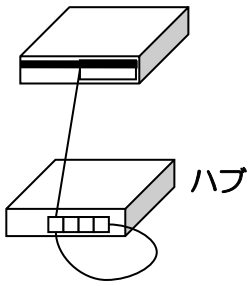
2.5.2 ループになる構成

以下のような接続を行った場合にループ構成となります。

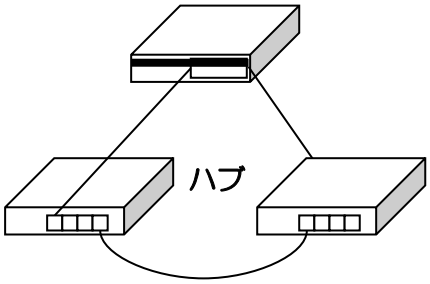
（1）ハブとの接続でループ



（2）ハブでループ



（3）複数のハブとの接続でループ



いずれのケースも対応可能ですが、（2）のケースでは、IX ルータがポートを shutdown してもハブのループ自体は解消しません。またハブやスイッチによっては、輻輳時に稀にループ検知フレームを受信しなくなり、ループを検出できなくなることがあります。

2.5.3 ループガード機能の設定

ループガード機能の設定は以下のコマンドで行います。

loop-detection enable	ループガード機能の有効化
loop-detection action	ループ検出時の動作を設定します。 デフォルトでポートを shutdown します。
loop-detection interval-time	ループ検出用フレームの送信間隔を指定します。
loop-detection threshold	ループと判定するフレーム数を設定します。 デフォルトは 1 で、通常は変更不要です。
loop-detection window-size	ループ検出用フレームの ID 保持数を設定します。 通常は変更不要です。
loop-detection restore	ループ検出状態を強制的に解除します。
show loop-detection information	ループガード機能の状態を表示します。

- threshold と window-size について

ループ検出用フレームは送信ごとに異なる ID を付与しています。フレームの受信数は ID ごとに管理しており、応答を待つ ID の保持数は window-size となります。受信フレームの合計数が threshold を越えるとループと検出します。

このため、threshold 5, window-size 4, interval-time 3 の場合、ループ検知フレームを 12 秒以内に 5 個以上受信すると、ループと検出されます。通常は 1 つでも受信したらループと判断すべきなので、threshold と window-size は変更する必要がありません。

- タグ VLAN 対応

サブインタフェースでループガード機能を有効にした場合は、ループ検知フレームにそのインタフェースの VLAN タグが付きます。

- ポート VLAN を利用しない場合の設定例

【設定例】

```
interface GigaEthernet2.0
  ip address 192.168.0.1/24
  loop-detection enable
  no shutdown
```

- ポート VLAN を利用した場合の設定例

```
【設定例】

device GigaEthernet2
   vlan-group 1 port 1 2 3 4
   vlan-group 2 port 5 6 7 8

interface GigaEthernet2.1:0
   ip address 192.168.1.1/24
   loop-detection enable
   no shutdown

interface GigaEthernet2.2:0
   ip address 192.168.2.1/24
   loop-detection enable
   no shutdown
```

いずれの場合も構成変更でループを解消した場合には、loop-detection restore コマンドでループ検出状態を解除してください。ループ状態が解消されたことを自動検出しないためです。

■2.6 端末認証の設定

UNIVERGE IX2000/IX3000 シリーズでは、以下の端末認証機能をサポートしています。

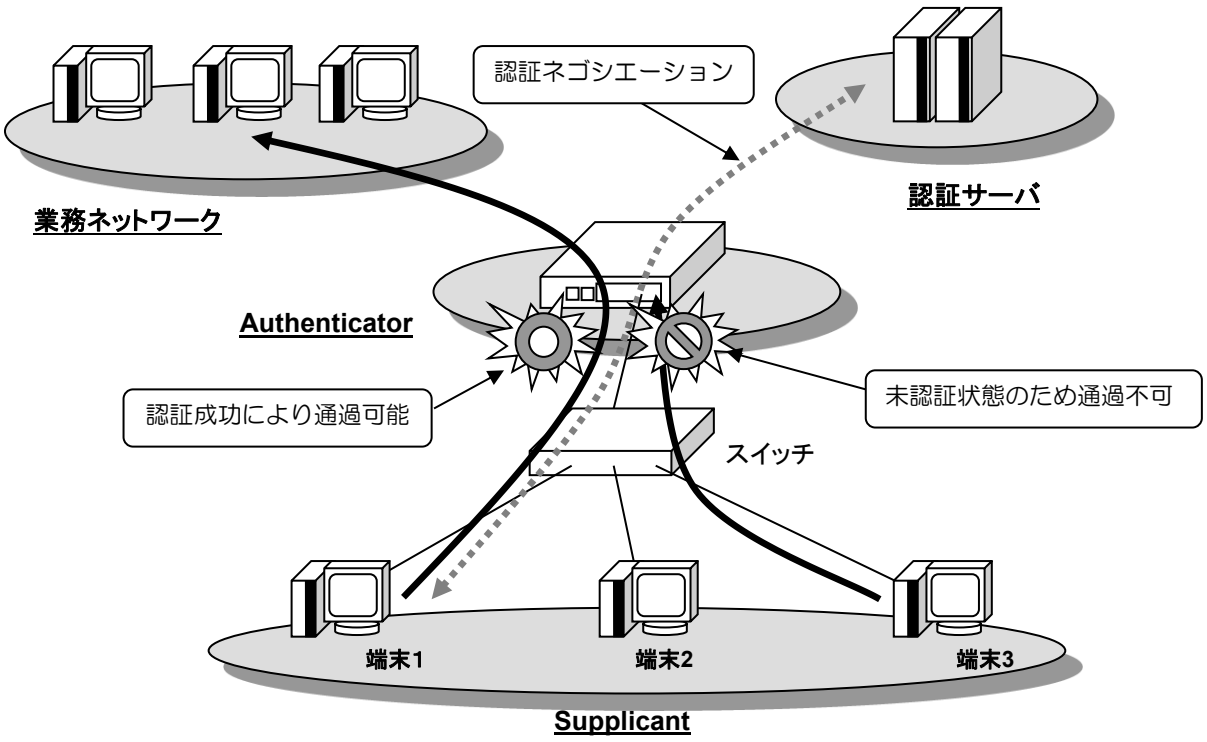
- IEEE802.1X 機能（※）
- MAC 認証機能（※）
- Web 認証機能（Ver9.5 以降）

端末認証機能とは、認証が完了した端末の通信のみを許可することで不正端末のネットワークアクセスを防止する機能です。

※ 別途 RADIUS サーバを用意する必要があります。

2.6.1 端末認証機能の概要

次の図は本装置で IEEE802.1X 機能を利用するネットワークの一般的な構成です。



2.6.1.1 IEEE802.1X 機能の概要

接続された端末（Supplicant）の使用者が正しいユーザであることを認証し、正規のユーザ以外の通信を遮断します。

- Authenticator
  - 本装置です。Supplicant と認証サーバ間での認証ネゴシエーションの橋渡し、および Supplicant の認証状態に応じた通信の制御を行います。認証情報は Authenticator と Supplicant の間では EAPoL(EAP over LAN)、Authenticator と認証サーバ間では EAP over RADIUS で交換します。

- Supplicant
  - PC 端末などです。認証される装置になります。

- 認証サーバ
  - RADIUS サーバです。Supplicant の認証を行います。

IEEE802.1X はスイッチなど多数のポートを持つ装置においてポート単位での認証を基本とする規格ですが、本装置では 1 つのポートで複数の Supplicant の認証を行う拡張機能をサポートしています。本拡張機能を使用した場合、Supplicant の認証は MAC アドレス単位で行われます。上図では端末(Supplicant)1, 2, 3 はスイッチを介して本装置の同一ポートに接続しています。端末 1 は認証済みのためポートの通過を許可されていますが、端末 3 は未認証状態のためフレームがポートで廃棄されています。

2.6.1.2 MAC 認証機能の概要

接続された端末の MAC アドレスを確認し、あらかじめ許可された MAC アドレスを持つ端末のみの通信を許可することで不正端末によるネットワークアクセスを防止します。

IX2000/IX3000 シリーズでは、端末からの通信を受信すると当該端末の MAC アドレスが接続許可されているかどうかを自動的に RADIUS サーバに問い合わせ、その結果に応じて通信を許可したり拒否したりします。

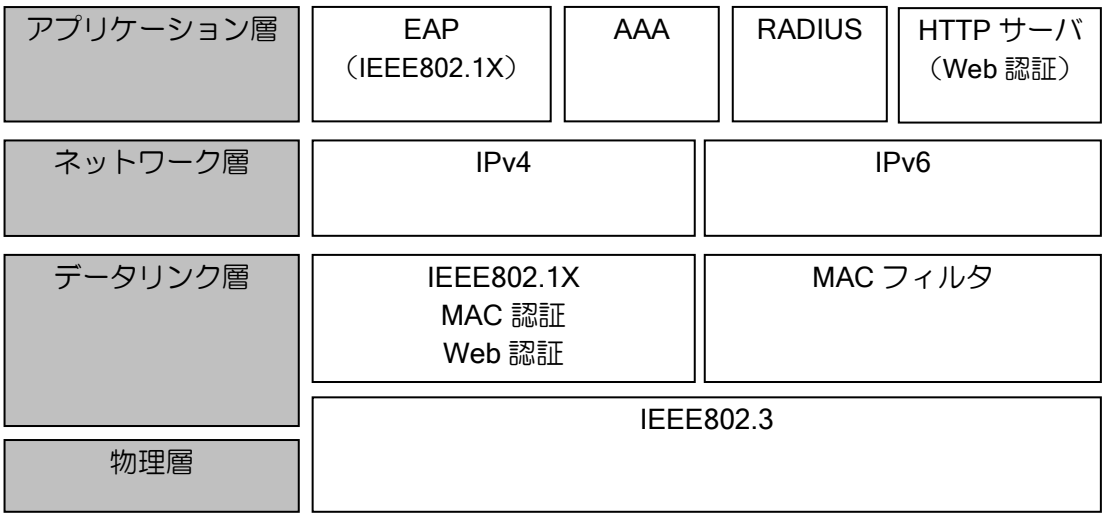
2.6.1.3 Web 認証機能の概要

接続された端末の使用者が正しいユーザであることを Web 画面で認証することで、不正端末によるネットワークアクセスを防止します。

IX2000/IX3000 シリーズでは、端末からの HTTP 通信を受信すると認証用 Web ページにリダイレクトし、ユーザ名・パスワードで認証を行います。認証結果に応じて通信を許可したり拒否したりします。

2.6.2 機能ブロック

本装置の IEEE802.1X 関連機能の機能ブロックは以下のようになります。



IEEE802.1X 機能および MAC 認証機能を使用する際は AAA、RADIUS の設定が必要になります。

IEEE802.1X を使用する場合の EAP 機能は、内部で自動的に動作しているため特に意識する必要はありません。

Web 認証機能を使用する際は、HTTP サーバの設定が必要になります。

2.6.3 IEEE802.1X 機能の設定

2.6.3.1 IEEE802.1X 機能の仕様

本装置の IEEE802.1X 機能の仕様は以下のようになります（諸元値を除く）。

項目		対応
認証動作モード（PAE モード）	Authenticator	○
	Supplicant	×
認証単位	ポート単位	○
	MAC アドレス単位	○
認証サーバ	外部 RADIUS サーバ	○
	ローカル認証	×
認証方式	EAP-MD5	○
	EAP-PEAP	○
	EAP-TLS	○

2.6.3.2 設定コマンド

IEEE802.1X の設定は以下のコマンドを使用します。

インタフェースコンフィグモード	
dot1x enable	IEEE802.1X を有効化します。
dot1x port-control	認証動作を設定します。
dot1x access-control	認証単位を設定します。
dot1x multiple-host	ポート単位の認証モードにおける、制御端末を設定します。
dot1x supplicant-detection	Supplicant 検出動作の設定を行います。
dot1x reauthentication	認証完了後、一定時間での再認証を有効化します。
dot1x max-supplicants	制御を行う最大 Supplicant 数を設定します。
dot1x ignore-address	認証せずに許可するアドレスを設定します。
dot1x authentication	AAA 認証リストを設定します。
dot1x accounting	AAA アカウンティングリストを設定します。
dot1x timeout	各種タイマの値を設定します。
dot1x version	送信フレームのバージョンを指定します。
dot1x max-req	許容する最大連続認証未完了回数を設定します。

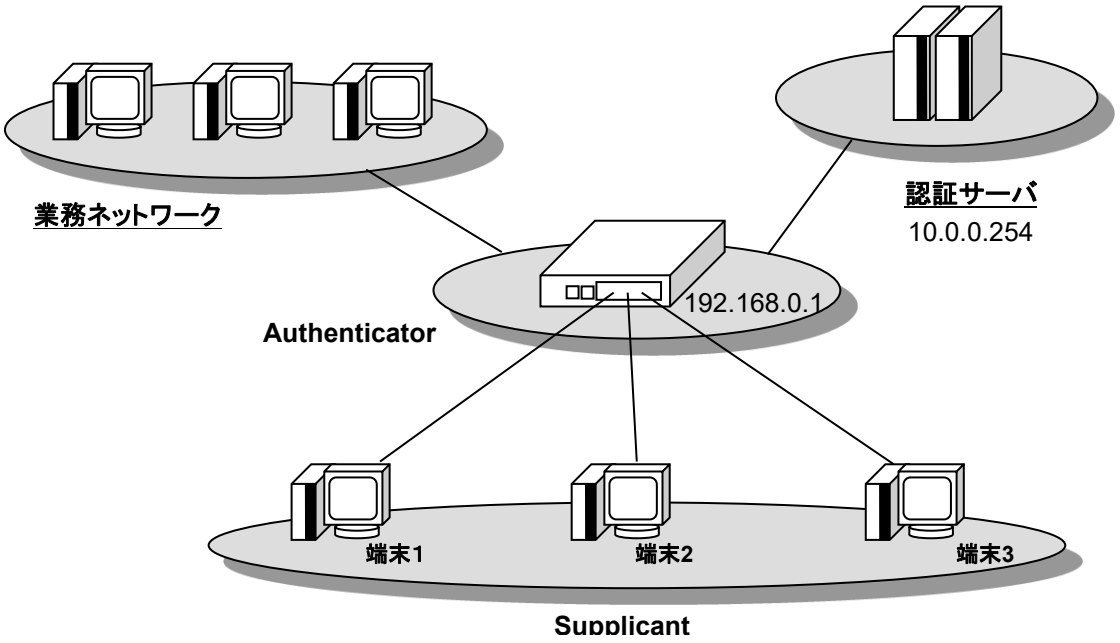
2.6.3.3 構成例

いくつかの IEEE802.1X を使用した場合の構成例と、その際のコンフィグを示します。

※図中の認証サーバや業務ネットワークへアクセスを行うためのインタフェースやルーティングの設定については記述していませんので、ご利用の環境に合わせて追加してください。

(a) 基本的な構成

端末を MAC アドレス単位で認証します。



【設定例】

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   dot1x enable
   no shutdown
```

(b) 認証サーバの冗長化

認証サーバを複数用意し、冗長構成を組むことができます。プライマリの認証サーバがダウンしても、バックアップの認証サーバへ問い合わせを行うことで認証処理を完了できます。

【設定例 1】 認証サーバ 1 が NG を返す場合は認証サーバ 2 へ問い合わせない。

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
radius host ip 10.0.0.253 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   dot1x enable
   no shutdown
```

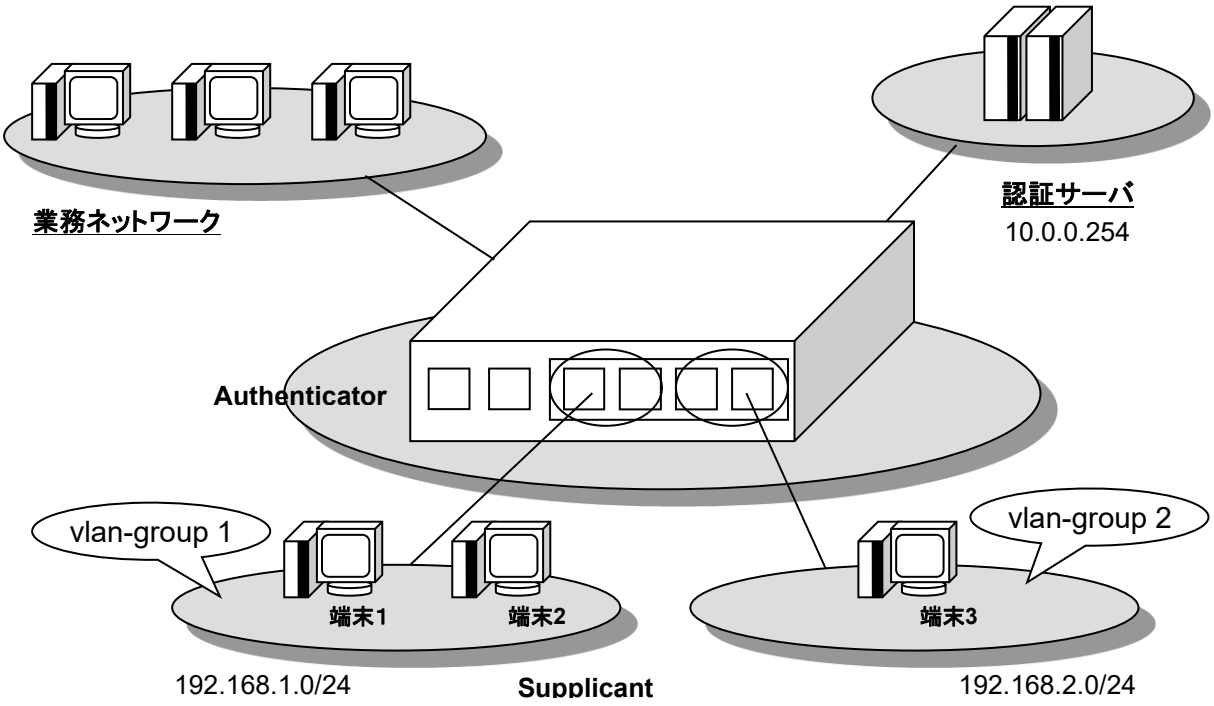
【設定例 2】認証サーバ 1 が NG を返しても認証サーバ 2 へ問い合わせる。

```
aaa enable
aaa group server radius rad-group1 ip 10.0.0.254
aaa group server radius rad-group2 ip 10.0.0.253
aaa authentication dot1x default group rad-group1 group rad-group2
!
radius host ip 10.0.0.254 key 0 secret-key
radius host ip 10.0.0.253 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   dot1x enable
   no shutdown
```

(c) IEEE802.1X + ポートベース VLAN

4 ポートスイッチング HUB で VLAN の設定を行っている場合、VLAN グループごとに IEEE802.1X を有効化することができます。

HUB ポートの VLAN グループ 1（ポート 1、ポート 2）で IEEE802.1X を使用し、VLAN グループ 2（ポート 3、ポート 4）では IEEE802.1X を使用しないといった構成が可能です。



【設定例】

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
device GigaEthernet2
   vlan-group 1 port 1 2
   vlan-group 2 port 3 4
!
interface GigaEthernet2:1.0
   ip address 192.168.1.1/24
   dot1x enable
```

```
   no shutdown
!
interface GigaEthernet2:2.0
   ip address 192.168.2.1/24
   no shutdown
```

2.6.3.4 その他の設定

(a) 複数ホスト接続の有効化

本設定は認証単位がポート単位となっている必要があります。

インタフェースコンフィグモード	
dot1x multiple-host	ポートベース認証モードにおける、制御端末を設定します。

一台の Supplicant が認証ネゴシエーションを完了するとポートが認証状態となり、全ての通信が許可されます。認証ネゴシエーションを行っていない端末も通信可能です。

デフォルトではこの機能は無効です。一台の Supplicant が認証ネゴシエーションを完了しても、通信が許可されるのは認証処理を行った Supplicant のみとなり、その他の通信は廃棄されます。また、最初に認証ネゴシエーションを行った Supplicant の認証状態がタイムアウトするかログアウトにより切断されるまでは、その他の Supplicant の認証要求フレームも廃棄されます。

(b) Supplicant 検出動作の変更

本装置の配下に接続されている Supplicant を検出するための動作を指定します。

インタフェースコンフィグモード	
dot1x supplicant-detection	Supplicant 検出動作を設定します。

本装置は配下に接続されている Supplicant を検出し、認証処理を行うために、デフォルトでは定期的に自身から EAP-Request/Identity をマルチキャスト(01:80:c2:00:00:03)で送信します。送信間隔はタイマ tx-period の設定値となります。

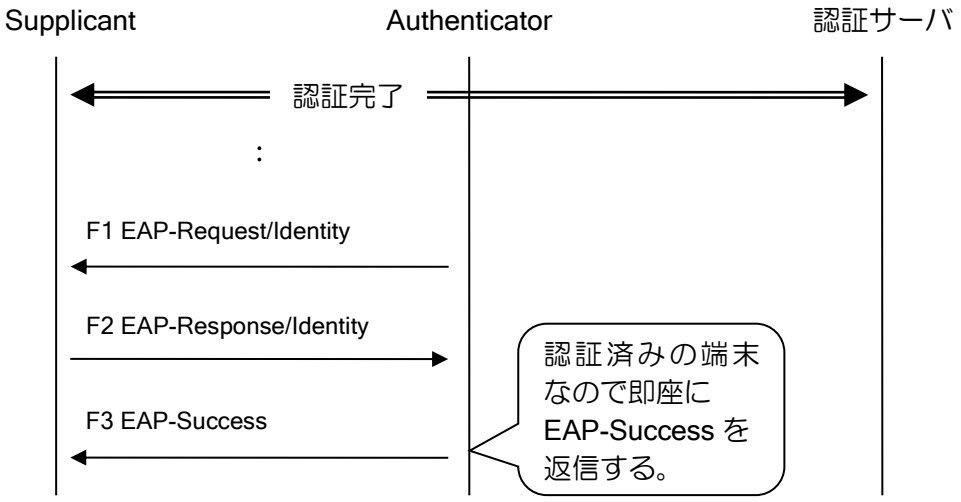
Supplicant 検出動作は full、shortcut、disable の 3 種類があります。接続する Supplicant の種類によっては特定のモードで認証失敗による通信断が発生する可能性があるため、Supplicant の動作特性に応じてモードを選択する必要があります。

	ユーザの操作により EAPoL-Start を送信可能	ショートカット認証を受け付けられる	推奨モード
タイプ 1	NG	NG	full
タイプ 2	NG	OK	shortcut
タイプ 3	OK	NG	disable
タイプ 4	OK	OK	disable

- full モード

  デフォルトの設定です。ルータから定期的に EAP-Request/Identity の送信を行います。Supplicant が定期的な EAP-Request/Identity に反応して EAP-Response/Identity を送信してきた場合、常に完全な形の認証ネゴシエーションを行います。
- shortcut モード

  ルータから定期的に EAP-Request/Identity の送信を行います。まだ認証されていない Supplicant が定期的な EAP-Request/Identity に反応して EAP-Response/Identity を送信してきた場合は完全な形の認証ネゴシエーションを行いますが、既に認証済みの Supplicant の場合は認証ネゴシエーションを省略し、即座に EAP-Success を返信します。



本設定はシステムにかかる負荷を下げるために認証済みの端末に関しては認証サーバへの問い合わせを行わず、認証処理を完了しています。しかし、使用する Supplicant の種類によっては省略された認証処理を受け入れない場合があり、これによって通信が途切れる場合があります。そのような Supplicant を使用している場合、Supplicant からユーザの操作により EAPoL-Start を送信できる場合は検出動作を disable としてください。ユーザの操作により EAPoL-Start を送信できない場合は検出動作を full としてください。

- disable モード
  ルータから定期的に EAP-Request/Identity の送信を行いません。Supplicant から EAPoL-Start を受信することで認証処理を開始します。

(c) 再認証の有効化

インタフェースコンフィグモード	
dot1x reauthentication	認証完了後、一定時間での再認証を有効化します。

本設定が無効化されている場合は、再認証は行われず、一度認証を行った Supplicant は EAPoL-Logoff フレームを受信するまで認証状態を継続します。

但し、Supplicant 検出動作の設定で、ルータから定期的な EAP-Request/Identity を送信するモードにしている場合、これに反応した Supplicant から EAP-Response/Identity が送信されることで再認証が行われる場合があります。

(d) 制御対象外アドレスの設定

認証を行わず、常に許可する MAC アドレスなどを設定することができます。

インタフェースコンフィグモード	
dot1x ignore-address	認証せずに許可するアドレスを設定します。

- multicast を選択すると、あて先がマルチキャストの全フレームを常に受信します。
- broadcast は、あて先がブロードキャストの全フレームを常に受信します。
- MAC アドレス指定の場合は、ルータから見て受信する場合は送信元アドレス、送信する場合は宛先アドレスが指定したアドレスと一致している場合に通過します。

また、本設定によらず、ルータから送信されるマルチキャスト・ブロードキャストフレームは認証結果に関わらず常に送信します。

(e) フレーム制御方向の設定

IEEE802.1X において制御を行うフレームの方向を指定します。

インタフェースコンフィグモード	
dot1x port-control direction	フレーム制御方向を設定します。

デフォルトは both であり、Inbound/Outbound の両方向のフレームが認証結果に依存して制御されます。

in と設定した場合は Inbound のフレームのみ認証結果に依存して制御されます。ルータから送信される Outbound のフレームは常に通過します。

(f) バージョンの設定

本装置が送信する EAPoL フレームのバージョン番号は 2 です。稀にバージョン 1 しか受け付けない Supplicant が存在しますので、その環境では値を変更してください。本装置が送信する EAPoL ヘッダが含む Version フィールドの値を指定します。

dot1x version	EAPoL ヘッダのバージョンの設定をします。

尚、変更しても本装置の内部的な動作は Version2(IEEE802.1X 2004 年度版)の実装のままです。

(g) IEEE802.1X ログ抑制の設定

IEEE802.1X に関するログの出力を抑制します。

インタフェースコンフィグモード	
dot1x port-control suppress-logging	イベントログの出力を抑制します。

イベントログの設定を行うことで、IEEE802.1X に関する以下のような情報を取得できます。

	ログの内容	イベントログのレベル				
		error	warn	notice	info	debug
a	メモリ確保エラー	○	○	○	○	○
b	各種内部処理（異常系）	×	○	○	○	○
c	Supplicantの認証の成功/失敗/解除	×	○	○	○	○
d	未認証フレームの廃棄	×	○	○	○	○
e	各種内部処理（正常系）	×	×	○	○	○
f	ステートマシンの状態遷移	×	×	×	○	○
g	認証済みフレームの送受信	×	×	×	○	○
h	EAPoL フレームの送受信	×	×	×	×	○

○：情報が出力される　×：情報が出力されない

本設定により、この中で「(d)未認証フレームの廃棄」「(g)認証済みフレームの送受信」に関するログの出力を停止します。IEEE802.1X をサポートしていない端末から大量にマルチキャストパケットを受けログが記録される場合などで抑止してください。

2.6.3.5 タイマの設定

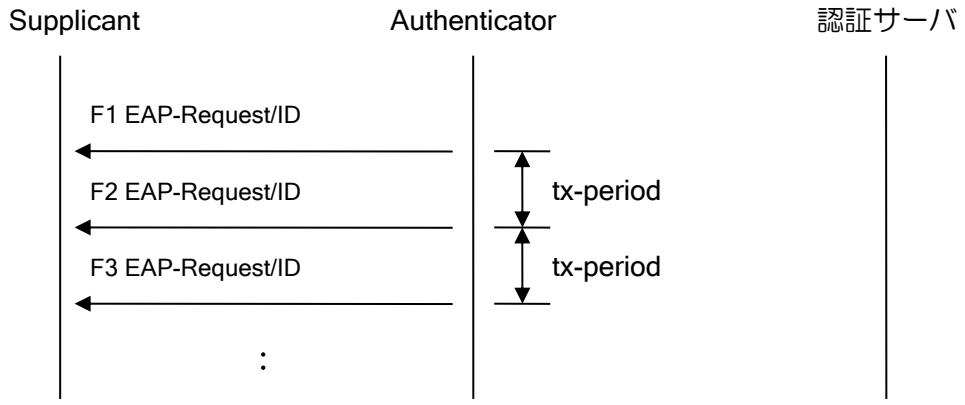
各種タイマの値を設定します。IEEE802.1X では以下のタイマを設定可能です。

インタフェースコンフィグモード	
dot1x timeout quiet-period	認証失敗後、再度認証を開始するまでの間隔
dot1x timeout reauth-period	Supplicant の認証完了後、再認証を行うまでの間隔
dot1x timeout server-timeout	ルータと認証サーバ間のパケットの待ち受け許容時間
dot1x timeout supp-timeout	EAP-Request に対する Supplicant からの応答待ち時間
dot1x timeout tx-period	EAP-Request パケットの再送間隔
dot1x timeout waiting-period	最大認証試行回数（3 回）を超えた場合の認証停止時間

tx-period

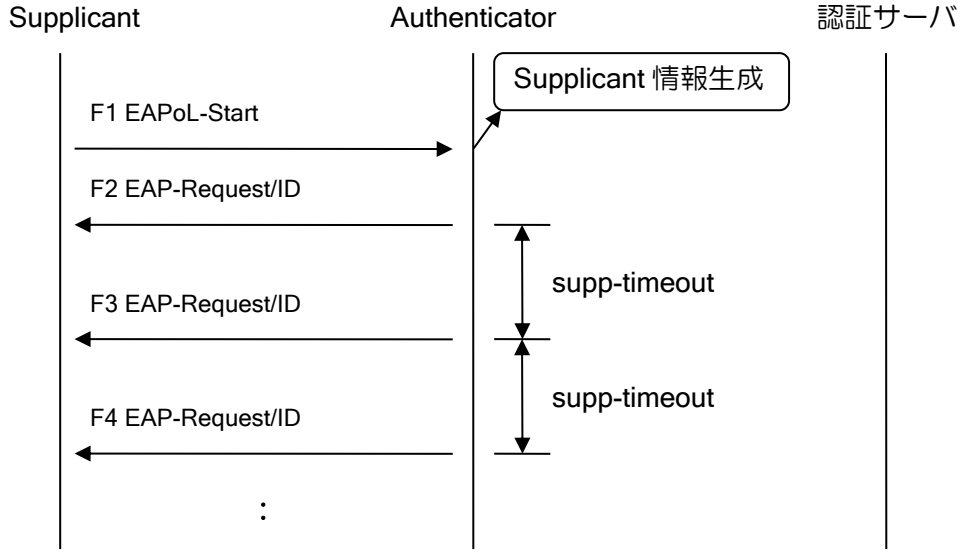
ルータのインタフェースで IEEE802.1X を有効にすると定期的に送信される EAP-Request/ID パケットの送信間隔を指定します。

EAP-Request/ID パケットの定期的な送信は、そのインタフェースで扱える最大数の Supplicant を検出するまで続きます。認証単位がポート単位の場合、一台の Supplicant を検出した時点で送信は停止します。また、Supplicant 検出を無効にした場合も送信されません。



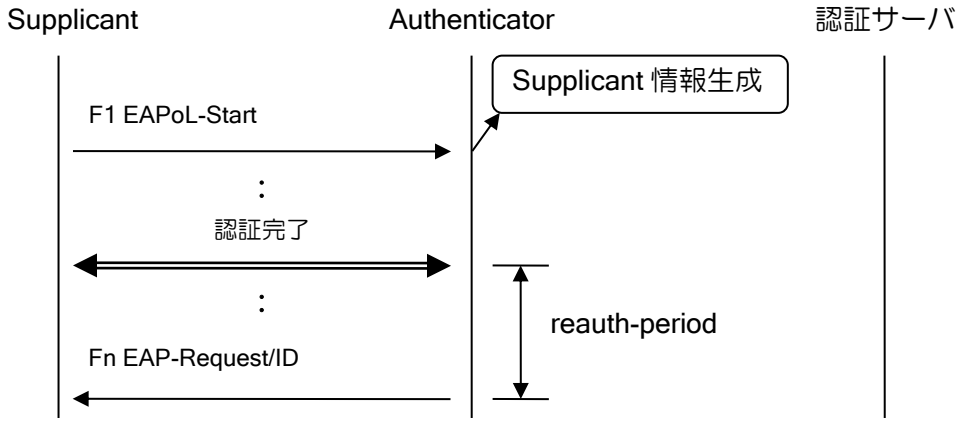
supp-timeout

Supplicant から EAPoL-Start を受信後に返信する EAP-Request/ID パケットなど、ルータとして情報を持っている Supplicant に対する EAP-Request パケットの再送間隔を指定します。



reauth-period

認証完了後、再度認証を行うまでの間隔を指定します。



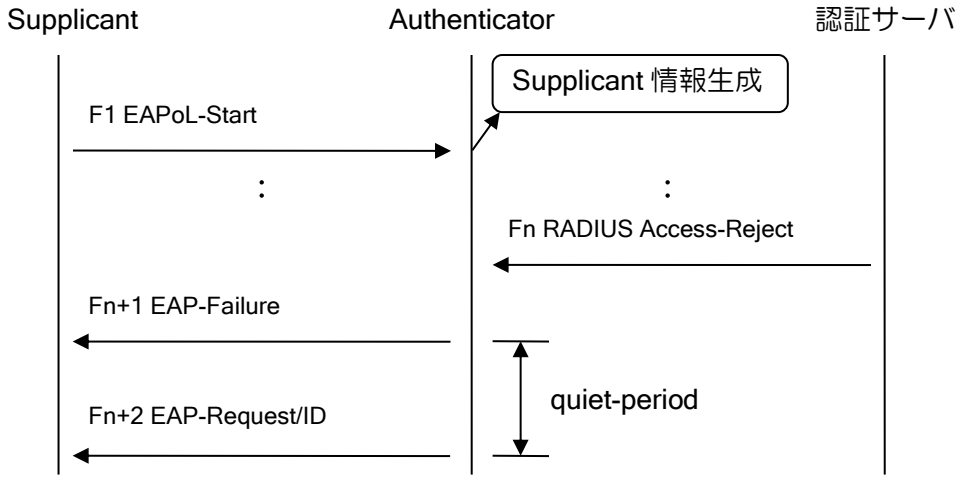
RADIUS サーバからの Session-Timeout を認証時間として使用する場合は、reauth-period に server を指定してください。

【設定例】
再認証間隔にサーバからの Session-Timeout を使用します。

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.1.1/24
   dot1x enable
   dot1x timeout reauth-period server
   no shutdown
```

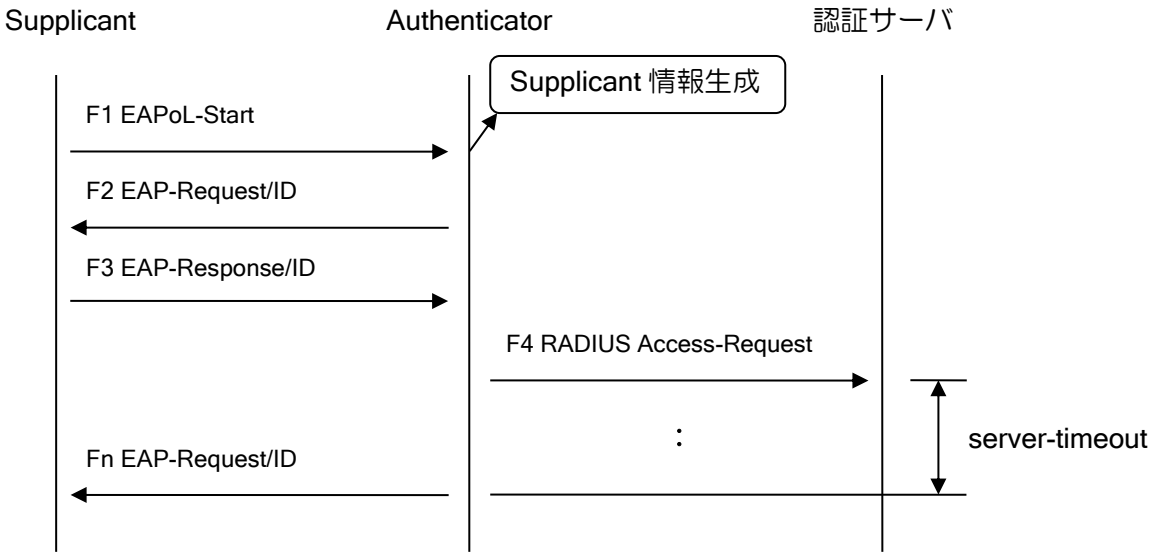
quiet-period

認証ネゴシエーションの失敗後、次の認証処理を開始するまでの間隔を指定します。認証に失敗してから quiet-period が経過するまでは Supplicant から EAPoL フレームを受信しても本装置は反応しません。



server-timeout

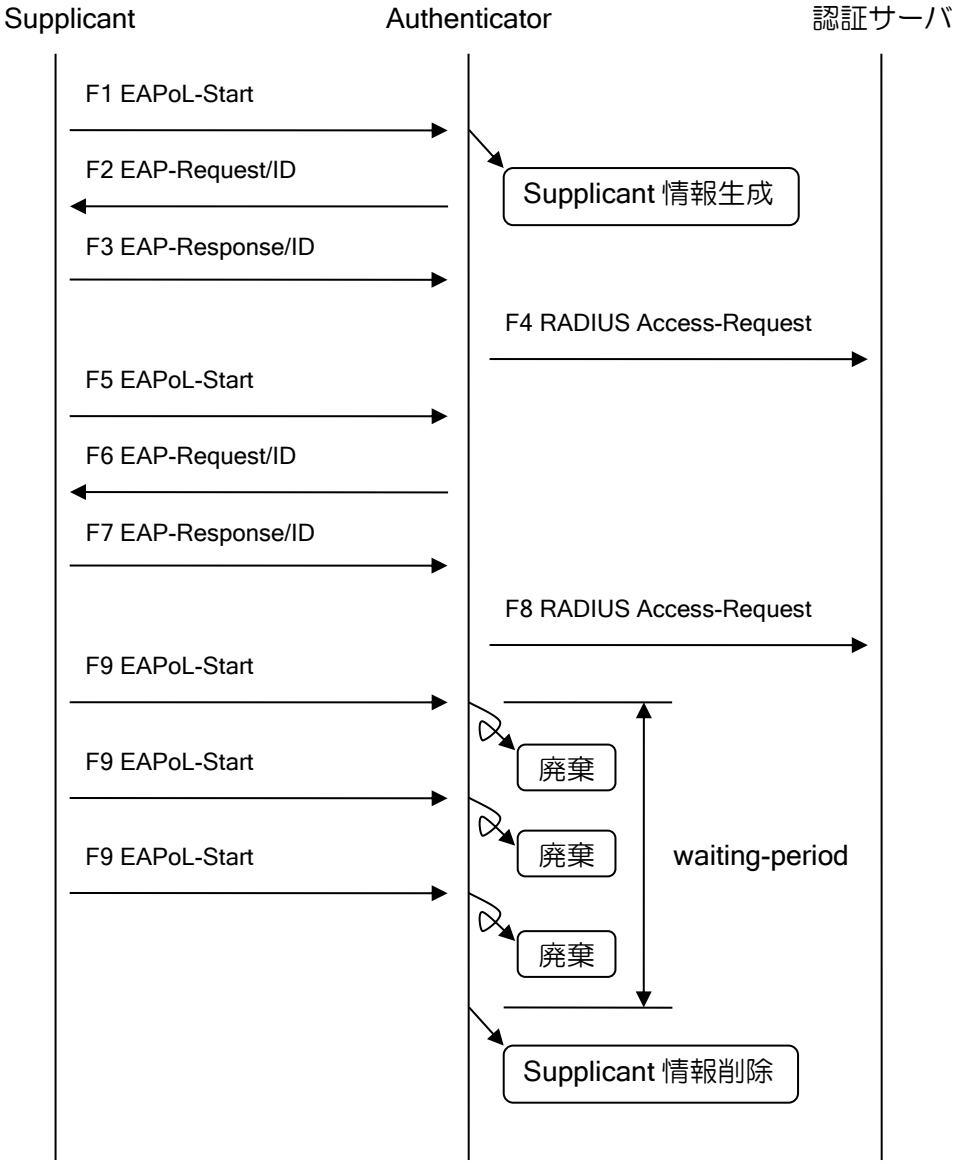
認証ネゴシエーション中に認証サーバから応答がなかった場合に、再度認証処理を開始するまでの待ち時間を指定します。



waiting-period

悪意のある端末がバースト的に EAPoL-Start を送信した場合、それに呼応して Authenticator(ルータ)から連続して認証サーバへパケットを送信し、ネットワークシステムを不安定にしてしまう可能性があります。

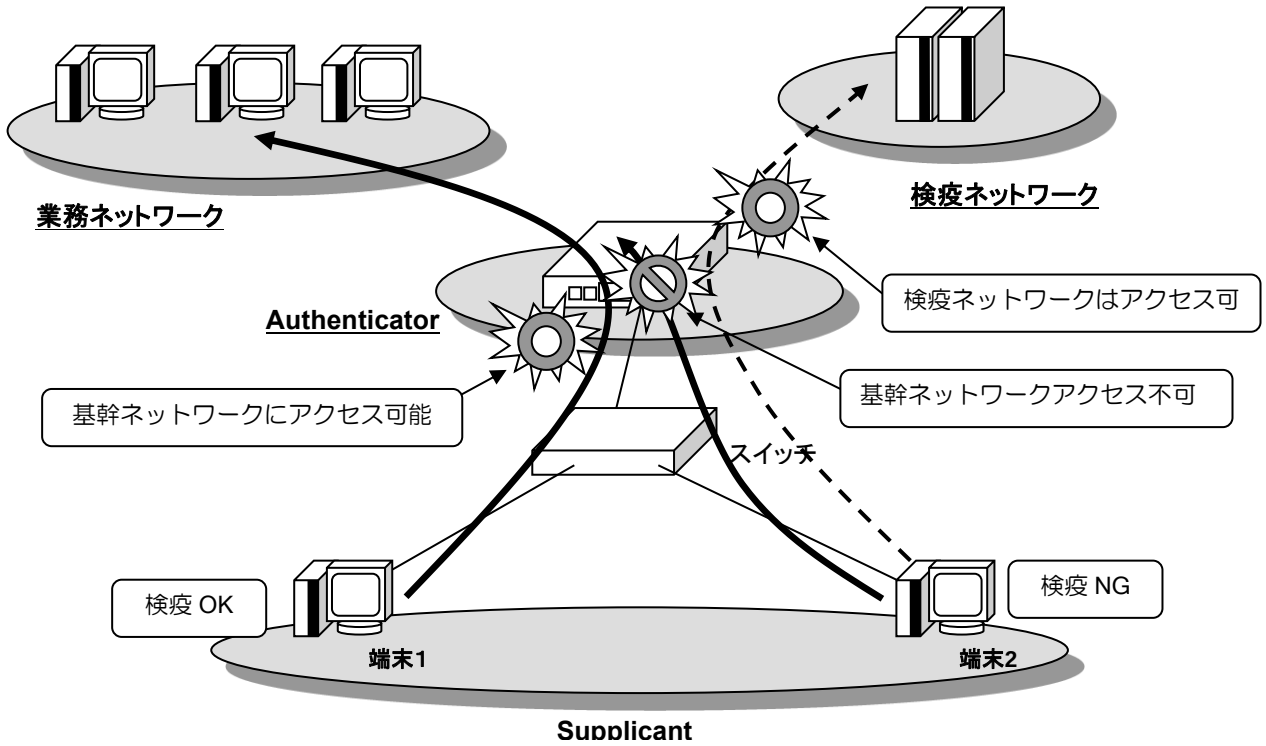
これを防ぐために本装置の IEEE802.1X では、認証試行回数が一定回数（3 回）を超えた場合、Supplicant から EAPoL フレームを受信しても一定時間反応しなくなります。waiting-period はその時の無反応時間を指定します。



2.6.4 検疫機能の設定

Ver.8.2 以降、IEEE802.1X を利用した検疫機能をサポートしています。

検疫機能では、ポリシーに違反している端末がアクセスするネットワークを制限することが可能となります。



2.6.4.1 基本設定

検疫機能を使用する際には IEEE802.1X の設定が必須となります。IEEE802.1X の設定に関しては、前項を参照してください。検疫機能では以下のコマンドを使用します。

インタフェースコンフィグモード	
dot1x quarantine enable	検疫機能を有効化します。
dot1x quarantine filter	検疫結果により、許可するネットワークを設定します。

【設定例】
ポリシー違反がある場合は、10.0.0.0/24 のみアクセスを許可
違反が無い場合は、全てのあて先に対してアクセスを許可

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   dot1x enable
   dot1x quarantine enable
   dot1x quarantine filter keneki ip 10.0.0.0/24
   dot1x quarantine filter kikan ip any
   no shutdown
```

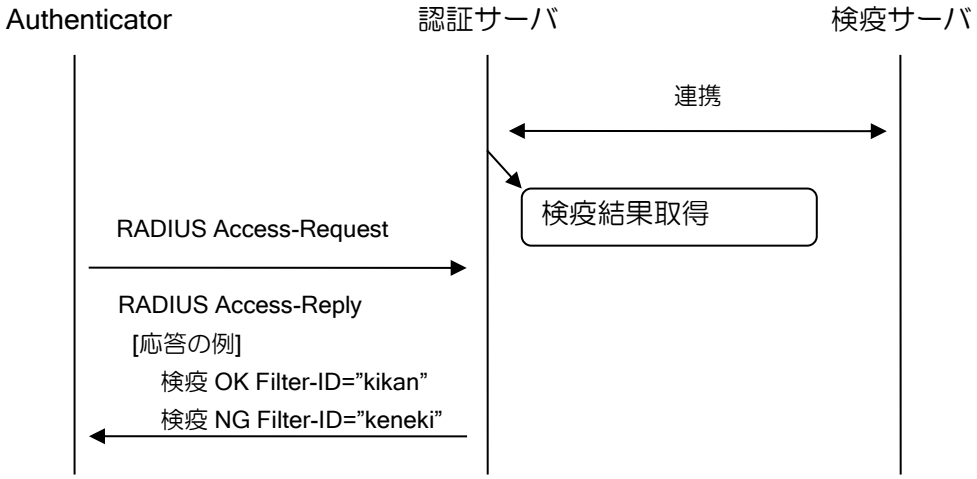
2.6.4.2 検疫機能の動作

(a)適用するフィルタの選択

IX2000/IX3000 の検疫機能では、認証サーバからの応答に含まれる Filter-ID アトリビュートの内容によって端末のアクセス制御を行います。

IEEE802.1X 認証の際に、認証サーバからの応答に含まれる Filter-ID に設定された値によって、IX2000/IX3000 に設定された何れかのフィルタを適用するかを決定します。なお、Filter-ID の設定内容は、認証サーバの設定となります。

前項の設定例では、ポリシー違反がある場合は、Filter-ID に”keneki”という文字列、ポリシー違反が無い場合は、”kikan”という文字列が設定される場合の設定例となります。



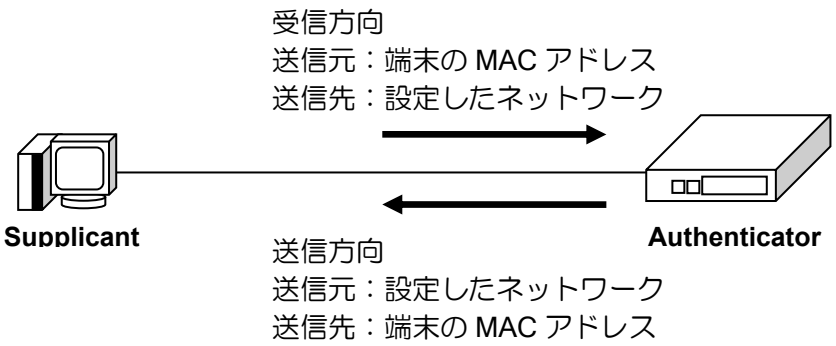
フィルタ設定では”default”の設定を行うことができます。Filter-ID が設定されていない場合、Filter-ID にマッチするフィルタ設定が存在しない場合は、この設定が適用されます。”default”が設定されていない場合は、廃棄されます。

【設定例】
該当するフィルタが無い場合 100.0.0.0/24 にアクセス可能とする。

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   dot1x enable
   dot1x quarantine enable
   dot1x quarantine filter default ip 100.0.0.0/24
   dot1x quarantine filter keneki ip 10.0.0.0/24
   dot1x quarantine filter kikan ip any
   no shutdown
```

(b)フィルタの動作

設定したフィルタは送信方向、受信方向ともに有効となります。以下の条件にマッチするパケットのみ通過可能となります。



2.6.4.3 その他の設定

(a)アトリビュートの変更

検疫に使用するアトリビュートは、デフォルトでは Filter-ID を使用します。

使用するアトリビュートを Tunnel-Private-Group-Id に変更することが可能です。設定コマンドは以下の通りです。

インタフェースコンフィグモード	
dot1x quarantine attribute	使用するアトリビュートを設定します。

【設定例】
アトリビュートに tunnel-private-group-id を使用

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   dot1x enable
   dot1x quarantine enable
   dot1x quarantine attribute tunnel-private-group-id
   dot1x quarantine filter keneki ip 10.0.0.0/24
   dot1x quarantine filter kikan ip any
   no shutdown
```

(b)ロギング抑止設定

検疫機能により、廃棄または通過したパケットのログ出力を抑止することができます。設定コマンドは以下の通りです。

インタフェースコンフィグモード	
dot1x quarantine suppress-logging	ロギング抑止設定

【設定例】
フィルタが通過した場合のログを抑止

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   dot1x enable
   dot1x quarantine enable
   dot1x quarantine filter keneki ip 10.0.0.0/24
   dot1x quarantine filter kikan ip any
   dot1x quarantine suppress-logging pass
   no shutdown
```

2.6.5 MAC 認証機能の設定

2.6.5.1 設定コマンド

MAC 認証の設定は、以下のコマンドを使用します。

インタフェースコンフィグモード	
mac-auth enable	MAC 認証機能を有効化します。
mac-auth address-format	MAC 認証で使用するアドレス形式を変更します。
mac-auth ignore-address	認証せずに許可するアドレスを設定します。
mac-auth authentication	AAA 認証リストを設定します。
mac-auth accounting	AAA アカウンティングリストを設定します。
mac-auth timeout	各種タイマの値を設定します。

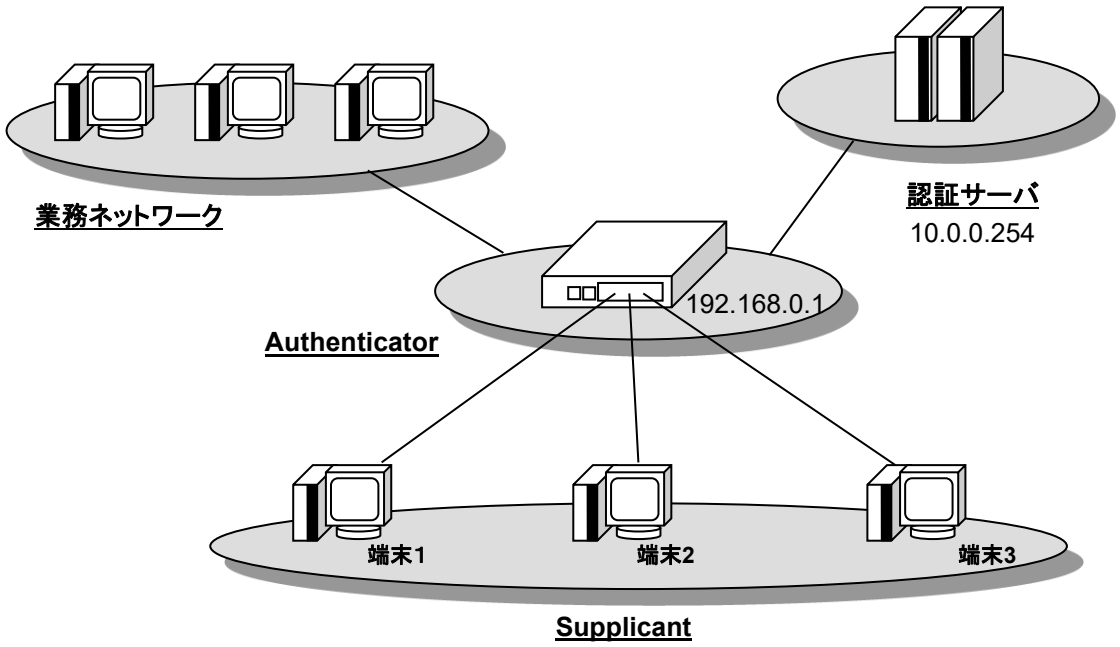
2.6.5.2 構成例

構成例とその際のコンフィグを示します。

※図中の認証サーバや業務ネットワークへアクセスを行うためのインタフェースやルーティングの設定については記述していませんので、ご利用の環境に合わせて追加してください。

基本的な構成

端末を MAC アドレスで認証します。



【設定例】

```
aaa enable
aaa authentication mac-auth default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
interface GigaEthernet2.0
   ip address 192.168.0.1/24
   mac-auth enable
   no shutdown
```

2.6.5.3 その他の設定

環境によっては、さらにいくつかの設定を追加する必要があります。下記にいくつかの例について説明します。

(a) 認証サーバの冗長化

認証サーバを冗長化する設定については IEEE802.1X の設定と同様です。前述の IEEE802.1X の項目を参照してください。

(b) 認証に使用する MAC アドレスのフォーマット変更

MAC 認証機能で使用されるユーザ / パスワードは「012345abcdef」という形式の MAC アドレスを使用します。他の表記で RADIUS に登録されている場合は変更してください。

インタフェースコンフィグモード	
mac-auth address-format	MAC 認証で使用するアドレス形式を変更します。

区切り文字として「：」「ー」をつけることができます。
16 進数のアルファベット表記を大文字に変更できます。

(c) Radius サーバと通信断になっても通信を継続させる

一定時間無通信が継続すると認証結果は削除されます。そのため、認証結果削除後に再度通信を行おうとした場合は再度認証を行います。この時、認証サーバ（RADIUS サーバ）の障害などの影響により認証に失敗すると、一度認証に成功した端末であっても通信ができなくなってしまいます。

Ver.8.2 以降は、認証設定の認証方法に none が追加されています。これを設定することにより、サーバから応答が無い場合は認証成功とすることが可能です。
詳細は AAA の設定の項の認証動作の説明を参照してください。

Ver.8.1 以前の場合は、再認証の設定は行わず、無通信検出の時間（オフライン検出タイマ）を十分長い値を設定してください。これにより、認証結果が削除されるまでに時間が長くなるため、認証サーバの障害の影響を低減できます。

インタフェースコンフィグモード	
mac-auth timeout offline-detection	オフライン検出タイマを設定します。

(d) 特定の端末を常に許可する

認証を行わず、常に許可する MAC アドレスを設定することができます。

インタフェースコンフィグモード	
mac-auth ignore-address	認証せずに許可するアドレスを設定します。

2.6.6 Web 認証機能の設定

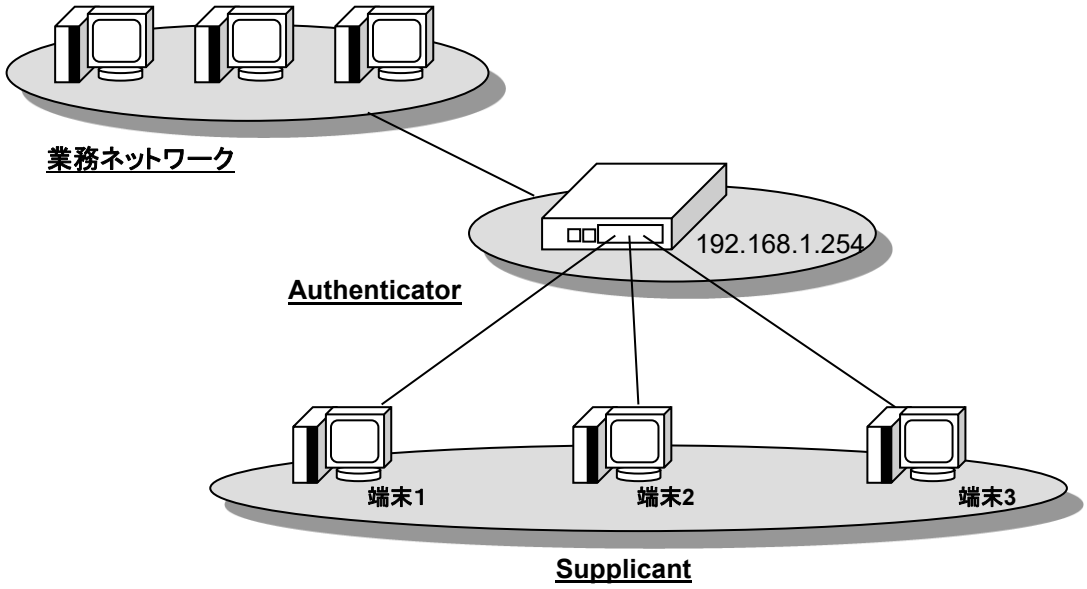
2.6.6.1 設定コマンド

グローバルコンフィグモード	
web-auth username	認証パスワードを設定します。
web-auth ignore-address	認証せずに許可するアドレスを設定します。
web-auth ignore-protocol	認証せずに許可するプロトコルを設定します。
web-auth timeout	各種タイマの値を設定します。
web-auth max-entry	最大端末数を設定します。

インタフェースコンフィグモード	
web-auth enable	Web 認証機能を有効化します。

2.6.6.2 構成例

構成図とその際のコンフィグを示します。（RADIUS を使用した認証は未対応です）




```
【設定例】
!
ip access-list web-list permit ip src any dest 192.168.1.254/32
!
http-redirect mode web-auth
!
http-server ip access-list web-list
http-server ip enable
!
web-auth username web-user password web-pass
!
interface GigaEthernet2.0
   ip address 192.168.1.254/24
   web-auth enable
   http-redirect enable
   no shutdown
!
```

2.6.6.3 注意事項

未認証の端末から HTTPS 通信を行った場合は、認証用 Web ページにリダイレクトは行われずパケットが廃棄されます。HTTP 通信を行い端末が認証された後は、HTTPS 通信は通過します。

2.6.6.4 その他の設定

環境によっては、さらにいくつかの設定を追加する必要があります。下記にいくつかの例について説明します。

(a) 特定の端末を常に許可する

認証を行わず、常に許可する MAC アドレスを設定することができます。

グローバルコンフィグモード	
web-auth ignore-address	認証せずに許可するアドレスを設定します。

(b) 特定のプロトコルを常に許可する

認証を行わず、常に許可するプロトコルを設定することができます。
指定できるプロトコルは以下の通りです。

- https

グローバルコンフィグモード	
web-auth ignore-protocol	認証せずに許可するプロトコルを設定します。

2.6.6.5 認証画面のカスタマイズ

認証画面は、独自のページに変更することができます。表示する内容の変更や、認証情報の入力なく「同意ボタン」を押すだけの画面に変更できます。

2.6.7 端末認証機能の併用

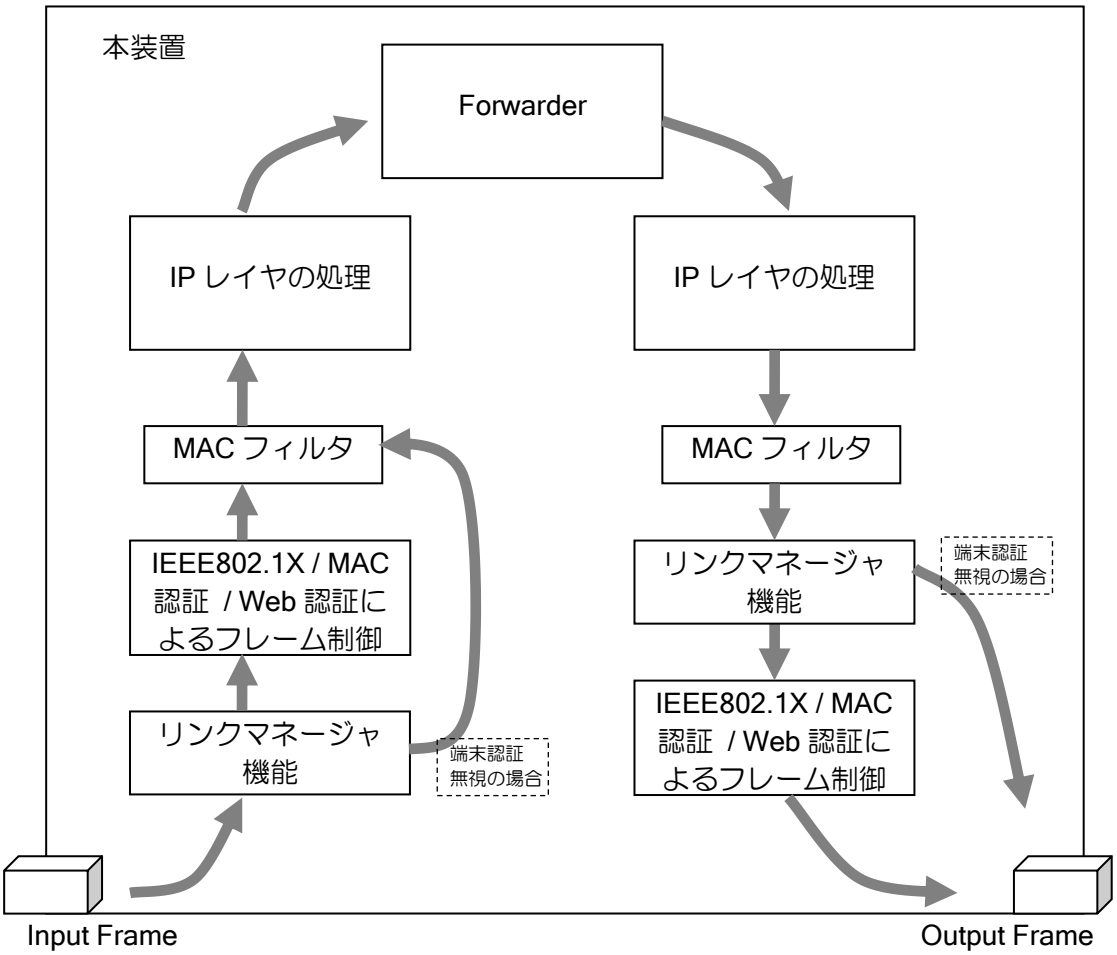
IEEE802.1X 認証は MAC 認証や Web 認証と併用することが可能です。IEEE802.1X の EAP パケットを受信したときは IEEE802.1X で認証します。EAP 以外の通常のフレームを受信した場合には、MAC 認証機能や Web 認証機能で認証します。

IEEE802.1X で使用する EAP のフレームは MAC 認証や Web 認証で廃棄しないため、これらの認証を設定しても IEEE802.1X 認証には影響はありません。

2.6.8 端末認証機能とフィルタ機能の併用

フィルタ機能も併用することが可能です。フィルタで許可されない通信は認証に成功しても通信することはできません。

併用した場合の適用順序は以下のとおりになります。



2.6.9 その他のプロトコルとの同時使用

端末認証機能と他の機能を併用する場合、端末認証機能の「認証されていない端末に関するフレームは廃棄する」という特性から、うまく動作しない場合があります。必要に応じて ignore-address コマンドを設定してください。

利用プロトコル	ignore-address の設定
マルチキャスト	ルータの MAC アドレスを登録するか、multicast を設定
ブロードキャスト	ルータの MAC アドレスを登録するか、broadcast を設定
ユニキャスト	ルータの MAC アドレスを登録する

(a) RIPv1

RIPv1 はブロードキャストを利用します。

(b) RIPv2

RIPv2 はマルチキャストを利用します。

(c) OSPFv2 / OSPFv3

OSPFv2, OSPFv3 はマルチキャストとユニキャストを使用します。

(d) VRRP

VRRP はマルチキャストを利用します。

尚、VRRP を使用して Authenticator を冗長化する場合、VRRP の状態に関係なくそれぞれの Authenticator が動作します。通常このままで使用可能ですが Backup ルータの Authenticator 機能を停止させたい場合は下記の設定を行ってください（Ver.7.5.50 以降）。

【設定例】

```
aaa enable
aaa authentication dot1x default group radius
!
radius host ip 192.168.2.250 key hogehoge
!
vrrp enable
!
watch-group vrrp-watch 10
   event 10 ip vr-inactive 1
   action 10 shutdown-dot1x GigaEthernet2.0
!
network-monitor vrrp-watch enable
!
interface GigaEthernet2.0
   ip address 192.168.0.252/24
   dot1x enable
   dot1x ignore-address multicast
   vrrp 1 ip 192.168.0.254
   vrrp 1 priority 200
   no shutdown
!
```

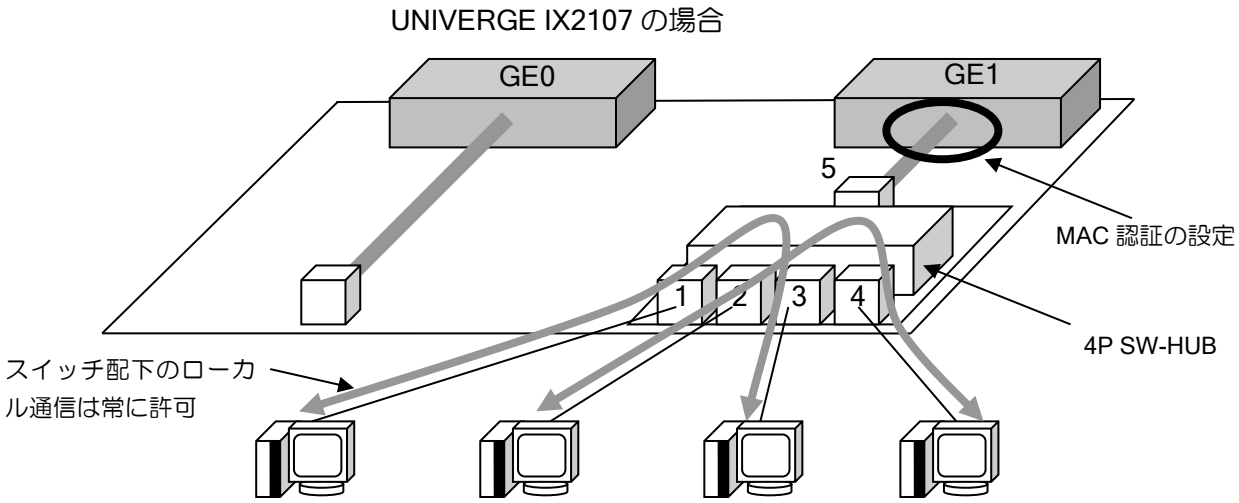
2.6.10 注意事項

(a) タグ VLAN との併用

Ver.8.1 までは、IEEE802.1Q インタフェースでは IEEE802.1X の設定および MAC 認証の機能は使用できません。

(b) スイッチング HUB における注意事項

ポートベース VLAN を使用しない状態でのスイッチング HUB インタフェースにおける端末認証機能では、認証の可否に関わらずスイッチ配下のローカル通信は常に許可されます。



(c) 認証済み端末のインタフェースの移動

本装置の IEEE802.1X と MAC 認証機能による認証は、全てインタフェースごとに記憶されます。認証済みの端末であっても接続するインタフェースを移動した場合はそのインタフェースで再度認証処理を行う必要があります。

Web 認証機能による認証は、インタフェースごとの記憶ではないため、端末がインタフェースを移動しても再度認証処理を行う必要はありません。

(d) ブリッジ機能との併用

ブリッジインタフェースで IEEE802.1X を有効化すると、IEEE802.1X フレームはそのインタフェースで終端されます。有効化しない場合はブリッジされます。

また BVI インタフェースでは IEEE802.1X 機能も MAC 認証も使用できません。

2.6.11 補足

MAC 認証と IEEE802.1X に関連する補足説明を記述します。

2.6.11.1 MAC 認証で使用する RADIUS 要求パケット

付加アトリビュート

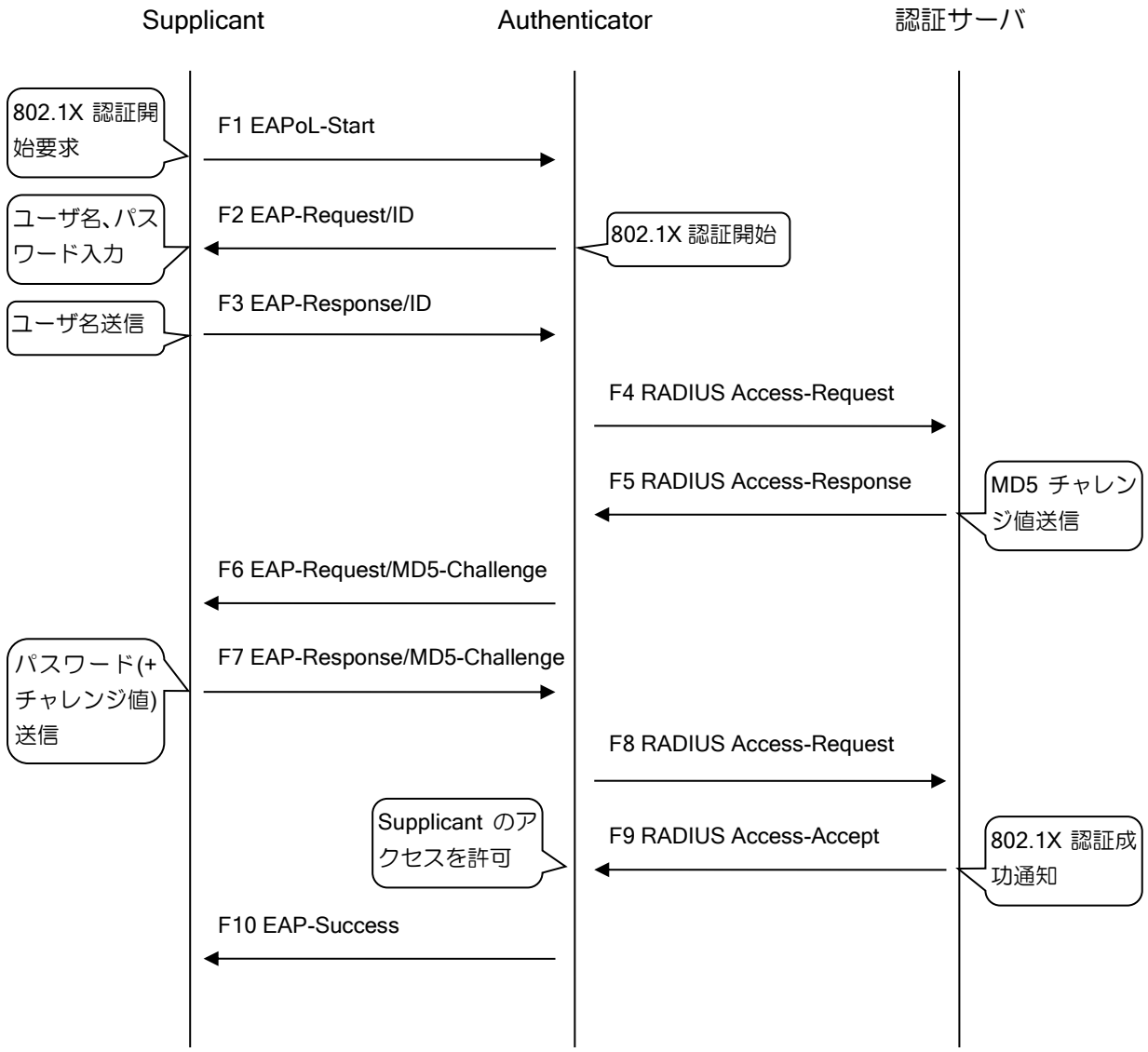
アトリビュート	Value
User-Name	端末の MAC アドレス（書式は変更可能）
User-Password	上記 MAC アドレスの MD5
Called-Station-Id	ルータインタフェースの MAC アドレス
Calling-Station-Id	端末の MAC アドレス
Service-Type	端末に提供するサービスタイプ（Framed:2 固定）
NAS-Port	接続インタフェース番号
NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
NAS-Port-Type	接続インタフェースのタイプ（Ethernet:15 固定）

メッセージ例

```
+ User Datagram protocol, Src Port: 3901 (3901), Dst port: radius (1812)
- Radius protocol
    Code: Access Request (1)
    Packet identifier: 0x38 (56)
    Authenticator: 0x9573C182.....
  - Attribute value pairs
      t:User Name(1) l:12, value:"000e12345678"
      t:User Password(2) l:12, value:"MD5(000E12345678)"
      t:Service Type(6) l:6, value:Framed(2)
      t:NAS Port(5) l:6, value:2
      t:NAS Port Type(61) l:6, value:Ethernet(15)
      t:NAS IP Address(4) l:6, value:192.168.1.1
      t:Called Station Id(30) l:17, value:"01-23-45-AB-CD-EF"
      t:Calling Station Id(31) l:17, value:"00-0E-12-34-56-78"!
```

2.6.11.2 IEEE802.1X のシーケンス例

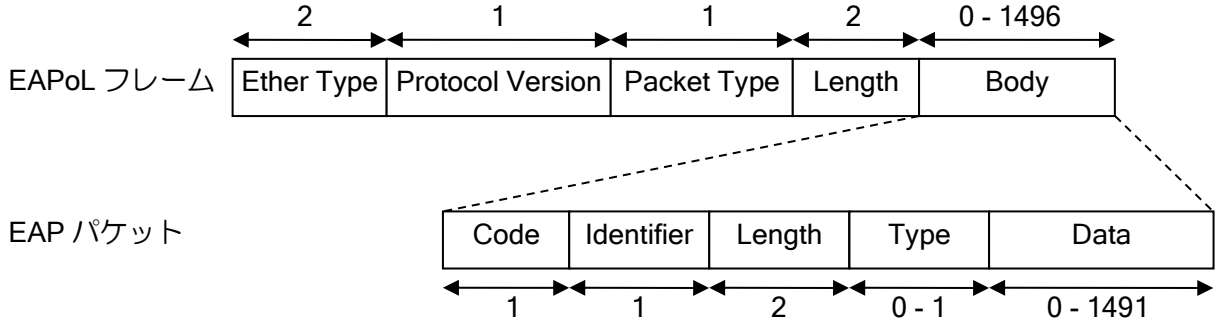
認証方式に EAP-MD5 を使用した場合の認証シーケンス例を示します。



本装置は F9 RADIUS Access-Accept の受信をトリガとして対象 Supplicant のアクセス許可を行います。

2.6.11.3 UNIVERGE IX シリーズの IEEE802.1X プロトコル詳細

IEEE802.1X の EAPoL フレーム、EAP パケットのフォーマットは以下のようになります。



Ether Type

IEEE802.1X を示す 0x888e を含みます。

Protocol Version

実装バージョンを示します。

規格	Value
IEEE802.1X 2001 年度版	0000 0001
IEEE802.1X 2004 年度版	0000 0010

本装置は 0000 0010 を送信します。稀ですが 0000 0001 でないと受け付けない Supplicant がある場合は値を変更してください。ただし値のみで内部動作は 2001 年度版に変更できません。

Packet Type

フレームのタイプを示します。サポートしないタイプのフレームは廃棄します。

Type	Value	意味
EAP-Packet	0000 0000	ボディに EAP パケットを含むことを示します。
EAPoL-Start	0000 0001	認証ネゴシエーションの開始要求を示します。Supplicant から送信されます。
EAPoL-Logoff	0000 0010	認証の解除要求を示します。Supplicant から送信されます。
EAPoL-Key	0000 0011	認証完了後の鍵情報を含むことを示します。本装置ではサポートしません。
EAPoL-Encapsulated-ASF-Alert	0000 0100	未認証状態のポートでアラートメッセージを送受信する際に使用します。本装置ではサポートしません。

Length (EAPoL)

パケットのボディ長を示します。

Body

フレームのタイプが EAP-Packet、EAPoL-Key、EAPoL-Encapsulated-ASF-Alert の時、このフィールドが存在します。認証処理に必要な種々の情報を含みます。

Code

Code	Value	意味
Request	0000 0001	Authenticator が Supplicant に情報を要求する際に使用します。
Response	0000 0010	Supplicant が Authenticator に情報を伝える際に使用します。
Success	0000 0011	認証が成功したことを示します。
Failure	0000 0100	認証が失敗したことを示します。

Identifier

EAP-Request パケットと EAP-Response パケットを関連付けます。ある EAP-Request に対する EAP-Response には同じ Identifier が指定されます。

Length (EAP)

EAP パケットの長さを示します。

Type

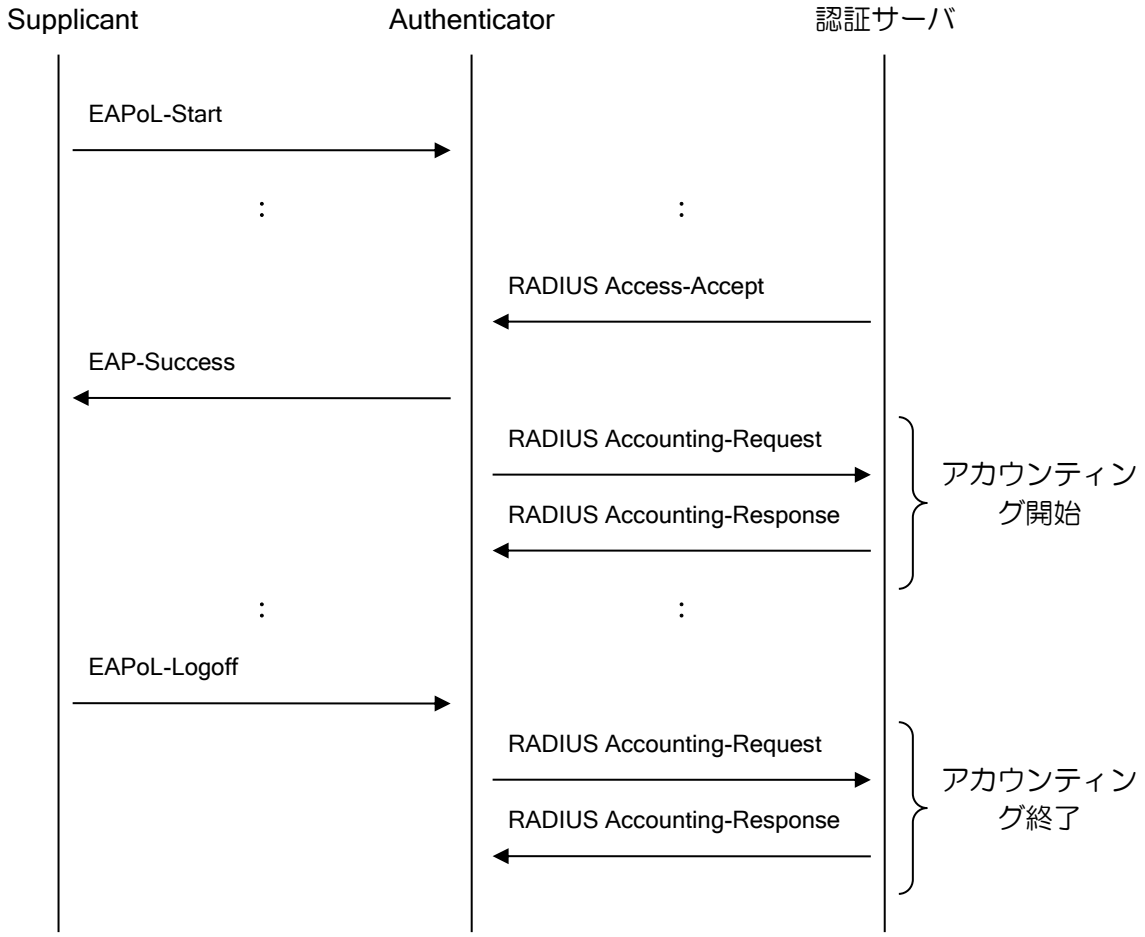
Type フィールド以降は Code が EAP-Request、EAP-Response のいずれかであった場合にのみ存在します。

Data

データフィールドです。

2.6.11.4 IEEE802.1X 機能のアカウンティング動作

IEEE802.1X のアカウンティングは以下のようなタイミングで行われます。



本装置の IEEE802.1X 切断要因には以下のようなものがあります。

値	切断理由	意味
1	User Request	Supplicant から EAPoL-Logoff を受信した
20	Reauthentication Failure	再認証に失敗した
21	Port Reinitialized	リンクダウン、又は Supplicant 情報の削除が行われる CLI が実行された

■2.7 VLAN の設定

VLAN 機能を使用することにより、1 つのインタフェースを仮想的に複数の LAN として利用することが可能となります。

IX2000/IX3000 シリーズでは、VLAN タギングとポート VLAN をサポートしています。

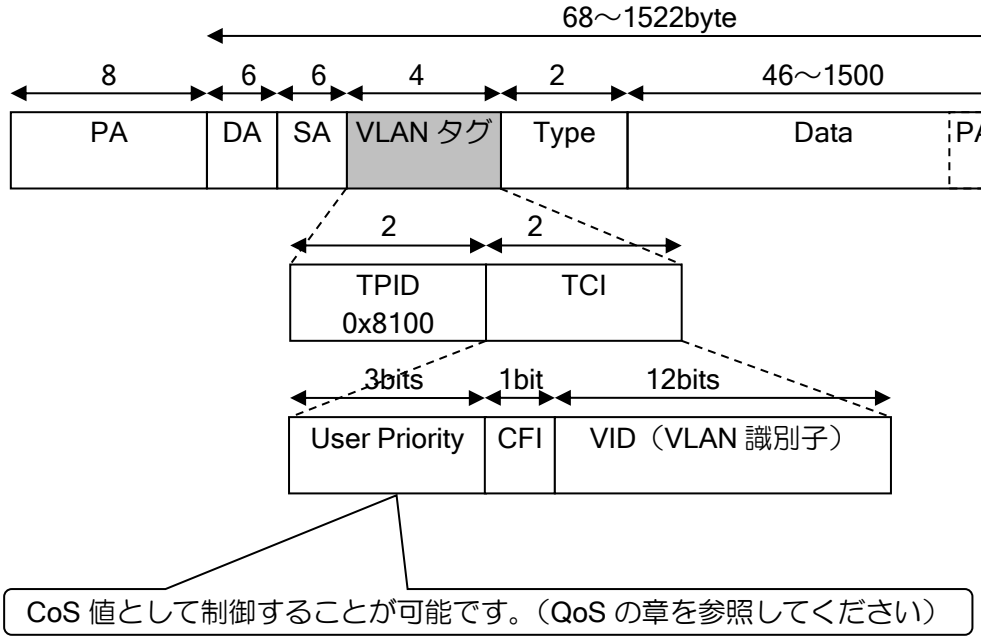
2.7.1 VLAN タギングの設定

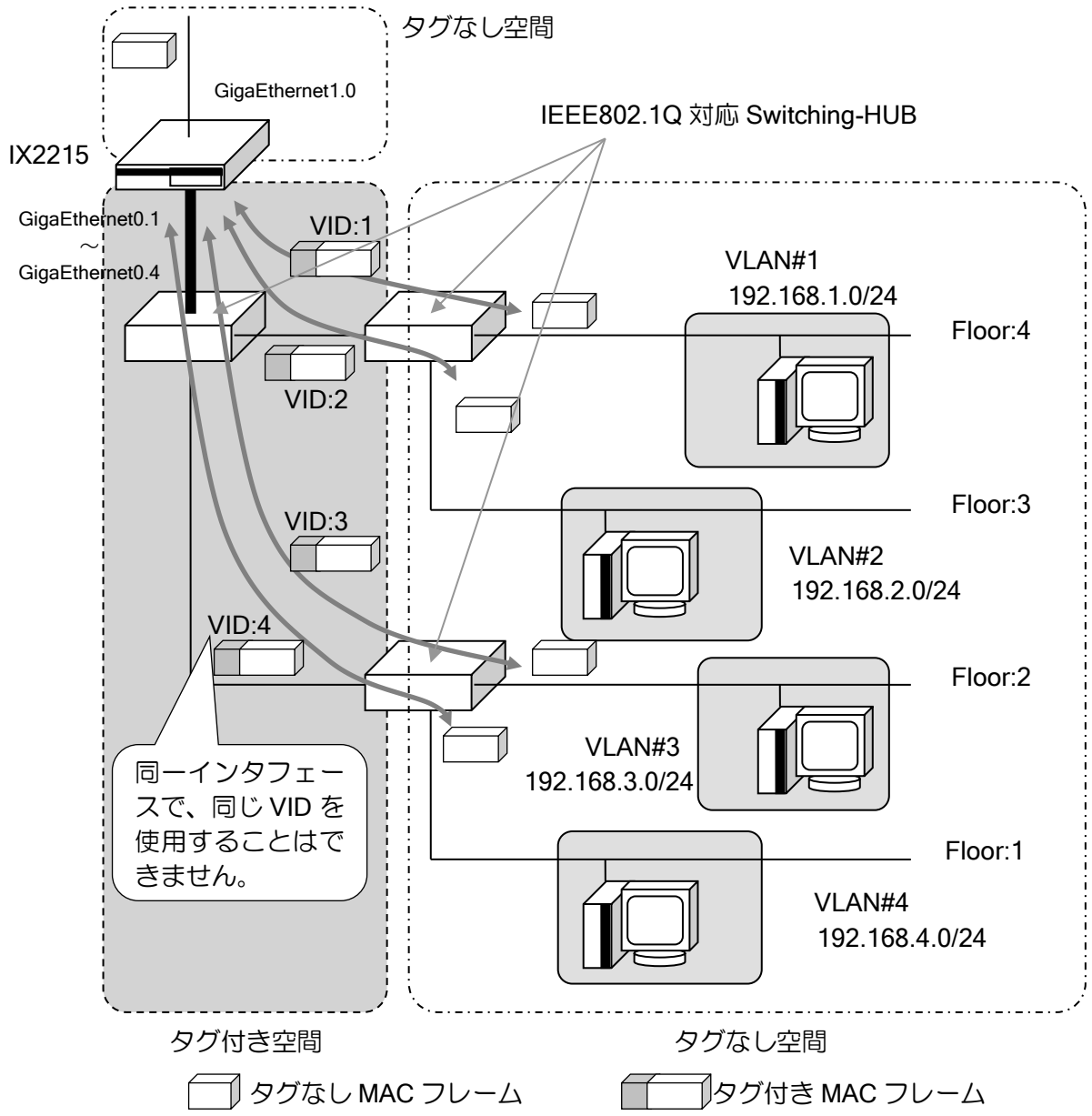
IX2000/IX3000 シリーズでは、VLAN タギング機能（IEEE802.1Q）をサポートしています。MAC フレームのタグと呼ばれる 4 オクテットの情報の中に VLAN 情報を組み込むことで、複数のスイッチング HUB を経由する VLAN（論理的な LAN）環境を実現することができます。

ただし、IEEE802.3 フレームフォーマットにタグが付与されている場合は受信できません。

インタフェース（GigaEthernet0.1-0.32 etc）
VLAN
デバイス（GigaEthernet0 etc）

Ethernet フレームフォーマット





以下に VLAN タギング登録のための設定および基本的な動作を説明します。

encapsulation dot1q	VLAN タギングの有効設定 （インタフェースコンフィグモード）

【設定例】

```
ip route default 10.10.10.1
interface GigaEthernet0.0
   ip address 192.168.0.254/24
   no shutdown
interface GigaEthernet0.1
   encapsulation dot1q 1
   ip address 192.168.1.254/24
   no shutdown
interface GigaEthernet0.2
   encapsulation dot1q 2
   ip address 192.168.2.254/24
```

GigaEthernet をタグ無しでも使用する場合に入力します。

```
   no shutdown
interface GigaEthernet0.3
   encapsulation dot1q 3
   ip address 192.168.3.253/24
   no shutdown
interface GigaEthernet0.4
   encapsulation dot1q 4
   ip address 192.168.4.253/24
   no shutdown
interface GigaEthernet1.0
   ip address 10.10.10.10/24
   no shutdown
```

(a) 最小フレームサイズ設定

タグを付与した場合の最小フレームサイズは、64byte または 68byte どちらでも良いことになっています。デフォルト値は 68byte です。

以下の設定で変更可能です。

dot1q min-frame-size	VLAN タギング時の最小フレームサイズ設定

【設定例】

最小フレームサイズを 64byte に設定

```
ip route default 10.10.10.1

interface GigaEthernet0.1
   encapsulation dot1q 1
   dot1q min-frame-size 64
   ip address 192.168.1.254/24
   no shutdown
```

2.7.2 ポート VLAN の設定

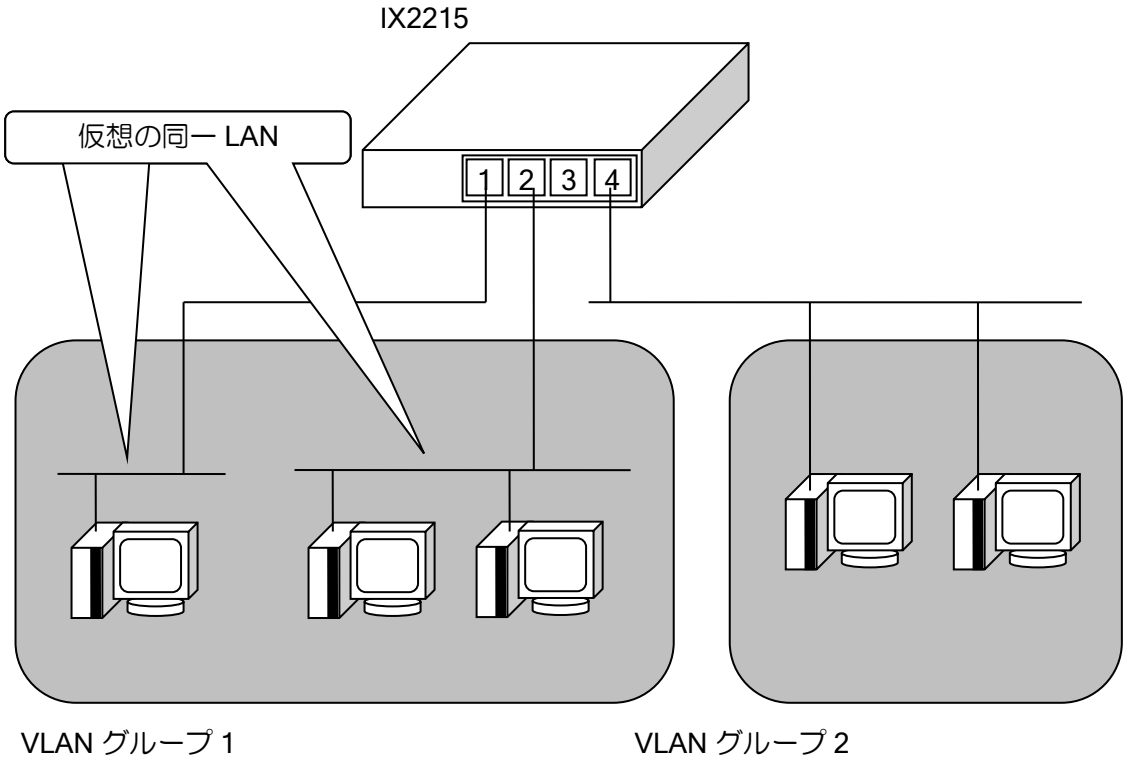
IX2000/IX3000 シリーズは SW-HUB カードでポート VLAN 機能をサポートしています。ポート VLAN を使用することで SW-HUB のポートをグループ化し、複数のセグメントとして利用することが可能となります。なお VLAN グループを設定していない場合は、SW-HUB として使用することができます。

- VRRP、ルーティングプロトコルを動作させることができます。
- 物理ポート単位に Rate，Duplex の設定ができます。

インタフェース（GigaEthernet2:1.1-1.8 etc）
VLAN
デバイス（GigaEthernet2）

以下にポート VLAN 登録のための設定および動作を説明します。

vlan-group	VLAN グループの設定 （デバイスコンフィグモード）
port	ポート毎の Rate,Duplex 設定 （デバイスコンフィグモード）



```
【設定例】

device GigaEthernet2
   vlan-group 1 port 1 2
   port 1 speed 100
   port 2 speed 10

interface GigaEthernet2.0
   ip address 192.168.1.254/24
   no shutdown

interface GigaEthernet2:1.0
   ip address 192.168.4.254/24
   no shutdown
```

ポート VLAN を設定した場合のインタフェースは以下のようになります。

```
[インタフェース][slot]/[port]:[group].[sub-interface]

GigaEthernet2.0     VLAN を設定していないインタフェース
                2.1
                  :
                2.8
                  :
                2:1.0 VLAN グループ 1  基本インタフェース
                2:1.1 VLAN グループ 1  サブインタフェース 1 PPPoE,タグ VLAN に使用
                2:1.2 VLAN グループ 1  サブインタフェース 2
                  :
                2:4.0 VLAN グループ 4
                2:4.1 VLAN グループ 4  サブインタフェース 1
                2:4.2 VLAN グループ 4  サブインタフェース 2
                  :
```

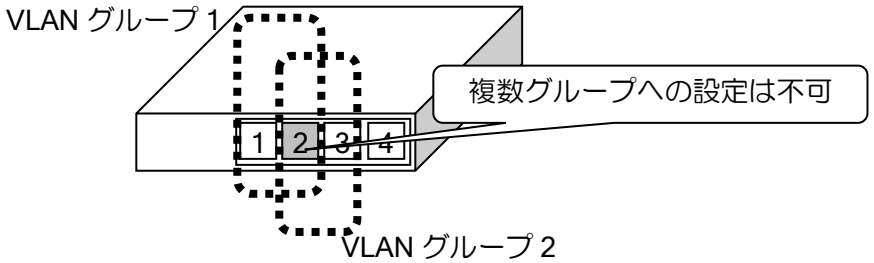
VLAN グループのサブインタフェース数の上限は、VLAN グループが設定されていない場合のサブインタフェース数の上限を SW-HUB のポート数で等分割したものになります。

2.7.3 VLAN の特徴と注意事項

VLAN 機能には下記のような特徴・注意事項があります。ネットワーク設計時には十分ご注意ください。

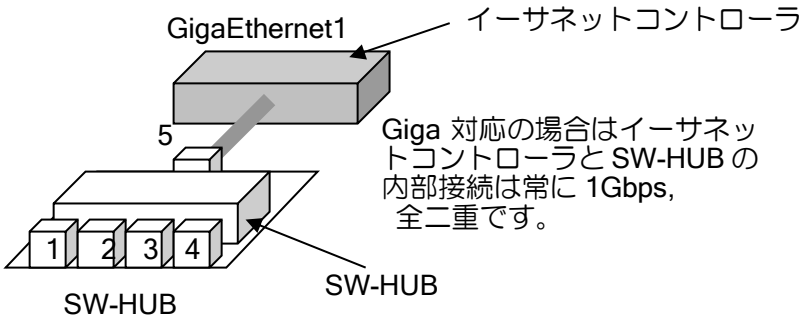
(a) VLAN グループの登録

1 つの VLAN グループに対して、複数の物理ポートを指定することはできますが、1 つの物理ポートに対して複数の VLAN グループを設定することはできません。



(b) 通信速度

SW-HUB とイーサネットコントローラの内部接続は、Giga 対応の場合は常に 1Gbps の全二重になります。非対応の場合は常に 100Mbps 全二重となります。



また、VLAN グループに対応するインタフェースの速度は、VLAN グループ内の最も早い回線速度になります。10Mbps のポートのみリンクアップしている場合インタフェースの速度は 10Mbps で、他のポートが 100Mbps でリンクアップした場合は 100Mbps となります。インタフェースは速度が変更になるとリセットがかかるため瞬断が発生します。問題がある場合は VLAN グループ内の回線速度が同一になるようにしてください。

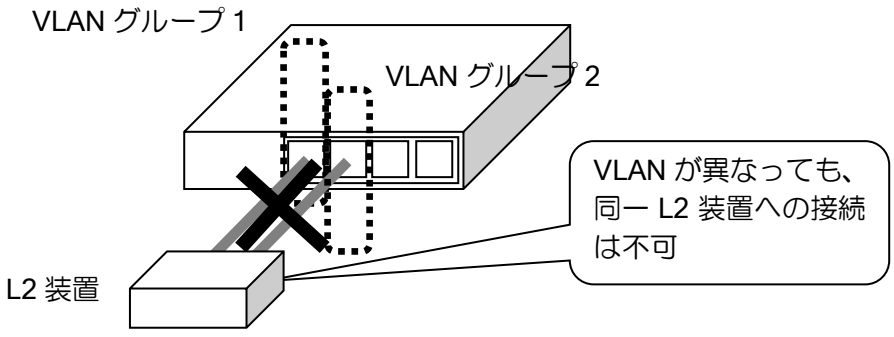
Ver9.2 以降では、デバイスコンフィグモードの no ifspeed-change コマンドにより、インタフェース速度を最大で固定し、速度変更による瞬断を抑止することが可能です。

(c) VLAN グループ間の通信

VLAN グループを設定した場合、SW-HUB 内では VLAN グループ間の通信は行われませんが、ルーティングによって VLAN グループ間の通信は可能です。VLAN グループ間の通信を行いたくない場合は、フィルタ等により VLAN グループ間の通信を制限する必要があります。

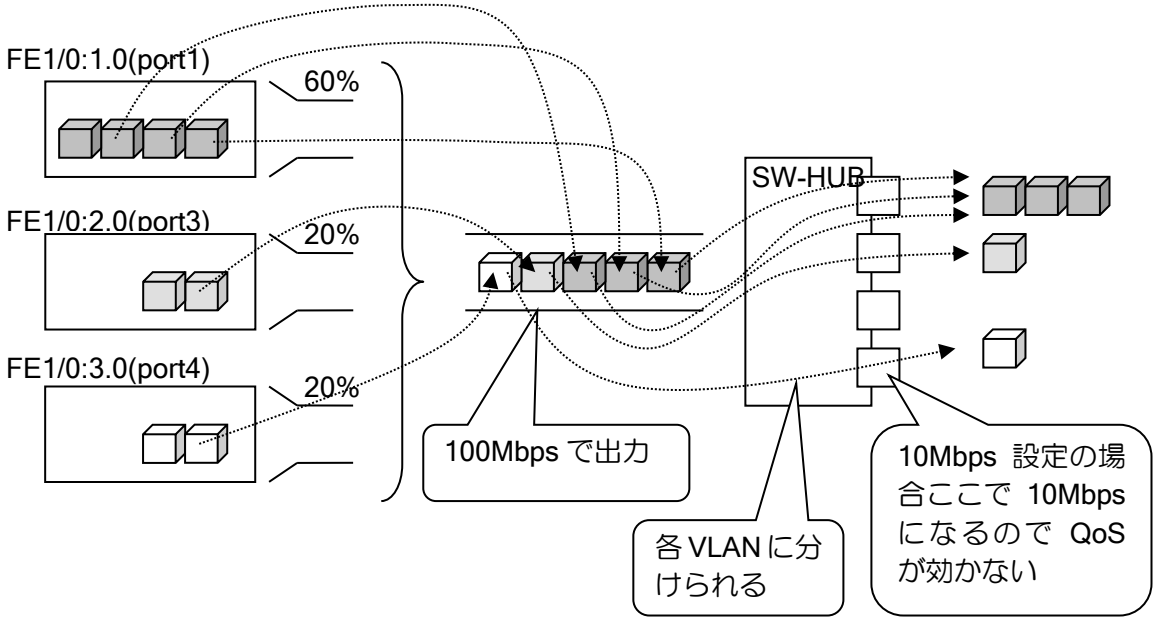
(d) MAC アドレス

SW-HUB のどのポートも同じ MAC アドレスが設定されます。そのため、VLAN グループやタグ VLAN が異なっても、同一の L2 装置のポートを接続した場合、同じ MAC アドレスが存在することになり、正常に通信を行うことができなくなる場合があります。



(e) 帯域制御

SW-HUB 側のインタフェースで QoS を設定した場合、QoS は内部接続の速度で動作することに注意してください。例えば 4FE SW-HUB を使用して 4 ポートとも 10Mbps に設定した場合、100Mbps を超えないと QoS は輻輳と判断せず、帯域制御は行われません。このような場合はシェーピング機能を併用する必要があります。



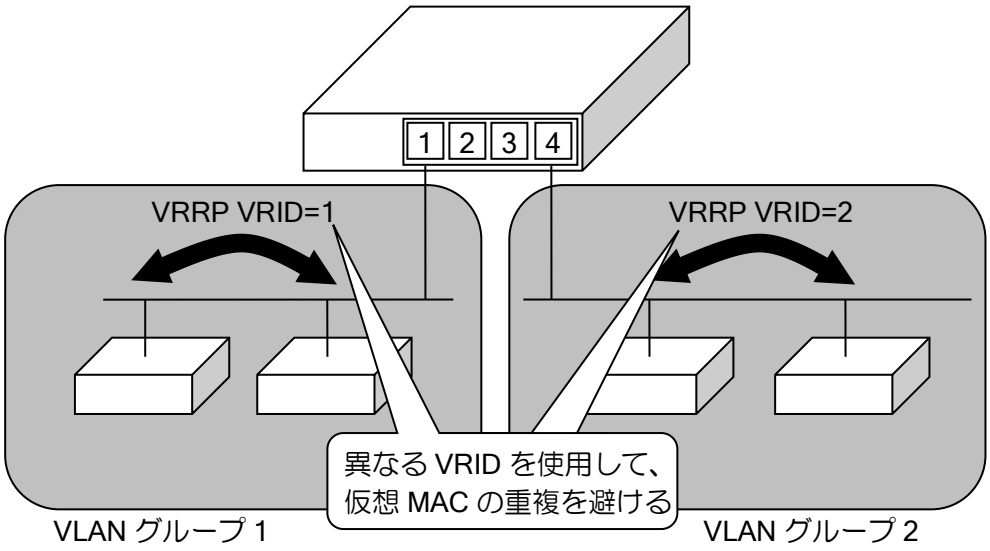
また、シェーピングの設定を行う場合も、SW-HUB のポートの速度を下げている場合は Bc が大きいと SW-HUB 内のキューで廃棄されて QoS の設定どおりに動作していないように見えることがありますのでご注意ください。

(f) OSPF のコスト計算

VLAN グループを設定したインタフェースに対して OSPF を設定した場合、グループ内の最も速いインタフェースの速度にしたがって OSPF のコスト計算を行います。

(g) VRRP など仮想 MAC アドレスの使用

タグ VLAN では、MAC アドレス学習テーブルが共通になっています。そのため、複数のタグ VLAN インタフェースにて VRRP などを使用する場合は、仮想 MAC アドレスが異なるようにしてください。



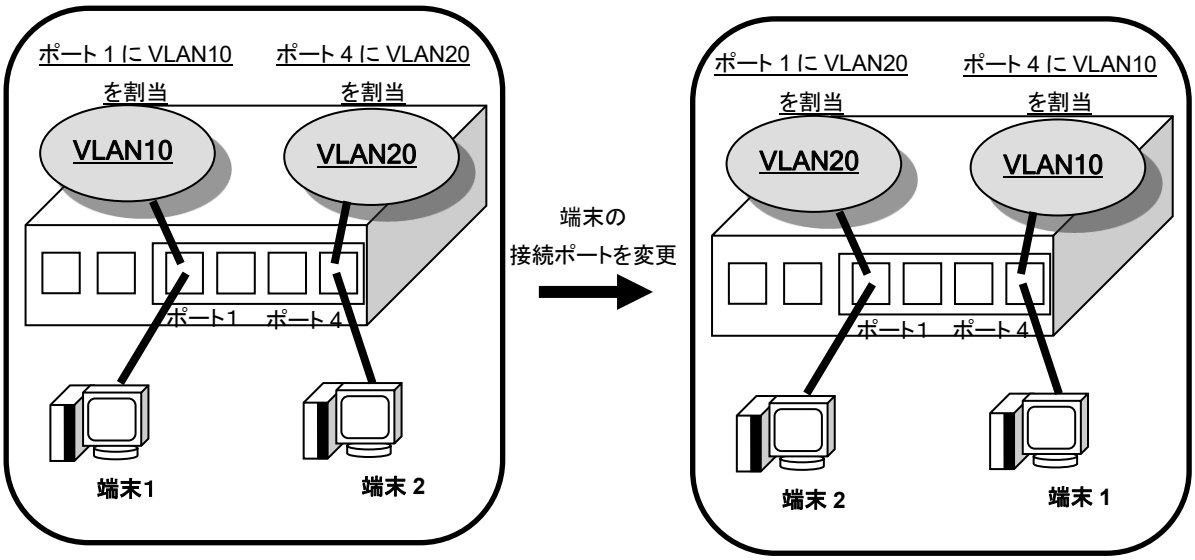
■2.8 ダイナミック VLAN 機能の設定

ダイナミック VLAN 機能を使用することによって、接続する端末の認証結果（※1）に応じて、端末が接続する VLAN を変更することができます。（Ver.10.0 以降）

※1 別途 RADIUS サーバを用意する必要があります。

2.8.1 ダイナミック VLAN 機能の概要

端末接続時に端末認証を行います。端末認証の結果、認証サーバから通知される VLAN ID を使用して、端末が接続するインタフェースの VLAN を決定します。本機能を利用することにより、端末を接続するポートに依存せず、接続する端末に応じた VLAN に接続することができます。



端末認証のために、IEEE802.1X 認証または、MAC 認証を使用します。どちらもローカルデータベースでの認証は対応していないため、RADIUS サーバを使用した認証が必要となります。
802.1X と MAC 認証は併用が可能です。

端末が未認証の状態では、インタフェースに設定した VLAN で動作します。この状態では、端末への送信を許可することができます。

認証に成功すると、接続したインタフェースに RADIUS サーバから通知された VLAN を割り当てます。

認証の結果が失敗の場合や、認証の応答が返らずタイムアウトした場合は、あらかじめ設定した VLAN に接続することができます。認証失敗時とタイムアウト時に接続する VLAN は IEEE802.1X 認証と MAC 認証でそれぞれ別な VLAN を設定できます。この場合、認証が成功していない状態（認証失敗、認証タイムアウト）でも、指定されている VLAN で通信することができます。

VLAN はポート単位で設定します。

2.8.2 ダイナミック VLAN の設定

以下の設定を行います。

- AAA 認証・RADIUS 認証の有効化
- ブリッジの有効化
- インタフェースへの bridge-group の割当
- IEEE802.1X または MAC 認証を使用したダイナミック VLAN の有効化
- ポートベース認証の適用

使用する VLAN の指定の際はブリッジグループを使用します。

2.8.2.1 AAA 認証、RADIUS 認証の設定コマンド

AAA 認証、RADIUS クライアントの設定は以下のコマンドを使用します。
詳細は「AAA の設定」の項を参照してください。

グローバルコンフィグモード	
aaa enable	AAA 機能の有効化
aaa group server	サーバグループの設定
aaa authentication dot1x	IEEE802.1X 認証リストの登録
radius host	RADIUS サーバホスト設定

2.8.2.2 IEEE802.1X 認証・MAC 認証設定コマンド

IEEE802.1X の設定は以下のコマンドを使用します。
詳細は「端末認証の設定」の項を参照してください。

インタフェースコンフィグモード	
dot1x enable	IEEE802.1X の有効化
dot1x dynamic-vlan	ダイナミック VLAN の有効化
dot1x port-control	認証動作の設定
dot1x port-control direction	フレーム制御方向の設定
dot1x access-control	認証単位の設定
dot1x authentication	AAA 認証リストの設定
dot1x event failure	認証失敗時に割り当てる VLAN 設定
dot1x event timeout	認証タイムアウト時に割り当てる VLAN 設定

MAC 認証の設定は以下のコマンドを使用します。
詳細は「端末認証の設定」の項を参照してください。

インタフェースコンフィグモード	
mac-auth enable	MAC 認証機能の有効化
mac-auth dynamic-vlan	ダイナミック VLAN の有効化
mac-auth port-control direction	フレーム制御方向の設定
mac-auth access-control	認証単位の設定
mac-auth event failure	認証失敗時に割り当てる VLAN 設定
mac-auth event timeout	認証タイムアウト時に割り当てる VLAN 設定

端末毎に VLAN を設定するため、認証単位はポートベース認証を使用します。
MAC ベース認証を使用する場合、1 ポートで複数の端末が接続されます。この場合は、最初に認証された端末の認証結果に応じた VLAN に接続します。後から接続された端末は認証を行いません。

未認証時は、インタフェースに設定した VLAN に接続しています。フレーム制御方向の設定内容に従って通信が許可されます。

認証失敗時、タイムアウト時に割り当てる VLAN を設定した場合は、認証失敗、タイムアウト時は設定した VLAN での双方向の通信が許可されます。認証失敗時、タイムアウト時は、再認証は行いません。

2.8.2.3 ブリッジ設定コマンド

ブリッジの設定は以下のコマンドを使用します。
詳細は「ブリッジの設定」の項を参照してください。

グローバルコンフィグモード	
bridge irb enable	ブリッジ機能（IRB）の有効化

インタフェースコンフィグモード	
bridge-group GROUP	ブリッジグループの設定

ブリッジグループを VLAN-ID として使用します。

端末が接続するインタフェースに設定したブリッジグループは未認証時に使用します。

2.8.2.4 RADIUS サーバの設定

RADIUS サーバでは以下のアトリビュートを使用します。

(a) IEEE802.1X 認証

番号	アトリビュート	Value
1	User-Name	Supplicant のユーザ名
30	Called-Station-Id	ルータインタフェースの MAC アドレス
31	Calling-Station-Id	Supplicant の MAC アドレス
6	Service-Type	端末に提供するサービスタイプ（Framed:2 固定）
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
5	NAS-Port	接続インタフェース番号（0x8000_0000+ifIndex）
61	NAS-Port-Type	接続インタフェースのタイプ（Ethernet:15 固定）
79	EAP-Message	EAP メッセージ
24	State	RADIUS サーバからの Access-Challenge に含まれている State アトリビュートをそのまま付与 （チャレンジに対する応答時に付与）
27	Session-Timeout	Authenticator のタイマ
80	Message-Authenticator	パケット全体の HMAC-MD5 ハッシュ値
81	Tunnel-Private-Group-ID	VLAN-ID（ブリッジグループ番号）

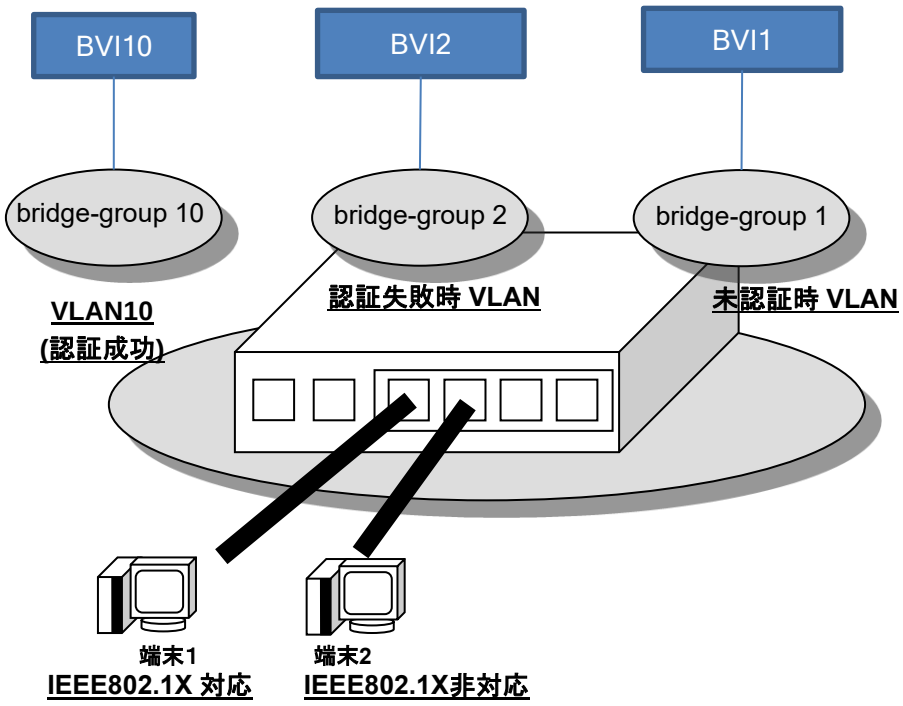
(b) MAC 認証

番号	アトリビュート	Value
1	User-Name	端末の MAC アドレス（書式は変更可能）
2	User-Password	上記 MAC アドレスの MD5
30	Called-Station-Id	ルータインタフェースの MAC アドレス
31	Calling-Station-Id	端末の MAC アドレス
6	Service-Type	端末に提供するサービスタイプ（Framed:2 固定）
5	NAS-Port	接続インタフェース番号（0x8000_0000+ifIndex）
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
61	NAS-Port-Type	接続インタフェースのタイプ（Ethernet:15 固定）

27	Session-Timeout	再認証タイマ
81	Tunnel-Private-Group-ID	VLAN-ID（ブリッジグループ番号）

2.8.2.5 設定例

ダイナミック VLAN を使用する場合の構成例と、その際のコンフィグを示します。




```
【設定例】
認証済みの端末はブリッジグループ 10 に接続
 - ブリッジグループ 10 は BVI10 と接続。
認証失敗端末はブリッジグループ 2 に接続
 - ブリッジグループ 2 は BVI2 と接続。
未認証端末はブリッジグループ 1 に接続
 - ブリッジグループ 1 は BVI1 に接続

aaa enable
aaa authentication dot1x default group radius
!
radius host ip 10.0.0.254 key 0 secret-key
!
Device GigaEthernet1
   vlan-group 1 port 1
   vlan-group 2 port 2
   vlan-group 3 port 3
   vlan-group 4 port 4
!
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   no shutdown
!
interface GigaEthernet1:1.0
```

```
   bridge-group 1
   dot1x enable
   dot1x dynamic-vlan
   dot1x access-control port-based
   dot1x event failure action bridge-group 2
   mac-auth enable
   mac-auth dynamic-vlan
   mac-auth access-control port-based
   mac-auth event failure action bridge-group 2
   no shutdown
!
interface GigaEthernet1:2.0
! GigaEthernet1:1.0 と同じ設定
interface GigaEthernet1:3.0
! GigaEthernet1:1.0 と同じ設定
interface GigaEthernet1:4.0
! GigaEthernet1:1.0 と同じ設定


interface BVI1
   ip address 192.168.1.254/24
   bridge-group 1
   no shutdown

interface BVI2
   ip address 192.168.2.254/24
   bridge-group 2
   no shutdown

interface BVI10
   ip address 192.168.10.254/24
   bridge-group 10
   no shutdown
```

2.8.3 端末認証機能の併用

ダイナミック VLAN 機能では IEEE802.1X 認証と MAC 認証を併用することができます。

IEEE802.1X の EAP パケットを受信したときは IEEE802.1X で認証します。EAP 以外の通常のフレームを受信した場合には、MAC 認証機能や Web 認証機能で認証します。

IEEE802.1X で使用する EAP のフレームは MAC 認証や Web 認証で廃棄しないため、これらの認証を設定しても IEEE802.1X 認証には影響はありません。

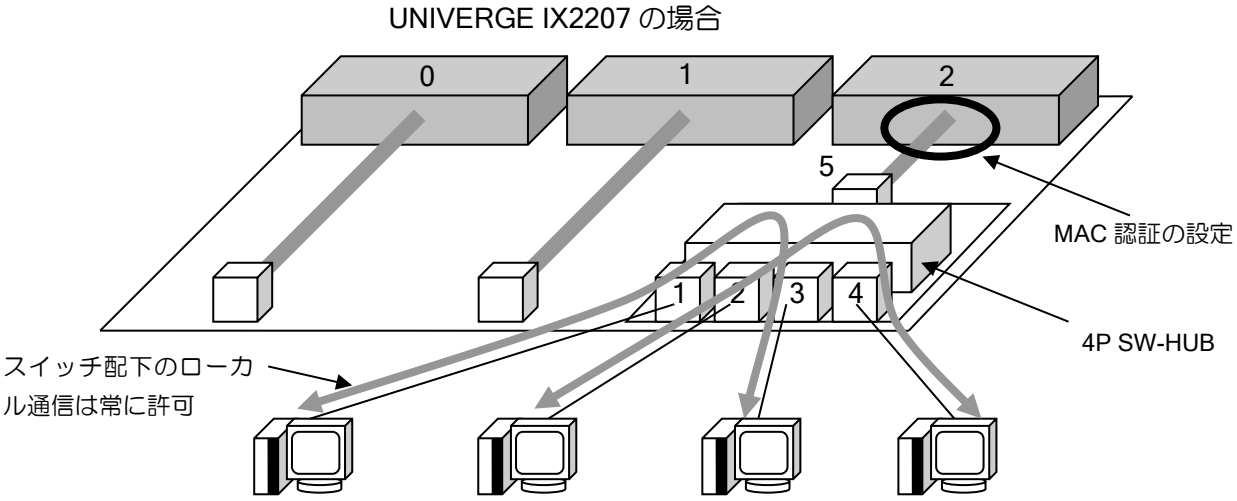
2.8.4 注意事項

(a) IEEE802.1X 検疫機能との併用

検疫フィルタ機能のフィルタ用のアトリビュートに Tunnel-Private-Group-Id を使用している場合、同一端末にて本機能との併用はできません。

(b) スイッチング HUB における注意事項

ポートベース VLAN を使用しない状態でのスイッチング HUB インタフェースにおける端末認証機能では、認証の可否に関わらずスイッチ配下のローカル通信は常に許可されます。



(c) 認証済み端末のインタフェースの移動

本装置の IEEE802.1X と MAC 認証機能による認証は、全てインタフェースごとに記憶されます。認証済みの端末であっても接続するインタフェースを移動した場合はそのインタフェースで再度認証処理を行う必要があります。

(d) ブリッジ機能との併用

ブリッジインタフェースで IEEE802.1X を有効化すると、IEEE802.1X フレームはそのインタフェースで終端されます。有効化しない場合はブリッジされます。

また BVI インタフェースでは IEEE802.1X 機能も MAC 認証も使用できません。

(e) 各機能使用時の注意事項

ダイナミック VLAN のために使用する各機能の注意事項については、各機能の項を参照してください。

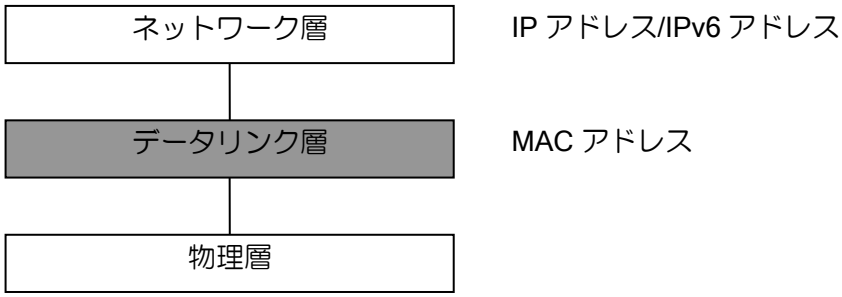
■2.9 ブリッジの設定

通常のルータは宛先の IP/IPv6 アドレス（ネットワーク層）から転送先を決定します。

ブリッジ機能を使用した場合は、宛先 MAC アドレス（データリンク層）から転送先を決定します。ブリッジ機能ではデータリンク層の情報を利用した機能(MAC フィルタ/MAC アクセスリスト等)を使用することができます。

ネットワーク層の情報は参照しませんので、ブリッジを設定したインタフェースでは、ネットワーク層の情報を利用した機能(NAT/URL オフロード/URL フィルタ等)は使用できません。

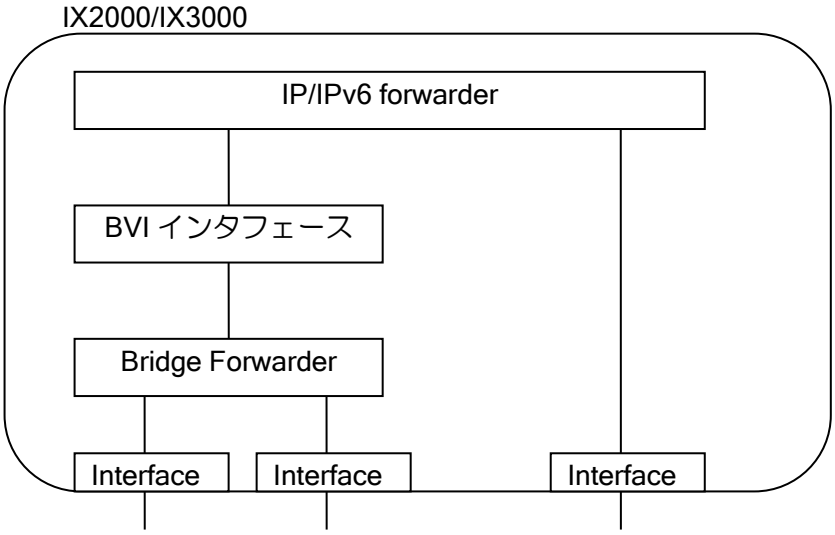
※ bridge ip filter コマンドを使用することで IP フィルタを使用することは可能です。



ブリッジとルータを併用する場合の動作の概要は次のようになります。

ブリッジ設定したインタフェースからのフレームは Bridge Forwarder に渡され、宛先に応じて転送されます。自装置宛のフレームは BVI インタフェース（詳細は後述）という仮想インタフェースに渡されます。IP/IPv6 パケットの場合は、更に IP/IPv6 Forwarder に渡され、宛先の IP/IPv6 アドレスに応じて転送されます。

ブリッジ機能使用時のブロック図



IX2000/IX3000 シリーズのブリッジ機能ではスパニングツリーはサポートしていませんので、パケットのループを検出できません。ループする可能性のある構成では、使用しないでください。また、ブリッジ機能は Ethernet のみサポートしています。Ethernet-PPP 間のブリッジはサポートしていません。

2.9.1 ブリッジの基本設定

グローバルコンフィグモード

bridge irb enable	ブリッジ機能（IRB）の有効化
bridge GROUP bridge ip/ipv6	ブリッジプロトコルの設定
bridge GROUP aging-time	アドレス学習テーブルのエントリ保持時間
bridge GROUP table-size	アドレス学習テーブルのテーブルサイズ

インタフェースコンフィグモード

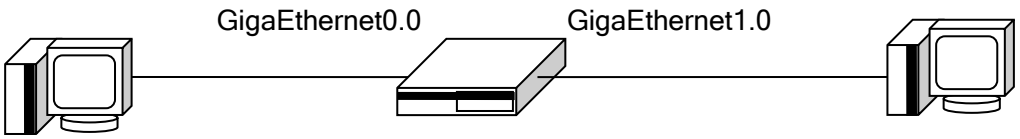
bridge-group GROUP	ブリッジグループの設定
bridge-group GROUP permanent-address	学習テーブルの固定エントリの登録

表示コマンド

show bridge	ブリッジの学習テーブルの表示
show bridge traffic	ブリッジの統計情報の表示

2.9.1.1 トランスペアレントブリッジ

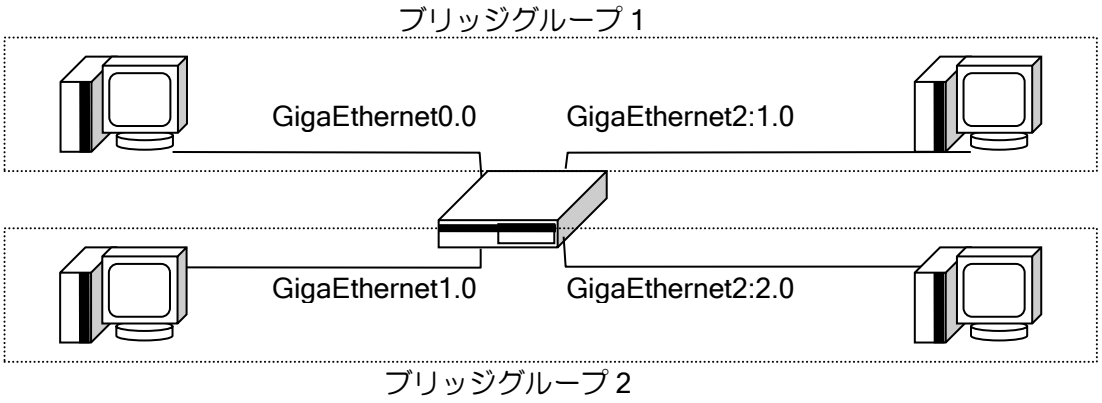
同じブリッジグループに属するインタフェース間を、MAC レベルで通信します。



【設定例】
GigaEthernet0.0，GigaEthernet1.0 でブリッジ

```
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
```

※ブリッジを有効にしたインタフェースでは、通常は IP/IPv6 アドレスを設定しないでください（ブルータ設定の場合を除く）。



【設定例】
GigaEthernet0.0 と GigaEthernet2:1.0 でブリッジ
GigaEthernet1.0 と GigaEthernet2:2.0 でブリッジ

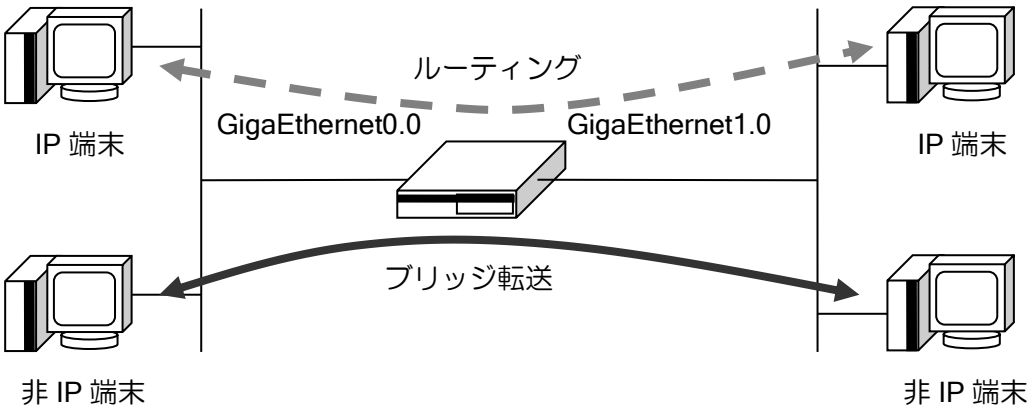
```
bridge irb enable
!
device GigaEthernet2
   vlan-group 1 port 1 2
   vlan-group 2 port 3 4
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 2
   no shutdown
!
interface GigaEthernet2:1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet2:2.0
   no ip address
   bridge-group 2
   no shutdown
```

※ ブリッジグループが異なる場合は、それぞれ独立にブリッジが構築されます。異なるブリッジグループに転送されることはありません。

2.9.1.2 ブルータの設定

インタフェースにブリッジの設定を行った場合、デフォルトでは全てのパケットをブリッジします（トランスペアレントブリッジ）。IPv4/IPv6 のどちらか、あるいは両方をブリッジしない設定を行うことにより、IP/IPv6 は通常通りルーティングを行い、非 IP を含むその他のパケットのみブリッジすることができます。

この場合、IP/IPv6 に関しては通常のインタフェースと同様な機能を使用することが可能です。これらのプロトコルに対してはブリッジの設定が全て無視されます。



【設定例】
IPv4 は通常通りルーティング
IPv6、その他のパケットは GigaEthernet0.0、GigaEthernet1.0 でブリッジ

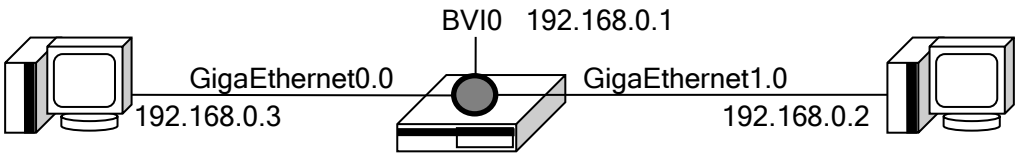
```
bridge irb enable
no bridge 1 bridge ip
!
interface GigaEthernet0.0
   ip address 192.168.0.1/24
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.0.0.1/24
   bridge-group 1
   no shutdown
```

2.9.1.3 BVI インタフェースの設定

ブリッジを有効にした状態で、ルータに telnet 等でアクセスする場合はブリッジ専用の仮想インタフェースである、BVI インタフェースを使用します。

BVI インタフェースは以下の特徴を持っています。

- インタフェースは、グループ内の何れかのインタフェースが up の時に、up します。
- インタフェースの速度は、グループ内の一番遅いインタフェースの速度に設定されます。
- MAC アドレスは最若番ポート（GigaEthernet0、または FastEthernet0/0）から取得します（Ver8.10 以前はグループ内から取得）



【設定例】
GigaEthernet0.0，GigaEthernet1.0 でブリッジ
BVI0 を使用して、192.168.0.1 宛のパケットを受信

```
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface BVI0
   ip address 192.168.0.1/24
   bridge-group 1
   no shutdown
!
```

BVI インタフェース使用時の注意事項

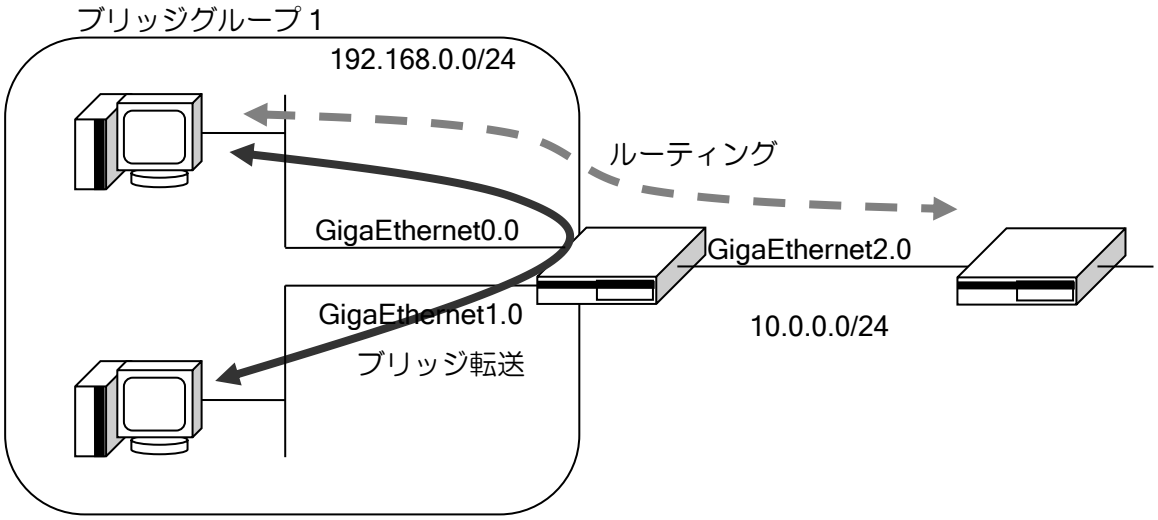
BVI インタフェースでは、以下の機能は使用できません。

- VRRP（Ver8.8 以降は利用可能）
- QoS（カラーリングは除く）

2.9.1.4 IRB（Integrated Routing and Bridging）

IP および IPv6 パケットに関しては、ブリッジとして使用しているインタフェースにおいても、仮想インタフェースであるBVIインタフェースを使用することにより、異なるブリッジグループ間、および、ブリッジを設定していないインタフェースとの間のルーティングを行うことができます。これにより、ブリッジグループを設定した複数のインタフェースをポート VLAN のように使用することができます。

非 IP パケットに関しては、異なるブリッジグループに属するインタフェースへ転送することはできません。

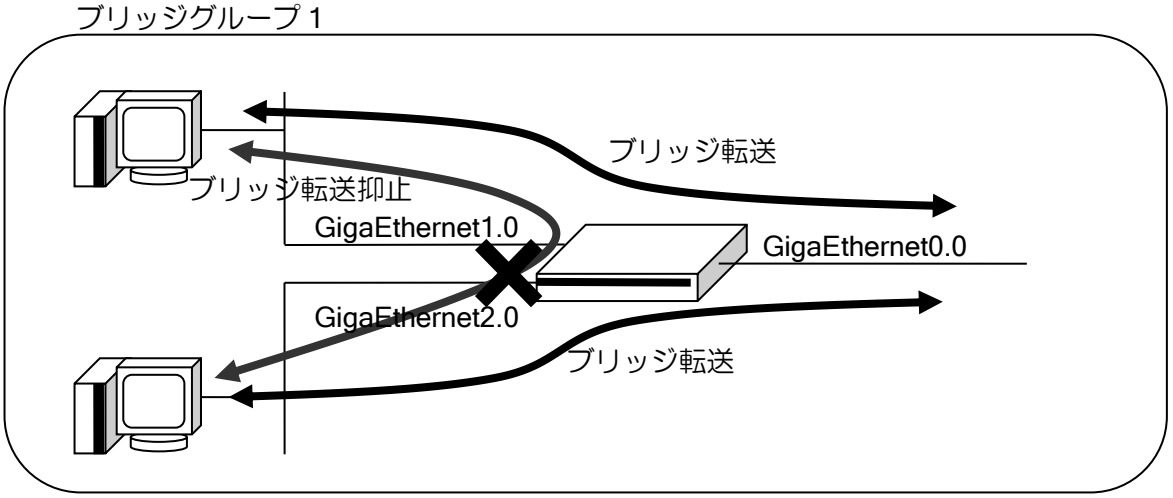


【設定例】
IP パケットをブリッジし、同時に BVI を経由してルーティングする。

```
ip route 10.0.1.0/24 10.0.0.2
!
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet2.0
   ip address 10.0.0.1/24
   no shutdown
!
interface BVI0
   ip address 192.168.0.1/24
   bridge-group 1
   no shutdown
```

2.9.1.5 ポート間転送抑止機能

ブリッジ設定したインタフェース配下にある端末間の通信が不要な場合、転送抑止設定を行うことにより、設定を行ったインタフェース間において、全てのフレームの転送を抑止することができます。Ver8.6 以降で対応しています。



bridge-group GROUP port-protected	インタフェース間フレーム転送抑止の設定

【設定例】
GigaEthernet1.0,GigaEtherent2.0 間のパケット転送を抑止。

```
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   bridge-group 1 port-protected
   no shutdown
!
interface GigaEthernet2.0
   no ip address
   bridge-group 1
   bridge-group 1 port-protected
   no shutdown
```

2.9.1.6 MAC アドレス学習数制限

ブリッジインタフェース毎に、学習する MAC アドレスの数を制限することができます。ブリッジインタフェース毎の学習数を超えた場合は、受信したフレームを廃棄します。固定エントリは学習数には含まれません。Ver.9.3 以降で対応しています。

bridge-group GROUP port-table-size	通信端末数制限設定（ポート単位）

【設定例】
GigaEthernet1.0, GigaEthernet2.0 の MAC アドレス学習数を 1 に制限。

```
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   bridge-group 1 port-table-size 1
   no shutdown
!
interface GigaEthernet2.0
   no ip address
   bridge-group 1
   bridge-group 1 port-table-size 1
   no shutdown
```

また、アドレス学習テーブルの設定でサイズを 0 に設定すると、MAC アドレス学習自体を抑制することができます。この場合は受信したフレームは廃棄でなく、常に MAC フレームをフラッディングする設定になります。なお SW-HUB の学習までは抑止できませんのでご注意ください。

bridge GROUP table-size	アドレス学習テーブルのテーブルサイズ

2.9.2 制限事項

SW-HUB を併用する場合、SW-HUB 自体の MAC アドレス学習機能およびポートベース VLAN 機能と競合する場合があるため、使用可能な構成と使用不可能な構成があります。

- SW-HUB でポートベース VLAN を設定し、それぞれの VLAN 間をブリッジする構成

1Gbps の SW-HUB を持つ装置は利用可能ですが、100Mbps の SW-HUB を持つ装置では利用できません。受信したパケットが別の VLAN で学習したアドレス宛の場合、SW-HUB が異なる VLAN 宛の通信と判断してパケットを廃棄するためです。

【構成例】
SW-HUB のポート 1,2 を VLAN グループ 1（GigaEthernet2:1.0）に設定。
GigaEthernet2:1.0 と GigaEthernet2:2.0 を同一ブリッジグループに設定。

```
bridge irb enable
!
device GigaEthernet2
   vlan-group 1 port 1 2
   vlan-group 2 port 3
   vlan-group 3 port 4
!
interface GigaEthernet2:1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet2:2.0
   no ip address
   bridge-group 1
   no shutdown
```

2.9.3 フィルタ

2.9.3.1 MAC フィルタ

MAC フィルタは、ブリッジ設定、ブルータ設定、およびブリッジを使用していない設定すべての場合で適用されます。全ての場合で、受信時には最初に、送信時には送信処理の直前でフィルタリングを行います。非 IP パケットは MAC フィルタでのみフィルタすることができます。

2.9.3.2 IP/IPv6 フィルタ

ブリッジング対象パケットに IP/IPv6 トラフィックフィルタを適用するには、ブリッジ IP/IPv6 トラフィックフィルタを使用します。

ブリッジ IP/IPv6 トラフィックフィルタ機能は通常の IP/IPv6 トラフィックフィルタと同様に、スタティックフィルタとダイナミックフィルタが使用できます。但し、強制リアセンブリ機能は使用できませんのでご注意ください。

トラフィックフィルタの詳細な設定の仕方はフィルタ機能の章を参照してください。コマンドの頭に”bridge”が入ることを除けば同様のイメージで設定できます。

インタフェースコンフィグモード

bridge ip/ipv6 filter	ブリッジ IP/IPv6 トラフィックフィルタの設定

表示コマンド

show bridge ip/ipv6 filter	フィルタエントリ情報の表示
show bridge ip/ipv6 filter statistics	統計情報の表示
show bridge ip/ipv6 filter dynamic	ダイナミックフィルタキャッシュの表示

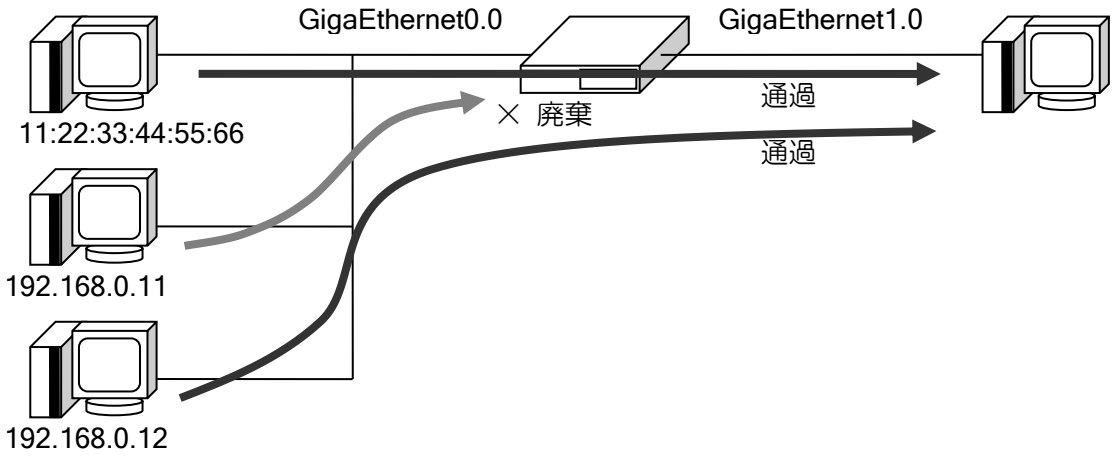
クリアコマンド

clear bridge ip/ipv6 filter hit-count	ヒットカウントのクリア
clear bridge ip/ipv6 filter statistics	統計情報のクリア （ヒットカウントも含めてクリアします）
clear bridge ip/ipv6 filter dynamic	ダイナミックフィルタキャッシュのクリア

ブルータ機能によりルーティング対象プロトコルに指定しているパケットにフィルタを適用する場合には、通常の IP/IPv6 トラフィックフィルタを使用します。BVI インタフェースでパケットにフィルタを適用したい場合も通常の IP/IPv6 トラフィックフィルタを使用します。

2.9.3.3 ブリッジの設定例

IP/IPv6 パケット，非 IP パケットともにブリッジを行う設定となっているインタフェースでパケットにフィルタを適用したい場合、ブリッジ IP フィルタを使用します。また、MAC フィルタも使用できます。



【設定例】
送信元 IP アドレスでフィルタ

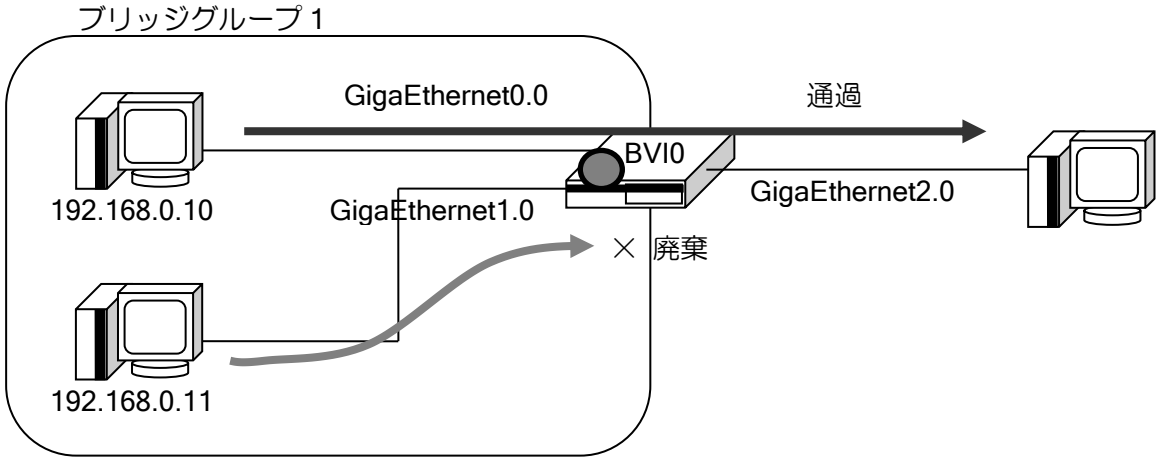
```
ip access-list acl1 permit ip src 192.168.0.12/32 dest any
!
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   bridge ip filter acl1 100 in
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
```

【設定例】
MAC アクセスリストのオフセット指定を使用して、送信元アドレスが
192.168.0.11 のパケットをフィルタ
（26 オクテット目[タグ無しの場合]から 4 オクテットが c0a8000b）

```
access-list delete deny src any dest any offset 26 4 c0a8000b
access-list delete permit src any dest any
!
bridge irb enable
!
interface GigaEthernet0.0
   filter delete 10 in
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
```

2.9.3.4 IRB の設定例

BVI を使用してルータにアクセスする場合、また IRB 機能により BVI 経由でルーティングする場合は、BVI インタフェースで IP フィルタおよび MAC フィルタを設定することができます。



【設定例】
BVI インタフェースを使用して、送信元 IP アドレスでフィルタ

```
ip access-list acl1 deny ip src 192.168.0.11/32 dest any
ip access-list acl1 permit ip src any dest any
!
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
```

```
!
interface GigaEthernet2.0
   ip address 10.0.0.1/24
   no shutdown
!
interface BVI0
   ip address 192.168.0.1/24
   ip filter acl1 10 in
   bridge-group 1
   no shutdown
```

2.9.4 TCP-MSS 調整

ブリッジング対象パケットに対して TCP-MSS 調整機能を適用可能です。これにはブリッジ TCP-MSS 調整機能を使用します。ブリッジ TCP-MSS 調整機能は EtherIP トンネルインタフェースでも設定可能です。

書き換えに指定する最適な MSS 値については「IPv4 の設定」「IPv6 の設定」のそれぞれの章の「TCP-MSS 調整」の項を参照してください。

インタフェースコンフィグモード

bridge ip/ipv6 tcp adjust-mss	ブリッジ TCP-MSS 調整機能の設定

【設定例】
GigaEthernet1.0 を通過する IP パケットの TCP SYN ペイロード中の MSS 値を 1414 に書き換える。

```
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   bridge ip tcp adjust-mss 1414
   no shutdown
```

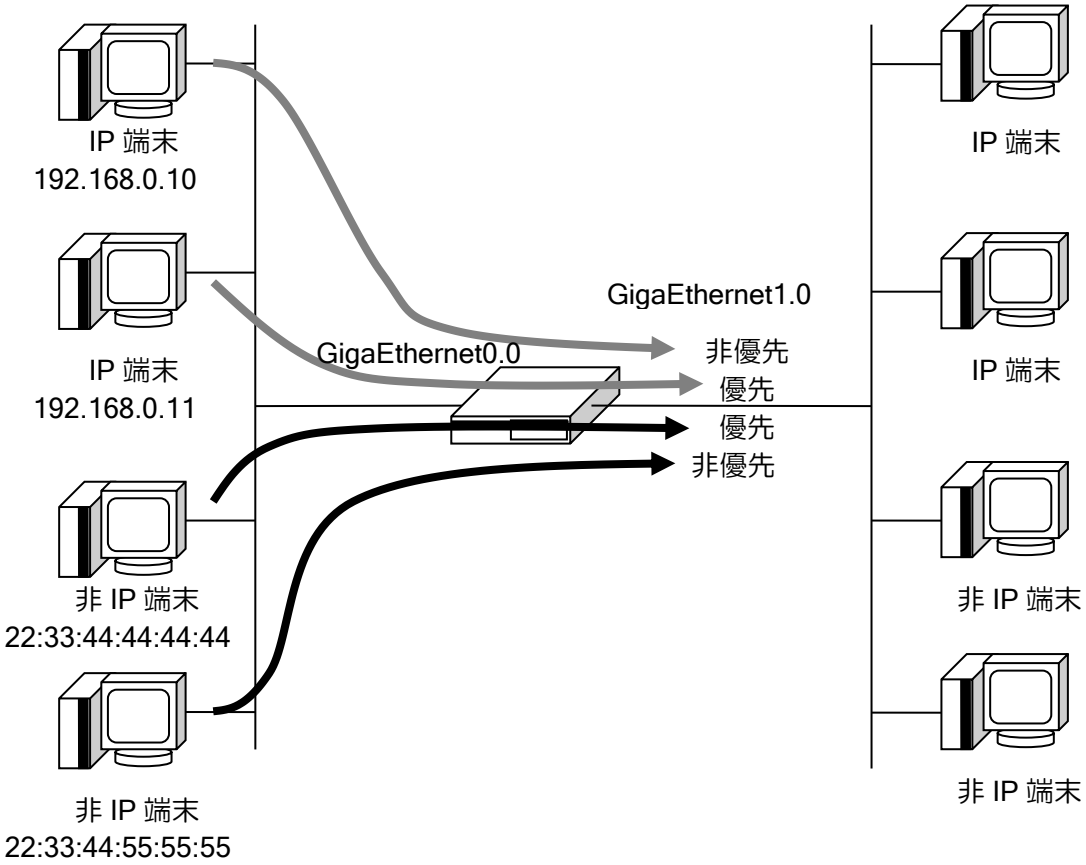
2.9.5 QoS

2.9.5.1 クラスベースキューイング（CBQ）／プライオリティキューイング（PQ）

ブリッジグループを設定した場合も、他の場合と同様にインタフェース単位で設定します。基本的な設定方法は通常の CBQ/PQ の設定方法と同様です。CBQ/PQ の詳細な設定については、QoS の項を参照してください。

※ IP, IPv6 をブリッジしているインタフェースでは match ip/ipv6 access-list を使用できません。また、match access-list（MAC アクセスリスト）はブリッジしているプロトコルのみで適用されます。

(a) MAC アクセスリスト



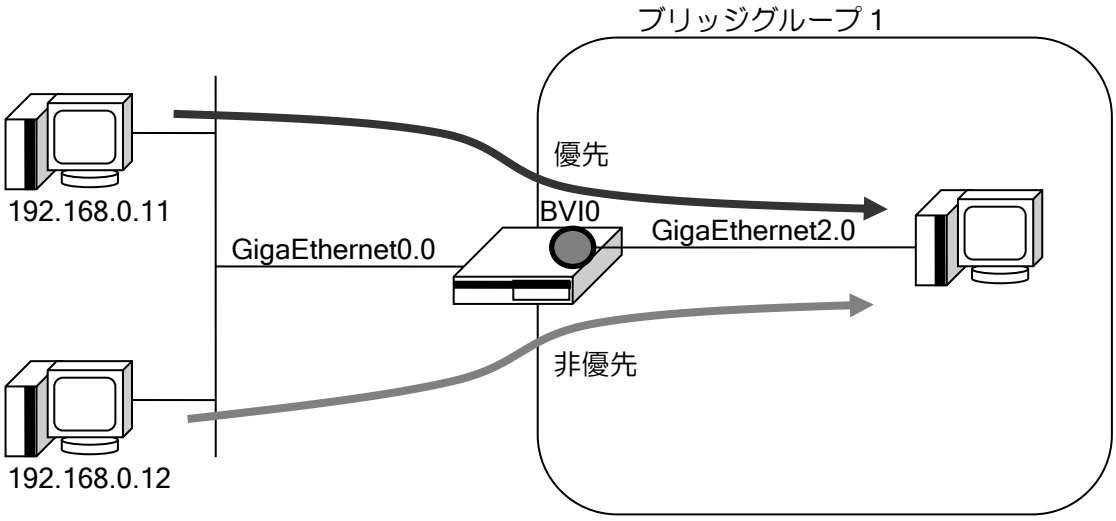
【設定例】
送信元のアドレスで PQ を設定

```
access-list highpri permit src 22:33:44:44:44:44 dest any
access-list lowpri permit src any dest any
ip access-list highpri permit ip src 192.168.0.11/32 dest any
ip access-list lowpri permit ip src any dest any

bridge irb enable
no bridge 1 bridge ip
no bridge 1 bridge ipv6
!
class-map match-any test
   match access-list highpri high
   match access-list lowpri low
   match ip access-list highpri high
   match ip access-list lowpri low
!
policy-map test-policy
   class test
   class class-local
   class class-default
!
interface GigaEthernet0.0
   ip address 10.1.0.1/24
   bridge-group 1
   no shutdown
```

```
!
interface GigaEthernet1.0
   ip address 10.2.0.1/24
   bridge-group 1
   service-policy enable
   service-policy output test-policy
   no shutdown
```

(b)QoS グループの使用

ブリッジを設定したインタフェースでは、データリンク層の情報のみ参照します。そのため、出力に QoS を設定する場合、IP アドレス等の情報を参照することができません。このような場合、QoS グループを使用します。入力インタフェースで IP アドレス等に応じて QoS グループを設定し、出力インタフェースで QoS グループを参照することにより、IP アドレス等の情報を使用した QoS の設定を行うことができます。



【設定例】
送信元の IP アドレスに応じて、QoS グループを設定。
出力インタフェースでは QoS グループを条件に QoS を実行。

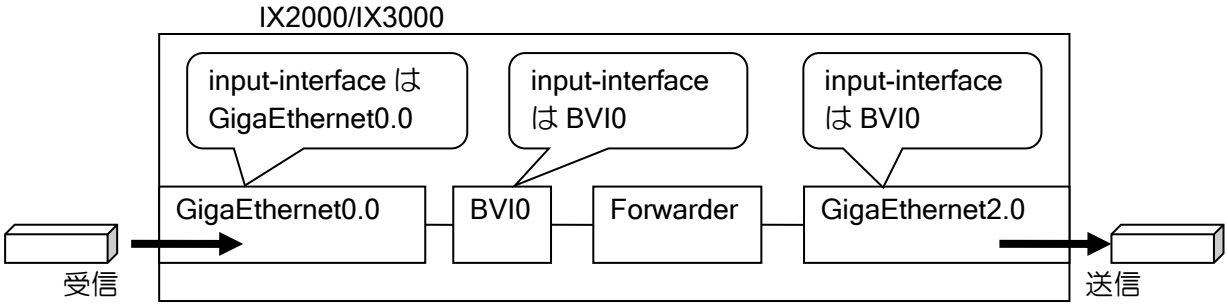
```
ip access-list high-priority permit ip src 192.168.0.11/32 dest any
ip access-list low-priority permit ip src 192.168.0.12/32 dest any
!
bridge irb enable
!
class-map match-any group1
   match ip access-list high-priority normal
!
class-map match-any group2
   match ip access-list low-priority normal
!
class-map match-any test
   match qos-group 1 high
   match qos-group 2 low
!
policy-map set-group
```

```
   class group1
      set qos-group 1
   class group2
      set qos-group 2
   class class-local
   class class-default
!
policy-map test-policy
   class test
   class class-local
   class class-default
!
interface GigaEthernet0.0
   ip address 192.168.0.1/24
   service-policy input set-group
   no shutdown
!
interface GigaEthernet2.0
   no ip address
   bridge-group 1
   service-policy enable
   service-policy output test-policy
   no shutdown
!
interface BVI0
   ip address 100.0.0.1/24
   bridge-group 1
   no shutdown
```

(c) 注意事項

- match input-interface に関して

  BVI インタフェースを使用している場合、BVI で受信するデータの入力インタフェースは GigaEthernet0.0 などのインタフェースですが、BVI で受信し、他のインタフェースへ出力する際に QoS 設定で match input-interface を使用する場合、入力インタフェースは GigaEthernet0.0 ではなく、BVI インタフェースとなります。



上記のような場合に、出力インタフェースにおいて、入力インタフェースを GigaEthernet0.0 として扱いたい場合は、GigaEthernet0.0 での受信時に QoS グループを設定し、出力インタフェースでは QoS グループを match 条件として使用してください。

【設定例】
GigaEthernet0.0 から受信したパケットを高優先
GigaEthernet1.0 から受信したパケットを低優先

```
bridge irb enable
!
class-map match-any set-group
   match any normal
!
class-map match-any out-class
   match qos-group 1 high
   match qos-group 2 low
!
policy-map ge0.0
   class set-group
      set qos-group 1
   class class-local
   class class-default
!
policy-map ge1.0
   class set-group
      set qos-group 2
   class class-local
   class class-default
!
policy-map out-policy
   class out-class
   class class-local
   class class-default
!
interface GigaEthernet0.0
   no ip address
   service-policy input ge0.0
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   service-policy input ge1.0
   bridge-group 1
   no shutdown
!
interface GigaEthernet2.0
   ip address 100.0.0.1/24
   service-policy enable
   service-policy output out-policy
   no shutdown
!
interface BVI0
   ip address 192.168.0.1/24
   bridge-group 1
   no shutdown
```

2.9.5.2 シェーピング

クラス単位または、出力インタフェース単位でシェーピングを行います。同一のブリッジグループ全体でのシェーピングを行うことはできません。また、BVI インタフェースでシェーピングの設定はできません。

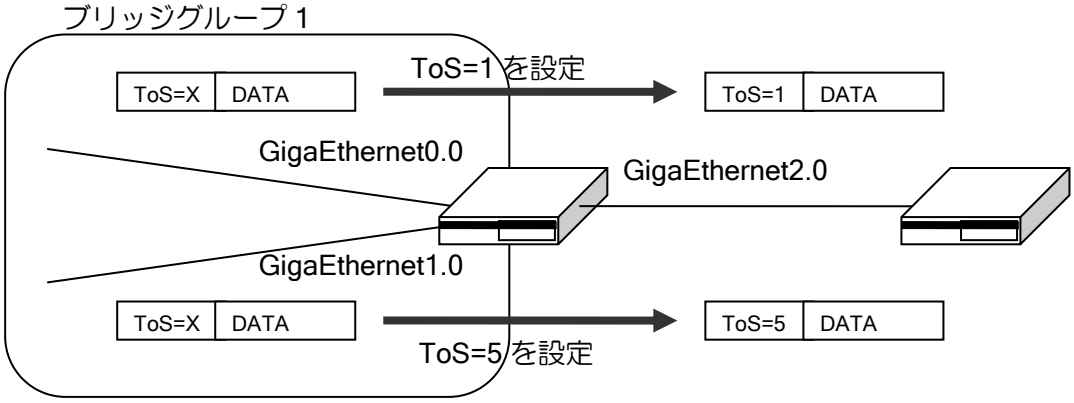
設定方法は通常のシェーピングと同様です。

2.9.5.3 QoS パラメータの付与

(a) DSCP /IP precedence 値の付与

IP パケットを含む全てのパケットをブリッジする設定を行っているインタフェースでは DSCP/IP precedence 値の付与はできません。設定を行った場合、設定は無効となります。

このような場合、BVI インタフェースにおいて DSCP/IP Precedence 値の付与を行います。



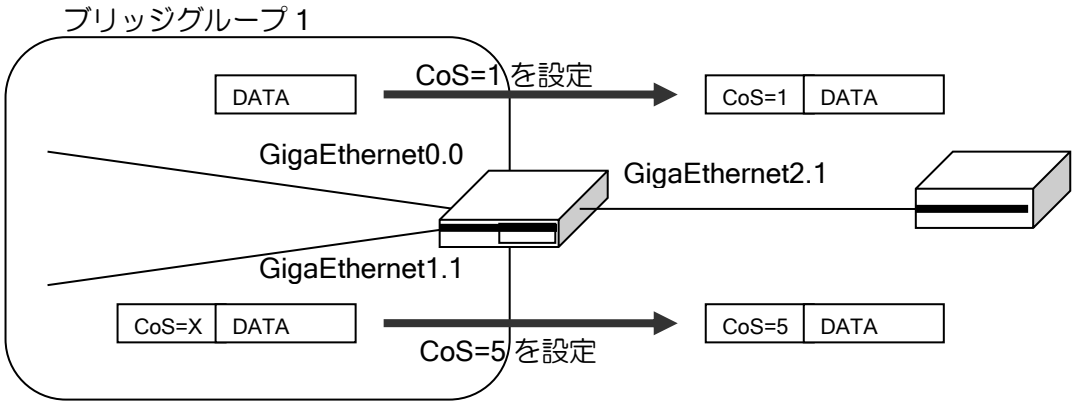
【設定例】
GigaEthernet0.0 から入力したパケットに ToS=1 を設定。
その他のインタフェースから入力したパケットに ToS=5 を設定。

```
bridge irb enable
!
class-map match-any tos1
   match input-interface GigaEthernet0.0
!
policy-map set-tos
   class tos1
      set ip precedence 1
   class class-local
   class class-default
      set ip precedence 5
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet2.0
   ip address 100.0.0.1/24
```

```
   no shutdown
!
interface BVI0
   ip address 192.168.0.1/24
   bridge-group 1
   service-policy input set-tos
   no shutdown
```

(b)CoS 値の付与

IP パケットを含む全てのパケットをブリッジする設定を行っているインタフェースでは CoS 値のみ付与することができます。入力インタフェースで設定を行った場合は、実際にパケットを出力する時点で CoS 値を設定します。出力インタフェースがタグ VLAN 以外の場合には本設定は無効となります。



【設定例】
GigaEthernet0.0 から入力したパケットに CoS=1 を設定。
その他のインタフェースから入力したパケットに CoS=5 を設定。

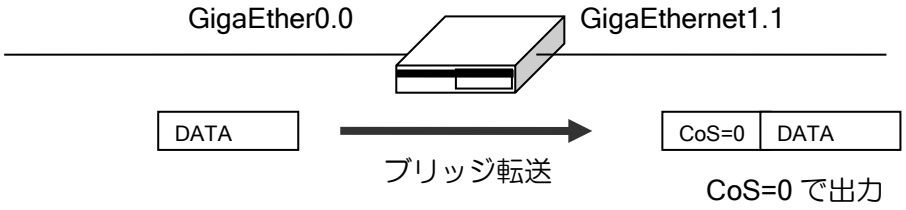
```
bridge irb enable
!
class-map match-any cos1
   match input-interface GigaEthernet0.0 normal
!
policy-map set-cos
   class cos1
      set cos 1
   class class-local
   class class-default
      set cos 5
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   service-policy input set-cos
   no shutdown
!
interface GigaEthernet1.1
   encapsulation dot1q 10 tpid 8100
   no ip address
   bridge-group 1
   service-policy input set-cos
   no shutdown
```

```
!
interface GigaEthernet2.1
   encapsulation dot1q 1 tpid 8100
   auto-connect
   ip address 10.0.0.1/24
   no shutdown
!
interface BVI0
   ip address 192.168.0.1/24
   bridge-group 1
   no shutdown
```

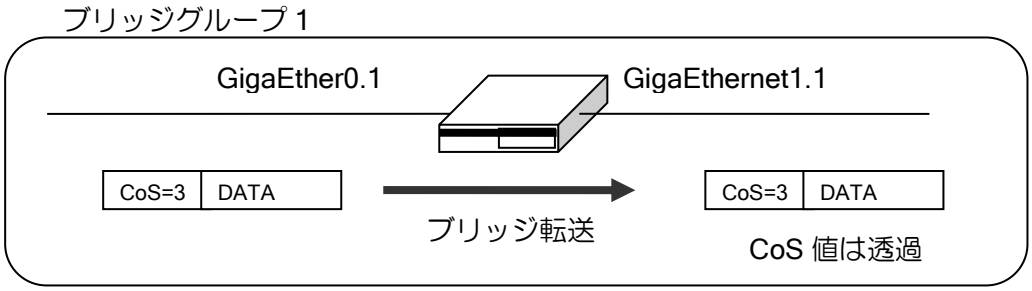
CoS 値設定を行わない場合、同一ブリッジグループ内のタグ VLAN インタフェースへ出力する CoS 値は入力時の CoS 値が設定されます。入力インタフェースがタグ VLAN 以外の場合は出力する CoS 値は 0 となります。異なるブリッジグループおよび、ブリッジグループを設定していないタグ VLAN インタフェースへ出力する場合は、入力の CoS 値にかかわらず、出力する CoS 値は 0 となります。

CoS 付与を行わない場合の出力 CoS 値

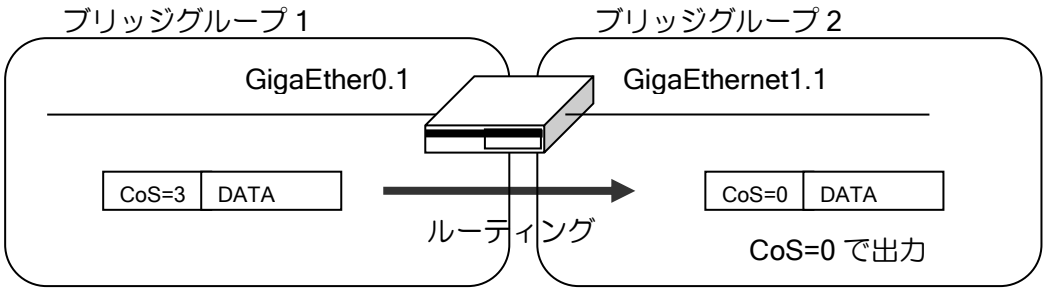
・入力がタグ VLAN 以外



・入力がタグ VLAN、同一ブリッジグループへ出力



・入力がタグ VLAN、異なるブリッジグループへ出力



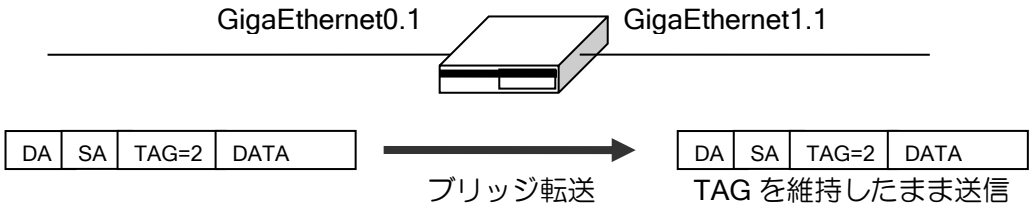
2.9.6 VLAN

2.9.6.1 VLAN タグ設定

VLAN タグ付きのフレームをブリッジしたい場合、基本的には encapsulation dot1q のインタフェースを作成して、そこに bridge-group の設定を行います。VLAN タグ番号を設定したインタフェースは、設定したタグをもつ VLAN フレームのみ送受信するインタフェースになります。

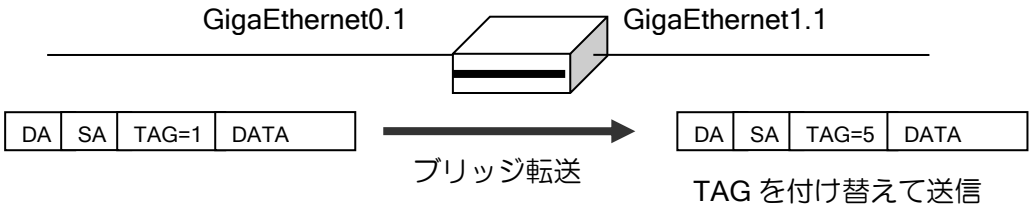
通常はブリッジを組んだ複数のインタフェースに同じ VLAN タグを設定し、VLAN タグ透過ブリッジとして利用します。BVI を同じグループにすることで BVI にアクセスすることも可能です。この場合、IRB 機能により BVI を介してルーティングされますので複数の VLAN を設定する場合は注意してください。

```
【設定例】
!
bridge irb enable
!
interface GigaEthernet0.1
   encapsulation dot1q 2 tpid 8100
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.1
   encapsulation dot1q 2 tpid 8100
   no ip address
   bridge-group 1
   no shutdown
```



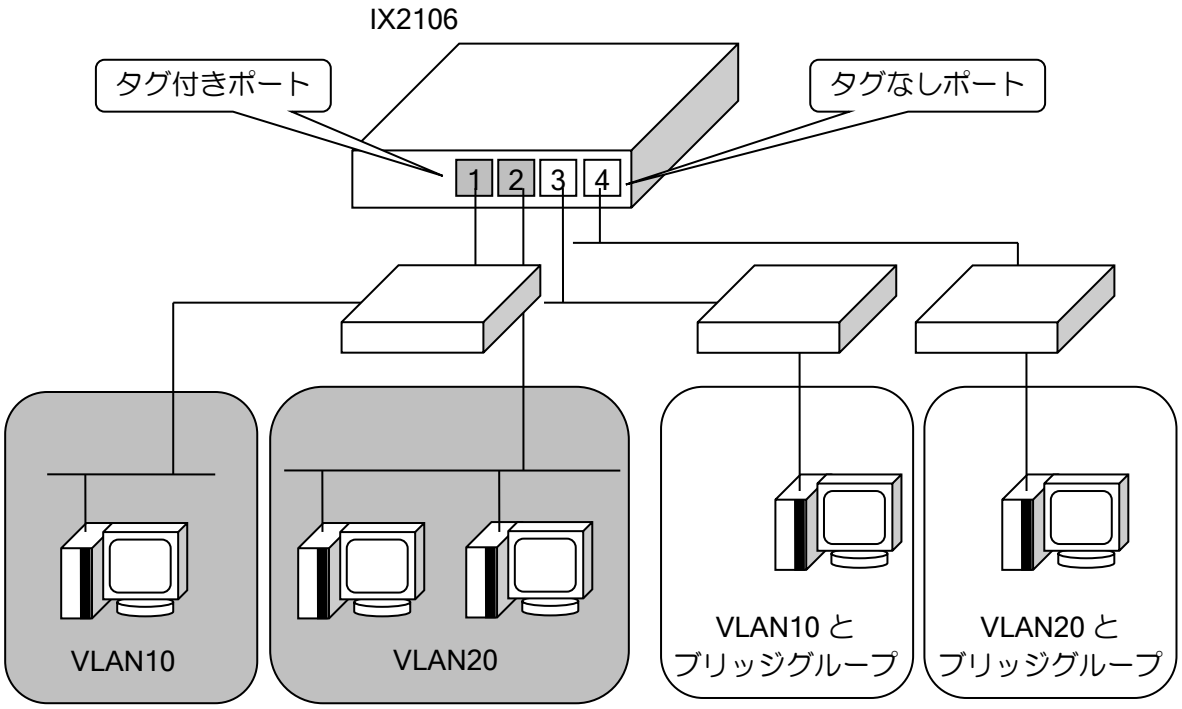
ブリッジのインタフェースに複数の VLAN タグを設定すると、VLAN タグを変換するブリッジになります。この場合も BVI を同じグループにすることで BVI にアクセスすることが可能です。

```
【設定例】
!
bridge irb enable
!
interface GigaEthernet0.1
   encapsulation dot1q 1 tpid 8100
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.1
   encapsulation dot1q 5 tpid 8100
   no ip address
   bridge-group 1
   no shutdown
```



※CoS 値の変更が可能です。

VLAN タグ付きのポートとタグなしのポートをブリッジしたい場合、下記設定となります。これにより、L2-SW のトランクポート・アクセスポートにあたる構成を実現できます。




```
【設定例】
bridge irb enable
 !
 device GigaEthernet1
    vlan-group 1 port 1 2
    vlan-group 2 port 3
    vlan-group 3 port 4
 !
 interface GigaEthernet1:1.1
    encapsulation dot1q 10 tpid 8100
    auto-connect
    no ip address
    bridge-group 1
    no shutdown
 !
 interface GigaEthernet1:1.2
    encapsulation dot1q 20 tpid 8100
```

```
    auto-connect
    no ip address
    bridge-group 2
    no shutdown
!
interface GigaEthernet1:2.0
    no ip address
    bridge-group 1
    no shutdown
!
interface GigaEthernet1:3.0
    no ip address
    bridge-group 2
    no shutdown
!
interface BVI0
    ip address 192.168.10.1/24
    bridge-group 1
    no shutdown
!
interface BVI1
    ip address 192.168.20.1/24
    bridge-group 2
    no shutdown
```

2.9.6.2 特殊な VLAN タグ設定

VLAN インタフェースで受信されなかった VLAN フレームは、基本インタフェースにブリッジの設定があれば「解析できなかった不明フレーム」という扱いで、基本インタフェースのブリッジで受信されます。この性質を利用して以下の設定を行うことができます。

- VLAN タグ付与, VLAN２重タグ設定
- VLAN タグ透過

解析できなかった不明フレームとして扱うため、ここで設定される VLAN フレームでは BVI は利用できません。そのフレームが実際は IP か IPv6 かなどの情報を取得させていないためです。

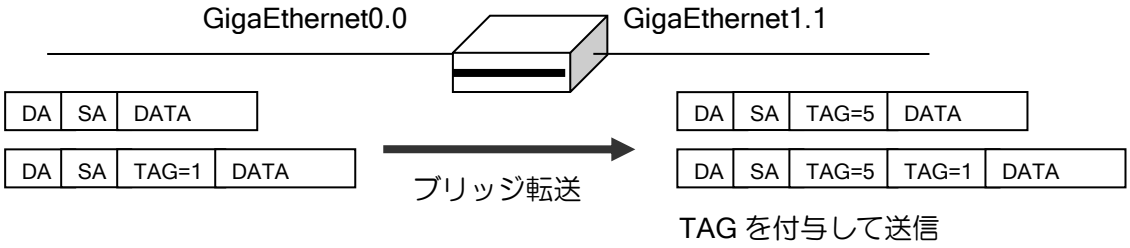
(a)VLAN タグ付与・２重タグ設定

LAN 側が VLAN タグ無しのパケットを WAN 側に送信する際に VLAN タグ付のパケットとしたい場合、また既に VLAN タグ付きのパケットに、さらに VLAN タグを付与したい場合は、次のように設定を行います。

該当する VLAN-ID のインタフェースが無い場合には基本インタフェースでフレームを受信します。これを利用して、送信インタフェースを VLAN タグのインタフェースになるように設定すると該当する VLAN タグを付与することができます。VLAN タグ付のパケットを受信した場合は、元の VLAN タグとルータで付与する VLAN タグの 2 つのタグが付与されます。

```
【設定例】
!
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.1
```

```
   encapsulation dot1q 5 tpid 8100
   no ip address
   bridge-group 1
   no shutdown
```



※外側の VLAN タグに対する CoS 値のみ設定が可能です（上記例では TAG=5 の部分）。
※内側の VLAN タグに対する CoS 値の変更はできません（上記例では TAG=1 の部分）。

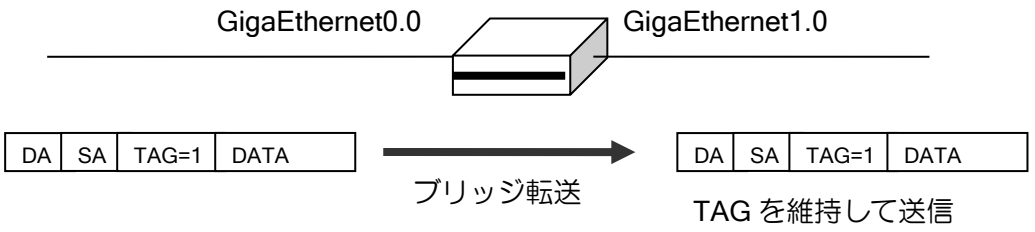
(b) VLAN タグ透過設定

受信インタフェースに適切な VLAN のインタフェースが設定されていない場合、これまでの説明のように基本インタフェースで受信します。ここで送信インタフェースも基本インタフェースになるようにブリッジを設定すると、すべての VLAN を透過することが出来ます。

この方法は最初の VLAN 設定と同じように見えますが、1 デバイスに設定できる VLAN インタフェース数以上の VLAN タグを透過したい場合に使用します。

bridge コマンドの tcp mss 調整機能とフィルタ機能については透過設定でも動作しますが、VLAN タグが 2 つ以上ある場合は適用できません。

```
 【設定例】
!
bridge irb enable
!
interface GigaEthernet0.0
   no ip address
   bridge-group 1
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
```



※CoS 値の変更はできません。

2.9.7 パススルー

2.9.7.1 PPPoE パススルー

PPPoE パススルーを設定することで指定したインタフェース間で受信した PPPoE のフレームを中継することができます。中継する PPPoE フレームのセキュリティーは PPPoE の終端装置により担保してください。

【設定例】

```
!
bridge irb enable
bridge 1 bridge-only pppoe

interface GigaEthernet0.0
  ip address 192.168.1.1/24
  bridge-group 1
  no shutdown
!
interface GigaEthernet1.0
    no ip address
    bridge-group 1
    no shutdown
!
```

■2.10 Ether over IP の設定

IP ネットワーク上にイーサネットのブリッジを形成する機能です。離れた拠点間のイーサネット上の通信を IP パケットでカプセル化し、あたかも同一リンク上に存在しているかのように見せかけることができます。

次のような特徴・用途があります。

- IP ネットワーク上の拠点同士で擬似的に広域イーサネット網を構築可能
  - ✧ 同一の IP ネットワーク同士を接続させることができる
  - ✧ 任意のプロトコルを IP ネットワーク上でブリッジさせることができる
- IPsec と併用することでセキュアな Ethernet over IPsec を構築可能
- PPPoE 上でもブリッジ機能が利用可能
- IPv6 に対応
- IPsec と組み合わせることで動的アドレスにも対応
- 宛先に FQDN を指定することも可能（Ver9.2 以降）

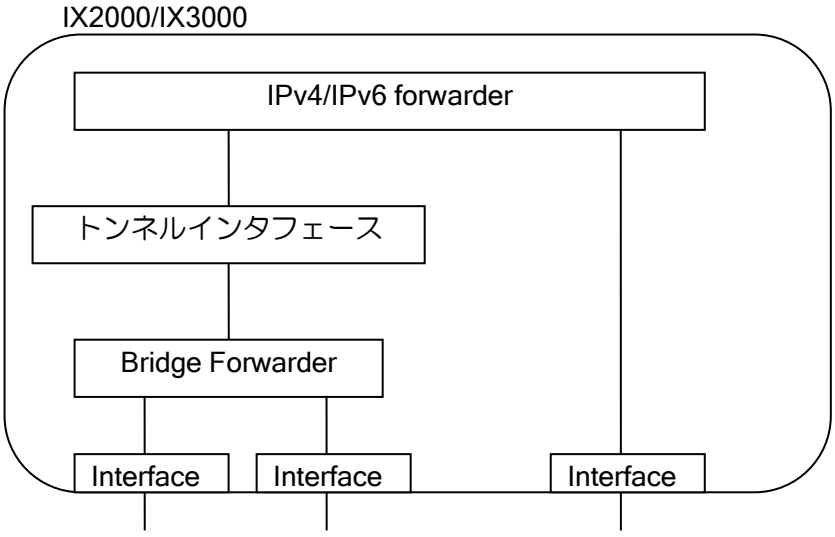
2.10.1 EtherIP 機能

イーサネットフレームを EtherIP パケットでカプセル化することで、IP ネットワーク上の離れた拠点間でのブリッジ通信を可能としています。

EtherIP は以下の RFC に準拠しています。

- Tunneling Ethernet Frames in IP Datagrams (EtherIP) - RFC3378

EtherIP 機能使用時のブロック図

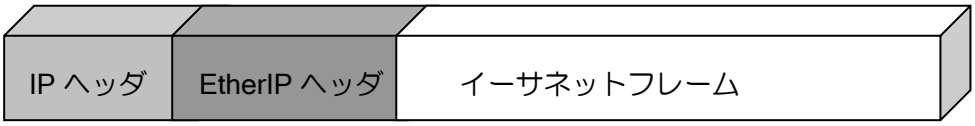


EtherIP 機能は、通常のトンネルとは異なりデータリンク層のフレームを直接 IP でカプセル化することで実現する機能です。ブリッジ機能を利用して物理インタフェースとトンネルインタフェースを接合し、トンネルインタフェースで tunnel mode ether-ip を指定することで、イーサネットフレームを IP でカプセル化できる仕組みです。

ブリッジ側のインタフェースからイーサネットフレームを受信した場合、ブリッジフォワーダによってトンネルインタフェースに転送されます。そこで IP パケットでカプセル化して受信したのち、IPv4/IPv6 フォワーダに転送されます。

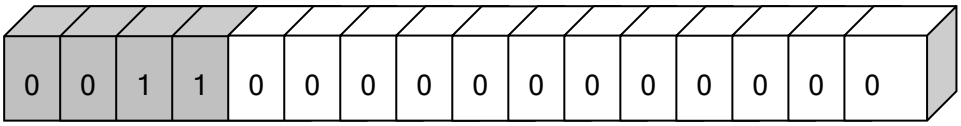
また IPv4/IPv6 フォワーダからトンネルインタフェースに送信する場合は、カプセル化したトンネルヘッダを取り外し、イーサネットフレームとしてからブリッジフォワーダに送信されます。

EtherIP パケットフォーマット（プロトコル番号：97）



イーサネットフレームは FCS を含みません。

EtherIP ヘッダフォーマット



- ビット 0-3　：プロトコルバージョン = 3
- ビット 4-15 ：予約 = 0

EtherIP のヘッダは、バージョン情報のみで構成されています。RFC3378 により上記と異なるヘッダを持つ EtherIP パケットを受信した場合は廃棄します。

EtherIP の基本設定

グローバルコンフィグモード

bridge irb enable	ブリッジ機能（IRB）の有効化
bridge GROUP bridge ip/ipv6	ブリッジプロトコルの設定

インタフェースコンフィグモード

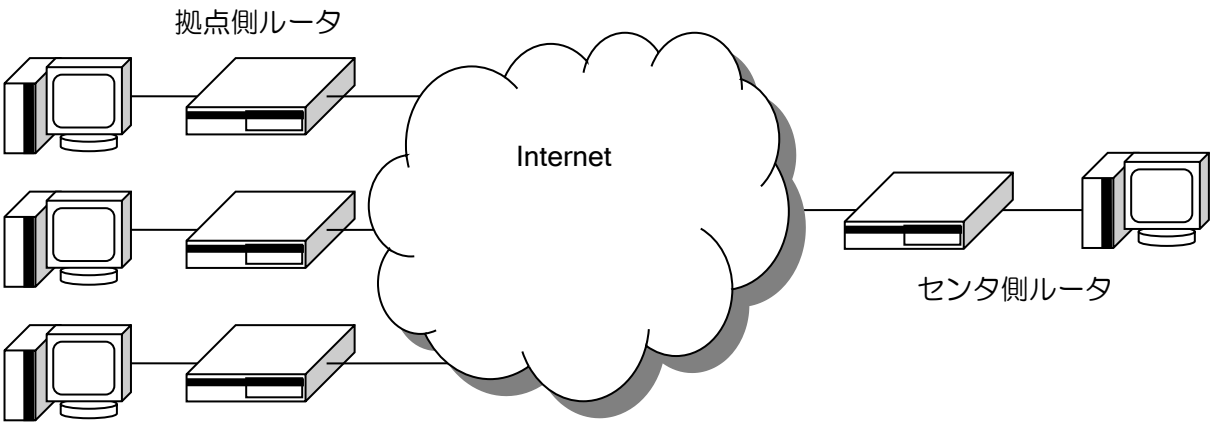
bridge-group GROUP	ブリッジグループの設定
tunnel mode ether-ip ip	EtherIP の設定（IPv4）
tunnel mode ether-ip ipv6	EtherIP の設定（IPv6）
tunnel mode ether-ip ipsec	EtherIP の設定（IPsec）

表示コマンド

show bridge	ブリッジの学習テーブルの表示
show bridge traffic	ブリッジの統計情報の表示

2.10.1.1 IPsec を使用しない EtherIP の設定

離れた拠点に存在する同一イーサネットリンク同士を接続し通信可能にします。
IPsec を使用しない場合は固定アドレスを持つルータ同士でのみ利用することが可能ですが、
Ver9.2 以降では宛先に FQDN を指定することで、動的アドレス環境でも利用可能です。



- ブリッジの機能を使用するため、bridge irb enable コマンドを設定します
- Tunnel I/F のモードを ether-ip の ip に設定します（IPsec を使用しない場合）
- EtherIP を使用する I/F と Tunnel I/F を同一ブリッジグループに設定します

【設定例: 拠点側ルータ】

```
bridge irb enable
!
interface GigaEthernet0.0
   ip address 10.0.0.2/24
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface Tunnel0.0
   tunnel mode ether-ip ip
   tunnel destination 10.0.0.1
   tunnel source 10.0.0.2
   no ip address
   bridge-group 1
   no shutdown
```

【設定例: センタ側ルータ】

```
bridge irb enable
!
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   no shutdown
!
```

```
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface Tunnel0.0
   tunnel mode ether-ip ip
   tunnel destination 10.0.0.2
   tunnel source 10.0.0.1
   no ip address
   bridge-group 1
   no shutdown
```

2.10.1.2 IPsec を使用した EtherIP の設定

セキュアな通信を行いたい場合、EtherIP に IKEv1/IPsec を使用することができます。Ver9.2 以降では IKEv2/IPsec も利用可能です。

IKEv1/IPsec の設定例

- ブリッジの機能を使用するため、bridge irb enable コマンドを設定します。
- Tunnel I/F のモードを ether-ip の ipsec に設定します（IPsec を使用する場合）。
- EtherIP を使用する I/F と Tunnel I/F を同一ブリッジグループに設定します。
- 動的アドレス環境では、IPsec 自動鍵ダイナミックポリシーマップ機能を適用します。動的アドレス側のルータはローカル ID を、固定アドレス側のルータはリモート ID をそれぞれ設定する必要があり、動的アドレス側からのみ通信を開始できます。
- ipsec policy transport によるトランスポートモードの設定は、デフォルトでは ID を送信しませんので、識別のため with-id-payload の設定が必要です。

【設定例: センタルータ】

```
ip route default GigaEthernet0.1
!
ip access-list etherip permit ip src any dest any
!
ike proposal ike-prop encryption aes hash sha
ike policy ike peer any key secret mode aggressive ike-prop
ike remote-id ike keyid remote
!
ipsec autokey-proposal ipsec-prop esp-aes esp-sha lifetime time 3600
ipsec dynamic-map dmap1 etherip ipsec-prop
ipsec remote-id dmap1 0.0.0.2
!
bridge irb enable
!
ppp profile pppoe
   authentication myname router1@example.com
   authentication password router1@ example.com password1
!
interface GigaEthernet0.1
   encapsulation pppoe
   auto-connect
   ppp binding pppoe
   ip address 10.0.0.1/24
   no shutdown
!
```

```
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface Tunnel0.0
   tunnel mode ether-ip ipsec
   no ip address
   ipsec policy transport dmap1 with-id-payload
   bridge-group 1
   no shutdown
```

【設定例: 拠点ルータ】

```
ip route default GigaEthernet0.1
!
ip access-list etherip permit ip src any dest any
!
ike proposal ike-prop encryption aes hash sha
ike policy ike peer 10.0.0.1 key secret mode aggressive ike-prop
ike local-id ike keyid remote
!
ipsec autokey-proposal ipsec-prop esp-aes esp-sha lifetime time 3600
ipsec autokey-map map1 etherip peer 10.0.0.1 ipsec-prop
ipsec local-id map1 0.0.0.2
!
bridge irb enable
!
ppp profile pppoe
   authentication myname router2@example.com
   authentication password router2@example.com password1
!
interface GigaEthernet0.1
   encapsulation pppoe
   auto-connect
   ppp binding pppoe
   ip address ipcp
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown
!
interface Tunnel0.0
   tunnel mode ether-ip ipsec
   no ip address
   ipsec policy transport map1 with-id-payload
   bridge-group 1
   no shutdown
```

2.10.1.3　IRB の設定

ブリッジ機能を利用しているため、非 IP 通信のみ EtherIP 転送したり、BVI インタフェースを経由してルータ機能を併用することも可能です。詳細はブリッジの説明を参照してください。

2.10.1.4 フィルタの設定

EtherIP トンネルインタフェースでは、ブリッジ IP/IPv6 フィルタと MAC フィルタが使用できます。詳細はブリッジ機能、パケットフィルタ機能、MAC フィルタ機能の章の説明を参照してください。

2.10.1.5 TCP-MSS 調整の設定

EtherIP トンネルインタフェースで TCP-MSS 調整機能が利用できます。機能の詳細はブリッジ機能、IPv4 機能、IPv6 機能の章の説明を参照してください。

EtherIP では MSS の値は自動調整できません。設定の際には付録の TCP-MSS 調整値の項を参考にしてください。

2.10.2 ネットワーク設計の注意事項

Ether over IP 機能はフラッディング処理の負荷が高いです。IX3000 シリーズは対地数の最大値を大きく設定できますが、トラフィックによっては推奨最大値まで使用できないことがあります。IX2000/IX3000 では対地数によらず装置の処理能力はほぼ一定値となりますので、使用可能な対地数は処理能力と各対地のトラフィックから決定してください。

処理可能なパケット数は以下のとおりです。※測定値は IMIX の場合です。

装置	処理能力（pps）	
	EtherIP	EtherIP+IPsec
IX3015（Ver.7.2）	70,000	25,000
IX3110（Ver.8.0）	175,000	90,000
IX3315（Ver.9.4）	600,000	200,000

ブロードキャストは、各対地にコピーを行うため、ユニキャストに比較して負荷が高く、また、対地数が増えるほど負荷が高くなります。そのため、転送可能なトラフィックを考える際には、ユニキャストとブロードキャストがどの程度転送するかを考慮する必要があります。

トラフィックの目安を計算するための条件として、以下を仮定します。

- センタ装置を中心とするスター型のモデル
- IPsec を使用
- ユニキャストは特定の相手にのみ送信される
- ユニキャストは各対地同じトラフィック量
- ユニキャストのフレームサイズの割合は IMIX
- ブロードキャストは全ての対地に転送される
- トラフィックは双方向
- 各対地からのブロードキャストも全ての対地に転送される

この場合、対地数に対して転送可能なトラフィックの目安は、以下のブロードキャストとユニキャストの欄のようになり、それぞれ 1 対地あたりの転送可能なトラフィック量となります。

IX3110

対地数	ブロードキャスト（pps）	ユニキャスト（pps）	全体転送量（pps）	備考
200	2.2	5	89,440	
200	0.1	420	88,020	OSPF の Hello 相当
100	2.2	660	88,220	
100	0.1	880	89,010	OSPF の Hello 相当

IX3015/IX2235

対地数	ブロードキャスト（pps）	ユニキャスト（pps）	全体転送量（pps）	備考
50	2.2	380	24,610	
50	0.1	480	24,255	OSPF の Hello 相当
30	2.2	750	24,546	
30	0.1	800	24,093	OSPF の Hello 相当
15	2.2	1,600	24,528	
15	0.1	1,600	24,024	OSPF の Hello 相当

IX3315

対地数	ブロードキャスト（pps）	ユニキャスト（pps）	全体転送量（pps）	備考
300	2.2	4	199,860	
300	0.1	600	189,030	OSPF の Hello 相当
200	2.2	500	188,440	
200	0.1	900	184,020	OSPF の Hello 相当
100	2.2	1,700	184,220	
100	0.1	1,900	191,010	OSPF の Hello 相当

上記では、各対地間のユニキャストの通信は考慮していません。この場合、EtherIP のタンデム接続となりますので、通常より負荷が高くなるため、拠点間の通信が多い場合は、上記より余裕を持った対地数とする必要があります。

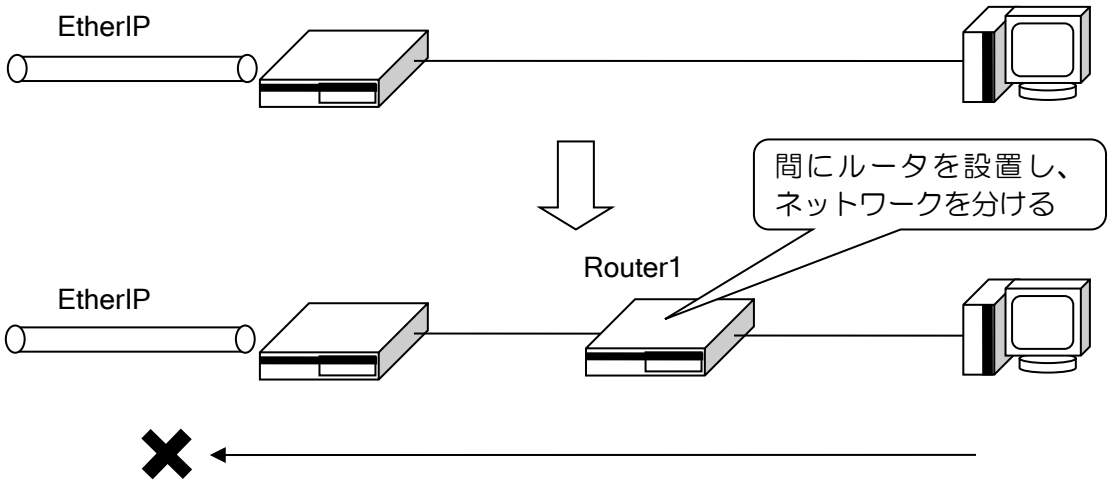
上記全体転送量の算出方法

- ブロードキャスト
- 各装置が（B）pps のトラフィックを（N）対地に送信する。（B）x（N）
- それらの装置が（N+1）台存在する。{（B）x（N）} x（N+1）
- ユニキャスト
- センタ装置または拠点装置から（U）pps のトラフィックを対向装置に送信する。（U）
- それらの装置が（N）台存在する。{（U）x（N）}
- 全体転送量
- ［{（B）x（N）} x（N+1）］+ {（U）x（N）}

使用したい対地数に対して、使用するトラフィック量が多い場合には、以下のような対処により、ブロードキャストを減らし、使用可能なユニキャストを増やすことで対応してください。

➢ 構成を変更

配下に端末が多い場合は、ARP によるトラフィックが増加します。このような場合、EtherIP を使用する IX の LAN 側にルータを設置し、ネットワークを分けることにより、EtherIP を通るブロードキャストパケットは、ルータが送信するパケットのみとすることができます。



➢ フィルタを使用

不要なブロードキャストをフィルタすることにより、ブロードキャストトラフィックを減らすことができます。

2.10.3 制限事項

- 複数のブリッジグループを 1 つのトンネルに通すことはできません。
- VLAN タグの付与、付替、削除等の操作はできません。VLAN タグは透過のみ設定可能です。
- CoS 値の書き換えはできません。
- スパニングツリーの機能がないためループになる構成では使用しないでください。

2.10.4 注意事項

- Ether IP で複数のトンネルを同じブリッジグループに設定した場合、パケットコピー処理がソフトウェアによって行われるため、性能が低下する場合があります。
- インターネット網などを使用する場合、網内遅延が発生するため、遅延の影響を受けるアプリケーションを利用する場合は注意が必要です。
- IP ネットワークで通信しますので、フレームの転送順序が逆転する可能性があります。

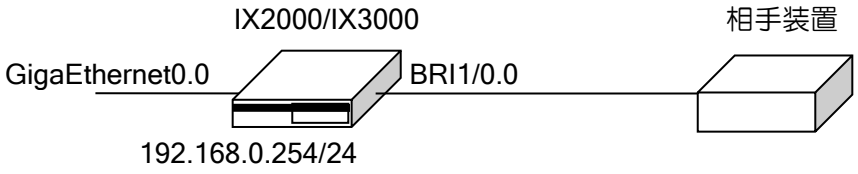
■2.11 PPP の設定

物理リンクレイヤと、PPP の関係は論理的に以下の構造をとっています。

インタフェース（BRI1/0.0 etc.）
PPP
デバイス（BRI1/0 etc.）

PPP について、簡単なネットワーク例における設定例を示します。

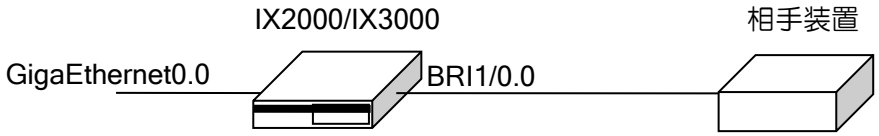
ネットワーク例（IPv4 の場合）



【設定例】

```
ip route default BRI1/0.0
ppp profile bri1/0.0
   authentication accept chap
   authentication myname my-router@example.com
   authentication password my-router@example.com my-password
interface GigaEthernet0.0
   ip address 192.168.0.254/24
   no shutdown
interface BRI1/0.0
   ppp binding bri1/0.0
   ip address ipcp
   ip napt enable
   no shutdown
```

ネットワーク例（IPv6 の場合）



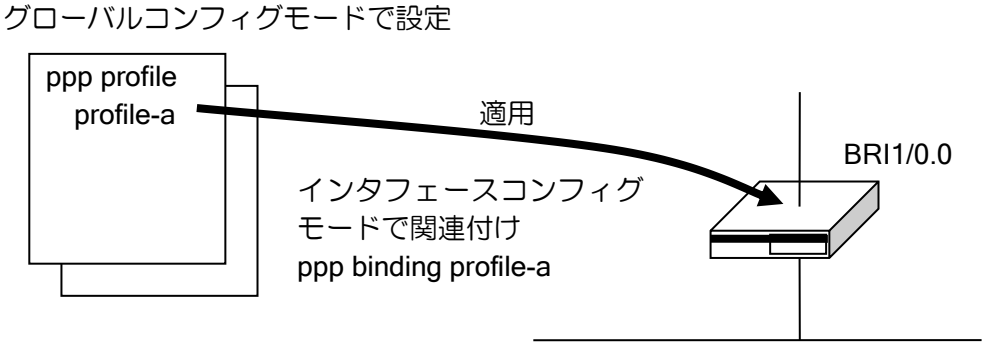
【設定例】

```
ipv6 route default BRI1/0.0
ppp profile bri1/0.0
   authentication accept chap
   authentication myname my-router@example.com
   authentication password my-router@example.com my-password
interface GigaEthernet0.0
   ipv6 address 2001:db8::1/64
   no shutdown
interface BRI1/0.0
   ppp binding bri1/0.0
   ipv6 enable
   no shutdown
```

PPP のそれぞれの設定について、以降に説明します。

2.11.1 PPP プロファイルの設定

PPP プロファイルは、グローバルコンフィグモードにて登録します。そのプロファイルを、インタフェースコンフィグモード上で ppp binding コマンドにより関連付けを行うことで、プロファイルをインタフェースに適用することができます。（Ver.2 以降）



PPP プロファイルの設定と関連付けを行うコマンドは、次のとおりです。

ppp binding	PPP プロファイルの割り当て設定
ppp profile	プロファイルの作成／変更

2.11.2 LCP の設定

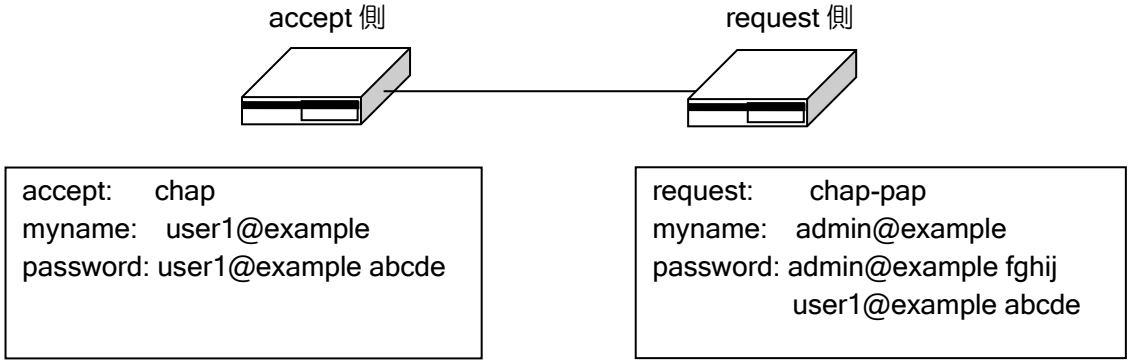
LCP（リンク制御プロトコル）を設定するコマンドは次のとおりです。

echo	LCP メンテナンスパケット送信の有効設定
lcp accm	Async-Control-Character-Map の設定
lcp acfc	Address-and-Control-Field-Compression の有効設定
lcp config-retry	configure-request 送信回数の設定
lcp echo-interval	LCP Echo-Request 送信間隔の設定
lcp echo-retry	LCP 切断までの LCP Echo Request パケット送信回数の設定
lcp magic-number	Magic-Number 使用の有効設定
lcp mru	Maximum-Receive-Unit 値の設定
lcp nak-retry	configure-nak 送信回数の設定
lcp pfc	Protocol-Field-Compression の有効設定
lcp retry-timer	configure-request/terminate-request 送信間隔の設定
lcp terminate-retry	terminate-request 送信回数の設定

※PPPoE の場合は、FCS、ACFC、ACCM、MRRU のネゴシエーションは行いません。

2.11.2.1 LCP 認証プロトコルの設定

LCP 認証プロトコルは、request 側と accept 側で互いを認証し、LCP を確立するためのプロトコルです。

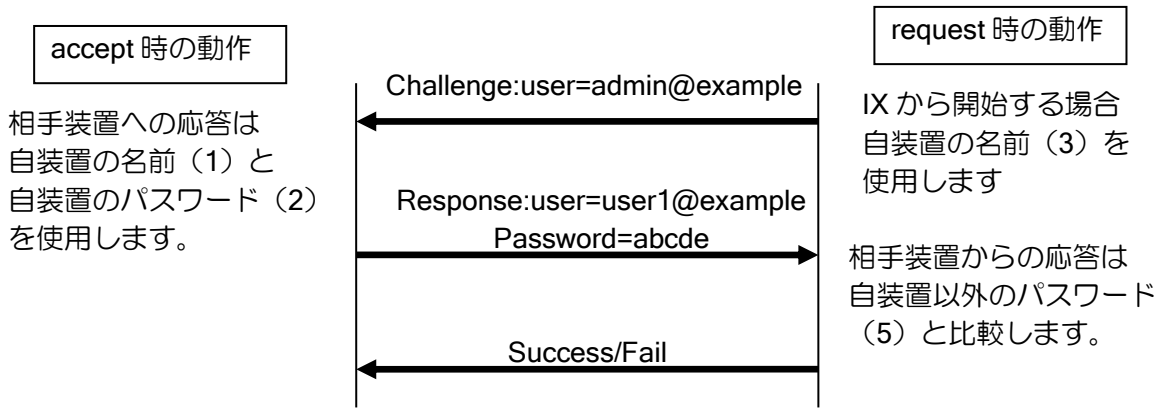


LCP 認証プロトコルを設定するコマンドは次のとおりです。

authentication accept	受諾認証タイプの設定 （chap と pap のどちらも選択されている場合は、どちらの認証でも対応可能であるという設定になります。）
authentication myname	送信する認証名の設定
authentication password	認証名に対するパスワードの設定
authentication request	要求認証タイプの設定 （chap と pap のどちらも選択されている場合は、どちらの認証でも対応可能であるという設定になります。）

```
【設定例】
accept 側
ipv6 route default BRI1/0.0
ppp profile bri1/0.0
   authentication accept chap
   authentication myname user1@example           - (1)
   authentication password user1@example abcde - (2)
interface GigaEthernet0.0
   ipv6 address 2001:db8:1::1/64
   no shutdown
interface BRI1/0.0
   ppp binding bri1/0.0
   ipv6 enable
   no shutdown

request 側
ipv6 route default BRI1/0.0
ppp profile bri1/0.0
   authentication request chap-pap
   authentication myname admin@example           - (3)
   authentication password admin@example fghij   - (4)
   authentication password user1@example abcde - (5)
interface GigaEthernet0.0
   ipv6 address 2001:db8:0::1/64
   no shutdown
interface BRI1/0.0
   ppp binding bri1/0.0
   ipv6 enable
   no shutdown
```

IX2000/IX3000 シリーズでは、PPP 認証のユーザ名，パスワードは以下の設定値を使用します。相手装置が IX2000/IX3000 シリーズ以外の場合は、相手装置の動作を考慮してユーザ名，パスワードの設定を行ってください。



(a) PAP の設定

PAP（パスワード認証プロトコル）は、認証のための最も簡単なプロトコルです。

PAP を設定するコマンドは次のとおりです。

pap max-request	request パケット受信回数の設定
pap request-timeout	request パケット受信待ち時間の設定
pap retry-timeout	ack/nak パケット受信待ち時間の設定

(b) CHAP の設定

CHAP（チャレンジハンドシェーク認証プロトコル）は、スリーウェイハンドシェークの方法を使用することで、PAP よりもより安全な認証を行うプロトコルです。

CHAP を設定するコマンドは次のとおりです。

chap challenge-timeout	チャレンジパケット受信待ち時間の設定
chap response-timeout	success/failure/response パケット受信待ち時間の設定
chap retry	チャレンジパケット送信回数の設定

2.11.3 NCP の設定

NCP（ネットワーク制御プロトコル）を設定するコマンドは次のとおりです。

ncp config-retry	configure-request 送信回数の設定
ncp nak-retry	configure-nak 送信回数の設定
ncp retry-timer	configure-request/terminate-request 送信間隔の設定
ncp terminate-retry	terminate-request 送信回数の設定

2.11.3.1 IPCP の設定

IPCP（IPv4 制御プロトコル）を設定するコマンドは次のとおりです。

ipcp ip-compression	Van Jacobson TCP/IP ヘッダ圧縮使用の有効設定
ipcp provide-remote-dns	相手からの DNS アドレス要求の有効設定
ipcp request-ip-address （Ver.8.9 以前） ipcp provide-ip-address （Ver.8.10 以降）	IPv4 での相手からの IP アドレス要求の有効設定
ipcp request-local-dns	DNS アドレスを相手に要求する設定
ipcp send-ip-address	IPv4 の IP アドレス送信の有効設定

2.11.3.2 IPV6CP の設定

IPV6CP（IPv6 制御プロトコル）を設定するコマンドは次のとおりです。

ipv6cp send-interface-id	IPv6 のインタフェース ID 送信の有効設定
ipv6cp suggest-interface-id	IPv6 での相手からのインタフェース ID 要求の有効設定

2.11.4 TCP の設定

PPP で TCP の設定を行うコマンドは次のとおりです。

tcp-mss	TCP max segment size の調整

2.11.5 無通信切断の設定

自動接続の設定がされていない場合、無通信が継続すると相手との接続を切断することができます。通信の有無の確認は、双方向、受信方向、送信方向の指定が可能です。

idle-time	無通信時間の設定

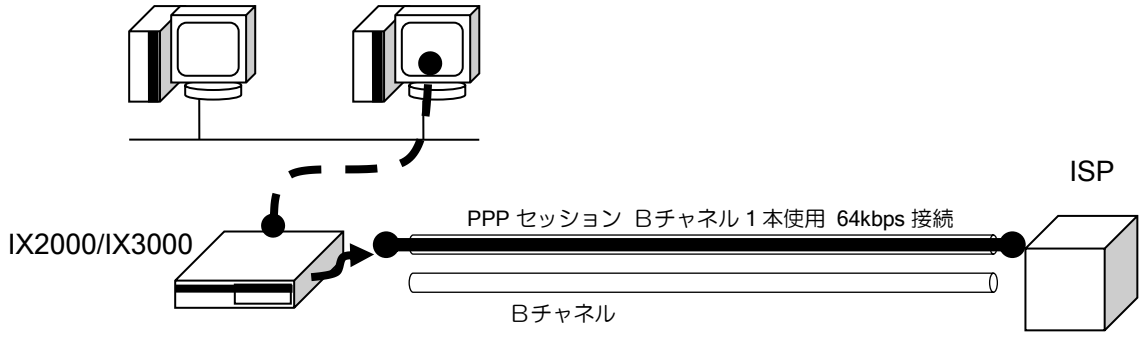
無通信切断の設定は、オンデマンド帯域幅制御にも使用されます。詳細は、オンデマンド帯域幅制御の項を参照してください。

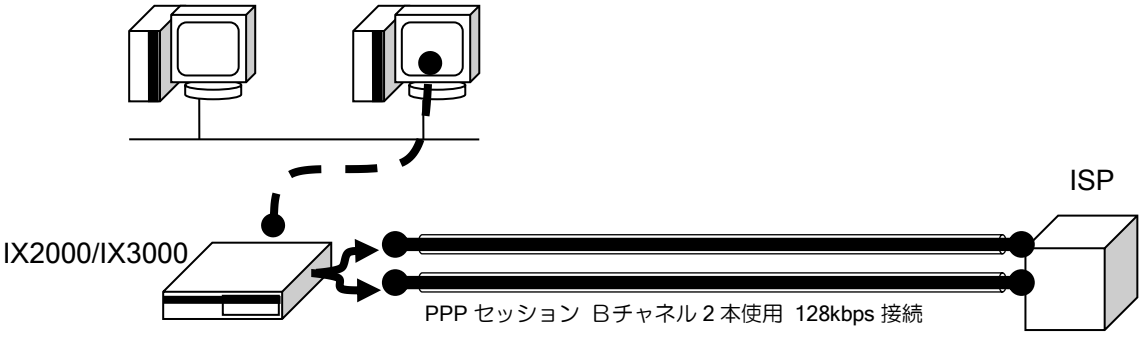
2.11.6 マルチリンク PPP の設定

PPP には、1 対 1 の通信を行うための通信手段の他、物理的には複数のリンクを仮想的な 1 つのリンクと見立てることで、よりバンド幅の広い通信を可能にする方法があります。この方法が、マルチリンク PPP です。ISDN では 1 つの B チャネルでは 64kbps ですが、例えば 2 つの B チャネルを同時に使用し、1 つのリンクとみなすことで、64 + 64 = 128 kbps の通信が可能になります。Ver.7.2 以降、装置で使用可能な最大チャネル数まで接続可能です。

ただし、マルチリンクの環境で音声パケットの通信を行う場合の音声品質は保証できません。

また、マルチリンク PPP は、PPPoE、専用線上では動作しません。





マルチリンク PPP を設定するコマンドは次のとおりです。

multilink enable	マルチリンク PPP の有効

注意事項として、マルチリンク PPP を有効にして IP45/C シリーズに接続する場合には、下記の条件を満たす必要があります。マルチリンク PPP インタリーブ等のみを使用する場合でも同様です。

- IP45/C シリーズ対向
  - IX2000/IX3000 の MRU はデフォルト値の 1500 としてください。

※fragment-delay の値は環境に応じて 10～30msec で調整してください。

2.11.6.1 オンデマンド帯域幅制御（BOD）の設定

帯域使用率のしきい値を超えた/下回った際にリンクの追加/削除を自動的に行うよう設定することができます。

本機能は bandwidth-on-demand コマンドを設定することで有効になり、設定時には反応速度を fast, medium, slow の三段階で設定します。速く設定するほどリンクの追加削除が素早く行われますが、逆に短時間の負荷で不要なリンク数の増減を行う可能性もありますので、使用環境に合わせて調整してください。

- 参考

BOD では、発呼側装置においてリンクの増減を制御します。4 秒おき（※）に帯域使用率を測定し、過去 8 回の帯域使用率に重み係数を加味した値の平均値を基にして、リンクの追加削除を決定します。設定の詳細は以下のようになります。

※現状 PRI では 1 秒おきに動作します。

新 ↑ / ↓ 旧

Fast

記録順	重み
8	50
7	25
6	10
5	5
4	4
3	3
2	2
1	1

medium

記録順	重み
8	23
7	20
6	17
5	13
4	11
3	8
2	5
1	3

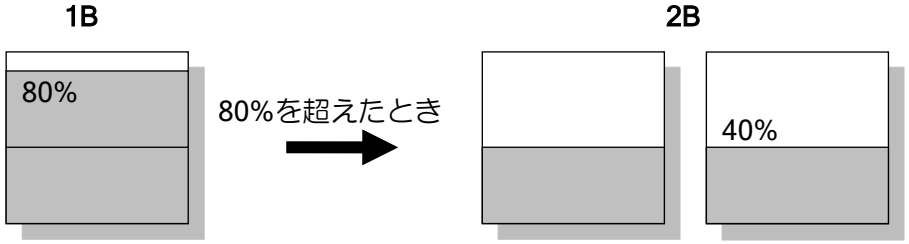
slow

記録順	重み
8	12
7	13
6	12
5	13
4	12
3	13
2	12
1	13

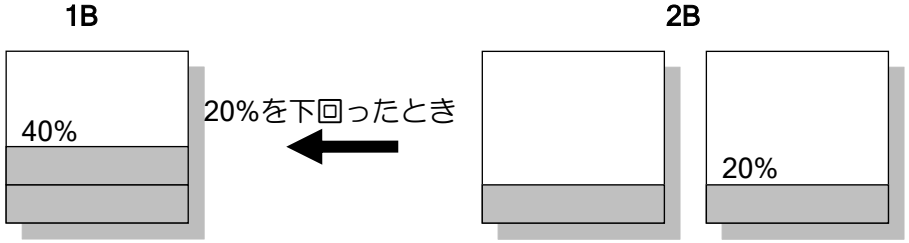
これらの、Σ（帯域使用率(i)×重み係数(i)）を基に帯域使用率を算出し、load-threshold コマンドで設定された値と比較してリンクの増減を決定します。リンク数の増減は 1 リンク毎に行います。そのため、1 リンク増減後に再度上記の計算を行い、次のリンクの増減を決定します。

また multilink load-threshold コマンドにより、リンク数を増加させる際の上限のしきい値（HIGH-THRESHOLD）と、減少させる際の下限のしきい値（LOW-THRESHOLD）を設定することも可能です。しきい値の設定は全帯域を 100 として設定します。

1B から 2B へ移行する場合（HIGH-THRESHOLD 80%の場合）



2B から 1B へ移行する場合（LOW-THRESHOLD 20%の場合）



※リンク数が減少する場合、最後のリンクが接続してからの時間が、自動接続設定の有無に関係なく idle-time コマンドで設定した時間（デフォルトでは 120 秒）経過していなければ、設定した時間が経過するまではリンクの切断は行いません。idle-time コマンドで設定した時間経過した後は、しきい値を下回った時点でリンクを切断します。再度リンク数が増加しなければ、それ以降のリンクは idle-time コマンドで設定した時間を待たずに切断を行います。

設定コマンドは次のとおりです。

multilink bandwidth-on-demand	オンデマンド帯域幅制御（BOD）の設定
multilink load-threshold	2B 接続用の回線使用率の閾値設定
idle-time	無通信時間（保護時間）の設定

2.11.6.2 リンク数の設定

リンク数の最大値と最小値を設定することができます。デフォルトの設定では最大リンク数が 2、最小リンク数が 1 となっています。最大リンク数を超えると、自側からの接続が抑制され、対向からの接続要求も受け付けません。また発呼時には、最小リンク数まで接続します。ただし、最小リンク数の設定は発呼時に有効で、着呼時には影響しません。

Ver.7.2 以降、最大リンク数は装置で使用可能なチャネル数まで拡張しています。

multilink max-links	マルチリンク PPP の最大リンク数の設定
multilink min-links	初期リンク数の設定

2.11.6.3 エンドポイント識別子の使用

エンドポイント識別子は、マルチリンク使用時に、接続した複数のチャネルが同じ装置からの着信かどうか判定するために使用します。

エンドポイント識別子の使用を設定すると、送信する LCP パケットへ、インタフェース毎に異なるエンドポイント識別子を自動的に設定します。

着信側では、エンドポイント識別子の設定に関係なく、複数チャネル接続時、それぞれのエンドポイント識別子を比較し、同じであれば同じ装置からの着信と判断して、接続した複数のチャネルをマルチリンクとして使用します。

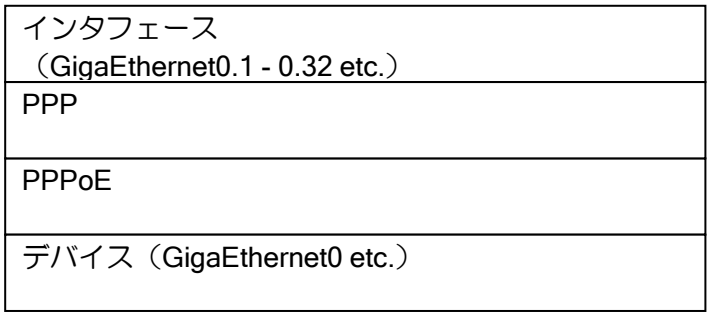
設定コマンドは次のとおりです。本機能はマルチリンク使用の設定を行っている場合のみ有効となります。

multilink endpoint	マルチリンクエンドポイント識別子使用の設定

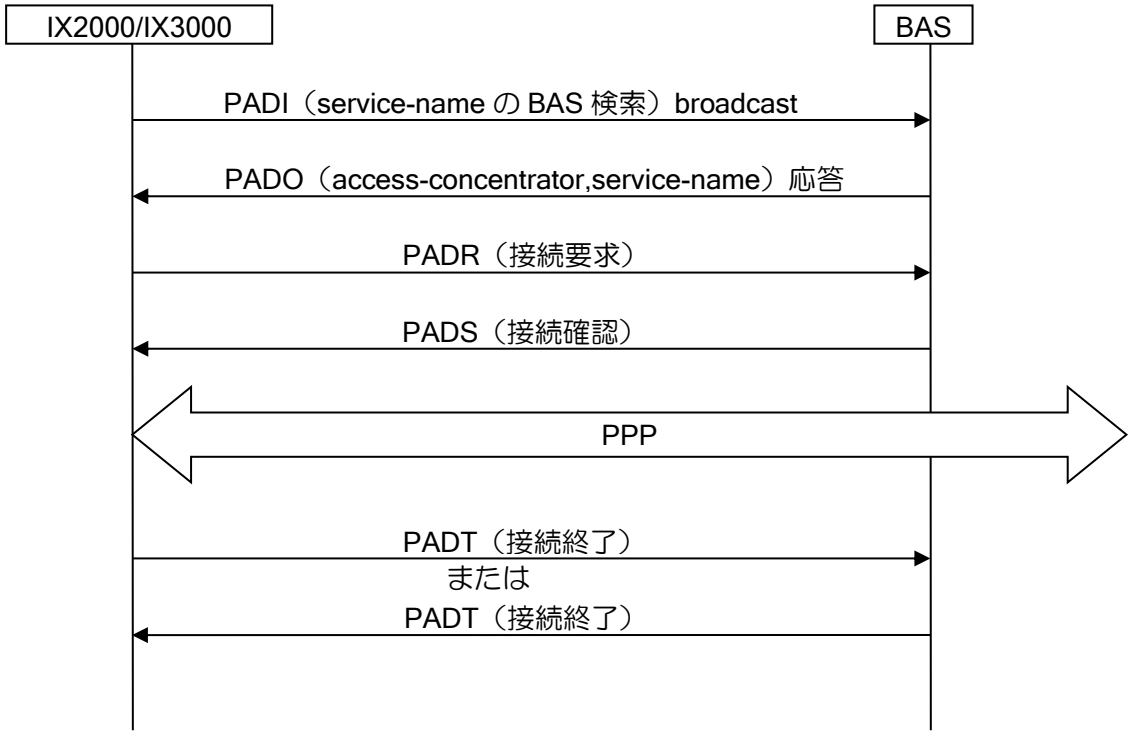
■2.12 PPPoE の設定

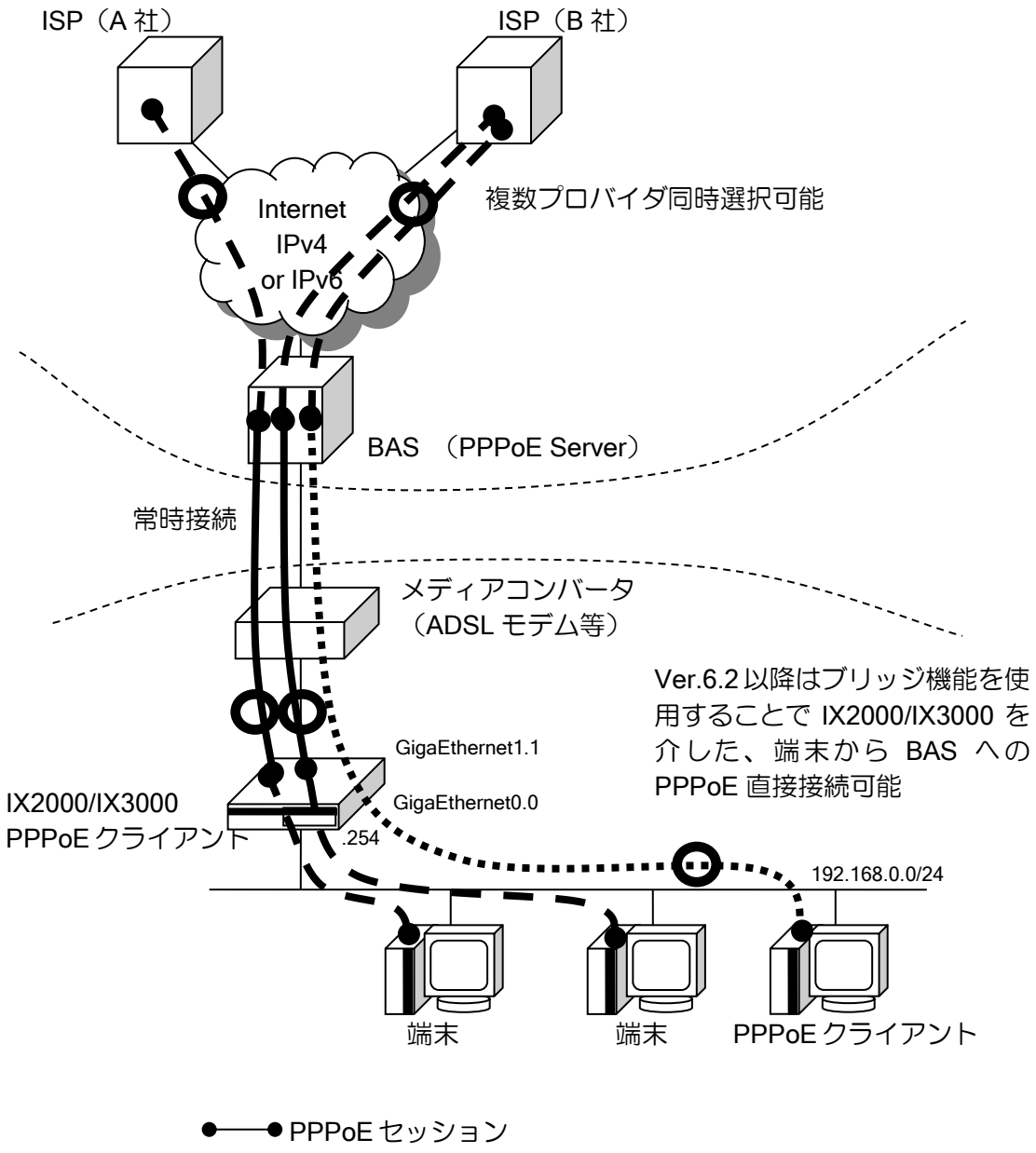
PPPoE では、サブインタフェース（GigaEthernet0.1 などの 0.0 ではないインタフェース）上で、PPP セッションを張り、そのセッション上で IPv4 または IPv6 の通信を実現することができます。

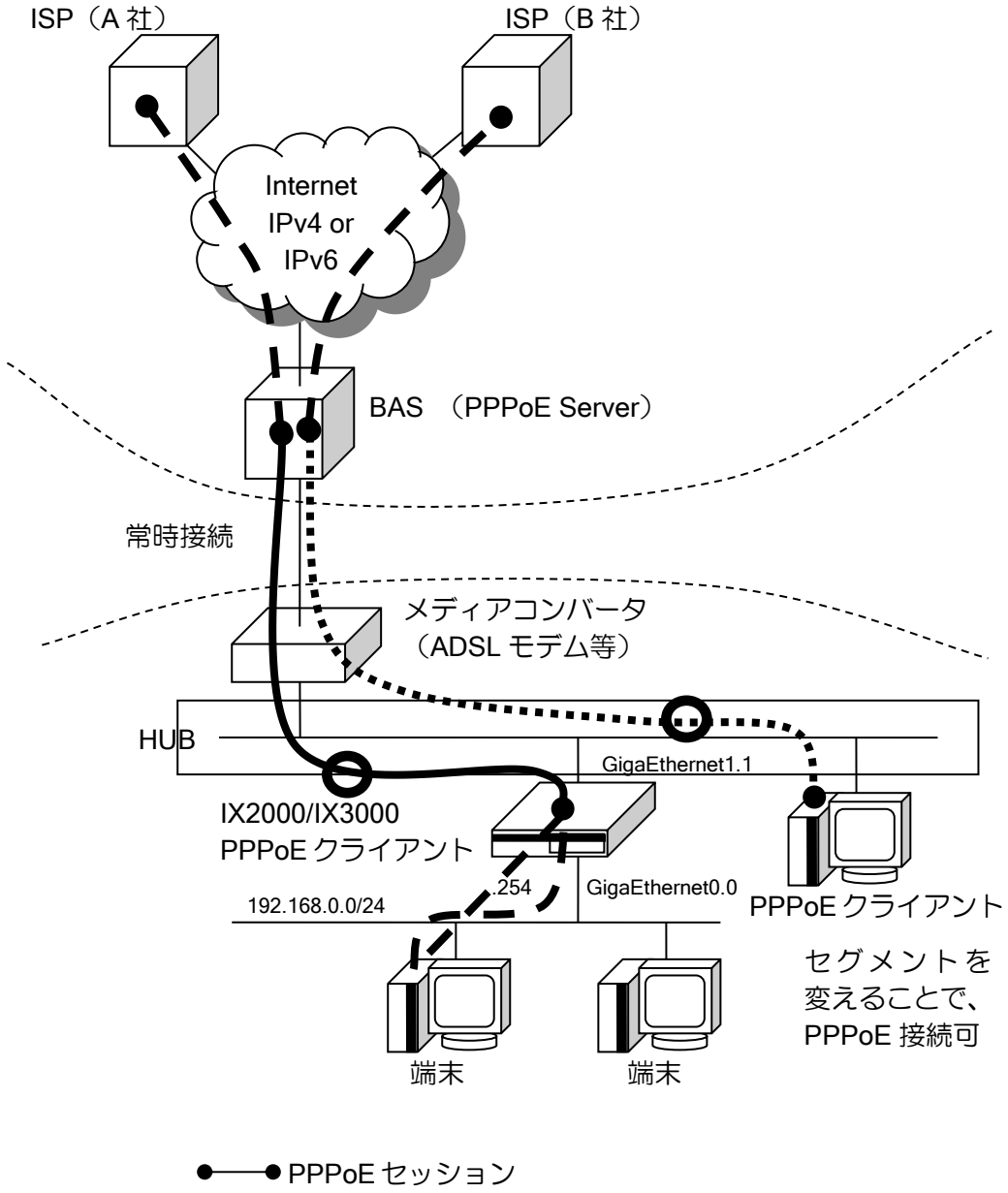
Ver9.7 以降では、PPPoE サーバの設定が可能です。



PPPoE のシーケンス




ISP（A 社）
ISP（B 社）
Internet
IPv4
or IPv6
複数プロバイダ同時選択可能
BAS （PPPoE Server）
常時接続
メディアコンバータ
（ADSL モデム等）
Ver.6.2 以降はブリッジ機能を使用することで IX2000/IX3000 を介した、端末から BAS への PPPoE 直接接続可能
GigaEthernet1.1
GigaEthernet0.0
IX2000/IX3000
PPPoE クライアント
.254
192.168.0.0/24
端末
端末
PPPoE クライアント
PPPoE セッション



2.12.1 PPPoE クライアントの設定

PPPoE 設定は、インタフェースコンフィグモード（イーサネットのサブインタフェース）で、encapsulation pppoe コマンドを使用して設定します。

以下に PPP 登録を含めた PPPoE 登録のための設定および基本的な動作を説明します。

encapsulation pppoe	PPPoE の有効
pppoe access-concentrator	アクセスコンセントレータの名称を設定
pppoe host-uniq-tag	ホスト特定タグ有効設定
pppoe service-name	サービス名の設定
ppp profile	プロファイルの設定
ppp binding	インタフェースとプロファイルの関連付け設定
ip address ipcp	IPCP で受理した自動割当アドレスの利用
show pppoe status	PPPoE 状態の表示

show ip address	IPv4 アドレス設定状態表示
show ipv6 address	IPv6 アドレス設定状態表示

【設定例】

```
ip route default GigaEthernet1.1
proxy-dns ip enable
proxy-dns interface GigaEthernet1.1 priority 100

ppp profile profile-1
   authentication myname my-router@example.com
   authentication password my-router@example.com my-password
   （PPPoE クライアントでは、authentication request  設定は不要です）

interface GigaEthernet0.0
   ip address 192.168.0.254/24
   no shutdown

interface GigaEthernet1.1
   encapsulation pppoe
   ppp binding profile-1
   ip address ipcp
   ip napt enable
   no shutdown

（Ver.4 以前では、proxy-dns コマンドに ip のパラメータは入力しません）
```

ブリッジ機能を使用することにより、PPPoE クライアントを接続することが可能です。ブリッジの設定については、ブリッジの節を参照してください。

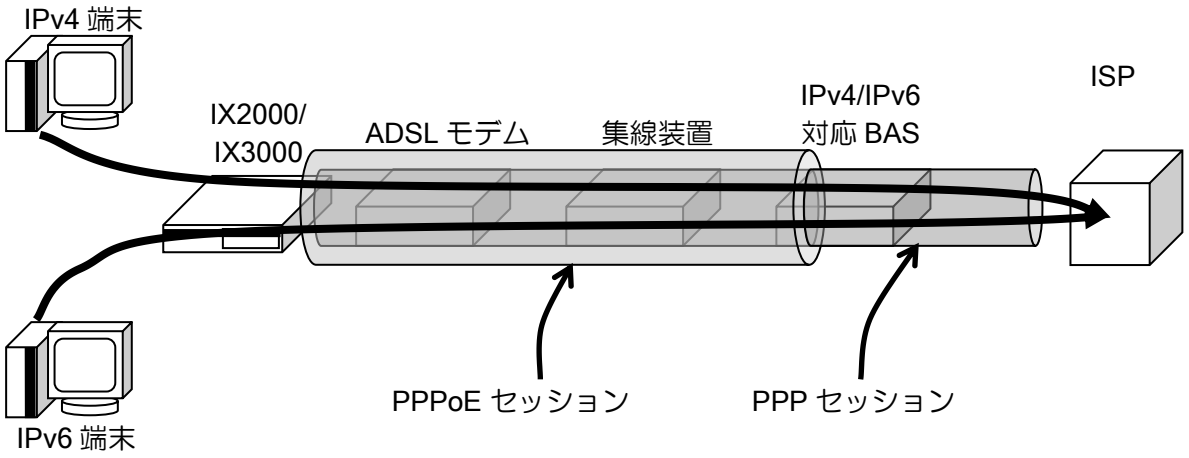
【設定例】

```
bridge irb enable
no bridge 1 bridge ip
no bridge 1 bridge ipv6

ip route default GigaEthernet1.1
proxy-dns ip enable
proxy-dns interface GigaEthernet1.1 priority 100
ppp profile profile-1
   authentication myname my-router@example.com
   authentication password my-router@example.com my-password

interface GigaEthernet0.0
   ip address 192.168.0.254/24
   bridge-group 1
   no shutdown

interface GigaEthernet1.0
   no ip address
   bridge-group 1
   no shutdown

interface GigaEthernet1.1
   encapsulation pppoe
   ppp binding profile-1
   ip address ipcp
   ip napt enable
   no shutdown
```

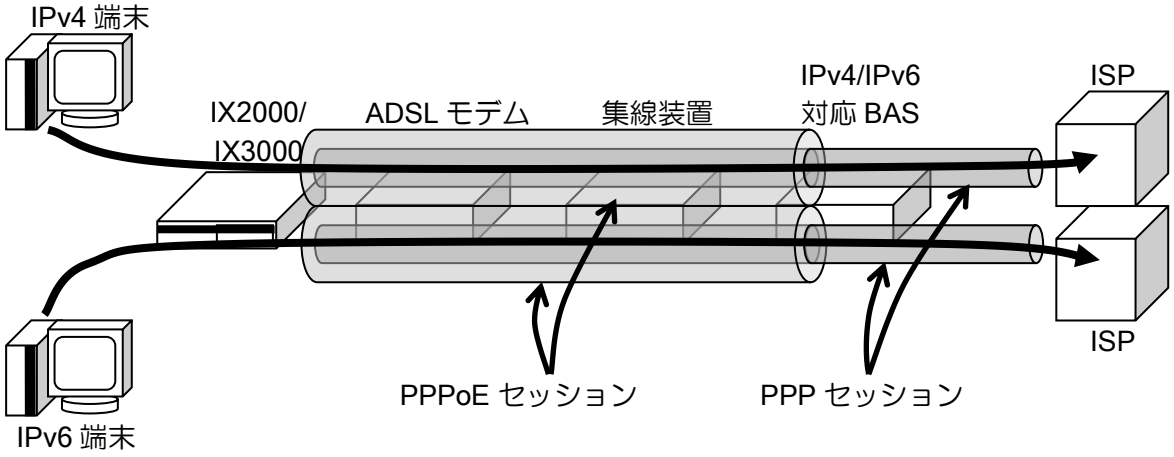
2.12.2 PPPoE クライアントの応用

PPPoE クライアント（PPP も同様）による接続では、IPv4、IPv6 などのセッションあるいは BAS との組み合わせが可能です。以下に、接続例を示します。

PPPoE（PPP）1 セッションによる接続例



PPPoE（PPP）複数セッション（単一 BAS）による接続例



通常のサービスでは特別な設定は必要ありません。別なインタフェースにそれぞれのセッションの設定を行ってください。

評価環境などで使用する場合は、サービス名を設定することで ISP の振り分けを行うことも可能です。設定したサービス名は、Service-Name タグとして付加されます。

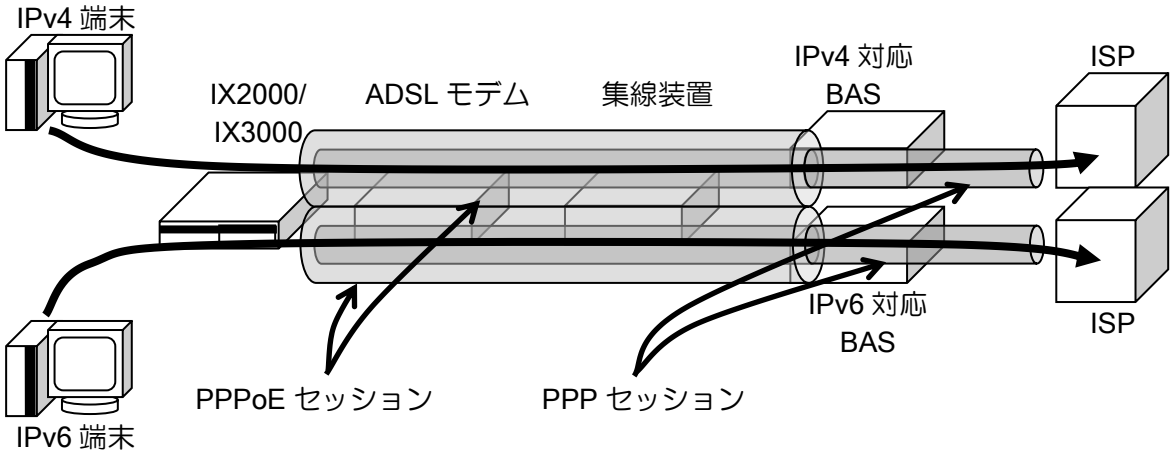
複数セッション使用時は、Host-Uniq タグを使用することで各セッションの振り分けを行います。Host-Uniq タグは pppoe host-uniq コマンドにより有効設定を行いますが、デフォルトで有効になっていますので、複数セッション使用時は設定を削除しないでください。

【設定例】

```
ip route default GigaEthernet1.1
ipv6 route default GigaEthernet1.2
proxy-dns ip enable
proxy-dns ipv6 enable
proxy-dns interface GigaEthernet1.1 priority 100

ppp profile profile-1
```

```
   authentication myname my-router@example1.com
   authentication password my-router@example1.com my-password

ppp profile profile-2
   authentication myname my-router@example2.com
   authentication password my-router@example2.com my-password

interface GigaEthernet0.0
   ip address 192.168.0.254/24
   ipv6 address 2001:db8::254/64
   no shutdown

interface GigaEthernet1.1
   encapsulation pppoe
   pppoe service-name ISP1
   ppp binding profile-1
   ip address ipcp
   ip napt enable
   no shutdown

interface GigaEthernet1.2
   encapsulation pppoe
   pppoe service-name ISP2
   ppp binding profile-2
   ipv6 enable
   no shutdown
```

PPPoE（PPP）複数セッション（複数 BAS）による接続例



通常のサービスでは特別な設定は必要ありません。2 セッション分の設定を行ってください。評価環境などで使用する場合は、アクセスコンセントレータ名を設定することで BAS の振り分けを行うことも可能です。設定したアクセスコンセントレータ名が、BAS から付与される AC-Name と同じ場合に、BAS に応答を返します。

【設定例】

```
ip route default GigaEthernet1.1
ipv6 route default GigaEthernet1.2
proxy-dns ip enable
proxy-dns ipv6 enable
proxy-dns interface GigaEthernet1.1 priority 100

ppp profile profile-1
  authentication myname my-router@example1.com
  authentication password my-router@example1.com my-password

ppp profile profile-2
  authentication myname my-router@example2.com
  authentication password my-router@example2.com my-password

interface GigaEthernet0.0
  ip address 192.168.0.254/24
  ipv6 address 2001:db8::254/64
  no shutdown

interface GigaEthernet1.1
  encapsulation pppoe
  pppoe access-concentrator BAS1
  ppp binding profile-1
  ip address ipcp
  ip napt enable
  no shutdown

interface GigaEthernet1.2
  encapsulation pppoe
  pppoe access-concentrator BAS2
  ppp binding profile-2
  ipv6 enable
  no shutdown
```

2.12.3 PPPoE サーバの設定

Ver9.7 以降では、PPPoE サーバの設定が可能です。

同時に通信するユーザの数だけサブインタフェースの設定が必要です。サブインタフェースの設定は、設定例のように範囲設定に対応しています。個別にも設定可能です。

ppp profile	プロファイルの設定
authentication password	認証するユーザとパスワードの設定
ipcp provide-static-ip-address	アドレス払い出し設定（固定払い出しの場合）
ipcp provide-ip-address range	アドレス払い出し設定（動的払い出しの場合）
encapsulation pppoe	PPPoE の有効化
pppoe server	PPPoE の動作モードをサーバに変更
ppp binding	インタフェースとプロファイルの関連付け設定
show pppoe server	セッション情報の取得

【設定例】

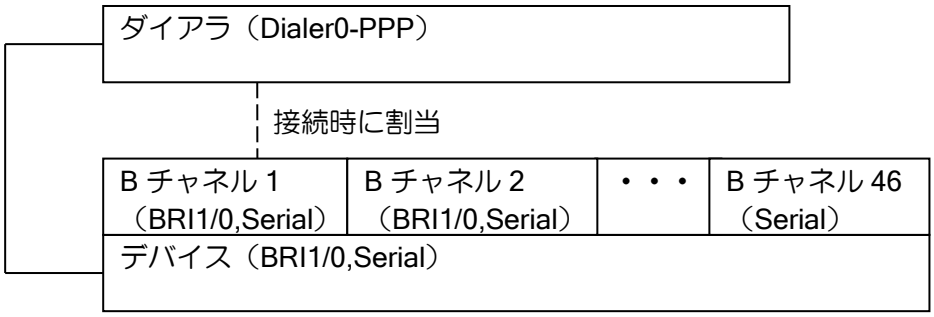
```
ppp profile pppoe_server
   authentication request chap
   authentication password user1@example.com <password1>
   authentication password user2@example.com <password2>
   authentication password user3@example.com <password3>
   ipcp provide-static-ip-address user1@example.com 192.168.1.1   （固定アドレス）
   ipcp provide-ip-address range 192.168.1.2 192.168.1.253   （動的アドレス）

interface GigaEthernet2.0
   ip address 192.168.1.254/24
   no shutdown

interface range GigaEthernet2 sub 1-3（GigaEthernet2.1～2.3 に同一設定を行う）
   encapsulation pppoe
   auto-connect
   pppoe server
   ppp binding pppoe_server
   ip unnumbered GigaEthernet2.0
   no shutdown
```

接続ユーザに関する情報は show pppoe server を利用してください。
ユーザ ID ごとの状態、MAC アドレス、送受信量、通信時間、無通信時間などを一覧表示します。

上の例では、interface range コマンドで GigaEthernet2.1～2.3 を一度に設定しています。インタフェースの一括設定は注意事項がありますので、保守・運用のインタフェース一括設定を参照してください。

■2.13 ダイアラの設定

ISDN の設定は、ダイアラインタフェースを使用します。
物理レイヤとダイアラインタフェースの関係は論理的に以下の構造をとっています。
他のインタフェースと異なり、ISDN 接続時に下位インタフェースが割り当てられます。



※PRI の複数ポート使用は、INS1500 のみサポートとなります。

ダイアラインタフェースを使用するための基本的な設定手順を次に示します。

2.13.1 基本設定

ISDN の設定は、以下のインタフェースで設定できます。いずれのインタフェースでも同じ設定を行うことができます。

- ✧ BRI0.0,BRI*/*.0
  IX2015/IX2215
- ✧ Dialer
  IX2215 :0-95
  IX3015 :0-511

ダイアラインタフェースの設定は次のとおりです。
全てダイアラのインタフェースコンフィグモードで設定を行います。

dialer string	相手電話番号の登録
dialer anonymous-caller	不特定着信許可の設定 Ver10.1 以降 すべての ISDN インタフェースで設定可能 Ver10.0 以前 IX2000 の場合は BRI インタフェース のみ設定可能 IX3000 の場合は Dialer0 のみ設定可能
dialer inbound-call	ISDN 着信設定
dialer outbound-call	ISDN 発信設定
dialer restraint	期間指定による ISDN 自動発信抑止の設定
dialer total-time	積算接続時間による ISDN 自動発信抑止の設定

forced-disconnect-time	強制切断の設定
idle-time	無通信時間の設定
no shutdown	インタフェースの有効設定
auto-connect	PPP 切断時、自動再接続有効設定
connect	ISDN 手動接続（強制接続）の実行
clear interface	ISDN 手動切断（強制切断）の実行
clear dialer total-time	積算接続時間の初期化
show interfaces	動作状態の表示

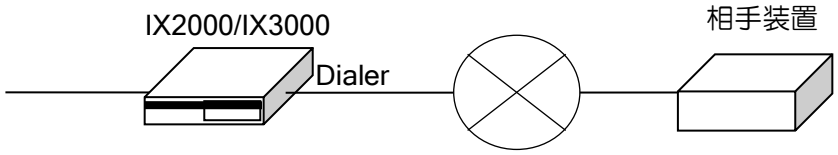
2.13.1.1 ISDN 発信／着信の設定

接続先の電話番号を dialer string を使用して設定します。設定した電話番号は以下の目的のために使用します。

- 発信時の接続先
- 着信時の発信者番号認証

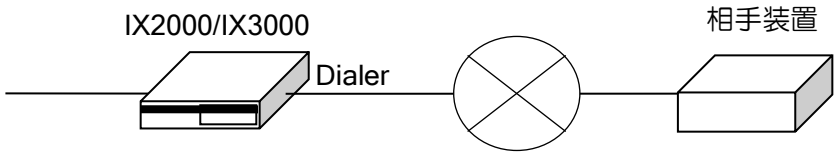
設定した電話番号を使用し、着信時の発信者番号認証を行いますので、設定した電話番号以外は着信しません。

発信時の動作



dialer string 宛てに発呼します。
その際に自分の電話番号として answer1 を使用して発呼します。
answer2 は使用しません。

着信時の動作



answer1 または answer2 に対する発呼のみ着信します。
発呼時に通知された相手電話番号が dialer string に一致していれば着信します。

※発信者番号認証はサブアドレスまで含めた番号が対象となります。サブアドレスを省略し、電話番号のみでの認証はできません。

ISDN（I.430）の設定例

```
【設定例】

ppp profile bri1/0.0
  authentication request chap
  authentication myname ix-1
```

```
   authentication password ix-1 ix-1
   authentication password ix-2 ix-2

device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567

interface GigaEthernet0.0
   ip address 172.18.1.1/24
   no shutdown

interface Dialer0
   encapsulation ppp
   no auto-connect
   dialer string 81-123-4568
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown
```

相手電話番号はインタフェース毎に 8 個まで設定できます。1 つのインタフェースには同じ相手装置（対地）の電話番号のみ設定してください。

複数の電話番号を設定している場合、設定している順番に発信します。1 つの電話番号の接続が失敗した場合、次の電話番号に発信します。

- 発信／着信専用設定

インタフェース毎に発信専用，または着信専用の設定を行うことができます。発信専用の場合は着信，着信専用の場合は発信を行いません。デフォルトでは、発着信可能となっています。

発信／着信の設定を行うコマンドは次の通りです。

dialer inbound-call	ISDN 着信設定
dialer outbound-call	ISDN 発信設定

発信専用／着信専用の設定例

```
【設定例】

!発信専用インタフェース
interface Dialer0
   encapsulation ppp
   no auto-connect
   no dialer inbound-call
   dialer string 81-123-4568
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown

!着信専用インタフェース
interface Dialer1
   encapsulation ppp
   no auto-connect
   no dialer outbound-call
   dialer string 81-123-9999
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown
```

2.13.1.2 不特定着信設定

通常はインタフェースに設定した電話番号にのみ着信しますが、dialer anonymous-caller を設定することにより、全ての電話番号からの着信を受け付けます（不特定着信）。

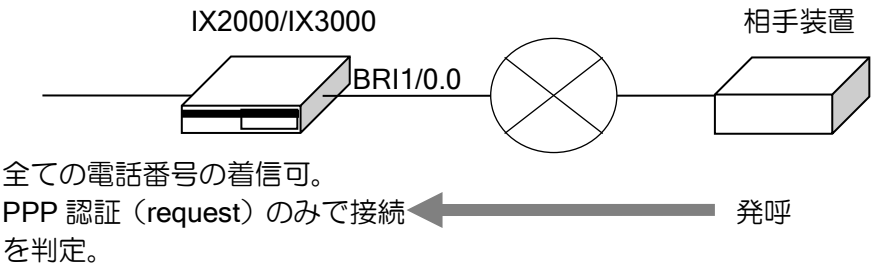
相手装置の電話番号が通知されていない（発信者番号非通知）場合も、同様に着信します。

不特定着信を設定した場合、発信者番号認証を行わず、ISDN の着信を行います。その後、PPP 認証を行い、PPP 認証失敗の場合、PPP セッションは確立せず ISDN は切断されます。また、PPP 認証未設定または、PPP 認証が accept のみの場合も、PPP のセッションは確立されませんので、不特定着信を設定する場合、PPP 認証の request の設定が必須となります。

※Ver.10.0 以前は以下の制限があります。

- IX3015 の場合は Dialer0 のみ設定可能です。
- IX3015 以外の場合は BRI インタフェース（BRI0.0,BRI1/0.0 等）のみ設定可能です。

着信時の dialer anonymous-caller 動作



不特定着信の設定を行うコマンドは次の通りです。

dialer anonymous-caller	不特定着信許可の設定 （Ver.10.0 以前は IX3015 使用時は Dialer0 のみ、その他は BRI インタフェースのみ設定可能）

不特定着信の設定例

【設定例】

```
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix-1
   authentication password ix-1 ix-1
   authentication password ix-2 ix-2

device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567

interface GigaEthernet0.0
   ip address 172.18.1.1/24
   no shutdown

interface BRI1/0.0
   encapsulation ppp
   no auto-connect
   dialer anonymous-caller
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown
```

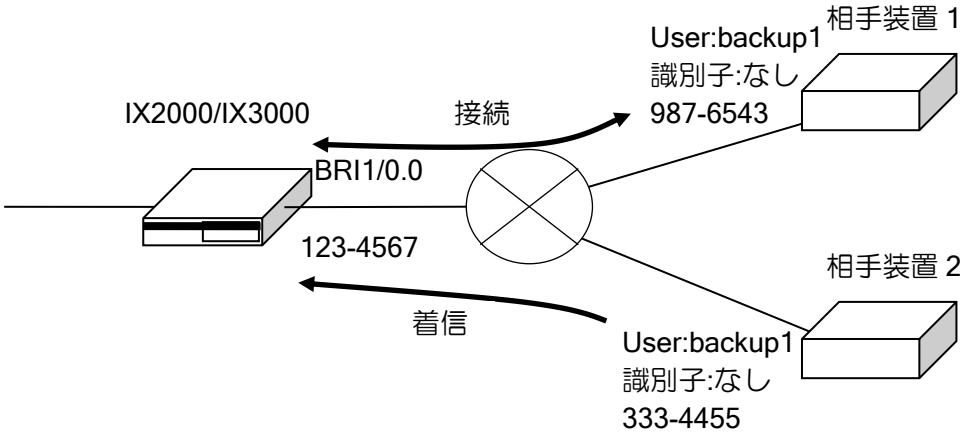
2.13.1.3 PPP の設定

PPP の設定については、PPP の設定の節を参照してください。

- マルチリンク使用時の注意事項

同一インタフェースに複数の電話番号を設定している場合、1 チャンネル接続時に、PPP 認証が同じで、エンドポイント識別子が設定されていない（または、エンドポイント識別子が同じ）同一インタフェースに設定している電話番号からの着信は、同じ装置からの着信とみなしマルチリンクとしてバンドルされますが、1 チャンネル目と異なる装置からの着信の場合、正常に通信できません。

装置が異なる電話番号は、別のインタフェースに設定してください。




```
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix-1
   authentication password backup1 backup1

device BRI1/0
   isdn switch-type ins64
   isdn answer1 123-4567

interface GigaEthernet0.0
   ip address 172.18.1.1/24
   no shutdown

interface BRI1/0.0
   dialer string 987-6543
   dialer string 333-4455
   no auto-connect
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown
```

上記の例のように、相手装置 1 と接続中に同じインタフェースに電話番号が設定されている相手装置 2 からの着信時、PPP 認証が同じでエンドポイント識別子が無い場合、接続中のチャネルと異なる装置からの着信であることの判別ができないため、マルチリンクとして接続されます。

このような状況を避けるために、同一のインタフェースには、同一装置の電話番号のみ設定し、異なる装置の電話番号は、別のインタフェースに設定してください。

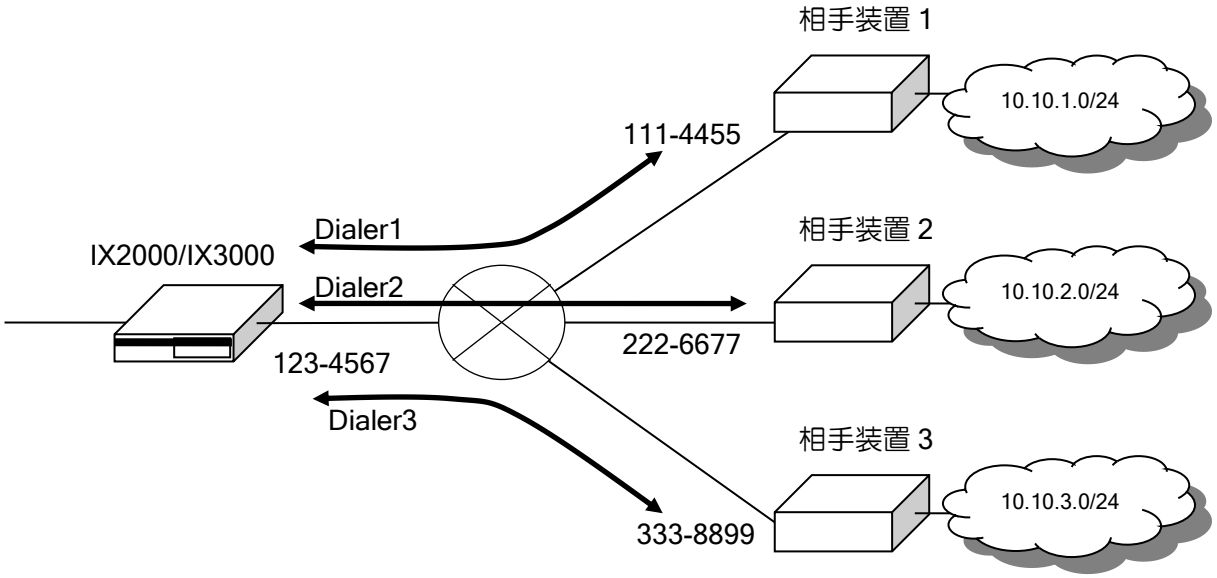
2.13.2 複数対地の設定

ISDN を複数の対地と接続することができます。
ISDN を接続する相手装置（対地）毎に別なダイアラインタフェースに設定を行います。

1 つのインタフェースに対して複数の電話番号を設定できますが、同時に接続可能な電話番号はマルチリンクの場合を除いて、1 つだけとなります。

物理インタフェースが BRI の場合、2B まで接続可能なので、2 対地まで同時に接続が可能です。マルチリンク PPP により、1 対地に対して既に 2B 接続している場合には、優先呼接続を有効にすると優先度に応じて接続中のチャネルの切断を行います。優先呼接続を有効にしていない場合は、既存のチャネルを切断しての発信は行いません。

- 複数のバックアップ



複数対地バックアップの設定例

```
【設定例】
ip route 10.10.1.0/24 Dialer1
ip route 10.10.2.0/24 Dialer2
ip route 10.10.3.0/24 Dialer3

ppp profile backup1
   authentication request chap
   authentication myname ix-1
   authentication password ix-1 ix-1
   authentication password backup1 backup1

ppp profile backup2
   authentication request chap
   authentication myname ix-1
   authentication password ix-1 ix-1
   authentication password backup2 backup2

ppp profile backup3
   authentication request chap
   authentication myname ix-1
   authentication password ix-1 ix-1
   authentication password backup3 backup3
```

```
device BRI1/0
  isdn switch-type ins64
  isdn answer1 123-4567

interface GigaEthernet0.0
  ip address 172.18.1.1/24
  no shutdown

interface Dialer1
  encapsulation ppp
  no auto-connect
  dialer string 111-4455
  ppp binding backup1
  ip unnumbered GigaEthernet0.0
  no shutdown

interface Dialer2
  encapsulation ppp
  no auto-connect
  dialer string 222-6677
  ppp binding backup2
  ip unnumbered GigaEthernet0.0
  no shutdown

interface Dialer3
  encapsulation ppp
  no auto-connect
  dialer string 333-8899
  ppp binding backup3
  ip unnumbered GigaEthernet0.0
  no shutdown
```

2.13.3 発信抑止設定

設定した条件により、自動で発信の抑止を行うことができます。
発信抑止を行う条件として、次の 2 つが設定可能です。

- 期間指定による発信抑止
- 接続時間の積算による発信抑止

2.13.3.1 期間指定による発信抑止

物理、リンクレイヤの設定の BRI インタフェースの設定の節を参照してください。

2.13.3.2 接続時間による発信抑止

接続時間の積算時間が一定時間を超えた後の発信を抑止することができます。再度発信を行うためには、接続時間の初期化が必要です。接続時間の積算は、インタフェース単位に、自装置から発信した場合に行います。ただし、オンデマンド帯域制御を使用している場合、2B 目以降の発信は抑止されません。

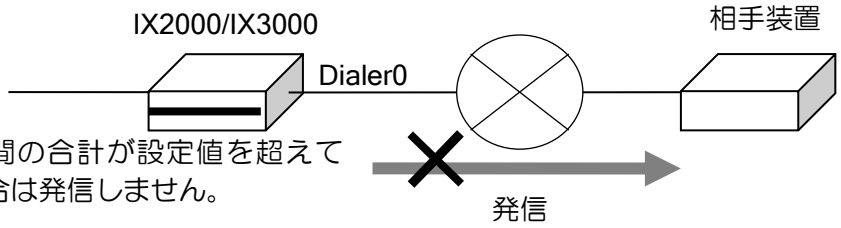
接続中に積算時間を超えた場合は、自装置から発呼した接続中の回線については、そのまま接続するか、切断するかを選択できます。

一定周期で積算時間を初期化する機能はありませんので、コマンドにより初期化する必要があります。

以下のような動作となります。

- 起動時から接続時間の積算を行います。発信抑止時間を設定時には必要に応じて、接続時間の初期化を行ってください。
- ISDN 接続中に接続時間の初期化を行った場合、その時点から接続時間の積算を行います。
- 接続途中でマルチリンク接続（2B 接続）を行った場合、最初に接続してから切断するまでの時間となります。マルチリンク接続の時間は 2 倍にはなりません。

接続時間による発信抑止の動作



積算接続時間による発信抑止を行うコマンドは次の通りです。

dialer total-time	積算接続時間による ISDN 自動発信抑止の設定

接続時間による発信抑止の設定例

【設定例】

合計時間 100 分で切断する場合の設定例

```
ppp profile bri1/0.0
  authentication request chap
  authentication myname ix-1
  authentication password ix-1 ix0-1
  authentication password ix-2 ix-2

device BRI1/0
  isdn switch-type ins64
```

```
   isdn answer1 81-123-4567

interface GigaEthernet0.0
   ip address 172.18.1.1/24
   no shutdown

interface Dialer0
   encapsulation ppp
   no auto-connect
   dialer total-time 100 disconnect
   dialer string 81-123-4568
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown
```

2.13.4 自動切断

2.13.4.1 無通信による切断

無通信状態が一定時間続いた場合に、切断します。デフォルトでは無通信時間 120 秒で切断します。

無通信の対象は、送信方向のみ，受信方向のみ，両方向を選択できます。

無通信による切断の設定を行うコマンドは次の通りです。

idle-time	無通信時間の設定

無通信による切断の設定例

【設定例】

両方向の無通信時間が 300 秒で切断する場合の設定例

```
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix-1
   authentication password ix-1 ix1-1
   authentication password ix-2 ix1-2

device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567

interface GigaEthernet0.0
   ip address 172.18.1.1/24
   no shutdown

interface BRI1/0.0
   encapsulation ppp
   no auto-connect
   idle-time 300
   dialer string 81-123-4568
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown
```

2.13.4.2 接続時間による強制切断

通信の状態に関係なく、一定時間接続している場合に切断します。
接続時間による切断の設定を行うコマンドは次の通りです。

forced-disconnect-time	強制切断の設定

接続時間による強制切断の設定例

【設定例】

100 分間接続で強制切断する場合の設定例

```
ppp profile bri1/0.0
   authentication request chap
   authentication myname ix-1
   authentication password ix-1 ix1-1
   authentication password ix1-2 ix1-2

device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567

interface GigaEthernet0.0
   ip address 172.18.1.1/24
   no shutdown

interface BRI1/0.0
   encapsulation ppp
   no auto-connect
   forced-disconnect-time 100
   dialer string 81-123-4568
   ppp binding bri1/0.0
   ip unnumbered GigaEthernet0.0
   no shutdown
```

2.13.5 優先接続

ISDN の全てのチャネルが使用中の状態で、接続を行いたいインタフェースが存在する場合、優先度の低いインタフェースの B チャネルを切断することにより、新規の呼を接続することが可能となります。

接続中のインタフェースと新規に接続するインタフェースの優先度は、以下の順で比較をおこないます。上にある条件が優先されます。

- 使用 B チャネル数（新規の呼は接続したいチャネルも接続中とカウントします）
  - 使用 B チャネルが 1 のインタフェース
  - 使用 B チャネルが 2 以上で初期リンク数（min-links）以下のインタフェース
  - 使用 B チャネルが初期リンク数（min-links）を超えるインタフェース
- プライオリティ値
  - 255
    :
  - 0
- 呼の種類
  - 既存の呼
  - 新規の呼

同じ条件のインタフェースが複数存在する場合は、ランダムに選択されます。

新規に接続するインタフェースの優先度が高い場合は、優先度の低いインタフェースから 1 チャネル切断します。チャネルが足りない場合は、必要なチャネル数を確保できるまで、優先度の低いインタフェースを選択し、1 チャネルずつ切断していきます。途中で、切断可能なインタフェースが存在しなくなった場合は、初期リンク数に満たない場合でも、その時点で接続を終了します。

【優先接続の動作例】

最初の状態

インタフェース	min-links	接続 Bch 数	Priority
Dialer1	3	5B	200
Dialer2	1	1B	50
Dialer3	5	2B	100

※動作例ですので、実際にこの状態から始まることはありません。
min-links 3 以上サポートは ver7.2 以降となります。

(1)Dialer4（min-links=3,Priority=150）の接続要求

(2) Dialer1 は min-links 以上接続,Dialer4 は 1B 接続なので、Dialer1 の 1B を切断

(2)の後の状態

インタフェース	min-links	接続 Bch 数	Priority
Dialer1	3	4B	200
Dialer2	1	1B	50
Dialer3	5	2B	100
Dialer4	3	1B	150

(3)Dialer4 は min-links に満たないので、再度優先度の比較を行う。
(4)まだ Dialer1 は min-links 以上なので、Dialer1 の 1B を切断

(4)の後の状態

インタフェース	min-links	接続 Bch 数	Priority
Dialer1	3	3B	200
Dialer2	1	1B	50
Dialer3	5	2B	100
Dialer4	3	2B	150

(5)Dialer4 は min-links に満たないので、再度優先度の比較を行う。
(6)既存の呼の中では min-links を超える呼は存在しない。接続数が 2 以上 min-links 以下の中では、Dialer3 の優先度が低い。
(7)Dialer3 と Dialer4 では、Dialer3 の Priority の方が低いので、Dialer3 の 1B を切断

(7)の後の状態

インタフェース	min-links	接続 Bch 数	Priority
Dialer1	3	3B	200
Dialer2	1	1B	50
Dialer3	5	1B	100
Dialer4	3	3B	150

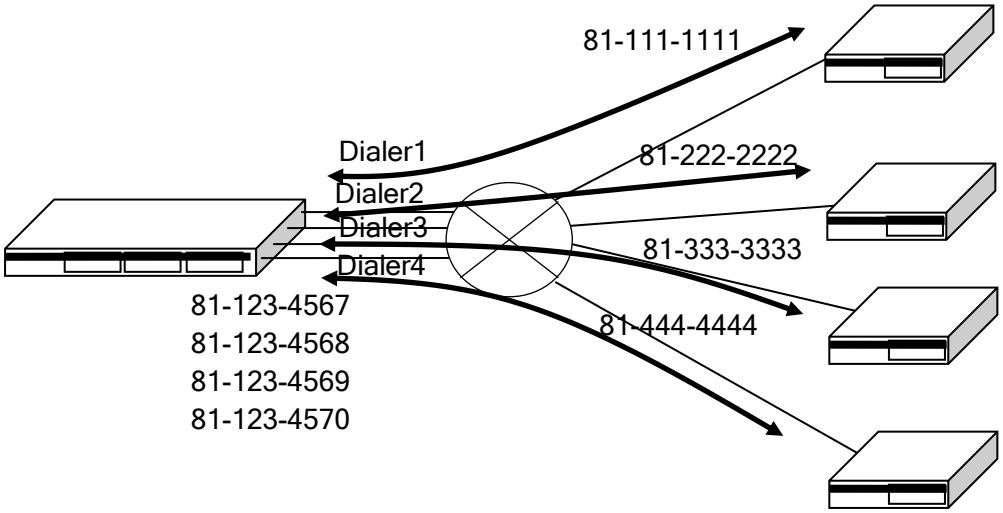
(8)Dialer4 は min-links まで接続できたので終了。

接続中のインタフェースと新規に接続されるインタフェースの初期リンク数の合計が、使用可能なチャネル数より小さい場合は、初期リンク数は確保されますが、初期リンク数の合計が使用可能なチャネル数より大きい場合は、プライオリティ値の低いインタフェースは初期リンク数以下となります。

接続 B チャネル数が初期リンク数以下のインタフェース（上記の例では Dialer3）が存在する場合に、他のインタフェースが切断しても、すぐには接続されません。オンデマンド帯域制御により、発呼処理が行われます。

プライオリティ値を設定するコマンドは次の通りです。

dialer priority-connection enable	優先接続有効設定 （グローバルコンフィグ）
dialer priority	優先接続プライオリティ値の設定 （インタフェースコンフィグ）



優先接続の設定例

【設定例】

```
dialer priority-connection enable

ppp profile ppp1
   authentication myname ix3000-1
   authentication password ix3000-1 ix3000-1
   authentication password ix2010-1 ix2010-1
   multilink enable
   multilink max-links 5
   multilink min-links 3

ppp profile ppp2
   authentication myname ix3000-1
   authentication password ix3000-1 ix3000-1
   authentication password ix2010-2 ix2010-2
   multilink enable
   multilink max-links 3
   multilink min-links 1

ppp profile ppp3
   authentication myname ix3000-1
   authentication password ix3000-1 ix3000-1
   authentication password ix2010-3 ix2010-3
   multilink enable
   multilink max-links 10
   multilink min-links 5
```

```
ppp profile ppp4
   authentication myname ix3000-1
   authentication password ix3000-1 ix3000-1
   authentication password ix2010-4 ix2010-4
   multilink enable
   multilink max-links 5
   multilink min-links 3

device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567

device BRI1/1
   isdn switch-type ins64
   isdn answer1 81-123-4568

device BRI1/2
   isdn switch-type ins64
   isdn answer1 81-123-4569

device BRI1/3
   isdn switch-type ins64
   isdn answer1 81-123-4570

interface GigaEthernet0.0
   ip address 172.18.1.1/24
   no shutdown

interface Dialer1
   encapsulation ppp
   dialer string 81-111-1111
   dialer priority 200
   ppp binding ppp1
   ip unnumbered GigaEthernet0.0
   no shutdown

interface Dialer2
   encapsulation ppp
   dialer string 81-222-2222
   dialer priority 50
   ppp binding ppp2
   ip unnumbered GigaEthernet0.0
   no shutdown

interface Dialer3
   encapsulation ppp
   dialer string 81-333-3333
   dialer priority 100
   ppp binding ppp3
   ip unnumbered GigaEthernet0.0
   no shutdown

interface Dialer4
   encapsulation ppp
   dialer string 81-444-4444
   dialer priority 150
   ppp binding ppp4
   ip unnumbered GigaEthernet0.0
   no shutdown
```

■2.14 データコネクト対応オンデマンド VPN 機能の設定

「フレッツ光ネクスト等の NGN」回線で「ひかり電話」を契約している場合、帯域確保型のデータ通信サービスである「データコネクト」を利用して、オンデマンドの VPN 環境を構築することができます。本機能は Ver8.6 以降で利用可能です（IX3010 のみ Ver8.7 以降）。

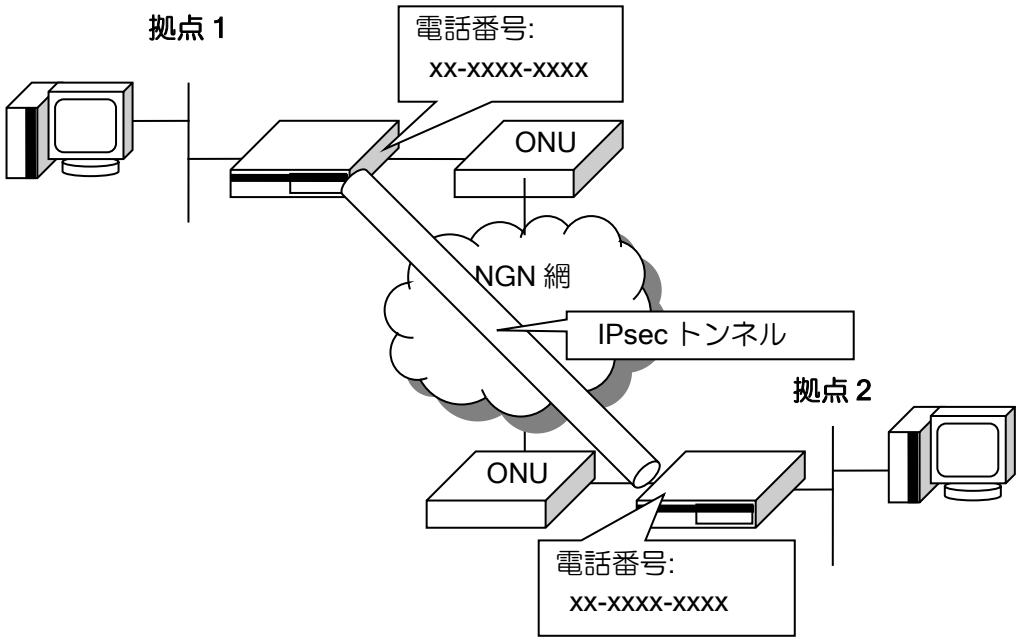
Ver8.7 以降では、ナンバーゲート接続やホームゲートウェイ（ひかり電話ルータ）・オフィスゲートウェイ（ひかり電話オフィスタイプ対応アダプタ）を介した接続も可能です。

Ver9.5 以降では、IPsec の IKEv2 対応および RADIUS 認証機能に対応しています。

2.14.1 データコネクト機能概要

データコネクトは、あて先に電話番号を使った帯域確保型のデータ通信サービスです。ベストエフォート型のサービスとは異なり、帯域保証型のサービスとなっているため安定した通信が可能です。

通信は SIP サーバを介して UDP で行う必要があるため、IX2000/IX3000 シリーズでは IPsec の NAT トラバーサル機能を利用します。また、帯域制御は装置側で行う必要があるため、QoS の設定が必要です。



2.14.2 契約条件

本機能は以下の契約条件で動作します。

- フレッツ光ネクスト
- ひかり電話
- ひかり電話オフィスタイプ
- ひかり電話オフィス A（エース）
- ナンバーディスプレイ（着信側のみ必要）
- 発信電話番号通知（発信側のみ必要）
- 対向先拠点数分のチャンネル数契約

データコネクトの回線速度の上限は、チャンネルごとに 1Mbps です。

2.14.3 制限事項

以下の機能はサポートしておりません。

- IX ルータ以外の装置との接続
- IPsec NAT トラバーサル機能を使用しない接続
- データコネクトサービスの IPv6 対応
- 複数の NGN 回線の収容
- 追加番号による発信（OGW 配下などでの発信は可能）
- VRF のインタフェースでの接続

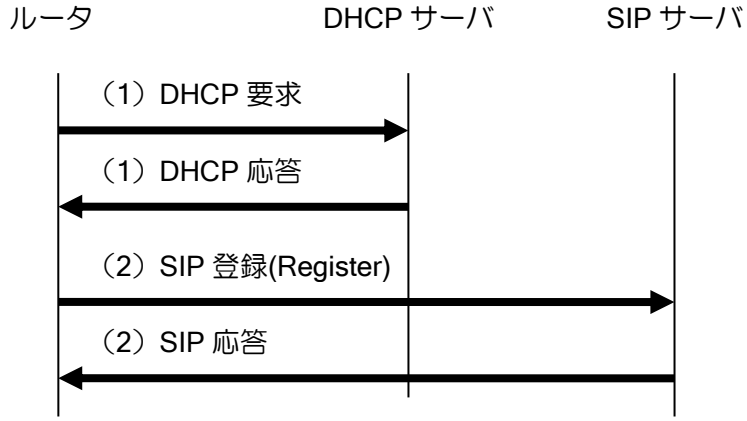
2.14.4 注意事項

- 複数の回線を契約していて、現在接続している回線から別の回線にケーブルを繋ぎかえる場合、2～3 分程度接続できないことがあります。ケーブルを抜いて繋ぎなおす前に NGN のインタフェースを shutdown としておくか、接続後装置を再起動してください。

2.14.5 データコネクトサービスの概要

NGN 機能を有効にして対象の回線にケーブルを接続すると、ルータは DHCP で IP アドレスのほかに電話番号や SIP サーバのアドレスを取得します。データコネクト機能を利用する場合の DHCP や SIP の動作概要を説明します。

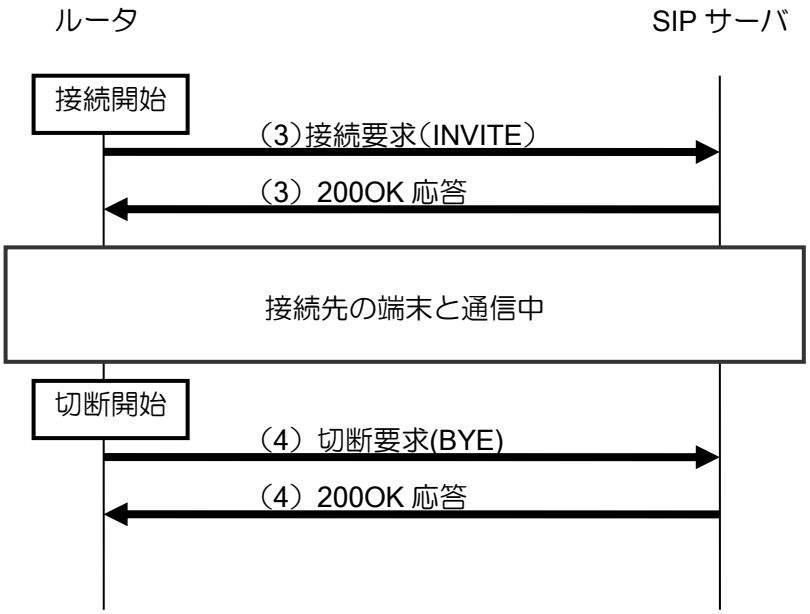
（主要なシーケンス以外は省略しています。DHCP サーバ、SIP サーバは NGN 網にあります）



（1） DHCP サーバからは、IP アドレス、電話番号、SIP サーバアドレスなどの情報を取得します。

（2） DHCP で取得した、アドレスと電話番号を SIP サーバに登録します。

登録が完了していれば、いつでも発着信可能です。拠点 1 側から発信して切断する場合のシーケンスを以下に示します（拠点 1 側のみで、主要なシーケンス以外は省略しています）。



(3)　SIP サーバに宛先の電話番号への INVITE を送信することで接続要求します。トラフィックの種類や帯域などの情報を通知し、相手装置と条件が一致すれば接続されます。

(4)　BYE を送信することで切断されます。

接続開始は他拠点宛の通信を受信したとき、切断開始は通信が全て終了して一定時間経過したときにそれぞれ自動的に行われます。

着信する場合も同様で、矢印の向きが反対になります。

2.14.6 基本設定（IKEv1/Ver8.8 以降）

NGN 網のデータコネクトサービスを利用して拠点間通信を行うためには、NGN コマンド以外に、IPsec や QoS などのいくつかの機能も合わせて設定が必要になります。
以下の全ての設定が必要です。

- イーサネットインタフェースの NGN 機能の設定
- NGN プロファイルの設定
- IPsec トンネル(NAT トラバーサル)の設定
- トンネルインタフェースの設定
- QoS の設定

なお、Ver8.8 以降では QoS 設定を省略する機能が追加されています。ここでは Ver8.8 でデータコネクト対応オンデマンド VPN 機能により拠点間通信を行う場合の全体の設定例を示し、それぞれの設定について詳細に説明します。

【設定例】

```
ip route 192.168.2.0/24 Tunnel0.0
ip ufs-cache enable

ip access-list sec-list permit ip src any dest any
ike proposal ike-prop encryption aes hash sha
ike policy ike-policy peer ngn-dynamic key secret mode aggressive ike-prop
ike local-id ike-policy keyid kyoten-1
ike remote-id ike-policy keyid kyoten-2
ike nat-traversal force
ipsec autokey-proposal ipsec-prop esp-aes esp-sha
ipsec dynamic-map ipsec-policy sec-list ipsec-prop ike-binding ike-policy
ipsec local-id ipsec-policy 192.168.1.0/24
ipsec remote-id ipsec-policy 192.168.2.0/24

ngn profile ngn_profile
   bandwidth 1000

interface GigaEthernet0.0
   ip address dhcp
   service-policy enable
   service-policy output default-policy-map-ngn
   ngn ip enable
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.1.254/24
   no shutdown

interface Tunnel0.0
   tunnel mode ipsec
   dialer string 2000
   idle-time 120
   ngn binding GigaEthernet0.0 ngn_profile ike-policy ike-policy
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   ipsec policy tunnel ipsec-policy df-bit ignore pre-fragment out
   no shutdown
```

2.14.6.1 イーサネットインタフェースの NGN 機能の設定

まず、NGN に接続するイーサネットインタフェースを決定し、以下のコマンドを設定します。

ngn ip enable	NGN 機能の有効化(イーサネットインタフェース)

【設定例】

```
interface GigaEthernet0.0
  ip address dhcp
  ngn ip enable
  no shutdown
```

ngn ip enable を設定すると、イーサネットインタフェースは NGN 網に接続可能になり、NGN 網に許可されていない通信を廃棄するフィルタリングが自動的に動作します（送信方向のみ）。

NGN 網に設定するインタフェースの IPv4 アドレスは DHCP で設定します。ngn ip enable が設定されているインタフェースの DHCP は、NGN 網に接続するための認証設定が行われ、DHCP 経由で IP アドレスのほか、SIP サーバのアドレスや電話番号などの情報を取得できるようになります（認証の設定は自動で行います。ip dhcp-client authentication の設定はしないでください)。

なお、このインタフェースには QoS も設定しますが、説明は後述の項目を参照してください。

2.14.6.2 NGN プロファイルの設定

NGN プロファイルを設定し、NGN 網に通知するセッション情報を設定します。データコネクト対応オンデマンド VPN 機能で使用するプロトコルやポート番号などは自動的に設定するので、ここでは帯域の設定を行います。

ngn profile	NGN プロファイルの設定 （グローバルコンフィグモード）
bandwidth	SDP で通知する帯域の設定 （NGN プロファイルコンフィグモード）

【設定例】

```
ngn profile ngn_profile
  bandwidth 1000
```

複数の拠点と接続する場合、NGN プロファイルは共用できます。

bandwidth の設定は接続先の拠点と同一の値を設定しないと接続できません。

2.14.6.3 IPsec（NAT トラバーサル）の設定

データコネクト対応オンデマンド VPN 機能では IPsec（NAT トラバーサル）の通信を利用します。IPsec（NAT トラバーサル）機能自体の説明は、IKE/IPsec の項目を参照してください。NGN 網に接続する場合は以下の 3 つの設定が必須です。

- IKE の宛先アドレスは NGN 網から動的に取得するため、peer は ngn-dynamic とします。
- ipsec dynamic-map の設定では、ike-binding で関連する ike のポリシーを指定します。
- 強制的に UDP でカプセル化するため ike nat-traversal の設定は force を指定します。

プロポーザルは任意の設定が利用可能です。

IKE/IPsec の設定の詳細については、IKE/IPsec の章を参照してください。

【設定例】
```
ip route 192.168.2.0/24 Tunnel0.0
ip ufs-cache enable

ip access-list sec-list permit ip src any dest any
ike proposal ike-prop encryption aes hash sha
ike policy ike-policy peer ngn-dynamic key secret mode aggressive ike-prop
ike local-id ike-policy keyid kyoten-1
ike remote-id ike-policy keyid kyoten-2
ike nat-traversal force
ipsec autokey-proposal ipsec-prop esp-aes esp-sha
ipsec dynamic-map ipsec-policy sec-list ipsec-prop ike-binding ike-policy
ipsec local-id ipsec-policy 192.168.1.0/24
ipsec remote-id ipsec-policy 192.168.2.0/24

interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   ipsec policy tunnel ipsec-policy df-bit ignore pre-fragment out
   no shutdown
```

ipsec policy の設定は pre-fragment が必須です。NGN 網はフラグメントパケットを許可しないため、暗号化前にフラグメントすることでフラグメントされる通信が可能になります。
また TCP のフラグメントを避けるため、ip tcp adjust-mss を設定することを推奨します。

2.14.6.4 IPsec 以外のトンネルインタフェースの設定

以下の 3 つの設定が必要です。

ngn binding	NGN 機能の割り当て。インタフェースに NGN プロファイルと IKE ポリシーを割り当てます。
dialer string	宛先の電話番号を指定します。
idle-time	設定時間無通信の場合に切断します。

【設定例】
```
interface Tunnel0.0
   dialer string 2000
   idle-time 120
   ngn binding GigaEthernet0.0 ngn_profile ike-policy ike-policy
```

2.14.6.5 QoS の設定（Ver8.8 以降）

NGN 網では保証帯域を超えるトラフィックは破棄されます。このため帯域を超えないようにシェーピング機能を設定しておく必要があります。

Ver8.8 以降では、default-policy-map-ngn という名前で QoS を設定するだけで、自動的に NGN の帯域にあわせてシェーピングを行います。QoS の設定は次のコンフィグのみで利用できます。

service-policy output default-policy-map-ngn	NGN の QoS 自動設定

```
【設定例】
 interface GigaEthernet0.0
    service-policy enable
    service-policy output default-policy-map-ngn
```

※default-policy-map-ngn では、内部的にトンネルごとのクラスを用意し、それぞれ回線帯域でシェーピングを設定します。NGN トンネルを通る通信が全てこれらのクラスの normal キューに分類され、回線帯域にあわせてシェーピングします。

NGN 網でシェーピング以外の QoS の機能を併用したい場合、Ver8.7 以前の場合については default-policy-map-ngn が利用できませんので、本章の QoS 詳細設定の方法を参照してください。

2.14.6.6 多対地の場合の設定

対地の数だけ IKE/IPsec の設定と QoS の設定が必要です。ngn profile は設定が同じ場合は共用できます。

IX3110 を使用する際、対地数が多い場合は receive-buffers コマンドでバッファサイズの調整が必要になる場合があります。詳しくは QoS の章を参照してください。

2.14.7 基本設定（IKEv2/Ver9.5 以降）

Ver9.5 以降では IKEv2 を利用してデータコネクト接続を利用できます。
IKEv2 の場合の設定例は以下のとおりです。

```
【設定例】
ip route 192.168.2.0/24 Tunnel0.0
ip ufs-cache enable

ikev2 authentication psk id keyid kyoten-1 key char secret1
ikev2 authentication psk id keyid kyoten-2 key char secret2

ikev2 default-profile
  local-authentication psk id keyid kyoten-1
  nat-traversal keepalive 20 force

ngn profile ngn_profile
  bandwidth 1000

interface GigaEthernet0.0
  ip address dhcp
  service-policy enable
  service-policy output default-policy-map-ngn
  ngn ip enable
  no shutdown

interface GigaEthernet1.0
  ip address 192.168.1.254/24
  no shutdown

interface Tunnel0.0
  dialer string 2000
  ngn binding GigaEthernet0.0 ngn_profile ikev2
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet1.0
  ip tcp adjust-mss auto
  ikev2 ipsec pre-fragment
  ikev2 peer-ngn-dynamic authentication psk id keyid kyoten-2
  no shutdown
```

IKEv2 の送信先は NGN 網から動的に取得するため peer-ngn-dynamic を指定します。また、NAT トラバーサルの設定を利用するため、デフォルトプロファイルに force で設定してください。さらに網内でのリアセンブルを防止するため、MSS 調整と ikev2 ipsec pre-fragment コマンドの設定を推奨します。その他の設定は IKEv2 の章を参照してください。

※IKEv2 使用時、自動接続（ikev2 connect-type auto）には対応していません。

2.14.8 RADIUS 連携の設定（IKEv2/Ver9.5 以降）

電話番号などの着信に必要な設定を RADIUS サーバに登録し、認証やアカウンティングを RADIUS サーバで一元管理することができます。ルータに 1 つ 1 つ電話番号を設定する必要がなく、利用者ごとの接続時間等を管理できるようになります。

2.14.8.1 アトリビュート

データコネクトの RADIUS 認証およびアカウンティングで送受信するアトリビュートです。

（a）Access-Request のアトリビュート

番号	アトリビュート	Value
1	User-Name	発信元の電話番号
2	User-Password	radius host コマンドで設定した秘密共有鍵
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
5	NAS-Port	利用しない
61	NAS-Port-Type	利用しない

（b）Access-Accept のアトリビュート

番号	アトリビュート	Value
22	Framed-Route	発信元への IPv4 スタティックルート
69	Tunnel-Password	発信元との IKEv2 事前共有鍵

Framed-Route の Radius サーバへの登録は、「192.168.0.0/24」のようにプレフィックス長を指定する形式で登録してください。登録可能な経路は 1 電話番号あたり最大 16 経路です。

この経路は接続中のみ有効です。ルーティングプロトコルで再配信することも可能です。

（c）Accounting-Request のアトリビュート

番号	アトリビュート	Value
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
30	Called-Station-Id	着信側電話番号
31	Calling-Station-Id	発信側電話番号
40	Acct-Status-Type	アカウンティングステータス（start/stop のみ）
44	Acct-Session-Id	アカウンティングセッション ID
46	Acct-Session-Time	セッション使用時間（切断時のみ）

2.14.8.2 着信側の設定

着信側の RADIUS 認証およびアカウンティングを行う場合の設定例です。
トンネルの設定は同時着信数分必要ですが、下記の設定例に示す通り一括での設定が可能です。

【着信側設定例】
16 拠点まで同時接続できるよう 16 トンネルを設定する場合

```
aaa enable
aaa authentication ngn default group radius
aaa accounting ngn default start-stop local group radius
!
radius host ip 192.168.0.1 key 0 <RADIUS 認証共通秘密鍵>
!
ikev2 authentication psk id keyid <着信側電話番号> key char <着信側  事前共有鍵>
!
ngn profile ngnprof
   bandwidth 1000
!
ikev2 default-profile
   local-authentication psk id keyid <着信側電話番号>
   nat-traversal keepalive 20 force
!
interface GigaEthernet0.0
   ip address dhcp
   service-policy enable
   service-policy output default-policy-map-ngn
   ngn ip enable
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.0.254/24
   no shutdown
!
interface range Tunnel 1-16
   ngn binding GigaEthernet0.0 ngnprof ikev2
   ngn authentication radius
   tunnel mode ipsec-ikev2
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   ikev2 ipsec pre-fragment
   ikev2 peer-ngn-dynamic authentication radius
   no shutdown
```

2.14.8.3 発信側の設定

発信側では RADIUS 認証はできませんが、アカウンティングは動作します。
以下は、アカウンティングを行う場合の設定例です。

```
【発信側設定例】
 aaa enable
 aaa accounting ngn default start-stop local group radius
 !
 radius host ip 192.168.0.254 key 0 <RADIUS 認証用共通秘密鍵>
 !
 ip route 192.168.2.0/24 Tunnel0.0
 !
 ikev2 authentication psk id keyid <発信側電話番号> key char <発信側  事前共有鍵>
 ikev2 authentication psk id keyid <着信側電話番号> key char <着信側  事前共有鍵>
 !
 ngn profile ngnprof
    bandwidth 1000
 !
 ikev2 default-profile
    local-authentication psk id keyid <発信側電話番号>
    nat-traversal keepalive 20 force
 !
 interface GigaEthernet0.0
    ip address dhcp
    service-policy enable
    service-policy output default-policy-map-ngn
    ngn ip enable
    no shutdown
 !
 interface GigaEthernet1.0
    ip address 192.168.0.1/24
    no shutdown
 !
 interface Tunnel0.0
    dialer string <対向装置電話番号>
    ngn binding GigaEthernet0.0 ngnprof ikev2
    tunnel mode ipsec-ikev2
    ip unnumbered GigaEthernet1.0
    ip tcp adjust-mss auto
    ikev2 ipsec pre-fragment
    ikev2 peer-ngn-dynamic authentication psk id keyid <着信側電話番号>
    no shutdown
```

2.14.9 QoS の詳細設定

データコネクト機能では自動的に NGN の帯域にあわせてシェーピングを行いますが、詳細な QoS の設定を行いたい場合は、通常の QoS の設定を行う必要があります。

NGN トンネルインタフェースごとに適切なシェーピングを設定する必要があるため、以下のように NGN トンネルを指定してクラスを選択する手段を用意しています（Ver8.8 以降）。

match ngn	NGN トンネルにマッチする

【設定例】

```
class-map match-any class-ngn-vpn
  match ngn Tunnel0.0

policy-map ngn-vpn-policy-map
  class class-ngn-vpn
    shape 1000000 16000
```

シェーピングの CIR 値は、ngn profile で設定した bandwidth 以下の値に設定してください。対地数が多く QoS の負荷が高い場合は、Tc が 16ms～50ms 程度となる範囲での運用を推奨します。

IPsec の機能を利用するため、IPsec のヘッダを送信する分だけ使用できる帯域は小さくなることに注意してください。

なお、シェーピングの帯域は通常 MAC ヘッダを含む値ですが、NGN 網では IP パケットサイズのみで計算します。Ver8.7 以降では、qos rate-accounting layer-3 の設定を行うことで IP パケットサイズで帯域計算を行うため、設定をしない場合よりも多くの帯域が利用できます。

2.14.9.1 発着信およびタイマ制御の設定

発着信専用にする設定、通信時間や時刻を監視して切断する設定、特定の時間帯で発信しないようにする設定などが可能です。全てトンネルインタフェースで設定します。

dialer inbound-call dialer outbound-call	着信拒否設定 発信拒否設定
dialer restraint dialer total-time	時刻による発信抑止 接続時間による発信抑止
idle-time	無通信時間の設定
forced-disconnect-time	強制切断タイマの設定

2.14.10 動作確認方法

多数の機能を組み合わせて動作させるため、動作確認する機能も多岐に渡ります。ここでは問題発生時の切り分け方法を簡単に説明します。

- NGN 網との接続確認
- 疎通確認

2.14.10.1 確認コマンド一覧

NGN 機能は以下の表示コマンドと、イベントログの記録コマンドがあります。NGN 機能のイベントログは内部の機能ブロック単位でさらに 3 つに細分化されていますが、特に理由がない場合は全て warn レベルで運用してください。

show ngn status	NGN 機能の状態を表示
show ngn statistics	NGN 機能の統計情報を表示
show ngn history show ngn active	発着信の履歴表示 （active は接続中のセッションのみを表示）
logging subsystem ngns	NGN 機能全体を統括する機能で発生したイベントを記録 • 内部エラーや遮断フィルタによる廃棄など
logging subsystem ngna	NGN 機能の、主に SIP プロトコル上のイベントを記録 • 登録やセッション管理上の問題（タイムアウト）など
logging subsystem ngnt	NGN 機能の、主にトンネルインタフェース上の機能に関するイベントを記録 • 発着信の問題（発信規制や輻輳の検出）など

2.14.10.2 NGN 網との接続確認

NGN 網にケーブルを接続すると、DHCP でアドレスや SIP サーバの情報を取得して、SIP サーバに登録するまでを自動的に行います。以上が正しく完了しない場合、通信はできません。

NGN 網との接続状態は show ngn status コマンドで確認できます。

show ngn status	NGN 網との接続状態を確認します。

NGN 回線にケーブルを接続して show ngn status で以下のように「Location is registered」と表示されていれば、NGN 網への登録（Register）までは成功したことになります。

```
【表示例】
Router(config)# show ngn status
  NGN service is enabled on GigaEthernet0.0
    SIP URI is sip:xxx-xxxx-xxxx@xxxx.xx.xx
    Call handle is 09CB3258
    Location is registered at 192.168.0.12, 0:00:26
    Pre-existing route set is
      sip:192.168.0.12:5060;lr
    Last update at 2011/01/01 0:00:00
    Last status: OK (200)
    3 call handles are using (1 register, 2 sessions)
```

registered にならない場合は、正しいポートにケーブルを接続したか、NGN 通信を行うインタフェースに ip address dhcp, ngn ip enable, no shutdown が設定されているか確認してください。また、SIP（UDP ポート 5060）の送信をフィルタリングしていないかも確認してください。

2.14.10.3 他拠点との疎通確認

NGN 回線に正しく登録されたら、Ping のコマンドで接続先の拠点と疎通確認を行ってください。応答がない場合は以下のコマンドで接続されているかどうかを確認してください。

show ngn active	接続中のセッションの表示
show ngn history	接続履歴の表示

```
【表示例】
Router(config)# show ngn history
2011/01/01 00:00:00, Tunnel0.0, out, xxxxxxxxxx > xxxxxxxxxx
  Used time 0:02:10, idle time 0:00:00/0:00:00, status active
    Trigger packet ip udp (src 192.168.1.1:60000, dest 192.168.1.2:60001)
```

2 行目の status が active となっていて通信ができれば設定は問題ありません。

status が failure となる場合は、NGN の宛先電話番号や、ngn profile の bandwidth の設定が他拠点の装置のものと一致しているか確認してください。また、イベントログを warn に設定していれば、何らかの障害が検出されている可能性があります。

status が active で通信できない場合は、SIP のセッションは確立しているため、IPsec の設定不備の可能性があります。

また、何も表示されない場合は発信できていないので、Ping の送信先、送信元アドレスや、Tunnel の IPsec の設定、発信抑止設定などを確認してください。

2.14.10.4 その他機能の確認

セッションが確立している場合（status が active で通信できない場合）は、NGN 以外の機能の問題の可能性があるので、IPsec や IKE などのログを確認する必要があります。

NGN 網では IPsec や IKE の宛先アドレスやポートは、相手側装置のアドレスやポートではなく、網内の SBC（SSE）と呼ばれる装置のアドレスやポートになります。このため、IPsec などの機能のログを確認する場合、show ngn status コマンドなどで問題のセッションの宛先アドレスやポートが何になっているか確認する必要があります。

show ngn status	NGN 網との接続状態を確認します。

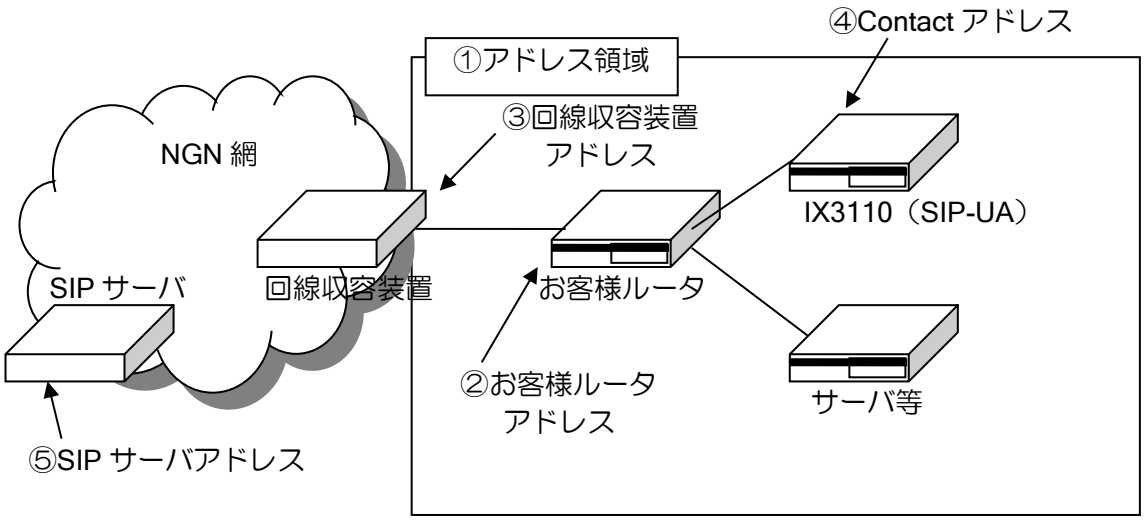
セッションが確立している場合は、登録情報の外にセッション情報が表示されます。

```
【表示例】
Router(config)# show ngn status
  NGN service is enabled on GigaEthernet0.0
    SIP URI is sip:xxx-xxxx-xxxx@xxxx.xx.xx
    Call handle is 09CB3258
    Location is registered at 192.168.0.12, 0:00:26
    Pre-existing route set is
      sip:192.168.0.12:5060;lr
    Last update at 2011/01/01 0:00:00
    Last status: OK (200)
    3 call handles are using (1 register, 2 sessions)
  Session list:
    Session id 1 on Tunnel0.0
      Dialer string is xxx-xxxx-xxxx
      Connection address is 192.168.0.1, 4500/udp
      Bandwidth is 1000kbps
      Handle is 099718D8
```

Connection address に記載されている情報が、IKE や IPsec などのログに表示される相手の IP アドレス、ポート、プロトコルになります。NGN 以外の機能の表示コマンドやログを確認する際には、この値を参照してください。

2.14.11 ひかり電話ナンバーゲート対応

Ver8.7 以降、オンデマンド VPN 機能は、ひかり電話ナンバーゲートサービスに対応しています。サービス提供事業者様や一般企業様のセンタ拠点向け大容量帯域確保型通信サービスで、同時に 200 回線まで利用可能となります。



通常のオンデマンド VPN 機能と異なり DHCP は利用しません。このため上記の①～⑤のアドレスと契約電話番号等が通知されますので、それらをコンフィグで設定します。

【設定例】（SIP-UA）

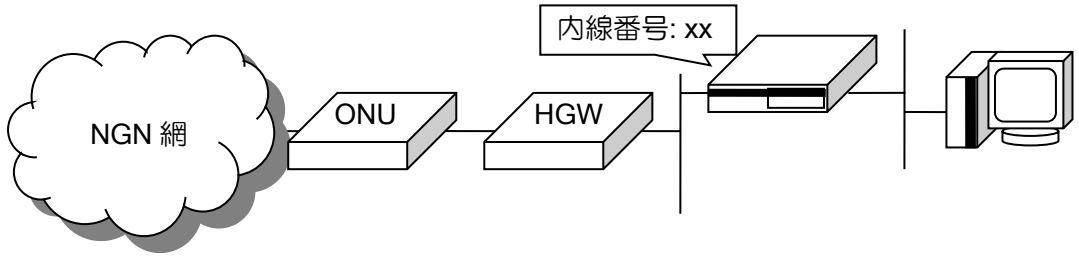
```
ip route default ③回線収容装置アドレス

ngn domain ntt-east.ne.jp （西網は ntt-west.ne.jp）
ngn subscriber 契約電話番号
ngn server ⑤SIP サーバアドレス

interface GigaEthernet0.0
  ngn ip enable
  ip address 割り当てアドレス領域範囲内のアドレス
  no shutdown
```

その他の設定はデータコネクト対応オンデマンド VPN 機能と同様です。

ナンバーゲート接続の場合、show ngn status で Service is statically configured を表示します。その他の項目は通常接続と同様です。

2.14.12 ホームゲートウェイ/オフィスゲートウェイ配下での接続

Ver8.7 以降では、ホームゲートウェイ（HGW）またはオフィスゲートウェイ（OGW）に IX ルータを配置した場合でも通信できるようになります。



基本的な設定はデータコネクト対応オンデマンド VPN の設定と同じですが、接続仕様が NGN 網に直接接続する場合と異なるため、以下の設定を投入するようにしてください。

【設定例】

ngn interface-type private

その他の設定はデータコネクト対応オンデマンド VPN 機能と同様です。

この接続では、show ngn status で Interface type is private を表示します。その他の項目は通常接続と同様です。

- 注意事項
  - HGW/OGW との基本的な接続確認は行っておりますが、全ての機種・バージョンとの接続を確認しているわけではありませんので、ご利用の際には動作確認を行ったうえでご利用ください。
  - 通信中に HGW/OGW で内線番号を変更しないでください。通信中の呼が正しく切断されないため、数分程度接続状態が残ります。
  - HGW/OGW は学習した MAC アドレスを自動的には消去しないので、MAC アドレステーブルが埋まっている場合は接続しても通信できません。不要な MAC アドレスを削除して運用してください。

2.14.13 最大接続数設定(Ver.9.6 以降)

ユーザごとに NGN の最大接続数を設定できます。
指定された接続数を超える場合接続を制限します。

ngn connect-group	NGN 最大接続数の設定
ngn binding-connect-group	NGN 最大接続数の割り当て設定

【設定例】

```
ngn connect-group ngn-group1 max-connections 5
ngn connect-group ngn-group2 max-connections 10

interface Tunnel1.0
   tunnel mode ipsec
   dialer string 81-111-1111
   ngn binding GigaEthernet0.0 ngn_profile ike-policy ike-policy
   ngn binding-connect-group ngn-group1
   ip unnumbered GigaEthernet1.0
   no shutdown
            :
interface Tunnel50.0
   dialer string 81-111-1150
   ngn binding GigaEthernet0.0 ngn_profile ike-policy ike-policy
   ngn binding-connect-group ngn-group1
   ip unnumbered GigaEthernet1.0
   no shutdown
            :
Interface Tunnel51.0
   tunnel mode ipsec
   dialer string 81-222-1111
   ngn binding GigaEthernet0.0 ngn_profile ike-policy ike-policy
   ngn binding-connect-group ngn-group2
   ip unnumbered GigaEthernet1.0
   no shutdown
            :
Interface Tunnel100.0
   tunnel mode ipsec
   dialer string 81-222-1150
   ngn binding GigaEthernet0.0 ngn_profile ike-policy ike-policy
   ngn binding-connect-group ngn-group2
   ip unnumbered GigaEthernet1.0
   no shutdown
```

上記の設定例では、グループ 1 のユーザは 5 接続が上限となり、グループ 2 のユーザは 10 接続が上限となります。

2.14.14 死活監視機能(Ver.9.6 以降)

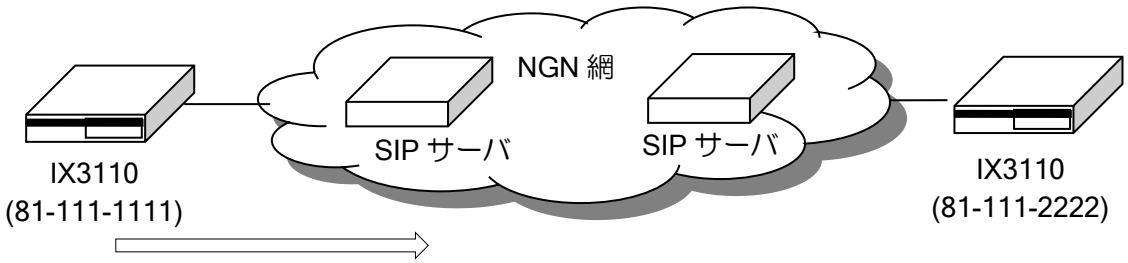
NGN 網のデータコネクト接続において、SIP サーバおよび接続先端末の死活監視を行うことができます。

本機能を使用することで SIP サーバの異常を検知し、経路切り替え等の対処が可能となります。
ネットワークモニタ機能に以下のイベントを設定することで、対象 SIP サーバにメッセージが送信され死活監視を開始することができます。ネットワークモニタ機能の説明は「ネットワークモニタの設定」の項を参照してください。
※SIP メッセージを利用しておりますが、この通信で利用料金が発生することはありません。

event ngn unreach-server	自 SIP サーバの死活監視設定
event ngn unreach-host	接続先端末の死活監視設定

【設定例】

```
network-monitor ngn-watch enable

watch-group ngn-watch
  event 1 ngn unreach-server 81-111-1111
```



死活監視の SIP メッセージの送信

上記の図では自 SIP サーバに死活監視 SIP メッセージを送信し、返答が返って来なければ SIP サーバの障害を検知します。
接続先 SIP サーバの死活監視を行う場合は以下のように設定します。

【設定例】

```
network-monitor ngn-watch enable

watch-group ngn-watch
  event 1 ngn unreach-host 81-111-2222
```

- 注意事項
  - NGN 死活監視機能では網の規定に従うため Network Monitor の各種設定が反映されません。(suppress restoration/suppress valiance コマンドのみ反映可)
  - 一部の HGW/OGW 配下では本機能を使用できない可能性があります。ご利用の際には動作確認を行った上でご利用ください。

■2.15 USB データ通信端末の設定

USB データ通信端末を接続することにより、「LTE」や「3G」回線を利用した無線接続ができます。

本機能は Ver8.8 以降の USB ポート付きの IX シリーズにて利用可能です。

※ IX2207 Ver9.1 以降では、USB0（USB-Serial0.0）および、USB1（USB-Serial1.0）の両方で USB データ通信端末が利用可能です。（Ver9.0 では、USB データ通信端末は USB0（USB-Serial0.0）でのみ利用可能）

2.15.1 対応するデータ通信端末

データ通信端末	対応キャリア名	対応バージョン
UX302NC-R	SIM フリー端末 (NTT ドコモ) NTT コミュニケーションズ	Ver10.1～
604HW	ソフトバンク	Ver9.7.54～ (※9)
FS040U	SIM フリー端末 (NTT ドコモ、ソフトバンク、KDDI(au))	Ver9.7～ (※8)
Speed USB STICK U03 （以下 U03 と記載）	KDDI(au)	Ver9.7～ (※3) (※5) (※7)
FS020U	SIM フリー端末 (NTT ドコモ)	Ver9.5～
Speed USB STICK U01 （以下 U01 と記載）	KDDI(au)	Ver9.2.54～ (※3) (※5) (※6)
403ZT	ソフトバンク	Ver9.2.54～ (※2)
L-03F	NTT ドコモ	Ver9.0.54～ (※2)
USB STICK LTE HWD12 （以下 HWD12 と記載）	KDDI(au)	Ver9.0～ (※3)(※4)
203HW	ソフトバンク	Ver9.0～ (※2)
UX302NC	NTT コミュニケーションズ	Ver9.0～
004Z	ソフトバンク	Ver8.10～
GL03D	イー・モバイル（サービス終了）	Ver8.10～
L-03D	NTT ドコモ	Ver8.9～
WM320	NTT コミュニケーションズ	Ver8.9～ (※1)
MF121	NTT コミュニケーションズ	Ver8.8.52～
MF636-BKIC	日本通信	Ver8.8.52～
L-05A	NTT ドコモ	Ver8.8～
L-08C	NTT ドコモ	Ver8.8～

※ サポート機器以外の接続はしないでください。（外付け USB-HUB 等）

※ 未サポートのデバイスを接続している状態でのルータ動作の正常性は保証できません。

※ 未サポートのデバイスを挿入後抜去した後においてもその後のルータ動作の正常性は保証できません。

※ 複数ポートで USB データ通信端末を同時に利用する場合、同一キャリア同一バンドを利用する端末では、電波干渉による通信劣化が発生する可能性があります。

※ モデムモードによる接続に対応しています。NDIS モードでの利用はできません。

※ IPv6 による接続はできません。

※1 WM320 は、1.3.0 以上のファームウェアバージョンのデータ通信端末で利用してください。（WM320 接続状態で show hardware を実行することによりファームウェアバージョンの確認ができます。）

※2 TCP MSS 調整を行っても網内で変更されてしまう可能性があります。

※3 U03、U01、HWD12 を利用するためには、KDDI 株式会社提供の専用ツールで動作モードをモデムモードに変更する必要があります。詳しくは、以下のサイトからお問い合わせください。
KDDI 株式会社 サポート・障害情報
https://biz.kddi.com/support/

※4 HWD12 に関する制限事項・注意事項
- (※3)のツールで動作モードを変更した初回の接続が失敗することがあります。一度リセットが掛かることで以降正常に接続できることを確認しています。
- データ通信端末ファームウェアをアップデートした後、3G 回線に接続不能になることがあります。(※3)のツールで動作モードを変更し、Windows アプリで一旦 3G に接続することで、接続可能になることを確認しています。
- 電波状態により、回線切断時に切断完了に時間がかかり、回線切断失敗の異常検出と判断される場合があります。（正常な切断検知よりも回線切断失敗検知による復旧のほうが早いため）
- 製造番号の読み出し結果が、データ通信端末の状態（LTE／CDMA 1X の在圏状態など）により異なります。
- CDMA 1X（3G）の場合、APN 設定が空の CID を指定した場合でも回線接続できることがありますが、必ず APN 設定が行われている CID で接続してください。

※5 U03、U01 に関する制限事項・注意事項
- PIN 認証は未サポートです。
- 3G での回線接続はできません。
- WiMAX2+を無効にすること（LTE 固定での利用）はできません。

※6 U01 に関する制限事項・注意事項
- 端末が圏外状態で回線接続された場合に、U01 の端末 LED の状態と実際の状態が不一致となることがあることを確認しています。
- CID 1 の端末設定保存はできません。
- Ver9.2.54 で、U01 のファームウェアバージョンを 11.211.13.30.824 に上げた場合、常に電波レベルが 1 で表示される問題、および回線切断後の再接続に非常に時間がかかる問題が確認されています。(Ver9.3 以降にバージョンアップしてください)
- Ver9.4 以前のバージョンで、U01 の新ファームウェアバージョン 11.211.13.43.824、11.211.13.44.824 に上げた場合、電波レベルが 1 で表示されるなどの問題を確認しています。(Ver9.5 以降にバージョンアップしてください)

※7 U03 に関する制限事項・注意事項

- 回線接続していない状態での、電波強度および電波レベルは確認できません。（電波環境が悪いなど回線接続できない場合での情報取得はできません。）
- CID 1 の端末設定保存はできません。グローバル IP の APN（au.au-net.ne.jp）で接続する場合や、任意の APN で接続する場合は、CID 2～10 を使用してください。
- CID 1 のデフォルト APN（kwx2.au-net.ne.jp）で接続する場合は、PPP の ID/PASSWORD として任意の値を設定しておく必要があります。（設定例は以下に記載）

```
【設定例】
 !
 ppp profile u03-cid1
    authentication myname au
    authentication password au au
    lcp acfc
 !
 interface USB-Serial0.0
    encapsulation ppp
    auto-connect
    ppp binding u03-cid1
    ip address ipcp
    ip napt enable
    mobile number *99***1#
    no shutdown
 !
```

※8 FS040U に関する制限事項・注意事項

- FS040U を利用するためには、富士ソフト株式会社提供の専用ツールで動作モードをモデムモードに変更する必要があります。詳しくは、以下のサイトよりお問い合わせください。
  http://www.fsi.co.jp/mobile/plusF/index.html

※9 604HW に関する制限事項・注意事項

- 604HW を利用するためには、ソフトバンク株式会社提供の専用ツールで動作モードの変更が必要です。詳しくは、ソフトバンク株式会社ユーザーサポートページを参照してください。
- PIN 認証は未サポートです。
- CID は、1 のみ利用可能です。

- （参考）動作確認端末ファームウェアバージョン（評価時に使用した端末のバージョン）

データ通信端末	IX バージョン	データ通信端末ファームウェアバージョン
UX302NC-R	Ver10.1～	v2.0.1
604HW	Ver9.7.54～	12.450.09.33.1420
FS040U	Ver9.7～	LWDJC02.1.0_M132
U03	Ver9.7～	alpha3.14
FS020U	Ver9.5～	LQTJC05.1.6_M012
U01	Ver9.5～	11.211.13.44.824
	Ver9.3～Ver9.4	11.211.13.30.824
	Ver9.2.54	11.211.13.25.824
403ZT	ALL	1.0.1
L-03F	ALL	L03F-MDM9625-V10b-MAY-09-2014-DCM-JP
HWD12	ALL	12.234.01.07.824
203HW	ALL	21.260.03.37.643
UX302NC	Ver9.2～	v1.0.7
	～Ver9.1	v1.0.3
004Z	Ver9.0～	BD_SBMMF682V1.0.0B27
	～Ver8.11	BD_SBMMF682V1.0.0B26
GL03D	ALL	11.433.31.00.168
L-03D	ALL	L03D-MDM9200-V10b-FEB-21-2012-DCM-JP
WM320	Ver9.0～	LQBJC02.1.5_MI34
	～Ver8.11	LQBJC02.1.3_MI34
MF121	ALL	BD_NTTMF121V1.0.0B02
MF636-BKIC	ALL	BD_JCINTP673M2V1.0.0B01
L-05A	ALL	L05A-01-VT0a-440-10
L-08C	ALL	Ver 10a

※ データ通信端末のファームウェアバージョンは、show hardware で確認できます。

2.15.2 USB データ通信端末の基本設定

```
【設定例】
 ip route default USB-Serial0.0
 ip ufs-cache enable
 !
 ppp profile usbwan
    lcp echo-interval 10
    lcp acfc
 !
 device USB0
    no shutdown
 !
 device USB1
    shutdown
 !
 interface USB-Serial0.0
    encapsulation ppp
    auto-connect
    ppp binding usbwan
    ip address ipcp
    ip napt enable
    mobile cid 1 pdp ip apn test.net
    mobile number *99***1#
    no shutdown
```

2.15.2.1 USB デバイスの設定

USB データ通信端末を利用するには、USB デバイスモード（device USB0、もしくは device USB1）で USB ポートを有効化します。

no shutdown shutdown	USB ポートの有効化 USB ポートの無効化（USB ポートの電源供給断）
reset	USB ポートのリセット
usb host-reset	USB ホストコントローラのリセット （※1） （グローバルコンフィグモード）

※ 他のデバイスモードと異なり、shutdown がデフォルトとなっています。
※ shutdown/no shutdown に関わらず show running-config にコンフィグが表示されます。
※ USB デバイスモードで shutdown にすることによって、USB ポートへの電源供給を停止することができます。（interface USB-Serial0.0 で shutdown しても電源供給は停止されません。）

※1 IX2207 など複数 USB ポートのある装置では、USB メモリの挿入されているポートを含む、すべてのポートがリセットされますので注意してください。

2.15.2.2 PPP プロファイルの設定

データ通信端末回線のデータ通信は PPP によって接続されています。PPP プロファイルで何も設定する内容が無い場合でも、最低限 PPP プロファイルを作成し、USB インタフェースにバインドする必要があります。

ppp profile	PPP プロファイルの作成 PPP プロファイルモードに遷移します。
authentication myname	ユーザ名の設定 ※プロバイダから指定のない場合は設定不要です。
authentication password	パスワードの設定 ※プロバイダから指定のない場合は設定不要です。
lcp acfc	Address-and-Control-Field-Compression の有効設定 ※L-05A、L-08C、MF121、MF636-BKIC 以外のデータ通信端末では設定してください。

2.15.2.3 USB インタフェースの設定

USB データ通信端末のインタフェース設定は interface USB-Serial*.0 で行います。アクセスポイントの設定と PPP プロファイルのバインドを行うことにより通信ができるようになります。

interface USB-Serial*.0	インタフェースコンフィグモードに遷移します。

※ デバイス名 USB0 の USB ポートに対応するインタフェース名は USB-Serial0.0 となります。

mobile cid CID pdp PDP-TYPE apn APN-NAME	アクセスポイントの設定 ※プロバイダなどから指定されたアクセスポイントと接続タイプを設定します。 ※CID 番号は任意ですが、プロバイダなどから指定されている場合はその番号で設定します。 ※L-05A、L-08C、MF121、MF636-BKIC 以外のデータ通信端末の PDP-TYPE は ip で設定してください。（端末によっては、利用しない CID に対して誤った PDP-TYPE を設定した場合においても接続できなくなる場合があります。） ※203HW は、CID 10 での回線接続はできません。 ※403ZT は、CID 9 での回線接続はできません。 ※403ZT は、CID 1 の端末設定保存はできません。 ※403ZT は、CID 1 で回線接続ができないことがあります。 ※U03、U01 は、CID 1 の端末設定保存はできません。CID 1 をデフォルト値の APN で利用する場合は、この設定をせずに利用してください。 ※604HW は、CID 1 のみ利用可能です。

mobile number NUMBER	電話番号の設定 ※プロバイダなどから指定された電話番号を設定します。 ※端末の自局ダイヤル番号（回線番号）とは異なります。 例) *99***<CID># <CID>は、mobile cid CID で設定した番号
ppp binding	PPP プロファイルをバインドします。
auto-connect	通信がない状態でも自動的に接続します。 常時接続する場合に設定します。
mobile cid-clean	アクセスポイントの設定（CID 1 から CID 10 まで）を工場出荷状態に初期化します。 ※ データ通信端末への設定変更となりますので、show running-config には反映されません。 ※004Z、GL03D、UX302NC、UX302NC-R、HWD12、U01、U03 は、CID 2 から CID 10 までを初期化します。 ※403ZT は、CID 2～8、および CID 10 を初期化します。 ※604HW では、CID 1 のみ初期化します。
mobile mode 3g-only	特定の LTE 対応端末で、接続方式を 3G に制限します。LTE 電波の弱い環境で接続が安定する可能性があります。（Ver9.2 以降） ※UX302NC、UX302NC-R、L-03F、203HW、GL03D、FS020U、FS040U で対応 ※本コマンドは設定後に、端末リセット、もしくは再挿入が必要です。 ※弱電波環境での接続安定性を保証するコマンドではありません。 ※WM320 では、3G-only 設定はしていますが接続実績はありません。
mobile mode lte-only	特定の LTE 対応端末で、接続方式を LTE に制限します。3G で接続できない環境で使用してください。（Ver10.7 以降） ※UX302NC-R、FS040U で対応 ※本コマンドは設定後に、端末リセット、もしくは再挿入が必要です。
mobile mode hsplus	U03、U01 で、「ハイスピードプラスエリアモード」を使用します。WiMAX2+に加え、LTE での通信が可能となります。 ※「ハイスピードプラスエリアモード」を選択すると、追加でオプション料が発生しますので、データ通信端末の利用規定を参照してください。

2.15.2.4 バックアップ用途のための追加設定

データ通信端末をバックアップ回線として利用する場合、回線契約（従量課金）や運用形態に応じて設定します。

idle-time	設定された時間、無通信状態が続いた場合に接続を切断します。 （インタフェースコンフィグモード）
forced-disconnect-time	一回の接続時間が設定値を超えた場合に強制的に切断します。 （インタフェースコンフィグモード）
no echo	PPP ECHO による疎通確認を行わなくなります。従量課金接続で PPP ECHO パケットによる課金を抑える場合に指定します。 （PPP プロファイルモード） ※データ通信端末の受信異常検知によるリカバリができなくなりますので、idle-time、forced-disconnect-time などと併用することをお勧めします。 （異常検出・リカバリ機能 受信異常検出を参照してください）

※ バックアップ回線として利用する場合でも、データ通信端末を常時接続で運用する場合（auto-connect）は、上記設定は特に必要はありません。（定額契約等であっても、no auto-connect で運用する場合には、必要に応じて上記設定を行います。）

※ データ通信が発生してから、回線接続完了するまでにはかなりの時間を要する場合がありますので、常時接続以外ではパケット廃棄等の影響を考慮した運用を行う必要があります。

※ データ通信端末が接続時に取得できる DNS アドレスを利用する場合、回線切断中は利用できませんので、固定設定等で対応する必要があります。

2.15.3 回線接続中の電波レベル

下記のデータ通信端末では、回線接続中の電波レベルが取得できます。（Ver9.0 以降）

- L-03F
- GL03D
- L-03D
- WM320
- FS020U
- FS040U
- U03
- 604HW
- UX302NC（Ver10.1 以降）
- UX302NC-R

※ U03 は回線接続中のみ電波レベルが取得できます。

2.15.4 LED

データ通信端末の状態に応じて、LED が点灯します。

- 低速点滅：1 秒間隔で点灯・点滅
- 高速点滅：0.25 秒間隔で点灯・点滅

状態	説明		点灯パターン
未使用	データ通信端末を取り付けていない時、または設定で USB ポートを無効化している時を示します。		3 （消灯） 2 （消灯） 1 （消灯）
利用不可	データ通信端末が、初期化中、コンフィグ不備、ネットワーク未登録、圏外の場合を示します。		3 （消灯） 2 （消灯） 1 （低速点滅）
PIN 認証失敗	PIN 認証に失敗していることを示します。		3 （高速点滅） 2 （高速点滅） 1 （高速点滅）
回線接続待ち	データ通信端末を正常に認識しており、回線接続可能な状態であることを示します。 点灯している LED の数により電波レベルを確認することができます。	微弱（レベル 1）	3 （消灯） 2 （消灯） 1 （点灯）
		弱（レベル 2）	3 （消灯） 2 （点灯） 1 （点灯）
		強（レベル 3）	3 （点灯） 2 （点灯） 1 （点灯）
回線接続中	回線接続中です。 回線接続中の電波レベル取得未対応のデータ通信端末では、点灯している LED は、回線を接続する直前の電波レベルを表示しています。（※1）	微弱（レベル 1）	3 （消灯） 2 （消灯） 1 （高速点滅）
		弱（レベル 2）	3 （消灯） 2 （高速点滅） 1 （点灯）
		強（レベル 3）	3 （高速点滅） 2 （点灯） 1 （点灯）

※ 電波レベルと回線接続安定度は必ずしも一致するものではありません。
※1 回線接続中の電波レベルの取得をサポートしている端末では、回線接続後の電波レベルの更新に応じて LED も更新されます。

2.15.5 デバイス状況の表示

show devices USB0	電波レベルの表示やデータ通信端末情報、エラーカウントを表示します。

【表示例】

```
Router(config) # show devices USB0
Device USB0 is up
  ifIndex is 7
  USB status:
    Port status is up
    PIN code security is deactivated
    Signal bar is 3
    Carrier is XXXXXXXXX
    Dialer string is "XXXXXXXXXXX",129
    Dial status is connected
    Statistics:
      0 input frames
      0 output frames, 0 output requests
      Rx errors:
        0 cancel errors, 0 unknown frames, 0 oversize frames
        0 other errors, 0 stuffing errors, 0 reassemble errors
        0 disassemble discards
      Tx errors:
        0 cancel errors, 0 other errors
        0 overflow errors, 0 stuffing errors
      Wireless adaptor reset cause:
        0 transmit timeouts
        0 modem timeouts, 0 startup timeouts
        0 terminate timeouts, 0 coverage timeouts
        0 connecting errors
      Device reset cause:
        0 mount timeouts
      Host controller reset cause:
        0 reset failures
        0 HUB power on failures, 0 HUB power off failures
        0 HUB health check failures
```

Device USB0	up： down：	デバイスモードが no shutdown デバイスモードが shutdown
Port status	up： down：	データ通信端末が挿入済でデバイスモードが no shutdown それ以外の状態
PIN code security	activated： deactivated： unsupported：	PIN 認証が有効 PIN 認証が無効 PIN 認証は未サポート

Security lock status	not authenticated： PIN コード入力待ち PIN locked： PIN ロック状態 PUK locked： 完全ロック状態 unsupported： PIN 認証は未サポート ※ show devices detail で表示されます。
Network registration GPRS network registration EPS network registration	not registered： 基地局に未登録 registered： 基地局に登録済 registering： 基地局に登録中 registration denied： 基地局での登録失敗 unknown： 基地局が未検出など registered(roaming)： 基地局に登録済（ローミングなどによる一時的な接続） illegal status： 異常状態 ※ show devices detail で表示されます。 ※ EPS network registration は Ver8.9.17A 以降で表示されます。 ※ 基地局に登録済（registered）にならないまま、30 秒以上経過した場合、要求に従い回線接続（ATD）を行います。このとき、回線接続が成功すると、登録状態は回線接続前の状態が表示され、登録済（registered）以外が表示されることがあります。 ※ 604HW、HWD12、L-03F では、Network registration のみの表示となります。
Signal bar	3： 電波レベル 3（強） 2： 電波レベル 2（弱） 1： 電波レベル 1（微弱） 0： 電波レベル 0（圏外） ※ LED の電波レベル表示と同期しています。 ※ 電波強度が 0 でなく、かつ、基地局に登録済がいずれか 1 つでもある場合に、1～3 で表示されます。
Signal strength	3： 電波強度 3（強） 2： 電波強度 2（弱） 1： 電波強度 1（微弱） 0： 電波強度 0（圏外） unknown： 不明 ※ 基地局の登録状態を加味しない、電波強度を表示します。 ※ 括弧内に電波強度を取得する AT コマンドの応答がそのまま表示されます。（データ通信端末により使用されている AT コマンドは異なりますので参考表示となります。） ※ show devices detail で表示されます。 ※ Ver8.9.17A 以降で表示されます。

Radio interface	接続回線種別 NO SERVICE CDMA 1X CDMA 1XEVDO AMPS GSM UMTS LTE ※ L-03F、L-03D、GL03D、WM320、FS020U、FS040U のみ表示されます。 ※ show devices detail で表示されます。 ※ Ver9.0 以降で表示されます。
Carrier	接続先の通信事業者名 ※ 604HW では表示されません。
Dialer string	自局ダイヤル番号（回線番号） ※ 604HW では表示されません。(ICCID が表示されます。)
Dial status	disconnected： 未接続 connecting： 接続手続き中 cancelling： 接続中断中 connected： 通信中 post processing： 切断処理中 illegal status： 異常状態
Connection database	データ通信端末に設定されているアクセスポイント情報 ※ show devices detail で表示されます。

2.15.6 統計情報の表示

6 章 統計情報を参照してください。

2.15.7 電波レベル・回線接続履歴表示

データ通信端末の電波レベルの変化や、回線接続・切断履歴を表示します。（Ver9.0 以降）

- 回線接続中の電波レベルの変化時や、接続回線種別の変化時（回線接続中の電波レベル対応端末のみ）
- 回線接続待ち時の電波レベルの変化時
- ポートアップ／ポートダウンの検出時
- 回線の接続完了／切断完了イベントの検出時

show mobile history [DEVICE]	電波レベル・回線接続履歴の表示 （オペレーションモード） （グローバルコンフィグモード） （インタフェースコンフィグモード）
clear mobile history [DEVICE]	電波レベル・回線接続履歴のクリア （グローバルコンフィグモード） （インタフェースコンフィグモード）

【表示例】

```
Router(config)# show mobile history
Mobile history

Device USB0 - 12 recorded
  2015/08/21 16:56:51, Detect port down, L-03D
  2015/08/21 12:37:05, Disconnected
  2015/08/21 12:37:00, Signal bar 3(strength 3, rssi -67 dBm), LTE
  2015/08/21 12:00:30, Signal bar 3(strength 3, rssi -67 dBm), UMTS
  2015/08/21 11:10:20, Connected
  2015/08/21 11:07:00, Signal bar 3(strength 3, rssi -67 dBm)
  2015/08/21 11:06:51, Detect port up, L-03D
  2015/08/20 16:56:51, Detect port down, MF121
  2015/08/20 11:07:00, Signal bar 3(strength 3, (+CSQ: 13, 99))
  2015/08/20 11:06:51, Detect port up, MF121
  2015/08/20 10:08:35, Detect port down, L-08C
  2015/08/20 10:08:30, Signal bar 3(strength 3, (*DANTE: 3))
  2015/08/20 10:07:15, Signal bar 0(strength 3, (*DANTE: 3))
  2015/08/20 10:07:00, Signal bar 3(strength 3, (*DANTE: 3))
  2015/08/20 10:06:51, Detect port up, L-08C
```

※ データ通信端末により、表示される情報は異なります。

2.15.8 活線挿抜（ホットプラグ）

装置が稼働している状態でのデータ通信端末の挿入および抜去が可能です。
必要なコンフィグがすべて投入されている場合には、挿入後自動的にデータ通信端末の利用が可能となります。

※ 不測のトラブルを避けるため、通信中の抜去はなるべく行わないでください。

- 安全な取り外し方法

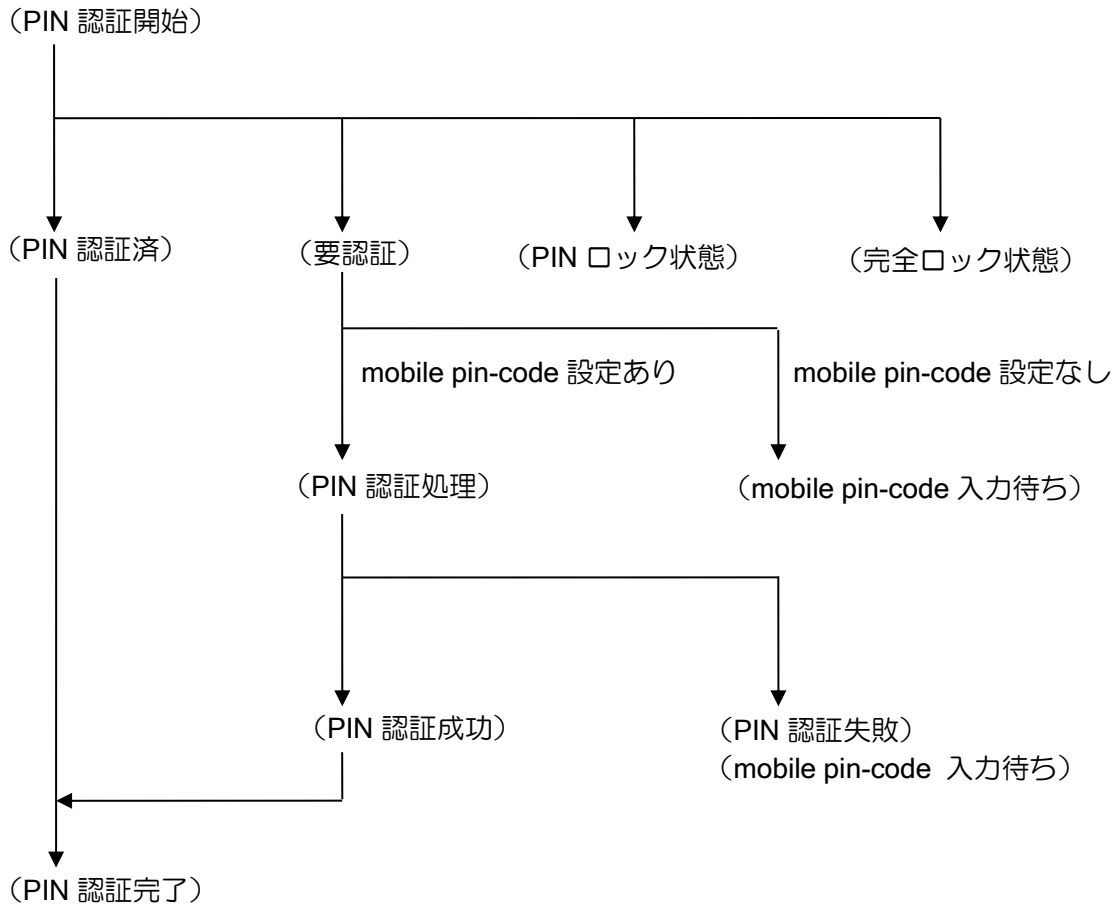
USB デバイスモードを一旦 shutdown にすることによって、安全な取り外しが可能です。

2.15.9 PIN 認証

データ通信端末の不正利用を防止するための PIN コードによる認証設定ができます。

mobile pin-code	PIN コードの認証設定 （インタフェースコンフィグモード）
mobile pin-auth	データ通信端末に PIN 認証の有効・無効を設定する。 （インタフェースコンフィグモード） ※ 回線接続中は設定変更できません。インタフェースを shutdown して設定します。 ※ データ通信端末への設定変更となりますので、show running-config には反映されません。 ※ L-05A/L-08C/L-03D/L-03F 以外のデータ通信端末の場合、PIN 認証後にのみ使用できます。（データ通信端末の挿入等による初期化時、または回線接続中は使用できません）
mobile puk	データ通信端末の PIN ロック状態を解除し、新しい PIN コードに設定します。 （インタフェースコンフィグモード） ※ データ通信端末への設定変更となりますので、show running-config には反映されません。

PIN 認証設定を行ったデータ通信端末を挿入時に、mobile pin-code で設定した PIN コードで認証します。
データ通信端末への PIN 認証設定は、mobile pin-auth、mobile puk コマンドによって設定します。



PIN 認証の設定不備などで接続できない場合、イベントログで現在の状態を確認することができます。

イベントログ MODM.037: Security lock status is XXXXXX	
SIM PIN	要認証状態となっています。（mobile pin-code 入力待ち） mobile pin-code コマンドで正しい PIN コードの設定を行います。 （PIN コード誤りで 3 回認証に失敗すると、PIN ロック状態になります。）
SIM PUK	PIN ロック状態となっています。 mobile pin-code で正しい PIN コードを設定した上で、mobile puk コマンドで PIN ロックを解除します。 （PUK コードを 10 回間違えると完全ロック状態になります。）
ERROR	完全ロック状態となっています。 L-05A、L-08C 等では、このログは表示されずに、一定時間内に起動処理が終了しない場合のリカバリ処理（1.1.9.4 データ通信端末 起動失敗検出）により USB ホストコントローラのリセットが繰り返されます。 完全ロック状態を解除するには、データ通信端末を購入した販売店にお問い合わせください。

2.15.10 QoS 設定時の注意事項

2.15.10.1 回線速度

データ通信端末の QoS や MIB 情報、回線使用率で使用する回線速度は、デフォルトでは受信の最大速度に基づいて計算されます。3G 回線では受信と送信で回線速度が大きく異なり、実際の回線速度は設置場所などで異なりますので、QoS を使用する場合、必要に応じて設定する必要があります。

データ通信端末	デフォルト回線速度	
604HW U03 U01 403ZT 203HW	110Mbps	※3G 回線や、高速回線接続時は接続環境の最大速度に合わせて設定してください。
FS040U FS020U L-03F UX302NC UX302NC-R HWD12	75Mbps	
004Z GL03D	42Mbps	※デフォルトでは、サポートされている 3G 回線の最大速度で設定されています。 ※LTE 回線などで接続される環境下では、実際の最大回線速度に合わせて設定してください。
L-03D WM320	14.4Mbps	
L-05A L-08C MF121 MF636-BKIC	7.2Mbps	

bandwidth	インタフェースの帯域幅情報を変更します。 （インタフェースコンフィグモード）
bandwidth percent	最小予約帯域割合の設定 （ポリシーマップクラスコンフィグモード）
priority percent	絶対優先クラスの設定 （ポリシーマップクラスコンフィグモード）

2.15.10.2 フレームサイズ

QoS の帯域計算で使用されるフレームサイズは、IP パケットサイズ+PPP ヘッダ（4byte）+FCS（2byte）+フラグ（2byte）となります。

ただし、lcp pfc、lcp acfc を指定時には、PPP ヘッダが 1byte となります。

2.15.10.3 無線回線における QoS 設定の注意事項

データ通信端末の回線では、有線によるインターネット回線や専用線接続と比べて一定の速度や遅延特性を確保することが難しくなる傾向がありますので、QoS を設定する際には以下のような点に注意する必要があります。

- 理論的回線速度と実際の速度が異なります。
  - データ通信サービスの速度表記は、規格上の理論最大速度であり、実際にその速度で利用できるわけではありません。
- 遅延が大きくなります。
  - 無線回線での遅延は、有線回線に比べて大きくなる傾向があります。3G 回線では 64 バイトの ping でも応答に 1 秒以上かかる場合もあります。
- 遅延や速度が常に一定となりません。
  - あらかじめ帯域や遅延を測定サイト等で測定したとしても、常に同等の帯域や遅延で通信できるわけではありません。
- TOS 値による制御はできません。
  - TOS 値をつけて送信しても網側で値がクリアされることがあります。

2.15.11 MIB

2.15.11.1 MIB-2（RFC1213）

USB に関する MIB は、interface USB-Serial0.0 もしくは interface USB-Serial1.0 に関する MIB-2（RFC1213）の interface Group のみのサポートとなります。

2.15.11.2 プライベート MIB（Ver9.2 以降）

Ver9.2 以降では、回線接続状況取得などのプライベート MIB に対応しています。
内容は付録の「プライベート MIB 詳細」の項を参照してください。

+- pico-mib	(.1.3.6.1.4.1.119.2.3.84)
+- picoMobileMIB	(.1.3.6.1.4.1.119.2.3.84.11)
+- picoMobileMIBObjects	(.1.3.6.1.4.1.119.2.3.84.11.1)
+- picoMobileDeviceTable	(.1.3.6.1.4.1.119.2.3.84.11.1.1)
+- picoMobileDeviceEntry	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1)
+- picoMobileDeviceIndex	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.1)
+- picoMobileDeviceVendorName	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.2)
+- picoMobileDeviceName	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.3)
+- picoMobileDeviceProductID	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.4)
+- picoMobileDeviceSoftwareVersion	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.5)
+- picoMobileDeviceSignalBar	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.6)
+- picoMobileDeviceSignalStrength	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.7)
+- picoMobileDeviceSignalQuality	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.8)
+- picoMobileDeviceSignalElapsedTime	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.9)
+- picoMobileDeviceRadioInterface	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.10)
+- picoMobileDeviceCarrier	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.11)
+- picoMobileDeviceDialerString	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.12)
+- picoMobileDeviceDialStatus	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.13)
+- picoMobileDeviceInRangeCounts	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.14)
+- picoMobileDeviceOutRangeCounts	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.15)
+- picoMobileDeviceResetCounts	(.1.3.6.1.4.1.119.2.3.84.11.1.1.1.16)

2.15.11.3 トラップ（Ver9.3 以降）

Ver9.3 以降では、ポートアップトラップ、ポートダウントラップ、電波状態トラップに対応しています。

+- pico-mib	(.1.3.6.1.4.1.119.2.3.84)
+- picoMobileMIB	(.1.3.6.1.4.1.119.2.3.84.11)
+- picoMobileMIBNotificationPrefix	(.1.3.6.1.4.1.119.2.3.84.11.2)
+- picoMobileMIBNotifications	(.1.3.6.1.4.1.119.2.3.84.11.2.0)
+- picoMobileDeviceDown	(.1.3.6.1.4.1.119.2.3.84.11.2.0.1)
+- picoMobileDeviceUp	(.1.3.6.1.4.1.119.2.3.84.11.2.0.2)
+- picoMobileSignalStatusChange	(.1.3.6.1.4.1.119.2.3.84.11.2.0.3)

2.15.12 異常検出・リカバリ機能

正しく設定がされているにもかかわらず、回線やデータ通信端末の状態によっては接続ができなかったり、通信途中で切断されたり、データ通信端末自体がフリーズする場合があります。IX シリーズでは、以下のような各種異常検出時に USB ポートのリセット等を行うことにより、リカバリを試みます。

2.15.12.1 未接続検出

データ通信端末を有効設定（device USB0 が no shutdown、かつ interface USB-Serial0.0 が no shutdown など）の状態で、一定時間デバイスの挿入が検出できない場合、USB ポートにデータ通信端末が挿入されているにも関わらず認識に失敗している可能性があるとみなして USB ポートをリセットします。

タイムアウト時間: 3 分

リカバリ回数と検出時イベントログ

```
【統計表示例】
  Router(config) # show devices USB0
          :
  Device reset cause:
     0 mount timeouts

【イベントログ表示例】
  USB.009: USB Device not found on USB0
```

※ 対象デバイスに USB メモリが挿入されている場合は、リカバリ処理は行われません。

2.15.12.2 送信異常検出

データ通信端末が接続されているにもかかわらず、データ送信要求が一定時間完了しなかった場合、データ通信端末に何らかの異常が発生している可能性があるとみなして USB ポートをリセットします。

タイムアウト時間: 30 秒

リカバリ回数と検出時イベントログ

```
【統計表示例】
  Router(config) # show devices USB0
          :
  Wireless adaptor reset cause:
     0 transmit timeouts

【イベントログ表示例】
  USB:003: Timeout error occurred during transmission device on USB0; 31 seconds has
passed
```

※ Ver8.9 以降 LTE 回線対応として 30 秒に変更。（Ver8.8 でのタイムアウト時間は 10 秒）

※ LTE サポートエリア境界付近など、回線接続状態の悪い環境においては、回線が切断されないままパケットが長時間送信されず送信異常検出となることがあります。データ通信端末の故障でないにもかかわらず、このタイムアウトが頻発する場合は、障害切り分け時に回線状態の確認も合わせて行う必要があります。

2.15.12.3 AT コマンドタイムアウト

データ通信端末に対して AT コマンドを発行した際、一定時間応答を受信できない場合、データ通信端末の状態に何らかの異常が発生している可能性があるとみなして USB ポートをリセットします。

タイムアウト時間: 1 分

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0
          :
 Wireless adaptor reset cause:
    0 modem timeouts

【イベントログ表示例】
 MODM:011: Timeout occurred during sending modem command on USB0
```

2.15.12.4 回線接続失敗

データ通信端末に対して回線接続 AT コマンド（ATD）を発行した際、ERROR 応答が複数回連続で返ってきた場合や回線接続後にすぐに切断された場合、データ通信端末もしくは回線の状態に何らかの異常が発生している可能性があるとみなして USB ポートをリセットします。

条件: 以下の条件が 10 回連続で発生した場合

- 回線接続完了前に切断された場合
- 回線接続完了後に 30 秒以内に切断された場合（Ver8.11 以降）

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0
          :
 Wireless adaptor reset cause:
    0 connecting errors

【イベントログ表示例】
 MODM:014: Connecting failure detected 10 times on USB0
```

※ LTE サポートエリア境界付近など、回線接続状態の悪い環境において、本状況が発生することがあります。設定間違いや、データ通信端末の故障でないにもかかわらず、このリセットが頻発する場合は、障害切り分け時に回線状態の確認も合わせて行う必要があります。

※ mobile number を間違えて設定している場合にも、このリセットが発生します。mobile number を確認してください。

2.15.12.5 データ通信端末 起動失敗検出

データ通信端末の挿入検出後、一定時間以内に使用する準備が完了しなかった場合、データ通信端末との接続に何らかの異常が発生している可能性があるとみなして USB ポートをリセットします。

タイムアウト時間: 3 分

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0
          :
 Wireless adaptor reset cause:
    0 startup timeouts

【イベントログ表示例】
 MODM:010: Timeout occurred during initialization device on USB0
```

2.15.12.6 回線切断失敗

回線切断処理が一定時間受信できない場合に、データ通信端末との接続に何らかの異常が発生している可能性があるとみなして USB ポートをリセットします。

タイムアウト時間: 1 分

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0
          :
 Wireless adaptor reset cause:
    0 terminate timeouts

【イベントログ表示例】
 MODM:012: Timeout occurred during disconnecting connection on USB0
```

2.15.12.7 電波状態異常

一定時間電波状態が圏外であった場合、データ通信端末の状態に何らかの異常が発生している可能性があるとみなして USB ポートをリセットします。

タイムアウト時間: 30 分

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0
          :
 Wireless adaptor reset cause:
    0 coverage timeouts

【イベントログ表示例】
 MODM:013: Device is out of range for a long time on USB0
```

2.15.12.8 定期電波状態読み出し連続失敗

データ通信端末に対し、定期電波状態読み出しのメッセージを送信した後、一定時間応答を受信できないことが連続で発生した場合、データ通信端末に何らかの異常が発生している可能性があるとみなして USB ポートをリセットします。（Ver9.0.54 以降）

条件: 15 秒間無応答が連続 4 回発生

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0 detail
          :
 Wireless adaptor reset cause:
    0 signal information errors

【イベントログ表示例】
 MODM:040: Timeout occurred during sending QMI message on USB0
 MODM:051: Detected signal information error on USB0
```

2.15.12.9 USB ホストコントローラ異常

装置内の USB ホストコントローラで異常を検出した場合、全 USB ポートをリセットします。

条件: USB ホストコントローラで 5 秒以内のエラーが 10 回連続で発生した場合

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0
          :
 Host controller reset cause:
    0 reset failures

【イベントログ表示例】
 USB:011: Reset host controller. (Port Reset)
```

2.15.12.10 内蔵 USB ハブ異常検出

USB ポートを複数実装している装置で、内蔵 USB ハブで異常を検出した場合、全 USB ポートをリセットします。

内蔵 USB ハブに対するヘルスチェック失敗: 5 分
内蔵 USB ハブのポート電源 ON の失敗: 10 回
内蔵 USB ハブのポート電源 OFF の失敗: 1 回

リカバリ回数と検出時イベントログ

```
【統計表示例】
 Router(config) # show devices USB0
          :
 Host controller reset cause:
    0 HUB power on failures, 0 HUB power off failures
    0 HUB health check failures

【イベントログ表示例】
 USB:011: Reset host controller. (Built-in USB hub Port Power ON)
 USB:011: Reset host controller. (Built-in USB hub Port Power OFF)
 USB:011: Reset host controller. (Built-in USB hub health check)
```

2.15.12.11 受信異常検出

通信中に PPP ECHO の応答が一定回数得られない場合、何らかの異常が発生しているとみなして、PPP 回線を切断します。その後改めて接続を行います。（PPP の標準機能）

lcp echo-interval	PPP ECHO の間隔を調整します。 （デフォルト 30 秒） （PPP プロファイルモード）
lcp echo-retry	PPP ECHO のリトライ回数を調整します。 （デフォルト 5 回） （PPP プロファイルモード）

※ デフォルトの PPP ECHO 設定値では検出に時間がかかる可能性があるため、運用状況に応じて PPP プロファイルモードで、lcp echo-interval、lcp echo-retry を調整します。

※ データ通信端末では通常運用においても、パケットロスや大きな遅延が発生することがあるため、極端に間隔を短くしたり、リトライ回数を少なくしたりする運用はおすすめできません。

2.15.12.12 IP レイヤでの通信異常検出

ping による疎通確認など、IP レイヤでの疎通異常検出を行う場合は、network monitor の機能を併用します。

action SEQ reset-device USB0	network monitor イベント発生時に USB デバイスをリセットします。 （Watch Group コンフィグモード） （Ver8.11 以降）

※ network monitor による疎通確認では回線契約している総通信量に注意が必要です。

■2.16 IPv4 の設定

物理リンクレイヤと、IPv4 レイヤの関係は論理的に以下の構造をとっています。

IPv4 レイヤ
インタフェース（GigaEthernet0.0 etc.）
デバイス（GigaEthernet0 etc.）

2.16.1 IPv4 アドレスの設定

IPv4 アドレスを設定するコマンドは次のとおりです。アドレスを複数設定したい場合はセカンダリアドレスを使用します。セカンダリアドレスは ver9.7 以降では複数登録可能です（最大 15）。

ip address	IPv4 アドレスの登録

【設定例】

```
ip address 192.168.0.254/24
ip address 10.10.10.1/24 secondary
```

※設定変更時はインタフェースが一旦 down します。

セカンダリアドレスは使用可能な機能に制限があります。使用可能機能は以下のとおりです。

機能	プライマリ	セカンダリ
ping の宛先	○	○
telnet,ssh の宛先	○	○
ゲートウェイアドレスとしての使用 （他装置のネクストホップとして使用）	○	○
DHCP の払い出し （DHCP リレー機能は使用不可） （使用方法については DHCP の項を参照してください）	○	△
NAT/NAPT アドレスとして使用	○	○
SNMP	○	○
RIP/OSPF/BGP の使用	○	×
VRRP	○	△
IPsec	○	×

※VRRP でセカンダリアドレスを使用する場合、広告パケットの送信元アドレスがプライマリアドレスになりますが、利用は可能です。

複数のインタフェースに同じアドレスを使用したい場合は、VRF-Lite 機能を利用することができます。VRF-Lite の章を参照してください。

2.16.2 unnumbered アドレスの設定

PPPoE やトンネルなどで IP アドレスが不要な場合、unnumbered の設定が可能です。設定コマンドは次のとおりです。

ip unnumbered	IPv4 アドレスを unnumbered で登録

【設定例】

```
ip unnumbered GigaEthernet1.0
```

ip unnumbered はインタフェースを指定して利用してください。ICMP エラーなどでアドレスが必要になった場合に、指定したインタフェースのアドレスを優先して使用します。インタフェースを指定しない場合は、最も大きいアドレスが自動的に選択されます。

unnumbered で指定したインタフェースがダウンした場合、unnumbered を設定したインタフェースは IPv4 レイヤがダウンするため、IPv4 パケットの転送はできますが、IPv4 レイヤで動作する機能（OSPF、RIP 等）は動作が停止します。

2.16.3 MTU の変更

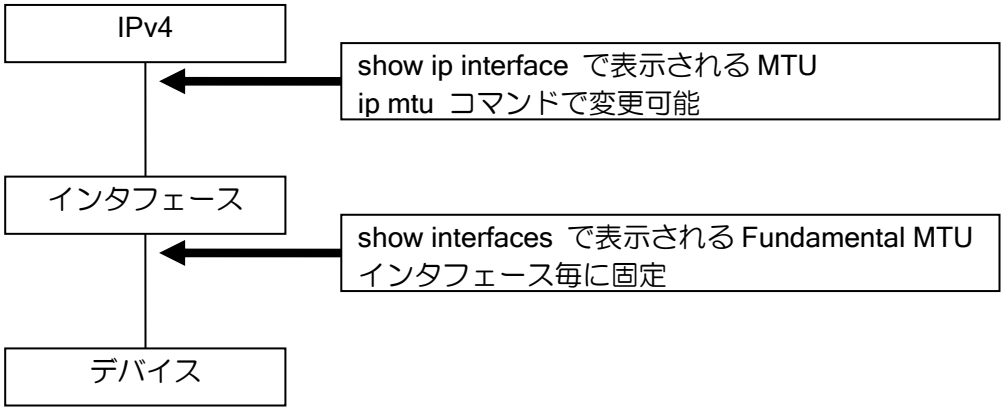
IPv4 で MTU 値をインタフェースの MTU より小さい値に変更するコマンドは次のとおりです。

ip mtu	MTU の変更 （インタフェースコンフィグモード）

【設定例】

```
ip mtu 1000
```

インタフェースの MTU と IPv4 の MTU の関係は次のようになります。



2.16.4 TCP MSS 調整

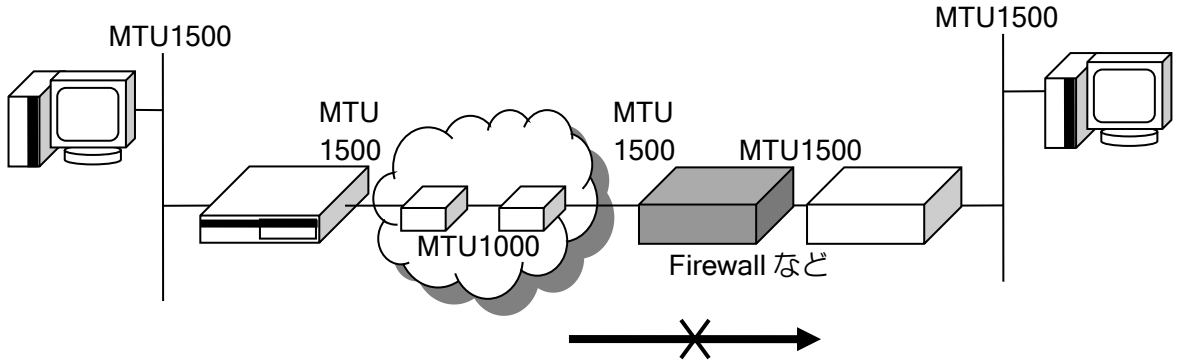
トンネルや PPPoE など MTU が 1500 でないインタフェースを利用する場合に、TCP のパケットサイズの上限をフラグメントされないサイズに制限し、性能低下を抑止する機能です。

TCP は接続を確立する際に syn パケットで MSS（Maximum Segment Size）情報を通知しますが、この値を強制的に書き換えることで実現します。

MSS = MTU － IP ヘッダ長 － TCP ヘッダ長（RFC879）です。

この機能は RFC2923 に記載されている Path MTU 探索の Black Hole 防止機能として利用することができます。下記のようなネットワークにおいて両端のホスト間で TCP の通信を行う場合、Path MTU 探索が有効でないと、ホストは MSS の値を 1460 と設定して接続を試みます。しかし MTU1000 の区間が経路の途中に存在するため、MSS が 960 以下でなければ通信はできません。このような場合に MSS の値を強制的に書き換えることで、TCP の通信を可能にします。ただし、パケットの MSS の値が設定値より小さい場合、書き換えは行いません。

PathMTU 探索ができないネットワーク例



TCP の MSS 値を変更するコマンドは次の通りです。ブリッジインタフェースでの MSS の調整機能は Ver.7.5 から使用可能です。

インタフェースコンフィグモード	
ip tcp adjust-mss	MSS の調整
bridge ip tcp adjust-mss	ブリッジインタフェースでの MSS の調整

【設定例】

```
interface GigaEthernet0.0
  ip tcp adjust-mss 960
```

設定は、トラフィックがトンネルインタフェースを通過する場合はトンネルインタフェースで行ってください。そうでない場合はトラフィックが通過する任意のインタフェースで設定してください。

"ip tcp adjust-mss auto"を設定すると、インタフェースの MTU に応じた値が自動的に設定されます(ルータインタフェースのみ。ブリッジインタフェース用コマンドでは未対応)。装置管理者が手動で MSS 調整値を計算する場合、以下の計算式を参考にしてください。(IPsec、トンネルモード、ESP のみ使用時。)

【計算式】

X = 出力インタフェース MTU - A - B - C - D
　A：認証データ　MD5/SHA1(12byte)
　　SHA256(16byte)
　　SHA384(24byte)
　　SHA512(32byte)
　B：IV(Initialization Vector)　DES/3DES(8byte)、AES(16byte)
　C：ESP ヘッダ(8byte)
　D：IP ヘッダ(20byte)

トンネルインタフェース MTU = (X / E の整数部) x E - F
　E：DES/3DES 8、AES 16
　F：パディング長(1byte) + 次ヘッダ番号(1byte)

MSS 調整値 = トンネルインタフェース MTU - G
　G：IP ヘッダ(20byte) + TCP ヘッダ(20byte)

※EtherIP の場合、ここからさらに EtherIP ヘッダ(2byte)、Ether ヘッダ(14byte)、合わせて 16byte を引いた値が適切な MSS 値となります。

【計算例】

出力回線がフレッツ ADSL/B フレッツ(MTU=1454)で、トンネルモードで 3DES/SHA1 使用時。

X = 1454 - 12(SHA1) - 8(3DES の IV) - 8(ESP ヘッダ) - 20(IP ヘッダ)
X = 1406

トンネルインタフェース MTU = (1406 / 8 の整数部) x 8 - 2
トンネルインタフェース MTU = 1398

トンネルインタフェース MSS 調整値 = トンネルインタフェース MTU - 40
トンネルインタフェース MSS 調整値 = 1358byte

以下の表は、上記の計算式を基にして各種設定での MSS 値を算出したものになります。

出力 I/F の MTU	EtherIP	IPsec	カプセル化モード	暗号、認証プロトコル	MSS 設定値
1500	あり	あり	トランスポート	DES/3DES + MD5/SHA1	1390
				AES + MD5/SHA1	1382
		なし	ー	ー	1424
	なし	あり	トランスポート	DES/3DES + MD5/SHA1	1426
				AES + MD5/SHA1	1418
			トンネル	DES/3DES + MD5/SHA1	1406
				AES + MD5/SHA1	1398
		なし	ー	ー	1460
1492 (PPPoE)	あり	あり	トランスポート	DES/3DES + MD5/SHA1	1382
				AES + MD5/SHA1	1374
		なし	ー	ー	1416
	なし	あり	トランスポート	DES/3DES + MD5/SHA1	1418
				AES + MD5/SHA1	1410
				DES/3DES + MD5/SHA1	1398

			トンネル	AES + MD5/SHA1	1390
		なし	ー	ー	1452
1454 (フレッツ ADSL/B フレッツ)	あり	あり	トランスポート	DES/3DES + MD5/SHA1	1342
				AES + MD5/SHA1	1334
		なし	ー	ー	1378
	なし	あり	トランスポート	DES/3DES + MD5/SHA1	1378
				AES + MD5/SHA1	1370
			トンネル	DES/3DES + MD5/SHA1	1358
				AES + MD5/SHA1	1350
		なし	ー	ー	1414

2.16.5 ICMP リダイレクトメッセージの送信制御設定

ICMP REDIRECTS メッセージの送信を制御することが可能です。デフォルトでは、ICMP REDIRECTS メッセージを送信しますので、REDIRECTS を送信したくない場合に、停止設定を行います。

ノンブロードキャストネットワーク（ポイントツーポイントネットワーク等）では、以下のコマンドは無視されます。

no ip redirects	ICMP リダイレクトメッセージの送信停止設定 （インタフェースコンフィグモード）

【設定例】

```
no ip redirects
```

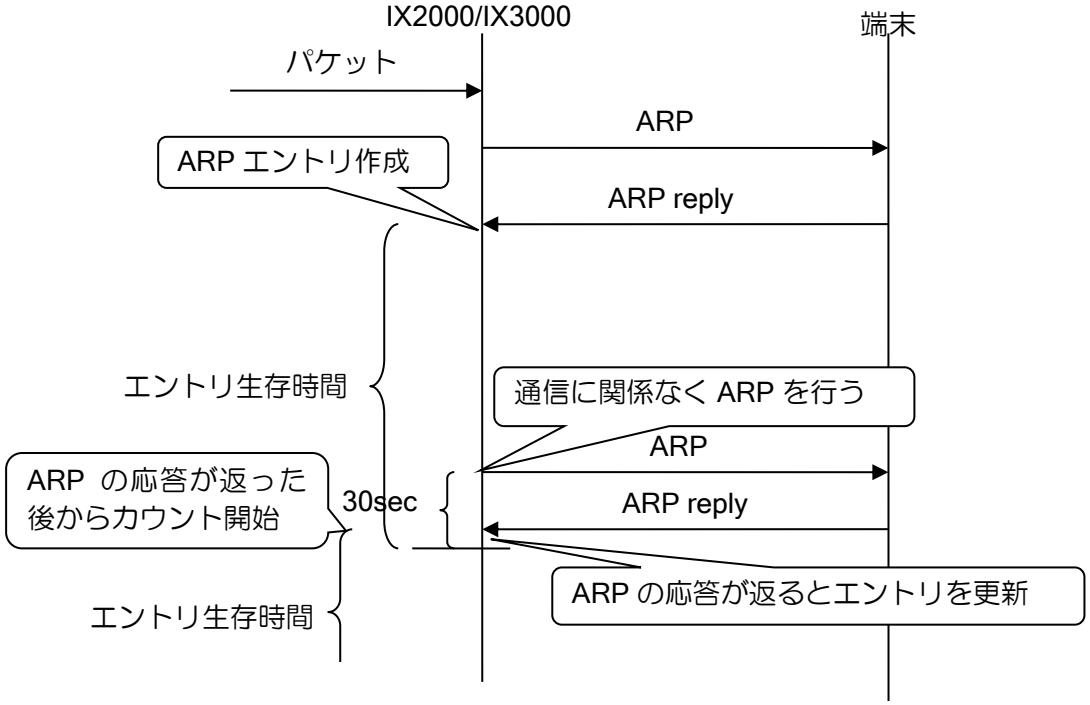
2.16.6 ARP の設定

ARP に関して、以下の設定を行うことができます。

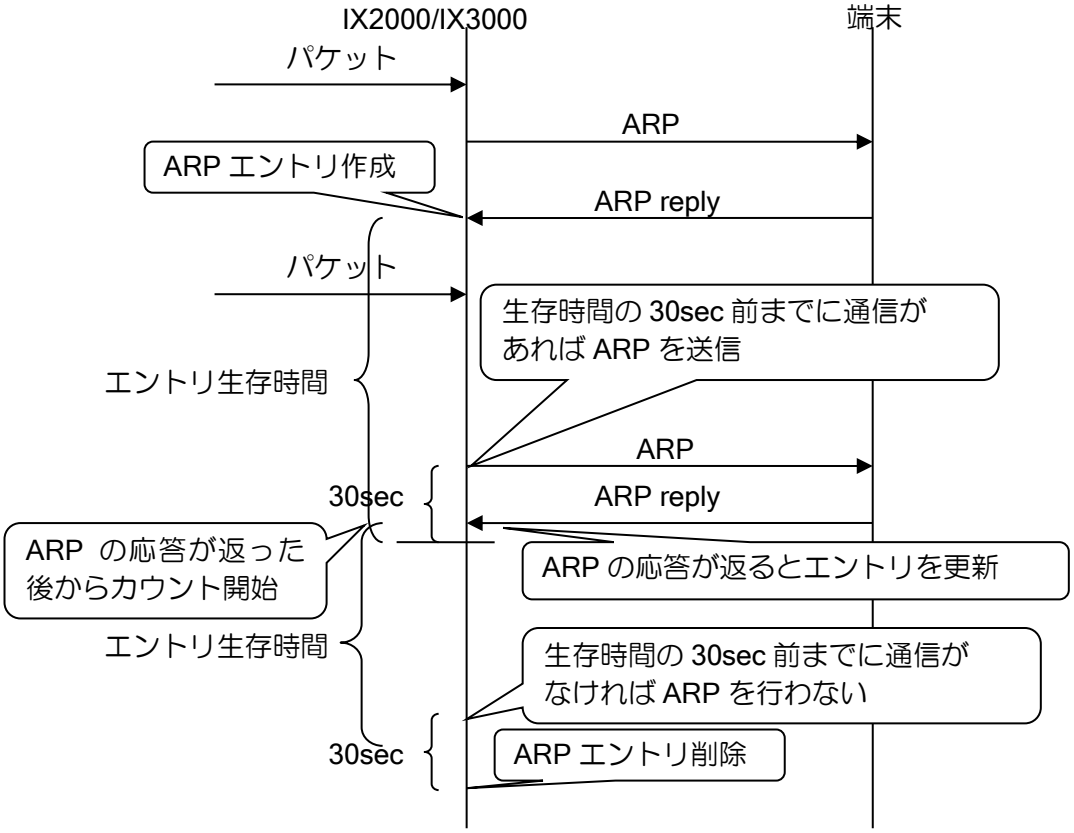
arp auto-refresh	ARP エントリ自動更新
arp timeout	ARP エントリ生存時間
arp entry	ARP エントリのスタティック登録

ARP エントリの登録･削除は以下の手順で行われます。コマンドで登録したエントリは生存時間に関係なく保持されます。

auto-refresh 設定の場合



auto-refresh なしの場合



通信の有無は、ルートキャッシュの情報から判断します。以下の場合は、ルートキャッシュを作成しません。そのため、通信がある場合でも通信が無かったと判断し ARP エントリの更新を行いません。ARP エントリの更新が必要な場合は、auto-refresh の設定を行ってください。

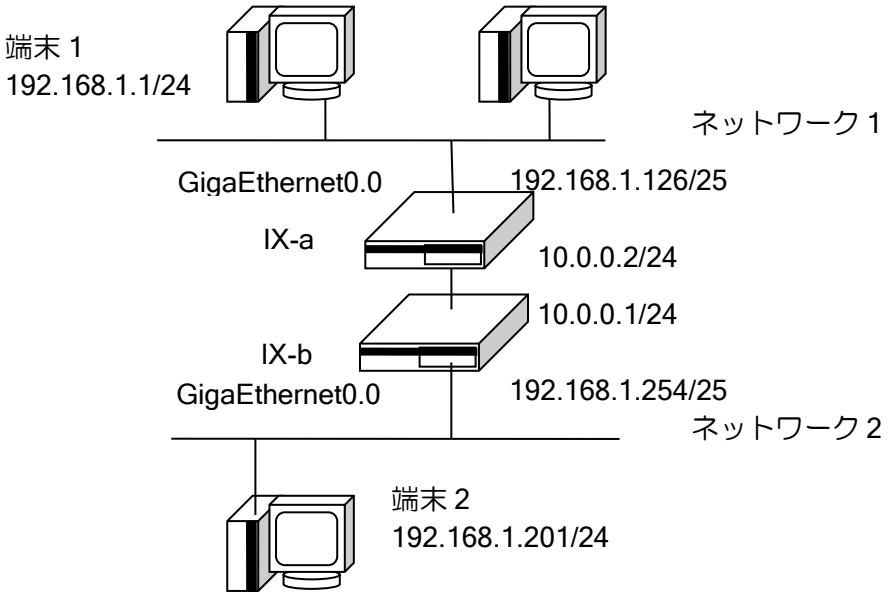
- QoS 使用時（Ver.7.3 以前）
- 自装置から送信する通信（ICMP reply など）

auto-refresh 設定のあり無しにかかわらず、ARP エントリの更新のための ARP の送信に対し、端末から応答が無ければ、ARP エントリは更新されず削除されます。

2.16.7 プロキシ ARP の設定

プロキシ ARP は ARP 応答できない端末の代理として、ARP 応答する機能です。Ver.4 以降でサポートしています。たとえば、同一リンク上にない端末を同一リンク上に存在する端末であるかのように見せかけることができます。

基本動作を以下に示します。



プロキシ ARP 機能は、あるアドレスに対する ARP 要求を受信し、そのアドレス宛の経路が存在する場合に応答します。基本的に同一リンク上のネットワークアドレスに対する場合には応答しません。上記の図のような場合に、端末 1 から端末 2 に対する ARP 要求に、代理応答します。

詳細は次のとおりです。

- IX-a の動作
  - 端末 1 からネットワーク 2 上に存在するアドレスに対する ARP 要求に代理応答します。
  - 端末 1 からネットワーク 1 上に存在するアドレスに対する ARP 要求には応答しません。
  - 端末 1 からネットワーク 2 上のアドレス宛のパケットを受信し、IX-b に送信します。

- IX-b の動作
  - 端末 2 からネットワーク 1 上に存在するアドレスに対する ARP 要求に代理応答します。
  - 端末 2 からネットワーク 2 上に存在するアドレスに対する ARP 要求には応答しません。
  - 端末 2 からネットワーク 1 上のアドレス宛のパケットを受信し、IX-a に送信します。

なお、受信ネットワークに存在するか否かは、ルーティングテーブルを見て判断していますので、受信ネットワークに対する ARP 要求であっても、経路の設定次第で代理応答させることも可能です。

プロキシ ARP を設定するコマンドは次のとおりです。

ip proxy-arp	プロキシ ARP の有効 （インタフェースコンフィグ）

【設定例】

ネットワーク 1 からの ARP をネットワーク 2 側へ,
ネットワーク 2 からの ARP をネットワーク 1 側へ
プロキシを行う

[IX-a]

```
ip route 192.168.1.128/25 10.0.0.1

interface GigaEthernet0.0
   ip address 192.168.1.126/25
   ip proxy-arp
   no shutdown
```

[IX-b]

```
ip route 192.168.1.0/25 10.0.0.2

Interface GigaEthernet0.0
   ip address 192.168.1.254/25
   ip proxy-arp
   no shutdown
```

proxy-arp コマンドでは特定ホストからの特定のアドレスに対してのみ ARP 代理応答をするように、アクセスリストを使用して設定することも可能です。
これらの範囲指定は次のように記述します。

- アクセスリストの送信元アドレスに、ARP 要求元アドレス
- アクセスリストの宛先アドレスに、ARP 要求対象アドレス
- permit の場合には宛先アドレスの経路情報の有無にかかわらず、指定範囲で ARP 代理応答し、deny の場合は代理応答しません。

これらを利用することで ARP 代理応答をする範囲を制限することができます。

【設定例】

前図の端末 1 からの ARP は全ての宛先に対してプロキシを行う

```
ip access-list list1 permit ip src 192.168.1.1/32 dest any

interface GigaEthernet0.0
   ip address 192.168.1.126/25
   ip proxy-arp list1
   no shutdown
```

2.16.7.1 ローカルプロキシ ARP

ローカルプロキシ ARP 機能を有効にした場合、同一サブネット内の全ての IP アドレスの ARP に応答を返します（Ver.8.8 以降）。

ただし、以下の ARP には応答を返しません。

- Gratuitous ARP（Sender=Target の重複チェック）
- DHCP クライアントの重複チェック（Sender Protocol Address=0.0.0.0）
- ネットワークアドレス（ホスト部分が全て 0）
- ブロードキャストアドレス（ホスト部分が全て 1）

設定は以下のとおりです。

ip local-proxy-arp	ローカルプロキシ ARP の有効 （インタフェースコンフィグ）

【設定例】
ローカルプロキシ ARP を設定

```
interface GigaEthernet1.0
  ip address 192.168.0.1/24
  ip local-proxy-arp
  no shutdown
```

本機能が有効の場合、ICMP リダイレクトメッセージを送信しません。ip redirect コマンド設定時も ICMP リダイレクトメッセージは送信しません。

特定ホストからの特定のアドレスに対してのみ ARP 代理応答をするように、アクセスリストを使用して設定することも可能です。（Ver.10.0 以降）
これらの範囲指定は次のように記述します。

- アクセスリストの送信元アドレスに、ARP 要求元アドレス
- アクセスリストの宛先アドレスに、ARP 要求対象アドレス

【設定例】
ローカルプロキシ ARP を設定
192.168.0.2 からの ARP のみ同一サブネット内全ての ARP に対して応答を返す

```
ip access-list accesslist1 permit ip src 192.168.0.2/32 dest any

interface GigaEthernet1.0
  ip address 192.168.0.1/24
  ip local-proxy-arp accesslist1
  no shutdown
```

注意事項

- ローカルプロキシ ARP 有効時は同一サブネット内の全ての IP アドレスに応答を返します。他に ARP の応答を返す装置がある場合、ARP 送信元の装置にてアドレス解決が正しく行われない可能性があります。ネットワーク構成にはご注意ください。

2.16.8 ダイレクトブロードキャスト

ダイレクトブロードキャストを有効化すると、指定したインタフェース宛のブロードキャスト
パケットを、指定のインタフェースへブロードキャストで転送することができます。

設定は以下のとおりです。

ip directed-broadcast	ダイレクトブロードキャストの設定 （インタフェースコンフィグ）

【設定例】
ダイレクトブロードキャストを設定

```
interface GigaEthernet1.0
   ip address 192.168.0.1/24
   ip directed-broadcast
   no shutdown
```

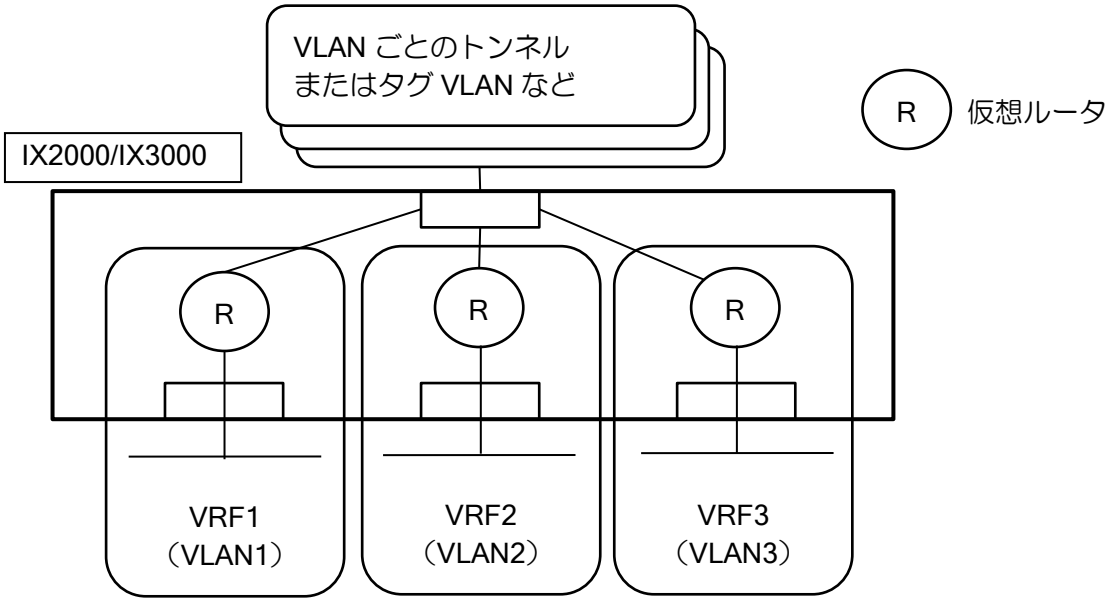
上記の設定を行うと、ダイレクトブロードキャストを設定した GigaEthernet1.0 のネットワーク
(192.168.0.0/24)のブロードキャストアドレスとなる 192.168.0.255 宛のパケットを、
GigaEthernet1.0 に転送するようになります。
ダイレクトブロードキャストを設定していない場合は、パケットを破棄します。
なお、それ以外のセグメント宛のブロードキャストパケットについては、ダイレクトブロードキャスト
設定の有無にかかわらず、ユニキャストパケットと同様に転送を行います。

■2.17 VRF-Lite の設定

VRF-Lite（以下 VRF）は、ルータの中に複数の仮想ルータを生成し、1 台のルータを複数ルータのように動作させる機能です。複数の独立したネットワークを安全に分離して管理することができ、IP アドレスが重複する環境でも利用可能です。Ver9.5 以降で対応しています。

2.17.1 機能概要

VRF 機能では、以下のように装置内に仮想的にルータを生成することができます。ルータのインタフェースをそれぞれの VRF に割り当てることで、各インタフェースが仮想ルータのインタフェースとして認識され、異なるルータと通信が分離されます。



VRF に割り当てた部分を仮想ルータ、VRF に属していない既存部分をベースルータと呼びます（グローバルルータとも呼ばれることもあります）。

それぞれのルータは、基本的な IPv4 機能のほか、スタティックルーティングやポリシールーティング、IPsec による暗号化、VRRP、ネットワークモニタ機能などに対応しています。

2.17.2 注意事項

- VRF としてサポートしている機能をよくご確認の上ご利用ください。特にルーティングプロトコル(BGP のみ対応)に未対応なため、これらの機能はベースルータ側で利用してください。
- VRF 上の IP アドレスは、VRF を設定した後に設定してください。IP アドレス設定済みのインタフェースに VRF を設定した場合、先に設定していたアドレスは削除されます。
- IP アドレスに関わるコマンドで VRF の情報を取得する場合は VRF 名の指定が必要です。VRF 名を指定しない場合、ベースルータの情報のみを取得します。
- VRF が異なっても VRRP の VRID は重複できません。
- VRF が異なっても VLAN タギング機能（IEEE802.1Q）の VLAN 識別子（VID）は重複できません。
- 複数の VRF を IPsec で暗号化して同一のセンタ装置と接続する場合、同一拠点間の IPsec 複数接続になるため、後述の説明を確認してください。

2.17.3 基本設定

VRF の設定は ip vrf forwarding コマンドで行います。このコマンドをインタフェースに設定することで、そのインタフェースは仮想ルータ上のインタフェースとして動作するようになります。

VRF 名ごとに仮想ルータを生成することができます。

VRF 用のルーティング設定は VRF 名を指定して設定します。

ip vrf forwarding	VRF インタフェースの設定
ip address	VRF 上の IPv4 アドレス設定
ip route vrf	VRF 上のスタティックルート設定
ip cache-size vrf	VRF のキャッシュサイズの設定

【設定例】

```
ip route vrf vrf1 default 192.168.0.1
ip route vrf vrf2 default 192.168.0.1
!
interface GigaEthernet0.0
   ip vrf forwarding vrf1
   ip address 192.168.0.254/24
   no shutdown
!
interface GigaEthernet1.0
   ip vrf forwarding vrf1
   ip address 192.168.1.254/24
   no shutdown

interface GigaEthernet2.0
   ip vrf forwarding vrf2
   ip address 192.168.0.254/24
   no shutdown
!
interface GigaEthernet3.0
   ip vrf forwarding vrf2
   ip address 192.168.1.254/24
   no shutdown
```

異なる VRF 間での通信はできません。送信先に異なる VRF のインタフェースを指定しても動作せず、設定例の vrf1 と vrf2 のネットワークは完全に分離されます。

VRF 上のルーティングキャッシュはベースルータと仕組みが異なります。そのため、キャッシュサイズのデフォルト値を小さくしていますが、不足する場合は調整してください。

2.17.4 VRF 対応機能の設定

従来と同じ設定で動作する機能と、VRF 名指定が必要となる機能があります。

インタフェース上で動作するフィルタや NAT、QoS、MSS 調整機能、VRRP などの機能は、従来と同じ設定で動作します。

以下のコマンドにおいては同時に VRF 名の指定が必要です。

ping vrf	VRF 上の Ping
traceroute vrf	VRF 上の traceroute
event NUM vrf ... action NUM vrf ...	ネットワークモニタ機能のホスト/経路監視 ネットワークモニタ機能の経路制御
nslookup vrf	VRF 上の DNS リゾルバ(nslookup)
telnet vrf	VRF 上の telnet
software-update vrf	VRF 上のファームウェア更新
startup software-update vrf	VRF 上の起動時自動ファームウェア更新
copy vrf	VRF 上のコピー
tftp get vrf	VRF 上の TFTP ファイル転送(受信)
tftp put vrf	VRF 上の TFTP ファイル転送(送信)
ip name-server vrf	VRF 上の DNS リゾルバ
proxy-dns vrf server	VRF 上の Proxy-DNS
snmp-agent vrf ip host	VRF 上のトラップ送信先の IP アドレスの設定
snmp-agent vrf ip trap-source	VRF 上のトラップ送信元アドレスの設定
syslog vrf ip host	VRF 上の SYSLOG の IPv4 送信ホストの設定
syslog vrf ip source	VRF 上の SYSLOG の送信元アドレスの設定
ntp vrf server	VRF 上の NTP サーバ
nm vrf ip enable	VRF 上の NetMeister クライアントの有効化

【入力例】

```
ping 192.168.0.1 vrf vrf1
```

【設定例】

```
watch-group example1
  event 1 vrf vrf1 ip unreach-host 192.168.0.1 GigaEthernet0.0
```

2.17.5 対応状況

VRF 機能の対応状況一覧です。
※下記の表に記載されていない機能は全て非対応です。

インタフェース機能

機能	対応
イーサネット（ベース、ポート VLAN、タグ VLAN、BVI） ※静的アドレスのみ	○
動的アドレス(PPP/PPPoE)	○（Ver.9.6 以降）
動的アドレス(DHCP)	○（Ver.10.4 以降）
動的アドレス(L2TP)	×
データコネクト	×
Null, Loopback (0.0 は VRF 指定不可)	○
Tunnel	○
ダイレクトブロードキャスト	○

ルーティング機能

対応しているルーティングプロトコルは BGP のみです。BGP 以外で経路制御を行う場合はネットワークモニタ機能を利用してください。

機能	対応
スタティックルーティング	○
BGP	○（Ver.9.6 以降) ※1
OSPF/RIP	×
ポリシールーティング（ローカルポリシーを除く）	○
マルチパス	×
VRF 間ルーティング（ルート漏洩）	×
マルチキャスト	×

※1　VRF では BGP の以下機能が使用できません

- ✧ Route Distinguisher (RD)
- ✧ Route Target (RT)
- ✧ Peer Group および Dynamic Neighbor (動的ピアアドレス) 【Ver.9.6 以前】
- ✧ Aggregate (経路集約) 【Ver9.6 以前】
- ✧ 異なる VRF 間の BGP 経路の再配信
- ✧ 複数プロセス対応(AS は 1 つのみ設定可能)

フォワーディング機能

機能	対応
IP フィルタ / MAC フィルタ	○
NAT/NAPT	○
QoS	○
IPsec / ダイナミック VPN Inner 対応 （トンネル内を VRF 化）	○
IPsec Outer 対応（トンネル外を VRF 化）	×
非 IPsec Tunnel Outer 対応（トンネル外を VRF 化）	×
MSS 調整	○
簡易 IDS	○
データコネクト	○
URL リダイレクト、URL オフロード、 URL フィルタリング	×

IPv4 機能

機能	対応
DHCP サーバ機能	○※1
DHCP クライアント機能	○（Ver.10.4 以降）
DHCP リレー機能	○（ver.9.7 以降）
VRRP 機能	○
ネットワークモニタ機能	○
プロキシ DNS 機能	○（Ver.9.6 以降）

※1　VRF では DHCP サーバの以下機能が使用できません

- ✧　除外アドレス設定

IPv6 機能

IPv6 はルーティング機能を含めて VRF 未対応です。

レイヤ 2 機能

認証系の機能を利用する場合、Radius が VRF 上では動作しないので、ご注意ください。ベースルータで Radius を動作させて、NAS-Port アトリビュートによって Radius サーバ側で VRF を識別してください。

機能	対応
タグ VLAN、ポート VLAN	○
MAC フィルタ	○
MAC 認証	△（Radius はベースルータ）
802.1X 認証	△（Radius はベースルータ）
リンクアグリゲーション	○
リンクマネージャ	○
Wake on Lan	△（監視不可）
ブリッジ機能	対象外
OpenFlow 機能	○※1

※1 OpenFlow 機能は複数のネットワークを独立に制御可能ですが、BVI を介してルータ機能を利用している場合、従来はルータ部分でネットワーク分離ができませんでした。VRF 機能によ

り、ルータ機能併用時でも完全にネットワークを分離・制御することができます。

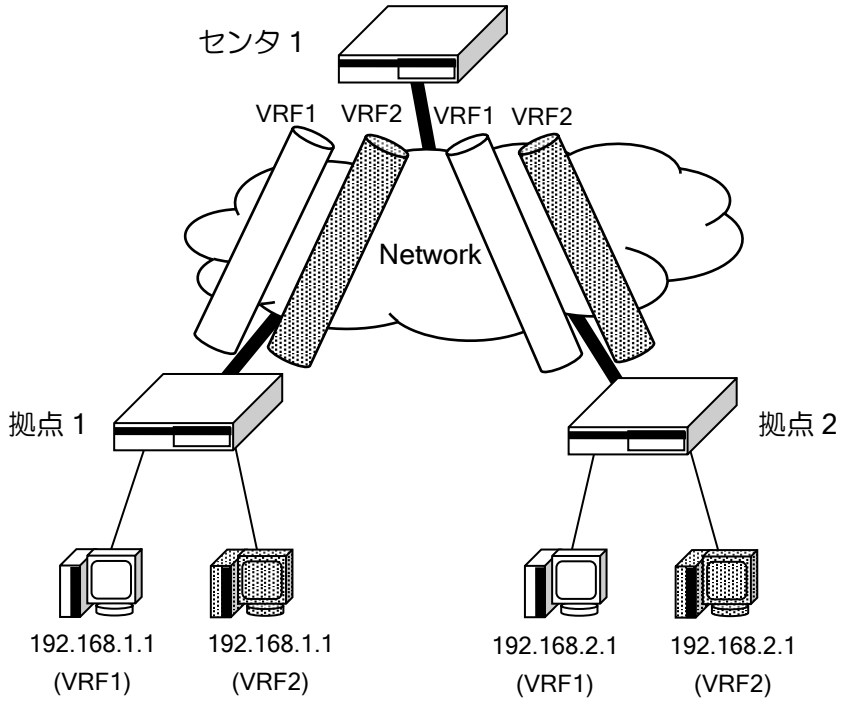
保守機能

機能	対応
ping / traceroute	○
telnet / SSH / Web コンソール機能	○（Ver.9.6 以降）
syslog 送信	○（Ver.9.6 以降）
SNMP/TRAP	○（Ver.9.6 以降）
DNS リゾルバ（nslookup）	○（Ver.9.6 以降）
NTP	○（Ver.10.4 以降）
Radius	×
ソフトウェア更新	○（Ver.9.6 以降）
コンフィグダウンロード	○（Ver.9.6 以降）
NetMeister 接続	○（Ver.10.7 以降）※1

※1　VRF で接続した場合、制限事項があります。詳細は NetMeister VRF 接続構成の章をご確認ください。

2.17.6 多対地 IPsec 構成

VRF を利用して 2 系統のネットワークを収容する VPN の構成例を以下に示します。例ではそれぞれのネットワークで重複したアドレスを使用しています。



VRF ごとにそれぞれ独立した IPsec を設定します。鍵交換プロトコルには IKEv2 を用い、センタ側の設定は peer any としてください。

ネットワークモニタ機能による制御や VRRP も併用可能です。

【設定例（センタ）】

ikev2 の設定を peer any で設定していることに注意してください。
拠点 1 との接続のみ記載しています。

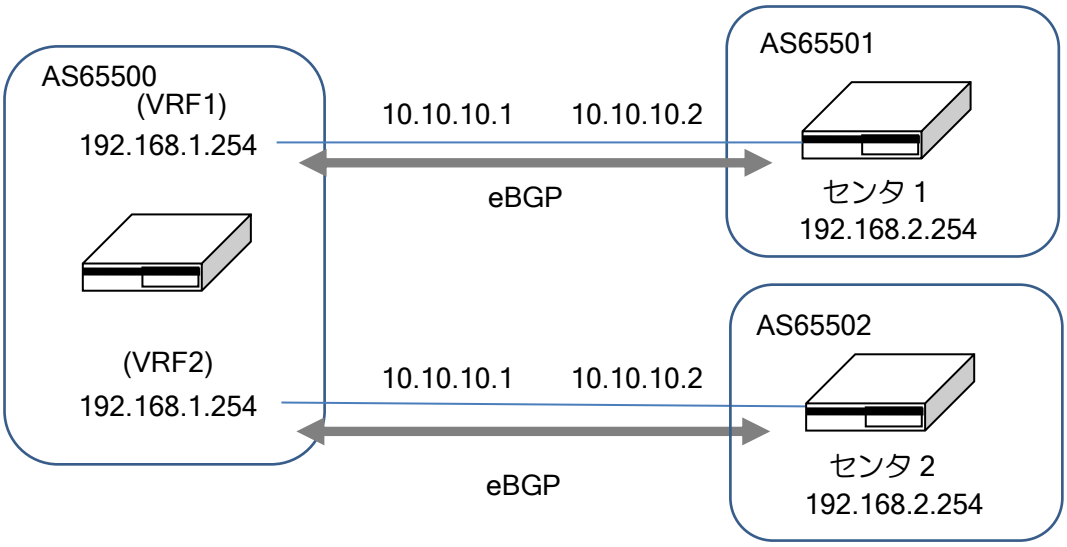
```
ip route default 10.10.10.254
ip route vrf VRF1 192.168.1.0/24 Tunnel0.0
ip route vrf VRF2 192.168.1.0/24 Tunnel1.0
!
ikev2 authentication psk id keyid CENTER-VRF1 key char himitsukagi1
ikev2 authentication psk id keyid CENTER-VRF2 key char himitsukagi1
ikev2 authentication psk id keyid SITE1-VRF1 key char himitsukagi2
ikev2 authentication psk id keyid SITE1-VRF2 key char himitsukagi2
!
device GigaEthernet1
   vlan-group 1 port 1
   vlan-group 2 port 2
!
interface GigaEthernet0.0
   ip address 10.10.10.1/24
   no shutdown
!
interface GigaEthernet1:1.0
   ip vrf forwarding VRF1
   ip address 192.168.0.254/24
   no shutdown
!
interface GigaEthernet1:2.0
   ip vrf forwarding VRF2
   ip address 192.168.0.254/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec-ikev2
   ip vrf forwarding VRF1
   ip unnumbered GigaEthernet1:1.0
   ip tcp adjust-mss auto
   ikev2 ipsec pre-fragment
   ikev2 local-authentication psk id keyid CENTER-VRF1
   ikev2 peer any authentication psk id keyid SITE1-VRF1
   no shutdown
!
interface Tunnel1.0
   tunnel mode ipsec-ikev2
   ip vrf forwarding VRF2
   ip unnumbered GigaEthernet1:2.0
   ip tcp adjust-mss auto
   ikev2 ipsec pre-fragment
   ikev2 local-authentication psk id keyid CENTER-VRF2
   ikev2 peer any authentication psk id keyid SITE1-VRF2
   no shutdown
```

【設定例（拠点）】

```
ip route default 20.20.20.254
ip route vrf VRF1 192.168.0.0/24 Tunnel0.0
ip route vrf VRF2 192.168.0.0/24 Tunnel1.0
!
ikev2 authentication psk id keyid CENTER-VRF1 key char himitsukagi1
ikev2 authentication psk id keyid CENTER-VRF2 key char himitsukagi1
ikev2 authentication psk id keyid SITE1-VRF1 key char himitsukagi2
ikev2 authentication psk id keyid SITE1-VRF2 key char himitsukagi2
!
device GigaEthernet1
   vlan-group 1 port 1
   vlan-group 2 port 2
!
interface GigaEthernet0.0
   ip address 20.20.20.1/24
   no shutdown
!
interface GigaEthernet1:1.0
   ip vrf forwarding VRF1
   ip address 192.168.1.254/24
   no shutdown
!
interface GigaEthernet1:2.0
   ip vrf forwarding VRF2
   ip address 192.168.1.254/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec-ikev2
   ip vrf forwarding VRF1
   ip unnumbered GigaEthernet1:1.0
   ip tcp adjust-mss auto
   ikev2 ipsec pre-fragment
   ikev2 local-authentication psk id keyid SITE1-VRF1
   ikev2 peer 10.10.10.1 authentication psk id keyid CENTER-VRF1
   no shutdown
!
interface Tunnel1.0
   tunnel mode ipsec-ikev2
   ip vrf forwarding VRF2
   ip unnumbered GigaEthernet1:2.0
   ip tcp adjust-mss auto
   ikev2 ipsec pre-fragment
   ikev2 local-authentication psk id keyid SITE1-VRF2
   ikev2 peer 10.10.10.1 authentication psk id keyid CENTER-VRF2
   no shutdown
```

2.17.7 多対地 BGP 構成

VRF を利用して 2 系統のネットワークを収容する VPN の構成例を以下に示します。例ではそれぞれのネットワークで重複したアドレスを使用しています。




```
【設定例（拠点）】

BGP(VRF)の設定

router bgp 65500
   vrf VRF1
      neighbor 10.10.10.2 remote-as 65501
      address-family ipv4 unicast
         network 192.168.1.0/24
   vrf VRF2
      neighbor 10.10.10.2 remote-as 65502
      address-family ipv4 unicast
         network 192.168.1.0/24
!
interface GigaEthernet0.1
   encapsulation dot1q 1 tpid 8100
   auto-connect
   ip vrf forwarding VRF1
   ip address 10.10.10.1/24
   no shutdown
!
interface GigaEthernet0.2
   encapsulation dot1q 2 tpid 8100
   auto-connect
   ip vrf forwarding VRF2
   ip address 10.10.10.1/24
   no shutdown
!
interface GigaEthernet1.1
   encapsulation dot1q 1 tpid 8100
```

```
   auto-connect
   ip vrf forwarding VRF1
   ip address 192.168.1.254/24
   no shutdown
!
interface GigaEthernet1.2
   encapsulation dot1q 2 tpid 8100
   auto-connect
   ip vrf forwarding VRF2
   ip address 192.168.1.254/24
   no shutdown
```

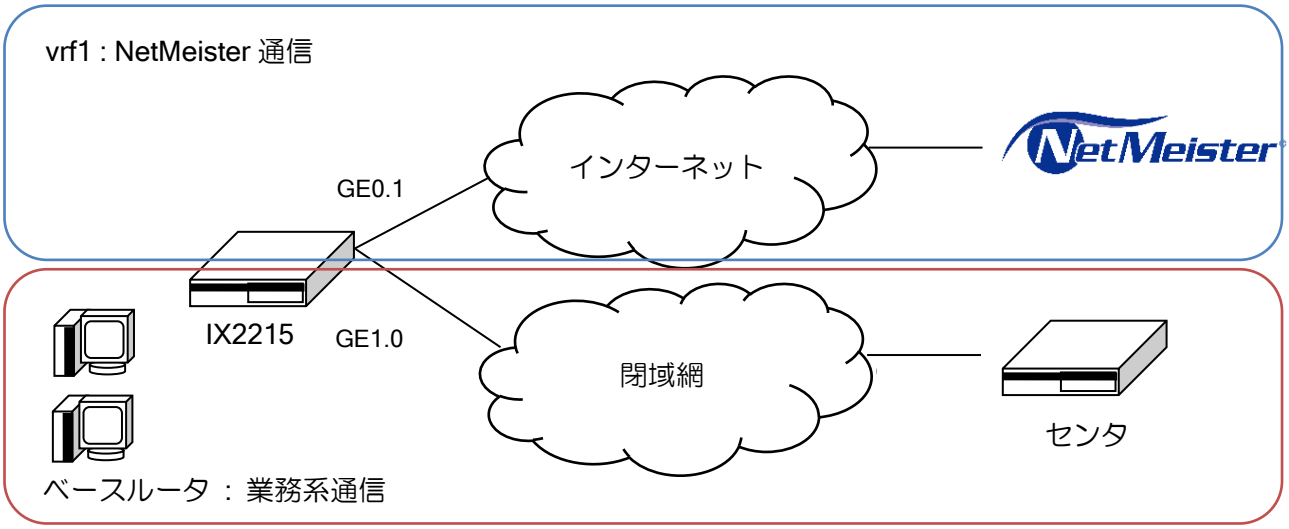
```
【設定例（センタ 1）】

router bgp 65501
   neighbor 10.10.10.1 remote-as 65500
   address-family ipv4 unicast
      network 192.168.2.0/24
!
interface GigaEthernet0.1
   encapsulation dot1q 1 tpid 8100
   auto-connect
   ip address 10.10.10.2/24
   no shutdown
!
interface GigaEthernet1.1
   encapsulation dot1q 1 tpid 8100
   auto-connect
   ip address 192.168.2.254/24
   no shutdown
```

2.17.8 ダイナミック VPN 構成

Ver.9.7 以降ではダイナミック VPN 構成も VRF ごとに利用可能です。拠点側、センタ側、どちらも VRF 対応にすることができます。設定はダイナミック VPN の章を参照してください。

2.17.9 NetMeister VRF 接続構成

VRF を利用して NetMeister を利用する例を以下に示します。通常、NetMeister はインターネット接続が必要のため、閉域網で接続することができません(NetMeister Prime を契約すると NGN 閉域網で利用可能)。閉域網で NetMeister を利用したい場合、NetMeister VRF 接続構成を利用することで閉域網のセキュリティ性を確保しつつ、NetMeister をご利用いただけます。VRF 側をインターネットに接続する NetMeister 用のネットワーク、ベースルータ側を閉域網の業務系通信ネットワークに分離し、閉域網の通信がインターネット側へ漏洩するのを防ぎつつ NetMeister で装置管理することができます。



【設定例】

```
ip route default 10.10.10.254
ip route vrf vrf1 default GigaEthernet0.1
!
nm vrf vrf1 ip enable
nm account “グループ ID” password plain “グループパスワード”
nm sitename tokyo
!
ppp profile sample
   authentication myname test@example.com
   authentication password test@example.com my-password
!
interface GigaEthernet1.0
   ip address 10.10.10.1/24
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.1.254/24
   no shutdown
!
interface GigaEthernet0.1
   encapsulation pppoe
   auto-connect
   ppp binding sample
   ip vrf forwarding vrf1
   ip address ipcp
   no shutdown
!
system information wan 1 GigaEthernet0.1
```

2.17.9.1 VRF 名指定が必要なコマンド

VRF を利用して NetMeister を利用する場合、NetMeister 関連のコマンドで VRF 名が必要なコマンドは有効化コマンドの nm vrf [VRF 名] ip enable のみになります。有効化コマンドで指定した VRF 上で NetMeister は動作します。その他の NetMeister 関連のコマンドは VRF 名の指定は不要です。例として、ダイナミック DNS 登録インタフェースの設定コマンドである nm ddns notify interface コマンドは VRF 名不要です。指定インタフェースを VRF インタフェースに指定してください。

2.17.9.2 リモートログイン機能の設定

VRF を利用して NetMeister を利用している際、リモートログイン機能を使用する設定例を以下に示します。リモートログイン機能を利用する場合、system information コマンド機能で VRF インタフェースを LAN として指定する必要があります。

【設定例】

```
device GigaEthernet2
   vlan-group 1 port 1
!
interface GigaEthernet2:1.0
   ip vrf forwarding vrf1
   ip address 192.168.100.254/24
   ssh-server ip enable
   http-server ip enable
   no shutdown!
!
interface GigaEthernet0.1
   encapsulation pppoe
   auto-connect
   ppp binding sample
   ip vrf forwarding vrf1
   ip address ipcp
   no shutdown
!
system information lan 1 GigaEthernet2:1.0
```

2.17.9.3 確認コマンド

登録状況を shown nm information コマンドで確認できます。NetMeister を VRF で有効化している場合、下記表示例のように VRF-NAME の欄で VRF 名が表示されます。

【表示例】

```
NetMeister Client:
   Result          : Success (20000)
   Last Request: 2022/09/13 10:41:31
   Next Request: 2022/09/19 05:23:31 (remain 327517 sec)
   VRF NAME       : vrf1
Information:
   IPv4 Address: <通知した IPv4 アドレス>
   IPv4 Domain : <通知した IPv4 ドメイン>
   IPv6 Address:
   IPv6 Domain :
   Interval       : 168 hour
API-GW:
   gpid             : sample-gpid
   stid             :
   htid             : sample-htid
```

```
   Interval      : 3600 sec
   Next Request: 2022/09/15 10:42:51 (remain 1077 sec)
   Status        : Registered
MQTT:
   Interval      : 60 sec
   Status        : Connected
```

2.17.9.4 利用できる NetMeister 機能

本環境で利用できる NetMeister 機能は、インターネット(IPv4)環境で利用できる機能と同じになります。詳細については、「NetMeister の設定」の章をご確認ください。ただし、一部の機能が使用できない等の制限事項があります。制限事項については下記を参照してください。

2.17.9.5 NetMeister VRF 接続構成の制限事項

- IPv6 は対応しておりません。
- NetMeister によるダイナミック VPN 設定には対応しておりません。
- ダイナミック DNS では、IPv6 アドレスを登録することができません。
- デバイスリスト・デバイスマップはリンクマネージャを有効化したインタフェースの情報を出力します。VRF インタフェースとベースインタフェースにリンクマネージャを有効化した場合、両インタフェースのデバイス情報が出力されます。確認したい側のインタフェースにリンクマネージャを有効化してください。
- Web-GUI を利用した設定には対応しておりません。
- UTM 機能は VRF-Lite に対応していないため、VRF 側では動作しません。UTM 機能を利用する場合、インターネット上の UTM サーバと通信する経路を別途設ける必要があります。なお NetMeister サーバに対する UTM 統計レポート・UTM 脅威分析の情報通知は VRF 側で通知します。
- URL オフロード機能は VRF-Lite に対応していないため、VRF インタフェース上では動作しません。URL オフロード機能を利用する場合、ベースインタフェース上で URL オフロードを実施するような構成でのみ利用できます。
- アプリケーション解析は VRF-Lite に対応していないため、VRF インタフェース上では動作しません。アプリケーション解析を利用する場合、ベースインタフェース上でアプリケーション解析を実施するような構成でのみ利用できます。アプリケーション解析の情報通知等は VRF 側で通知します。

■2.18 DHCP の設定

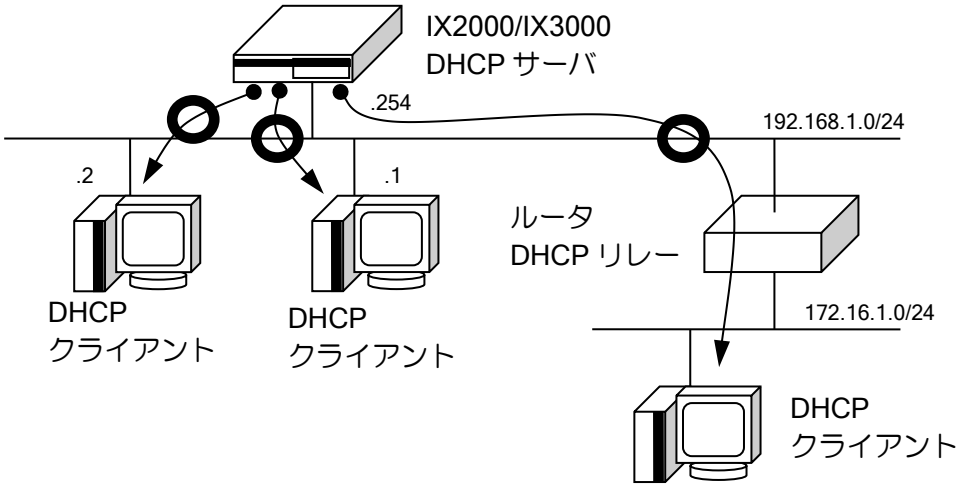
DHCP は主に、端末の IP アドレスを一元管理する場合に利用します。

IX2000/IX3000 では、DHCP のサーバ機能、クライアント機能、およびリレーエージェント機能をサポートします。

以下に DHCP 登録のための設定および基本的な動作を説明します。

2.18.1 DHCP サーバ機能

DHCP サーバ機能では、DHCP クライアントに対して IPv4 アドレスを割り付けることができます。以下に DHCP サーバのための設定および基本的な動作を説明します。



2.18.1.1 DHCP サーバ設定方法

DHCP サーバは以下の設定で行います。

1. DHCP プロファイルを作成する（ip dhcp profile）
2. DHCP プロファイルをインタフェースまたは全体に割り当てる（ip dhcp binding）
3. DHCP サーバを起動する（ip dhcp enable）

サーバの諸設定は、作成したプロファイルの中で設定します。プロファイルはインタフェースに接する LAN 上で使用する場合はインタフェースコンフィグモードで、それ以外の遠隔ネットワークに対してはグローバルコンフィグモードで設定します。

DHCP サーバの設定および確認は次のコマンドを使用します。

ip dhcp enable	DHCP サーバの有効
ip dhcp excluded-address	割り当てないアドレス範囲の設定
ip dhcp profile	プロファイルの作成
ip dhcp binding	プロファイルの割り当て
assignable-range	IPv4 アドレス割り当て範囲の設定 （省略時はリンク上の未使用アドレスになります。）
bootfile	ブートファイル名を通知します（Ver7.5.50 以降）

default-gateway	デフォルトルータの通知設定 （省略時はインタフェースのプライマリアドレス）
dns-server	DNS サーバを通知します。
domain-name	ドメイン名を通知します。
fixed-assignment	固定 IPv4 アドレスの割り当て設定
lease-time	アドレス利用可能時間の変更
netbios-name-server	NetBIOS ネームサーバ（WINS）を通知します。
next-server	ネクストサーバアドレスの設定（Ver.7.5.50 以降） （省略時はインタフェースのプライマリアドレス）
subnet-mask	サブネットマスクの設定(省略時はインタフェースのプライマリアドレスのサブネットマスク)
option	任意オプションの追加設定
show ip dhcp server	サーバ情報の表示
show ip dhcp profile	プロファイル情報の表示

- 同一 LAN 上のクライアントを管理する場合

【設定例】

```
ip dhcp enable
ip dhcp profile profile1
   assignable-range 192.168.1.1 192.168.1.10
   subnet-mask 255.255.255.0

interface GigaEthernet0.0
   ip address 192.168.1.254/24
   ip dhcp binding profile1
   no shutdown
```

- リレーエージェントを介して、他の LAN 上のクライアントを管理する場合

【設定例】

```
ip dhcp enable
ip dhcp profile profile2
   assignable-range 172.16.1.1 172.16.1.10
   subnet-mask 255.255.255.0

ip dhcp binding profile2
```

- リレーエージェントを介して、同一サブネット上のクライアントを管理する場合

【設定例】

```
ip dhcp enable
ip dhcp profile profile3
   assignable-range 192.168.0.100 192.168.0.200
   subnet-mask 255.255.255.0

ip dhcp binding profile3

interface GigaEthernet0.0
   ip address 192.168.0.254/24
   no shutdown
```

2.18.1.2 セカンダリアドレスを利用した DHCP サーバの設定

- セカンダリアドレス側で DHCP サーバ機能を利用

セカンダリアドレス側のネットワークで DHCP サーバを利用する場合、プロファイルの設定で assignable-range, subnet-mask, default-gateway の 3 つを必ず設定してください。

【設定例】

```
ip dhcp enable
!
ip dhcp profile local
   assignable-range 192.168.0.1 192.168.0.200
   subnet-mask 255.255.255.0
   default-gateway 192.168.0.254
   dns-server 192.168.0.254
!
interface GigaEthernet0.0
   ip address 10.0.0.254/29
   ip address 192.168.0.254/24 secondary
   ip dhcp binding local
   no shutdown
```

- プライマリアドレスとセカンダリアドレスの両方で DHCP サーバ機能を利用（Ver8.9 以降）

DHCP を使って 1 つのインタフェースで、動的アドレスのプライベートアドレスと固定アドレスのグローバルアドレスを払い出すことができます。
動的アドレスを払い出すプロファイルをインタフェースに設定し、固定アドレスを払い出すプロファイルはグローバルに設定します。

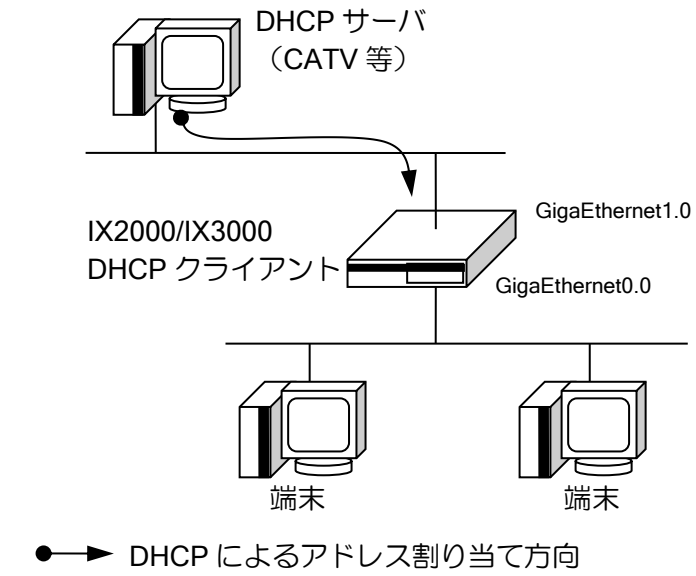
【設定例】

```
ip dhcp enable
ip dhcp binding dhcp-sec

ip dhcp profile dhcp-pri
   assignable-range 192.168.0.1 192.168.0.200
   subnet-mask 255.255.255.0
   default-gateway 192.168.0.254
   dns-server 192.168.0.254

ip dhcp profile dhcp-sec
   default-gateway 10.0.0.1
   dns-server 10.0.0.1
   fixed-assignment 10.0.0.2 xx:xx:xx:xx:xx:xx
   fixed-assignment 10.0.0.3 yy:yy:yy:yy:yy:yy
!
interface GigaEthernet0.0
   ip address 192.168.0.254/24
   ip address 10.0.0.1/28 secondary
   ip dhcp binding dhcp-pri
   no shutdown
```

2.18.2 DHCP クライアントの設定

DHCP クライアント機能は、DHCP サーバに IPv4 アドレスを要求し、その DHCP サーバから通知された IPv4 アドレスをインタフェースに自動的に割り当てることができます。

以下に DHCP クライアントのための設定および基本的な動作を説明します。



DHCP クライアント設定は、インタフェースコンフィグモードで、ip address dhcp コマンドを使用して設定します。

ip address dhcp	DHCP クライアントの有効
ip address dhcp receive-default	DHCP サーバからデフォルトルートを受信
hostname	DHCP サーバに対してホスト名を送信する場合に設定
show ip address	IPv4 アドレス設定状態表示

【設定例】

```
interface GigaEthernet1.0
  ip address dhcp receive-default
  no shutdown
```

DHCP サーバからのゲートウェイアドレスをスタティックルートのネクストホップに指定できます。また、DHCP で取得したデフォルトルートの metric，distance を設定することができます。

【設定例 1】
10.0.0.1 宛のネクストホップを DHCP からのゲートウェイアドレスを設定

```
ip route 10.0.0.0/24 GigaEthernet1.0 dhcp

interface GigaEthernet1.0
  ip address dhcp
  no shutdown
```

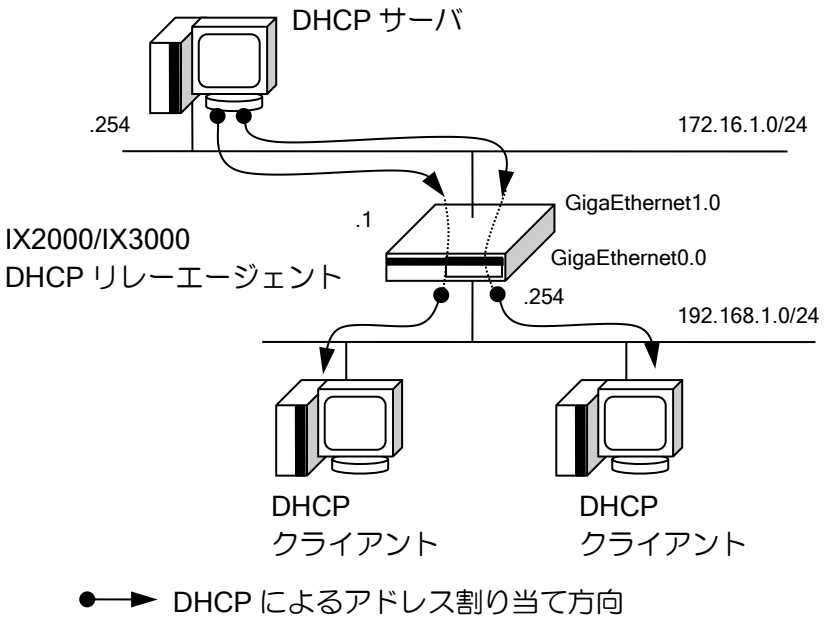
【設定例 2】
DHCP で取得したデフォルトルートの metric を 10，distance を 200 に設定

```
interface GigaEthernet1.0
  ip address dhcp receive-default distance 200 metric 10
  no shutdown
```

2.18.3 DHCP リレーエージェントの設定

DHCP リレーエージェント機能では、DHCP クライアントからの IPv4 アドレス取得要求を DHCP サーバにリレーし、DHCP サーバからのデータを DHCP クライアントにリレーすることができます。

以下に DHCP リレーエージェントのための設定および基本的な動作を説明します。



DHCP リレーエージェント設定は、グローバルコンフィグモードで、ip dhcp-relay enable コマンドを使用して設定します。

ip dhcp-relay enable	DHCP リレーエージェントの有効
ip dhcp-relay server	DHCP サーバの選択
ip dhcp-relay minimum-retry-time	クライアントからの最初の DHCP 要求から、要求パケットを廃棄し続ける時間の設定
ip dhcp-relay maximum-hop	経由可能な DHCP リレー数の設定 （指定した数値以上の DHCP リレーを経由した場合にパケットを廃棄）
show ip dhcp-relay	リレー状態表示

サーバ選択の設定はインタフェースコンフィグモードで行います。

設定を行ったインタフェースから受信したリクエストに対してのみ、指定したサーバへ DHCP パケットのリレーを行います。1 つのインタフェースに対して複数のサーバを設定した場合、全てのサーバに対してパケットをリレーします。

【設定例】

```
ip dhcp-relay enable
interface GigaEthernet1.0
   ip address 172.16.1.1/24
   no shutdown
interface GigaEthernet0.0
   ip address 192.168.1.254/24
   ip dhcp-relay server 172.16.1.254  ： サーバ設定（インタフェースコンフィグモード）
   no shutdown
```

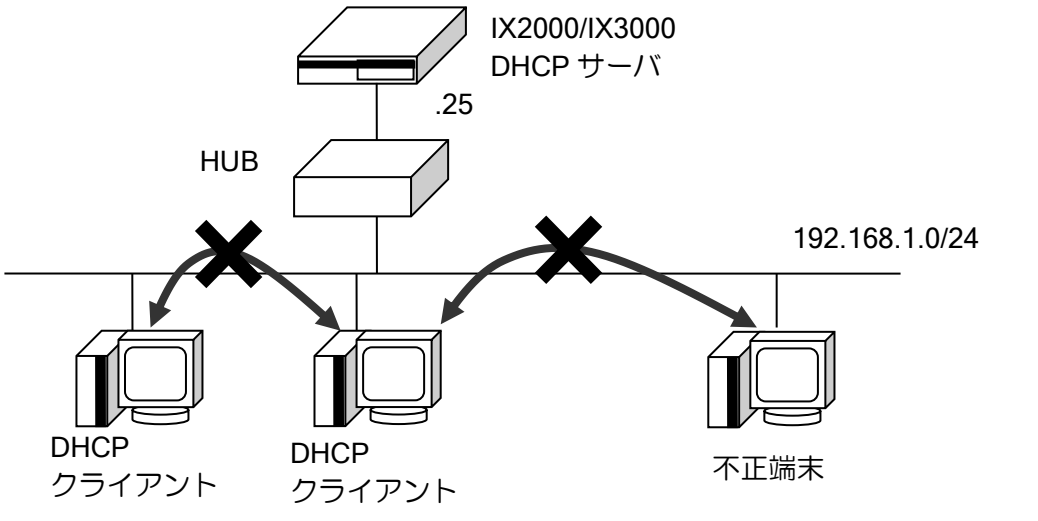
2.18.4 不正端末検知機能の設定

DHCP は、全ての ARP 要求に応答を返す装置を接続されてしまうと、
アドレスを払い出せなくなる問題があります。
マンションやホテル等の不特定多数のユーザが利用する環境で発生
することがありますが、本機能はその現象を回避することができます。
Ver9.4 以降で対応しています。

2.18.4.1 不正端末検知機能の概要

ここではあらゆる ARP 要求に応答する端末を不正端末と定義します。
DHCP ではアドレスの配布時に同じネットワーク上で IP アドレスが
重複しないことを ARP 要求で確認します。
不正端末がネットワーク上に存在しているとき、
全ての ARP 要求に対して ARP 応答を返すため、DHCP サーバは全てのアドレスが
使用されていると判断し、IP アドレスの配布が行えなくなります。

本機能は ARP 機能を利用します。複数の IP アドレスに ARP 応答する
端末を検出し、その端末との ARP 通信を制限することで、DHCP サーバのアドレス枯渇を
抑止することができます。



HUB 以下の端末は同一セグメントだが、直接通信を制限している構成

2.18.4.2 不正端末検知機能の設定

不正端末検知機能は以下の設定で行います。
同一 MAC アドレス登録数の上限の設定（arp limit-proxy-arp）
DHCP プロファイルに DHCP DECLINE の破棄設定(ignore-decline)

インタフェースコンフィグモード

arp limit-proxy-arp	インタフェースの不正端末検知機能の有効化

DHCP プロファイルモード

ignore-decline	DHCP DECLINE の破棄設定の有効化

【設定例】

```
ip dhcp enable
ip dhcp profile profile1
   assignable-range 192.168.1.1 192.168.1.200
   subnet-mask 255.255.255.0
   ignore-decline

interface GigaEthernet1.0
   ip address 192.168.1.254/24
   ip dhcp binding profile1
   arp limit-proxy-arp 3
   no shutdown
```

2.18.4.3 制限の確認

制限されている端末の確認は以下のコマンドで行います。
制限された端末は、180 秒間ネットワークから切り離すことで制限が解除されます。

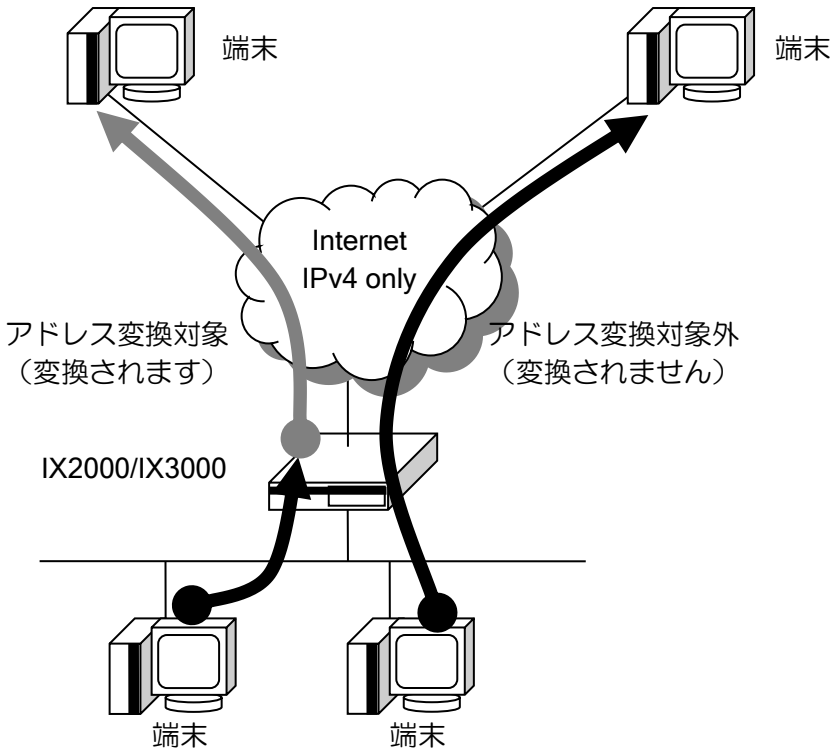
show arp entry	ARP エントリと制限 MAC アドレスの表示

2.18.4.4 注意事項

- 本機能は DHCP リレー機能と併用することができません。
- 不正端末と直接通信可能な端末は DHCP によるアドレス配布ができません。
- 設定数 IP アドレスを変更した場合不正端末として制限される可能性があります。
- 本機能は不正端末がある状態での通信を保証するものではありません。

■2.19 NAT/NAPT の設定

NAT（ネットワークアドレス変換）と NAPT（ネットワークアドレスポート変換）機能に対応しています。NAT は IPv4 アドレスのみを変換し、NAPT は IPv4 アドレスの他、TCP/UDP のポート番号などを変換することで、端末のアドレスとは異なるアドレスで通信可能です。



プライベートアドレスとして使用できる IPv4 アドレスは、RFC1918 によって次のように定義されています。これ以外のアドレスでも変換は可能です。

10.0.0.0	～	10.255.255.255	(10/8 prefix)
172.16.0.0	～	172.31.255.255	(172.16/12 prefix)
192.168.0.0	～	192.168.255.255	(192.168/16 prefix)

2.19.1 NAT の設定

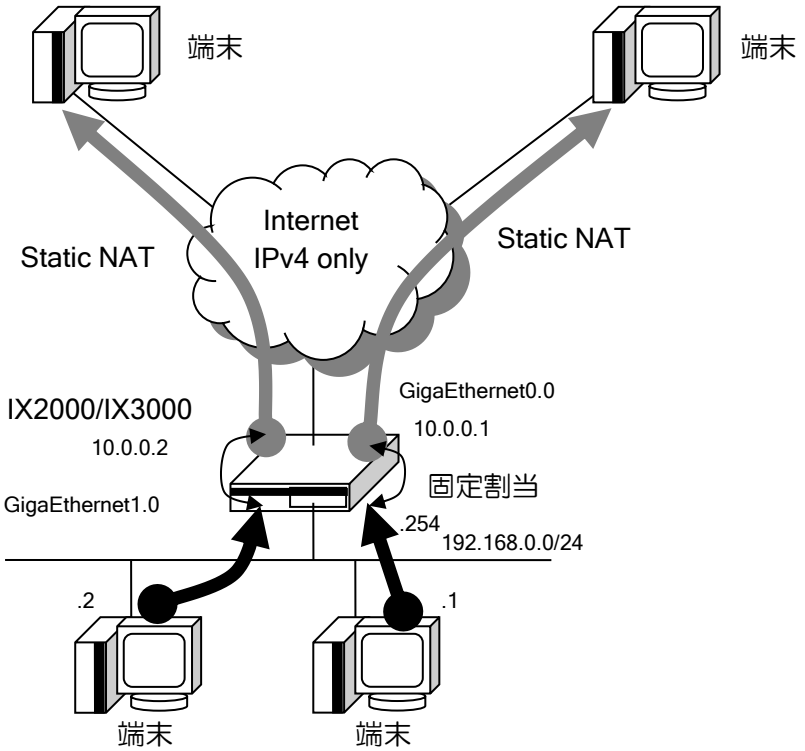
ネットワークアドレス変換（NAT）は、プライベート IPv4 アドレスを、グローバル IPv4 アドレスに変換する機能です。NAT の登録は、次のように大別することができます。

- 静的 NAT（Static NAT）
  - 内部ネットワークの端末のアドレスと外部ネットワーク用に取得したアドレスを、固定的に一対一にマッピングします。
- 動的 NAT（Dynamic NAT）
  - 外部ネットワーク用に取得した複数のアドレスをプールし、内部ネットワークの端末が外部にアクセスする際に、動的に外部ネットワークアドレスを割り当てて通信を行います。

静的 NAT または動的 NAT で範囲指定内に設定されていないパケットを外部ネットワークから受信した場合は、内部ネットワーク内にグローバルアドレス空間があるものと判断し、内部ネットワーク向けにパケットを転送します。

2.19.1.1 静的 NAT（Static NAT）の設定

静的 NAT は、プロバイダから割り当てられた IPv4 アドレスに対して、プライベートアドレス空間の端末の IPv4 アドレスを、一対一で割り当てます。グローバルアドレスが十分確保できる場合は、この設定を利用してください。



静的 NAT の設定および確認は次のコマンドを使用します。

ip nat enable	NAT の有効
ip nat static	変換テーブルの登録
show ip nat translation	変換テーブルの表示
show ip nat statistics	統計情報の表示

【設定例】

```
interface GigaEthernet0.0
   ip address 10.0.0.254/24
   ip nat enable
   ip nat static 192.168.0.1 10.0.0.1
   ip nat static 192.168.0.2 10.0.0.2
   no shutdown
```

Ver.6.0 以降、ネットワーク単位で静的 NAT の指定を行うことができます。この場合、アドレス部分は同じ値となります。複数の設定が重なっている場合は、Ver.7.1 以降はプレフィックス長の長い方が優先されます。Ver.7.0 以前は、先に設定されている方が優先となります。

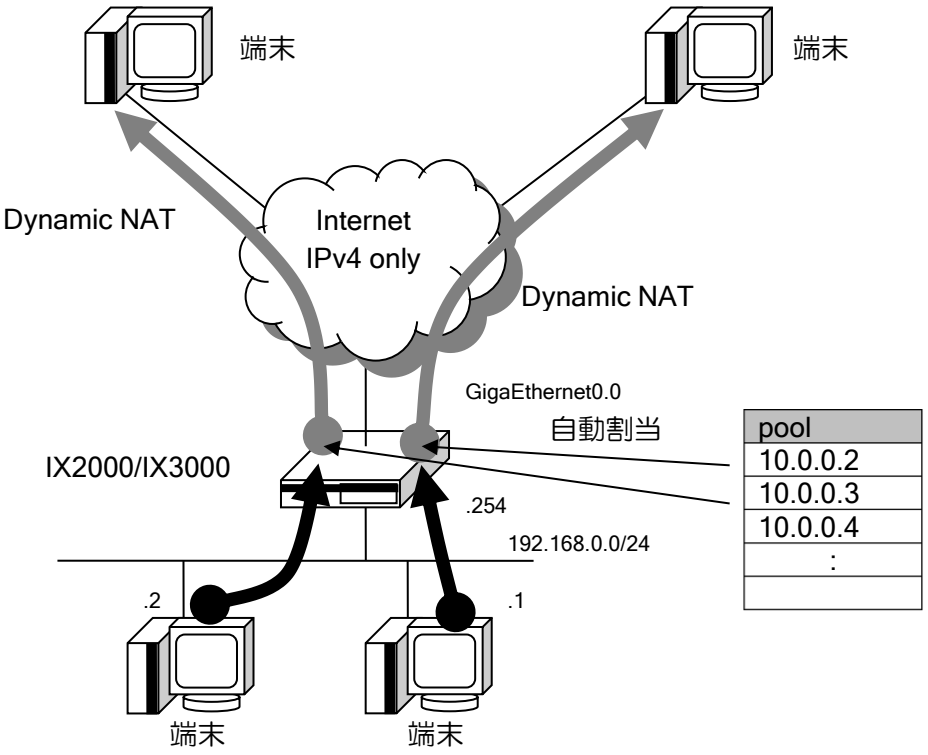
【設定例】
192.168.0.x を 10.0.0.x に変換（x は 0～127）

```
interface GigaEthernet0.0
   ip address 10.0.0.254/24
   ip nat enable
   ip nat static network 192.168.0.0/25 10.0.0.0/25
   no shutdown
```

2.19.1.2 動的 NAT（Dynamic NAT）の設定

動的 NAT は、グローバルアドレスの数が不足している場合に有効です（ただし NAPT の方が有効なので通常は NAPT を利用してください）。複数の IPv4 アドレスを予めプールに格納しておくことで、端末からグローバルアドレス空間へのアクセスがあった場合に、そのプールから自動的に送信元 IPv4 アドレスを割り当てます。

変換情報は通信が無くなった後も一定時間保持し、保持している間は同じアドレスで変換を行うことができます。情報を保持する時間はデフォルトでは 3600 秒で、変更することも可能です。



動的 NAT の設定および確認は次のコマンドを使用します。

ip nat enable	NAT の有効
ip nat pool	グローバル IPv4 アドレスのプールの設定
ip nat dynamic	動的 NAT の設定
ip nat translation	NAT キャッシュ最大エントリ数，保持時間設定
show ip nat translation	変換テーブルの表示
show ip nat statistics	統計情報の表示

【設定例】

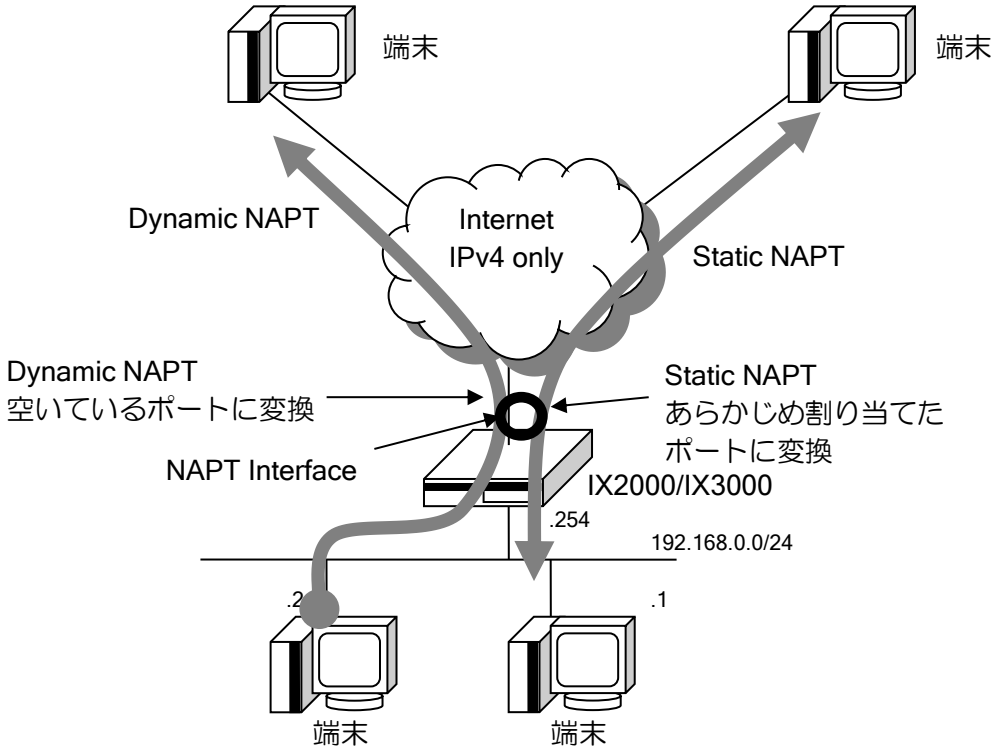
```
ip access-list access-1 permit ip src 192.168.0.0/24 dest any
ip nat pool pool-1 10.0.0.2 10.0.0.10
interface GigaEthernet0.0
   ip address 10.0.0.1/8
   ip nat enable
   ip nat dynamic list access-1 pool pool-1
   no shutdown
```

2.19.2 NAPT の設定

ネットワークアドレスポート変換（NAPT）機能は、内部ネットワークで使用しているプライベート IPv4 アドレスとトランスポートレイヤのポートから、外部ネットワークアクセス用のグローバル IPv4 アドレスとトランスポートレイヤのポートに変換します。

NAPT の登録は、次のように大別することができます。

- NAPT
  - 内部ネットワークの端末のアドレスとアプリケーションを判断し、外部ネットワーク用に取得したアドレス（1 つの IPv4 アドレス）と必要なポートに動的に変換します。
- 静的 NAPT（Static NAPT）
  - NAPT 使用中に、特定の内部ネットワーク側の端末上の特定のアプリケーションのポートを固定したい場合に使用します。
- サーバサービス設定
  - NAPT 使用中に、プライベートアドレス空間に存在するサーバをグローバルアドレス空間に提供する場合に使用します。



2.19.2.1 NAPT の設定

NAPT の設定および確認は次のコマンドを使用します。

ip napt enable	NAPT の有効
ip napt address	NAPT アドレスの変更
ip access-list	内部ネットワーク内の端末の IPv4 アドレス範囲指定
ip napt inside ...	内部ネットワークの端末を選択します。 （この設定により、内部ネットワークについて、グローバルアドレス空間と、プライベートアドレス空間を区別することができます。）

ip napt inside ... outside ...	NAPT の複数設定に使用します。 インタフェースに 2 つ目以降の NAPT アドレスを割り当てたい場合に使用します。
ip napt translation	NAPT キャッシュ最大エントリ数，保持時間設定
show ip napt translation	変換テーブルの表示
show ip napt statistics	統計情報の表示

NAPT は、ip napt enable の設定だけで動作します。アドレス、範囲指定は省略することが可能です。これらを省略した場合は、内部的に以下の設定で動作します。

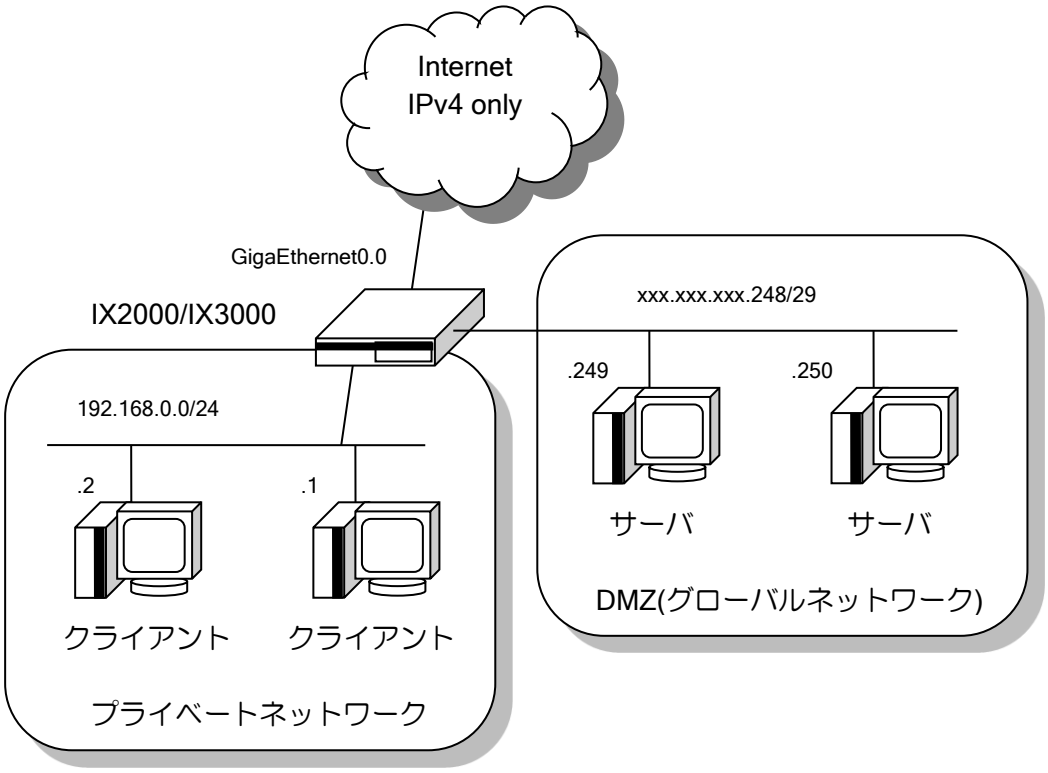
- ip napt address <インタフェースアドレス>
- ip napt inside <any>

【設定例】

・端末を指定しない場合
```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  no shutdown
```

2.19.2.2 NAPT 範囲指定（DMZ の設定）

NAPT 配下の内部ネットワークをプライベートアドレス空間とグローバルアドレス空間に分けることができます。これは、例えば DMZ 上に公開サーバを設置するような場合に使用できます。



【設定例】
```
ip access-list napt-list1 permit ip src 192.168.0.0/24 dest any
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt inside list napt-list1
  no shutdown
```

この設定例では、napt-list1 に当てはまらないパケットは NAPT 変換対象外となります。ただし、NAPT アドレスに指定しているアドレス（ip napt address がない本設定ではインタフェースアドレス）は、常に NAPT の変換対象です。

この設定より、外から内への通信時も、napt-list1 で指定されていない IP アドレス宛ての場合は後述する静的 NAPT やサーバサービスの設定を行わなくともそのまま通信可能となり、ここでは DMZ へのアクセスが実現できます。napt-list1 で指定されている IP アドレス空間については NAPT 変換対象となるため、通常、外から内への通信は行えません。

※内側ネットワークは基本的にアクセスリストの src アドレスで指定します。
※必要な場合は dest アドレス、src ポート、dest ポート、プロトコルを指定することも可能ですが、ネットワークが複雑になるので注意して利用してください。また、これら以外のフィールドは設定しないでください。

2.19.2.3 NAPT 複数指定

1 つの I/F に複数の NAPT アドレスを設定することも可能です。

【設定例 1】
送信元が 10.10.10.0/24 の場合は NAPT アドレスに 10.0.0.2 を使用
送信元が 10.10.20.0/24 の場合は NAPT アドレスに 10.0.0.3 を使用
送信元がそれ以外の場合は、NAPT しない

```
ip access-list access-1 permit ip src 10.10.10.0/24 dest any
ip access-list access-2 permit ip src 10.10.20.0/24 dest any
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt address 10.0.0.2
  ip napt inside list access-1
  ip napt inside list access-2 outside 10.0.0.3
  no shutdown
```

【設定例 2】
送信元が 10.10.10.0/24 の場合は NAPT アドレスに 10.0.0.2 を使用
送信元が 10.10.20.0/24 の場合は NAPT アドレスに 10.0.0.3 を使用
送信元がそれ以外の場合は、NAPT アドレスに 10.0.0.1 のを使用

```
ip access-list access-1 permit ip src 10.10.10.0/24 dest any
ip access-list access-2 permit ip src 10.10.20.0/24 dest any
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt inside list access-1 outside 10.0.0.2
  ip napt inside list access-2 outside 10.0.0.3
  no shutdown
```

※ NAPT アドレスを複数設定する場合の注意
NAPT しない条件がある場合、設定例 1 のように、1 つを ip napt inside の outside 指定無しの設定にする必要があります（デフォルト動作の全アドレスをインタフェースのアドレスで変換する設定を無効化する必要があるため）。
それぞれのアクセスリストで許可されるアドレス範囲は重複しないよう設定してください。
なお、設定例 2 のケースは outside なしの inside list の設定は不要です。outside ありの設定を先に判定するため、範囲指定されなかった通信が 10.0.0.1 で変換されます。

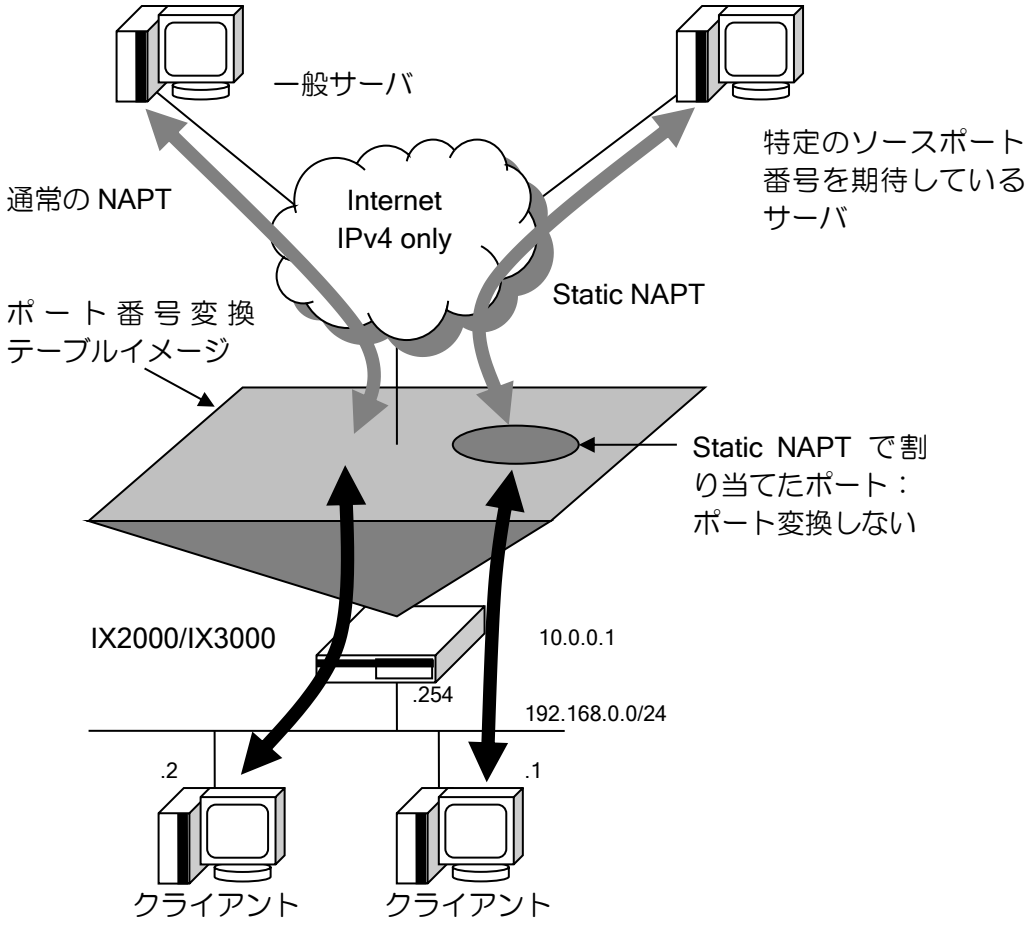
【設定例 3】
送信元が 10.10.10.0/24 の場合は NAPT アドレスに 10.0.0.2 を使用
送信元が 10.10.20.0/24 または自発パケットの場合は NAPT アドレスに 10.0.0.1 を使用
送信元がそれ以外の場合は、NAPT しない

```
ip access-list access-1 permit ip src 10.10.10.0/24 dest any
ip access-list access-2 permit ip src 10.10.20.0/24 dest any
ip access-list access-2 permit ip src 10.0.0.1/24 dest any

interface GigaEthernet0.0
   ip address 10.0.0.1/24
   ip napt enable
   ip napt address 10.0.0.2
   ip napt inside list access-1
   ip napt inside list access-2 outside 10.0.0.1
   no shutdown
```

※ outside アドレスに物理アドレスを指定する場合の注意
設定例 3 のように、outside アドレスと物理アドレスを同じにする場合、
outside の inside list のアクセスリストに物理アドレス(設定例では 10.0.0.1)を含める必要があります。
アクセスリストに設定をしない場合、自発パケットは NAPT の変換対象になりません。

2.19.2.4 静的 NAPT（Static NAPT）の設定

静的 NAPT の設定では、NAPT アドレスで使用するプロトコル、ポート番号を特定の端末専用に割り当てることができます。



静的 NAPT の設定および確認は、NAPT 設定コマンドに加え、次のコマンドを使用します。

ip napt static	内部ネットワーク内の端末とポートの設定

【設定例】
TCP/UDP の場合

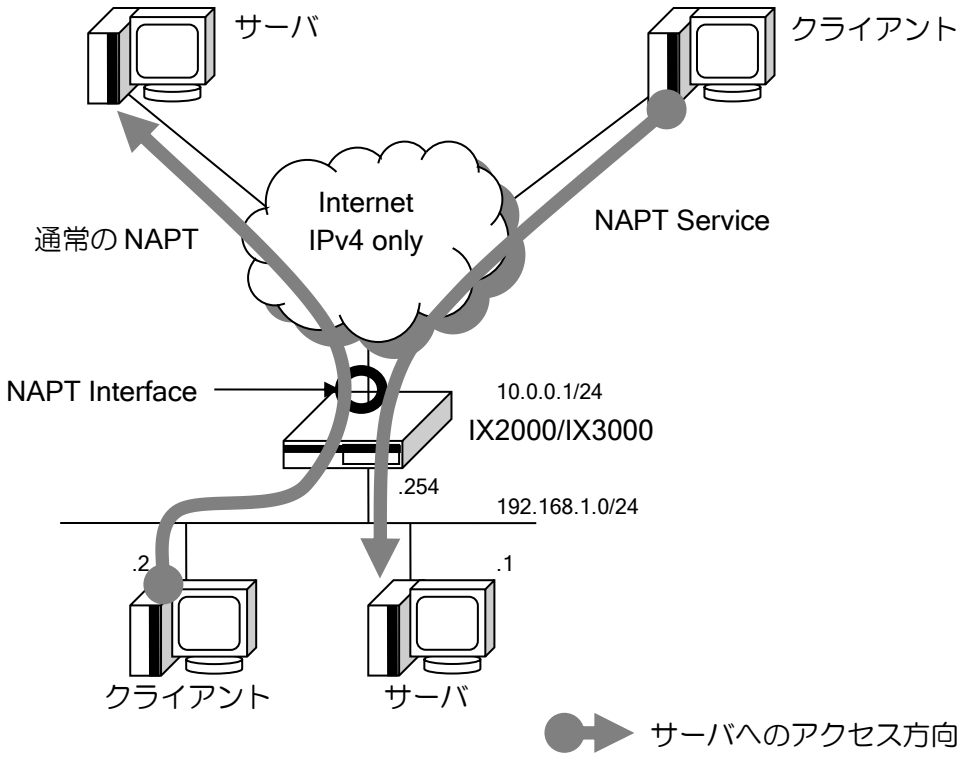
```
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   ip napt enable
   ip napt static 192.168.0.1 tcp 1000-1010
   no shutdown
```

TCP,UDP 以外のプロトコルの場合 （Ver.2 以降）

```
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   ip napt enable
   ip napt static 192.168.0.1 41
   no shutdown
```

2.19.2.5 サーバサービスの設定

サーバサービス設定は、プライベートアドレス空間にあるサーバに、グローバルアドレス空間にあるクライアントからアクセスするために使用します。



サーバサービス設定は、インタフェースコンフィグモードで、ip napt service コマンドを使用して設定します。サーバサービスの設定および確認は、NAPT 設定コマンドに加え、次のコマンドを使用します。

ip napt service	内部ネットワーク内のサーバとポートの設定

【設定例】

登録されているサービスの場合
```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt service telnet 192.168.1.1
  no shutdown
```

登録されていないサービスの場合
```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt service tftp 192.168.1.1 none udp 69
  no shutdown
```

2.19.2.6 NAPT キャッシュ数の制限の設定 - インタフェース単位での制限

NAPT キャッシュ数の制限の設定には、「インタフェース単位での制限」と「ホスト単位での制限」があります。

「インタフェース単位での制限」は、設定を行ったインタフェース上での NAPT キャッシュのエントリ数の上限値になります。エントリ数が上限値に達している状態で新たなパケットを受信しても通信は行えません。頻繁に NAPT キャッシュのオーバーフローが発生している場合は仕様範囲内で「インタフェース単位での制限」の値を増やすか、タイムアウトを調整してください。

【設定例】

```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt translation max-entries 16384
  no shutdown
```

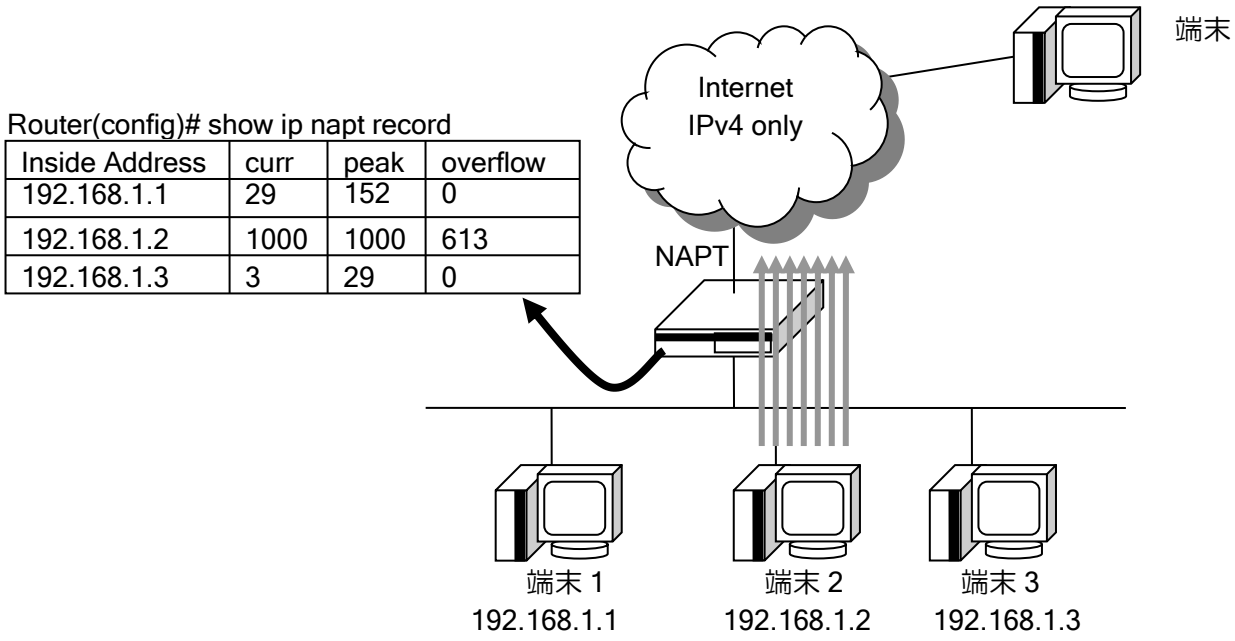
2.19.2.7 NAPT キャッシュ数の制限の設定 - ホスト単位での制限

「P2P アプリケーションの使用」「コンピュータウィルスの感染」などで一部のホストが大量に NAPT キャッシュを消費することが原因で、他のホストが通信できなくなってしまうことがあります。これを防ぐには NAPT キャッシュの「ホスト単位での制限」を行ってください。

【設定例】

```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt translation max-entries 16384
  ip napt translation max-entries per-address 1000
  no shutdown
```

本設定により、配下のホストごと(ープライベートアドレスごと)に生成可能な NAPT キャッシュ数が 1000 個となります。インタフェース全体としては 16384 個までの NAPT キャッシュを生成可能です。



Router(config)# show ip napt record

Inside Address	curr	peak	overflow
192.168.1.1	29	152	0
192.168.1.2	1000	1000	613
192.168.1.3	3	29	0

上図では、端末 2 は既に NAPT キャッシュを 1000 個生成しているため、オーバーフローが発生しています。その場合でも端末 1 と端末 3 は NAPT キャッシュを生成可能です。

2.19.2.8 ヘアピン NAT の設定

Ver9.3 以降は、ヘアピン NAT 機能を有効にすることで、同一プライベートネットワークの端末同士がグローバルアドレスを用いて通信することが可能です。

ip napt hairpinning	ヘアピン NAT の設定

【設定例】

```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt hairpinning
  no shutdown
```

本設定により、プライベートネットワークの端末から NAPT アドレス宛てに送信されたパケットに NAPT 変換を適用します。ヘアピン NAT を適用するパケットは TCP、UDP と ping のみです。

ヘアピン NAT は ip napt address コマンドで指定したアドレス宛のパケットにのみ適用します。ip napt address コマンドが未設定の場合、インタフェースのプライマリアドレスを使用します。インタフェースのアドレスがアンナンバード設定の場合も使用可能です。

ヘアピン NAT は 1 装置に 1 インタフェースのみ設定可能です。

注意事項

- ヘアピン NAT 機能では 1 回の変換あたり 2 つの NAPT キャッシュを生成します。
- 1 インタフェースに複数の NAPT を設定した環境でのヘアピン NAT はサポートしません。

2.19.2.9 NAPT 変換テーブルの保持時間

また NAPT の変換情報はトラフィックがなくなっても一定時間保持されます。保持時間を変更するコマンドは以下のとおりです。

ip napt translation	NAPT キャッシュ最大エントリ数，保持時間設定

保持時間のデフォルトと変更するパラメータは以下のとおりです。

- TCP　900 秒　[tcp-timeout]
- TCP セッション開始　30 秒　[syn-timeout]
  （Ver.8.5 以降設定可能）
- TCP セッション終了後
  （FIN または RST 片方向受信）60 秒　[finrst-timeout:第 1 パラメータ]
  （FIN または RST 双方向受信）1 秒　[finrst-timeout:第 2 パラメータ]
  （Ver.8.3.13 以降変更可能）
- UDP　300 秒　[udp-timeout]
- DNS　60 秒　[dns-timeout]
- ICMP　60 秒　[icmp-timeout]
- GRE　60 秒　[gre-timeout]
- その他　60 秒　[other-timeout]

2.19.3 対応アプリケーション

ペイロードにもプライベートアドレスが記載されているなど、特殊な接続を行う通信については、それぞれ専用の変換処理が必要になります。これらの機能をアプリケーション・レベル・ゲートウェイ（ALG）と呼びますが、NAT/NAPT で対応している ALG は以下になります。

- FTP(Ver9.3 以降は ip napt alg コマンドでポート番号を指定できます)
- TFTP
- ICMP（Ping の識別子の変換は Ver7.0 以降のサポートです）

それ以外の特殊なプロトコルに関しては対応していません。

- H.323
- FTP 以外でペイロードに IPv4 アドレス情報が含まれるプロトコルなど

その他のヘッダ変換だけでよいプロトコルは対応しています。

- telnet
- SSH
- SMTP
- POP3
- NTP
- HTTP 等

2.19.4 アクセスログ機能

NAPT 環境から外部ネットワークに対して不正アクセスが行われた場合、不正アクセスを行ったユーザを特定するために、NAPT の変換情報を記録するアクセスログ機能があります。

アクセスログ機能を有効にすることで、NAPT の変換ログを装置内に保存したり、syslog サーバに送信することができます。Ver9.2 以降で対応しています。

2.19.4.1 アクセスログ機能の設定

アクセスログ機能の設定は、次のコマンドを使用します。

ip napt access-log type ... size ...	アクセスログ機能を設定します。
ip napt access-log access-list	ログに記録する条件を設定します。

ip napt access-log type ... size ... コマンドで、アクセスログに記録する情報のタイプと、装置内の保存領域のサイズを設定します。

タイプには、normal と compact の 2 種類のタイプがあります。それぞれのタイプで記録される情報と、1 エントリのサイズは下記の通りです。

タイプ	記録される情報	サイズ
normal	送信元 IP アドレス / 送信元 MAC アドレス / プロトコル / NAPT 変換ポート / 送信先アドレス	24 byte
compact	送信元 IP アドレス / プロトコル / NAPT 変換ポート / 送信先アドレス	16 byte

装置内の保存領域のサイズは Mbyte 単位で設定します。なお、アクセスログが大量に発生する環境など、装置内の保存領域ではサイズが不十分な場合は syslog の利用をご検討ください。

アクセスログは NAPT 変換情報生成時(通信開始)と、情報削除時(通信終了)のそれぞれのログを記録します。なお、生成時のログがあれば、削除時のログがなくてもアドレス変換後の通信とアドレス変換前の通信を対応付けることは可能です。設定コマンドの末尾に「create-only」を指定することで、生成時のログのみを記録できます。

```
【設定例】
タイプ normal でサイズ 100Mbyte。生成と削除の両方を記録
ip napt access-log type normal size 100

タイプ compact でサイズ 32Mbyte。生成のみ記録
ip napt access-log type compact size 32 create-only
```

アクセスログ機能では、ip napt static、ip napt service の設定に合致するトラフィックは送信元アドレスを特定できるので、ログの記録対象になりません。

またアクセスリストにより、特定のトラフィックのみを記録することも可能です。

```
【設定例】
TCP の宛先ポート 80 と 443 の通信のみを記録（HTTP/HTTPS）
ip access-list napt-log permit tcp src any sport any dest any dport eq 80
ip access-list napt-log permit tcp src any sport any dest any dport eq 443
ip napt access-log access-list napt-log
```

2.19.4.2 アクセスログ機能の表示

アクセスログ機能の確認は、次のコマンドを使用します。

show ip napt access-log	アクセスログを表示します。

表示コマンドは日時指定が可能です。定期的にログを収集する場合に 1 日単位や 1 時間単位でログを表示させることができます。

```
【表示例】
日時指定なし
  show ip napt access-log
  保存されている全てのログを表示

年月日を指定
  show ip napt access-log datetime 2015 7 7
  2015/7/7 00:00:00～2015/7/7 23:59:59 のログを表示

年月日時を指定
  show ip napt access-log datetime 2015 7 7 17
  2015/7/7 17:00:00～2015/7/7 17:59:59 のログを表示

年月日時分を指定
  show ip napt access-log datetime 2015 7 7 17 50
  2015/7/7 17:50:00～2015/07/07 17:50:59 のログを表示
```

2.19.4.3 アクセスログの syslog 送信機能

Ver9.4 以降、アクセスログ送信コマンドを利用し、通信負荷の小さい時間帯に syslog を一定速度で送信することができます。また、Ver9.5 以降ではアクセスログだけを異なる syslog サーバに送信することも可能です（syslog ip host コマンドの match/unmatch コマンドを利用します）。

ip napt access-log send	アクセスログを syslog 送信します。
syslog ip host	送信先と送信内容を指定します。 （送信内容指定は Ver9.5 以降）

ip napt access-log send コマンドで、送信するアクセスログの送信周期および周期あたりの送信量を設定します。送信周期(interval)の単位はミリ秒[ms]で、周期あたりの送信量(count)は、1 周期毎に送信する送信パケット数です。送信の停止は no コマンドで行います。

```
【設定例】
毎日 AM8 時から 1 ログ/10ms の速度で 192.168.0.100 のサーバに送信。
他の syslog はイベント発生時に 192.168.0.101 に送信。

logging subsystem nat warn

syslog ip host 192.168.0.100 match nat-access-log
syslog ip host 192.168.0.101 unmatch nat-access-log
syslog timestamp datetime
syslog id hostname

ip napt access-log type normal size 32 create-only

command-action list send-syslog
  command 1 ip napt access-log send interval 10 count 1
scheduler timetable send-syslog datetime 8 0
```

2.19.4.4 注意事項

- アクセスログを時間帯をずらして送信する場合は、NAT のログレベルを warn または error にしてください。この方式では、syslog rate-limit（送信抑止機能）の影響を受けません。
- NAT のログレベルを notice, info, debug レベルに設定した場合は通常の syslog 送信になり、syslog rate-limit（送信抑止機能）の影響を受けます。利用する場合は送信抑止機能の無効化が必要です（no syslog rate-limit notice）。
- 送信中に送信コマンドを再実行することで、送信周期や送信量を変更できます。今回のみ早く終了させたい場合などに利用してください。送信中にコマンドを再実行しても、最初にコマンドを実行したときに保存されていたログまでしか送信しません。

2.19.4.5 送信履歴と動作確認

次のコマンドで履歴や動作状況の確認ができます。

show ip napt access-log send	送信履歴、動作情報を表示

本コマンドで最大 10 件の送信履歴を参照できます。また、送信中に実行することで、送信完了までの残り時刻を表示します。

なお、残り時刻は目安であり、装置負荷等により完了時刻が遅れる場合があります。

```
【表示例】
Router(config)# show ip napt access-log send
Current:
   2016/06/13 18:57:58 -
      Time remaining: 0:01:36, 330/850 messages

History:
   2016/06/13 17:22:00 - 2016/06/13 17:22:13,        1290 messages
   2016/06/12 17:22:00 - 2016/06/12 17:22:13,        1290 messages
```

2.19.5 パケット評価フロー

NAT、NAPT 機能は、処理の方向により以下の順番で処理します。

NAT と NAPT を併用した場合、NAT の設定が優先です。ただし NAT でも NAPT のキャッシュを生成することがあるので、キャッシュ処理は NAPT を優先します。

説明中、記述は省略しますが、NAT/NAPT 変換した場合は必ずキャッシュ生成も行います。

2.19.5.1 外部ネットワーク向きのパケット評価フロー

以下の順番に処理します。

1. キャッシュ処理
   1.1 NAPT キャッシュに該当する場合は、変換して終了
   1.2 NAT キャッシュに該当する場合は、変換して終了
2. NAT が有効の場合は 3、無効の場合は 4 へ
3. NAT 処理
   3.1 staticNAT に該当する場合は、変換して終了
   3.2 dynamicNAT に該当し変換できる場合は、変換して終了
   3.3 dynamicNAT に該当し変換できない場合は、廃棄して終了
4. NAPT が有効の場合は 5、無効の場合は 6 へ
5. NAPT 処理
   5.1 NAPT 対象の判定を行い（範囲指定がなければ全て対象）。対象外の場合は 6 へ
   5.2 staticNAPT に該当する場合は、変換して終了
   5.3 serviceNAPT に該当する場合は、変換して終了
   5.4 NAPT 変換できる場合は、変換して処理終了
   5.5 NAPT 変換できない場合は、廃棄して終了
6. 処理終了（パケット透過）

3.3 の「dynamicNAT に該当し変換できない場合」は、変換アドレスが枯渇した場合です。

5.5 の「NAPT 変換できない場合」は、通信が競合しポート変換が必要なときに変換ポートが枯渇している場合です。ポートが存在しないプロトコルで通信が競合した場合も変換できません。

2.19.5.2 内部ネットワーク向きのパケット評価フロー

以下の順番に処理します。

内部向きでは、static または service の設定がないと、外部から通信は開始できません。

1. キャッシュ処理
   1.1 NAPT キャッシュに該当する場合は、変換して終了
   1.2 NAT キャッシュに該当する場合は、変換して終了
2. NAT が有効の場合は 3、無効の場合は 4 へ
3. NAT 処理
   3.1 staticNAT に該当する場合は、変換して終了
4. NAPT が有効の場合は 5、無効の場合は 6 へ
5. NAPT 処理
   5.1 あて先が NAPT アドレスでも NAPT の内部アドレスでもない場合は 6 へ
   5.2 あて先が NAPT の内部アドレス宛ての場合は、廃棄して終了
   5.3 staticNAPT に該当する場合は、変換して終了
   5.4 serviceNAPT に該当する場合は、変換して終了
   5.5 例外として、内部向けのトンネルパケット（IPsec 等）は透過します。
6. 処理終了（パケット透過）

2.19.6 MAP-E(動的 IP アドレス)トンネルでの NAPT 動作モードについて

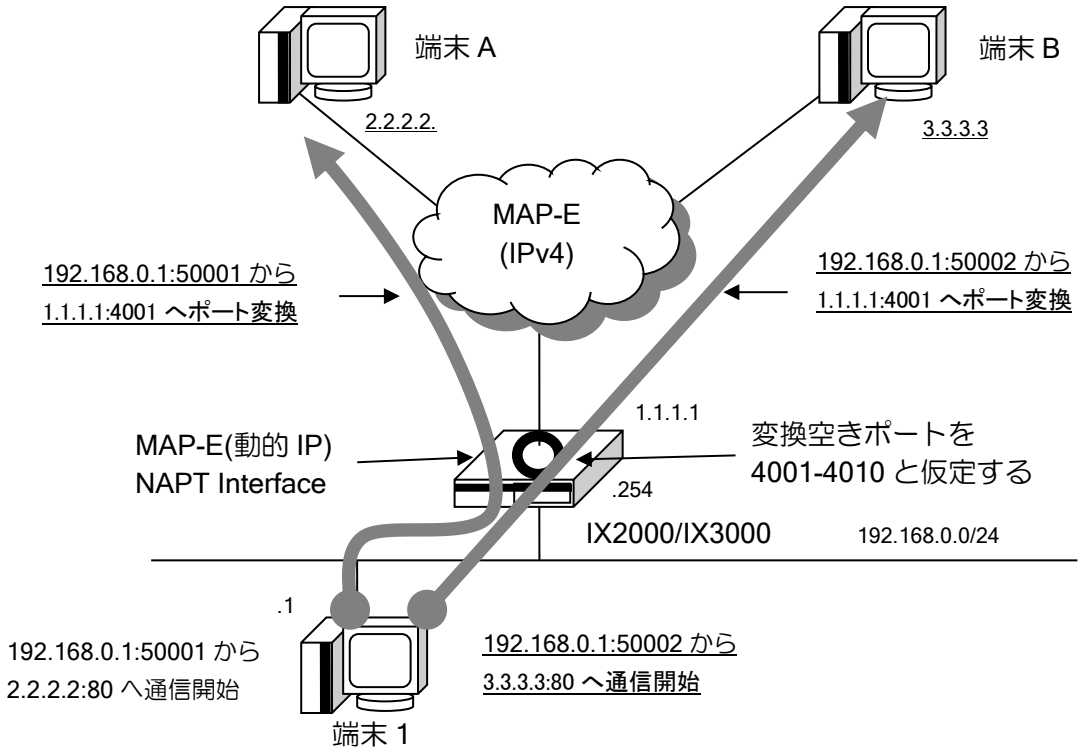
MAP-E(動的 IP アドレス)サービスでは、他の IPv4 インターネット接続と比べて、
サービスの仕様上ルータが使用できる変換ポート数が制限されています。

そのため、IX2000/IX3000 シリーズでは、MAP-E(動的 IP アドレス)で動作するトンネルインタフェースであっても多くの NAPT セッションを確立できるよう、NAPT のポート変換ルールを変更しています。

なお、このポート変換ルールは MAP-E(固定 IP アドレス)トンネルや、MAP-E でないインタフェースでは適用されません。

2.19.6.1 変換ルール

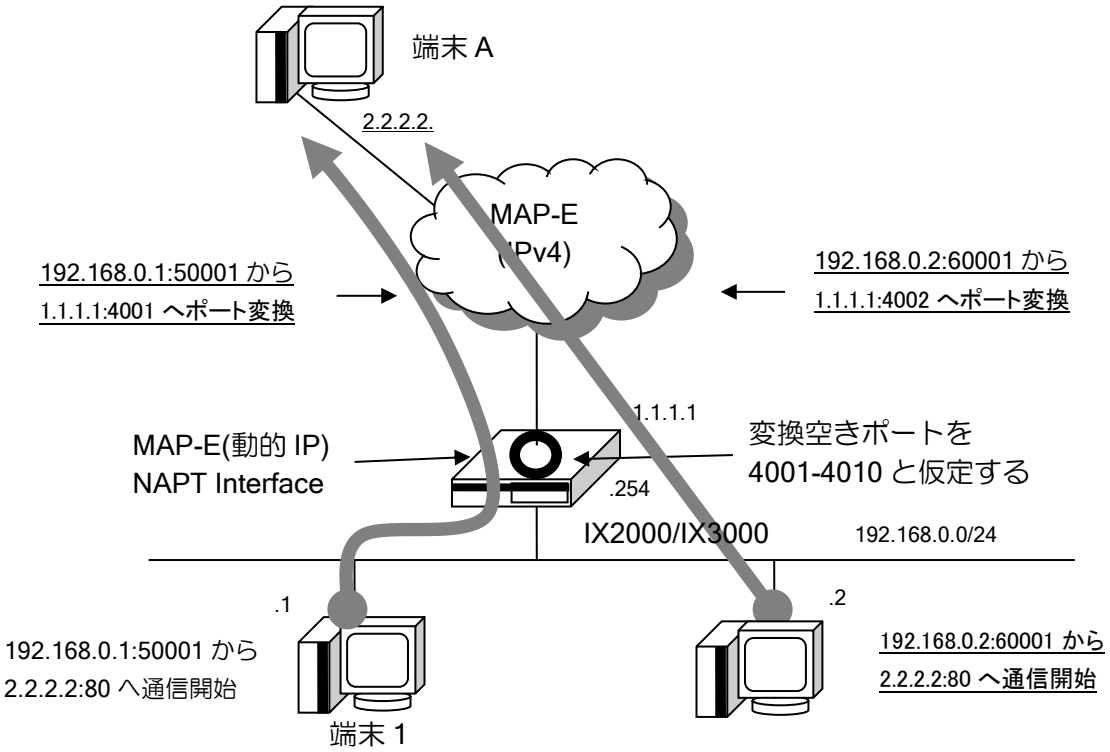
MAP-E(動的 IP アドレス)トンネルインタフェースでの NAPT ポート変換ルールを
以下のように行います。



端末 1 から端末 A に通信する際、端末 1 は 192.168.0.1、送信元ポート番号 50001 番
(以降、192.168.0.1:50001 と表記)から端末 A(2.2.2.2:80)へ通信を行うものとします。
このとき NAPT インタフェースは、変換空きポートの先頭、ここでは 4001 番を使用して
ポート変換を行います。
インターネット側の通信は、1.1.1.1:4001(IX2000/3000)と 2.2.2.2:80(端末 A)の通信となります。

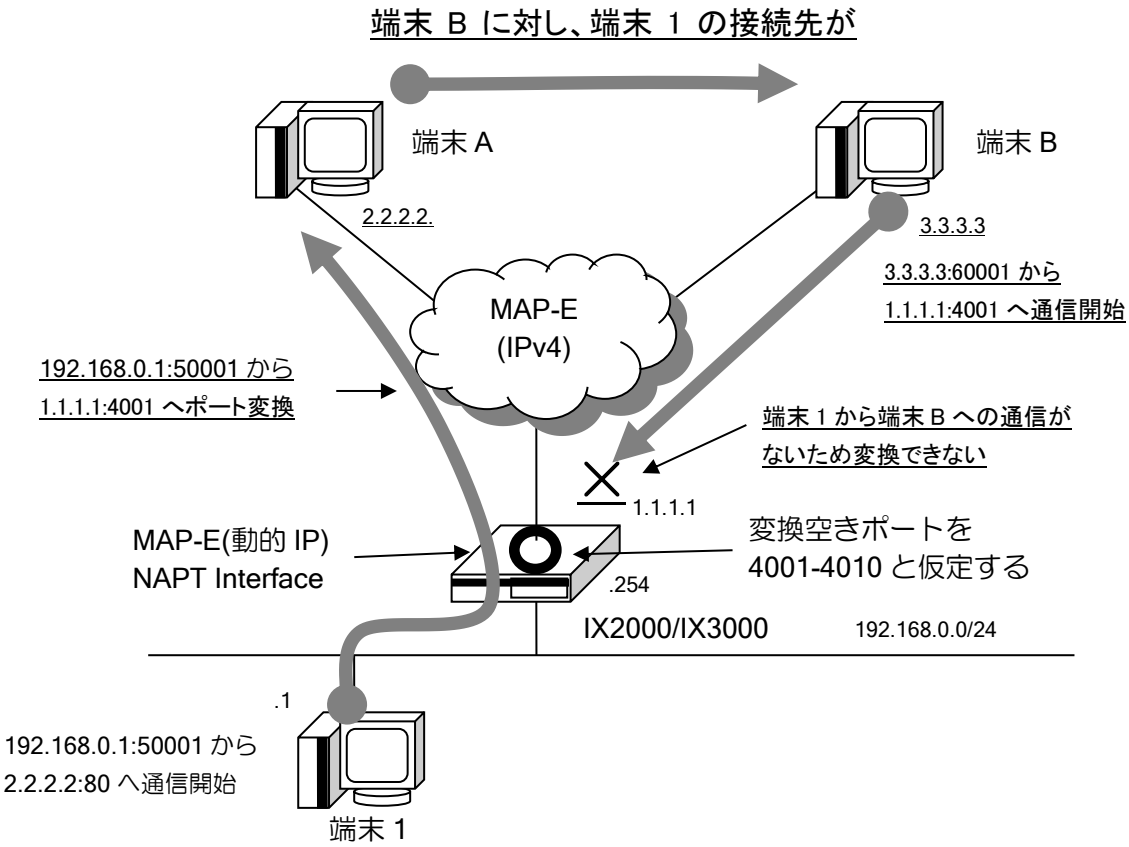
また、同時に端末 1 から端末 B に通信する際、端末 1 は 192.168.0.1:50002 から端末 B
(3.3.3.3:80)へ通信を行うものとします。
このとき NAPT インタフェースでは、他に端末 B(3.3.3.3:80)へポート変換している NAPT セッションが存在しない場合は、同様に変換ポートとして 4001 番を使用してポート変換を行います。
インターネット側の通信は、1.1.1.1:4001(IX2000/3000)と 3.3.3.3:80(端末 B)の通信となります。

上記のように、通信先の IP アドレスおよびポート番号が異なっているセッション同士の場合は IX2000/IX3000 では同一のポート番号にポート変換を行います。
これにより、サービス側で変換ポート数が制限されている MAP-E(動的 IP アドレス)でも
変換ポート数以上の NAPT セッションを確立することができます。



一方、複数のセッションを同一端末 A(IP アドレス・ポート番号)へ確立した場合は、
先に通信を開始した端末 1 から端末 A への通信のポート変換は 4001 番で行いますが、
後から通信を開始した端末 2 から端末 A への通信のポート変換は、次の空きポートである
4002 番で行います。
インターネット側からの通信に対して NAPT インタフェースでポート変換前の IP アドレス•ポート番号への変換は、インターネット側の変換後 IP アドレス・ポート(Outside)と接続先アドレス(Dest)の組から変換を行っているため、これらの 2 つが装置内で一意である必要があり、接続先アドレス(Dest)が同一の場合は上記のように異なるポート番号でポート変換を行っています。

ただし、MAP-E(動的 IP アドレス)インタフェースで行っているポート変換ルールの場合、
以下のような P2P 通信などで発生するポートパンチングを行う通信ができません。
このような通信が発生する環境では、EIM モード NAPT をご利用ください。



インターネット側からの通信に対する NAPT はインターネット側の変換後 IP アドレス・ポート(Outside)と接続先アドレス(Dest)の組から変換を行いますが、端末 1 は端末 B に対して通信を開始していないため、該当の変換情報(NAPT キャッシュ)が存在せず、端末 B からの通信をポート変換することができません。

2.19.6.2 EIM モード NAPT

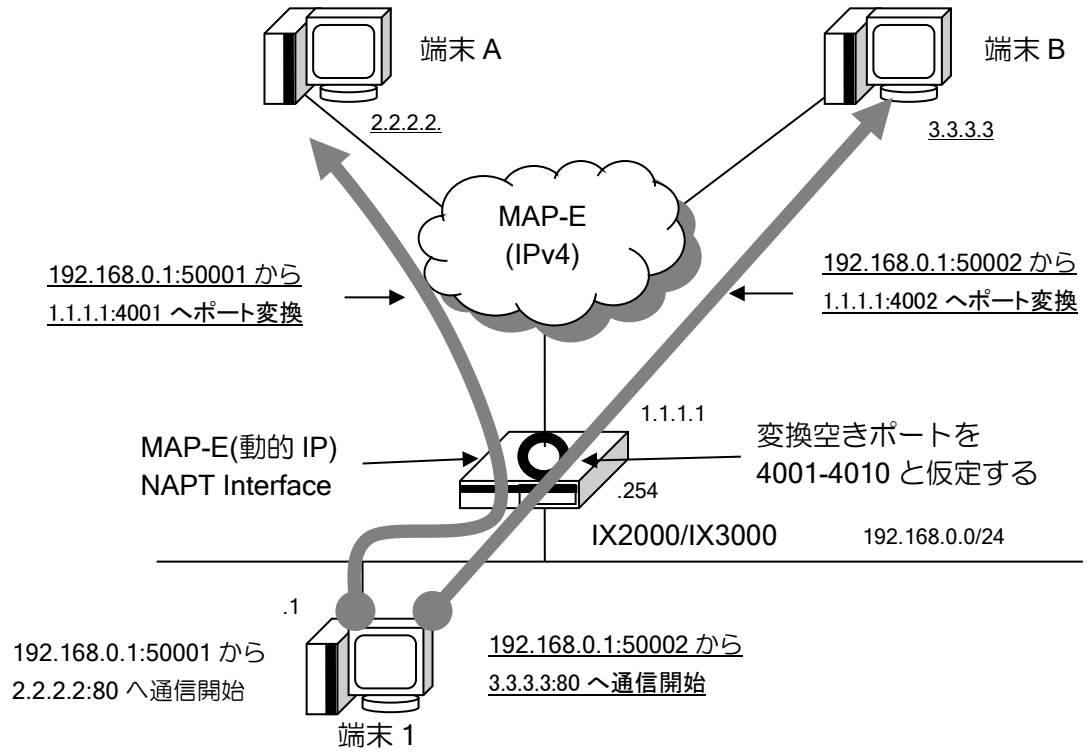
MAP-E(動的 IP アドレス)での NAPT 変換ルールの場合、上記のとおり P2P 通信などで影響が発生する場合があります。

この場合、EIM(Endpoint independent Mapping)モード NAPT を使用することでポートパンチングを行う通信が可能になります。

EIM モード NAPT は Ver10.2 以降ご利用いただけます。

以下に動作概要を説明します。

ip napt eim-mode	EIM モード NAPT の有効化設定



EIM モード NAPT の場合は、インターネット側からの通信に対して NAPT インタフェースでポート変換前の IP アドレス・ポート番号への変換は、変換前 IP アドレス・ポート(Inside)と変換後 IP アドレス・ポート(Outside)と接続先アドレス(Dest)の組から変換を行います。

つまり、接続先(Dest)に関係なく NAPT 変換前側の通信が発生すると、その通信に対応したポート番号を 1 つ消費します。

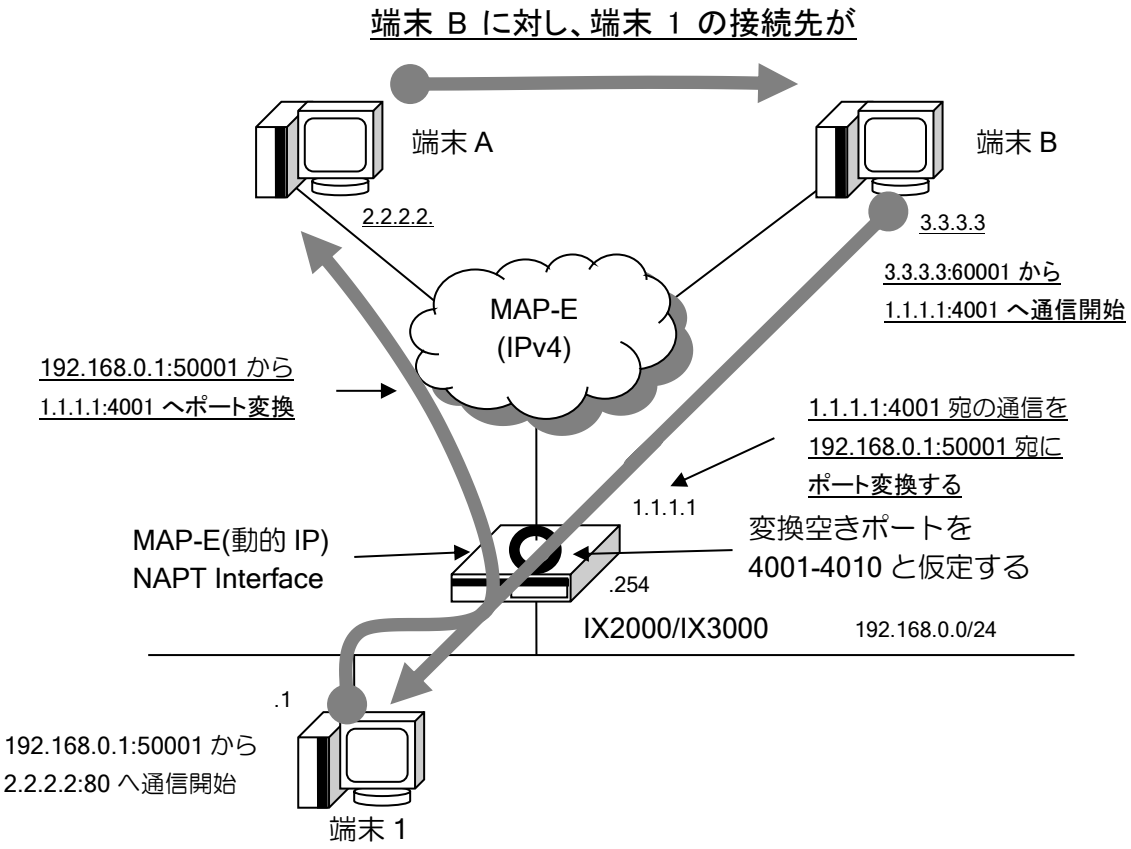
ただし、同じ変換前 IP アドレス・ポート(Inside)から異なる接続先(Dest)への通信は
同じポート番号で変換を行います。(Endpoint independent Mapping)

また、EIM モード NAPT はインターネット側からの通信に対して変換後 IP アドレス・ポート(Outside)のみを使用して、変換前 IP アドレス・ポート(Inside)へ変換を行うため、
EIF(Endpoint Independent Filtering)となります。

EIM モード NAPT は変換前アドレス・ポートからの通信ごとに 1 つのポート番号を消費するため、MAP-E(動的 IP)インタフェースで使用する場合は基本的にセッション数の上限は TCP・UDP でそれぞれサービスで定められた使用可能ポート数と同等になります。

なお、Ver10.2.26 以降、UDP のみ EIM モード NAPT を動作させることができます。

EIM モード NAPT によるポートパンチングを行う通信での IX2000/IX3000 の
動作は以下のようになります。



端末 B は 1.1.1.1:4001 宛に通信を行います。このとき、NAPT インタフェースでは
端末 A との通信開始時に 192.168.0.1:50001 からの通信で変換ポート 4001 番を
割り当てているため、EIF 動作により、1.1.1.1:4001 宛の通信は対向の端末に関係なくすべて
端末 1(192.168.0.1:50001)にポート変換されます。
これにより端末 B から端末 1 への通信を開始することができます。

2.19.6.3 EIM モード NAPT の注意事項

- EIM モード NAPT は外部からの通信に対して透過性の高い NAPT となっていますので、必要に応じて端末へのセキュリティ対策を推奨いたします。
- IPv4 ダイナミックフィルタを併用した場合、ダイナミックフィルタは EIF の動作に対応しておりませんので、NAPT インタフェース外からの通信は廃棄されます。

■2.20 IPv6 の設定

物理リンクレイヤと、IPv6 レイヤの関係は論理的に以下の構造をとっています。

IPv6 レイヤ
インタフェース（GigaEthernet0.0 etc.）
デバイス（GigaEthernet0 etc.）

以下に設定手順を示します。

- ipv6 enable コマンドによる有効化設定
- IPv6 アドレスの設定
- RA の設定（必要に応じて）
- ルーティング制御の設定

2.20.1 IPv6 の有効設定

IPv6 を使用する場合には、インタフェースで次のコマンドを設定します。

ipv6 enable	IPv6 の有効

このコマンドを設定すると IPv6 のリンクローカルアドレスが動作します。
インタフェースにグローバルアドレスを付与した場合は、enable 設定は省略可能です。

有効/無効 アドレス状態	ipv6 enable	no ipv6 enable
リンクローカルアドレス以外のアドレス付与	付与したアドレスは動作	付与したアドレスは動作
	リンクローカルアドレスは動作	リンクローカルアドレスは動作
リンクローカルアドレス以外のアドレス無し	リンクローカルアドレスは動作	リンクローカルアドレスは動作せず

IPv6 アドレスを unnumbered 指定した場合、unnumbered 指定している先の IPv6 アドレスをどのように設定していても、該当のインタフェースにて ipv6 enable 指定しなければ、そのインタフェースのアドレスは有効になりません。

また、ipv6 unnumbered 設定は、ブロードキャストネットワークのインタフェース上では設定できません。

Loopback インタフェースでは IPv6 は常に有効に設定されております。したがって Loopback インタフェースでは、ipv6 enable コマンドを実行することはできません。

また、Null インタフェースでも IPv6 は常に有効です。RIPng 等のアドレス集約に使用されます。

2.20.2 IPv6 アドレスの設定

IPv6 アドレスを設定するコマンドは次のとおりです。

ipv6 address	IPv6 アドレスの設定
ipv6 interface-identifier	インタフェース ID の設定

直接アドレスを記載する方法、EUI-64 形式で登録する方法、RA で自動設定する方法、DHCPv6-PD で設定する方法があります。
リンクローカルアドレスはインタフェース ID から生成するため、インタフェース ID を変更するとリンクローカルアドレスと、EUI-64 形式で登録したグローバルアドレスを変更します。

【設定例】

（1）直接指定
ipv6 address 2001:db8::1/64

（2）EUI-64 形式で指定（リンクローカルアドレスも末尾 64bit を::1 で揃える例）
ipv6 interface-identifier 0:0:0:0:0:0:0:1
ipv6 address 2001:db8::/64 eui-64 （EUI-64 形式）

（3）RA 受信でアドレス自動設定（Ver8.1 以降）
ipv6 address autoconfig receive-default

（4）DHCPv6-PD で自動設定（Ver6.2 以降）
DHCPv6 の章を参照してください。

インタフェース ID の変更は、インタフェースにアドレスが付与された状態でも可能ですが、アドレスが変更になるので注意してください。インタフェース ID の手動設定は、アドレスの競合に注意してください。

RA 受信でアドレスを設定する場合は、以下の制限があります。

- 1 つのルータからのみ RA 受信が可能です。複数のルータから RA を受信している場合は後から受信した RA の情報が上書きされます。
- 1 つの RA に複数のプレフィックスが設定されている場合
  - Ver.10.2 以前では、最初の有効なプレフィックスが付与されます。
  - Ver.10.3 以降では、Preferred Lifetime が 0 ではない設定済みグローバルアドレスと同一のプレフィックスが付与されます。グローバルアドレスが未設定の場合、Preferred Lifetime が 0 ではないプレフィックスを優先的に付与します。
- アドレスの LifeTime の管理は行いません。RA を受信しない状態で LifeTime が経過してもアドレスは無効にはなりません。

Ver9.7 以降、RA を送信する装置をネクストホップとして、スタティックルートを登録できます。

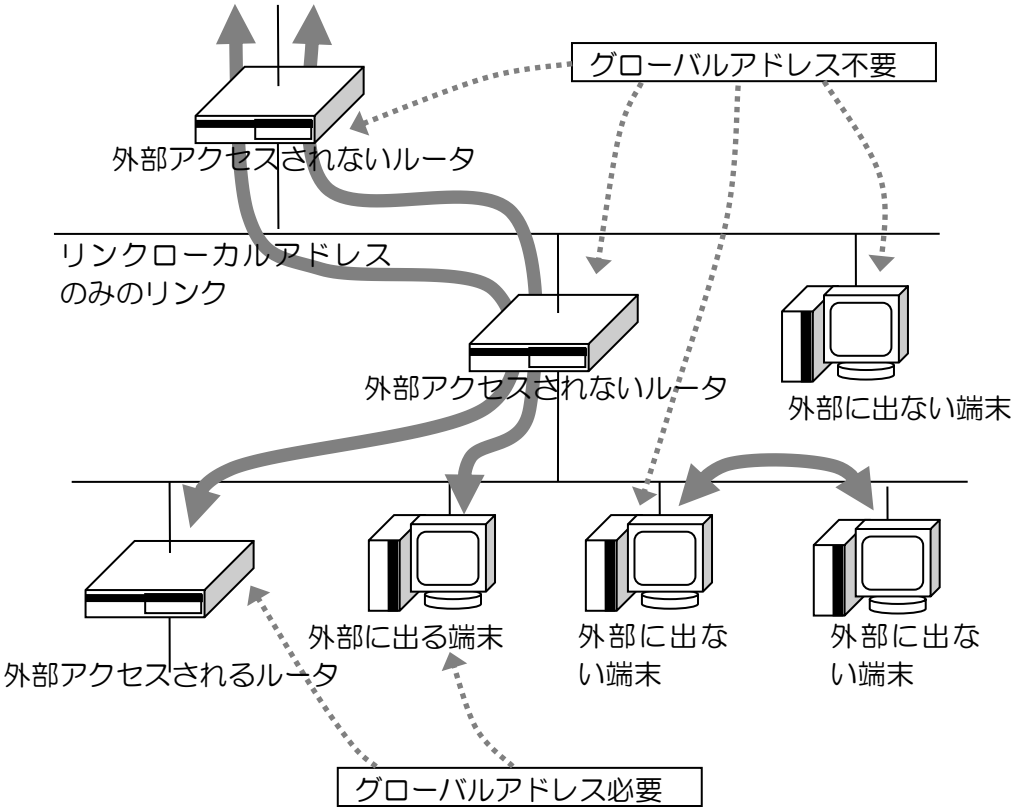
【設定例】

```
ipv6 route 2001:db8::/64 GigaEthernet0.0 ra
interface GigaEthernet0.0
  ipv6 address autoconfig
  no shutdown
```

2.20.3 リンクローカルアドレスの補足

IPv6 ではリンクローカルアドレスが必ず付与され、リンク内の通信が可能です。パケットを中継するだけならグローバルアドレスを付与する必要はありません。

ただし、外部（同一リンク以外）からルータの制御監視等を行う場合は、ルータのいずれかのインタフェースにグローバルアドレスが付与されている必要があります。



2.20.4 MTU の変更

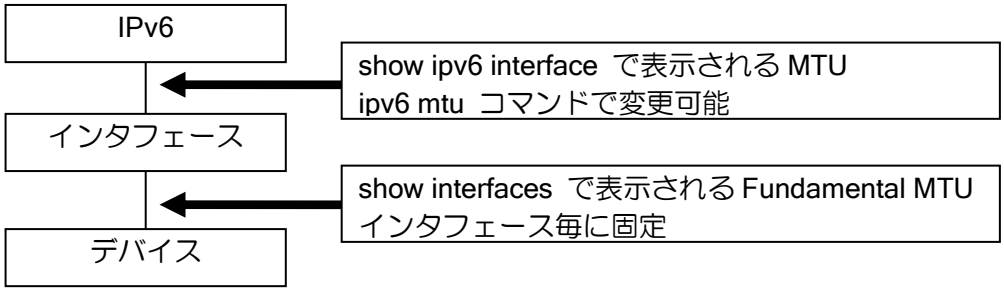
IPv6 で MTU 値をインタフェースの MTU より小さい値に変更するコマンドは次のとおりです。

ipv6 mtu	MTU の変更

【設定例】

```
ipv6 mtu 1280
```

インタフェースの MTU と IPv6 の MTU の関係は次のようになります。



2.20.5 TCP MSS 調整

TCP パケットの MSS（Maximum Segment Size）値を変更するコマンドは次の通りです。Path MTU 探索ができないネットワークで、TCP パケットのフラグメントによる性能低下を防止します。

インタフェースコンフィグモード	
ipv6 tcp adjust-mss	MSS の調整
bridge ipv6 tcp adjust-mss	ブリッジインタフェースでの MSS の調整

```
【設定例】

ipv6 tcp adjust-mss 1360
```

設定は、最も MTU が小さいインタフェースで設定してください（トンネルインタフェースを通過する場合は、トンネルインタフェースで設定）。

"ipv6 tcp adjust-mss auto"を設定すると、インタフェースの MTU に応じた値が自動的に設定されます。手動で MSS 調整値を計算する場合、以下の計算式を参考にしてください(IPsec、トンネルモード、ESP のみ使用時)。

【計算式】
X = 出力インタフェース MTU - A - B - C - D
A：認証データ　MD5/SHA1(12byte)
SHA256(16byte)
SHA384(24byte)
SHA512(32byte)
B：IV(Initialization Vector)　DES/3DES(8byte)、AES(16byte)
C：ESP ヘッダ(8byte)
D：IPv6 ヘッダ(40byte)

トンネルインタフェース MTU = (X / E の整数部) x E - F
E：DES/3DES 8、AES 16
F：パディング長(1byte) + 次ヘッダ番号(1byte)

MSS 調整値 = トンネルインタフェース MTU - G
G：IPv6 ヘッダ(40byte) + TCP ヘッダ(20byte)

※EtherIP の場合、ここからさらに EtherIP ヘッダ(2byte)、Ether ヘッダ(14byte)、合わせて 16byte を引いた値が適切な MSS 値となります。

【計算例】

出力回線がフレッツ ADSL/B フレッツ(MTU=1454)で、トンネルモードで 3DES/SHA1 使用時。

X = 1454 - 12(SHA1) - 8(3DES の IV) - 8(ESP ヘッダ) - 40(IPv6 ヘッダ) = 1386
トンネルインタフェース MTU = (1386 / 8 の整数部) x 8 - 2 = 1382
トンネルインタフェース MSS 調整値 = トンネルインタフェース MTU - 60 = 1322

以下の表は、上記の計算式を基にして各種設定での MSS 値を算出したものになります。

出力 I/F の MTU	EtherIP	IPsec	カプセル化モード	暗号、認証プロトコル	MSS 設定値
1500	あり	あり	トランスポート	DES/3DES + MD5/SHA1	1354
				AES + MD5/SHA1	1346
		なし	ー	ー	1384
	なし	あり	トランスポート	DES/3DES + MD5/SHA1	1410
				AES + MD5/SHA1	1402
			トンネル	DES/3DES + MD5/SHA1	1370
				AES + MD5/SHA1	1362
		なし	ー	ー	1440
1492 (PPPoE)	あり	あり	トランスポート	DES/3DES + MD5/SHA1	1346
				AES + MD5/SHA1	1338
		なし	ー	ー	1376
	なし	あり	トランスポート	DES/3DES + MD5/SHA1	1402
				AES + MD5/SHA1	1394
			トンネル	DES/3DES + MD5/SHA1	1362
				AES + MD5/SHA1	1354
		なし	ー	ー	1432
1454 (フレッツ ADSL/B フレッツ)	あり	あり	トランスポート	DES/3DES + MD5/SHA1	1306
				AES + MD5/SHA1	1298
		なし	ー	ー	1338
	なし	あり	トランスポート	DES/3DES + MD5/SHA1	1362
				AES + MD5/SHA1	1354
			トンネル	DES/3DES + MD5/SHA1	1322
				AES + MD5/SHA1	1314
		なし	ー	ー	1394

2.20.6 強制リアセンブリ

Ver.10.3 以降は以下のコマンドをインタフェースコンフィグモードで行うことで、IPv6 フラグメントパケットを一時的にリアセンブル状態とし、通常のパケットと同様にアクセスリストを適用することができます。

インタフェースコンフィグモード	
ipv6 forced-reassembly	IP フィルタにおける強制リアセンブリの有効化

本コマンドを設定したインタフェースで受信した IPv6 フラグメントパケットが対象となります。
送信時には元のサイズにフラグメントしますが、元のサイズが MTU を超えている場合はパケットを廃棄して ICMP エラー(Packet Too Big)を送信します。

2.20.7 RA の設定

リンクに端末が存在する場合、通常、RA を送信する必要があります。
RA のパラメータは特別な場合を除いて変更する必要はありませんので、必要に応じて変更してください。
Ver.8.3 以降、全ての RA 関連のコマンド名が変更になっているので、ご注意ください。Ver.8.2 以前から Ver.8.3 以降にバージョンアップしても、設定は引き継ぎます。

- Ver.8.3 以降

ipv6 nd ra enable	RA 送信の設定
ipv6 nd ra managed-config-flag	メッセージフラグ設定（M フラグ）
ipv6 nd ra other-config-flag	メッセージフラグ設定（O フラグ）
ipv6 nd ra prefix-advertisement	メッセージプレフィックスオプションの設定
ipv6 nd ra lifetime	ルータ生存時間の設定
ipv6 nd ra max-interval	送信間隔最大値の設定
ipv6 nd ra min-interval	送信間隔最小値の設定
ipv6 nd ra reachable-time	近隣ノード到達可能性時間の設定
ipv6 nd ra import-prefix	プレフィックスオプション自動生成の設定
ipv6 nd ra retrans-timer	再送タイマ設定
ipv6 nd ra cur-hoplimit	ホップリミット設定
ipv6 nd ra linkmtu	リンク MTU 設定
ipv6 nd ra dns-server	DNS サーバアドレス送信（Ver.10.0 以降）
ipv6 nd ra domain-name	DNS サーチリスト送信（Ver.10.0 以降）

- Ver.8.2 以前

ipv6 nd send-ra（Ver.5.2 以降） ipv6 nd ra-transmit（Ver5.1 以前）	RA 送信の設定
ipv6 nd managed-config-flag	メッセージフラグ設定（M フラグ）
ipv6 nd other-config-flag	メッセージフラグ設定（O フラグ）
ipv6 nd prefix-advertisement	メッセージプレフィックスオプションの設定
ipv6 nd ra-lifetime	ルータ生存時間の設定
ipv6 nd max-ra-interval	送信間隔最大値の設定
ipv6 nd min-ra-interval	送信間隔最小値の設定
ipv6 nd ra-reachable-time	近隣ノード到達可能性時間の設定
ipv6 nd import-prefix	プレフィックスオプション自動生成の設定

RA パラメータ

ルータ広告(RA)は、ルータがリンク上の端末に定期的に送信する情報で、ルータの所在およびリンクの各種情報を通知するものです。

端末は、RA を受信すると、リンクの各種情報をもとにアドレス生成等の各種自動設定を行うとともに、送信元ルータをデフォルトルータに設定します。

以下に、RA を用いた端末に対する自動設定の指示に関して具体的に説明します。コマンドに関しては、Ver.8.3 以降のコマンドで説明します。Ver.8.2 以前で設定を行う場合は、上記のコマンド一覧を参照してください。

M フラグと O フラグ

RA には、M フラグおよび O フラグの 2 つの重要なフラグが含まれており、この値を変更することにより、端末に対してのアドレスの自動設定方法を指示することが可能です。

M フラグは、Managed Address Configuration フラグのことで、アドレス自動設定をルータが広告したプレフィックスにより生成するステートレスで行うか、DHCPv6 等のプロトコルを使用したステートフルで行うかを指示するものです。

O フラグは、Other Stateful Configuration フラグのことで、アドレス以外の情報、たとえば DNS サーバのアドレス等を DHCPv6 等のプロトコルを使用して取得することを指示します。デフォルトでは、ステートレスアドレス自動設定（M=無効）、DHCPv6 等によるアドレス以外の情報取得なし（O=無効）です。IX2000/IX3000 では、M フラグを ipv6 nd ra managed-config-flag コマンド、O フラグを ipv6 nd ra other-config-flag コマンドにより変更することが可能です。

ipv6 nd ra managed-config-flag	ルータ通知メッセージフラグ設定（M フラグ）
ipv6 nd ra other-config-flag	ルータ通知メッセージフラグ設定（O フラグ）

たとえば、ステートレスアドレス自動設定と DHCPv6 によるアドレス以外の情報取得の指示を行う場合、次のように設定します。

```
no ipv6 nd ra managed-config-flag
no ipv6 nd ra other-config-flag
```

ルータからの通知情報を使用せず、完全にアドレスおよびその他情報の自動設定を DHCPv6 サーバに任せる場合は、次のように設定します。

```
ipv6 nd ra managed-config-flag
ipv6 nd ra other-config-flag
```

on-link フラグと autonomous フラグ

また、ステートレスアドレス自動設定等で使用するプレフィックス情報の中にも、on-link フラグおよび autonomous フラグの 2 つの重要なフラグが含まれており、この値を変更することにより、通知する個々のプレフィックスの使用を指定することが可能です。

on-link フラグは、通知するプレフィックスが同一リンクの決定に使用できるかどうかを指示するものです。端末は、on-link フラグで指定されたプレフィックスを持つ端末とはダイレクトで、off-link で指定されたプレフィックスを持つ端末とはルータ経由で通信を行うようになります。

autonomous フラグは、通知するプレフィックスがステートレスアドレス自動設定で使用可能かどうかを指示するものです。

デフォルトでは、on-link、ステートレスアドレス自動設定使用可能（autonomous=有効）です。

IX2000/IX3000 では、ipv6 address コマンドによりインタフェースに付与したアドレスのプレフィックス部分を通知するとともに、プレフィックス情報のオプションを ipv6 nd prefix-advertisement コマンドおよび ipv6 prefix コマンドにより変更することが可能です。

たとえば、インタフェースにプレフィックスが異なる 2 つのアドレスを付与し、一方のプレフィックスをステートレスアドレス自動設定の対象から除きたい場合、以下のように設定します。

ipv6 prefix	ルータ通知用プレフィックスの設定
ipv6 nd ra prefix-advertisement	ルータ通知メッセージプレフィックスオプションの設定

```
ipv6 prefix prefix-1 2001:db8:0:ffff::/64 on-link
interface GigaEthernet0.0
  ipv6 address 2001:db8:0:1::1/64
  ipv6 address 2001:db8:0:ffff::1/64
  ipv6 nd ra prefix-advertisement prefix-1
  no shutdown
```

なお、off-link のプレフィックス情報通知は、サイト内で使用しているプレフィックス（サイトプレフィックス）を端末に認識させる場合に使用します。

2.20.8 ND プロキシの設定

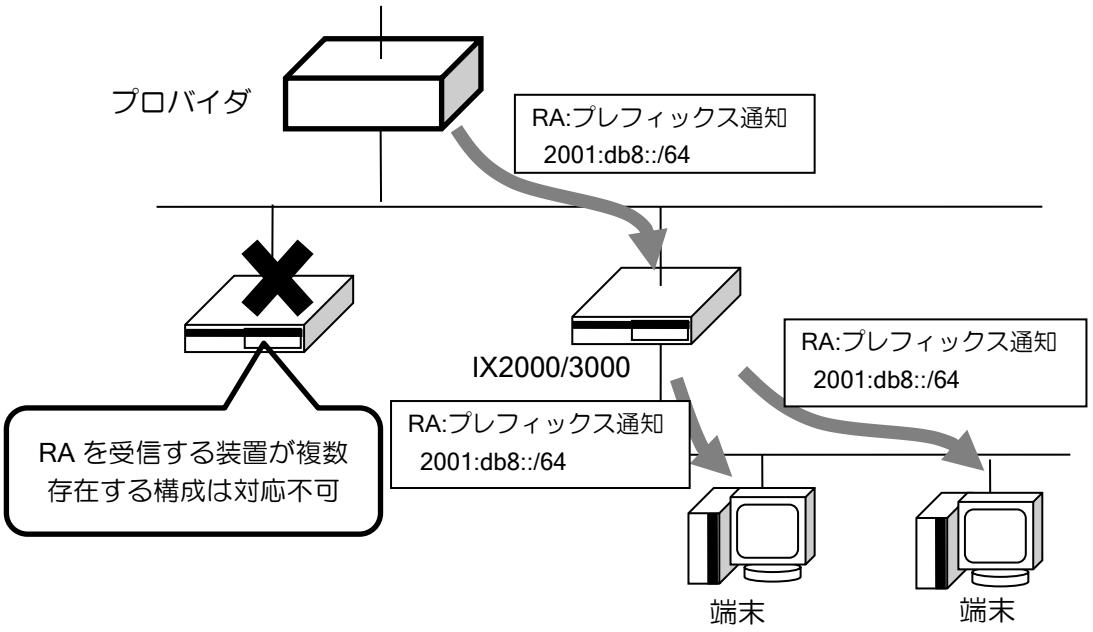
WAN 側から受信した RA にて通知されたプレフィックスを、LAN 側に RA により通知することができます。（Ver.10.0 以降）

ブリッジを使用することにより、同様な動作をさせることは可能ですが、ND プロキシを使用することによって、IX2000/3000 にて WAN 側へのブロードキャストやマルチキャストパケットの送信を抑止することができます。

Ver.10.3 以降、WAN 側と LAN 側でのアドレス重複の検知ができます。

Ver.10.3 以降、IX2000/IX3000 のプレフィックスが無効になった(削除された)場合、配下の端末にプレフィックス無効の RA を送信します。

RA を受信するルータは 1 台のみの構成で使用できます。ルータを複数設置する場合は DHCPv6-PD 機能を使用してください。



ND プロキシの設定は以下のとおりです。

ipv6 nd proxy	ND プロキシ設定 （インタフェースコンフィグモード）

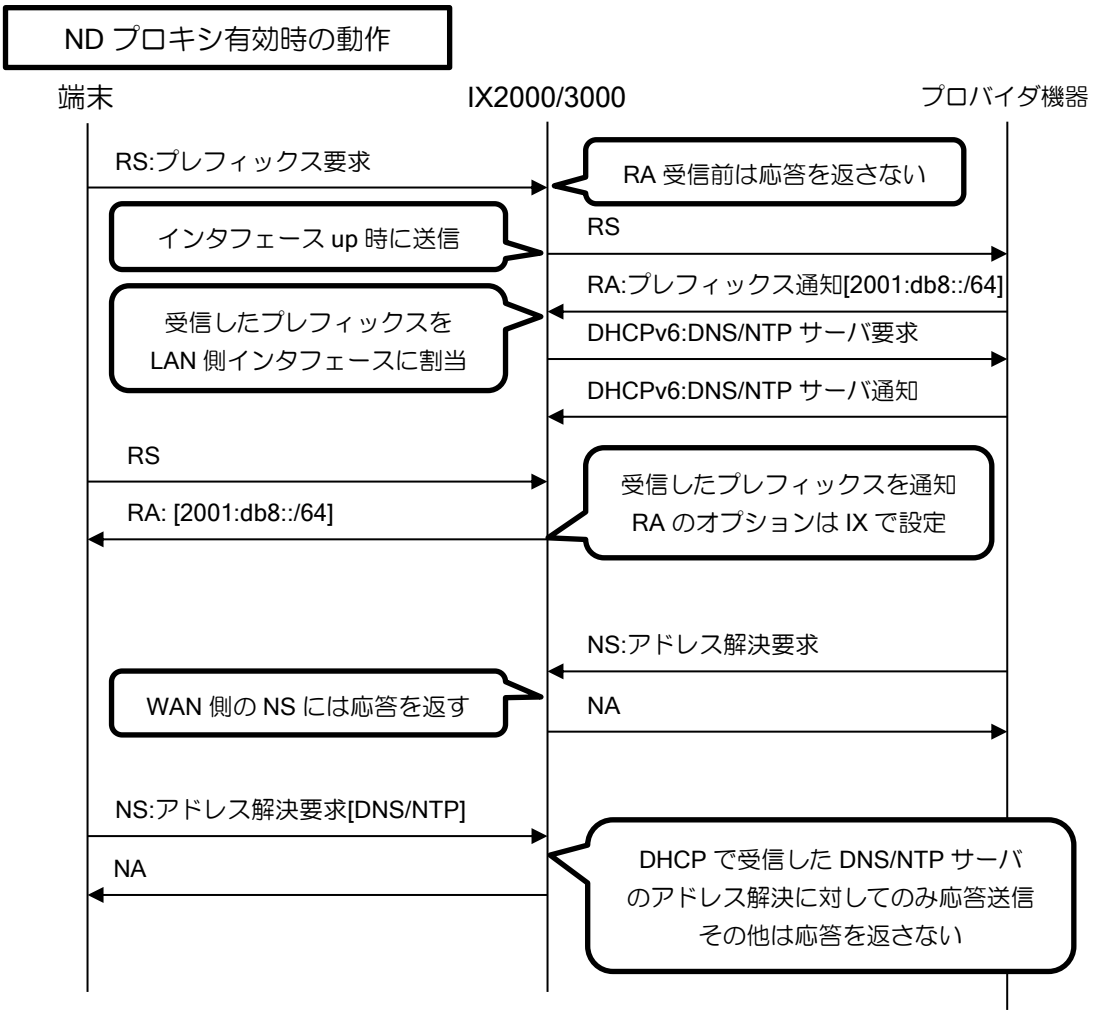
【設定例】
GigaEthernet0.0 から RA を受信し、GigaEthernet1.0 に RA を送信
DHCPv6 の Information にて DNS サーバ、NTP サーバのアドレスを受信

```
proxy-dns ipv6 enable

ipv6 dhcp client-profile dhcpv6-cl
   information-request
   option-request dns-servers
   option-request ntp-servers

interface GigaEthernet0.0
   ipv6 enable
   ipv6 dhcp client dhcpv6-cl
   ipv6 nd proxy GigaEthernet1.0
```

```
   no ipv6 redirects
   no shutdown

interface GigaEthernet1.0
   ipv6 enable
   ipv6 nd ra enable
   ipv6 nd ra dns-server fe80::260:11ff:fe11:1111
   no shutdown
```

ND プロキシは、1 インタフェースのみ設定可能です。

ND プロキシ有効時の動作は以下のようになります。
WAN 側インタフェース up 時にプレフィックス要求（RS）を送信します。プレフィックス通知（RA）受信時、RA を送信した装置を出力先としたデフォルトルートを設定し、受信したプレフィックスを LAN 側に割り当てます。RA 受信後は、LAN 側の端末からの RS に対して、受信したプレフィックスを通知します。



アクセスリストを設定することにより、特定ホストからの特定アドレスに対する要求のみ、アドレス解決要求（NS）に応答するように制限することができます。
アクセスリストは次のように比較を行います。

- 送信元アドレスと、アドレス要求（NS）の送信元アドレス
- 送信先アドレスと、アドレス要求（NS）で解決するアドレス（Target Address）

permit の場合は応答し、deny の場合は応答しません。

【設定例】
解決するアドレスが x:x:x:x::0～x:x:x:x::ff は応答を返さない

```
ipv6 access-list wan-hosts deny ip src any dest :: ffff:ffff:ffff:ffff::ff
ipv6 access-list wan-hosts permit ip src any dest any

interface GigaEthernet0.0
  ipv6 enable
  ipv6 nd proxy GigaEthernet1.0 wan-hosts
  no ipv6 redirects
  no shutdown

interface GigaEthernet1.0
  ipv6 enable
  ipv6 nd ra enable
  no shutdown
```

注意事項

- DHCP で配布された、DNS サーバ、NTP サーバを除き、WAN 側インタフェースのネットワーク内に設置した装置とは通信できません。次項のローカル ND プロキシを設定した場合、NS の応答を返すため、端末から WAN 側インタフェースのネットワーク宛のパケットは送信されますが、IX2000/3000 では WAN 側インタフェースに転送されないため、通信はできません。
- Ver.10.2 以前では WAN 側と LAN 側でのアドレス重複は検出できません。アドレスを固定設定する場合は同一アドレスにならないように注意してください。

2.20.9 ローカル ND プロキシの設定

ローカル ND プロキシ機能を有効にした場合、全ての IPv6 アドレスの NS に応答を返します。（Ver.10.0 以降）

ただし、以下の NS には応答を返しません。

- アドレス重複検出（送信元アドレスが未指定）の場合
- Target Address がマルチキャストの場合
- Target Address がリンクローカルアドレスの場合

アクセスリストを設定することにより、特定ホストからの特定アドレスに対する要求のみ、アドレス解決要求（NS）に応答するように制限することができます。
アクセスリストは次のように比較を行います。

- 送信元アドレスと、アドレス要求（NS）の送信元アドレス
- 送信先アドレスと、アドレス要求（NS）で解決するアドレス（Target Address）

設定は以下のとおりです。

ipv6 nd local-proxy	ローカル ND プロキシ設定 （インタフェースコンフィグモード）

【設定例】
2001:db8::100 からの NS のみ全ての NS に対して応答を返す。

```
ipv6 access-list lan-hosts permit ip src 2001:db8::100/32 dest any

interface GigaEthernet1.0
```

```
ipv6 enable
ipv6 address 2001:db8::1/64
ipv6 nd local-proxy lan-hosts
no shutdown
```

本機能が有効の場合、ICMP リダイレクトメッセージを送信しません。

注意事項

- ローカル ND プロキシ有効時は、全ての IP アドレスに応答を返します。他に NS の応答を返す装置がある場合、NS 送信元の装置にてアドレス解決が正しく行われない可能性があります。ネットワーク構成にはご注意ください。

2.20.10 ICMPv6 リダイレクトメッセージの送信制御設定

ブロードキャストネットワークにおいて、ICMPv6 REDIRECTS メッセージの送信を制御します。デフォルトでは、ICMPv6 REDIRECTS メッセージを送信しますので、REDIRECTS を送信したくない場合に、停止設定を行います。

ノンブロードキャストネットワーク（ポイントツーポイントネットワーク等）では、以下のコマンドは無視されます。

no ipv6 redirects	ICMP リダイレクトメッセージの送信停止設定 （インタフェースコンフィグモード）

```
【設定例】

interface GigaEthernet1.0
  ipv6 enable
  no ipv6 redirects
  no shutdown
```

2.20.11 サイトの設定

サイトローカルユニキャストアドレスは RFC4291 により非推奨となり、グローバルアドレスとして扱うことになりました。Ver.8.3 以降は RFC4291 準拠としているため、サイト関連の設定および Auto-tunnel インタフェースは削除しています。Ver8.2 以前でも利用しないでください。

以下に IX2000/IX3000 シリーズの Ver8.2 以前におけるサイトローカルスコープの取り扱いを説明します。

- インタフェースへのサイトローカルアドレスの付与（必要な場合）
  - ipv6 address コマンドによりサイトローカルアドレスを付与。サイトローカルスコープはデフォルトで、site1 に設定されます。
- RA によるサイトアドレス情報の広告設定（必要な場合）
  - ipv6 nd prefix-advertisement および ipv6 prefix コマンドにより、サイトアドレスの広告情報設定。
- サイトローカルスコープの設定
  - ipv6 scope-zone site-local コマンドにより、サイトローカルスコープを設定。デフォルトでは、site1 がスコープゾーンに設定されています。

■2.21 DHCPv6 の設定

IX2000/IX3000 シリーズでは、DHCPv6 の Prefix Delegation 機能をサポートしています。DHCPv6 Prefix Delegation 機能（以下 PD）を用いることにより、DHCPv6 PD クライアント（CPE）は DHCPv6 PD サーバ（PE）から IPv6 プレフィックスや DNS サーバアドレスを取得し、配下の端末へ自動的に IPv6 グローバルアドレスを割り振ることができます。

Ver.8.9 以降では、DHCPv6 の Prefix Delegation 再配布機能（以下 PD 再配布機能）を追加しています。PD 再配布機能を用いることにより、IX で取得した IPv6 プレフィックスを下位ネットワークの複数の CPE へ分割して配布することができます。

2.21.1 サポートメッセージ

IX2000/IX3000 シリーズでは、現在以下の DHCPv6 オプションをサポートしています。

- メッセージ
  - Solicit (1)
  - Advertise (2)
  - Request (3)
  - Renew (5)
  - Rebind (6)
  - Reply (7)
  - Reconfigure (10)
  - Information Request (11)

- オプション
  - Client Identifier (1)
  - Server Identifier (2)
  - Option Request Option (6)
  - Preference (7)
  - Elapsed Time (8)
  - Status Code (13)
  - Rapid Commit (14)
  - Reconfigure Message (19)
  - Reconfigure Accept (20)
  - Domain Name Servers (23)
  - IA PD (25)、IA Prefix (26)
  - NTP Servers (31)

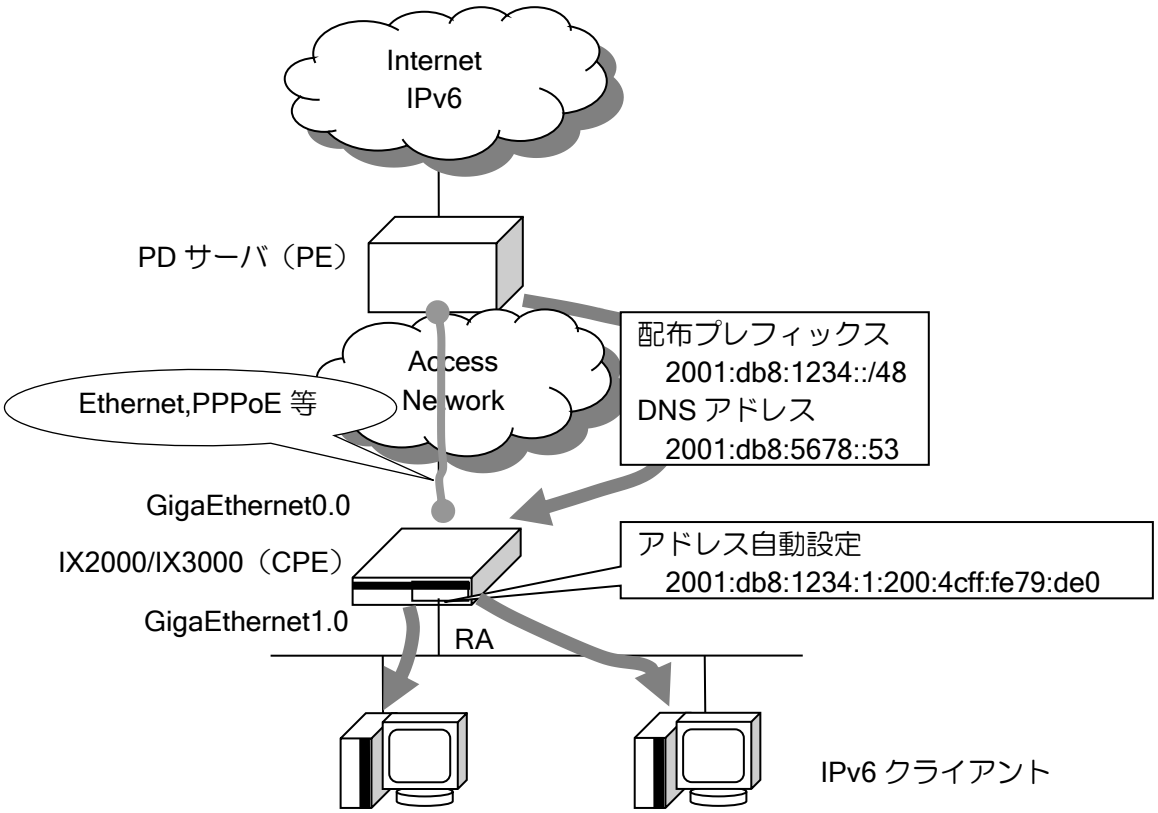
※Ver.8.7 以前は、特定サービス対応として Prefix Delegation(30), Prefix Information (31), NTP Servers (35)としておりましたが、サービス終了に伴いサポートを終了しています。Ver8.7 以前で NTP Servers を 31 としたい場合はオプション番号を変更して利用してください。

※Reconfigure(10)等で利用される認証オプションは未サポートです。

2.21.2 Prefix Delegation クライアントの設定

DHCPv6 Prefix Delegation クライアント機能（以下 PD）を用いることにより、DHCPv6 PD サーバ（PE）から IPv6 プレフィックスや DNS サーバアドレスを取得し、ルータ配下の端末へ自動的に IPv6 グローバルアドレスを割り振ることができます。

(a) PD によるアドレスの割り当て



IX2000/IX3000 シリーズでは、PD サーバ（PE）から配布されたプレフィックス情報を元に指定したインタフェースに対して、プレフィックスレングス 64 のアドレスを自動的に割り当てます。（指定により任意のプレフィックス長を割り当てることもできます。）

このインタフェースに RA を送信する設定が行われていた場合、アドレスが割り当てられたインタフェース配下の IPv6 クライアントに RA にてアドレスが自動設定されます。

ipv6 dhcp client	DHCPv6 クライアントの起動 （インタフェースコンフィグモード）
ipv6 dhcp client-profile	DHCPv6 クライアントコンフィグモードへの移行 （グローバルコンフィグモード）
ia-pd subscriber	アドレスを自動設定するインタフェース設定 （DHCPv6 クライアントコンフィグモード）
ia-option	IA オプションの設定 （DHCPv6 クライアントコンフィグモード）
show ipv6 dhcp client	DHCPv6 クライアントの状態表示

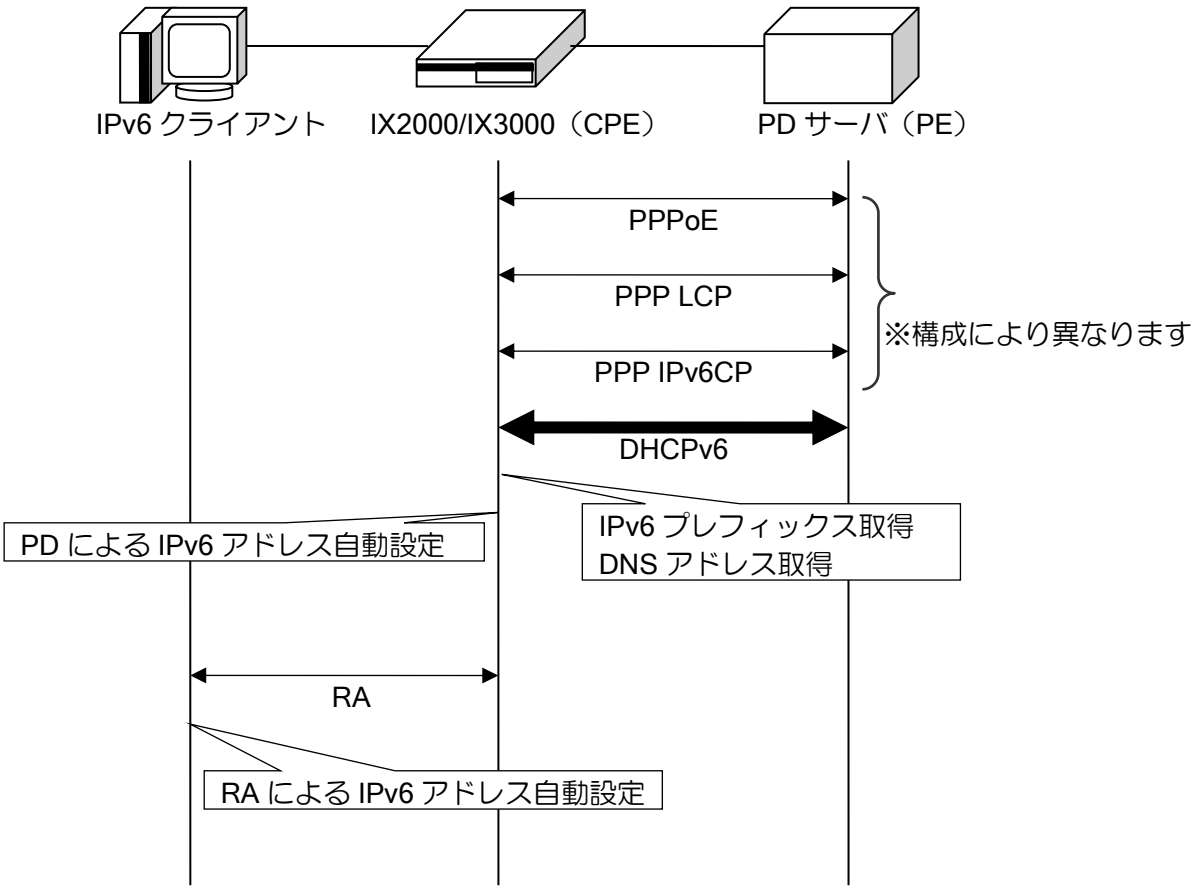
```
【設定例】
!
ipv6 dhcp client-profile pd6c
   ia-pd subscriber GigaEthernet1.0
   option-request dns-servers
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 dhcp client pd6c
   no shutdown
!
interface GigaEthernet1.0
   ipv6 enable
   ipv6 nd ra enable
   no shutdown
```

※Ver8.9 以降では、同一の DHCPv6 クライアントプロファイルを複数の" ipv6 dhcp client"コマンドで指定することはできません。

(b) PD 接続シーケンス

PD における、接続シーケンスを以下に示します。ここでは、PPPoE 上にて PD を利用した場合におけるシーケンスを例としています。

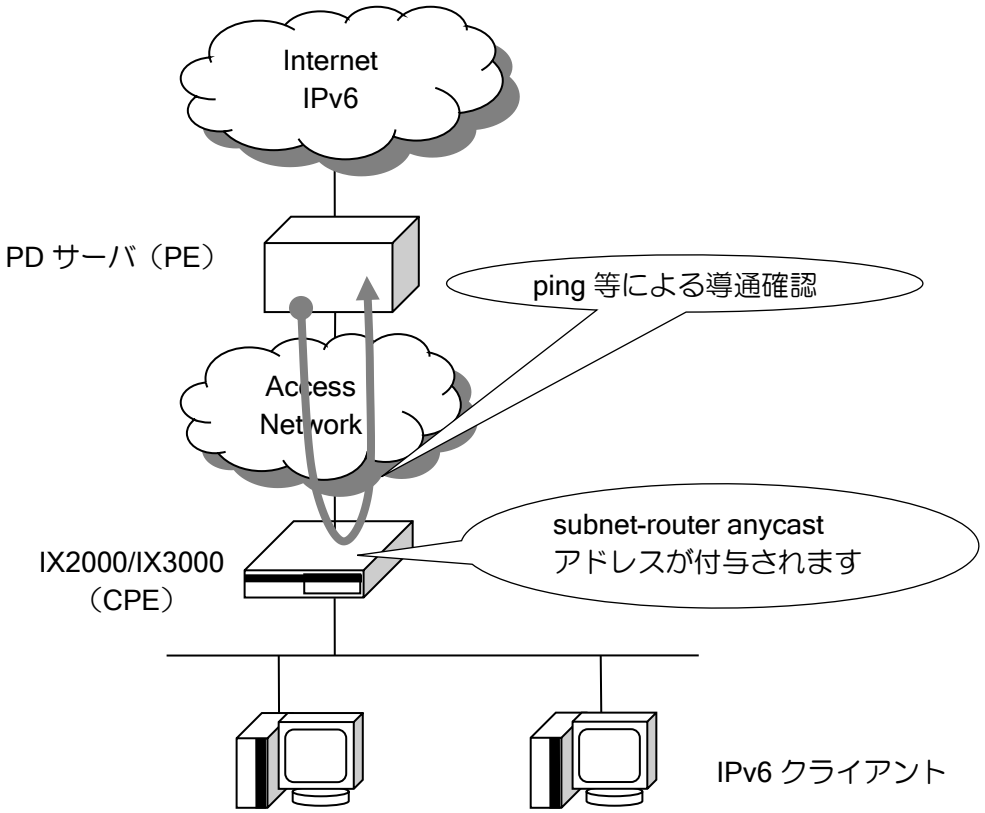
PD 以外のメッセージについての詳細は各該当項目を参照してください。



(c) PD ルータの導通確認

IX2000/IX3000 シリーズでは、PD サーバ等からの導通確認に応答することができます。

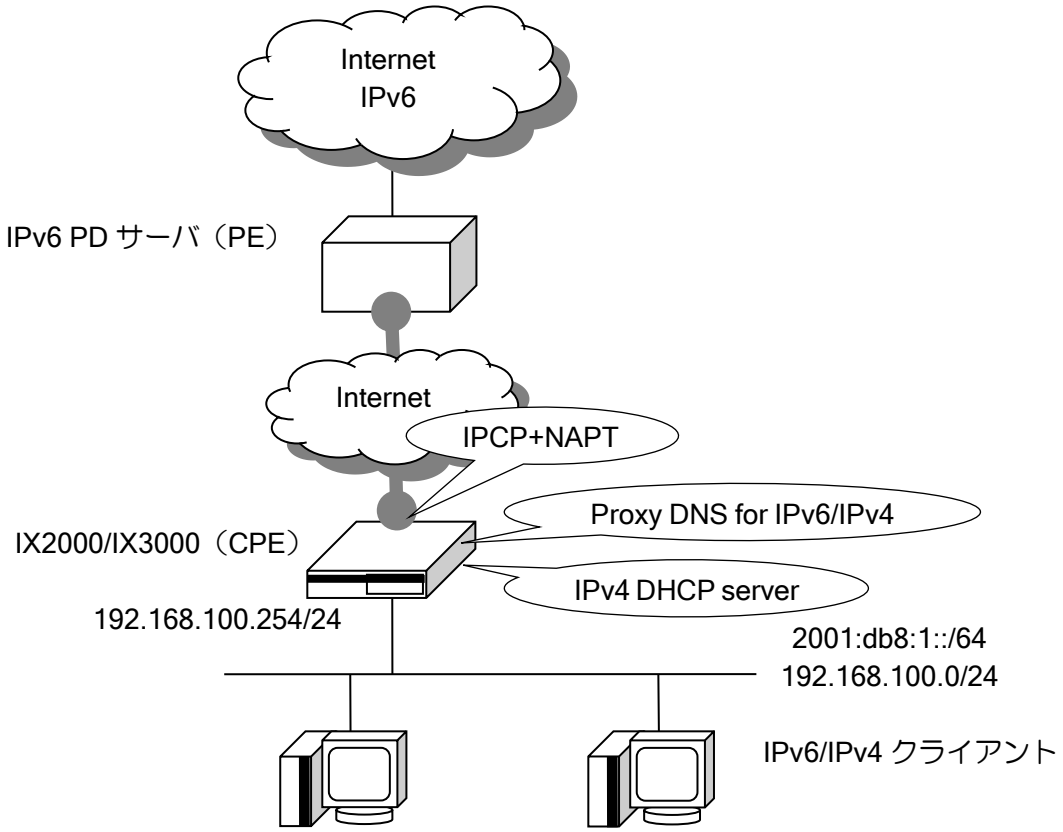
PD サーバより、プレフィックスが配布されると PD クライアントのリクエスタインタフェースに、配布プレフィックスの subnet-router anycast address*1 が自動的に設定されます。PD サーバ等はこの subnet-router anycast address*1 宛ての ping 等によって IX2000/IX3000 の導通を確認することができます。



*1 subnet router anycast address
subnet router anycast address とは、任意のプレフィックス長以下のインタフェース ID 部がすべて 0 である IPv6 アドレス。（RFC2373 参照）

(d) PD を用いた IPv6/IPv4 自動設定構成

IPv6 の Prefix Delegation 機能と IPv4 の DHCP サーバ機能を併用することにより、IPv6/IPv4 デュアルスタックな自動設定構成を構築することができます。また、Proxy DNS 機能を使うことにより、グローバルな DNS アドレスをクライアントで意識することなく利用することも可能となります。



※NAPT、IPv4 DHCP、ProxyDNS の詳細については、それぞれの節を参照してください。

【設定例】

```
ip dhcp enable
!
proxy-dns ip enable
proxy-dns ipv6 enable
!
ipv6 dhcp client-profile pd6c
   ia-pd subscriber GigaEthernet1.0
   option-request dns-servers
!
ppp profile pppoe
   authentication myname xxxx@xxxx.nec.co.jp
   authentication password xxxx@xxxx.nec.co.jp xxxxx
!
ip dhcp profile dhcp4server
   dns-server 192.168.100.254
!
interface GigaEthernet0.1
   encapsulation pppoe
   ppp binding pppoe
   ip address ipcp
   ip napt enable
```

```
   ipv6 enable
   ipv6 dhcp client pd6c
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.100.254/24
   ip dhcp binding dhcp4server
   ipv6 enable
   ipv6 nd ra enable
   no shutdown
```

(e) Information Request 設定

IX2000/IX3000 では、DHCPv6 の Information Request メッセージをサポートしています。このメッセージは、IPv6 プレフィックスは取得する必要がないが、DNS サーバや NTP サーバのアドレスは DHCPv6 で取得したいといったときに使用します。

このコマンドは、オプション要求の設定を行っているときのみ有効となります。

information-request	Information Request の設定 （DHCPv6 クライアントコンフィグモード）
option-request	オプション要求の設定 （DHCPv6 クライアントコンフィグモード）
show ipv6 dhcp client	DHCPv6 クライアントの状態表示

```
【設定例】
!
ipv6 dhcp client-profile get-dns
   information-request
   option-request dns-servers
   option-request ntp-servers
!
interface GigaEthernet0.0
   ipv6 address 2001:db8:200::/64 eui-64
   ipv6 dhcp client get-dns
   no shutdown
```

※ DHCPv6 で取得した DNS アドレスは、Ver.8.8 以降、リゾルバと ProxyDNS で使用可能です。
Ver.8.7 以前は ProxyDNS でのみ再利用可能です。

(f) スタティックルートの設定

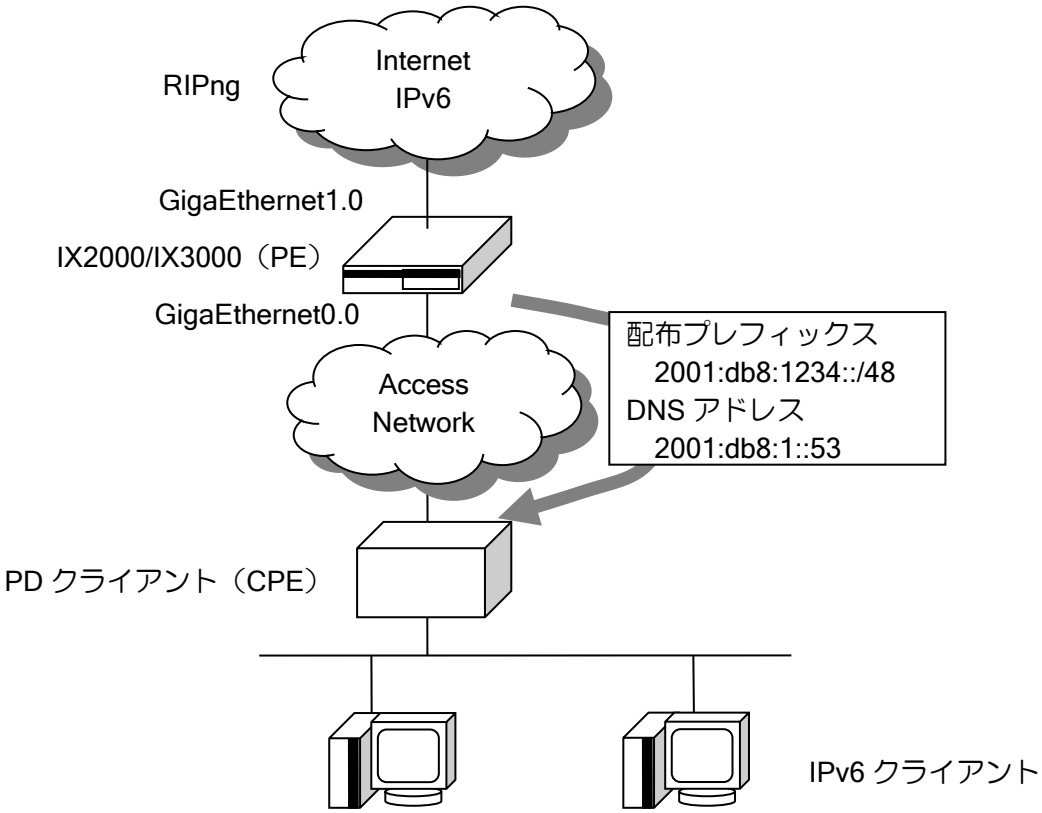
Ver9.7 以降、サーバをネクストホップとして、スタティックルートを登録できます。

```
【設定例】

ipv6 route 2001:db8::/64 GigaEthernet0.0 dhcp
```

2.21.3 Prefix Delegation サーバの設定

DHCPv6 Prefix Delegation サーバ機能（以下 PD）を用いることにより、DHCPv6 PD クライアント（CPE）へ IPv6 プレフィックスや DNS サーバアドレスを配布することができます。

(a) PD によるアドレスの割り当て



IX2000/IX3000 シリーズでは、PD クライアント（CPE）からの要求に対して

ipv6 dhcp enable	DHCPv6 サーバの起動 （グローバルコンフィグモード）
ipv6 dhcp server	DHCPv6 サーバの設定 （インタフェースコンフィグモード）
ipv6 dhcp server-profile	DHCPv6 サーバコンフィグモードへの移行 （グローバルコンフィグモード）
ia-option	IA オプションの設定 （DHCPv6 サーバコンフィグモード）
ia-pd prefix	CPE に配布する Prefix 情報の設定 （DHCPv6 サーバコンフィグモード）
ia-pd static	特定の CPE に配布する Prefix 情報の設定 （DHCPv6 サーバコンフィグモード）
dns-server	オプションで広告する DNS サーバの設定 （DHCPv6 サーバコンフィグモード）
show ipv6 dhcp server	DHCPv6 サーバの状態表示

【設定例】

```
!
ipv6 dhcp enable
!
ipv6 dhcp server-profile pd6s
   dns-server 2001:db8:1::53
   ia-option ia-pd 300 600
   ia-pd prefix 2001:db8::/48 nla-length 16 life-time 1200 600
!
ipv6 router rip
   redistribute static
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 dhcp server pd6s
   no shutdown
!
interface GigaEthernet1.0
   ipv6 enable
   ipv6 rip enable
   no shutdown
```

CPE へ配布するプレフィックスの設定は、配布するプレフィックスに対して何ビットを NLA として割り当てるかを設定します。NLA のビット分は、自動的に割り当てられます。（プレフィックスの設定においては、NLA のビット部分は 0 となるように設定する必要があります。）

※Ver8.9 以降では、同一の DHCPv6 サーバプロファイルを複数の” ipv6 dhcp server”コマンドで指定することはできません。

(b)パラメータの設定

- ルーティングの設定

デフォルトでは、配布したプレフィックス宛のルーティングは、プレフィックスを配布した CPE に対してスタティックルートを設定します。不要な場合は、設定を削除してください。

設定は以下のとおりです。

auto-static	スタティックルートの自動設定 （DHCPv6 サーバコンフィグモード）

- DNS の設定

オプションのパラメータにより、CPE へ DNS サーバを広告することができます。

Ver.10.3 以降、インタフェースに設定されたグローバルアドレスを DNS サーバとして使用することができます。

設定は以下のとおりです。

dns-server	オプションで広告する DNS サーバの設定 （DHCPv6 サーバコンフィグモード）

- CPE への Renew／Rebind の設定

CPE へ通知する Renew／Rebind の周期を設定します。Renew／Rebind は CPE から PE への接続確認のため使用します。PE を再起動した場合など、PE 側で CPE 接続情報が無くなった場合には、CPE から Renew／Rebind を受信することで再度設定が行われます。スタティックルートの自動設定で使用する場合には、PE を再起動後は、スタティックルートが削除されます。PPPoE など、PE 再起動によりセッションが切断するような場合は、接続後プレフィックスを再度配布するので問題ありませんが、Ethernet で使用する場合は Renew／Rebind を受信するまでスタティックルートが作成されないため、通信できなくなります。そのため、Ethernet で使用する場合は、数分程度に設定した方が、通信断の時間が短くなります。

設定するコマンドは以下のとおりです。

ia-option	IA オプションの設定 （DHCPv6 サーバコンフィグモード）

2.21.4 PD/RA 自動判別

Ver.10.3 以降、DHCPv6 Prefix Delegation サーバ機能（以下 PD）と RA 受信のどちらのプレフィックスを使用するかを自動で判定することができます。PD と RA のどちらかが利用可能な場合に共通のコンフィグで接続できるようになります。PD、RA の両方が動作している場合でもどちらかが選択されます（PD 優先）。

2.21.4.1 PD/RA 自動判別の有効化

PD/RA 自動判別機能を使用する場合には、インタフェースで次のコマンドを設定します。あわせて DHCPv6 クライアント機能とステートレスアドレス自動設定（または、ND プロキシ設定）を設定します。

ipv6 autoselect enable	PD/RA 自動判別機能の有効化 （インタフェースコンフィグモード）
ipv6 autoselect ra-refresh	RA モード中に動作モードを監視する間隔(分) （インタフェースコンフィグモード）
ipv6 autoselect ra-delay	RA モードを確定するまでの猶予時間(秒) （インタフェースコンフィグモード）

【設定例 1】
自動判別を動作させるインタフェース自体にグローバルアドレスを設定する場合(ステートレスアドレス自動設定、DHCPv6 クライアントを併用)

```
!
ipv6 dhcp client-profile pd6c
   option-request dns-servers
   ia-pd subscriber GigaEthernet0.0
!
interface GigaEthernet0.0
   ipv6 autoselect enable
   ipv6 address autoconfig receive-default
   ipv6 dhcp client pd6c
   no shutdown
```

※ PD で WAN インタフェースにアドレスを付与する設定は接続環境によっては不具合が発生する場合があります。

【設定例 2】
LAN インタフェースにグローバルアドレスを設定し、LAN 側にプレフィックスや DNS サーバを配布する場合（ND プロキシ、DHCPv6 クライアント、DHCPv6 サーバを併用）

```
ipv6 dhcp enable
!
proxy-dns ipv6 enable
!
ipv6 dhcp client-profile pd6c
   option-request dns-servers
   ia-pd subscriber GigaEthernet1.0
!
ipv6 dhcp server-profile pd6s
   dns-server autoconfig
!
interface GigaEthernet0.0
   description ## WAN ##
   ipv6 enable
   ipv6 autoselect enable
   ipv6 nd proxy GigaEthernet1.0
```

```
   ipv6 dhcp client pd6c
   no shutdown
!
interface GigaEthernet1.0
   description ## LAN ##
   ipv6 enable
   ipv6 dhcp server pd6s
   ipv6 nd ra enable
   ipv6 nd ra other-config-flag
   no shutdown
```

2.21.4.2 動作モード

自動判別の有効化後、PD を使用している状態の「PD モード」、 RA を使用している状態の「RA モード」の判定を行います。動作モードの確定条件は以下の通りです。

動作モード	モード確定条件
PD モード	PD Reply 受信
RA モード	PD Reply より先に RA（※）を受信し、猶予期間（ra-delay）内に PD Reply の受信がない場合（猶予期間が 0 の場合は RA を受信後即時 RA モード確定）

※RA 受信が以下に該当する場合は、グローバルアドレスを設定しないため、RA モードになりません。

- Autonomous フラグが 0
- プレフィックスのサイズが 16 バイト未満
- プレフィックスアドレスが非グローバルアドレス
- Preferred Lifetime が Valid Lifetime より大きい
- Valid Lifetime が 0

動作モード確定後も常時監視を行い、動作モードを自動的に切り替えます。ただし、PD モードを優先的に動作させるため、モード切替には以下の条件があります。

- PD モード中に RA を受信しても RA を廃棄し、RA モードに切り替わりません。
- PD モード中に PD の Renew/Rebind メッセージの応答が無く、DHCPv6 クライアントがリセットされた場合、再度動作モードの判定を行います。
- RA モード中に、ra-refresh で設定した時間毎に PD Solicit を送信し、PD 接続シーケンスが成功した場合、PD モードに切り替わります。

※グローバルアドレス変更時、または上位ルータ変更によるデフォルトルート変更時に information-request を送信し、最新のオプション情報(DNS サーバアドレスなど)を取得します。

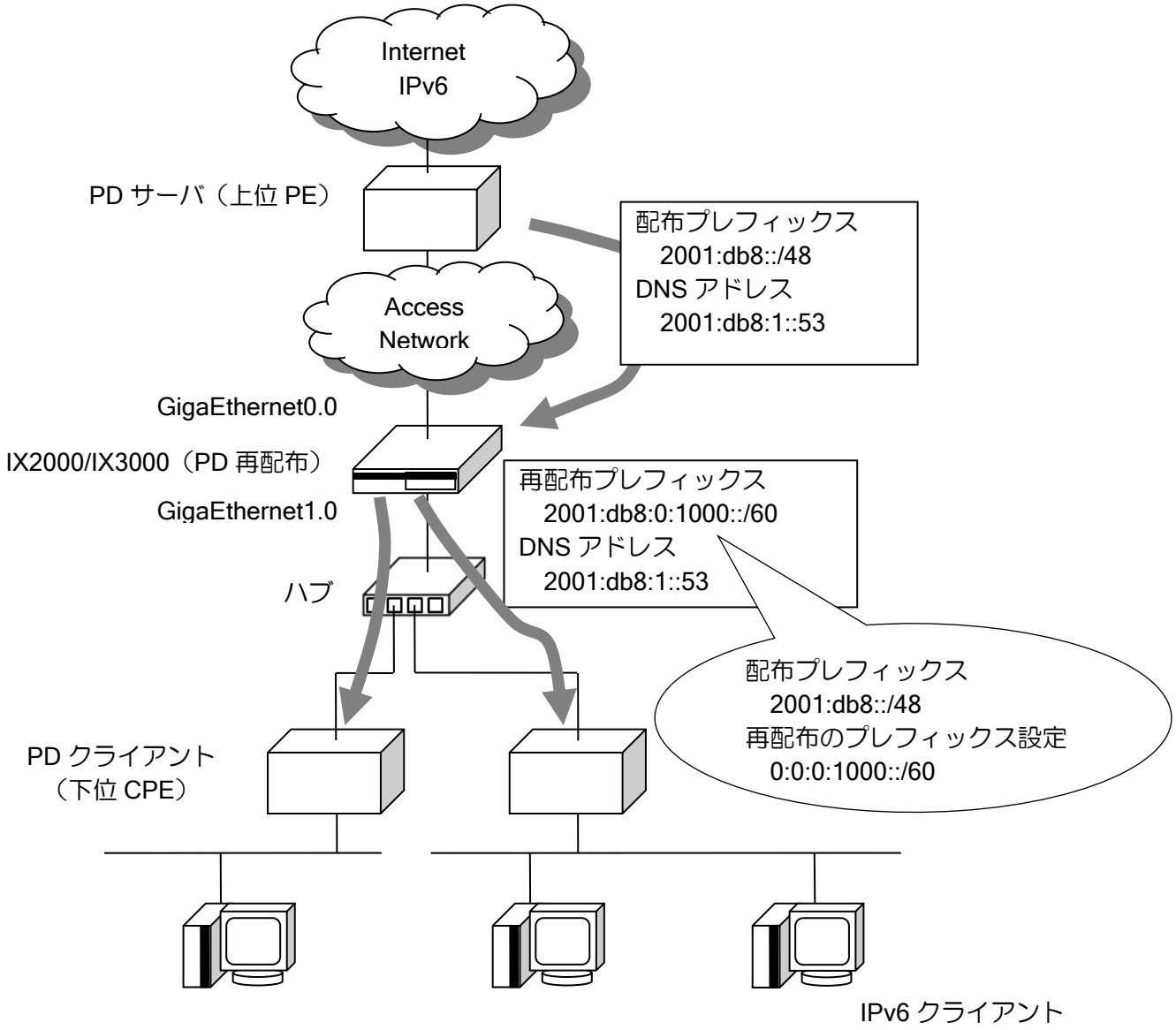
2.21.4.3 注意事項

- 自動判別が無効化(no ipv6 autoselect enable)された場合、現在の動作モードをリセットし設定済みのグローバルアドレスを削除します。
- 自動判別が動作するインタフェースのリンクがダウンした場合、リンクアップ後に再度動作モードの判定を行います。
- 自動判別動作中にステートレスアドレス自動設定や DHCPv6 クライアントのコンフィグを変更した場合、動作モードがリセットされる場合があります。

2.21.5 Prefix Delegation 再配布の設定

DHCPv6 Prefix Delegation 再配布機能（以下、PD 再配布機能）を用いることにより、上位ネットワークの DHCPv6 PD サーバ（上位 PE）から IX の DHCPv6 PD クライアントに配布された IPv6 プレフィックスを複数の下位ネットワークの CPE（下位 CPE）に分割して再配布することができます（ver.8.9 以降正式リリース）。

(a) PD による割り当てアドレスの再配布



ia-pd redistribute	再配布のための IPv6 プレフィックスのプール情報の設定 （DHCPv6 クライアントコンフィグモード）
ia-pd redistribute-prefix	下位 CPE に再配布するプレフィックスのプール情報の設定 （DHCPv6 サーバコンフィグモード）
ia-pd redistribute-static	特定の下位 CPE に再配布するプレフィックスのプール情報の設定 （DHCPv6 サーバコンフィグモード）

```
【設定例】
!
ipv6 dhcp enable
!
ipv6 dhcp client-profile ix-cpe
   option-request dns-servers
   ia-pd redistribute pool dynamic_pool 0:0:0:1000::/60 nla-length 4
   ia-pd redistribute pool static_pool 0:0:0:2000::/60
   shutdown-delay 100
!
ipv6 dhcp server-profile ix-pe
   ia-pd redistribute-prefix pool dynamic_pool
   ia-pd redistribute-static fe80::1 pool static_pool
   shutdown-delay 100
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 dhcp client ix-cpe
   no shutdown
!
interface GigaEthernet1.0
   ipv6 enable
   ipv6 dhcp server ix-pe
   no shutdown
```

再配布している IPv6 プレフィックスや DNS/NTP の情報に変更が発生した場合、IX の PE は情報を再配布している下位 CPE に対して再設定を促すメッセージを送信します。

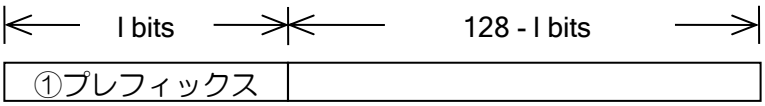
※PD 再配布機能の設定について、以下の注意事項があります。

- "ia-pd redistribute"コマンドで定義した IPv6 プレフィックスのプール情報は、複数の"ia-pd redistribute-prefix"または"ia-pd redistribute-static"コマンドを設定する場合、1 つのコマンドでのみ指定可能です。
- 同一の DHCPv6 サーバプロファイルでは、既存の配布設定コマンド("ia-pd prefix"、"ia-pd static")と再配布設定コマンド("ia-pd redistribute-prefix"、"ia-pd redistribute-static")のうち一方のみ設定可能です。
- DNS／NTP サーバアドレスについて、IX の PE は”dns-server”や”ntp-server”コマンドが設定されていなくても、上位 PE から配布された情報を再配布します。

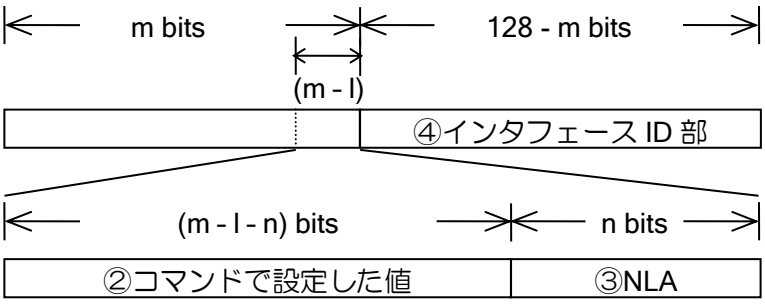
(b)再配布プレフィックスの生成

IX の PE が再配布する IPv6 プレフィックスは、上位 PE から IX の CPE に配布された IPv6 プレフィックスと、再配布のための IPv6 プレフィックスのプール情報の設定（DHCPv6 クライアントプロファイル）を組み合わせて生成されます。以下ではこの生成方法について説明します。

上位 PE から配布された IPv6 プレフィックス （プレフィックス長 l）



DHCPv6 クライアントプロファイルに設定した再配布のための IPv6 プレフィックス(プレフィックス長 m, NLA 長 n)



IX の PE が再配布する IPv6 プレフィックスは上図の①と②と③（NLA）と④（すべてのビットが'0'）を組み合わせて生成されます。

設定例「(a)PD による割り当てアドレスの再配布」の"dynamic_pool"のプール情報の設定によって生成される再配布プレフィックスを例として説明します。

①は上位 PE から配布された IPv6 プレフィックスの 1～48 ビットの範囲で"2001:db8:0"、②はプール情報の設定の IPv6 プレフィックスの 49～56 ビットの範囲で"10"、③はプール情報の設定の IPv6 プレフィックス長である/60 から NLA 分 4 ビットである 57～60 ビットの範囲で、自動的に割り当てられる NLA のビットの値、④はインタフェース ID 部である 61～128 ビットの範囲で全て"0"になります。これにプール情報の設定の IPv6 プレフィックス長である/60 を組み合わせて IX の PE は"2001:db8:0:1000::/60"の IPv6 プレフィクスを再配布します。

※③の NLA の値は、IX が CPE 毎に自動的で割り当てる値です。詳しくは「Prefix Delegation サーバの設定」の章を参照してください。

2.21.6 接続情報の保持時間設定

DHCPv6 を設定したインタフェースがリンクダウンした時に、接続先情報が削除されるまでの遅延時間を設定することができます。設定は以下のとおりです。

shutdown-delay	リンクダウン後の DHCPv6 接続情報の保持時間設定 （DHCPv6 サーバコンフィグモード、DHCPv6 クライアントコンフィグモード）

本コマンドを設定することで、 インタフェースの一時的なリンクダウン発生時に接続情報が削除されることにより生じる以下の影響をおさえることができます。

- CPE インタフェースがリンクダウンすることにより、Subscriber で指定したインタフェースに割り当てられた IPv6 アドレスが削除される。
- CPE インタフェースがリンクダウンすることにより、再配布の IPv6 プレフィックスが削除され、下位 CPE との接続が切断される。
- PE インタフェースがリンクダウンすることにより、接続している CPE に関する情報や経路設定が削除される。

- 接続情報の保持時間中に再リンクアップしたときの動作

  - DHCPv6 クライアントでは、接続状態を保持しつつ Solicit もしくは Information Request を送信します。Reply 受信時に以前の接続状態と異なる場合は、その時点で更新されます。
  - DHCPv6 サーバでは、保持している接続先に Reconfigure を送信します。

■2.22 ルーティングの設定

パケット転送は、ルーティングテーブル情報に基づき実行します。このため、IX2000/IX3000 をルータとして動作させるためには、ルーティングテーブルへのルート登録が必要となります。登録するルートは、次のように大別することができます。

- ダイレクトルート（Connected）
  - インタフェースのサブネットアドレス
- スタティックルート（Static）
  - 手動で設定する固定的なルート
- ダイナミックルート（Dynamic）
  - ダイナミックルーティングプロトコルを使用し、学習したルートから求めた最適経路

これらのルートのルーティングテーブルへの登録は、経路制御情報に基づき、対応する各ルーティングプロトコル処理（ダイレクト、スタティックルートを含む）により実行します。
これ以外にもルート解決方法として、ポリシールーティングによるルート設定があります。

2.22.1 経路制御とディスタンス

ルーティングテーブルと各ルーティングプロトコル（ダイレクトルート、スタティックルートを含む）との経路のやりとり（経路制御）は、ルートタイプを基に実行されます。
ルートタイプは、ルーティングテーブル内に登録されたルートとともに管理されている情報源のルーティングプロトコルを示す情報で、IPv4 では次の 10 種類があります。

- Connected（ダイレクトルート）
- Static（スタティックルート）
- RIP
- OSPF external
- OSPF inter-area
- OSPF intra-area
- OSPF nssa-external
- BGP external
- BGP internal
- BGP local

また、IPv6 では次の 4 種類があります。

- Connected（ダイレクトルート）
- Static（スタティックルート）
- RIP
- OSPF

以下にルートタイプによる経路制御の動作概要について説明します。

各ルーティングプロトコルは、独立して動作し、学習（設定）した経路から求めた最適経路をルートタイプとともにルーティングテーブルに書き込みます。
したがって、異なるルーティングプロトコルが、ルーティングテーブルに同一経路を書き込もうとする場合が考えられます。

このような場合、情報源を示すルートタイプの優先度（ディスタンス）に従い、どのルーティングプロトコルからの経路を書き込むかを決定します。

デフォルトのディスタンスは、次のとおりです。

ルートタイプ	ディスタンス	優先度
Connected	0（固定値）	↑高
Static	1	
BGP external	20	
OSPF intra-area	110	
OSPF inter-area	110	
OSPF external	110	
OSPF nssa-external	110	
RIP	120	
BGP internal	200	
BGP local	200	↓低

ディスタンスの変更は、次のコマンドで登録します。

ip route	Static のディスタンス値変更 （distance オプションにより変更）
distance	RIP のディスタンス値変更 （RIP コンフィグモード）
distance	OSPF のディスタンス値変更 （OSPF コンフィグモード）
distance	BGP のディスタンス値変更 （BGP アドレスファミリモード）
clear ip route	ディスタンス変更時のルーティングテーブル削除
clear ip rip process	ディスタンス変更時の RIP プロセス再起動
clear ip ospf process	ディスタンス変更時の OSPF プロセス再起動

ipv6 route	Static のディスタンス値変更 （distance オプションにより変更）
distance	RIPng のディスタンス値変更 （RIPng コンフィグモード）
distance	OSPFv3 のディスタンス値変更 （OSPFv3 コンフィグモード）
clear ipv6 route	ディスタンス変更時のルーティングテーブル削除
clear ipv6 rip process	ディスタンス変更時の RIPng プロセス再起動
clear ipv6 ospf process	ディスタンス変更時の OSPFv3 プロセス再起動

【設定例】

1. Static のディスタンスを変更する。

```
ip route default 192.168.0.254 distance 240
ipv6 route default GigaEthernet0.1 distance 240
```

2. RIP/RIPng のディスタンスを変更する。

```
ip router rip
  distance 50

ipv6 router rip
  distance 50
```

3. OSPF のディスタンスを変更する。

```
ip router ospf 1
  distance external 150 inter-area 100 intra-area 50
```

4. BGP のディスタンスを変更する。

```
router bgp 10
  address-family ipv4 unicast
    distance ebgp 10 ibgp 100
```

5. RIP/RIPng のディスタンス変更時にはルーティングテーブルを削除、もしくは RIP プロセスを再起動する必要があります。

```
clear ip rip process
clear ipv6 rip process
```

6. OSPF のディスタンス変更時には、OSPF プロセスを再起動する必要があります。

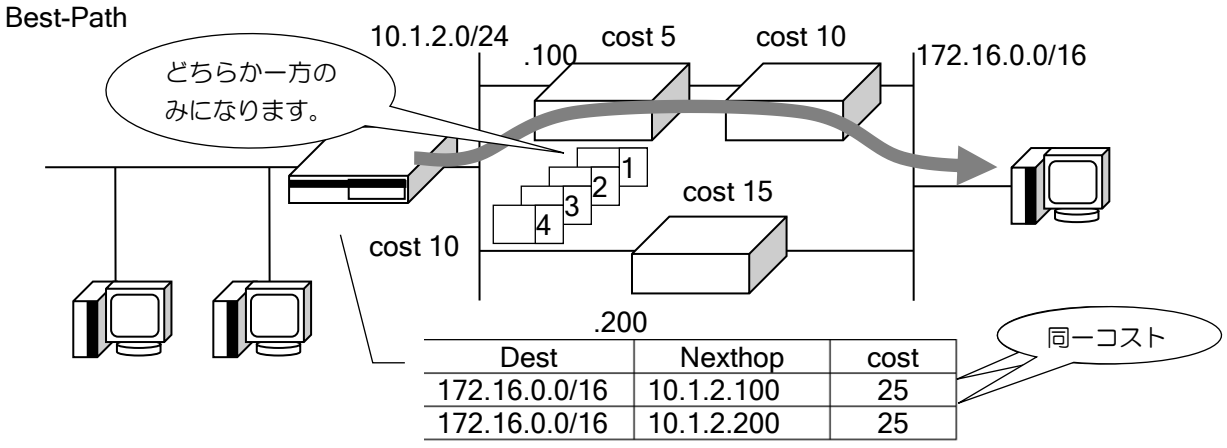
```
clear ip ospf process
```

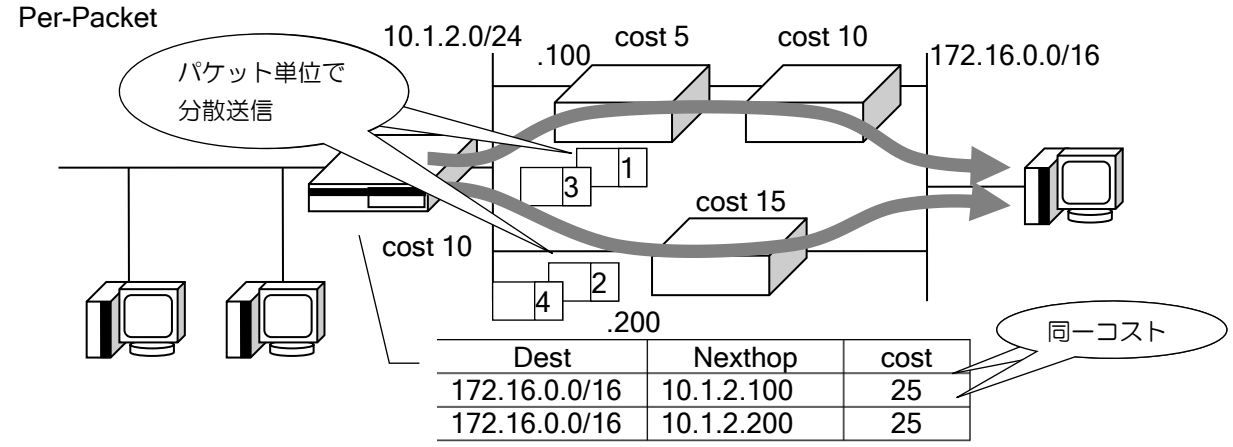
2.22.2 イコールコストマルチパス

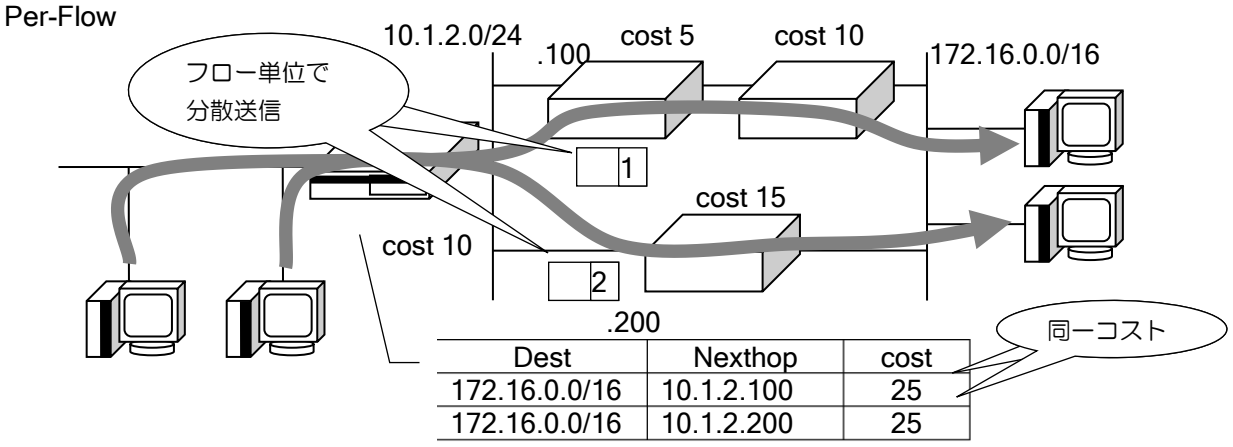
イコールコストマルチパスとは、同一終点宛にコストの等しい中継点が存在する（複数の最適経路が存在する）ということを意味します。このような場合においては、どちらか 1 つだけを選択する方法や、両方を使用してロードバランシングを行う方法が考えられます。

ロードバランシングとは、複数のパスを利用し、簡易的に負荷を分散させる機能です。次のような分類を考えることができます。これらの機能はルーティングプロトコルと、プログラムのバージョンによって動作が異なります。対応状況については付録を参照してください。

- ロードバランスしない（Best-Path）
  システム固定のパス選択基準によって複数のパスの中から 1 つを選択し利用します。
- Per-Packet
  等コストのパスをパケット単位で順番に（ラウンドロビンで）利用します。つまり、パケット毎にどの中継点を利用するかは予測不可能です。パケット到着順が不定となるため、エンドーエンドの通信で性能が低下することが考えられます。
- Per-Flow
  等コストのパスをパケットの始点アドレス、終点アドレスおよびプロトコルのセット単位で順番に（ラウンドロビンで）利用します。これにより、始点アドレス、終点アドレス等からどの中継点を利用するか予測可能となります。
- Per-Flow-Fix-Interface (Ver10.7 以降)
  等コストのパスをパケットの始点アドレス、終点アドレスのセット単位で順番に（ラウンドロビンで）利用します。これにより、始点アドレス、終点アドレス等からどの中継点を利用するか予測可能となります。
  Per-Flow では、IP キャッシュが削除された際に出力インタフェースが変更される可能性がありますが、本設定を用いた場合常に固定のインタフェースから出力されます。
- Per-Session（未対応）
  等コストのパスをパケットの種々のパラメータ単位で順番に（ラウンドロビンで）利用します。これにより、始点アドレス、終点アドレス等からどの中継点を利用するか予測可能となります。







※ Per-Flow-Fix-Interface では送信元と送信先から出力インタフェースが一意に決まります。

コマンドの設定は次のとおりです。

ip multipath per-packet	Per-Packet で動作します。（デフォルト）
ip multipath per-flow	Per-Flow で動作します。
ip multipath per-flow-fix-interface	Per-Flow(インタフェース固定)で動作します。
no ip multipath	ロードバランシングは行いません。
show ip cache	現在の動作とパスを表示します。

※デフォルトの ip multipath per-packet は設定が表示されません。

2.22.3 スタティックルート

スタティックルーティングは、コマンドにより経路情報をあらかじめ装置に設定しておくことにより、ルーティングを行います。スタティックルーティングでは、次の情報を設定します。

- ディスティネーション（サブネットアドレス（プレフィックス）、マスク長（プレフィックス長））
- ネクストホップアドレス
- 送出先インタフェース
  出力先が Ethernet，FastEthernet，GigaEthernet の場合は、送出先インタフェースを指定する場合は、ネクストホップアドレスを指定してください。送出先インタフェースのみ設定した場合は、パケットの送出先が分からないため、正常にルーティングできない場合があります。
- メトリック値、ディスタンス値、タグ値

スタティックルートの設定および確認は次のコマンドを使用します。

ip route	IPv4 スタティックルートの登録
ipv6 route	IPv6 スタティックルートの登録
show ip static-routes	IPv4 スタティックルートの表示
show ipv6 static-routes	IPv6 スタティックルートの表示

【設定例】

デフォルトルートの設定

```
ip route default 192.168.0.254
ip route default Tunnel0.0

ipv6 route default fe80::1%GigaEthernet0.0
ipv6 route default Tunnel0.0
```

※IPv6 では、ネクストホップアドレスを指定する場合には、通常はリンクローカルアドレスを使用します。
※リンクローカルアドレスは、ネクストホップルータの設定を確認する他、ping6 コマンドを使用して調査することも可能です。

(a) フローティングスタティック

フローティングスタティックルートは、普段は RIP/OSPF などのダイナミックルーティングを使用し、ダイナミックルーティングが何らかの障害により使用不能になった場合に、設定されているスタティックルートの設定にてルーティングを行います。フローティングスタティックは、スタティックルート設定のディスタンス値を大きくすることにより使用することができます。

【設定例】

フローティングスタティックの設定

```
ip route 10.1.2.0/24 192.168.0.1 distance 200

ip router rip
   redistribute connected

interface GigaEthernet1.0
   ip address 192.168.0.254/24
   ip rip enable
   no shutdown
```

(b) DHCP 機能との連携

DHCP サーバからアドレスを取得した場合に、DHCP サーバがネクストホップになる経路を設定できます。スタティックルートコマンドに dhcp のオプションを設定します。

【設定例】

```
ip route 10.1.2.0/24 192.168.0.1 dhcp
```

(c) connected オプション

Dialer や PPPoE, NGN トンネルのような接続処理を行うインタフェースについて、接続中の場合だけ有効になる経路を設定することができます。Ver8.7 以降で対応しています。IPv6 は未サポートです。

【設定例】

NGN トンネルインタフェース Tunnel0.0 が接続中の場合のみ有効になる設定

```
ip route 192.168.20.0/24 Tunnel0.0 connected
```

2.22.4 RIP/RIPng

RIP/RIPng は、AS（Autonomous System）内部で動作する IGP（Interior Gateway Protocol）の 1 つです。RIP には、IPv4 で用いられる RIPv1/RIPv2 と IPv6 で用いられる RIPng があります。以下 RIP/RIPng は RIP と表記します。

2.22.4.1 ルータの設定

(a)RIP の起動

RIP を起動するコマンドは、ip/ipv6 router rip コマンドです。RIP コンフィグモードに移行すると同時に RIP が起動します。

また、RIP を動作させるインタフェースと送信および受信の動作指定を各インタフェースにて、ip/ipv6 rip enable コマンドにより設定します。

ip router rip	RIP 動作開始/RIP コンフィグモード移行 （グローバルコンフィグモード）
ip rip enable	RIP 動作開始（インタフェースコンフィグモード）
ip rip send	RIP 送信設定（インタフェースコンフィグモード）
ip rip send version	RIP 送信バージョン設定 （インタフェースコンフィグモード）
ip rip receive	RIP 受信設定（インタフェースコンフィグモード）
ip rip receive version	RIP 受信バージョン設定 （インタフェースコンフィグモード）
ip rip split-type	スプリットホライズン種別の設定 （インタフェースコンフィグモード）
ipv6 router rip	RIPng 動作開始/RIPng コンフィグモード移行 （グローバルコンフィグモード）
ipv6 rip enable	RIPng 動作開始 （インタフェースコンフィグモード）
ipv6 rip send	RIPng 送信設定 （インタフェースコンフィグモード）
ipv6 rip receive	RIPng 受信設定 （インタフェースコンフィグモード）
ipv6 rip split-type	スプリットホライズン種別の設定 （インタフェースコンフィグモード）

上記コマンドの他、RIP コンフィグモードでの各種コマンド、インタフェースコンフィグモードの ip/ipv6 rip コマンドにより各種詳細設定が可能です。

【設定例】

GigaEthernet1.0 インタフェースにおいて、RIPv2 にて通知させます。
また、直接接続ルート（connected route）を RIP で通知します。

```
ip router rip
   redistribute connected
!
interface GigaEthernet1.0
   ip address 192.168.0.254/24
   ip rip enable
   no shutdown
```

GigaEthernet0.0 インタフェースにおいて、RIPng を送受信とも動作させ、
かつそのインタフェース以外のサブネットワークを RIPng にて通知させます。

```
ipv6 router rip
   redistribute connected
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 address 2001:db8:1::1/64
   ipv6 rip enable
   no shutdown
```

RIPv1/RIPv2 の両方を送信または受信する設定とした場合の動作は次のようになります。

- 送信の場合、該当リンクに RIPv1 のみサポートするルータが 1 台でも存在する場合は、RIPv1/RIPv2 両方のパケットを送信します。すべて RIPv2 をサポートしている場合は、RIPv2 のパケットのみを送信します。
- 受信の場合、同一の隣接ルータから RIPv1 および RIPv2 でルーティング情報を受信した場合、RIPv1 で受け取った情報は廃棄します。

(b) タイマの設定

RIPv1/RIPv2 では、定期更新タイマ、無効タイマ、ガーベジコレクションタイマを変更することができます。

- 定期更新タイマ
  - RIP が有効となっているインタフェースより、定期更新タイマ時間毎に RIP 情報を隣接ルータに送信します。
- 無効タイマ
  - RIP のメトリック値を 16 に変更します。
- ガーベジコレクションタイマ
  - ルーティングテーブルより経路を削除します。ディスタンス値の大きな RIP 以外のルートがあった場合には、そのルートが有効となります。

timers	タイマ値の変更 （RIP コンフィグモード）

【設定例】

```
ip router rip
   timers 20 120 80
```

※RIP における、タイマの値は RFC によって明確に規定されています。この値をコンフィグで変更する場合においては、その変更による挙動、リスクを正しく把握・検査した上で行ってください。

※RIPng でタイマ値を変更することはできません。

(c) 無効ルートの扱い

RIP により広告される経路がタイムアウトした場合、次のように扱います。

無効タイマのタイムアウトにより、メトリックが 16 に設定されます。ディスタンスは変更されませんので経路情報にはそのまま残ります。

ガーベジコレクションタイマ（120 秒）により、タイムアウトした経路は経路情報から削除されます。代わりの経路が存在する場合は、この時に経路情報に表示します。

```
RIPv1/RIPv2 の場合
最初の状態
  R        10.41.211.0/24 [120/2] via 172.16.222.254, GigaEthernet0.0,
  C        172.16.222.0/24 [0/1] is directly connected, GigaEthernet0.0,
（S        10.41.211.0/24 [150/2] via 172.16.222.1, GigaEthernet0.0,）
            →RIP の経路があるときは表示されません

10.41.211.0/24 がタイムアウト
  R        10.41.211.0/24 [120/16] via 172.16.222.254, GigaEthernet0.0,
  C        172.16.222.0/24 [0/1] is directly connected, GigaEthernet0.0,

ガーベジコレクションタイマ（120 秒）タイムアウト
 他の経路が無い場合
  C        172.16.222.0/24 [0/1] is directly connected, GigaEthernet0.0,


 他の経路がある場合
  S        10.41.211.0/24 [150/2] via 172.16.222.1, GigaEthernet0.0,
  C        172.16.222.0/24 [0/1] is directly connected, GigaEthernet0.0,


RIPng の場合
最初の状態
  C     2001:db8:1::0/64 global [0/1]
          via ::, GigaEthernet0.0, 0:01:05/0:00:00
  R     2001:db8:2::0/64 global [120/5]
          via fe80:: 200:4cff:fe64:6264, GigaEthernet0.0, 0:01:06/0:00:00
（S     2001:db8:2::0/64 global [150/1]
          via fe80:: 200:4cff:fe64:6358, GigaEthernet0.0, 0:01:06/0:00:00）
            ->RIPng の経路がある時は現れません

2001:db8:2::0/64 がタイムアウト
  C     2001:db8:1::0/64 global [0/1]
          via ::, GigaEthernet0.0, 0:01:05/0:00:00
  R     2001:db8:2::0/64 global [120/16]
          via fe80:: 200:4cff:fe64:6264, GigaEthernet0.0, 0:01:06/0:00:00

ガーベジコレクションタイマ（120 秒）タイムアウト
  他の経路が無い場合（上記のスタティックが無い場合）
  C     2001:db8:1::0/64 global [0/1]
          via ::, GigaEthernet0.0, 0:01:05/0:00:00

  他の経路がある場合（上記のスタティックがある場合）
  C     2001:db8:1::0/64 global [0/1]
          via ::, GigaEthernet0.0, 0:01:05/0:00:00
  S     2001:db8:2::0/64 global [150/1]
          via fe80:: 200:4cff:fe64:6358, GigaEthernet0.0, 0:01:06/0:00:00
```

2.22.4.2 経路制御の設定

(a) メトリックオフセット

ネットワーク内に、同一宛先への経路が複数存在する場合、RIP ではメトリック値（Hop 数）を比較することにより、最適経路を確定します。IX2000/IX3000 シリーズでは、経路情報のメトリックを操作すること（メトリックオフセット値の加算）により、経路を意図的に操作することが可能です。

メトリックオフセット値は、次のコマンドでインタフェースコンフィグモードにて設定します。

ip rip metric-offset	RIP 受信メトリックオフセット値の設定 （インタフェースコンフィグモード）

ipv6 rip metric-offset	RIPng 受信メトリックオフセット値の設定 （インタフェースコンフィグモード）

※受信メトリックオフセットは、応答メッセージの受信直後に、そのパケットに含まれる経路情報のメトリック値に加算します。受信メトリックオフセットのデフォルト値は 1 です。
※送信メトリックオフセットの設定はありません。

(b) 経路フィルタ

IX2000/IX3000 シリーズでは、経路フィルタを設定することにより RIP の送受信を行う隣接ルータのフィルタリングもしくは、交換する RIP の経路のフィルタリングを行うことができます。

経路情報に関するフィルタは、次のコマンドで設定します。

ip rip distribute-list	RIP 経路情報フィルタの選択 （インタフェースコンフィグモード）
distribute-list	RIP 経路情報フィルタの選択 （RIP コンフィグモード）

ipv6 rip distribute-list	RIPng 経路情報フィルタの選択 （インタフェースコンフィグモード）
distribute-list	RIPng 経路情報フィルタの選択 （RIPng コンフィグモード）

※経路フィルタの経路条件指定にはプレフィックスリストが用いられます。プレフィックスリストについては、プレフィックスリストの設定の節を参照してください。

【設定例】
RIP 応答により受信した 10.0.0.0/8 への経路情報をフィルタリングします。

```
ip prefix-list rip-dlist-1 100 deny 10.0.0.0/8
ip prefix-list rip-dlist-1 1000 permit any
!
ip router rip
   distribute-list prefix rip-dlist-1 in
!
interface GigaEthernet0.0
   ip add 192.168.0.254/24
   ip rip enable
   no shutdown
```

RIPng 応答により受信した 2001:db8:1::/64 への経路情報をフィルタリングします。

```
ipv6 prefix-list ripng-dlist-1 100 deny 2001:db8:1::0/64
ipv6 prefix-list ripng-dlist-1 200 permit any
!
ipv6 router rip
   distribute-list prefix ripng-dlist-1 in
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 address 2001:db8:1::1/64
   ipv6 rip enable
   no shutdown
```

※設定を有効にするためには、clear ip rip process/clear ipv6 rip process が必要です。
※プレフィックスリストで deny 設定した経路がフィルタリングされます。
※permit 設定の 1 つもないプレフィックスリストを適用すると、すべての経路がフィルタリングされます。

(c) デフォルトルート広告

RIP を使用する場合において、広告するルート情報にデフォルトルートを含めることができます。

originate-default	RIP でデフォルトルートを広告する （RIP コンフィグモード）
ip rip originate-default	RIP でデフォルトルートを広告する （インタフェースコンフィグモード）
ip rip send-default	デフォルトルート送信設定 （インタフェースコンフィグモード）
ip rip receive-default	デフォルトルート受信設定 （インタフェースコンフィグモード）

originate-default	RIPng でデフォルトルートを広告する （RIPng コンフィグモード）
ipv6 rip originate-default	RIPng でデフォルトルートを広告する （インタフェースコンフィグモード）
ipv6 rip send-default	デフォルトルート送信設定 （インタフェースコンフィグモード）
ipv6 rip receive-default	デフォルトルート受信設定 （インタフェースコンフィグモード）

【設定例】

RIPv1/RIPv2 にて自分のインタフェースアドレスをデフォルトルートとして広告します。

```
ip router rip
   originate-default
```

RIPng にて自分のインタフェースアドレスをデフォルトルートとして広告します。

```
ipv6 router rip
   originate-default
```

デフォルトルート広告の設定を行った場合、設定を行ったルータ自身のデフォルトルートの有無にかかわらず、常にデフォルトルートを広告します。

デフォルトルート送信拒否（no ip/ipv6 rip send-default）を行っている場合には、デフォルトルート広告設定は無効となります。

(d) 経路再配信

IX2000/IX3000 シリーズでは、RIP 利用時において RIP 以外のルーティング情報を再配信することができます。再配信時のメトリックはデフォルトでは再配信元のメトリックを使用します。元のメトリックが 16 を超える場合は、メトリック 16 の無効経路として再配信されますので、メトリックの設定を行ってください。

redistribute	RIP 以外の IPv4 ルーティング情報を RIP で再配信（RIP コンフィグモード）

redistribute	RIPng 以外の IPv6 ルーティング情報を RIPng で再配信（RIPng コンフィグモード）

【設定例】

GigaEthernet0.0 インタフェースにおいて、RIPv2 を送受信とも動作させ、かつそのインタフェース以外のサブネットワークを通知させます。

```
ip router rip
   redistribute connected
!
interface GigaEthernet0.0
   ip address 192.168.0.254/24
   ip rip enable
   no shutdown
```

GigaEthernet0.0 インタフェースにおいて、RIPng を送受信とも動作させ、
かつスタティックルートをメトリック 5 で再配信させます。

```
ipv6 route 2001:db8:1::0/64 fe80::1%GigaEthernet0.0
!
ipv6 router rip
   redistribute static metric 5
!
interface GigaEthernet0.0
   ipv6 rip enable
```

redistribute は経路制御の設定（ルートマップ設定、プレフィックスリストの設定等）の後に行ってください。redistribute 設定後に経路制御の設定の変更を行った場合、clear ip/ipv6 ospf process が必要です。

- OSPF の経路を再配信する際の注意事項

RIP と OSPF を同一のインタフェースで動作させているような場合、OSPF の Type2 の外部経路のネクストホップのネットワークアドレスが RIP 送信インタフェースのネットワークアドレスと同じくなる経路は、split-type を none にしていなければ、RIP の経路として広告されません。Type1 の外部経路，エリア内，エリア間経路については、ネクストホップに関係なく RIP の経路として広告されます。

(e) 経路再配信（ルートマップ設定）

経路再配信オプションに、ルートマップオプションを利用することにより、再配信経路をさらに詳細に制御することが可能となります。経路再配信で利用するルートマップのマッチ条件とセット条件には以下があります。ルートマップの詳細は、ルートマップの項を参照してください。

route-map	ルートマップを設定します。
match interface	出先インタフェースを条件とします。
match ip address prefix-list	IPv4 宛先アドレスを条件とします。
match ipv6 address prefix-list	IPv6 宛先プレフィックスを条件とします。
match ip next-hop prefix-list	IPv4 ネクストホップを条件とします。
match ipv6 next-hop prefix-list	IPv6 ネクストホップを条件とします。
match metric	メトリック値を条件とします。
match tag	タグ値を条件とします。
set metric	メトリック値を書き換えて再配信します。
set tag	タグ値を書き換えて再配信します。
set ip next-hop	IPv4 ネクストホップを書き換えて再配信します。
set ipv6 next-hop	IPv6 ネクストホップを書き換えて再配信します。

※ルートマップに経路再配信と無関係なオプションが設定されていた場合、その設定は無視されます。
※経路再配信設定で、指定したルートマップが作成されていなかった場合、すべて条件にマッチしなかったとして処理されます。
※ルートマップに条件が 1 つも設定されていなかった場合、条件にマッチしたとして処理されます。
※RIPv1 を利用時には、タグ値、宛先アドレスの書き換えは無効となります。
※RIPv2 においてタグ値の 16 ビットより大きいビットは切り捨てて再配信されます。
※宛先アドレスとして、無効なアドレスが設定されていた場合、宛先アドレスの書き換えは行われません。

2.22.4.3 RIPv1 利用時の注意事項

RFC1058 RIPv1 では、経路送信において現在一般的に用いられている可変長サブネットマスクにおけるダイナミックルーティングはサポートしていません。

IX2000/IX3000 においても、上記 RFC に基づいた実装となっており、RIPv1 における可変長サブネットマスクアドレスの使用はサポートされていません。可変長サブネットマスクを用いたネットワークを構築する場合には、RIPv2 を用いる必要があります。

- 可変長サブネットマスクの予測に関する拡張

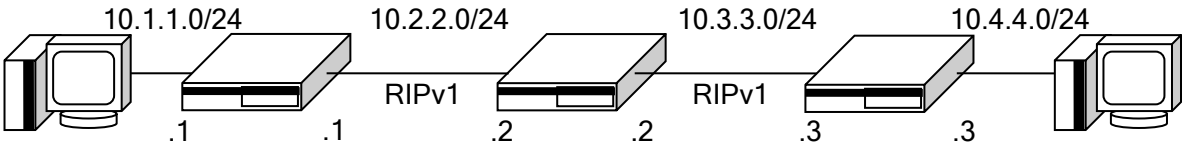
RIPv1 の可変長サブネットマスクの予測に関する拡張により、構成によっては RIPv1 にて可変長サブネットの利用が可能となります。

RIP インタフェースアドレスを元に、RIPv1 においてサブネットマスクを決定します。これにより、いくつかの可変長サブネット環境において RIPv1 による構築が可能となります。

※いずれにおいても、RIPv1 にはプロトコル仕様上の問題もあるため、RIPv1 を使わなくてはならない場合においては、十分に注意して構築・検証する必要があります。

実現可能なネットワーク構成例（1）

RIPv1 を利用するすべてのインタフェースのサブネットマスク長を一致

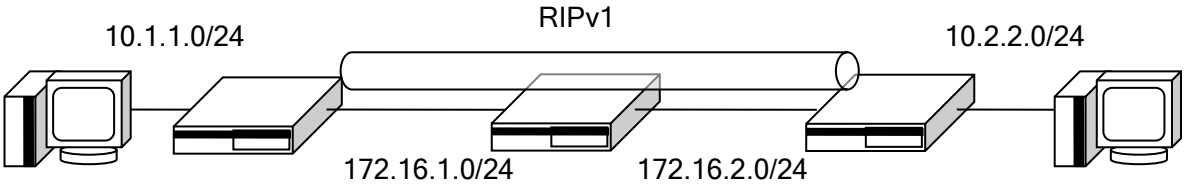


この場合、RIPv1 インタフェースでは、RIP 送信・受信時に 10.x.x.0 のルートは、/24 であると認識されます。クラスフルネットワーク 10.0.0.0/8 は送信されず、もし 10.0.0.0 を受け取った場合には、10.0.0.0/24 となります。

※Ver.5.0 以前にて本構成をとった場合、不要なルート 10.0.0.0 が送信されます。

実現可能なネットワーク構成例（2）

Unnumbered トンネルを利用した構成

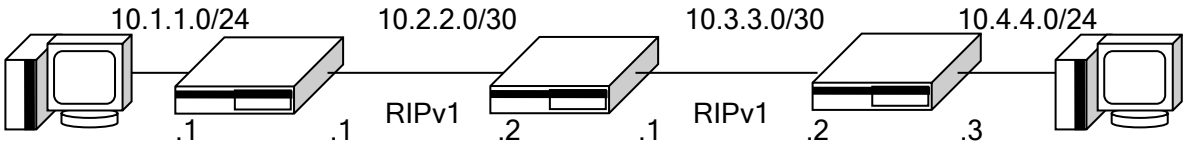


同一クラスのネットワークが分断されている場合において、Unnumbered トンネルを用いて RIPv1 を用いる構成です。Unnumbered インタフェースのソースアドレスインタフェース指定は、10.x.x.0/24 のインタフェースを指定する必要があります。

この場合、Unnumbered トンネルからは、10.x.x.0 と同時に、10.0.0.0 が送信されます。これは、Unnumbered トンネルの場合、終端のトンネルアドレスが同一サブネットアドレスでなくてもよいため、通常のネットワークアドレス 10.0.0.0/8 を出す必要があるためです。上記の環境においては、10.0.0.0 を Unnumbered トンネルから受け取ったルータは、そのルートを 10.0.0.0/24 のルートと判定します。

実現不可能なネットワーク構成例（1）

RIPv1 を利用するインタフェースのサブネットマスク長が不一致



同一クラスアドレスのネットワーク構成にて、異なるサブネットマスク長を持つネットワークにおいては、RIPv1 を利用することはできません。これは、RIP 送信・受信インタフェースにおいて、正しいサブネットマスク長が予測できないためです。

※送信インタフェースアドレスと同一のクラスアドレスを持ち、サブネットマスク長の異なる経路は、RIPv1 では送信されません。

- IX2000/IX3000 のバージョンによらず、RIPv1 のプロトコル仕様により、以下の不具合が発生する可能性があります。

RIPv1 による経路集約により到達できないネットワーク構成ができることがあります。

[原因]

- RIPv1 は、広告する情報にサブネットマスクを追加できないためです。
- IX2000/IX3000 の 2 つ以上のインタフェース上もしくはネットワークの先にクラスフルアドレスが同一となるネットワークが存在した場合、どちらのインタフェースからパケットを出すべきかが不定となります。この状態は、インタネット上のどこかに同一クラスフルアドレスを持った宛先が存在した場合に、意図せずパケット到達不能を発生させる場合があります。

[対処法]

- RIPv2 を使うことによりこの問題は発生しません。
- クラスフルアドレスが同一となるネットワークをすべてのネットワークで 2 つ以上作らないことで回避可能です。しかしこの場合、ネットワークの細分化ができません。（可変長サブネットを使う意味を失います。）

※可変長サブネットネットワークにおける RIPv1 の利用は、未サポート環境下における利用であるため、すべての不具合が記述されているとは限りません。

※対処法は、その不具合状態のみを解決するために考えられる物であり、RIPv1 により発生したあらゆる障害に対応できる物ではありません。

2.22.5 OSPFv2/OSPFv3

OSPF（Open Shortest Path First） は、RIP と同様に AS（Autonomous System）内部で動作する IGP（Interior Gateway Protocol） の 1 つです。OSPF は、リンクステートと呼ばれるネットワークに関する情報を運ぶパケットをルータ間で交換し、この情報をもとに最短経路アルゴリズム（Dijkstra algorithm）を実行し、経路情報をルーティングテーブルに反映させます。

OSPF には IPv4 で用いられる OSPFv2 と IPv6 で用いられる OSPFv3 があります。以下、特に違いが無い場合には OSPFv2/OSPFv3 は OSPF と表記します。

IX2000/IX3000 で利用可能な OSPF のルータタイプ

- Internal ルータ
  - ルータが直接接続しているネットワークがすべて同じエリアに属しているルータ
- Area Border ルータ（ABR）
  - AS 内の複数エリアに接続しているルータ
- Autonomous System Boundary ルータ（ASBR）
  - 他の自律システム(AS)に接続しているルータ
  - 他 OSPF との ASBR にはなれません。
- バックボーンルータ
  - バックボーンエリアへのインタフェースを持つルータ

IX2000/IX3000 で利用可能な OSPF のネットワークリンク

- トランジットネットワーク
- スタブネットワーク
- バーチャルリンクネットワーク
- ポイントツーポイントネットワーク
- NBMA（Non-Broadcast Multi-Access）ネットワーク

(a)OSPF の起動/再起動

OSPF を動作させるためには、OSPF プロセスを有効にする必要があります。OSPF を動作させるためには以下のコマンドを使用します。

ip router ospf	OSPFv2 動作開始/OSPF コンフィグモード移行 （グローバルコンフィグモード）
clear ip ospf process	OSPFv2 プロセス再起動 （グローバルコンフィグモード）

ipv6 router ospf	OSPFv3 動作開始/OSPF コンフィグモード移行 （グローバルコンフィグモード）
clear ipv6 ospf process	OSPFv3 プロセス再起動 （グローバルコンフィグモード）

【設定例】
基本的な OSPF の設定

```
ip router ospf 100
   area 0
   network GigaEthernet0.0 area 0
!
interface GigaEthernet0.0
   ip address 192.168.1.254/24
   no shutdown
```

```
ipv6 router ospf 100
   router-id 0.0.0.1
   area 0
   network GigaEthernet0.0 area 0
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 address 2001:db8:1::1/64
   no shutdown
```

※OSPF プロセス番号は、装置間で一致させる必要はありません。
※IX2000/IX3000 で同時に動作可能な OSPF プロセスは装置に対して 1 つです。

(b)ルータ ID

OSPF では、ルータを一意に認識できるようにルータ ID をもちます。ルータ ID を設定するには以下のコマンドを使用します。
ルータ ID は OSPFv2 と OSPFv3 で動作が異なりますので注意してください。

- OSPFv2
  ルータ ID はインタフェースに割り当てられている IP アドレスのうちのいずれかになります。
  ルータ ID を任意に設定することも可能です。

- OSPFv3
  必ずルータ ID を設定する必要があります。
  ルータ ID を設定していない場合は、OSPF は起動しません。

router-id	ルータ ID の設定 （OSPFv2/OSPFv3 コンフィグモード）

設定後の値を有効にするためには、clear ip/ipv6 ospf process が必要です。restart の場合は、ID 変更通知を周囲のルータに広告しないため、一時的に経路情報が不安定になります。

(c)経路計算タイマの設定

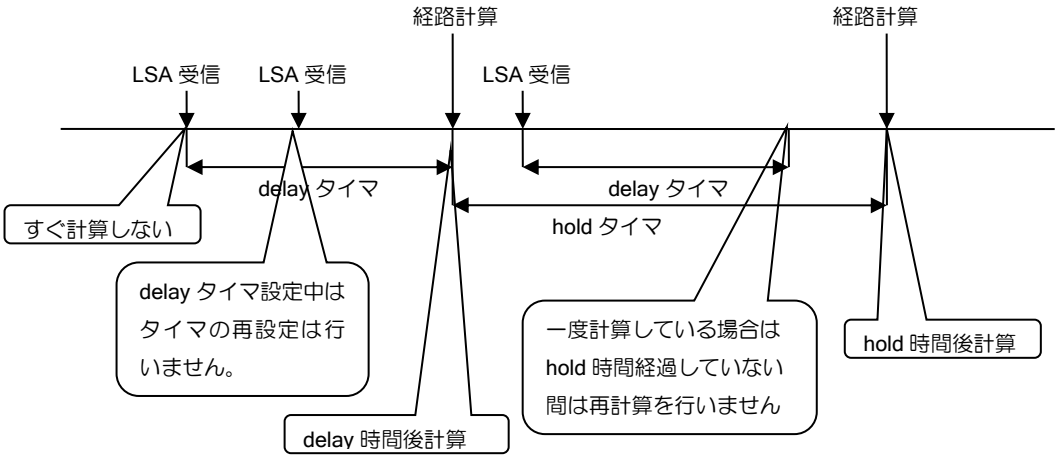
OSPF では、ルータの負荷を軽減するためトポロジ変化時にすぐに経路計算を行わず、タイマを設定することで、複数のトポロジ変化をまとめて経路計算を行います。

以下のタイマに関して変更が可能です。

- delay（デフォルト 5 秒）
  トポロジ変化を検出（LSA を受信）してから経路計算を行うまでの時間。
- hold（デフォルト 10 秒）
  一度経路計算を行ってから次の計算を行うまでの時間

トポロジ変化（LSA 受信）と経路計算のタイミングは以下のようになります。

デフォルトでは、トポロジ変化後 5 秒後に計算を行います。また、1 度経路計算を行っている場合には、10 秒間経路計算は行いません。



タイマ設定コマンドは以下のとおりです。

timers	経路計算タイマの設定 （OSPFv2/OSPFv3 コンフィグモード）

【設定例】

delay タイマを 10 秒，hold タイマを 15 秒に設定。

```
ip router ospf 100
   timers delay 10 hold 15
   area 0
   network GigaEthernet0.0 area 0

ipv6 router ospf 100
   router-id 0.0.0.1
   timers delay 10 hold 15
   area 0
   network GigaEthernet0.0 area 0
```

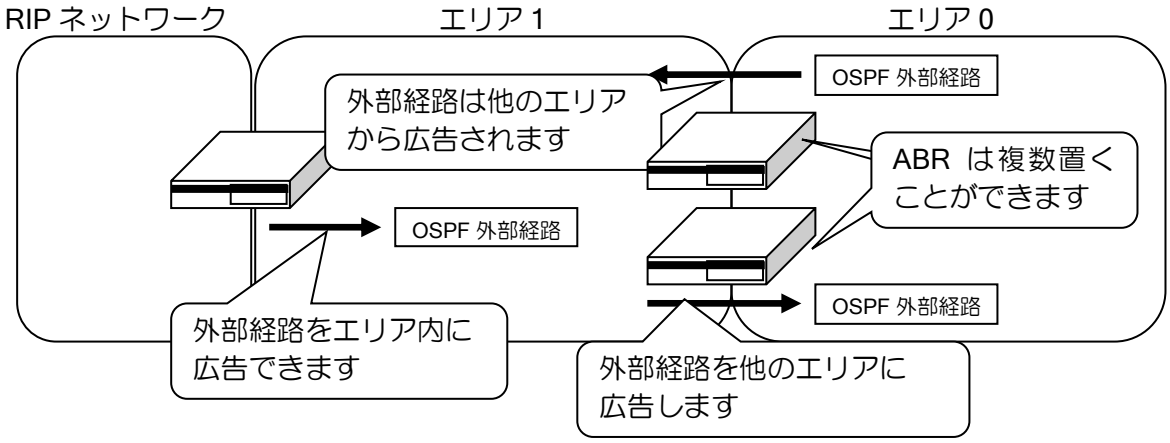
※エリア間経路（タイプ 3 LSA）、OSPF 外部経路（タイプ 5 LSA）、NSSA 外部経路（タイプ 7 LSA）の更新時はタイマを設定せずに経路計算を行います。ただし、タイマ設定中に更新された場合は、タイマ満了後に経路計算を行います。

2.22.5.1 エリアの設定

IX2000/IX3000 では以下のエリアをサポートしています。

- エリア

通常のエリアです。エリア内に AS 境界ルータ（ASBR）を置くことができ、OSPF 外部経路を広告できます。また、他のエリアからの OSPF 外部経路（タイプ 5 LSA）も広告されます。エリア境界ルータを複数置くことができます。

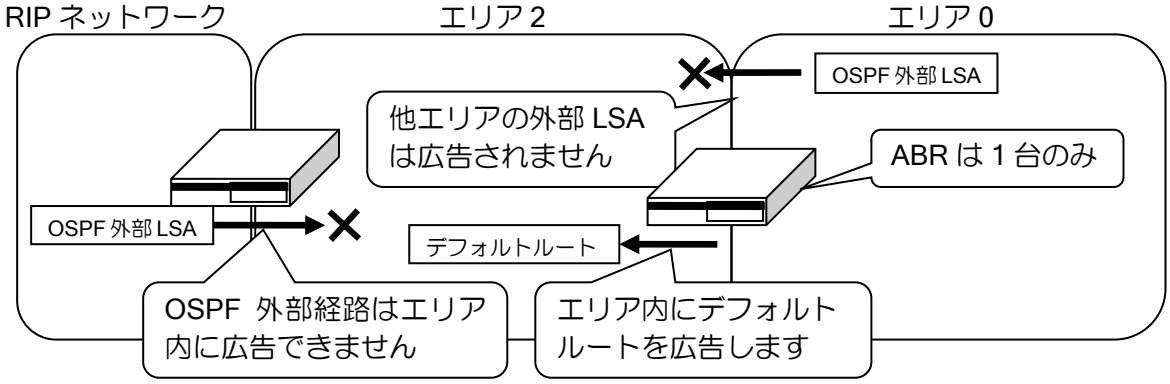


- スタブエリア

エリア内のエリア境界ルータ（ABR）が 1 台のみの場合に設定できます。

エリア内には ABR 宛のデフォルトルートがエリア内に広告されます。ABR が 1 台のみのため、エリア内の他のルータは ABR 宛のデフォルトルートを受信することにより、OSPF エリア間、OSPF 外部との通信が可能となります。このため、エリア間経路、OSPF 外部経路はエリア内に広告する必要がなくなりますので、エリア内で扱う経路数を減らすことができ、エリア内のルータの負荷を軽減することができます。

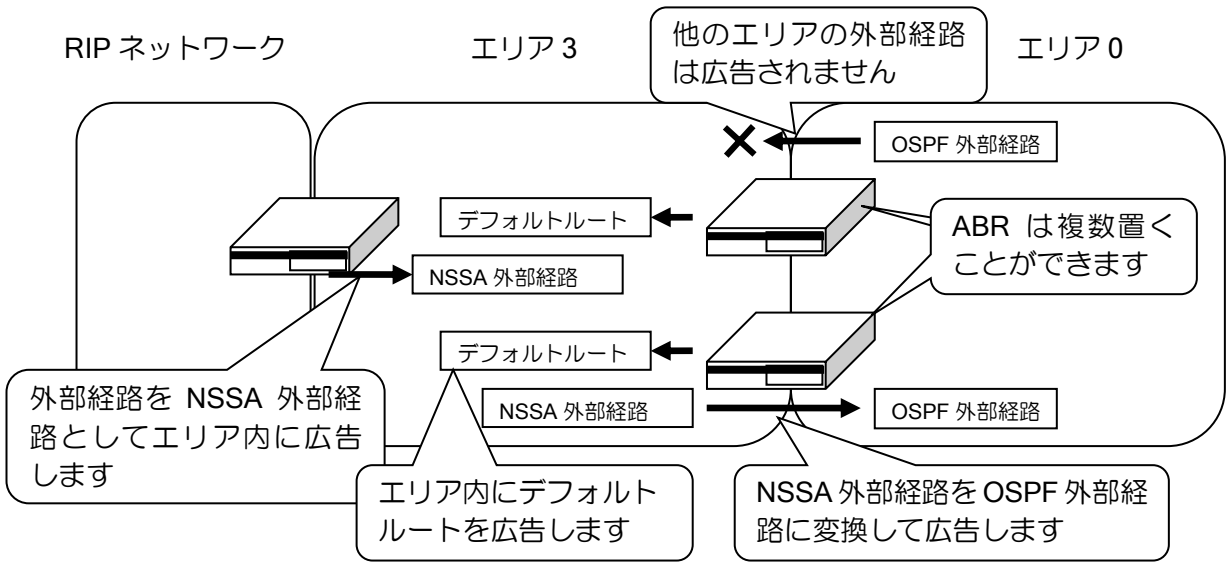
また、スタブエリア内では、OSPF 外部経路は扱えませんので、エリア内では他のプロトコルからの再配信を行うことができません。



- NSSA（Not So Stubby Area： IPv4 のみ）

スタブエリアと同様に、ABR 宛のデフォルトルートを広告することにより OSPF エリア間、OSPF 外部との通信が可能となるため、エリア内にエリア間経路、OSPF 外部経路を広告する必要がありません。エリア内で扱う経路数を減らすことができ、エリア内のルータの負荷を軽減することができます。

スタブエリアではエリア内に他のプロトコルからの経路の再配信を行うことができませんでしたが、NSSA では、NSSA 外部経路（タイプ 7 LSA）として広告することができます。NSSA 内では、NSSA 外部経路は OSPF 外部経路と同様に扱われます。また、NSSA 外部経路は、ABR において OSPF 外部経路へ変換されバックボーンエリアに広告されます。



(a)エリアの設定

OSPF では、AS 内のネットワークをバックボーンエリア（Area0 もしくは Area0.0.0.0 で表される）とそれに接続されるエリアの 2 階層の構成で運用されます。どのエリアも必ずバックボーンエリアに接続されている必要があり、各エリア間の通信はバックボーンエリアを通して行われます。それぞれのエリアは、32 ビットのエリア ID で区別され、以下のコマンドにて設定します。

area	エリアの登録 （OSPFv2/OSPFv3 コンフィグモード）

(b) エリアレンジの設定

エリア境界ルータにてエリア内のサブネットアドレスを指定の範囲で集約し、他のエリアに広告します。他のエリアに対して内部の細かい情報を集約することで、データベースの大きさを小さくすることができます。また、登録したレンジを広告しない設定もできます。

area AID range	レンジの設定 （OSPFv2/OSPFv3 コンフィグモード）

【設定例】

area1 の経路を 10.0.0.0/16 に集約して area0 へ広告

```
ip router ospf 100
   area 0
   area 1
   area 1 range 10.0.0.0/16 advertise
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 1
```

area1 の経路を 2001:db8:1::/48 に集約して area0 へ広告

```
ipv6 router ospf 100
   area 0
   area 1
   area 1 range 2001:db8:1::/48 advertise
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 1
```

(c)スタブエリアの設定

スタブエリアでは、ABR からデフォルトルートがエリア間経路として広告されます。他エリアのエリア間経路はエリア内に広告するか、しないかを選択できます。

設定コマンドは次のとおりです。

area AID stub	スタブエリアの設定 （OSPFv2/OSPFv3 コンフィグモード）
area AID default-cost	スタブエリアのデフォルトコスト設定 （OSPF v2/OSPFv3 コンフィグモード）

【設定例】

area1 をスタブエリアに設定。
area1 にエリア間経路を広告しない。

```
ip router ospf 100
   area 0
   area 1
   area 1 stub no-summary
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 1

ipv6 router ospf 100
   area 0
   area 1
   area 1 stub no-summary
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 1
```

(d)NSSA の設定（IPv4 のみ）

NSSA では、ABR からデフォルトルートが NSSA 外部経路として広告されます。スタブエリアと同様に、他エリアのエリア間経路はエリア内に広告するか、しないかを選択できます。

設定コマンドは次のとおりです。

area AID nssa	NSSA の設定（OSPFv2 コンフィグモード）

【設定例 1】

area2 を NSSA に設定。
area2 にエリア間経路を広告しない。

```
ip router ospf 100
   area 0
   area 2
   area 2 nssa no-summary
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 2
```

【設定例 2】
area2 を NSSA に設定。
area2 に広告するデフォルトルートのコストを 5，ルートタイプ 1 に設定。

```
ip router ospf 10
   area 0
   area 2
```

```
   area 2 nssa default-metric 5 default-metric-type 1
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 2
```

- NSSA 外部経路から OSPF 外部経路（タイプ 5 LSA）への変換

NSSA では ABR において、NSSA 外部経路を OSPF 外部経路へ変換して、バックボーンへ広告します。この変換を行うルータをトランスレータと言います。

トランスレータの設定を行っているルータはすべて変換を行います。トランスレータの設定を行っているルータが存在せず、NSSA 内で複数の ABR が存在する場合、1 台のみトランスレータとして選択されます。トランスレータは、ルータ ID が大きいルータが選択され、トランスレータに設定されたルータ、または、ルータ ID が大きいルータが現れると、一定時間（スタビリティインターバル）経過後、変換処理を停止します。

```
【設定例 1】
トランスレータとして動作するように設定

ip router ospf 10
   area 0
   area 2
   area 2 nssa translate
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 2

【設定例 2】
スタビリティインターバルを 60 秒に設定

ip router ospf 10
   area 0
   area 2
   area 2 nssa stability-interval 60
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 2
```

- NSSA レンジの設定

NSSA の ABR において、NSSA 内で生成した NSSA 外部経路をバックボーンに OSPF 外部経路として広告する際に、経路を集約して広告することができます。

設定コマンドは以下の通りです。

nssa-range	NSSA のレンジ設定（OSPFv2 コンフィグモード）

```
【設定例】
area2 の NSSA 外部経路を 192.168.0.0/16 に集約して area0 へ広告。

ip router ospf 10
   area 0
   area 2
   area 2 nssa no-summary
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 2
   nssa-range 192.168.0.0/16
```

2.22.5.2 インタフェースの設定

(a)OSPF インタフェースの設定

OSPF を動作させるためには、OSPF が動作するインタフェースの設定を行う必要があります。パラメータには、インタフェース名，IP アドレスどちらでも指定可能です。IP アドレスを指定した場合は、該当するインタフェースにおいて OSPF が動作します。

network	OSPF インタフェースの設定 （OSPFv2/OSPFv3 コンフィグモード）

【設定例】

GigaEthernet0.0 で OSPF を動作

```
ip router ospf 100
   area 0
   network GigaEthernet0.0 area 0
```

GigaEthernet0.0 で OSPF を動作

```
ipv6 router ospf 100
   router-id 0.0.0.1
   area 0
   network GigaEthernet0.0 area 0
```

(b)コストの設定

OSPF では、コストを設定することによってトラフィックの経路の優先度を決めることができます。またコストを設定していない場合、そのインタフェースのコストは以下のようになります。計算結果が 1 より小さい場合は、1 となります（GigaEthernet インタフェースの場合等）。

- 通常のインタフェース　　：100M / インタフェースのスピード（bps）
- トンネルインタフェース　　：（100M / インタフェースのスピード（bps））×10

bandwidth コマンドにて、インタフェースの速度情報設定を行っている場合は、bandwidth コマンドの設定値をインタフェースのスピードとして使用します。

bandwidth コマンドで設定した値は、OSPFv2/OSPFv3 ともに反映されます。

ip ospf cost	OSPFv2 コストの設定 （インタフェースコンフィグモード）
ipv6 ospf cost	OSPFv3 コストの設定 （インタフェースコンフィグモード）
bandwidth	インタフェース帯域幅情報の変更 （Ver.5.2 以降、インタフェースコンフィグ）

(c) DR プライオリティの設定

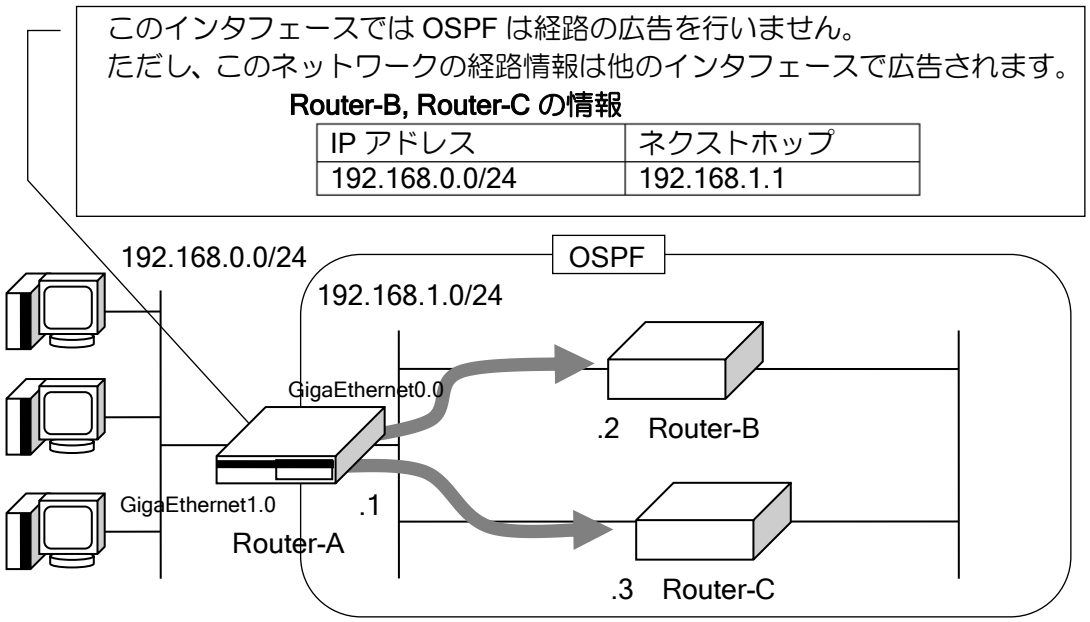
OSPF では、エリア内ルータで同じデータベースを維持する為にリンクステートの交換を行いますが、すべてのルータ同士でリンクステートを交換するわけではありません。そこで、同一ネットワーク内の OSPF ルータから 1 つの指名ルータ DR（Designated Router）、バックアップ指名ルータ BDR（Backup Designated Router）を選出し、DR が他の全 OSPF ルータとリンクステートの交換を行います。また、送信元ルータの DR、BDR へのなりやすさを以下のコマンドにて設定することができます。優先度を 0 にすることで、DR にも BDR にも絶対にならないようにすることもできます。

ip ospf priority	OSPFv2 ルータ優先度の設定 （インタフェースコンフィグモード）

ipv6 ospf priority	OSPFv3 ルータ優先度の設定 （インタフェースコンフィグモード）

(d) パッシブインタフェース

OSPF で経路を広告したくないインタフェースがあるが、そのインタフェースが属するネットワークの経路情報を他のインタフェースで使用している OSPF に広告する必要がある場合に設定します。OSPF ルーティング領域の端にあるルータにおいて設定されます。



passive-interface	パッシブインタフェースの設定 （OSPFv2/OSPFv3 コンフィグモード）

【設定例】

```
ip router ospf 100
   passive-interface GigaEthernet1.0
   area 0
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 0

ipv6 router ospf 100
   router-id 0.0.0.1
   passive-interface GigaEthernet1.0
   area 0
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 0
```

(e) タイマの設定

次のタイマの変更が可能です。

- hello interval（デフォルト 10 秒）
  Hello パケットを送信する間隔

- dead interval（デフォルト 40 秒）
  隣接ルータダウンを認識する時間。
- retransmit interval（デフォルト 5 秒）
  隣接ルータへのパケット再送間隔
- transmit-delay（デフォルト 1 秒）
  LSA 受信から他のルータへ広告するまでの時間

設定コマンドは次のとおりです。

ip ospf hello-interval	hello-interval の設定 （インタフェースコンフィグモード）
ip ospf dead-interval	dead-interval の設定 （インタフェースコンフィグモード）
ip ospf retransmit-interval	retransmit-interval の設定 （インタフェースコンフィグモード）
ip ospf transmit-delay	transmit-delay の設定 （インタフェースコンフィグモード）

ipv6 ospf hello-interval	hello-interval の設定 （インタフェースコンフィグモード）
ipv6 ospf dead-interval	dead-interval の設定 （インタフェースコンフィグモード）
ipv6 ospf retransmit-interval	retransmit-interval の設定 （インタフェースコンフィグモード）
ipv6 ospf transmit-delay	transmit-delay の設定 （インタフェースコンフィグモード）

(f) MTU 不一致無視設定

OSPF では、隣接関係を確立する際にお互いの MTU を交換し、異なる場合は隣接関係の確立を行いません（隣接状態が ExStart より先に進みません）。

IPsec トンネル使用時等、運用中に MTU が変更になる場合や、実装により MTU が合わない場合など、MTU 不一致により、隣接関係を確立することができない場合があります。

次の設定により、MTU が不一致でも隣接関係を確立することができます。ただし、MTU のチェックは対向するそれぞれのルータで行いますので、隣接のルータでも同様の機能が必要です

ip ospf mtu-ignore	MTU 不一致無視の設定 （インタフェースコンフィグモード）

ipv6 ospf mtu-ignore	MTU 不一致無視の設定 （インタフェースコンフィグモード）

(g) ネットワーク種別設定

ネットワーク種別は、デフォルトではインタフェース種別に応じた値が設定されますが、コマンドにより設定変更が可能です。設定コマンドは次のとおりです。

ip ospf network	ネットワーク種別設定 （インタフェースコンフィグモード）

(h) OSPF 認証

OSPF では、ルータ間で OSPF パケットの認証を行うことができます。例えば装置の交換や、ネットワークの接続ミスなどにより、不用意な OSPF パケットが流入してきて動作を不安定にさせ

ない効果が期待できます。
OSPF パケットの認証を行う場合、OSPFv2 と OSPFv3 では手順が異なります。
OSPFv2 の認証には、単純パスワード（Simple Password）、暗号化パスワード（MD5）の 2 つがあり、以下のコマンドにて設定することができます。

ip ospf authentication	認証の設定 （インタフェースコンフィグモード）
ip ospf authentication-key	単純パスワードの設定 （インタフェースコンフィグモード）
ip ospf message-digest-key	暗号化パスワードの設定 （インタフェースコンフィグモード）

OSPFv3 の認証には、IPsec を使用します。

2.22.5.3 隣接ルータの設定

(a) 隣接ルータの設定

ネットワークタイプが NBMA（Non-Broadcast Multiple Access）ネットワークの場合、マルチキャストは使用できませんので、ユニキャストでパケットを送信します。そのため、隣接ルータをスタティックに登録する必要があります。

ip ospf neighbor	隣接ルータの設定 （インタフェースコンフィグモード）

ipv6 ospf neighbor	隣接ルータの設定 （インタフェースコンフィグモード）

2.22.5.4 経路制御の設定

(a) デフォルトルート広告

OSPF を使用する場合において、広告するルート情報にデフォルトルートを含めることができます。次の設定を行うことで、外部経路としてデフォルトルートを広告します。

originate-default	OSPF でデフォルトルートを広告する （OSPFv2/OSPFv3 コンフィグモード）

【設定例】
常にデフォルトルートを広告

```
ip router ospf 100
  originate-default always
  area 0
  network GigaEthernet0.0 area 0

ipv6 router ospf 100
  router-id 0.0.0.1
  originate-default
  area 0
  network GigaEthernet0.0 area 0
```

デフォルトルート広告の設定を”always”に設定した場合は、設定を行ったルータ自身のデフォルトルートの有無にかかわらず、常にデフォルトルートを広告します。”always”を指定しない場合は、自ルータがデフォルトルートを持っている場合のみ、デフォルトルートを広告します。また、デフォルトルート広告の設定を行わない場合でも、デフォルトルートを持っているプロトコルの再配信を行うことでも、デフォルトルートは広告されます。（always 設定は IPv4 のみ）

(b) 経路再配信

IX2000/IX3000 シリーズでは、OSPF 利用時において OSPF 以外のルーティング情報を再配信することができます。NSSA 内では NSSA 外部経路、その他のエリアでは OSPF 外部経路として広告されます。スタブエリアでは再配信は行うことができません。

再配信時のコストは以下の優先度で設定されます。

- route-map で設定したコスト
- redistribute のパラメータで設定したコスト
- default-metric で設定したコスト
- 何も設定しない場合：IPv4 の場合 1
  IPv6 の場合 再配信元のメトリック

redistribute	OSPF 以外のルーティング情報を OSPF で再配信 （OSPFv2/OSPFv3 コンフィグモード）
default-metric	経路再配信時のメトリック設定 （OSPFv2 コンフィグモード）

【設定例】

GigaEthernet0.0 インタフェースにおいて OSPF を動作させ、RIP で学習した経路を OSPF 経路に通知します。

```
ip router ospf 100
  redistribute rip metric 10
  area 0
  network GigaEthernet0.0 area 0

ipv6 router ospf 100
  router-id 0.0.0.1
  redistribute rip metric 10
  area 0
  network GigaEthernet0.0 area 0
```

redistribute はルートマップ設定、プレフィックスリスト設定の後に行ってください。redistribute 設定後にルートマップ設定、プレフィックスリスト設定の変更を行った場合、プロセスの再起動（clear ip/ipv6 ospf process）が必要です。

(c) 経路再配信（ルートマップ設定）

経路再配信オプションに、ルートマップオプションを利用することにより、再配信経路をさらに詳細に制御することが可能となります。経路再配信で利用するルートマップのマッチ条件とセット条件には以下があります。ルートマップの詳細は、ルートマップの項を参照してください。

route-map	ルートマップを設定します。
match interface	出先インタフェースを条件とします。
match ip address prefix-list	IPv4 宛先アドレスを条件とします。
match ipv6 address prefix-list	IPv6 宛先プレフィックスを条件とします。
match ip next-hop prefix-list	IPv4 ネクストホップを条件とします。
match ipv6 next-hop prefix-list	IPv6 ネクストホップを条件とします。
match metric	メトリック値を条件とします。
match tag	タグ値を条件とします。
set metric	メトリック値を書き換えて再配信します。

set metric-type	OSPF メトリックタイプを指定して再配信します。
set tag	タグ値を書き換えて再配信します。
set ip next-hop	IPv4 ネクストホップを書き換えて再配信します。
set ipv6 next-hop	IPv6 ネクストホップを書き換えて再配信します。

(d) 経路フィルタ（IPv4 のみ）

ルータの経路情報（FIB: Forwarding Information Base）へ OSPF の経路を登録する際に、経路をフィルタすることができます。対象は OSPF のすべての経路になります。ネットワークのみ指定する場合は、プレフィックスリストを使用し、その他の条件を設定する場合はルートマップを使用します。ルートマップでは、セット条件は適用されません。

FIB への書き込み時にフィルタするのみで、データベース送信の際にはフィルタは適用されないため、他のルータの経路情報には影響を与えません。そのため、設定の際はルーティングループが発生しないよう注意してください。

distribute-list	経路情報のフィルタ （OSPFv2 コンフィグモード）

【設定例】
172.16.0.0/24 の経路をフィルタします。

```
ip prefix-list route-filter 10 deny 172.16.0.0/24
ip prefix-list route-filter 20 permit any

ip router ospf 10
  distribute-list prefix route-filter
  area 0
  network GigaEthernet0.0 area 0
```

また、ルートマップで使用可能なマッチ条件は以下のとおりです。

route-map	ルートマップを設定します。
match interface	出先インタフェースを条件とします。
match ip address prefix-list	IPv4 宛先アドレスを条件とします。
match ip next-hop prefix-list	IPv4 ネクストホップを条件とします。
match metric	メトリック値を条件とします。
match tag	タグ値を条件とします。

OSPF への再配信を行っている場合、経路フィルタ適用前の経路が再配信されます。フィルタ適用により、OSPF の経路がフィルタされ他のプロトコルの経路が有効になっている場合、該当経路は再配信されませんので、該当経路のプロトコルの distance を OSPF より高くなるように設定してください。

(e) OSPF 最大エントリ数の設定

OSPFv2 で使用するアドレスエントリ数を設定することができます。本設定は、ip max-route コマンドと以下のような依存関係を持っています。

	rib max-entries 設定有	rib max-entries 設定無
ip max-route 設定有	rib max-entries で設定された値を使用する※1	ip max-route で設定された値を使用する※1※2
ip max-route 設定無	rib max-entries で設定された値を使用する※1	デフォルト値（2048）を使用する

※1 設定されたエントリ分のメモリが確保できない場合はデフォルト値を使用します。
※2 ip max-route unlimited と設定されている場合はデフォルト値を使用します。

rib max-entries	最大エントリ数を設定します。 （OSPFv2 コンフィグモード）

※この設定で扱うエントリ数とは、扱える経路数ではなく、OSPFv2 で使用するすべてのアドレスの総数となります。

(f) イコールコストマルチパス

OSPF では、同じコストの経路が複数ある場合、データトラフィックを各経路に分散して送信します。この他に、分散しない方法や（Best-Path）、パケットの始点終点アドレスおよびプロトコルのセット（フロー）ごとに分散させる方法（Per-flow）を選択することもできます。詳細はマルチパスの項を参照してください。

- AS 外部ルートのマルチパス

  AS 外部ルートのマルチパスは、次の 2 通りがあります。

  - 1 つの ASBR からルートを広告

    AS 外部ルートを広告している ASBR に対する同一コストの経路が複数存在する場合、マルチパスとなります。

  - 複数の ASBR から同一ルートを広告

    外部ルートタイプ 1 の場合は、ASBR までのコストと広告されるコストの合計が等しい経路が存在する場合、外部ルートタイプ 2 の場合は、ASBR までのコストが等しくかつ広告されるコストが等しいルートが存在する場合マルチパスとなります。

- ポイントツーポイントインタフェースのマルチパス

  トンネルインタフェースなどのポイントツーポイントインタフェースではマルチパスは対応していません。ポイントツーポイントインタフェースにおいて、マルチパスを使用する場合は、アドレスを設定し、ネットワーク種別設定コマンド（ip/ipv6 ospf network）にてインタフェース種別を broadcast に設定してください。

2.22.5.5 OSPF 状態の表示

OSPF のインタフェース、接続ルータ、エリア、LSA データベース、ルーティングテーブル、仮想リンク、および統計等の情報をコマンドで確認することができます。

show ip ospf area	OSPF エリアおよび各エリア内のノード数の一覧、又は詳細情報の表示
show ip ospf database	LSA データベースの一覧、又は詳細情報の表示

show ip ospf interface	OSPF が動作しているインタフェース状態の一覧、又は詳細情報の表示
show ip ospf neighbor	接続している OSPF ルータ状態の一覧、又は詳細の表示
show ip ospf rib	OSPF 内部のルーティングテーブル情報(RIB 情報)の表示
show ip ospf statistics	OSPF 統計情報の表示
show ip ospf virtual-links	OSPF 仮想リンク状態の一覧、又は詳細情報の表示

OSPF 内部ルーティングテーブルはパケットのルーティングで使用されるルーティングテーブルとは異なります。OSPF 経路計算により OSPF 内部ルーティングテーブルの情報が生成され、そこから経路をルータの経路情報（FIB: Forwarding Information Base）へ反映されます。

2.22.6 BGP4

BGP（Border Gateway Protocol）は AS（Autonomous System）間で動作する EGP（Exterior Gateway Protocol）の 1 つで、AS 間の経路交換を行うためのルーティングプロトコルです。

BGP4 では TCP（ポート：179）を使用し、1 対 1 の BGP セッションを確立し、経路情報の交換を行います。

BGP4 では以下のメッセージを使用します。

- OPEN メッセージ
  BGP セッションの確立のために使用します。
- UPDATE メッセージ
  経路情報の広告に使用します。セッション確立時はすべての経路情報を送信しますが、通常は経路情報の変更があった場合のみ広告を行います。
- KEEPALIVE メッセージ
  ピアの到達確認のためにピアの間で定期的に交換を行います。
  KEEPALIVE メッセージまたは、UPDATE メッセージが一定時間到達しない場合ピアへの到達確認が無くなったと判断し、セッションを切断します。
- NOTIFICATION メッセージ
  エラー検出をピアに通知するために使用します。

2.22.6.1 ピアの設定

BGP4 を動作させるためには、router bgp コマンドにより BGP コンフィグモードへ移行して設定を行います。また、アドレスファミリに対する設定を行う場合には、address-family コマンドにより BGP アドレスファミリモードへ移行します。

設定は以下のコマンドを使用します。

router bgp	BGP の動作開始 （グローバルコンフィグモード）
address-family	アドレスファミリの設定 （BGP コンフィグモード）
neighbor remote-as	ピアの設定 （BGP コンフィグモード）
neighbor description	ピア情報の記述 （BGP コンフィグモード）
neighbor shutdown	ピアの停止 （BGP コンフィグモード）
show ip bgp	パス情報の表示
show ip bgp neighbors	ピア情報の表示
show ip bgp summary	ピア情報の表示
clear ip bgp	ピアのリセット

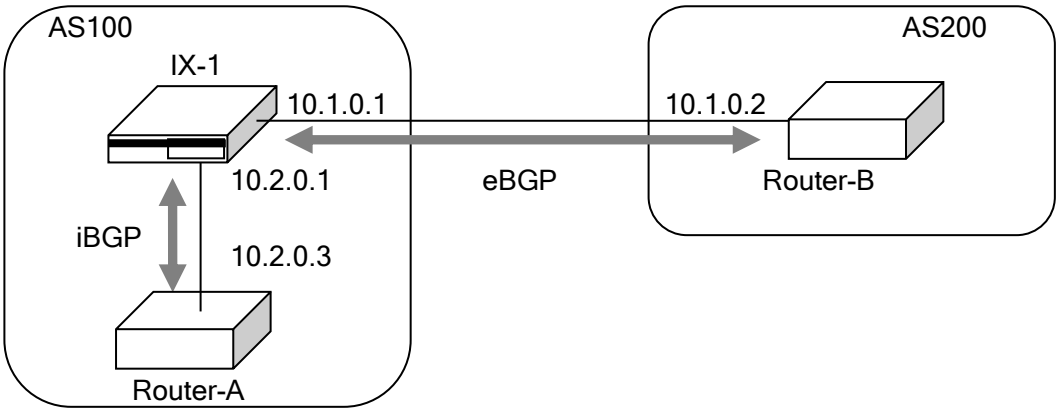
BGP のピアの種類には以下の 2 種類があります。

- eBGP（外部ピア）
  異なる AS 間での接続を eBGP（external-BGP）と呼びます。
  eBGP では、ピアは直接接続しているネットワークに接続している必要があります。
  直接接続していないネットワーク間で eBGP ピアを確立する場合は、マルチホップの設定が必要となります。

- iBGP（内部ピア）
  同一 AS 内での接続を iBGP（internal-BGP）と呼びます。

iBGP では、ピアは直接接続している必要はありませんが、RIP などの IGP を使用し、ピアへ到達できる必要があります。iBGP で学習した経路は、他の iBGP ルータへは広告を行いません。このため、同一 AS 内に複数の iBGP ルータが存在する場合、それらのルータはフルメッシュでピアを確立する必要があります。フルメッシュでピアを確立していない場合は、他のルータの経路が広告されないなどの問題が発生します。

設定の際は eBGP,iBGP の指定はありません。ピア指定時に自 AS と異なる AS を指定した場合は eBGP、同じ AS を設定した場合は iBGP として動作します。



【設定例】
ピアの設定例

```
router bgp 100
   neighbor 10.2.0.3 remote-as 100
   neighbor 10.2.0.3 description Router-A
   neighbor 10.1.0.2 remote-as 200
   neighbor 10.1.0.2 description Router-B
   address-family ipv4 unicast
      redistribute connected
```

(a)ルータ I D

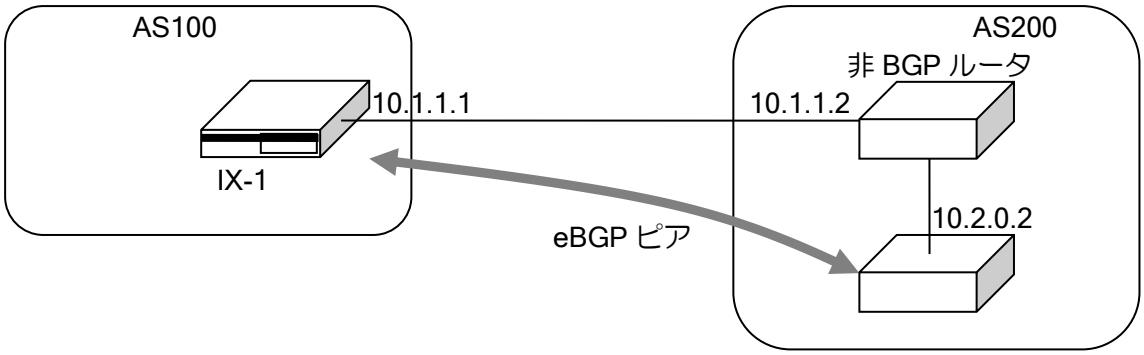
BGP では、ルータを一意に識別できるようにルータ ID を持ちます。ルータ ID はインタフェースに割り当てられている IP アドレスのうちのいずれかになります。ルータ ID の選択の方法については、付録のルータ ID セレクションの節を参照してください。ルータ ID を任意の値に設定するには、以下のコマンドを使用します。

router-id	ルータ ID の設定 （BGP コンフィグモード）

(b)マルチホップの設定

マルチホップ設定を行うことで、直接接続していないネットワーク間で eBGP ピアを確立することができます。通常は、直接接続したネットワークに接続するルータとピアを確立しますが、間に非 BGP ルータが存在する場合などには、直接接続していないルータ間で eBGP ピアを確立する必要があります。このような場合は、マルチホップの設定を行います。N 個先のルータと eBGP ピアを確立する場合は、ebgp-multihop のパラメータを N 以上に設定します。

neighbor ebgp-multihop	マルチホップの設定
show ip bgp neighbors	ピア情報の表示



【設定例】

マルチホップのピアの設定

```
router bgp 100
  neighbor 10.2.0.2 remote-as 200
  neighbor 10.2.0.2 ebgp-multihop 2
  address-family ipv4
    redistribute connected
```

(c)ソースアドレスの設定

ピアとの通信に使用するソースアドレスは、TCP パケットを送信するインタフェースを使用します。そのため、運用中にソースアドレスが変更になる場合があります。

ソースアドレスを固定にするために、ソースアドレスとして使用するインタフェースを指定することができます。指定したインタフェースがダウンしている場合は、TCP のセッションを確立することはできません。

neighbor update-source	指定ピアに対するソースアドレス指定

【設定例】

ソースアドレス指定の設定
ソースアドレスとして、GigaEthernet0.0 のアドレスを使用

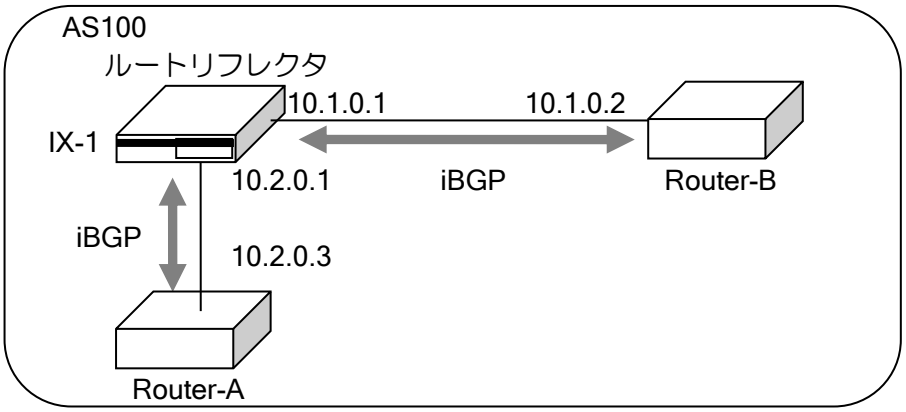
```
router bgp 100
  neighbor 10.2.0.2 remote-as 200
  neighbor 10.2.0.2 update-source GigaEthernet0.0
  neighbor 10.2.0.2 ebgp-multihop 2
  address-family ipv4
    redistribute connected
```

(d)ルートリフレクタの設定

iBGP ルータ間はフルメッシュで接続する必要があります。そのため、ルータ数が増えるとルータの負荷が高くなります。これを解決するためにルートリフレクタを使用します。

ルートリフレクタを設定することにより、iBGP ピアから学習した経路を別の iBGP へ広告できるようになります。これにより、各 BGP ルータはルートリフレクタを設定した BGP ルータ以外とはピアを確立する必要は無くなります。

IX2005 については未サポートとなります。



neighbor route-reflector-client	ルートリフレクタクライアントの設定
cluster-id	クラスタ ID の設定

【設定例】

10.1.0.2，10.2.0.3 のルータをルートリフレクタのクライアントとして設定。
クラスタ ID に 1000 を設定。

```
router bgp 100
   cluster-id 1000
   neighbor 10.1.0.2 remote-as 100
   neighbor 10.1.0.2 route-reflector-client
   neighbor 10.2.0.3 remote-as 100
   neighbor 10.2.0.3 route-reflector-client
```

(e)認証の設定

Ver.6.2 以降、ピア間で TCP を利用した MD5 認証を使用することができます。MD5 認証を使用することにより、不正なアクセスなどの攻撃による影響を低減することができます。

設定は次のとおりです。

neighbor password	MD5 認証設定

【設定例】
MD5 認証の設定

```
router bgp 100
   neighbor 10.2.0.2 remote-as 200
   neighbor 10.2.0.2 password NEC
   address-family ipv4
      redistribute connected
```

(f)タイマの設定

BGP で使用するタイマ値をコマンドにより変更することができます。
以下のタイマの設定を行うことができます。

- キープアライブタイム：キープアライブの送信間隔
- ホールドタイム：ピアが切断したと認識する時間
- 最小広告間隔：学習した経路をピアに広告する最小間隔
- TCP 再接続間隔：BGP セッション切断の状態から再度 TCP の接続を開始するまでの間隔

設定を有効にするにはピアのリセットが必要です。

キープアライブタイムを"0"に設定すると、キープアライブメッセージを送信しません。また、キープアライブタイムをホールドタイム以上に設定することはできません。

ホールドタイムは相手ピアとのネゴシエーションの結果、小さい方が採用されます。自ルータで設定したキープアライブタイムがネゴシエーションの結果決定したホールドタイム以上の場合は、キープアライブタイムがネゴシエーションの結果決定したホールドタイムの 3 分の 1 に設定されます。

タイマ値はピア毎に設定ができます。ピア毎の設定が無い場合は、全ピアに対するタイマ値を使用します。

timers	全ピアに対するタイマの設定
neighbor timers	指定ピアに対するタイマの設定
neighbor advertisement-interval	指定ピアに対する最小広告間隔
neighbor connect-interval	指定ピアに対する TCP 再接続間隔
show ip bgp neighbors	ピア情報の表示

【設定例】
全ピアのキープアライブタイムを 50 秒、ホールドタイムを 200 秒に設定
10.1.1.2 のピアのキープアライブタイムを 70 秒、ホールドタイムを 280 秒に設定
最小広告間隔を 10 秒に設定

```
router bgp 100
   timers 50 200
   neighbor 10.1.1.2 remote-as 200
   neighbor 10.1.1.2 timers 70 280
   neighbor 10.1.1.2 advertisement-interval 10
   address-family ipv4
      redistribute connected
```

(g)ケイパビリティの設定

BGP4 では、BGP セッションを確立する際にサポートしているケイパビリティのネゴシエーションを行い、双方のルータがサポートしているケイパビリティのみを使用します。

ケイパビリティは OPEN メッセージに設定されます。これにより、ピアルータのケイパビリティを知ることができます。自分がサポートしていないケイパビリティを受信した場合は、ピアへ NOTIFICATION メッセージを送信します。NOTIFICATION メッセージを受信することにより、ピアがサポートしていないケイパビリティを知ることができるので、そのケイパビリティを設定せずに、再度セッションの確立を行うことにより、お互いがサポートしているケイパビリティのみを使用できます。

IX2000/IX3000 シリーズでは以下のケイパビリティが使用可能です。

- IPv4 unicast：IPv4 ユニキャスト広告
- route-refresh：ルートの再広告要求

コマンドにより、ピアへ送信を行うケイパビリティを設定することができます。デフォルトでは、すべてのオプションを送信します。

また、受信時にケイパビリティを確認しない設定を行うことができます。これにより、IX2000/IX3000 がサポートしていないケイパビリティを受信した場合に、NOTIFICATION の送信を行いません。

これらの機能は、ピアのルータがケイパビリティのネゴシエーションをサポートしていない場合など、正常に BGP セッションが確立できない場合に使用し、自ルータのケイパビリティを調整することにより、正常に BGP セッションを確立することができるようになります。

neighbor send-capability	送信ケイパビリティの設定
neighbor receive-capability	受信ケイパビリティの設定
show ip bgp neighbors	ピア情報の表示

送信時のケイパビリティは、neighbor send-capability コマンドのパラメータに" multi-protocol"を指定した場合は IPv4 unicast，" route-refresh"を設定した場合は route-refresh が送信されます。

このコマンドは、OPEN メッセージでどのケイパビリティを送信するかを設定するコマンドです。従って、IPv4 unicast を送信しない設定にした場合でも、BGP セッションが確立できれば IPv4 の経路情報の広告は行います。

受信時のケイパビリティは、neighbor receive-capability コマンドで設定を行います。パラメータに" override"を指定した場合は、受信時のケイパビリティの確認を行いません。これにより、ピアから自ルータが処理できないオプションを受信した場合、IX2000/IX3000 では、これらのオプションを無視しますので、BGP のセッションが確立できます。

Ver.8.9 以降は、neighbor receive-capability コマンドはありません。未設定の状態でも受信時のケイパビリティの確認は行いません。

【設定例】
IPv4 unicast を送信、route-refresh を送信しない、受信時のケイパビリティの確認を行わない設定

```
router bgp 100
   neighbor 10.1.1.2 remote-as 200
   neighbor 10.1.1.2 receive-capability override
   no neighbor 10.1.1.2 send-capability route-refresh
   address-family ipv4
      redistribute connected
```

(h)パッシブモードの設定（Ver.10.9 以降）

自装置からのピア接続を開始しません。相手装置からの接続のみ可能です。

neighbor passive	パッシブモード設定

【設定例】

自装置からピア接続を行わず、相手装置から接続開始時に接続を行う

```
router bgp 100
   neighbor 10.2.0.2 remote-as 200
   neighbor 10.2.0.2 passive
   address-family ipv4
      redistribute connected
```

2.22.6.2 経路の制御

(a)デフォルトルート広告

広告する経路情報にデフォルトルートを含めることができます。

Ver.8.1 以降は、デフォルトルート広告の設定を"always"に設定した場合は、設定を行ったルータ自身のデフォルトルートの有無にかかわらず、常にデフォルトルートを広告します。"always"を設定しない場合は、自ルータがデフォルトルートを持っている場合のみ、デフォルトルートを広告します。また、デフォルトルート広告の設定を行わない場合でも、デフォルトルートを持っているプロトコルの再配信を行うことにより、デフォルトルートを広告することができます。

ピアへデフォルトルートの広告を行わない場合は、該当ピアのデフォルトルートの送信設定を削除してください。

Ver.8.0 以前では、デフォルトルートの広告設定を行うと、設定を行ったルータ自身がデフォルトルートの有無にかかわらず、デフォルトルートが広告されます。デフォルトルートの状態に合わせてデフォルトルートの広告を行うことはできません。

設定は BGP アドレスファミリモードで行います。コマンドは以下のとおりです。

originate-default	デフォルトルートの広告設定（全ピア） （BGP アドレスファミリモード）
neighbor originate-default	デフォルトルートの広告設定（指定ピア） （BGP アドレスファミリモード） （Ver.8.0 以前）
neighbor send-default	デフォルトルートの送信設定 （BGP アドレスファミリモード） （Ver.8.1 以降）

【設定例 1】（Ver.8.1 以降）
デフォルトルートがある場合にデフォルトルートを広告します
10.1.1.2 へ対してデフォルトルートを広告しません。

```
router bgp 100
  neighbor 10.1.1.2 remote-as 200
  neighbor 10.2.1.2 remote-as 300
  address-family ipv4
    originate-default
    no neighbor 10.1.1.2 send-default
    redistribute connected
    redistribute static
```

【設定例 2】
常にデフォルトルートの広告を行います。

（Ver.8.1 以降）

```
router bgp 100
  neighbor 10.1.1.2 remote-as 200
  neighbor 10.2.1.2 remote-as 300
  address-family ipv4
    originate-default always
    redistribute connected
    redistribute static
```

（Ver.8.0 以前）

```
router bgp 100
  neighbor 10.1.1.2 remote-as 200
  neighbor 10.2.1.2 remote-as 300
  address-family ipv4
    originate-default
    redistribute connected
    redistribute static
```

(b)経路再配信

BGP 以外のルーティング情報を再配信することができます。

経路再配信オプションに、ルートマップオプションを利用することにより、再配信経路をさらに詳細に制御することが可能となります。BGP の経路再配信で利用可能なルートマップのマッチ条件とセット条件には以下があります。ルートマップの詳細はルートマップの項を参照してください。

Ver.8.1 以降、再配信設定によりデフォルトルートを再配信されます。
Ver.8.0 以前では、再配信設定ではデフォルトルートは再配信されません。

redistribute	経路再配信の設定 （BGP アドレスファミリモード）
route-map	ルートマップ（グローバルコンフィグモード）
match ip address prefix-list	IPv4 宛先アドレスを条件とします。
match interface	インタフェースを条件とします。
match ip next-hop prefix-list	ネクストホップを条件とします。
match metric	メトリック値（MED）を条件とします。
match tag	タグを条件とします。
match community	コミュニティ属性を条件とします。（Ver.8.9 以降）
set ip next-hop	IPv4 ネクストホップを設定します。
set metric	メトリック値（MED）を設定します。
set as-path prepend	AS パスに AS 番号をプリペンドします。
set local-preference	ローカルプリファレンスの値を設定します。
set origin	オリジン属性を設定します。
set community	コミュニティ属性を設定します。（Ver.8.9 以降）

【設定例】

OSPF、スタティックの経路を再配信します。
スタティックルートの 192.168.0.0/24 の経路に対しては、ルートマップを用いてメトリックを 6 に設定します。その他の経路に対しては、メトリックは 5 を設定します。

```
ip prefix-list prf-list1 10 permit 192.168.0.0/24
ip prefix-list prf-list2 10 permit any

route-map stat-redist permit 10
   match ip address prefix-list prf-list1
   set metric 6

route-map stat-redist permit 20
   match ip address prefix-list prf-list2
!
router bgp 100
   default-metric 5
   neighbor 10.1.1.2 remote-as 200
   address-family ipv4
      redistribute ospf 1
      redistribute static route-map stat-redist
```

redistribute はルートマップ設定、プレフィックスリストの設定等の後に行ってください。redistribute 設定後に経路制御の設定の変更を行った場合、ピアのリセット（clear ip bgp）が必要です。

(c)経路広告

ネットワーク単位で広告する経路を設定することができます。設定した経路は、ルーティングテーブルに存在する場合のみに広告されます。

設定コマンドは以下のとおりです。

network	広告するネットワークの設定 （BGP アドレスファミリモード）

【設定例】

10.10.0.0/24 を広告します。

```
router bgp 100
  neighbor 10.1.1.2 remote-as 200
  address-family ipv4
    network 10.10.0.0/24
```

(d)経路の集約

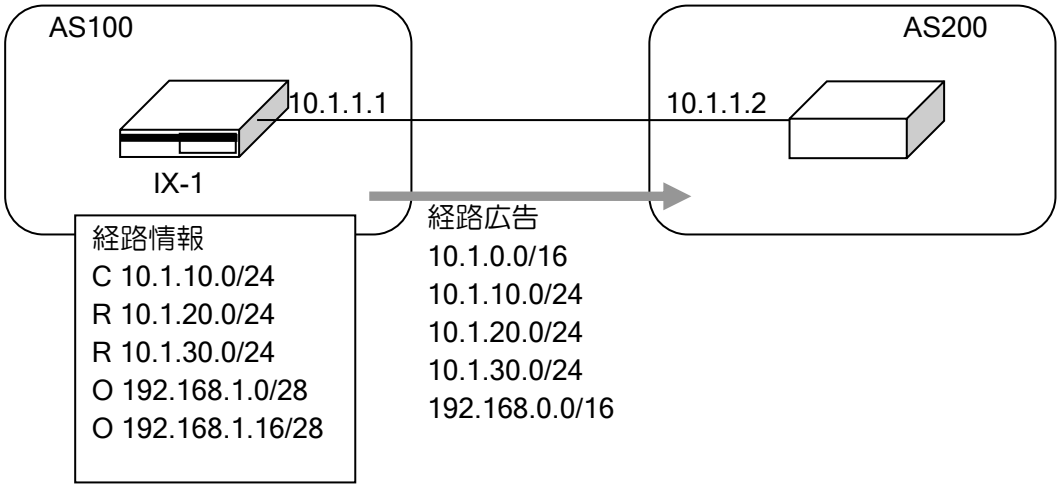
経路の集約には以下の種類があります。

- 指定したアドレスへの集約

aggregate-address コマンドを summary-only オプションなしで設定した場合は、指定した集約アドレスと、個々のルートの両方が広告されます。summary-only オプションをつけて設定した場合は、指定した集約アドレスのみが広告されます。

設定コマンドは以下の通りです。

aggregate-address	指定アドレスへの集約



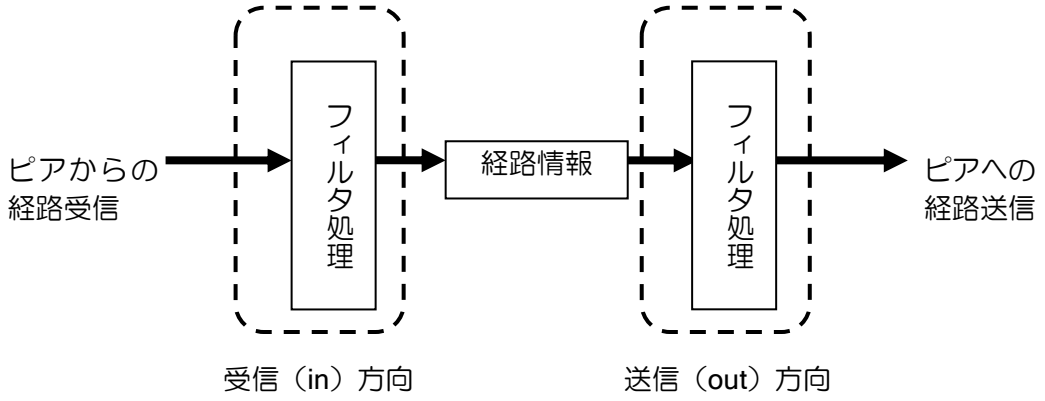
【設定例】

経路集約の設定

```
router bgp 100
  neighbor 10.1.1.2 remote-as 200
  address-family ipv4
    aggregate-address 10.1.0.0/16
    aggregate-address 192.168.0.0/16 summary-only
    redistribute connected
    redistribute rip
    redistribute ospf 1
```

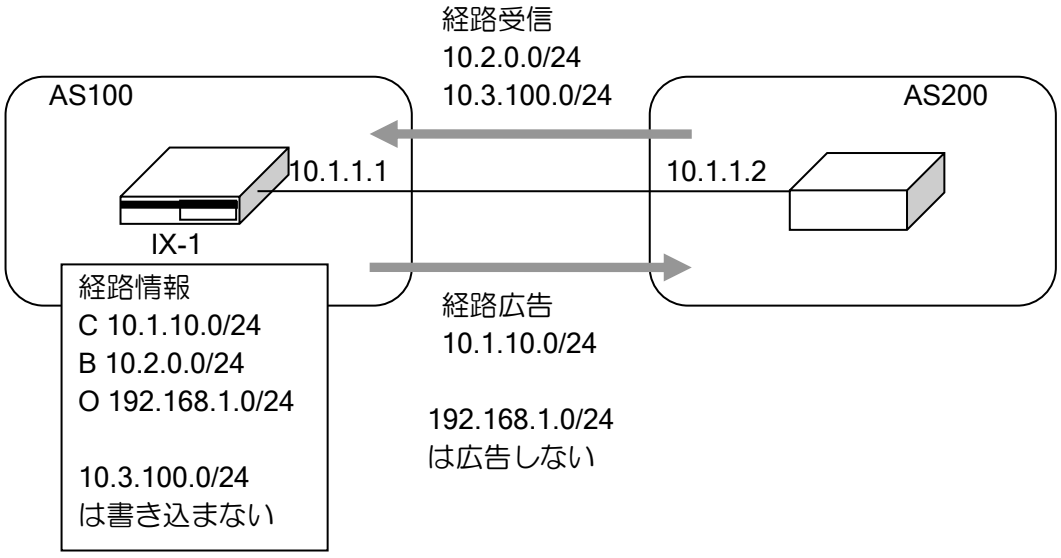
(e)経路フィルタ（プレフィックスリスト）

経路フィルタを使用することにより、受信する経路，送信する経路を制御することが可能です。
フィルタはピア毎に、受信（in）方向，送信（out）方向それぞれ別に設定が可能です。



設定は以下の通りです。
設定を有効にするには、ピアのリセットが必要です。

neighbor distribute-list	経路フィルタの設定



【設定例】

経路フィルタの設定

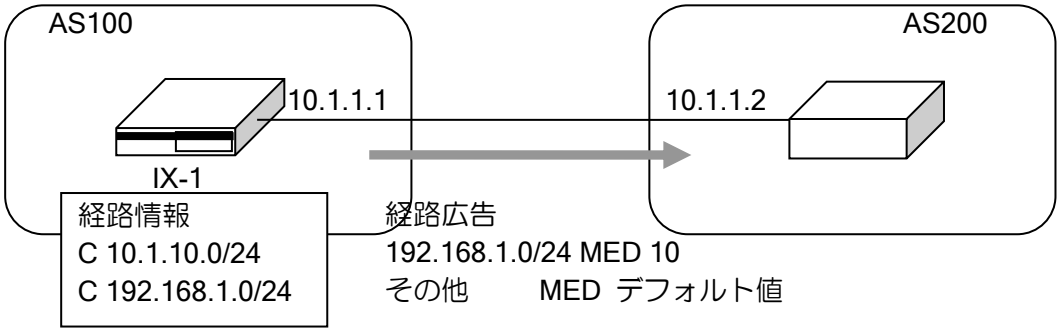
10.1.1.2 から、10.3.100.0/24 の経路は受信しない。
10.1.1.2 に対し、10.1.10.0/24 の経路のみ送信する。

```
ip prefix-list pref-in 10 deny 10.3.100.0/24
ip prefix-list pref-in 20 permit any
ip prefix-list pref-out 10 permit 10.1.10.0/24

router bgp 100
   neighbor 10.1.1.2 remote-as 200
```

```
  address-family ipv4
    neighbor 10.1.1.2 distribute-list pref-in in
    neighbor 10.1.1.2 distribute-list pref-out out
    redistribute rip
    redistribute ospf 1
```

(f)経路フィルタ（ルートマップ）

ルートマップを使用することにより、受信する経路（in）、または送信する経路（out）に対して、パス属性の変更等を更に詳細に制御することが可能となります。BGP で利用可能なルートマップのマッチ条件とセット条件には以下があります。ルートマップの詳細はルートマップの項を参照してください。



neighbor route-map	経路フィルタの設定
route-map	ルートマップ設定
match ip address prefix-list	IPv4 宛先アドレスを条件とします。
match ip next-hop prefix-list	ネクストホップを条件とします。
match metric	メトリック値（MED）を条件とします。
match community	コミュニティ属性を条件とします。（Ver.8.9 以降）
set ip next-hop	IPv4 ネクストホップを設定します。
set metric	メトリック値（MED）を設定します。
set metric-type internal	メトリックタイプを設定します。
set as-path prepend	指定した AS パスを付加します。
set local-preference	ローカルプリファレンスの値を設定します。
set origin	オリジン属性を設定します。
set community	コミュニティ属性を設定します。（Ver.8.9 以降）

【設定例】

10.1.1.2 に対し、192.168.0.0/24-192.168.255.0/24 の経路広告時に MED を+10、
他の経路は MED デフォルト値を広告

```
ip prefix-list prefix1 10 permit 192.168.0.0/16 max 24
ip prefix-list any-addr 10 permit any

route-map bgp1 permit 10
  match ip address prefix-list prefix1
  set metric +10
!
route-map bgp1 permit 20
  match ip address prefix-list any-addr
```

```
!
router bgp 100
   neighbor 10.1.1.2 remote-as 200
   address-family ipv4 unicast
      neighbor 10.1.1.2 route-map bgp1 out
      redistribute connected
```

2.22.6.3 パス属性

パス属性は、経路の特性を表すパラメータの集合です。BGP における最適経路の選択には、これらの属性を使用します。パス属性は、UPDATE メッセージの到達可能情報とともにピアに伝播されます。パス属性をうまく使うことにより、経路制御においてその AS のポリシーを反映させるなど、他の AS に自分の持つポリシーを伝えることができます。

BGP4 では以下の属性があります。

タイプ	属性	カテゴリ	サポート
1	ORIGIN	周知強制	○
2	AS_PATH	周知強制	○
3	NEXT_HOP	周知強制	○
4	MED（MULTI-EXIT-DISC）	オプション非通過	○
5	LOCAL_PREFERENCE	周知任意	○
6	ATOMIC_AGGREGATE	周知任意	○
7	AGGREGATOR	オプション通過	○
8	COMMUNITY	オプション通過	○ （Ver.8.9 以降）
9	ORIGINATOR	オプション非通過	○
10	CLUSTER_LIST	オプション非通過	○
14	MP_REACH_NLRI	オプション非通過	
15	MP_UNREACH_NLRI	オプション非通過	
16	EXT_COMMUNITY	オプション通過	

すべてのパス属性は以下の 4 つのカテゴリのいずれかに分類されます。

- 周知強制
  すべての BGP ルータがサポートしています。すべての UPDATE メッセージに含まれます。
- 周知任意
  すべての BGP ルータがサポートしています。UPDATE メッセージに含むかどうかは、任意となります。
- オプション通過
  サポートするかどうかはルータにより異なります。サポートしていない場合でも、他の BGP ルータへ伝えます。
- オプション非通過
  サポートするかどうかはルータにより異なります。サポートしていない場合、廃棄します。

ルートマップでサポートしているパス属性については任意の値が設定可能です。

以下に主なパス属性についての動作について説明します。

(a)オリジン属性

経路情報の出所を表します。次の 3 つが定義されています。

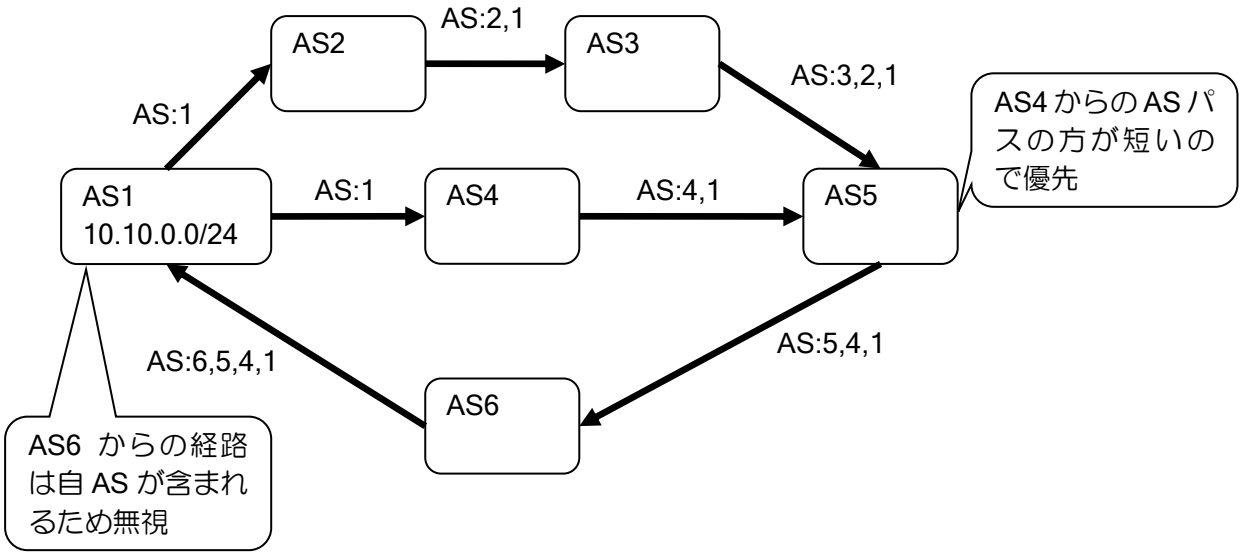
- IGP（タイプ 0）：IGP を通して学習した経路
- EGP（タイプ 1）：EGP を通して学習した経路
- INCOMPLETE（タイプ 2）：上記以外の別の手段で学習した経路

経路選択の際は、タイプの番号が低い方が優先されます。
ルートマップを使用することにより EGP を除く任意の値を設定できます。

(b)AS パス属性

経路情報が通過したパスを表す AS を格納します。各 AS は経路情報を AS 外部へ送信する際に自分の AS 番号をリストの先頭へ付け加えます。従って、AS パス属性には、経路が通過してきた AS 番号がすべて含まれています。経路受信時に AS 番号を確認することで、ループを防ぐことができます。また、AS パス属性は、最適経路の決定にも使用されます。2 つのルートを比較する際には AS パスが短いルートが長いルートより優先されます。

Ver.6.0 以降、ルートマップを使用することによって任意の値を設定（AS パスプリペンド）できます。



(c)ネクストホップ属性

BGP のネクストホップは次のいずれかになります。

- eBGP では、経路を広告したピアルータの IP アドレスがネクストホップとなります。
- iBGP では、AS 内で配信された経路については、経路を広告したピアルータのアドレスがネクストホップとなります。eBGP を通して AS に注入された経路については、eBGP から学習したネクストホップがそのまま iBGP へ広告されます。
- 経路再配信でルートマップにネクストホップを設定
- route-map コマンドでルートマップにネクストホップを設定

BGP のネクストホップは、IGP のネクストホップとは多少異なり、ネクストホップは複数のネットワークをまたがった先にある場合があります。その場合は、IGP などの経路情報によってネクストホップへ到達できる必要があります。

iBGP へ経路を広告する場合、iBGP へ広告を行うルータ自身をネクストホップとして設定することが可能です。設定コマンドは以下の通りです。

neighbor next-hop-self	ネクストホップ属性の自アドレス指定

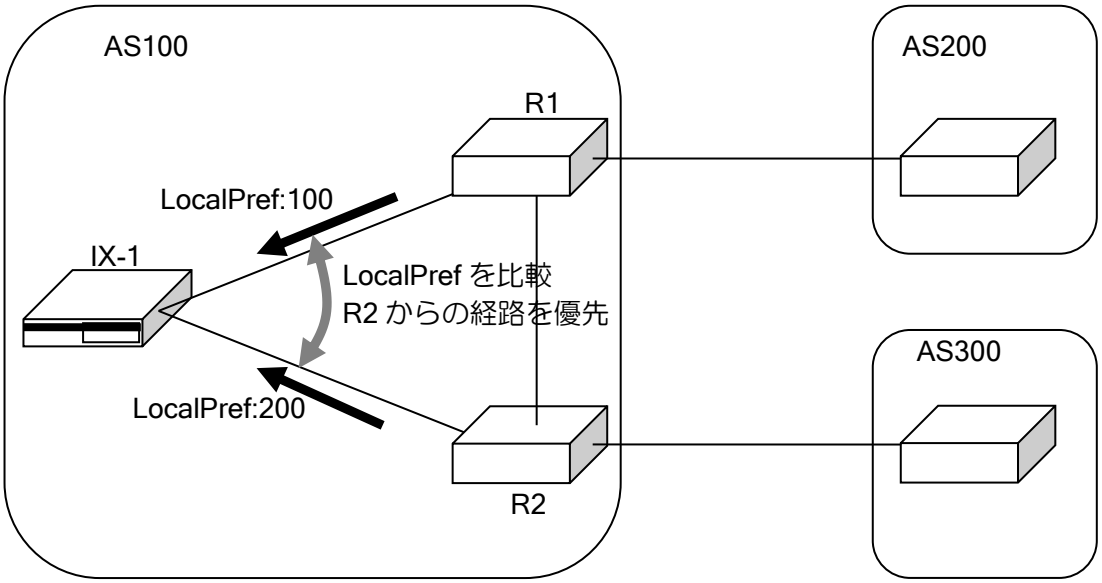
【設定例】
iBGP への経路広告時、ネクストホップに自アドレスを設定します。

```
router bgp 100
  neighbor 10.0.0.2 remote-as 100
  address-family ipv4
    neighbor 10.0.0.2 next-hop-self
```

(d)ローカルプリファレンス属性

ローカルプリファレンスは、AS 内での経路の優先度を決定するために使用します。AS 内では、ローカルプリファレンスの値が大きい経路が小さい経路より優先されます。ローカルプリファレンスは、eBGP から学習した経路に対して設定を行い、iBGP に広告します。AS 内では、同一の評価を行う必要があるので、AS 内のすべて BGP ルータに対して交換されます。AS 内でのみ有効な属性ですので、AS 外には送信されません。

ローカルプリファレンスを設定することにより、自 AS から他 AS に送信するデータの経路を制御することができます。



route-map を使用することにより任意の値を設定することができます。

eBGP から受信した経路の場合、経路受信時にデフォルトのローカルプリファレンス値が設定されます。

設定コマンドは以下のとおりです。

設定を有効にするには、ピアのリセットが必要です。

default-local-preference	デフォルトローカルプリファレンス設定
show ip bgp neighbor	ピアの状態確認

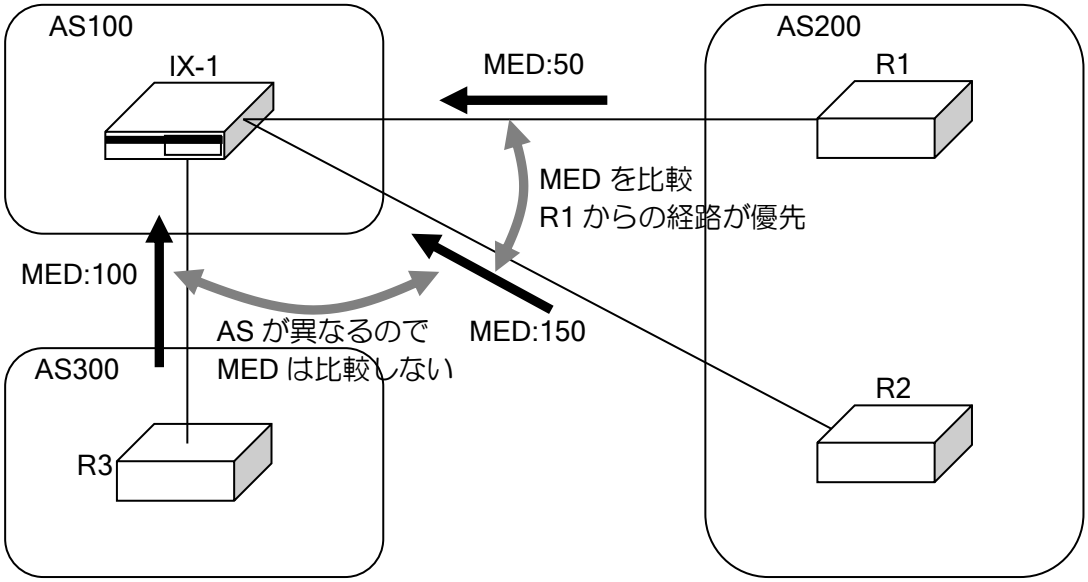
【設定例】
デフォルトローカルプリファレンスを 50 に設定します。

```
router bgp 100
  neighbor 10.0.0.2 remote-as 200
  default-local-preference 50
```

(e)MED 属性

MED は同じ AS に対して複数のピアが存在する場合に、経路の優先度を決定するために使用します。同じ AS の別なピアから、優先度が同じ経路を受信した場合、MED の値が低い経路が高い経路より優先されます。AS が異なるピアから受信した経路に対しては、MED の比較は行いません。MED は AS 間で交換されますが、受け取った MED は別の AS には送信しません。別な AS に経路を送信する際は、MED はゼロにクリアされます。iBGP へ送信する場合は、MED はそのままの値で送信します。

MED を設定することにより、相手 AS から自 AS へ送信されるデータの経路を制御することができます。



MED は、次の方法によって設定が可能です。

- 経路再配信の MED 指定
- 経路再配信でルートマップに MED を設定
- route-map コマンドを使用

経路再配信時に MED 未設定の場合，または network 設定時は default-metric にて設定した値を MED として設定します。default-metric が未設定の場合は、注入元の経路のコスト（IGP のコスト）を設定します。また、route-map コマンド設定時に MED 未設定の場合は、0 を設定します。

設定を有効にするには、ピアのリセットが必要です。

default-metric	デフォルトメトリック設定 （BGP コンフィグモード）

【設定例】

OSPF,スタティックの経路を再配信します。
スタティックルートに対しては、redistribute コマンドの metric オプションを用いてメトリックを 6 に設定します。その他の経路に対しては、メトリックは 5 を設定します。

```
router bgp 100
   default-metric 5
   neighbor 10.1.1.2 remote-as 200
   address-family ipv4
      redistribute ospf 1
      redistribute static metric 6
```

(f)コミュニティ属性

Ver.8.9 以降、コミュニティ属性を使用することができます。ルートマップを使用することにより、該当するコミュニティ属性を持つ経路情報の条件指定や、経路情報へコミュニティ属性を設定することができます。

コミュニティ属性は次の方法によって指定可能です。

- 経路再配信（ルートマップ指定）
- 経路フィルタ（ルートマップ指定）

コミュニティ属性の条件指定は、以下の指定が可能です。

- 指定したコミュニティ属性を含む経路情報
- 指定したコミュニティ属性と完全に一致する経路

【設定例】
コミュニティ属性に 0:10 と 0:20 が含まれる場合に MED 5 を設定

```
route-map bgp-map permit 10
  match community 0:10 0:20
  set metric 5
```

コミュニティ属性が 0:30 と 0:40 の場合に MED 5 を設定

```
route-map bgp-map permit 10
  match community 0:30 0:40 exact-match
  set metric 5
```

コミュニティ属性の設定は、以下の指定が可能です。

- コミュニティ属性の上書き
- コミュニティ属性の追加・削除

【設定例】
コミュニティ属性に 0:10 と 0:20 を上書き

```
route-map bgp-map permit 10
  set community 0:10 0:20
```

コミュニティ属性に 0:30 と 0:40 を追加、0:20 を削除

```
route-map bgp-map permit 10
  set community 0:30 0:40 additive delete 0:20
```

コミュニティ属性は、重複した値がある場合は 1 つにまとめます。受信したコミュニティ属性、設定したコミュニティ属性どちらの場合も重複している場合は、1 つの値として扱います。

Well-known コミュニティは、次の値に対応しています。

値	コマンド指定	動作
0xFFFFFF01	no-export	eBGP に広告しない
0xFFFFFF02	no-advertise	いずれのピアにも広告しない
0xFFFFFF03	no-export-subconfed	eBGP に広告しない

2.22.6.4 ピアグループ設定

Ver.9.2 以降、ピアグループを使用することにより、1 つの設定を複数のピアに対して適用することができます。

ピアグループでは以下の設定を行うことができます。

peer-group	ピアグループ設定 （BGP コンフィグモード）
neighbor	ピア設定
advertisement-interval	経路情報更新最小間隔設定
connect-interval	TCP 再接続待ち間隔設定
description	ピア情報設定
ebgp-multihop	eBGP マルチホップ設定
passive	パッシブモード設定（Ver.10.9 以降）
password	MD5 認証パスワード設定
route-reflector-client	ルートリフレクタクライアント設定
send-capability	送信ケーパビリティ設定
shutdown	ピア停止設定
timers	タイマ(Hold/Keepalive)値設定
update-source	ソースアドレス設定
address-family ipv4 distribute-list	経路フィルタ設定
address-family ipv4 next-hop-self	NEXTHOP 属性の自アドレス設定
address-family ipv4 route-map	ルートマップ設定
address-family ipv4 send-default	デフォルトルート送信設定

【設定例】
AS200 10.0.0.2、AS300 10.0.0.3 のピアに keepalive 30 秒、holdtime90 秒を設定

```
router bgp 100
   peer-group group1 remote-as 200
      neighbor 10.0.0.2
      neighbor 10.0.0.3 remote-as 300
      timers 30 90
```

上記設定例は以下と同等の設定となります。

```
router bgp 100
   neighbor 10.0.0.2 remote-as 200
   neighbor 10.0.0.2 timers 30 90
   neighbor 10.0.0.3 remote-as 300
   neighbor 10.0.0.3 timers 30 90
```

2.22.6.5 動的ピア接続

Ver.9.2 以降、ピアを範囲で指定することにより、固定の IP アドレスを指定せずに動的にピアと接続することができます。本機能を使用する場合は、自装置からは接続できません。相手装置からの接続によりピア接続を行います。また、設定はピアグループを使用します。設定は以下のとおりです。

listen range	動的ピア設定 （BGP ピアグループコンフィグモード）

【設定例】
10.0.0.0/24 の範囲のピアの接続。
AS は 200,300,400 の場合に接続。

```
router bgp 100
  peer-group group1 remote-as 200
    listen range 10.0.0.0/24 alternate-as 300 400
    timers 30 90
```

2.22.6.6 最適経路の決定

BGP では、同じ宛先の経路が存在する場合には、パス属性を用いて最適経路の決定を行います。以下の手順で最適経路を決定します。

（1）ネクストホップへ到達できない場合はその経路は使用しない。
（2）ローカルプリファレンスが最も高い経路が優先される。
（3）自ルータが生成した経路が優先される。
（4）AS パスが最も短い経路が優先される。
（5）オリジン属性のタイプ番号が最も低い経路が優先される。
（6）隣接する外部 AS への経路が複数存在する場合、MED の低い経路が優先される。
（7）iBGP の経路より eBGP の経路が優先される。
（8）ネクストホップへ最も近い（IGP のコストが低い）経路が優先される。
（9）ルータ ID が最も小さい BGP ルータからの経路が優先される。

最適経路として選択された経路が UPDATE メッセージによって他のピアへ送信されます。

2.22.6.7 マルチパスの設定

設定追加によりマルチパスとすることができます。（Ver.10.0 以降）
マルチパスのパケット転送動作についての詳細はイコールコストマルチパスの項を参照してください。
マルチパス設定時は、以下の条件の比較のみを行います。
すべての条件が同じ場合はマルチパスになります。ただし、他装置に広告する経路は、マルチパス未設定時と同様、ベストパスの経路のみとなります。

（1）ネクストホップへ到達できない場合はその経路は使用しない。
（2）ローカルプリファレンスが最も高い経路が優先される。
（4）AS パスが最も短い経路が優先される。
（5）オリジン属性のタイプ番号が最も低い経路が優先される。
（6）隣接する外部 AS への経路が複数存在する場合、MED の低い経路が優先される。
（8）ネクストホップへ最も近い（IGP のコストが低い）経路が優先される。

設定は以下のとおりです。

multipath	マルチパス設定 （BGP アドレスファミリコンフィグモード）

【設定例】
マルチパス数 4 に設定

```
router bgp 100
   address-family ipv4
      multipath 4
```

マルチパス設定時の注意事項は以下になります。

- （4）の AS パスについては、AS が同じ場合にマルチパスとなります。
- （8）の IGP のコストについては、IGP のプロトコル種別、コストが同じ場合にマルチパスとなります。マルチパス指定のオプションに ignore-igp-cost を指定した場合は IGP のコストの比較は行いません。
- パラメータで指定した数以上のマルチパスの経路がある場合、ルータ ID が大きい経路が優先されます。

2.22.6.8 NOTIFICATION

ピアが異常を検出した場合は、NOTIFICATION メッセージを送信し、接続を切断します。NOTIFICATION メッセージを確認することによって、異常の種類を知ることができます。

	エラーコード		エラーサブコード
1	メッセージヘッダエラー	1	接続が同期になっていない
		2	メッセージ長が正しくない
		3	メッセージタイプが正しくない
2	OPEN メッセージエラー	1	バージョン番号がサポートされていない
		2	ピア AS 番号が正しくない
		3	BGP 識別子が正しくない
		4	オプションがサポートされていない
		5	認証に失敗した
		6	ホールドタイマが受け入れられない
		7	ケイパビリティがサポートされていない
3	UPDATE メッセージエラー	1	属性リストが不正
		2	周知属性が識別できない
		3	周知属性がない
		4	属性フラグエラー
		5	属性長エラー
		6	オリジン属性が無効
		7	AS ルーティングループ
		8	ネクストホップ属性が無効
		9	オプション属性エラー
		10	ネットワークフィールドが無効
		11	AS パスが不正
4	ホールドタイマの時間切れ		
5	状態遷移の異常		
6	切断要求、上記以外のエラー		

主なエラーについての対処方法について説明します。

- エラーコード:2、サブコード:7
  - ➢ 原因
    - ✧ ピアが受信したケイパビリティをサポートしていない場合に発生します。
  - ➢ 対処方法
    - ✧ ピアに該当するケイパビリティを送信しないように設定を行ってください。
- エラーコード:4
  - ➢ 原因
    - ✧ ホールドタイマの間、ピアが自装置の UPDATE または KEEPALIVE のいずれも受信していない場合に発生します。ピアの NOTIFICATION は受信しているので、自装置からの送信または、ピアのルータでの受信処理または、自装置からピア方向の通信路に異常があると考えられます。
  - ➢ 対処方法
    - ✧ ルータ，通信路の確認を行ってください。

2.22.7 ポリシールーティング

IX2000/IX3000 シリーズでは、送信先に基づいた経路選択（スタティックルーティングおよびダイナミックルーティング等）のみではなく、ポリシーに基づくポリシールーティングによる経路選択をサポート（Ver.2 以降）しています。ポリシールーティングを使用することにより、ルーティングテーブルによる経路制御に加えて、より細かな経路制御が可能となります。

ESP パケットはポリシールーティングの対象外です。IKEv2 を使用する場合は ikev2 outgoing-interface コマンドをご使用ください。

Ver.4.3 以降では、UFS キャッシュを使用することにより、ポリシールーティングの転送が高速化します。UFS キャッシュについては、UFS キャッシュの項目を参照してください。

ポリシールーティングは、ルートマップやアクセスリストとの組み合わせにより、高度な経路制御を行うことができますが、ここでは最も代表的な構成例として、送信元によってトラフィックのルートを決定するソースルーティングを以下に説明します。

ポリシールーティングは、以下の 2 つの設定から構成されます。

- ルートマップによるトラフィックのポリシー設定
- ポリシールーティングを実施するトラフィックへのルートマップの適用

(a) ルートマップによるトラフィックのポリシー設定

ルートマップでトラフィックのポリシーを設定することにより、通常のルーティング処理ではできない、高度なルーティング処理をおこなうための条件設定や制御設定をおこなうことができます。

経路制御のポリシーの設定には、route-map コマンドを使用します。ルートマップの設定は、以下の 3 つのステップにより構成します。

- ルートマップの作成
- トラフィックのマッチ条件設定
- マッチしたトラフィックの動作設定

ルートマップの設定および確認には次のコマンドを使用します。

route-map	ルートマップ追加/ルートマップコンフィグモード
show route-map	ルートマップの状態表示

ポリシールーティングを行うためには、ルートマップを作成しておく必要があります。

【設定例】

```
route-map route1 permit 10
```

同一ルートマップ名で、シーケンス番号の違う複数のルートマップを作成した場合は、シーケンス番号の小さいルートマップから順次評価され、一番先にマッチしたルートマップが適用されます。

【設定例】

```
route-map route1 permit 10
   match ip address access-list rmap-acc1
!
route-map route1 permit 20
   match ip address access-list rmap-acc2
```

ポリシールーティングで制御するトラフィックをルートマップにマッチさせます。ポリシールー

ティングで利用可能であるルートマップのマッチ条件として以下の条件があります。
マッチ条件を設定しない場合は、すべてのパケットが対象となります。

- IPv4/IPv6 アクセスリストによるアドレス条件

match ip address access-list	IPv4 アクセスリストによるアドレス条件設定
match ipv6 address access-list	IPv6 アクセスリストによるアドレス条件設定

【設定例】

```
ip access-list rmap-acc1 permit ip src 10.10.10.1/32 dest any
ip access-list rmap-acc2 permit ip src 10.10.10.2/32 dest any
!
route-map route1 permit 10
   match ip address access-list rmap-acc1
!
route-map route1 permit 20
   match ip address access-list rmap-acc2
```

※ポリシールーティングで用いるルートマップのマッチ条件には、アクセスリストを使用します。
アクセスリストについての詳細は、アクセスリストの設定の節を参照してください。

ルートマップにマッチしたトラフィックに対する動作を設定します。ポリシールーティングで利用可能なルートマップの動作条件として以下の条件があります。
動作条件を指定しない場合は、ルーティング情報に従います。

set interface	送信インタフェース指定
set default interface	デフォルト送信インタフェース指定
set ip/ipv6 next-hop	IPv4/IPv6 ネクストホップ指定
set ip/ipv6 default next-hop	IPv4/IPv6 デフォルトネクストホップ指定

【設定例】

```
ip access-list rmap-acc1 permit ip src 10.10.10.1/32 dest any
ip access-list rmap-acc2 permit ip src 10.10.10.2/32 dest any
!
route-map route1 permit 10
   match ip address access-list rmap-acc1
   set ip next-hop 10.10.20.254
!
route-map route1 permit 20
   match ip address access-list rmap-acc2
   set ip next-hop 172.16.1.254
```

※送信インタフェース指定/デフォルト送信インタフェース指定は PPP や Tunnel などのポイントツーポイントネットワークで用いられます。Ethernet 等で設定を行った場合、ネクストホップアドレスが解決できないため、パケットのフォワーディングができなくなります。

(b) ルートマップの適用

ルートマップを適用するトラフィックに割り当てることによって、ポリシールーティングを行います。適用できるトラフィックの種類には、以下の 2 つがあります。

- 受信パケットに対するポリシールーティング

受信パケットに対してポリシールーティングを行うには、受信インタフェースのインタフェースコンフィグモードにおいて、ルートマップを適用します。

【設定例】

```
interface GigaEthernet0.0
  ip policy route-map v4route1
  ipv6 policy route-map v6route1
```

- ローカルパケットに対するポリシールーティング

telnet、ping 等ルータにて生成されたパケットに対してポリシールーティングを行うには、グローバルコンフィグモードにて、ルートマップを適用します。

【設定例】

```
ip local policy route-map localv4route1
```

(c) ポリシールーティング設定時の経路選択の優先順位

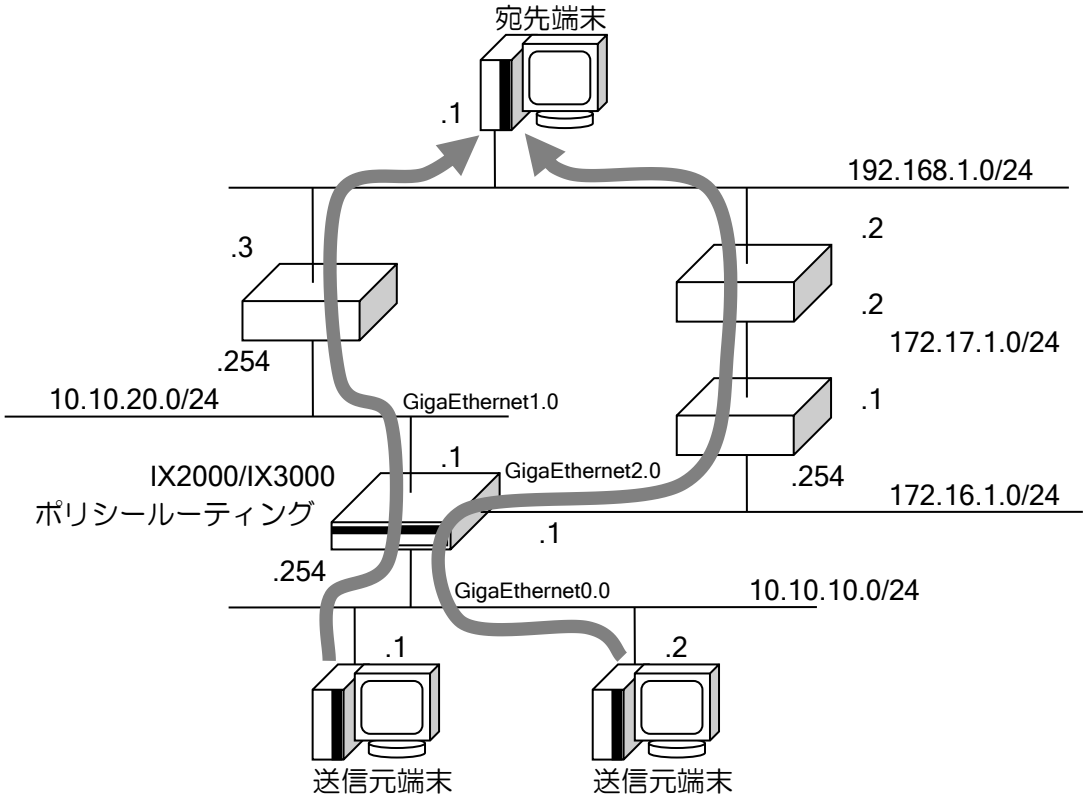
ポリシールーティングと、通常のルーティング（スタティックルーティングおよびダイナミックルーティング等）を同時に設定した場合の経路選択優先順位を示します。

ルーティングの優先度	優先度
set interface（インタフェースがリンクアップしていれば適用）	↑高
set ip/ipv6 next-hop（ネクストホップへの経路が存在すれば適用）	
通常のルーティング処理	
set default interface（経路が存在しない場合に適用）	
set ip/ipv6 default next-hop（経路が存在しない場合に適用）	↓低

2.22.7.1 ポリシールーティングの構成例

(a)ソースルーティング

ポリシールーティングに使用するアクセスリストに、送信元アドレスを指定することにより、特定の送信元からのパケットを通常のルーティングに従わずルーティングさせることができます。



【設定例】
10.10.10.1 の端末からのパケットは 10.10.20.254 へ転送
10.10.10.2 の端末からのパケットは 172.16.1.254 へ転送
その他は通常のルーティングに従う
（ルーティングの設定例は省略します）

```
ip access-list rmap-acc1 permit ip src 10.10.10.1/32 dest any
ip access-list rmap-acc2 permit ip src 10.10.10.2/32 dest any
!
route-map route1 permit 10
   match ip address access-list rmap-acc1
   set ip next-hop 10.10.20.254
!
route-map route1 permit 20
   match ip address access-list rmap-acc2
   set ip next-hop 172.16.1.254
!
interface GigaEthernet0.0
   ip address 10.10.10.254/24
   ip policy route-map route1
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.10.20.1/24
```

```
   no shutdown
!
interface GigaEthernet2.0
   ip address 172.16.1.1/24
   no shutdown
```

(b)DNS ルーティング

アクセスリストのドメイン名指定の不具合のため、現在使用を制限しています。

■2.23 マルチキャストの設定

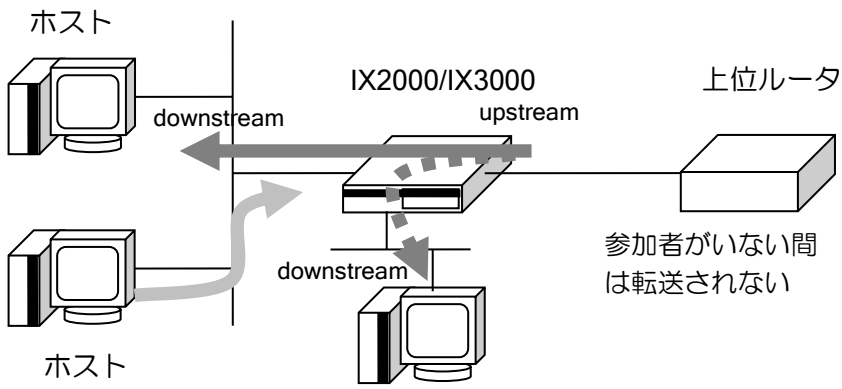
IX2000/IX3000 シリーズは、下記のマルチキャスト転送をサポートします。

- IPv4 IGMP プロキシ機能（IGMPv1/v2 サポート）
- IPv4 マルチキャスト スタティック転送
- IPv4 PIM-SM（Ver.8.4 以降サポート）
- IPv6 MLD プロキシ機能
  - MLDv1
  - MLDv2

2.23.1 機能概要

2.23.1.1 IGMP/MLD 機能概要

IGMP/MLD とは、マルチキャストを正しく受信者のみに転送するために、配下のホストが参加しているマルチキャストグループを管理するプロトコルです。ルータはマルチキャストグループごとにホストからの参加・離脱メッセージを処理し、参加者が存在するインタフェース全てに対してマルチキャストパケットを送信します。また、ルータからは定期的に参加者が存在しているかどうかの確認なども行われます。



2.23.1.2 IGMP/MLD プロキシ機能概要

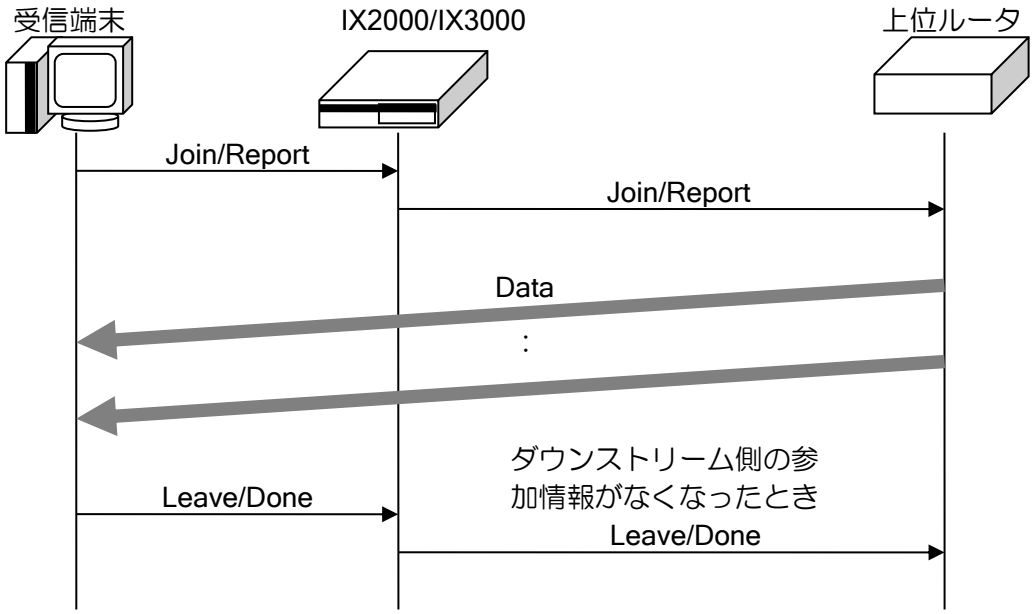
IGMP/MLD プロキシ機能は、以下のように動作することでマルチキャストを転送します。

IX2000/IX3000 のホスト側インタフェース（downstream）では、上位ルータの代わりに IGMP/MLD ルータとなり、ホストへ問い合わせを行います。ホストからの参加・離脱メッセージを受信すると、「マルチキャストアドレス」と「参加者の存在するインタフェース」からなるデータベースを構築すると同時に、マルチキャストルーティングエントリを作成します。上位ルータから該当するマルチキャストアドレスが送信されている場合には、ルーティング情報に従ってマルチキャストパケットを各インタフェースに送信します。

一方、上位ルータ側インタフェース（upstream）では、IGMP/MLD ホストとして振舞います。IX2000/IX3000 は、ホストからの情報を集約して構築したデータベースを基に、上位ルータからの問い合わせに対して代理応答します。また新規にマルチキャストアドレスの参加メッセージを受信した場合には、直ちに上位ルータへ参加メッセージを送信して、マルチキャストパケット転送を要求します。さらにホストが全て離脱したマルチキャストアドレスについては、上位ルータに離脱メッセージを送信して、パケット転送の停止を要求します。

※ IGMPv1 モードで動作中の場合には離脱メッセージはありませんので、上位ルータは一定時間応答のないことを検出して、マルチキャストパケットの転送を停止します。

このようにルータ/ホストのお互いを代理（プロキシ）することで、ホストからの参加・離脱メッセージが上位ルータとホストとの間で正しく処理され、IX2000/IX3000 はマルチキャストパケットをルーティングすることができるようになります。



2.23.1.3 PIM-SM 機能概要

PIM-SM はマルチキャストルーティングプロトコルです。マルチキャストを受信する端末が存在するインタフェースにのみマルチキャストパケットを転送します。

PIM-SM ではランデブーポイント（RP）が必要となります。ネットワーク内の全てのルータは RP のアドレスを認識している必要があります。RP はマルチキャストアドレス毎に設定しますが、複数のマルチキャストアドレスで 1 つの RP を使用することも可能です。

マルチキャストの受信端末は、IGMP を使用して受信要求を行います。端末からの要求は接続するルータ（Last Hop Router：LHR）を経由して RP に伝達され、RP をルートとしたツリー（共有ツリー）を構築します。マルチキャスト送信元端末からのパケットは接続するルータ（First Hop Router：FHR）から RP へ送信され、RP から共有ツリーを使用して受信端末へ転送されます。

送信元端末から受信端末への経路として、共有ツリーより最適な経路が存在する場合は、最短パスツリー（SPT）を形成します。これにより最適な経路を使用した転送を行うことが可能となります。

2.23.2 IPv4 マルチキャスト機能

IPv4 マルチキャスト機能を使用するには、以下の 3 種類の方法があります。

- IGMP プロキシ機能
- スタティック設定機能
- PIM-SM 機能（Ver.8.4 以降）

IGMP プロキシ機能を使用した場合は、ホストから要求のあるインタフェースにのみマルチキャストデータを転送します。スタティックに設定した場合は、無条件に設定したインタフェースに転送します。

IPv4 マルチキャストの設定は次のコマンドを使用します。

ip multicast-routing	IPv4 マルチキャスト機能の起動/停止
show ip mroute	マルチキャストルーティングテーブルの確認
show ip mcache	マルチキャストルーティングキャッシュの確認
clear ip mroute	マルチキャストルーティングテーブルの削除
clear ip mcache	マルチキャストルーティングキャッシュの削除

※ mcache が作成されるのは、ダウンストリームインタフェース数が 1 のマルチキャストグループアドレスのみです。参加者が複数のインタフェースにわたる場合は、コピー処理を行うため、キャッシュは削除されスローパスルーティングで処理されます。

2.23.3 IGMP プロキシ機能

IGMP プロキシの設定および確認は次のコマンドを使用します。

ip igmp upstream	アップストリームインタフェースの設定
ip igmp downstream	ダウンストリームインタフェースの設定
ip igmp query-interval	クエリ送信間隔の設定
ip igmp query-max-response-time	クエリ最大応答時間の設定
ip igmp version	IGMP の動作バージョン変更
show ip igmp group	グループメンバシップ情報の表示
show ip igmp interface	インタフェース情報の表示
show ip igmp proxy-cache	IGMP プロキシキャッシュ情報の表示

(a) IGMPv1/v2 対応ホストのみの場合

```
【設定例】
ip multicast-routing
interface GigaEthernet0.0
   ip address 10.1.1.1/24
   ip igmp upstream
   no shutdown
interface GigaEthernet1.0
   ip address 10.2.2.1/24
   ip igmp downstream
   no shutdown
```

(b) IGMPv3 対応ホストが存在する場合

IGMP 対応ホストは、一般的に同一リンク内でより低いバージョンの IGMP メッセージを受信すると、そのバージョンに状態遷移します。IX2000/IX3000 は IGMPv2 までのサポートですが、IX2000/IX3000 の General Query（デフォルト 125 秒間隔）を受信すると IGMPv3 対応ホストも IGMPv2 で動作するようになります。

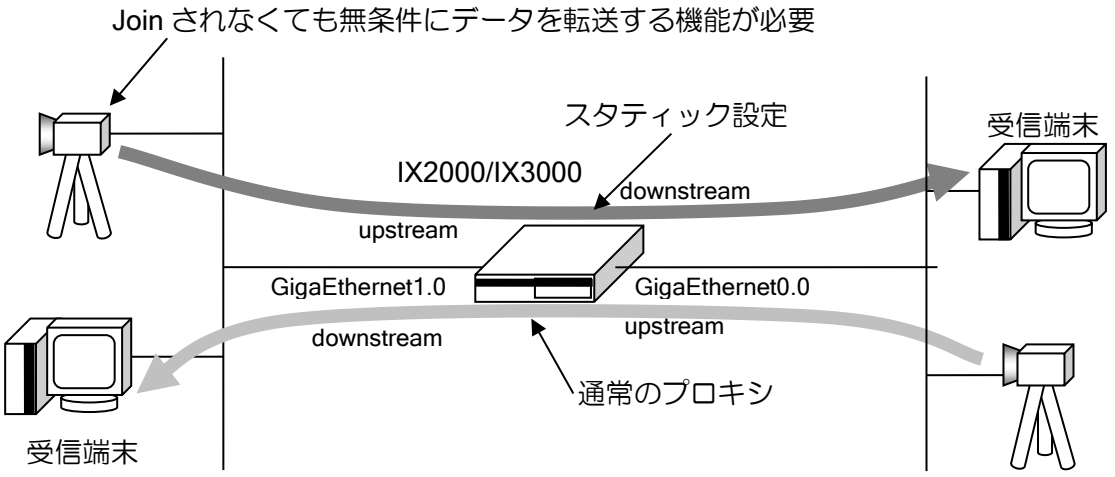
ただし、デフォルト 125 秒間隔ですので接続直後の端末では最大 125 秒もの間参加を受け付けられません。これを回避するため IX2000/IX3000 は IGMPv3 メッセージに対して即座に IGMPv2 ルータであることを通知し（待機時間を無視して Query を送信）、ホストを IGMPv2 に切り替わらせることができます。ホストは一般的に応答がなければ連続で参加要求を繰り返すのでこの方法が有効です。本機能は RFC 準拠の動作ではありませんが、必要な場合には ip igmp version 2 notify コマンドを v3 ホストの存在する IGMP のダウンストリームインタフェース上で設定してください。

```
【設定例】
ip multicast-routing
interface GigaEthernet0.0
   ip address 10.1.1.1/24
   ip igmp upstream
   no shutdown
interface GigaEthernet1.0
   ip address 10.2.2.1/24
   ip igmp downstream
   ip igmp version 2 notify
   no shutdown
```

2.23.4 スタティック設定

IGMP プロキシ機能以外に、スタティックにマルチキャストデータの転送設定を行うことができます。IGMP プロキシを使用する場合は、ホスト側から要求のある場合のみマルチキャストデータを転送しますが、スタティックに設定した場合は、マルチキャストデータを無条件に転送します。スタティックに設定する場合は、アップストリームは IGMP プロキシ機能のアップストリームと異なるインタフェースに設定することが可能です。

スタティック設定の場合、IGMP をアップストリームへ送信しませんので、アップストリーム側には、IGMP を受信していないインタフェースへマルチキャストデータを転送できるルータ、または、マルチキャストサーバを接続する必要があります（PIM 等のダイナミックなプロトコルのみ動作している場合、IX2000/IX3000 側へはマルチキャストデータが転送されません）。



設定は次のとおりです。

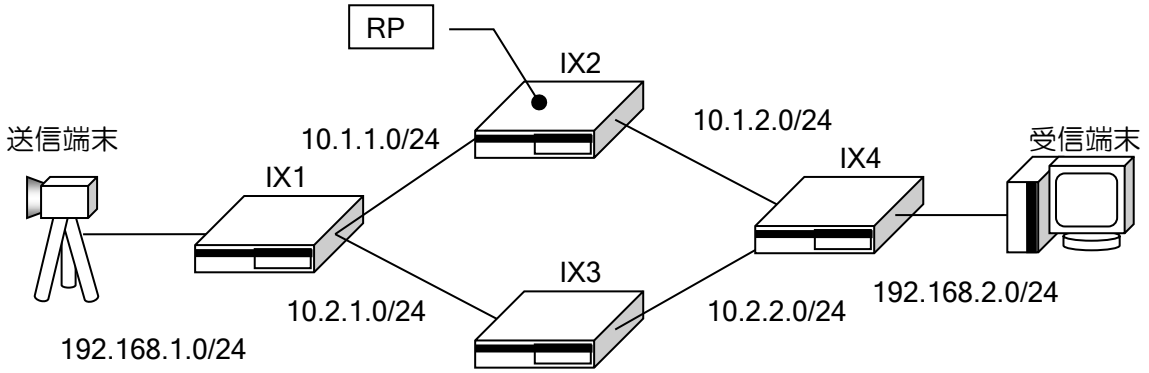
ip mroute	転送するマルチキャストグループの設定 （グローバルコンフィグモード）
downstream	ダウンストリームインタフェースの設定 （IPv4 マルチキャストルートコンフィグモード）

```
【設定例】

ip multicast-routing
!
ip mroute 224.0.10.100 GigaEthernet1.0
   downstream GigaEthernet0.0
!
interface GigaEthernet0.0
   ip address 10.1.1.1/24
   ip igmp upstream
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.2.2.1/24
   ip igmp downstream
   no shutdown
```

2.23.5 PIM-SM 機能

2.23.5.1 基本設定

PIM-SM 機能を使用する場合、PIM-SM を使用するインタフェースにおいて PIM 有効の設定を行います。ランデブーポイント（RP）を固定設定します。または Ver10.4 以降、BSR による RP とマルチキャストグループのマッピングおよび RP の冗長を行うことができます。



PIM-SM の設定は次のコマンドを使用します。

ip multicast-routing	マルチキャストルーティング有効設定 （グローバルコンフィグモード）
ip pim sparse-mode	PIM 機能有効設定 （インタフェースコンフィグモード）
ip pim rp-address	ランデブーポイント設定 （グローバルコンフィグモード）
show ip pim database	PIM エントリ情報の確認

show ip mroute	マルチキャストルーティングテーブルの確認

【設定例】
IX4 の設定例

```
ip multicast-routing
ip pim rp-address 10.1.1.1 224.0.0.0/4
!
ip router ospf 1
   area 0
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 0
   network GigaEthernet2.0 area 0

interface GigaEthernet0.0
   ip address 10.1.2.2/24
   ip pim sparse-mode
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.2.2.1/24
   ip pim sparse-mode
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.2.1/24
   ip pim sparse-mode
   no shutdown
```

（a）Hello パケットの送信

PIM を有効にしているインタフェースでは定期的に Hello パケットを送信します。Hello パケットを受信することによって、ネイバを認識します。

送信間隔は 30 秒固定となります。Hello パケットにて使用するオプションは以下があります。未サポートのオプションは送信しません。また、未サポートのオプションを受信した場合は該当オプションを無視します。

オプション名	サポート	値	概要
Holdtime	○	105 秒固定	ネイバ情報を有効にしておく時間
DR Priority	×	-	DR 選出時のプライオリティ
LAN Prune Delay	×	-	Prune の送信遅延を調節
Generation ID	×	-	インタフェース up 時に値を変更
Address List	×	-	セカンダリアドレスを示す

（b）DR の選択

ネットワークに複数の PIM ルータが存在する場合、DR を選択します。DR は FHR,LHR として動作します。IX2000/IX3000 シリーズでは DR は、IP アドレスが最も大きいルータが選択されます。プライオリティによる DR 選択は未サポートですが、プライオリティ設定をサポートしている装置が同一ネットワーク内に存在する場合でも、IP アドレスが最も大きいルータが選択されます。

DR は以下のコマンドで確認できます。

show ip pim interface	PIM インタフェース情報の確認

【表示例】

```
(config)# show ip pim interface
Interface is GigaEthernet2.0
   PIM is active
   PIM mode is sparse
   PIM version is 2
   Designated router is 192.168.160.5    ：DR アドレス
Neighbor count is 1
   Hello interval is 30 seconds, expire 30 seconds
   Join/Prune interval is 60 seconds
```

（c）RPF ネイバの決定

RPF（Reverse Path Forwarding）は、マルチキャストパケットが最短経路のインタフェースで受信できているかを判断し、パケットがループすることを防ぐための機能です。RPF に合致する隣接ルータを RPF ネイバと呼びます。また、RPF ネイバへのインタフェースが RPF インタフェースとなります。RPF ネイバはユニキャストルーティング情報から決定します。同じあて先に対して複数の経路が存在する場合でも、RPF ネイバは以下の手順で 1 つに決定します。

- ユニキャストルーティングを参照し、あて先への最短経路を使用
- 最短経路が複数存在する場合は、出力先インタフェースの小さい経路を使用。インタフェースの順序は以下（各インタフェースの ifIndex のデフォルトの値の順）。
  - ✧ 基本インタフェース
    （スロット、ポート順）
  - ✧ ポート VLAN、サブインタフェース
    （スロット、ポート、サブインタフェース番号順）
  - ✧ Dialer インタフェース
  - ✧ Tunnel インタフェース
- 出力インタフェースが同じ場合は、ネクストホップアドレスが小さい経路を使用

RPF ネイバの決定手順は、上記の手順固定になります。RPF ネイバの固定設定はできません。RPF ネイバ、RPF インタフェースについては以下のコマンドで確認できます。

show ip pim database	PIM エントリ情報の確認

【表示例】

```
(config)# show ip pim database
PIM Database Entry - 2 entries (1 *g-entries, 1 sg-entries), 2 peek
                          1 groups, 0 overflows, 1 sources
Flags: S - Shortest Path Tree, R - RP Tree
       F - Registering Flag, A - upstream router is selected for Assert
       P - Pruned
Timers: Uptime/Expires
```

```
(*, 224.1.0.10), 0:02:48/0:00:00, RP 100.0.0.100, flags R
   Incoming interface: GigaEthernet0.0, RPF nbr 192.168.100.2
   Outgoing interface list:
      GigaEthernet1.0
(10.0.0.100, 224.1.0.10), 0:01:56/0:00:00, RP 100.0.0.100, flags S
   Incoming interface: GigaEthernet1:4.0, RPF nbr 192.168.40.4  ：RPF ネイバ
                       RPF インタフェース
   Outgoing interface list:
      GigaEthernet1.0
```

2.23.5.2 グループアドレス固定設定

インタフェースに該当するグループアドレスのエントリを固定的に作成することができます。この設定により、マルチキャストを受信したい端末が IGMP を送信しないような場合でも、設定したインタフェースにマルチキャストパケットを転送します。

ip igmp static-group	グループアドレス固定設定 （インタフェースコンフィグモード）

```
【設定例】
GigaEthernet2.0 にグループアドレス 224.1.0.10 を設定

interface GigaEthernet2.0
   ip address 192.168.2.1/24
   ip igmp static-group 224.1.0.10
   ip pim sparse-mode
   no shutdown
```

2.23.5.3 Join/Prune の設定

マルチキャストグループの参加・離脱の通知のために Join/Prune メッセージを使用します。

Join/Prune に含まれるマルチキャストグループアドレスからマルチキャストエントリが作成されます。エントリの作成を制限することにより、特定のグループアドレスのみ通信を行うことや、特定のグループアドレスの通信を行わせないことができます。

ip pim accept-join-prune	Join/Prune のメッセージフィルタ設定 （インタフェースコンフィグモード）

```
【設定例】
225.0.1.1 のみエントリ生成を可能

ip access-list pim-filter permit ip src any dest 225.0.1.1/32

interface GigaEthernet0.0
   ip address 10.1.2.2/24
   ip pim accept-join-prune pim-filter
   ip pim sparse-mode
   no shutdown
```

Join/Prune の送信は、エントリ作成後の定期的な送信とエントリ情報に変更があった場合の送信があります。定期的な送信については、送信間隔の変更ができます。

ip pim message-interval	Join/Prune のメッセージ送信間隔設定 （グローバルコンフィグモード）

【設定例】
メッセージ送信間隔を 120 秒に設定

```
ip pim message-interval 120
```

2.23.5.4 Register の設定

マルチキャストパケットが直近のルータ（FHR）に到達すると、FHR はマルチキャストパケットをカプセル化し、Register メッセージとしてユニキャストで RP へ送信します。Register メッセージはカプセル化を行って送信するため、負荷が高くなる可能性があります。この負荷を抑制するために、Register メッセージの送信最大レートを設定することができます。

ip pim register-rate-limit	Register メッセージ最大レート設定 （グローバルコンフィグモード）

【設定例】
10 パケット/秒で送信
バーストで 20 パケットまで送信可能

```
ip pim register-rate-limit rate 10 burst 20
```

Register メッセージのチェックサム計算は RFC2362 に準拠していますが、他社装置では別な計算を行っている場合があります。IX2000/IX3000 シリーズでは以下の何れかの方式を設定できます。
IX2000/IX3000 シリーズのみで構築する場合は、変更の必要はありません。

- RFC 準拠（デフォルト動作）
  マルチキャストデータを除いた部分のみをチェックサムの計算領域として使用
- RFC 非準拠
  PIM ヘッダおよび、カプセル化するデータ領域をチェックサムの計算領域として使用

ip pim register-checksum	Register メッセージ チェックサム計算方法変更 （グローバルコンフィグモード）

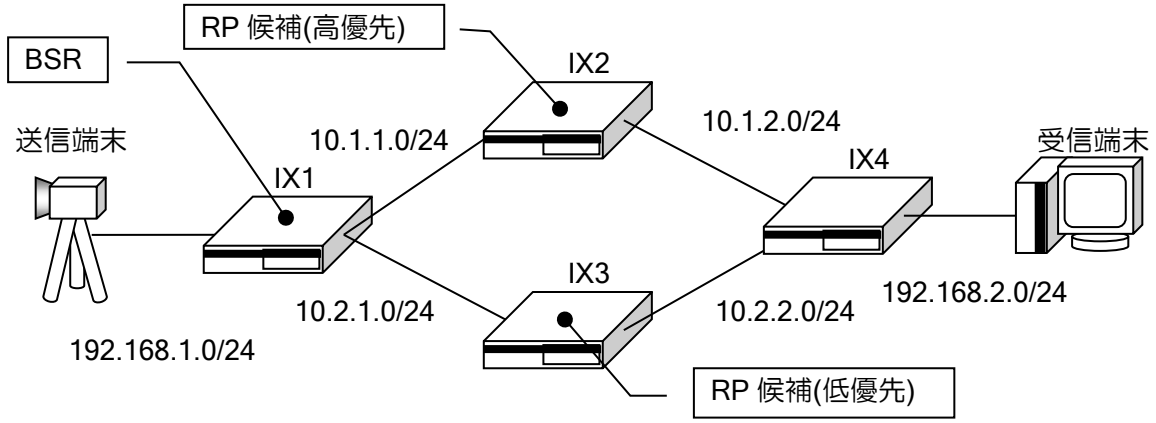
【設定例】
チェックサム計算を RFC 非準拠方式に設定

```
ip pim register-checksum
```

2.23.5.5 BSR による RP の冗長

BSR ルータは RP 候補ルータの RP 候補情報を収集し、各 PIM ルータに通知します。
BSR 候補ルータが複数存在する場合は、優先度の値が大きいルータが BSR となります。
優先度が同一の場合は、IP アドレスが大きいルータが BSR となります。

RP 候補ルータは BSR ルータに自身が RP 候補であることを示す通知を送信します。
各 RP 候補ルータの情報は BSR から通知され、各ルータが RP を自動的に選択します。
同一マルチキャストグループに対する RP 候補ルータが複数存在する場合は、優先度の値が小さいルータが RP となります。優先度が同一の場合はハッシュ値が大きいルータが RP となります。さらにハッシュ値が同一の場合は IP アドレスが大きいルータが RP となります。



ip pim bsr-candidate	ブートストラップルーター候補の設定 （グローバルコンフィグモード）
ip pim rp-candidate	ランデブーポイント候補の設定 （グローバルコンフィグモード）

【設定例】
IX1 の設定例

```
ip multicast-routing
ip pim bsr-candidate GigaEthernet0.0 hashlen 30 priority 0
!
ip router ospf 1
   area 0
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 0
   network GigaEthernet2.0 area 0

interface GigaEthernet0.0
   ip address 10.1.1.1/24
   ip pim sparse-mode
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.2.1.1/24
   ip pim sparse-mode
   no shutdown
!
interface GigaEthernet2.0
```

```
   ip address 192.168.1.1/24
   ip pim sparse-mode
   no shutdown
!
```

IX2 の設定例

```
ip multicast-routing
ip pim rp-candidate GigaEthernet0.0 priority 0 group 224.0.0.0/4
!
ip router ospf 1
   area 0
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 0

interface GigaEthernet0.0
   ip address 10.1.1.2/24
   ip pim sparse-mode
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.1.2.1/24
   ip pim sparse-mode
   no shutdown
!
```

IX4 の設定例

```
ip multicast-routing
!
ip router ospf 1
   area 0
   network GigaEthernet0.0 area 0
   network GigaEthernet1.0 area 0
   network GigaEthernet2.0 area 0

interface GigaEthernet0.0
   ip address 10.1.2.2/24
   ip pim sparse-mode
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.2.2.1/24
   ip pim sparse-mode
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.2.1/24
   ip pim sparse-mode
   no shutdown
!
```

2.23.5.6 注意事項.

- IX2000/IX3000 の PIM-SM 機能は、基本的には RFC2362 に準拠しています。ただし、以下の機能については、RFC4601 の動作となりますので、ご注意ください。
  - ✧ Assert 機能
- インタフェースのアドレスを unnumbered で設定している場合、必ずインタフェースを指定してください。

2.23.5.7 制限事項

IX2000/IX3000 の PIM-SM 機能には以下の制限があります。

- IPv6 は未サポートです。
- PIM-SM v1、PIM-SSM、PIM-DM は未サポートです。
- IGMP プロキシ機能、スタティック設定機能との併用はできません。
- マルチキャスト MIB は未サポートです。
- MSDP は未サポートです。
- RP に VRRP 仮想 IP アドレスは使用できません。

2.23.6 IPv6 マルチキャスト機能

IPv6 マルチキャスト機能は MLD プロキシ機能のみ対応しています。MLD プロキシは、ホストからの要求を Upstream に通知するとともに、要求のあったインタフェースにのみマルチキャストデータを転送する機能です。

MLDv2 に対応し、マルチキャストグループに加えて、ソースアドレスの情報も伝えることが可能です。

IPv6 マルチキャスト、MLD プロキシの設定および確認には次のコマンドを使用します。

設定コマンド

ipv6 multicast-routing	IPv6 マルチキャスト機能の起動/停止
ipv6 mld upstream	アップストリームインタフェースの設定
ipv6 mld downstream	ダウンストリームインタフェースの設定
ipv6 mld query-interval	クエリ送信間隔の設定
ipv6 mld query-max-response-delay	クエリ最大応答時間の設定
ipv6 mld robustness	信頼性変数の設定
ipv6 mld version	バージョンの設定

確認コマンド

show ipv6 mcache	マルチキャストルーティングキャッシュの確認
show ipv6 mroute	マルチキャストルーティングテーブルの確認
show ipv6 mld status	MLD 情報の確認
show ipv6 mld listeners	参加しているグループの確認
show ipv6 mld routers	MLD ルータ機能のキャッシュの確認
show ipv6 mld proxy	MLD proxy 状態の確認
show ipv6 mld statistics	MLD 統計情報の確認

削除コマンド

clear ipv6 mcache	マルチキャストルーティングキャッシュの削除
clear ipv6 mroute	マルチキャストルートの削除
clear ipv6 mld statistics	MLD 統計情報の削除

【設定例】

GigaEthernet0.0（upstream）

- version 2 で動作する（デフォルト）

GigaEthernet1.0（downstream）

- version 1 で動作する
- クエリ送信間隔を 30 秒とする（デフォルト 125 秒）
- クエリ最大応答時間を 5 秒とする（デフォルト 10 秒）

GigaEthernet2.0（downstream）

- version 2 only で動作する
- 信頼性変数を 3 とする（デフォルト 2）

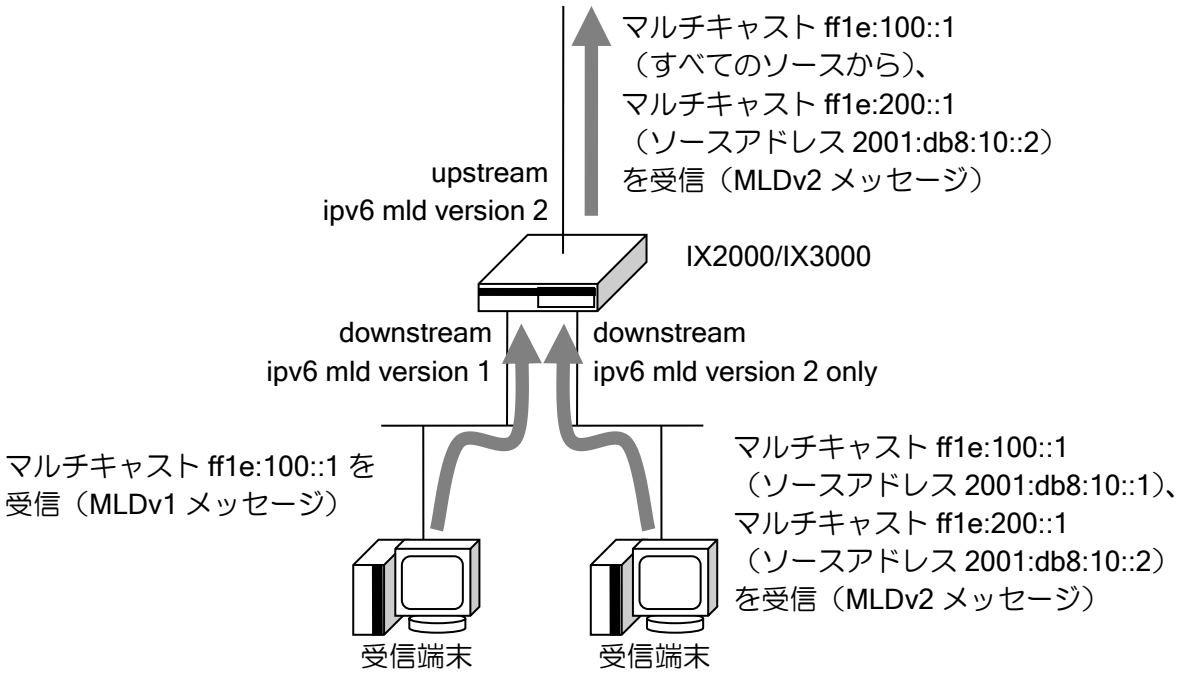
```
ipv6 multicast-routing
interface GigaEthernet0.0
  ipv6 address 2001:db8:10::1/64
  ipv6 mld upstream
  no shutdown
interface GigaEthernet1.0
  ipv6 address 2001:db8:20::1/64
  ipv6 mld downstream
```

```
   ipv6 mld version 1
   ipv6 mld query-interval 30
   ipv6 mld query-max-response-delay 5
   no shutdown
interface GigaEthernet2.0
   ipv6 address 2001:db8:30::1/64
   ipv6 mld downstream
   ipv6 mld version 2 only
   ipv6 mld robustness 3
   no shutdown
```

※ query-interval、query-max-response-delay、robustness をデフォルト値以外にする場合、同一リンク上のすべてのルータ、ホストで同じ値を設定してください。MLD では robustness 回未満の連続したパケットロスが起こっても正しく動作することが保証されます。

※ MLD インタフェースの設定の追加・削除、バージョンの変更を行うと、ルータの全インタフェースが再起動されます。

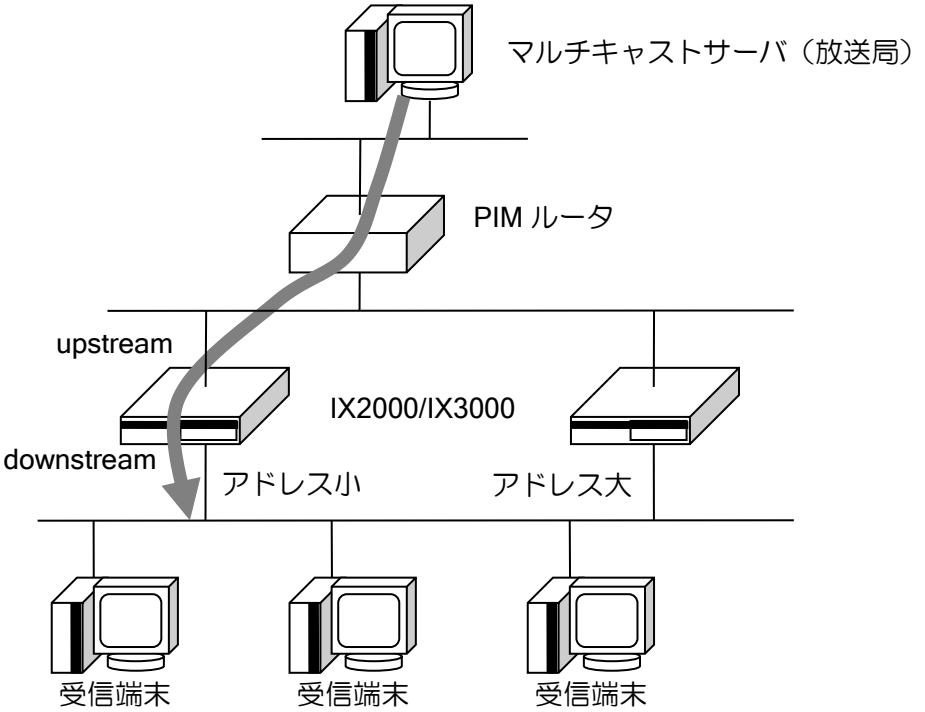
MLD プロキシでは、すべての downstream の受信状態を集約し、上位ルータに受信状態を報告します。version 1 の downstream はすべてのソースアドレスからのマルチキャストパケットを要求しているものとして扱います。



同一リンクにルータが複数ある場合には、リンクローカルアドレスの最も小さいルータがマルチキャストパケットを転送し、他のルータは転送しません。リンクローカルアドレスの最も小さいルータがダウンした場合には、リンクローカルアドレスが 2 番目に小さいルータがマルチキャストパケットを転送します。

同一リンク上のルータは、動作する MLD のバージョンを統一してください。プロトコルの仕様上、ルータの MLD のバージョンが異なると正しく動作しません。

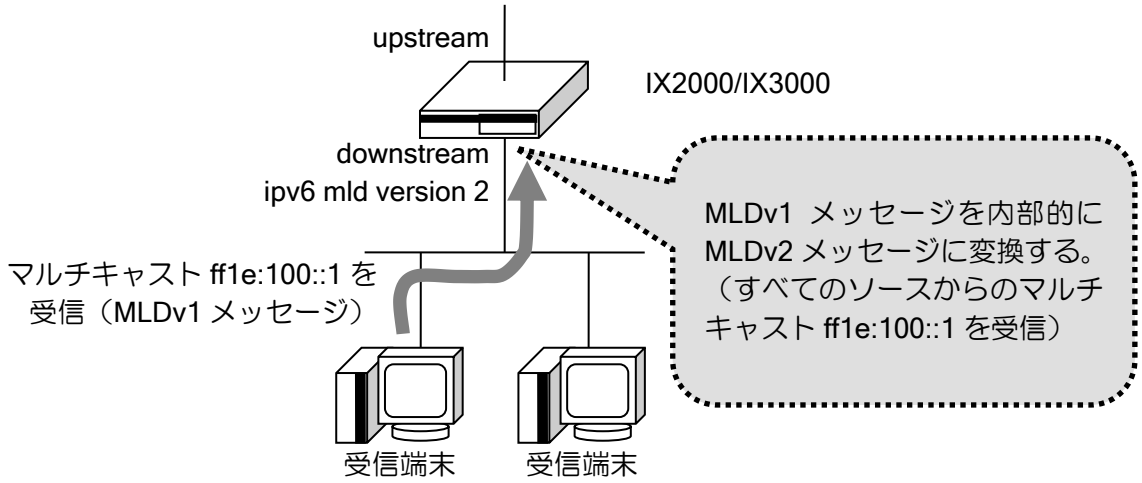
ルータが複数の構成



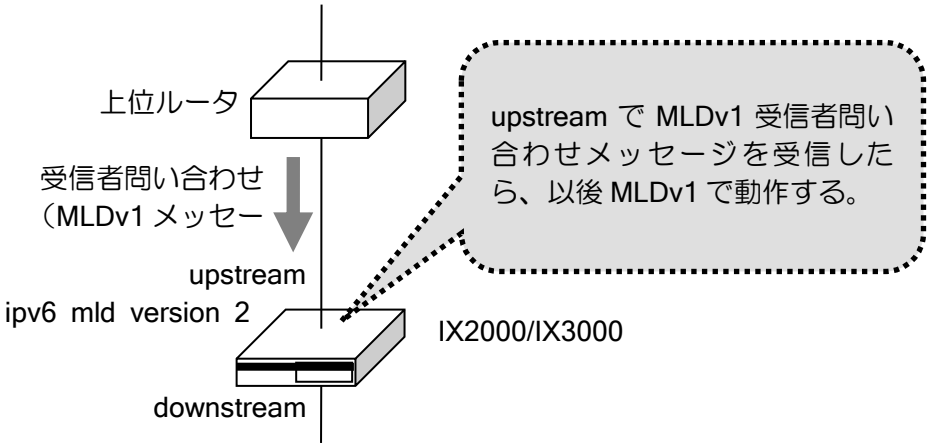
2.23.6.1 MLD のバージョンによる動作の違い

ipv6 mld version コマンドでは、1、2、2 only の 3 通りを設定できます。1 に設定した場合には MLDv1 で動作し、2、2 only に設定した場合には MLDv2 で動作します。version 2 設定時に MLDv1 メッセージを受信すると MLDv1 互換動作をしますが、version 2 only 設定時に受信した MLDv1 メッセージは無視します。

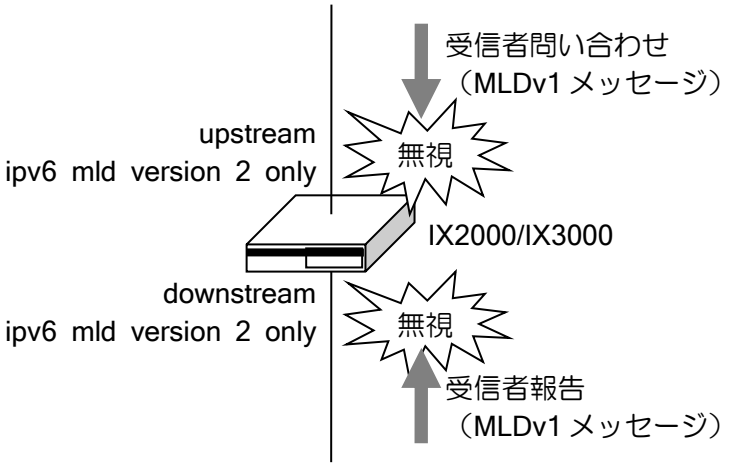
バージョン 2 に設定された downstream で MLDv1 メッセージを受信したときの動作



バージョン 2 に設定された upstream で MLDv1 メッセージを受信したときの動作



バージョン 2 only に設定されたインタフェースで MLDv1 メッセージを受信したときの動作



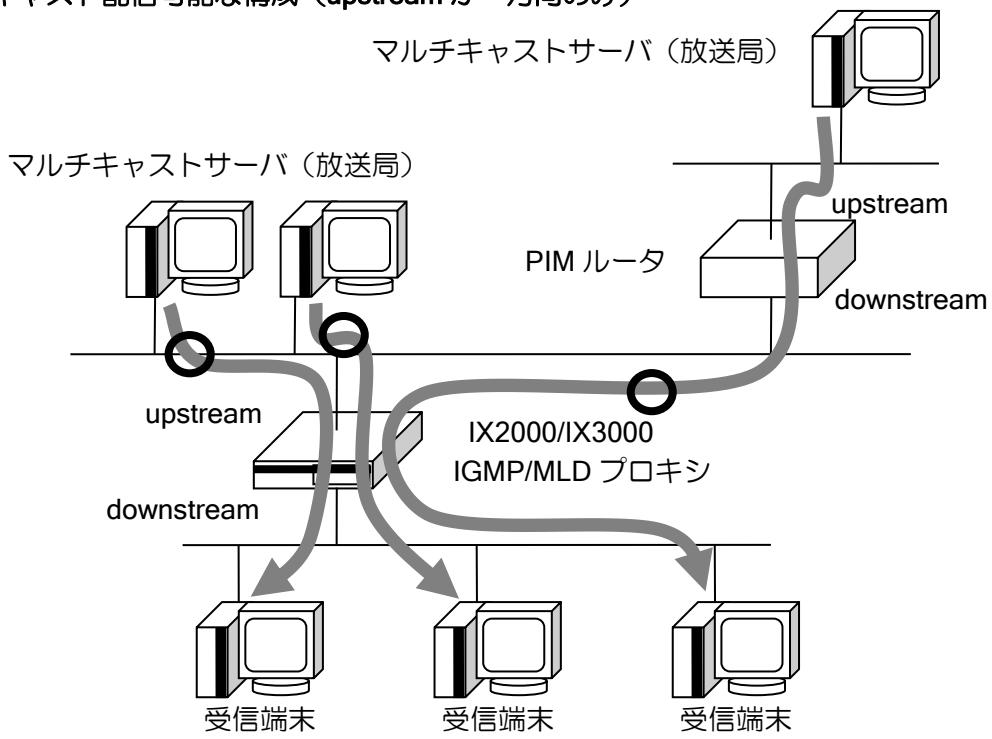
2.23.7 制限事項・注意事項・サポート構成

IGMP/MLD プロキシでは、下記の制限事項・注意事項が存在します。

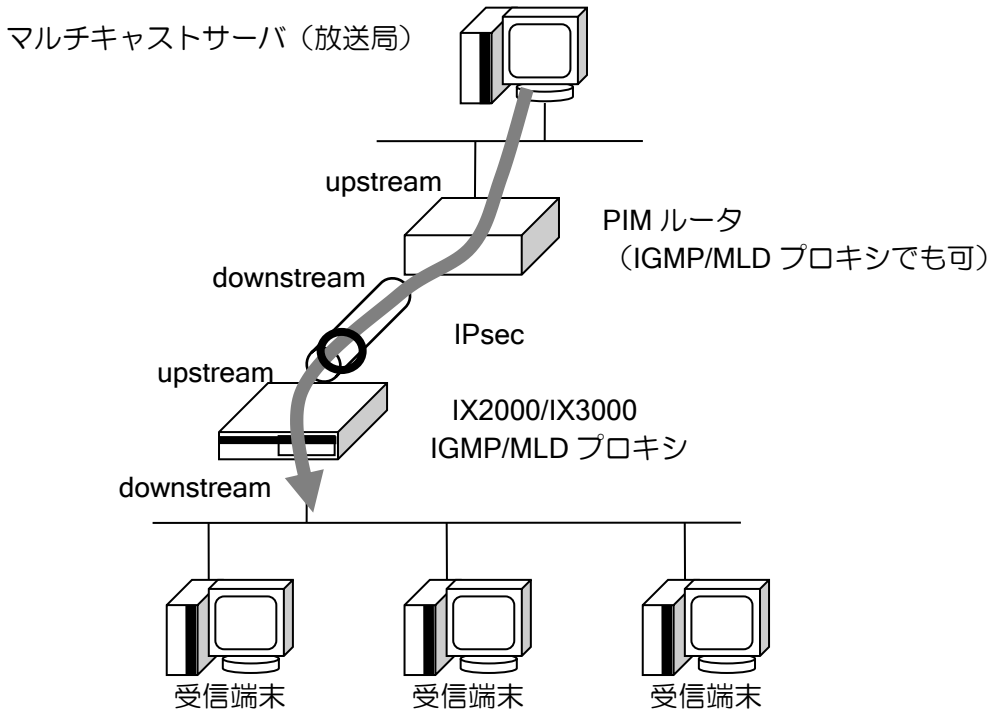
- 設定可能なアップストリームインタフェース数は IGMP、MLD ともに 1 つのみです。
- MLDv2 プロキシはソースアドレス情報もプロキシしますが、MLDv2 プロキシ自体はソースアドレスによる転送の制御を行いません。ただし、上位に PIM-SSM 対応のルータがある場合は、PIM-SSM ルータが指定したソースアドレスのマルチキャストパケットだけを転送するので、結果的に要求したソースアドレスのマルチキャストだけが転送されます。
- 同一リンク上に複数のルータを置くとき、IGMP/MLD のバージョンをすべてのルータで統一してください。
- ネットワークモニタ機能でマルチキャストの経路を操作することはできません。
- IPv4 マルチキャストパケットは、NAPT で廃棄されません。廃棄する必要がある場合にはフィルタを設定してください。
- IPv4 マルチキャストを VRRP と連携する場合、IGMP をマスタ側で動作させるには VRRP でプライオリティの設定をマルチキャストにあわせる必要があります。
- IPsec などのトンネルを使用する場合、PathMTU に注意してください。フラグメントが発生するとパケットの順序が入れ替わることがあるため、負荷が軽くても受信状態に支障をきたすことがあります。

IGMP/MLD プロキシでは、ネットワーク構成上、配送可能な構成と配送不可能な構成が存在します。以下にいくつかの例を示します。

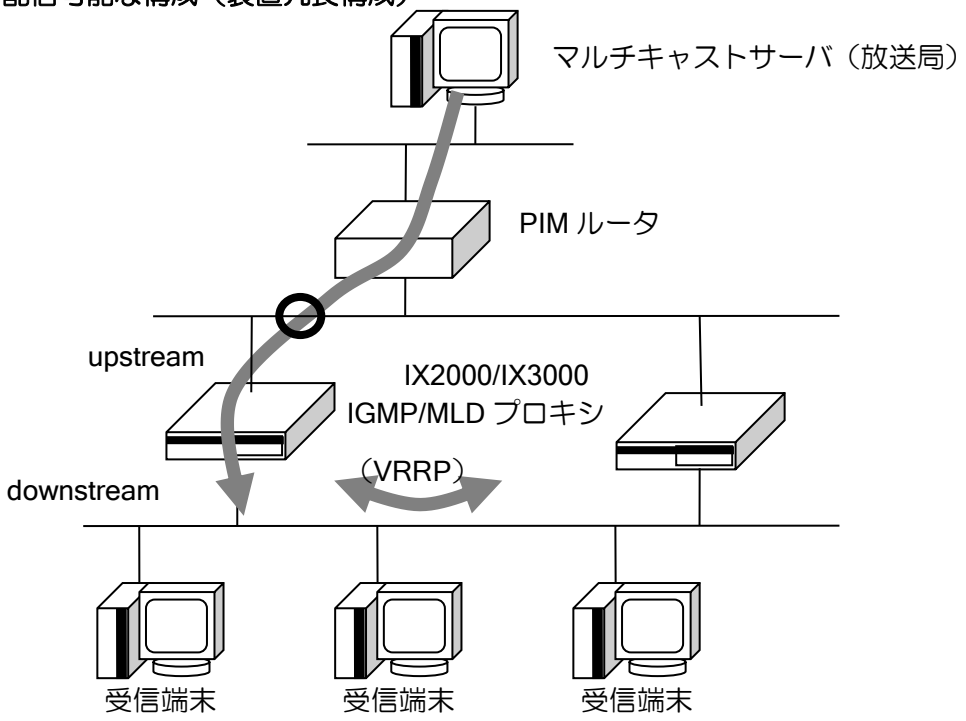
マルチキャスト配信可能な構成（upstream が一方向のみ）



マルチキャスト配信可能な構成（VPN）



マルチキャスト配信可能な構成（装置冗長構成）

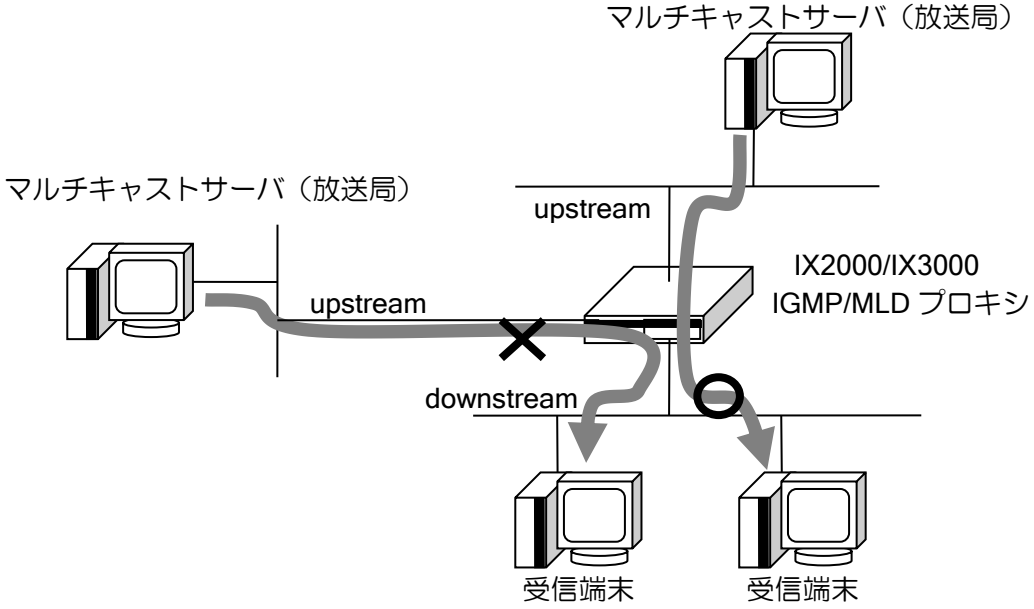


装置の冗長構成は IGMP/MLD プロキシの仕様により実現可能です。マルチキャスト転送ルータは最もアドレスの小さいルータだけが選択されます。選択されなかったルータはマルチキャストを転送しませんが、転送ルータのクエリを常に監視して障害時に切り替わる仕組みです。

さらに障害検出は VRRP と連動させており、併用すると切り替え時間が大幅に短縮されます。マスタは一致させる必要があるので、VRRP はアドレスの小さいルータをマスタにしてください。

※　IGMP/MLD プロキシの仕様では upstream インタフェースと上位ルータの間に障害が起きた場合に転送ルータを切り替える機能がありません。ネットワークモニタ機能を使用して上位ルータまでの経路を監視し、shutdown-interface で強制的にクエリ送信を停止すれば切り替えられますが、マルチキャスト以外の通信にも影響しますので注意して設定してください。

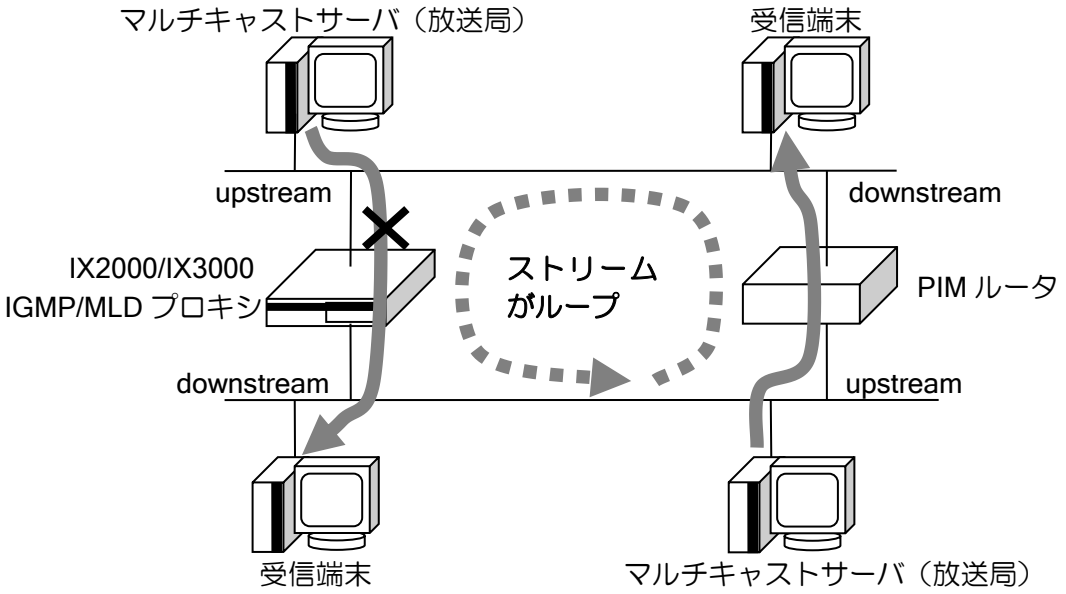
マルチキャスト配信不可能な構成（upstream が複数方向）



アップストリームインタフェースは、IGMP/MLD プロキシでは 1 つしか設定できません。複数のインタフェースからマルチキャストパケットを受信して転送することはできません。

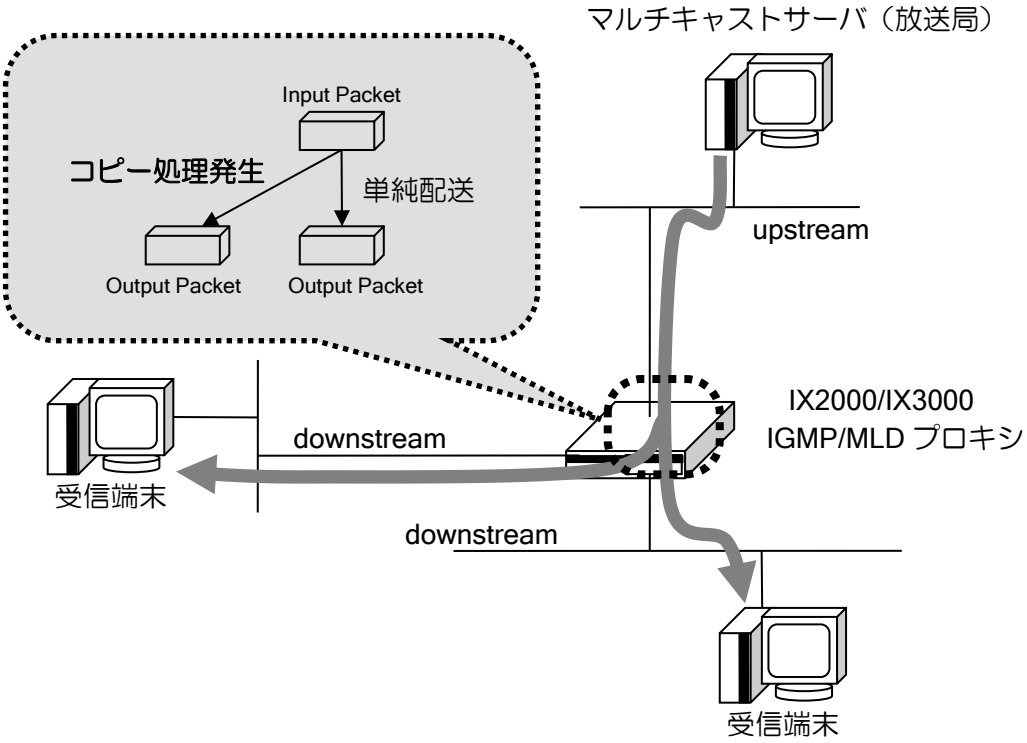
マルチキャスト配信不可能な構成（ストリームがループ）

マルチキャストパケットがループする構成の場合でも自動的にループを検出することはできません。ネットワークが機能しなくなりますので注意してください。



マルチキャスト転送性能が低下する構成（downstream が複数方向）

IX2000/IX3000 の IGMP プロキシ/MLD プロキシ/PIM-SM では、複数インタフェースへパケット転送する場合、ソフトウェアでコピー処理を行うため、インタフェース数に応じて転送性能は急激に低下します。必要な転送性能が確保できることを確認して使用してください。



2.23.7.1 ネットワーク設計上の注意事項

マルチキャストを使用するネットワークを構築する際には、以下のパラメータを考慮する必要があります。

- ダウンストリームの数
- 同時配信するマルチキャストグループの数および、ストリーム量

1 つのマルチキャストグループに対してダウンストリームが複数存在する場合、ソフトウェアによるデータのコピーが発生するため、ルータ負荷が増え、アップストリームからロスせずに配信できる総ストリーム量（=配信能力）は低下します。従って、この処理能力を超えないようにダウンストリーム数と同時配信を行うマルチキャストグループ数およびストリーム量を決定する必要があります。

- 使用可能な構成
  使用するマルチキャストグループ中の最大ダウンストリーム数での配信能力
  ≧ 同時配信する全マルチキャストグループの合計のストリーム量

- 使用不可能な構成
  使用するマルチキャストグループ中の最大ダウンストリーム数での配信能力
  ＜ 同時配信する全マルチキャストグループの合計のストリーム量

  この場合、いずれかの方法での調整が必要となります
  ✧ ダウンストリーム数を減らす →配信能力が増える
  ✧ 同時配信するマルチキャストグループを減らす → 合計ストリーム量が減る
  ✧ 各マルチキャストグループのストリーム量を減らす→ 合計ストリーム量が減る

※ なお、同時配信可能なマルチキャストグループは諸元を確認してください。

以下に IX2000/IX3000 シリーズでの各マルチキャストグループ中の最大ダウンストリーム数と配信能力の関係を示します。

MLD Proxy

機種	最大 downstream 数		
	1	2	4
IX3015	90Mbps	50Mbps	25Mbps
IX2105/IX2106/IX2207/IX2215/IX2235	900Mbps	200Mbps	100Mbps
IX3110	1Gbps	600Mbps	300Mbps

IGMP Proxy

機種	最大 downstream 数		
	1	2	4
IX3015	90Mbps	50Mbps	25Mbps
IX2105/IX2106/IX2207/IX2215/IX2235	900Mbps	200Mbps	100Mbps
IX3110	1Gbps	600Mbps	300Mbps

上記データは以下の条件の場合の値です。下記条件以外の構成、例えば、アップストリームに IPsec を使用したり、データがバースト的に送信されるような場合では、上に示した性能に満たない場合があります。ダウンストリームが 1 の場合の性能は、単純性能とほぼ同等です。

- アップストリームは IPv4/IPv6 の物理インタフェース
- ストリーミングのデータは一定間隔で送信（バースト的ではない）
- パケットサイズは 1446byte
- マルチキャストデータを通すための設定のみ

上記では、ダウンストリームが 4 までのデータを示していますが、それ以上使用する場合でも、増やす割合に応じてストリーム量を減すことで対応が可能です。
使用環境によっては、上記の性能に達しない場合もあります。上記の性能を参考に、運用環境に応じた適切なデータ量にて使用してください。

以下に設計例を示します。

【設定例】
（1）IX3015 で 1Mbps のストリームを 30 グループ使用したい場合
全てを同時に配信する場合、
1Mbps×30 グループ＝30Mbps
の帯域が必要になります。
IX3015 ではダウンストリームが 4 の場合、配信能力は 25Mbps までとなるため
ダウンストリームに 4 インタフェースは使用できません。
30Mbps なので 2～3 インタフェースをダウンストリームとして使用できます。

（2）IX3015 で 4 つのダウンストリームを使用する場合は、
25Mbps まで使用可能です。500kbps のストリーミングデータであれば、
50 マルチキャストグループが同時使用可能となります。

2.23.8 IGMP スヌーピング機能

Ver.8.9 以降、IGMP スヌーピング機能に対応しています。

IGMP スヌーピング機能を使用することにより、SW-HUB において、マルチキャストの受信要求のあったポートのみマルチキャストを送信することができます。

IX2215 の SW-HUB でのみ使用可能です。

設定コマンドは以下のとおりです。

igmp-snooping enable	IGMP スヌーピング機能の有効化 （デバイスコンフィグモード）
igmp-snooping static	マルチキャストグループメンバスタティック設定 （デバイスコンフィグモード）
igmp-snooping group-member-interval	マルチキャストグループメンバ確認間隔設定 （デバイスコンフィグモード）
show igmp-snooping group	マルチキャストグループ情報の表示

【設定例】

```
device GigaEthernet2
  igmp-snooping enable
```

2.23.8.1 制限事項

IX2000/IX3000 の IGMP スヌーピング機能には以下の制限があります。

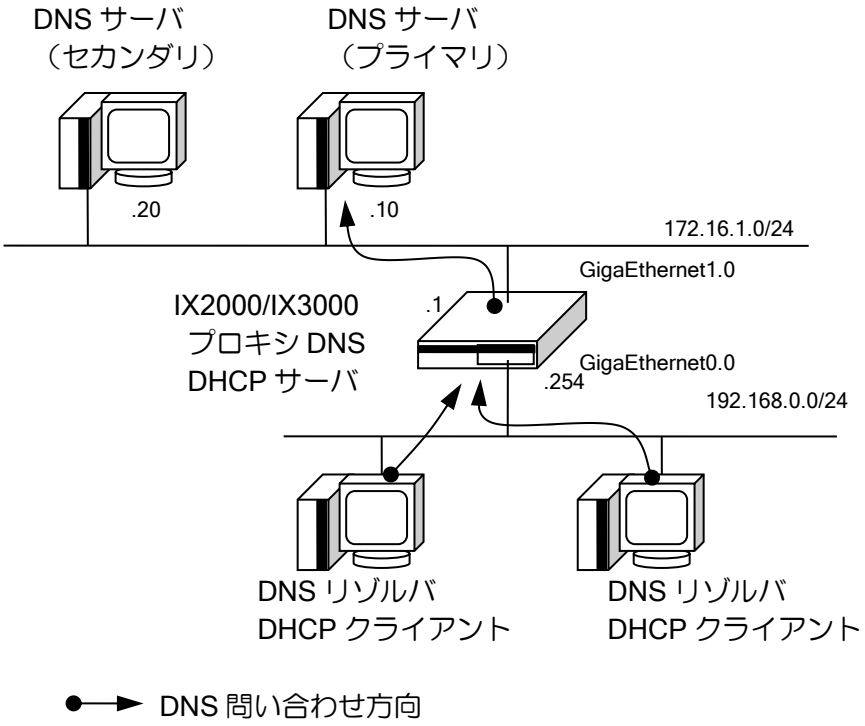
- MLD スヌーピング機能は対応していません。
- IGMPv3 には対応していません。
- リンクアグリゲーションとの併用はできません。
- ブリッジ機能との併用はできません。

■2.24 DNS の設定

IX2000/IX3000 シリーズは、プロキシ DNS および、DNS リゾルバ機能をサポートしています。

プロキシ DNS は、クライアント端末からの名前解決要求をルータが中継して代理応答する機能で、UDP のみに対応しています。なお、512byte を超える応答パケットは Ver8.6 以降のみ中継可能です。Ver10.3 以降、クライアントからの名前解決要求をルータが TCP で待ち受けられるようになりました。(DNS サーバへの問い合わせは UDP となります)

2.24.1 プロキシ DNS の設定



以下にプロキシ DNS 登録のための設定および基本的な動作を説明します。

proxy-dns server	DNS サーバのアドレス指定と優先度設定
proxy-dns interface	PPP/DHCP で取得した DNS サーバの優先度設定
proxy-dns ip/ipv6 enable	プロキシ DNS の有効設定
proxy-dns ip/ipv6 max-sessions	最大セッション数の設定
proxy-dns ip/ipv6 query-interval	DNS 要求パケット送信間隔の設定
proxy-dns ip/ipv6 query-response	DNS 応答パケット待ち時間の設定
proxy-dns ip/ipv6 query-retries	DNS 要求パケット再送回数
proxy-dns ip/ipv6 access-list	DNS リゾルバのアクセス制限（Ver.9.2 以降）
proxy-dns ip/ipv6 request	DNS 要求パケット転送方法の設定
show proxy-dns	プロキシ DNS 設定状態の表示

【設定例】
プロキシ DNS と DHCP を組み合わせた設定（Ver.4.3 以降）

```
ip dhcp enable
proxy-dns ip enable
ip dhcp profile ge0.0
   assignable-range 192.168.0.1 192.168.0.10
   dns-server 192.168.0.254
interface GigaEthernet0.0
   ip address 192.168.0.254/24
   ip dhcp binding ge0.0
   no shutdown
interface GigaEthernet1.0
   ip address dhcp receive-default
   no shutdown
```

- DNS サーバの優先度の設定

複数のサーバを登録した場合に優先度を設定することができます。優先度は、固定設定ではサーバ単位、動的設定では取得するインタフェース単位に設定することができ、数値の大きい方を優先します。同じ場合は以下の順で優先されます。

- 固定的に登録したサーバは動的に取得したサーバより優先されます。
- 先に設定(取得)したサーバが優先されます。

【設定例】

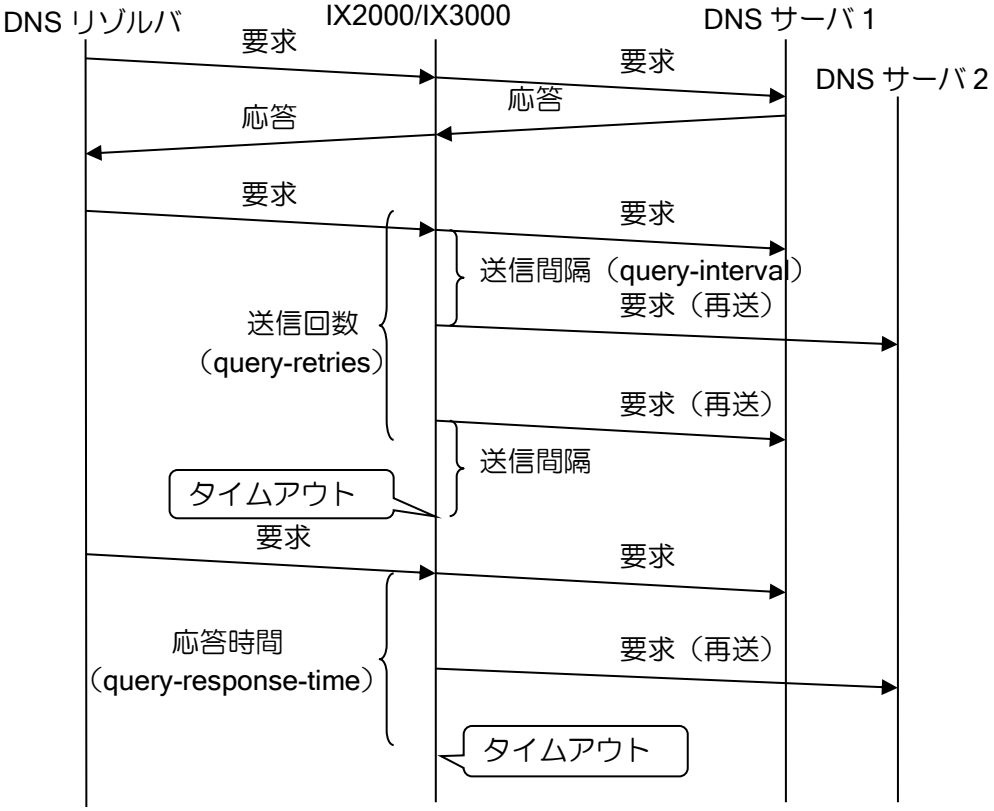
```
proxy-dns server 172.16.1.10 priority 50
proxy-dns server 172.16.1.20 priority 40
proxy-dns interface GigaEthernet0.0 priority 60
proxy-dns interface GigaEthernet1.0 ignore
```

この場合の優先度は以下の通りとなります。
(1)GigaEthernet0.0 から取得した DNS サーバ
(2)172.16.1.10
(3)172.16.1.20

Ver.9.2 以降、IPv4 リゾルバからの要求、または IPv6 リゾルバからの要求を、IPv4 サーバ、IPv6 サーバどちらのサーバにもプロキシすることができます。IPv4 サーバ、IPv6 サーバが混在している場合でも、サーバの優先度に従って問い合わせを行います。同じ優先度の場合は、リゾルバと同じプロトコルのサーバが優先されます。

- DNS サーバへの要求／応答の設定

  DNS サーバへの要求の応答時間，再送間隔，再送回数を設定することができます。




```
【設定例】
送信回数 3 回，送信間隔 2 秒，応答時間 20 秒に設定

proxy-dns ip query-response 20
proxy-dns ip query-retries 3
proxy-dns ip query-interval 2
proxy-dns server 172.16.1.10
```

再送間隔の時間に DNS サーバから応答が無い場合再送を行います。複数の DNS サーバが存在する場合は、次の DNS サーバへ要求を送信します。設定した再送回数の送信を行い、次の再送周期を過ぎても応答が無い場合、タイムアウトとなります。

応答時間を設定した場合は、最初の送信から設定した応答時間を過ぎても DNS サーバから応答が無い場合は、再送回数，再送間隔の時間が残っていてもタイムアウトとなります。先に再送によるタイムアウトが発生した場合は、その時点でタイムアウトとなり、応答時間は無視されます。

DNS サーバから Failure 受信時、複数の DNS サーバが存在する場合は、次の再送周期に次の DNS サーバに送信を行います。Ver.9.2 以降は、Failure 受信時には再送間隔を待たずに次の DNS サーバへ送信を行います。

- DNS リゾルバのアクセス制限（Ver.9.2 以降）
  プロキシする DNS リゾルバのアクセス制限を行うことができます。

【設定例】
192.168.0.0/24 からの要求のみ許可する

```
ip access-list resolver-acl permit ip src 192.168.0.0/24 dest any

proxy-dns ip enable
proxy-dns ip access-list resolver-acl
proxy-dns server 10.0.0.1
```

- DNS 問合せ出力先指定(Ver.9.6 以降)
  DNS リゾルバ、Proxy-DNS ともに IPv4 の DNS サーバへの問合せを指定したインタフェースから送信できます。インタフェースを指定する場合は「ip name-server」、「proxy-dns server」コマンドにオプションをつけて設定を行ってください。

  また、IPCP/DHCP で動的に取得した DNS サーバへの問合せは取得したインタフェースから送信されます(Proxy-DNS も同様)。
  Ver.9.5 以前の動作(ルーティングに従った問合せ)に戻すときには下記の「no ip name-server dynamic fixed-interface」コマンドを設定してください。

ip name-server dynamic fixed-interface	IPv4 動的取得 DNS の送信元固定設定

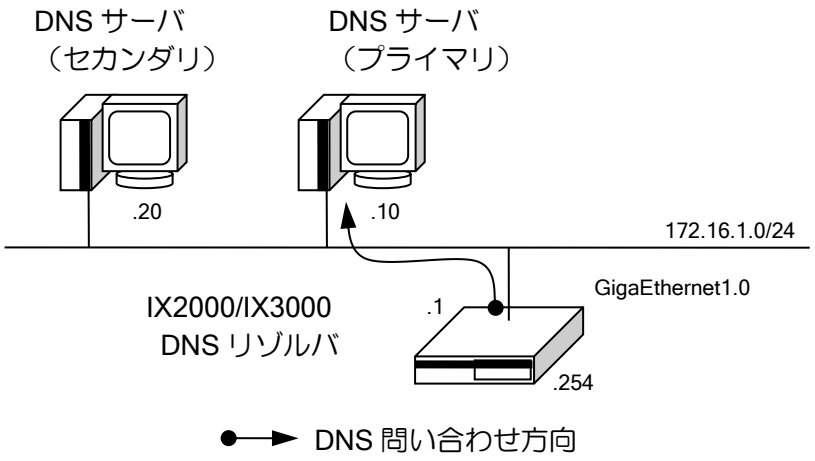
- インタフェース単位の Proxy-DNS サーバ有効化設定（Ver.9.6 以降）
  Ver.9.5 以前では Proxy-DNS の機能を装置全体でしか有効に出来ませんでしたが、Ver.9.6 以降ではインタフェースコンフィグモードに enable コマンドを設定することで特定のインタフェースでのみ機能を有効にすることができます。
  意図しないインタフェースへの問合せを防止することが可能です。

- TCP 対応（Ver.10.3 以降）
  端末から TCP の DNS クエリー受信に対応しています。
  IX から DNS サーバへの名前解決は UDP を使用します。

2.24.2 DNS リゾルバの設定

DNS リゾルバは、DNS サーバへ DNS 情報取得要求を出し、登録されているサーバから DNS 情報を取得する機能です。IPv4, IPv6 ともに利用可能です。

DNS リゾルバは、ping, ping6, traceroute, traceroute6, telnet, nslookup で使用することができます。Ver.8.8 以降、EDNS0 と 512byte 以上の応答をサポートしています。TCP での問合せはサポートしておりません。



DNS サーバは DHCPv4 や IPCP、Ver.8.8 以降は DHCPv6-PD で自動取得されたものを使用しますが、自動で取得しない場合は以下の設定を行います。
DNS サーバを複数設定している場合、設定順に問い合わせを行います。

DNS の問い合わせ順番は以下となります。

- IPv4 優先(dns transport-priority ip)の場合【デフォルト設定】
  - 固定で設定した IPv4 の DNS サーバ(登録順)
  - 固定で設定した IPv6 の DNS サーバ(登録順)
  - DHCPv4、IPCP で学習した DNS サーバ(学習順)
  - DHCPv6-PD で学習した DNS サーバ(学習順)
- IPv6 優先(dns transport-priority ipv6】)の場合
  - 固定で設定した IPv6 の DNS サーバ(登録順)
  - 固定で設定した IPv4 の DNS サーバ(登録順)
  - DHCPv6-PD、IPCP で学習した DNS サーバ(学習順)
  - DHCPv4、IPCP で学習した DNS サーバ(学習順)

Ver10.7 以降では各機能で設定した outgoing-interface で設定したインタフェースを最優先に DNS 解決を行います。outgoing-interface が存在しない機能に関しては上記のルールに従います。
下記が outgoing-interface 対応機能です。

IKEv2(ドメイン解決)	ikev2 outgoing-interface
NHRP(ドメイン解決)	nhrp nhs 【IPv4 アドレス】 nbma example.com ipv4/ipv6
UTM(ドメイン解決)	utm outgoing-interface
NetMeister(ドメイン解決)	nm outgoing-interface
Tunnel(ドメイン解決)	tunnel outgoing-interface

ip/ipv6 name-server	DNS の IPv4/IPv6 アドレスを固定的に設定
dns transport-priority	DNS 問い合わせ IPv4, IPv6 優先設定
dns transport-routing	DNS 問い合わせインタフェース固定無効設定(Ver10.7 以降) ※ Ver10.7 以降では outgoing-interface 対応機能の DNS 問い合わせは指定されたインタフェースから出力されますが、本設定を行うことで Ver10.6 以前と同様にルーティングに従い問い合わせを行います。

【設定例】

```
ip name-server 172.16.1.10
ip name-server 172.16.1.20 GigaEthernet1.0
interface GigaEthernet0.0
   ip address 192.168.0.254/24
   no shutdown
interface GigaEthernet1.0
   ip address 172.16.1.1/24
   no shutdown
```

- EDNS0 対応（Ver.8.8 以降）
  EDNS0 に対応することを示すオプションをメッセージに追加して DNS サーバに送信します。
  DNS サーバから EDNS0 未対応のエラーが返った場合は、EDNS0 を付与しないメッセージを送信します。

2.24.3 DNS キャッシュの設定

2.24.3.1 DNS キャッシュ

DNS の問い合わせの結果をキャッシュすることができます。DNS キャッシュを使用することにより、通常はキャッシュテーブルを参照し DNS 解決を行い、キャッシュに存在しない場合のみ、DNS サーバに問い合わせを行います。キャッシュは生存時間経過までにアクセスがあった場合は DNS サーバに問い合わせを行い、存在していれば更新します。アクセスが無い場合は、削除されます。

DNS キャッシュには、DNS 解決が成功した情報と DNS 解決が失敗した情報（ネガティブキャッシュ）があり、それぞれ、別々な生存時間を設定することができます。

設定コマンドは以下のとおりです。

dns cache enable	DNS キャッシュの有効
dns cache max-records	DNS レコード数設定
dns cache lifetime	DNS キャッシュ生存時間設定
dns ncache lifetime	DNS ネガティブキャッシュ生存時間設定
show dns cache	DNS キャッシュの表示

2.24.3.2 DNS アドレスデータベース

DNS サーバの設定によっては、A レコードのみ登録し、PTR レコードが無い場合があります。このような場合、DNS の逆引きができないため、アクセスリストでの FQDN 指定が使用できません。

DNS の正引き時の結果をもとに、アドレスとドメイン名のデータベースを作成することにより、逆引きができない環境においても、アクセスリストのドメイン名指定を使用することが可能となります。アドレスデータベースは、DNS キャッシュと連動して削除されます。設定コマンドは以下のとおりです。

dns cache address-database	DNS アドレスデータベース設定
show dns cache address-database	DNS アドレスデータベースの表示

2.24.3.3 アクセスリストとの連携

アクセスリストのドメイン名指定時には、DNS キャッシュの PTR レコードまたは、DNS アドレスデータベースを使用し、対応するアドレスを検索します。dns cache address-database の設定により、どちらを優先して使用するかを設定することができます。どちらの場合も、アドレスが検索できない場合は逆引きを行います。

- 指定なし　　：最初にアドレスデータベースを使用します。データが存在しなければ DNS キャッシュの PTR レコードを使用します。
- only　　：DNS アドレスデータベースのみ使用します。
- not-preferred：最初に DNS キャッシュの PTR レコードを使用します。データが存在しなければアドレスデータベースを使用します。

2.24.4 FQDN 指定対応

指定した FQDN の名前解決を行い、対応するアドレスを使用することができます（Ver.8.8 以降）。FQDN に対して定期的に名前解決を行い、対応するアドレス情報の更新を行います。

対応している機能は以下になります。

- IKEv1/IPsec
  - ike policy のピア指定
  - ipsec autokey-map のピア指定
- IKEv2
  - IKEv2 のピア指定（ikev2 peer-fqdn-ipv4／ikev2 peer-fqdn-ipv6）
- Tunnel
  - 宛先アドレス（Ver.9.2 以降）

各機能から要求時、および定期的に FQDN の名前解決を行います。名前解決した情報は FQDN データベースに記録されます。名前解決が一度も成功していない状態では、FQDN に対応したアドレスが分からないため、FQDN を使用した通信等を行うことができません。一度名前解決が成功した後は、定期的な解決に失敗した場合でも、解決済みのアドレスを使用し続けます。

定期的な更新については、更新周期とリトライ回数、タイムアウト時間を設定できます。1 度も名前解決が成功していない時の名前解決周期と 1 度名前解決が成功した後の名前解決周期は別な値を設定することができます。複数サーバ設定時は、タイムアウト時間をサーバ台数分で等分した間隔で名前解決を行います。
設定は以下の通りです。

dns fqdn-database initial-interval	アドレス更新周期（名前解決前）
dns fqdn-database update-interval	アドレス更新周期（名前解決後）
dns fqdn-database resolver retry	名前解決のリトライ回数
dns fqdn-database resolver timeout	名前解決のタイムアウト時間
show dns fqdn-database	FQDN データベースの表示

【設定例 1】
一度も名前解決していない時の更新周期を 50 秒、
名前解決後の更新周期を 24 時間（86400 秒）に設定

```
dns fqdn-database initial-interval 50
dns fqdn-database update-interval 86400
```

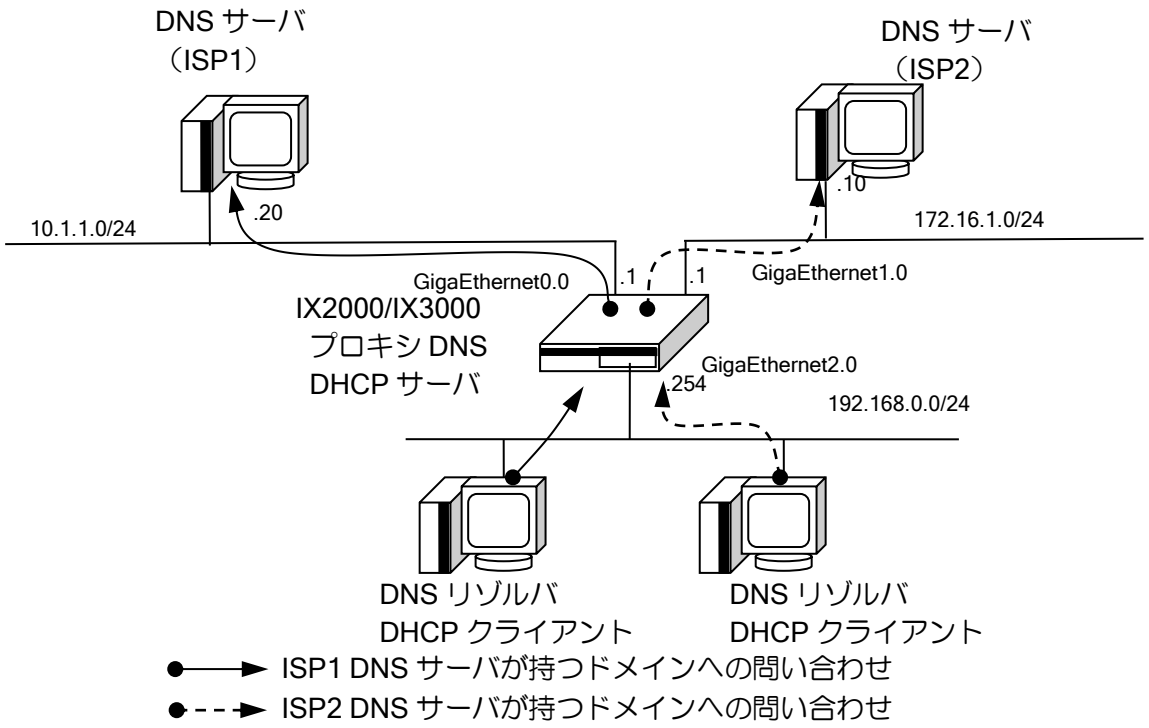
【設定例 2】
名前解決できない場合、20 秒間隔で 3 回までリトライを行う
（初回を含めて 4 回送信を行います）

```
dns fqdn-database resolver retry count 3
dns fqdn-database resolver timeout 20
```

上記設定でサーバが 2 台の場合、10 秒（20 秒の 1/2）間応答が無い場合、
次のサーバに送信します。

2.24.5 DNS サーバアクセス振り分け

指定したドメインの名前解決サーバのアクセスを指定することができます。（Ver10.2 以降）
複数の ISP を使い分ける場合などに指定したドメインを利用したい ISP の DNS サーバへのアクセスの振り分けを行います。



【設定例】
・example.com ドメインへの DNS 問い合わせを ISP2 の DNS サーバへ、それ以外の DNS 問い合わせを ISP1 の DNS サーバへと行う。

```
ip route default GigaEthernet0.0
ip route 172.16.1.0/24 GigaEthernet1.0
ip dchp enable
proxy-dns ip enable
proxy-dns interface GigaEthernet1.0 url-list isp2 priority 200

url-list isp2 permit domain *example.com

ip dhcp profile gigaethernet2.0
   assignable-range 192.168.0.1 192.168.0.10
   dns-server 192.168.0.254
interface GigaEthernet0.0
   ip address 10.1.1.1/24
   no shutdown
interface GigaEthernet1.0
   ip address 172.16.1.1/24
   no shutdown
interface GigaEthernet2.0
   ip address 192.168.0.254/24
   ip dhcp binding gigaethernet2.0
   no shutdown
```

2.24.6 ローカル DNS サーバ

クライアント端末から指定したドメインの名前解決要求を、外部サーバにアクセスする代わりにルータが指定した IP アドレスレコードで名前解決応答を行うことができます。（Ver10.3 以降）

ルータが名前解決要求を受信し、ルータが応答するか外部サーバに問い合わせるかを振り分けるため、プロキシ DNS の併用が必要となります。

【設定例】
・example.com ドメインへの DNS 問い合わせをルータが A レコード(192.168.0.200)で応答し、それ以外の DNS 問い合わせを外部 DNS サーバへ行う。

```
ip route default GigaEthernet0.0
ip dchp enable
proxy-dns ip enable

dns host example.com ip 192.168.0.200

ip dhcp profile gigaethernet2.0
   assignable-range 192.168.0.1 192.168.0.10
   dns-server 192.168.0.254
interface GigaEthernet0.0
   ip address 10.1.1.1/24
   no shutdown
interface GigaEthernet2.0
   ip address 192.168.0.254/24
   ip dhcp binding gigaethernet2.0
   no shutdown
```

※IPv4 アドレスでの登録レコードは、名前解決要求の Query Type が A または ANY の場合に適用します。
※IPv6 アドレスでの登録レコードは、名前解決要求の Query Type が AAAA または ANY の場合に適用します。それ以外の Query Type の場合は、外部サーバへ問合せを行います。

■2.25 ダイナミック DNS 機能の設定

2.25.1 ダイナミック DNS 機能

ダイナミック DNS 機能とは、外部のダイナミック DNS サービスに対してドメイン名のアドレス更新を依頼する機能です。自己のアドレスが動的に変わる環境であっても、常に同じドメイン名でアクセスできるようになります。Ver8.8 以降でサポートしています。

Ver9.7 以降では、NetMeister 機能を利用することで、NEC プラットフォームズが提供するダイナミック DNS サービスを利用することができます。NetMeister のページも参照してください。

IPv4、IPv6 の HTTP, HTTPS（ver9.0.14A 以降 TLS1.0 対応）による更新に対応しています。

2.25.2 ダイナミック DNS の設定

ダイナミック DNS 機能は、次のコマンドで設定します。

ddns enable	ダイナミック DNS クライアント機能の有効設定
ddns profile	ダイナミック DNS プロファイルの作成
url	ダイナミック DNS サーバの登録
query	更新内容の登録(クエリ登録)
source（Ver.9.1 以前） source-interface（Ver.9.2 以降）	送信元・アドレス登録インタフェースの設定
notify-interface	アドレス登録インタフェースの設定
transport	通信に使用するプロトコルの設定(IPv4/IPv6)
account	ユーザアカウント名の登録
password	パスワードの登録
update-interval	更新周期の変更

ddns profile コマンドでダイナミック DNS サーバの設定を行うプロファイルを用意し、登録に必要な情報を設定します。

一般に、ダイナミック DNS サーバへのアドレス登録には、ドメイン名、登録するアドレス、認証用パスワードの情報が必要となります。登録するアドレスを明示的に指定せずに、登録用通信の送信元アドレスを利用する場合もあります。登録の方法は、ダイナミック DNS サーバ事業者によって異なりますので、各事業者の説明を参照してください。

以下にいくつかのパターンの登録方法を記載しますので、それぞれ該当するものを参照してください。

2.25.2.1 ドメイン名とパスワードをクエリで設定する場合

以下のようにドメイン名とパスワードをクエリで登録するように指定されている場合の設定方法です。

- https://example.com/update.cgi?d=<ドメイン名>&p=<パスワード>&a=<IPv4 アドレス>

【設定例】

```
ddns profile server1
   url https://example.com/update.cgi
   query d=ix-router&p=<PW>&a=<IP4>
   password plain pass
   transport ip
! Ver.9.2 以降は source-interface になります。source でも設定可能です。
   source GigaEthernet0.0
```

クエリには<PW>,<IP4>,<IP6>, <SN>の環境変数が利用できます。

- <PW>はダイナミック DNS プロファイルの password コマンドで設定したパスワードに変換されます。
- <IP4>は source で指定したインタフェースのプライマリアドレスに変換されます。
- <IP6>は source で指定したインタフェースの先頭のグローバル IPv6 アドレスに変換されます。
- <SN>は装置の製造番号に変換されます。

インタフェースのアドレス以外の固定アドレスを登録したい場合は、直接クエリにアドレスを記載してください。また、パスワードは直接クエリに記載しても構いませんが、password コマンドを利用した場合は、service password-encryption コマンドで暗号化してコンフィグに保存することができます。

2.25.2.2 ドメイン名やパスワードをベーシック認証で設定する場合

以下のようにドメイン名とパスワードを登録するように指定されている場合の設定方法です。

1. URL の設定例でアカウントとパスワードを@の前に設定している場合
   - https://<アカウント>:<パスワード>@example.com/
2. URL の設定例にクエリがなく、ベーシック認証を使うと記載されている場合
   - https://example.com/

【設定例】

```
ddns profile server2
   url https://example.com/
   account ix-router
   password plain pass
   transport ip
! Ver.9.2 以降は source-interface になります。source でも設定可能です。
   source GigaEthernet0.0
```

2.25.2.3 IPv6 アドレスを登録する場合

ダイナミック DNS サーバ事業者が IPv6 に対応しているかどうかを確認してください。IPv6 に対応している場合でも、更新パケットを IPv6 で送信できない場合がありますので、あわせて確認が必要です。

【設定例】

IPv6 パケットで IPv6 アドレスを更新する場合

```
ddns profile server1
   url https://example.com/update.cgi
   query d=ix-router&p=<PW>&a=<IP6>
   password plain pass
   transport ipv6
! Ver.9.2 以降は source-interface になります。source でも設定可能です。
   source GigaEthernet0.0
```

IPv4 パケットで IPv6 アドレスを更新する場合

```
ddns profile server1
   url https://example.com/update.cgi
   query d=ix-router&p=<PW>&a=<IP6>
   password plain pass
   transport ip
! Ver.9.2 以降は source-interface になります。source でも設定可能です。
   source GigaEthernet0.0
```

2.25.2.4 送信元インタフェースとアドレスを通知するインタフェースが異なる場合

Ver.9.2 以降、送信元インタフェースと通知したいアドレスを持つインタフェースに、異なるインタフェースを指定できます。Ver.9.1 以前は、source コマンドで設定したインタフェースを、送信元インタフェースとアドレスを通知するインタフェースとして使用します。

【設定例】

GigaEthernet0.0 にパケットを送信
GigaEthernet1.0 のアドレスをサーバに通知

```
ddns profile server1
   url https://example.com/update.cgi
   query d=ix-router&p=<PW>&a=<IP4>
   password plain pass
   transport ip
   notify-interface GigaEthernet1.0
   source-interface GigaEthernet0.0
```

2.25.3 ダイナミック DNS の動作

ダイナミック DNS 機能は、以下のタイミングで更新動作を行います。

- notify-interface コマンドで設定したインタフェース、notify-interface 未設定時は source-interface コマンドで設定したインタフェースのアドレスが変化した場合(10 秒後に送信)（Ver.9.2 以降）
- source コマンドで設定したインタフェースのアドレスが変化した場合(10 秒後に送信)（Ver.9.1 以前）
- 周期更新（デフォルト 24 時間）
- ddns update コマンド実行時

短時間で繰り返し更新パケットを送信することはダイナミック DNS サーバ側の負荷になりますので、必要以上に短い周期で更新しないようにしてください。

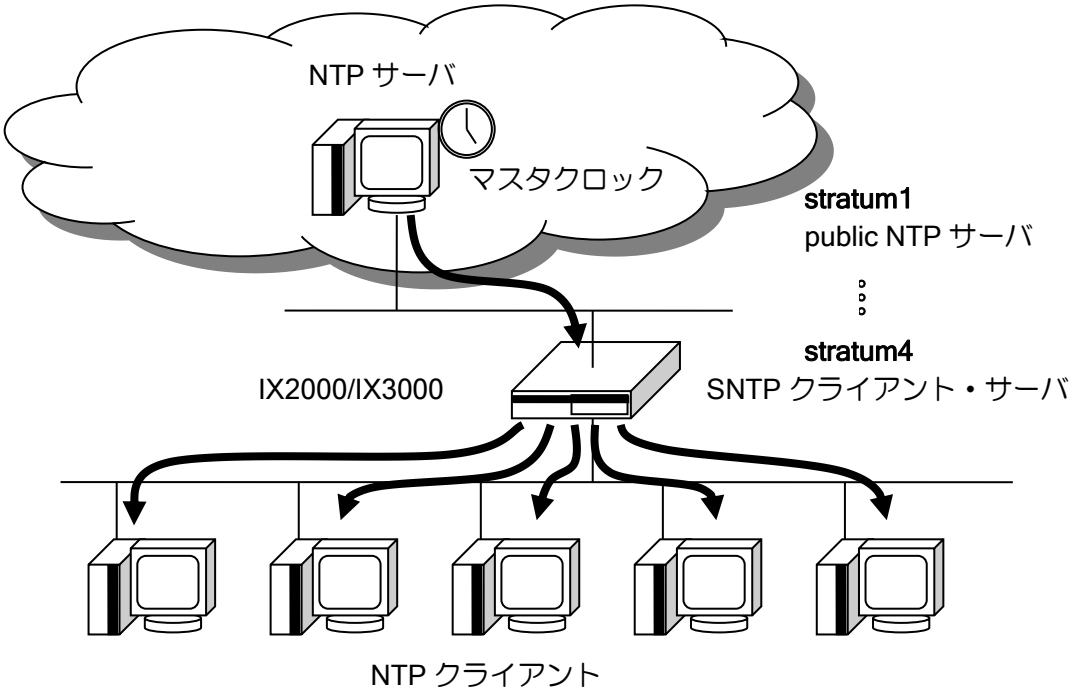
2.25.4 注意事項

- ダイナミック DNS のサービスはサーバ事業者によって実装方法が異なり、決まった更新手順がないため、サーバの実装によっては対応できない場合があります。運用する場合は事前に動作を確認してください。
- 一度の GET リクエストでアドレスを更新することができないサーバには対応しておりません。
- ダイナミック DNS 機能ではサーバから応答があると成功と判断します。応答内容が成功か失敗かを検出することができませんので、正常に更新される設定であることを 1 度確認してからご利用ください。show ddns コマンドで最後に登録した時刻、アドレスと、そのとき受信したサーバからの応答メッセージを確認することができます。
- 運用中に設定を変更した場合は、必ず ddns update コマンドで即時更新を実施してください。
- 回線接続がプライベートアドレスの場合では利用できません。

■2.26 NTP の設定

IX2000/IX3000 では、IPv4/IPv6 ともに対応した SNTP サーバ・クライアントをサポートしています。

SNTP は、NTP との接続性が保たれており、また NTP より簡易なプロトコルです。



2.26.1 NTP クライアントの設定

IX2000/IX3000 では、SNTP クライアントの以下の機能をサポートしています。MD5 などによる NTP 認証機能はサポートしていません。

- ユニキャストモード
- IPv6 対応
- DHCPv6 対応

以下に SNTP クライアントのための設定および基本的な動作を説明します。

ntp server	同期をとる NTP サーバの設定
ntp source	NTP ソースインタフェースの設定
ntp retry	NTP 同期リトライ回数の設定
ntp interval	NTP 同期間隔の設定
ntp ip/ipv6 access-list	NTP アクセスリストの設定

【設定例】1 時間に 1 回、時刻同期。タイムアウト 10 秒で 10 回までリトライ。

```
ntp interval 3600
ntp server 10.0.0.1 retry 10 timeout 10
```

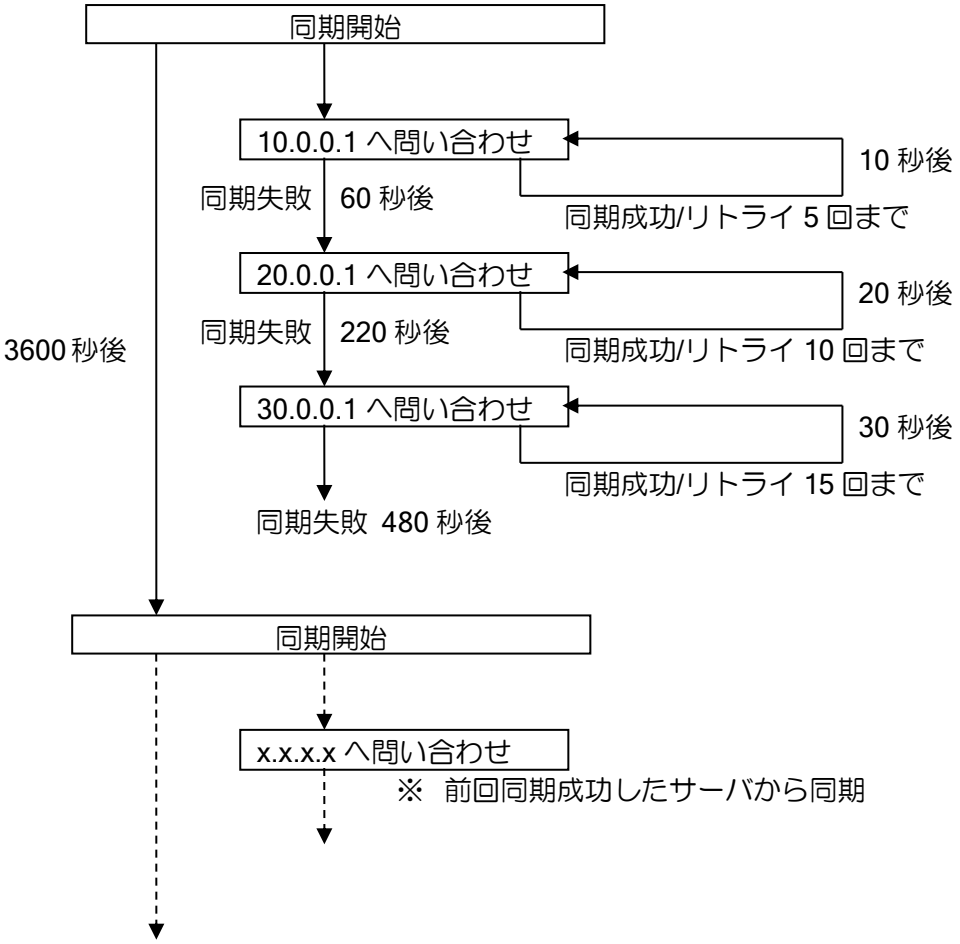
2.26.1.1 複数 NTP サーバ登録時の動作

- 同一プライオリティのサーバ問合せ

複数の NTP サーバが登録されている場合、登録順に問い合わせを行います。まず、最初に登録されている NTP サーバに問い合わせを行い、時刻の同期が取れた場合は、次の周期も同じ NTP サーバへ問い合わせを行います。時刻の同期が取れない場合は、次の周期に次の NTP サーバへ問い合わせを行います。

【設定例】

```
ntp interval 3600
ntp server 10.0.0.1 retry 5 timeout 10
ntp server 20.0.0.1 retry 10 timeout 20
ntp server 30.0.0.1 retry 15 timeout 30
```



※時刻同期周期（ntp interval）が設定されていない場合、タイムアウト設定（ntp server … timeout TIMEOUT）が時刻同期周期となります。

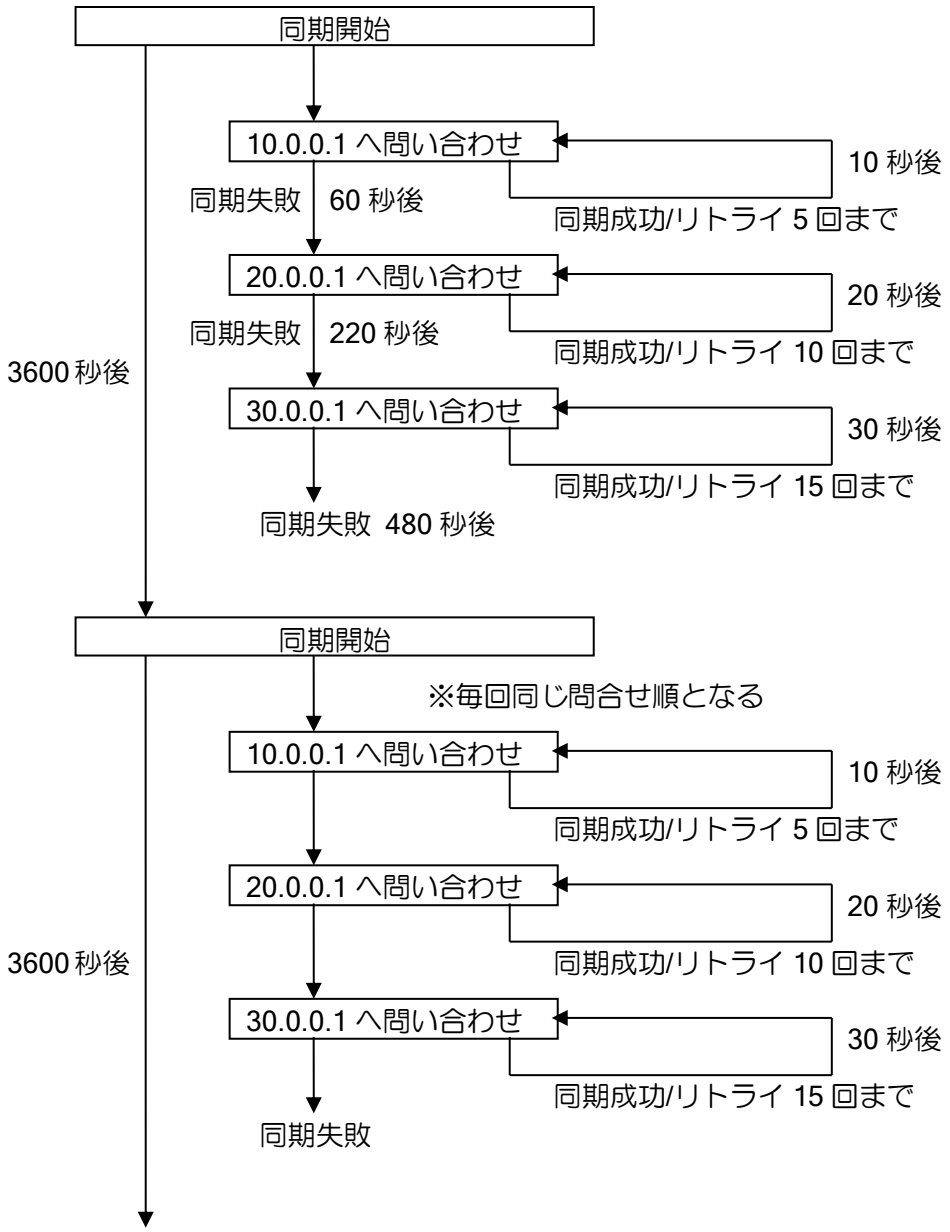
※時刻同期周期（ntp interval）は同期失敗となる時間よりも長く設定する必要があります。同期失敗する前に次の同期時刻となった場合、前回の同期はリセットされ新たに同期プロセスを開始します。

- プライオリティに従ったサーバ問合せ

NTP サーバの優先度を設定することで、問合せ順を制御することができます。NTP サーバに優先度を指定した場合、時刻同期周期で問合せるサーバは、プライオリティの大きい順となります。（デフォルトプライオリティは 1）

【設定例】

```
ntp interval 3600
ntp server 10.0.0.1 retry 5 timeout 10 priority 100
ntp server 20.0.0.1 retry 10 timeout 20 priority 50
ntp server 30.0.0.1 retry 15 timeout 30
```



2.26.1.2 DHCPv6 対応

DHCPv6 クライアントで取得した NTP サーバオプションのアドレスを利用して、NTP クライアントを動作させることができます。

```
【設定例】

ntp server dhcpv6
```

※DHCPv6 の詳細については、DHCPv6 の項目を参照してください。

2.26.2 NTP サーバの設定

IX2000/IX3000 では、SNTP サーバの以下の機能をサポートしています。MD5 などによる NTP 認証機能はサポートしていません。

- ユニキャストモード
- IPv6 対応

以下に SNTP サーバのための設定および基本的な動作を説明します。

ntp ip/ipv6 enable	NTP サーバの有効化
ntp master	ローカル NTP サーバの設定
ntp ip/ipv6 access-list	NTP アクセスリストの設定

```
【設定例】
外部 NTP サーバで、時刻同期を行います。

ntp ip enable
ntp ipv6 enable
ntp server 10.0.0.1

IX2000/IX3000 の時刻をマスタクロックとします。

ntp ip enable
ntp ipv6 enable
ntp master
```

※ローカル NTP サーバ設定（ntp master）を行っていない場合、NTP クライアントが時刻同期できない限り、NTP サーバとして機能しません。（NTP クライアントの要求に対し無効である応答を返します）

※ローカル NTP サーバ設定（ntp master）は推奨しません。信頼できる時刻サーバと時刻同期を行ってください。

2.26.3 NTP アクセスリスト

IX2000/IX3000 の NTP パケットは、アクセスリストによってアクセス制御することができます。

以下に NTP アクセスリストの設定を説明します。

ntp ip/ipv6 access-list	NTP アクセスリストの設定

【設定例】

NTP アクセスリストでは、ソースアドレスのみ評価されます。

```
ip access-list ntp-acl permit ip src 10.1.1.1/32 dest any
ntp ip access-list ntp-acl
```

■2.27 VRRP の設定

IX2000/IX3000 シリーズでは、ルータ冗長機能として VRRP をサポートしています。VRRP は次の機能を有しており、ネットワーク全体の信頼性を向上させることができます。

- ルータバックアップ
  - 一組のルータを、同一 LAN 上で同じ VRRP グループとすることで、一方のルータ（マスタルータ）が故障した場合に、他方のルータ（バックアップルータ）がそのルータのバックアップとして動作する機能です。
- ロードバランシング
  - 一組のルータの双方を、2 つの VRRP グループに属させ、双方がマスタルータおよびバックアップルータとすることで、バックアップの機能を有しながらロードバランスを行う機能です。
- ノンプリエンプトモード
  - バックアップルータがマスタ状態になったとき、プライオリティの高いマスタルータが正常にもどっても、自動切り戻ししない機能です。（デフォルトはプリエンプトモード）

2.27.1 基本設定

以下に VRRP 登録のための設定および基本的な動作を説明します。

アドレス設定以外は、IPv4、IPv6 ともに同じコマンドを使用します。同一インタフェースに IPv4,IPv6 同時に設定することは可能です。ただし、IPv4、IPv6 を含め、装置内で同じ VRID を使用することはできません。

vrrp enable	VRRP の有効
vrrp VRID authentication	VRRP 認証の設定(同一 VR グループ内では同じ値に設定する必要があります)
vrrp VRID ip	IPv4 VRRP の設定
vrrp VRID ipv6	IPv6 VRRP の設定
vrrp VRID priority	VRRP 優先度の設定 （数値の大きい方が優先度は高くなります。）
vrrp VRID redirects	ICMP リダイレクトの設定 （仮想 IP アドレス宛のパケットに対して、リダイレクトメッセージを送信）
vrrp VRID timers	VRRP タイマの設定 ・広告間隔の設定 (同一 VR グループ内では同じ値に設定する必要があります) ・切り戻りタイマの設定
vrrp VRID ip virtual-host	VR IP アドレス宛の ping/traceroute の応答の設定

2.27.1.1 IPv4 と IPv6 の動作差分

対応 RFC、プロトコルの違いにより、IPv4 と IPv6 の VRRP は以下の点が異なります。

項目	IPv4	IPv6
対応 RFC	RFC2338	RFC5798
仮想 MAC	00-00-5E-00-01- {VRID}	00-00-5E-00-02- {VRID}
仮想 IP 設定	1 個	複数設定可 ただしリンクローカルアドレスは必要
仮想 IP 宛	デフォルト不可	可能

パケット受信	設定により可能	
仮想 IP 設定インタフェース	Virtual インタフェース	VRRP を設定したインタフェース
広告送信間隔	秒単位	センチ秒（1/100 秒）単位
認証	設定可能	VRRPv3 に認証機能がなく動作しません
MIB・トラップ	対応	未対応

(a) 対応 RFC

IPv4 は RFC2338（VRRPv2）、IPv6 は RFC5798（VRRPv3）に対応しています。
VRRPv3 の IPv4 には対応していません。

(b) 仮想 MAC アドレス

仮想 MAC アドレスは以下を使用します。

IPv4	00-00-5E-00-01- {VRID}	VRID は VR グループ ID
IPv6	00-00-5E-00-02- {VRID}	VRID は VR グループ ID

(c) 仮想 IP アドレス設定

IPv4 VRRP の設定コマンド（vrrp ip）により、IPv4 の VRRP が動作します。
アドレスを省略した場合、アドレスオーナとして動作します。
また、IPv6 VRRP の設定コマンド（vrrp ipv6）により、IPv6 の VRRP が動作します。
IPv6 の場合、アドレスを複数設定することができます。アドレス設定には、リンクローカルアドレスの設定が必要です。リンクローカルアドレスが設定されていない場合、VRRP は動作しません。設定したアドレスのうち、いずれか 1 つが物理インタフェースのアドレス（グローバルアドレス、リンクローカルアドレスは問いません）と同じ場合、アドレスオーナとして動作します。

(d) 仮想 IP アドレス宛のパケット受信

IPv4 の場合は、デフォルトでは無効となります。設定により仮想 IP アドレス宛のパケットを受信できます。
IPv6 の場合は、常時仮想 IP アドレス宛のパケット受信は有効となります。設定の変更はできません。

(e) 仮想 IP アドレスの設定インタフェース

IPv4 の場合は、Virtual インタフェースに設定されます。
IPv6 の場合は、VRRP を設定したインタフェースのアドレスとして設定されます。
ソースアドレスをインタフェースで設定する場合に、仮想 IP アドレスを使用する際は、IPv4、IPv6 の該当するインタフェースを指定してください。

(f) 広告パケット送信設定

VRRP 広告パケットの送信間隔は、IPv6 では、センチ秒（1/100 秒）単位での設定ができます。IPv4 では秒単位の設定となります。センチ秒で設定した場合は秒単位に切り上げた値で動作します。

(g) 認証

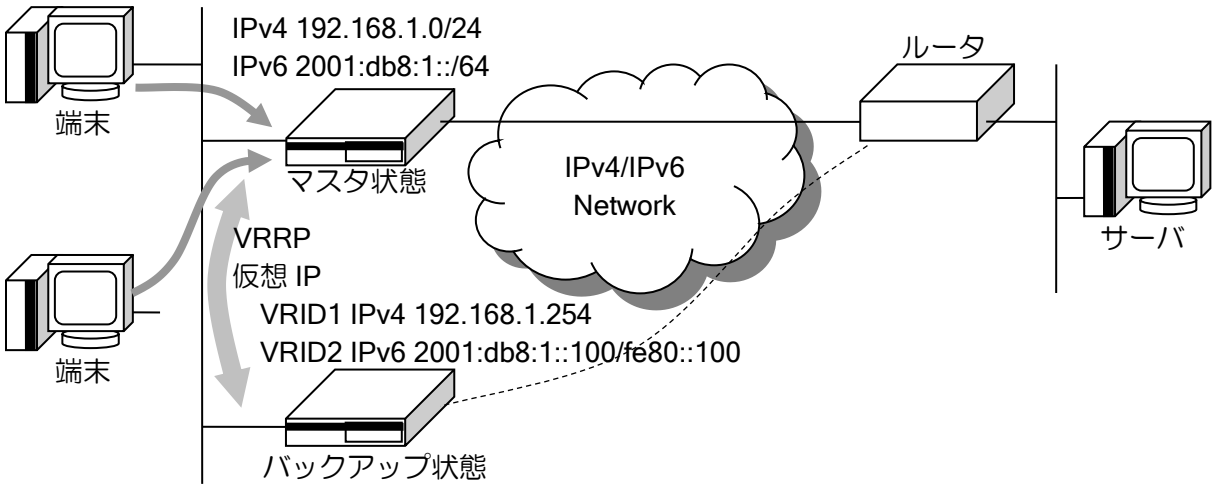
IPv4 では認証設定ができます。RFC5798 は認証をサポートしていないため、IPv6 では認証設定は動作しません。

(h) MIB・トラップ

IPv4 は RFC2787 の VRRP MIB に対応しています。IPv6 は未対応です。

2.27.1.2 設定例

IPv4 と IPv6 の VRRP を同一インタフェースで使用した場合の設定例を示します。



【設定例】

マスタルータ側の設定例

```
vrrp enable
interface GigaEthernet0.0
  ip address 192.168.1.1/24
  no ip redirects
  ipv6 address 2001:db8:1::1/64
  vrrp 1 ip 192.168.1.254
  vrrp 1 priority 200
  vrrp 2 ipv6 fe80::100
  vrrp 2 ipv6 2001:db8:1::100
  vrrp 2 priority 200
  no shutdown
```

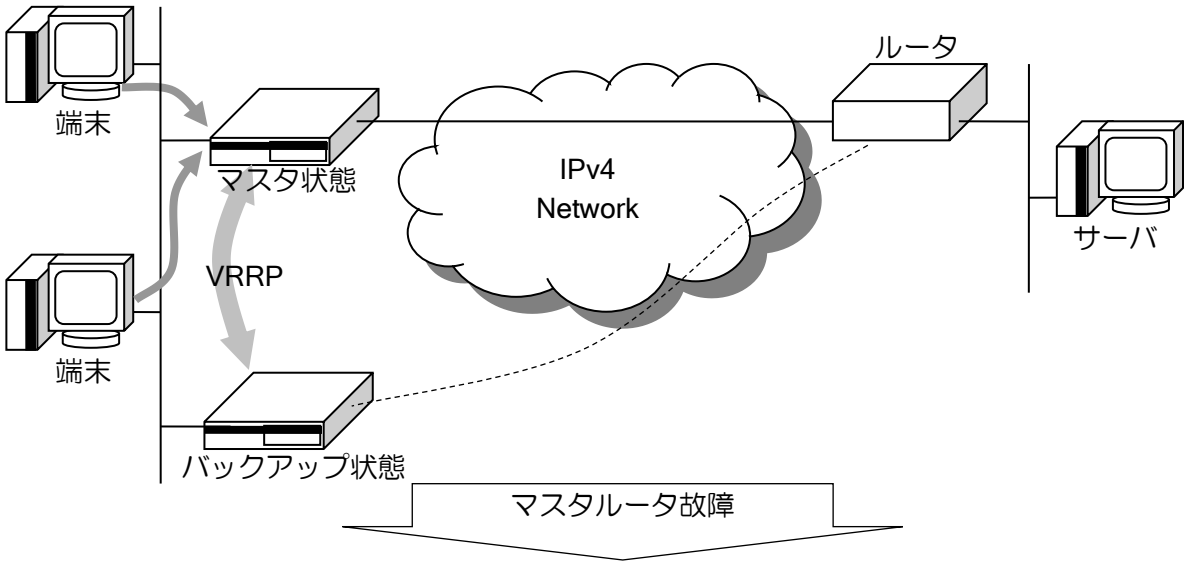
バックアップルータ側の設定例

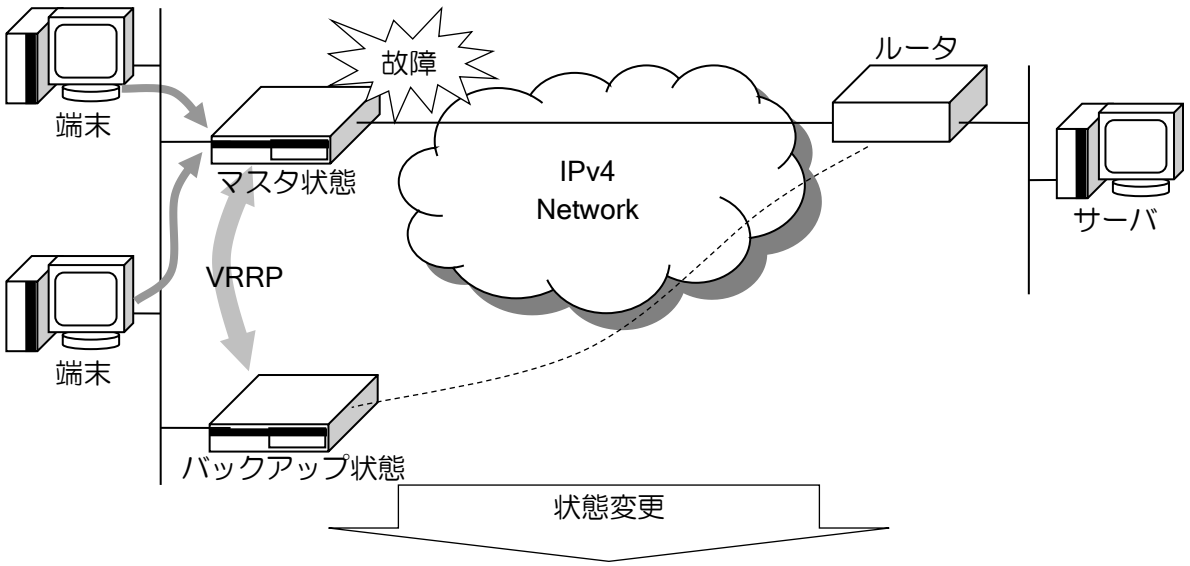
```
vrrp enable
interface GigaEthernet0.0
  ip address 192.168.1.2/24
  no ip redirects
  ipv6 address 2001:db8:1::2/64
  vrrp 1 ip 192.168.1.254
  vrrp 1 priority 100
  vrrp 2 ipv6 fe80::100
  vrrp 2 ipv6 2001:db8:1::100
  vrrp 2 priority 100
  no shutdown
```

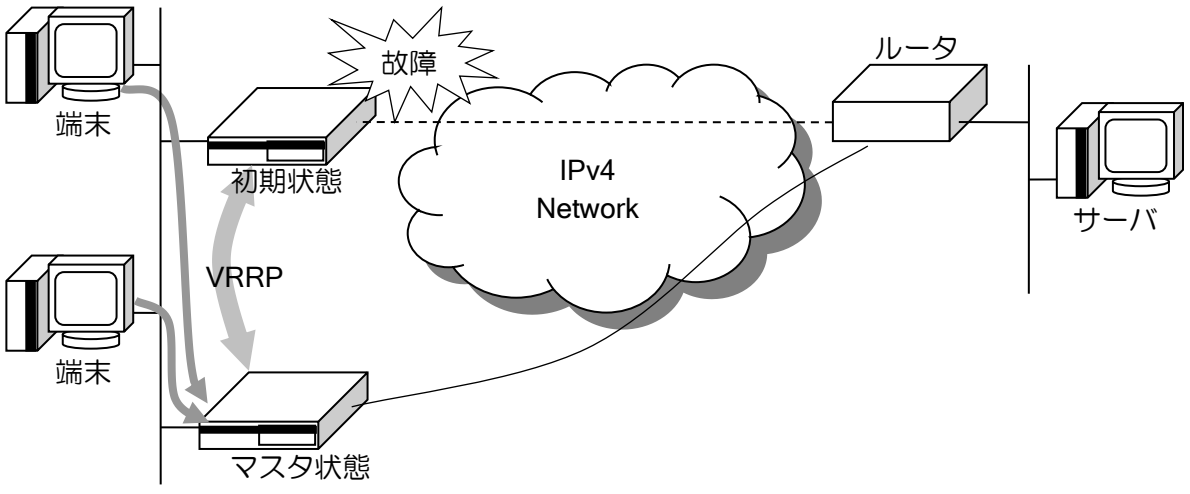
端末の設定は以下とします。
ルータの実アドレスは使用しません。
　　デフォルトルート設定
　　IPv4 : 192.168.1.254
　　IPv6：2001:db8:1::100（グローバルアドレス）
　　fe80::100（リンクローカルアドレス）

2.27.2 ルータバックアップ

ルータバックアップの基本動作と設定例を示します。







【設定例】

マスタルータ側の設定例
```
vrrp enable
interface GigaEthernet0.0
   ip address 192.168.1.1/24
   no ip redirects
   vrrp 1 ip 192.168.1.254
   vrrp 1 priority 200
   no shutdown
```

バックアップルータ側の設定例
```
vrrp enable
interface GigaEthernet0.0
   ip address 192.168.1.2/24
   no ip redirects
   vrrp 1 ip 192.168.1.254
   vrrp 1 priority 100
   no shutdown
```

端末の設定
デフォルトルートを 192.168.1.254 とします。
ルータの実アドレスは使用しません。

バックアップルータは、マスタルータからの広告パケットを一定時間受信しなかった場合、マスタルータがダウンしたと認識します。優先度が高い（設定値が大きい）程、先にマスタルータのダウンを検出します。

マスタルータのダウンを検出する時間（マスタダウンタイマ）は、以下の式で表されます。

VRRPv2

マスタダウンタイマ ＝（広告間隔×3）+（256ー優先度）／ 256

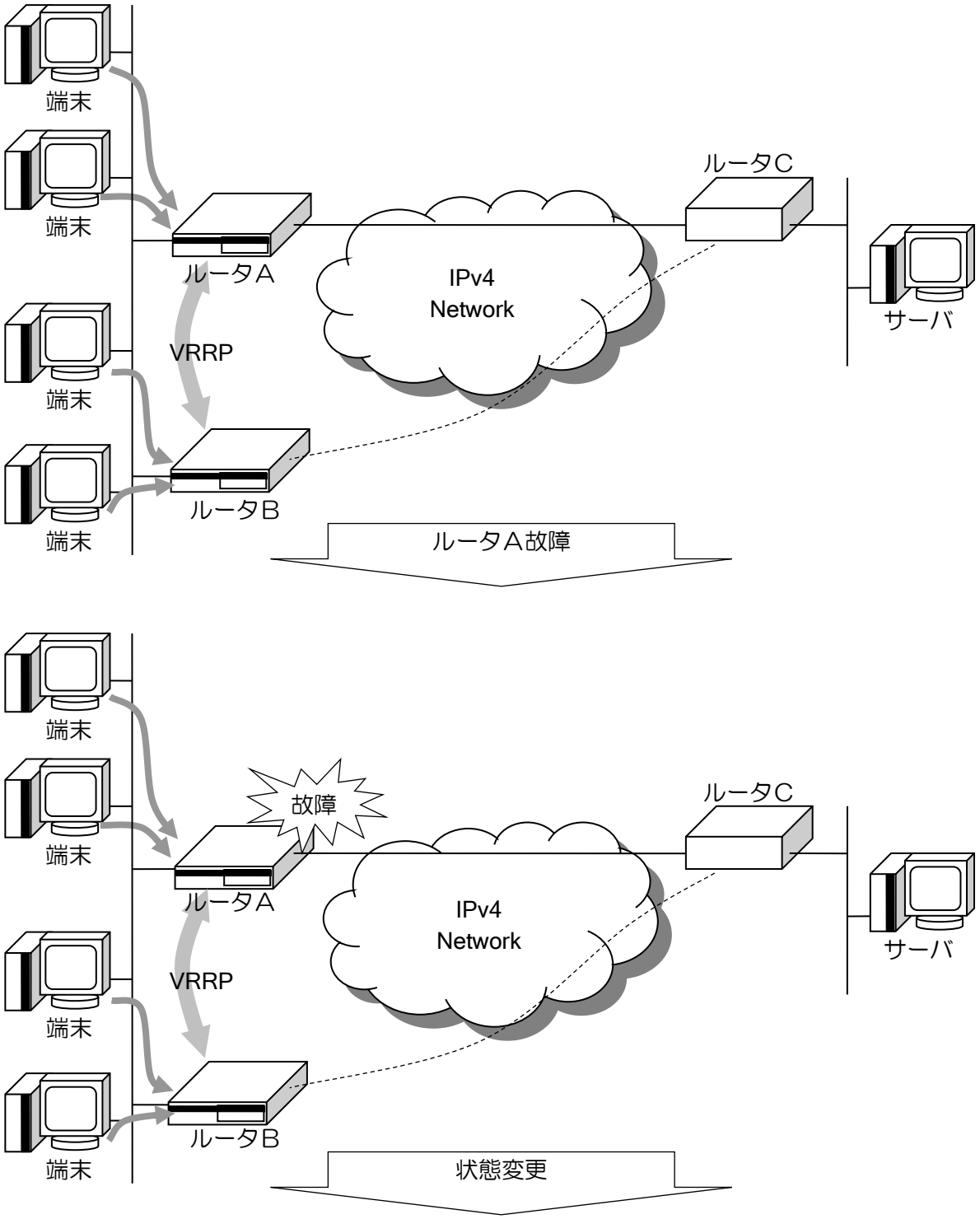
VRRPv3

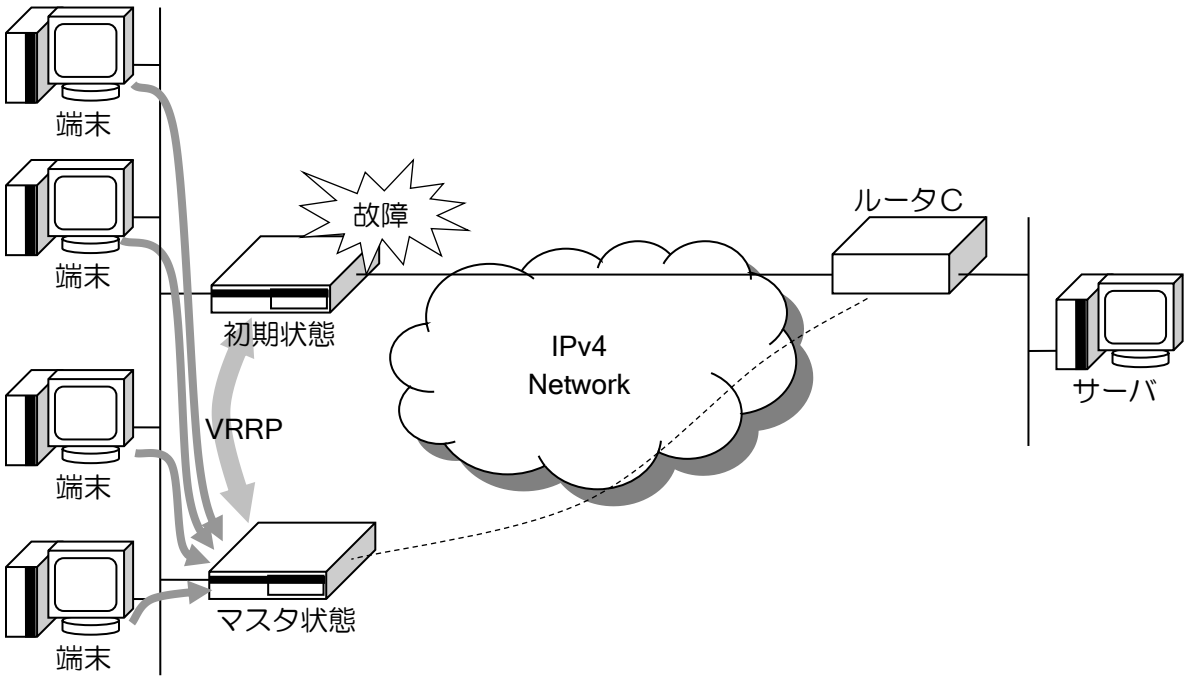
マスタダウンタイマ ＝（広告間隔×3）+（256ー優先度）× 広告間隔 ／ 256

VRRP は 1/60 秒単位でタイマ制御を行っているため、1/60 秒区切りで丸められます。

2.27.3 ロードバランシング

ロードバランシング機能の基本動作と設定例を示します。





【設定例】

ルータＡ側の設定例

```
vrrp enable
interface GigaEthernet0.0
   ip address 192.168.1.1/24
   no ip redirects
   vrrp 1 ip 192.168.1.254
   vrrp 1 priority 200
   vrrp 2 ip 192.168.1.253
   vrrp 2 priority 100
   no shutdown
```

ルータＢ側の設定例

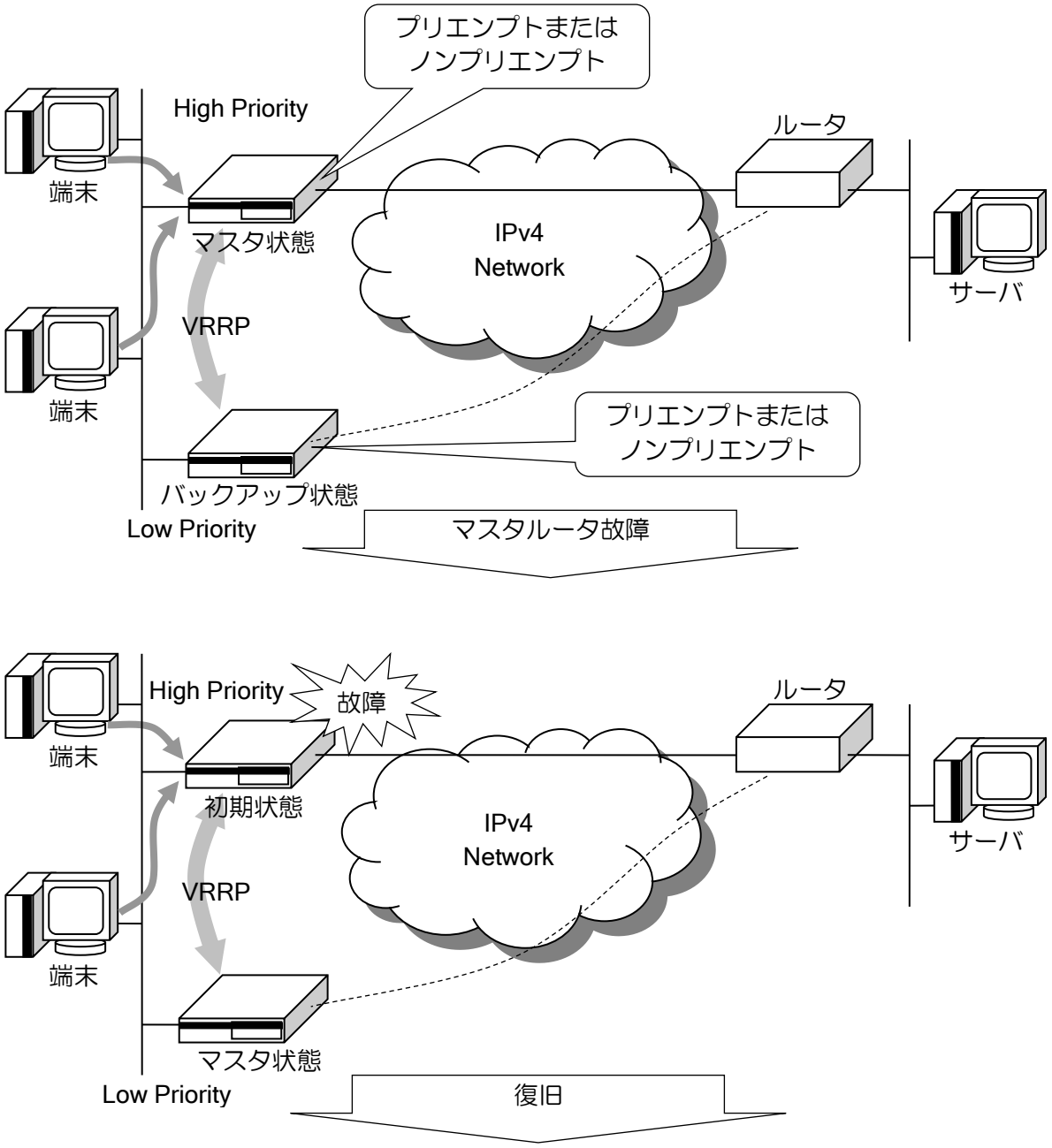
```
vrrp enable
interface GigaEthernet0.0
   ip address 192.168.1.2/24
   no ip redirects
   vrrp 1 ip 192.168.1.254
   vrrp 1 priority 100
   vrrp 2 ip 192.168.1.253
   vrrp 2 priority 200
   no shutdown
```

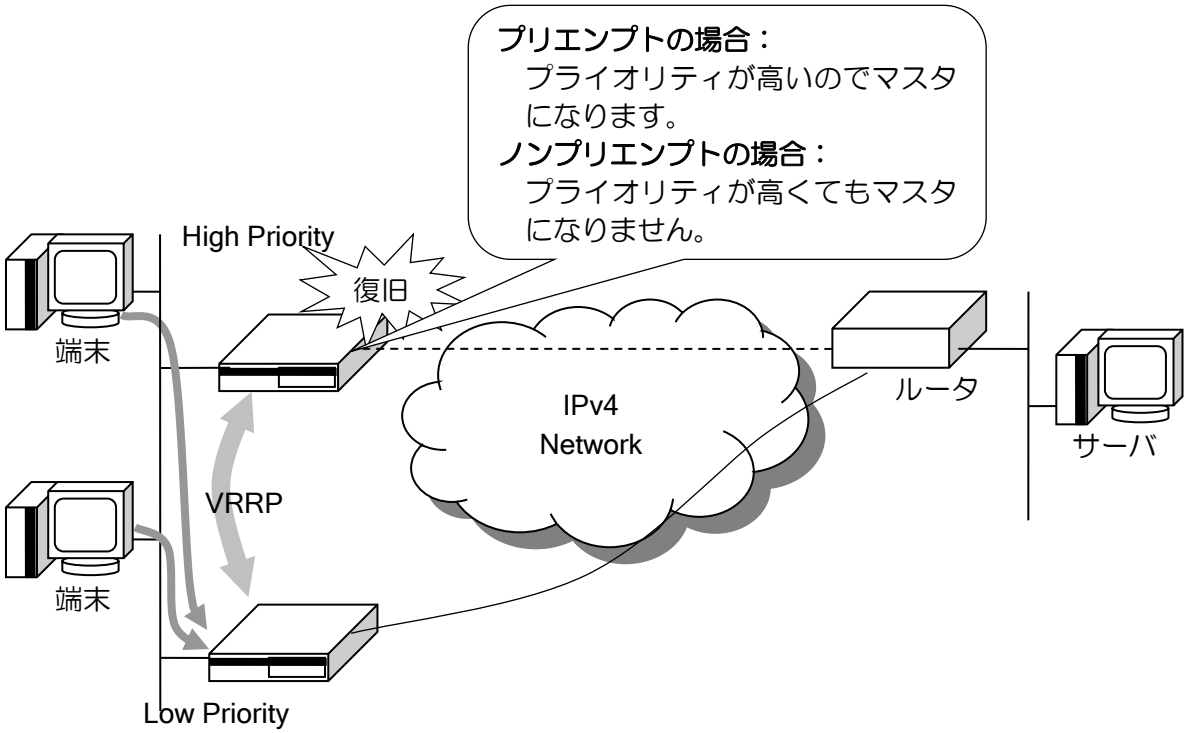
端末の設定

デフォルトルートを 192.168.1.254, 192.168.1.253 と設定します。
ルータの実アドレスは使用しません。

2.27.4 プリエンプトモードとノンプリエンプトモード

プリエンプトモードとノンプリエンプトモードの基本動作を示します。





【設定例】

マスタルータ側の設定例

```
vrrp enable
interface GigaEthernet0.0
   ip address 192.168.1.1/24
   no ip redirects
   vrrp 1 ip 192.168.1.254
   vrrp 1 priority 200
   no vrrp 1 preempt          ←この設定により、自動切りもどししなくなります
   no shutdown
```

バックアップルータ側の設定例

```
vrrp enable
interface GigaEthernet0.0
   ip address 192.168.1.2/24
   no ip redirects
   vrrp 1 ip 192.168.1.254
   vrrp 1 priority 100
   vrrp 1 preempt             ←デフォルトは、プリエンプトモードです
   no shutdown
```

※プリエンプト設定はマスタ側とバックアップ側で設定を合わせてください。

端末の設定

デフォルトルートを 192.168.1.254 と設定します。
ルータの実アドレスは使用しません。

2.27.5 VR IP アドレス宛のパケット処理

VRRPv2（IPv4）の動作

IPv4 の場合、デフォルトでは VR IP アドレス宛のパケットは廃棄します。
以下の設定を行うことで、一部の VR IP アドレス宛パケットを受信することができます。

vrrp VRID ip virtual-host	VR IP アドレス宛の応答の設定（Ver4.3 以降）

受信できるパケットは以下のとおりです。

- ping/traceroute
  ping,traceroute のパケットを受信し、応答を返します。ICMP echo request の応答は VR IP アドレスをソースアドレスとして echo reply を返します。UDP port unreachable ならば、VR IP アドレスをソースアドレスとして ICMP port unreachable を返します。

- トンネル
  トンネルの宛先となっている場合、パケットを受信します。IPsec トンネルでの使用も可能です。ソースアドレスは、tunnel source で設定した値となります。IPsec の場合は、ipsec source-address で指定した値となります。
  IPv4 の場合、VR IP アドレスをソースアドレスに使用する場合のインタフェースには Virtual インタフェースを指定してください。インタフェース番号は、VRID と同じ値となります。例えば、VRID=10 の場合のインタフェースは Virtual10 となります。

VRRPv3（IPv6）の動作

IPv6 の場合、常に VR IP アドレス宛パケットを受信することができます。
IPsec トンネルでの使用も可能です。IPv6 で VR IP アドレスをソースアドレスに使用する場合のインタフェースは、IPv4 と異なり VRRP を設定したインタフェース（GigaEthernet0.0 等）を指定してください。

2.27.6 タイマ設定

VRRP では以下のタイマの設定ができます。

- 広告タイマ
- Master 切り戻りタイマ

タイマは以下のコマンドで設定することができます。

vrrp VRID timers	VRRP タイマの設定

- 広告タイマ
  マスタルータからの広告パケットの広告間隔です。デフォルトでは 1 秒となります。広告間隔はマスタルータのダウン検出にも使用します。
  同一の VRRP グループ内では、広告間隔は全てのルータで同一の値とする必要があります。
  IPv4 では秒単位、IPv6 ではセンチ秒（1/100 秒）単位で設定できます。IPv4 使用時に、センチ秒で設定した場合は、秒単位に切り上げた値で動作します。

【設定例】
IPv6 の広告タイマを 1.5 秒に設定。

```
vrrp enable
!
interface GigaEthernet0.0
   ipv6 address 2001:db8:1::1/64
   vrrp 1 ipv6 fe80::100
   vrrp 1 priority 200
   vrrp 1 timers advertisement csec 150
   no shutdown
```

- Master 切り戻りタイマ

  プリエンプトモードの場合、優先度の高いインタフェースが up するとすぐに Master に遷移します。しかし、インタフェースが up してもルーティングが安定するまで時間がかかる構成の場合には、すぐに Master に遷移しない方が良い場合があります。そこで、すぐに Master に遷移しないようにするためにタイマを設定することができます。

  設定後は、マスタダウンタイマ＋切り戻りタイマ経過後、Master に遷移するようになります。

  以下の場合は、切り戻りタイマの時間内でもマスタに遷移します。
  - 他に Master が存在しない場合
  - 切り戻りタイマの時間内に Master が存在しなくなった場合

【設定例】
切り戻りタイマを 20 秒に設定

```
vrrp enable
!
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   vrrp 1 ip 10.0.0.254
   vrrp 1 priority 200
   vrrp 1 timers delay 20
   no shutdown
```

なお、アドレスオーナの場合は Master 切り戻りタイマは設定しないでください。実 MAC アドレスで応答を返すため、正常に通信ができない可能性があります。

2.27.7 ネットワークモニタ機能との組み合わせ

ネットワークモニタ機能と VRRP を組み合わせることで、より高度で信頼性の高いネットワークを構築することができるようになります。ネットワークモニタと VRRP 機能の組み合わせについては、ネットワークモニタの設定の項を参照してください。

ネットワークモニタで shutdown-vrrp を設定することで、プライオリティを0で広告し、即座に master を切り替えることができます。任意の条件で VRRP を強制切り替えすることが可能です。

2.27.8 VRRP 使用時の注意点

- VR IP アドレス宛の ping/traceroute 受信
  - IPv4 の場合、デフォルトは VR IP アドレス宛のパケットは廃棄します。
  - ICMP echo request の応答は VR IP アドレスをソースアドレスとして reply を返します。
  - UDP port unreachable ならば、VR IP アドレスをソースアドレスとして ICMP port unreachable を返します。

- IP アドレス設定時の動作
  - IPv4 アドレスオーナ設定時に IP アドレスが設定されていない場合は、Initialize 状態のままとなります。
  - VRRP 動作時に IP アドレスを変更した場合は、一旦 Initialize 状態となります。

- 同一インタフェースでの NAT との併用
  - 同一インタフェース内では 1 つの VRRP のみ設定してください。
  - なお、NAPT アドレスがインタフェースのアドレスと異なる場合、VRRP が Backup 状態では NAPT 変換を行いません。

■2.28 ネットワークモニタの設定

2.28.1 ネットワークモニタ機能の概要

IX2000/IX3000 シリーズでは、ネットワークモニタ機能をサポートしています。

ネットワークモニタ機能では、ICMP ECHO によるエンドエンドで常時監視やルーティングテーブル上の到達可能経路を監視することで、ネットワークの障害を検出し、迂回ルートに切り替えて通信を確保することができます。

また、同一 LAN 上に VRRP 機能を有するルータをもう一台準備し、ネットワークモニタ機能と VRRP 機能（VRRP の設定の節を参照してください）を組み合わせることで、さらなるネットワークの信頼性を向上させることもできます。

※ネットワークモニタ機能には下記の制限事項があります。

- ネットワークモニタ機能で隠蔽できるルートは Static, Connected ,ポリシールーティングの経路に限られます。
- 自分のインタフェースに設定されているアドレスをホスト監視することはできません。
- 出力先のインタフェースがダイヤルアップインタフェースの場合には、監視用 ICMP パケットが ISDN の発呼のトリガとなります。そのため、ISDN 回線の接続の有無の確認には使用できません。

以下に、ネットワークモニタ機能のコマンドと基本動作および設定例について示します。

ネットワークモニタを使用するためには、watch グループを作成する必要があります。watch グループの作成はグローバルコンフィグで、watch-group コマンドによって行います。ネットワークモニタの各種条件の設定は、watch グループコンフィグモードで行います。

watch-group	watch グループの作成（グローバルコンフィグ）
network-monitor enable	watch グループ監視の起動/停止 （グローバルコンフィグ）
network-monitor directed-response	ホスト監視パケットの応答指定 （グローバルコンフィグ）
network-monitor startup-delay	watch グループ監視起動遅延時間設定 （Ver.8.0.50 以降）（グローバルコンフィグ）
probe-counter	ICMP 個数の設定
probe-timer	各種タイマ値の設定
probe-size	各種サイズの設定
suppress	状態遷移抑止（Ver.8.5 以降）
event ip/ipv6 unreach-host	端末到達不可監視の設定
event ip/ipv6 reach-host	端末到達監視の設定
event ip/ipv6 unreach-route	経路到達不可監視の設定
event ip/ipv6 reach-route	経路到達監視の設定
event ip vr-inactive	VRRP Master 以外状態監視の設定
event ip vr-active	VRRP Master 状態監視の設定
event watch-group-status	Watch グループ状態監視の設定（Ver.8.5 以降）
event always	常時発生イベントの設定（Ver.8.5 以降）
event interface-up	インタフェース up 監視の設定（Ver.9.2 以降）
event interface-down	インタフェース down 監視の設定（Ver.9.2 以降）

action ip/ipv6 shutdown-route	隠蔽経路の設定
action ip/ipv6 resume-route	可視経路の設定
action ip/ipv6 shutdown-policy	ポリシールーティングの無効設定
action ip/ipv6 resume-policy	ポリシールーティングの有効設定
action ip shutdown-vrrp	VRRP shutdown trigger の設定
action ip resume-vrrp	VRRP resume trigger の設定
action invoke-watch-group	watch グループの開始
action revoke-watch-group	watch グループの停止
action ipsec clear-sa	IKE/IPsec SA の削除
action shutdown-interface	インタフェースの停止
action resume-interface	インタフェースの開始
action turn-BAK-LED-on	BAK LED 点灯
action shutdown-dot1x	IEEE802.1X 機能の停止
action ip decrement-vrrp-priority	VRRP プライオリティ変更（Ver.8.5 以降）
action shutdown-device	デバイスの停止（Ver.8.5 以降）
action reset-device	デバイスのリセット（Ver.8.11 以降）
action command-action-list	コマンドリストの実行（Ver.9.3 以降）
action netmeister-alarm	NetMeister アラームの設定（Ver.10.1 以降）
action netmeister-switch-mode	NetMeister 冗長時のモード変更設定(Ver10.7 以降)
clear watch-group session	watch グループの全てのアクションの復旧

2.28.2 ネットワークモニタの基本動作

ネットワークモニタの基本動作を説明します。

ネットワークモニタでは、端末到達不可監視等の監視条件（イベント）と、経路隠蔽等の監視条件を満たした場合に実行する処理（アクション）を設定します。監視条件を満たすとイベントは発生（stand）状態となり、アクションが実行されます。監視条件を満たさなくなるとイベントは通常（normal）状態に戻り、アクションは元の状態に戻ります。

【動作例】
ICMP echo により 10.1.1.254 の監視を行います。
応答が返らなくなるとイベントが発生し、10.1.30.0/24 の経路を隠蔽します。
再度応答が返るようになると、10.1.30.0/24 の経路の隠蔽を解除します。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.1
  action 10 ip shutdown-route 10.1.30.0/24 192.168.1.254
```

- 注意事項

ネットワークモニタが有効な状態で、イベント発生中にアクションを設定しても実行されません。ネットワークモニタ有効時に設定を追加する場合は、ネットワークモニタを一旦停止するか、設定後”clear watch-group session [watch グループ名]”を実行してください。

2.28.3 イベントの設定

2.28.3.1 イベント共通の動作

(a)複数イベントの動作

1 つの watch グループに複数のイベントを設定することができます。設定時に、イベントにシーケンス番号を設定します。

シーケンス番号は同一 watch グループ内で有効です。異なる watch グループ（watch グループのシーケンス番号が異なる場合も含みます）のシーケンス番号は関連しません。シーケンス番号を省略した場合は、登録順に空いている番号が使用されます。

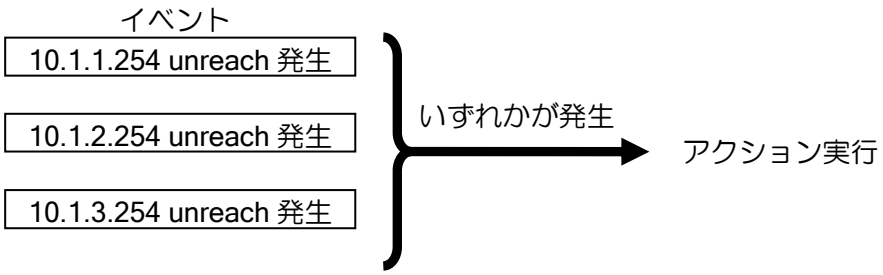
複数のイベントを設定した場合、以下のいずれかの条件でアクションを実行します。

- いずれかのイベントが発生した場合（OR 条件：デフォルト動作）

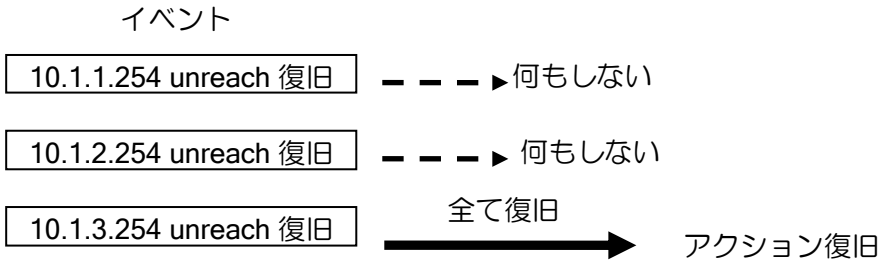
  シーケンス番号が異なるイベントはいずれかが発生した場合にアクションを実行します。

  一度アクションを実行すると、別のイベントが発生してもアクションは実行しません。アクションの復旧は、全てのイベントが復旧した場合に実行します。途中いくつかのイベントが復旧した時点では、アクションの復旧は行いません。

【イベント発生とアクション実行】



【イベント復旧とアクション復旧】



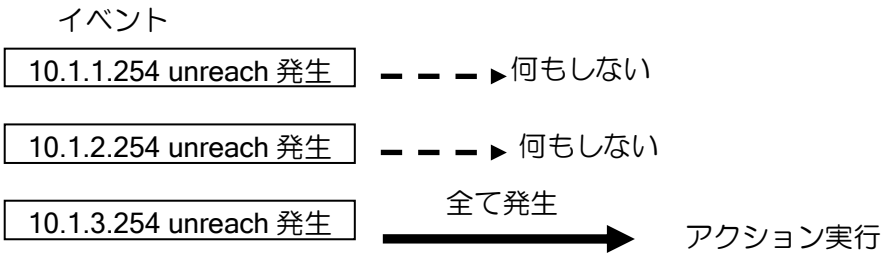
【設定例】

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
  event 20 ip unreach-host 10.1.2.254 GigaEthernet0.0 192.168.1.254
  event 30 ip unreach-host 10.1.3.254 GigaEthernet0.0 192.168.1.254
  action 10 ip shutdown-route 10.1.30.0/24

network-monitor router-1 enable
```

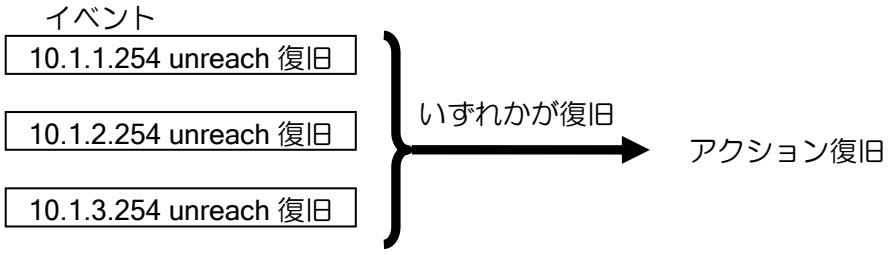
➢ 全てのイベントが発生した場合（AND 条件）（Ver.8.5 以降）

サブシーケンス番号を設定します。同じシーケンス番号のイベントの全てが発生した場合に、アクションを実行します。アクションの復旧はいずれかのイベントが復旧した場合に実行します。

【イベント発生とアクション実行】



【イベント復旧とアクション復旧】

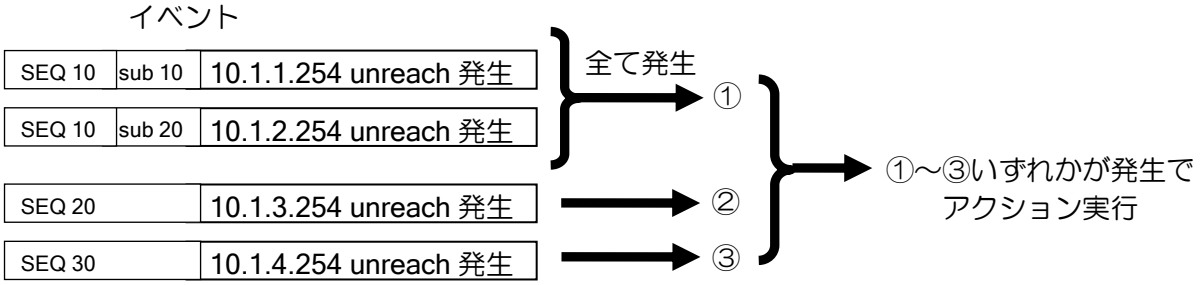


【設定例】

```
watch-group router-2 10
   event 10 sub 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
   event 10 sub 20 ip unreach-host 10.1.2.254 GigaEthernet0.0 192.168.1.254
   event 10 sub 30 ip unreach-host 10.1.3.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.30.0/24
!
network-monitor router-2 enable
```

OR 条件と AND 条件の 2 つが混在する場合は、同じシーケンス番号のイベントは全てのサブシーケンス番号のイベントが発生した場合に発生と判断し、異なるシーケンス番号のうち、いずれかが発生した場合にアクションが実行されます。

【イベント発生】



```
【設定例】

watch-group router-2 10
   event 10 sub 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
   event 10 sub 20 ip unreach-host 10.1.2.254 GigaEthernet0.0 192.168.1.254
   event 20 ip unreach-host 10.1.3.254 GigaEthernet0.0 192.168.1.254
   event 30 ip unreach-host 10.1.4.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.30.0/24
!
network-monitor router-2 enable
```

2.28.3.2 ホスト監視イベントの設定

ネットワークモニタでは、ICMP ECHO を利用したホスト監視により、イベントを発生させることができます。ホストへの到達不可の検知だけでなく、ホストへ到達可能となったときにもイベントを発生させることができます。

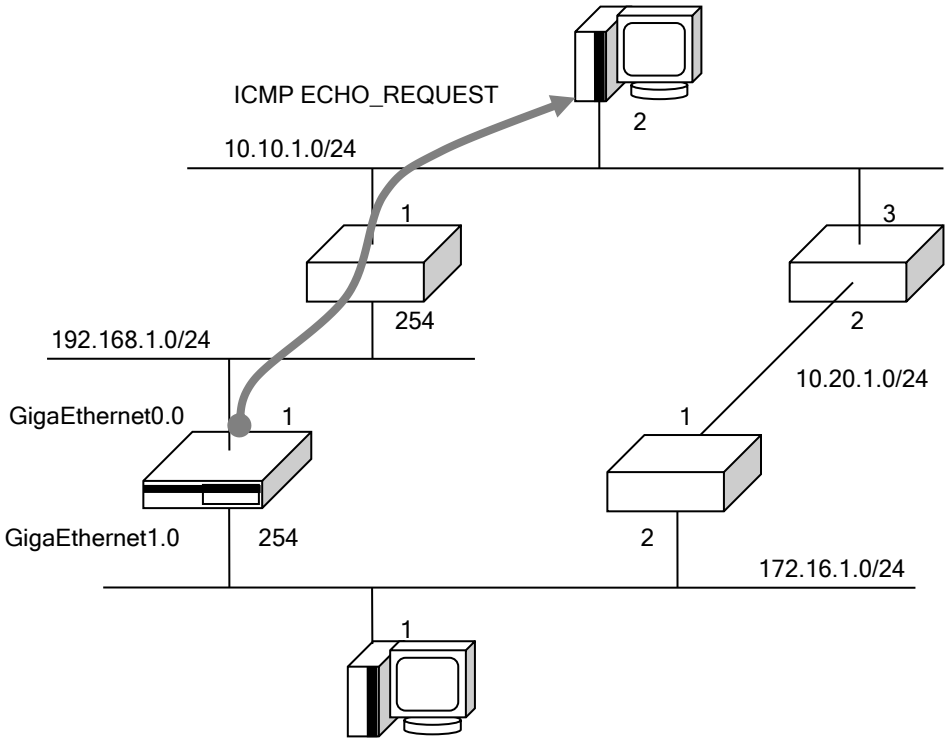
(a)ホスト監視の基本動作

ホスト監視では、設定したあて先に対して ICMP ECHO_REQUEST を送信し、応答として返される ICMP ECHO_REPLY を監視します。

ホスト監視イベントには、到達不能ホスト監視と到達可能ホスト監視の 2 種類があります。イベントの発生／復旧条件は以下のようになります。

- 到達不能ホスト監視（unreach-host）
  ICMP ECHO_REPLY が返ってきた場合、正常状態
  タイムアウトした場合、そのホストは障害が発生していると判断し、イベントが発生
- 到達可能ホスト監視（reach-host）
  タイムアウトした場合、正常状態
  ICMP ECHO_REPLY が返ってきた場合、そのホストは到達可能と判断しイベントが発生

以下は到達不能ホスト監視の場合の例になります。

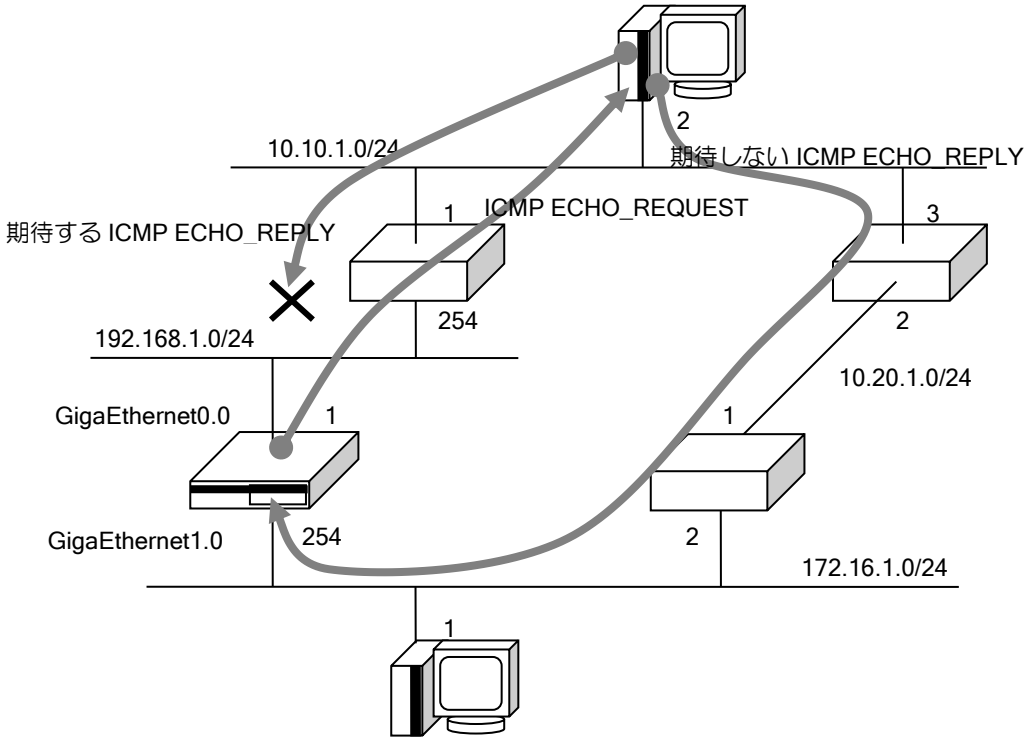


【設定例】

```
watch-group router-1 10
   event 10 ip unreach-host 10.10.1.2 GigaEthernet0.0 192.168.1.254
```

※イーサネットでオンリンク上のホスト以外を監視する場合、ネクストホップは省略しないでください。

ネットワーク設計上の注意点



IX から送信される ICMP ECHO_REQUEST は、ルーティングテーブルの情報に従わず、設定された情報を基に送信します。送信された ICMP ECHO_REQUEST、応答の ICMP ECHO_REPLY は通常の ICMP ECHO_REQUEST/REPLY と同様に扱われます。そのため、途中の装置では、ルーティングテーブルの情報に従って転送されます。

途中の経路状態によっては、ICMP ECHO_REQUEST とは異なる経路で、ICMP ECHO_REPLY が到達する場合があります。通った経路に関係なく、ICMP ECHO_REPLY が到達すると、ネットワークモニタでは正常に監視できていると見なされます。

ネットワーク設計時には注意してください。

ネットワークモニタにおけるホスト監視時に使用される、ICMP ECHO_REQUEST、ICMP ECHO_REPLY に関する設定可能なパラメータについて示します。

WATCH-COUNT	1 回の監視で送信する ICMP ECHO の個数を示します。 Ver.8.5 以降、3msec 間隔で送信します。応答があった場合は、それ以降のパケットは送信しません。 （通常運用時と障害発生時双方で有効） （デフォルト: 1 個）

VARIANCE-COUNT	イベント発生の判定回数 　イベント発生を判定するための回数となります。 　（イベント未発生時のみ有効） 　（デフォルト: 6 回） unreach-host： 　連続で ICMP ECHO REPLY を受信できなかった個数 reach-host： 　連続で ICMP ECHO REPLY を受信した個数
VARIANCE-PERCENT	イベント発生の条件（Ver8.5 以降） 　VARIANCE-COUNT にて指定した回数のうち、設定した割合の回数、監視条件を満たした場合に障害と判定します。 　（デフォルト：100%） 　未設定の場合と Ver.8.4 以前の場合は、100%として扱います。VARIANCE-COUNT の回数連続で監視条件を満たした場合に障害と判定します。
RESTORE-COUNT	イベント復旧の判定回数 　イベント復旧を判定するための回数となります。 　（イベント発生時のみ有効） 　（デフォルト: 1 回） unreach-host 　連続で ICMP ECHO REPLY を受信できた個数 reach-host 　連続で ICMP ECHO REPLY を受信できなかった個数
RESTORE-PERCENT	イベント復旧の条件（Ver8.5 以降） 　RESTORE-COUNT にて指定した回数のうち、設定した割合の回数、監視条件を満たさない場合に復旧と判定します。 　（デフォルト：100%） 　未設定の場合と Ver.8.4 以前の場合は、100%として扱います。VARIANCE-COUNT の回数連続で監視条件をみたさない場合に障害と判定します。
VARIANCE-WATCH-INT	イベント発生を判定するために ICMP ECHO REQUEST 送信する周期 （イベント未発生時のみ有効） （デフォルト: 5 秒） Ver.8.5 以降、msec 単位の指定が可能
RESTORE-WATCH-INT	イベント復旧を判定するために ICMP ECHO REQUEST 送信する周期 （イベント発生時のみ有効） （デフォルト: 5 秒） Ver.8.5 以降、msec 単位の指定が可能
WAIT-TIME	ICMP ECHO REQUEST の応答タイムアウト時間 （デフォルト: 2 秒） Ver.8.5 以降、msec 単位の指定が可能 VARIANCE-WATCH-INT，RESTORE-WATCH-INT のどちらの値よりも小さい値か同じ値を設定してください。
DATA-SIZE	ICMP ECHO REQUEST のデータサイズ （デフォルト: 56byte）

カウンタ、タイマは watch グループ設定モードで設定を行います。

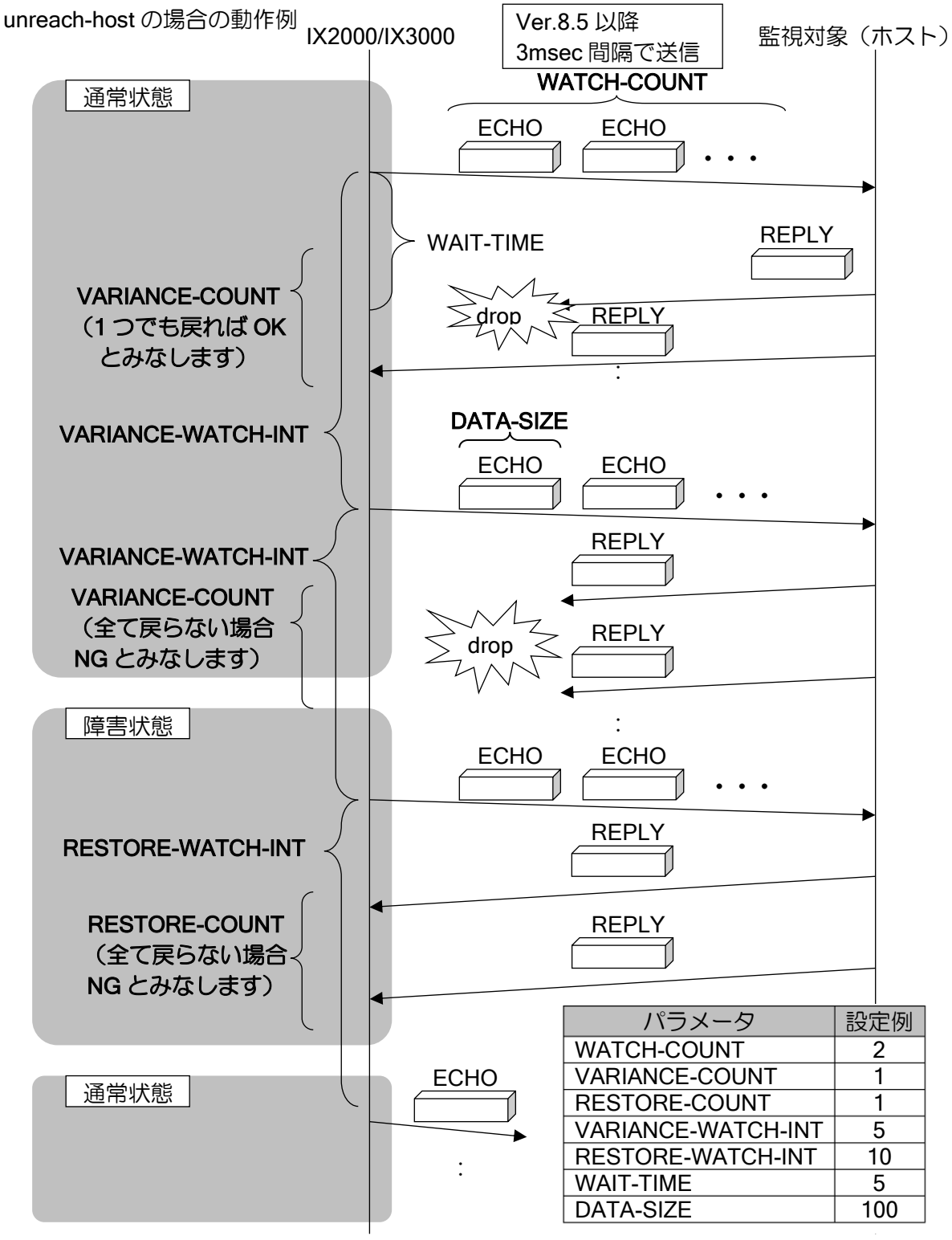
【設定例】

```
watch-group router-1 10
   probe-counter watch WATCH-COUNT
   probe-counter variance VARIANCE-COUNT percent VARIANCE-PERCENT
   probe-counter restorer RESTORE-COUNT percent RESTORE-PERCENT

   probe-timer variance VARIANCE-WATCH-INT
   probe-timer restorer RESTORE-WATCH-INT
   probe-timer wait WAIT-TIME

   probe-size DATA-SIZE
```

(b) イベント発生条件

Ver.8.4 以前、Ver.8.5 以降のデフォルト設定の場合、以下の条件で発生／復旧します。

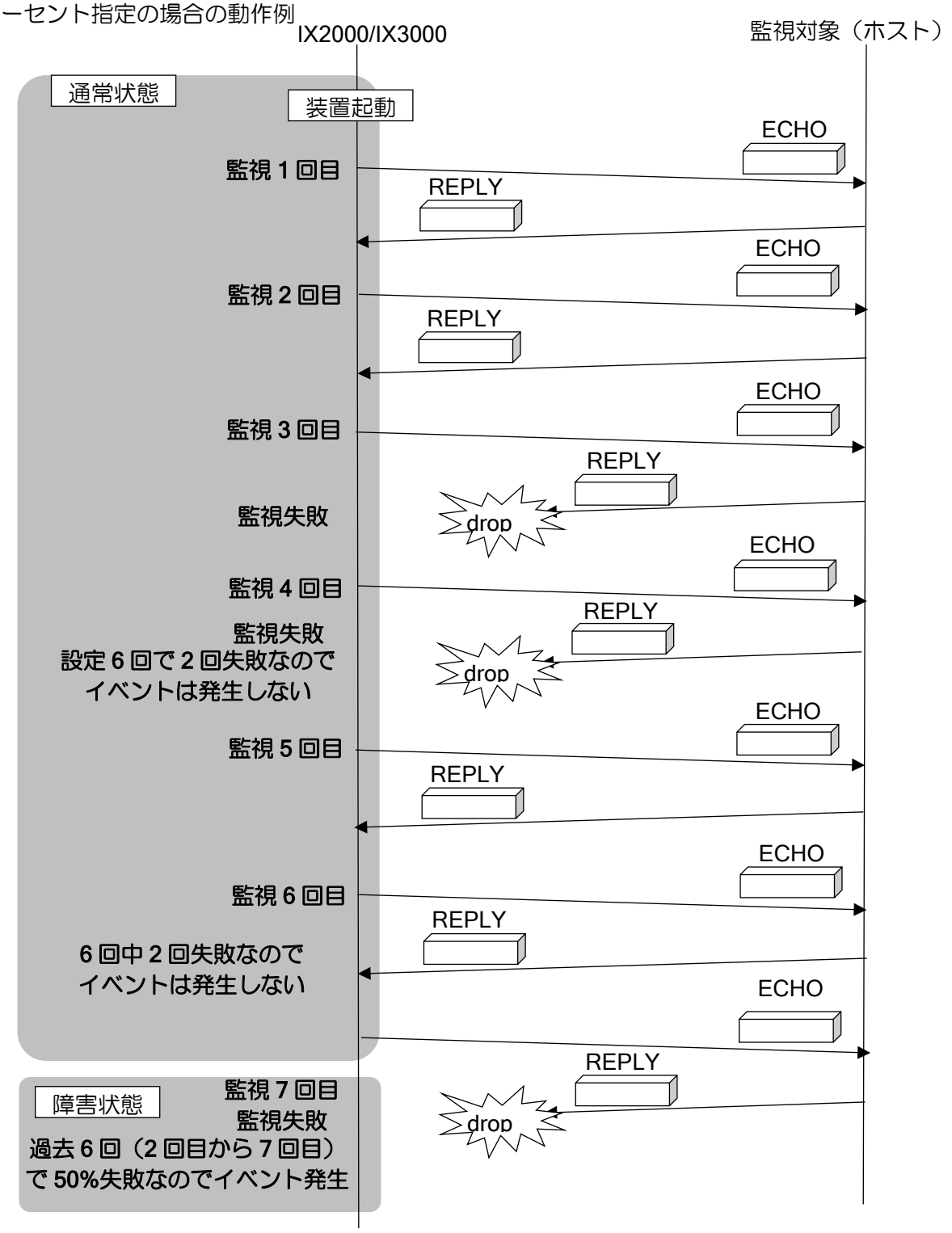
通常状態では指定間隔（VARIANCE-WATCH-INT）で ICMP ECHO-REPLY を送信し、指定回数（VARIANCE-COUNT）連続して監視条件を満たさなかった場合に、イベントが発生し障害状態となります。障害状態では指定間隔（RESTORE-WATCH-INT）で ICMP ECHO-REPLY を送信し、指定回数（RESTORE-COUNT）連続して監視条件を満たす場合に、イベントが復旧して通常状態となります。



パラメータ	設定例
WATCH-COUNT	2
VARIANCE-COUNT	1
RESTORE-COUNT	1
VARIANCE-WATCH-INT	5
RESTORE-WATCH-INT	10
WAIT-TIME	5
DATA-SIZE	100

Ver.8.5 以降では、指定回数に対する割合（VARIANCE-PERCENT、RESTORE-PERCENT）を超えた場合にイベントを発生／復旧させることが可能です。

パーセント指定の場合の動作例



【設定例】
6 回中 50%ホスト監視が失敗した場合、イベントを発生

```
watch-group test1 10
   event 10 ip unreach-host 10.0.0.1 Tunnel1.0
   action 10 ip shutdown-route 192.168.0.0/24 Tunnel1.0
   probe-counter variance 6 percent 50

network-monitor test1 enable
```

(c)ホスト監視パケット応答指定

片方向の通信障害が発生しているような状況では、双方向の監視を行っている場合、片方のみ障害を検出し迂回経路を選択する可能性があります。このため、回線障害が発生しているにもかかわらず、往復の経路が異なり、正常に通信できているように見えてしまいます。

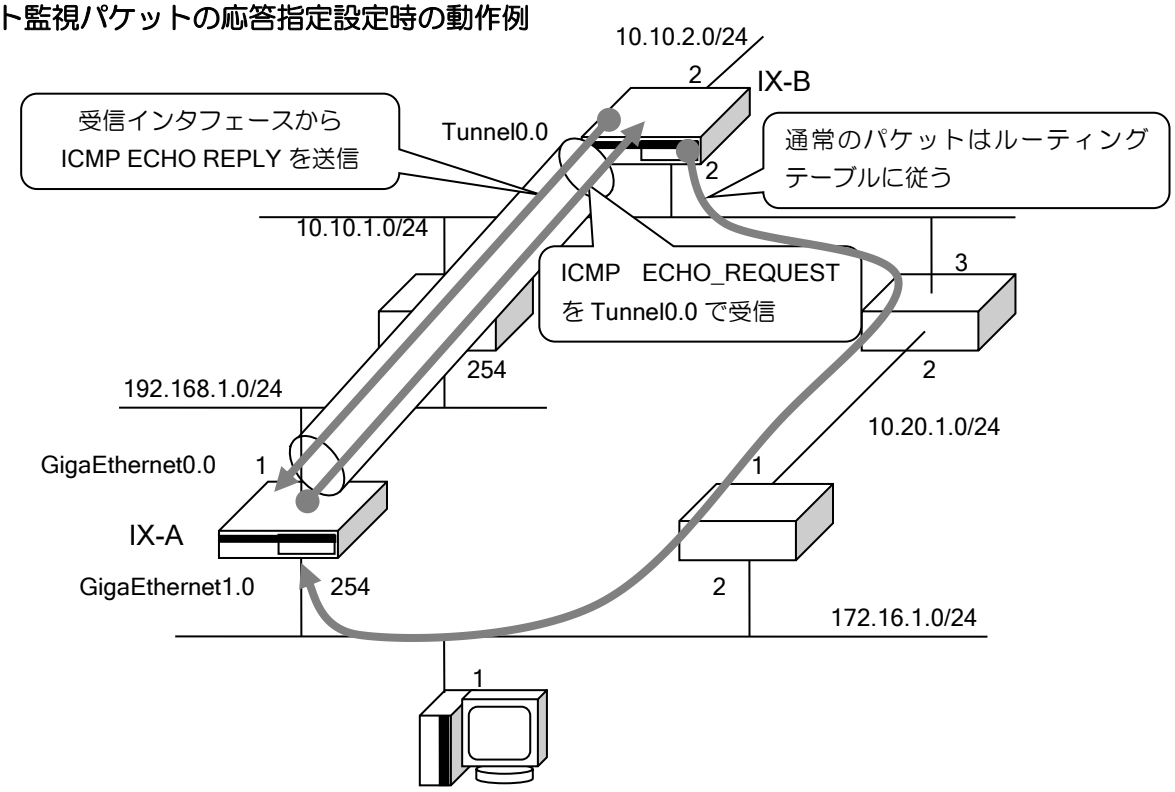
ネットワークモニタの監視用 ICMP ECHO REQUEST を送信するインタフェースから受信した ICMP ECHO REQUEST に対する ICMP ECHO REPLY は、ルーティングテーブルには依存せず、受信したインタフェースから送信することにより、往復で同じ経路を監視することができます。

IX2000/IX3000 シリーズが双方向でネットワークモニタにより監視を行っている場合、network-monitor directed-response コマンドを設定することにより、応答のパケットも監視しているインタフェースから送信することが可能(※)となります。ただし、ネットワークモニタ以外、ping 実行時の ICMP ECHO REQUEST に対しても、受信インタフェースから ICMP ECHO REPLY を送信しますので、到達性確認等の作業を行う場合はご注意ください。

対応可能なインタフェースはトンネルインタフェースや PPP など、ポイントツーポイントのインタフェースのみとなります。

※ 監視の送信元と送信先が相手側(送信先)の設定と合っていない場合は動作しません。

ホスト監視パケットの応答指定設定時の動作例




```
【設定例】
IX-A の設定

ip route default Tunnel0.0
ip route default 172.16.1.2 metric 10
!
watch-group test 10
   event 10 ip unreach-host 10.10.1.2 Tunnel0.0 source GigaEthernet1.0
   action 10 ip shutdown-route 0.0.0.0/0 Tunnel0.0
!
network-monitor test directed-response
network-monitor test enable
```

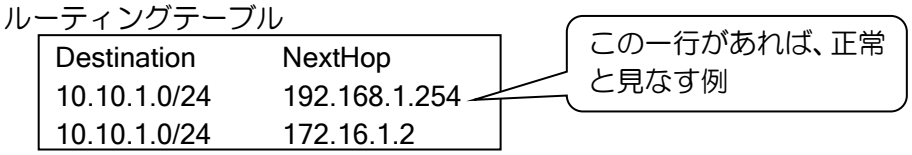
```
!
interface GigaEthernet0.0
   ip address 192.168.1.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 172.16.1.254/24
   no shutdown


IX-B の設定

ip route default Tunnel0.0
ip route default 10.10.1.3 metric 10
!
watch-group test 10
   event 10 ip unreach-host 172.16.1.254 Tunnel0.0 source GigaEthernet1.0
   action 10 ip shutdown-route 0.0.0.0/0 Tunnel0.0
!
network-monitor test directed-response
network-monitor test enable
!
interface GigaEthernet0.0
   ip address 10.10.2.2/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.10.1.2/24
   no shutdown
```

2.28.3.3 経路監視イベントの設定

ネットワークモニタではホスト監視によるイベント発生のほかに、ルーティングテーブルの経路を監視することによりイベントを発生させることができます。また、特定経路が現れたときにイベントを発生させることもできます。

(a)経路監視の基本動作

ルーティングテーブルの情報を監視し、ルーティングテーブル上にその経路がエントリされていれば正常と見なし、エントリされていなければ障害が発生していると見なします。




```
【設定例】
  watch-group router-1 10
    event 10 ip unreach-route 10.10.1.0/24 192.168.1.254

※ネクストホップを省略した場合は、ルーティングテーブル上の 10.10.1.0/24 に関わるすべてが対象となるため、すべてのエントリが削除されない限り、障害発生と見なしません。
```

ルーティング情報は以下の周期で監視を行います。

VARIANCE-WATCH-INT	イベント発生を判定する周期 （イベント未発生時のみ有効） （デフォルト: 5 秒） Ver.8.5 以降、msec 単位の指定が可能
RESTORE-WATCH-INT	イベント復旧を判定する周期 （イベント発生時のみ有効） （デフォルト: 5 秒） Ver.8.5 以降、msec 単位の指定が可能

(b)経路監視の設定

【設定例】
10.1.1.0/24 への経路監視によるイベント発生時に、10.1.31.0/24 の経路を隠蔽します。また、suppress-restoration オプションにより、この経路監視が正常に戻ったときに自動的に回復させないようにします。

```
watch-group router-1 10
  event 10 ip unreach-route 10.1.1.0/24
  action 10 ip shutdown-route 10.1.31.0/24 suppress-restoration
```

2.28.3.4 VRRP 状態監視イベントの設定

VRRP の状態を監視することにより、VRRP がマスタになった時、または、VRRP がマスタ以外になった時にイベントを発生させることができます。Ver.8.6 以降では、IPv6 の VRRP にも対応しています。

VRRP の状態監視は以下の周期で行います。

VARIANCE-WATCH-INT	イベント発生を判定する周期 （イベント未発生時のみ有効） （デフォルト: 5 秒） Ver.8.5 以降、msec 単位の指定が可能
RESTORE-WATCH-INT	イベント復旧を判定する周期 （イベント発生時のみ有効） （デフォルト: 5 秒） Ver.8.5 以降、msec 単位の指定が可能

【設定例】
GigaEthernet0.0 の VRID=1 の VRRP がマスタ以外になった時に、10.1.31.0/24 の経路を隠蔽します。

```
vrrp enable

watch-group router-1 10
  event 10 ip vr-inactive 1
  action 10 ip shutdown-route 10.1.31.0/24

interface GigaEthernet0.0
  ip address 10.0.0.1/24
  vrrp 1 ip 10.0.0.254
  no shutdown
```

2.28.3.5 watch グループ状態監視イベントの設定

Ver.8.5 以降、他の watch グループの状態を監視することにより、watch グループの状態が変更になった時にイベントを発生させることができます。

watch グループの状態が変更した時点でイベントが発生します。

【設定例】

watch グループ watch1、シーケンス番号 10 が stand になった時に、10.1.1.0/24 の経路を隠蔽します。

```
watch-group watch1 10
   event 10 ip unreach-host 10.0.0.1 Tunnel0.0
!
network-monitor watch1 enable

watch-group test 10
   event 10 watch-group-status watch1 10 stand
   action 10 ip shutdown-route 10.1.1.0/24
!
network-monitor test enable
```

2.28.3.6 常時発生／復旧イベントの設定

Ver.8.5 以降、即時に発生／復旧するイベントを設定することができます。watch グループ起動直後にイベントが発生するため、アクションも watch グループ起動直後に実行されます。

有効化するアクション（resume-route,resume-policy 等）は、アクションにより隠蔽（shutdown-route,shutdown-policy 等）する必要があります。イベントに常時発生イベントを設定し、これらのアクションを設定することにより、最初に隠蔽のアクションを実行させておくことが可能となります。

【設定例】
192.168.0.1 へ到達不可能となった場合に、10.0.0.0/24 の経路を有効化します。

watch グループ test2 10 にて常時イベントを使用することにより、ネットワークモニタ起動後に 10.0.0.0/24 の経路が隠蔽されます。
watch グループ test2 20 にて通常の監視設定を行います。

```
watch-group test2 10
   event 10 always stand
   action 10 ip shutdown-route 10.0.0.0/24 Tunnel1.0
!
watch-group test2 20
   event 10 ip unreach-host 192.168.0.1 Tunnel2.0
   action 10 ip resume-route 10.0.0.0/24 Tunnel1.0
!
network-monitor test2 enable
```

ネットワークモニタが有効な状態で、コマンドを設定した場合は、すぐにイベント発生と判断されるため、その後にアクションを設定しても実行されません。ネットワークモニタ有効時に設定を追加する場合は、ネットワークモニタを一旦停止するか、または、設定後 clear watch-group session [watch グループ名]を実行してください。これは同一内容の設定を再設定する場合も同様です。

2.28.3.7 インタフェース状態監視の設定

Ver.9.2 以降、インタフェース状態を監視することにより、インタフェースが up/down した時にイベントを発生させることができます。

【設定例】
GigaEthernet0.0 が down した場合に、Tunnel0.0 を shutdown します。

```
watch-group test 10
  event 10 interface-down GigaEthernet0.0
  action 10 shutdown-interface Tunnel0.0
!
network-monitor test enable
```

2.28.4 アクションの設定

2.28.4.1 アクション共通の動作

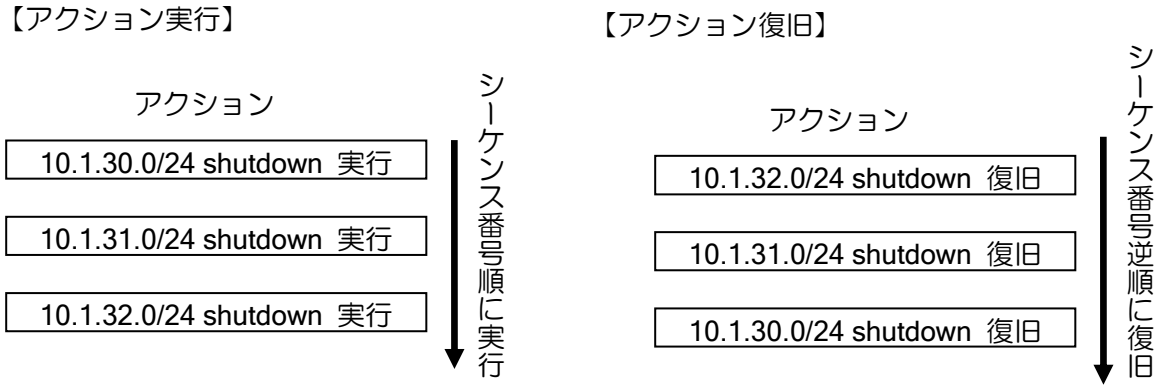
アクションは、イベント（ホスト/ネットワーク不到達等）発生時に実行され、イベント復旧時に元の状態に復旧します。action コマンドのパラメータに suppress-restoration オプションを指定することにより、イベント復旧時にアクションを復旧させないこともできます。この場合、clear watch-group session コマンドを実行することにより、アクションを復旧させることができます。

ただし、以下のアクションは、イベント復旧時、アクションの復旧を行いません。

- IKE／IPsec SA の削除

1 つの watch グループに複数のアクションを設定することができます。設定時に、アクションに、シーケンス番号を設定します。

複数のアクションを設定している場合は、アクションの実行はシーケンス番号順に行います。



【設定例】

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
  action 10 ip shutdown-route 10.1.30.0/24
  action 20 ip shutdown-route 10.1.31.0/24
  action 30 ip shutdown-route 10.1.32.0/24

network-monitor router-1 enable
```

同一のターゲットに対するアクションを複数の watch グループで設定している場合は、いずれかの watch グループのイベントが発生した場合にアクションを実行、全ての watch グループのイベントが復旧した場合にアクションを復旧します。

以下の設定例では、10.1.30.0/24 を隠蔽するアクションが test1，test2 の 2 つの watch グループで設定されています。この場合、test1，test2 のどちらか一方のイベントが発生するとアクションを実行します。また、test1，test2 両方のイベントが復旧するとアクションが復旧します。

【設定例】

```
watch-group test1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.30.0/24
!
watch-group test2 10
   event 10 ip unreach-host 10.1.2.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.30.0/24
```

2.28.4.2 経路の隠蔽・可視化

経路の隠蔽・可視化の設定を行うことにより、イベント発生時にルーティングテーブルの経路変更によって、パケットの送出先を変更することができます。

隠蔽・可視化を行うことのできる経路は以下のとおりです。

- 隠蔽：Static,Connected の経路
- 可視化：ネットワークモニタ機能で隠蔽した経路

【設定例】

10.1.1.254 へのホスト監視によるイベント発生時に、10.1.31.0/24 の経路を隠蔽します。また、suppress-restoration オプションにより、このホスト監視が正常に戻ったときに自動的に回復させないようにします。

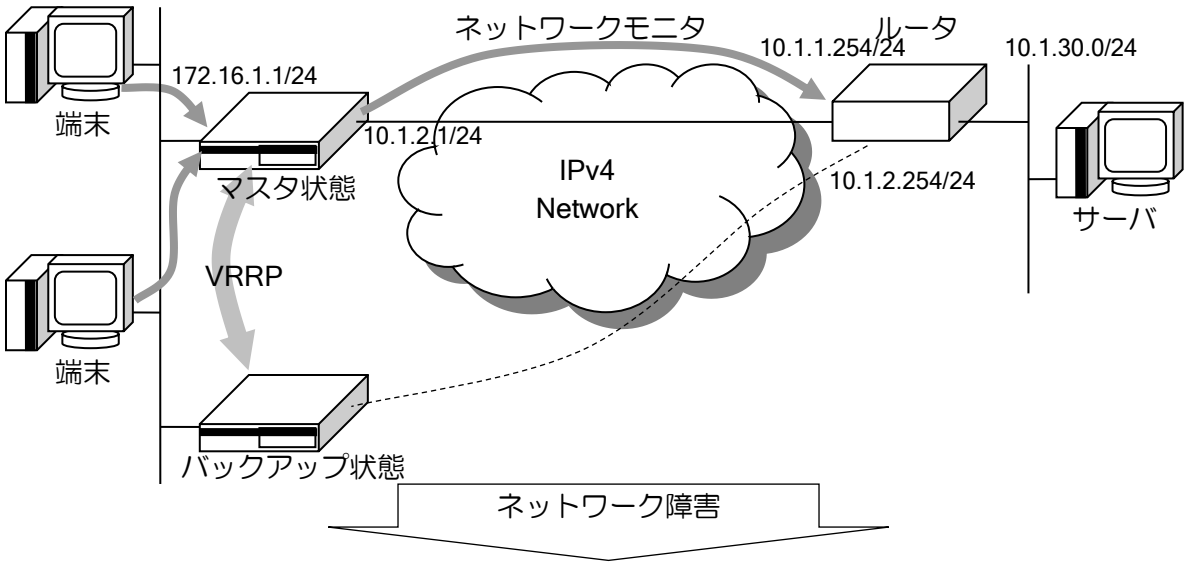
```
watch-group router-1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet0.1
   action 10 ip shutdown-route 10.1.31.0/24 suppress-restoration
```

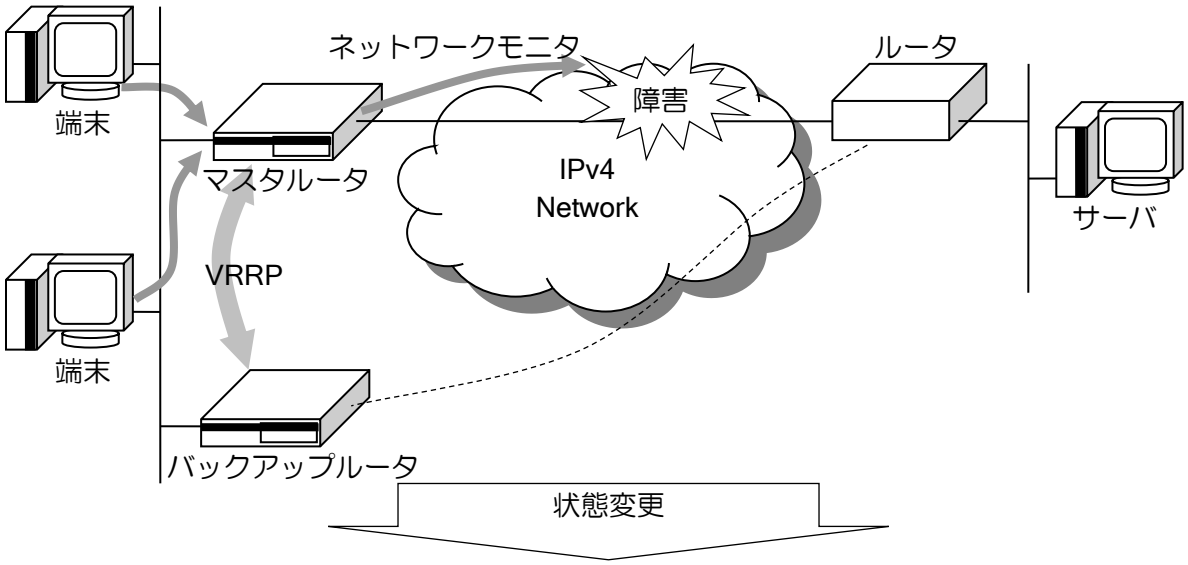
2.28.4.3 VRRP との連携

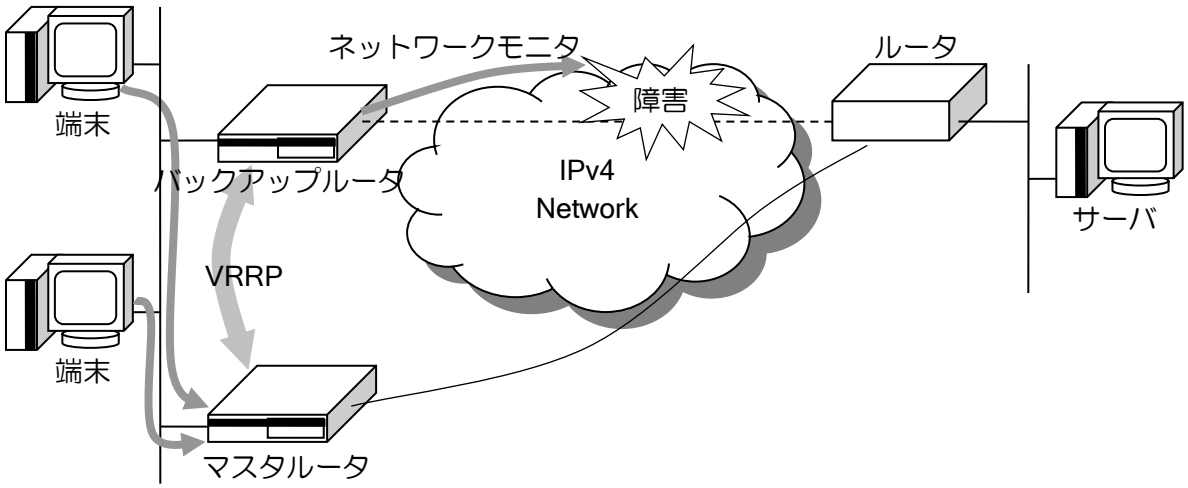
(a)VRRP シャットダウントリガ

IX2000/IX3000 のネットワークモニタでは、VRRP 機能と連携することにより、より高度で信頼性の高いネットワークを構築することができるようになります。VRRP シャットダウントリガのためのイベントと VRRP レジュームトリガのためのイベントを分けることにより、さらに高度な VRRP 制御が可能となっています。以下に VRRP とネットワークモニタ機能の組み合わせの概要を説明します。

Ver.8.6 以降、IPv6 の VRRP にも対応しています。


ネットワークモニタ
ルータ
10.1.1.254/24
10.1.30.0/24
172.16.1.1/24
端末
10.1.2.1/24
IPv4
Network
マスタ状態
10.1.2.254/24
サーバ
VRRP
端末
バックアップ状態
ネットワーク障害


ネットワークモニタ
ルータ
障害
端末
IPv4
Network
マスタルータ
サーバ
VRRP
端末
バックアップルータ
状態変更


ネットワークモニタ
ルータ
障害
端末
バックアップルータ
IPv4
Network
サーバ
VRRP
端末
マスタルータ

【設定例】

マスタルータ側の設定例

```
vrrp enable
!
watch-group host-watch 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet1.1
   action 10 ip shutdown-vrrp 1
!
network-monitor host-watch enable
interface GigaEthernet0.0
   ip address 172.16.1.254/24
   no ip redirects
   vrrp 1 ip 172.16.1.1
   vrrp 1 priority 200
   no shutdown
```

バックアップルータ側の設定例

```
ip route default 10.1.2.254
vrrp enable
interface GigaEthernet0.0
   ip address 172.16.1.253/24
   no ip redirects
   vrrp 1 ip 172.16.1.1
   no shutdown
```

端末の設定
　　デフォルトルートを 172.16.1.1 と設定します。
　　ルータの実アドレスは使用しません。

※VRRP シャットダウントリガを使用するときは必ず実 IP アドレスと VRRP 仮想 IP アドレスを別の値にする必要があります。VRRP 仮想アドレスと実アドレスを同一にした場合、そのルータの VRRP 優先度は "255"となり、必ずマスタルータになるためです。

(b) VRRP 優先度変更

Ver.8.5 以降、アクションにより VRRP 優先度を減算することが可能です。VRRP シャットダウンでは VRRP は Init 状態となり停止しますが、優先度変更では、自装置の優先度がネットワークで最大であれば VRRP マスタとして動作します。

VRRP 仮想 IP アドレスが実 IP アドレス（アドレスオーナー）の場合、優先度変更は無視されます。

【設定例】
10.1.1.254 への到達不可となった場合、VRRP の優先度を 100 減算します。

アクションが実行された場合、マスタルータ側の優先度は 50 となるため、バックアップアップルータ側が新しく VRRP マスタとなります。
バックアップルータが停止した場合は、再度マスタルータ側が VRRP マスタとなります。

マスタルータ側の設定例

```
vrrp enable
!
watch-group host-watch 10
```

```
   event 10 ip unreach-host 10.1.1.254 GigaEthernet1.1
   action 10 ip decrement-vrrp-priority 1 100
!
network-monitor host-watch enable
interface GigaEthernet0.0
   ip address 172.16.1.254/24
   no ip redirects
   vrrp 1 ip 172.16.1.1
   vrrp 1 priority 150
   no shutdown

バックアップルータ側の設定例

ip route default 10.1.2.254
vrrp enable
interface GigaEthernet0.0
   ip address 172.16.1.253/24
   no ip redirects
   vrrp 1 ip 172.16.1.1
   no shutdown

端末の設定
      デフォルトルートを 172.16.1.1 と設定します。
      ルータの実アドレスは使用しません。
```

複数 watch グループにおいて減算を行い、減算した結果が 0 以下となる場合は、優先度は 1 として動作します。また、アクションが復旧した場合も、1 以上になるまでは、優先度は 1 として動作します。

```
【設定例】
複数 watch グループから VRRP 優先度変更を行った場合の動作例

watch-group test1 10
   event 10 ip unreach-host 192.168.0.1 Tunnel1.0
   action 10 ip decrement-vrrp-priority 1 60
!
network-monitor test1 enable

watch-group test2 10
   event 10 ip unreach-host 192.168.0.2 Tunnel1.0
   action 10 ip decrement-vrrp-priority 1 60
!
network-monitor test2 enable

watch-group test3 10
   event 10 ip unreach-host 192.168.0.3 Tunnel1.0
   action 10 ip decrement-vrrp-priority 1 60
!
network-monitor test3 enable

interface GigaEthernet0.0
   ip address 172.16.1.254/24
   no ip redirects
   vrrp 1 ip 172.16.1.1
   no shutdown
```

【動作例】

動作	減算結果	watch グループ状態			補足
		test1	test2	test3	
100	100	正常	正常	正常	
40	40	障害発生（-60）	正常	正常	
1	-20	障害	障害発生（-60）	正常	結果がマイナスの場合は 1
1	-80	障害	障害	障害発生（-60）	結果がマイナスの場合は 1
1	-20	障害	障害	障害復旧（+60）	結果がマイナスの場合は 1
40	40	障害	障害復旧（+60）	正常	
100	100	障害復旧（+60）	正常	正常	

2.28.4.4 ポリシールーティングとの連携

ネットワークモニタのイベント発生時に、指定インタフェースのポリシールーティングを有効・無効にすることができます。また、ローカルパケットのポリシールーティングについても、有効・無効にすることができます。

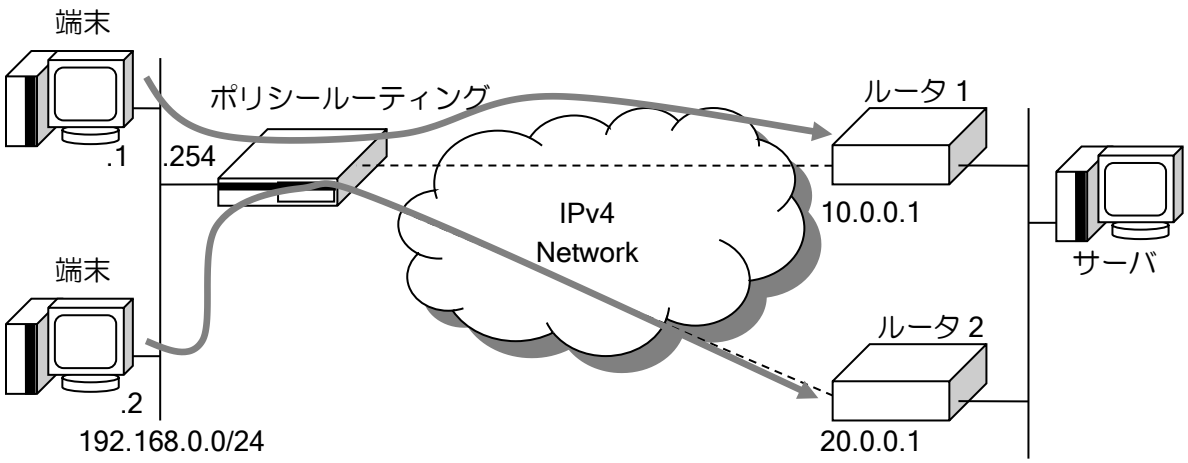
ポリシールーティングの詳細については、ポリシールーティングの項を参照してください。

【設定例】

20.0.0.1 へ到達不可となった場合、TCP パケットのポリシールーティングの設定を無効にする。

```
ip access-list acl1 permit tcp src any sport any dest any dport any
!
watch-group prte 10
   event 10 ip unreach-host 20.0.0.1 GigaEthernet1.0 10.1.1.254
   action 10 ip shutdown-policy GigaEthernet0.0
!
network-monitor prte enable
!
route-map rmap permit 10
   match ip address access-list acl1
   set ip next-hop 10.1.1.254
!
interface GigaEthernet0.0
   ip address 10.1.1.1/24
   no ip redirects
   ip policy route-map rmap
   no shutdown
```

route-map のシーケンス番号単位に有効・無効を設定することができます。



【設定例】
10.0.0.1 へ到達不可となった場合、ルータ 1 へのポリシールーティングを無効にし、
20.0.0.1 へ到達不可となった場合、ルータ 2 へのポリシールーティングを無効にする。

```
!
ip route default 192.168.0.100

ip access-list host1 permit ip src 192.168.0.1/32 dest any
ip access-list host2 permit ip src 192.168.0.2/32 dest any
!
watch-group router1 10
   event 10 ip unreach-host 10.0.0.1 GigaEthernet0.0 100.0.0.1
   action 10 ip shutdown-policy GigaEthernet2.0 route-map-seq 10
!
network-monitor router1 enable
!
watch-group router2 10
   event 10 ip unreach-host 20.0.0.1 GigaEthernet1.0 200.0.0.1
   action 10 ip shutdown-policy GigaEthernet2.0 route-map-seq 20
!
network-monitor router2 enable
!
route-map rmap permit 10
   match ip address access-list host1
   set ip next-hop 100.0.0.1
!
route-map rmap permit 20
   match ip address access-list host2
   set ip next-hop 200.0.0.1
!
interface GigaEthernet0.0
   ip address 100.0.0.254/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 200.0.0.254/24
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.0.254/24
   ip policy route-map rmap
   no shutdown
```

2.28.4.5 IPsecとの連携

ネットワークモニタのイベント発生時に、IKE/IPsec SA を削除することができます。デフォルトでは IKE/IPsec 両方の SA を削除します。設定により、IPsec の SA のみ削除することも可能です。このアクションはイベント発生時にのみ実行し、イベント復旧時には何も行いません。IKE／IPsec の詳細については、IKE／IPsec の項を参照してください。

【設定例】
Tunnel0.0 の IPsec トンネルを監視し、障害発生時に、IPsec SA の削除を行う。
（IKE／IPsec の設定は省略します）

```
watch-group ipsec-keepalive 10
  event 10 ip unreach-host 192.168.0.2 Tunnel0.0
  action 10 ipsec clear-sa Tunnel0.0 mode ipsec-only
!
network-monitor ipsec-keepalive enable
```

Ver8.4 以前はアクション実行時に一度 SA を削除しますが、アクション実行中に SA が生成された場合には削除されません。

Ver8.5 以降では周期的に SA を監視することでアクション実行中に作成された SA も削除を行います。監視周期は「復旧時間 ×（監視回数+2)」で、それ以上の値で変更も可能です。

2.28.4.6 インタフェースの停止・開始

イベント発生時にインタフェースの停止・開始を行うことができます。インタフェースの開始は、ネットワークモニタのアクションにより停止を行っているインタフェースに対してのみ行うことができます。

shutdown を設定しているインタフェースに対して、インタフェースの開始を行うことはできませんが、インタフェースの停止は有効になります。ネットワークモニタによりインタフェース停止中は、no shutdown を設定しても、インタフェースは有効になりません。イベントが復旧するか、インタフェース開始のアクションを実行することで、インタフェースが有効になります。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、GigaEthernet0.0 を停止します。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet1.0
  action 10 shutdown-interface GigaEthernet0.0
```

2.28.4.7 デバイスの停止

Ver.8.5 以降、イベント発生時にデバイスの停止を行うことができます。停止可能なデバイスは Ethernet デバイスのみとなります。BRI や Serial デバイスはアクションにより停止することはできません。

ネットワークモニタによりデバイス停止中は、no shutdown を設定しても、デバイスは有効にはなりません。イベントが復旧することによりデバイスが有効になります。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、GigaEthernet0 を停止します。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet1.0
  action 10 shutdown-device GigaEthernet0
```

2.28.4.8 デバイスのリセット

Ver.8.11 以降、イベント発生時にデバイスのリセットを行うことができます。リセット可能なデバイスは USB デバイス、Ethernet デバイス（Ver.9.3 以降）となります。その他のデバイスはアクションによりリセットすることはできません。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、USB0 をリセットします。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0
  action 10 reset-device USB0
```

イベント発生中は、「復旧時間 ×（監視回数+2）」かリセットの最短周期の短い方の周期でデバイスをリセットします。

2.28.4.9 BAK-LED の点灯

BAK-LED は、ネットワークモニタで制御できます。イベントが発生することでアクションが実行され LED が点灯します。複数の watch グループで点灯の設定を行っている場合、いずれかの watch グループでイベントが発生している場合に点灯し、全ての watch グループのイベントが復旧すると消灯します。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、192.168.0.0/24 の経路を隠蔽し、BAK-LED を点灯します。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet1.0
  action 10 ip shutdown-route 192.168.0.0/24 GigaEthernet0.1
  action 20 turn-BAK-LED-on
```

2.28.4.10 IEEE802.1X 機能との連携

イベント発生時に IEEE802.1X 機能を停止することができます。IEEE802.1X 機能を停止すると IEEE802.1X 認証は行いません。IEEE802.1X の詳細については、IEEE802.1X の項を参照してください。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、GigaEthernet1.0 の IEEE802.1X 機能を停止します。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 10.0.0.1
  action 10 shutdown-dot1x GigaEthernet1.0
```

2.28.4.11 NetMeister 機能との連携

(a) NetMeister アラーム通知

Ver10.1 以降、NetMeister にアラームを上げることができます。イベントが発生することでアクションが実行され NetMeister にアラームが送信されます。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、NetMeister にアラームを送信します。

```
!
watch-group router1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 10.0.0.1
   action 10 netmeister-alarm severity warn description wan-watch
```

(b) NetMeister 冗長モードの変更

Ver10.7 以降、NetMeister の冗長モードの変更を行うことができます。イベントが発生することでアクションが実行され NetMeister の冗長モードが変更されます。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、NetMeister の冗長モードを変更します。

```
!
watch-group router1 10
   event 10 ip unreach-host 10.1.1.254 Tunnel0.0
   action 10 netmeister-switch-mode standby
```

2.28.4.12 コマンドリストの実行

Ver.9.3 以降、イベント発生時にコマンドリストを実行することにより、任意のコマンドを実行することができます。イベント発生時とイベント復旧時に異なるコマンドリストを指定することができます。

コマンドリストの詳細については、スケジューラの項を参照してください。

【設定例】
10.1.1.254 へのホスト監視によるイベント発生時に、show interfaces を実行します。

```
command-action list com-show-int
   command 10 show interfaces
!
watch-group router1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 10.0.0.1
   action 10 command-action-list variance com-show-int
```

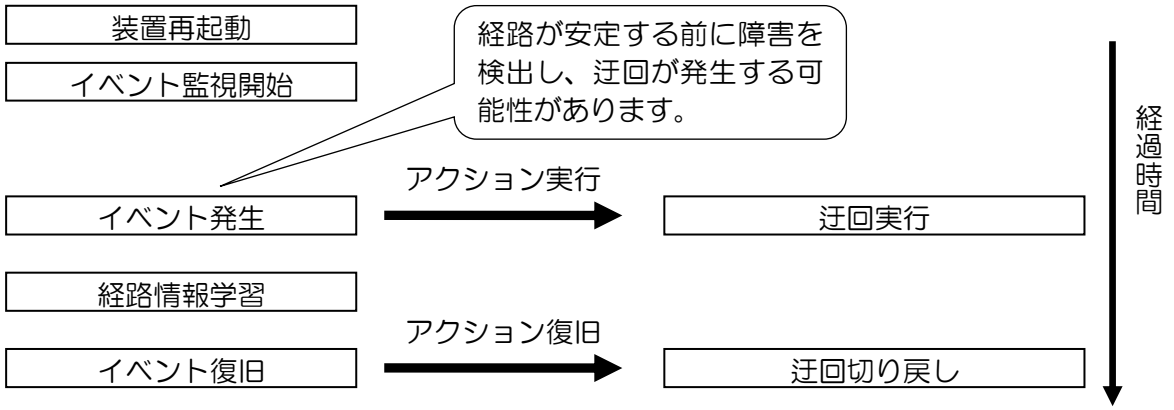
2.28.5 watch グループ毎の設定

2.28.5.1 watch グループ監視起動遅延時間設定

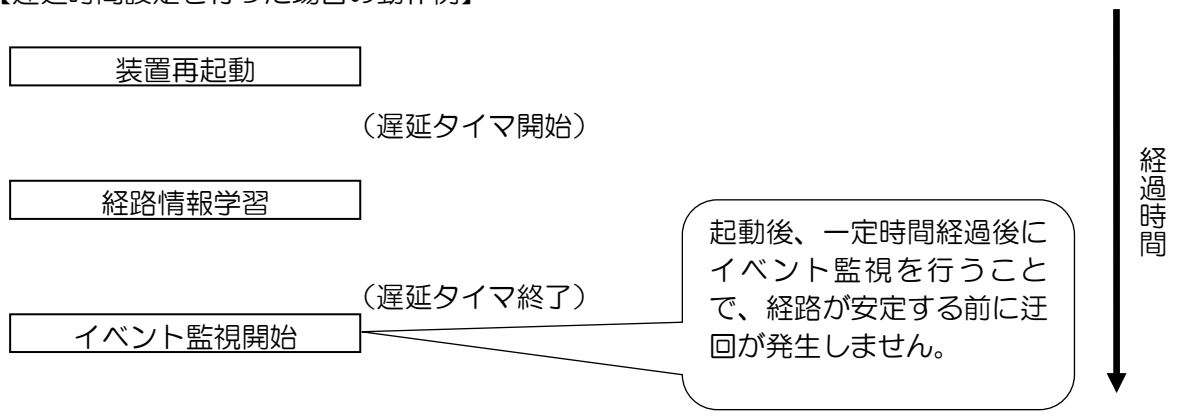
Ver.8.0.50 以降では、装置の再起動の際に watch グループによる監視の開始を遅らせることができます。装置起動から設定した遅延時間の間は、イベントの監視を行いません。これにより、装置起動直後の経路情報が安定していない状態のときに迂回が発生することを回避することができます。

本機能は、装置起動直後のみ有効です。装置起動から指定時間経過後は従来の動作となります。

【遅延時間設定を行わない場合の動作例】



【遅延時間設定を行った場合の動作例】



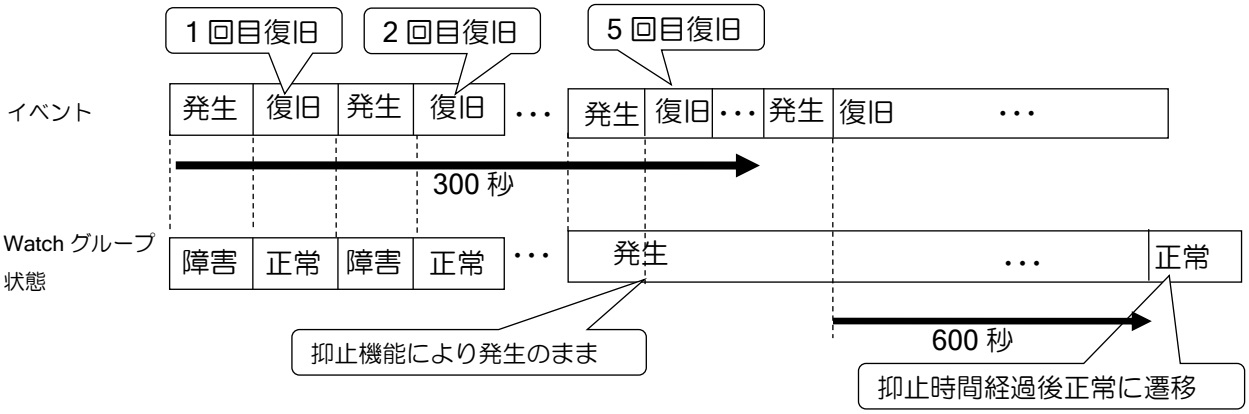
【設定例】
起動開始後、200 秒後にイベント監視を開始します。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
  action 10 ip shutdown-route 10.1.31.0/24

network-monitor router-1 enable
network-monitor router-1 startup-delay 200
```

2.28.5.2 状態変更抑止

Ver.8.5 以降、一定時間に watch グループの状態が一定回数変化した場合、一定時間 watch グループの状態変更を抑止することができます。これにより、短時間に状態変更が繰り返されるような不安定な状態が継続している場合は、状態を変更させずに、安定したネットワーク運用を行うことが可能となります。

抑止期間中に状態変更が発生しなかった場合、その時点の状態に応じて状態を変更します。抑止期間中に状態変更が発生した場合は、その時点から抑止時間を計測します。



【設定例】
300 秒以内に 5 回復旧が発生した場合、600 秒間復旧を抑止します。

```
watch-group router-1 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
  action 10 ip shutdown-route 10.1.31.0/24
  suppress restoration period 300 count 5 suppress-time 600

network-monitor router-1 enable
```

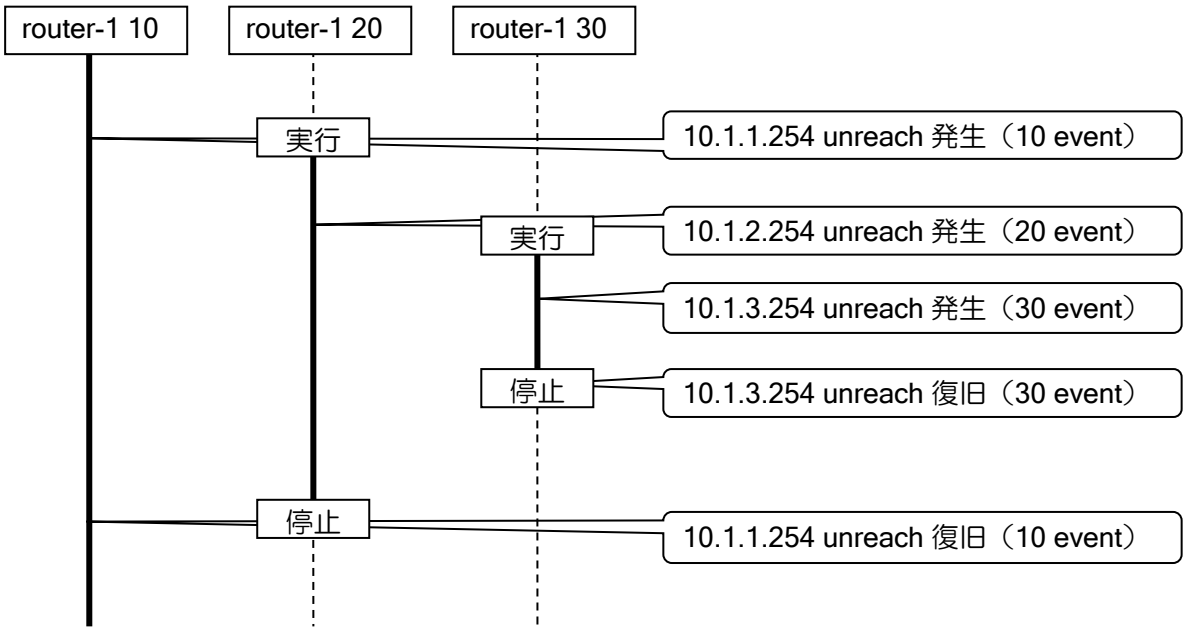
2.28.5.3 複数の watch グループの連動

シーケンス番号の設定により、複数の watch グループを 1 つの watch グループとして管理することができます。

watch グループを開始した時は、最も低いシーケンス番号の watch グループが実行され、この watch グループのイベントが発生すると、次のシーケンス番号の watch グループが実行されます。通常は、その watch グループのイベントが復旧すると watch グループは停止します。しかし、1 つの watch グループの中で、複数の watch グループを実行している時に、低いシーケンス番号の watch グループが復旧した場合は、そのシーケンス番号より大きいシーケンス番号の watch グループは、全て停止します。watch グループ停止の際、実行していた action は全て復旧します（action を復旧しない設定の場合を除く）。

1 つの watch グループ内に同じシーケンス番号の watch グループを設定することはできません。

シーケンス番号省略時は、登録順に空いている番号が使用されます。



【設定例】

```
watch-group router-1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.31.0/24
watch-group router-1 20
   event 10 ip unreach-host 10.1.2.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.32.0/24
watch-group router-1 30
   event 10 ip unreach-host 10.1.3.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.33.0/24

network-monitor router-1 enable
```

2.28.6 その他の動作モード

以下のモードは、ネットワークモニタの最大プロファイル数に近い値で使用する場合に、負荷の軽減のために使用してください。特に問題が無い場合は、通常のホスト監視モードで使用してください。

2.28.6.1 パッシブモード

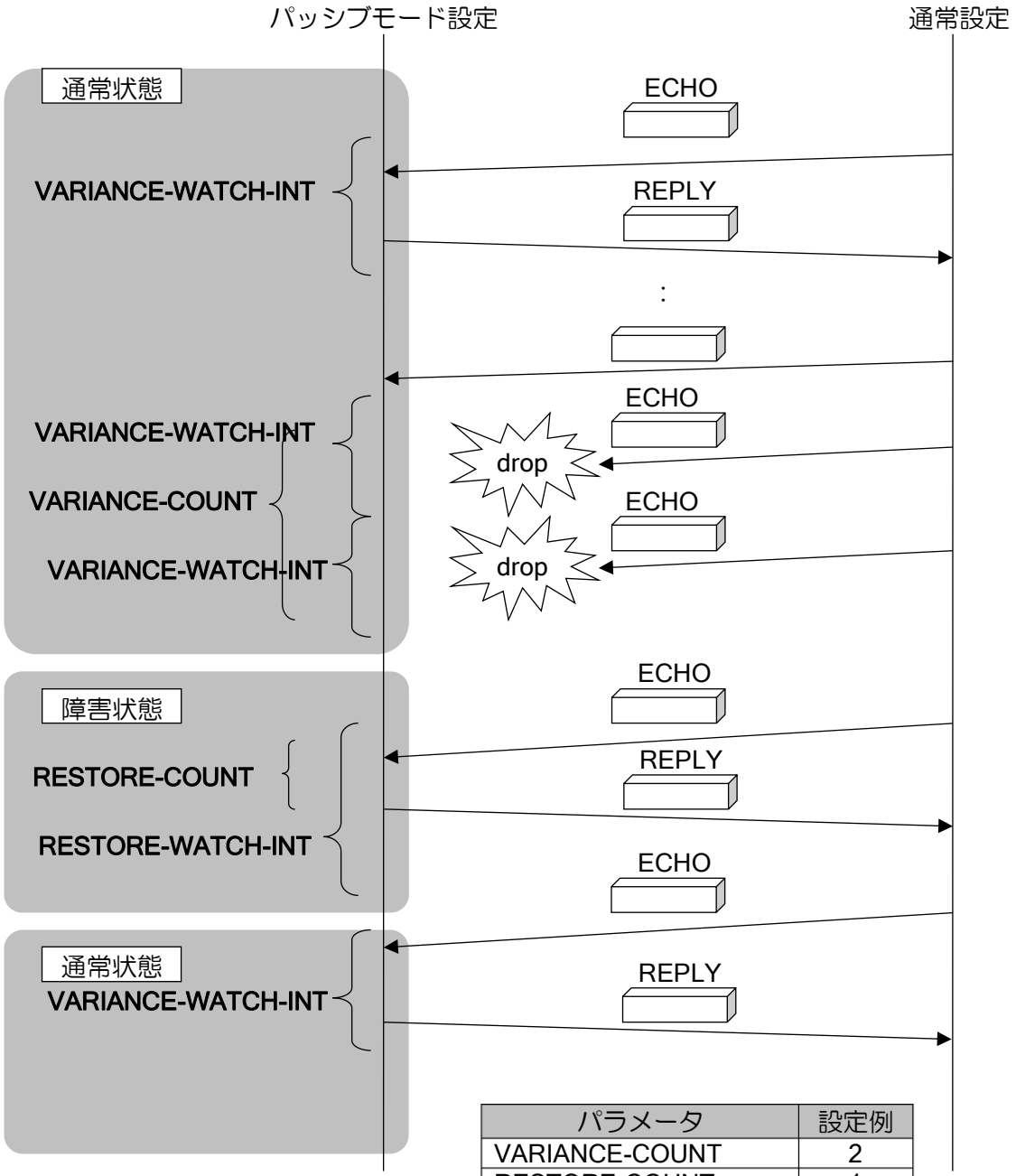
パッシブモードでは、相手からの ICMP ECHO パケットの監視を行います。通常の ICMP ECHO を送信する間隔で、相手装置から ICMP ECHO が届いているかの監視を行い、パケットが届いている場合は通信可能と判断します。最初に相手からパケットを受信するまでは、ready 状態となり、障害状態にはなりません。パッシブモードを設定した場合、自装置からは、ICMP ECHO の送信は行いません。

パッシブモードの設定を行う場合、相手装置では通常のホスト監視を設定する必要があります。また、お互いの装置で以下の設定を一致させる必要があります。

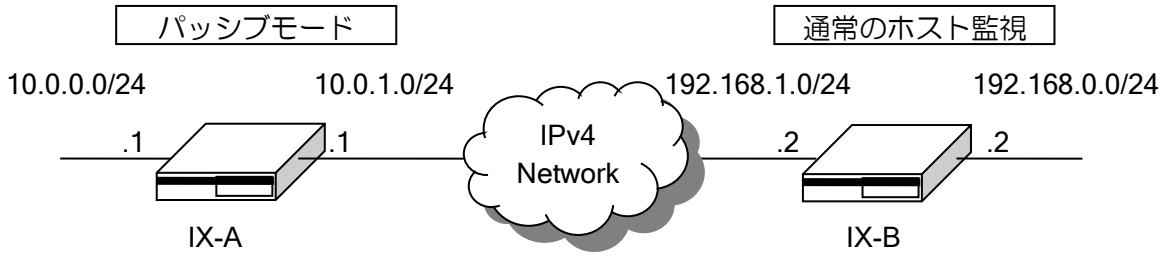
- 片方の監視先アドレスと、もう一方のソースアドレス
- 障害監視の間隔（VARIANCE-WATCH-INT,RESTORE-WATCH-INT）

パッシブモードの場合、送信間隔の間にパケットが到達すると通信可能と判断します。そのため、相手装置での応答タイムアウト時間（WAIT-TIME）が短い場合、遅延が発生すると相手装置では障害状態となりますが、パッシブモード設定側は正常のままとなり、対向で状態が不一致となる可能性があります。RTT 監視など、応答タイムアウト時間を短くする場合はご注意ください。

パッシブモードの場合の動作例



パラメータ	設定例
VARIANCE-COUNT	2
RESTORE-COUNT	1
VARIANCE-WATCH-INT	5
RESTORE-WATCH-INT	10



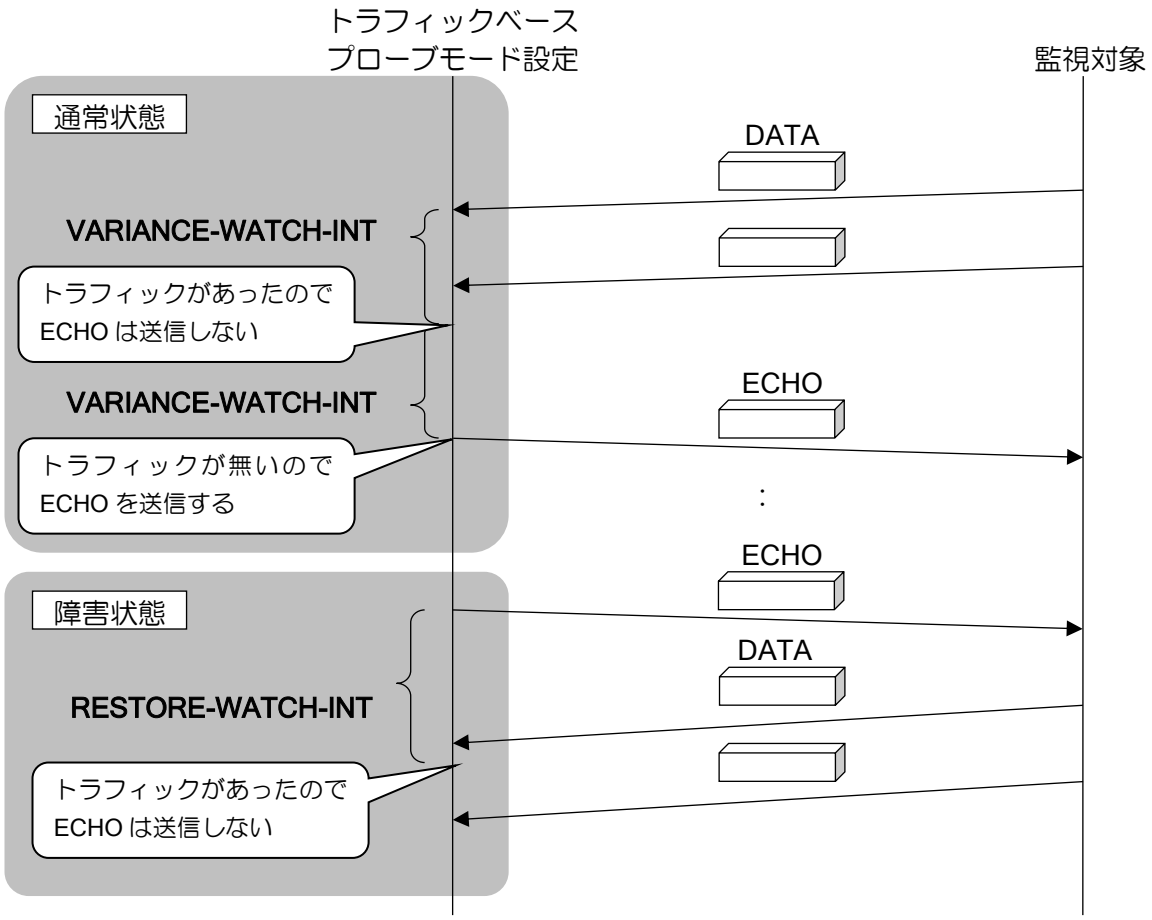
【設定例】

```
[IX-A の設定（パッシブモード）]
ip route 192.168.0.0/24 10.0.1.254
ip route 192.168.0.2/32 10.0.1.254
ip route default 10.0.0.254
!
watch-group passive-watch 10
   event 10 ip unreach-host 192.168.0.2 GigaEthernet1.0 10.0.1.254
                                                    source GigaEthernet0.0
   probe-mode passive event 10
   action 10 ip shutdown-route 192.168.0.0/24 10.0.1.254
   probe-counter variance 1
   probe-timer restorer 10
!
network-monitor passive-watch enable
!
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.0.1.1/24
   no shutdown

[IX-B の設定（通常のホスト監視）]
ip route 10.0.0.0/24 192.168.1.254
ip route 10.0.0.1/32 192.168.1.254
ip route default 192.168.0.254
!
watch-group host-watch 10
   event 10 ip unreach-host 10.0.0.1 GigaEthernet1.0 192.168.1.254
                                          source GigaEthernet0.0
   action 10 ip shutdown-route 10.0.0.0/24 192.168.1.254
   probe-counter variance 1
   probe-timer restorer 10
!
network-monitor host-watch enable
!
interface GigaEthernet0.0
   ip address 192.168.0.2/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.1.2/24
   no shutdown
```

2.28.6.2 トラフィックベースプローブモード

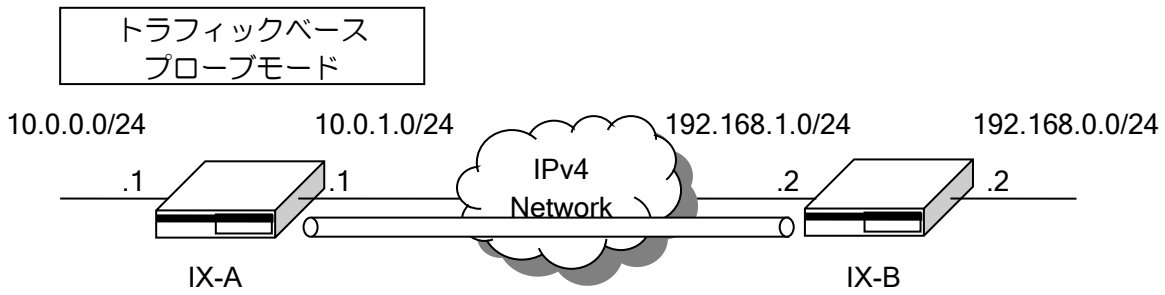
トラフィックベースプローブモードでは、ICMP ECHO を送信する周期で、ICMP ECHO を送信インタフェースからデータを受信している場合は、インタフェースの到達性があると判断し、ICMP ECHO の送信を行いません。ICMP ECHO/ECHO REPLY はデータ受信確認の対象外となります。これらのパケットのみ受信している場合は、データを受信していないと判断し、ICMP ECHO の送信を行います。データ受信の有無は統計情報から判断するため、ICMP ECHO を送信するインタフェースがポイントツーポイント（トンネル，PPP 等）以外の場合、受信の統計からはどの装置から受信したデータか判断できません。従って、トラフィックベースプローブモードは、ポイントツーポイントインタフェースの場合のみ有効です。

トラフィックベースプローブモードの場合の動作例



トラフィックベースプローブモードの場合、次のような構成で、IX-A から IX-B を監視し、IX-A 側から 192.168.0.0/24 へのトラフィックが定常的に発生している場合、192.168.0.2 のインタフェースが down しても、destination unreachable が IX-B からトンネルインタフェース経由で送信されるため、IX-A のネットワークモニタでは障害を検出できません。

トラフィックベースプローブモードは、ポイントツーポイント区間の障害の監視の場合のみ、使用してください。



【設定例】

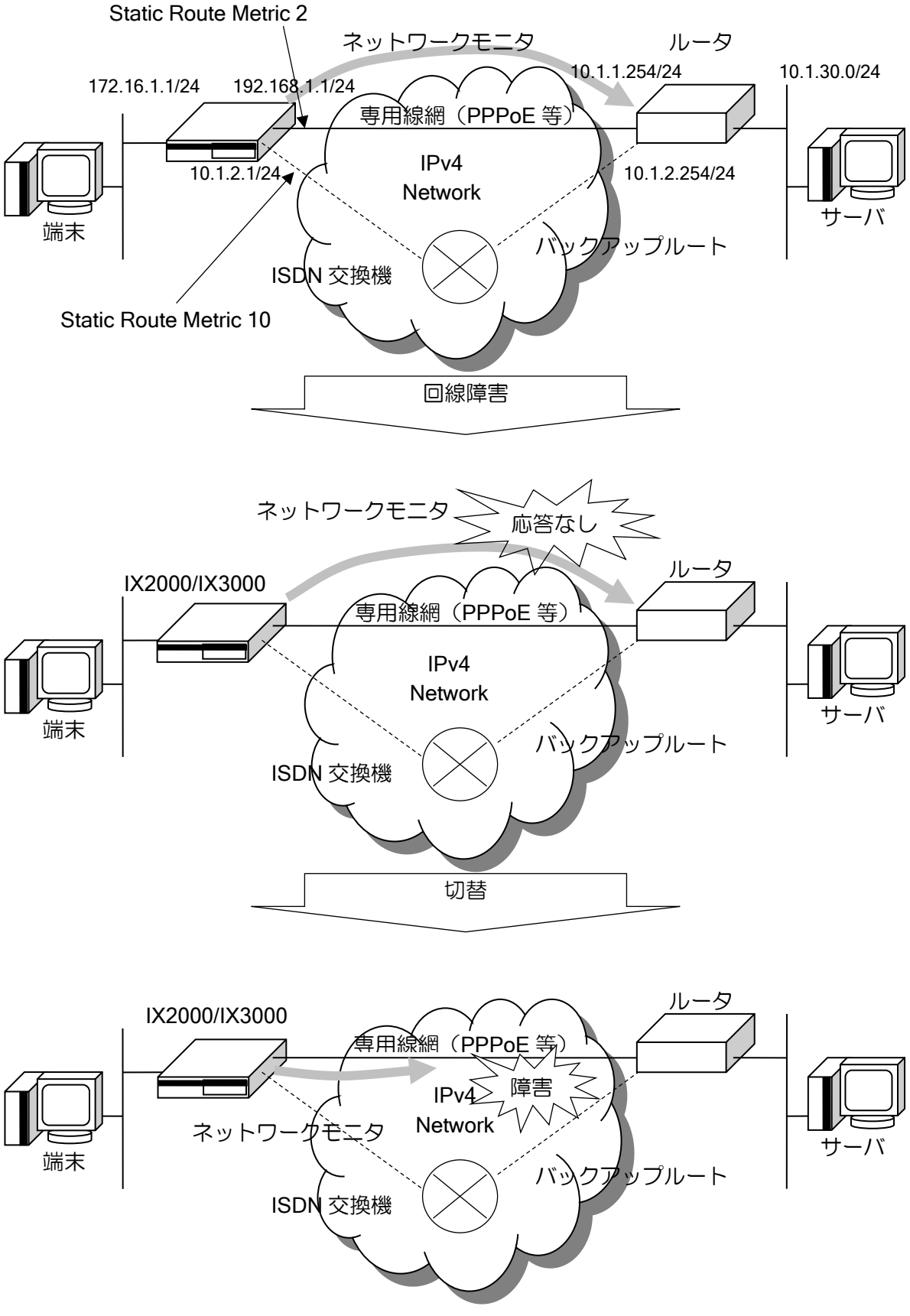
[IX-A の設定例]

```
ip route default Tunnel0.0
ip route default 10.0.0.254 metric 100
ip route 192.168.1.2/32 10.0.1.254
!
watch-group traffic-watch 10
   event 10 ip unreach-host 192.168.0.2 Tunnel0.0
   probe-mode traffic event 10
   action 10 ip shutdown-route 0.0.0.0/0 Tunnel0.0
   probe-counter variance 1
   probe-timer restorer 10
!
network-monitor traffic-watch enable
!
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.0.1.1/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode 4-over-4
   tunnel destination 192.168.1.2
   tunnel source 10.0.1.1
   ip unnumbered GigaEthernet0.0
   no shutdown
```

2.28.7 使用例

2.28.7.1 ISDN とネットワークモニタ機能の組み合わせ

(a) 専用線のバックアップ 1



ネットワークモニタにより専用線の監視を行います。障害発生時は専用線へのルートを隠蔽することにより、ルートが ISDN 側へ切替わります。専用線復旧時は隠蔽したルートが復旧しますので、専用線に切戻ります。

【設定例】

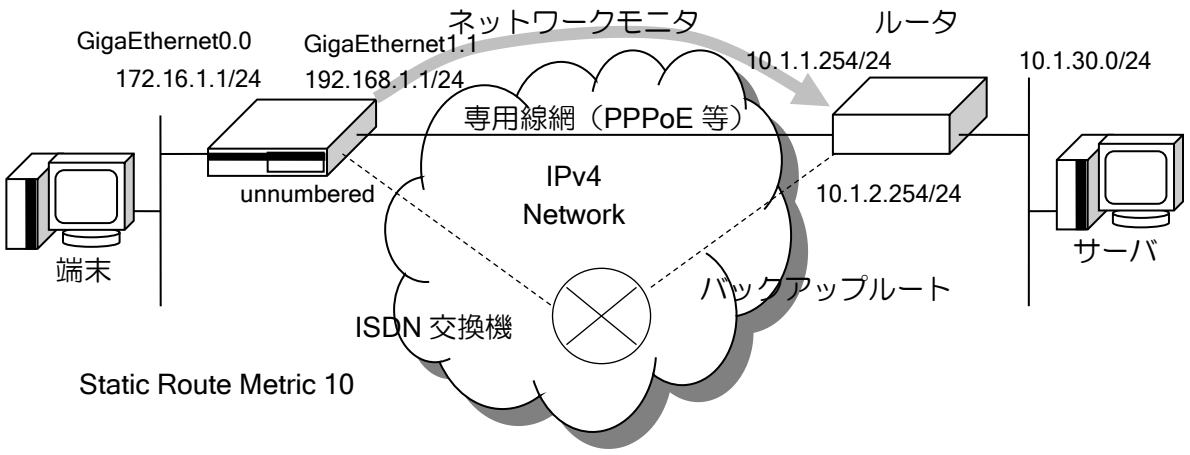
```
ip route 10.1.30.0/24 GigaEthernet1.1 metric 2
ip route default BRI1/0.0 metric 10
watch-group router-1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet1.1
   action 10 ip shutdown-route 10.1.30.0/24 GigaEthernet1.1
network-monitor router-1 enable
ppp profile pro-1
   authentication myname ix
   authentication password ix ix
   authentication password prouter prouter
device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567
interface GigaEthernet1.1
   encapsulation pppoe
   auto-connect
   ip address 192.168.1.1/24
   no shutdown
interface BRI1/0.0
   dialer string 81-123-4568
   no auto-connect
   ppp binding pro-1
   ip address 10.1.2.1/24
   no shutdown
```

※Dialer／BRI インタフェースのアドレス設定について

ネットワークモニタを利用して ISDN の迂回を行う場合、Dialer／BRI インタフェースのアドレスは、unnumbered を使用せず、実際のアドレスを使用してください。

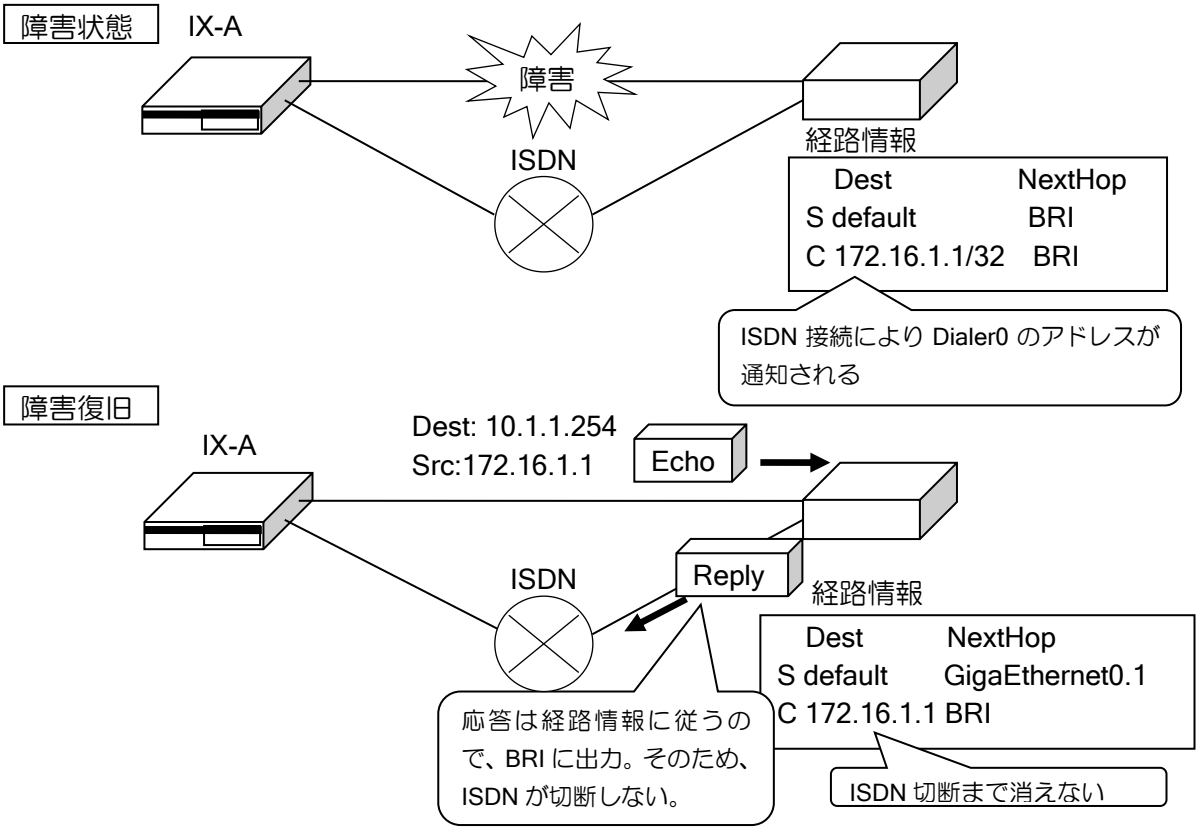
IX2000/IX3000 シリーズでは、デフォルトで PPP の IP アドレス送信が有効になっているため、Dialer／BRI インタフェースに unnumbered を使用した場合、意図しない経路が相手側で作成され、ネットワークモニタの誤動作や、ISDN が切断しないなどの動作となる場合があります。unnumbered を設定する場合は、PPP の IP アドレス送信機能を無効（ppp profile で no ipcp send-ip-address を設定）にするか、ネットワークモニタの動作とは関係の無いインタフェースを使用してください。

以下に、ISDN が切断しない場合の例を示します。



【設定例】

```
ip route 10.1.30.0/24 GigaEthernet1.1 metric 2
ip route default Dialer0 metric 10
watch-group router-1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet1.1 source GigaEthernet0.0
   action 10 ip shutdown-route 10.1.30.0/24 GigaEthernet1.1
network-monitor router-1 enable
ppp profile pro-1
   authentication myname ix
   authentication password ix ix
   authentication password prouter prouter
device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567
interface GigaEthernet0.0
   ip address 172.16.1.1/24
   no shutdown
interface GigaEthernet1.1
   encapsulation pppoe
   auto-connect
   ip address 192.168.1.1/24
   no shutdown
interface Dialer0
   dialer string 81-123-4568
   no auto-connect
   ppp binding pro-1
   ip unnumbered GigaEthernet0.0
   no shutdown
```



(b) 専用線のバックアップ 2

専用線のバックアップ 1 の例では、専用線復旧時に隠蔽したルートが復活し、専用線にルートが切戻ります。

アクションを復活させない設定を行うことができます。この機能を使用して、専用線復旧時、ルートを専用線に戻さないようにすることができます。

- 専用線復旧時に専用線にルートを戻さない設定

```
【設定例】

ip route 10.1.30.0/24 GigaEthernet1.1 metric 2
ip route default BRI1/0.0 metric 10
watch-group router-1 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet1.1
   action 10 ip shutdown-route 10.1.30.0/24 GigaEthernet1.1 suppress-restoration
network-monitor router-1 enable
ppp profile pro-1
   authentication myname ix
   authentication password ix ix
   authentication password prouter prouter
device BRI1/0
   isdn switch-type ins64
   isdn answer1 81-123-4567
interface GigaEthernet1.1
   encapsulation pppoe
   auto-connect
   ip address 192.168.1.1/24
   no shutdown
interface BRI1/0.0
   dialer string 81-123-4568
   no auto-connect
```

```
ppp binding pro-1
ip address 10.1.2.1/24
idle-time 30
no shutdown
```

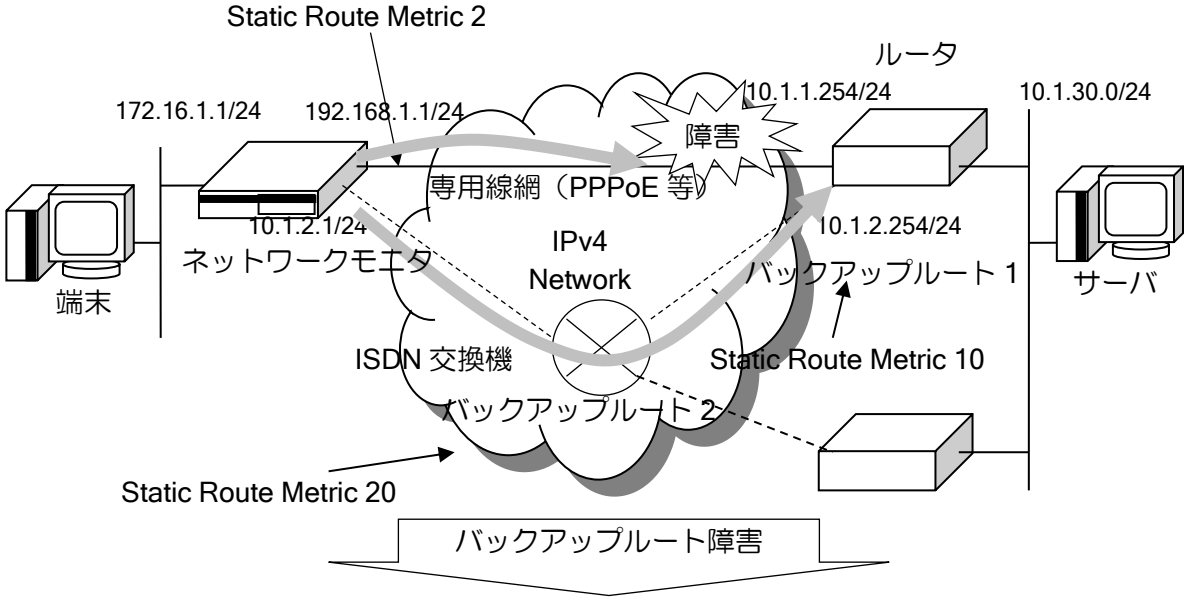
専用線に切戻す場合は、以下のコマンドを実行してください。無通信切断の設定を行っている場合は、ISDN 切断を実行しない場合でも、無通信切断時間経過後、ISDN は自動で切断します。

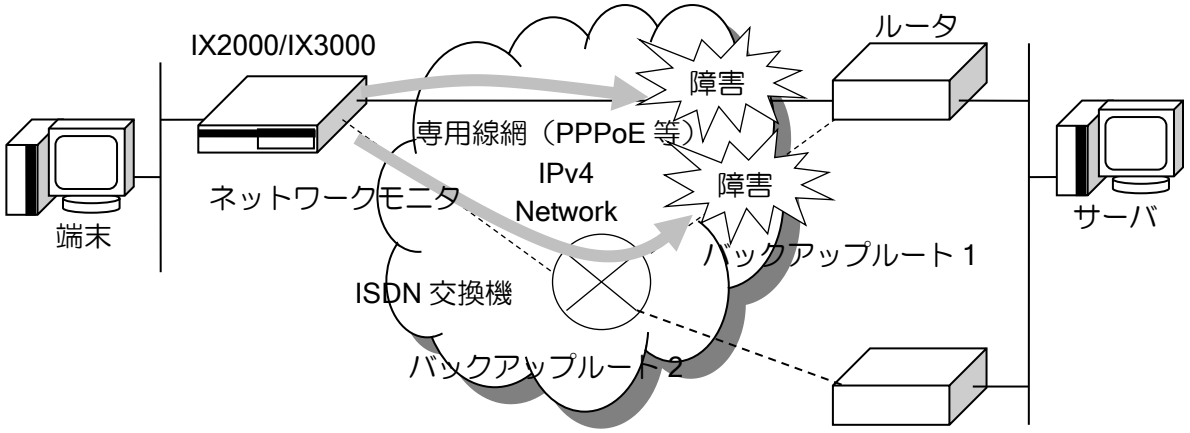
- 専用線にルートを戻す場合のコマンド実行例

```
【実行例】

Router(config)# clear watch-group session router-1
Router(config)# clear interface BRI1/0.0
```

(c) 複数対地設定時のインタフェース変更

ISDN の複数対地をサポートしています。ネットワークモニタと複数対地の設定を使用して、1 つの対地への接続が失敗，切断した場合に、次の接続先へ迂回することができます。





【設定例】

```
ip route 10.1.30.0/24 GigaEthernet1.1 metric 2
ip route default Dialer1 metric 10
ip route default Dialer2 metric 20
!
watch-group isdn 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet1.1
   action 10 ip shutdown-route 10.1.30.0/24 GigaEthernet1.1
!
watch-group isdn 20
   event 10 ip unreach-host 10.1.2.254 Dialer1
   action 20 ip shutdown-route 0.0.0.0/0 Dialer1
!
network-monitor isdn enable
!
ppp profile backup1
   authentication myname ix
   authentication password ix ix
   authentication password prouter prouter
!
ppp profile backup2
   authentication myname ix
   authentication password ix ix
   authentication password prouter2 prouter2
!
device BRI1/0
   isdn switch-type ins64
   isdn answer1 111-1111
!
interface Dialer1
   dialer string 222-2222
   no auto-connect
   ppp binding backup1
   idle-time 60
   no shutdown
!
interface Dialer2
   dialer string 333-3333
   no auto-connect
   ppp binding backup2
   idle-time 60
   no shutdown
```

上記の設定例では、バックアップルート 1（Dialer1）が復旧すると、再度バックアップルート 1 へ迂回します。また、専用線が復旧した場合は、バックアップ 1,2 どちらに迂回していても専用線に切戻ります。

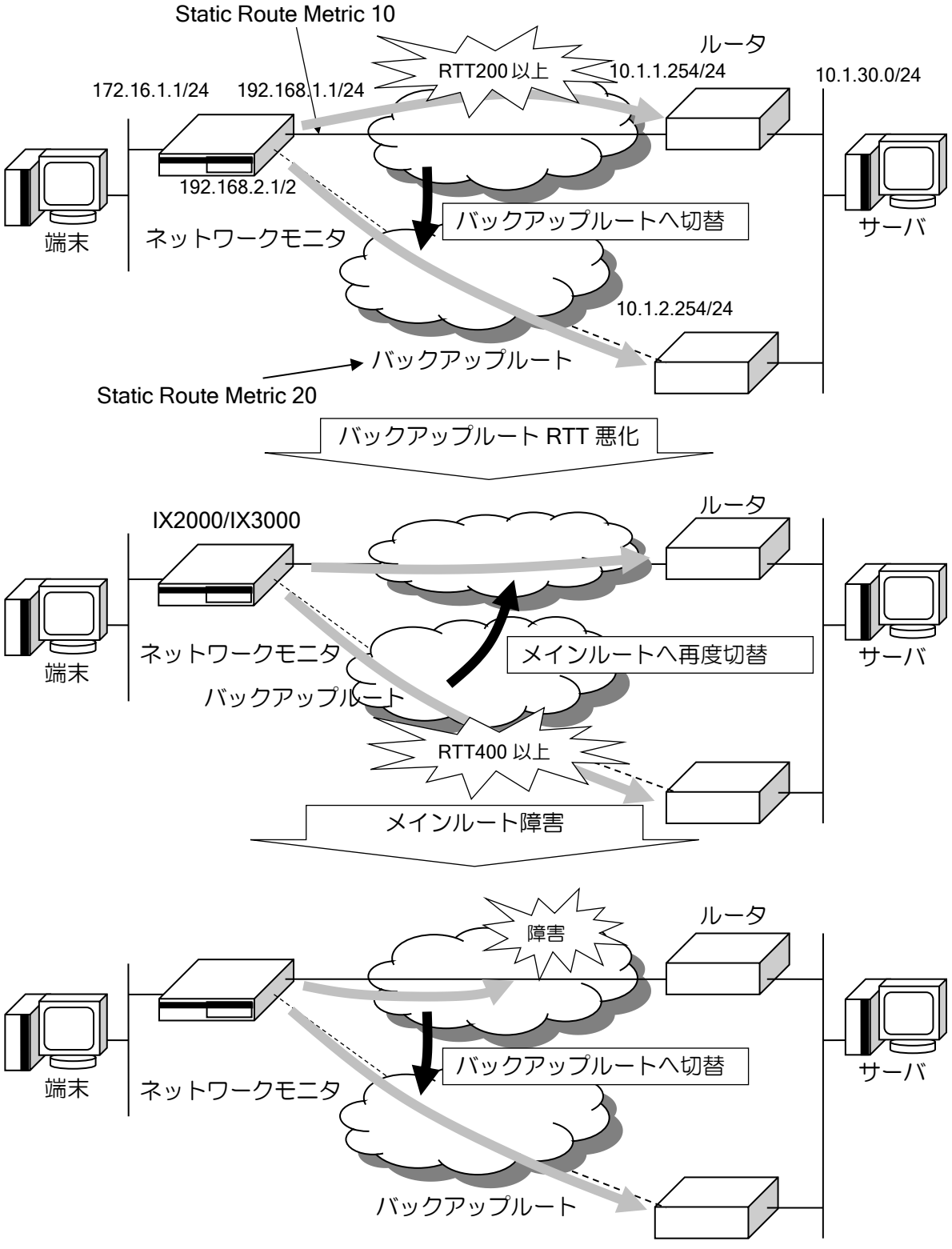
ISDN 回線でネットワークモニタを使用する場合、以下の点で注意が必要です。

- ✧ 監視用の ICMP ECHO パケットが ISDN 発呼の契機になります。

2.28.7.2 RTT（Round Trip Time）監視の例

Ver.8.5 以降、msec 単位の監視が行えます。これを利用して RTT を監視することができます。
以下のような RTT 監視を考えます。

（1）通常はメインルートを利用
（2）メインルートの RTT が 200msec 以上となった場合は、バックアップルートを利用
（3）メインルートの RTT が 200msec 以上かつ、バックアップルートの RTT が 400msec 以上となった場合、再度、メインルートを利用
（4）メインルートの応答が無い場合は、バックアップルートを利用



【設定例】

```
ip route 10.1.30.0/24 192.168.1.254 metric 10
ip route 10.1.30.0/24 192.168.2.254 metric 20
!
watch-group watch_main 10
   event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
   probe-timer wait msec 200
! メインルートの RTT 監視
!
watch-group watch_main 20
   event 10 ip unreach-host 10.1.1.254 GigaEthernet0.0 192.168.1.254
   action 10 ip shutdown-route 10.1.30.0/24 192.168.1.254
! メインルートの応答が 200msec 以上になると起動
! 2sec 応答が来ない場合（通信不可と判断）、メインルートの経路を削除
! 条件（4）用

network-monitor watch_main enable
!
watch-group watch_backup 10
   event 10 sub 10 ip reach-host 10.1.2.254 GigaEthernet1.0 192.168.2.254
   event 10 sub 20 watch-group-status watch_main 10 stand
   action 10 ip shutdown-route 10.1.30.0/24 192.168.1.254
   probe-timer wait msec 400
! バックアップルートの応答が 400msec 以内で、かつ、
! メインルートの応答が 200msec 以上の場合にメインルートを削除
! バックアップルートの応答が 400msec 以上になると、event 10 sub 10 の監視が
! 正常となるため、メインルートが復旧
! 条件（2），（3）用

network-monitor watch_backup enable
!
interface GigaEthernet0.0
   ip address 192.168.1.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.2.1/24
   no shutdown
```

2.28.8 ネットワークモニタ機能の注意事項

ネットワークモニタ機能には、いくつかの注意事項があります。

(a) 同一リンクにないターゲット監視（イーサネットの場合のみ）

同一リンクにないターゲット（ホスト）を監視するには、next-hop 指定を必ず使用してください。

(b) ネスティング

watch グループの action で watch グループを起動するようなネスティングは無限呼び出しとなる場合があります。この場合、正常には動作しなくなりますので、設定には十分注意してください。

(c) ホスト監視での 100 対地以上の使用

ホスト監視の場合、ICMP ECHO_REQUEST を送信するため、対地数が増えるとシステムの負荷が上昇します。これを避けるため、対地数が 100 を超える場合は、送信間隔を長めに設定してください。

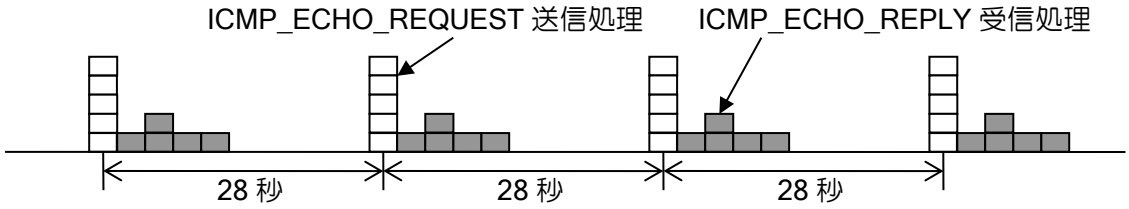
また、送信間隔が同じ対地へは、一定間隔を空けて ICMP ECHO_REQUEST を送信しているため、送信時のシステムの負荷は軽減していますが、対地数が多い場合は送信時のシステムの負荷は一時的に上昇します。

これを避けるために、対地数が 100 を超える場合は、100 対地ごとに送信間隔を 1,2 秒程度ずらすなどにより、負荷分散してください。

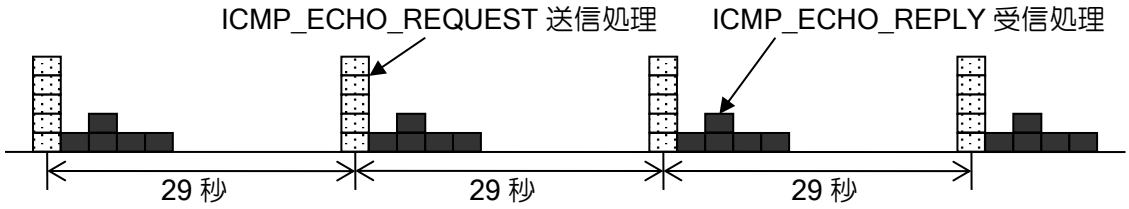
送信間隔については、以下の値を推奨します。
なお、Ver8.5 以降は自動で 10 秒のランダムディレイを行うため、この対処は不要です。

- 対地数 128：送信間隔　平均 8 秒
- 対地数 256：送信間隔　平均 10 秒
  1～100 対地目　：　9 秒
  101～200 対地目：　10 秒
  201～256 対地目：　11 秒
- 対地数 512：送信間隔　平均 15 秒
  1～100 対地目　：　13 秒
  101～200 対地目：　14 秒
  201～300 対地目：　15 秒
  301～400 対地目：　16 秒
  401～512 対地目：　17 秒

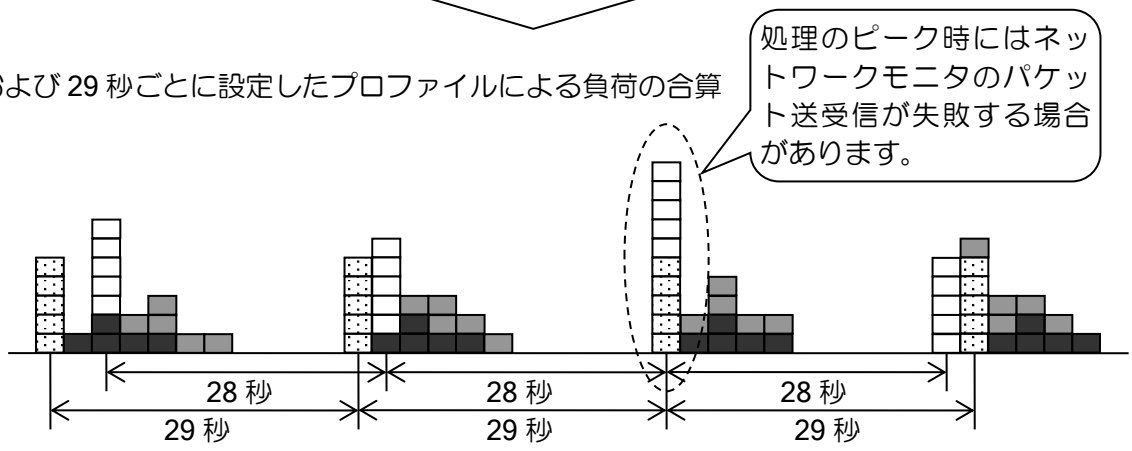
28 秒ごとに設定したプロファイルによる負荷例



29 秒ごとに設定したプロファイルによる負荷例



28 および 29 秒ごとに設定したプロファイルによる負荷の合算



(d) msec 指定の場合の対地数

Ver.8.5 以降、監視周期を msec 単位に指定可能となっています。ただし、msec 指定は装置に負荷がかかるため、1 秒以下に設定する場合は、対地数は 10 以下を推奨します。

■2.29 スケジューラ機能の設定

2.29.1 スケジューラ機能

スケジューラ機能は、指定した時刻または指定した時間間隔で、事前に設定しておいたコマンド群を自動的に実行する機能です（Ver8.8 以降サポート）。コンフィグモードで投入可能なコマンドほぼ全てに対応しており、設定の変更やログの取得などが行えます（ログはイベントログとして取得します）。

2.29.2 スケジューラ機能の設定

2.29.2.1 スケジューラ機能の基本設定

スケジューラ機能は、次のコマンドで設定します。

command-action list	コマンドリストの設定 （Ver.9.3 以降）
scheduler list	スケジューラアクションリストの設定 （Ver.9.2 以前）
command	実行コマンドの設定
scheduler timetable	実行日時・間隔の設定

まず、command-action list（Ver.9.3 以降）／scheduler list（Ver.9.2 以前） コマンドでアクションリストコンフィグモードに遷移し、実行したいコマンドを実行順に command で設定します。通常のコンフィグと異なりコマンドの補完機能は働きませんので、誤入力に気をつけてください。

また、コマンドは常にグローバルコンフィグモードから開始されます。各種モード遷移のコマンドも投入可能です。

次に scheduler timetable コマンドで実行日時や実行間隔を設定すると、指定したスケジュールでコマンドリストのコマンドが連続実行されます。timetable コマンドは複数設定可能です。timetable コマンドの詳細な設定方法は、次の項目で詳しく説明します。

【設定例】
Ver.9.3 以降

```
scheduler timetable cmdlist1 datetime 18 00 fri
command-action list cmdlist1
   command 1 device GigaEthernet2
   command 2 port 1 shutdown
```

Ver9.2 以前

```
scheduler timetable cmdlist1 datetime 18 00 fri
scheduler list cmdlist1
   command 1 device GigaEthernet2
   command 2 port 1 shutdown
```

また、以下のコマンドで即時実行および動作確認をすることができます。

scheduler execute command-action execute （Ver.9.3 以降）	即時実行
show scheduler timetable	実行スケジュールの表示

スケジューラによるコマンド実行時にコンフィグモードで作業しているユーザがいる場合、ユーザ側の動作に影響があります（詳細は注意事項を参照してください）。

2.29.2.2 スケジューラ機能のタイムテーブル設定（時間間隔設定）

スケジューラ機能のタイムテーブルの設定は、時間間隔の指定と、日時の指定の 2 つの方法があります。時間間隔指定する場合の設定方法は次のとおりです。

【設定例 1】1 時間間隔でコマンドを実行

```
scheduler timetable cmdlist1 interval hour 1
```

【設定例 2】10 分間隔でコマンドを実行

```
scheduler timetable cmdlist1 interval minute 10
```

2.29.2.3 スケジューラ機能のタイムテーブル設定（時刻設定）

スケジューラ機能のタイムテーブルを時刻指定する場合の設定方法です。

年月日や曜日、時分などで設定し、省略または * で設定された項目は全ての条件が合致します。範囲指定はありませんが、複数の設定が投入可能です。

【設定例 1】毎月 1 日の AM8:30 にコマンドを実行

```
scheduler timetable cmdlist1 datetime 8 30 1
```

【設定例 2】毎時 30 分にコマンドを実行

```
scheduler timetable cmdlist2 datetime * 30
```

【設定例 3】指定した日時に 1 度だけ実行（2012 年 1 月 1 日 0:00）

```
scheduler timetable cmdlist3 datetime 0 0 1 1 2012
```

【設定例 4】月曜から金曜までの AM8:00 にコマンドを実行

```
scheduler timetable cmdlist4 datetime 8 0 mon
scheduler timetable cmdlist4 datetime 8 0 tue
scheduler timetable cmdlist4 datetime 8 0 wed
scheduler timetable cmdlist4 datetime 8 0 thu
scheduler timetable cmdlist4 datetime 8 0 fri
```

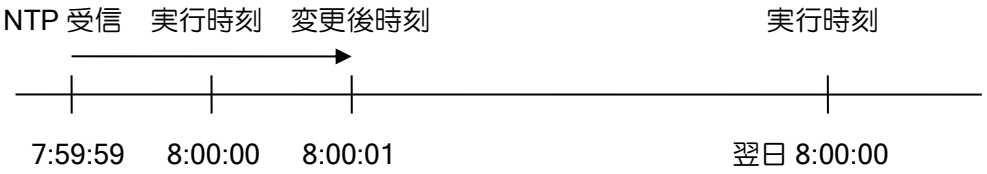
2.29.3 スケジューラ機能の時刻指定と NTP による時刻変更

NTP や clock コマンドにより、スケジューラ機能が動作する直前に実行時刻を過ぎてしまうことや、動作した直後に時刻が戻ってしまうことがあります。

大きく時刻を変更した場合には単純にスケジュールを再計算しますが、内部時計とのズレやうるう秒などによって短時間の時刻補正が行われた場合には、その補正の影響を受けないように動作します。

時刻変更の詳細な動作仕様を毎朝 8:00 にコマンドを実行する例で説明します。

コマンド実行直前で時刻が進む場合

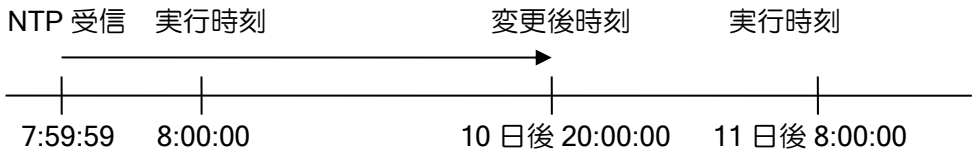


コマンド実行直前に時刻が進んだ場合（3 分以内）、その間のコマンドを全て実行します。時刻が補正されなかった場合と同じように動作します。

コマンド実行直後に時刻が戻る場合

コマンド実行直後に時刻が戻った場合（3 分以内）、スケジュールは再計算しません。次に実行されるのは時刻が戻る前に予定していた翌日の 8:00:00 です。時刻が補正されなかった場合と同じように動作します。

大きく時刻を変更した場合



3 分以上の時刻変更を行った場合は時刻補正ではないと判断し、進む場合も戻る場合も、その間のコマンドは実行せず、常にスケジュールを再計算します。

これらにより、時刻補正とコマンド実行タイミングが重なっても、その影響は受けません。
なお、スケジュールを時間間隔で指定している場合は、NTP などによる時刻補正の影響は受けません。経過時間で判定するためです。

2.29.4 コマンドリストの一時停止

コンフィグモードで作業する必要がある場合、スケジューラ等によるコマンド実行を一時的に停止させることができます。オペレーションモードで以下のコマンドを実行してください。なお、コマンド実行を抑制するだけで、時間間隔指定の測定時間などスケジュール動作は継続します。

scheduler suspend	スケジューラー時停止
scheduler resume	スケジューラー時停止解除
command-action stop	コマンドリストー時停止（Ver.9.3 以降）
command-action start	コマンドリストー時停止解除（Ver.9.3 以降）

一時停止機能は再開忘れ防止のため、停止時間を入力して利用してください。

【設定例】一時停止の解除を忘れても 10 分後にスケジューラを再開します。

scheduler suspend 10

2.29.5 コンフィグモードで作業中の場合のスケジューラ機能の影響

スケジューラ機能はコマンド実行をコンフィグモードを占有して行うため、指定時刻にコンフィグモードで作業しているユーザは、以下のような影響を受けます。大きな作業を行う場合は、できるだけ影響のない時間帯に作業するか、一時停止して作業するようにしてください。

- グローバルコンフィグモード以外のコンフィグモードにいる場合は、グローバルコンフィグモードに強制的に遷移します。
- コマンド入力中の場合は、入力内容が破棄されます。
- show コマンド表示中や Ping コマンド実行中など、コマンド実行中の場合はキャンセルされます。
- スケジューラ機能のコマンド投入が全て完了するまでコマンドは受け付けられません。ctrl + Z でコンフィグモードから抜けることは可能です。

2.29.6 スケジューラ機能・コマンドリストの注意事項

- 同じコマンドリストを同一時刻に複数実行するように設定しても 1 度しか動作しません。
  1 つのコマンドリストに「毎月 1 日 8:00 に実行」「月曜 8:00 に実行」の 2 つが設定されていた場合、月の初日が月曜でもそれ以外でも 8:00 には 1 度しか起動されません。時間指定と時刻指定が重なったときも同様です。

- ゼロコンフィグ利用環境では、スケジューラ機能は利用できません。

- command で指定するコマンドは省略せずに設定してください。
  省略して登録することは可能ですが、現時点で一意に決定できる省略形でもバージョンアップによりコマンドや入力パラメータが追加されると、選択肢が増えて補完できなくなる可能性があるためです。一時的に利用する設定では省略して登録しても問題ありません。

- コマンドリストで実行不可能なコマンド
  以下のコマンドはコマンドリストでは実行できません。
  - scheduler suspend, scheduler resume
  - event-terminal, show logging
  - password
  - pki
  - 対話形式で yes/no やパスワードなどの入力を求められるコマンド（以下は除く）
    - reload
    - software-update（パラメータに”no-interactive”を指定した場合）
    - erase default-config（コマンドの後ろに”yes”を指定した場合）
    - erase startup-config（コマンドの後ろに”yes”を指定した場合）

■2.30 パケットフィルタの設定

パケットフィルタ（トラフィックフィルタ）は、インタフェースの入口あるいは出口で、パケット単位にフィルタリングを実行します。

以下にパケットフィルタ登録のための設定および基本的な動作を説明します。

Ver.2 以降では、通常の条件固定のスタティックフィルタの他に、パケットに応じて動的にアクセスを許可するダイナミックフィルタを設定することも可能です。

Ver10.4 以降、UTM サーバおよび NetMeister サーバ宛の通信はスタティックフィルタおよびダイナミックフィルタでフィルタリングされません。

2.30.1 スタティックフィルタ

スタティックフィルタは、インタフェースコンフィグモードで、ip filter/ipv6 filter コマンドを使用して設定します。1 つでもフィルタを登録した場合、そのインタフェースでは、パケット検索に一致しないパケットは自動的に廃棄する設定となります。

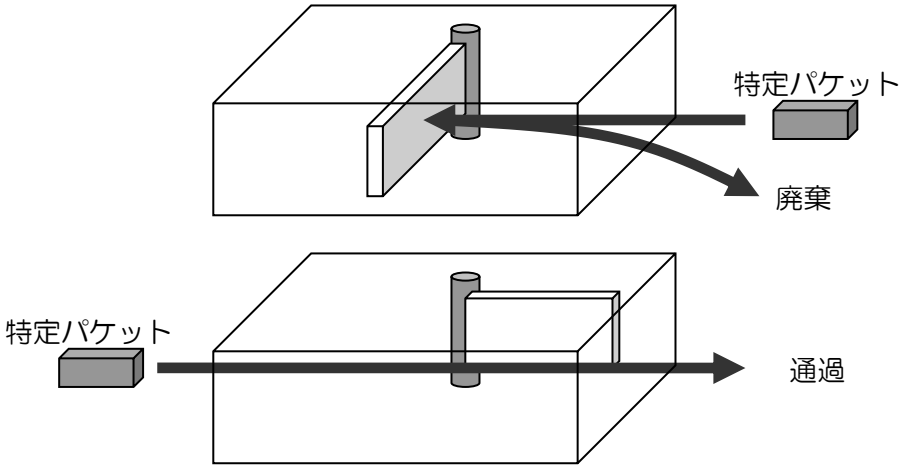
※スタティックフィルタは、UFS キャッシュを利用することにより、転送が高速化します。UFS キャッシュについては、UFS キャッシュの項目を参照してください。

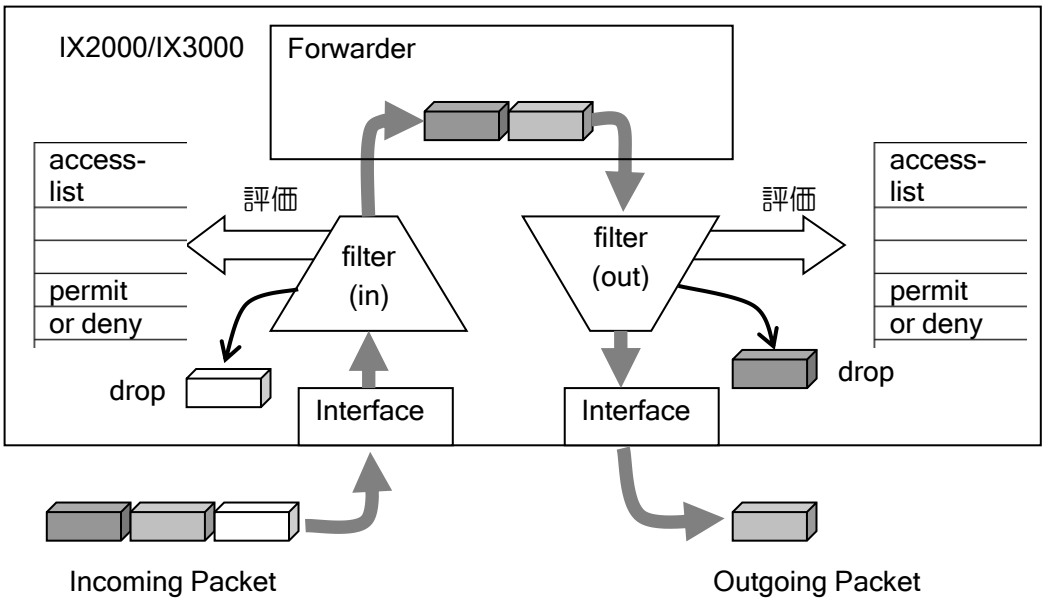
- 評価条件（アクセスリストと同一となります）
  - 送信元アドレス，プレフィックス指定
  - 送信先アドレス，プレフィックス指定
  - プロトコル指定
  - 送信元ポート指定（TCP、UDP、ICMP のみ）
  - 送信先ポート指定（TCP、UDP、ICMP のみ）
  - TCP ヘッダ制御フラグ
  - TOS/TRAFFIC-CLASS フィールド（PRECEDENCE/DSCP/TOS）
  - ICMP/ICMPv6 メッセージ

パケット評価順は、フィルタコマンドにて登録された優先順位に基づいて、それぞれのフィルタコマンドから参照されているアクセスリストの登録順通りにパケットを評価します。

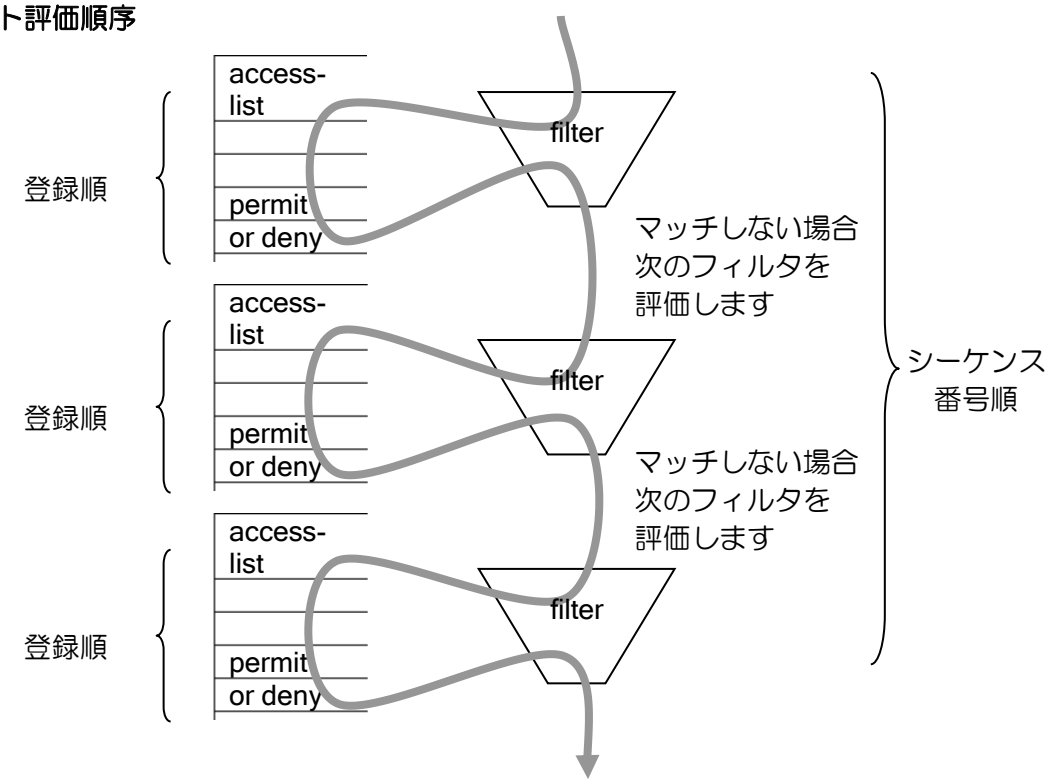
以下にスタティックフィルタの評価ポイントおよび評価ポイントにおける処理を示します。

スタティックフィルタ概念図





パケット評価順序



全てマッチしない場合、パケットは廃棄されます。

スタティックフィルタの設定は次のコマンドを使用します。
アクセスリストについては、アクセスリストの設定の節を参照してください。

ip filter	IPv4 パケットフィルタの使用を設定
ipv6 filter	IPv6 パケットフィルタの使用を設定
ip access-list	IPv4 パケットの評価ルールを設定
ipv6 access-list	IPv6 パケットの評価ルールを設定

【設定例】

IPv4 スタティックフィルタの場合

```
ip access-list access-1 permit ip src 192.168.0.0/24 dest any
interface GigaEthernet0.0
   ip address 10.0.0.1/8
   ip filter access-1 100 in
   no shutdown
```

IPv6 スタティックフィルタの場合

```
ipv6 access-list access-1 permit icmp neighbor-advertisement src any dest any
ipv6 access-list access-1 permit icmp neighbor-solicitation src any dest any
ipv6 access-list access-2 permit ip src 2001:db8:1::/64 dest any

interface GigaEthernet0.0
   ipv6 address 2001:db8:1::1/64
   ipv6 filter access-1 100 in
   ipv6 filter access-2 200 in
   no shutdown
```

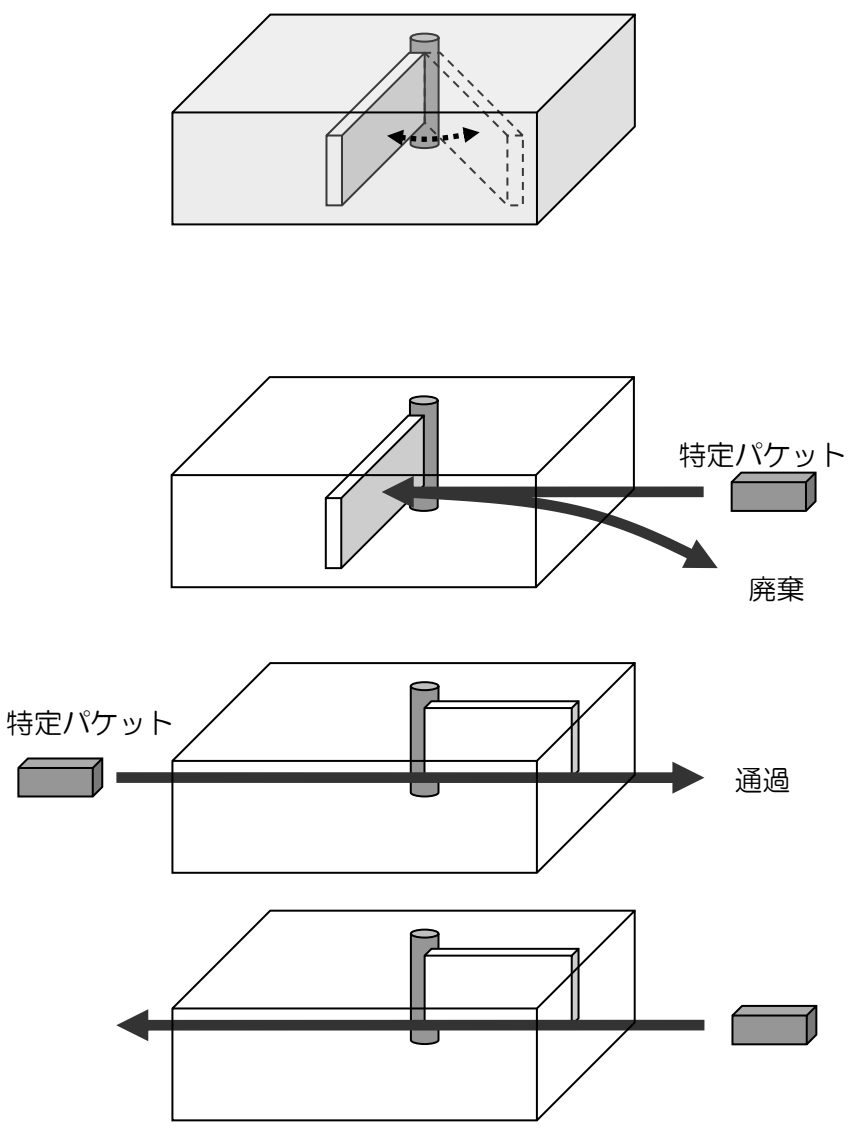
※IPv6 では、ICMPv6 を使い近隣探索（ルータの検索、アドレス解決、近隣不能検知、リダイレクトなど）が行われているため、あらかじめ NA と NS の通過フィルタを設定しておく必要があります。

2.30.2 ダイナミックフィルタ

ダイナミックフィルタとは、トリガとなるパケットを指定して、そのパケットがフィルタを通過する際に動的にフィルタを操作できるパケットフィルタです。

以下にダイナミックフィルタの処理を示します。

ダイナミックフィルタ概念図



ダイナミックフィルタの基本的な使い方は、内側からのパケットの通過をトリガとして、動的に外側からのフィルタに穴をあけることです。内側からのみセッションを確立できるようにすることもできるためセキュリティが向上します。

通常時はパケットフィルタで外側からのパケットを廃棄するように設定しておきます。

内側からパケットが通過した場合に、ダイナミックフィルタが動作し、一時的に外側からのパケットも通過できるようになります。

ダイナミックフィルタは 2 種類の設定方法があります。

1 つは HTTP や FTP など予約されているサービス名を指定して、内側からセッションを張った場合にのみ、これらのサービスを使用可能にする設定です。もう 1 つは、ダイナミックアクセスリストを使用して詳細に設定を行う方法です。

- 注意事項
  最後のフィルタがダイナミックフィルタで、全てのフィルタにマッチしない時パケットは廃棄されます。

設定コマンドは次のとおりです。ダイナミックフィルタの設定には、スタティックフィルタと同様に、ip filter/ipv6 filter コマンドを使用します。スタティックフィルタの利用時には、通常のアクセスリストを指定していましたが、ダイナミックフィルタの場合には、ダイナミックアクセスリストを指定します。

ip filter	IPv4 パケットフィルタの使用を設定
ipv6 filter	IPv6 パケットフィルタの使用を設定
ip access-list dynamic	IPv4 アドレスとダイナミックなルールを設定
ipv6 access-list dynamic	IPv6 アドレスとダイナミックなルールを設定
show ip filter dynamic	IPv4 ダイナミックフィルタの確認
show ipv6 filter dynamic	IPv6 ダイナミックフィルタの確認

2.30.2.1 サービス指定の場合のダイナミックフィルタ

HTTP や FTP など直接サービス名を指定して、内側からセッションを張った場合にのみ、これらのサービスを使用可能にする設定です。HTTP などの場合にはそのセッションのみ外部からのパケットを受け付けるようにし、FTP の場合にはデータコネクション用の通信も可能にします。

指定可能なサービスには、以下があります。これ以外のサービスを指定する場合には、下記項目のアクセスリストを利用したダイナミックフィルタを参照してください。

- HTTP
- FTP
- TFTP
- DNS
- telnet

内側のネットワークから FTP で外側ネットワークにアクセスしたときのみ外側から FTP に関連するフィルタに穴を開ける場合には、以下のような設定を行います。

【設定例】

IPv4 ダイナミックフィルタの場合

```
ip access-list access-1 deny ip src any dest any
ip access-list dynamic dynamic-1 ftp src 192.168.0.0/24 dest any
interface GigaEthernet1.0
   ip address 10.0.0.1/8
   ip filter dynamic-1 100 out
   ip filter access-1 200 in
   no shutdown
```

IPv6 ダイナミックフィルタの場合

```
ipv6 access-list access-1 permit icmp neighbor-advertisement src any dest any
ipv6 access-list access-1 permit icmp neighbor-solicitation src any dest any
ipv6 access-list access-2 deny ip src any dest any
ipv6 access-list dynamic dynamic-2 ftp src 2001:db8:1::/64 dest any
interface GigaEthernet1.0
   ipv6 address 2001:db8:1::1/64
   ipv6 filter access-1 100 out
   ipv6 filter dynamic-2 200 out
   ipv6 filter access-1 100 in
   ipv6 filter access-2 200 in
   no shutdown
```

2.30.2.2 アクセスリストを利用したダイナミックフィルタ

ダイナミックアクセスリストの設定にアクセスリストを使用することにより、あらかじめ用意されたサービスだけでなく、内側から開始された通信のみを許可したり、特定の通信に連動して、動的に全く異なるパケットへのフィルタ条件を生成したりすることも可能です。
ダイナミックアクセスリストの設定の詳細は、アクセスリストの設定の節を参照してください。

ダイナミックフィルタは、フィルタを動的に deny から permit にすることが目的ですので、通常時は deny となるようスタティックフィルタで設定をしておく必要があります。

(a) 内側からのみ通信を開始したい場合

ダイナミックフィルタに使用するアクセスリストの設定で、スタティックフィルタで外部からの通信を遮断し、トリガとなる access のアクセスリストを指定した場合、「内側からは通信を行うことができるが、外部から開始された場合にはすべての通信を遮断する」という設定となります。これは、外側からのパケットをスタティックフィルタにて特に穴を開けなくても、access で指定したトリガパケットの通信は動的に許可されるためです。

access に指定したダイナミックアクセスリストにパケットがマッチすることにより、外部より許可されるパケットは、以下の条件にすべてマッチするパケットのみとなります。

- 送信元アドレスと送信先アドレスを反転したパケット
- 同一プロトコル
- 送信元ポートと送信先ポートを反転したパケット（TCP、UDP の場合）

なお、アクセスリストを指定する方法でも FTP のパケットを検知した場合には、自動的に通信可能にします。別途サービス指定で FTP を設定したダイナミックフィルタを用意する必要はありません。FTP で使用する TCP のポート 21 番がトリガの範囲にある必要があります。

【設定例】
内側から接続を開始したフローだけを通過許可させる。

IPv4 ダイナミックフィルタの場合

```
ip access-list deny-all deny ip src any dest any
ip access-list access1 permit ip src any dest any
ip access-list dynamic dyn-access access access1
!
interface GigaEthernet1.0
   ip address 10.0.0.1/8
   ip filter dyn-access 100 out
   ip filter deny-all 100 in
   no shutdown
```

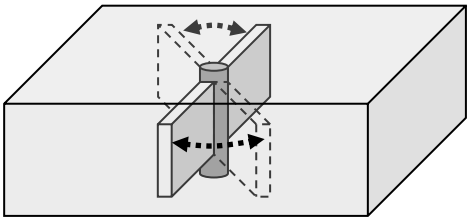
IPv6 ダイナミックフィルタの場合

```
ipv6 access-list access-1 permit icmp neighbor-advertisement src any dest any
ipv6 access-list access-1 permit icmp neighbor-solicitation src any dest any
ipv6 access-list access-2 deny ip src any dest any
ipv6 access-list access-3 permit ip src any dest any
ipv6 access-list dynamic dynamic-1 access access-3
!
interface GigaEthernet1.0
   ipv6 address 2001:db8:1::1/64
```

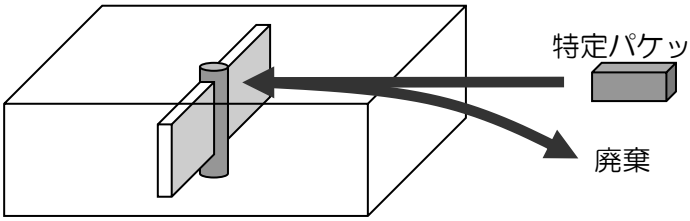
```
ipv6 filter dynamic-1 100 out
ipv6 filter access-1 100 in
ipv6 filter access-2 200 in
no shutdown
```

(b) 内側から開始された通信に応じて外部からの特定の通信を許可したい場合

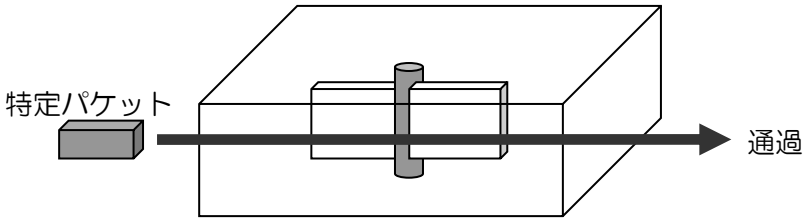
ダイナミックフィルタ（高度な利用）概念図



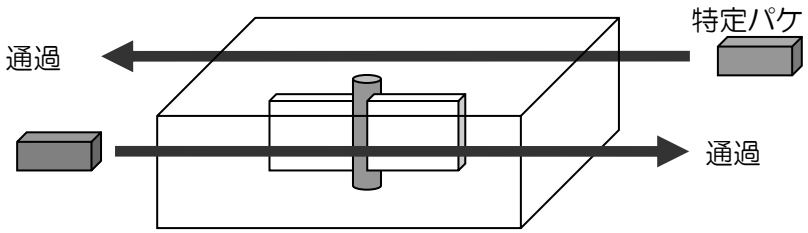
トリガとなるパケットと、トリガパケットの通過に伴って穴を開けたいフィルタを、任意の条件のアクセスリストを使用して、より詳細に設定することができます。



通常時は基本動作の場合と同様に廃棄の設定にしておきます。



特定パケットの通過に伴い、そのパケットとは別のフィルタに穴を開けることができます。



これにより複数のプロトコル、ポートを使用するアプリケーション等でも、使用時のみフィルタを通過させるような設定ができます。

ダイナミックフィルタに使用するアクセスリストの設定で、トリガとなる access のアクセスリストにパケットがヒットした場合に、逆方向または順方向に permit のフィルタを動的に作成することができます。この際トリガパケットの通信も動的に許可されます。

access に指定したダイナミックアクセスリストにパケットがマッチすることにより、IN/OUT アクセスリストの評価対象となるパケットは、以下の条件にすべてにマッチするパケットのみとなります。

- 送信元アドレスと送信先アドレスを反転したパケット
- 同一プロトコル

※ip access-list dynamic コマンドでは、in に設定したアクセスリストが逆方向、out に設定した

アクセスリストが順方向となるようにフィルタが作成されます。

【設定例】

内側から外側に TCP の 5000 番ポートを使用した場合に限り、
TCP の 6000 番ポートの通信を可能にします。

IPv4 ダイナミックフィルタの場合

```
ip access-list access-1 deny ip src any dest any
ip access-list dyn-access permit tcp src any sport eq 5000 dest any
ip access-list dyn-in permit tcp src any dest any dport eq 6000
ip access-list dynamic dynamic-1 access dyn-access in dyn-in
!
interface GigaEthernet0.0
   ip address 10.0.0.1/8
   ip filter dynamic-1 100 out
   ip filter access-1 200 in
   no shutdown
```

IPv6 ダイナミックフィルタの場合

```
ipv6 access-list access-1 permit icmp neighbor-advertisement src any dest any
ipv6 access-list access-1 permit icmp neighbor-solicitation src any dest any
ipv6 access-list access-2 deny ip src any dest any
ipv6 access-list dyn-access permit tcp src any sport eq 5000 dest any
ipv6 access-list dyn-in permit tcp src any dest any dport eq 6000
ipv6 access-list dynamic dynamic-1 access dyn-access in dyn-in
!
interface GigaEthernet0.0
   ipv6 address 2001:db8:1::1/64
   ipv6 filter dynamic-1 100 out
   ipv6 filter access-1 100 in
   ipv6 filter access-2 200 in
   no shutdown
```

2.30.2.3 IN/OUT アクセスリストの取り扱い

IN/OUT 評価は、アクセスリストの評価方法と一致します。IN もしくは OUT で指定したアクセスリストで permit にマッチしたパケットに対して通過許可を行います。deny にマッチした場合、IN/OUT アクセスリストにはマッチしなかったこととなります。

※評価条件の複数指定が可能です。

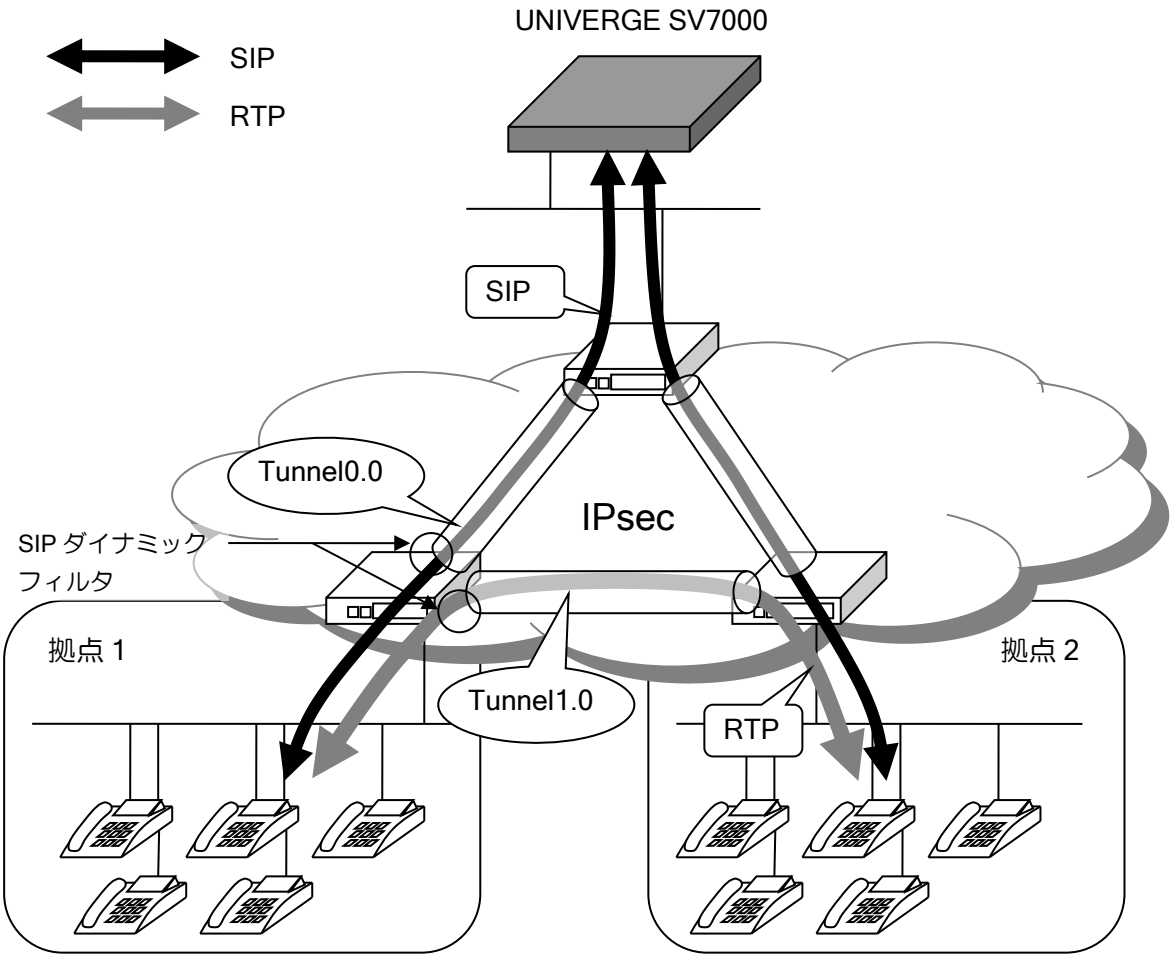
2.30.2.4 NAPT との連係

NAPT との連係を行う場合、NAPT は動的に外側にポートを開くことができませんので、NAPT 側では static あるいは service の設定を行っておいて、ダイナミックフィルタでパケットの通過または廃棄を決定するように設定を行ってください。

※評価条件の複数指定ができません。

2.30.2.5 ダイナミックフィルタグループの設定

本設定は主に以下のような環境で使用します。



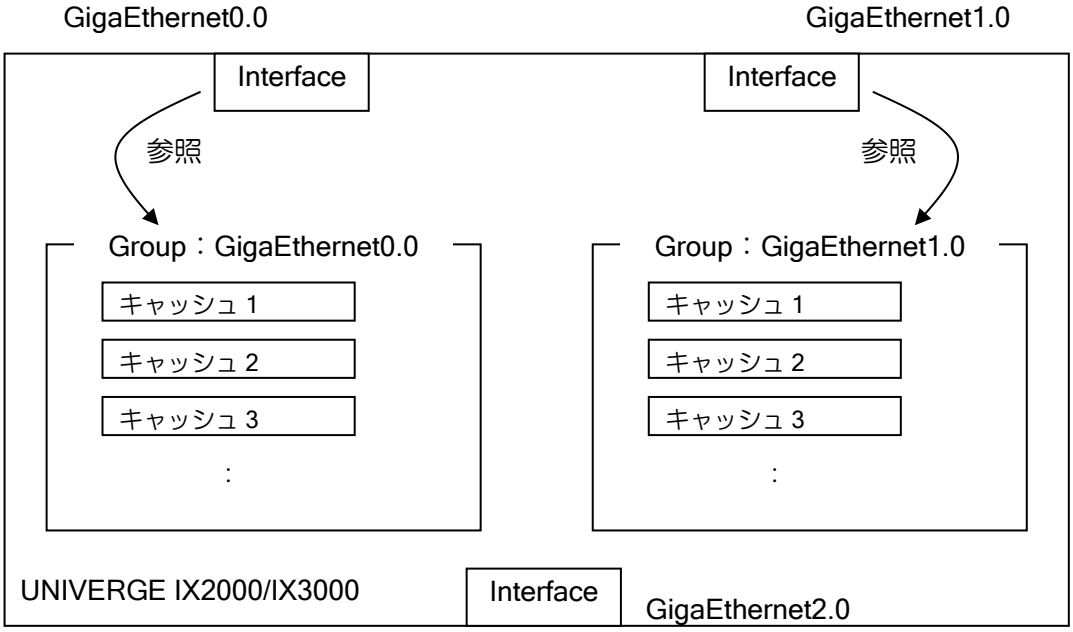
上の構成では、各拠点間でメッシュ上に IPsec トンネルを張っており、拠点ルータのトンネルインタフェースでは SIP ダイナミックフィルタを使用しています。拠点 1 では IPsec トンネルとして Tunnel0.0 と Tunnel1.0 が存在し、センタと接続している Tunnel0.0 には SIP のトラフィックが、拠点 2 と接続している Tunnel1.0 には RTP のトラフィックが流れます。

ここで SIP ダイナミックフィルタは SIP パケットを解析し、RTP パケットが通過するためのピンホール(ダイナミックフィルタキャッシュ)の生成を行いますが、デフォルトの設定では RTP パケット用のピンホールは SIP パケットが通過するインタフェースに生成されるため、SIP と RTP が通過するインタフェースが異なる場合、正常に通信できなくなります。

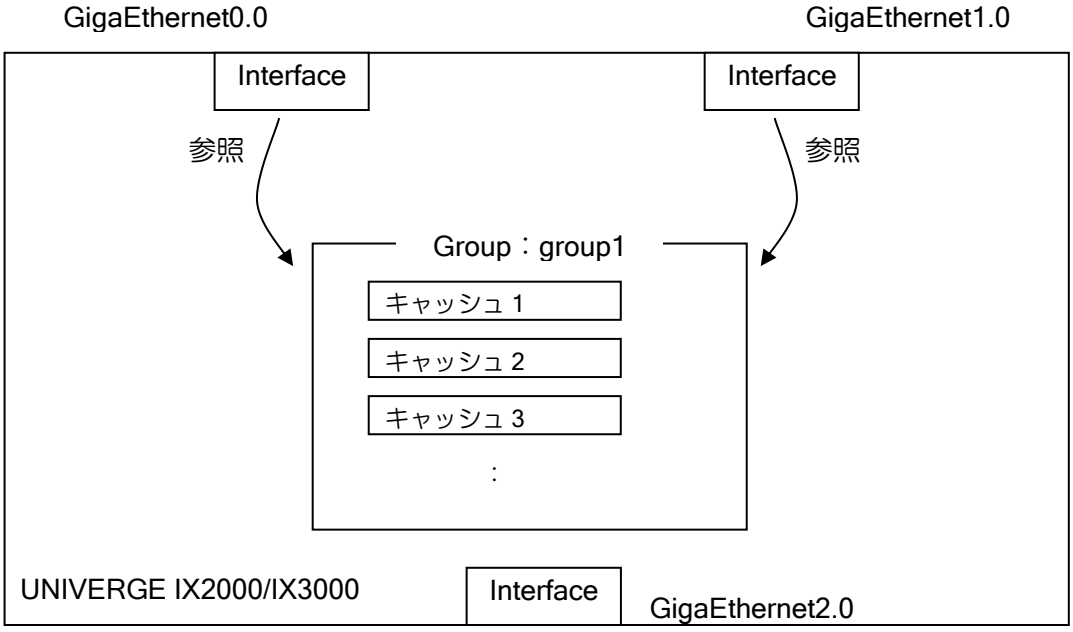
このような場合にダイナミックフィルタグループの設定を行うことで、異なるインタフェースから共通のダイナミックフィルタキャッシュの参照を行えるようになります。これにより SIP と RTP が通過するインタフェースが異なる場合でも、正常に通信が行えるようになります。

インタフェースコンフィグモード	
ip dynamic-filter group	ダイナミックフィルタのグループ化

以下はダイナミックフィルタのグループ化を「行わない場合」の内部の動作イメージです。各インタフェースで生成されたダイナミックフィルタキャッシュは独立して管理され、そのインタフェース経由でのみ参照が可能です。(グループ化の設定を行っていない場合、各インタフェースのみが所属する、各インタフェース名のグループが内部的に作られています)



以下はダイナミックフィルタのグループ化を「行った場合」の内部の動作イメージです。GigaEthernet0.0 と GigaEthernet1.0 はグループ化されているため共通の場所にキャッシュを生成します。これにより、たとえば GigaEthernet0.0 を通過したパケットにより生成されたダイナミックフィルタキャッシュが GigaEthernet1.0 を通過するパケットも参照可能になります。



【設定例】

```
ip access-list acl1 permit ip src any dest any
ip access-list dynamic dlist1 access acl1
!
interface GigaEthernet0.0
   ip address 10.1.0.1/24
   ip filter dlist1 100 out
   ip dynamic-filter group group1
   no shutdown
!
interface GigaEthernet1.0
```

```
ip address 10.2.0.1/24
ip filter dlist1 100 out
ip dynamic-filter group group1
no shutdown
```

2.30.3 強制リアセンブリ

以下のコマンドをグローバルコンフィグで行うことで、フラグメントパケットをリアセンブリしてから IP スタティックフィルタ、IP ダイナミックフィルタの処理を行うことができます。

グローバルコンフィグモード	
ip filter forced-reassembly	IP フィルタにおける強制リアセンブリの有効化 （グローバルコンフィグモード）
ipv6 forced-reassembly	IPv6 における強制リアセンブリの有効化 （インタフェースコンフィグモード）（Ver10.3 以降）

2.30.4 MAC フィルタ

MAC アクセスリストを使用することにより、レイヤ 2 情報でフィルタリングすることができます。評価条件が異なる以外は、通常のフィルタと同様な動作をします。

- 評価条件（MAC アクセスリストと同一になります）
  - 送信元 MAC アドレス指定
  - 送信先 MAC アドレス指定
  - Ethernet ヘッダの Type フィールド指定
  - VLAN タグの TPID フィールド指定
  - VLAN タグの COS フィールド指定
  - VLAN タグの CFI フィールド指定
  - VLAN タグの VLAN-ID 指定
  - 任意の位置（オフセット）指定

設定コマンドは以下のとおりです。

filter	MAC フィルタの設定

【設定例】
送信元 MAC アドレスが 11:22:33:44:55:66 のフレームのみ通過させる。

```
access-list access1 permit src 11:22:33:44:55:66 dest any

interface GigaEthernet0.0
  filter access1 100 in
  ip address 192.168.0.1/24
  no shutdown
```

2.30.5 パケットフィルタのロギング

パケットフィルタ機能とロギングの機能を使用することにより、フィルタによりパケットが廃棄された場合のログを残すことが可能です。この機能により、簡易的な攻撃監視を行うことができます。

ログ出力のための設定コマンドは以下のとおりです。

logging subsystem	表示するログ種別の指定
logging timestamp	ログの時間表示設定
event-terminal start	ログの画面出力開始
event-terminal stop	ログの画面出力停止

【設定例】
フィルタにより廃棄した時のログを表示する。

```
logging subsystem flt warn       :通常のフィルタ（IP/IPv6 フィルタ）
logging subsystem mflt warn    :MAC フィルタ

ip access-list access1 permit ip src 10.0.0.0/24 dest any
interface GigaEthernet0.0
   ip address 10.0.0.1/8
   ip filter access1 100 in
   no shutdown
```

【動作例】

```
event-terminal start

20:01:27 FLT.007:BLOCK icmp 10.1.0.2 > 10.10.10.254, match access 1, GigaEthernet0.0 in
20:01:28 FLT.007: BLOCK icmp 10.2.0.5 > 10.20.30.155, match access1, GigaEthernet0.0 in
```

＊event-terminal start コマンドはコンフィグとして保存されません。
装置再起動後は再度、コマンドを入力する必要があります。

上記の設定例のように、トラフィックフィルタのイベントログのレベルを「warn」に設定して運用することで、遮断フィルタによるパケットの廃棄ログを取得することができます。

しかし、大量のパケットが遮断フィルタに引っかかるような環境の場合、遮断ログが大量に出力されてしまい運用上望ましくない場合もあります。そのような場合はパケット廃棄ログ抑制機能を使用することで指定したフィルタによるパケット遮断ログの出力を停止することができます。

インタフェースコンフィグモード	
{ip | ipv6} filter FLT_NAME SEQ_NUM {in | out} suppress-logging	パケット廃棄ログを出力しない

本装置では、イベントログの設定を行うことでトラフィックフィルタに関する以下のような情報を取得できます。

	ログの内容	イベントログのレベル				
		error	warn	notice	info	debug
a	各種内部処理(致命的なエラー)	○	○	○	○	○
b	各種内部処理(異常系)	×	○	○	○	○
c	遮断フィルタにマッチしたので廃棄	×	○	○	○	○
d	暗黙の deny で廃棄	×	○	○	○	○
e	各種内部処理(正常系)	×	×	×	○	○

f	通過フィルタにマッチ	×	×	×	○	○
g	DNS キャッシュに変化が発生	×	×	×	×	○
h	フラグメントパケットの正常処理	×	×	×	×	○

○：情報が出力される　×：情報が出力されない

本設定を行うことで「(c)遮断フィルタにマッチしたので廃棄」に関するログの出力を停止させることができます。

【設定例】
NetBIOS のパケットを LAN 側インタフェース(GigaEthernet0.0)で遮断する。
その際の遮断ログを出力しない。

```
ip access-list rej-netbios deny tcp src any dest any dport eq 137
ip access-list rej-netbios deny tcp src any dest any dport eq 138
ip access-list rej-netbios deny tcp src any dest any dport eq 139
ip access-list rej-netbios permit ip src any dest any
!
interface GigaEthernet0.0
   ip address 192.168.0.1/24
   ip filter rej-netbios 100 in suppress-logging
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.0.0.1/24
   no shutdown
```

インタフェースで複数のフィルタリストを設定している場合、「suppress-logging」を指定していないフィルタに関しては「(c)遮断フィルタにマッチしたので廃棄」に関するログも出力されます。

パケット廃棄ログ抑制機能(suppress-logging)は MAC フィルタでも使用することができます。

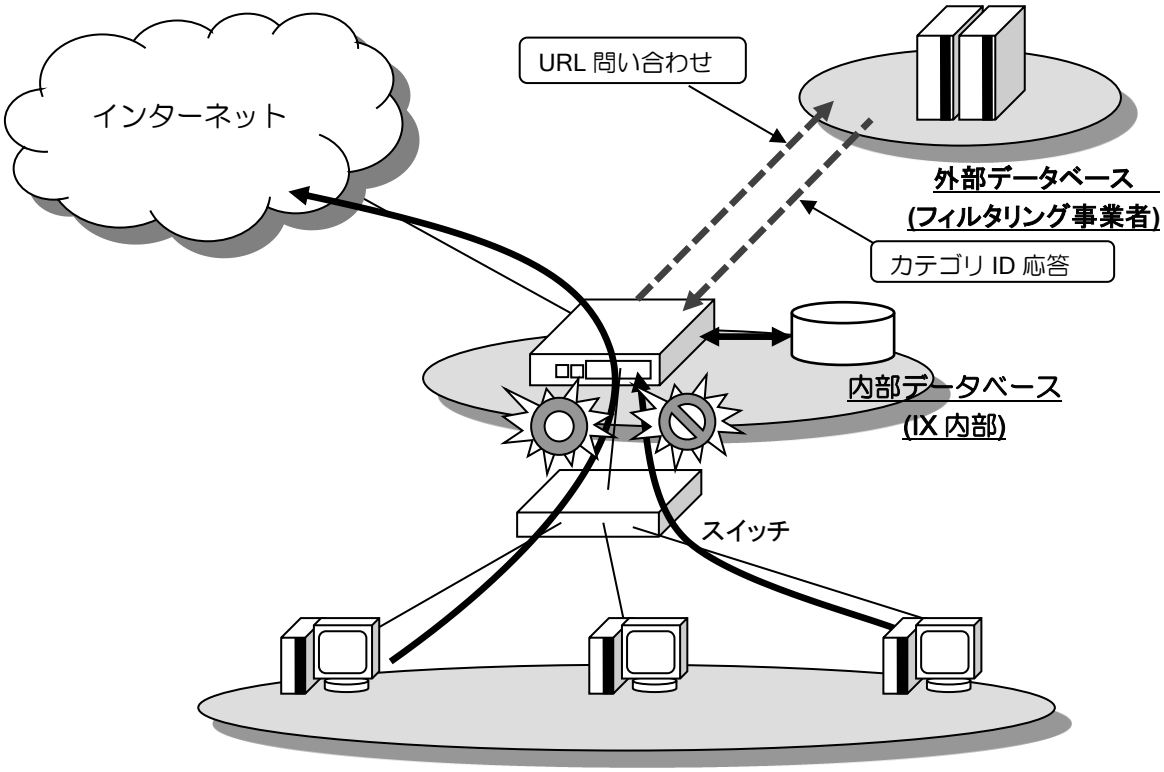
また、syslog を利用することにより、出力内容を syslog サーバへ送信することも可能です。詳しい設定方法は、ロギング機能の設定の節を参照してください。

ロギング機能は IX2000/IX3000 に負荷がかかりますので、全体的な転送性能は低下しますので注意してください。

■2.31 URL フィルタリング

URL フィルタリング機能は、HTTP/HTTPS パケットの URL を参照してフィルタを行う機能です。内部 URL フィルタリング機能と、外部 URL フィルタリング機能があり、どちらも Ver9.5 以降で利用できます。

URL フィルタリング機能の設定およびフィルタ時にユーザに表示するブロック画面の設定は Web コンソール機能に対応しており、設定画面や独自のブロック画面を用意することも可能です。Web コンソール機能による設定の説明は Web 設定マニュアルを参照してください。



2.31.1 注意事項

- 外部 URL フィルタリング機能を利用するには、別途フィルタリング事業者との契約が必要です。
- HTTPS の URL フィルタリングは以下の制限があります。
  - ドメイン名のみ参照します（パスやクエリは参照できません）。
  - ブラウザやアプリケーションによってはドメイン名が取得できない場合があります。その場合は宛先 IP アドレスによる判定のみを行います。
  - ブロック画面を表示できません。TCP の RST 送信によってセッションそのものを切断します。セッション切断時の動作はブラウザやアプリケーションに依存します（ブラウザ上にエラーメッセージが表示される等）。
- HTTP(80)、HTTPS(443)以外のポートを利用する通信には対応していません。
- IPv6 通信の URL フィルタリングには対応していません。
- ルータ自身の通信は URL フィルタリング機能の対象になりません。
- IP フィルタと併用する場合は、IP フィルタでの HTTP(80)、HTTPS(443)の廃棄は行わないでください

2.31.2 内部 URL フィルタリング機能

装置単体で利用可能な URL フィルタリング機能です。対象となる URL を URL リストとして装置内に直接登録して、通信の透過、廃棄を制御します。

内部 URL フィルタリング機能ではドメイン名のみを参照します。パスやクエリ部分は無視しますので、URL リストにはドメイン名のみを設定してください。

2.31.2.1 基本設定

内部 URL フィルタリング機能は次のコマンドを使用します。

url-list	URL リストの設定
url-filter	内部 URL フィルタリング機能の設定

【設定例】URL 末尾が example1.com または example2.com の通信と、ドメイン名に IP アドレスを指定したすべての通信を廃棄します。それ以外の通信は透過します。

```
url-list urll1 deny domain *example1.com
url-list urll1 deny domain *example2.com
url-list urll1 deny ip any
!
interface GigaEthernet0.0
  url-filter urll1 1 out
  no shutdown
```

ドメイン名に「*」を記述しない場合は完全一致、先頭のみに記述した場合は後方一致、先頭と末尾に記述した場合は部分一致となります。それ以外の条件で「*」は記述できません。

指定方法	設定例	一致する URL
完全一致	www.example.com	www.example.com に完全に一致する URL
後方一致	*example.com	末尾が example.com に一致する URL
部分一致	*example*	ドメイン名に example を含む URL

http://203.0.113.212/login/ のようにドメイン名部分に IP アドレスを指定した通信はドメイン名でフィルタすることができません。このような方法で URL フィルタリング機能をすり抜けることができないようにしたい場合は、設定例のとおりすべての IP アドレスを廃棄してください。

内部 URL フィルタリング機能の条件にマッチしない通信には、引き続き後述の外部 URL フィルタリング機能が適用されます。外部 URL フィルタリング機能の設定がない場合、内部 URL フィルタリング機能の条件にマッチしなかった通信は透過（暗黙の permit）になります。

2.31.2.2 Web コンソールからの設定

Web コンソール機能から内部 URL フィルタリング機能を設定したい場合、url-filter コマンドのシーケンス番号には 65535 を使用します。コマンドラインから設定する際に、シーケンス番号として 65535 を指定することで、Web コンソールからも設定の参照や編集が可能になります。

2.31.3 外部 URL フィルタリング機能

フィルタリング事業者が提供している URL データベースを参照するフィルタリング機能です。別途フィルタリング事業者との契約が必要です。

データベースサービスとして、アルプス システム インテグレーション株式会社のサイトアンパイアに対応しています。URL を 76 種類のカテゴリに分類し、カテゴリ単位で透過・廃棄を設定できます。

動作やカテゴリの詳細は、サイトアンパイアのページを参照してください。
http://www.alsi.co.jp/security/siteumpire/

※ このほか、同様の機能として UTM の URL フィルタリング機能があります。別途 UTM の章を参照してください。
※ 外部 URL フィルタリング機能と UTM の URL フィルタリング機能の併用は非推奨です。

2.31.3.1 利用までの準備

事前にフィルタリング事業者との契約が必要です。前述のサイトアンパイアのページから「資料請求」を選択して利用申請してください。申請には装置 MAC アドレスが必要です。MAC アドレスは以下のいずれかの方法で確認してください。

- Web コンソール機能の URL フィルタリングのページに記載された MAC アドレス
- show url-filter server コマンドを実行して表示された MAC アドレス

契約後、フィルタリング事業者の認証サーバに装置の MAC アドレスが登録されます。Web コンソール機能の URL フィルタリングの設定画面のライセンス更新ボタン、またはライセンス更新コマンド（url-filter license update）で認証状態を更新してください。認証状態が認証成功（valid）になれば外部 URL フィルタリング機能が利用可能です。

ライセンス情報は、装置起動時や 48 時間ごとに自動更新します。

2.31.3.2 基本設定（単一カテゴリグループの設定）

外部 URL フィルタリング機能は、Web コンソール機能による設定を推奨します。カテゴリ ID の説明やテンプレートを参照しながら簡単に設定できます。

以下では主にコマンドで設定する場合について説明します。外部 URL フィルタリング機能のプロファイル設定で廃棄するカテゴリを設定し、作成したプロファイルをインタフェースに適用します。

url-filter profile	外部 URL フィルタプロファイルの作成
reject category	廃棄カテゴリ ID の設定 （外部 URL フィルタプロファイル）
ignore file-extension	除外拡張子の設定 （外部 URL フィルタプロファイル）
url-filter server	外部 URL フィルタリング機能の適用 （インタフェースコンフィグモード）

【設定例】

```
url-filter profile alsi
   reject category 101-404 2501
   ignore file-extension jpg gif ico png bmp jpeg tif … mpeg mp4 asx asf wax wvx mov
!
interface GigaEthernet0.0
   url-filter server alsi out
   no shutdown
```

廃棄カテゴリ ID は、廃棄したいカテゴリを列挙して指定します。プロファイルを作成するとデフォルト値として標準的な廃棄カテゴリ（101-204 301-404 1301 2501）が設定されます。

除外拡張子に指定したファイルの通信は外部 URL フィルタリング機能の対象にならず、常に透過となります。指定した拡張子のファイルについては事業者サーバへの問合せを抑制するので、性能の低下を防止できます。除外拡張子を個別に設定することもできますが、大量のファイルを含む Web ページなどを表示する際、ファイルごとに事業者サーバへの問い合わせが発生すると性能低下の原因となるため、通常は変更せずに推奨設定のままご利用ください。なお、Web コンソール機能では除外拡張子にはデフォルト値が設定されており、変更できません。

IP アドレス形式の問い合わせを全て廃棄したい場合は、内部 URL フィルタリング機能を併用して IP アドレス形式をすべて廃棄に設定します。詳しくは内部 URL フィルタリング機能の項目をご確認ください。

そのほか特殊な設定として以下の設定が可能です（Web コンソールからは設定できません）。

reject no-category	カテゴリ ID 未定義のページの廃棄設定
reject no-response	応答がない場合の廃棄設定

2.31.3.3 複数カテゴリグループの設定

端末を複数のグループに分け、グループごとに異なるフィルタ条件を設定することができます。年齢や役職などで条件を変えたい場合に利用します。

グループの分類はアクセスリストで指定します。どのグループにも属さない通信はデフォルトの reject category の設定に従います。グループは最大 8 グループまで作成できます。

url-filter group	外部 URL フィルタグループの作成
reject group category	グループごとの廃棄カテゴリ ID の設定 （外部 URL フィルタプロファイル）

【設定例】
192.168.0.1 および 192.168.0.2 の端末のみ、通常とは別のルール（カテゴリ 101-103 のみを廃棄）を適用します。

```
ip access-list urlf-group1 permit ip src 192.168.0.1/32 dest any
ip access-list urlf-group1 permit ip src 192.168.0.2/32 dest any

url-filter group 1 ip access-list urlf-group1

url-filter profile alsi
   reject group 1 category 101-103
   reject category 101-404 1301 2501
   ignore file-extension jpg gif ico png bmp jpeg tif … mpeg mp4 asx asf wax wvx mov
!
interface GigaEthernet0.0
   url-filter server alsi out
   no shutdown
```

※ グループ設定は外部 URL フィルタリング機能のみで有効です。内部 URL フィルタリング機能では利用できません。

2.31.4 URL フィルタリング対象外の設定

URL フィルタリング機能の対象外にする条件をアクセスリストで設定できます。

特定の端末を URL フィルタリング機能の対象外とする、HTTPS 通信だけを URL フィルタリング機能の対象外とするなど特定の条件で URL フィルタリング機能の例外を設定できます。設定した条件は内部 URL フィルタリング機能と外部 URL フィルタリング機能の両方で対象外となります。

url-filter ignore	対象外のアクセスリストの設定
ip access-list	アクセスリスト

【設定例】
192.168.0.0/24 を送信元とする通信と、HTTPS 通信はいずれも URL フィルタリング機能の対象外とする。

```
ip access-list ignore-list permit ip src 192.168.0.0/24 dest any
ip access-list ignore-list permit tcp src any sport any dest any dport eq 443

url-filter ignore ip access-list ignore-list
```

アクセスリストでは、除外する条件を permit で指定します。なお、Web コンソールからは除外端末の設定しかできません。

2.31.5 ブロック画面の設定

内部 URL フィルタリング機能や外部 URL フィルタリング機能で廃棄と判定した場合に、ブロック画面で廃棄理由などを利用者に表示することができます。以下のコマンドで設定します。

url-filter reject-action	廃棄動作設定（ブロック画面表示設定）

【設定例】

装置内のブロック画面を指定（通常 LAN 側インタフェースを指定してください）

```
url-filter reject-action local GigaEtheret1.0
```

他装置のブロック画面を表示

```
url-filter reject-action redirect http://example.com/block.html
```

あらかじめ装置内に用意されているブロック画面を利用したい場合は廃棄動作設定に local を指定してください。通常は LAN 側のインタフェースを指定します。ブロック画面はカスタマイズできますので、後述の項目を参照してください。

なお、装置内のブロック画面を表示するためには端末側から Web コンソール画面にアクセスできる必要があります。Web コンソール機能のアクセス制御でアクセス端末を制限している場合は、それ以外の端末にはブロック画面が表示されませんのでご注意ください。

また、HTTPS 通信を廃棄した場合は、ブロック画面は表示されません。利用者側ではブラウザ上に通信エラーなどのエラーメッセージが表示されます。

2.31.6 URL フィルタキャッシュの設定

URL フィルタリング機能は、キャッシュ機能を実装しています。同一の URL への通信が多い場合や再送された通信を処理する場合などに、事業者サーバへの同一の問い合わせを抑制して高速化します。デフォルト設定で有効になっているので、通常はそのままご利用ください。

通信中に URL リストを変更した場合、キャッシュが残っていると即時反映されない場合があります。キャッシュが消えるまで待つか、キャッシュをクリアしてください。

2.31.7 URL フィルタリング機能の処理順序

以下の順番で処理します。

1. 対象外の条件の判定
2. グループの分類
3. 内部 URL フィルタリング機能の処理
4. 外部 URL フィルタリング機能の処理

内部 URL フィルタリングの条件にマッチしなかった通信のみが、外部 URL フィルタリング機能の対象になるため、双方を併用することで次のような処理が可能です。

- 外部 URL フィルタリング機能で廃棄するカテゴリの一部だけを、内部 URL フィルタリング機能で透過する
- IP アドレス形式の URL を持つ通信を内部フィルタリング機能ですべて廃棄し、それ以外の通信のみを外部 URL フィルタリング機能で送信する

2.31.8 その他の設定

以下のような設定も可能です（Web コンソールからは設定できません）。

- カテゴリが設定されていないページの廃棄設定（デフォルト設定では透過）
- 事業者サーバと通信できない場合の廃棄設定（デフォルト設定では透過）
- スケジューラ機能と併用し、休憩時間など時間帯ごとにカテゴリ ID の設定を切り替える設定

2.31.9 ブロック画面のカスタマイズ

ブロック画面は、独自のページに変更することができます。装置内部のブロック画面は「/url-filter/block.html」 です。拡張ページ機能で、このファイルを上書きしてください。

なお、URL フィルタリング機能は通信廃棄時に以下のクエリを送信します。

【外部 URL フィルタリング機能で廃棄した場合】

sv=alsi&id=<カテゴリ ID>&url=<URL>

【内部 URL フィルタリング機能で廃棄した場合】

list=<リスト名>&url=<URL>

■2.32 不正アクセス検知（IDS）の設定

不正アクセス検知（IDS:Intrusion Detection System）機能は、不正なパケット受信を検知する機能です。IPv4 のみサポートとなります。

2.32.1 不正アクセス検知条件

本機能では、パケット受信時に以下の条件で不正アクセスの検知を行います。
不正アクセス検知は IP ヘッダ、IP オプションヘッダ、ICMP、UDP、TCP、FTP の６種類のタイプに分類されます。

タイプ	イベントログ番号	名称	内容
IP ヘッダ			
	IDS.001○	Short header	IP ヘッダ長が 20 バイト未満 （全てのタイプのうち、1 つでも設定された場合、有効になります。）
	IDS.002○	Malformed packet	IP パケットの構造が不正 （全てのタイプのうち、1 つでも設定された場合、有効になります。）
	IDS.003	Unknown protocol	プロトコル領域の値が 143 以上
	IDS.004	Land attack	送信元 IP アドレスと宛先 IP アドレスが同じ
	IDS.005	Localhost source spoof	送信元 IP アドレスが 127.0.0.1
	IDS.006	Broadcast source address	送信元 IP アドレスが 255.255.255.255
	IDS.007	Multicast source address	送信元 IP アドレスがマルチキャストアドレス
IP オプションヘッダ			
	IDS.051○	Malformed option packet	オプションヘッダの構造が不正
	IDS.052	Security and handling restriction header	Security and handling restriction header を受信
	IDS.053	Loose source routing header	Loose source routing header を受信
	IDS.054	Internet timestamp header	Internet timestamp header を受信
	IDS.055	Record route header	Record route header を受信
	IDS.056	Stream identifier header	Stream identifier header を受信
	IDS.057	Strict source routing header	Strict source routing header を受信
ICMP			
	IDS.101○	Short header	ICMP ヘッダ長が 4 バイト未満
	IDS.102	Source quench	Source quench を受信
	IDS.103	Timestamp request	Timestamp request を受信
	IDS.104	Timestamp reply	Timestamp reply を受信
	IDS.105	Information request	Information request を受信
	IDS.106	Information reply	Information reply を受信
	IDS.107	Address mask request	Address mask request を受信
	IDS.108	Address mask reply	Address mask reply を受信
	IDS.109	Too large	1025 バイト以上の ICMP を受信
	IDS.110	Ping of death attack	Ping of death attack を受信
UDP			
	IDS.151○	Short header	UDP ヘッダ長が 8 バイト未満

	IDS.152	UDP bomb	UDP パケットの構造が不正
TCP			
	IDS.201〇	Short header	TCP ヘッダ長が 20 バイト未満 （FTP が設定されている場合、有効となります）
	IDS.202	No bits set	フラグに何もセットされていない
	IDS.203	SYN and FIN	SYN と FIN が同時にセット
	IDS.204	FIN and no ACK	ACK のない FIN を受信
FTP			
	IDS.251	Improper port	不正なデータ通信用ポートを指定

※イベントログ番号欄の〇の項目に関しては、検知時の動作設定にかかわらず廃棄されます。

不正パケット検知の有無は、タイプ毎に設定できます。
不正パケット検知時の動作は以下になります。

- 検知のみ・廃棄（タイプ毎にどちらかを選択）
  - 検知のみの場合は、同一タイプの他のイベントの検知は行わず、次のタイプの検知を行います。
  - 廃棄の場合は、以降のイベントの検知は行いません。
- イベントログの出力（IDS としてログ出力を設定）
  - syslog 機能利用により外部への通知ができます。
- 統計情報のカウント

イベントログの出力例は以下のとおりです。

【イベントログ出力例】
プロトコル領域が 143 以上

IDS.003: [IP] Unknown protocol packet was detected (protocol 180) 10.44.20.139 > 192.168.160.105, GigaEthernet0.0

2.32.2 不正アクセス検知条件の設定

設定は以下のとおりです。

ids ip type	IDS 機能の有効化
show ids statistics	IDS 統計情報の表示

【設定例】

全ての条件を検知
イベントログに出力を行う。
logging subsystem ids warn
logging timestamp datetime

ids ip type all action detect

IP ヘッダと ICMP のみ検知し、検知時は廃棄
検知時にイベントログと syslog で出力を行う
syslog ip host 192.168.0.100

logging subsystem ids warn

```
logging timestamp datetime

ids ip type ip-header action discard
ids ip type icmp action discard
```

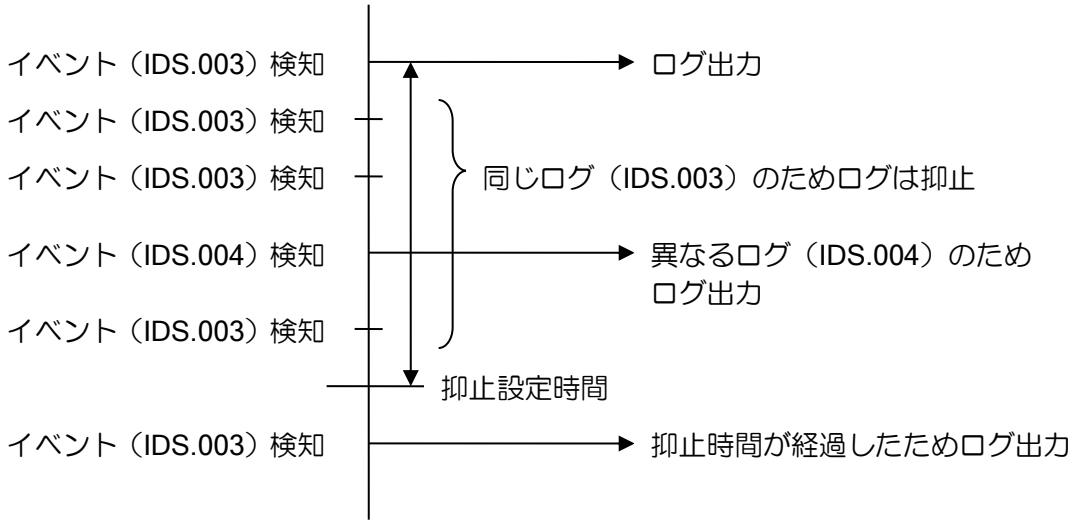
イベント検知後、一定時間内に同一のイベントが検知された場合、イベントログ出力を抑止することができます。これにより、ログ出力による負荷を軽減することができます。ログを抑止した場合でも、イベントの検知は行います。

ids logging-interval	重複したイベントのログ抑止設定

【設定例】

60 秒間に同じイベントが発生した場合にログの出力を抑止

```
logging subsystem ids warn
logging timestamp datetime

ids ip type all action discard
ids logging-interval 60
```



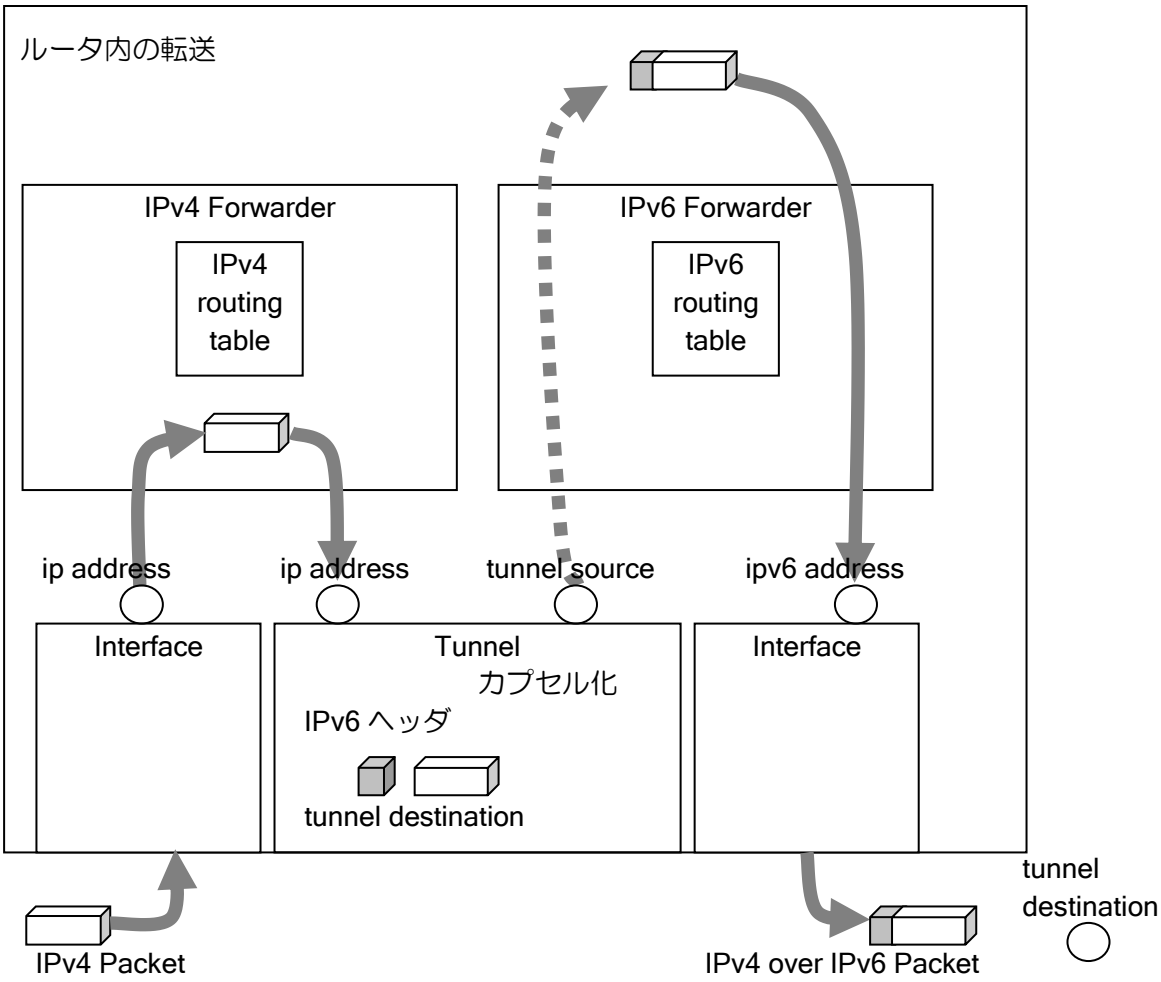
※clear ids statistics 実行時に、抑止の経過時間はクリアされます

■2.33 トンネルの設定

2.33.1 トンネル機能の概要

2 台のルータ間を仮想的なトンネルで接続し、離れた 2 点間で直接パケットを送受信する仕組みです。インターネット上にプライベートアドレスで通信したり、IPv6 網上で IPv4 通信を行うことができます。

以下は IPv4 over IPv6 トンネルの例です。IPv4 のパケットに IPv6 ヘッダを付与して（カプセル化）送信します。受信側は矢印を逆に辿りカプセル化を解除し、IPv4 パケットを受け取れます。



IX2000/IX3000 シリーズは以下のトンネル機能をサポートしています。

- IPv6 over IPv4 モード
- IPv4 over IPv6 モード
- IPv6 over IPv6 モード
- IPv4 over IPv4 モード
- IPsecモード （詳細はIPsecの設定の章を参照してください）
- GRE（Generic Routing Encapsulation）モード（Ver.5.2以降）
- EtherIPモード（Ver.7.2以降。詳細はEther over IPの設定の章を参照してください）
- L2TP IPsecモード （詳細はL2TPの設定の章を参照してください）
- MAP-E モード（Ver.10.1以降）
- 標準プロビジョニング方式（Ver.10.8以降）

なお、Ver9.5 以降ではトンネルインタフェースの一括設定をサポートしています。複数のトンネルの設定が同一または一部名称だけ変化する場合に活用できます。詳細は保守・運用の章のインタフェース一括設定を参照してください。

2.33.2 トンネルの設定

トンネルはインタフェースとして実装しています。トンネルインタフェースにパケットをルーティングすることで tunnel mode で指定した種別のカプセル化が行われます。
トンネル設定で使用する主なコマンドは以下のとおりです。

tunnel mode	トンネルモードの選択
tunnel destination	トンネルの送信先アドレス設定
tunnel source	トンネルの送信元アドレス設定
tunnel outgoing-interface	トンネルの送信インタフェース設定(Ver10.7 以降)
tunnel checksum	チェックサム設定（GRE 専用）
tunnel keepalive	キープアライブ設定（GRE 専用）
tunnel key	キー設定（GRE 専用）
tunnel sequence-number	シーケンス番号設定（GRE 専用）

IPsec を利用する場合は、IPsec の章を参照してください。

2.33.3 フラグメントの設定

トンネルは IPv4 または IPv6 ヘッダでパケットをカプセル化するため、パケットのサイズが大きくなります。送信可能なパケットサイズには上限があり（MTU サイズ）、カプセル化により送信インタフェースの MTU を超えると、そのままではパケットが送信できません。
カプセル化して MTU を超えるパケットは、通常分割してパケットを送信します（フラグメント）。ただし、IPv4 でフラグメント禁止ビットが 1（有効）のパケットや IPv6 パケットはフラグメントが禁止されているため、デフォルトではパケットを廃棄し、送信元に MTU を下げて送信するよう ICMP エラーを通知します（Path MTU Discovery）。

ただし Path MTU Discovery は動作しない場合も多いことから、IX ルータでは no tunnel adjust-mtu コマンドでフラグメント禁止でも強制的にフラグメントして送信する設定が可能です（GRE トンネルは tunnel df-bit ignore で設定します）。
また、ip forced-fragment という、パケットのフラグメント禁止ビットを 0（無効）に書き換えるコマンドもありますので、ヘッダ情報を書き換えて良い場合に利用してください。

tunnel df-bit	トンネルのフラグメント設定
tunnel adjust-mtu	トンネルインタフェースの MTU 指定
ip forced-fragment	強制フラグメント機能の有効設定

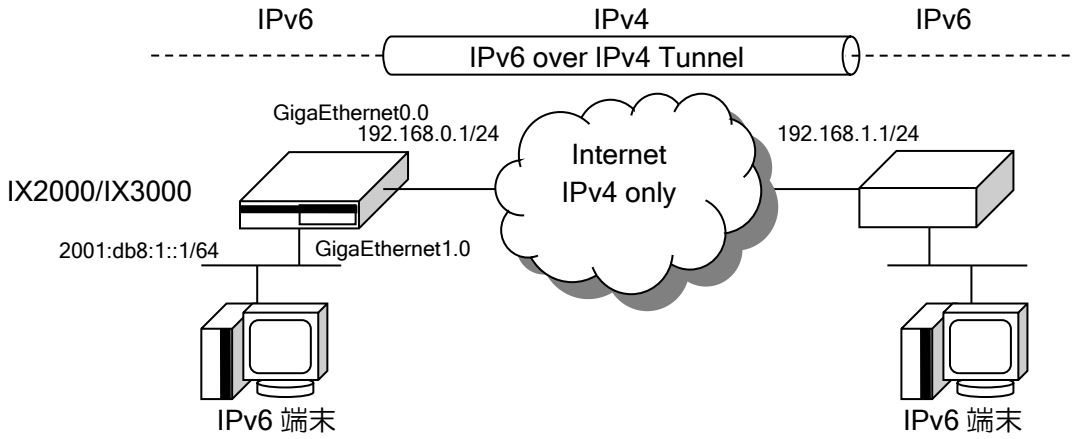
また、TCP の通信は MSS 調整機能により端末が MTU を超えない範囲で TCP パケットを送信するように設定できます。TCP の性能劣化を抑制するため、通常設定するようにしてください。
なお、no tunnel adjust-mss を設定している場合 MSS は自動調整できませんので、適切な値を指定する必要があります。ip forced-fragment コマンドの場合には自動調整が可能です。

ip tcp adjust-mss	TCP（IPv4）の MSS 調整
ipv6 tcp adjust-mss	TCP（IPv6）の MSS 調整

- tunnel adjust-mtu について
  - no tunnel adjust-mtuの場合、トンネルのMTUはシステムの最大MTU値となります。
  - トンネルのMTUを超えるパケットは、DFビットでフラグメントの可否を判断します。
  - カプセル化後のサイズが送信する物理インタフェースのMTUを超える場合（no tunnel adjust-mtuは常に）は、DFビットによらずフラグメントし、DFビットを0にします。
  - tunnel adjust-mtu autoの場合、DFビットはtunnel df-bitの設定に従います。

2.33.4 IPv6 over IPv4 トンネルの設定

IPv6 over IPv4 トンネルで登録する情報は以下のようになります。



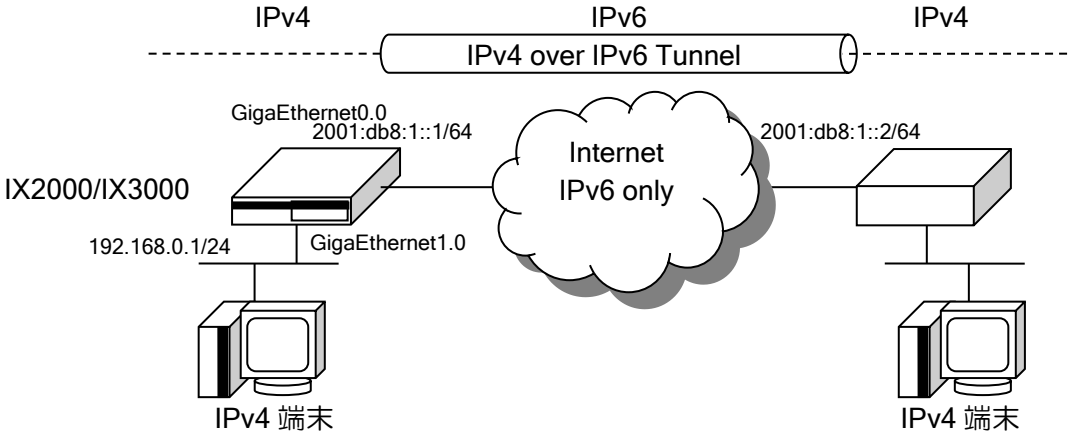
【設定例】

IPv6 over IPv4 トンネルを登録し、アドレスを付与します。

```
ip route default 192.168.0.254
ipv6 route default Tunnel0.0

interface GigaEthernet0.0
   ip address 192.168.0.1/24
   no shutdown

interface GigaEthernet1.0
   ipv6 address 2001:db8:1::1/64
   no shutdown

interface Tunnel0.0
   tunnel mode 6-over-4
   tunnel destination 192.168.1.1
   tunnel source GigaEthernet0.0
   ipv6 enable
   ipv6 tcp adjust-mss auto
   no shutdown
```

2.33.5 IPv4 over IPv6 トンネルの設定

IPv4 over IPv6 トンネルで登録する情報は以下のようになります。



【設定例】

IPv4 over IPv6 トンネルを登録し、アドレスを付与します。
（強制的にフラグメントする場合の設定例）

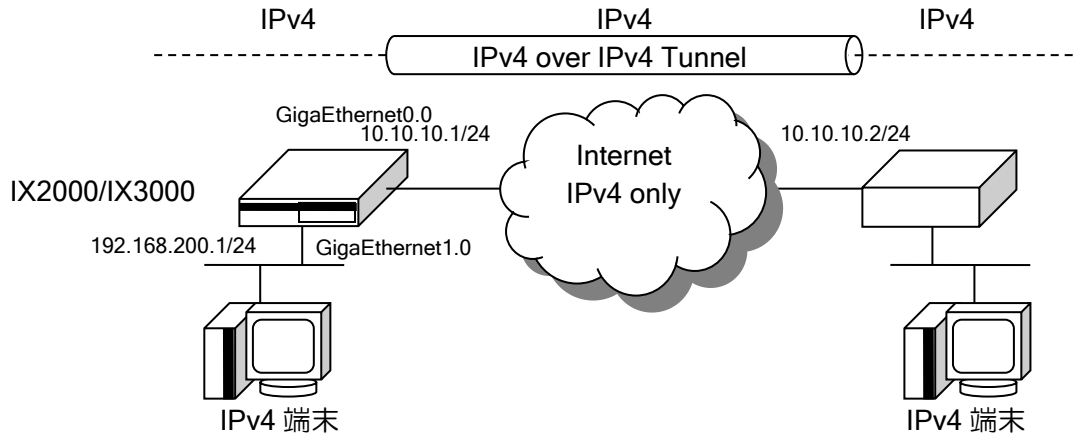
```
ip route default Tunnel0.0

interface GigaEthernet0.0
   ipv6 address 2001:db8:1::1/64
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.0.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode 4-over-6
   no tunnel adjust-mtu
   tunnel destination 2001:db8:1::2
   tunnel source 2001:db8:1::1
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss 1400
   no shutdown
```

トンネル内が IPv4 の場合には IPv4 アドレスの設定が必要です（ip address コマンドまたは ip unnumbered コマンド）。トンネルに固有の IPv4 アドレスが必要でなければ、ip unnumbered コマンドを設定してください（設定の際は IPv4 アドレスが割り当てられたインタフェースを指定してください。通常 LAN 側のインタフェースになります）。

2.33.6 IPv4 over IPv4 トンネルの設定

IPv4 over IPv4 トンネルで登録する情報は以下のようになります。

予め通信相手となるネットワークがわかっている場合で、プライベートアドレスを用いたネットワークからプライベートアドレスを用いたネットワークにグローバルアドレス空間を介して通信する場合などに有効となる機能です。



【設定例】

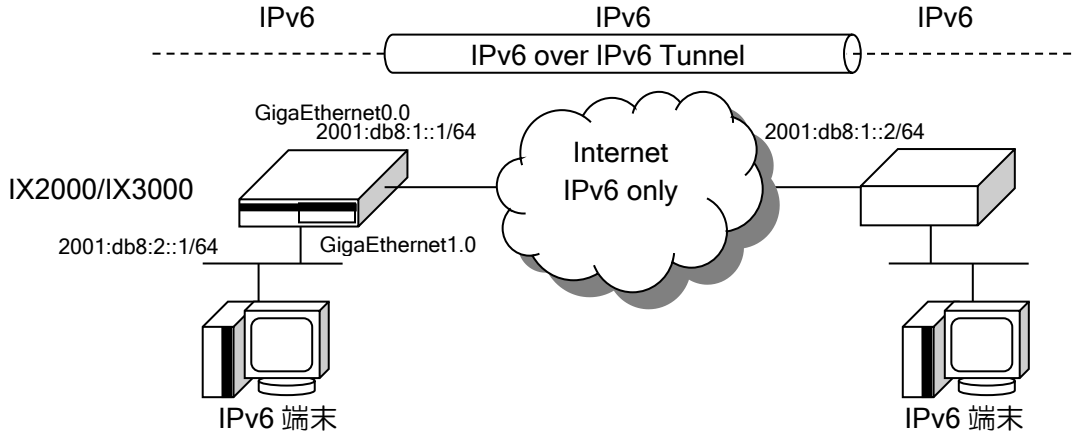
IPv4 over IPv4 トンネルを登録し、アドレスを付与します。

```
ip route default Tunnel0.0

interface GigaEthernet0.0
   ip address 10.10.10.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.200.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode 4-over-4
   tunnel destination 10.10.10.2
   tunnel source GigaEthernet0.0
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   no shutdown
```

トンネル内が IPv4 の場合には IPv4 アドレスの設定が必要です（ip address コマンドまたは ip unnumbered コマンド）。トンネルに固有の IPv4 アドレスが必要でなければ、ip unnumbered コマンドを設定してください（設定の際は IPv4 アドレスが割り当てられたインタフェースを指定してください。通常 LAN 側のインタフェースになります）。

2.33.7 IPv6 over IPv6 トンネルの設定

IPv6 over IPv6 トンネルで登録する情報は以下のようになります。



【設定例】

IPv6 over IPv6 トンネルを登録し、アドレスを付与します。

```
ipv6 route default Tunnel0.0

interface GigaEthernet0.0
   ipv6 address 2001:db8:1::1/64
   no shutdown

interface GigaEthernet1.0
   ipv6 address 2001:db8:2::1/64
   no shutdown

interface Tunnel0.0
   tunnel mode 6-over-6
   tunnel destination 2001:db8:1::2
   tunnel source 2001:db8:1::1
   ipv6 enable
   ipv6 tcp adjust-mss auto
   no shutdown
```

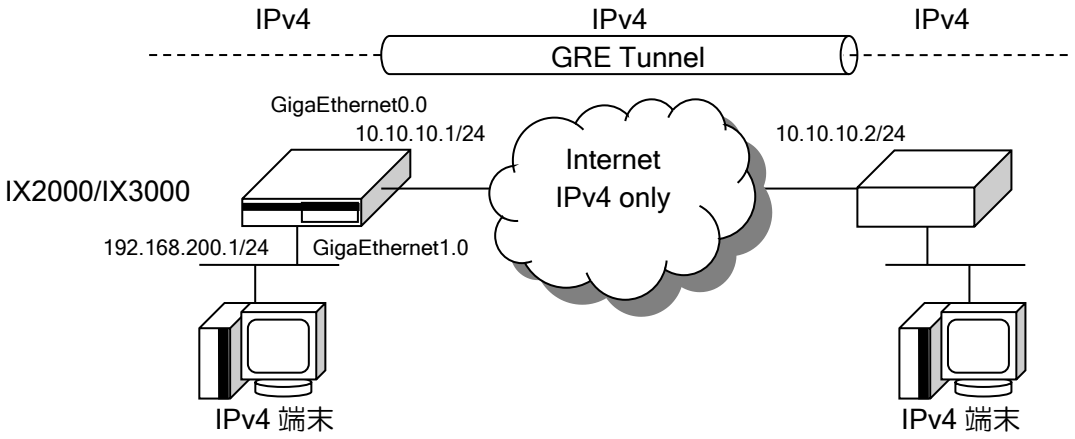
2.33.8 GRE（Generic Routing Encapsulation）トンネルの設定

GRE トンネルは、レイヤやプロトコルの異なるパケットの後に GRE 用のヘッダを付与し、カプセル化を行います。GRE トンネルでは他のトンネルではサポートしていないキープアライブ機能をサポートしています。この機能を利用することで IX2000/IX3000 以外の装置と対向する場合でも冗長構成を構築することができます。キープアライブ機能の他にも、チェックサム等通信の信頼性を向上するための機能をサポートしています。（対向装置も GRE トンネルをサポートしている必要があります）

GRE トンネルでは、以下の機能をサポートしております。

- IPv4でのカプセル化
- IPv6でのカプセル化（Ver.9.1以降）
- IPv4パケットのカプセル化
- IPv6パケットのカプセル化
- Ethernetパケットのカプセル化（Ver.8.9以降）
- IPsecトランスポートモードと組み合わせた通信
- GRE over IPsec（Ver.8.9以降）

GRE トンネルで登録する情報は以下のようになります。



【設定例】
GRE トンネルを登録し、unnumbered に設定します。

```
ip route default Tunnel0.0

interface GigaEthernet0.0
   ip address 10.10.10.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.200.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode gre ip
   tunnel destination 10.10.10.2
   tunnel source GigaEthernet0.0
   ip unnumbered GigaEthernet1.0
   no shutdown
```

GRE では以下の機能をサポートしています。これらの機能は複数を同時に使用することが可能です。

(a)キープアライブの設定

トンネルの接続先の対向装置との正常性を確認する機能です。

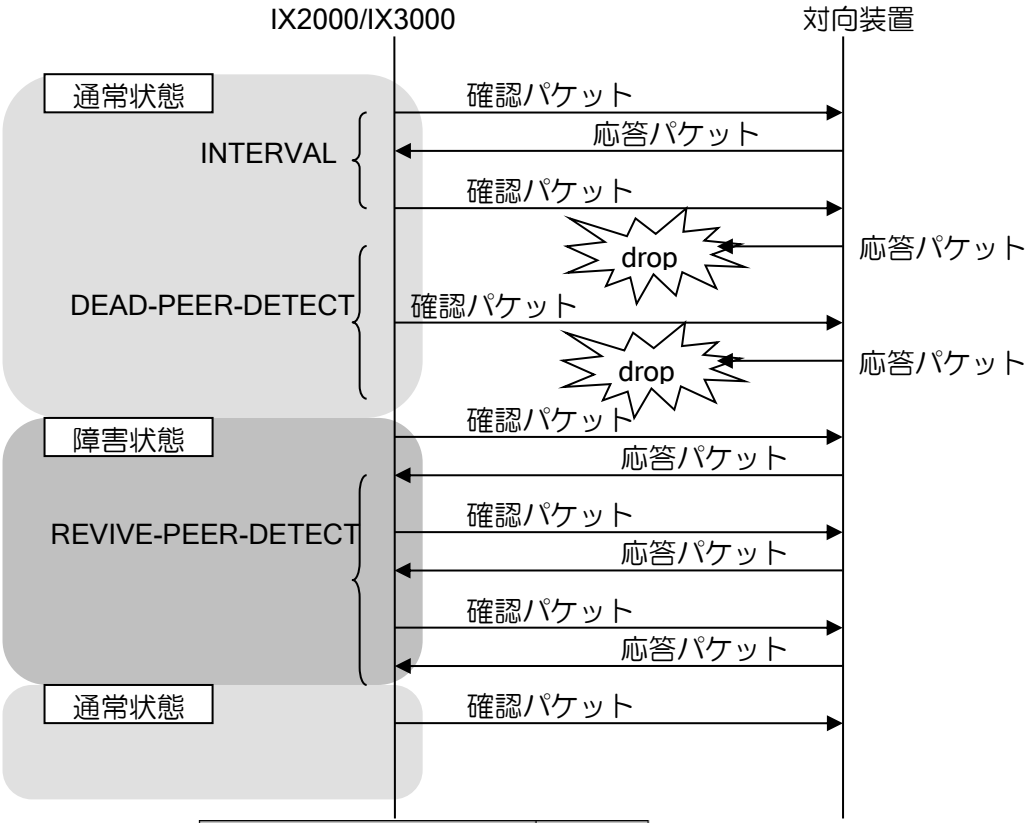
キープアライブでは、一定周期で確認用のパケットを送信し、次の送信時までに応答が返らなければ、応答が無かったと判断します。一定回数応答が返らなければ障害を検出し、インタフェースのプロトコル状態を down にします。（復旧確認のために、パケットの送信は継続します）

また、障害中に一定回数応答が返ると復旧を検出し、インタフェースのプロトコル状態を up にします。なお、確認パケットの送信間隔，障害検出の回数、復旧検出の回数は設定が可能です。

上記機能によりトンネル区間障害中は、トンネルが出力先となる経路はルーティングテーブルから削除されるため、他の経路へ迂回を行うことが可能になります。

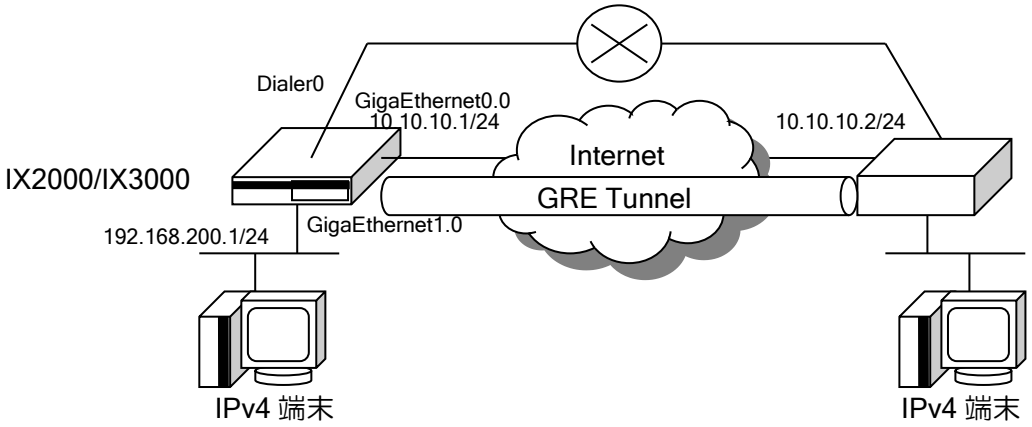
Ver.8.6 以降、以下の動作仕様が異なります。

動作	Ver.8.6 以降	Ver.8.5 以前
キープアライブ起動時の状態	障害状態から開始 復旧時間経過後、正常状態	正常状態から開始
キープアライブ障害検出時のトンネルの状態	トンネルインタフェースが down	トンネルインタフェースの IP 状態が down （トンネルインタフェースは up）



パラメータ	設定例
INTERVAL	5
DEAD-PEER-DETECT	2
REVIVE-PEER-DETECT	3

設定は以下のコマンドで行います。



tunnel keepalive	キープアライブの設定

【設定例】

GRE トンネルのキープアライブを使用した ISDN 迂回構成

```
ip route default Tunnel0.0 distance 100
ip route default Dialer0 distance 150

ppp profile isdn

device BRI0
   isdn switch-type ins64
   isdn answer1 011-987-6543

interface GigaEthernet0.0
   ip address 10.10.10.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.200.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode gre ip
   tunnel destination 10.10.10.2
   tunnel source 10.10.10.1
   tunnel keepalive period 5 retries 2
   ip unnumbered GigaEthernet1.0
   no shutdown

interface Dialer0
   encapsulation ppp
   no auto-connect
   dialer string 03-1234-5678
   ppp binding isdn
   ip unnumbered GigaEthernet1.0
   no shutdown
```

(b)チェックサムオプションの設定

GRE ヘッダにチェックサムを付与します。GRE トンネルでパケット受信時は、チェックサムが付与されている場合のみ、チェックサムの計算を行い、付与されたチェックサムと異なる場合はパケットを廃棄します。

設定は以下のコマンドで行います。

tunnel checksum	チェックサムの設定

【設定例】

```
ip route default Tunnel0.0

interface GigaEthernet0.0
   ip address 10.10.10.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.200.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode gre ip
   tunnel destination 10.10.10.2
   tunnel source 10.10.10.1
   tunnel checksum
   ip unnumbered GigaEthernet1.0
   no shutdown
```

(c)キーオプションの設定

GRE ヘッダにキー値を設定します。パケット受信時は、トンネルインタフェースに設定しているキー値と一致した場合のみ受信しますので、GRE トンネルの両端でキー値は一致している必要があります。キー値が一致するインタフェースが存在しない場合はパケットを廃棄します。

設定は以下のコマンドで行います。

tunnel key	キー値の設定

【設定例】

キー値に 10 を設定

```
ip route default Tunnel0.0

interface GigaEthernet0.0
   ip address 10.10.10.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.200.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode gre ip
   tunnel destination 10.10.10.2
   tunnel source 10.10.10.1
   tunnel key 10
   ip unnumbered GigaEthernet1.0
   no shutdown
```

(d)シーケンス番号オプションの設定

GRE ヘッダにシーケンス番号を付与します。IX2000/IX3000 では、送信時のシーケンス番号の付与のみ行い、受信時のシーケンス番号のチェック等は行いません。

設定は以下のコマンドで行います。

tunnel sequence-number	シーケンス番号の設定

【設定例】

```
ip route default Tunnel0.0

interface GigaEthernet0.0
   ip address 10.10.10.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.200.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode gre ip
   tunnel destination 10.10.10.2
   tunnel source 10.10.10.1
   tunnel sequence-number
   ip unnumbered GigaEthernet1.0
   no shutdown
```

(e)GRE トンネルと IPsec の連携

GRE トンネルと物理インタフェース上の IPsec 設定を併用することにより、GRE トンネルのパケットを暗号化することができます。また、Ver.8.9 以降は、トンネルインタフェースで直接 GRE over IPsec を設定が可能です。

前者の方式は、動的アドレス環境で利用できない、性能が低いなどの制限がありますので、通常は後者のトンネルインタフェース方式を利用してください。

IPsec はトランスポートモードで利用します。トランスポートモードの詳細については、IPsec の項を参照してください。with-id-payload は必ず設定してください。

なお、Ver9.2 以降では GRE over IKEv2 も設定可能です。モードをトランスポートにして設定してください。

【設定例（IKEv1/IPsec 物理インタフェース方式)】

```
ip route default Tunnel1.0
ip access-list acl permit 47 src 10.0.0.1/32 dest 10.0.0.2/32

ike proposal ike-prop encryption aes hash sha
ike policy ike-policy peer 10.0.0.2 key gre-key ike-prop

ipsec autokey-proposal sec-prop esp-aes esp-sha
ipsec autokey-map sec-policy acl peer 10.0.0.2 sec-prop

interface GigaEthernet0.0
   ip address 10.0.0.1/24
   ipsec policy transport sec-policy with-id-payload
   no shutdown
```

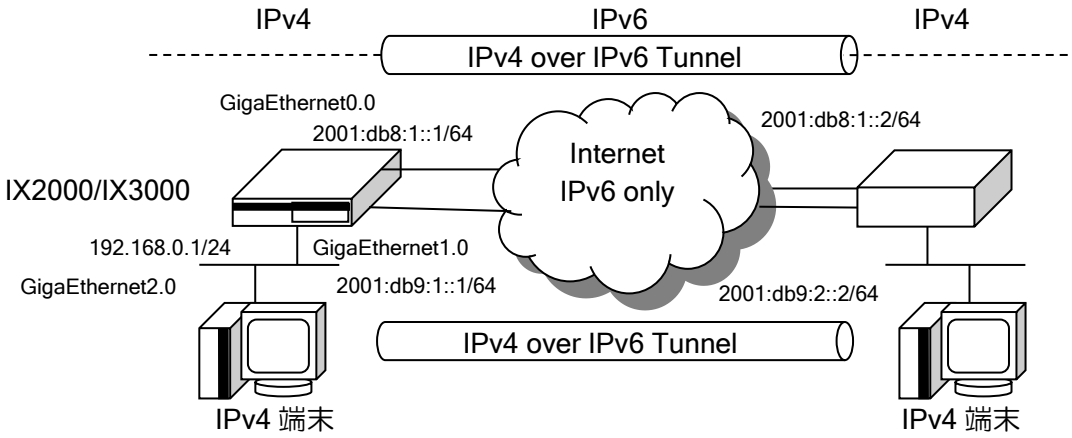
```
interface GigaEthernet1.0
   ip address 192.168.0.1/24
   no shutdown

interface Tunnel1.0
   tunnel mode gre ip
   tunnel destination 10.0.0.2
   tunnel source 10.0.0.1
   ip address 100.0.0.1/30
   no shutdown
```

【設定例（IKEv1/IPsec トンネルインタフェース方式）】

```
ip route default Tunnel1.0
ip access-list acl permit 47 src 10.0.0.1/32 dest 10.0.0.2/32

ike proposal ike-prop encryption aes hash sha
ike policy ike-policy peer 10.0.0.2 key gre-key ike-prop

ipsec autokey-proposal sec-prop esp-aes esp-sha
ipsec autokey-map sec-policy acl peer 10.0.0.2 sec-prop

interface GigaEthernet0.0
   ip address 10.0.0.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.0.1/24
   no shutdown

interface Tunnel1.0
   tunnel mode gre ipsec
   ip address 100.0.0.1/30
   ipsec policy transport sec-policy with-id-payload
   no shutdown
```

2.33.9 IPv4 over IPv6 トンネル(冗長)の設定

Ver10.7 からトンネルの冗長が可能となりました。
本例では IPv4 over IPv6 トンネルを例としていますが、他のトンネルについても同様です。
tunnel outgoing-interface を指定することで任意のインタフェースからの出力が可能となります。



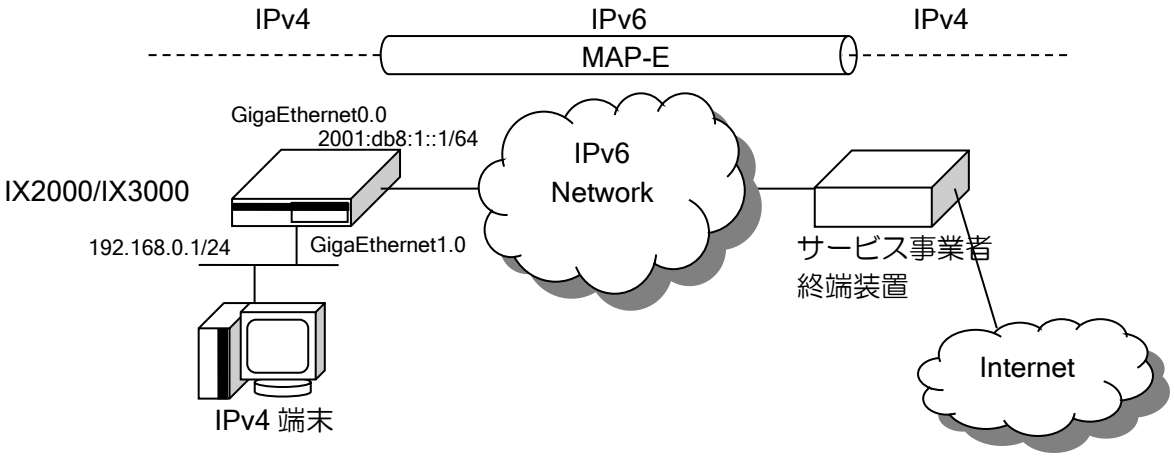
【設定例】

IPv4 over IPv6 トンネルを登録し、アドレスを付与します。

```
ip route default Tunnel0.0

interface GigaEthernet0.0
   ipv6 address 2001:db8:1::1/64
   no shutdown

interface GigaEthernet1.0
   ipv6 address 2001:db9:1::1/64
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.0.1/24
   no shutdown

interface Tunnel0.0
   tunnel mode 4-over-6
   no tunnel adjust-mtu
   tunnel destination 2001:db8:1::2
   tunnel outgoing-interface GigaEthernet0.0 auto
   tunnel source 2001:db8:1::1
   ip unnumbered GigaEthernet1.0
   no shutdown

interface Tunnel1.0
   tunnel mode 4-over-6
   no tunnel adjust-mtu
   tunnel destination 2001:db9:1::2
   tunnel outgoing-interface GigaEthernet1.0 auto
   tunnel source 2001:db9:1::1
   ip unnumbered GigaEthernet1.0
   no shutdown
```

2.33.10 MAP-E の設定

MAP-E は、IPv4 通信を IPv4 over IPv6 にてカプセル化して通信することで、IPv6 サービス事業者経由で IPv4 インターネットに接続可能にする技術です。



2.33.10.1 利用環境

- 収容可能回線
  - Ver10.7以前は収容可能なMAP-Eサービス回線は1回線です。
  - Ver10.8以降は複数回線を収容可能です。

- Ver.10.1以降では株式会社JPIXが提供する「v6プラス」サービスに接続できます。
- Ver.10.2以降ではビッグローブ株式会社が提供するIPv6接続サービス「IPv6オプション」に接続できます。
- Ver10.2以降ではNTTコミュニケーションズ株式会社が提供する「OCNバーチャルコネクト」サービスに接続できます。
- 光回線終端装置(ONU)のほか、ひかり電話ルータを設置している環境では、IXルータはひかり電話ルータのLAN側に接続し、RA(設定例2)での設定を行ってください。また、ひかり電話ルータを複数段にまたがって設置している環境では利用できません。

※「v6プラス」は、株式会社JPIXの登録商標または商標です。
※「OCNバーチャルコネクト」は、NTTコミュニケーションズ株式会社の登録商標または商標です。
※「IPv6オプション」は、ビッグローブ株式会社の登録商標または商標です。

また、MAP-E で動的 IP アドレスの回線をご利用の場合は、あわせて以下もご確認ください。

- MAP-E(動的IPアドレス)では、複数のユーザに対し同一IPv4アドレスで異なる範囲のローカルポート番号が払い出されます。
  冗長構成で使用する場合、契約状況により同一IPv4アドレスが払い出される可能性がありますが、異なるローカルポート番号が払い出されるため問題ありません。
- 使用可能なローカルポートが限定されているため、特定ポート番号での待ち受けはできません。
- TCP、UDP、ICMP以外のポート番号をもたないプロトコルでの通信はできません。

- NAPT変換の動作が他のインタフェース上での動作と異なります。詳細はNATの設定ページを参照してください。

2.33.10.2 設定

MAP-E 接続のために、以下の設定が必要です。

tunnel mode map-e jpix/ocn	トンネルモード設定
ip address map-e	IP アドレス設定
ip napt enable	NAPT 設定

※注意事項
IPv6 アドレスを取得するインタフェースが複数存在する場合は、” tunnel outgoing-interface” の設定が必須となります。未設定時は動作保証しません。

【設定例 1】ひかり電話ルータを設置していない環境での設定例(v6 プラス)

ひかり電話ルータを設置していない環境では、IPv6 PD/RA 自動判別により、
ひかり電話契約の有無にかかわらず同一コンフィグで接続が可能です。

```
【設定例】

ip ufs-cache enable
ip route default Tunnel0.0
ip dhcp enable
ipv6 ufs-cache enable
!
proxy-dns ip request both
!
ip dhcp profile dhcp-lan
   default-gateway 192.168.0.254
   dns-server 192.168.0.254
!
ipv6 dhcp client-profile dhcpv6-cl
   option-request dns-servers
   ia-pd subscriber GigaEthernet2.0 ::/64 eui-64
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 autoselect enable
   ipv6 autoselect ra-delay 0
   ipv6 dhcp client dhcpv6-cl
   ipv6 nd proxy GigaEthernet2.0
   ipv6 traffic-class tos 0
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.0.254/24
   ip dhcp binding dhcp-lan
   proxy-dns ip enable
   ipv6 enable
   ipv6 dhcp server dhcpv6-sv
   ipv6 nd ra enable
   ipv6 nd ra other-config-flag
   no shutdown
!
interface Tunnel0.0
   tunnel mode map-e jpix
   ip address map-e
```

```
   ip tcp adjust-mss auto
   ip napt enable
   no shutdown
```

- proxy-dns ip request both
  IPv4 DNS 要求パケットを、IPv6 DNS サーバに問い合わせるために必要です。

- ia-pd subscriber GigaEthernet2.0 ::/64 eui-64
  MAP-E で利用する IPv6 アドレスのサブネット部が"00"になる必要があります。このため、ひかり電話契約ありの回線(DHCPv6 PD)で接続する場合の対応として、DHCPv6 PD アドレスの割り当て時に”::/64”を指定します。

- tunnel mode map-e jpix/ocn/ocn-fixed
  MAP-E のトンネルを指定します。
  ビッグローブ株式会社が提供する IPv6 接続サービス「IPv6 オプション」に接続する場合は、jpix を指定してください。
  NTT コミュニケーションズ株式会社が提供する「OCN バーチャルコネクト」の動的 IP アドレス回線に接続する場合は、ocn を指定してください。
  NTT コミュニケーションズ株式会社が提供する「OCN バーチャルコネクト」の 固定 1IP アドレス回線に接続する場合は、ocn-fixed を指定してください。
  複数固定 IP アドレス回線に接続する場合の設定例は、【設定例 3】を参照してください。

- ip address map-e
  MAP-E で指定された IPv4 アドレスを動的に割り当てる設定が必要です。

- ip napt enable
  MAP-E(動的 IP)での接続時には NAPT 有効化が必要です。
  ※IPv6アドレスをLAN側でも利用する場合は、ダイナミックフィルタの設定など適切なセキュリティ設定を行ってください。

【設定例 2】ひかり電話ルータを設置している環境での設定例(v6 プラス)

ひかり電話ルータを設置している環境では、IPv6 RA での設定を行ってください。
DHCPv6-PD では MAP-E が動作しません。

```
【設定例】

ip ufs-cache enable
ip route default Tunnel0.0
ip dhcp enable
ipv6 ufs-cache enable
!
proxy-dns ip request both
!
ip dhcp profile dhcp-lan
   default-gateway 192.168.0.254
   dns-server 192.168.0.254
!
ipv6 dhcp client-profile dhcpv6-cl
   information-request
   option-request dns-servers
!
interface GigaEthernet0.0
   ipv6 address autoconfig receive-default
```

```
   ipv6 dhcp client dhcpv6-cl
   ipv6 traffic-class tos 0
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.0.254/24
   ip dhcp binding dhcp-lan
   proxy-dns ip enable
   no shutdown
!
interface Tunnel0.0
   tunnel mode map-e jpix
   ip address map-e
   ip tcp adjust-mss auto
   ip napt enable
   no shutdown
```

- proxy-dns ip request both
  IPv4 DNS 要求パケットを、IPv6 DNS サーバに問い合わせるために必要です。

- tunnel mode map-e jpix/ocn/ocn-fixed
  MAP-E のトンネルを指定します。

- ip address map-e
  MAP-E で指定された IPv4 アドレスを動的に割り当てる設定が必要です。

- ip napt enable
  MAP-E(動的 IP)での接続時には NAPT 有効化が必要です。

※IPv6アドレスをLAN側でも利用する場合は、ダイナミックフィルタの設定など適切なセキュリティ設定を行ってください。

【設定例 3】OCN バーチャルコネクト複数固定 IP 回線の設定

OCN バーチャルコネクトで複数固定 IP アドレスのサービスを使用する際の設定例です。
ここではひかり電話ルータ設置環境でのご利用時の設定を行います。

```
【設定例】

ip ufs-cache enable
ip route default Tunnel0.0
ipv6 ufs-cache enable
ipv6 dhcp enable
!
proxy-dns ip enable
proxy-dns ip request both
!
ipv6 dhcp client-profile dhcpv6-cl
   information-request
   option-request dns-servers
!
ipv6 dhcp server-profile dhcpv6-sv
   dns-server dhcp
!
interface GigaEthernet0.0
   no ip address
   ipv6 enable
   ipv6 dhcp client dhcpv6-cl
   ipv6 nd proxy GigaEthernet1.0
   ipv6 traffic-class tos 0
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.10.10.1/29 (※)
   ipv6 enable
   ipv6 dhcp server dhcpv6-sv
   ipv6 nd ra enable
   ipv6 nd ra other-config-flag
   no shutdown
!
interface Tunnel0.0
   tunnel mode map-e ocn-fixed
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   no shutdown
!
```

- tunnel mode map-e ocn-fixed
  OCN バーチャルコネクトの固定 IP アドレストンネルを指定します。

- ip unnumbered GigaEthernet1.0
  複数固定 IP アドレスのサービスをご利用の場合、MAP-E トンネルでの IP アドレス設定は行わず、他のインタフェースをアンナンバード指定します。
  アンナンバード先のインタフェースで、インターネット事業者から指定されたグローバル IPv4 アドレスを手動で設定する必要があります。

【設定例 4】MAP-E2 回線収容時の設定

MAP-E2 回線収容時の設定例となります。

Tunnel インタフェースに”tunnel outgoing-interface”設定は必須となります。

```
【設定例】
ip ufs-cache enable
ip multipath per-flow-fix-interface
ip route default Tunnel0.0
ip route default Tunnel1.0

ipv6 ufs-cache enable
!
proxy-dns ip enable
proxy-dns ip request both
!
ipv6 dhcp client-profile dhcpv6-cl1
   information-request
   option-request dns-servers
!
ipv6 dhcp client-profile dhcpv6-cl2
   information-request
   option-request dns-servers
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 dhcp client dhcpv6-cl1
   ipv6 address autoconfig receive-default
   ipv6 traffic-class tos 0
   no shutdown
!
interface GigaEthernet1.0
   ipv6 enable
   ipv6 dhcp client dhcpv6-cl2
   ipv6 address autoconfig receive-default
   ipv6 traffic-class tos 0
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.1.254/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode map-e jpix
   tunnel outgoing-interface GigaEthernet0.0 auto
   ip address map-e
   ip tcp adjust-mss auto
   ip napt enable
   no shutdown
!
interface Tunnel1.0
   tunnel mode map-e jpix
   tunnel outgoing-interface GigaEthernet1.0 auto
   ip address map-e
   ip tcp adjust-mss auto
   ip napt enable
   no shutdown
```

- tunnel outgoing-interface GigaEthernet0.0 auto

  MAP-E を接続する物理インタフェースを指定してください。

2.33.10.3 MAP-E(動的 IP)での IPv4 VPN 設定

MAP-E(動的 IP)の IPv4 アドレスを使用して VPN を使用する際の設定例です。
ここではひかり電話ルータ設置環境でのご利用時の設定を行います。
また、MAP-E(動的 IP)の場合は以下に注意が必要です。

- MAP-E(動的IP)側がイニシエータである必要があります。
- MAP-E(動的IP)側がレスポンダの構成(L2TP/IPsecなど)はご利用になれません。
- 必ずNATトラバーサルを使用してください。

【MAP-E(動的 IP)側 設定例】

```
ip ufs-cache enable
ip route default Tunnel0.0
ip route 192.168.0.0/24 Tunnel10.0
ipv6 ufs-cache enable
!
proxy-dns ip enable
proxy-dns ip request both
!
ikev2 authentication psk id keyid ID_A key char key_A
ikev2 authentication psk id keyid ID_B key char key_B
!
ipv6 dhcp client-profile dhcpv6-cl
   information-request
   option-request dns-servers
!
ikev2 default-profile
   local-authentication psk id keyid ID_A
!
interface GigaEthernet0.0
   no ip address
   ipv6 address autoconfig receive-default
   ipv6 dhcp client dhcpv6-cl
   ipv6 traffic-class tos 0
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.1.254/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode map-e
   ip address map-e
   ip tcp adjust-mss auto
   ip napt enable
   no shutdown
!
interface Tunnel10.0
   tunnel mode ipsec-ikev2
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   ikev2 connect-type auto
   ikev2 ipsec pre-fragment
   ikev2 nat-traversal keepalive 20
   ikev2 outgoing-interface Tunnel0.0
   ikev2 peer 172.16.255.1 authentication psk id keyid ID_B
   no shutdown
```

【対向レスポンダ側 設定例】

```
!
ip ufs-cache enable
ip route default GigaEthernet0.1
ip route 192.168.1.0/24 Tunnel10.0
!
ikev2 authentication psk id keyid ID_A key char key_A
ikev2 authentication psk id keyid ID_B key char key_B
!
ppp profile wan
   authentication myname cl1@test.com
   authentication password cl1@test.com cl1_pass
!
ikev2 default-profile
   local-authentication psk id keyid ID_B
!
interface GigaEthernet1.0
   ip address 192.168.0.254/24
   no shutdown
!
interface GigaEthernet0.1
   encapsulation pppoe
   auto-connect
   ppp binding wan
   ip address 172.16.255.1/32
   ip napt enable
   ip napt static GigaEthernet0.1 udp 500
   ip napt static GigaEthernet0.1 udp 4500
   ip napt static GigaEthernet0.1 50
   no shutdown
!
interface Tunnel10.0
   tunnel mode ipsec-ikev2
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   ikev2 ipsec pre-fragment
   ikev2 nat-traversal keepalive 20
   ikev2 outgoing-interface GigaEthernet0.1
   ikev2 peer any authentication psk id keyid ID_A
   no shutdown
!
```

2.33.10.4 MAP-E(固定 IP)での IPv4 VPN 設定

MAP-E(固定 IP)の IPv4 アドレスを使用して VPN を使用する際の設定例です。
ここではひかり電話ルータ設置環境でのご利用時の設定を行います。
MAP-E(動的 IP)と異なり、レスポンダでの VPN 接続ができます。

【設定例】

```
ip ufs-cache enable
ip route default Tunnel0.0
ip access-list sec-list permit ip src any dest any
!
ipv6 ufs-cache enable
!
ike nat-traversal
!
ike proposal ike1 encryption aes-256 hash sha group 1024-bit
ike proposal ike2 encryption aes hash sha group 1024-bit
ike proposal ike3 encryption 3des hash sha group 1024-bit
!
ike policy ike-policy peer any key secret ike1,ike2,ike3
!
ipsec autokey-proposal sec1 esp-aes-256 esp-sha
ipsec autokey-proposal sec2 esp-aes esp-sha
ipsec autokey-proposal sec3 esp-3des esp-sha
!
ipsec dynamic-map ipsec-map sec-list sec1,sec2,sec3
!
ppp profile lns
   authentication request chap
   authentication password user-A@example.com password-1
   lcp pfc
   lcp acfc
   ipcp ip-compression
   ipcp provide-ip-address range 192.168.1.101 192.168.1.102
!
interface GigaEthernet0.0
   no ip address
   ipv6 dhcp client dhcpv6-cl
   ipv6 address autoconfig receive-default
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.1.1/24
   ip proxy-arp
   no shutdown
!
interface Tunnel0.0
   tunnel mode map-e ocn-fixed
   ip address map-e
   ip tcp adjust-mss auto
   ip napt enable
   ip napt static Tunnel0.0 udp 500
   ip napt static Tunnel0.0 udp 4500
   ip napt static Tunnel0.0 50
   no shutdown
!
```

```
interface Tunnel10.0
   ppp binding lns
   tunnel mode l2tp-lns ipsec
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   ipsec policy transport ipsec-map
   no shutdown
!
interface Tunnel11.0
   ppp binding lns
   tunnel mode l2tp-lns ipsec
   ip unnumbered GigaEthernet1.0
   ip tcp adjust-mss auto
   ipsec policy transport ipsec-map
   no shutdown
!
```

- ip napt static Tunnel0.0 udp 500
  MAP-E(固定 IP)で静的 NAPT など、各種 NAPT に関する設定を行う場合は
  MAP-E トンネルインタフェースに行います。

2.33.11 IPv6 国内標準プロビジョニング方式の設定

IPv6 国内標準プロビジョニング方式に対応した IPv4 over IPv6 トンネルの接続を行います。
以下のトンネル種別に対応しています。

トンネル種別	対応バージョン
DS Lite	Ver.10.8 以降
IPIP	Ver.10.8 以降

以下のプロバイダに対応しています。

- ビッグローブ株式会社（Ver.10.8以降）
- 株式会社朝日ネット（Ver.10.8以降）

上記プロバイダ以外でも、サーバ認証を行っていないサービスの場合は接続が可能です。

設定コマンドは以下になります。

tunnel mode	トンネルモードの選択
tunnel v6pv user	接続ユーザ名設定 （ユーザ名、パスワードの指定がある場合）
tunnel outgoing-interface	トンネルパケット送信先インタフェースの設定 （複数トンネルを設定する場合）
ip address v6pv	IP アドレスの設定
ip napt enable v6pv	NAPT 有効設定

IPv6 標準プロビジョニングが動作するためには、「tunnel mode」では「v6vp」を選択します。
「ip addres v6pv lan」の設定が必須となります。

設定例は以下になります。

【設定例】

```
ip ufs-cache enable
ip route default Tunnel0.0
ip dhcp enable
ipv6 ufs-cache enable
!
proxy-dns ip request both
!
ip dhcp profile dhcp-lan
   default-gateway 192.168.0.254
   dns-server 192.168.0.254
!
ipv6 dhcp client-profile dhcpv6-cl
   option-request dns-servers
   ia-pd subscriber GigaEthernet1.0 ::/64 eui-64
!
interface GigaEthernet0.0
   ipv6 enable
   ipv6 autoselect enable
   ipv6 autoselect ra-delay 0
```

```
   ipv6 dhcp client dhcpv6-cl
   ipv6 nd proxy GigaEthernet1.0
   ipv6 traffic-class tos 0
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.0.254/24
   ip dhcp binding dhcp-lan
   proxy-dns ip enable
   ipv6 enable
   ipv6 dhcp server dhcpv6-sv
   ipv6 nd ra enable
   ipv6 nd ra other-config-flag
   no shutdown
!
interface Tunnel0.0
   tunnel mode v6pv
   ip address v6pv lan GigaEthernet1.0
   ip napt enable v6pv
   no shutdown
```

- ip address v6pv lan
  unnumbered にて使用する LAN インタフェース、複数固定 IP 時にアドレスを割り当てる LAN インタフェースを指定します。
- ip napt enable v6pv
  v6pv を設定した場合は、IPIP(固定 IP1)の場合に NAPT が有効になります。

  ※注意事項
  IPv6 アドレスを取得するインタフェースが複数存在する場合は、” tunnel outgoing-interface” の設定が必須となります。未設定時は動作保証しません。

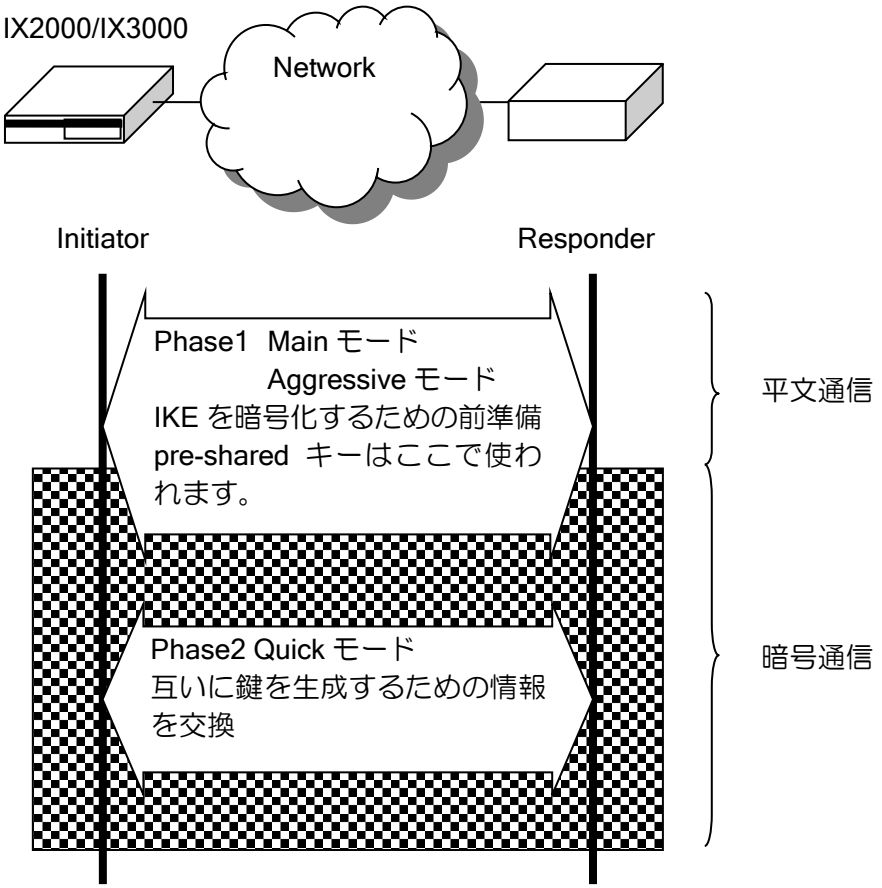
■2.34 IKE の設定

IKE（Internet Key Exchange）は、鍵交換プロトコルのことで、IPsec 通信を行う通信相手（ピア）との鍵を自動的に生成するために使用します。IX2000/IX3000 では、通信相手のアドレスが不定の場合についてもサポートしております。

IKE（RFC2409）には、Phase1 として Main モードと Aggressive モード、Phase2 として Quick モードが定義されており、IX2000/IX3000 でサポートされております。この他、New Group モードが定義されていますが、IX2000/IX3000 ではサポートしておりません。

また、NAT トラバーサル機能に対応しています。こちらの詳細は IPsec の章を参照してください。

【構成



Aggressive モードと Main モードとの違いは次の通りです。

- Main モード

安全な通信が確立されるまで ID を暗号化して保護します。事前共有鍵は通信相手ごとに選択する必要がありますが、相手を識別するための情報が IP アドレスしか利用できないため、IP アドレスが動的に変化する環境では使用できません。

- Aggressive モード

ID を暗号化せずに開示することで、受信側はどの事前共有鍵を使用するかをアドレスではなく ID 情報から判断することができます。これにより、動的アドレス環境やアドレス変換の場合にも IKE のネゴシエーションを行うことができます。また Main モードと比較して Phase1 の一部のス

テップが省略されるため、IKE のネゴシエーションが高速化されます。

2.34.1 IKE の基本設定

Phase1 では、IKE プロトコル自身を暗号化するための前準備を行います。Phase2 では、鍵を生成するための情報を実際に交換します。Phase1 および Phase2 で使用できる ID 情報は以下のとおりです。

- Phase1

  下記の ID が選択可能です。

ID_IPV4_ADDR, ID_IPV6_ADDR	IPv4/IPv6 ソースアドレス
ID_KEY_ID	任意文字列
ID_FQDN	ドメイン名
ID_USER_FQDN	ユーザ名付きドメイン名

※ DNS リゾルバを利用してドメイン名を自動設定することはできません。

- Phase2

デフォルトとして ipsec autokey-map コマンドで指定したアクセスリストの src, dest のネットワークアドレスを ID に使用する以外に、コマンドで下記の ID を設定できます。

ID_IPV4_ADDR, ID_IPV6_ADDR	IPv4/IPv6 アドレス
ID_IPV4_ADDR_SUBNET ID_IPV6_ADDR_SUBNET	IPv4/IPv6 ネットワークアドレス

IKE を設定する際に使用される用語について説明します。

- ポリシー
  - ✧ 鍵交換を実行するか否かを決定するもの
- プロポーザル
  - ✧ 鍵交換を実行する場合の手段やアルゴリズムなどを決定するもの
- pre-shared キー（事前共有鍵）
  - ✧ Initiator と Responder が互いに共有する事前鍵。（pre-shared キーを使用することで、接続相手の確認を行うことができます。）
- DH グループ
  - ✧ Diffie-Hellman 計算式の分母に相当する値のビット長

(a) IKE ポリシー

IKE ポリシーは、どの通信相手とどのプロポーザルで IKE 処理するか等を決定するもので、以下の設定項目があります。

- IKE 通信相手アドレス
- 事前共有鍵の設定
- モード選択
- ID の選択
- IKE プロポーザル選択

IKE ポリシーの設定は、次のコマンドを使用します。

ike policy	IKE ポリシーの設定
ike local-id	IKE の自側 ID（IKE Phase 1）の設定
ike remote-id	IKE の相手側 ID（IKE Phase 1）の設定
ipsec local-id	IPsec の自側 ID（IKE Phase 2）の設定
ipsec remote-id	IPsec の相手側 ID（IKE Phase 2）の設定
show ike policy	IKE ポリシーの確認

show ike sa	IKE SA 状態の確認

(b) IKE プロポーザルおよびクイック設定

IKE プロポーザルは、IKE で使用する暗号/認証アルゴリズム、自動鍵の有効期限、DH グループ値等を決定します。

IKE プロポーザルの設定は、次のコマンドを使用します。

ike proposal	プロポーザルの設定
show ike proposal	プロポーザルの確認

IKE ポリシー入力時、IKE プロポーザル名の設定を省略した場合、自動的に以下のプロポーザルが使用されます。

暗号アルゴリズム	DES
認証アルゴリズム	MD5
認証手段	pre-shared
PFS	DH グループ:768 bit
鍵の有効期限	28800 秒

【構成例】

IKE の設定
暗号アルゴリズム　3des
認証アルゴリズム　sha1
認証手段　pre-shared(default)
PFS　DH グループ:768 bit(default)

【設定例】

```
ike proposal ikeprop encryption 3des hash sha
ike policy policy1 peer 10.2.2.2 key xxxxxxxx ikeprop
```

(c) アルゴリズム

IX2000/IX3000 シリーズの IKE では、以下のアルゴリズムをサポートしています。

暗号アルゴリズム	DES-CBC Triple DES-CBC AES-CBC 128bit AES-CBC 192bit、256bit（Ver8.1 以降）
認証アルゴリズム	HMAC-MD5-96 HMAC-SHA1-96 HMAC-SHA2-256（Ver.8.6 以降） HMAC-SHA2-384（Ver.8.6 以降） HMAC-SHA2-512（Ver.8.6 以降）

2.34.1.1 宛先の FQDN 指定（Ver.8.8 以降）

Ver.8.8 以降、宛先を FQDN で指定することが可能です。指定した FQDN の名前解決を行い対応したアドレスを宛先として使用します。宛先の FQDN 指定を利用することにより、不定アドレス同士での接続が可能となります。詳細は DNS の項を参照してください。

名前解決の契機、アドレス更新時の動作、未解決時の動作は以下のとおりです。

名前解決の契機	定期的な更新 全ての SA が削除された場合
アドレス更新時の動作	該当する SA を削除
名前未解決時の動作	SA 作成不可

設定例は以下のとおりです。

【設定例】
宛先を host1.example.com で指定

```
ip access-list acl permit ip src any dest any

ike proposal ike-prop encryption aes hash sha
!
ike policy ike-policy peer-fqdn-ipv4 host1.example.com key secret ike-policy
ike keepalive ike-policy 10 3

ipsec autokey-proposal sec-prop esp-aes esp-sha

ipsec autokey-map sec-map acl peer-fqdn-ipv4 host1.example.com sec-prop

interface Tunnel0.0
   tunnel mode ipsec
   ip address 10.0.0.1/30
   ipsec policy tunnel sec-map out
   no shutdown
```

2.34.2 対向装置の監視

IX2000/IX3000 シリーズでは、対向装置の監視の機能として、以下の 2 つの機能があります。

- IKE キープアライブ
- ネットワークモニタを利用した監視

2.34.2.1 IKE キープアライブ機能

IKE キープアライブ機能は相手の生存を常に監視する機能です。

IPsec リモートアクセスの場合など、一方のアドレスが動的に変化する環境の場合には、相手の存在を常に監視しておく必要があります。

この機能を使用しない場合、例えばセンタ側ルータがリブートしたときに、センタ側ルータは自身のリブートをアドレス不定の拠点側ルータに通知する手段がありません。このため拠点側ルータの SA は削除されず、センタ側ルータと拠点側ルータの状態がずれてしまい、IPsec による通信が停止してしまいます。

IX2000/IX3000 の IKE キープアライブ機能は RFC3706 に基づく仕様です。IX2000/IX3000 同士の接続確認のみ行っております。

設定・確認コマンドは次のとおりです。

ike keepalive	IKE キープアライブの設定
show ike keepalive	IKE キープアライブ設定の表示

IX2000/IX3000 の IKE キープアライブ機能は、片方向のみキープアライブを行う、パッシブモードの動作が可能です。

- パッシブモード動作
  IKE キープアライブを使用しない設定でも、自身が IKE キープアライブをサポートしていることを表明します。このため、対向装置に IKE キープアライブを行う設定がされている場合、対向装置の IKE キープアライブは動作します。IX2000/IX3000 シリーズは、対向装置から受信した keepalive に対して keepalive-ack を返します。

2.34.2.2 ネットワークモニタ機能を利用した相手装置監視

前項のキープアライブ機能をサポートしていない装置と対向している場合には、ネットワークモニタ機能を利用することにより、同様な監視を行うことが可能となります。

ネットワークモニタ機能では、ICMP echo を送信し、ICMP echo reply を受信することにより、相手装置の生存確認を行います。相手装置との通信が不可になった場合には、SA の削除を行います。

ネットワークモニタ機能については、ネットワークモニタの項を参照してください。

action ipsec clear-sa	監視異常時の SA の削除 （watch グループコンフィグモード）

【設定例】
相手装置（192.168.0.2）の監視を行い、障害発生時に SA の削除を行う
（IKE／IPsec の設定は省略します）

```
watch-group ipsec-keepalive 10
  event 10 ip unreach-host 192.168.0.2 Tunnel0.0
  action 10 ipsec clear-sa Tunnel0.0
!
network-monitor ipsec-keepalive enable
```

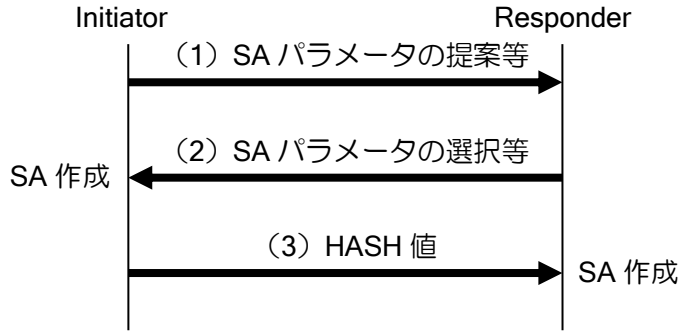
2.34.3 commit-bit 対応

IKE フェーズ 1 において commit-bit を使用することにより、Initiator と Responder の SA 状態不一致が発生する可能性を低下させることができます。

本機能は Aggressive モードの Responder において設定する場合のみ有効です。Main モードの場合もしくは Initiator での動作についてはサポートしていません。

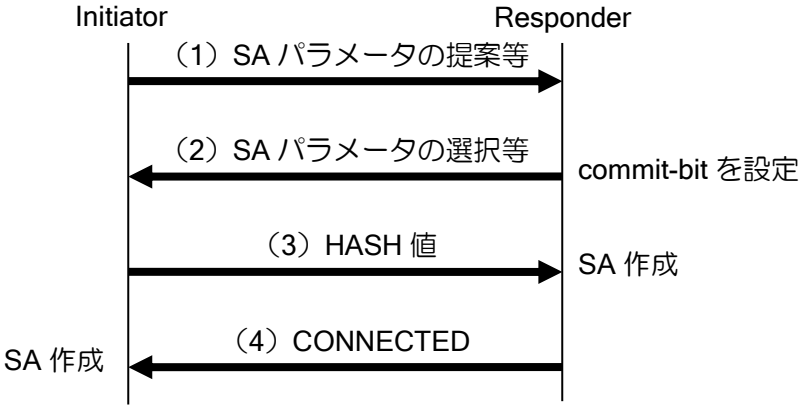
以下に commit-bit の動作を説明します。

Aggressive モード使用時の通常のシーケンスは、次のようになります。



このシーケンスにおいて、(3) を Responder が受信できなかった場合、Responder では SA が作成されませんが、Initiator では Responder が（3）を受信しなかったことの確認を行う手段が無いため、SA は作成されたままとなり、Initiator と Responder で SA の状態の不一致が発生します。

このような SA 状態不一致の発生する可能性を低下させるために、commit-bit を使用します。commit-bit を使用した場合のシーケンスは次のようになります。



commit-bit を使用した場合、Responder は commit-bit 使用フラグを設定し（2）を送信します。そして、(3) を受信後に SA を作成し、(4) を送信します。

Initiator は、commit-bit を使用する場合には、(4) を受信後、SA の作成を行います。また（4）を受信できない場合、(3) を再送信します。

これにより Initiator では（3）の応答確認後、SA の作成を行うことができるので、Responder で（3）を受信できなかった場合でも SA の状態不一致の発生を防ぐことができます。

設定コマンドは次の通りです。

ike commit-bit	commit-bit 使用の設定
ike retransmit-count	IKE パケットの再送回数の設定
ike retransmit-interval	IKE パケットの再送間隔の設定

commit-bit の設定は Responder でのみ行います。Initiator で設定した場合、設定は無視されます。

【設定例】

```
ike commit-bit ike_policy1
```

commit-bit を使用した場合でも SA の状態不一致を完全に防ぐことはできません。例えば、以下の場合には SA の状態不一致が発生します。

（4）を Initiator が受信できなかった場合、Responder では Initiator が（4）を受信したことを知る手段が無いため Responder には SA があり、Initiator には SA が無い状態となり、状態不一致が発生します。

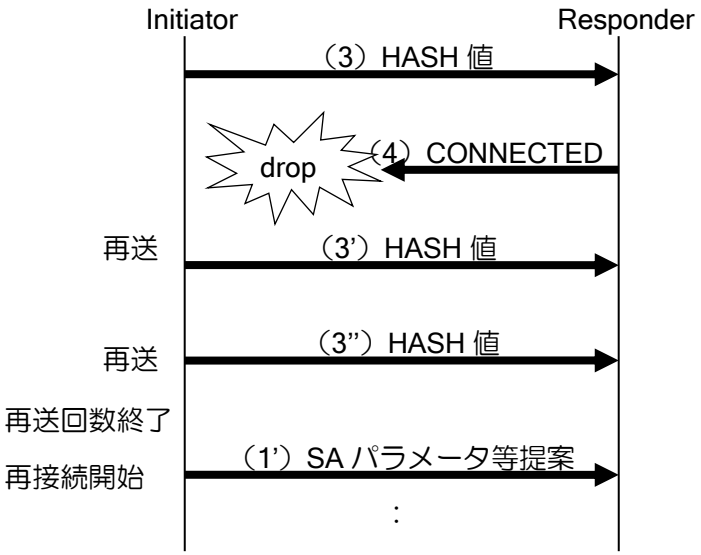
この状態の場合、Initiator は指定回数再送を行いますが、Responder は SA 作成済みなので（4）の再送は行いません。したがって、そのまま再送回数が終了しますので、SA 状態の不一致が発生します。

このような場合の状態不一致を解消するために、再送回数が終了した場合に自動で再接続を行います（IKE 自動再接続機能）。

以下の状態になると、再接続機能は停止します。

- CLI による SA 削除
- DELETE メッセージ受信による SA 削除
- 当該ピアとの別 Phase1 接続完了

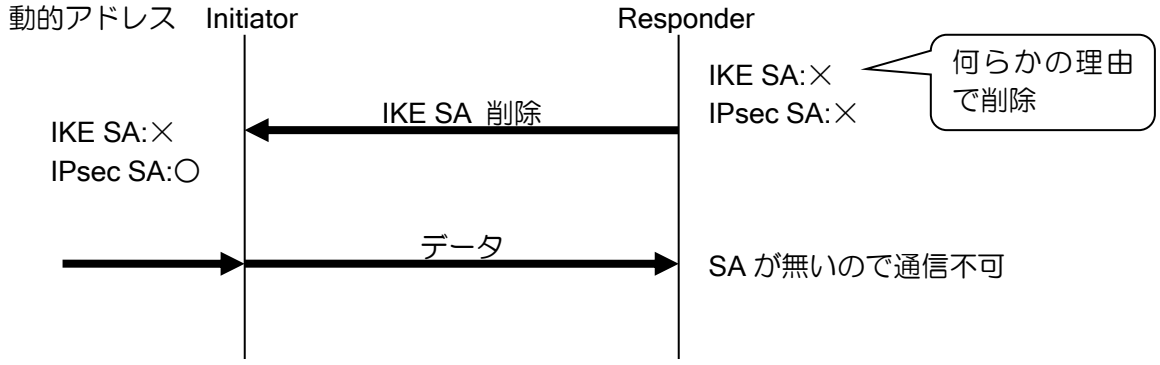
設定はありませんので、自動で再接続を行います。



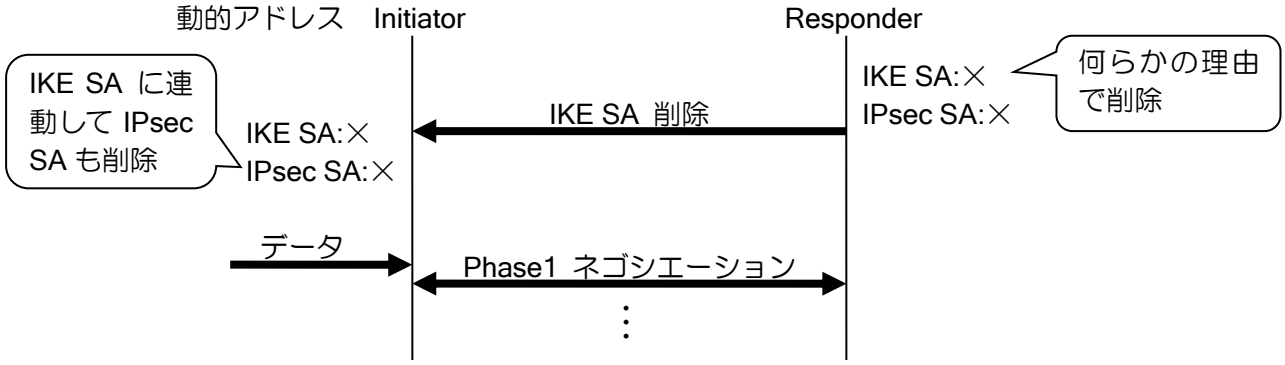
2.34.4 Dangling SA 型/Continuous-channel SA 型

SA の管理方式には、IKE SA と IPsec SA を独立に管理する、Dangling SA 型と、IKE SA と IPsec SA が連動する Continuous-channel SA 型があります。IX2000/IX3000 シリーズでは、Dangling SA 型で動作しています。

Dangling SA 型の場合には、オペレーションミス等により、一方の IKE SA、IPsec SA ともに削除され、もう一方の IPsec SA のみが残る状態となる場合が考えられます。動的アドレス環境で使用する場合、Initiator 側の IPsec SA のみが残った状態となると、IPsec SA のライフタイムが満了するか、IPsec SA を削除しなければ、通信はできない状態となります。



Continuous-channel SA 型では、IKE SA と IPsec SA が連動するため、IKE SA が削除されると IPsec SA が削除されます。従って、上記のように、動的アドレス環境において、Initiator の IPsec SA のみが残り、通信不可となる状態に陥ることを回避することができます。



Continuous-channel SA 型の設定コマンドは次の通りです。

ike suppress-dangling	Dangling SA の抑止設定

【設定例】

```
ike policy policy1 peer 192.168.0.2 key KEY
ike suppress-dangling policy1
```

2.34.5 リキー設定

SA のライフタイム満了時に、新たに SA の再生成を行います（リキー）。IKE SA は、デフォルトではライフタイム満了の 30 秒前に、リキーを行います。

Ver.8.1 以降、リキー開始タイミングの設定の変更ができます。

設定は次のとおりです。

ike rekey remaining-lifetime	IKE SA リキータイミングの設定

【設定例】
全ポリシーのリキーを 300 秒前に行う。

```
ike rekey remaining-lifetime default second 300
```

特定ポリシー（policy1）のリキーを 300 秒前に行う。

```
ike policy policy1 peer 192.168.0.2 key KEY
ike rekey remaining-lifetime policy policy1 second 300
```

2.34.6 DELETE 送信抑止設定

Ver.9.4 以降、SA 削除時の DELETE メッセージの送信を抑止することができます。

設定は次のとおりです。

no ike send-delete	DELETE 送信抑止の設定

【設定例】
SA 削除時の DELETE メッセージの送信を抑止する。

```
no ike send-delete
```

■2.35 IPsec の設定

IPsec には、データの完全性を保持するための認証ヘッダ（AH:Authentication Header）と、データの機密性を保持するための暗号ペイロード（ESP：Encapsulated Security Payload）の機能があり、IX2000/IX3000 はいずれもサポートします。

また、IPsec には、トンネルモードによる転送と、トランスポートモードによる転送方式があり、IX2000/IX3000 はどちらもサポートします。

- アドレスが動的に変化するリモートアクセス環境でも利用できます。
- トンネルインタフェースを利用して IPsec を設定できます。トンネルインタフェースを利用することで、冗長構成やルーティングプロトコルの併用が可能になります。
- EtherIP や GRE と組み合わせて非 IP パケットを暗号化することができます。
- NAT トラバーサル機能が利用可能です。

IPsec を設定する際に使用される用語について説明します。

- SA（Security Association）
  - IPsec を実施する装置間で合意する内容
- ポリシー
  - 鍵交換を実行するか否かを決定するもの
- プロポーザル
  - 鍵交換を実行する場合の手段やアルゴリズムなどを決定するもの
- 固定鍵
  - IPsec で通信する装置が互いに共有する鍵
- 自動鍵
  - IPsec で通信する装置が、IKE を使用して自動的に生成された鍵（IKE については、IKE の節を参照してください。）
- PFS（Perfect Forward Secrecy）のための DH グループ値
  - PFS を使用するとよりセキュリティが高くなります。

2.35.1 IPsec の基本設定

(a) IPsec ポリシー

IPsec ポリシーは、どのモードで IPsec 処理するか等を決定するもので、以下の設定項目があります。

- モード選択
  - トンネルモード、トランスポートモードのいずれかを選択します。
- インタフェース指定
  - IPsec 処理を実施するパケットの受信インタフェースを選択します。
- 鍵のポリシー選択

IPsec ポリシーの設定は、次のコマンドを使用します。

ipsec policy	IPsec ポリシーの設定 （インタフェースコンフィグモード）
show ipsec policy	IPsec ポリシーの確認

(b) 自動鍵ポリシーと自動鍵プロポーザルおよびクイック設定

自動鍵ポリシーは、どのパケットをどの自動鍵で IPsec を実施するかを決定するもので、以下の設定項目があります。

- アクセスリスト名
  - アクセスリストにより、IPsec 処理を実施するパケットを選択します。トンネルインタフェースに IPsec を設定する場合は通常 src any dest any で設定してください。
  - アクセスリスト設定時、ワイルドカードビット指定は使用しないでください。
  - IPsec の ID の設定を省略した場合、アクセスリストのアドレスが IPsec の ID に使用されます。ID の設定を省略する場合は、対向装置と対になるように設定してください。
  - IPv4，IPv6 の選択もアクセスリストにより行います。IPv4，IPv6 で同じアクセスリスト名が存在する場合は、IPv4 のアクセスリストが使用されます。
- IPsec 通信相手アドレス
- PFS 値
- セキュリティレベル
  - 送受信時の IPsec 使用のレベルを設定します。
  - アクセスリストにマッチするトラフィックが対象となります。

use	送信	IPsec を行います。SA が無ければ SA を作成します。
	受信	IPsec の有無に関係なく受信します。
require	送信	IPsec を行います。SA が無ければ SA を作成します。
	受信	IPsec されていないパケットは廃棄します。

また、自動鍵プロポーザルは、IPsec で使用する暗号/認証アルゴリズムおよび自動鍵の有効期限を決定します。

自動鍵ポリシーと自動鍵プロポーザルの設定は、次のコマンドを使用します。

ipsec autokey-map	自動鍵ポリシーの設定
ipsec dynamic-map	自動鍵ダイナミックポリシーの設定
ipsec autokey-proposal	自動鍵プロポーザルの設定
ipsec sa-autorefresh	自動鍵の自動更新の有効/無効
show ipsec autokey-map	自動鍵ポリシーの確認
show ipsec dynamic-map	自動鍵ダイナミックポリシーの確認
show ipsec autokey-proposal	自動鍵プロポーザルの確認
show ipsec sa-autorefresh	自動鍵の自動更新の有効/無効の確認

自動鍵ポリシー入力時、自動鍵プロポーザル名の設定を省略した場合、自動的に以下のプロポーザルが使用されます。

ESP 暗号アルゴリズム	DES-CBC
ESP 認証アルゴリズム	HMAC-MD5-96
PFS	Off
鍵の有効期限	28800 秒

なお、自動鍵は IKE と連係した設定を行う必要があります。IKE については、IKE の節に詳細を記述します。

(c) 固定鍵ポリシーと固定鍵

固定鍵ポリシーには、どのパケットをどの固定鍵で IPsec を実施するかを決定するもので、以下の設定項目があります。

- アクセスリスト名
  - アクセスリストにより、IPsec 処理を実施するパケットを選択します。
- IPsec 通信相手アドレス
- 受信用鍵の指定
- 送信用鍵の指定
- セキュリティレベル
  - 送受信時の IPsec 使用のレベルを設定します。
  - アクセスリストにマッチするトラフィックが対象となります。

use	送信	IPsec を行います。SA が無ければ SA を作成します。
	受信	IPsec の有無に関係なく受信します。
require	送信	IPsec を行います。SA が無ければ SA を作成します。
	受信	IPsec されていないパケットは廃棄します。

また、固定鍵は、鍵および IPsec で使用する暗号/認証アルゴリズム等を決定します。

ipsec manualkey-map	固定鍵ポリシーの設定
ipsec manualkey	固定鍵の設定
show ipsec manualkey-map	固定鍵ポリシーの確認
show ipsec manualkey	固定鍵の確認

(d) アルゴリズム

IX2000/IX3000 シリーズの IPsec では、以下のアルゴリズムをサポートしています。

ESP 暗号アルゴリズム	DES-CBC Triple DES-CBC AES-CBC 128bit AES-CBC 192bit、256bit （Ver.8.1 以降） NULL
ESP 認証アルゴリズム	HMAC-MD5-96 HMAC-SHA1-96 HMAC-SHA2-256（Ver.8.6 以降） HMAC-SHA2-384（Ver.8.6 以降） HMAC-SHA2-512（Ver.8.6 以降）
AH 認証アルゴリズム	HMAC-MD5-96 HMAC-SHA1-96 HMAC-SHA2-256（Ver.8.6 以降） HMAC-SHA2-384（Ver.8.6 以降） HMAC-SHA2-512（Ver.8.6 以降）

2.35.1.1 DF ビット対応

IPsec ではパケットの DF ビットを設定により直接操作することができます。

IPsec のカプセル化によってパケットサイズがインタフェースの MTU を超過した場合、オリジナルパケットの DF ビットがセットされていなければフラグメントしてパケットを送信します。また、DF ビットがセットされていれば、ICMP エラーによって IPsec を考慮した MTU 値をホストに通知します（Path MTU Discovery 機能）。Path MTU Discovery 機能が使用できないネットワークでは、フラグメント禁止パケットが通信不可となりますので、必要に応じてこの機能を抑止することも可能です。

これらの設定は以下のコマンドで行います。

ipsec policy ... df-bit	DF ビット設定

このソフトのバージョンに応じて動作が異なります。それぞれの設定を確認してください。

auto, on, off	カプセル化した後の DF ビットを設定します。 auto はオリジナルパケットの DF ビットの情報を引き継ぎます。 DF ビットが 1 の場合、MTU サイズ以上のパケットを受信すると送信元宛に ICMP パケット（Fragment needed but df-bit is set）を送信します。
ignore	DF ビットによらず、MTU サイズ以上のパケットをフラグメントして送信します。その際 DF ビットは必ず 0 にします。

※デフォルトは off で設定されています。

2.35.1.2 commit-bit 対応

IKE フェーズ 2 において commit-bit を使用することにより、Initiator と Responder の SA 状態不一致が発生する可能性を低下させることができます。
本機能は Responder において設定する場合のみサポートしています。

動作については、IKE の場合と同様ですので、「IKE の設定」の章を参照してください。

設定は以下のコマンドで行います。

ipsec commit-bit	commit-bit 使用の設定

commit-bit の設定は Responder でのみ行います。Initiator で設定した場合、設定は無視されます。クイック交換を行う装置を使用する場合は、commit-bit 設定時に quick-mode を指定してください。また、再送回数，再送間隔は、ike retransmit-count,ike retransmit-interval コマンドでの設定と同じ値が使用されます。変更する場合は、これらのコマンドを使用してください。

【設定例】

個別に交換を行う装置と対向する場合

```
ike retransmit-count 20
ipsec commit-bit ipsec_policy1
```

クイック交換を行う装置と対向する場合

```
ike retransmit-count 20
ipsec commit-bit ipsec_policy1 quick-mode
```

2.35.1.3 Anti-Replay 機能の無効化

Anti-Replay 機能を無効化することができます。IPsec では、シーケンス番号を監視し、重複して受け取ったパケットを廃棄することによりリプレイ攻撃からの防御を行います。Anti-Replay 機能を無効化することにより、受信時のシーケンス番号の監視を行いません。

QoS と IPsec を併用している場合、プライオリティキューイングによりパケットが間引きされるためシーケンス番号の監視が行き届かなくなります。この結果、リプレイ攻撃と誤認しパケットを廃棄する場合があります。このような場合は、Anti-Replay 機能を無効化することにより、パケットの廃棄を防ぐことができます。

デフォルトでは、Anti-Replay 機能は有効になっています。これを無効にすることは、セキュリティホールとなる可能性がありますので、無効化の設定を行う場合には使用環境を十分考慮する必要があります。

設定は以下のコマンドで行います。

ipsec anti-replay	Anti-Replay 防御機能の有効/無効化

【設定例】
Anti-Replay の無効化

```
no ipsec anti-replay policy1
```

2.35.1.4 DELETE 送信機能

復号できないパケットを受信した場合に、相手装置に対し DELETE メッセージを送信する機能です。

IKE はデータ転送プロトコルとして UDP を使用します。従って、IKE パケットがやり取りされるときには、エンドツーエンドのコネクションは張られません。失われた IKE パケットがプロトコルレベルで確認されないため思わぬ事態を引き起こす可能性があります。例えば、IKE 接続状態にある装置間の片方の IPsec SA 情報が何らかの要因で消えてしまったとき、ほとんどの場合は、IPsec SA 削除通知（DELETE メッセージ）を送信することで、もう片方の装置は接続相手の IPsec SA 情報が消えたことを知ります。しかし、信頼性のない UDP によるこの通知が確実に届くとは限りません。届かなかった場合、IPsec SA 情報がある装置は相手に IPsec SA 情報が無いことを知らずに暗号パケットを送信し続け、相手装置は復号できず受信できない状態になります。

もし、暗号パケットを送信する側が不定アドレスを持つ装置ならば、IPsec SA を持たない装置は、接続を開始することができずに相手からの再接続（Re-key）まで待つしかない状態となります。この様な状態で復号できないパケットを一定時間に一定回数受信した場合に、相手装置に対し削除通知（DELETE メッセージ）を再度送信します。削除通知（DELETE メッセージ）を確実に受け取った場合、IPsec SA 情報がある装置は、IPsec SA を削除し再接続を開始することで IPsec 通信が復旧します。

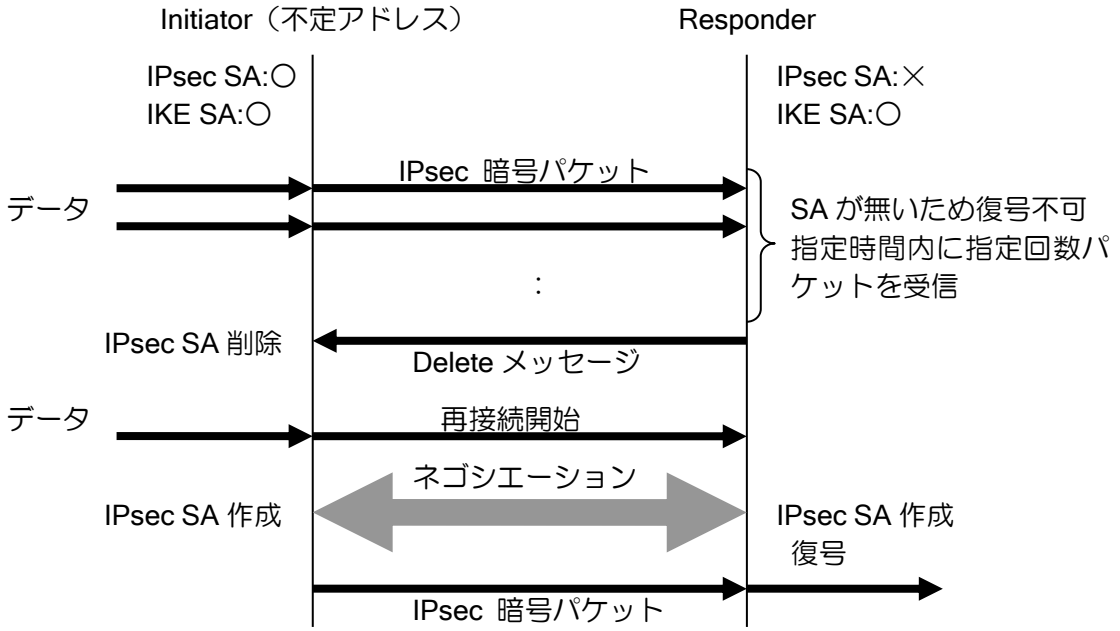
DELETE 送信機能は、相手装置に無効な IPsec SA 情報を削除させる機能です。ただし、DELETE メッセージを送信できるのは IKE SA が存在しているときのみです。

設定／確認コマンドは次のとおりです。

ipsec delete-notify	SA 削除要求送信の設定
show ipsec delete-notify	SA 削除要求送信の表示

【設定例】
30 秒間に 100 パケットを受信した場合に、DELETE メッセージを送信

```
ipsec delete-notify 100 30
```



2.35.1.5 不定アドレス宛フェーズ 2 開始機構

IKE SA が存在し、IPsec SA が存在しない状態で、不定アドレス宛のデータの送信を行う場合に、IKE SA の情報を利用し自装置からフェーズ 2 のネゴシエーションを開始する機能です。

パケット受信時、指定した IKE SA の情報から相手アドレスを調べ、自装置からフェーズ 2 の接続を行うことができます。これにより、IPsec SA が作成され、再度通信を行うことができます。

Ver.8.6 以降は、指定した IKE ポリシーに一致する相手からのみフェーズ 2 の接続させるように指定することができます。

設定は、自動鍵ダイナミックポリシーの設定コマンドを使用します。

ipsec dynamic-map	自動鍵ダイナミックポリシーの設定

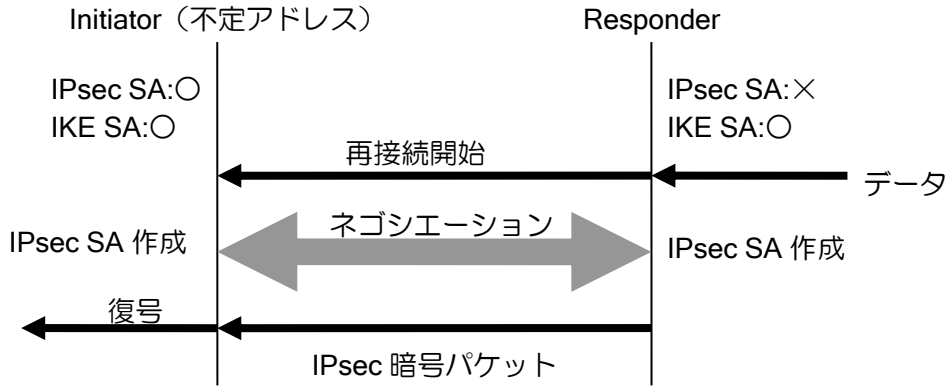
【設定例】

IKE ポリシーを自装置からの接続のみ使用

```
ipsec dynamic-map policy1 alist ike ikepolicy
```

IKE ポリシーを対向装置からの接続にも使用（Ver.8.6 以降）

```
ipsec dynamic-map policy1 alist ike-binding ikepolicy
```



不定アドレス宛フェーズ 2 開始機能の有無による、アグレッシブモード使用時の Responder 側(固定 IP 側)の SA 状態とトンネルインタフェース状態を以下に示します。

不定アドレス宛 フェーズ 2 開始機能	IPsec SA ○ IKE SA ○	IPsec SA ○ IKE SA ×	IPsec SA × IKE SA ○	IPsec SA × IKE SA ×	インタフェース スダウン
有り	up	up	up	up	down
無し	up	up	down	down	down

2.35.1.6 リキー設定

デフォルトではライフタイム満了の 1 分前、また、リキー開始までに該当 SA を使用して通信が行われた場合に、IPsec-SA のリキーを行います。

Ver.8.1 以降、リキー開始タイミングの設定の変更、通信の有無によらずリキーする設定ができます。

設定は次のとおりです。

ipsec rekey remaining-lifetime	IPsec SA リキータイミング設定
ipsec rekey unconditional-rekeying	IPsec SA 無通信リキー設定

【設定例】

全ポリシーのリキーを 120 秒前に行う。
ipsec rekey remaining-lifetime default second 120

特定ポリシー（map1）のリキーを 180 秒前に行う
ipsec rekey remaining-lifetime policy map1 second 180

通信が無くても SA のリキーを行う。
ipsec rekey unconditional-rekeying

リキー開始タイミング設定は、ライフタイムの 1/2 以下の値を設定してください。ライフタイムの 1/2 以上の値を設定した場合、ライフタイムの 1/2 の値で動作します。

2.35.1.7 宛先の FQDN 指定（Ver.8.8 以降）

Ver.8.8 以降、宛先を FQDN で指定することが可能です。指定した FQDN の名前解決を行い対応したアドレスを宛先として使用します。宛先の FQDN 指定を利用することにより、不定アドレス同士での接続が可能となります。詳細は DNS の項を参照してください。

名前解決の契機、アドレス更新時の動作、未解決時の動作は以下のとおりです。

名前解決の契機	定期的な更新
アドレス更新時の動作	該当する SA を削除
名前未解決時の動作	SA 作成不可

設定例は以下のとおりです。

```
【設定例】
宛先を host1.example.com で指定

ip access-list acl permit ip src any dest any

ike proposal ike-prop encryption aes hash sha
!
ike policy ike-policy peer-fqdn-ipv4 host1.example.com key secret ike-policy
ike keepalive ike-policy 10 3

ipsec autokey-proposal sec-prop esp-aes esp-sha

ipsec autokey-map sec-map acl peer-fqdn-ipv4 host1.example.com sec-prop

interface Tunnel0.0
   tunnel mode ipsec
   ip address 10.0.0.1/30
   ipsec policy tunnel sec-map out
   no shutdown
```

2.35.1.8 IKE フェーズ２ ID 送信なし機能

Ver9.7 以降、IKE フェーズ２のネゴシエーションに ID を含めないように設定することが可能です。 この設定を行うことにより、IKE フェーズ２のネゴシエーションに ID が利用できない装置への接続が可能となります。

以下のコマンドのパラメータ、without-id-payload を設定してください。

ipsec policy	IKE フェーズ２ ID 送信なし設定（Ver9.7 以降）

設定例は以下のとおりです。

```
【設定例】

interface Tunnel0.0
   tunnel mode ipsec
   ip address 10.0.0.1/30
   ipsec policy tunnel sec-map without-id-payload out
   no shutdown
```

2.35.2 トンネルモード

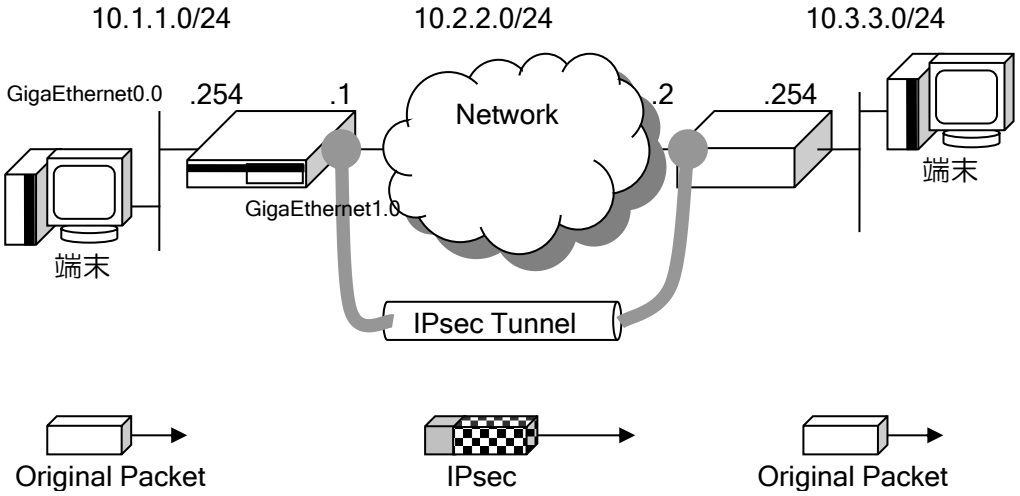
トンネルモードは、主にネットワーク対ネットワークでのセキュリティを確保するためのモードで、通常のパケット転送時にパケットすべてをカプセル化して転送する機能です。

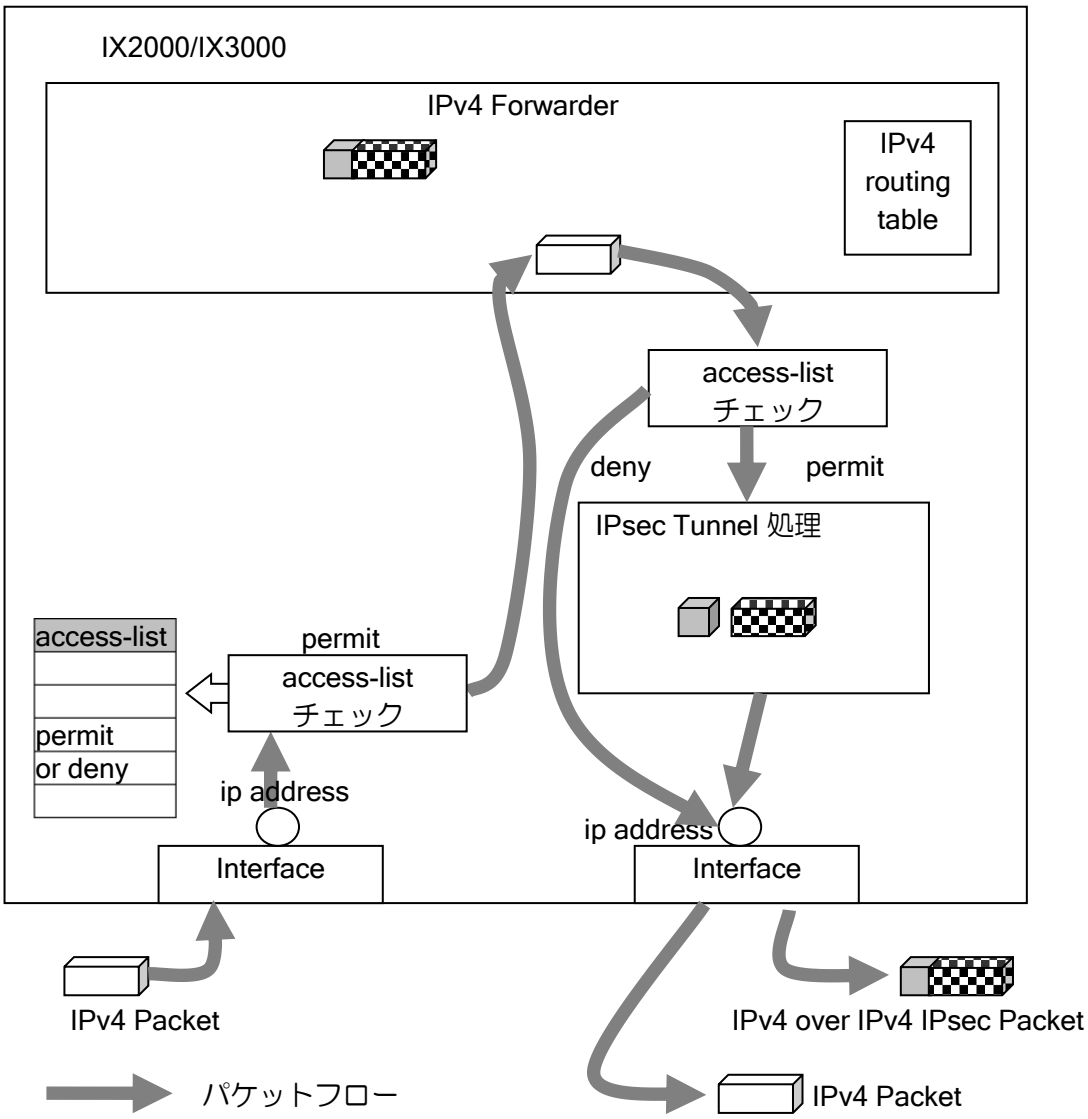
認証ヘッダ（AH）を使用する場合、暗号ペイロード（ESP）を使用する場合、あるいは組み合わせて使用する場合、オリジナルのパケットに対して、AH および ESP の他、IP ヘッダ（IPv4 あるいは IPv6）を付加して転送します。

トンネルモードで使用する主なコマンドは、前述した ipsec コマンドの他、次に示すコマンドを使用します。

ipsec policy tunnel	トンネルモードの設定

以下に、IPsec のトンネルモードの動作原理(例)と設定例を示します。





また IPsec はパケットフィルタや NAT/NAPT よりも後で処理されます。
処理順の詳細についてはパケット評価フローの章を参照してください。

【構成例】

IKE の設定

暗号アルゴリズム	3des
認証アルゴリズム	sha1
認証手段	pre-shared(default)
PFS	DH グループ:1024 bit

IPsec の設定

モード	tunnel
暗号アルゴリズム	ESP 3des
認証アルゴリズム	ESP sha1
PFS	off(default)
鍵の有効期限	28800 秒

物理インタフェースに設定する場合とトンネルインタフェースに設定する場合は、それぞれ次のようになります。

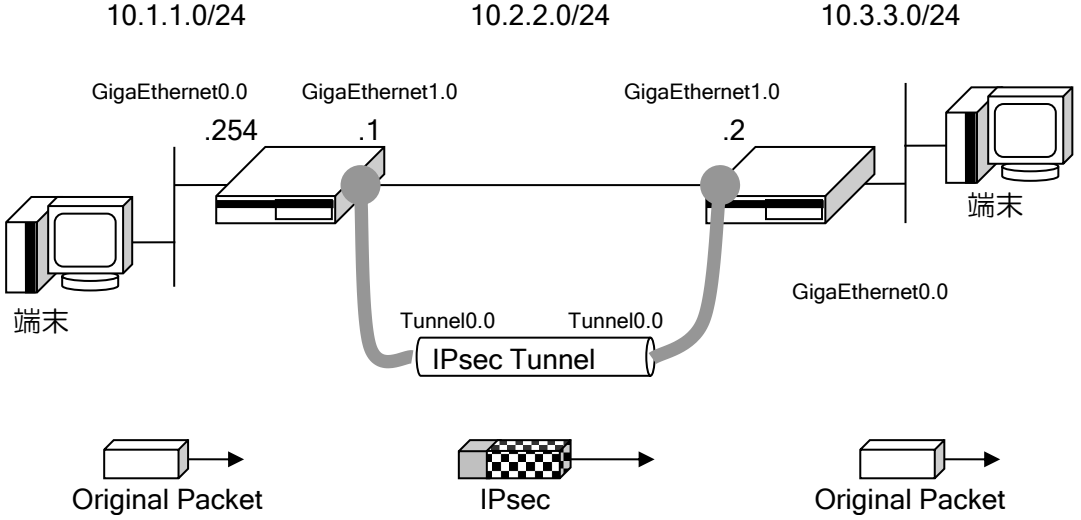
(a) 仮想トンネルインタフェースを使用する場合

IPsec トンネルを仮想トンネルインタフェースに設定することができます。同一の宛先に複数の IPsec トンネルを設定し、ネットワークモニタやルーティングプロトコルを利用して 2 重化構成を組む場合などに必要です。

仮想トンネルインタフェースでの設定は、tunnel-mode コマンドで ipsec を指定します。

このモードを設定した場合には IP over IP トンネルのカプセル化は行われません。

IX2000/IX3000 では、この方式の利用を推奨します。



【設定例】

```
ip route 10.3.3.0/24 Tunnel0.0
ip access-list alist1 permit ip src any dest any
ike proposal ike-prop encryption 3des hash sha group 1024-bit
ike policy policy1 peer 10.2.2.2 key xxxxxxxx ike-prop
ipsec autokey-proposal ipsec-prop esp-3des esp-sha
ipsec autokey-map auto1 alist1 peer 10.2.2.2 ipsec-prop
!
interface GigaEthernet0.0
   ip address 10.1.1.254/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.2.2.1/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet0.0
   ipsec policy tunnel auto1 out
   no shutdown
```

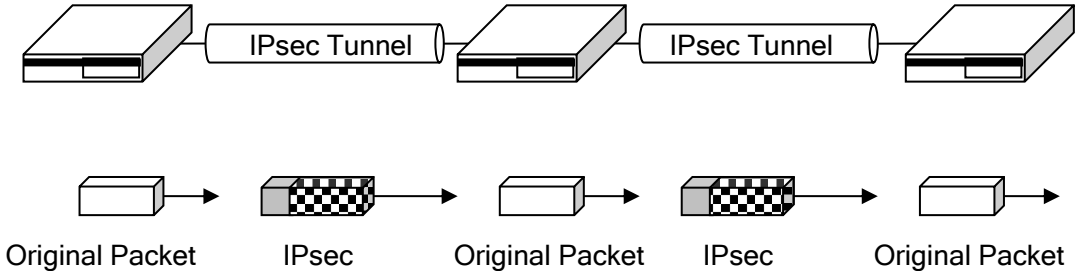
※tunnel mode ipsec を指定した場合、他の tunnel コマンドは設定できません。

※仮想トンネル 1 本に対して、指定できる ipsec policy は 1 つです。

※GRE,EtherIP,L2TP 以外はトランスポートモードを仮想トンネル方式で使用できません。

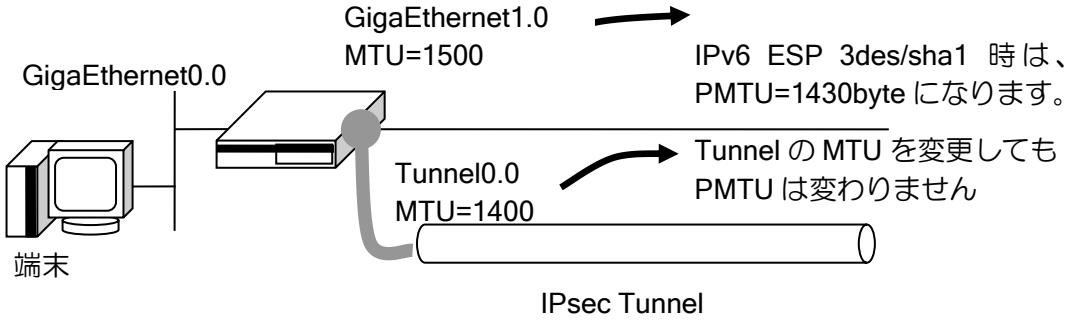
※トンネルにルーティングされたパケットは全て暗号化する必要があるので、アクセスリストの設定は permit ip src any dest any としてください。

また、下記のように IPsec のパケットを転送する際に、異なる IPsec トンネルを使用するような場合にも仮想トンネルインタフェースを使用する必要があります。



※トンネルモード使用時の MTU に関する注意事項

- ✧ トンネルモード時の MTU は、出力する物理インタフェースの MTU を使用します。そのため、IPsec の MTU を調整する場合、IPsec に使用するトンネルインタフェースの MTU を変更しても、IPsec の MTU は変更されません。
- ✧ Ver5.0 以降、IPsec の MTU は出力するインタフェースの MTU からヘッダ,トレイラを引いた値に自動調整されます。OSPF 等、MTU のネゴシエーションを行う場合には注意してください。



(b) 物理インタフェースを使用する場合

この方式では、ルーティングプロトコルは併用できません。また、IPsec 処理自体も仮想トンネルインタフェースを使用した場合よりも重くなるため、この方式での使用は非推奨です。

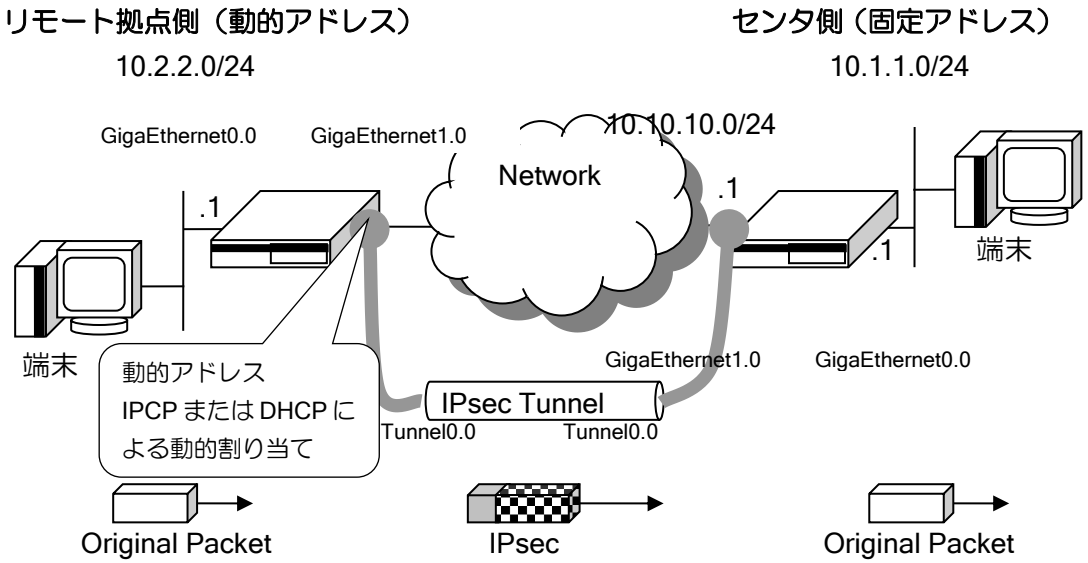
【設定例】

ここでは、自動鍵プロポーザルの設定は省略しています。

```
ip access-list alist1 permit ip src 10.1.1.0/24 dest 10.3.3.0/24
ike policy policy1 peer 10.2.2.2 key xxxxxxxx
ipsec autokey-map auto1 alist1 peer 10.2.2.2

interface GigaEthernet0.0
   ip address 10.1.1.254/24
   no shutdown

interface GigaEthernet1.0
   ip address 10.2.2.1/24
   ipsec policy tunnel auto1 out
   no shutdown
```

2.35.3 IPsec リモートアクセス機能

一方のルータのアドレスが動的に変化するような場合（ADSL 等の固定 IP アドレスが配布されないサービスなど）にも、VPN を構築することが可能です。



上記の例でリモート拠点側のアドレスは不定のため、センタ側の IKE の peer は any で設定し、IPsec は dynamic-map を利用します。また双方のルータで、事前共有鍵を選択できるようにするため、モード設定にはアグレッシブモードを使用し拠点ごとに固有の ID を設定しておきます。さらにリモート拠点側のルータのアドレスが変化した場合やセンタ側がリブートした場合などに IKE/IPsec SA を削除できるよう、IKE のキープアライブ機能を有効にする必要があります。

これらの設定を行うことにより、動的アドレス環境下でも IPsec トンネルを利用できます。

ただし、以下の制限がありますので注意が必要です。

- アドレスが不定のリモート拠点同士で通信を行うことはできません。
- IPsec 双方の内側ネットワークアドレスは、お互いに既知である必要があります。
- 動的アドレス環境でのトランスポートモードはサポートしておりません。

【設定例】
リモート拠点側（動的アドレス側）

```
ip route 10.1.1.0/24 Tunnel0.0
ip access-list alist1 permit ip src 10.2.2.0/24 dest 10.1.1.0/24
!
ike proposal iprop1 encryption des hash sha
ike policy ikepol1 peer 10.10.10.1 key xxxxxxxx iprop1 mode aggressive
!
ike local-id ikepol1 keyid sg1-site
ike keepalive ikepol1 10 3
!
ipsec autokey-proposal prop1 esp-3des esp-sha
ipsec autokey-map map1 alist1 peer 10.10.10.1 prop1
ipsec local-id map1 10.2.2.1
ipsec remote-id map1 10.1.1.1
!
interface GigaEthernet0.0
```

```
   ip address 10.2.2.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address dhcp receive-default
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet0.0
   ipsec policy tunnel map1 out
   no shutdown


センタ側（固定アドレス側）

ip route 10.2.2.0/24 Tunnel0.0
ip access-list alist1 permit ip src 10.1.1.0/24 dest 10.2.2.0/24
!
ike proposal iprop1 encryption des hash sha
ike policy ikepol1 peer any key xxxxxxxx iprop1 mode aggressive
!
ike remote-id ikepol1 keyid sg1-site
ike keepalive ikepol1 10 3
!
ipsec autokey-proposal prop1 esp-3des esp-sha
ipsec dynamic-map map1 alist1 prop1
ipsec local-id map1 10.1.1.1
ipsec remote-id map1 10.2.2.1
!
interface GigaEthernet1.0
   ip address 10.10.10.1/24
   no shutdown
!
interface GigaEthernet0.0
   ip address 10.1.1.1/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet0.0
   ipsec policy tunnel map1 out
   no shutdown
```

※ipsec dynamic-map を設定した側から IKE のネゴシエーションを行うことはありません。IKE ネゴシエーションは常にリモート拠点側から行われます。
※モードの設定はネゴシエーションを開始する側の設定のみ有効です。受け入れる側は設定に拠らず、相手のモードに合わせます。
※アドレスが変化したことを検知した場合には、関連する SA をすべて削除します。

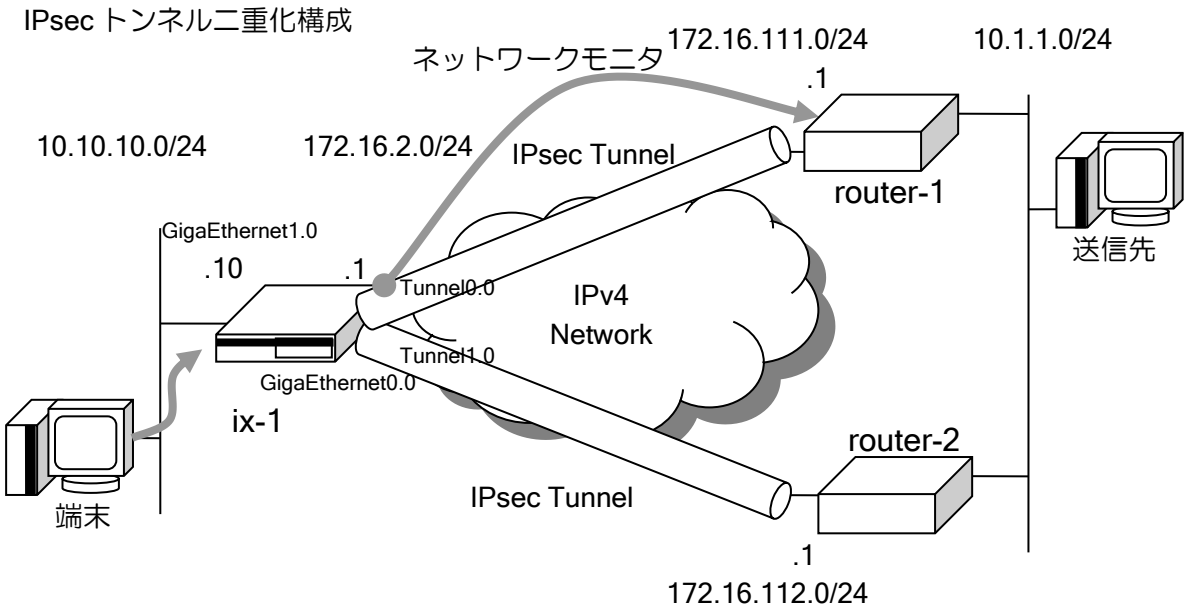
2.35.4 IPsec トンネル二重化対応

IPsec トンネルの二重化構成を組むためには、IPsec とともに以下の機能を併用する必要があります。これらは、IPsec を仮想トンネルインタフェース上で設定することで実現可能です。

- ルーティングプロトコル
- ネットワークモニタ
- フローティング・スタティック

経路監視を使用した IPsec の冗長構成例を以下に示します。

IPsec トンネル二重化構成



【設定例】

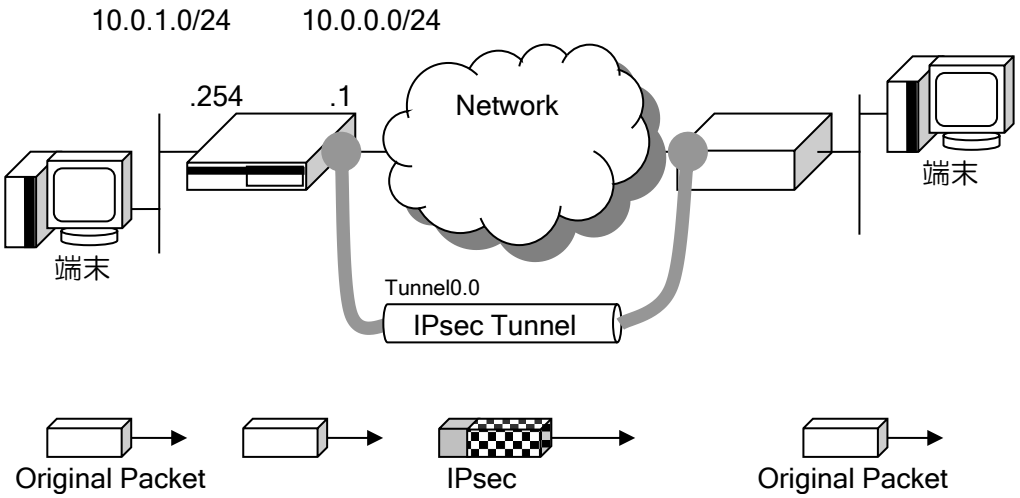
```
ip route default 172.16.2.254
ip route 10.1.1.0/24 Tunnel0.0
ip route 10.1.1.0/24 Tunnel1.0 metric 100
ip access-list list1 permit ip src any dest 10.1.1.0/24
ike proposal ike-pro1 encryption 3des hash sha lifetime 3600
ike policy ike-poli1 peer 172.16.111.1 key key1 mode aggressive ike-pro1
ike policy ike-poli2 peer 172.16.112.1 key key2 mode aggressive ike-pro1
ike local-id ike-poli1 keyid ix-1
ike local-id ike-poli2 keyid ix-1
ike remote-id ike-poli1 keyid router-1
ike remote-id ike-poli2 keyid router-2
ike keepalive ike-poli1 10 3
ike keepalive ike-poli2 10 3
ipsec autokey-proposal ipsec-pro1 esp-3des esp-sha lifetime time 3600
ipsec autokey-map ipsec-poli1 list1 peer 172.16.111.1 ipsec-pro1
ipsec autokey-map ipsec-poli2 list1 peer 172.16.112.1 ipsec-pro1
!
watch-group ipsec1 10
   event 10 ip unreach-host 172.16.111.1 Tunnel0.0
   action 10 ip shutdown-route 10.1.1.0/24 Tunnel0.0
!
network-monitor ipsec1 enable
```

```
!
watch-group ipsec2 10
   event 10 ip unreach-host 172.16.112.1 Tunnel1.0
   action 10 ip shutdown-route 10.1.1.0/24 Tunnel1.0
!
network-monitor ipsec2 enable
!
interface GigaEthernet0.0
   ip address 172.16.2.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.10.10.10/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet1.0
   ipsec policy tunnel ipsec-poli1 out
   no shutdown
!
interface Tunnel1.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet1.0
   ipsec policy tunnel ipsec-poli2 out
   no shutdown
```

2.35.5 IPsec と NAT/NAPT の連携

IPsec のパケットは通常 NAT/NAPT 変換できません。経路の途中に NAT/NAPT ルータが存在する場合は NAT トラバーサルという設定が必要になります。詳細は NAT トラバーサル機能を参照してください。

(1) インターネット VPN の設定（送信インタフェースで NAPT を利用）



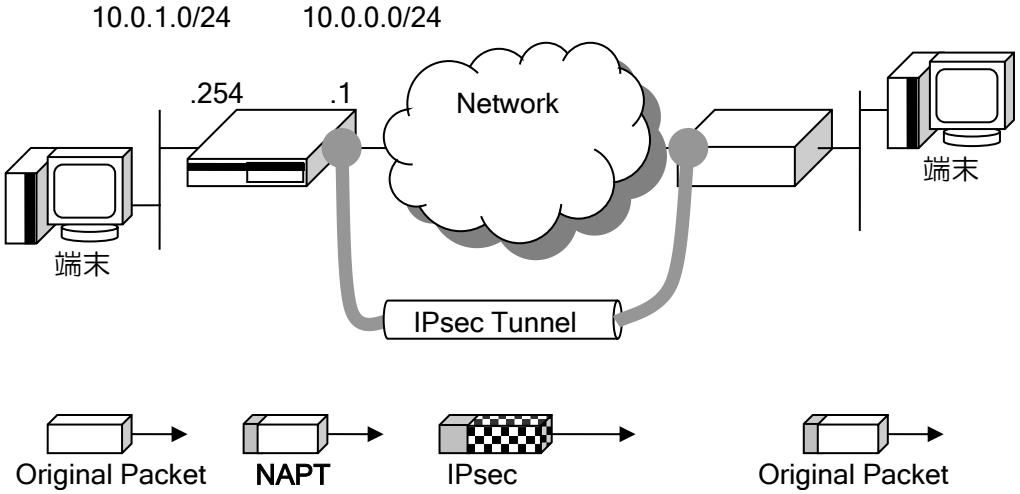
インターネット VPN の設定などで、WAN 側インタフェースで NAT/NAPT を有効にし、IPsec の設定も行う場合、アドレスは変換されないので NAT トラバーサルの設定は不要です。ただし、相手側から通信が開始された場合に、NAT/NAPT でパケットが廃棄されないように、静的 NAPT の設定が必要になります。

【設定例】
ルーティングや IKE/IPsec の設定は省略しています。

```
interface GigaEthernet0.0
   ip address 10.0.0.1/24
   ip napt enable
   ip napt static GigaEthernet0.0 udp 500
   ip napt static GigaEthernet0.0 50
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.0.1.254/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet1.0
   ipsec policy tunnel auto1 out
   no shutdown
```

※1 送信元アドレスが NAPT のアドレスになる場合は NAT トラバーサルの設定は不要です。
※2 NAPT は相手側から開始される通信を廃棄するので、NAPT やフィルタでは udp の 500 番および ESP のプロトコル 50 番を開けておく必要があります。

（2）IPsec 対象のアドレス変換設定（Tunnel インタフェースに NAT/NAPT を適用）



IPsec でカプセル化するパケットの中身に NAT/NAPT やフィルタを適用したい場合には、トンネルインタフェースでそれらの機能を設定してください。これらの機能が適用されたあとに暗号化されます。

【設定例】

IPsec トンネルの設定以外は省略しています。

```
interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet0.0
   ip napt enable
   ipsec policy tunnel auto1 out
   no shutdown
```

2.35.6 トランスポートモード

トランスポートモードは、主にホスト対ホストでのセキュリティを確保するためのモードで、通常のパケット転送時にトランスポートレイヤのデータを認証、または暗号化して転送する機能です。

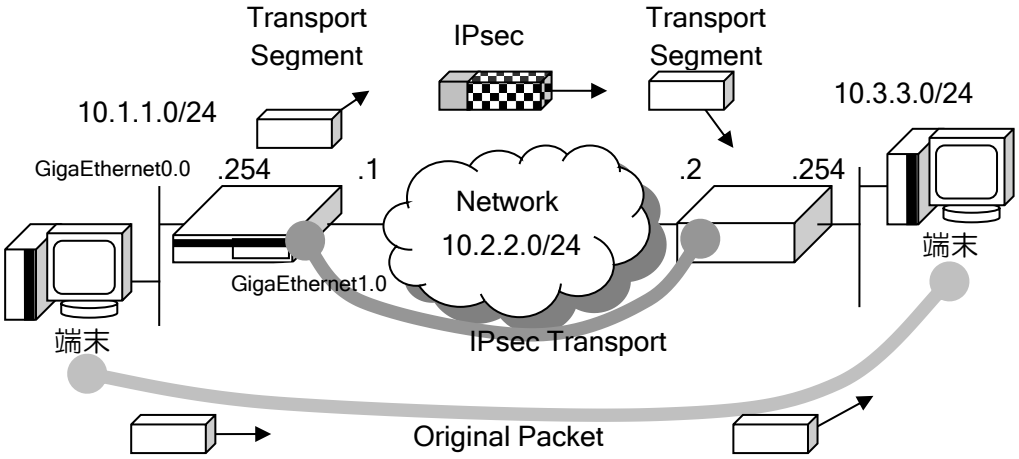
認証ヘッダ（AH）を使用する場合、暗号ペイロード（ESP）を使用する場合、あるいは組み合わせて使用する場合、オリジナルのペイロードに対して、AH および ESP の他、IP ヘッダ（IPv4 あるいは IPv6）を付加して転送します。

トランスポートモードで使用する主なコマンドは、前述した ipsec コマンドの他、次に示すコマンドを使用します。

ipsec policy transport	トランスポートモードの設定

トランスポートモードはトンネルモードと異なりデフォルトでは ID を送信しませんので、ID が必須の対向装置との接続や EtherIP 使用時は、with-id-payload を設定してください。

以下に、IPsec のトランスポートモードの動作原理(例)と設定例を示します。



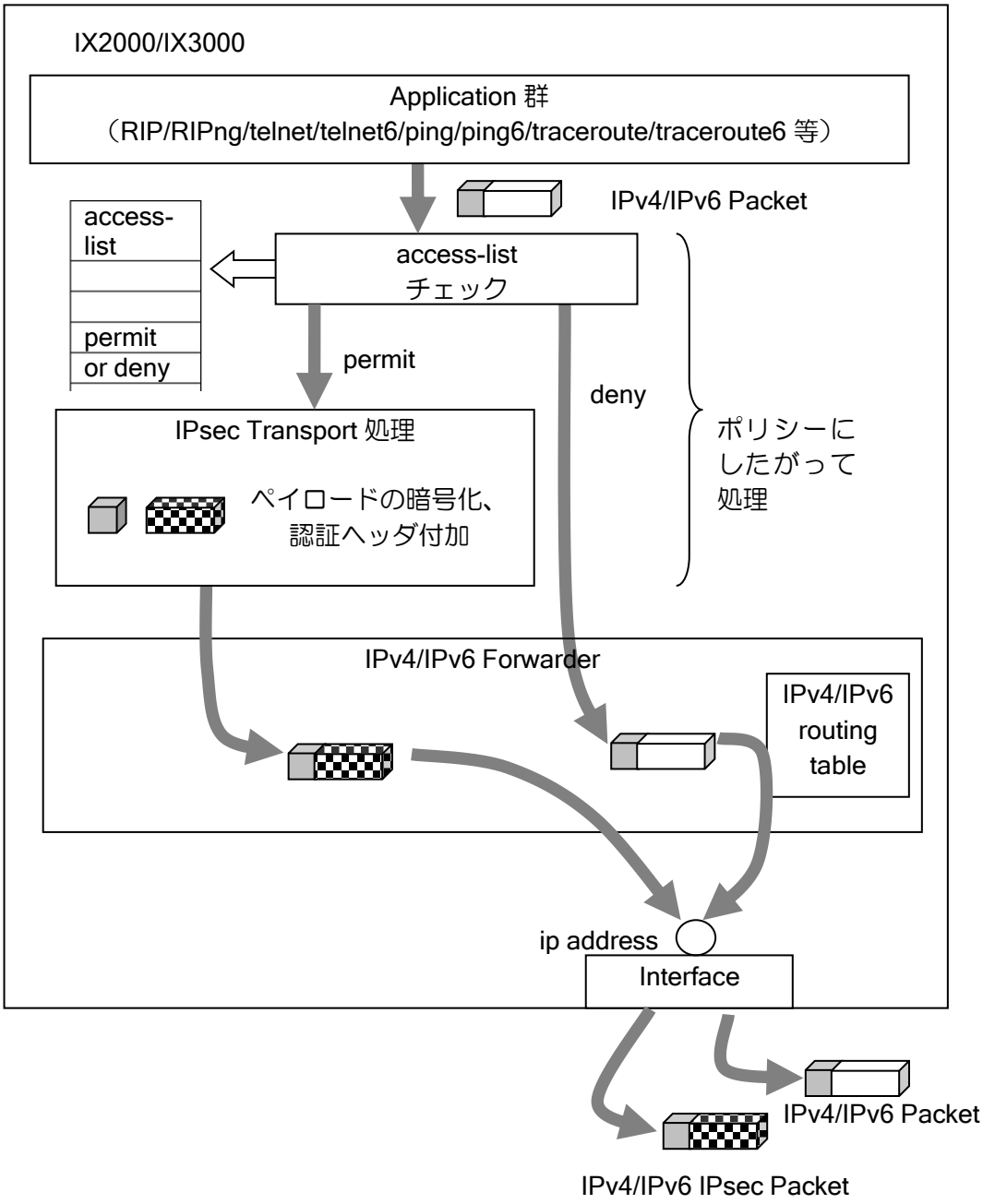
【構成例】

IKE の設定

暗号アルゴリズム	des(default)
認証アルゴリズム	md5(default)
認証手段	pre-shared(default)
PFS	DH グループ:768 bit(default)

IPsec の設定

モード	transport
認証アルゴリズム	ESP md5(default)
暗号アルゴリズム	ESP des(default)
PFS	off(default)
鍵の有効期限	3600 秒



【設定例】

ここでは、自動鍵プロポーザルの設定は省略しています。

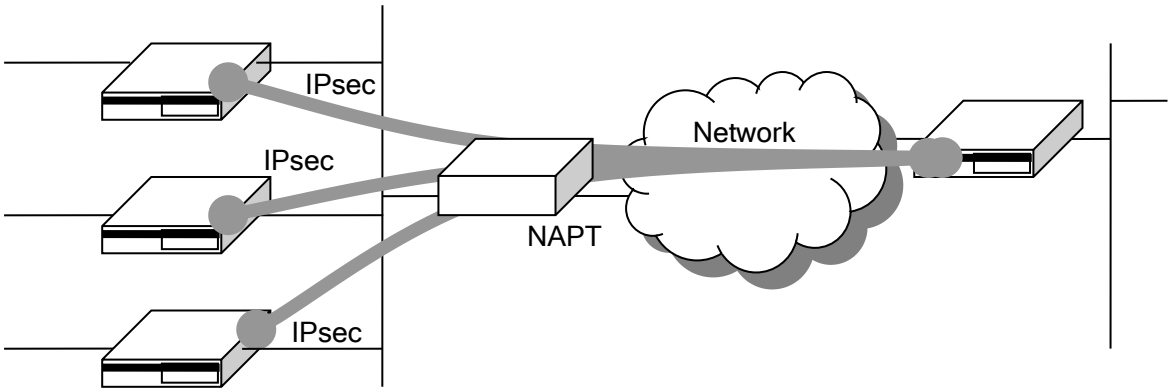
```
ip access-list alist1 permit ip src 10.2.2.1/32 dest 10.2.2.2/32
ike policy policy1 peer 10.2.2.2 key xxxxxxxx
ipsec autokey-map auto1 alist1 peer 10.2.2.2
interface GigaEthernet1.0
   ip address 10.2.2.1/24
   ipsec policy transport auto1
   no shutdown
```

アクセスリストの設定については、アクセスリストの節を参照してください。

2.35.7 NAT トラバーサル機能

NAT トラバーサルは、IPsec のパケットを NAPT 変換できるように拡張する機能です。NAT/NAPT を使用している環境でも、NAPT 内部の複数の IPsec クライアントが 1 つの NAPT アドレスで同時に IPsec を利用できるようになります。

本機能を使用しない場合、途中に存在する NAT/NAPT ルータの VPN パススルー機能を使用することにより、NAT/NAPT 内部に存在する 1 台の IX ルータのみが IPsec を使用することが可能になります。（NAT/NAPT ルータに VPN パススルー機能が必要です。）



概要

NAT トラバーサルは、暗号化したパケットにさらに UDP のヘッダを付与する機能です。IPsec のパケットにはポート番号がないためポート変換ができず、複数の IPsec クライアントを 1 つの NAPT アドレスに集約することはできません。

暗号化したペイロード全体を UDP ヘッダでカプセル化することにより、経路上の装置からは単なる UDP パケットに見えるので、NAPT 装置ではポート変換が可能となり、通信が可能になります。

具体的には、NAT トラバーサル機能で IKE のネゴシエーションに以下の機能が付与されます。

- サポートしている NAT トラバーサル機能の種別を相手に通知する
- NAT/NAPT を検出する（ネゴシエーションパケットが変換されたかどうかを判断できる）
- 変換されていた場合、NAT トラバーサルのカプセル化モードを提案し採用する。

NAT トラバーサルが有効になると、IPsec パケットは UDP でカプセル化されるようになります。この UDP は送信先/送信元の両方で 4500 番ポートを固定的に使用しますので、フィルタを設定している場合は、廃棄されることがないように注意してください。

制限事項

- メインモードは未対応です。アグレッシブモードを使用してください。
- NAT トラバーサルには RFC といくつかのドラフトの仕様が存在しており、これらは互換性がありません。このうち RFC と以下のドラフトのみ対応しています。それ以外のドラフトのみサポートする装置とは NAT トラバーサルで接続できません。
  - draft-ietf-ipsec-nat-t-ike-02, draft-ietf-ipsec-udp-encaps-02
  - draft-ietf-ipsec-nat-t-ike-03, draft-ietf-ipsec-udp-encaps-03
- プロトコルの仕様上、AH と併用することはできません。

設定方法

NAT トラバーサルの設定は、以下のコマンドを使用します。

ike nat-traversal	NAT トラバーサル機能を有効にします。

プロポーザルやポリシーの設定は通常の IKE/IPsec と変わりません。上記コマンドで全体またはポリシーごとに有効にすることにより、対向装置とのネゴシエーションを行い必要に応じて UDP ヘッダを付与して通信するようになります。

動作する条件は、有効にしたポリシーについて相手装置も NAT トラバーサルに対応しており、かつ相手装置との間に NAT が存在することです。アドレス変換されない場合は、設定を有効にしても NAT トラバーサル機能が使用されずに普通の IPsec になります。

また NAT トラバーサルには通信が停止している場合に NAT/NAPT 装置のキャッシュを維持するための NAT キープアライブの機能が標準で備わっています。この時間間隔も本コマンドで変更できますのでキャッシュが削除されないよう調整してください。デフォルトは 20 秒です。

フラグメント対策（推奨）

IX2000/IX3000 の IPsec はデフォルトでは暗号化してからフラグメントを行う順序ですが、NAT トラバーサルを使用する場合は、暗号化する前にフラグメントする設定が推奨です。

以下のコマンドのパラメータ、pre-fragment を有効にしてください。

ipsec policy	フラグメント方式の変更

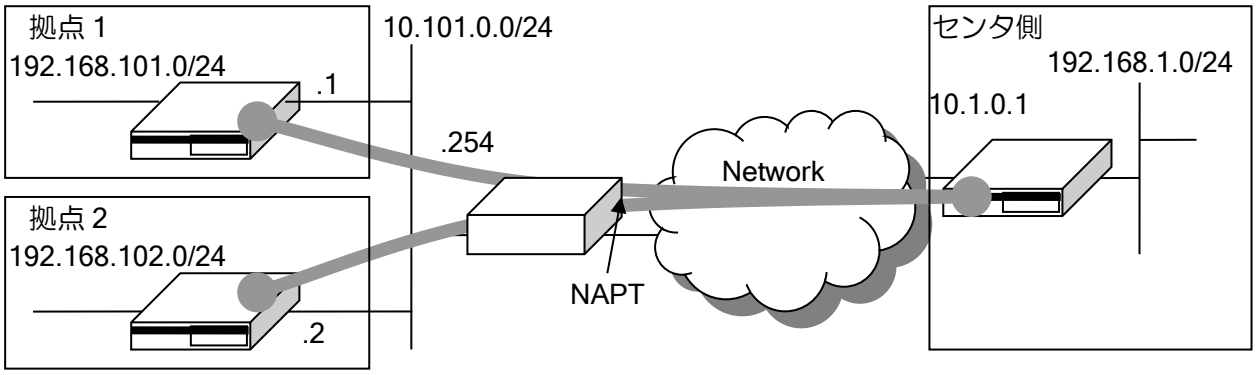
この設定を行わなかった場合、フラグメントパケットが NAT/NAPT ルータで正しく変換されずに廃棄されてしまう可能性があります。

暗号化してからフラグメントした場合（デフォルト）、フラグメントされた２番目以降のパケットには UDP のヘッダがつきません。NAT/NAPT ルータは一般に UDP や TCP のヘッダを参照してアドレス変換を行っているため、UDP ヘッダがつかないフラグメントパケットを正しく変換できない場合があります。暗号化する前にフラグメントする設定にした場合、すべてのパケットに UDP ヘッダが付与されるため、NAT/NAPT ルータで正しく変換することが可能になります。

その他の注意事項

- NAT 装置を検出しない限り（相手装置からのパケットがアドレス変換されていない限り）、NAT トラバーサルのカプセル化モードを提案することはありません。
- MTU サイズは通常の IPsec よりも UDP ヘッダサイズ分（8byte）だけ小さくなります。
- UDP は 500 番ポートのほか 4500 も使用されます。

設定例



【設定例】
センタと拠点 1 の設定です。

センタ側設定（固定アドレス側）

```
ip route default 10.1.0.254
ip route 192.168.101.0/24 Tunnel1.0
ip route 192.168.102.0/24 Tunnel2.0
ip access-list alist-any permit ip src any dest any
!
ike nat-traversal
!
ike policy ike-site1 peer any key secret-site1 mode aggressive ikeprop
ike keepalive ike-site1 10 3
ike remote-id ike-site1 keyid site1
!
ike policy ike-site2 peer any key secret-site2 mode aggressive ikeprop
ike keepalive ike-site2 10 3
ike remote-id ike-site2 keyid site2
!
ipsec autokey-proposal ipsecprop esp-aes esp-sha
!
ipsec dynamic-map ipsec-site1 alist-any ipsecprop ike ike-site1
!
ipsec dynamic-map ipsec-site2 alist-any ipsecprop ike ike-site2
!
interface GigaEthernet0.0
   ip address 10.1.0.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.1.1/24
   no shutdown
!
interface Tunnel1.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet1.0
   ipsec policy tunnel ipsec-site1 pre-fragment out
   no shutdown

interface Tunnel2.0
   tunnel mode ipsec
   ip unnumbered GIgaEthernet1.0
   ipsec policy tunnel ipsec-site2 pre-fragment out
   no shutdown
```

```
拠点１設定（動的アドレス側設定）
ip route default 10.101.0.254
ip route 192.168.0.0/16 Tunnel0.0
ip access-list alist-any permit ip src any dest any
!
ike nat-traversal
!
ike proposal ikeprop encryption aes hash sha
!
ike suppress-dangling
!
ike policy ike-site1 peer 10.1.0.1 key secret-site1 mode aggressive ikeprop
ike keepalive ike-site1 10 3
ike local-id ike-site1 keyid site1
!
ipsec autokey-proposal ipsecprop esp-aes esp-sha
!
ipsec autokey-map ipsec-site1 alist-any peer 10.1.0.1 ipsecprop
!
interface GigaEthernet0.0
   ip address 10.101.0.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.101.1/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet1.0
   ipsec policy tunnel ipsec-site1 pre-fragment out
   no shutdown
```

確認方法

IPsec 接続中に以下のコマンドを実行することにより、NAT トラバーサルで接続されていることを確認することができます。

show ike sa	IKE SA の情報を表示します。
show ipsec sa	IPsec SA の情報を表示します。

- show ike sa

```
    :
  NAT-Traversal RFC3947          （動作中の NAT トラバーサルの種類）
  NAT detected at remote side    （自ルータがグローバルアドレス側と自動認識）
    :
```

- show ipsec sa

```
        :
    UDP encapsulation Tunnel mode, 4-over-4, dynamic-map    （UDP でカプセル化）
        :
```

2.35.8 IPsec のネスト時の注意

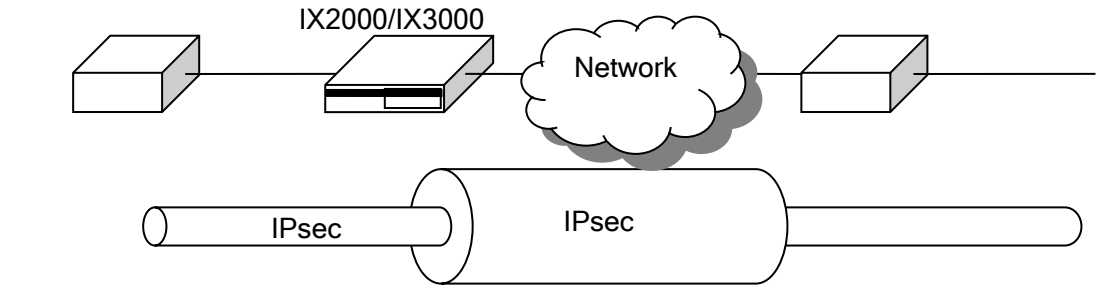
IPsec トンネルのネスト時に、IPsec トンネルの中を通る IKE パケットはデフォルトでは暗号化されず、IP-IP のパケットとしてトンネルを通過します。

受信側でフィルタを設定している場合、これらのパケットは廃棄される可能性がありますので、ご注意ください。

※NAT トラバーサルの場合 Ver8.9 以前のバージョンでは暗号化されます。

IKE を暗号化したい場合は以下の設定で変更可能です。

ipsec ike-passthru	IKE パケットのバイパス設定



通常のパケット

データ　暗号化　更に全体を暗号化

IKE デフォルト動作（ipsec ike-passthru）

IKE　暗号化せずカプセル化

IKE バイパス未設定時（no ipsec ike-passthru）

IKE　暗号化

■2.36 スマートデバイス対応（L2TP LNS 機能）の設定

スマートフォンやタブレットなどに実装されている L2TP/IPsec のクライアントを利用して、IX ルータ配下の LAN にインターネット経由でリモートアクセスすることが可能です。Ver8.10 以降で対応しています。L2TP のクライアント側の動作は L2TP LAC 機能を参照してください。

2.36.1 L2TP LNS 機能の概要

IX ルータでサポートしている L2TP LNS 機能は、スマートデバイスと接続するための機能として実装しています。対応状況は以下のとおりです。

- L2TP LNS の接続は IPsec（IKEv1 かつ IPv4）との併用が必須です。
- NAT トラバーサルに対応しており、プライベートアドレス環境でも利用可能です。
- L2TP-MIB（RFC3371）はサポートしていません。

2.36.2 動作確認端末

動作確認した端末は以下のとおりです。

- MEDIAS N-02E(Android 4.0.4)
- iPhone X（iOS 12.3.1）
- Windows 7 Professional Service Pack 1
- Windows 8 Pro
- Windows 10

等

以下の端末は動作しません。

- Windows XP
- Windows Vista
- MeDIAS NEC-102

その他の確認端末については、以下の URL をご覧ください。

https://jpn.nec.com/univerge/ix/faq/l2tpv2.html#Q1-1

端末の設定は、端末ごとに設定方法が異なるため、端末側の設定は別途設定マニュアルを参照してください。

2.36.3 注意事項

NAT が多段になっている環境（プライベートアドレスが払い出される環境で、さらに NAT ルータを介して接続する環境）では、以下の制限があります。

IPsec の NAT トラバーサルは peer アドレスと ID で端末を区別しますが、スマートデバイスは ID が IP アドレスで固定されている装置が多く、同一のグローバルアドレス内で同じ IP アドレスの端末が存在する場合、原理的に端末を区別できないため同時利用できません。

2.36.4 L2TP LNS/IPsec の基本設定

L2TP, IPsec, PPP の機能を組み合わせて実現します。設定例は以下のとおりです。

【設定例】

```
ip access-list sec-list permit ip src any dest any
!
ike nat-traversal
!
ike proposal ike-prop encryption 3des hash sha group 1024-bit
ike policy ike-policy peer any key SECRET ike-prop
!
ipsec autokey-proposal ipsec-prop esp-3des esp-sha
ipsec dynamic-map ipsec-policy sec-list ipsec-prop
!
ppp profile lns
   authentication request chap
   authentication password user1 pass1
   authentication password user2 pass2
   authentication password user3 pass3
   lcp pfc
   lcp acfc
   ipcp ip-compression
!user1 に 192.168.1.1 を払い出し
   ipcp provide-static-ip-address user1 192.168.1.1
!その他のユーザは空いているアドレスを払い出し
   ipcp provide-ip-address range 192.168.1.2 192.168.1.253
!
interface GigaEthernet0.0
   ! WAN 側
   ip address dhcp receive-default
   ip napt enable
   ip napt static GigaEthernet0.0 udp 500
   ip napt static GigaEthernet0.0 udp 4500
   ip napt static GigaEthernet0.0 50
   no shutdown
!
interface GigaEthernet1.0
   ! LAN 側
   ip address 192.168.0.254/24
   ip proxy-arp
   no shutdown
!
interface Loopback0.0
   ip address 192.168.1.254/24
!
interface Tunnel0.0
   ppp binding lns
   tunnel mode l2tp-lns ipsec
   ip unnumbered Loopback0.0
   ip tcp adjust-mss auto
   ipsec policy transport ipsec-policy
   no shutdown
!
interface Tunnel1.0
   ppp binding lns
   tunnel mode l2tp-lns ipsec
   ip unnumbered Loopback0.0
```

```
ip tcp adjust-mss auto
ipsec policy transport ipsec-policy
no shutdown
```

2.36.4.1 L2TP LNS/IPsec トンネルの設定

同時接続するユーザの数だけトンネルインタフェースを L2TP LNS/IPsec モードに変更する必要があります。

以下のコマンドでトンネルインタフェースを L2TP モードに設定してください。その際、装置の再起動が必要になるので注意してください。

tunnel mode l2tp-lns ipsec	トンネルを L2TP/IPsec 対応に変更（要再起動）

トンネルモードを他のモードから L2TP に変更する場合、L2TP から他のモードに変更する場合は他のモード変更と異なり再起動が必要です。なお Ver9.6 までは l2tp-lns ではなく l2tp と表示されます。

2.36.4.2 IPsec の設定

アドレスが不定の端末と L2TP LNS/IPsec で接続するために、設定例のようにダイナミックポリシーマップを1つ設定し、全てのL2TP LNS/IPsecトンネルインタフェースに割り当ててください。

ipsec dynamic-map	ダイナミックポリシーマップの設定

IPsec は通常接続先ごとに 1 つのポリシー設定が必要ですが、L2TP LNS/IPsec でダイナミックポリシーマップを利用する場合に限り、1 つのポリシーで複数の端末と接続することができます。この設定では 1 つの事前共有鍵を全ユーザで利用します。

IPsec の設定内容については IPsec の章を参照してください。なお、プロポーザルの設定は、全ての端末が接続できる条件を指定する必要があります。特に理由がなければ設定例と同様の設定にしてください。

端末にはプライベートアドレスが払い出される場合があるため、NAT トラバーサルの設定も必ず有効にしてください。

2.36.4.3 PPP の設定

L2TP は PPP を利用するプロトコルです。認証や端末に払い出すアドレスは PPP で設定します。ユーザごとの認証の設定と、接続された端末にアドレスを払い出す以下の設定が必要です（Radius サーバと連携する場合には不要です）。

ユーザ名は複数設定可能です。使用するユーザ分の設定を行ってください。1 つのユーザ名を複数の端末で使用することもできます。

ipcp provide-ip-address range	アドレスの複数払い出し設定
ipcp provide-static-ip-address	アドレス固定払い出し設定

また、PPP プロファイルの pfc, acfc, ip-compression の設定は、通常設定例と同じ設定にしてください。

2.36.5 接続情報の取得

L2TP で接続された情報は、以下のコマンドで参照できます。
通常の IPsec と異なり、接続されるトンネルが不定なことに注意してください。

show interfaces	インタフェース情報の表示
show l2tp active	接続中の L2TP トンネルの情報表示
show l2tp history	L2TP トンネルの情報と L2TP 接続履歴の表示
show l2tp statistics	L2TP 統計情報表示

2.36.6 Radius 連携

PPP の認証を Radius サーバで行う場合、以下のアトリビュートを送信します。

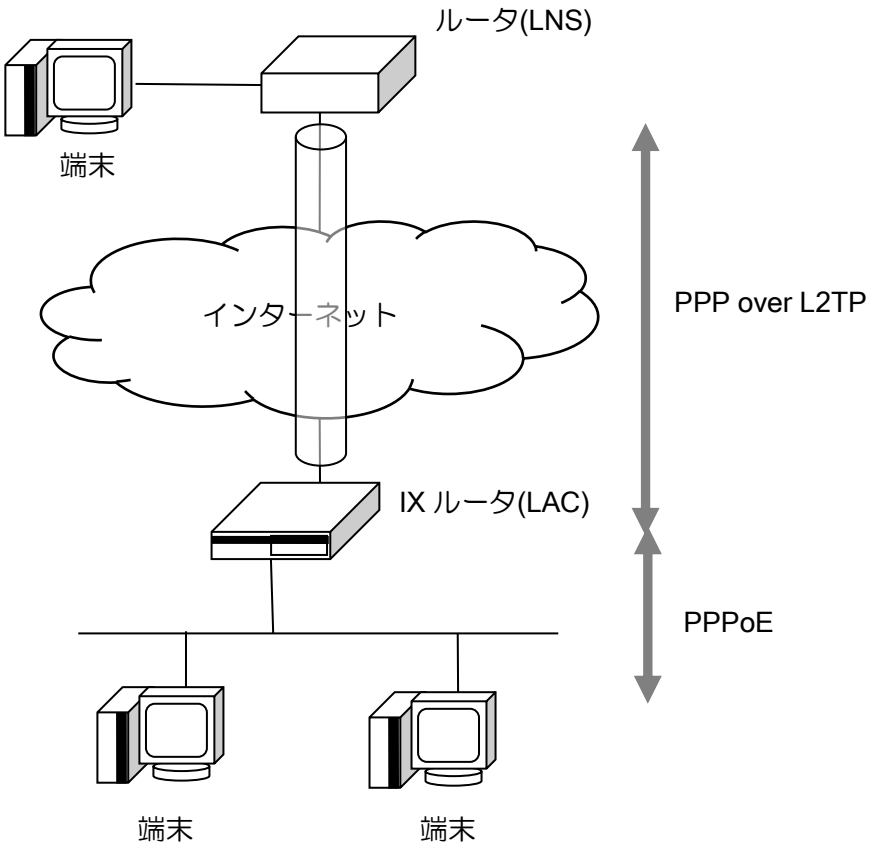
User-Name	PPP ユーザ名
CHAP-Password	PPP 認証パスワード
CHAP-Challenge	CHAP チャレンジ
NAS-Port-Type	Virtual （5）
NAS-Port	接続インタフェース番号
Framed-Protocol	PPP
Service-Type	Framed-User
NAS-IP-Address	Radius パケット送信インタフェースの IP アドレス

■2.37 L2TP LAC 機能によるリモートアクセス設定

IX ルータが配下の PPPoE クライアントの通信を L2TP トンネルでリモートの LNS 装置まで中継する機能です。Ver9.7 以降で対応しています。

スマートフォンやタブレットなどを接続するための L2TP 機能は「L2TP LNS 機能によるスマートデバイス対応の設定」を参照してください。

2.37.1 L2TP LAC 機能の概要



2.37.2 注意事項

IX ルータでサポートしている L2TP LAC 機能は以下の制限があります。

- L2TP over IPv6 はサポートしていません（L2TP over IPv4 over IPv6 は可能）。
- プロキシ認証機能には対応しておりません。
- L2TP-MIB（RFC3371）はサポートしていません。
- ユーザごとに RADIUS に問い合わせて LNS を切り替える機能はサポートしていません。

なお、接続試験は一部の L2TP LNS 装置のみで実施しています。利用の際には事前検証をお願い致します。

2.37.3 L2TP LAC および PPPoE サーバ機能の基本設定

PPPoE で接続する端末は L2TP でリモートの LNS 装置に転送し、それ以外の端末はインターネット通信を行う設定です。

1) PPPoE サーバの設定
2) L2TP LAC トンネルの設定
3) L2TP LAC 転送条件の設定

まず、全体の設定例を示し、それぞれの設定について説明します。

【設定例】

```
ip route default GigaEthernet0.1
!
url-list l2tp-user permit domain *example.co.jp
!
ppp profile pppoe_client
   authentication myname xxxxxxxx@xxxx.jp
   authentication password xxxxxxxx@xxxx.jp xxxxxxxxxx
!
ppp profile pppoe_server
   authentication request chap
!
interface GigaEthernet0.1
   encapsulation pppoe
   auto-connect
   ppp binding pppoe_client
   ip address ipcp
   ip napt enable
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.0.254/24
   no shutdown
!
interface range GigaEthernet2 sub 1-16
   encapsulation pppoe
   auto-connect
   pppoe l2tp interface Tunnel1.0 url-list l2tp-user
   pppoe server
   ppp binding pppoe_server
   ip unnumbered GigaEthernet2.0
   no shutdown
!
interface Tunnel1.0
   l2tp session idle-time 120
   tunnel mode l2tp-lac ip
   tunnel destination fqdn lns.example.co.jp
   no ip address
   no shutdown
```

GE2 に接続した*example.co.jp の PPPoE クライアントは、GigaEthernet2.1～GigaEthernet2.16 と Tunnel1.0 を介して LNS に接続し、それ以外の一般ユーザは GigaEthernet2.0 で送受信する設定です。PPP で転送する IPv4 パケットは MSS を自動調整します。

*example.co.jp 以外の ID で接続を試みた PPPoE クライアントには IX ルータが認証エラーを返します。

2.37.3.1 L2TP LAC トンネルの設定

LAC トンネルの設定は以下のとおりです。

tunnel mode l2tp-lac ip	トンネルを L2TP LAC 機能で利用
tunnel destination	L2TP のトンネルのあて先(LNS)
l2tp session idle-time	L2TP トンネルの無通信時間の設定

【設定例】

```
interface Tunnel1.0
   l2tp session idle-time 120
   tunnel mode l2tp-lac ip
   tunnel destination fqdn lns.example.co.jp
   no ip address
   no shutdown
```

2.37.3.2 PPPoE サーバの設定

PPPoE サーバの詳細設定は、PPPoE サーバの章を参照してください。

ユーザの認証は LNS 側で実施しますので、L2TP で利用する場合はユーザ設定は不要です。
また、以下のコマンドで L2TP LAC 機能を利用するドメインと、L2TP LAC トンネルインタフェースを指定します。

url-list	L2TP に転送するドメインを指定します。
pppoe l2tp interface	L2TP に転送する条件とトンネルを指定します。

【設定例】

```
url-list l2tp-user permit domain *example.co.jp
!
ppp profile pppoe_server
   authentication request chap
!
interface range GigaEthernet2 sub 1-16
   encapsulation pppoe
   auto-connect
   pppoe server
   pppoe l2tp interface Tunnel1.0 url-list l2tp-user
   ppp binding pppoe_server
   ip unnumbered GigaEthernet2.0
   no shutdown
```

2.37.4 接続情報の取得

L2TP で接続された情報は、以下のコマンドで参照できます。

show pppoe server	セッション情報の取得
show l2tp active	接続中の L2TP トンネルの情報表示
show l2tp statistics	L2TP 統計情報表示

接続ユーザに関する情報は show pppoe server を利用してください。
ユーザ ID ごとの状態、MAC アドレス、送受信量、通信時間、無通信時間などを一覧表示します。

■2.38 IKEv2/IPsec の設定

IX2000/IX3000 シリーズでは、Ver8.7 以降で IKEv2 が利用できます。IKEv2 は IKEv1 との互換性はありませんが、IKEv1 のプロトコルでは不明確だった動作仕様が明確化されており、事前共有鍵以外の認証方式のサポート、耐障害性を考慮したプロトコル設計などが特徴となっています。

また IKEv2 機能のサポートにあたり、コンフィグ体系の見直しや常時接続などの機能を追加しています。IKEv1 と IKEv2 は異なる点が多いので注意してください。

2.38.1 IKEv2/IPsec の概要

IKEv1 を利用していた方を対象に、IKEv2 機能の概要を説明します。

IKEv2 は IKEv1 と互換性がなく、使われる用語も異なります。

- ISAKMP-SA, IPsec-SA 相当の機能は、それぞれ IKE-SA, Child-SA となります。
- ハッシュアルゴリズム相当の機能は、認証アルゴリズムと擬似乱数アルゴリズムです。
- メインモード、アグレッシブモードという概念はなくなり、動作は共通化されました。
- Phase1-ID、Phase2-ID も共通化され、一組の local-ID, remote-ID だけになります。

2.38.1.1 IKEv2/IPsec のサポート機能一覧

IKEv2 でサポートしている機能は以下のとおりです。事前共有鍵方式以外に、EAP-MD5 方式、デジタル署名方式にも対応しています（Ver10.0 以前は拠点側の機能のみ）。

- ID/認証方式

認証方式		
事前共有鍵方式	EAP-MD5 方式	デジタル署名方式
ID		
ID_IPV4_ADDR	ID_FQDN	ID_RFC822_ADDR
ID_IPV6_ADDR	ID_KEY_ID	

- アルゴリズム関係

暗号アルゴリズム（enc）		
ENCR_AES_CBC (256bit)	ENCR_AES_CBC (192bit)	ENCR_AES_CBC (128bit)
ENCR_3DES	ENCR_AES_GCM(128bit) （Ver.10.5 以降） （IX3110/IX3015 を除く）	ENCR_AES_GCM(256bit) （Ver.10.5 以降） （IX3110/IX3015 を除く）
認証アルゴリズム（integrity）		
AUTH_HMAC_SHA2_512	AUTH_HMAC_SHA2_384	AUTH_HMAC_SHA2_256
AUTH_HMAC_SHA1_96	AUTH_HMAC_MD5_96	
擬似乱数アルゴリズム（prf）		
PRF_HMAC_SHA2_512	PRF_HMAC_SHA2_384	PRF_HMAC_SHA2_256
PRF_HMAC_SHA1	PRF_HMAC_MD5	
DH グループ（DH）		
MODP-2048	MODP-1536	MODP-1024
MODP-768	MODP-3072 （Ver.10.9 以降）※1	

※1 DH グループ MODP-3072 を 3000 対地以上で使用する場合は再送間隔を 10 秒以上に設定してください。

SHA2 は一部の機種が H/W 対応しておりません。大幅に性能が低下することから設定数などの

制限がありますので、諸元値等を確認してください。

- その他の新規サポート機能
  - 常時接続（オートコネクト）に対応しました。
  - ポリシーの一括設定手段を用意し、多対地環境のコンフィグを軽減しました。
  - IKEv2 では IPv4 と IPv6 を 1 つのトンネルインタフェースで併用できます。
  - 送信インタフェースを固定できます。WAN インタフェースダウン時に IPsec パケットを迂回させないように制御できます。

2.38.1.2 IKEv2/IPsec の未サポート機能一覧

IX2000/IX3000 シリーズの IKEv2 では以下の機能をサポートしておりません。

IKEv1 でサポートしている機能		
トランスポートモード（Ver.9.2 以降一部対応）	AH 認証	NAT トラバーサル（Ver.9.1 以前）
プライベート MIB 対応	NGN トンネル対応（Ver.9.4 以前）	Web コンソール対応
ether-ip ipsec 対応（Ver9.1 以前）		

その他の代表的な IKEv2 機能		
コンフィグペイロード	トラフィックセレクタの範囲指定（Ver9.1 以前）	デジタル署名クライアント DSS 認証（Ver10.0 以前）
ESP 拡張シーケンス	ESP TFC パディング	REAUTH

2.38.1.3 その他の IKEv1 との主な違い

- IKEv1 と IKEv2 のプロトコルに互換性はなく、設定、表示コマンドも全て異なります。
- IKEv2 のイベントログは IKE では表示されません。IKE2 を使用します。
- IKE-SA が削除されると常に Child-SA も削除されます。
- SA の削除条件の変更
  - インタフェースダウンやコンフィグ変更で SA は削除されません。
  - clear ikev2 sa のコマンドでも即座に SA は削除されません。削除を通知し、その応答確認後に削除します（応答がない場合、タイムアウトするまで削除されません）。
- トリガパケットは廃棄されません。
- lifetime がネゴシエーションされません。個別に値を設定することができます。
- DPD（キープアライブ）のパケットは、IKEv1 では IPsec 通信を検出した場合は抑止していましたが、IKEv2 では常に指定した周期で送信されます。
- IKEv1 では IKE のパケットはデフォルトでは暗号化対象としていませんでしたが、IKEv2 のパケットは常に IPsec の暗号化対象となります。

2.38.2 事前共有鍵による設定例

IKEv2 の事前共有鍵の設定では、ポリシーの設定、事前共有鍵の設定、および接続先の設定が必要です。拠点間を IKEv2 で暗号化する場合のサンプルコンフィグは以下のとおりです。

※以下の設定例では IP アドレスやルーティングなどの設定は除外しています。

```
【設定例】拠点 1 側

ikev2 authentication psk id keyid site1 key char secret1
ikev2 authentication psk id keyid site2 key char secret2
ikev2 default-profile
   child-pfs 2048-bit
   child-proposal enc aes-cbc-256
   child-proposal integrity sha1
   dpd interval 10
   local-authentication psk id keyid site1
   sa-proposal enc aes-cbc-256
   sa-proposal integrity sha1
   sa-proposal prf sha1

interface Tunnel1.0
   tunnel mode ipsec-ikev2
   ip unnumbered GigaEthernet1.0
   ikev2 outgoing-interface GigaEthernet0.0 10.0.0.254
   ikev2 peer 10.2.0.1 authentication psk id keyid site2
   no shutdown

【設定例】拠点 2 側
ikev2 authentication psk id keyid site1 key char secret1
ikev2 authentication psk id keyid site2 key char secret2
ikev2 default-profile
   dpd interval 10
   local-authentication psk id keyid site2

interface Tunnel0.0
   tunnel mode ipsec-ikev2
   ip unnumbered GigaEthernet1.0
   ikev2 outgoing-interface GigaEthernet0.0 10.0.1.254
   ikev2 peer 10.1.0.1 authentication psk id keyid site1
   no shutdown
```

以下、順番に設定方法を説明します。

2.38.2.1 IKEv2 ポリシーの設定（認証や暗号の設定）

はじめに IKEv2 ポリシーを設定します。IKEv2 では全体のポリシーを一括で設定するデフォルトプロファイルや、一部のポリシーをまとめて設定する IKEv2 プロファイル、またトンネル単位でポリシーをインタフェースに直接設定する方法など、3 種類の設定方法があります。

通常、装置で利用するポリシーは 1 つであるため、ここではデフォルトプロファイルの設定を説明します。その他の設定は、後述の項を参照してください。

なお、ポリシー設定は全ての項目が省略可能です。暗号や認証の設定は、省略しても高いセキュリティの設定が利用されるようにデフォルト動作を設定しています。省略した場合のポリシーは次のとおりです。

省略時の設定	
IKE-SA プロポーザル	暗号、認証、PRF、DH は、装置で対応しているものを全て提案します（H/W 対応していない認証アルゴリズムを除く）。相手から複数の提案を受けた場合は、最もセキュリティの高いものを採用します。
Child-SA プロポーザル	暗号、認証、PFS は、装置で対応しているものを全て提案します（H/W 対応していない認証アルゴリズムを除く）。相手から複数の提案を受けた場合は、最もセキュリティの高いものを採用します。
接続モード	トリガモード（パケット送受信時に SA 作成）
DPD（キープアライブ）	無効
ネゴシエーション方向	双方向
リプレイ攻撃検出	有効
トラフィックセレクタ	any 固定（IPv4, IPv6 全て）
イニシャルコンタクト	有効（変更不可）
出力インタフェース	固定しない
ソースアドレス	固定しない
再送とタイムアウト	2、4、8 秒間隔で再送し、16 秒後にタイムアウト（合計 30 秒）
IKE-SA ライフタイム	86400 秒（1 日）
Child-SA ライフタイム	28800 秒（8 時間）
フラグメント動作	ポストフラグメント（暗号化処理のあとフラグメント） ただし自生成パケットは常にプリフラグメントになります。
強制フラグメント設定	なし

デフォルトプロファイルの設定

デフォルトプロファイルは、以下のコマンドで設定します。

ikev2 default-profile	デフォルトプロファイルの設定

このプロファイルで設定したものは、全ての IKEv2/IPsec 通信に適用されます。ただし、デフォルトプロファイル以外の方法でポリシー設定を行っている場合は、そちらが優先されます。

自装置の認証設定

詳細は次の事前共有鍵の設定で説明します。

local-authentication	自装置の認証設定

プロポーザルの変更

暗号や認証の設定を 1 つまたはいくつかの組み合わせに限定できます。以下の設定で変更可能です。

sa-proposal は IKEv1 の ike proposal、child-proposal は IKEv1 の ipsec autokey-proposal 相当のコマンドです。また、IKEv1 の hash 相当の設定は integrity と prf を使います。

sa-proposal enc	IKEv2 プロポーザル 暗号化アルゴリズム設定
sa-proposal integrity	IKEv2 プロポーザル 認証アルゴリズム設定
sa-proposal prf	IKEv2 プロポーザル PRF アルゴリズム設定
sa-proposal dh	IKEv2 プロポーザル DH グループ設定
child-proposal enc	Child プロポーザル 暗号化アルゴリズム設定
child-proposal integrity	Child プロポーザル 認証アルゴリズム設定
child-pfs	Child PFS 設定

IKE-SA や Child-SA のプロポーザルで複数のアルゴリズムが選択されている場合、イニシエータ側は選択した全てを提案します。レスポンダ側の場合は提案されたものの中から1つ選択しますが、選択肢が複数ある場合はセキュリティが高いものを優先して利用します。

このため IKE-SA や Child-SA のプロポーザルを固定したい場合も、どちらかの装置で設定すれば他方の装置では設定を省略できます。

Lifetime の変更

Lifetime の変更は以下のコマンドで行います。

sa-lifetime	IKEv2 SA ライフタイム設定（デフォルト: 1 日）
child-lifetime	Child SA ライフタイム設定（デフォルト: 8 時間）

IKEv2 では lifetime はネゴシエーションされません。このため接続装置間で一致させる必要はありません。リキーは IKE-SA では lifetime の 30 秒前、Child-SA では lifetime の 60 秒前に実行します。

なお、相手が動的アドレス環境の場合はリキーを開始しないため、動的アドレス側の lifetime を長くしないでください。

DPD の変更

DPD（キープアライブ）の設定は以下のコマンドで行います。

dpd	キープアライブの設定

IKEv1 では DPD の設定を行っても、パケット受信中は通信可能と判断して、監視パケットの送信を抑制していました。IKEv2 では常に設定間隔で監視パケットを送信します（何らかの IKEv2 のネゴシエーションパケットを送受信している場合のみ送信が抑制されます）。

この機能かネットワークモニタ機能の、どちらかは有効にしておくことを推奨します。

アンチリプレイ機能

アンチリプレイ機能の設定は以下のコマンドで行います。

anti-replay	リプレイ検出 有効/無効設定

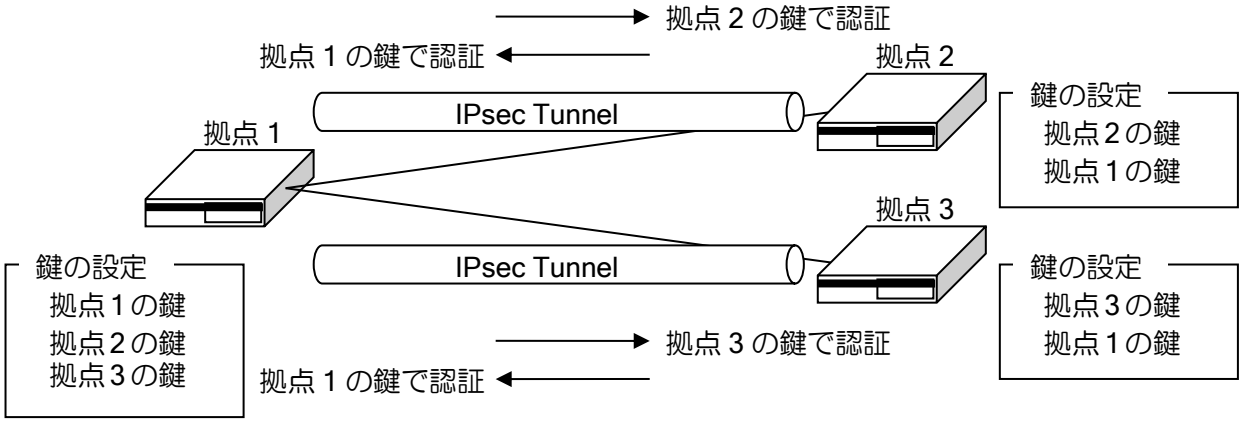
アンチリプレイの機能はデフォルト有効ですが、QoS の影響などでパケットの到着順序が入れ替わる可能性があるネットワークで利用される場合、アンチリプレイ機能が原因でパケットが破棄される可能性があります。そのような環境で利用する場合は、無効化してください。

2.38.2.2 事前共有鍵の設定

次に事前共有鍵の設定を行います。ID と鍵の設定は以下のコマンドで設定します。

ikev2 authentication	認証情報の設定
ikev2 default-profile	デフォルトプロファイルの設定
local-authentication	IKE 自装置情報設定
ikev2 peer	接続先登録

それぞれの装置で自装置を認証するための鍵と、接続相手が認証に使う鍵を設定します。



まず、自装置および全ての接続先の装置の ID と鍵の組み合わせ（データベース）を ikev2 authentication コマンドで用意します。次に、自装置の鍵を local-authentication psk で、接続先装置の鍵を ikev2 peer コマンドの authentication psk でそれぞれ設定します。

それぞれの装置の local-authentication の鍵と、その装置に接続している装置の peer の鍵が一致するように全ての装置を設定します。

```
【設定例】拠点 1
ikev2 authentication psk id keyid site1 key char secret1
ikev2 authentication psk id keyid site2 key char secret2
ikev2 authentication psk id keyid site3 key char secret3
ikev2 default-profile
  local-authentication psk id keyid site1   （拠点 1 の ID の鍵を自装置の鍵に指定）
interface Tunnel1.0
  ikev2 peer <拠点 2> authentication psk id keyid site2 （拠点 2 の鍵を指定）
interface Tunnel2.0
  ikev2 peer <拠点 3> authentication psk id keyid site3 （拠点 3 の鍵を指定）

【設定例】拠点 2 （拠点 3 も同様）
ikev2 authentication psk id keyid site1 key char secret1
ikev2 authentication psk id keyid site2 key char secret2
ikev2 default-profile
  local-authentication psk id keyid site2   （拠点 2 の ID の鍵を自装置の鍵に指定）
interface Tunnel0.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet0.0
  ikev2 peer <拠点 1> authentication psk id keyid site1 （拠点 1 の鍵を指定）
  no shutdown
```

※local-authentication を個別に設定する必要がある場合は、プロファイルやトンネルインタフェースに設定できます。

2.38.2.3 接続先の設定

接続先ごとの設定は主にトンネルインタフェースで行います。一部プロファイルでも設定可能です。

```
【設定例】

interface Tunnel0.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet1.0
  ikev2 outgoing-interface GigaEthernet0.0 auto
  ikev2 peer 10.1.0.1 authentication psk id keyid site1
  no shutdown
```

IKEv2 トンネルの設定と接続先の設定

以下の 2 つのコマンドは IKEv2 で必須の設定です。

tunnel mode ipsec-ikev2	IKEv2/IPsec 用のトンネル設定
ikev2 peer	接続先登録

tunnel mode ipsec-ikev2 でトンネルを IKEv2 専用に設定します。IKEv2 では、従来の IKEv1/IPsec で使用していたトンネルモード（tunnel more ipsec）は利用しません。

接続先は ikev2 peer コマンドを使用します。固定アドレスの場合はアドレスと ID を、不定アドレスの場合は any と ID を設定します。any の設定については動的アドレスの項目を参照してください。

Ver.8.8 以降、宛先を FQDN で指定することが可能です。指定した FQDN の名前解決を行い対応したアドレスを宛先として使用します。宛先の FQDN 指定を利用することにより、不定アドレス同士での接続が可能となります。詳細は DNS の項を参照してください。

名前解決の契機、アドレス更新時の動作、未解決時の動作は以下のとおりです。

名前解決の契機	定期的な更新
アドレス更新時の動作	該当する SA を削除
名前未解決時の動作	SA 作成不可

宛先を FQDN 指定時に ID を設定していない場合、宛先の FQDN を ID として使用します。

常時接続（オートコネクト）の設定

IPsec を常時接続する場合は以下のコマンドを設定してください。IPsec トンネルは通常は通信が発生したときにネゴシエーションを開始して SA を生成しますが（トリガ接続）、通信がなくても常に SA を作成、維持します。

ikev2 connect-type	SA 生成タイプ設定

常時接続の設定では、通信の有無に関わらず 10 秒間隔で IPsec トンネルの SA を周期的に監視し、SA が存在しない場合には SA を生成します。SA が存在しない状態でトンネルインタフェースは down となり、トンネル宛の経路は無効化されます。

出力先インタフェース、送信元アドレス固定設定

出力先インタフェースと送信元アドレスの固定設定は以下のコマンドで行います。

outgoing-interface ikev2 outgoing-interface	出力先設定
source-address ikev2 source-address	送信元アドレスの設定

出力先インタフェースは次のように決定されます。また、トンネルの up 条件もそれぞれ異なります。

出力先インタフェース	
出力先 I/F 設定なし	ルーティングテーブルを参照して、出力先 I/F とネクストホップを決定します。宛先への経路が存在すればトンネルは up します。
出力先 I/F 設定あり ネクストホップ指定 （アドレス指定）	ルーティングテーブルを参照せず、常に指定した I/F から送信します。出力先 I/F が up している場合のみトンネルが up します。
出力先 I/F 設定あり ネクストホップ指定 （auto 指定）	ルーティングテーブルを参照して、出力先 I/F とネクストホップを決定し、設定した出力先 I/F と一致する場合のみトンネルが up します。DHCP 使用時など、ネクストホップが指定できない場合にのみ auto を指定してください。

※ Ethenet のインタフェースの場合は nexthop または auto の設定が必要です。

送信元アドレスは次のように決定されます。

送信元アドレス	
送信元アドレス設定なし	イニシエータ時は送信インタフェースのアドレス レスポンダ時は受信したアドレス
送信元アドレス設定あり	設定したアドレス。設定したアドレスがインタフェースダウン等で無効になった場合は通信不可

出力先インタフェースを固定すると、これにより障害検出時にデフォルトルートを迂回させるような設定でも IPsec トンネルが迂回しなくなります。さらにネクストホップを設定すれば、障害検出による経路切り替えの際に IPsec トンネルが送信先を決定するためにルーティングテーブルを参照する必要がなくなるため、負荷が軽減されます。

Ver8.8 以降では outgoing-interface と source-address コマンドが受信インタフェースの選択にも使用されます。同一の peer アドレスに対して複数のインタフェースから IKEv2/IPsec トンネルを張ることも可能です。また、Ver8.8 以降では設定をプロファイル上で行うことも可能です。プロファイルを利用する全てのインタフェースに適用されます。

強制フラグメント設定

IPsec で暗号化したことにより送信インタフェースの MTU を超えた場合に、常にフラグメントを実行する設定です（IKEv1 の df-bit ignore と同様）。以下のコマンドで設定します。

ikev2 ipsec mtu ignore	MTU 無視設定

デフォルトでは df-bit がついているパケット、および IPv6 のパケットについては ICMP エラーを返します。TCP については ip tcp adjust-mss auto の設定でフラグメントの発生そのものを抑止できますので、設定しておくことを推奨します。

なお、自生成のパケット（Ping など）は常に強制的にフラグメントを行います。

フラグメント順序の設定

IPsec でフラグメントする場合に、暗号化を先に実行してからフラグメント処理を行うか（ポストフラグメント）、暗号化しても MTU を超えないようにフラグメントしてから暗号化を実行するか（プリフラグメント）を指定することができます。

ikev2 ipsec pre-fragment	プリフラグメントの設定

なお、自生成パケットは本コマンドの設定によらず、プリフラグメント動作となります。

トラフィックセレクタの設定

Ver.9.2 以降、イニシエータ時に通知するトラフィックセレクタを指定することができます。トラフィックセレクタは、相手装置と折衝することにより決定します。指定した場合、折衝した範囲に該当するパケットのみ送受信し、それ以外のパケットは廃棄します。トラフィックセレクタには、IP アドレス、プロトコル番号、ポート番号を指定することができます。

トラフィックセレクタは以下のコマンドで設定します。

local-ts ikev2 local-ts	ローカル側トラフィックセレクタの設定
remote-ts ikev2 remote-ts	リモート側トラフィックセレクタの設定

SA 作成時、イニシエータの装置は、設定されたトラフィックセレクタを相手装置に提案します。Ver.9.1 以前および設定しない場合は IPv4/IPv6 の全範囲を通知します。

レスポンダの装置は、設定に関係なくイニシエータが提案したトラフィックセレクタを使用します。

パケット送受信時は、トラフィックセレクタに該当する範囲以外のパケットは廃棄します。アドレス、ポートは送信時にはローカル側が送信元、リモート側が送信先になります。受信時は、ローカル側が送信先、リモート側が送信元となります。

NAT トラバーサル、トランスポートモードを併用する場合は、設定に関係無く IKE-SA で使用するアドレスを使用します。

2.38.3 NAT トラバーサル機能

Ver.9.2 以降 NAT トラバーサル機能を使用できます。NAT/NAPT を使用している環境でも、NAPT 内部の複数の IPsec クライアントが、1 つの NAPT アドレスを使用して同時に IPsec を利用できるようになります。

NAT トラバーサルは以下のコマンドで設定します。NAPT の変換テーブルを維持するため、keepalive は必ず設定してください。

ikev2 nat-traversal	NAT トラバーサルの設定
ikev2 nat-traversal keepalive	NAT トラバーサル キープアライブ送信間隔設定

IPsec 接続中に以下のコマンドを実行することにより、NAT トラバーサルで接続されていることを確認することができます。

show ikev2 sa	SA 情報表示

【表示例】

```
Interface Tunnel0.0
            :
      NAT detection : local side
      NAT-T keepalive interval[sec] : 20
            :
```

2.38.4 DELETE・REKEY 送信抑止設定

Ver9.5 以降、SA 削除時の DELETE メッセージの送信を抑止することができます。
また、REKEY メッセージの送信も抑止することができます。

suppress send-delete ikev2 suppress send-delete	DELETE 送信抑止の設定
suppress send-rekey ikev2 suppress send-rekey	REKEY 送信抑止の設定

上記のコマンドを使用するときは suppress send-delete と suppress send-rekey の両方の設定を推奨しています。
suppress send-delete のみ設定すると rekey による鍵の更新が失敗し、通信ができなくなります。

2.38.5 注意事項

フィルタ機能、NAPT 機能

IKEv2 の IPsec を送受信するインタフェースにフィルタや NAPT を設定する場合、IKE（UDP ポート番号：500, 4500）と ESP（プロトコル番号：50）を遮断しないように注意してください。

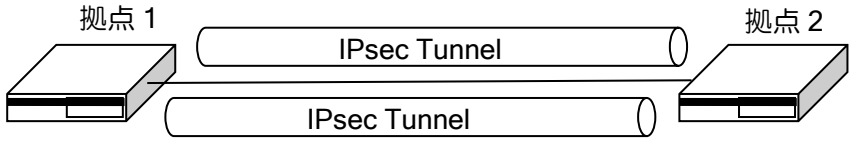
IKEv1 ではトンネルインタフェースに IPsec の設定がある IKE/IPsec パケットに関しては、フィルタリング設定や NAPT 設定を無視して送受信させるケースがありますが、IKEv2 ではフィルタリング設定や NAPT 設定がそのまま適用されます。IKEv1 の動作は変わりません。

【設定例】NAPT の場合

```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  ip napt enable
  ip napt static GigaEthernet0.0 udp 500
  ip napt static GigaEthernet0.0 udp 4500
  ip napt static GigaEthernet0.0 50
  no shutdown
```

同じ宛先に IKEv2 の IPsec を複数設定する場合

2 つの装置間に複数の IKEv2 を設定する場合、片方の拠点の peer アドレスを any にしてください。各トンネルは異なる ID を設定してください。



【設定例】

拠点 1

```
interface Tunnel0.0
  ikev2 local-authentication psk id keyid site1A
  ikev2 peer <拠点 2> authentication psk id keyid site2A

interface Tunnel1.0
  ikev2 local-authentication psk id keyid site1B
  ikev2 peer <拠点 2> authentication psk id keyid site2B
```

拠点 2

```
interface Tunnel0.0
  ikev2 local-authentication psk id keyid site2A
  ikev2 peer any authentication psk id keyid site1A

interface Tunnel1.0
  ikev2 local-authentication psk id keyid site2B
  ikev2 peer any authentication psk id keyid site1B
```

通常の設定とは異なる箇所のみ表示しています。

2.38.6 複数ポリシーの設定

2.38.6.1 IKEv2 プロファイルの設定

複数のポリシーで IKEv2 を利用したい場合は、IKEv2 プロファイルを設定します。複数の IKEv2 プロファイルでそれぞれポリシーを設定し、Tunnel インタフェースで利用したいプロファイルを指定することで、複数の設定が利用できます。

ikev2 profile	IKEv2 プロファイルの設定
ikev2 binding	IKEv2 プロファイルの割り当て

【設定例】

```
ikev2 profile prof1
   child-proposal enc aes-cbc-256
   child-proposal integrity sha1
   dpd interval 10
   sa-proposal enc aes-cbc-256
   sa-proposal integrity sha1

interface Tunnel0.0
   tunnel mode ipsec-ikev2
   ip unnumbered GigaEthernet0.0
   ikev2 binding prof1
   ikev2 peer 10.1.0.1 authentication psk id keyid site1
```

2.38.6.2 Tunnel インタフェースでの設定

Tunnel インタフェースに直接ポリシー設定を記述することも可能です（コマンドは全て先頭に ikev2 を付けます）。トンネルの設定をまとめて確認しやすくなります。

【設定例】

```
interface Tunnel0.0
   tunnel mode ipsec-ikev2
   ip unnumbered GigaEthernet0.0
   ikev2 child-proposal enc aes-cbc-256
   ikev2 child-proposal integrity sha1
   ikev2 dpd interval 10
   ikev2 sa-proposal enc aes-cbc-256
   ikev2 sa-proposal integrity sha1
   ikev2 sa-proposal prf sha1
   ikev2 peer 10.1.0.1 authentication psk id keyid site1
```

2.38.6.3 設定の優先度

同じ設定を複数の設定方法で行った場合は以下の順に設定が参照されます。

- Tunnel インタフェースの設定
- IKEv2 プロファイルの設定
- デフォルトプロファイルの設定
- デフォルト動作

2.38.7 IPsec リモートアクセス機能(拠点側動的アドレス対応)

拠点側のアドレスが不定の場合の設定方法について説明します。

基本的な設定は固定アドレスの場合と同じです。センタルータ側の ikev2 peer コマンドは、拠点側のアドレスを特定しないので any とし、拠点ごとの ID を設定してください。

【設定例】センタ側

```
ikev2 authentication psk id keyid center key char secret-c
ikev2 authentication psk id keyid site1 key char secret-s1
ikev2 authentication psk id keyid site2 key char secret-s2
                    :
ikev2 default-profile
  local-authentication psk id keyid center
interface Tunnel1.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet0.0
  ikev2 peer any authentication psk id keyid site1
  no shutdown
interface Tunnel2.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet0.0
  ikev2 peer any authentication psk id keyid site2
  no shutdown
        :
```

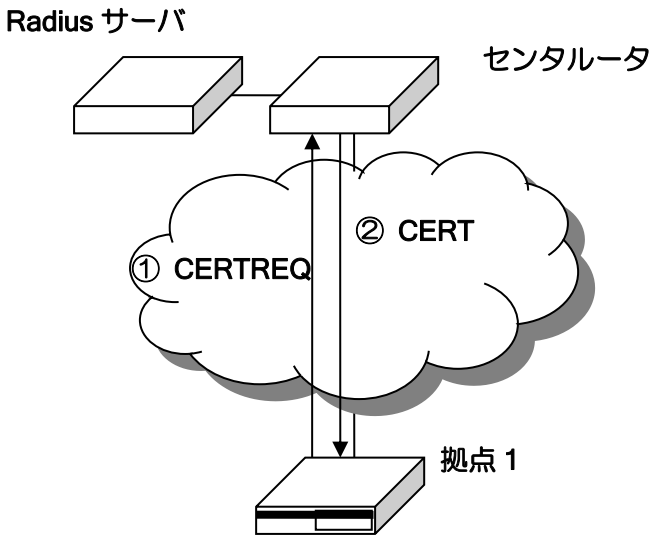
【設定例】拠点 1 側

```
ikev2 authentication psk id keyid center key char secret-c
ikev2 authentication psk id keyid site1 key char secret-s1
ikev2 default-profile
  local-authentication psk id keyid site1
interface Tunnel0.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet0.0
  ikev2 peer 10.0.0.1 authentication psk id keyid center
  no shutdown
```

動的アドレス環境の場合、各種ポリシーの設定はデフォルトプロファイルに記載してください。IKEv2 のイニシエータが送信する最初のパケットには ID 情報が含まれないため、最初のパケット受信では受信インタフェースの設定を参照できないためです。

2.38.8 その他の認証方式

2.38.8.1 デジタル署名認証



IX ルータがサポートしているデジタル署名認証の機能は、認証局が発行する CA 証明書を使って接続先の装置を認証する機能です（Ver.10.0 以前は、上図の拠点ルータの動作のみ）。

デジタル署名認証では、pki cert import コマンドでルータに事前に CA 証明書をインストールする必要があります。

動作概要

拠点側ルータがセンタルータに接続する場合のデジタル署名認証は次のように動作します。

最初に拠点側ルータからセンタ側ルータへ認証要求を行います。拠点側ルータは CA 証明書内の公開鍵を使ってセンタ側ルータへ CERTREQ ペイロード含めて認証要求を送信します。

CERTREQ ペイロードを含む認証要求を受けたセンタ側ルータでは、CERTREQ ペイロードを解析して CA を特定し、その CA 証明書に署名された証明書と秘密鍵で CERT ペイロードを生成して認証応答に含めて応答します。

CERT ペイロードを含む認証応答を受けた拠点側ルータは、CA 証明書のデジタル署名と公開鍵で CERT ペイロードを検証し、問題がなければ認証が成功します。

証明書の取得

証明書の取得/削除は以下のコマンドで行います。

pki cert import	証明書のインポート
pki cert erase	証明書の削除
pki cert export	証明書のエクスポート

証明書の取得は URL を指定して直接取得する方法と、テキスト形式で show コマンドの表示結果を流し込む方法があります。

```
【https で取得】
pki cert import pem name caCert url https://192.168.100.1/Cert/caCert.pem

【コマンドで流し込み】
pki cert import pem name caCert
Input certificate(abort with CNTL/C).
-----BEGIN CERTIFICATE-----
```

```
MIIBoDCCAUqgAwIBAgIBATANBgkqhkiG9w0BAQQFADAmMSQwIgYDVQ...
bzEuY2lzY28uY29tIEw9UlRQIEM9SlAwHhcNMTEwNzA4MDEzNDE5WhcN...
nJ7N/GI0XqkPrmIGP4xfU/exaa8VVMbGjof+aCyoJOVBYECfvRLcZQIDAQA...
dHRdkIYIJ8S8m7whVoDTOXAYtDAdBgNVHQ4EFgQUbXR0XZCGCCfEvJu...
...
-----END CERTIFICATE-----
```

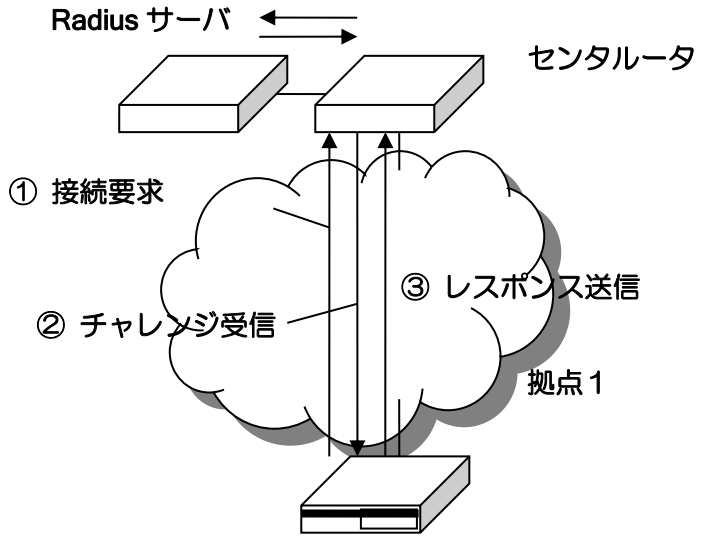
取得した証明書は、証明書バンドルファイル（SYSTEM-CERT-BUNDLE）に保存されます。show flash で表示可能ですが、削除は pki cert erase コマンドでしかできません。

テキスト形式の証明書は、pki cert export コマンドでも表示されます。

設定例

設定例は、次の EAP-MD5 とあわせて示します。

2.38.8.2 EAP-MD5 認証



EAP-MD5 認証は、接続要求を行う拠点側の装置の機能に対応しています。

動作概要

拠点側ルータがセンタルータに接続する場合の EAP-MD5 認証は次のように動作します。

拠点ルータが接続要求を行うと、センタ側の装置からチャレンジが送信されます。チャレンジと ID と鍵を元に応答パケットを送信することで、チャレンジレスポンス方式でリモート認証が行われます。

2.38.8.3 設定例

拠点側はセンタ側の認証にデジタル署名を使用し、センタ側は拠点側の認証に EAP-MD5 を使用する構成の、拠点側のコンフィグ例です。

IKEv2 以外の設定や、IKEv2 のプロファイル設定は省略しています。

```
【設定例】

ikev2 authentication eap-md5 id fqdn site1.example.com key char secret1
interface Tunnel0.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet0.0
  ikev2 cert cacert name caCert
  ikev2 local-authentication eap-md5 id fqdn site1.example.com
  ikev2 peer 192.168.0.1 authentication rsa id fqdn center.example.com
  no shutdown
```

2.38.9 表示コマンド/イベントログ

IKEv2 の動作確認のためのコマンドについて説明します。

2.38.9.1 show ikev2 sa

show ikev2 sa で IKE-SA の状態を表示できます。
表示される内容は以下のとおりです。

【表示例】

```
Interface Tunnel0.0
  SPI (I)0xf633bdfd0188a348  (R)0xc35d1aa6e0ce1c67
    Remain lifetime[sec] : 86381
    Serial : 11
    Direction : initiator
    Local Addr  : 10.1.0.1:500
    Remote Addr : 10.2.0.1:500
    Local ID : IPv4-ADDR 10.1.0.1
    Peer ID  : IPv4-ADDR 10.2.0.1
    Status : establish
    Local message ID : 2
    Peer message ID  : 0
    Encryption alg : AES-CBC-256
      initiator key : 0xa4610bea…
      responder key : 0x0fdae963…
    Integrity alg : HMAC-SHA1-96
      initiator key : 0xf1f246b6...
      responder key : 0x6e32c07a…
    PRF alg  : HMAC-SHA1
    DH group : MODP-1536
    PFS : MODP-2048
    DPD : disable
    Child
      Prot SPI(IN)      SPI(OUT)     Lifetime[sec]
      ESP  0x1511ab8e 0x571a182d 28780
```

2.38.9.2 show ikev2 child-sa

show ikev2 child-sa で Child-SA の状態を表示できます。
また、SA が生成された場合と全て削除された場合について、過去 10 回分の履歴を表示します。

【表示例】

```
Interface Tunnel0.0
  IKE Peer ID : IPv4-ADDR 10.2.0.1
    IKE SPI (I)0xf633bdfd0188a348  (R)0xc35d1aa6e0ce1c67
    IKE SA serial : 11
    Child SA
      Protocol : ESP
      Local Addr : 10.1.0.1
      Peer Addr  : 10.2.0.1
      Enc alg  : AES-CBC-256
      Hash alg : HMAC-SHA1-96
      Remain lifetime[sec] : 28776
      Anti-replay : on
      Direction is outbound
```

```
        SPI : 0x571a182d
        Serial : 4
        Authkey : 0x4dd70b5f…
        Enckey   : 0xace632bd…
    Direction is inbound
        SPI : 0x1511ab8e
        Serial : 3
        Authkey : 0x5cf49660…
        Enckey   : 0xba70b368…
    Local TS:
    TS type : IPV4-ADDR-RANGE
        Protocol 0
        Address Range 0.0.0.0 to 255.255.255.255
        Port Range 0 to 65535
    Peer TS:
    TS type : IPV4-ADDR-RANGE
        Protocol 0
        Address Range 0.0.0.0 to 255.255.255.255
        Port Range 0 to 65535
Statistics
    Outbound
        9 packets, 756 octets
        0 cipher failure,   0 out of memory, 0 ts unacceptable
        122 misc error
    Inbound
        9 packets, 756 octets
        0 invalid sa, 0 replay detected, 0 integrity failure
        0 cipher failure, 0 packet truncated, 0 invalid padding,
        0 unknown protocol, 0 out of memory, 0 ts unacceptable
        0 misc error
History
    Time                        Event
    2011/01/01 09:00:40 Create
    2011/01/01 19:22:03 Delete : Delete IKE SA by command
    2011/01/01 19:22:29 Create
```

show ikev2 sa では現在通信に使用している鍵の内容も表示します。キャプチャデータを復号して解析する場合などに利用します。

2.38.9.3 イベントログ

IKEv2 のイベントログは ike2 を使用します。ike は IKEv1 専用です。IPsec については、従来同様 sec を使用します。

ikev2 のイベントログは主に以下のように構成されています。

主なイベント	
Error / Warning	SA の生成削除および何らかの異常が発生した場合
Notice	ネゴシエーションの開始、終了、タイムアウト（DPD を除く）
Info	DPD、Cookie などの情報
Debug	送受信パケットの詳細情報、作成した鍵情報

通常は Warning で利用し、問題が発生した場合に適宜 Notice、Info などの設定を検討してください。Debug については大量にログが表示されますので通常は利用しないでください。

鍵の情報を含むイベントログは syslog では送信されません。

■2.39 ダイナミック VPN の設定

IX2000/IX3000 シリーズでは、Ver9.2 以降でダイナミック VPN 機能が利用できます。

2.39.1 ダイナミック VPN の概要

ダイナミック VPN では、ハブ（センタ側）とスポーク（拠点側）の構成において、スポーク間の動的な VPN 接続を行うことができます。

センタ側はダイナミック用のトンネルを設定するのみで複数拠点と VPN を接続することができます。また、拠点側は、センタ側との接続設定を行うのみで、拠点間の VPN 設定は行わずに VPN の接続ができます。

センタと拠点間は起動時に VPN を接続し、VPN は接続したままとなります。拠点間の VPN は拠点間の通信が発生した時に、VPN を接続し、無通信状態が継続すると VPN を切断します。

ダイナミック VPN では以下の機能を使用します。

- 動的接続対応機能：NHRP
- VPN 機能：IKEv2+GRE トンネル
- ルーティング機能：BGP、スタティックルート

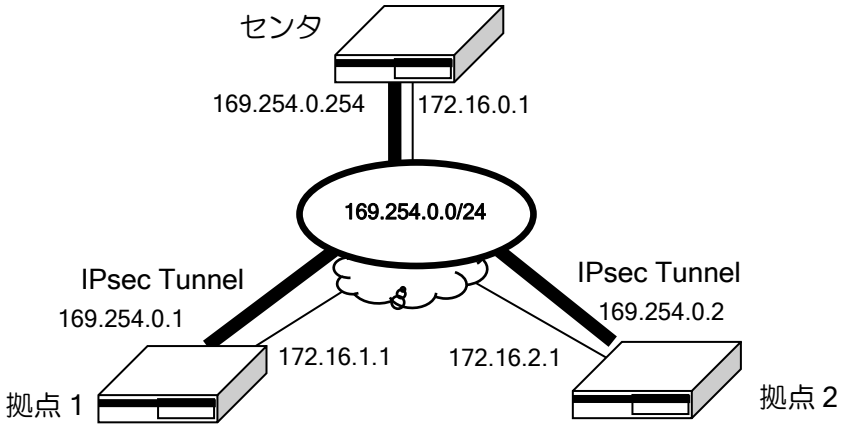
2.39.1.1 制限事項

- IX と WA(Ver8.6 以降)のみ接続可能です。それ以外の装置とは接続できません。
- NAT 配下の装置とは直接 VPN 接続は行わず、センタ側を経由します。
- GRE のキープアライブ機能は使用できません。
- ダイナミック VPN のトンネルには以下は送信できません。
  - ✧ IPv6 パケット
  - ✧ Ethernet フレーム
  - ✧ マルチキャストパケット
  - ✧ ブロードキャストパケット
- ダイナミック VPN トンネルと IKEv2/IPsec トンネルを同時に利用する場合、以下の制限があります。
  - ✧ IPsec トンネル側の peer が固定(any 以外)の場合、ダイナミック VPN のトンネル番号は IPsec のトンネル番号よりも老番にする必要があります。
  - ✧ IPsec のトンネル側の peer が不定(any)の場合、IPsec のトンネル番号はダイナミック VPN のトンネル番号よりも老番にする必要があります。

2.39.2 設定例

2.39.2.1 基本構成

1 台のセンタと複数拠点を使用する構成です。



【設定例】

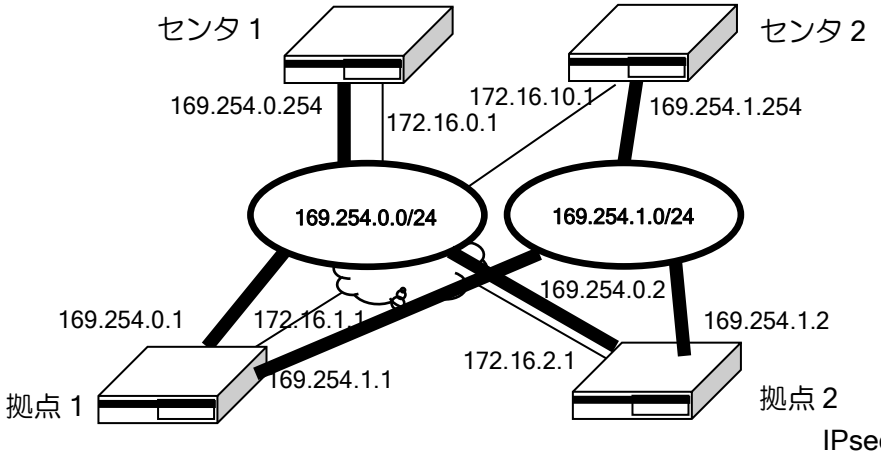
センタ側

```
ip route default 172.16.0.254

ikev2 authentication psk id ipv4 169.254.0.254 key char test

route-map redist-connect permit 10
   match interface GigaEthernet2.0
!
route-map set-nexthop permit 10
   set ip next-hop 169.254.0.254
!
router bgp 65534
   address-family ipv4 unicast
      redistribute connected route-map redist-connect
   peer-group dmvpn-group remote-as 65534
      listen range 169.254.0.0/24
      connect-interval 10
      timers 5 15
      route-reflector-client
      address-family ipv4 route-map set-nexthop out
!
interface GigaEthernet0.0
   ip address 172.16.0.1/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode mgre ipsec-ikev2
   ip address 169.254.0.254/24
   ip tcp adjust-mss auto
   ikev2 local-authentication psk id ipv4 169.254.0.254
   ikev2 outgoing-interface GigaEthernet0.0 172.16.0.254
   ikev2 ipsec-mode transport
```

```
   ikev2 peer any authentication psk
   no shutdown

拠点 1 側
拠点 2 側も同様な設定となります。

ip route default 172.16.1.254

nhrp local GigaEthernet1.0
!
ikev2 authentication psk id ipv4 169.254.0.1 key char test
!
route-map redist-connect permit 10
   match interface GigaEthernet1.0
!
router bgp 65534
   neighbor 169.254.0.254 remote-as 65534
   neighbor 169.254.0.254 connect-interval 10
   neighbor 169.254.0.254 timers 5 15
   address-family ipv4 unicast
      redistribute connected route-map redist-connect
!
interface GigaEthernet0.0
   ip address 172.16.1.1/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 192.168.1.254/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode mgre ipsec-ikev2
   ip address 169.254.0.1/24
   ip tcp adjust-mss auto
   nhrp nhs 169.254.0.254/24 nbma 172.16.0.1
   ikev2 dpd interval 10
   ikev2 local-authentication psk id ipv4 169.254.0.1
   ikev2 outgoing-interface GigaEthernet0.0 172.16.1.254
   ikev2 ipsec-mode transport
   ikev2 peer any authentication psk
   no shutdown
```

2.39.2.2 センタ冗長構成

センタ装置を複数台用意して、冗長構成にすることも可能です。



Ver9.7 以降では、トンネルインタフェースで nhrp shortcut-priority コマンドを設定することで、ショートカット経路の優先度を簡単に設定することができます（値の小さい方が優先、設定なしが最低優先）。Ver9.6 までは BGP の優先度を MED で設定する必要があります。

【センタ 1, 2 設定例】
基本構成と同一のため省略します。ただし、センタ 1 とセンタ 2 のトンネルインタフェースのアドレスは、異なるものを使用してください。

【拠点 1, 2 設定例】
拠点 1 の例を示します。拠点 2 も同様です。

```
ip route default 172.16.1.254
!
nhrp local GigaEthernet1.0
!
ikev2 authentication psk id ipv4 169.254.0.1 key char test
ikev2 authentication psk id ipv4 169.254.1.1 key char himitsu
!
route-map redist-connect permit 10
   match interface GigaEthernet1.0
!
route-map set-ip permit 10
   set local-preference 50
!
router bgp 65534
   neighbor 169.254.0.254 remote-as 65534
   neighbor 169.254.0.254 connect-interval 10
   neighbor 169.254.1.254 remote-as 65534
   neighbor 169.254.1.254 connect-interval 10
   address-family ipv4 unicast
      neighbor 169.254.1.254 route-map set-ip in
      redistribute connected route-map redist-connect
!
interface GigaEthernet0.0
   ip address 172.16.1.1/24
   no shutdown
!
interface GigaEthernet1.0
```

```
   ip address 192.168.1.254/24
   no shutdown
!
interface Tunnel0.0
   tunnel mode mgre ipsec-ikev2
   ip address 169.254.0.1/24
   nhrp shortcut-priority 1
   nhrp nhs 169.254.0.254/24 nbma 172.16.0.1
   ikev2 dpd interval 10
   ikev2 local-authentication psk id ipv4 169.254.0.1
   ikev2 outgoing-interface GigaEthernet0.0 172.16.1.254
   ikev2 ipsec-mode transport
   ikev2 peer any authentication psk
   no shutdown
!
interface Tunnel1.0
   tunnel mode mgre ipsec-ikev2
   ip address 169.254.1.1/24
   nhrp nhs 169.254.1.254/24 nbma 172.16.10.1
   ikev2 dpd interval 10
   ikev2 local-authentication psk id ipv4 169.254.1.1
   ikev2 outgoing-interface GigaEthernet0.0 172.16.1.254
   ikev2 ipsec-mode transport
   ikev2 peer any authentication psk
   no shutdown
```

2.39.3 各機能の設定

2.39.3.1 NHRP 機能

宛先ネットワークへのトンネルのネクストホップのアドレス解決のために、NHRP（NextHop Resolution Protocol）を使用しています。

センタ側は NHRP の設定は必要ありません。
拠点側はセンタ側に接続するための設定を設定します。接続先に FQDN を指定することができます。

NHRP では、拠点（スポーク）間の通信をする際にトンネルの宛先の IP アドレスを解決します。解決した IP アドレスを使用して VPN の接続を行います。また、NHRP ではトンネルの IP アドレスの解決を行うため、必ずトンネルの IP アドレスの設定が必要となります。

設定方法は以下のとおりです。

nhrp nhs	接続するセンタの設定 （インタフェースコンフィグモード）
nhrp local	ローカルインタフェースの設定 （グローバルコンフィグモード）
nhrp disable-traffic-indication	拠点間の動的接続抑止設定 （グローバルコンフィグモード）
nhrp holding-time	NHRP キャッシュの生存時間設定 （グローバルコンフィグモード）
nhrp register-holding-time	登録用 NHRP キャッシュの生存時間設定 （インタフェースコンフィグモード）
nhrp max-connections	センタ側最大接続数の設定（Ver.9.3 以降）

【設定例】
NHRP の設定は不要です。
拠点側は、センタ（HUB）のトンネルアドレスと物理アドレスを設定します。

```
nhrp local GigaEthernet2.0

interface Tunnel0.0
  tunnel mode mgre ipsec-ikev2
  ip address 169.254.0.1/24
  nhrp nhs 169.254.0.254/24 nbma 10.0.0.254
   :
```

2.39.3.2 VPN 機能

VPN 機能として GRE トンネルと IKEv2 を使用します。
センタ側は 1 つのトンネルで全ての拠点の VPN 接続を行います。

ダイナミック VPN では、拠点間通信の IP アドレス解決用に GRE トンネルにネットワークを割り当て、各装置にアドレスを設定する必要があります。

設定方法は以下のとおりです。

tunnel mode mgre ipsec-ikev2	ダイナミック VPN 設定 （インタフェースコンフィグモード）
ikev2 peer	ピア設定 （インタフェースコンフィグモード）
ikev2 outgoing-interface outgoing-interface	出力インタフェース設定 （インタフェースコンフィグモード、 IKEv2 プロファイルコンフィグモード）
ikev2 local-authentication local-authentication	自装置認証設定 （インタフェースコンフィグモード、 IKEv2 プロファイルコンフィグモード）
ikev2 ipsec-mode transport ipsec-mode	トランスポートモード設定 （インタフェースコンフィグモード IKEv2 プロファイルコンフィグモード）

【設定例】
・トンネル設定
トンネルモードは mgre ipsec-ikev2 を設定してください。
Unnumbered 設定は行わず、アドレスを設定してください。

・IKEv2 設定
接続先は、NHRP で制御するためピアは any で設定します。
認証設定はセンタ側と拠点側で同じ事前共有鍵を使用してください。
また、自装置の ID はトンネルのアドレスを使用してください。
IPsec 動作モードはトランスポートを使用してください。

```
ikev2 authentication psk id ipv4 169.254.0.1 key char test

interface Tunnel0.0
  tunnel mode mgre ipsec-ikev2
  ip address 169.254.0.1/24
  nhrp nhs 169.254.255.254/24 nbma 10.0.0.254
  ikev2 local-authentication psk id ipv4 169.254.0.1
  ikev2 outgoing-interface GigaEthernet0.0 172.16.1.254
  ikev2 ipsec-mode transport
  ikev2 peer any authentication psk
  no shutdown
```

2.39.3.3 ルーティング機能

ルーティングの設定ではスタティックルートと BGP を使用することができます。
BGP ではピアを動的に学習するため、拠点追加時の設定の追加が不要となります。
スタティックルートでの運用も可能ですが、拠点追加毎に設定の追加が必要となります。

以下、BGP の場合の設定方法を説明します。

peer-group	ピアグループ設定（センタ側） （BGP コンフィグモード）
listen range	ピア範囲指定（センタ側） （BGP ピアグループコンフィグモード）
bgp listen limit	動的ピア接続最大数 （BGP コンフィグモード）

route-reflector-client	ルートリフレクタ設定 （BGP ピアグループコンフィグモード）
address-family ipv4 route-map	ルートマップ設定 （BGP ピアグループコンフィグモード）
neighbor remote-as	ピア設定（拠点側） （BGP ピアグループコンフィグモード）

【設定例】
・共通設定
同一 VPN 内の装置は全て同じ AS に設定してください。
同一 VPN 内の装置は keepalive, holdtime は全て同じ値に設定してください。
他の装置からアクセスされる経路については、再配信設定してください。
ダイナミック VPN のトンネルのネットワークは再配信しないでください。

・センタ側設定
センタ側は事前に拠点側のアドレスは特定できません。
そのため、ピア設定は範囲指定します。トンネルに設定したネットワークアドレスを含む範囲を設定してください。
拠点間はピア接続設定を行わないため、ルートリフレクタを設定してください。
センタ側がネクストホップとなるようにネクストホップを設定してください。

```
route-map set-nexthop permit 10
  set ip next-hop 169.254.0.254

router bgp 65534
  peer-group dmvpn-group remote-as 65534
    listen range 169.254.0.0/24
    route-reflector-client
    address-family ipv4 route-map set-nexthop out
```

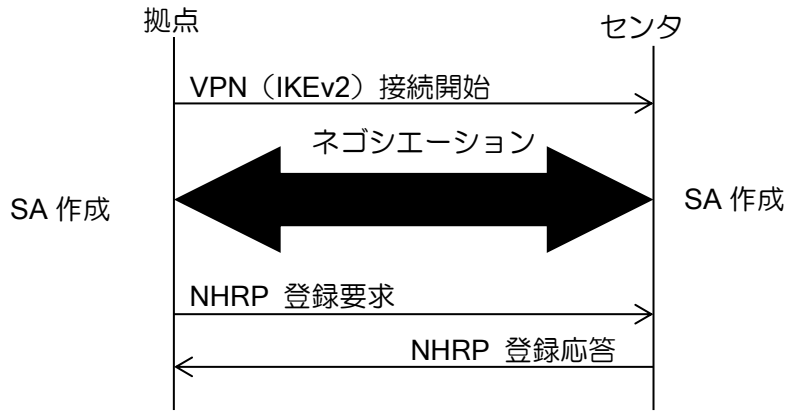
・拠点側設定
センタ側とピア接続してください。

```
router bgp 65534
  neighbor 169.254.255.254 remote-as 65534
  address-family ipv4 unicast
    redistribute connected
```

2.39.4 動作

2.39.4.1 接続動作

拠点側は最初に VPN の接続を行います。VPN 接続完了後、センタ側へ NHRP の登録要求を行います。センタに登録されると拠点間の動的な VPN 接続が可能となります。



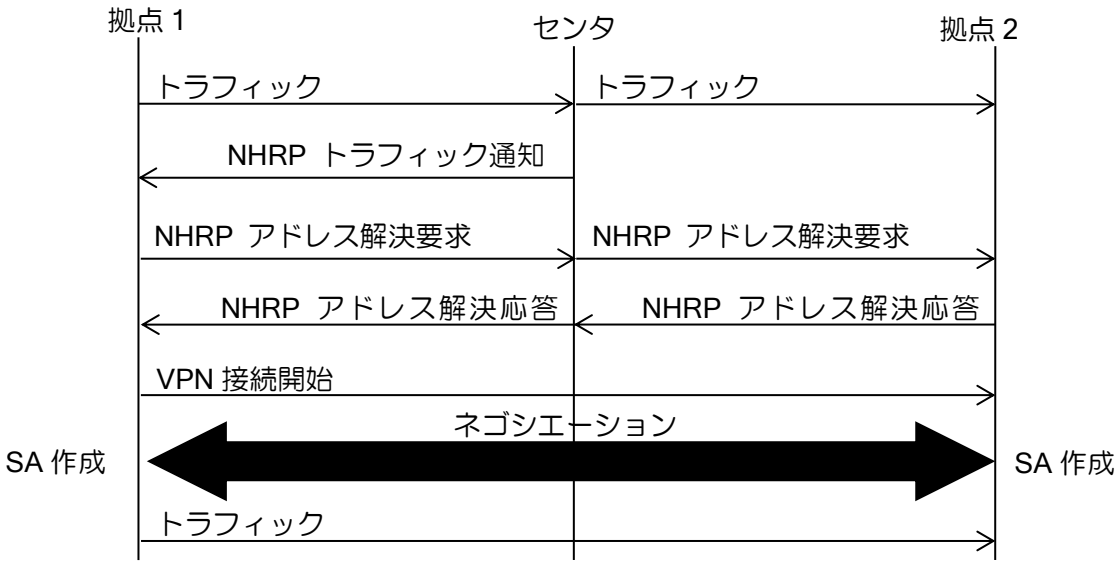
2.39.4.2 拠点間接続

拠点間の VPN はトラフィックが発生した場合に接続を行います。別拠点宛の最初のパケットはセンタ側に送信されます。その後、NHRP により宛先ネットワークに転送するためのネクストホップのアドレス解決を行い、解決したアドレスに対して VPN 接続を行います。VPN 接続が完了した時点で、解決したネクストホップを使用したスタティックルートが登録され、拠点間は直接通信を行います。

センタは別拠点宛のトラフィックを受信した場合、トラフィック通知監視のためトリガパケット情報を作成し、送信元の拠点にトラフィック通知を送信します。拠点間の VPN が接続し、拠点間の通信を開始した後、一定時間（120 秒）経過するとトリガパケット情報を削除します。同時に処理を行えるトラフィック通知監視数が装置の最大に達した場合、トラフィック通知を送信せず、センタ経由の通信のままとなります、

また、トラフィック通知を抑止することにより、拠点間の動的接続を抑止することができます。

nhrp disable-traffic-indication	拠点間の動的接続抑止設定 （グローバルコンフィグモード）



2.39.4.3 切断

トンネル切断の検出には、IKEv2 DPD 機能を使用します。障害時は SA が削除されトンネルがダウンします。また、出力インタフェースダウン時にもトンネルはダウンします。

BGP のキープアライブでは、障害時には BGP のピアがダウンし、経路情報は削除されますが、トンネルはダウンしません。

ikev2 dpd interval dpd interval	IKEv2 DPD タイマ設定 （インタフェースコンフィグモード IKEv2 プロファイルコンフィグモード）
timers	BGP タイマ設定 （BGP コンフィグモード BGP ピアグループコンフィグモード）

2.39.5 状態確認

ダイナミック VPN の情報は以下のコマンドで参照できます。

一度接続した拠点の情報は、VPN が切断してもクリアされるまでは情報は削除されません。

show dmvpn	ダイナミック VPN 状態表示

2.39.6 ダイナミック VPN の VRF 構成

Ver9.7 以降ではダイナミック VPN を VRF ごとに利用可能です。拠点側、センタ側、どちらも VRF 対応にすることができます。設定はダイナミック VPN の章を参照してください。

2.39.6.1 注意事項

ダイナミック VPN で使用するトンネル内部の IP アドレスは、VRF が異なっていても同じアドレスを使用しないでください。必ずどの装置にも設定されていないアドレスを使用してください。IKEv2/IPsec の ID としても利用するため、VRF に関わらず区別できる必要があります。

LAN 側 IP アドレスなどは重複可能です。

2.39.6.2 設定例（拠点側）

【設定例】

VRF の設定
GigaEthernet1.1 に接続した LAN の通信を Tunnel1.0 から送信
GigaEthernet1.2 に接続した LAN の通信を Tunnel2.0 から送信

```
ip prefix-list lan 10 permit 192.168.0.0/16 min 16 max 32
!
nhrp local GigaEthernet1.1
nhrp local GigaEthernet1.2
!
ikev2 authentication psk id ipv4 172.16.1.1 key char secret-1
ikev2 authentication psk id ipv4 172.16.2.1 key char secret-2
!
route-map lan permit 10
  match ip address prefix-list lan
!
router bgp 65000
  router-id 10.0.0.1
  vrf 1
    neighbor 172.16.1.254 remote-as 65000
    neighbor 172.16.1.254 connect-interval 10
    address-family ipv4 unicast
      redistribute connected route-map lan
  vrf 2
    neighbor 172.16.2.254 remote-as 65000
    neighbor 172.16.2.254 connect-interval 10
    address-family ipv4 unicast
      redistribute connected route-map lan
!
interface GigaEthernet0.0
  ip address 10.0.0.1/8
  no shutdown
!
interface GigaEthernet1.1
  encapsulation dot1q 101 tpid 8100
  auto-connect
  ip vrf forwarding 1
  ip address 192.168.1.254/24
  no shutdown
!
interface GigaEthernet1.2
  encapsulation dot1q 201 tpid 8100
  auto-connect
```

```
   ip vrf forwarding 2
   ip address 192.168.1.254/24
   no shutdown
!
interface Tunnel1.0
   tunnel mode mgre ipsec-ikev2
   ip vrf forwarding 1
   ip address 172.16.1.1/16
   nhrp nhs 172.16.1.254/16 nbma 10.0.0.254
   ikev2 dpd interval 10
   ikev2 local-authentication psk id ipv4 172.16.1.1
   ikev2 outgoing-interface GigaEthernet0.0 auto
   ikev2 ipsec-mode transport
   ikev2 peer any authentication psk
   no shutdown
!
interface Tunnel2.0
   tunnel mode mgre ipsec-ikev2
   ip vrf forwarding 2
   ip address 172.16.2.1/16
   nhrp nhs 172.16.2.254/16 nbma 10.0.0.254
   ikev2 dpd interval 10
   ikev2 local-authentication psk id ipv4 172.16.2.1
   ikev2 outgoing-interface GigaEthernet0.0 auto
   ikev2 ipsec-mode transport
   ikev2 peer any authentication psk
   no shutdown
```

2.39.6.3 設定例（センタ側）

センタ側で VRF を使用する場合は次のとおりです。

なお、VRF を設定することで IPsec トンネルの消費が増えるため、IPsec の設定数が不足する場合は、VRF ごとに収容するセンタルータを分けるなどで、対応してください。

```
【設定例】

ip prefix-list lan 10 permit 192.168.0.0/16 min 16 max 32
!!
ikev2 authentication psk id ipv4 172.16.1.254 key char secret-1
ikev2 authentication psk id ipv4 172.16.2.254 key char secret-2
!
route-map export permit 10
   set ip next-hop self
!
route-map lan permit 10
   match ip address prefix-list lan
!
router bgp 65000
   router-id 10.0.0.254
   vrf 1
      address-family ipv4 unicast
         redistribute connected route-map lan
      peer-group kyoten remote-as 65000
         listen range 172.16.0.0/16
         timers 10 30
         route-reflector-client
         address-family ipv4 route-map export out
   vrf 2
```

```
      address-family ipv4 unicast
        redistribute connected route-map lan
      peer-group kyoten remote-as 65000
        listen range 172.16.0.0/16
        timers 10 30
        route-reflector-client
        address-family ipv4 route-map export out
!
interface GigaEthernet0.0
  description WAN
  ip address 10.0.0.254/8
  no shutdown
!
interface GigaEthernet1.1
  encapsulation dot1q 100 tpid 8100
  auto-connect
  ip vrf forwarding 1
  ip address 192.168.0.254/24
  no shutdown
!
interface GigaEthernet1.2
  encapsulation dot1q 200 tpid 8100
  auto-connect
  ip vrf forwarding 2
  ip address 192.168.0.254/24
  no shutdown
!
interface Tunnel1.0
  tunnel mode mgre ipsec-ikev2
  ip vrf forwarding 1
  ip address 172.16.1.254/16
  ikev2 dpd interval 10
  ikev2 local-authentication psk id ipv4 172.16.1.254
  ikev2 outgoing-interface GigaEthernet0.0 auto
  ikev2 ipsec-mode transport
  ikev2 peer any authentication psk
  no shutdown
!
interface Tunnel2.0
  tunnel mode mgre ipsec-ikev2
  ip vrf forwarding 2
  ip address 172.16.2.254/16
  ikev2 dpd interval 10
  ikev2 local-authentication psk id ipv4 172.16.2.254
  ikev2 outgoing-interface GigaEthernet0.0 auto
  ikev2 ipsec-mode transport
  ikev2 peer any authentication psk
  no shutdown
```

■2.40 QoS の設定

ユーザ/アプリケーションごとなど自由にトラフィックを分別し、それぞれのトラフィックごとに様々な優先度を設定し、優先度に応じたサービスを実現することが可能です。

IX2000/IX3000 シリーズでは以下の QoS 機能に対応しています。

優先制御・帯域制御機能

- ローレイテンシキューイング（LLQ）
  - 音声パケットなどの遅延（レイテンシ）が問題になるパケットを最優先で送信するための機能です。キューイングせずにパケットを送信する形となり、ここに分類されたパケットは最小限の遅延で最優先に送信されます。
  - FastEthernet, GigaEthernet インタフェースのみサポートとなります。

- クラスベースキューイング（CBQ）
  - QoS クラス毎のキューに重み付けを行い、その割合によってパケットの出力を制御します。指定した割合は最小予約帯域として必ず確保されるので、重み付けの小さいクラスでも通信量が制限されることはあっても通信できなくなることはありません。

- プライオリティキューイング（PQ）

  High/Medium/Normal/Low という 4 つの優先度の異なるキューにキューイングし、優先順位に従って出力します。高いプライオリティのパケットが流れている間は、低いプライオリティのパケットは流れません。ver8.9 以降は、キューの階数を High/Medium/Normal/Low/ Sub-a/Sub-b/Sub-c/Sub-d の 8 段階で設定できます。

- トラフィックシェーピング
  - クラスまたはインタフェース単位で帯域を制御し、最大転送レート制限によるパケットの出力を行います。ただし、Ver8.4 までは 100Mbps を越える設定はサポートしておりません。

- VoIP フォワーディング制御
  - 低速回線での VoIP の制御機能です。VoIP の章を参照してください

- SW-HUB ポート入力優先制御・・・Ver.8.3 以降
  - SW-HUB 内の各ポート間の入力時の優先制御を行います。

マーキング・カラーリング機能

- マーキング・カラーリング
  - パケットに DSCP 値，Precedence 値、または CoS 値の付与を行います。

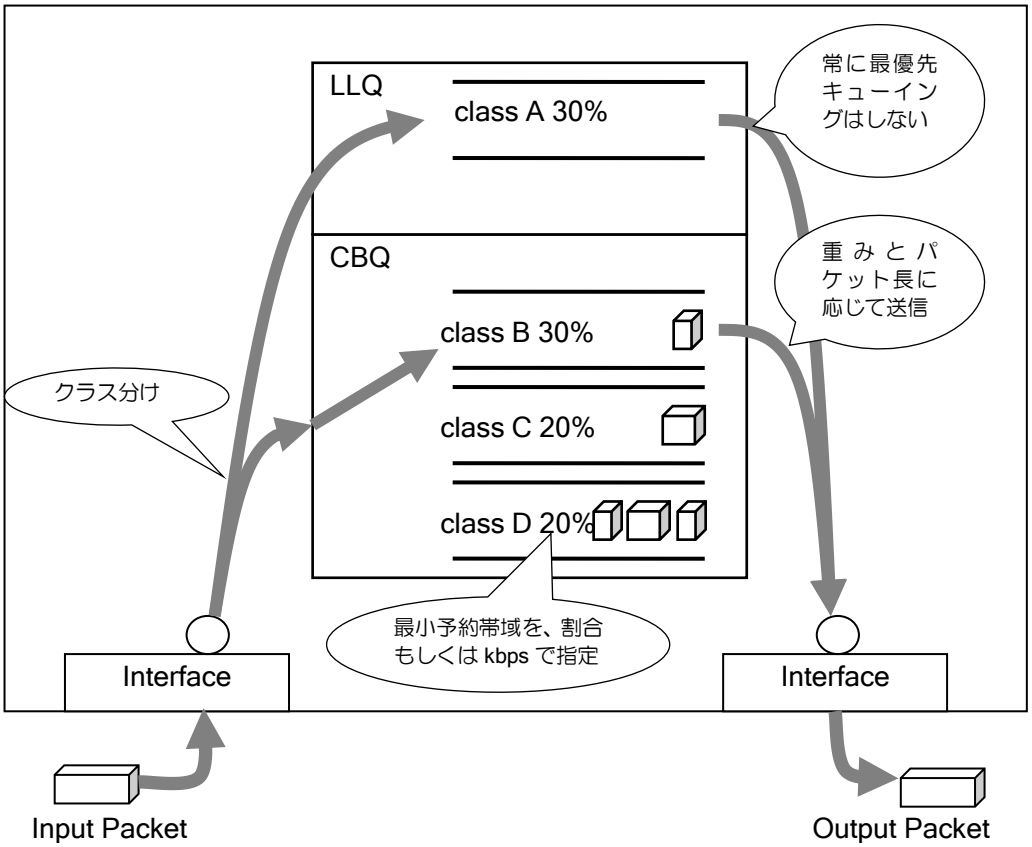
2.40.1 優先制御/帯域制御の動作

QoS の機能により、さまざまな手段で優先制御/帯域制御を行うことが出来ます。QoS の各機能の詳細は以下の通りです。

2.40.1.1 ローレイテンシキューイング（LLQ）とクラスベースキューイング（CBQ）

トラフィックをいくつかのクラスに分類し、それぞれに指定した割合で送信する機能です。

LLQ は、指定した帯域を最優先で確保し遅延を最小限にして送信します。音声パケットなどの遅延（レイテンシ）が問題になるパケットに向いています。CBQ は輻輳時に指定した割合でパケット送信を行います。こちらはデータトラフィックに向いています。



LLQ の動作

音声パケットなどの遅延（レイテンシ）が問題になるパケットを最優先で送信するための機能です。キューイングせずにパケットを送信する形となり、ここに分類されたパケットは最小限の遅延で最優先に送信されます。

この設定は帯域の上限を指定する必要があり、それ以上のトラフィックがある場合には廃棄します（ポリシング）。また、LLQ のクラスにパケットが流れていない限り、他のクラスは LLQ で指定している帯域を使用することができます。

注意事項

トラフィックが帯域を超えると廃棄されますので、帯域が不足することがないように注意して設定してください。使用する帯域が不定になるデータトラフィックには向きません。廃棄が発生する場合は後述の帯域制御の調整の項目も参照してください。

CBQ の動作

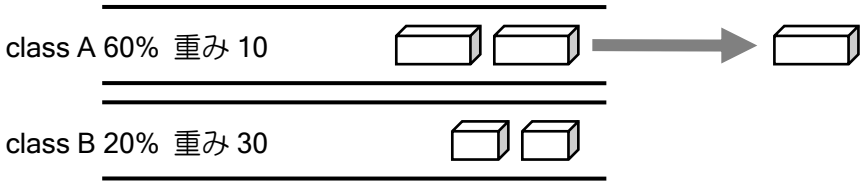
このクラスは送信割合を指定することができ、輻輳時に指定した割合でパケット送信を行います。指定した割合は最小予約帯域として必ず確保されるので、割り当ての小さいクラスでも、通信量が制限されることはあっても通信できなくなることはありません。

CBQ は指定した帯域で固定値を割った重み（weight）という値を用いて、帯域を制御します。以下の式に従って送信されます。

「既に送信したパケット送信量」 + 「重み x 次に送信するパケットのサイズ」

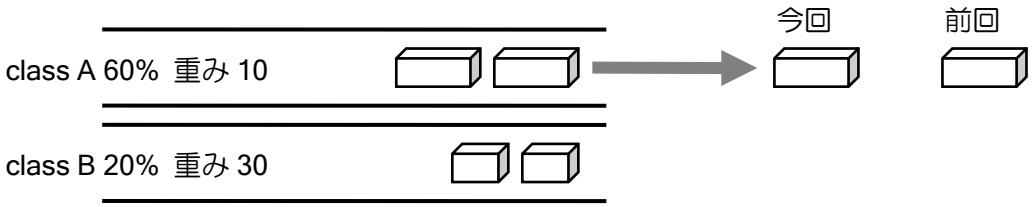
具体的に説明します。Class A（帯域 60%）と Class B（帯域 20%）があるとして、簡単のためそれぞれ Class A には 1500byte のパケット, Class B には 1200byte のパケットが、同じサイズで連続して送信されているとします。重みは比率だけの問題なので仮に 10 と 30 とします。

1 回目) 最初に送信するパケットの判定は次の通りです。



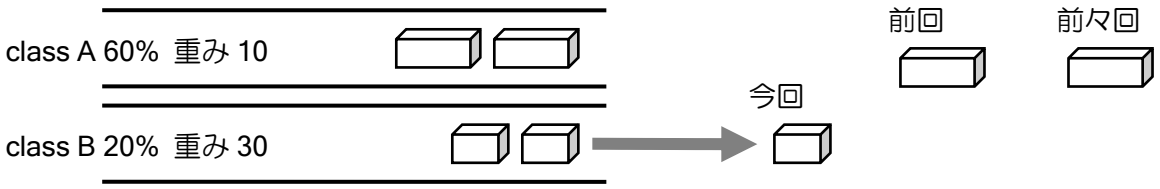
Class A から送信した場合の重みつき送信量 1500byte x 10 = 15000
Class B から送信した場合の重みつき送信量 1200byte x 30 = 36000
→従って、Class A からパケットが 1 つ送信されます。

2 回目) 送信済みの量を ClassA の計算に加えて次のパケットを判定します。



Class A から送信した場合の重みつき送信量 15000 + 1500byte x 10 = 30000
Class B から送信した場合の重みつき送信量 1200byte x 30 = 36000
→従って、Class A からパケットがもう 1 つ送信されます。

3 回目) さらに送信済みの量を加えて計算していきます。

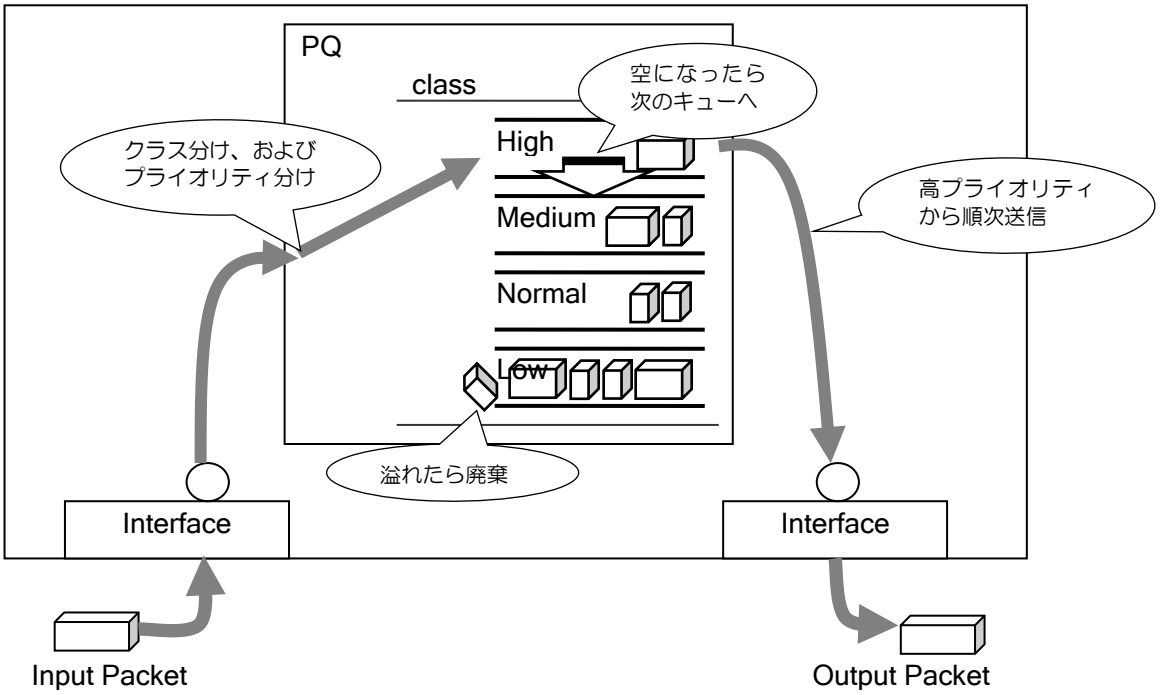


Class A から送信した場合の重みつき送信量 30000 + 1500 x 10 = 45000
Class B から送信した場合の重みつき送信量 1200 x 30 = 36000
→従って、次は Class B から 1 個送信されます。

これを繰り返すと輻輳時に指定した帯域で送信されます。送信するパケットがなければ次のクラスから送信しますので、予約帯域まで使用していないクラスがあれば他のクラスが利用します。

2.40.1.2 プライオリティキューイング（PQ）

トラフィックをプライオリティに応じて、4 段階（Ver8.9 以降 8 段階）のキューに割り当てることができます。パケット配信は、高プライオリティ（High）が最優先で行われます。



高プライオリティのキューが必ず優先され、上位のキューが空になるまで低プライオリティのキューは処理されません。CBQ と異なり High の通信が大量に行われてインタフェースの回線速度（インタフェースシェーピングの設定速度）以上になってしまうと Normal や Low のキューからはその間全く送信されません。停止して欲しくない場合は CBQ を利用してください。

注意事項

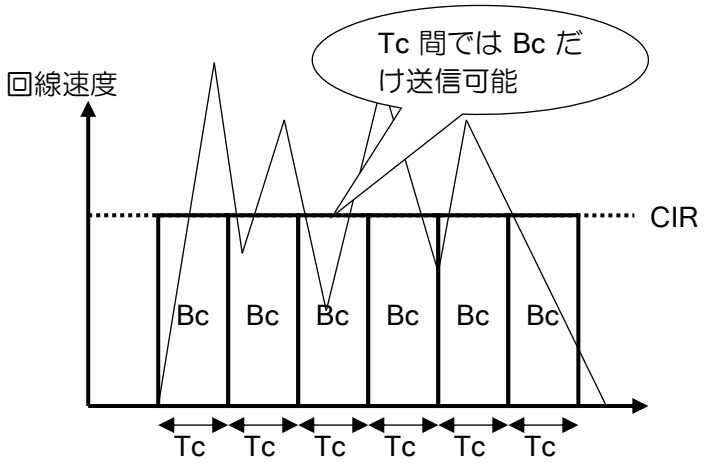
プライオリティによる優先度はクラス内でのみ有効です。同じポリシーマップでも別クラスのキューとの優先度は無視されます。PQ で優先度をつけたいトラフィックは、まとめて 1 つのクラスに記述する必要があります。

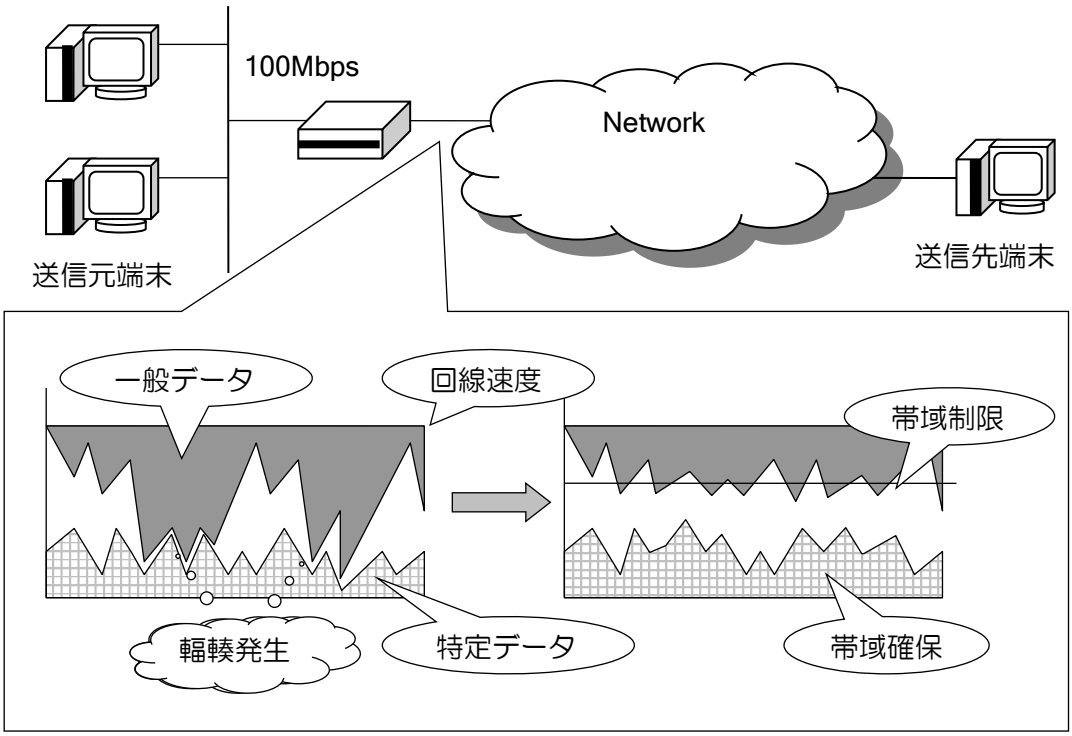
2.40.1.3 トラフィックシェーピング

トラフィックシェーピング機能は、帯域を制限し最大転送レートを超えるようなバーストデータをキューイングし、平均化して出力します。クラス単位とインタフェース単位で設定できます。

トラフィックシェーピングの動作原理

トラフィックシェーピングでは、設定した帯域 CIR（bps）を越えないように動作させるため、実際には単位時間 Tc 秒 の間に Bc（bit）ずつ送信を許可し、溢れた分をキューイングするという動作を繰り返します。





インタフェース単位やクラス単位で最大転送速度の制御が可能です。バーストしやすい特定のトラフィックに制限をかけることで、他のトラフィックの帯域を確保することができます。

トラフィックシェーピングのパラメータ

トラフィックシェーピングで設定・表示されるパラメータの意味は以下の通りです。

- 認定情報速度 CIR（Committed Information Rate）：[単位：ビット／秒]
  - CIR は、輻輳していない通常の状態で保証されるデータ速度です。

- 認定バーストサイズ Bc（Committed Burst Size）：[単位：ビット]
  - Bc は、Tc 内で、ネットワークが伝送を許容する、ビット単位での最大データ量です。
  - Bc の値が小さいほど平均化され、一定の流量のパケットが送信されます。

- 時間間隔 Tc：[単位：秒]
  - シェーピング動作の単位時間です。Tc ＝ Bc／CIR で決定されます。
  - Tc の最小値は 1ms です。

- 超過バーストサイズ Be（Excess Burst Size）：[単位：ビット]
  - Bc を越えて回線上で伝送できる未認定データ量です。通常この値は設定しません。
  - Be に値が設定されることがありますが、CIR を超過することはありません。

シェーピングの計算に使用するフレームサイズ

- Ethernet フレーム
  - Ethernet フレームサイズ（FCS を含む）
  - プリアンブルやフレーム間ギャップも含めたサイズ
  - IP/IPv6 パケットサイズ（Ethernet ヘッダと FCS を含まないサイズ）
    ※IP/IPv6 パケットサイズはブリッジの場合は使用できません。

Ver8.6 以前や、Ver8.7 以降のデフォルト動作は一番上の定義で計算します。Ver8.7 以降の Ethernet では、以下のコマンドで計算式を変更することができます。

qos rate-accounting	帯域計算対象のフレームサイズ変更

QoS をベースインタフェースのみで設定してサブインタフェースに適用した場合でも、本コマンドは送信インタフェース全てで設定する必要があります。

- PPP フレーム（以下の一種類のみ）
  - PPP ヘッダから FCS までを含む値

2.40.2 優先制御/帯域制御の設定方法

QoS の設定方法は以下の通りです。

- クラスマップを設定し、ポリシーごとにクラスを作成する（クラス分け）。
- ポリシーマップを設定し、クラスごとに QoS の設定を行う。
  - ✧ マーキングの設定（入力インタフェース / 出力インタフェース）
  - ✧ CBQ、LLQ、シェーピングの設定（出力インタフェース）
- ポリシーマップをインタフェースに適用し、QoS を有効化する。

※QoS をベースインタフェースで有効にした場合、同じデバイスに属する全てのサブインタフェースにも適用されます。QoS をサブインタフェースで有効にした場合、インタフェースごとに設定が有効になります。

2.40.2.1 クラス分け/PQ の設定

QoS の設定は基本的に class-map で設定する QoS クラス単位で行います。クラスマップの設定・表示コマンドは次のとおりで、さまざまな条件を用いてフローを分類することができます。
またクラス内で有効な PQ の設定もここで行います。

class-map	クラスマップの作成
match any	すべてのパケットにマッチします
match input-interface	入力インタフェースを条件とします
match access-list	MAC アクセスリストを条件とします
match ip/ipv6 access-list	IPv4/IPv6 アクセスリストを条件とします
match ip/ipv6 access-list cos	IPv4/IPv6 アクセスリストと CoS 値を条件とします
match cos	CoS 値を条件とします
match qos-group	qos-group を条件とします
match local-generate-packet	自装置送信パケットを条件とします
show class-map	クラスマップを表示します

【設定例】

(1) match-all を設定した場合、マッチ条件を and により判定します。

```
class-map match-all qos-class1
  match ip access-list access-class1
  match input-interface GigaEthernet0.0
```

(2) match-any を設定した場合、表示順に判定を行い、条件に合致した時点で
指定の優先度のキューに格納されます。

```
class-map match-any qos-class1
  match ip access-list access-class1 high
  match ip access-list access-class2 cos 6 normal
  match any low
  match ip access-list access-class3 medium
```

上記の例では、access-class3 の判定は行われません。

※CoS 値を match 条件に使用できるのは受信インタフェースのみです。受信時の CoS 値はルーティングすると 0 になります。また受信インタフェースで CoS 値を書き換えた場合も、その設定は送信直前に適用されます。いずれも送信インタフェースでは match させられません。
※入力インタフェースでの条件を送信側で判定したい場合は qos-group を利用してください。

2.40.2.2 ポリシーマップの設定

クラスマップで作成した条件を、ポリシーマップにて関連付けし、その条件に対する QoS 動作を設定します。ポリシーマップを設定・表示するコマンドは次のとおりです。設定内容の詳細は後の節で説明します。

policy-map	ポリシーマップの作成と指定ポリシーマップコンフィグモードへの移行
class	ポリシーマップクラスコンフィグモードへ移行
priority	LLQ の設定（Ver7.3 以降）
bandwidth	CBQ の最小予約帯域を設定
shape	クラスシェーピングを設定
set ip/ipv6 dscp/precedence	IPv4/IPv6 の DSCP/precedence を設定
set cos	CoS 値を設定（Ver.5.2 以降）
set qos-group	qos-group を設定（Ver.6.2 以降）
show policy-map	ポリシーマップの表示

【設定例】

```
policy-map qos-policy1
  class qos-class1
    bandwidth percent 20
```

ポリシーマップには、ローカルクラスとデフォルトクラスがあらかじめ作成されています。このクラスは以下のような特徴をもっており、コマンドにて削除することはできません。

- ローカルクラス（class-local）
  - ルータ自身が生成するパケットが対象となります。主なパケットに ICMP エコー、ダイナミックルーティングパケット等があります。
  - クラス分けに当てはまらなかったパケットが対象となります。
  - 10%の帯域が初期値として割り当てられています。
- デフォルトクラス（class-default）
  - クラス分けに当てはまらなかったパケットが対象となります。
  - 10%の帯域が初期値として割り当てられています。

2.40.2.3 インタフェースシェーピング

QoS クラス毎シェーピングの他にインタフェース毎にシェーピングを行うことができます。これにより、複数の QoS クラスをまとめてシェーピングすることができます。

service-policy enable	優先制御/帯域制御の有効化
traffic-shape rate	インタフェーストラフィックシェーピングの設定

ポリシーマップは不要ですが、設定したインタフェースで service-policy enable は必要です。基本インタフェースとサブインタフェースでシェーピングを有効化した場合は排他動作となるため、デバイスからは合計のシェーピング速度で送信します。

2.40.2.4 QoS の有効化とポリシーマップの関連付け

QoS を使用するインタフェースで QoS を有効にし、設定したポリシーマップを入力もしくは出力インタフェースに関連付けします。これらのコマンドは次のとおりです。

マーキングのみ行うインタフェースの場合は enable の設定は必要ありません。

service-policy enable	優先制御/帯域制御の有効化
service-policy input	受信インタフェースへのポリシーマップの割当
service-policy output	送信インタフェースへのポリシーマップの割当

```
【設定例】

interface GigaEthernet0.0
  service-policy enable
  service-policy output qos-policy1
```

2.40.2.5 帯域制御の設定

LLQ と CBQ、およびシェーピングの設定例です。

```
【設定例】

ip access-list voice permit ip src xx.xx.xx.xx/28 dest any (音声パケットを分類)
ip access-list data1 permit ip src xx.xx.xx.xx/24 dest any (データパケットを分類 1)
ip access-list data2 permit ip src any dest any (データパケットを分類 2)
!
class-map match-any voice
  match ip access-list voice normal
class-map match-any data1
  match ip access-list data1 normal
class-map match-any data2
  match ip access-list data2 normal
!
policy-map pmap
  class voice
    priority 250
  class data1
    bandwidth percent 40
  class data2
    shape 500000 1000 0
    bandwidth percent 20
  class class-local
  class class-default
!
interface GigaEthernet0.0
  ip address 10.0.0.254/24
```

```
   service-policy enable
   service-policy output pmap
   traffic-shape rate 1000000 1000 0
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.1.1.254/24
   no shutdown
```

LLQ、インタフェースシェーピング、クラスシェーピング、CBQ の設定は全て同時に満たすように動作します。CBQ の設定（最低保証帯域）よりも LLQ、シェーピングの設定が優先です。保証帯域がシェーピングを超える場合は均等に減少します。この設定は次のように動作します。

全ての通信の合計が 1Mbps を超えません。音声パケットは 250kbps まで遅延なく送信されます。data1 は全体の 40%（400kbps）までは必ず送信できます。data2 は全体の 20%（200kbps）まで必ず送信できますが、500kbps を超えることはありません。

2.40.2.6 プライオリティキューイング（PQ）の設定

PQ の設定例です。優先度はクラス単位で判定されます。

```
【設定例】
ip access-list voice permit ip src xx.xx.xx.xx/28 dest any
ip access-list data1 permit ip src xx.xx.xx.xx/24 dest any
ip access-list data2 permit ip src any dest any
!
class-map match-any pq
   match ip access-list voice high
   match ip access-list data1 normal
   match ip access-list data2 low
!
policy-map pmap
   class pq
   class class-local
   class class-default
!
interface GigaEthernet0.0
   ip address 10.0.0.254/24
   service-policy enable
   service-policy output pmap
   traffic-shape rate 1024000 1000 0
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.1.1.254/24
   no shutdown
```

2.40.3 帯域制御/優先制御設定の注意事項

帯域制御/優先制御の設定は、使用状況にあわせて細かなチューニングが必要になることがあります。特殊な運用環境や問い合わせの多い症例について記載します。

2.40.3.1 Ver7.3 での変更点（Ethernet インタフェースのみ）

Ethernet の帯域制御/優先制御の機能は Ver7.3 で大幅に改良が行われています。それ以前の QoS を利用している場合の注意点をまとめます。

(a) 仕様追加・仕様変更

LLQ が実装されました。これによりクラス間の優先制御/帯域制御が可能になりました。LLQ は遅延がなく、帯域を完全予約することが可能ですので音声パケットに適しています。

QoS の精度および速度が大幅に向上しています。シェーピングの分解能は Ver7.2 までは 16ms ですが、Ver7.3 以降は 1ms と大幅に向上しました。このため高負荷時にも安定して QoS を制御することができ、キューイングした際の遅延時間も大幅に改善されています。QoS のキュー長は設定なしで自動的に最適な値に設定するようになります。

QoS の転送処理がファストパスに対応しました。UFS cache 機能を有効にすることで適用され、クラスの検索処理が高速化されます。QoS 使用時の転送性能が向上するとともに、大量のクラスを使用した場合も速度低下の割合が小さくなります。

service-policy enable コマンドのリブートが不要になりました。ただし、policy-map、class-map 等に変更があった場合は、従来と同様に即時反映ではありません。設定変更後 clear policy-map interface を実行すると、全ての設定が反映されるようになります。

動作の変更にともない表示コマンドが変更になりました。次の項目で表示内容を説明します。

(b) 表示コマンド

show policy-map interface コマンドで確認できる情報についても、Ver7.3 以降で大きく変化しています。Ver7.3 以降の表示内容を大きく 4 段階のセクションにわけて説明します。

- デバイス単位の状態表示
- 論理インタフェース/ポリシーマップ単位の状態表示
- クラス単位の状態表示
- キュー単位の状態表示

セクションごとに表示を説明します。

デバイス単位の情報

【表示例】

```
Device GigaEthernet1
   Device buffer 0 packets, 0 bytes, peak 2414 bytes
   Queued 53 packets, 6784 bytes, peak 18250 bytes
```

- Queued 53 packets, 6784 bytes, peak 18250 bytes
  - ✧ デバイスごとのパケット数/サイズ/これまでの最大値
  - ✧ デバイスにあるキューではなく全インタフェースのキューの合計値です。
- Device buffer 0 packets, 0 bytes, peak 2414 bytes

✧ デバイスに存在する QoS の処理後に積まれる送信キューの情報です。
✧ 最適値に自動調整される内部値で設定はできません。

インタフェース単位の情報

【表示例】

```
Interface GigaEthernet1.0
   Queued 53 packets, 6784 bytes, peak 18250 bytes
   Burst size 160 bytes for priority class
   Traffic shaping is enabled, activated 358 times
      CIR 10000000 bps, Bc 10000 bits, Be 0 bits, Tc 1 ms
      Current token 10000 bits
   Output policy-map pmap attached
```

- Queued 53 packets, 6784 bytes, peak 18250 bytes
  ✧ インタフェースごとのパケット数/サイズ/これまでの最大値
- Burst size 160 bytes for priority class
  ✧ インタフェースからバースト転送される可能性のある最大バイト数。
  ✧ 全クラスのバーストサイズ（Bc+Be）
- Traffic shaping is enabled, activated 358 times
  ✧ 帯域があふれシェーピングが動作した回数（traffic-shape rate コマンド）
- CIR, Bc, Be, Tc
  ✧ シェーピングの章を参照してください。
- Current token
  ✧ シェーピングの内部計算で使用する値です。マイナス値が表示されている場合は、シェーピングにより転送が抑制されている状態であることを示しています。

クラス単位の情報（LLQ）

【表示例】

```
      Class 1
         Priority 64 kbps
         Traffic policing is enabled, activated 92 times
            CIR 64000 bps, Bc 320 bits, Be 320 bits, Tc 5 ms
            Current token 640 bits
         Queue normal 0 packets, peak 0 packets
            Output 88 packets, 5632 bytes
               0 tail drops, 862 excess bandwidth, 0 buffer exhausted
```

- Traffic policing is enabled, activated 92 times
  ✧ ポリシング動作回数です。帯域を超えて一定時間パケットを送信できない状態に遷移したことを示します。帯域の上限に近い場合はカウントされることがありますが、excess bandwidth（後述）がカウントされなければ廃棄はしていないので問題はありません。
- CIR, Bc, Be, Tc, Current token
  ✧ シェーピングの章を確認してください。
- Queue normal 0 packets, peak 0 packets
  ✧ 使用したレベルのキュー情報が表示されます。詳細はキューの項を参照してください。

クラス単位の情報（CBQ）

【表示例】

```
    Class 2
      Queued 52 packets, 6656 bytes, peak 12160 bytes
      Bandwidth 10 percent, weight 512
      Traffic shaping is active, activated 15765 times
        CIR 8000 bps, Bc 8 bits, Be 0 bits, Tc 1 ms
        Current token -728 bits
      Queue normal 52 packets, peak 95 packets
        Output 124 packets, 15872 bytes
          844 tail drops, 0 excess bandwidth, 0 buffer exhausted
```

- Queued 52 packets, 6656 bytes, peak 12160 bytes
  - ✧ クラスごとのパケット数/サイズ/予約領域のサイズ/これまでの最大値
- Bandwidth 10 percent, weight 512
  - ✧ CBQ の設定値と重み。詳細は CBQ の章を確認してください。
- Traffic shaping is active, activated 15765 times
  - ✧ シェーピングが動作した回数（shape コマンド）
- CIR, Bc, Be, Tc, Current token
  - ✧ シェーピングの章を確認してください。
- Queue normal 0 packets, peak 0 packets
  - ✧ 使用したレベルのキュー情報が表示されます。詳細はキューの項を参照してください。

キュー単位の情報

【表示例】

```
      Queue normal 52 packets, peak 95 packets
        Output 124 packets, 15872 bytes
          844 tail drops, 0 excess bandwidth, 0 buffer exhausted
```

- Queue normal 52 packets, peak 95 packets
  - ✧ キューの現在のパケット数とキューイングされたパケット数のピーク値。
  - ✧ High/Medium/Normal/Low のうち使用したキューのみ表示される。
- Output 124 packets, 15872 bytes
  - ✧ 送信したパケット数, バイト数
- 844 tail drops
  - ✧ キュー長が不足し廃棄したパケット数
- 0 excess bandwidth
  - ✧ LLQ のときに帯域を超えたため廃棄したパケット数。CBQ では常に 0 です。
- 0 buffer exhausted
  - ✧ 受信バッファが枯渇したためキューに積まず廃棄したパケット数

buffer exhausted がカウントされている場合

ルータ内に保持できるパケット数は制限があり、各装置の制限値は次の表の入力バッファプール数になります。入力バッファプールが全て QoS のキューに積まれたままになってしまうと、それ以降キューに積むことはできなくなるため、廃棄します。キュー長を制限するか、転送量を削減してください。show buffers コマンドで確認することができます。

装置	入力バッファプール数 （Ethernet 系インタフェース）
IX2105/IX2106/IX2107/IX2207/IX2215	2000
IX2235	10000
IX2310	20000
IX3015	1500
IX3110	2000
IX3315	1G デバイス：10000 10G デバイス/SW-HUB：20000

従って QoS のキュー長は各クラスのキュー長の合計が入力インタフェースのバッファプール数を超えないように設計してください。

2.40.3.2 帯域制御の調整

帯域制御の設定は、利用する環境によって最適な設定が異なるため、適切に設定しないと正しく動作しない場合があります。問い合わせの多い症例について説明します。

- LLQ で十分な帯域を設定したのに廃棄が発生する

トラフィックは連続量ではないため、例えば 10ms ごとに 10kbit ずつ送信する場合と、10ms の間に 1Mbit 送信して残り 990ms が無通信の場合、どちらも 1Mbps になりますが、必要な設定が異なります。

映像トラフィックなどでは、この例の後者のように、まとまったデータを一度に送信する傾向が強いため、帯域のみの設定では廃棄が発生します。これはバーストサイズ Be（一度に送信してよいパケットの合計サイズ）で調整する必要があります。

適切な値を priority コマンドの第 2 パラメータに設定してください。不明な場合は 3000～10000 程度の値で確認してください。

帯域が 500kbps 未満で 3000～4000byte ずつ送信される映像トラフィックを扱う場合の設定例

```
【設定例】

policy-map pmap
  class video
    priority 500 4000
```

- シェーピングで十分な帯域を設定したのに廃棄が発生する

シェーピングを設定した場合も同様に、バーストサイズ Bc を適切に設定しないと期待した動作ができないことがあります。Bc の設定を省略した場合、通常運用の負荷を想定して自動設定していますが、環境によって最適値が異なることと、試験環境などの極端な負荷条件の場合には、ただしく制御されないことがあります。

バーストサイズの設定により、以下のように特性が変化します。

- バーストサイズが小さい場合
  - 利点：短時間で細かく送信するため滑らかにシェーピングされます。
  - 欠点：バーストトラフィックで廃棄が発生しやすくなります。
- バーストサイズが大きい場合
  - 利点：バーストトラフィックでも廃棄されにくくなります。
  - 欠点：バーストを許可するのでシェーピングが荒くなります。

デフォルトでは Bc は CIR の 1/1000 の値で動作し、Tc が 1ms になるように設定されています。1ms ごとに送信可能かどうかの判断を行います。それほどの精度が必要でない場合、Bc の値を例えば 2～10 倍程度にするとバーストの多い環境でも動作しやすくなります。必要に応じて調整してください。

【設定例】

traffic-shape rate 1000000 10000

負荷試験機を用いて運用時に流れないような負荷をかけた場合に設定が必要になることがありますが、それが運用時の最適値とは限りません。上記の特性に注意して設定してください。

- キュー長の調整方法と自動調整について

QoS の制御に必要なキュー長は、クラス・プライオリティごとに用意されています。帯域制御や優先制御により送信順序を変更するため、ある程度のパケット数を蓄えられないとパケットが廃棄されてしまいます。

キュー長の設定により、以下のように特性が変化します。

- 長い場合
  - 利点：QoS の制御が行いやすく、パケットが廃棄されにくくなります。
  - 欠点：低帯域の場合に遅延が大きくなります。全クラスあわせて 600 個以上キューに積まれることがあると、受信バッファが枯渇して通信に支障が出ることがあります。このため、相対的に設定できるクラスが少なくなります。
- 短い場合
  - 利点：低帯域の場合にも遅延が抑えられます。数多くのクラスが設定できます。
  - 欠点：PQ やシェーピングの制御に支障が出ます。パケットが過剰に廃棄されます。

Ver7.3 以降のバージョンは、Ethernet のみですがキュー長を設定しなければ、自動で調整するようにしています。シェーピングや CBQ の設定にあわせて必要な数を自動的に確保しますが、この自動調整は運用環境の負荷を想定しており、試験環境などでの極端な負荷条件には対応できないこともあります（現実的に不要なキュー長を確保してしまうため、その場合は手動で設定が必要です）。

自動調整される値は Bc+Be のサイズおよび 10ms 分相当(ただしクラスごとに最低 32 個 / Ver7.3 は最低 3 個）のパケットがキューイングできる数を基準に設定されます。

Ver7.2 以前の場合や、BRI などの低速回線では、High/Medium/Normal/Low のプライオリティごとに 10 個ずつのキューがデフォルトでは用意されます。これは調整された値ではないので変更が必要です。高優先/低遅延なら 10～25、それ以外は 25～100 程度が推奨です。

キュー長は queue-limit コマンドで変更できます。

queue-limit	キュー長の調整

※キューの合計値は、受信インタフェースのバッファ数を超えない範囲で利用してください。

2.40.3.3 多対地設定の帯域制御の調整

64 以上のクラスを同時に利用し帯域制御する場合、以下の項目を確認してください。

- 受信バッファ数の調整

パケットを大量にキューイングするため、パケットバッファ数の変更が必要です。IX3110 のみ変更可能で、設定変更は QoS を有効にしたインタフェース側ではなく、「パケットを受信するインタフェース側」で行います。

変更コマンドは以下のとおりです。デバイスコンフィグモードで設定します。

receive-buffers	受信バッファサイズの変更

バッファの必要数は、帯域制御に使用されるクラス全てのキューのキュー長の合計になります。キュー長を設定しない場合は、1 つのクラスあたり 32 で計算してください。なお、QoS 以外の機能でも受信バッファは 200 以上利用されることがありますので、余裕をもった値を設定してください。

PQ を利用すると必要なキュー数が大幅に増えるので、キューを High と Normal のみとする、キュー長を大きく設定しない、などの調整が必要になる場合があります。

なお、全てのクラスが同時に輻輳して最大までキューイングされてしまう場合を想定した計算ですが、実際の運用環境では通常そのような状態にはならないため、設定数が不足する場合は、そのあたりを考慮して検討してください。

- シェーピングの設定

64 以上のクラスシェーピングでは、過剰な負荷をかけないように設計する必要があります。

デフォルトでは Tc = 1ms となるように調整されていますが、Tc = 10ms や 16ms でも問題がない場合は、その値に変更して運用することも検討してください。

shape	クラスシェーピングの設定

2.40.3.4 サブインタフェースを使った帯域制御の調整

タグ VLAN や PPPoE など、サブインタフェースを複数利用している場合の制御方法です。

設定方法は以下の 2 通りがあります。

- 基本インタフェースで設定し 1 つの QoS として制御する方法
- サブインタフェースごとに QoS の設定を個別に行う方法

(a) 基本インタフェースにおける帯域制御と優先制御

基本インタフェースのみで service-policy enable を設定すると、サブインタフェースを含む全インタフェースのトラフィックが、基本インタフェースに設定した QoS の設定に従って動作します。

※ポート VLAN 利用時の基本インタフェースは QoS ではサブインタフェースとして扱います。

(b) サブインタフェースごとの帯域制御

サブインタフェースごとに service-policy enable を設定することで、サブインタフェースごとに QoS のポリシーを適用することもできます。

2.40.4 マーキング・カラーリングの設定

パケットの DSCP や IP precedence、CoS の値を、設定した条件にあわせて書き換えることができます。

2.40.4.1 DSCP 値、IP precedence 値、CoS 値について

- RFC791 で定義されている Type of Service フィールド

Precedence 3bits	TOS 4bit				0
	D	T	R	M	

precedence（=優先度）：
- 111 - Network Control
- 110 - Internetwork Control
- 101 - CRITIC/ECP
- 100 - Flash Override
- 011 - Flash
- 010 - Immediate
- 001 - Priority
- 000 - Routine

D（Delay=遅延）：
- 0 = Normal Delay
- 1 = Low Delay

T（Throughput=スループット）：
- 0 = Normal Throughput
- 1 = High Throughput

R（Reliability=信頼度）：
- 0 = Normal Reliability
- 1 = High Reliability

M（Money=コスト）
- 0 = Normal money cost
- 1 = Minimum money cost

- RFC2474 で Diffserv 用に定義されている Type of Service フィールド

DSCP（Diffserv codepoint） 6bits	未使用

DSCP	
Default PHB 0（000000）	ベストエフォート（優先制御なし）
EF（Expedited Forwarding PHB） 46（101110） cf. RFC3246	パケットを最優先で転送 仮想専用線（低損失 低遅延 低ジッタ）
AF（Assured Forwarding PHB） 12 種類 cf. RFC2597	輻輳時に確率的にパケット廃棄 輻輳時の最低帯域を保証可能

- IEEE802.1D で定義されているタグ付きフレームの Priority（CoS）フィールド

Priority（=優先度）：

111 - Network Control	高
110 - Voice（< 10ms latency and jitter）	↑
101 - Video（< 100ms latency and jitter）	
100 - Controlled load	
011 - Excellent Effort	
000 - Best Effort（default）	
010 - Spare	↓
001 - Background	低

2.40.4.2 ルータが送信するパケットへの付与

Ver.8.0 以降、ルータが送信するパケットについては QoS 機能を使用せずに Precedence, TOS, DSCP の値を設定することができます。対象となるパケットは以下になります。

- BGP
- DHCP
- DNS
- EtherIP
- GRE(keepalive)　Ver.8.8 以降のみ
- HTTP
- ICMP　（ICMP echo request/reply は対象外）
- IGMP
- IKE
- L2TP-ctrl　L2TP（コントロールパケットのみ）
- ネットワークモニタ
- NTP
- OpenFlow　OpenFlow Channel（Ver9.2 以降）
- OSPF
- PIM
- RADIUS
- RIP
- sFlow
- SNMP
- SSH
- SYSLOG
- telnet
- TFTP
- VRRP

設定コマンドは次のとおりです。

ip type-of-service	IPv4 Type of Service の設定
ipv6 traffic-class	IPv6 Traffic Class の設定

【設定例】
BGP の DSCP を 63、OSPF の TOS を 10、ICMPv6 の precedence を 6 に設定

```
ip type-of-service bgp dscp 63
ip type-of-service ospf tos 10
ipv6 traffic-class icmp precedence 6
```

これらのコマンドは policy-map や service-policy の設定は不要です。

2.40.4.3 転送パケットへの付与

DSCP や IP precedence の値の付与は、クラス単位で付与します。

【設定例】

```
policy-map qos-policy1
  class qos-class1
    set ip dscp 46
```

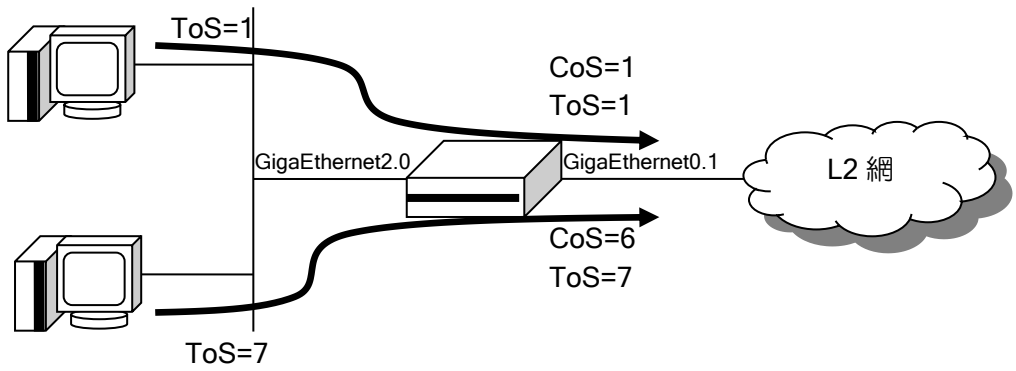
こちらの方法では CoS 値も同様に付与することができます。

【設定例】

```
policy-map qos-policy1
  class qos-class1
    set cos 4
```

※set cos で設定した値を使って match cos を動作させることはできません。CoS の set の設定はパケット送信時に適用する仕様のため、CoS 値を入力側で set しても出力側の QoS ではその値で match しません。CoS の引継ぎなど受信インタフェースの条件により送信インタフェースで CoS をセットしたい場合は、後述の qos-group の設定を利用してください。

ToS-CoS 変換の設定例



【設定例】

ToS 値に応じて CoS 値を設定
出力時に ToS 値の大きいパケットを優先して出力

```
ip access-list tos7 permit ip src any dest any precedence 7
ip access-list tos1 permit ip src any dest any precedence 1
!
class-map match-any in-class1
  match ip access-list tos7
!
class-map match-any in-class2
  match ip access-list tos1
!
class-map match-any out-class
```

```
   match ip access-list tos7 high
   match ip access-list tos1 medium
!
policy-map cos-set
   class in-class1
      set cos 6
   class in-class2
      set cos 1
!
policy-map out-policy
   class out-class
!
interface GigaEthernet0.1
   encapsulation dot1q 10 tpid 8100
   ip address 10.0.0.1/24
   service-policy enable
   service-policy output out-policy
   no shutdown
!
interface GigaEthernet2.0
   ip address 192.168.1.1/24
   service-policy input cos-set
   no shutdown
```

2.40.5 qos-group 値の付与

qos-group は、DSCP や CoS と異なり、パケットに含まれる値ではありません。ルータ内部だけで利用されるパケットのパラメータで、入力インタフェース側でパケットをクラス分けし、出力インタフェース側でその分類したクラスごとに QoS を適用したい場合に使用する値です。

入力インタフェースごとに QoS の処理を分けたり、通過したトンネルインタフェースごとにクラスを分類したい場合などに利用します。

【設定例】

```
class-map match-any qos-class1
   match cos 1 normal

class-map match-any qos-class2
   match cos 2 normal

class-map match-any qos-class3
   match qos-group 1 normal

class-map match-any qos-class4
   match qos-group 2 normal

policy-map qos-in
   class qos-class1
      set qos-group 1
   class qos-class2
      set qos-group 2

policy-map qos-out
   class qos-class3
      set cos 1
   class qos-class4
      set cos 2

interface GigaEthernet0.1
```

```
   encapsulation dot1q 10 tpid 8100
   ip address 10.0.0.1/24
   service-policy output qos-out
   no shutdown
!
interface GigaEthernet2.1
   encapsulation dot1q 10 tpid 8100
   ip address 10.1.1.1/24
   service-policy input qos-in
   no shutdown
```

Ver.9.4 以降、ルータが送信するパケットに対して、policy-map や service-policy の設定は行わずに qos-group 値を設定することができます。
対象となるパケットは以下になります。

- IKE
- GRE keepalive

設定コマンドは次のとおりです。

ip qos-group	IPv4 qos-group 値の設定
ipv6 qos-group	IPv6 qos-group 値の設定

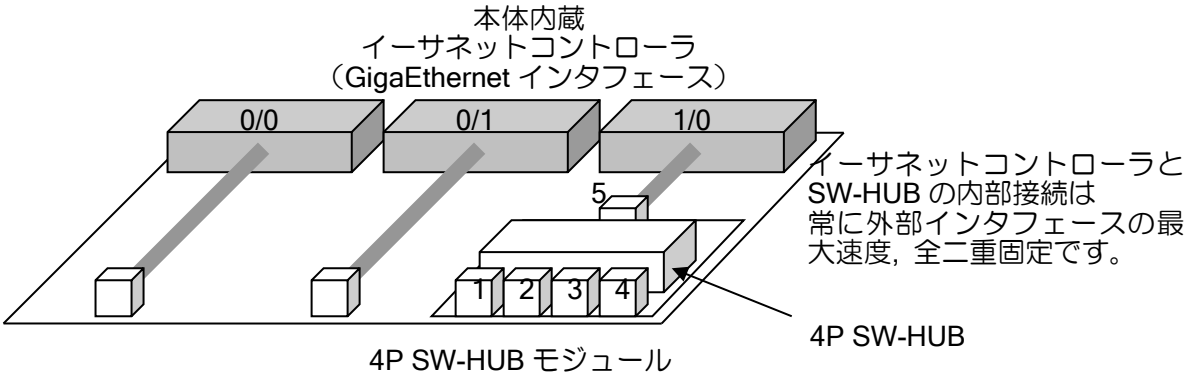
【設定例】
IPv4 の IKE に qos-group 10 を設定

```
ip qos-group ike 10
```

2.40.6 SW-HUB の優先制御（Ver.8.3 以降）

SW-HUB の各ポートで受信したパケットをイーサネットコントローラ側に送信する際の優先度を設定することができます。これにより、SW-HUB のポートで音声とデータが混在した環境で、輻輳が発生するような場合でも、音声パケットを廃棄せずにイーサネットコントローラ側に送信することができます。

SW-HUB モジュールの接続は、内部的には以下の図のようになっています。イーサネットコントローラと SW-HUB の内部接続は外部のインタフェースの最大速度と同じ速度（ギガ対応装置の場合 1Gbps,それ以外は 100Mbps）に固定されています。そのため、全ポートの入力の合計が外部インタフェースの最大速度以上になると、SW-HUB 内で廃棄が発生します。各ポートの優先度を設定することにより、指定したポートからの受信を優先してイーサネットコントローラ側に送信することができます。



ポートの優先度の設定は 8 段階で行いますが、SW-HUB のキューの優先度は 4 段階となり、以下のように割り当てられます。キューの優先度が大きい方が優先となり、優先度が同じ場合は設定する優先度が異なっていても、同じ優先度となります。

設定する優先度	0(デフォルト)	1	2	3	4	5	6	7
キューの優先度	1	0		1	2		3	

また、送信のスケジューリングの方法については、以下の 2 種類が設定できます。

- wfq
  キューの優先度順から、フレーム数が 8:4:2:1 の割合で送信されます。
  最優先のパケットでも廃棄される可能性があります。
- strict（デフォルト）
  優先度の高いフレームから送信されます。
  最優先パケットが存在する間は、他のキューのパケットが送信されません。

コマンドは以下のとおりです。

port qos default-priority	SW-HUB ポート優先度の設定
qos scheduler	スケジューリング方法の設定

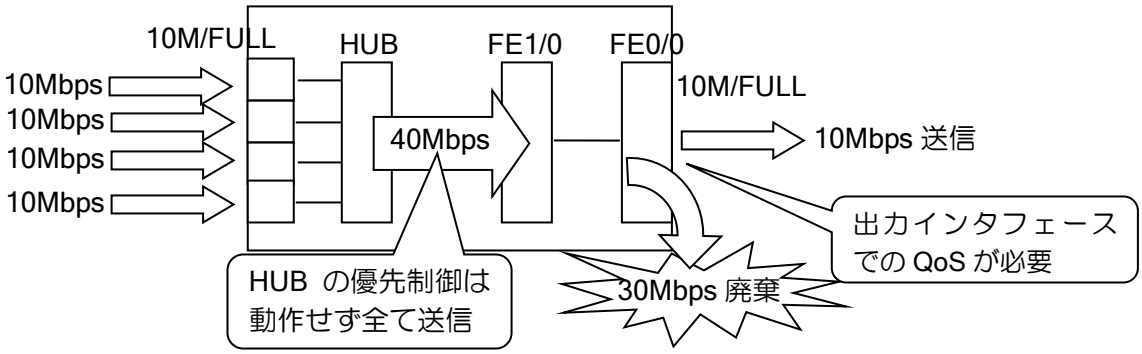
【設定例】
ポート 1 を優先
優先のスケジューリング方法を WFQ に設定

```
device GigaEthernet2
  qos scheduler wfq
  port 1 qos default-priority 7
```

※注意事項

ルータの性能を超える負荷となっている場合は、バッファが枯渇するため高優先のフレームでも廃棄される可能性があります。

SW-HUB モジュールからの入力の合計が、外部インタフェースの最大速度以下の場合、全てイーサネットコントローラに送信可能なため、本機能による優先制御は動作しません。出力インタフェースの速度を、最大速度以下に設定している場合は、出力インタフェースにより廃棄されます。このような場合、SW-HUB による優先制御は使用せず、出力インタフェースに通常の QoS を設定してください。



2.40.7 ダイナミック QoS の設定

端末の通信量に応じて専用の QoS クラスを動的に割り当てることにより、通信量の多い端末の通信を制限することができます。（Ver.10.0 以降）

2.40.7.1 概要

通常時は QoS の設定に従って動作します。通信量が一定の値を超えると、別途指定する専用の QoS クラスに割り当て、また、通信量が一定の値以下になると、再度通常の QoS 設定に従って動作します。これにより、通信量の多い端末の通信を一時的に制限するこができます。

端末の通信量の測定はリンクマネージャを利用します。端末は MAC アドレス毎に管理します。

2.40.7.2 設定

ダイナミック QoS のために、以下の設定が必要です。

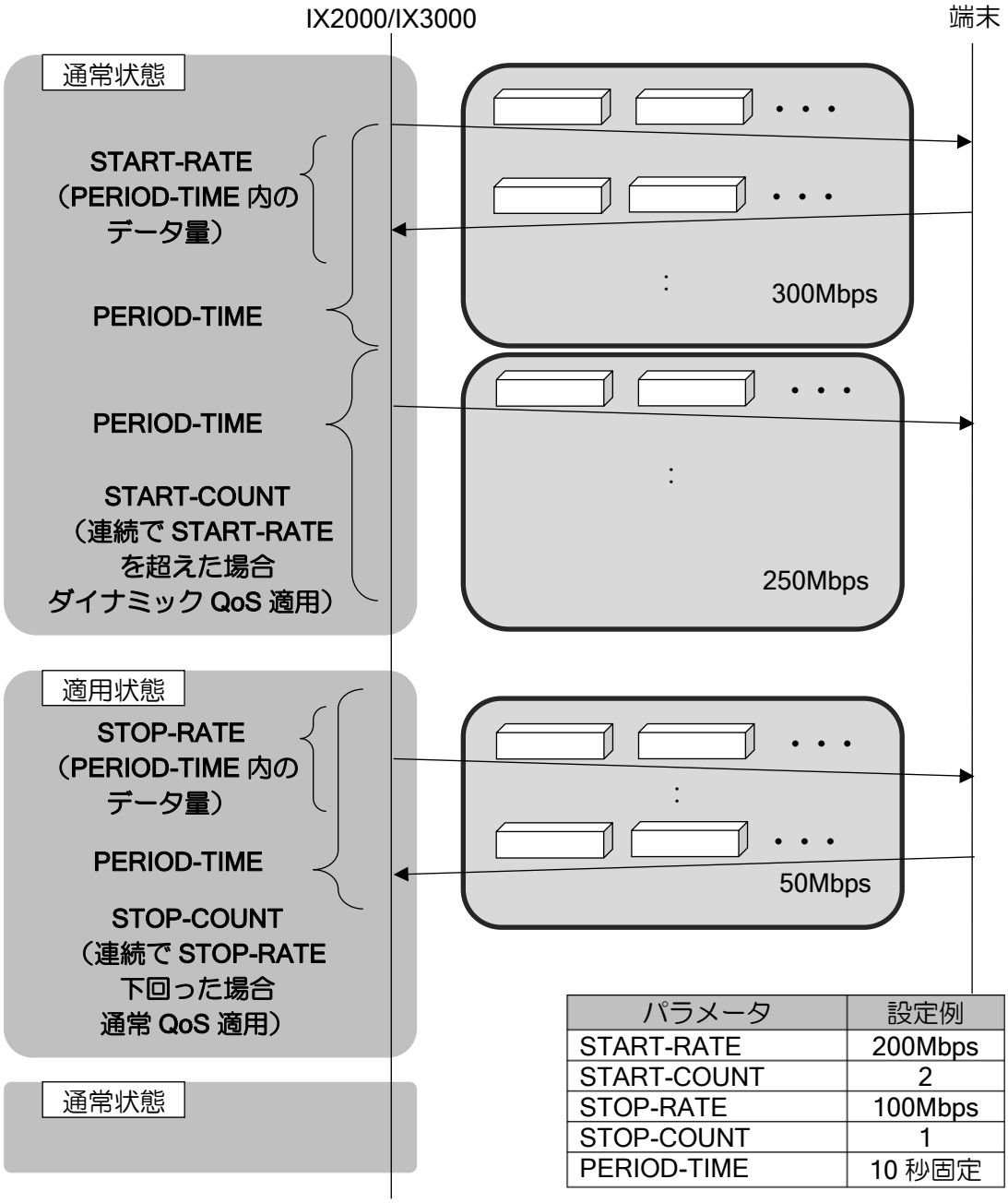
dynamic-qos detect-rate	ダイナミック QoS の設定（レート指定）
dynamic-qos detect-size	ダイナミック QoS の設定（総トラフィック量）

設定可能なパラメータは以下になります。

START-SIZE	ダイナミック QoS 開始トラフィック量 トラフィック量指定時、Gbyte,Kbyte,Mbyte から選択
START-COUNT	ダイナミック QoS 開始の判定回数 （デフォルト：3 回）
STOP-SIZE	ダイナミック QoS 終了トラフィック量 トラフィック量指定時、Gbyte,Kbyte,mbyte から選択
STOP-COUNT	ダイナミック QoS 終了の判定回数 （デフォルト：3 回）
PERIOD-TIME	計測周期 detect-size 指定の場合のみ detect-rate の場合は 10 秒固定
both|in|out	トラフィックの監視方向 both ：双方向 in ：LAN→WAN 方向 out ：WAN→LAN 方向

ダイナミック QoS の設定は 1 インタフェースでレート指定と総トラフィック量指定の併用が可能です。併用した場合、いずれかの開始条件を満たした際にダイナミック QoS を開始し、全ての終了条件を満たした際にダイナミック QoS を終了します。

dynamic-qos detect-rate 時の動作例



パラメータ	設定例
START-RATE	200Mbps
START-COUNT	2
STOP-RATE	100Mbps
STOP-COUNT	1
PERIOD-TIME	10 秒固定

上記以外に、リンクマネージャ、QoS の設定が必要になります。

インタフェースコンフィグモード	
service-policy enable	QoS の有効化
service-policy output	ポリシーマップ指定
linkmgr enable	リンクマネージャ有効

グローバルコンフィグモード	
policy-map	ポリシーマップの設定

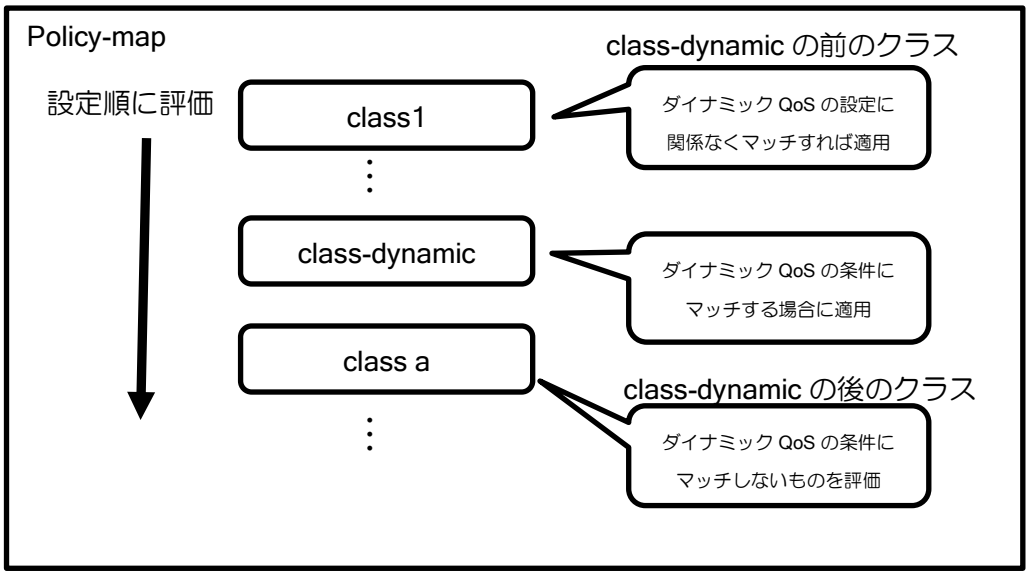
ダイナミック QoS を適用するクラスは、policy-map 設定にて”class-dynamic”を指定します。

通常の QoS の設定と同様、policy-map は上から順に評価を行います。
”class-dynamic”設定より前に設定されたクラスにマッチする場合は、通常の QoS 処理を行います。”class-dynamic”のマッチ条件は、”dynamic-qos”コマンドで指定した条件になります。指定した条件に該当する場合は、”class-dynamic”に設定した内容で QoS 制御を行います。条件に当てはまらない場合は、”class-dynamic”設定以降のクラスに該当するか評価を行います。

“class-dynamic”は 1 つのみの設定を行います。“class-dynamic”に該当する場合、制限数までは該当する端末毎に 1 クラスが割り当てられます。制限数を超えた場合は、複数端末が 1 クラスに割り当てられます。複数端末の通信の合計が、指定した帯域に制限されます。

詳細については関連する項を参照してください。

ダイナミック QoS 設定時のクラスの評価



2.40.7.3 設定例

【設定例 1】
LAN→WAN 方向のトラフィックを監視
10 秒間の通信量が 3 回続けて 1Mbps を超えると、800Kbps に制限
10 秒間の通信量が 3 回続けて 100Kbps を下回ると制限を解除

```
policy-map wan-outmap
   class voice-up
      priority 2000
   class class-dynamic
      shape 800000
   class class-local
   class class-default

interface GigaEthernet0.0
   ip address 10.0.0.1/24
   service-policy enable
   service-policy output wan-outmap
   no shutdown
interface GigaEthernet1.0
   ip address 192.168.1.254/24
   linkmgr enable
   dynamic-qos detect-rate start 1000 kbps stop 100 kbps in
   no shutdown
```

【設定例 2】
192.168.0.253/32 の端末は LLQ で制御
双方向のトラフィックを監視
72 時間以内の合計通信量が 10Gbyte を超えた時点で、800Kbps に制限
72 時間の合計通信量が 1Gbyte を下回ると制限を解除

```
ip access-list list-voice-up permit ip src 192.168.0.253/32 dest any
!
class-map match-any voice-up
   match ip access-list list-voice-up high
!
policy-map wan-outmap
   class voice-up
      priority 2000
   class class-dynamic
      shape 800000
   class class-local
   class class-default

interface GigaEthernet0.0
   ip address 10.0.0.1/24
   service-policy enable
   service-policy output wan-outmap
   no shutdown
interface GigaEthernet1.0
   ip address 192.168.1.254/24
   linkmgr enable
   dynamic-qos detect-size start 10 gbyte count 1 stop 1 gbyte count 1 period 72 both
   no shutdown
```

【設定例 3】
LAN→WAN 方向の 10 秒間の通信量が 3 回続けて 1Mbps を超える
または、双方向の 72 時間以内の合計通信量が 10Gbyte を超えた時点で
800Kbps に制限
LAN→WAN 方向の 10 秒間の通信量が 3 回続けて 100Kbps を下回る
かつ、双方向の 72 時間の合計通信量が 1Gbps を下回ると制限を解除

上記の条件に該当しない場合は、500Mbps

[QoS 設定は設定例 1 と同じ]

```
class-map match-any all-traffic
   match any normal

policy-map wan-outmap
   class class-dynamic
      shape 800000
   class all-traffic
      shape mbps 500
   class class-local
   class class-default

interface GigaEthernet0.0
   ip address 10.0.0.1/24
   service-policy enable
   service-policy output wan-outmap
   no shutdown
interface GigaEthernet1.0
   ip address 192.168.1.254/24
   linkmgr enable
   dynamic-qos detect-rate start 1000 kbps stop 100 kbps in
   dynamic-qos detect-size start 10 gbyte count 1 stop 1 gbyte count 1 period 72 both
   no shutdown
```

2.40.7.4 制限事項・注意事項

ダイナミック QoS には以下の制限事項・注意事項があります。

- Ver.10.0 以前からバージョンアップする場合、クラス名に” class-dynamic”を使用している場合は、クラス名を変更してください。
- トラフィック監視対象は Ethernet 系インタフェースのみ対応しています。
- ダイナミック QoS 用クラスは service-policy output のみ対応しています。
- BVI インタフェースには対応しておりません。

■2.41 VoIP のフォワーディング設定

IX2000/IX3000 シリーズでは、VoIP パケットをフォワーディングするための機能をサポートしています。

2.41.1 VoIP のフォワーディングのための実現機能

IX2000/IX3000 シリーズに VoIP フォワーディングを設定する方法について説明します。VoIP の音質は、音声パケットの遅延と遅延のゆらぎによって決まります。IX2000/IX3000 では下記の機能を用いることにより、音声パケットにおける遅延を小さくすることができます。

下記の設定により、VoIP のフォワーディングをサポートします。

- マルチリンク PPP インタリーブ
- ヘッダ圧縮
- 送出遅延制御

※マルチリンク PPP インタリーブを使用される際は注意事項をよく確認してください。

2.41.2 RTP の QoS 設定

VoIP の遅延を抑えるために、まず QoS を有効化し、VoIP で使用する RTP パケットの優先度を高く設定しておく必要があります。QoS の有効化の方法は QoS の章を参照してください。RTP パケットの優先度を高く設定するためには、クラスマップで次のように条件を設定します。

match rtp port	RTP 使用ポート番号の設定

【設定例】

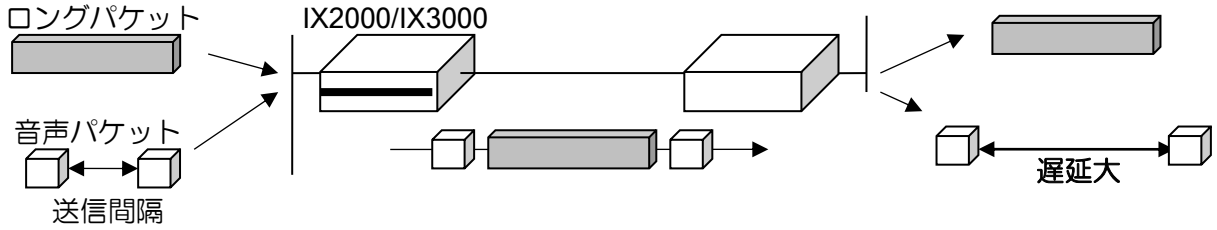
```
ppp profile prof1
   authentication myname ix2010
   authentication password ix2010 router

class-map match-any cmap1
   match rtp port 16384 160 high
      match any

policy-map pmap1
   class cmap1
   class class-local
   class class-default

interface BRI1/0.0
   ip address 10.0.0.1/24
   service-policy enable
   service-policy output pmap1
   no shutdown
```

2.41.3 マルチリンク PPP インタリーブの設定

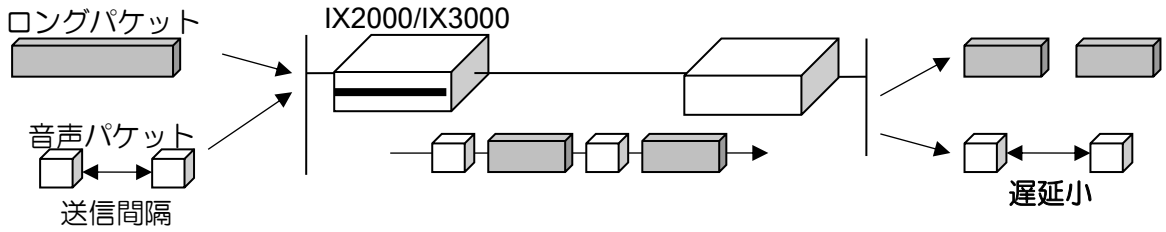
BRI のような低速回線では、ロングパケット 1 つ送信するのに数十 ms 以上の時間がかかる場合があり、QoS のパケット単位の優先制御だけではこの遅延が回避できません。

マルチリンク PPP インタリーブの設定は、低優先のパケットを常に一定サイズ以下となるように分割して送信するもので、下記のように最大送信遅延時間を短く抑えることができます。

ロングパケットを処理すると遅延が発生します



ロングパケットを分割し、音声パケットが割り込めるようにすることで遅延を抑えます



この設定は ISDN のみ有効で、QoS を有効化する必要があります。

制限事項

- 高優先パケットには音声パケット以外を使用しないでください。
  - マルチリンク PPP では、シーケンス番号を持つマルチリンクヘッダが付与され送信順序が保護されますが、本機能ではパケットを優先して送信するために高優先のパケットにはマルチリンクヘッダを付けません。動作原理上高優先パケット自体の送信順序は保護されないため、高優先パケットに十分な送信間隔がないと、送信順序が入れ替わり性能低下や正常に通信できないことがあります。
- 低優先のパケットの性能が帯域より低くなることがあります。
  - マルチリンク PPP ではパケットの送信はラウンドロビンで行われるため、例えば 2B 接続時に 200byte で分割する設定で 250byte の単一トラフィックを送信し続けた場合、常に 1B 目に 200byte パケット、2B 目に 50byte のパケットを送信することになり、2B 目の帯域が 1/4 しか利用されません。実環境ではある程度緩和されますが、ご注意ください。
- IP45/C シリーズとの接続はマルチリンク PPP の項も参照してください。

設定に使用するコマンドは次のとおりです。

multilink enable	マルチリンク PPP の有効
multilink fragment-delay	フラグメントの最大遅延時間の設定
multilink interleave	音声パケットのインタリーブの有効
multilink sequence-num-length	シーケンス番号種別の設定
show ppp control multilink	マルチリンク PPP の運用情報の表示
show ppp multilink	マルチリンク PPP の統計情報の表示

```
【設定例】
ppp profile prof1
  authentication myname ix2010
  authentication password ix2010 router
  multilink enable
  multilink interleave
```

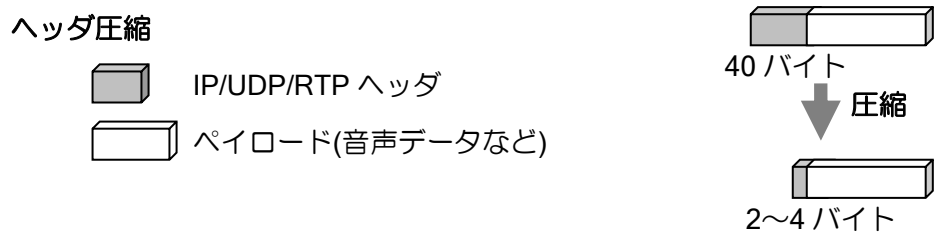
※フラグメントされるパケットのサイズは、以下の計算式で決定されます。（ただし、設定値に関わらず最小値は 50byte です。）

パケット分割サイズ（byte）（ヘッダ 6byte,FCS 2byte を含んだ値です）
= （ fragment-delay 設定値（msec）÷ 1000）×（回線速度（bps）÷ 8）
（1000 は ミリ秒を秒に変換するため、8 は bit を byte に変換するための値です）

※マルチリンク PPP インタリーブでは、medium 以下の優先度のパケットを分割し、分割されたパケットの優先度は、high ＞ マルチリンク PPP ＞ medium として扱われます。

2.41.4 ヘッダ圧縮

RTP（Real-Time Transport Protocol）は、音声などのリアルタイムにパケットを伝送する必要がある場合に使用されるプロトコルです。これらのパケットには IP/UDP/RTP ヘッダが付き、ヘッダのサイズは通常 40 バイトになります。これを 2～4 バイトのヘッダ情報に圧縮し、大量の RTP トラフィックを送受信することによるネットワークのオーバーヘッドを軽減します。低速リンク上で、RTP のペイロードサイズが小さい音声などのパケットに対して有効です。IPv6 では設定することができません。



RTP ヘッダ圧縮は BRI，Serial，Dialer で設定できます。

また細い回線を有効に使うため、音声パケットのヘッダ圧縮だけでなく、優先度の低い TCP パケットについてもヘッダ圧縮を行うことが有効です。RTP ヘッダ圧縮を設定した場合には、TCP についても RFC2507 に基づくヘッダ圧縮が行われます。

※対向ルータで、最大接続数を 257 以上に設定した場合は接続できません。また、他社製ルータのバージョンによっては、接続できないものがあります。

2.41.5 RTP ヘッダ圧縮（CRTP）

RTP ヘッダ圧縮の設定は次のコマンドを使用します。
BRI，Serial，Dialer 有効です。

ip rtp header-compression	RTP ヘッダ圧縮の有効
ip rtp compression-connections	RTP ヘッダ圧縮接続数の変更
ip rtp port	RTP で使用する UDP ポート範囲の設定
ip rtp compression-mode	圧縮モードの設定
show ip rtp header-compression	CRTP 統計情報の表示
clear ip rtp header-compression	CRTP 統計情報のクリア

【設定例】
接続数を 20
RTP で使用する UDP ポート番号を 20000 番から 200 個分

```
interface Serial1/0.0
  encapsulation ppp
  ppp binding prof1
  ip address 10.0.0.1/24
  ip rtp compression-connections 20
  ip rtp header-compression
  ip rtp port 20000 200
  no shutdown
```

- 圧縮モード

  CRTP の圧縮モードには以下の 2 種類の設定が可能です。対向装置の圧縮方法に応じて、圧縮モードの設定を行ってください。

  デフォルトは de-fact-standard モードです。

  - proprietary モード：IP45/951 シリーズとの接続時に使用します。
  - de-fact-standard モード：その他の装置との接続時に使用します。

2.41.6 TCP ヘッダ圧縮（CTCP）

TCP ヘッダ圧縮（RFC2507）の設定は次のコマンドを使用します。
BRI，Serial，Dialer で有効です。

ip rtp header-compression	RTP ヘッダ圧縮の有効
ip rtp tcp-compression-connections	TCP ヘッダ圧縮接続数の変更
show ip rtp tcp-header-compression	CTCP 統計情報の表示
clear ip rtp tcp-header-compression	CTCP 統計情報のクリア

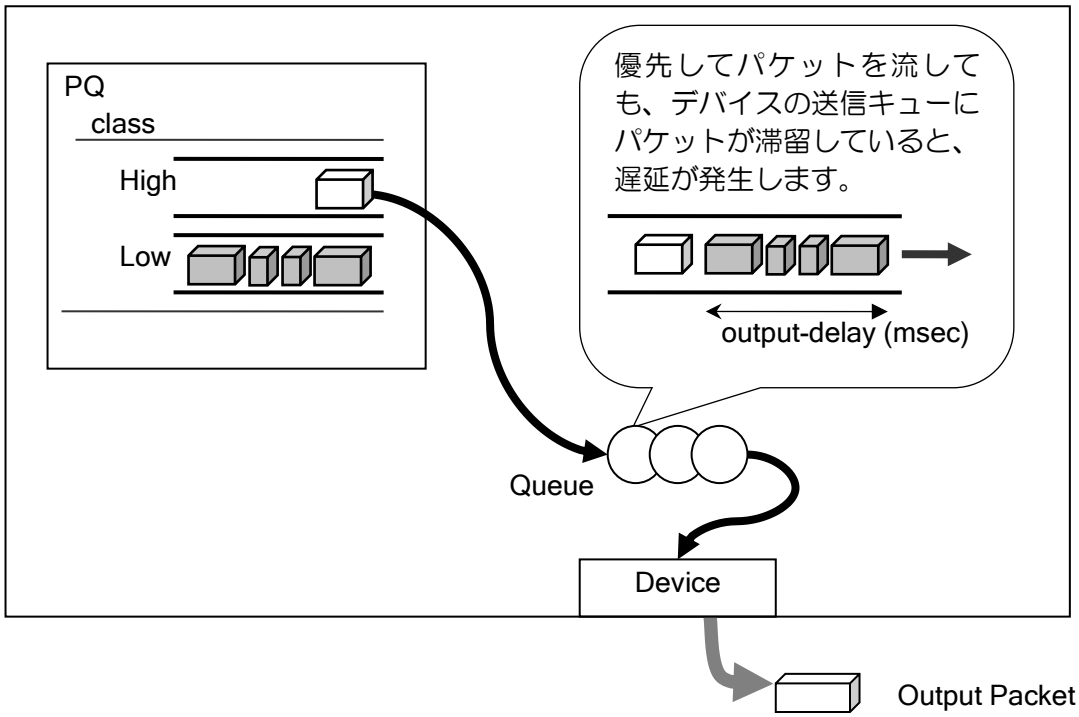
【設定例】

```
ppp profile prof1
  authentication myname ix2010
  authentication password ix2010 router

class-map match-any cmap1
  match rtp port 16384 160 high
  match any

policy-map pmap1
  class cmap1
  class class-local
  class class-default

interface Dialer0
  encapsulation ppp
  no auto-connect
  dialer string 111-1111
  ppp binding prof1
  ip address 10.0.0.1/24
  ip rtp compression-connections 20
  ip rtp header-compression
  ip rtp tcp-compression-connections 20
  service-policy enable
  service-policy output pmap1
  no shutdown
```

設定は PPP の再接続後に有効になります。

2.41.7 送出遅延制御

音声パケットを QoS のキューから優先的に取り出してもデバイス単位の送信キューで低い優先度のパケットが詰まっている場合には遅延が起こります。



この部分での遅延がどの程度まで許容できるかを、パケットをキューから取り出して回線に送信するまでの最大遅延時間によって制限することができます。この設定は BRI および Serial 基本インタフェースで有効で QoS を有効にしておく必要があります。

送信データ量が設定値をこえる場合パケットは QoS キューに留まりますが、QoS のキューも溢れればパケットは廃棄されます。

送信データ量制御の設定は次のコマンドを使用します。

output-delay	送信までにかかる遅延時間（msec）
show queue	デバイスキューの確認
show policy map interface	QoS キューの確認

【設定例】

```
class-map match-any cmap1
   match rtp port 16384 160 high
   match any

policy-map pmap1
   class cmap1

interface BRI1/0.0
   ppp binding prof1
   ip address 10.0.0.1/24
   service-policy enable
   service-policy output pmap1
   output-delay 3
   no shutdown
```

■2.42 AAA の設定

IX2000/IX3000 シリーズでは AAA 機能をサポートしています。
AAA とはネットワークのユーザおよびセキュリティ管理を行うための機能であり、以下に示す 3 つの機能の頭文字をとった略称です。

- 認証（Authentication）
- 許可（Authorization）
- アカウンティング（Accounting）

2.42.1 AAA の有効化

AAA を有効化するためには、以下のコマンドを実行します。

aaa enable	AAA 機能の有効化

AAA 機能では、サーバとして装置自身の他に RADIUS サーバを利用することができます。
使用するサーバの指定には以下の 4 種類の方法があります。

local	:	装置内のユーザデータベースを使用します。
local-case	:	装置内のユーザデータベースに該当情報が存在する場合にはそのデータベースを使用します。存在しない場合は次に指定されたサーバを使用します。 アカウンティングの場合はこの方法は使用できません。
group radius	:	登録された全ての RADIUS サーバを使用します。
group GROUP-NAME	:	サーバグループ指定コマンドで指定されたサーバを使用します。

複数のサーバをグループ化して扱うには、次のコマンドを使用します。

aaa group server	サーバグループの設定

認証，許可，アカウンティングそれぞれのリストにつき、データベースの指定を 4 個まで登録することができます。登録可能な順序は以下の表のとおりです。
実行時には、1 番から順にアクセスを行います。

データベース指定	設定方法			
	1	2	3	4
local	○	○	○	○
local-case	○	○	○	○
group radius	○	○	×	×
group GROUP-NAME	○	○	○	○

○：指定可能 ×：指定不可

※ group GROUP-NAME 以外は複数回の指定不可
※ local、local-case は同時指定不可
※ group radius、group GROUP-NAME は同時指定不可
※ local-case のみの指定不可

- local
  - ユーザの有無に関わらずローカルデータベースで認証を行います。ユーザが存在しなかった場合は認証 NG となります。
- local-case
  - ユーザが存在した場合のみローカルデータベースで認証を行います。ユーザが存在しなかった場合は認証タイムアウトとして処理されます。
- group radius
  - RADIUS サーバへ問い合わせを行います。
- group GROUP-NAME
  - RADIUS サーバへ指定グループを単位として問い合わせを行います。

2.42.2 認証（Authentication）の設定

ユーザが装置に対してアクセスする場合に、ユーザに対してログインとパスワード等を指定させ、ユーザの正当性を証明するための機能です。
認証では以下に示す機能をサポートします。

- ログイン認証
- PPP（CHAP/PAP）認証
- IEEE802.1X 認証（認証方式は RADIUS サーバのみサポート）
- MAC 認証（認証方式は RADIUS サーバのみサポート）（Ver.8.0 以降）

装置内のデータのみを使用する場合は、AAA 機能を利用しない場合でも認証を行うことができます。AAA 機能を利用することにより、RADIUS サーバを使用しデータベースを一元管理することが可能になります。

(a) ログイン認証

コンソール，telnet，SSH からのログイン時にユーザ名とパスワードの認証を行います。

認証方法を RADIUS サーバのみに設定すると、RADIUS サーバへアクセスできない場合は装置へログインできなくなりますので、RADIUS サーバを使用する場合でも、local のデータベースでログインできるように設定しておく事を推奨します。

ログイン認証の設定は次のコマンドを使用します。

グローバルコンフィグモード	
aaa authentication login	ログイン認証リストの登録
terminal authentication	ローカルコンソール認証リストの指定
telnet-server authentication	telnet 認証リストの指定
ssh-server authentication	SSH 認証リストの指定（Ver.8.7 以降）

【設定例】

telnet でのログイン時の認証に AAA を使用する。
最初にローカルデータベースに問い合わせを行い、
存在しなければ RADIUS サーバに問い合わせを行う。

```
aaa enable
aaa authentication login auth-list local-case group radius

radius host ip 192.168.160.10 key 0 test
```

```
radius host ip 192.168.160.11 key 0 test

telnet-server authentication auth-list
telnet-server ip enable
```

(b) PPP 認証

PPP 接続時にユーザ名とパスワードの認証を行います。

PPP 認証の設定は次のコマンドを使用します。

グローバルコンフィグモード	
aaa authentication ppp	PPP 認証リストの登録
PPP プロファイルコンフィグモード	
authentication list	PPP 認証リストの設定

【設定例】

PPP の認証に AAA を使用する。
RADIUS サーバに問い合わせを行う。

```
aaa enable
aaa authentication ppp ppp-auth group radius

radius host ip 192.168.160.10 key 0 test
radius host ip 192.168.160.11 key 0 test

ppp profile ins-ppp
  authentication list ppp-auth
  authentication accept chap
  authentication request chap

interface Dialer0
  ip address 10.0.0.1/30
  dialer string 01-234-567
  ppp binding ins-ppp
  no shutdown
```

(c) IEEE802.1X 認証

IEEE802.1X で Supplicant の認証を行います。認証方法は RADIUS サーバのみサポートします。

IEEE802.1X 認証の設定は次のコマンドを使用します。

グローバルコンフィグモード	
aaa authentication dot1x	IEEE802.1X 認証リストの登録
インタフェースコンフィグモード	
dot1x authentication	IEEE802.1X 認証リストの設定

【設定例】

```
IEEE802.1X の認証に AAA を使用する。
RADIUS サーバに問い合わせを行う。

aaa enable
aaa authentication dot1x dot1x-auth group radius

radius host ip 10.0.0.254 key 0 test

interface GigaEthernet1.0
   ip address 192.168.0.1/24
   dot1x enable
   dot1x authentication dot1x-auth
   no shutdown
```

(d) MAC 認証

MAC アドレスで端末の認証を行います。認証方法は RADIUS サーバのみサポートします。

MAC 認証の設定は次のコマンドを使用します。

グローバルコンフィグモード	
aaa authentication mac-auth	MAC 認証リストの登録
インタフェースコンフィグモード	
mac-auth authentication	MAC 認証リストの設定

【設定例】

```
MAC 認証に AAA を使用する。
RADIUS サーバに問い合わせを行う。

aaa enable
aaa authentication mac-auth mac-auth-list group radius

radius host ip 10.0.0.254 key 0 test

interface GigaEthernet1.0
   ip address 192.168.0.1/24
   mac-auth enable
   mac-auth authentication mac-auth-list
   no shutdown
```

2.42.2.1 認証の動作

(a) RADIUS サーバへの問い合わせ

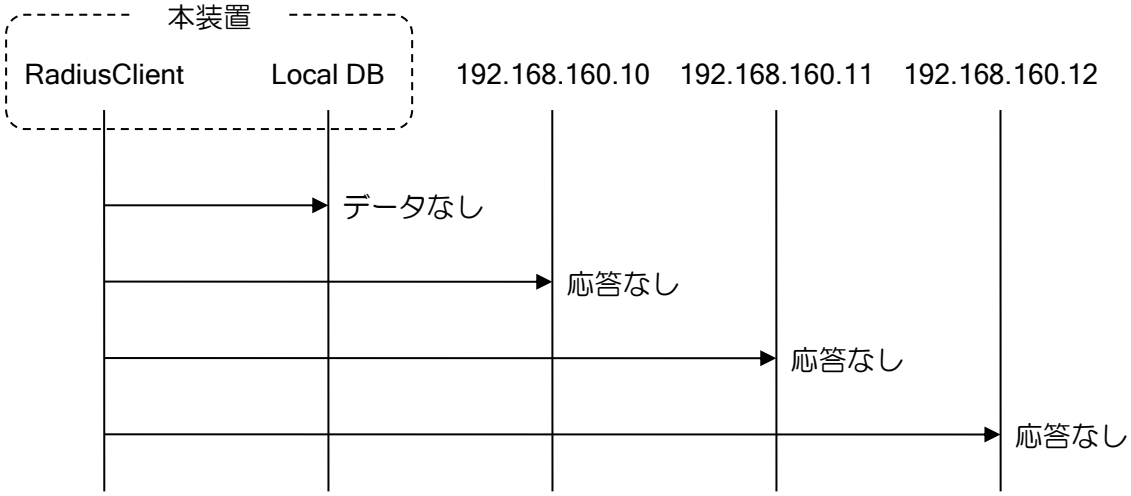
認証方法に group radius を指定した場合は、radius host コマンドで登録されているホストに対し、登録順に問い合わせを行います。認証結果の OK/NG に関係なく、RADIUS サーバから応答が返ってくると次のサーバに対する問い合わせは行いません。

また、認証方法にサーバグループを指定した場合は、サーバグループに設定された順番に問い合わせを行い、RADIUS サーバから認証 OK が返ってくると次のサーバに対する問い合わせは行いません。認証 NG の場合は、「(b)認証 NG 時の動作」の設定に従い、次に設定されている認証方法で問い合わせを行うか否か決定します。

(1) サーバグループを設定していない場合

【設定例】

```
aaa enable
aaa authentication login auth-list local-case group radius

radius host ip 192.168.160.10 key 0 test
radius host ip 192.168.160.11 key 0 test
radius host ip 192.168.160.12 key 0 test

telnet-server authentication auth-list
```



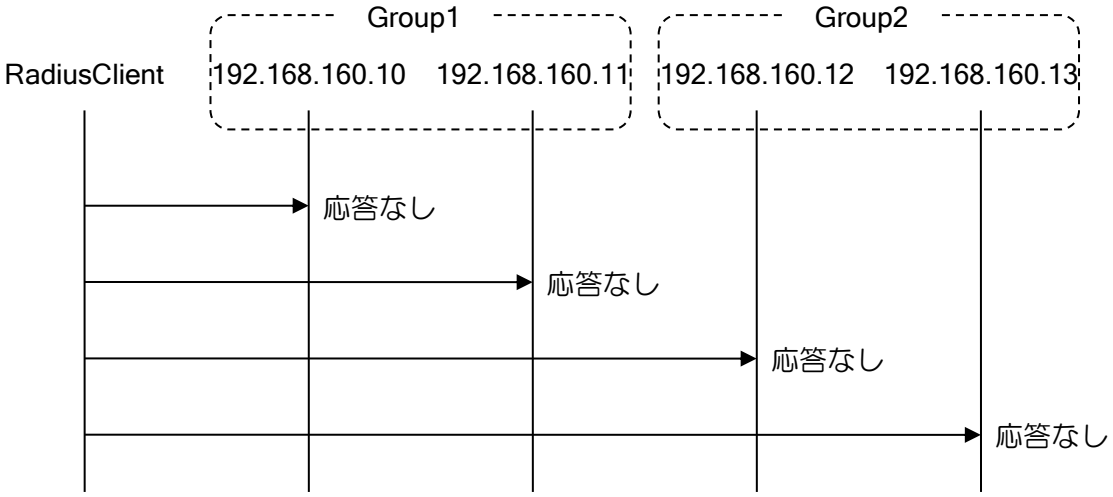
応答がない場合、radius host で指定した順序で問い合わせを行います。
認証 OK か認証 NG が返った場合はその場で問い合わせを終了します。

(2) サーバグループを設定している場合

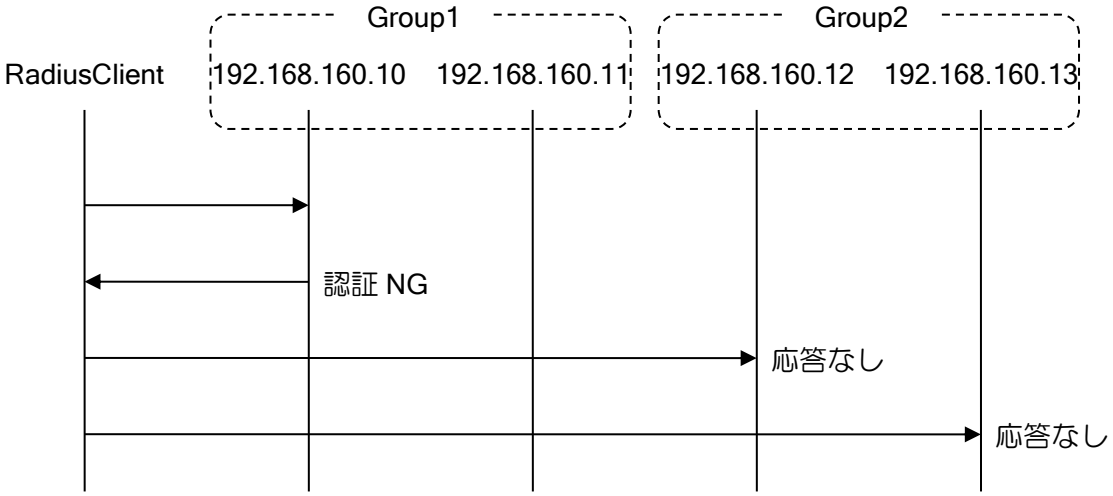
【設定例】

```
aaa group server radius group1 ip 192.168.160.10
aaa group server radius group1 ip 192.168.160.11
aaa group server radius group2 ip 192.168.160.12
aaa group server radius group2 ip 192.168.160.13

aaa authentication login auth-list group group1 group group2

radius host ip 192.168.160.10 key 0 test
radius host ip 192.168.160.11 key 0 test
```

```
radius host ip 192.168.160.12 key 0 test
radius host ip 192.168.160.13 key 0 test

telnet-server authentication auth-list
```



応答がない場合、指定されたサーバグループの順序で問い合わせを行います。



認証 NG が返った場合、「(b)認証 NG 時の動作」の設定によって動作が変わります。詳細は「(b) 認証 NG 時の動作」を参照してください。デフォルトでは次の認証方法（本設定の場合はサーバグループ）への問い合わせを行います。

認証 OK が返った場合、その場で問い合わせを終了します。

(b) 認証 NG 時の動作

認証 NG が返った場合に、次に設定されている認証方式で問い合わせを行うか否かを設定します。

グローバルコンフィグモード	
aaa authentication fail-action	認証 NG の動作を指定する

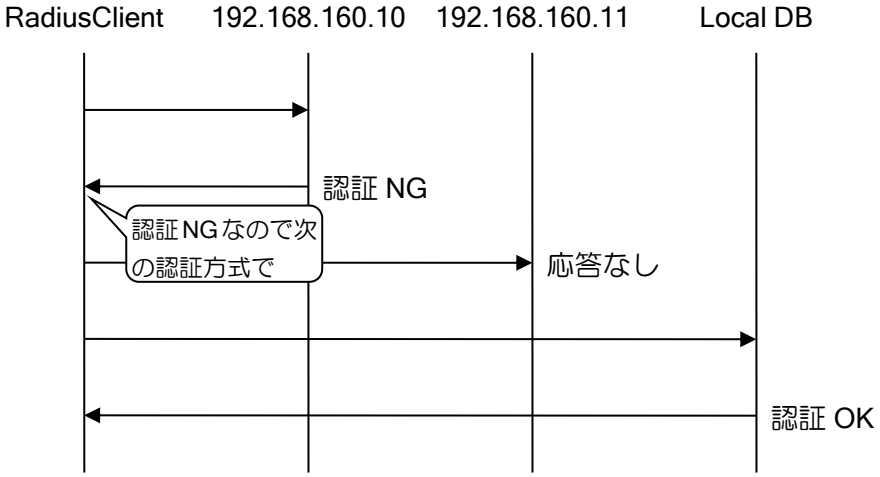
continue と stop が選択可能です。デフォルトは continue です。

【設定例１】

```
aaa group server radius group1 ip 192.168.160.10
aaa group server radius group2 ip 192.168.160.11

aaa authentication fail-action continue (デフォルト設定のため非表示)

aaa authentication login auth-list group group1 group group2 local

radius host ip 192.168.160.10 key 0 test
radius host ip 192.168.160.11 key 0 test

telnet-server authentication auth-list
```

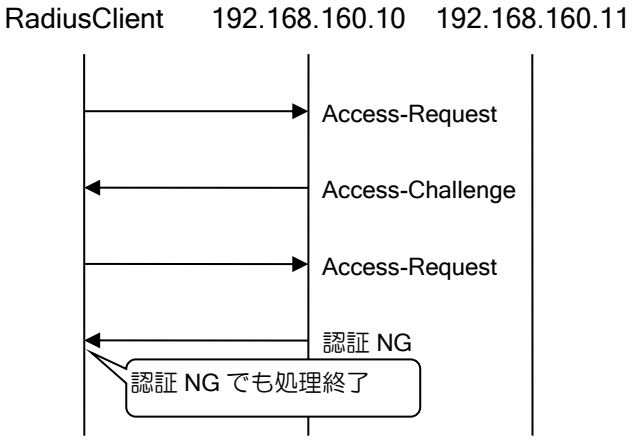
continue を設定した時の動作はログイン認証、PPP 認証の場合と、IEEE802.1X 認証の場合とで若干異なります。

ログイン認証、PPP 認証の場合は以下のように認証 NG 発生時は常に次に設定されている認証方式で問い合わせを行います。



IEEE802.1X 認証の場合は、RADIUS サーバへ送信した Access-Request に対して即座に Access-Reject が返った場合は上図と同様に次に設定されている認証方式で問い合わせを行います。

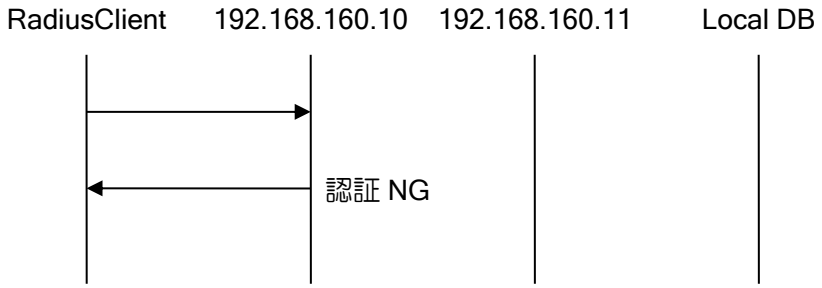
しかし Access-Request に Access-Challenge が返り、認証シーケンスが進んでしまった場合は、たとえ最終的に認証 NG となり Access-Reject が返っても次に設定されている認証方式への問い合わせを行いません。



【設定例２】

```
aaa group server radius group1 ip 192.168.160.10
aaa group server radius group2 ip 192.168.160.11

aaa authentication fail-action stop

aaa authentication login auth-list group group1 group group2 local

radius host ip 192.168.160.10 key 0 test
radius host ip 192.168.160.11 key 0 test

telnet-server authentication auth-list
```

stop を指定した場合、認証 NG 時に認証処理終了となります。



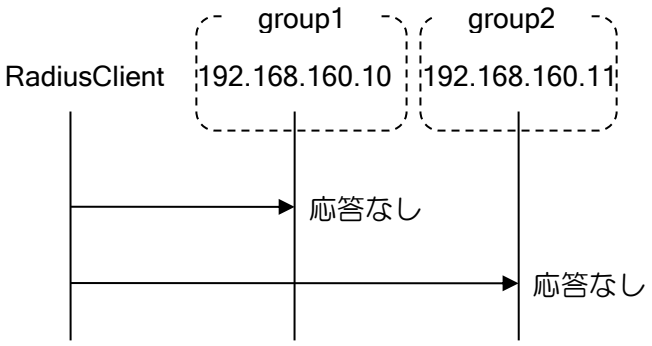
(c)サーバから応答が無い場合の動作

Ver.8.2 以降、認証時のサーバ指定に”none”を設定することにより、認証サーバから応答が無い場合に、認証を成功とすることが可能です。

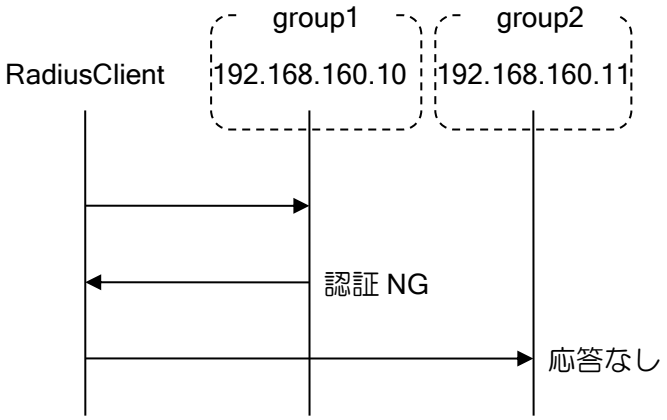
“none”の設定は、全ての認証方式に対して応答が無かった場合のみ、有効となります。途中の応答が認証 NG となっている場合には、”none”を設定しても、認証成功となりません。

【設定例】

```
aaa group server radius group1 ip 192.168.160.10
aaa group server radius group2 ip 192.168.160.11

aaa authentication login auth-list group group1 group group2 none

radius host ip 192.168.160.10 key 0 test
radius host ip 192.168.160.11 key 0 test

telnet-server authentication auth-list
```



group2 の応答が無い場合、none が有効となり認証が許可されます。



途中で認証 NG が返った場合、none は有効とならず、認証は許可されません。

none で認証成功となった場合、以下の動作となります。

- Login 認証時のユーザ権限は Administrator となります。
- 検疫機能使用時は、検疫フィルタは適用されません。
- アカウンティングのサーバタイプは LOCAL(2)となります。

2.42.3 許可（Authorization）の設定

認証完了後、ユーザに対してどのようなサービス実行を許可するかを制御します。
許可は単独では使用できません。認証の設定が必要となります。また、認証と許可ではデータベースの指定方法は一致させる必要があります。
許可では以下の機能をサポートしています。

- シェルサービス実行許可
- ネットワークサービス許可

(a)シェルサービス実行許可

コマンドプロンプトの実行を許可します。
ログイン認証後に、コマンドプロンプトの実行可能かどうかの確認を行います。許可されない場合は、ログインが失敗となります。

シェルサービス実行許可の設定は次のコマンドを使用します。

aaa authorization exec	シェルサービス実行許可リストの登録
terminal authorization	ローカルコンソール許可リストの指定
telnet-server authorization	telnet 許可リストの指定
ssh-server authorization	SSH 許可リストの設定（Ver.8.7 以降）

【設定例】

telnet 時の認証，シェルサービスの許可を行う。
最初にローカルデータベースへ問い合わせを行い、
存在しなければ、RADIUS サーバ（GROUP1）に
問い合わせを行う。

```
aaa enable
aaa group server radius group1 ip 10.10.10.10
aaa group server radius group1 ip 10.10.10.11
aaa group server radius group1 ip 10.10.10.12
aaa authentication login authen-list local-case group group1
aaa authorization exec author-list local-case group group1

radius host ip 10.10.10.10 key 0 test1
radius host ip 10.10.10.11 key 0 test2
radius host ip 10.10.10.12 key 0 test3

telnet-server authentication authen-list
telnet-server authorization author-list
telnet-server ip enable
```

(b)ネットワークサービス許可

PPP のネットワークサービス(IPCP 接続)を許可します。

PPP 認証後、サービスタイプによりネットワークサービスが実行可能かどうかの確認を行います。ネットワークサービスが許可時、RADIUS サーバから払い出し IP アドレスが提示されている場合に、IPCP の IP-Address オプションを用いて払い出しを行います。PPP の対向装置で払い出し IP アドレスを使用したい場合、ip address ipcp コマンド設定が必要です。許可されない場合、PPP は切断されます。

ネットワークサービスの許可の設定は次のコマンドを使用します。

aaa authorization network	ネットワークサービス実行許可リストの登録
authorization list	PPP 許可リストの指定 （PPP プロファイルコンフィグモード）

【設定例】

PPP の認証，ネットワークサービスの許可を行う。
RADIUS サーバ（GROUP1）に問い合わせを行う。

センタ側

```
aaa enable
aaa group server radius group1 ip 10.10.10.10
aaa group server radius group1 ip 10.10.10.11
aaa group server radius group1 ip 10.10.10.12
aaa authentication ppp ppp-authen group group1
aaa authorization network ppp-author group group1

radius host ip 10.10.10.10 key 0 test1
radius host ip 10.10.10.11 key 0 test2
radius host ip 10.10.10.12 key 0 test3

ppp profile ppp-profile
   authentication list ppp-authen
   authorization list ppp-author

interface Dialer0
   encapsulation ppp
   ip address 10.0.0.1/30
   ppp binding ppp-profile
   no shutdown
```

```
リモート側
ppp profile ppp-profile
   authentication myname ix-router
   authorization password ix-router ix-router

interface Dialer0
   encapsulation ppp
   ip address ipcp
   ppp binding ppp-profile
   no shutdown
```

2.42.3.1 許可の動作

(a)許可方法の設定時の注意事項

RADIUS プロトコルでは、許可に使用するデータも認証実行時に一括で取得します。そのため、認証と許可に使用するサーバが異なる場合、許可データが正しく取得できない場合があります。そのため、AAA では認証サーバと許可サーバが異なる場合、許可失敗として処理します。従って、認証と許可では使用するデータベースの指定方法は一致させる必要があります。

```
【設定例】

正しい例（指定するサーバグループが同じ）
認証設定　1:local-case 2: server-group
許可設定　1:local-case 2: server-group
aaa authentication ppp ppp-authen local-case group server-group
aaa authorization network ppp-author local-case group server-group

ppp profile ppp-profile
   authentication list ppp-authen
   authorization list ppp-author

正しくない例（指定するサーバグループが異なる）
認証設定　1:local-case 2:group11
許可設定　1:group2 2:group12
aaa authentication ppp ppp-authen local-case group group11
aaa authorization network ppp-author group group2 group group12

ppp profile ppp-profile
   authentication list ppp-authen
   authorization list ppp-author
```

(b)サーバから応答が無い場合の動作

Ver.8.2 以降、認証の場合と同様に、サーバ指定に”none”を設定可能です。許可の場合は、”none”を設定することにより、無条件で許可成功となります。

2.42.4 アカウンティング（Accounting）の設定

装置内で発生した各事象に対するアカウンティング（記録）を行います。

以下の事象についてアカウンティングを行います。また、認証失敗以外については、開始と終了または終了のみをアカウンティングするかを設定することができます。

- シェルサービスアカウンティング
  - シェルサービスの開始（ログイン）
  - シェルサービスの終了（ログアウト）
- ネットワークサービスアカウンティング
  - ネットワークサービスの開始（PPP 接続）

- ✧ ネットワークサービスの終了（PPP 切断）
- ➢ IEEE802.1X アカウンティング
  - ✧ 認証完了
  - ✧ 認証解除
- ➢ 認証失敗アカウンティング
  - ✧ ログイン認証失敗
  - ✧ PPP 認証失敗
  - ✧ IEEE802.1X 認証失敗
- ➢ 呼接続・切断アカウンティング
  - ✧ ISDN の呼接続
  - ✧ ISDN の呼切断（接続した呼に対する切断）
- ➢ システムイベントアカウンティング
  - ✧ restart,reload の実行
  - ✧ 起動完了

アカウンティングの場合は複数のデータベースを指定している場合は、全てに対してアカウンティングを行います。

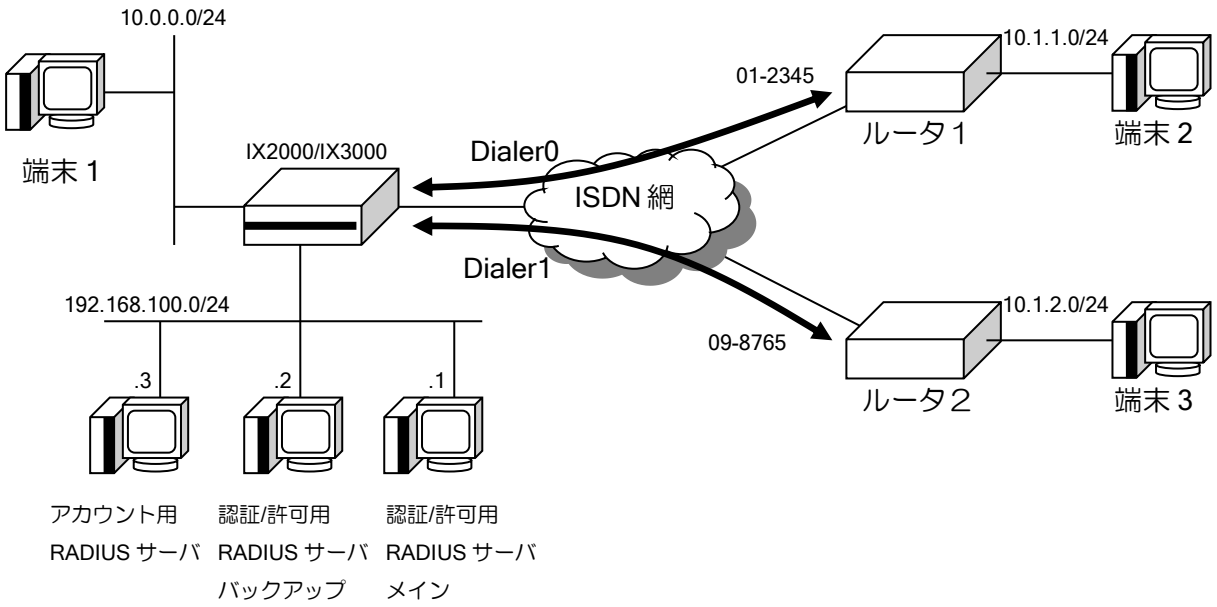
アカウンティングの設定は次のコマンドを使用します。

aaa accounting dot1x	IEEE802.1X アカウンティングの登録
aaa accounting exec	シェルサービスアカウンティングの登録
aaa accounting network	ネットワークサービスアカウンティングの登録
aaa accounting send	認証失敗アカウンティングの登録
aaa accounting resource	呼接続・切断アカウンティングの登録
aaa accounting system	システムアカウンティングの登録
aaa accounting system-delay	スタートイベントアカウンティング遅延時間設定
terminal accounting	ローカルコンソールアカウンティングリストの指定
telnet-server accounting	telnet アカウンティングリストの指定
ssh-server accounting	SSH アカウンティングリストの指定（Ver8.7 以降）
accounting list	PPP アカウンティングリストの指定 （PPP プロファイルモード）
aaa accounting max-records	ローカルアカウンティングレコード数の設定
show aaa accounting-records	ローカルアカウンティングレコードの表示
clear aaa accounting-records	ローカルアカウンティングレコードのクリア

【設定例】
コンソールからのログイン/ログオフ,認証失敗,システム停止/起動
のイベントに関してローカル、Radius サーバ（group1）に
アカウンティングを行う。

```
terminal accounting login-acc

aaa enable
aaa group server radius group1 ip 10.10.10.10
aaa group server radius group1 ip 10.10.10.11
aaa group server radius group1 ip 10.10.10.12
aaa accounting send stop-record authentication-failure
aaa accounting exec login-acc start-stop local group group1
aaa accounting system default start-stop local group group1

radius host ip 10.10.10.10 key 0 test1
radius host ip 10.10.10.11 key 0 test2
radius host ip 10.10.10.12 key 0 test3
```

2.42.5 AAA の使用例



【設定例】
PPP 認証/ネットワークサービス許可は RADIUS サーバ（メイン,バックアップ）を使用
アカウントはローカルとアカウント用の RADIUS サーバを使用。
アカウントの対象は
　PPP 接続完了/終了
　ISDN 接続/切断
　装置の起動/停止
　認証失敗

```
aaa enable
aaa group server radius auth-grp1 ip 192.168.100.1
aaa group server radius auth-grp1 ip 192.168.100.2
aaa group server radius acc-grp1 ip 192.168.100.3
aaa authentication ppp ppp-auth1 local-case group auth-grp1
aaa authorization network ppp-auth2 local-case group auth-grp1
aaa accounting send stop-record authentication-failure
aaa accounting network acc-list1 start-stop local group acc-grp1
aaa accounting resource default start-stop local group acc-grp1
aaa accounting system default start-stop local group acc-grp1

radius host ip 192.168.100.1 key 0 auth-host
radius host ip 192.168.100.2 key 0 auth-host
radius host ip 192.168.100.3 key 0 acc-host

ip route 10.1.1.0/24 Dialer0
ip route 10.1.2.0/24 Dialer1

ppp profile ppp1
  accounting list acc-list1
  authentication list ppp-auth1
  authentication accept chap
  authentication request chap
```

```
   authentication myname center
   authentication password center ix-router
   authorization list ppp-auth2

interface GigaEthernet0.0
   ip address 10.0.0.254/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.100.254/24
   no shutdown

interface Dialer0
   encapsulation ppp
   no auto-connect
   dialer string 01-2345
   ppp binding ppp1
   ip address ipcp
   no shutdown
!
interface Dialer1
   encapsulation ppp
   no auto-connect
   dialer string 09-8765
   ppp binding ppp1
   ip address ipcp
   no shutdown
```

2.42.6 RADIUS クライアント

IX2000/IX3000 シリーズでは RADIUS クライアント機能をサポートしています。

RADIUS クライアントの設定には次のコマンドを使用します。

radius host	RADIUS サーバホスト設定
radius deadtime	無応答サーバのアクセスブロック時間
show radius statistics	RADIUS 統計情報の表示

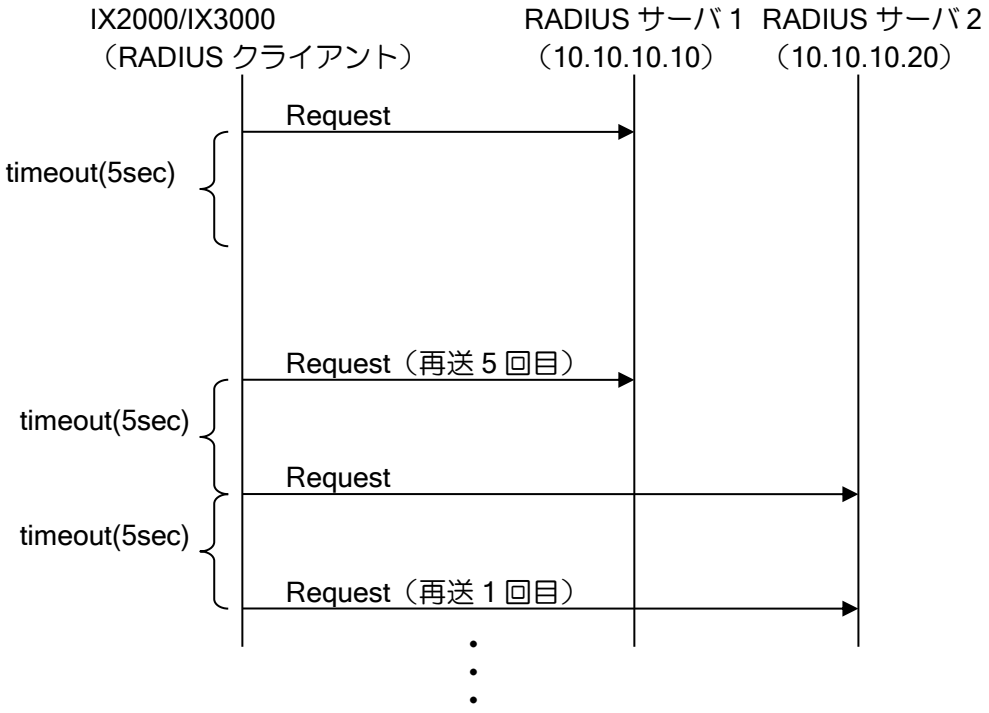
【設定例】

```
radius deadtime 15
radius host ip 10.10.10.10 retransmit 5 timeout 10 key 0 radius source
                                                          GigaEthernet0.0
radius host ip 10.10.10.20 retransmit 5 timeout 10 key 0 radius source
                                                          GigaEthernet0.0
```

RADIUS サーバでは、通常、送信元アドレスと秘密鍵の組み合わせで認証を行いますので、RADIUS サーバへの経路が複数存在する場合は、送信元アドレスを固定するために、RADIUS サーバ設定時に source オプションで送信元アドレスの指定を行ってください。

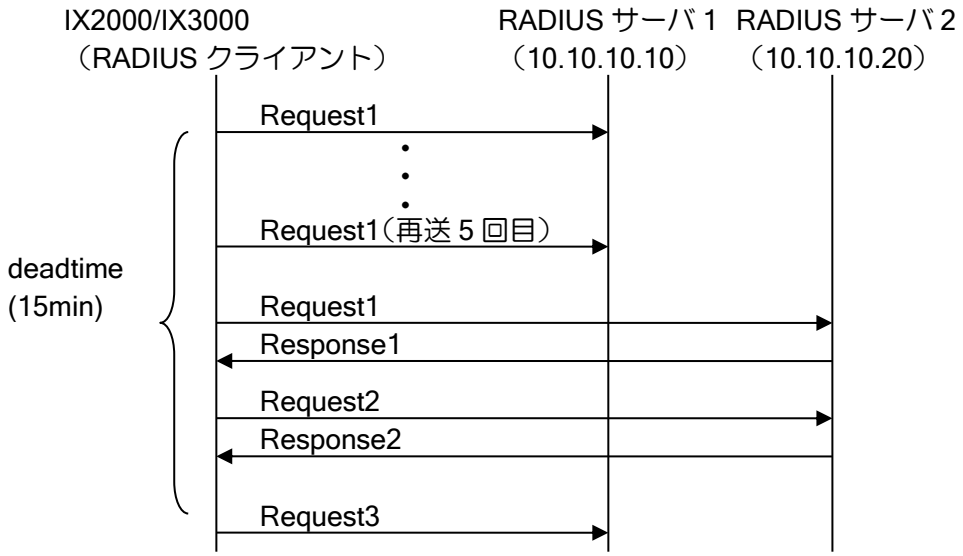
- 複数サーバ設定時の再送

  複数の RADIUS サーバが存在する場合、1 つのサーバに対して指定された回数の再送を行った後、次のサーバへ問い合わせを行います。



- dead time

  指定回数再送しても応答が返らない場合、deadtime の間はそのサーバへの問い合わせを行わず、次のサーバへ問い合わせを行います。deadtime 経過後は、再度そのサーバへ問い合わせを行ないます。



- サポートするアトリビュート
  以下のアトリビュートをサポートしています。

RADIUS

番号	名称	内容
1	User-Name	ユーザ名
2	User-Password	パスワード
3	CHAP-Password	CHAP パスワード
4	NAS-IP-Address	RADIUS クライアントのアドレス
5	NAS-Port	RADIUS クライアントのポート番号
6	Service-Type	提供するサービス種別
7	Framed-Protocol	プロトコル種別
8	Framed-IP-Address	IPCP で払い出す IP アドレス
18	Reply-Message	応答メッセージ
27	Session-Timeout	提供するサービスの時間
30	Called-Station-Id	着信番号
31	Calling-Station-Id	発信番号
60	CHAP-Challenge	CHAP チャレンジ
61	NAS-Port-Type	RADIUS クライアントのポート種別
79	EAP-Message	EAP メッセージ
80	Message-Authenticator	パケット全体の HMAC-MD5 ハッシュ
96	Framed-Interface-Id	インタフェース ID

アカウンティング

番号	名称	内容
40	Acct-Status-Type	サービスの開始/終了
41	Acct-Delay-Time	ネットワーク転送時間
42	Acct-Input-Octets	受信オクテット数
43	Acct-Output-Octets	送信オクテット数
44	Acct-Session-Id	セッション ID
45	Acct-Authentic	ユーザの認証方法
46	Acct-Session-Time	サービスを受けた時間
47	Acct-Input-Packets	受信パケット数
48	Acct-Output-Packets	送信パケット数
49	Acct-Terminate-Cause	終了の要因

2.42.6.1 各機能で使用するアトリビュート

(a) ログイン認証

番号	アトリビュート	Value
1	User-Name	ログインユーザ名
2	User-Password	ログインパスワード
61	NAS-Port-Type	ローカルコンソール時（async:0） telnet,SSH 時（Virtual:5 固定）
5	NAS-Port	TTY 番号
31	Calling-Station-Id	接続元 IP アドレス（telnet,SSH 時に付与）
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス

(b) PPP 認証

番号	アトリビュート	Value
1	User-Name	PPP ユーザ名
2	User-Password	PPP 認証パスワード（PAP 認証時に付与）
3	CHAP-Password	PPP 認証パスワード（CHAP 認証時に付与）
60	CHAP-Challenge	CHAP チャレンジ（CHAP 認証かつ CHAP チャレンジの長さが 16 オクテット以外の場合に付与）
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
5	NAS-Port	接続インタフェース番号（0x8000_0000+ifIndex）
61	NAS-Port-Type	専用線時（sync:1） ISDN 時（ISDN-sync:2） PPPoE 時（Ethernet:15）
7	Framed-Protocol	フレームプロトコル（PPP:1 固定）
6	Service-Type	端末に提供するサービスタイプ（Framed:2 固定）
30	Called-Station-Id	着信端末電話番号（ISDN 接続時に付与） 発呼時（相手電話番号） 着呼時（自己電話番号）
31	Calling-Station-Id	発信端末電話番号（ISDN 接続時に付与） 発呼時（自己電話番号） 着呼時（相手電話番号）

(c) IEEE802.1X 認証

番号	アトリビュート	Value
1	User-Name	Supplicant のユーザ名
30	Called-Station-Id	ルータインタフェースの MAC アドレス
31	Calling-Station-Id	Supplicant の MAC アドレス
6	Service-Type	端末に提供するサービスタイプ（Framed:2 固定）
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
5	NAS-Port	接続インタフェース番号（0x8000_0000+ifIndex）
61	NAS-Port-Type	接続インタフェースのタイプ（Ethernet:15 固定）
79	EAP-Message	EAP メッセージ
24	State	RADIUS サーバからの Access-Challenge に含まれている State アトリビュートをそのまま付与 （チャレンジに対する応答時に付与）
27	Session-Timeout	Authenticator のタイマ
80	Message-Authenticator	パケット全体の HMAC-MD5 ハッシュ値

(d) MAC 認証

番号	アトリビュート	Value
1	User-Name	端末の MAC アドレス（書式は変更可能）
2	User-Password	上記 MAC アドレスの MD5
30	Called-Station-Id	ルータインタフェースの MAC アドレス
31	Calling-Station-Id	端末の MAC アドレス
6	Service-Type	端末に提供するサービスタイプ（Framed:2 固定）
5	NAS-Port	接続インタフェース番号（0x8000_0000+ifIndex）
4	NAS-IP-Address	RADIUS パケット送信インタフェースの IP アドレス
61	NAS-Port-Type	接続インタフェースのタイプ（Ethernet:15 固定）
27	Session-Timeout	再認証タイマ

2.42.7 サーバの設定

(a)RADIUS の場合

- 認証に関する設定

  Service-Type によって、ユーザレベルを決定します。

  IX2000/IX3000 シリーズでは administrator/monitor/operator の 3 種類のレベルが使用可能ですが、RADIUS サーバを使用する場合は、monitor レベルの設定はできません。

  Service-Type

設定値	ユーザレベル
Login(1)	operator
Framed(2)	administrator
Administrative(6)	administrator
NAS Prompt(7)	operator
指定無し	operator

- 許可に関する設定

  Service-Type/Framed-Protocol によって、サービスに対する許可/拒否を決定します。

  Service-Type

設定値	シェルサービス	ネットワークサービス
Login(1)	○	×
Framed(2)	○	○
Callback Login(3)	×	×
Callback Framed(4)	×	○
Outband(5)	×	○
Administrative(6)	○	×
NAS Prompt(7)	○	×
Authenticate Only(8)	×	×
Callback NAS Prompt(9)	×	×
指定なし	×	×

  Framed-Protocol（Service-Type=Framed のみ指定してください）

設定値	シェルサービス	ネットワークサービス
PPP(1)	×	○
その他	○	×
指定なし	○	○

- ネットワークサービスに関する設定

  PPP の IPCP による IP アドレス払い出しを行いたい場合、Framed-IP-Address で払い出したい IP アドレスを設定します。Framed-IP-Address が設定されていない場合は IP アドレスの払い出しは行いません。

項目名	内容
Framed-IP-Address	IPCP にて払い出しを行う IP アドレス

【例】
RADIUS 設定例 1
　User-Name：nec01
　User-Password："nec01passwd"
　Service-Type = Framed,
　Framed-Protocol = PPP,
　Framed-IP-Address = 192.168.1.1
動作
　　PPP からの接続のみが許可される。
　　IP アドレス=192.168.1.1 が払い出される。
　　telnet,コンソールからのログインは許可されない。

RADIUS 設定例 2
　User-Name：ix01
　User-Password："ix01passwd"
　Service-Type = Login,

動作
　　telnet,コンソールからは operator モードでのログインが許可される。
　　PPP からの接続は許可されない。

■2.43 Web コンソールの設定

Web ブラウザで装置の設定や各種状態確認を行うことができる Web コンソール機能をサポートしています。ただし、Ver.9.2 以降から仕様を大きく変更しており、バージョンアップごとに対応機能を増やしているため、できるだけ新しいバージョンをご利用ください。

Ver9.1 までの Web コンソール機能は付録の仕様を参照してください。

2.43.1 Web コンソール機能の特徴

Web コンソール機能は、主に以下の用途で利用することができます。対応バージョンや設定される内容の詳細は、後述の説明を参照してください。

- かんたん設定

  インターネット接続や、インターネット接続＋VPN 接続、クラウド接続などを、指示通り入力するだけで、かんたんに設定することができます。また UNIVERGE Aspire シリーズをご利用の場合に IP 電話サービスのネットワーク設定も、かんたんに設定することができます。

- 詳細設定・端末管理

  詳細設定では、フィルタや NAPT、QoS など、かんたん設定に含まれない詳細な設定ができます。端末管理では、LAN 側に接続した端末のさまざまな情報を管理する「リンクマネージャ機能」を利用できます。

- 保守管理

  装置状態の確認、ソフトウェアの更新、コンフィグ管理、ping の実行など、各種保守機能を利用できます。

- 拡張ページ

  用途にあわせてカスタマイズしたページを登録することができます。HTML と Javascript で、任意の show コマンドの結果を参照して現在の設定や状態を表示したり、ほぼ全ての CLI コマンドを生成して実行する任意のページを作成可能です。

2.43.2 注意事項

- Web コンソールで設定できる機能は、CLI で設定できる一部の機能しか対応しておりません。CLI で設定したあとに Web コンソールで設定を変更すると正しく制御できないことがありますので（例えばフィルタ機能は Web コンソールから設定した内容以外参照・変更できません）、CLI で設定を変更したあとに利用する場合は、変更後のコンフィグをよく確認してご利用ください。
- 工場出荷状態で Web コンソールが利用できる装置は、IX2105,IX2106,IX2107,IX2207,IX2235 です。それ以外の装置は CLI で Web コンソール機能を有効化してから利用する必要があります。

2.43.3 Web コンソールを利用する設定

IX2105,IX2106,IX2107,IX2207,IX2235,の工場出荷時から Web コンソールが利用できる装置は、以下の設定が最初から投入されているため、設定は不要です。

```
LAN インタフェースは機種によって異なります。
最老番のインタフェースが LAN インタフェースとなります。

logging buffered 131072
logging subsystem all warn
logging timestamp datetime
!
ip ufs-cache enable
ip dhcp enable
ip access-list web-http-acl permit ip src any dest 192.168.1.254/32
!
http-server ip access-list web-http-acl
http-server ip enable
!
ip dhcp profile web-dhcp-gigaethernet1.0
   dns-server 192.168.1.254
!
interface GigaEthernet1.0
   ip address 192.168.1.254/24
   ip dhcp binding web-dhcp-gigaethernet1.0
   no shutdown
!
web-console system information
   o lan1 GigaEthernet1.0
```

Web コンソールの初期設定がない装置は、同様の設定を投入してご利用ください。

```
LAN インタフェースを GE0.0、WAN インタフェースを GE2.0 とする場合。

Ver9.6 以降ではインタフェースで http-server ip enable 設定をすることで
既存の ACL と同様の効果が得られます。

logging buffered 131072
logging subsystem all warn
logging timestamp datetime
!
ip ufs-cache enable
ip dhcp enable
!
ip dhcp profile web-dhcp-gigaethernet0.0
   dns-server 192.168.1.254
!
interface GigaEthernet0.0
   ip address 192.168.1.254/24
   ip dhcp binding web-dhcp-gigaethernet0.0
   http-server ip enable
   no shutdown
!
web-console system information
   o lan1 GigaEthernet0.0
   o wan1 GigaEthernet2.0
```

2.43.3.1 HTTP サーバの設定

Web コンソールを使用するために、HTTP サーバを有効にする必要があります。Web コンソールへのアクセスを制限する場合は、アクセスリストを利用してください。

http-server ip/ipv6 enable	HTTP サーバの有効化(IPv6 は Ver.10.3 以降)
http-server ip/ipv6 access-list	HTTP サーバのアクセスリスト設定 (IPv6 は Ver.10.3 以降)

Ver.9.6 以降では HTTP サーバの有効化設定はインタフェースコンフィグモードでも設定できます。この場合、設定したインタフェースからの通信のみ HTTP サーバが動作します。

Ver.10.1 以降では HTTPS 接続に対応しています。（TLS1.2 のみ）

初期状態の証明書は埋め込みタイプの自己証明書です。必要に応じて pki コマンドで取り込んだ任意の証明書を利用してください。

2.43.3.2 Web コンソールログインユーザの設定

Web コンソールへログインするユーザの設定を行います。Web コンソールへログインするユーザは 1 ユーザのみ設定可能で、username コマンドで administrator 権限のユーザを設定している必要があります。

また、無操作の場合に自動ログアウトする時間を設定することができます。未設定の場合は、Ver.9.1 以前では自動ログアウトを行わず、Ver.9.2 以降は 60 分で自動ログアウトを行います。

http-server username	Web コンソールログインユーザの設定
http-server terminal timeout	Web コンソールログインタイムアウトの設定

2.43.3.3 工場出荷設定の切り替え

出荷時に Web コンソールが使用可能な装置は、初期状態は Web コンソールが使用できるコンフィグで起動するモードに設定されています。Web コンソール用コンフィグで起動するモード（Web コンソールモード）と通常の何も設定されていない状態で起動するモード（通常モード）をコマンドで変更することができます。

Web コンソールモードの場合、startup-config,default-config が存在しない状態で再起動すると、Web コンソール用のコンフィグで起動します。

startup-config,default-config が存在する場合は、startup-config,default-config で起動します。

通常モードの場合、startup-config,default-config が存在しない場合、何も設定されていない状態で起動します。

Web コンソールを使用しない場合は、通常モードへ設定を変更して使用してください。

モード変更コマンドは以下の通りです。この変更はコンフィグに表示されません。

default-console	デフォルトコンフィグモード変更 （オペレーションモード）

```
【コマンド実行例】
Web コンソールモードに変更
# default-console web
```

2.43.4 対応ブラウザ

対応している Web ブラウザは以下の通りです。

- Internet Explorer® 7 （～Ver9.4）
- Internet Explorer® 8/9/10 （Ver.8.9～Ver9.4）
- Internet Explorer® 11 （Ver.9.0 以降）
- Microsoft Edge®（Ver9.3 以降）
- Microsoft Edge® (Chromium 版)（Ver10.4 以降）

※Internet Explorer®および Microsoft Edge®は、米国 Microsoft Corporation の、米国およびその他の国における登録商標または商標です。

2.43.5 Web コンソールの操作

詳細は Web 設定マニュアルを参照してください。

2.43.5.1 ログイン/ログアウト

ログインを行うことにより、Administrator 権限の操作を行うことができるようになります。ログインを行えるユーザは、コンソール，telnet 合わせて、1 ユーザです。

画面左側のメニューから「ログイン」を選択すると、ユーザ名とパスワードを入力する画面が表示されます。ユーザ名、パスワードを入力してください。一度ログインした後は、ブラウザを終了するまでユーザ名、パスワードの入力は不要になります。

ログイン状態の管理のため Cookie を使用していますので、ブラウザの Cookie の設定は有効にしてください。また、ログイン中は Cookie の削除は行わないでください。

操作終了後は、画面右側のメニューから「ログアウト」を選択し、表示された画面の［ログアウト実行］ボタンを押してログアウトしてください。

2.43.5.2 強制ログイン/強制ログアウト

ログインを行えるユーザは、コンソール，telnet 等合わせて、1 ユーザです。既に別のユーザがログインしている場合はログインできませんが、強制ログインを行えば、ログイン中のユーザを強制的にログアウトさせて新しくログインすることができます。

「ログイン」を選択し、ユーザ名、パスワードを入力すると、強制ログインの画面に遷移します。［強制ログイン実行］を押すとログインします。

2.43.5.3 設定の保存

画面左上のメニューから「設定の保存」を選択すると、設定の保存の画面に遷移します。［保存実行］を押すと設定の保存ができます。

「!!注意!! 設定が変更されています。」と赤字で表示されている場合は、設定が保存されていませんので、設定の保存を行ってください。メッセージ内の「設定の保存」を選択した場合も、設定の保存の画面に遷移します。

2.43.6 Web コンソールの保守管理

利用方法は Web 設定マニュアルを参照してください。ここでは各ページの機能について説明します。

2.43.6.1 装置状態の表示

装置の状態を表示します。設定追加後のトップページも同様の内容です。

自動更新(Ver.9.6 以降)	
自動更新間隔	ページを自動で更新する間隔です。(default：停止) 自動更新後も、指定した間隔でページの更新をします。

装置情報	
装置名	装置名を表示します。 hostname コマンドの設定名です。
バージョン	ソフトウェアバージョンを表示します。 show version の Software バージョンです。
稼働時間	装置の起動時間を表示します。 show uptime の System uptime です。
稼働率	システムの Utilization を表示します。 show utilization の System utilization です。
メモリ	メモリ使用量をパーセントで表示します。 show memory の Heap memory の memory used です。
内部温度	装置内部温度を表示します。 show environment の Internal temperature です。 正常時は青、異常時は赤で表示します。
内部電圧	装置内部電圧を表示します。 show environment の 3.3 volt line measured です。 正常時は青、異常時は赤で表示します。

ネットワーク情報	
デバイス	デバイス名を表示します。 T1 カード、4BRI-ST カードは非対応です。
接続状態	デバイスの状態を表示します。 show devices の情報を参照し、リンク状態や up の場合に speed, duplex を表示します。 SW-HUB の場合はポート毎に状態を表示します。
送信量	現在のデバイスの送信の使用率を表示します。 show utilization の last transmit util です。
受信量	現在のデバイスの受信の使用率を表示します。 show utilization の last receive util です。

WAN 情報（設定可能な機種）	
接続名	接続名を表示します。 description で設定した値を表示します。

接続状態	接続状態を表示します。 接続： 通信可能です。 IP 接続の場合は、リンク up している状態です。 PPPoE・USB の場合は、IPCP まで OPEN している状態です。 アドレス取得中： DHCP でアドレス取得中に表示します。 IPCP 確立中： PPPoE で認証終了後の IPCP 接続中に表示します。 認証中： PPPoE で認証処理中に表示します。 この状態のまま接続できない場合は、ppp profile のユーザ ID、パスワードや ppp profile 名などの設定に誤りがある可能性があります。 接続されていません： この状態のまま接続できない場合は、物理的な接続に問題がある可能性があります。 Ver.9.6 以降、IPv4 と IPv6 が同時に設定している場合、両方の設定を表示します。
情報	接続情報を表示します。 IP アドレスと DNS アドレスを表示します。 また、Ver.9.6 以降、IPv6 アドレスと IPv6 DNS アドレスも表示します。

VPN 情報(Ver.9.5 以前)	
接続名	接続名を表示します。 description で設定した内容を表示します。
接続種別	接続種別を表示します。 ダイナミック VPN（拠点）／（センタ）：ダイナミック VPN で接続 IPsec：IPsec トンネルで接続 IP トンネル：GRE トンネルで接続 L2TP/IPsec：L2TP/IPsec で接続
接続状態	接続状態を表示します。 接続：通信可能です。 GRE の場合 Tunnel インタフェースが Up した状態です。 その他の場合 IPsec-SA が作成された状態です。 接続されていません：通信できません。

VPN 情報(Ver.9.6 以降)	
接続名	接続名を表示します。 接続名の設定で表示した日本語文字列 または、description で設定した内容を表示します。
接続状態	接続状態を表示します。 接続：通信可能です。 GRE の場合 Tunnel インタフェースが Up した状態です。 IPsec(IKEv1)の場合 IPsec-SA が作成された状態です。

	IPsec(IKEv2)の場合 Child-SA が作成された状態です。 L2TP/IPsec の場合 L2TP トンネルがアクティブの状態です。 ダイナミック VPN の場合 接続先と通信状態が Up した状態です。 接続されていません：通信できません。 - (ハイフン) ： 4-over-4 / 4-over-6 / 6-over-4 / 6-over-6 / Ether-IP の場合、表示します。
通信量	通信量を表示します。 送信：接続先に送信したパケット数 受信：接続先から受信したパケット数
接続種別	マウスカーソルが各 VPN 情報上にある場合に表示します。 接続種別を表示します。 ダイナミック VPN（拠点）／（センタ） ：ダイナミック VPN で接続 拠点番号がある場合、各拠点番号を表示します(拠点 1, 拠点 2 …)。 IPsec(IKEv1) ：IPsec トンネルで接続 IPsec(IKEv2) ：IPsec-ikev2 トンネルで接続 IP トンネル(GRE) ：GRE トンネルで接続 IP トンネル(x-over-x)：4-over-4 / 4-over-6 / 6-over-4 / 6-over-6 トンネルで接続 IP トンネル(Ether-IP)：Ether-IP トンネルで接続 L2TP/IPsec ：L2TP/IPsec で接続
接続先アドレス	マウスカーソルが各 VPN 情報上にある場合に表示します。 接続先の IP アドレス、IPv6 アドレスを表示します。

2.43.6.2 VPN の接続名設定（Ver.9.6 以降）

「装置状態の表示」の「接続名編集」で、VPN の接続名を日本語で表示することができます。
“(二重引用符)以外の任意の文字を最大 32 文字まで設定可能です。

接続名の編集	
接続名	接続名と以下の情報を表示します。 ダイナミック VPN の場合： 接続先の Tunnel アドレス ダイナミック VPN 以外の場合： 接続をしている Tunnel 番号 description コマンドの文字列

設定時には、以下のコンフィグが設定されます。

【設定コマンド】
web-console system vpn
o alias ipv4 [接続先 IPv4 アドレス] [ascii | base64] [接続名]（ダイナミック VPN）
o alias interface TunnelX.0 [ascii | base64] [接続名] （ダイナミック VPN 以外）

2.43.6.3 装置ログの取得

以下の情報をテキストファイルでダウンロードします。

- show tech-support
- show logging

「保守管理」から「装置ログの取得」を選択してください。「テキストファイルでダウンロード」を右クリックし、ファイルの保存を行ってください。

Ver.9.6 以降、テクニカルサポート情報(show tech-support, show logging)に加え、以下の情報の取得が可能です。

装置ログ情報	
テクニカルサポート情報	show tech-support show logging
インタフェース/ デバイス情報	show interfaces detail show devices detail
ルーティング情報	show ip route show ip cache show ipv6 route show ipv6 cache
NAT / NAPT 情報	show ip nat translation show ip napt translation
DHCP 情報	show ip dhcp lease
VRRP 情報	show vrrp
IKE/IPsec 情報	show ike sa show ike statistics show ipsec sa show ipsec statistics show ikev2 sa show ikev2 child-sa show ikev2 statistics show dmvpn detail
BGP 情報	show ip bgp
OSPF 情報	show ip ospf neighbor show ip ospf interface show ip ospf database show ip ospf statistics
QoS 情報	show policy-map interface
不正アクセス監視情報	show ids statistics
ロギング情報	show logging

2.43.6.4 設定データの管理

装置の設定データ（startup-config）の管理を行います。

「保守管理」から「設定データの管理」を選択します。

- 装置データのダウンロード

  装置の設定データ（startup-config）をパソコン等へ取得します。

  「設定データのダウンロード（バックアップ）」の「テキストファイルでダウンロード」を右クリックし、ファイルの保存を行ってください。

- 装置データのアップロード

  パソコン等の設定ファイルを装置の startup-config にコピーします。

  「設定データのアップロード（リストア）」から［参照］ボタンを押して装置にアップロードするファイルを選択し、［アップロード実行］ボタンを押してください。

2.43.6.5 設定の初期化

装置の設定データ（startup-config）を削除します。

「保守管理」から「設定の初期化」を選択し、[初期化実行]ボタンを押してください。初期化終了後、「!!注意!! 保存されていた設定を削除しました」と赤字で表示されます。「再起動」を選択すると、再起動の画面に遷移します。再起動を実行することで、初期状態で起動します。

2.43.6.6 ソフトウェアの更新

装置のソフトウェアの更新を行います。

「保守管理」から「ソフトウェアの更新」を選択します。［参照］を押し、更新に使用するファイルを指定し、［アップデート実行］ボタンを押してください。更新が終了すると「アップデートが完了しました」とメッセージが表示されます。［再起動実行］ボタンを押すと、再起動を行い、更新したソフトウェアが適用されます。

アップデート実行時に「ファイル容量が制限を超えています。」のメッセージが表示された場合、アップロードファイルのサイズ設定コマンドで制限値を変更してください。デフォルト値は 10M バイトに設定されています。

http-server upload-limit	アップロードファイルのサイズ設定

2.43.6.7 Ping の実行

Ping を実行します。

「保守管理」から「ping の実行」を選択します。必要な項目を設定し、[ping 実行]ボタンを押してください。

2.43.6.8 任意コマンドの実行

任意の CLI コマンドを実行します。

「保守管理」から「任意コマンドの実行」を選択します。コマンド入力の画面に実行するコマンドを入力し、[コマンド実行]ボタンを押してください。

複数コマンド同時に実行可能です。コマンド入力は 1,000,000 文字（ver9.2 は 4,000 文字）まで可能です。

※自律的な画面表示を伴うコマンド、コマンド実行後に実行確認など入力が必要となるコマンドは実行できません。（以下のコマンドが全てではありません）

実行できないコマンドの一例

- event-terminal start
- erase startup-config
- license

2.43.6.9 IP 電話サービス保守

IP 電話サービス利用時のリモートメンテナンスで利用します。

詳細は UNIVERGE Aspire シリーズのマニュアルを参照してください。

2.43.6.10 URL オフロード (Ver.9.6 以降)

内部データベースおよび、外部データベースの一覧を表示します。

「保守管理」から「URL オフロード」を選択します。

2.43.6.11 リンクマネージャ (Ver.9.6 以降)

リンクマネージャ機能で追加した端末情報を、グループ単位で表示します。
表示を行う場合、リンクマネージャ機能を有効化する必要があります。
「保守管理」から「リンクマネージャ」を選択します。

2.43.6.12 Wake on LAN

Wake on LAN 端末の一覧表示と状態の確認を行います。
制御する端末は、あらかじめ CLI で設定する必要があります。
「保守管理」から「Wake on LAN」を選択します。

2.43.6.13 再起動

装置の再起動を行います。
「保守管理」から「再起動」を選択します。[再起動実行] ボタンを押してください。再起動完了後は、再度トップページにアクセスしてください。

2.43.7 かんたん設定

インターネット接続や VPN など、構成に応じた必要な設定をまとめて行うことができます。

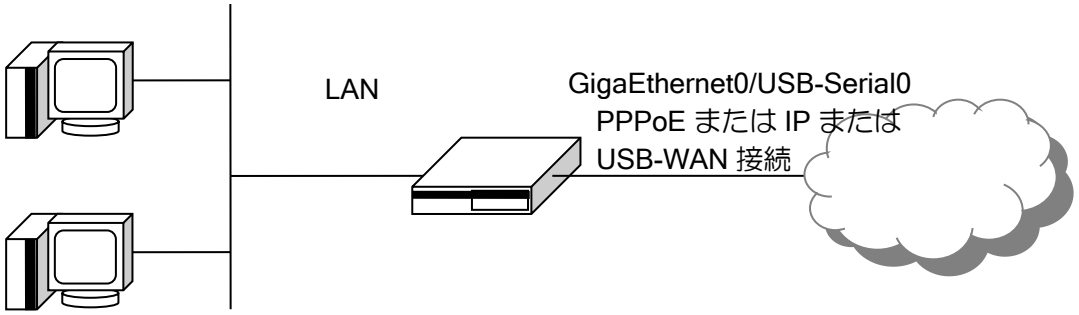
選択可能な構成は以下となります。

- インターネット接続
- インターネット接続＋VPN 接続
- インターネット接続＋フレッツ・VPN ワイド接続
- フレッツ・VPN ワイド接続
- クラウド接続（Ver.9.3 以降）
- IP 電話サービス接続

設定方法の詳細は Web 設定マニュアルを参照してください。
構成を変更する場合は、一度設定を初期化し、再起動後に設定を行ってください。

2.43.7.1 インターネット接続

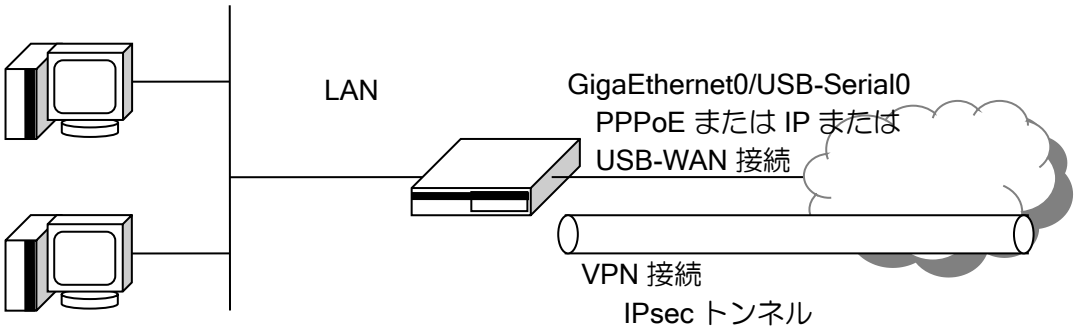
インターネット接続のみの構成です。



設定コンフィグは、詳細設定の「プロバイダの設定」、「通信セキュリティの設定」の項目を参照してください。
通信セキュリティの設定は、Ver9.3 では設定項目がなく自動的にレベル 2（強）の設定を行います。変更が必要な場合は詳細設定の通信セキュリティの設定から変更してください。

2.43.7.2 インターネット接続＋VPN 接続

インターネット接続と、ダイナミック VPN による接続を行う構成です。ダイナミック VPN はセンタと拠点の両方の設定が可能です。

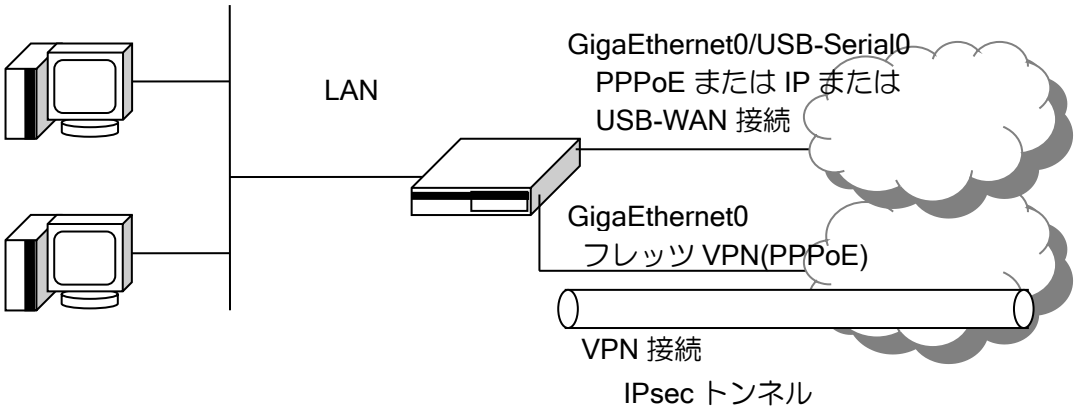


設定コンフィグは、詳細設定の「プロバイダの設定」、「通信セキュリティの設定」、「VPN の設定」（ダイナミック VPN）の項目を参照してください。

通信セキュリティの設定は、Ver9.3 では設定項目がなく自動的にレベル 2（強）の設定を行います。変更が必要な場合は詳細設定の通信セキュリティの設定から変更してください。

2.43.7.3 インターネット接続＋フレッツ・VPN ワイド接続

インターネット接続と、フレッツ・VPN ワイド接続を利用して VPN 接続を行う構成です。

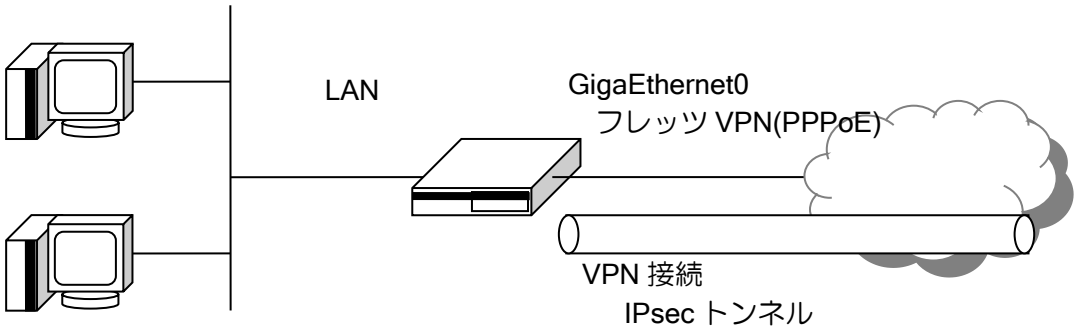


設定コンフィグは、詳細設定の「プロバイダの設定」、「通信セキュリティの設定」、「VPN の設定」（ダイナミック VPN）の項目を参照してください。フレッツ・VPN ワイドの設定は「プロバイダの設定」と同様ですが、GigaEthernet0.2 に設定します。

通信セキュリティの設定は、Ver9.3 では設定項目がなく自動的にレベル 2（強）の設定を行います。変更が必要な場合は詳細設定の通信セキュリティの設定から変更してください。

2.43.7.4 フレッツ・VPN ワイド接続

フレッツ・VPN ワイド接続のみで VPN 接続を行う構成です。



設定コンフィグは、詳細設定の「プロバイダの設定」、「通信セキュリティの設定」、「VPN の設定」（ダイナミック VPN）の項目を参照してください。この設定では、デフォルトルートはトンネルを指定します。

通信セキュリティの設定は、Ver9.3 では設定項目がなく自動的にレベル 2（強）の設定を行います。変更が必要な場合は詳細設定の通信セキュリティの設定から変更してください。

2.43.7.5 クラウド接続

いくつかのクラウドサービスを利用する構成です。

設定コンフィグは、詳細設定のクラウドの設定の項目を参照してください。

2.43.7.6 IP 電話サービス接続

IP 電話サービスを利用する構成です。

詳細は UNIVERGE Aspire シリーズのマニュアルを参照してください。

2.43.8 詳細設定

Web コンソールでは、機能ごとに詳細な設定を行うことができます。

設定方法の詳細は Web 設定マニュアルを参照してください。

2.43.8.1 パスワードの設定

「詳細設定」から「基本設定」／「装置」（Ver.9.4 以前）の「パスワードの設定」を選択します。

「パスワードの設定」では以下の設定を行うことができます。

管理者パスワードの設定(Ver.9.6 以降) ／パスワードの設定(Ver.9.5 以前)	
ユーザ名	初期状態では admin となります。 変更する場合は CLI で変更してください。
ログインパスワード	ログインパスワードを設定します。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

username [ユーザ名] password plain 1 [ログインパスワード] administrator
http-server username [ユーザ名] password [パスワード]        : Ver.9.3 以降のみ
http-server authentication-method digest                    : Ver.9.3 以降のみ
```

Ver.9.6 以降、「利用者メニュー」にログインするために必要なユーザ名と、パスワードの設定を行うことができます(「装置状態の表示」は未ログイン状態でも閲覧可能)。

利用者パスワードの設定(ver.9.6 以降)	
利用者ユーザ	利用者ユーザの有効／無効を設定します。
ユーザ名	初期状態では monitor となります。
パスワード	「利用者メニュー」にログインするためのパスワードを設定します。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】
username [ユーザ名] password plain 1 [ログインパスワード] monitor
http-server monitor-username [ユーザ名] password [パスワード]
http-server authentication-method digest
```

また、「装置状態の表示」にログインするための認証の有効／無効を設定することができます。
ログインするためのユーザ名／パスワードは、管理者パスワードの設定または、利用者パスワードの設定で設定した情報になります。

画面表示認証の設定 (ver.9.6 以降)	
認証の有無	「装置状態の表示」での認証の有無を設定します。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】
http-server guest-username guest secret-password dummy-password
```

2.43.8.2 装置名の設定

「詳細設定」から「基本設定」／「装置」（Ver.9.4 以前）の「装置名の設定」を選択します。
「装置名の設定」では以下の設定を行うことができます。

装置名の設定	
装置名	装置名を設定します。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

hostname [装置名]
```

2.43.8.3 時刻の設定

「詳細設定」から「基本設定」／「装置」（Ver.9.4 以前）の「時刻の設定」を選択します。
「時刻の設定」では時刻の設定を行うことができます。

以下の方法で設定ができます。

装置時刻	
PC の現在時刻を設定する	操作している PC の時刻を装置時刻として設定します。
手動で設定する	設定する時刻を手動で設定します。
NTP サーバと同期する	NTP サーバに同期して時刻設定を行います。 NTP サーバの設定を行ってください。

NTP サーバ設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

ntp ip enable
ntp server [NTP サーバアドレス]
ntp source [LAN 側インタフェース]
```

NTP サーバと同期する設定から方式を変更した場合、NTP の設定は削除されます。

2.43.8.4 保守の設定 (Ver.9.6 以降)

「詳細設定」から「基本設定」の「保守の設定」を選択します。
「保守の設定」では以下の設定を行うことができます。

- SSH/Telnet の設定
- SNMP の設定
- ロギングの設定

- SSH/Telnet の設定

SSH/Telnet の設定	
SSH 設定	SSH サーバの有効／無効を設定します。
Telnet 設定	telnet サーバの有効／無効を設定します。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
! SSH 設定時
ssh-server ip enable
pki private-key generate rsa

! telnet 設定時
telnet-server ip enable
```

- SNMP の設定

SNMP の設定（Ver.10.3 以前）	
SNMP 設定	SNMP 機能の有効／無効を設定します。
コミュニティ設定	コミュニティの設定します。
トラップ設定	トラップ送信先の IP アドレスを設定します。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
snmp-agent ip enable
snmp-agent ip community [コミュニティ名]

! トラップ設定時
snmp-agent ip host [トラップ送信先 IP アドレス] [コミュニティ名] version 1
```

Ver10.4 以降、SNMPv3 対応に伴い以下の設定を行うことができます。

SNMP の設定（ver10.4 以降）	
SNMP 設定	SNMP 機能の有効／無効を設定します。
バージョン	利用する SNMP のバージョンを設定します。 [v1/v2c]：SNMPv1 or SNMPv2c を利用 [v3]：SNMPv3 を利用
コミュニティ設定	コミュニティの設定します。
トラップ設定	トラップ送信先の IP アドレスを設定します。
ユーザ名の設定	SNMPv3 で使用する認証用ユーザ名を設定します。
認証アルゴリズム	認証時に使用するハッシュ関数を設定します。 認証アルゴリズム： MD5,SHA-1,SHA-192,SHA-256,SHA-384,SHA-512
認証パスワード	認証に使用するパスワードを設定します。
暗号化アルゴリズム	通信の暗号化に使用するアルゴリズムを設定します。 暗号化アルゴリズム： DES,AES-128
暗号化パスワード	暗号化に使用するパスワードを設定します。
トラップ設定	トラップ送信先の IP アドレスを設定します。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド（バージョンで[v1/v2c]を選択した場合）】
snmp-agent ip enable
snmp-agent ip community [コミュニティ名]

! トラップ設定時
snmp-agent ip host [トラップ送信先 IP アドレス] [コミュニティ名]

【設定コマンド（バージョンで[v3]を選択した場合）】
snmp-agent ip enable
snmpv3 group [セキュリティグループ(※)] priv
snmpv3 user [ユーザ名] [セキュリティグループ(※)] auth [認証アルゴリズム] [認証パスワード] priv [暗号化アルゴリズム] [暗号化パスワード]

! トラップ設定時
snmpv3 ip host [トラップ送信先 IP アドレス] user [ユーザ名]

※設定反映時に snmpv3 group の設定がない場合、
  セキュリティグループは” webgui-group”となります。
  snmpv3 group が設定ある場合、セキュリティグループは変更されません。
```

- ロギングの設定

ロギングの設定	
装置ロギング設定	ロギング設定の有効化をします。
Syslog 設定	syslog 機能の有効／無効を設定します。
Syslog サーバ	syslog サーバの IP アドレスを設定します。

【設定コマンド】
! 装置ロギング設定有効時
logging buffered
既に logging buffered が有効の場合は、上書きしません。

! syslog 設定有効時
syslog ip host [syslog サーバ IP アドレス]

ロギングレベルの設定	
ロギングレベル設定	ロギングレベルの設定をします。 変更しない：設定を現在のまま変更しません。 推奨設定：全機能のレベルを warn で設定します。 詳細設定：機能単位(サブシステム)でレベルを設定します。
全体設定	個別に設定できない機能のレベルを設定します。
イーサネット IPv4 IPv6 PPP/PPPoE L2TP USB/モデム フィルタリング NAT RIP BGP OSPF IKE IKEv2 不正アクセス検知 URL フィルタリング URL オフロード	機能単位でレベルの設定をします。 • error (1：エラーレベル) • warn (2：警告レベル) • notice (3：注意レベル) • info (4：情報レベル) • debug (5：デバッグレベル) 左記以外の機能は、全体設定のレベルになります。 各サブシステムの詳細は、ロギング機能を参照してください。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
! 変更しない
設定の変更はありません。

! 推奨設定
logging subsystem all warn

! 詳細設定
logging subsystem all [ロギングレベル]
logging subsystem [サブシステム名] [ロギングレベル]
```

2.43.8.5 NetMeister の設定

Ver9.7 で利用可能です。NetMeister の章を参照してください。

2.43.8.6 LAN アドレスの設定

「詳細設定」から「LAN」の「LAN アドレスの設定」を選択します。
「LAN アドレスの設定」では、以下の設定を行うことができます。

LAN アドレスの設定	
IP アドレス	LAN 側の IP アドレスとマスク長を設定します。

設定時は以下のコンフィグが設定されます。
LAN 側インタフェースは最老番のインタフェースを使用します。

```
【設定コマンド】
ip access-list web-http-acl permit ip src any dest [LAN 側 IP アドレス]/32
http-server ip access-list web-http-acl

! DHCP プロファイル名は  web-dhcp-[LAN 側インタフェース名]となります。
ip dhcp profile web-dhcp-gigaethernet1.0
   dns-server [LAN 側 IP アドレス]            :DHCP サーバ有効時

interface Gigaethernet1.0
   description LAN1
   ip address [IP アドレス]/[マスク長]
   ip dhcp binding web-dhcp-gigaethernet1.0
   no shutdown
```

2.43.8.7 DHCP サーバの設定

「詳細設定」から「LAN」の「DHCP サーバの設定」を選択します。
「DHCP サーバの設定」では、以下の設定を行うことができます。

DHCP サーバの設定	
IP アドレス	「LAN 側アドレスの設定」から変更してください。
DHCP サーバ	DHCP サーバの有効／無効を設定します。
割当範囲	割当範囲を設定する場合は固定設定を選択してください。

設定時は、以下のコンフィグが設定されます。

【設定コマンド】

```
ip dhcp enable

! DHCP プロファイル名は web-dhcp-[LAN 側インタフェース名]となります。
ip dhcp profile web-dhcp-gigaethernet1.0
   assignable-range [割り当て範囲]
   dns-server [LAN 側 IP アドレス]

interface GigaEthernet1.0
   ip dhcp binding web-dhcp-gigaethernet1.0
```

2.43.8.8 プロバイダの設定

「詳細設定」から「WAN」の「プロバイダの設定」を選択します。
かんたん設定のインターネット接続と同様です。

最初に WAN インタフェースの接続形態を選択します。

接続形態	
PPPoE 接続	フレッツ光回線等、PPPoE を使用します。
IP 接続	ケーブルテレビ回線など、DHCP によるアドレス付与や、直接 IP アドレス設定する場合に使用します。
USB 接続	WAN 回線に USB 無線通信端末を使用し、LTE,3G 回線を使用します。

PPPoE 接続の場合は以下を設定します。

PPPoE 接続の設定	
ユーザ名	PPPoE 接続のためのユーザ ID を設定します。
パスワード	PPPoE 接続のためのパスワードを設定します。
IP アドレス	IPCP で設定する場合は自動設定を選択してください 固定の場合は IP アドレスを入力してください。
DNS アドレス	IPCP で設定する場合は自動設定を選択してください。 固定の場合は IP アドレスを入力してください。DNS アドレスは 2 個まで設定可能です。
NAPT	NAPT の設定を行います。 PPPoE では有効しか選択できません。

設定時は以下のコンフィグが設定されます。
WAN 側インタフェースは GigaEthernet0.1 を使用します。

```
【設定コマンド】

ip route default GigaEthernet0.1

proxy-dns ip enable
proxy-dns interface GigaEthernet0.1 priority 254    : DNS アドレス自動設定時
proxy-dns server [DNS アドレス 1] priority 254      : DNS アドレス固定設定時
proxy-dns server [DNS アドレス 2] priority 254      : DNS アドレス固定設定時
ip name-server [DNS アドレス 1]         :Ver9.7 以降のみ、DNS アドレス固定設定時
ip name-server [DNS アドレス 2]         :Ver9.7 以降のみ、DNS アドレス固定設定時

!PPP プロファイル名は web-ppp-[WAN 側インタフェース名]となります。
ppp profile web-ppp-gigaethernet0.1
   authentication myname [ユーザ名]
   authentication password [ユーザ名] [パスワード]

interface GigaEthernet0.1
   description WAN1
   encapsulation pppoe
   auto-connect
   ppp binding web-ppp-gigaethernet0.1
   ip address ipcp                          : IP アドレス自動取得時
   ip address [WAN 側 IP アドレス]          : IP アドレス固定設定時
   ip tcp adjust-mss auto
   ip napt enable
   ip napt hairpinning                                : Ver.9.3 以降のみ
   ip napt translation max-entries 65535
   no shutdown
```

IP 接続の場合は、以下を設定します。

IP 接続の設定	
WAN 側 IP アドレス	IP アドレスを設定します。 DHCP クライアントを使用しない場合に設定します。
DNS アドレス	DNS サーバを設定します。2 個まで設定可能です。 DHCP クライアントを使用しない場合に設定します。
デフォルトゲートウェイ	ゲートウェイのアドレスを設定します。 WAN 側 IP アドレスを固定設定する場合に設定します。
NAPT	NAPT の設定を行います。 プロバイダ接続では、通常有効化して利用してください。 NAPT ルータが別に存在する場合のみ、無効化して利用可能です。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】

ip route default [デフォルトゲートウェイ]   :IP アドレス指定時

proxy-dns ip enable
proxy-dns interface GigaEthernet0.0 priority 254 :DHCP クライアント使用時
proxy-dns server [DNS アドレス 1] priority 254   :DNS アドレス指定時
```

```
proxy-dns server [DNS アドレス 2] priority 254   :DNS アドレス指定時
ip name-server [DNS アドレス 1]       :Ver9.7 以降のみ、DNS アドレス固定設定時
ip name-server [DNS アドレス 2]       :Ver9.7 以降のみ、DNS アドレス固定設定時

interface GigaEthernet0.0
  description WAN1
  ip address dhcp receive-default          :DHCP クライアント使用時
  ip address [WAN 側 IP アドレス]        : IP アドレス指定時
  ip napt enable                              : NAPT 有効時
  ip napt hairpinning                         : NAPT 有効時、Ver.9.3 以降のみ
  ip napt translation max-entries 65535       : NAPT 有効時
  no shutdown
```

USB 接続の場合は、以下を設定します。

USB 接続の設定	
ユーザ名	ユーザ名を指定します。
パスワード	パスワードを設定します。
PDP タイプ	PDP タイプを設定します。
APN	APN を設定します。
WAN 側 IP アドレス	IP アドレスを設定します。 PPP でアドレスを自動で取得する場合は自動取得を選択します。
DNS アドレス	DNS サーバを設定します。2 個まで設定可能です。 PPP で取得する場合は自動取得を選択します。
NAPT	NAPT の設定を行います。 USB 接続では有効しか選択できません。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】

ip route default USB-Serial0.0

proxy-dns ip enable
proxy-dns interface USB-Serial0.0 priority 254   :DNS 自動取得時
proxy-dns server [DNS アドレス 1] priority 254   :DNS 固定設定時
proxy-dns server [DNS アドレス 2] priority 254   :DNS 固定設定時
ip name-server [DNS アドレス 1]       :Ver9.7 以降のみ、DNS アドレス固定設定時
ip name-server [DNS アドレス 2]       :Ver9.7 以降のみ、DNS アドレス固定設定時

!PPP プロファイル名は web-ppp-[WAN 側インタフェース名]となります。
ppp profile web-ppp-usb-serial0.0
  authentication myname [ユーザ名]
  authentication password [ユーザ名] [パスワード]
  lcp acfc

interface USB-Serial0.0
  description WAN1
  encapsulation ppp
  auto-connect
  ppp binding web-ppp-usb-serial0.0
  ip address ipcp                          : IP アドレス自動取得時
  ip address [WAN 側 IP アドレス]        : IP アドレス固定設定時
  ip tcp adjust-mss auto
```

```
ip napt enable
ip napt hairpinning                                    : Ver.9.3 以降のみ
ip napt translation max-entries 65535
mobile cid 1 pdp [PDP タイプ] apn [APN]
mobile number *99***1#
no shutdown
```

2.43.8.9 静的 NAPT の設定

「詳細設定」から「WAN」の「静的 NAPT の設定」を選択します。

「静的 NAPT の設定」は、機能リストから選択する方法とポート番号を指定する方法が選択できます。設定時はプロバイダの設定で NAPT を有効化している必要があります。

- 機能リスト選択

静的 NAPT の設定（機能リスト選択）	
機能リスト	公開するプロトコル・ポート番号を選択します。
プライベート側アドレス	プライベート側端末の IP アドレスを設定します。

- ポート番号指定

静的 NAPT の設定（ポート番号指定選択）	
NAPT 名	任意の名称を設定します。
プロトコル	TCP/UDP を設定します。
ポート番号	ポート番号を設定します。 範囲で指定することもできます。
プライベート側アドレス	プライベート側端末の IP アドレスを設定します。
プライベート側ポート番号	プライベート側端末のポート番号を設定します。

[詳細設定]から[静的 NAPT の設定]を選択すると、設定した静的 NAPT の一覧が表示されます。削除する場合は、[削除]を選択してください。変更はできません。一旦削除後、新規に追加設定してください。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

interface [WAN 側インタフェース]

  !機能リストでプライベート側アドレスを指定しなかった場合
  ip napt static [WAN 側インタフェース] [プロトコル] [ポート番号]

  !機能リストでプライベート側アドレスを指定した場合
  ip napt static [プライベート側アドレス] [プロトコル] :ESP,GRE を選択した場合
  ip napt service [NAPT 名] [プライベート側アドレス] none
                          [プロトコル] [ポート番号]          :ESP,GRE 以外を選択した場合

  !ポート番号指定の場合
  ip napt service [NAPT 名] [プライベート側アドレス] [プライベート側ポート番号]
                       [プロトコル] [ポート番号]
```

2.43.8.10 WAN フィルタの設定

「詳細設定」から「WAN」の「WAN フィルタの設定」を選択します。
「WAN フィルタの設定」では以下の設定を行うことができます。
設定時はプロバイダの設定が必要です。

WAN フィルタの設定	
シーケンス番号	シーケンス番号を設定します。
動作	透過（permit）・廃棄（deny）を選択します。
プロトコル	プロトコルを設定します。
IP アドレス	送信元、送信先のアドレスを設定します。
ポート番号	送信元、送信先のポート番号を設定します。 プロトコルが TCP または UDP の場合に設定します。
ログの記録	ログ出力の抑止の有無を設定します。

[詳細設定]から[WAN フィルタの設定]を選択すると、設定したフィルタの一覧が表示されます。変更する場合は[変更]を、削除する場合は[削除]を選択してください。

シーケンス番号は使用済みの番号は使用できません。設定済みのシーケンス番号を変更するか、または、一旦削除後、新規に登録してください。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

!アクセスリスト名は web-f-w[WAN 番号]_[方向][シーケンス番号]となります。
!（WAN 番号は 1 または 2、方向は i または o です）
ip access-list [アクセスリスト名] [動作] [プロトコル]
                    src [送信元 IP アドレス] sport [送信元ポート番号]
                    dest [送信先 IP アドレス] dport [送信先ポート番号]

interface [WAN 側インタフェース]
  ip filter [アクセスリスト名] [シーケンス番号] [方向] [suppress-logging:ログ抑止時]
```

CLI で設定したフィルタは上の条件を満たさないと解析されません。

2.43.8.11 URL フィルタの設定 (Ver.9.5 以降)

「詳細設定」から「WAN」の「URL フィルタの設定」を選択します。
設定の詳細は、「URL フィルタリング」機能を参照してください。

2.43.8.12 QoS の設定（Ver.9.6 以降）

「詳細設定」から「WAN」の「QoS の設定」を選択します。
「QoS の設定」では以下の設定を行うことができます。

QoS の設定	
QoS の設定	QoS 機能の有効／無効を設定します。

インタフェースシェーピングの設定	
シェーピング設定	シェーピング機能の有効／無効を設定します。
帯域	シェーピングする帯域の設定をします。 Mbps : 1 - 10000 Kbps：8 - 10000000 bps ：8000 - 1000000000

また、「PQ の設定」では、以下の項目について設定ができます。

PQ の設定の追加	
優先度	通信の優先度を設定します。 高優先：High / 中優先：Medium / 標準：Normal （指定しなかった通信は Low になります）
プロトコル	プロトコルの設定をします。 全プロトコルや任意のプロトコルを設定できます。
送信元	送信元の IP アドレスを設定します。 すべて：すべての IPv4 アドレス 指定：ネットワークアドレス単位で設定できます。
送信先	送信先の IP アドレスを設定します。 すべて：すべての IPv4 アドレス 指定：ネットワークアドレス単位で設定できます。
ToS	ToS の設定をします。 なし：設定なし Precedence：Precedence の設定をします。 DSCP：DSCP の設定をします。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】
!QoS の設定
interface GigaEthernet0.0
   service-policy enable
!
!PQ の設定
ip access-list qos-[優先度] permit [プロトコル] src [送信元] dest [送信先] [ToS]

class-map match-any pq-class
   match ip access-list qos-high high
   match ip access-list qos-medium medium
   match ip access-list qos-normal normal
   match any low
!
policy-map pq-policy
   class pq-class
   class class-local
   class class-default
!
interface GigaEthernet0.0
   service-policy enable
   service-policy output pq-policy


!インタフェースシェーピングの設定
interface GigaEthernet0.0
   traffic-shape rate [kbps | mbps] [帯域]
   qos rate-accounting ethernet-overhead
```

※ シェーピングの計算はプリアンブルやフレーム間ギャップも含めた値で行います。

2.43.8.13 通信セキュリティの設定（Ver.9.3 以降）

セキュリティ強度を指定したフィルタ設定や不正アクセス検知（IDS）の設定を行います。
「詳細設定」から「WAN」の「通信セキュリティの設定」を選択します。
「通信セキュリティの設定」では以下の設定を行うことができます。

セキュリティ強度	
レベル 1（オフ）	NAPT により外部からのパケットを廃棄します。
レベル 2（標準）	NAPT による外部からのパケット廃棄に加えて、送信フィルタにより、内部からの通信を制限します。
レベル 3（強）	VPN 通信以外のパケットは全て廃棄します。 インターネット上の Web アクセスも禁止します。

不正アクセス検知（IDS）	
無効	不正アクセスの検知を行いません。
有効	不正アクセスを検知した場合は不正パケットを廃棄します。

設定時は、以下のコンフィグが設定されます。

【設定コマンド】
1．セキュリティ強度 レベル 2（標準）
WAN インタフェースではデフォルトで NAPT が有効になっているため、設定コマンドから省略します。

[Ver.9.4 以降]
```
ip access-list web-f-w1-s1 deny ip src any dest 0.0.0.0/8
ip access-list web-f-w1-s1 deny ip src any dest 127.0.0.0/8
ip access-list web-f-w1-s1 deny ip src any dest 169.254.0.0/16
ip access-list web-f-w1-s1 deny ip src any dest 224.0.0.0/4
ip access-list web-f-w1-s1 deny tcp src any sport eq 135 dest any dport any
ip access-list web-f-w1-s1 deny tcp src any sport any dest any dport eq 135
ip access-list web-f-w1-s1 deny tcp src any sport range 137 139 dest any dport any
ip access-list web-f-w1-s1 deny tcp src any sport any dest any dport range 137 139
ip access-list web-f-w1-s1 deny tcp src any sport eq 445 dest any dport any
ip access-list web-f-w1-s1 deny tcp src any sport any dest any dport eq 445
ip access-list web-f-w1-s1 permit ip src any dest any

interface [WAN インタフェース]
  ip filter web-f-w1-s1 101 out suppress-logging
```

[Ver.9.3] では以下のアクセスリストも設定されます。
※プライベートアドレス利用時は無効化してください。
```
ip access-list web-f-w1-s1 deny ip src any dest 10.0.0.0/8
ip access-list web-f-w1-s1 deny ip src any dest 172.16.0.0/12
ip access-list web-f-w1-s1 deny ip src any dest 192.168.0.0/16
ip access-list web-f-w1-s1 deny ip src any dest 240.0.0.0/4
```

2．セキュリティ強度 レベル 3（強）
WAN インタフェースではデフォルトで NAPT が有効になっているため、設定コマンドから省略します。

```
ip access-list web-f-w1-s3 permit 47 src any dest any
ip access-list web-f-w1-s3 permit 50 src any dest any
ip access-list web-f-w1-s3 permit udp src any sport eq 500 dest any dport any
ip access-list web-f-w1-s3 permit udp src any sport any dest any dport eq 500
ip access-list web-f-w1-s3 permit udp src any sport eq 4500 dest any dport any
ip access-list web-f-w1-s3 permit udp src any sport any dest any dport eq 4500
ip access-list web-f-w1-s3 deny ip src any dest any

interface [WAN インタフェース]
```

```
   ip filter web-f-w1-s3 103 in suppress-logging
   ip filter web-f-w1-s3 103 out suppress-logging

３．不正アクセス検知 有効

ids ip type all action discard
ids logging-interval 10
```

2.43.8.14 VPN の設定

「詳細設定」から「VPN・クラウド」／「VPN」（Ver.9.2）の「VPN の設定」を選択します。
「VPN の設定」では、最初に接続種別を設定します。
設定時はプロバイダの設定が必要です。

接続種別	
ダイナミック VPN	ダイナミック VPN を使用します。 複数のダイナミック VPN は設定しないでください。
IPsec	IPsec を使用した VPN 接続になります。
IP トンネル	GRE トンネルを使用した VPN 接続になります。 暗号化は行いません。
L2TP/IPsec	L2TP/IPsec を使用した VPN 接続になります。

- ダイナミック VPN
  ダイナミック VPN の設定では、以下の設定を行います。

ダイナミック VPN の設定	
タイプ	拠点側・センタ側を設定します。
拠点番号	拠点を選択した場合に拠点番号を設定します。
パスワード	IPsec の事前共有鍵を設定します。 全ての拠点で同じ値を設定してください。
センタ WAN 側 IP アドレス	接続するセンタの WAN 側 IP アドレスを設定します。

設定時は以下のコンフィグが設定されます。

拠点の場合

```
【設定コマンド】

nhrp local [LAN 側インタフェース]

ikev2 authentication psk id ipv4 169.254.0.[拠点番号] key char [パスワード]

route-map web-dmvpn-map permit 10
   match interface [LAN 側インタフェース]

router bgp 65535
   timers 5 15
   neighbor 169.254.255.254 remote-as 65535
   neighbor 169.254.255.254 connect-interval 10
   address-family ipv4 unicast
      redistribute connected route-map web-dmvpn-map

interface [WAN 側インタフェース]
   ip napt static [WAN 側インタフェース] 50
   ip napt static [WAN 側インタフェース] udp 500
   ip napt static [WAN 側インタフェース] udp 4500
```

```
interface Tunnel0.0
  description DynamicVPN_#1
  tunnel mode mgre ipsec-ikev2
  ip address 169.254.0.[拠点番号]/16
  ip tcp adjust-mss auto
  nhrp nhs 169.254.255.254/16 nbma [センタ WAN 側 IP アドレス]
  ikev2 child-pfs 2048-bit
  ikev2 child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
  ikev2 child-proposal integrity sha2-512 sha2-384 sha2-256
  ikev2 dpd interval 10
  ikev2 local-authentication psk id ipv4 169.254.0.[拠点番号]
  ikev2 nat-traversal keepalive 20
  ikev2 outgoing-interface [WAN 側インタフェース] auto
  ikev2 sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
  ikev2 sa-proposal integrity sha2-512 sha2-384 sha2-256
  ikev2 sa-proposal dh 2048-bit
  ikev2 sa-proposal prf sha2-512 sha2-384 sha2-256
  ikev2 ipsec-mode transport
  ikev2 peer any authentication psk
  no shutdown
```

センタの場合

【設定コマンド】

```
ikev2 authentication psk id ipv4 169.254.255.254 key char [パスワード]

route-map web-dmvpn-map permit 10
  match interface [LAN 側インタフェース]

route-map web-dmvpn-map-tunnel0.0 permit 10
  set ip next-hop 169.254.255.254

router bgp 65535
  timers 5 15
  address-family ipv4 unicast
    redistribute connected route-map web-dmvpn-map
  peer-group web-dmvpn-group-tunnel0.0 remote-as 65535
    listen range 169.254.0.0/16
    connect-interval 10
    route-reflector-client
    address-family ipv4 route-map web-dmvpn-map-tunnel0.0 out

interface [WAN 側インタフェース]
  ip napt static [WAN 側インタフェース] 50
  ip napt static [WAN 側インタフェース] udp 500
  ip napt static [WAN 側インタフェース] udp 4500

interface Tunnel0.0
  description DynamicVPN
  tunnel mode mgre ipsec-ikev2
  ip address 169.254.255.254/16
  ip tcp adjust-mss auto
  ikev2 child-pfs 2048-bit
  ikev2 child-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
  ikev2 child-proposal integrity sha2-512 sha2-384 sha2-256
  ikev2 dpd interval 10
  ikev2 local-authentication psk id ipv4 169.254.255.254
  ikev2 nat-traversal keepalive 20
```

```
ikev2 outgoing-interface [WAN 側インタフェース] auto
ikev2 sa-proposal enc aes-cbc-256 aes-cbc-192 aes-cbc-128
ikev2 sa-proposal integrity sha2-512 sha2-384 sha2-256
ikev2 sa-proposal dh 2048-bit
ikev2 sa-proposal prf sha2-512 sha2-384 sha2-256
ikev2 ipsec-mode transport
ikev2 peer any authentication psk
no shutdown
```

- IPsec

  IPsec を選択した場合、接続先アドレス、接続アドレスの契約（固定、動的）を選択します。
  IPsec では以下の設定を行うことができます。

IPsec の詳細設定		
接続名		Web コンソールの画面表示に使用します。
接続先	WAN 側 IP アドレス	IPsec の接続先のアドレスを設定します。 接続先が動的アドレスの場合、アドレスは設定不要です。 Ver9.7 以降 FQDN で指定可能です。
	LAN 側 ネットワーク	接続先装置の LAN 側ネットワークを設定します。
ルーティング		スタティックルートの宛先を設定します。
IKE	事前共有鍵	事前共有鍵を設定します。
	アルゴリズム	暗号化アルゴリズム：AES（128bit,192bit,256bit）, 3DES,DES 認証アルゴリズム　：SHA2-256,SHA2-384,SHA2-512, SHA,MD5
	DH グループ	DH group 1(768bit),2(1024bit),5(1536bit),14(2048bit)
	ID	アグレッシブモード時の ID を設定します。 Initiator の場合は自分の ID（Local-ID） Responder の場合は相手の ID（Remote-ID）
IPsec	アルゴリズム	暗号化アルゴリズム：AES（128bit,192bit,256bit）, 3DES,DES 認証アルゴリズム　：SHA2-256,SHA2-384,SHA2-512, SHA,MD5

いくつかの動作、設定値は、接続先と接続元の WAN 側アドレスの固定 IP アドレス，動的 IP アドレスの組み合わせによって決定します。

IPsec ローカル ID/リモート ID に関しては、接続先装置にて、対応する値を設定する必要があります。

接続元契約	固定IPアドレス	動的IPアドレス	固定IPアドレス	動的IPアドレス
接続先契約	固定IPアドレス	固定IPアドレス	動的IPアドレス	動的IPアドレス
モード	メイン	アグレッシブ	アグレッシブ	設定できません
動作	ー	Initiator	Responder	設定できません
IPsec ローカル ID	0.0.0.0/0	接続元 LAN 側	0.0.0.0/0	設定できません

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
!Tunnel は 0 から順に空いている番号を使用します。
!以下は最初の接続(Tunnel0.0)の場合になります。

!ポリシー名等の番号は Tunnel 番号+1 を使用します。
ip route [接続先 LAN 側ネットワーク] Tunnel0.0
ip route [ルーティング] Tunnel0.0

ip access-list web_vpnlist permit ip src any dest any
ike nat-traversal
ike proposal web_vpn1ikeprop encryption [IKE 暗号アルゴリズム]
                                  hash [IKE 認証アルゴリズム]
                                  group [IKE DH グループ]
ipsec autokey-proposal web_vpn1secprop [IPsec 暗号アルゴリズム]
                                                [IPsec 認証アルゴリズム]

!接続元固定―接続先固定
ike policy web_vpn1ikepolicy peer [接続先 WAN 側アドレス] key [事前共有鍵]
                                    mode main web_vpn1ikeprop
ipsec autokey-map web_vpn1secpolicy web_vpnlist
                                peer [接続先 WAN 側アドレス] web_vpn1secprop

!接続元動的―接続先固定
ike policy web_vpn1ikepolicy peer [接続先 WAN 側アドレス] key [事前共有鍵]
                                    mode aggressive web_vpn1ikeprop
ike keepalive web_vpn1ikepolicy 30 6
ike local-id web_vpn1ikepolicy fqdn [IKE ID]
ike suppress-dangling web_vpn1ikepolicy
ipsec autokey-map web_vpn1secpolicy web_vpnlist
                                peer [接続先 WAN 側アドレス] web_vpn1secprop
ipsec local-id web_vpn1secpolicy [接続元 LAN 側ネットワーク]

!接続元固定―接続先動的
ike policy web_vpn1ikepolicy peer any key [事前共有鍵]
                                    mode aggressive web_vpn1ikeprop
ike remote-id web_vpn1ikepolicy fqdn [IKE ID]
ipsec dynamic-map web_vpn1secpolicy web_vpnlist
                                web_vpn1secprop ike-binding web_vpn1ikepolicy
ipsec remote-id web_vpn1secpolicy [接続先 LAN 側ネットワーク]

interface [WAN 側インタフェース]
  ip napt static [WAN 側インタフェース] 50
  ip napt static [WAN 側インタフェース] udp 500
  ip napt static [WAN 側インタフェース] udp 4500

interface Tunnel0.0
  description [接続名]
  tunnel mode ipsec
  ip unnumbered [LAN 側インタフェース]
  ip tcp adjust-mss auto
  ipsec policy tunnel web_vpn1secpolicy out
  no shutdown
```

- IP トンネル
  IP トンネルでは、GRE トンネルの設定を行うことができます。

IP トンネルの詳細設定		
接続名		Web コンソールの画面表示に使用します。
接続先	WAN 側アドレス	トンネル接続先のアドレスを設定します。
	LAN 側ネットワーク	接続先装置の LAN 側ネットワークを設定します。
ルーティング		スタティックルートの宛先を設定します。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
!Tunnel は 0 から順に空いている番号を使用します。
!以下は最初の接続(Tunnel0.0)の場合になります。

ip route [接続先 LAN 側ネットワーク] Tunnel0.0
ip route [ルーティング] Tunnel0.0

interface Tunnel0.0
  description [接続名]
  tunnel mode gre ip
  tunnel destination [接続先 WAN 側アドレス]
  tunnel source [接続元 WAN 側インタフェース]
  tunnel keepalive
  ip unnumbered [LAN 側インタフェース]
  ip tcp adjust-mss auto
  no shutdown
```

2.43.8.15 L2TP の設定

「詳細設定」から「VPN・クラウド」の「L2TP の設定」を選択します（Ver9.3 以降）。
「VPN の設定」を選択しても接続種別から「L2TP/IPsec」を選択できます。

「L2TP/IPsec の設定」では、以下の設定を行うことができます。なお、L2TP/IPsec 設定時は再起動が必須です。設定後、設定の保存を行い、再起動してください。
Web コンソールで設定できるのは L2TP LNS の設定です。L2TP LAC の設定はできません。

L2TP/IPsec の詳細設定	
同時接続数	同時に接続する端末数を設定します。 設定数分、トンネルインタフェースを使用します。 設定数を変更する場合は再起動が必要となります。
アドレス割当範囲	端末に払い出すアドレスの範囲を設定します。

暗号/認証の詳細設定	
IKE 事前共有鍵	IKE の事前共有鍵を設定します。 全ての接続に同じ事前共有鍵を使用します。

接続ユーザの認証設定	
ユーザ名	ユーザ名を設定します。 ユーザ名は同時接続数以上の設定をすることができます。
パスワード	パスワードを設定します。
固定割当アドレス	ユーザに固定のアドレスを割り当てる場合に設定します。 省略時は、アドレス割当範囲から自動で割り当てます。

L2TP/IPsec の設定は、1 つのみとなります。接続する端末を追加する場合は、ユーザ認証を追加してください。同時接続数が増える場合は同時接続数を変更してください。また、「VPN の設定」から L2TP の設定の追加・変更を行う場合は、接続名の[変更]を選択してください。

設定時は以下のコンフィグが設定されます。

【設定コマンド】

```
! トンネルインタフェースは最老番-1 から使用します。
! 同時接続数分のトンネルインタフェースを使用します。
! ユーザ認証設定は、全て同一のプロファイルに設定されます。

ip access-list web_vpnlist permit ip src any dest any

ike nat-traversal
!
ike proposal web_l2tp_ikeprop1 encryption aes-256 hash sha group 1024-bit
ike proposal web_l2tp_ikeprop2 encryption aes hash sha group 1024-bit
ike proposal web_l2tp_ikeprop3 encryption 3des hash sha group 1024-bit
!
ike policy web_l2tp_ikepolicy peer any key [事前共有鍵]
  web_l2tp_ikeprop1,web_l2tp_ikeprop2,web_l2tp_ikeprop3

ipsec autokey-proposal web_l2tp_secprop1 esp-aes-256 esp-sha
ipsec autokey-proposal web_l2tp_secprop2 esp-aes esp-sha
ipsec autokey-proposal web_l2tp_secprop3 esp-3des esp-sha
!
ipsec dynamic-map web_l2tp_secpolicy web_vpnlist
  web_l2tp_secprop1,web_l2tp_secprop2,web_l2tp_secprop3

ppp profile web-ppp-l2tp
  authentication request chap
  authentication password [ユーザ名] [パスワード]
  lcp pfc
  lcp acfc
  ipcp ip-compression
  ipcp provide-ip-address range [アドレス割当 1] [アドレス割当 2]
  ipcp provide-static-ip-address [ユーザ名] [固定割当アドレス]

interface [LAN 側インタフェース]
  ip proxy-arp （Ver9.4 以降）

interface Tunnel126.0
  description L2TP_#1
  ppp binding web-ppp-l2tp
  tunnel mode l2tp ipsec
  ip unnumbered [LAN 側インタフェース]
  ip tcp adjust-mss auto
  ipsec policy transport web_l2tp_secpolicy
  no shutdown
```

2.43.8.16 クラウドの設定

「詳細設定」から「VPN・クラウド」の「クラウドの設定」を選択します（Ver9.3 以降）。
「クラウド接続の設定」では、クラウドに接続するための設定を行います。
最初にクラウドのサービス種別を選択します。

サービス種別	
Amazon Web Services に接続	Amazon Web Services に接続する場合に選択します。
Microsoft Azure に接続	Microsoft Azure に接続する場合に選択します。
NEC Cloud IaaS に接続	NEC Cloud IaaS に接続する場合に選択します。

Amazon Web Services に接続する場合は、接続形態を選択します。
その他の場合は”インターネット VPN で接続”で固定になります。

接続形態	
インターネット VPN で接続	Amazon Web Services Virtual Private Cloud（VPC）の場合に選択します。
専用線で接続	Amazon Web Services ダイレクトコネクトの場合に選択します。

接続先、暗号／認証の設定を行います。

インターネット VPN で接続	
接続先（クラウド） WAN 側 IP アドレス	接続先の IP アドレスを設定します。
接続先（クラウド） LAN 側ネットワーク	接続先の LAN 側ネットワークアドレスを設定します。 （Microsoft Azure,NEC Cloud IaaS の場合）
接続先（クラウド） VPN アドレス	接続先の VPN アドレスを設定します。 （Amazon Web Services の場合）
接続先（クラウド） AS 番号	接続先の AS 番号を設定します。 （Amazon Web Services の場合）
接続元（IX） VPN アドレス	接続元の VPN アドレスを設定します。 （Amazon Web Services の場合）
接続元（IX） AS 番号	接続元の AS 番号を設定します。 （Amazon Web Services の場合）

専用線で接続	
接続先（クラウド） WAN 側 IP アドレス	接続先の WAN 側 IP アドレスを設定します。
接続先（クラウド） AS 番号	接続先の AS 番号を設定します。
接続先（クラウド） BGP パスワード	接続先の BGP パスワードを設定します。
接続元（IX） WAN 側 IP アドレス	接続元の WAN 側 IP アドレスを設定します。
接続元（IX） AS 番号	接続元の AS 番号を設定します。
接続元（IX） VLAN 番号	接続元の VLAN 番号を設定します。

暗号／認証の詳細設定	
事前共有鍵	接続先と共通のパスワードを設定します。
その他	自動で設定されます。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
Amazon Web Services VPC 接続の場合

web-console wizard easy-cloud-[接続形態]
web-console remote-lan [接続先 VPN アドレス]/[マスク長] [TunnelX.0]
!
ip access-list web_vpnlist permit ip src any dest any
!
ike nat-traversal
ike proposal web_cloud_ikeprop encryption aes hash sha group 1024-bit
ike policy web_cloud_ikepolicy peer [接続先 WAN 側 IP アドレス] key [事前共通鍵]
web_cloud_ikeprop
ike keepalive web_cloud_ikepolicy 10 3
!
ipsec autokey-proposal web_cloud_secprop esp-aes esp-sha lifetime time 3600
ipsec autokey-map web_cloud_secpolicy web_vpnlist peer [接続先 WAN 側 IP アドレス]
web_cloud_secprop pfs 1024-bit
!
route-map web-cloud-map permit 10
  match interface [LAN1]
!
router bgp [接続元 AS 番号]
  neighbor [接続先 VPN アドレス] remote-as [接続先 AS 番号]
  neighbor [接続先 VPN アドレス] timers 10 30
  address-family ipv4 unicast
    redistribute connected route-map web-cloud-map
    originate-default always
!
interface [TunnelX.0]
  description Cloud-AWS-VPN
  tunnel mode ipsec
  ip address [接続元 VPN アドレス]/[マスク長]
  ip tcp adjust-mss auto
  ipsec policy tunnel web_cloud_secpolicy out
  no shutdown

Amazon Web Services ダイレクトコネクトの場合

web-console wizard easy-cloud-direct
web-console interface wan1 [WAN1.2]
!
route-map web-cloud-map permit 10
  match interface [LAN1]
!
router bgp [接続元 AS 番号]
  neighbor [接続先 WAN 側アドレス] remote-as [接続先 AS 番号]
  neighbor [接続先 WAN 側アドレス] password [接続先 BGP パスワード]
  neighbor [接続先 WAN 側アドレス] timers 10 30
  address-family ipv4 unicast
    redistribute connected route-map web-cloud-map
```

```
      originate-default always
!
interface [WAN2.1]
   description Cloud-AWS-DC
   encapsulation dot1q [接続元 VLAN 番号] tpid 8100
   auto-connect
   ip address [接続元 WAN 側 IP アドレス]/[ マスク長]
   no shutdown
```

Microsoft Azure VPC 接続の場合

```
web-console wizard easy-cloud-[接続形態]
web-console remote-lan [接続先 LAN 側ネットワーク]/[マスク長] [TunnelX.0]
!
ip route [接続先 LAN 側ネットワーク]/[マスク長] [TunnelX.0]
ip access-list web_vpnlist permit ip src any dest any
!
ike nat-traversal
ike proposal web_cloud_ikeprop encryption aes hash sha group 1024-bit
ike policy web_cloud_ikepolicy peer [接続先 WAN 側 IP アドレス] key [事前共通鍵]
web_cloud_ikeprop
ike keepalive web_cloud_ikepolicy 10 3
!
ipsec autokey-proposal web_cloud_secprop esp-aes esp-sha lifetime time 3600
ipsec autokey-map web_cloud_secpolicy web_vpnlist peer [接続先 WAN 側 IP アドレス]
web_cloud_secprop
ipsec local-id web_cloud_secpolicy [接続元 LAN 側ネットワーク]/[マスク長]
ipsec remote-id web_cloud_secpolicy [接続先 LAN 側ネットワーク]/[マスク長]
!
interface [WAN1]
   ip napt static [WAN1] udp 500
   ip napt static [WAN1] udp 4500
   ip napt static [WAN1] 50
!
interface [TunnelX.0]
   description Cloud-Azure-VPN
   tunnel mode ipsec
   ip unnumbered [LAN1]
   ip tcp adjust-mss auto
   ipsec policy tunnel web_cloud_secpolicy df-bit ignore pre-fragment out
   no shutdown
```

NEC Cloud IaaS VPC 接続の場合

```
web-console wizard easy-cloud-[接続形態]
web-console remote-lan [接続先 LAN 側ネットワーク]/[マスク長] [TunnelX.0]
!
ip route [接続先 LAN 側ネットワーク]/[マスク長] [TunnelX.0]
ip access-list web_vpnlist_nci permit ip src [接続元 LAN 側ネットワーク]/[マスク長] dest
[接続先 LAN 側ネットワーク]/[マスク長]
!

ike nat-traversal
ike proposal web_cloud_ikeprop encryption aes hash sha group 1024-bit
ike policy web_cloud_ikepolicy peer [接続先 WAN 側 IP アドレス] key [事前共通鍵]
web_cloud_ikeprop
ike keepalive web_cloud_ikepolicy 10 3
!
```

```
ipsec autokey-proposal web_cloud_secprop esp-aes esp-sha lifetime time 3600
ipsec autokey-map web_cloud_secpolicy web_vpnlist_nci peer [接続先 WAN 側 IP アドレス] web_cloud_secprop pfs 1024-bit
!
interface [WAN1]
   ip napt static [WAN1] udp 500
   ip napt static [WAN1] udp 4500
   ip napt static [WAN1] 50
!
interface [TunnelX.0]
   description Cloud-NECCI-VPN
   tunnel mode ipsec
   ip unnumbered [LAN1]
   ip tcp adjust-mss auto
   ipsec policy tunnel web_cloud_secpolicy df-bit ignore pre-fragment out
   no shutdown
```

2.43.8.17 SSH/Telnet の設定 （Ver.9.5 以前）

「詳細設定」から「リモート保守」の「SSH/Telnet の設定」を選択します。
（Ver.9.6 以降は、「保守の設定」を選択してください。）
「SSH/Telnet の設定」では、以下の設定を行うことができます。

SSH/Telnet の設定	
SSH	SSH サーバの有効／無効を設定します。
Telnet サーバ機能	telnet サーバの有効／無効を設定します。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
! SSH 設定時
ssh-server ip enable
pki private-key generate rsa

! telnet 設定時
telnet-server ip enable
```

2.43.8.18 デバイスの設定

「詳細設定」から「デバイス」の「デバイスの設定」を選択します。
デバイスの一覧が表示されますので、設定変更するデバイスの[変更]を押してください。
「デバイスの設定」では、以下の設定を行うことができます。

デバイスの設定	
デバイスの利用	shutdown/no shutdown を設定します。
回線速度	回線速度を設定します。Duplex は速度が auto の場合は auto、固定の場合は全二重に設定されます。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】

device [選択デバイス]
   speed [回線速度]
   duplex [duplex]
   no shutdown
```

2.43.9 拡張ページ

Ver9.3 以降、用途にあわせてカスタマイズしたページを登録することができます。HTML と Javascript で、任意の show コマンドの結果を参照して現在の設定や状態を表示したり、ほぼ全ての CLI コマンドを生成して実行する任意のページを作成可能です。

使用するファイルを ZIP 形式で圧縮して「拡張ページ」からアップロードしてください。アップロードしたあとは一度 Web サーバとの接続を切って再接続してください。
アップロードされたファイルはフラッシュメモリに書き込まれます。フラッシュメモリのサイズにご注意ください。show flash コマンドにより確認できます。

- ファイル名、フォルダ名に日本語は使用できません。
- ファイル名、フォルダ名は大文字、小文字は区別されません。
- フォルダ名を含めたファイル名の最大長は 255 文字です。
- ファイルの文字コードは UTF-8 のみとなります。
- 対応する拡張子は、以下のとおりです。
  - ✧ html、htm、css、js、xml（Ver9.4 以降）
  - ✧ jpeg、jpg、gif、png、bmp、ico
- アップロード可能なファイルは 1 つのみです。複数ファイルをアップロードする場合は 1 つのファイルに ZIP 圧縮してください。

2.43.10 WebAPI 機能

WebAPI 機能により、外部の Web サーバ上のページから設定変更を行うことができます（Ver9.6 以降）。WebAPI 機能を利用するためのコマンドは以下のとおりです。

http-server cross-site allow	WebAPI 機能の有効化
http-server cross-site password	WebAPI 機能のパスワード設定
http-server cross-site ip access-list	WebAPI 機能のアクセスリスト設定

Web コンソールの有効化が必要です。また、WebAPI はパスワードなしでは動作しません。
WebAPI のアクセスリストの評価は、Web コンソールのアクセスリストの評価後に行われます。

WebAPI の使用は、IX にパスワードと CLI コマンドを POST で送信することで可能です。
送信先 URL は /api/config.html または /api/config.txt です。
/api/config.html の場合は、コマンド実行の成否が HTML で返ってきます。
/api/config.txt の場合は、コマンド実行のログが TXT で返ってきます。

【使用例（/api/config.html）】

```
<html><body>
   <form action=http://192.168.1.254/api/config.html
    method="post" enctype="multipart/form-data">
      <input type="submit" value="反映" />
      <input type="hidden" name="cross-site-password" value="PASSWORD" />
      <input type="hidden" name="command" value="
interface GigaEthernet0.0
   ip address dhcp receive-default
   no shutdown
interface GigaEthernet2.0
   no shutdown" />
   </form>
</body></html>
```

【結果（成功時）】

```
<title>success</title>
<h4>設定変更を行いました。</h4>
```

【結果（失敗時）】

```
<title>failure</title>
<h4>設定変更に失敗しました。</h4>
```

【使用例（/api/config.txt）】

```
<html><body>
   <form action="http://192.168.1.254/api/config.txt"
   method="post" enctype="multipart/form-data">
      <input type="submit" value="反映" />
      <input type="hidden" name="cross-site-password" value="PASSWORD" />
      <input type="hidden" name="command" value="
interface GigaEthernet0.0
   ip address dhcp receive-default
   no shutdown
interface GigaEthernet2.0
   no shutdown" />
   </form>
</body></html>
```

```
【結果】
Router(config)# interface GigaEthernet0.0
Router(config-GigaEthernet0.0)#     ip address dhcp receive-default
Router(config-GigaEthernet0.0)#     no shutdown
Router(config-GigaEthernet0.0)# interface GigaEthernet2.0
% GigaEthernet2.0    -- Invalid command.
Router(config-GigaEthernet0.0)#     no shutdown
Router(config-GigaEthernet0.0)#
```

2.43.11 その他

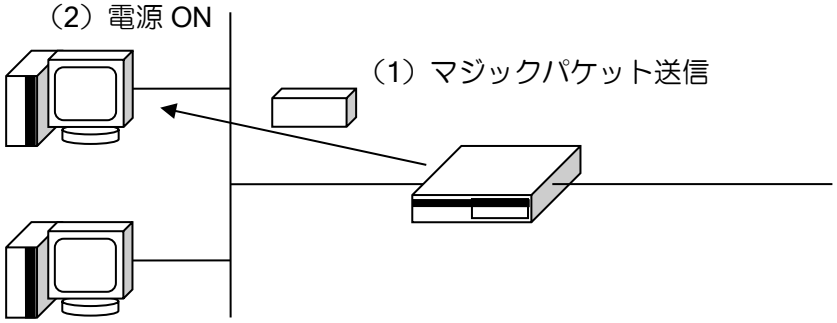
Ver9.5 以降対応のリンクマネージャ機能、Web 認証機能、URL フィルタリング機能については、各項目の説明を参照してください。

■2.44 Wake on LAN の設定

Ver.8.9 以降、ルータから Wake on LAN 機能により端末を起動する機能をサポートしています。端末の起動はコマンドラインおよび Web コンソール機能から実行可能です。

2.44.1 Wake on LAN 機能概要

IX ルータがサポートする Wake on LAN 機能は、ルータに接続されている端末の MAC アドレスに対し、マジックパケットと呼ばれる特殊なパケットを送信することで、指定した端末を起動する機能です。端末が Wake on LAN 機能に対応している必要があります。



2.44.2 制限事項

ルータに直接接続されている同一リンク上の端末以外を起動することはできません。

2.44.3 コマンドラインからの利用

端末を起動するためのコマンドは以下のとおりです。

wol terminal	Wake on LAN 起動端末の登録
wol ethernet-type	マジックパケットのイーサネットタイプ変更
wol send	マジックパケットの送信

wol send コマンドは MAC アドレスを指定してマジックパケットを送信できます。また、wol terminal コマンドで端末の MAC アドレスに名前を設定し、その名前を指定でマジックパケットを送信することも可能です。

イーサネットタイプは通常変更する必要はありません。

【設定例】

```
wol terminal user1 mac 00:00:00:00:00:11 interface GigaEthernet0.0
wol terminal user2 mac 00:00:00:00:00:22 ip 192.168.0.2 interface GigaEthernet0.0

user1 と名前を設定した端末を起動します。
wol send terminal user1
```

2.44.4 Web コンソールからの利用

Web コンソール機能を利用して端末を起動したい場合は、以下の手順で行います。

2.44.4.1 Wake on LAN 用ログインユーザの設定

Wake on LAN 機能を利用するユーザの設定を行います。Web コンソールの Wake on LAN 機能は 1 ユーザのみ設定可能で、username コマンドで設定されている必要があります（通常 monitor モードで登録します）。Ver.8.11 以降は、Web コンソールのアカウントを使用して Wake on LAN 機能のページへログインすることもできます。Ver.9.6 以降、設定コマンドが変わるため注意してください。

http-server ip enable	HTTP サーバの有効化
http-server wol-username	Wake on LAN 機能を利用可能なユーザの指定 （Ver.9.5 以前）
http-server monitor-username	monitor モードにログイン可能なユーザの指定 （Ver.9.6 以降）

2.44.4.2 起動端末の登録

Web コンソールの Wake on LAN 機能を利用する場合は、端末を全てコンフィグで登録しておく必要があります。固定アドレスの端末の場合には IP アドレスまで設定しておくと、Web コンソールの画面で Ping 機能により起動確認を行うことができます。

wol terminal	Wake on LAN 起動端末の登録
wol ethernet-type	マジックパケットのイーサネットタイプ変更

2.44.4.3 Wake on LAN 機能のページへのログイン

端末を起動したいユーザは、Wake on LAN 機能専用のトップページ（/wol/index.html）から Wake on LAN のアカウントでログインしてください。Ver.8.11 以降は、Web コンソールのトップページのリンクから「端末の起動制御」に移動できます。

2.44.4.4 端末を起動する

設定されている端末が一覧表示されます。起動したい端末の「起動」ボタンを押すことにより、端末が起動します。IP アドレスを設定してある端末については「端末状態の確認」で起動したことを確認することができます（端末が Ping に応答する必要があります）。

2.44.4.5 表示項目

Web コンソールで表示する項目は以下のとおりです。

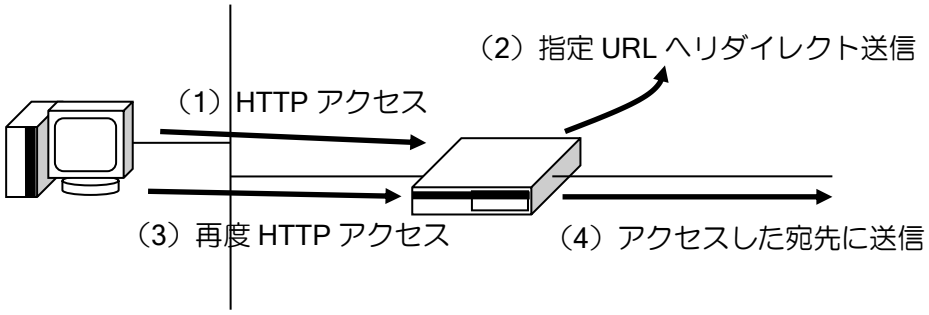
端末情報一覧	
端末名	設定した端末名を表示します。
MAC アドレス	設定した MAC アドレスを表示します。
IP アドレス	設定した IP アドレスを表示します。 未設定の場合は“-”が表示されます。
送信インタフェース	設定した送信インタフェースを表示します。
端末状態	端末状態を表示します。 端末応答あり：“ON” 端末応答なし：“-”

■2.45 URL リダイレクトの設定

Ver.9.0 以降、ネットワークの利用者が外部へ HTTP アクセスする際に、設定したサイトを利用者のブラウザへ表示させることが可能です。IPv6 にも対応しています。

2.45.1 URL リダイレクト機能概要

IX ルータが受信する最初の HTTP アクセスの場合、設定した URL へリダイレクトを行います。その後は、通常どおりに通信が可能となります。最初のアクセスの後、一定時間経過後に再度リダイレクトされます。リダイレクトの制御は端末毎に行います。



URL リダイレクト機能を利用するためのコマンドは以下のとおりです。

http-redirect enable	URL リダイレクト機能有効化 （インタフェースコンフィグモード）
http-redirect exclude	URL リダイレクト除外設定（Ver.9.2 以降） （インタフェースコンフィグモード）
http-redirect url	リダイレクト先 URL の設定 （グローバルコンフィグモード）
show http-redirect information	リダイレクト端末情報

【設定例】
GigaEthernet1.0 から受信した場合に example.com/example.html へリダイレクト

```
http-redirect url http://example.com/example.html

interface GigaEthernet1.0
  ip address 192.168.0.1/24
  http-redirect enable
  no shutdown

10.0.0.0/24 宛てのアクセスの場合はリダイレクトを行わない

ip access-list acl1 permit ip src any dest 10.0.0.0/24

http-redirect url http://example.com/example.html

interface GigaEthernet0.0
  ip address 192.168.0.1/24
  http-redirect enable
  http-redirect exclude ip acl1
  no shutdown
```

URL リダイレクト機能は、リダイレクト対象のアクセスを端末ごとに管理します。端末は MAC アドレスで区別します。

ユーザにリダイレクト先のページを表示させた後、再度表示するまでの間隔を設定することによって、ネットワークの利用者に対して、1 日に 1 回などの頻度で強制的にリダイレクト先のページを表示させることができます。また、ユーザの通信の途中でリダイレクトすることを防止するため、無通信時間を設定することが可能です。無通信時間を設定した場合、リダイレクト先のページを表示する時刻になってもすぐにはリダイレクトせず、ユーザの画面操作が一定時間停止した後の最初の通信でリダイレクトを行います。

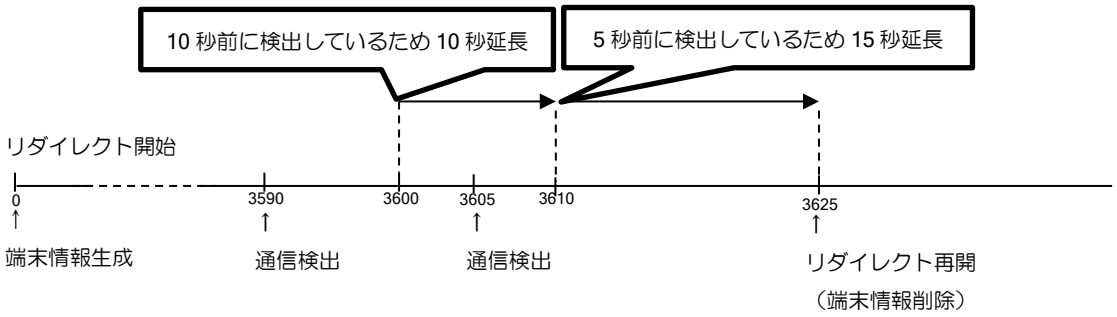
タイマの設定は以下のとおりです。

http-redirect interval	ブラウザアクセス時の指定 URL 表示間隔の設定（グローバルコンフィグ）
http-redirect non-browser-interval	非ブラウザアクセス時の指定 URL 表示間隔の設定（グローバルコンフィグ）
http-redirect idle	無通信時間の設定（グローバルコンフィグ）

【設定例】
指定 URL 表示間隔：1 時間
無通信時間：20 秒

```
http-redirect interval hour 1
http-redirect idle 20
```

設定例の場合の動作例



なお、ブラウザ以外の HTTP 通信でもリダイレクト処理は実行されます。動作原理上、ブラウザの通信かどうか判別できるようになる前にリダイレクトする必要があるためです。

起動時に OS やアプリケーションの自動アップデート機能が動作する場合、それらの最初の通信もリダイレクトされます。その後、ユーザがブラウザを利用する時点では、その端末はすでにリダイレクト実施済みの状態となっているため、ユーザのブラウザ通信はリダイレクトされません。このような状態を防止するため、非ブラウザによる通信はリダイレクトの間隔を短く設定できます（http-redirectnon-browser-interval）。

ただし非ブラウザ用のリダイレクト間隔が短すぎると、非ブラウザによる通信完了前にリダイレクトが再度発生して障害になる可能性もありますので、設定値には注意してください。

2.45.2 注意事項

- HTTPS アクセスはリダイレクトを行いません。
- 端末登録エントリ数、同時セッション接続数の上限を超えた場合、リダイレクトを行いません。
- 本機能はリダイレクトの制御のため、TCP の 10080, 10081 番ポートを利用します。
- ブラウザによる通信か否かの判定は HTTP の User-Agent フィールドで行います。主要なブラウザが指定する文字列を含まない場合には、正しく判定されない場合があります。
- 起動時に非ブラウザのアプリケーションがブラウザの User-Agent を利用する場合、ユーザの通信よりも先に URL リダイレクトの動作が完了してしまう場合があります。

■2.46 URL オフロードの設定

Ver.9.4 以降、特定の宛先（URL/IP アドレス）向けのトラフィックのみを通常と異なる経路に転送できます。

データセンタを経由してインターネットを利用する環境において、クラウドサービス通信のみを直接インターネット経由でアクセスさせることによって、データセンタへのトラフィックの集中を軽減することができます。

Ver10.5 以降では、NetMeister 連携時に UDP などの HTTPS 以外のすべてのプロトコルでオフロードすることができます。ただし、NetMeister の URL オフロード画面上のチェックボックスで選択された宛先・追加 URL 欄に IP アドレスで宛先を記載された場合に限ります。追加 URL 欄に URL 等で記載した場合は対象となりません。

プロキシサーバがある構成で URL オフロードを使用する場合、PC などの端末側に「プロキシ例外」の設定が必要になります。Ver9.6 以降では、端末側での「プロキシの例外」設定の自動化を行うことができます。

2.46.1 URL オフロード機能概要

特定の宛先（URL/IP アドレス）向けのトラフィックに対して、通常と異なるルーティングを行います。以降、この動作を「オフロード」と呼びます。

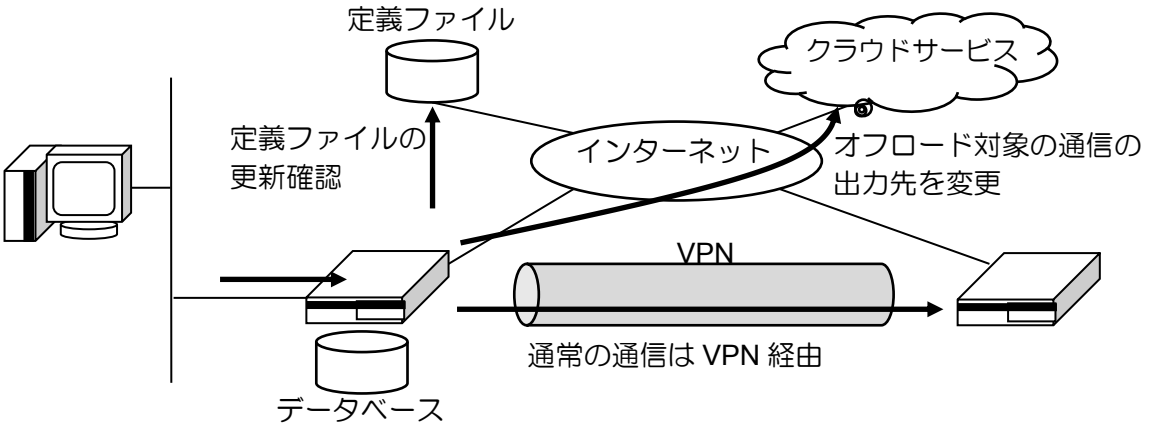
オフロード対象となる宛先（URL/IP アドレス）は、外部定義ファイルから読み込み、装置内にデータベースを作成します。定期的に定義ファイルを読み込むことで、定義ファイルの更新にも対応できます。

Ver.9.5 以降、URL リストを使用することでオフロード対象となる宛先を任意で設定することができます。また、定義ファイルでオフロード対象となっている宛先をオフロード対象外にすることができます。

Ver9.6 以降、HTTPS 通信だけでなく HTTP 通信(TCP/80)もオフロードすることができます。

Ver10.1 以降、外部定義ファイルを NetMeister と連携することで受信することができます。

Ver10.5 以降、NetMeister と連携中であれば、UDP などを含むすべてのプロトコルをオフロード対象にすることができます。



パケットの宛先（URL/IP アドレス）を、データベース上の情報と比較して、データベースと一致したパケットをオフロードします。

なお、インターネットアクセスにプロキシサーバを使用している場合、パケットの宛先 IP アドレスは全てプロキシサーバのアドレスとなり、オフロード対象かどうかを判定することができません。このため、プロキシサーバを使用している場合は、端末側で「プロキシの例外」を設定する必要があります。

Ver9.6 以降では、プロキシの自動構成スクリプト配信に対応しており、端末側での「プロキシの例外」設定が自動化できます。

Ver10.4 以降、UTM サーバおよび NetMeister サーバ宛の通信はオフロード対象になりません。

Ver10.5 以降、NetMeister 子機からの NetMeister サーバ宛の通信はオフロード対象になりません。

2.46.2 制限事項

- IPv6 通信はオフロードされません。
- HTTPS/HTTP 通信は、プロキシサーバを使用していない構成時の設定の場合、最初の通信は通常の経路での通信となり、以降のセッションからオフロードされます。
- オフロード対象は、Ver9.5 までは IPv4 の HTTPS 通信のみ、Ver9.6 以降では IPv4 の HTTP 通信も対象にすることができます。HTTPS/HTTP 以外(FTP など)の通信はオフロードされません。ただし、Ver10.5 以降では、NetMeister 連携時に限り HTTPS/HTTP 以外の通信もオフロード対象にすることができます。
- 定義ファイルの形式は、XML ベースの URL リストに対応しています。

➢ IPv6 アドレスは未対応です。
➢ URL には以下の制限があります。
✧ 末尾のワイルドカードには未対応です。

- インターネットアクセスにプロキシサーバを使用している場合、端末側で「プロキシの例外」を設定する必要があります。Ver9.6 以降では「プロキシの例外」設定が自動化できます。
- URL リストの評価順は、IP アドレスの評価の後、ドメインおよび any を評価します。
- 定義ファイルの最大サイズは 1Mbyte です。

2.46.3 基本設定

URL オフロード機能を利用するためのコマンドは以下のとおりです。設定変更を即時反映するには、url-offload update の実行が必要です。

url-offload profile	URL オフロードプロファイルの作成 （グローバルコンフィグモード）
ip url-offload profile	URL オフロード判定の有効化 （インタフェースコンフィグモード）
match ip url-offload	URL オフロードデータベース条件 （ルートマップコンフィグモード）
wpad	プロキシ自動設定ファイルの URL 指定 （DHCP コンフィグモード）
url	URL オフロード定義ファイルの指定 （URL オフロードコンフィグモード）
list	URL リストの指定 （URL オフロードコンフィグモード）
proxy-config	プロキシサーバやプロキシ定義ファイルの指定 （URL オフロードコンフィグモード）
offload-protocol	URL オフロード対象プロトコルの指定 （URL オフロードコンフィグモード）
offload-scheme	URL スキームチェックの設定 （URL オフロードコンフィグモード）
source-interface	送信元インタフェースの設定 （URL オフロードコンフィグモード）
ssl-protocol	SSL プロトコルの設定 （URL オフロードコンフィグモード）
transport	通信プロトコルの設定 （URL オフロードコンフィグモード）
update-interval	更新周期の変更

	（URL オフロードコンフィグモード）

2.46.3.1 外部定義ファイルの利用

起動後に外部定義ファイルを取得し、装置内にデータベースを作成します。作成したデータベースを使用してオフロード対象の判定を行います。

外部定義ファイル取得後は、一定の周期で外部定義ファイルを取得し、データベースを更新します。一度取得に成功した後は、その後の外部定義ファイルの取得に失敗した場合でも、その時点で保持しているデータベースを使用し、オフロード処理を行います。

外部定義ファイルを取得するには以下の設定が必要です。また、NetMeister から取得することも可能です。（Ver10.1 以降）

```
【設定例 1】
外部定義ファイルの URL を指定
データベースの更新周期を 1 週間に設定

url-offload profile urlo-prof
  url https://example.com/OffloadList.xml
  update-interval 168

【設定例 2】
NetMeister にある外部定義ファイルを指定（Ver10.1 以降）

url-offload profile urlo-prof
  url netmeister
```

NetMeister からすぐに定義ファイルを反映する場合は、先に nm update コマンドにより NetMeister 情報を更新してから、url-offload update コマンドする必要があります。

起動後に外部定義ファイルを取得し、装置内にデータベースを作成します。作成したデータベースを使用してオフロード対象の判定を行います。
起動後、外部定義ファイルを取得しデータベース構築に成功するまでは、60 秒周期に取得処理を行います。定義ファイルを取得できていない状態では、オフロード対象が存在しない状態の動作となります。

定義ファイルを取得できていない状態での動作：

- プロキシサーバなし
  オフロード対象のパケットは通常のルーティングに従い送信されます。
- プロキシサーバあり
  オフロード対象のパケットは廃棄されます。

※ Microsoft 365 ® の利用について

本機能は XML ベースの URL リストに対応しております。Microsoft 365 ® の URL リストは、2018 年 10 月以降 XML ベースから JSON ベースの web サービスに変更されており、そのままの設定では利用できません。
クラウドサービス「NetMeister」では Microsoft 社のリストを XML 方式に変換するサービスを運用しておりますので、URL リストの入手先を変更いただければ Microsoft 社の URL リストを継続利用することが可能になります。（NetMeister へのユーザ登録は不要です。）

変更前
https://support.content.office.net/en-usstatic/O365IPAddresses.xml

変更後
url https://offload.nw-meister.jp/v1/o365.xml

2.46.3.2 内部 URL リストの利用

Ver.9.5 以降、URL リストを利用することで、外部定義ファイルのオフロード対象を削除したり、追加したりすることができます。内部 URL リストのみでオフロードすることも可能です。

URL リストの詳細説明は、URL フィルタリング機能を参照してください。ドメインを permit で指定するとオフロード対象に、deny で指定するとオフロード対象外になります。
URL リストは外部定義ファイルよりも先に適用されるため、URL リストで permit 指定した通信は外部定義ファイルの内容に関わらずオフロード対象となり、URL リストで deny 指定した通信は外部定義ファイルの内容に関わらずオフロード対象外となります。

【設定例】
URL リストでオフロード対象を追加・削除

```
url-list urll-1 deny domain *.example1.com
url-list urll-1 permit domain *.example2.com

url-offload profile urlo-prof
  url https://example.com/OffloadList.xml
  list urll-1
```

この設定例では以下のとおり動作します。

- *.example1.com の通信は、外部定義ファイルの設定によらずオフロードしません。
- *.example2.com の通信は、外部定義ファイルの設定によらずオフロードします。
- その他の通信は、外部定義ファイルに従います。

2.46.3.3 URL オフロードの設定

URL オフロードの判定には、経路制御処理とフィルタ処理の 2 つの処理があります。経路制御処理は、ポリシールーティングを使用してオフロード対象の経路変更を行います。フィルタ処理は、オフロード対象ドメインの IP アドレスキャッシュの作成や、オフロード対象外パケットの廃棄を行います。

【設定例】
経路制御処理として、ポリシールーティングの条件に URL オフロードを指定
フィルタ処理として、Tunnel0.0 に URL オフロード設定を追加

```
route-map urlo-map permit 1
  match ip url-offload urlo-prof
  set interface GigaEthernet0.1
!
interface GigaEthernet2.0
  description LAN
  ip policy route-map urlo-map
!
interface Tunnel0.0
  description VPN
  ip url-offload profile urlo-prof
```

Ver10.6 以降、URL オフロードデータベース条件(match ip url-offload)の設定に URL リスト名またはアプリケーション名を指定することができ、特定の通信を URL オフロード対象にすることができます。また、複数ルートマップを作成することで、アプリーション単位で別々のインタフェースに振り分けることができます。

※アプリケーション名を使用する場合、URL オフロードデータベースの指定コマンド(url)で”netmeister”をデータベースとして指定する必要があります。

```
【設定例】
URL オフロードデータベース条件へのアプリケーション名、URL リスト名の設定

route-map urlo-map-1 permit 10
  match ip url-offload urlo-prof app office
  set interface GigaEthernet1.0

route-map urlo-map-1 permit 11
  match ip url-offload urlo-prof url-list my_list
  set interface GigaEthernet2.0
```

設定可能なアプリケーション名は以下になります。

NetMeister 画面表示上の名称	アプリケーション名
Office365	Office365
Skype/Teams	Skype/Teams
Windows Update	WindowsUpdate
Box	Box
G Suite	GSuite
Adobe Creative Cloud	AdobeCreativeCloud
Salesforce	Salesforce
Zoom	Zoom
WebEX	WebEX
UNIVERGE BLUE	UNIVERGEBLUE
Google	Google
NetMeister	NetMeister
ユーザ定義	UserDefined

※XML 形式のデータベース内容または、PAC ファイル URL をポリシールーティングの対象にする場合、URL オフロードデータベース条件の設定に default を指定する必要があります。

```
【設定例】
route-map urlo-map-1 permit 10
  match ip url-offload urlo-prof url-list default
  set interface GigaEthernet1.0
```

2.46.3.4 URL オフロード対象の設定

Ver9.6 以降、オフロード対象に HTTP 通信を追加することができます。『HTTPS 通信のみ』または『HTTPS 通信と HTTP 通信の両方』の設定が可能です。

Ver10.5 以降、オフロード対象に全てのプロトコルを指定することができます。ただし、HTTPS と HTTP 以外の通信に対して実際にオフロードが動作するのは NetMeister と連携している時のみとなります。

コマンドは以下の通りです。

【設定例 1】
オフロード対象を『HTTPS 通信と HTTP 通信の両方』に設定

```
url-offload profile urlo-prof
  offload-protocol both
```

【設定例 2】
オフロード対象を『全プロトコル』に設定（Ver10.5 以降）

```
url-offload profile urlo-prof
  offload-protocol any
```

2.46.4 基本動作

URL オフロード機能の基本動作は以下となります。

2.46.4.1 オフロード対象

オフロード対象とオフロード動作については以下となります。

バージョン	データベース	種別	プロトコル	動作
Ver.9.6 以降	外部データ URL リスト	URL/IP	HTTPS	2 番目の通信からオフロード
Ver.9.7 以降	外部データ URL リスト	URL/IP	HTTP	2 番目の通信からオフロード
Ver.10.0 以降	NetMeister	URL/IP	HTTP/HTTPS	2 番目の通信からオフロード
Ver.10.5 以降	NetMeister	IP	HTTP/HTTPS 以外	最初の通信からオフロード
Ver.10.8 以降	NetMeister 外部データ URL リスト	IP	HTTP/HTTPS	最初の通信からオフロード
---	URL リスト	IP	HTTP/HTTPS 以外	未サポート

Ver.10.8 の動作については、設定により Ver.10.5 の動作に変更することができます。

url-offload compatibility	従来バージョンとの互換モードの設定 （グローバルコンフィグモード）

2.46.4.2 ルートマップ

ルートマップの match 条件に URL オフロードプロファイルを設定した場合は以下の動作になります。

①セッションキャッシュを参照し、存在する場合は match しない
②アドレスキャッシュを参照し、「positive」が存在する場合はオフロード
③アドレスキャッシュを参照し、「negative」が存在する場合は match しない
④IP アドレスのデータベースを参照し、該当する場合はアドレスキャッシュを「positive」で作成してオフロード
（HTTPS/HTTP：Ver.10.8 以降、HTTP/HTTPS 以外：Ver.10.5 以降）
⑤その他の場合は、match しない

ルートマップに match しない場合は、次のシーケンスのルートマップを参照します。
次が無い場合は、ルーティングに従って転送されます。

2.46.4.3 URL オフロードプロファイル設定（インタフェース）

インタフェースに URL オフロードプロファイルを設定した場合は以下の動作になります。

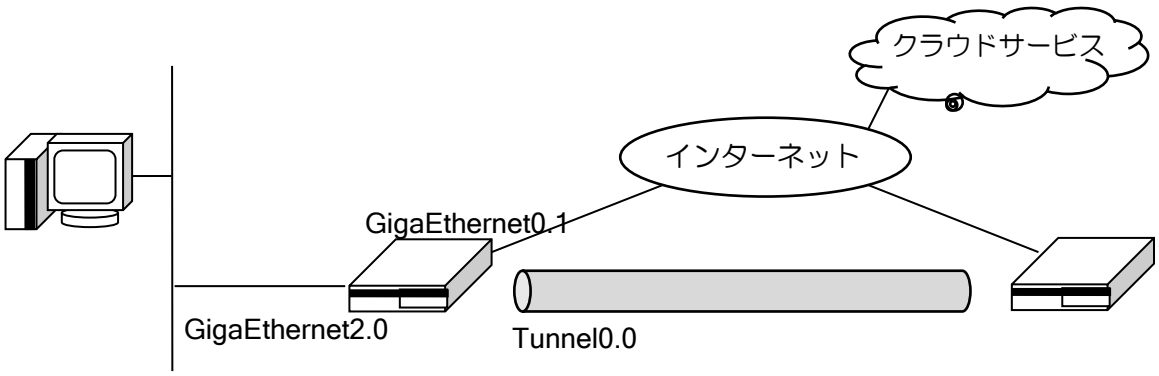
①データベースに該当する場合は、アドレスキャッシュを「positive」で作成
　HTTP/HTTPS の場合はセッションキャッシュを作成
②データベースに該当しない場合は、アドレスキャッシュを「negative」で作成

オプション指定時の対象プロトコル、動作は以下のとおりです。

オプション	対象	種別	備考
unmatch-action discard	HTTP/HTTPS	データベースに該当しない場合は廃棄	
unmatch-action discard no-negative-cache	すべて	データベースに該当しない場合は廃棄し、アドレスキャッシュ「negative」は作成しない	Ver.10.4 以降
match-action ignore-filter	すべて	データベースに該当する場合は、フィルタを無視して通過	Ver.10.5 以降

2.46.5 構成別設定例

URL オフロード機能は、プロキシサーバのあり／なしで設定方法が異なります。
下図の構成を例として、プロキシサーバなし／ありの場合それぞれについて説明します。



2.46.5.1 プロキシサーバ利用なし

すべてのインターネットアクセス通信を Tunnel0.0 にルーティングするように設定したうえで、オフロード対象の通信のみ、ポリシールーティングで出力インタフェースを変更します。ポリシールーティングの対象を指定するための match 条件には url-offload を指定します。また、Tunnel0.0 を通過するトラフィックがオフロード対象かを判断するために、Tunnel0.0 に URL オフロードを設定します。

【設定例】
通常のパケットは Tunnel0.0 に出力。
オフロード対象のパケットの場合は GigaEthernet0.1 に出力。

```
ip route default Tunnel0.0
!
url-offload profile urlo-prof
   url https://example.com/OffloadList.xml
!
! ルートマップの match 条件に URL オフロードを指定
route-map urlo-map permit 1
   match ip url-offload urlo-prof
   set interface GigaEthernet0.1
!
interface GigaEthernet0.1
   description Internet
   encapsulation pppoe
   ppp binding ppp1
   ip address ipcp
   ip napt enable
!
! LAN 側インタフェースで、ポリシールーティングを有効
interface GigaEthernet2.0
   description LAN
   ip address 192.168.1.254/24
   ip policy route-map urlo-map
!
! Tunnel0.0 に URL オフロードを指定
interface Tunnel0.0
   description VPN
   tunnel mode ipsec
   ip unnumbered GigaEthernet2.0
   ip url-offload profile urlo-prof
```

2.46.5.2 プロキシサーバ利用構成

あらかじめ端末側でオフロード対象に対する「プロキシの例外」を設定しておきます。ver9.6 以降では、プロキシの自動構成スクリプトを使うことで、「プロキシの例外」の設定を自動的に行うことができます。

プロキシ宛てを含むイントラネット内の通信を Tunnel0.0 に、インターネット宛ての通信を GigaEthernet0.1 にルーティングすることで、「プロキシの例外」の通信をオフロード対象としてインターネットに直接ルーティングします。

また、本来オフロード対象ではない通信がインターネットに直接ルーティングされないように、GigaEthernet0.1 に URL オフロードを設定します。URL オフロード機能によって、オフロード対象ではない通信を破棄します。なお、URL オフロード機能では HTTPS 通信または HTTP 通信しか識別できないため、それ以外の通信を制限したい場合は、アクセスリストによって明示的に制限します。例では HTTPS と VPN 以外の通信がインターネットに直接ルーティングされないように制限しています。Ver.10.5 以降の場合は、「match-action ignore-filter」を設定することにより、オフロード対象の通信の場合は、アクセスリストにて許可していない場合でも、通信が許可されます。

【設定例】
イントラネット内のパケットは Tunnel0.0 に出力。
その他のパケットは GigaEthernet0.1 に出力
オフロード対象に該当しないパケットを GigaEthernet0.1 に出力した場合は廃棄

```
ip route default GigaEthernet0.1
ip route 192.168.0.0/16 Tunnel0.0
!

ip access-list urlo-acl permit 50 src any dest any
ip access-list urlo-acl permit udp src any sport eq 500 dest any dport any
ip access-list urlo-acl permit udp src any sport any dest any dport eq 500
ip access-list urlo-acl permit udp src any sport eq 4500 dest any dport any
ip access-list urlo-acl permit udp src any sport any dest any dport eq 4500
ip access-list urlo-acl deny ip src any dest any
!
url-offload profile urlo-prof
   url https://example.com/OffloadList.xml
!
! インターネット側インタフェースで、
! 廃棄オプションを有効にして URL オフロードを設定
interface GigaEthernet0.1
   description Internet
   encapsulation pppoe
   ppp binding ppp1
   ip address ipcp
   ip napt enable
   ip filter urlo-acl 1 out
   ip url-offload profile urlo-prof unmatch-action discard no-negative-cache match-action
ignore-filter
!
interface Tunnel0.0
   description VPN
   tunnel mode ipsec
   ip unnumbered GigaEthernet2.0
```

2.46.6 プロキシ例外設定の自動化

プロキシサーバ利用構成では、端末側にプロキシ例外の設定が必要になります。プロキシ例外の設定は、端末に直接設定する以外に、PAC ファイルと呼ばれる「プロキシ例外条件を記述したファイル」を端末に読み込ませることでも設定できます。

Ver9.6 以降では、PAC ファイルを利用して端末側でのプロキシ例外設定の自動化を行うことができます。URL オフロード対象のプロキシ例外の条件を記述した PAC ファイルを IX ルータ内に自動的に生成し、端末に配信します。

端末側では、IX ルータ内の PAC ファイルの URL(http://<IX ルータの IP アドレス>:<ポート番号>/proxy.pac)を設定する必要がありますが、DHCP を利用している環境であれば、PAC ファイルの URL を DHCP で端末に通知することもできます。

2.46.6.1 PAC ファイルの生成

URL オフロード対象をプロキシの例外とするための PAC ファイルを自動的に生成します。URL オフロード対象の例外設定だけを含む PAC ファイルを新規に生成したり、既存の PAC ファイルをもとにして URL オフロード対象の例外設定を追加した PAC ファイルを生成したりできます。

URL オフロード対象の例外設定だけを含む PAC ファイルを新規に生成する場合は、通常のインターネットアクセス時に使用するプロキシサーバのアドレスを設定します。

【設定例】
プロキシサーバのアドレスを指定

```
url-offload profile urlo-prof
  proxy-config server 192.168.80.80:8080
```

新規に PAC ファイルを生成する場合、下記のような PAC ファイルが生成されます。

【生成 PAC ファイル例】

```
function FindProxyForURL (url, host) {
  if (isPlainHostName(host)) {
    return "DIRECT";
  }

  /* URL-OFFLOAD */
  if ((url.startsWith(“https:”) || url.startsWith(“wss:”)) && (
       isInNet(host, "172.16.0.0", "255.255.0.0") ||
           :
       shExpMatch(host, "*.offload.com") ||
           :
       )) {
    return "DIRECT";
  }

  return "PROXY 192.168.80.80:8080";
}
```

既存の PAC ファイルをもとにして URL オフロード対象の例外設定を追加した PAC ファイルを生成する場合は、既存 PAC ファイルの URL を設定します。IX ルータから、当該の PAC ファイルにアクセスできる必要があります。

【設定例】
既存の PAC ファイルを指定

```
url-offload profile urlo-prof
  proxy-config pac-file http://example.com/proxy.pac
```

既存の PAC ファイルに例外を追加する場合、既存 PAC ファイルの「FindProxyForURL()関数」の先頭に URL オフロード対象の例外設定が追加されます。例外設定を追加する位置をファイル内で指定したい場合は、既存 PAC ファイルに「/* URL-OFFLOAD */」というコメント行を追加します。追加したコメント行の直後に URL オフロード対象の例外設定が追加されます。

【既存 PAC ファイル例】
挿入位置指定なし

```
function FindProxyForURL (url, host) {
  if (既存の判定文) {
    return “PROXY proxy.example.com:8080”;
  }

  return “PROXY 192.168.80.80:8080”;
}
```

【生成 PAC ファイル例】

```
function FindProxyForURL (url, host) {
  /* URL-OFFLOAD */
  if ((url.startsWith(“https:”) || url.startsWith(“wss:”)) && (
      isInNet(host, "172.16.0.0", "255.255.0.0") ||
          :
      shExpMatch(host, "*.offload.com") ||
          :
      )) {
    return "DIRECT";
  }

  if (既存の判定文) {
    return “PROXY proxy.example.com:8080”;
  }

  return “PROXY 192.168.80.80:8080”;
}
```

【既存 PAC ファイル例】
挿入位置指定あり

```
function FindProxyForURL (url, host) {
   if (既存の判定文) {
      return “PROXY proxy.example.com:8080”;
   }

   /* URL-OFFLOAD */

   return “PROXY 192.168.80.80:8080”;
}
```

【生成 PAC ファイル例】

```
function FindProxyForURL (url, host) {
   if (既存の判定文) {
      return “PROXY proxy.example.com:8080”;
   }

   /* URL-OFFLOAD */
   if ((url.startsWith(“https:”) || url.startsWith(“wss:”)) && (
         isInNet(host, "172.16.0.0", "255.255.0.0") ||
            :
         shExpMatch(host, "*.offload.com") ||
            :
         )) {
      return "DIRECT";
   }

   return “PROXY 192.168.80.80:8080”;
}
```

URL オフロード用の PAC ファイル生成は、外部定義ファイルを取得した直後に行われます。既存の PAC ファイルを参照する場合は、PAC ファイル生成時に最新の既存 PAC ファイルを取得してから PAC ファイルを生成します。外部定義ファイルの取得に失敗した場合や、既存の PAC ファイルの取得に失敗した場合は、PAC ファイルは再生成せずに、すでに生成済みの PAC ファイルを維持します。

2.46.6.2 スキームチェックの設定

URL のスキームの対象はデフォルトで https と wss をオフロード対象にしています。新しい URL スキームに対応したい場合や、除外したい URL スキームがある場合、以下のように設定してください。

【設定例】
http と ftp を URL スキームのチェック対象に設定する

```
url-offload profile urlo-prof
   offload-schem permit http ftp
```

2.46.6.3 PAC ファイルの配信

IX ルータ内に生成された PAC ファイルは、”http://<IX ルータの IP アドレス>:<ポート番号>/proxy.pac”にアクセスすることで端末から参照できます（IX ルータで HTTP サーバ機能を有効にする必要があります。また、HTTP サーバのポート番号を変更した場合は PAC ファイルへのアクセス時のポート番号も変更後のポート番号になります）。

IX ルータの DHCP サーバ機能を利用している場合、IX ルータが生成した PAC ファイルの上記 URL を DHCP で端末に配信することができます。上記 URL を端末利用者が端末に直接設定することも可能です。

【設定例】
DHCP で IX ルータ内に生成した PAC ファイルの URL を通知

```
ip dhcp profile dhcp-prof
   wpad auto
```

【配布される URL 例】
DHCP が動作しているインタフェースの IP アドレスが 192.168.1.254 で、
HTTP サーバのポート番号がデフォルトの 80 の場合

配布される URL　“http://192.168.1.254:80/proxy.pac”

2.46.6.4 端末側の設定

端末側の設定は、端末の OS やアプリケーションに依存します。例として、Windows 10 における Internet Explorer 11 の設定を紹介します。

1. 「ツール」から「インターネット オプション」を選択する
2. 「インターネット オプション」ダイアログの「接続」タブを選択する
3. 「LAN の設定」を選択する
4. DHCP で PAC ファイル URL 通知を行う場合は、自動構成欄の「設定を自動的に検出する」にチェックする。
   PAC ファイルの URL を直接設定する場合は、自動構成欄の「自動構成スクリプトを使用する」にチェックし、アドレス欄に「http://<IX ルータの IP アドレス>:<ポート番号>/proxy.pac」を入力する。
5. 「OK」を選択して設定を完了する。

上記の設定後、端末は IX ルータ内の PAC ファイルを参照して例外設定に従って動作します。

2.46.6.5 設定例

PAC ファイルを生成して、IX ルータ内の PAC ファイル URL を DHCP で端末に配信する場合の設定例を紹介します。

【設定例】
URL オフロードの例外設定のみを含む PAC ファイルを新規に生成する場合

```
! DHCP で PAC ファイル URL 通知を有効化
ip dhcp profile dhcp-prof
   wpad auto
!
! プロキシサーバのアドレスを指定
url-offload profile urlo-prof
   proxy-config server 192.168.80.80:8080
!
! DHCP と HTTP サーバを有効化
interface GigaEthernet2.0
   description LAN
   ip dhcp binding dhcp-prof
   http-server ip enable
```

【設定例】
既存 PAC ファイルに URL オフロードの例外を追加して PAC ファイルを生成する場合

```
! DHCP で PAC ファイル URL を通知
ip dhcp profile dhcp-prof
   wpad auto
!
! 既存の PAC ファイルを指定
url-offload profile urlo-prof
   proxy-config pac-file http://example.com/proxy.pac
!
! DHCP と HTTP サーバを有効化
interface GigaEthernet2.0
   description LAN
   ip dhcp binding dhcp-prof
   http-server ip enable
```

2.46.7 運用情報

2.46.7.1 アクセスログの取得

Ver9.6 以降、ロギング機能を使用することにより、オフロードされた通信のログを残すことが可能です。なお以下のログを残すには、ロギングレベルを warn ではなく notice に設定する必要があります。

ある宛先に対して最初に通信を始める場合、URLO.024 が表示されます。それ以降の通信では、URLO.025 が表示されます。

プロキシサーバ利用なしの場合、URLO.024 の通信はまだオフロードされておらず、URLO.025 の通信のみがオフロードされています。プロキシサーバ利用構成では、URLO.024 と URLO.025 ともにオフロードされています。

Ver10.6 以降、URLO.24 および URLO.25 を含む一部ログはアプリケーション解析機能のログに移行しました。上記の確認をする場合、アプリケーション解析機能のロギングレベルを notice に設定する必要があります。

【設定例】
logging subsystem urlo notice

【動作例】
12:34:56 URLO.024: Start offload, 192.168.1.1 > 172.16.200.187:443, www.example2.com, profile urlo-prof
12:34:57 URLO.025: Do offload, 192.168.1.1 > 172.16.200.187:443, profile urlo-prof

【設定例】(ver10.6 以降)
logging subsystem apa notice

【動作例】
10:54:27 APA.024: Start offload, 192.168.160.1:63609 > 172.16.200.187:443, www.example2.com, application undefined

10:54:27 APA.025: Do offload, prot tcp, 192.168.160.1:63614 > 172.16.200.187:443, application undefined

2.46.7.2 オフロード対象の取得

オフロード対象の宛先は以下で確認することができます。

- CLI の場合
  show running-config url-list （Ver9.5 以降）
  show url-offload database

  前者のコマンドで、装置内に設定している URL リストの内容を表示します。後者のコマンドで、外部定義ファイルをもとに生成したオフロード用 URL リストを表示します。

- Web コンソールの場合
  URL オフロード（保守管理）（Ver9.6 以降）

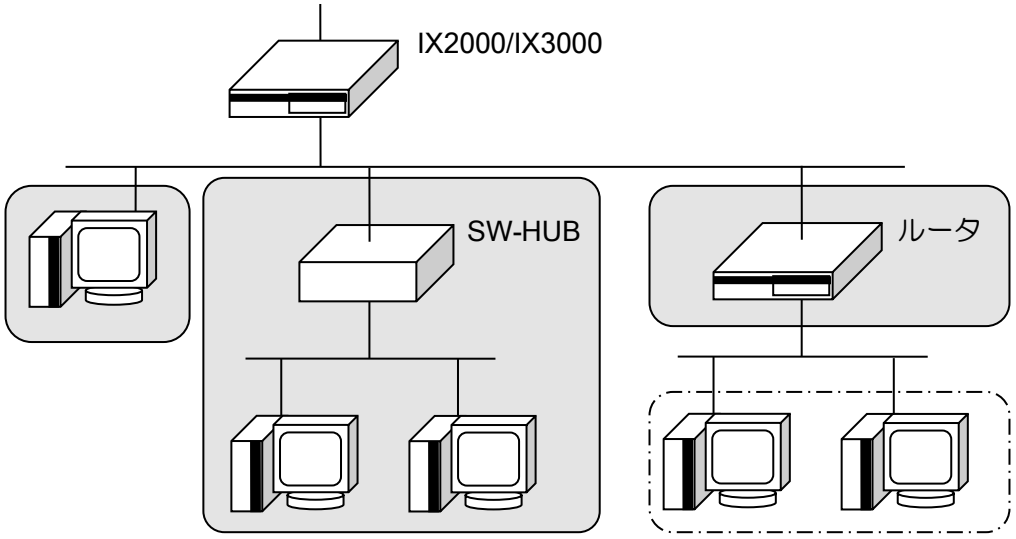
  装置内に設定している URL リストの内容と、外部定義ファイルをもとに生成したオフロード用 URL リストを、合わせて表示します。

■2.47 リンクマネージャの設定

リンクマネージャ機能は、IX ルータにどのような端末が接続されているかを MAC アドレス単位でわかりやすく一覧表示し、制御する機能です。端末をグループ化して説明に日本語のコメントを付与したり、端末単位の通信制御を行うことができます。リンクマネージャ機能は Ver9.5 以降で利用可能です。

2.47.1 機能概要

リンクマネージャ機能は、以下に示す範囲の端末を可視化・制御することができます。



：端末情報の取得が可能な範囲

：端末情報の取得が不可能な範囲

主な機能

- 可視化機能
  - Web コンソール機能で、接続機器一覧を表示できます。
    - 端末ごとの MAC アドレス、IP アドレスや接続・切断状態、通信量などを確認できます。
  - 接続機器は所属や機器種別ごとにグループ化して表示できます。
  - 日本語での設定/表示が可能です（Web コンソール表示時のみ）。

- 制御機能
  - 端末単位で簡単にフィルタリング動作を切り替えられます。
  - 端末単位で端末認証機能を無視する動作を切り替えられます。
    - 無視できる端末認証は、IEEE802.1X 認証・MAC 認証・Web 認証です。

2.47.2 注意事項

- MAC アドレス単位で同一リンク上の接続端末のみを認識します。配下にルータがある場合、ルータの先に存在する端末は表示できません。
- 同一リンク上にルータがある場合、ルータの MAC アドレスが表示されますが、IP アドレスはルータの IP アドレス、または、ルータが転送したパケットの送信元 IP アドレスが表示されます。表示される IP アドレスは通信状態により異なります。
- 端末の接続状態は通信の時間で判定するため、端末との接続状態が変化しても即時反映はされません。IP アドレスや接続インタフェースも一定周期で監視しているため、反映には時間がかかります。監視時間の周期は変更可能です。

2.47.3 Web コンソールからの利用方法

リンクマネージャ機能は、Web コンソール機能で表示や設定の変更が可能です。日本語でわかりやすく表示することができます。詳しい設定方法は、Web 設定マニュアルも参照してください。

2.47.3.1 メインページ

装置に接続されたことがある全ての端末を MAC アドレス単位で表示します。表示内容は以下のとおりです。

端末情報	
メイングループ	メイングループごとにテーブル形式で表示
サブグループ	サブグループ
端末情報	MAC アドレスおよび IP アドレス
説明	任意の説明文（日本語登録可能） 登録なしの場合も DHCP ならホスト名、VendorID を表示
インタフェース	端末との接続を検出したインタフェース(Ver9.5)
インタフェース (ポート番号)	端末との接続を検出したインタフェースと SW-HUB ポート番号(Ver9.6 以降) ※
状態	up（監視周期以内に通信あり）、down（通信なし）
経過時間	最後の状態検出からの経過時間
受信	端末が受信したフレームのバイト数（unicast のみ）
送信	端末から送信したフレームのバイト数
動作	端末と通信するフレームの透過・廃棄 端末認証の無視設定

※ ポート番号は、IX2215、IX2207、IX3315、IX2106、IX2107、IX2235 の SW-HUB ポートに接続した場合のみ、表示します。

テーブルの項目名の▼をクリックすると、その項目でソートすることができます。通信量の多い端末の特定などに利用できます。

各種設定ページへは、このページのボタンから遷移します。

2.47.3.2 基本設定

基本設定では以下の設定が可能です。

リンクマネージャ	有効・無効
初期動作	未登録端末（ゲスト端末）を接続した場合の初期動作 (デフォルト：透過)
メイングループ名	メイングループ名の設定（63 種類設定できます）
サブグループ名	サブグループ名の設定（63 種類設定できます）

端末管理の有効化の対象は Web コンソールで管理している LAN 側インタフェースです。その他のインタフェースで利用する場合はコマンドラインで有効化してください。なお、Web コンソール機能で有効化した場合、arp auto-refresh コマンドも同時に設定されます。

グループ名は端末をグループ化してわかりやすく表示するために登録します。グループはメインとサブの 2 種類用意しています。メイングループで所属や場所を、サブグループで端末の種別を登録するなどの使い分けができます。メイングループの分類が不要な場合、デフォルトの「登録済み」を利用してください。

グループ名には日本語も登録可能です。全角 10 文字以内を目安に設定してください。

2.47.3.3 端末情報の追加・編集

端末情報の追加および編集を行います。端末を登録済みのグループに分類したり、説明文を付与することができます。接続済みの端末は、IP アドレス、DHCP 接続時はホスト名、ベンダ情報なども参照して設定できます。

説明文には日本語も登録可能です。全角 16 文字以内を目安に設定してください。

グループの設定	
選択	設定変更の必要/不要
端末情報	MAC アドレスおよび IP アドレス
説明	上段：ホスト名、VendorID (不明の場合はハイフン(-)) 下段：任意の説明文（日本語登録可能）
メイングループ	登録したメイングループ名
サブグループ	登録したサブグループ名
インタフェース	端末が接続している(接続していた)インタフェース
インタフェース (ポート番号)	端末との接続を検出したインタフェースと SW-HUB ポート番号(Ver9.6 以降) ※
状態	up（監視周期以内に通信あり）、down（なし）
経過時間	最後の状態検出からの経過時間
動作	端末と通信するフレームの透過・廃棄
端末認証なし	端末認証の無視設定

※ ポート番号は、IX2215、IX2207、IX3315、IX2106、IX2107、IX2235 の SW-HUB ポートに接続した場合のみ、表示します。

端末数が 100 を超えた場合は一度に表示されません。端末を表示している表の右上に表示範囲を示していますので、101 以降の端末設定を変更したい場合はここから選択してください。

2.47.3.4 端末情報一括取得（CSV 形式）

メインページで表示グループを全てにしている場合、端末情報の右上にある「端末情報を CSV 形式で表示」ボタンから、すべての端末情報を CSV 形式で表示するページに遷移できます。

Ver9.7 以降で Option 情報にて、端末認証の無視設定が追加されました。

2.47.3.5 端末情報一括登録 (Ver9.6 以降)

Ver9.6 以降、「端末情報一括取得」で取得した情報や、CSV 形式で作成したテキストデータを利用し、端末情報を一括で登録することができます。

設定ページへは、メインページの「端末情報を CSV 形式で追加」ボタンから遷移できます。

本機能を利用する場合、グループ名や説明文(Description)にカンマ(,)を設定しないでください。

また、グループ名の設定は反映されないため、以下の方法でグループを設定してください。

- 「端末管理」の「リンクマネージャ」で、グループ名を設定する。
- 「保守管理」の「任意コマンドの実行」から、グループ設定のコンフィグを反映する。

自身で作成した CSV 設定を反映する場合、以下に示す CSV ヘッダ情報と端末情報を必ず記載してください。

また、CSV ヘッダ情報は端末情報より先に記載してください。

記載形式は、「端末情報一括取得」で取得できる情報、および、【設定例】を参照してください。

CSV ヘッダ情報	
MG	メイングループ番号の CSV ヘッダ
SG	サブグループ番号の CSV ヘッダ
MAC Address	MAC アドレスの CSV ヘッダ
Description	説明文の CSV ヘッダ
Action	透過・廃棄設定の CSV ヘッダ
Option	オプションの CSV ヘッダ（省略可）

CSV ヘッダ情報の文字列は、大文字/小文字に関係なく完全一致した場合のみ、CSV ヘッダ情報と判断します。

ただし、MAC アドレスヘッダは、MAC と Address 間の空白(スペース)の有無(MACAddress や MAC Address など)に関係なく、CSV ヘッダ情報と判断します。

同一の CSV ヘッダ情報が複数存在する(MG ヘッダが 2 つ以上あるなど)場合、最後に取得した CSV ヘッダ情報を使用します。

端末情報	
メイングループ番号	登録するメイングループ番号 範囲：1 ～ 63
サブグループ番号	登録するサブグループ番号 範囲：0 ～ 63
MAC アドレス	登録する MAC アドレス
説明文(Description)	任意の説明文（日本語登録可能） 全角 16 文字以内を目安に設定してください。
透過・廃棄設定	登録する透過・廃棄設定 透過：permit / 廃棄：deny
オプション	有効にするオプションの設定 （Option ヘッダがある場合のみ有効） 端末認証の無視：ignore-auth

以下の場合、設定の反映に失敗しますので、注意してください。

- CSV ヘッダ情報の要素数よりも端末情報の要素数が少ない場合
- 範囲外の値を設定した場合
- スペルミスや入力形式外の設定をした場合
- 禁止文字列(“ 二重引用符、 , カンマ)は設定しないでください。
- 最大登録数を超える設定を行った場合

自身で作成した CSV 設定例は以下のとおりです。

【設定例】

```
MG,SG,MAC Address,Description,Action
1,1,00:11:22:33:44:55,sample,permit
2,2,11:22:33:44:55:66,”サンプル”,deny
3,3,22:33:44:55:66:77,,deny
```

2.47.3.6 端末情報確認ページ (Ver9.6 以降)

monitor 権限で、全端末情報のダウンロードとグループごとに端末情報の確認ができます。

ページへは、『利用者メニュー』の『リンクマネージャ』から遷移できます。

また、administrator 権限からも『保守管理』の『リンクマネージャ』から同様のページに遷移できます。

本ページでグループごとの端末情報を確認する場合、リンクマネージャ機能を有効化してください。無効状態では、端末情報の表示はできません。ただし、全端末情報のダウンロードは可能です。

本ページでは、端末情報(『メインページ』と同様の内容)に加え、以下の設定・確認が可能です。

- Wake on LAN 機能
  - ✧ 端末が down 状態の場合に、Wake on LAN 機能にて指定端末を起動することが可能です。
- 統計情報の初期化、初期化からの経過時間の表示
  - ✧ グループ単位で、統計情報の初期化が可能です。
  - ✧ 経過時間から一定時間内での通信量の確認が可能です。
  - ✧ 経過時間を表示する場合、一度表示を行うグループで統計情報を初期化する必要があります。
- 自動更新機能
  - ✧ 一定間隔で、表示情報を最新の状態に更新します。
  - ✧ ページ遷移、ページの再読込、統計情報の初期化を行った場合、自動更新は停止します。

2.47.4 コマンドラインでの利用方法

以下のコマンドでリンクマネージャ機能を有効化します。

linkmgr enable	リンクマネージャ機能の有効化
arp auto-refresh	ARP による接続監視

端末の状態は通信の有無で判定するため、arp auto-refresh 機能との併用を推奨します。
また、リンクマネージャ機能を有効化するだけでも自動収集した端末情報を表示できますが、各端末のグループ化や説明の追加、受信動作の変更などを行う場合は、以降の設定を行ってください。

2.47.4.1 グループの登録

グループの登録は端末管理プロファイルで行います。

linkmgr profile	端末管理プロファイルの作成
group-main	メイングループ名の設定
group-sub	サブグループ名の設定

グループ名は日本語入力/表示に対応していますが、コマンドラインからは日本語は設定できません。ascii を指定して半角文字で登録してください。日本語の入力と表示は Web コンソールで行ってください。

【設定例】

```
linkmgr profile
  group-main 1 ascii Group1
  group-main 2 ascii Group2
  group-sub 1 ascii pc
  group-sub 2 ascii printer
```

2.47.4.2 端末情報の登録

端末情報の登録は、端末情報プロファイルで行います。

linkmgr terminal	端末情報プロファイルの作成
terminal	端末情報の設定

説明文は日本語入力/表示に対応していますが、コマンドラインからは日本語は設定できません。ascii を指定して半角文字で登録してください。日本語の入力と表示は Web コンソールで行ってください。

【設定例】

```
linkmgr terminal group-main 1 group-sub 1
terminal 00:00:00:00:00:01 permit desc-ascii user1
terminal 00:00:00:00:00:02 permit desc-ascii user2

! プリンタは、端末認証を行わない
linkmgr terminal group-main 1 group-sub 2
terminal 00:00:00:00:00:03 permit ignore-auth desc-ascii printer1
```

2.47.4.3 端末情報の表示

端末情報は以下のコマンドで確認可能です。

show linkmgr terminal	端末情報の表示

【表示例】

```
Ver.9.6 以降
Router(config)# show linkmgr terminal
Link Manager Table - 4 entries, 4092 free, 0 overflows
Elapsed time after clear counters : 10d 01:43:39(group-main 1)
Codes: D - Deny, P - Permit
   MG/SG MAC Address       IP Address          State                Interface
D 01/01    00:00:00:00:00:01 192.0.2.1          up (00:02:46)        GigaEthernet2.0(1)
      In: 0 bytes, Out: 600 bytes
      Desc: user1
      DHCP Info: -
P 01/01    00:00:00:00:00:02 192.0.2.2          up (00:04:35)        GigaEthernet2.0(2)
      In: 135164 bytes, Out: 92590 bytes
      Desc: user2
      DHCP Info: samplePC(MSFT 5.0)
P 01/02    00:00:00:00:00:03                    down (01:07:38)      GigaEthernet1.0
      In: 3219 bytes, Out: 2193 bytes
      Desc: printer1
      DHCP Info: -
D 02/00      00:00:00:00:00:04                  down (--:--:--)      -
      In: 0 bytes, Out: 0 bytes
      Desc: -
      DHCP Info: -
```

Ver.9.5 の場合、Elapsed time after clear counters：の表示および、SW-HUB ポート番号表示はありません。

- Elapsed time after clear counters：10d 01:43:39(group-main 1)　(Ver9.6 以降)
  - ✧ 統計情報の初期化(clear linkmgr statistics コマンド)を実行してから経過した時間です。( )内には、初期化した対象を表示します(ゲスト：guest、グループ単位：group-main X) 。全端末の統計情報を初期化した場合や 1 度も統計情報の初期化を行っていない場合、経過時間のみを表示します。
- MG/SG
  - ✧ メイングループとサブグループの番号です。未登録の場合 00 を表示します。
- MAC Address / IP Address
  - ✧ 登録している端末の MAC アドレス および IP アドレスです。
- State
  - ✧ 端末の接続状態です。通信検出時に up、5 分間（デフォルト）の無通信で down です。
- Interface
  - ✧ 接続インタフェースを表示します。
  - ✧ IX2215、IX2207、IX3315、IX2106、IX2107、IX2235 の SW-HUB に接続した場合、接続しているポート番号を表示します。(Ver9.6 以降)
- In: 0 bytes, Out: 600 bytes
  - ✧ 端末視点の通信量です。In は端末が受信したサイズ、Out は端末が送信したサイズです。
- Desc
  - ✧ terminal コマンドで設定した端末の説明です。
  - ✧ 日本語で設定されている場合は BASE64 形式に変換されて表示されます。
- DHCP Info
  - ✧ DHCP 機能で保持している端末のホスト名/ VendorID を表示します。

2.47.4.4 切断判定時間の設定

リンクマネージャ機能では、端末の接続/切断状態を通信の有無で判定します。
切断状態と判定するまでの無通信時間はデフォルト 5 分で、以下のコマンドで変更できます。

connect-timeout	端末切断判定時間の設定 (端末管理コンフィグモード)

※ 更新周期の設定(refresh-interval コマンド)以上の値を設定してください。

2.47.4.5 更新周期の設定

リンクマネージャ機能では、IP アドレスおよび接続インタフェース情報を、一定の時間間隔で更新します。更新周期は、以下のコマンドで設定できます。

refresh-interval	端末情報更新周期の設定 (端末管理コンフィグモード) (デフォルト： 5 分)

※ 切断判定時間の設定値(connect-timeout コマンド)以下の値を設定してください。
※ 更新周期経過後に端末からフレームを受信したタイミングで更新を行います。

2.47.4.6 クリアコマンド

統計情報の消去やゲスト端末の削除などは、以下のコマンドで実行します。

clear linkmgr refresh-interval	端末情報の強制更新
clear linkmgr statistics	端末の統計情報の消去
clear linkmgr terminal	端末情報（ゲスト端末）の消去

※ 強制更新は次フレーム受信時に必ず情報が更新されるようにするコマンドです。コマンド実行時に全ての情報が更新されるわけではありません。

2.47.5 主な利用方法

リンクマネージャ機能の主な利用方法について説明します。

2.47.5.1 通常利用

メイングループで場所や所属を、サブグループで端末の種別（PC やプリンタなど）を登録し、端末情報を登録します。先に端末を接続できる場合は MAC アドレスを自動的に検出するので、グループの選択と説明文の付与だけで設定できます。端末が DHCP 接続の場合は、端末のホスト名やベンダ情報などを収集するので、それらを参照しながら設定可能です。

なお、グループを利用する予定がなく、説明文のみ設定したい場合は、デフォルトで用意している「登録済み」のグループを選択してください（設定の保存にはグループの選択が必須です）。

2.47.5.2 登録端末のみ通信可能なセキュアネットワークの構築

通信を許可する全ての端末を登録し、未登録端末の通信を全て廃棄に設定することで、セキュアなネットワークを構築できます。

端末情報を 1 つ 1 つ登録する代わりに、以下のような手順で登録することも可能です。Web コンソールのみでも実施できます。

1. 一定期間内に、登録する端末を 1 度はルータと接続するように利用者に依頼する。
2. 「デフォルト動作」を透過に設定して、端末情報を収集する。
3. 一定期間後に「デフォルト動作」を廃棄に設定する。
4. DHCP のホスト名などの情報を参照しながら適切なグループに振り分ける。
5. 以降は利用者からの申請ごとに MAC アドレスを追加する。

2.47.5.3 端末認証との併用 (Ver9.7 以降)

端末認証と併用する場合、特定の端末を端末認証の対象外とすることができます。

これにより既知の端末は端末認証を行わず、ゲスト端末のみ端末認証を行うことが可能です。

2.47.6 リンクマネージャの通信制御機能 (Ver.9.6 以降)

リンクマネージャのグループ番号を IPv4 / IPv6 アクセスリストおよび、MAC アクセスリストの判定条件として設定が可能です。

これにより、アクセスリストを利用する機能(フィルタ/QoS/ポリシールーティング)で、リンクマネージャのグループ毎に条件の設定ができます。

2.47.6.1 設定方法

リンクマネージャのグループ番号をアクセスリストの判定条件に設定する場合、以下のコマンドで設定が可能です。

アクセスリストの詳細については、アクセスリストの項目を参照してください。

【設定例】

```
ip access-list list1 deny ip src any dest any linkmgr mg 0          -(1)
ip access-list list1 deny ip src any dest any linkmgr sg 1          -(2)
ip access-list list1 deny ip src any dest any linkmgr mg 1 sg 2   -(3)
```

(1)：ゲスト端末のパケット通過拒否
(2)：サブグループが 1 の端末のパケット通過拒否
(3)：メイングループ 1 サブグループが 2 の端末のパケット通過拒否

IPv6 アクセスリスト、MAC アクセスリストにも同様の設定が可能です。

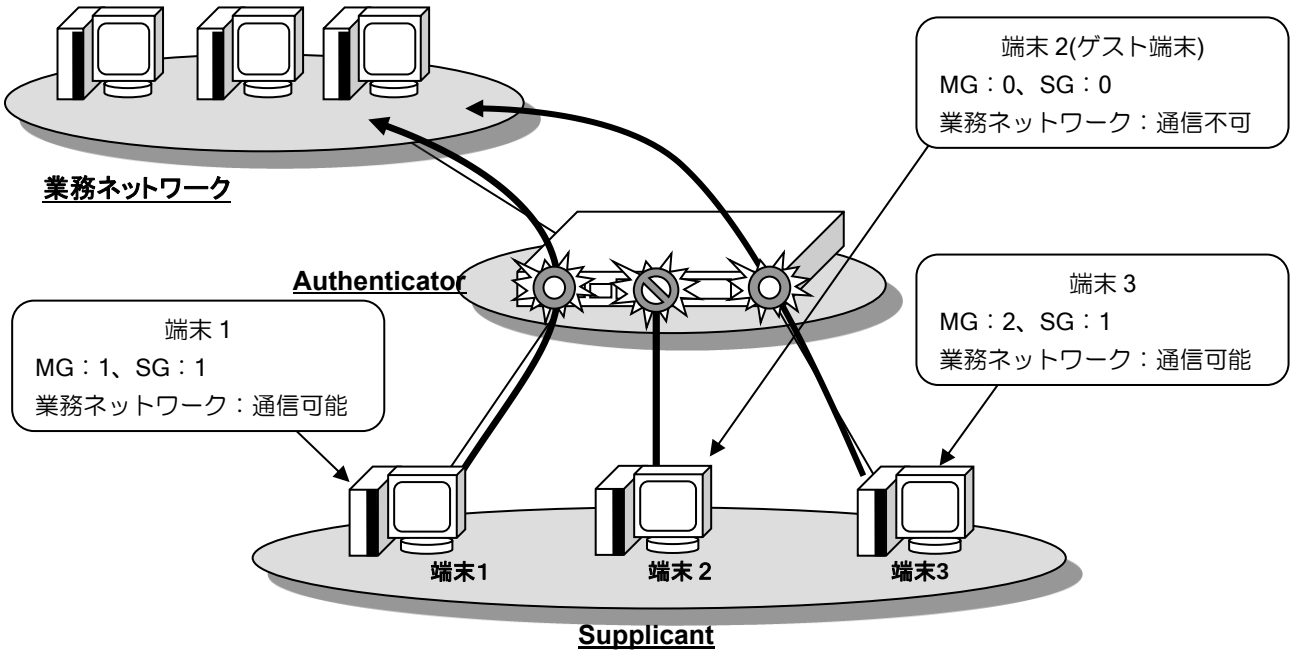
各パラメータで設定可能な範囲は以下のようになります。

パラメータ	
MG	メイングループ番号 範囲：0 ～ 63　(0 はゲスト端末になります)
SG	サブグループ番号 範囲：0 ～ 63

2.47.6.2 IP フィルタによる通信制御

アクセスリストにリンクマネージャのグループ番号を設定し、IP フィルタ機能の条件として設定することで、特定のネットワークやサーバへの接続をグループ単位で制御できます。

また、フィルタを受信(in)側や送信(out)側に設定することで、グループ単位で接続できるネットワークを制御することができます。

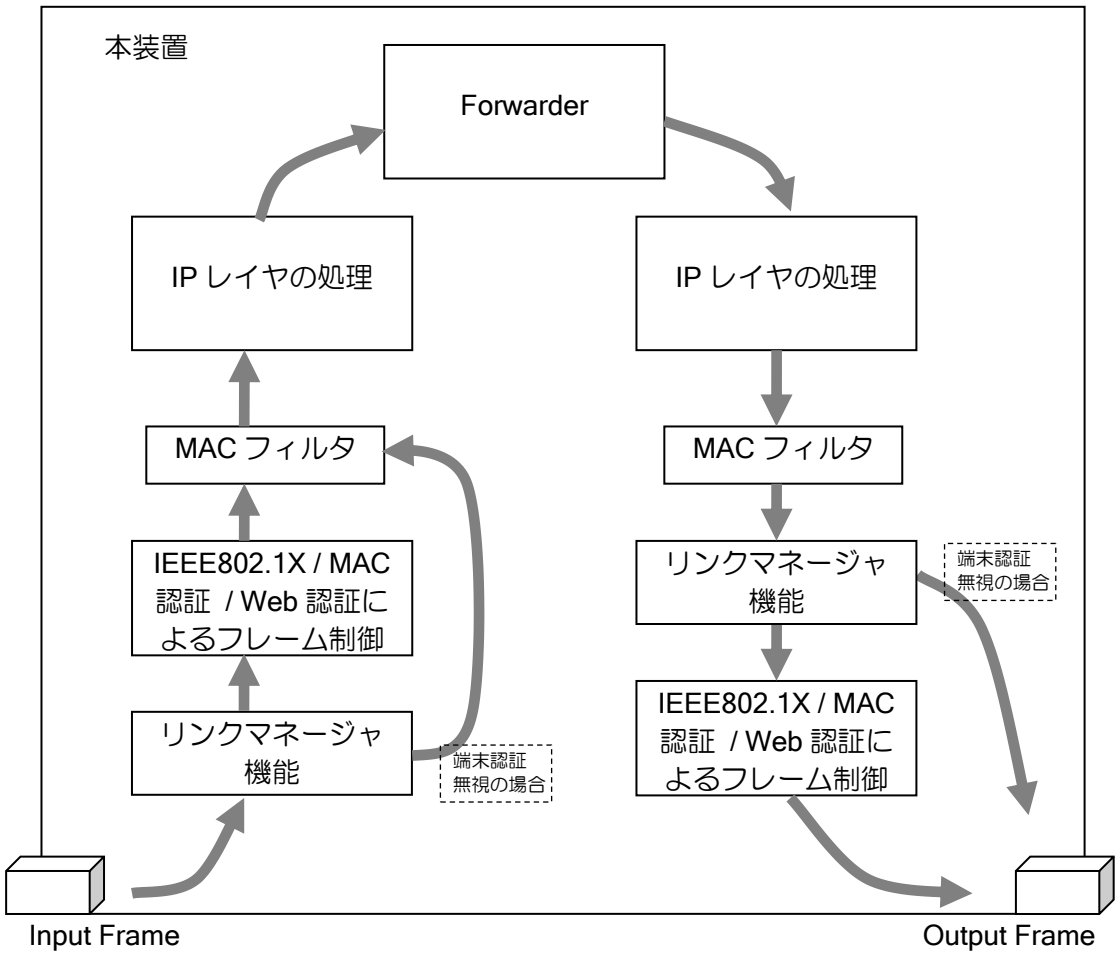


【設定例】

```
!
ip access-list list1 deny ip src any dest any linkmgr mg 0 sg 0 //ゲスト端末の通信を拒否
ip access-list list1 permit ip src any dest any linkmgr mg 1 //MG1 の通信を許可
ip access-list list1 permit ip src any dest any linkmgr mg 2 //MG2 の通信を許可
!
interface GigaEthernet0.0   //業務ネットワーク
  ip address 203.0.113.1/24
  no shutdown
!
interface GigaEthernet1.0 // LAN 側
  ip address 192.168.1.254/24
  linkmgr enable
  ip filter list1 1 in
  no shutdown
!
```

2.47.7 処理順序

MAC フィルタや認証機能と併用した場合の処理順序は以下のとおりです。



■2.48 NetMeister の設定

NetMeister は、IX2000/3000 シリーズ等のネットワーク機器管理をクラウド上で提供するサービスです。企業・団体等の管理体ごとに、対応しているネットワーク機器を一元管理することができます。NetMeister の詳細については、以下の URL を参照してください。

https://www.necplatforms.co.jp/product/netmeister/

また、NetMeister の操作方法などは以下の URL を参照してください。

https://support.necplatforms.co.jp/netmeister/manual/

NetMeister では主に以下のサービスが利用できます。利用料金は NetMeister Prime の機能を除き、無償となります。

バージョン	サービス	概要
Ver9.7 以降	ダイナミック DNS	ダイナミック DNS
Ver10.0 以降	装置管理	装置情報や接続状態・アラームの確認
	拠点管理	拠点単位での状態確認
	アラーム通知 (†)	装置アラームの通知・表示
	メール送信	アラームやファームウェア更新のメール通知
	アクション実行 (†)	ファームウェア更新（即時・時刻指定） コンフィグ、show tech-support 取得
	デバイスリスト (†)	装置の接続機器情報の管理
	NGN 閉域網での利用	装置管理やダイナミック DNS が利用可能 (Ver10.0 では一部制限があります)
Ver10.1 以降	アラーム通知拡張	電源、ネットワークモニタ、リンクダウンアラーム
	UTM 統計レポート	UTM 機能で検出のネットワーク上の脅威表示
	アクション実行拡張 (†)	任意コマンド実行、再起動、コンフィグ保存
	デバイスマップ (†)	装置の接続機器情報の可視化
	コンフィグ管理 (†)	コンフィグ情報の管理・反映機能
	URL オフロード拡張 (‡)	URL オフロードの URL を編集・管理する機能
	他機種収容 (†)	他機種を NetMeister 接続子機として収容
Ver10.2 以降	UTM 脅威分析 (†)	UTM 機能で収集したログ情報表示
	リモートログイン (‡)	装置や NetMeister 接続子機への外部アクセス
	ダイナミック VPN 設定 (‡)	ダイナミック VPN を設定・管理する機能
Ver10.3 以降	メトリクス (†)	トラフィックや CPU 使用率などの表示
	ポート情報 (†)	ポート状態や LED の表示
	NTT 東西自動判別機能	NTT の回線を自動で判別する機能
Ver10.4 以降	アラーム管理拡張	不正端末検知アラーム
	デバイスマップ拡張 (†)	端末の削除や、不明 MAC の通信不許可
	他機種収容拡張 (†)	子機として収容した他機種の死活監視
Ver10.5 以降	URL オフロード拡張 (‡)	Teams/Skype/Zoom/WebEX に対応
	リモートログイン拡張 (‡)	接続許可アドレスの任意指定など
	NetMeister Prime	Wake on LAN や任意 IP アドレスの死活監視などの有償サービス
Ver10.6 以降	アプリケーション解析機能(‡)	アプリケーション単位での通信振り分け、UTM 除外設定など（NetMeister Prime の機能）
	Find Your Device	装置特定のために LED を一定時間点滅
	リモートログイン拡張 (‡)	LAN 側からのリモートログインに対応
	NGN 閉域網での利用の拡張	子機の NGN 閉域網利用に対応

Ver10.7 以降	イベントログ送信機能　(‡)	イベントログ情報を定期的に送信する機能 （NetMeister Prime の機能）
	回線冗長機能	冗長用の回線を設定する機能

†/‡　一部環境では利用できない場合があります（次ページ「利用環境」を参照してください）

2.48.1 利用方法

NetMeister は、事前にユーザーアカウントと管理対象のグループアカウントの登録が必要です。
次の URL にアクセスして登録を行ってください。

https://www.nw-meister.jp/service/

ユーザーアカウントの登録には、メールアドレス、氏名、会社名、電話番号の登録が必要です。

2.48.2 利用環境

利用環境により、利用できる機能が異なります。

項目	インターネット （IPv4）	インターネット （IPv6）	NGN 閉域網
ダイナミック DNS	○	○	○
基本保守機能 (前ページの†以外の機能）	○	△ (*)	○
基本保守機能 (前ページの†の機能)	○	△ (*)	△ (*)
リモートログイン	○	×	×
URL オフロード拡張 アプリケーション解析機能	○	×	△ (*)
ダイナミック VPN 設定	○	×	×
イベントログ送信機能	○	△ (*)	△ (*)

* IPv4 インターネットへの経路がある場合、△になっている機能も利用可能です。
　一部、MQTT 通信ができる必要があります

- NetMeister との通信では、HTTPS(TCP/443)と MQTT(TCP/8883)を使用しています。
  また、一部の通信は設定にかかわらず IPv4 で行います。また、MQTT 通信は SSL インスペクションを行うプロキシ環境では使用することができません。
- nm mqtt port 設定で、MQTT(TCP/443)にすることもできます (Ver10.1 以降)。
- nm proxy の設定がある場合､MQTT をプロキシ経由で接続することができます (Ver10.2 以降)。
- ファイヤウォール等を利用している場合は、上記通信を許可してください。
- NetMeister サーバとの通信は、IP フィルタ機能、URL フィルタリング および URL オフロード機能で、廃棄されません (Ver10.4 以降)。
- ダイナミック DNS 機能のご利用には、
  管理対象装置にグローバル IP アドレスが付与されている必要があります。1 つのグローバル IP アドレスを複数の装置で共用している環境では、ダイナミック DNS 機能は利用できません。
- リモートログイン機能のご利用には、
  同じグループ内の装置に IPv4 グローバルアドレスが付与されている必要があります。
- URL オフロード拡張のご利用は、
  URL オフロード機能自体が IPv6(NGN 閉域網含む)に未対応ですのでご注意ください。
- ダイナミック VPN 設定は、IPv6(NGN 閉域網含む)に未対応です。
  WebUI では、NGN 閉域網でのダイナミック VPN の設定が可能です。
- Ver10.6 より、NGN 閉域網内の IPv6 通信量を軽減するため、一部の通信が IPv4 を利用するようになりました。このため、NGN 閉域網へ接続している環境でアラームとメトリクスを利用す

るには、IPv4 インターネットの併用または prime での NGN 閉域網コントロールの利用が必要になります。

2.48.3 注意事項

- 登録時に利用規約と個人情報の取り扱いをよくご確認ください。
- 無償提供のため、高頻度にログを収集するなどの過度な利用はご遠慮ください。
- パスワードは他のサービスと併用せず、強度の高いパスワードを設定してください。
- 各サービスは初期状態で有効です。Ver10.0 以降、ダイナミック DNS やアラーム管理を無効化することができます。
- 本機能はクラウドサーバ上で機器を管理するために、基本情報として次の情報を通知します。
  - シリアル番号、MAC アドレス、機種名、バージョン、IP アドレス、ホスト名
- デバイスリストでは、次の情報を通知します。
  - MAC アドレス、IP アドレス、接続状態

2.48.4 基本設定

NetMeister のグループ登録ページで設定した、以下の情報をルータの設定で使用します。

- ネットワーク機器の管理体を特定するための「グループ ID」
- ネットワーク機器が情報更新時に使用する「グループパスワード」

NetMeister の設定は、主に以下のコマンドで行います。

nm ip enable （nm ipv6 enable）	NetMeister 機能の有効化 （NGN 閉域網では ipv6 を指定）
nm account	グループアカウントの設定 （グループ ID とグループパスワードの設定）
nm sitename	拠点 ID の設定（Ver10.0 以降）
hostname	ホスト名（装置名）
nm update	即時更新
show nm information	NetMeister 情報の表示
show nm statistics	NetMeister 統計情報の表示（Ver10.1 以降）

【設定例】

```
hostname tokyo-rt1

nm ip enable
nm account “グループ ID” password plain “グループパスワード”
nm sitename tokyo
```

Web コンソール機能でも基本設定を行うことが可能です。かんたん設定（Ver10.0 以降）や詳細設定の NetMeister のページで設定を行ってください。Web コンソール機能では nm ipv6 enable の設定はできません。

グループ ID とグループパスワードは、事前に登録したものを設定してください。

ホスト名

グループ内で一意になるように設定してください。任意の文字が利用可能ですが、ダイナミック DNS 機能を利用される場合でドメインに利用できない文字列を設定している場合は、別途ダイナミック DNS のホスト名を変更するコマンドを設定してください。

拠点 ID

拠点保守機能の利用に必須の設定です。クラウド上での設定は必要ありません。

なお、運用中に設定を変更した場合は、設定変更時に必ず nm update コマンドを実行して設定を反映させてください。Web コンソール機能で設定した場合は、自動的に実行します。

2.48.4.1 WAN・LAN インタフェースの指定

WAN インタフェースおよび LAN インタフェースを指定する場合、以下の設定を行います。

Ver.10.6 以降では下記で設定することができます。

```
【設定例】

system information wan 1 GigaEthernet0.0
system information lan 1 GigaEthernet2.0
```

Ver.10.5 以前では下記で設定することができます。

```
【設定例】

web-console system information
  o lan1 GigaEthernet0.0
  o wan1 GigaEthernet2.0
```

2.48.4.2 送信インタフェース、送信元アドレスの指定

NetMeister 接続に使用される送信インタフェースおよび送信元アドレスを指定する場合、以下の設定を行います。

nm outgoing-interface	送信インタフェース指定（Ver10.3 以降）
nm source-address	送信元アドレス指定（Ver10.2 以降）

※ Ver10.6 以前では送信インタフェース指定は、IPv4 の NetMeister 送信にのみ適用されます。Ver10.7 からは IPv6 の NetMeister 送信にも適用されます。

※ 送信インタフェースを指定した場合は、送信元アドレスも同時に指定してください。（送信インタフェースが指定されており経路情報が不足している場合、同時に送信元アドレスが指定されていないと NetMeister 通信に失敗します）

2.48.4.3 デバイスリスト・デバイスマップ設定

デバイスリスト・デバイスマップを利用する場合、LAN インタフェースでリンクマネージャの有効化が必要です。

また、NetMeister のサービスにてデバイスリストを使用するサービスがあります。利用する場合、本機能を有効化してください。

linkmgr enable	リンクマネージャ有効

2.48.4.4 動作確認

管理サーバ上で正しく登録されていることを確認してください。
登録状況は、以下のように show nm information コマンドでも確認できます。

【表示例】

```
NetMeister Client:
  Result      : Success (20000)
  Last Request: 2018/01/01 23:59:59
  Next Request: 2018/01/09 15:44:46 (remain 9999 sec)
Information:
  IPv4 Address: <通知した IP アドレス>
  IPv4 Domain : <通知した IPv4 ドメイン>
  IPv6 Address: <通知した IPv6 アドレス>
  IPv6 Domain : <通知した IPv6 ドメイン>
  NGN Access  : NTT EAST
  ErrorCode1  :
  ErrorCode2  :
  Interval    : 168 hours
API-GW:
  gpid        : sample-id
  stid        : sample-site
  htid        : 406186deadbc
  Interval    : 3600 sec
  Next Request: 2018/01/02 00:59:59 (remain 2999 sec)
  Status      : Registered
  Detail      :
    wanif     : GigaEthernet0.1
    lanif     : GigaEthernet2:1.0, GigaEthernet2:2.0
    https     : enable
    ssh       : enable
MQTT:
  Interval    : 60 sec
  Status      : Connected
```

通信が成功しない場合は以下をご確認ください。

ErrorCode1 が 550 の場合はアカウントエラー（グループ ID が存在しない）。
ErrorCode1 が 551 の場合はパスワードエラー（グループパスワードが不一致）。
ErrorCode1 が 001 の場合はダイナミック DNS が無効。
ErrorCode1 が上記以外の場合や、Result が Failure の場合は、サーバとの通信失敗です。

API-GW の Status が Registered でない場合、Ver10.0 以降のサービスが利用できません。
MQTT の Status が Connected でない場合、基本保守機能の一部が利用できません。

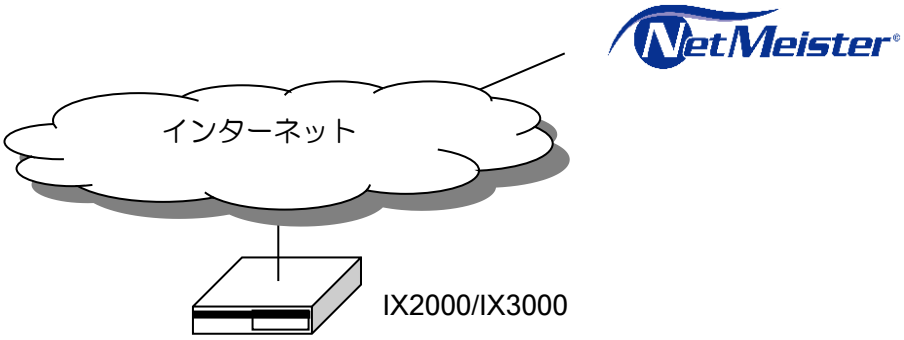
2.48.5 NetMeister との接続

NetMeister との接続構成と設定例について説明します。

サーバの名前解決をおこなうため、本装置で DNS サーバ指定の設定が必要です。
デバイスリストの利用のために、リンクマネージャ機能の有効化が必要です。

2.48.5.1 インターネット接続

IX2000/3000 をインターネットに直接接続する構成です。
Ver9.7 まではこの構成のみ、NetMeister と接続できます。

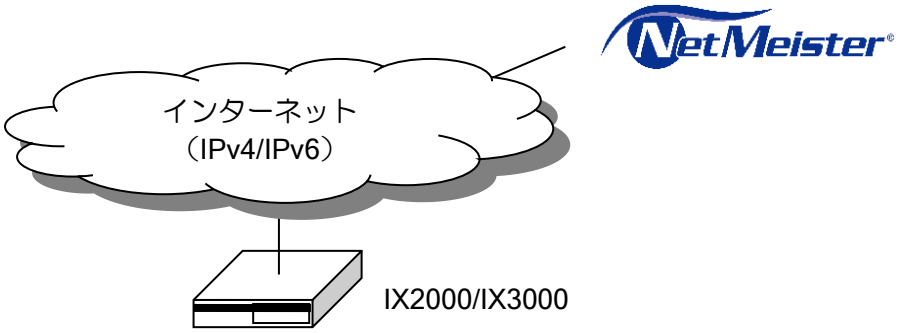


【設定例】
IX2000/3000 をインターネットに直接接続

```
hostname tokyo-rt1

nm ip enable
nm account example-gp1 password plain example-pass1
nm sitename tokyo

ip name-sever 10.0.0.1

interface GigaEthernet0.0
   ip address 172.16.1.1/29
   ip napt enable
   no shutdown

interface GigaEthernet2.0
   description LAN
   ip address 192.168.0.254/24
   linkmgr enable
   no shutdown
```

2.48.5.2 IPv4/IPv6 デュアル環境

IX2000/3000 を IPv4/IPv6 でインターネットに接続する構成です。
NetMeister に接続するプロトコルとして、IPv4、または IPv6 のどちらかを設定します。
NetMeister の接続に IPv6 を設定した場合、基本保守機能を利用するために、IPv4 を使用します。
IPv6 のみの環境では、基本保守機能は利用できません。

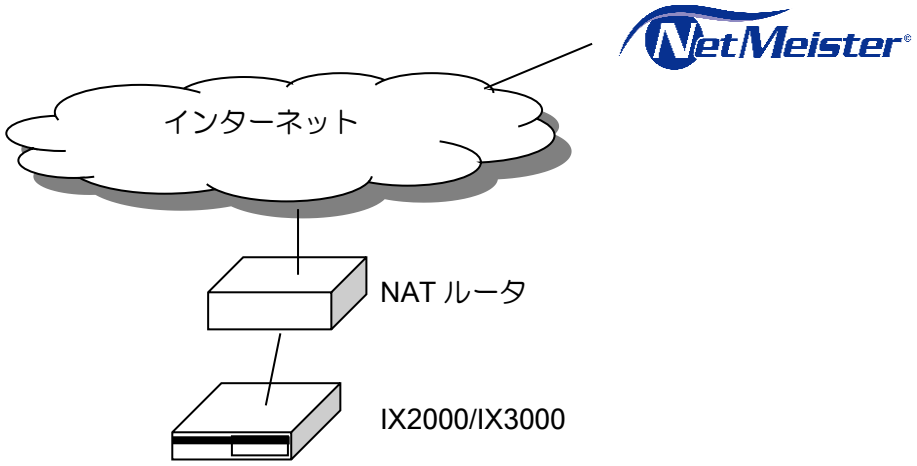


【設定例】
IX2000/3000 をインターネットに直接接続
IPv6 を使用して NetMeister に接続

```
hostname tokyo-rt1

nm ipv6 enable
nm account example-gp1 password plain example-pass1
nm sitename tokyo
nm ddns notify interface GigaEthernet0.1 protocol ip
nm ddns notify interface GigaEthernet0.0 protocol ipv6

ppp profile pppoe
  authentication myname test@example.com
  authentication password test@example.com test

ipv6 dhcp client-profile get-dns
  information-request
  option-request dns-servers

interface GigaEthernet0.0
  ipv6 address autoconfig receive-default
  ipv6 dhcp client get-dns
  no shutdown

interface GigaEthernet0.1
  encapsulation pppoe
  auto-connect
  ppp binding pppoe
  ip address ipcp
  ip napt enable
  no shutdown

interface GigaEthernet2.0
  description LAN
  ip address 192.168.0.254/24
  linkmgr enable
  no shutdown
```

2.48.5.3 NAT 経由の接続

IX2000/3000 から NAT を経由して NetMeister に接続する構成です。
ダイナミック DNS へは NAT ルータの WAN アドレスが登録されます。
※NAT の配下に複数の IX2000/3000 が存在する場合は、ダイナミック DNS は利用できません。
登録されるダイナミック DNS アドレスが NAT のアドレスとなるため

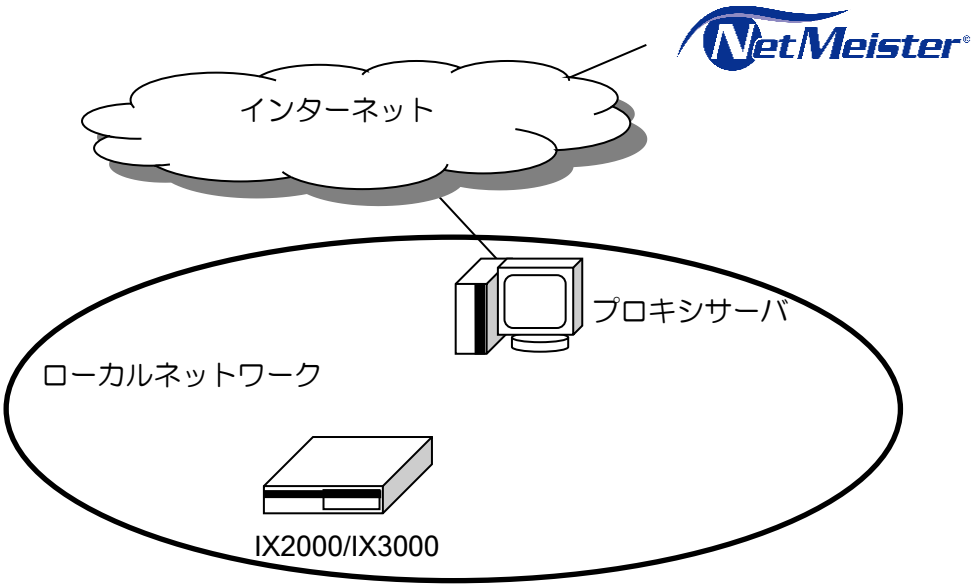


【設定例】
NAT 経由で NetMeister に接続

```
hostname tokyo-rt1

nm ip enable
nm account example-gp1 password plain example-pass1
nm sitename tokyo
nm suppress-feature ddns

interface GigaEthernet0.0
   ip add dhcp receive-default
   no shutdown

interface GigaEthernet2.0
   description LAN
   ip address 192.168.0.254/24
   linkmgr enable
   no shutdown
```

2.48.5.4 プロキシ経由の接続

プロキシサーバを通して NetMeister に接続する構成です。（Ver10.0 以降）
プロキシサーバ設定により、プロキシサーバを通して NetMeister に接続することができます。
プロキシサーバ経由の環境では、ローカルネットワークとインターネットの接続に NAT を使用するため、ダイナミック DNS 機能は利用できません。



設定は以下のコマンドで行います。

nm proxy	プロキシサーバ設定

【設定例】
プロキシサーバに http://example.com:8080 を使用して NetMeister に接続

```
hostname tokyo-rt1

nm ip enable
nm account example-gp1 password plain example-pass1
nm sitename tokyo
nm proxy http://example.com:8080
nm suppress-feature ddns

interface GigaEthernet0.0
   ip address dhcp receive-default
   no shutdown

interface GigaEthernet2.0
   description LAN
   ip address 192.168.0.254/24
   linkmgr enable
   no shutdown
```

2.48.5.5 NGN 閉域網対応

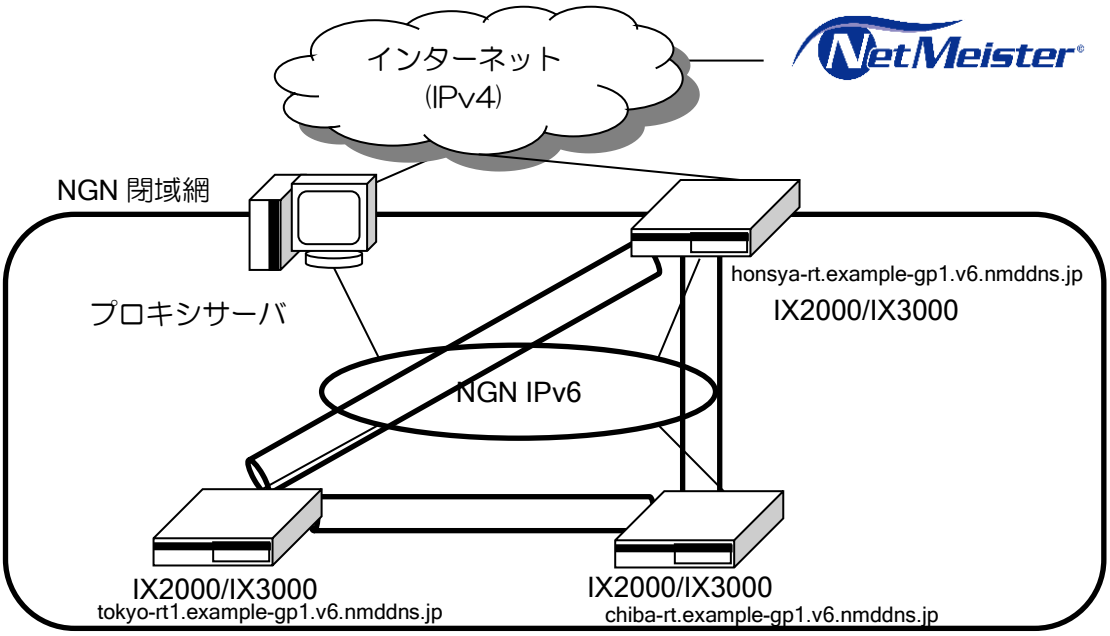
IX2000/3000 を NGN 閉域網内に設置している場合の構成です。

NGN 閉域網内の IPv6 環境において、ダイナミック DNS 機能を利用することができます。
ダイナミック DNS には、IX2000/3000 の IPv6 アドレスを登録します。
登録したホスト名を使用して NGN 閉域網内の VPN 接続ができます。
nmddns.jp の名前解決する側にも NetMeister を設定する必要があります。
IX 以外が nmddns.jp を名前解決する場合は、IX の proxy-dns を使用してください。

Ver.10.0 では、NGN 閉域網内でアクション実行などの一部基本保守機能を利用いただけません。
Ver.10.1 以降、IPv4 インターネットへ接続できる経路がある場合、mqtt force オプションを設定することで基本保守機能をご利用いただけます。
NetMeister Prime をご利用の場合、IPv4 インターネットへ接続できる経路がなくとも基本保守機能をご利用いただけます。また、mqtt force オプションは不要です。

Ver10.6 より、NGN 閉域網内の IPv6 通信量を軽減するため、一部の通信が IPv4 を利用するようになりました。このため、NGN 閉域網へ接続している環境でも、アラームとメトリクスを利用するには IPv4 インターネットの併用が必要になりました。

(a) NTT 東日本 NGN 網構成例



設定は以下のコマンドで行います。

nm ipv6 enable ngn-private	NGN 網接続設定 ※ アクション実行を使用する場合は mqtt force オプション(ver10.1 以降)が必要です

【設定例】
NTT 東日本 NGN に接続した装置で NetMeister に接続
登録したホスト名を使用して IPsec 接続

```
hostname tokyo-rt1

ip route default Tunnel1.0
ip route 192.168.0.0/24 Tunnel1.0
ip route 192.168.2.0/24 Tunnel2.0
ipv6 route default GigaEthernet0.0 dhcp

nm ipv6 enable ngn-private east mqtt force
nm account example-gp1 password plain example-pass1
nm sitename tokyo
nm ddns notify interface GigaEthernet0.0 protocol ipv6

ikev2 authentication psk id keyid honsya key char honsya-key
ikev2 authentication psk id keyid tokyo key char tokyo-key
ikev2 authentication psk id keyid chiba key char chiba-key

ikev2 default-profile
  local-authentication psk id keyid tokyo

ipv6 dhcp client-profile dhcpv6-cl
  option-request dns-servers
  ia-pd subscriber GigaEthernet0.0

interface GigaEthernet0.0
  ipv6 enable
  ipv6 dhcp client dhcpv6-cl
  no shutdown

interface Tunnel1.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet2.0
  ikev2 peer-fqdn-ipv6 honsya-rt.example-gp1.v6.nmddns.jp authentication psk id keyid
honsya
  ikev2 outgoing-interface GigaEthernet0.0 auto
  no shutdown

interface Tunnel2.0
  tunnel mode ipsec-ikev2
  ip unnumbered GigaEthernet2.0
  ikev2 peer-fqdn-ipv6 chiba-rt.example-gp1.v6.nmddns.jp authentication psk id keyid
chiba
  ikev2 outgoing-interface GigaEthernet0.0 auto
  no shutdown

interface GigaEthernet2.0
  description LAN
  ip address 192.168.1.254/24
  no shutdown
```

(b) NTT 東日本と NTT 西日本間の NGN 閉域網

NTT 東日本と NTT 西日本の両方の NGN 網を用いたダイナミック DNS を利用することができます。

※東日本エリアと西日本エリアそれぞれで最低 1 つは ISP 契約が必要です。

Ver.10.3 以降、NTT 東日本と NTT 西日本の回線を自動で判別することができます。利用する場合、以下の設定をしてください。

【設定例】

```
nm ipv6 enable ngn-private auto mqtt force

ipv6 dhcp client-profile dhcpv6-cl
   option-request domain-search-list
```

2.48.6 ダイナミック DNS

NetMeister を利用すると、装置に以下のドメインでアクセスできるようになります。
<任意のホスト名> . <任意のグループ ID> . nmddns.jp （IPv6 の場合は v6.nmddns.jp）

NetMeister のダイナミック DNS の機能は基本設定のみで動作します。基本設定以外の設定は不要です。利用開始時にグループ ID の登録は必要ですが、装置の追加や交換、ホスト名の変更などはサーバの設定変更なしで対応できます。ホスト名の重複登録にはご注意ください。

装置の追加
- これまで利用していないホスト名を設定し、インターネットに接続してください。

装置の交換
- 交換前の機器の設定をそのまま投入することにより、切り替え可能です。

ホスト名変更
- ホスト名を変更して nm update を実行することにより、変更可能です。

デフォルトで有効のため、利用する必要がない場合は以下のコマンドで無効化してください。

nm suppress-feature ddns	ダイナミック DNS の無効化

2.48.6.1 ダイナミック DNS の通知インタフェース指定

DDNS の通知インタフェースコマンドについて説明します。

基本設定では、サーバへの送信アドレスをダイナミック DNS に登録するため、IPv4 アドレスと IPv6 アドレスを同時に登録することができません。
IPv4 と IPv6 を同時に登録したい場合や、送信インタフェースと異なるインタフェースのアドレスを通知する必要がある場合は、以下のコマンドで通知インタフェースを指定してください。
通知するインタフェースがダウンしている場合、NetMeister の更新ができなくなります。
通知するインタフェースがダウンしないようにご注意ください。
そのインタフェースを使用しなくなった場合は、通知インタフェースの設定を削除してください。
NetMeister 通信冗長化を行う場合、冗長時に登録するダイナミック DNS のアドレスは、冗長用の設定に従います。スタンバイ用の設定を行っていない場合は、スタンバイ時は送信アドレスをダイナミック DNS に登録します。

nm ddns notify interface	ダイナミック DNS 登録インタフェースの設定
nm standby ddns notify interface	ダイナミック DNS 登録インタフェースの設定 (冗長用)(Ver10.7 以降)

【設定例】
IPv4 アドレスの通知インタフェースは GigaEthernet0.0
IPv6 アドレスを通知するインタフェースは GigaEthernet1.0

```
nm ip enable
nm account example-gp1 password plain example-pass1
nm sitename tokyo
nm ddns notify interface GigaEthernet0.0 protocol ip
nm ddns notify interface GigaEthernet1.0 protocol ipv6

interface GigaEthernet0.0
  ip address dhcp receive-default

interface GigaEthernet1.0
  ipv6 address autoconfig receive-default
```

基本設定ではホスト名を hostname コマンドで設定しますが、hostname を変更せず NetMeister に通知するホスト名だけを変更したい場合は、次のコマンドで設定してください。通常は hostname コマンドで設定してください。

nm ddns hostname	ダイナミック DNS 登録ホスト名の設定

Ver.10.8 以降、シーケンス番号を指定することにより、追加でダイナミック DNS 登録することが可能です。。
元々のダイナミック DNS 登録を含めて、MAC アドレス分までの登録ができます。
追加するダイナミック DNS に関してはインタフェースの指定は省略できません。

ホスト名には、シーケンス番号が付与されます。
<任意のホスト名> -<シーケンス番号>. <任意のグループ ID> . nmddns.jp
（IPv6 の場合は v6.nmddns.jp）

追加登録をする場合、NetMeister 通信冗長化利用時には、プライマリ、スタンバイともに同じインタフェースのアドレスで通知を行います。

【設定例】
GigaEthernet0.0 のアドレスを router1.test.nmddns.jp で登録
GigaEthernet1.0 のアドレスを router1-1.test.nmddns.jp で登録

```
hostname router1

nm ip enable
nm account test password secret XXXXXXXX
nm ddns notify interface GigaEthernet0.0
nm ddns notify seq 1 interface GigaEthernet1.0
```

2.48.7 アラーム通知

装置で発生したアラームを NetMeister に通知します。

項目		発生条件	復旧条件
クラッシュによる再起動		show uptime の caused by が crash の場合	---
FAN の異常・復旧 （FAN のある機種のみ）	※1	FAN アラーム発生時	FAN アラーム復旧時
温度の異常・復旧	※1	温度アラーム発生時	温度アラーム復旧時
CPU 使用率の異常・復旧	※2	show utilization history の per 5 seconds の average が 95 以上	show utilization history の per 5 seconds の average が 80 以下
メモリ使用率の異常・復旧	※2	show memory の Heap memory の average が 3 回連続で 95 以上	show memory の Heap memory の average が 3 回連続で 80 以下
切断通知	※3	MQTT の切断	MQTT の接続
UTM 関連通知		UTM の章を参照してください	---
電源	※4	電源供給不能時	電源供給復旧時
ネットワークモニタ通知	※5	ネットワークモニタイベン	ネットワークモニタイベン

		ト検出時	ト復旧時
リンクダウン通知	※5	物理ポートのリンクダウン	物理ポートのリンクアップ
不正端末検知	※6	通信不許可端末の検知	---
イベントログ欠落	※7	イベントログ送信機能で記録バッファが溢れた場合	--

※1 装置アラームの発生・復旧条件については、機能概要のハードウェア諸元を参照してください。
※2 監視周期は 1 分となります。
※3　MQTT の通信ができない環境では使用できません。
※4 電源二重化環境でのみ対象となります。
※5 通知を設定する必要があります。
※6 通知周期は 6 時間となります。
※7 通知は送信周期につき 1 回となります。

クラウド側にアラーム情報を通知したくない場合は、以下の設定で無効化してください。なお切断通知はクラウド側で検出するため、本コマンドで停止することはできません。

nm suppress-feature alarm	アラーム通知の無効化

2.48.8 NetMeister 通信冗長化

Ver10.7 より、NetMeister の装置登録が失敗した場合に異なる回線から接続を行うことが可能になります。

本機能を使用することにより、回線障害時に他の回線から NetMeister の通信を継続することができます。

※ 装置登録更新から切り替わりまで最大 5 分程度かかります。

NetMeister の装置登録が失敗すると使用する回線が切り替わります。
装置登録の契機には以下の種類があります。

- 定期更新(約 7day)
- インタフェースの状態変化
- IP アドレスの情報変更
- 「nm update」コマンドの実行

また、ネットワークモニタの設定(action netmeister-switch-mode)によりネットワークを監視して回線を切り替えることが可能です。

※ ネットワークモニタに関してはネットワークモニタの章を参照してください。

設定は以下のコマンドで行います。

nm standby ip enable （nm standby ipv6 enable）	NetMeister(冗長)機能の有効化 ※ （NGN 閉域網では ipv6 を指定） (Ver10.7 以降)
nm standby outgoing-interface	送信インタフェース(冗長)指定 (Ver10.7 以降)
nm standby source-address	送信元アドレス(冗長)指定(Ver10.7 以降)
nm standby ddns notify interface	ダイナミック DNS 登録インタフェースの設定(冗長) (Ver10.7 以降)

※ nm account、nm sitename、nm hostname は nm ip enable / nm standby ip enable 共通の設定です。

※ NetMeister 通信冗長を使用する場合、上記コマンドは全て入力推奨です。

ダイナミック DNS 使用時に冗長化を使用する場合、障害時でもダイナミック DNS 登録が成功する必要があります。冗長時のダイナミック DNS 登録インタフェースを設定する場合、障害時に通知可能なインタフェースを設定してください。

冗長用のダイナミック DNS 登録インタフェース設定が未設定の場合は、送信インタフェースのアドレスを通知します。この場合、冗長の切り替わり時にはダイナミック DNS で登録されるアドレスも切り替わります。VPN 接続にダイナミック DNS で登録したホスト名を使用する場合はご注意ください。

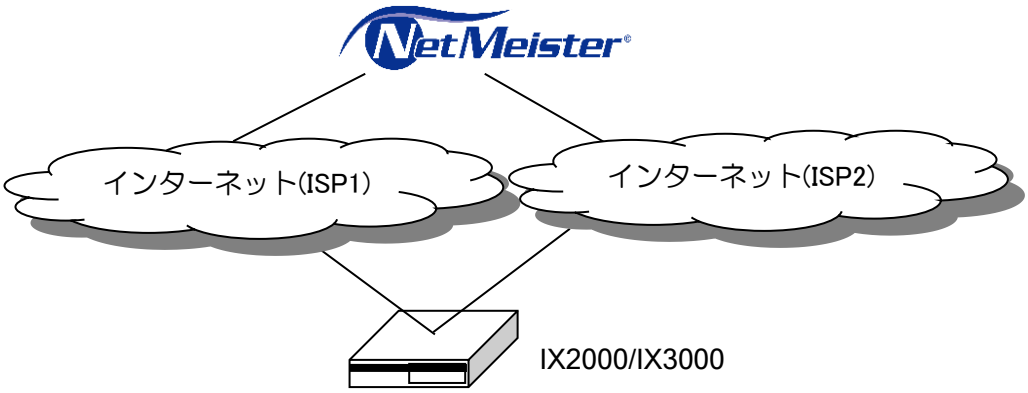
Ver.10.8 以降の場合は、複数アドレス通知（シーケンス番号指定）は冗長の切り替わり時には登録アドレスは変更になりません。VPN 接続に固定インタフェースのアドレスを使用したい場合は、複数アドレス通知をご利用ください。

※複数の VPN を接続する場合は、MAC アドレスが 2 個の装置では対応できません。

(a) 冗長構成例 1(NetMeister 冗長)

IX2000/3000 でインターネットに直接接続する構成です。
片方の回線(ISP1)に障害が発生した場合にもう片方の回線(ISP2)から接続します。

本設定により、回線(ISP1)が接続できない状態でも NetMeister で装置管理が可能となります。



【設定例】
IX2000/3000 で ISP1(GE0.1)と ISP2(GE1.0)で冗長
ICMP echo により GigaEthernet0.1 から 10.1.1.254 の監視を行います。
応答が返らなくなるとイベントが発生し、ISP2 から NetMeister に接続されます。
ICMP echo により GigaEthernet0.2 から 10.1.1.254 の監視を行います。
応答が返らなくなるとイベントが発生し、ISP1 から NetMeister に接続されます。
※※10.1.1.254 はインターネット上の監視対象、若しくはトンネル対向装置の LAN インタフェースのアドレスをイメージしています。

```
hostname tokyo-rt1

nm ip enable
nm standby ip enable
nm account example-gp1 password plain example-pass1
nm sitename tokyo
nm ddns notify interface GigaEthernet0.1
nm standby ddns notify interface GigaEthernet1.1
nm source-address GigaEthernet0.1 protocol ip
nm standby source-address GigaEthernet1.1 protocol ip
nm outgoing-interface GigaEthernet0.1 auto protocol ip
nm standby outgoing-interface GigaEthernet1.1 auto protocol ip

ppp profile isp1
  authentication myname test1@example.com
  authentication password test1@example.com test

ppp profile isp2
  authentication myname test2@example.com
  authentication password test2@example.com test

watch-group wan1-watch 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet0.1
  action 10 netmeister-switch-mode standby suppress-restration
  network-monitor wan1-watch enable

watch-group wan2-watch 10
  event 10 ip unreach-host 10.1.1.254 GigaEthernet1.1
  action 10 netmeister-switch-mode primary suppress-restration
```

```
    network-monitor wan2-watch enable

interface GigaEthernet0.1
    encapsulation pppoe
    auto-connect
    ppp binding isp1
    ip address ipcp
    ip napt enable
    no shutdown

interface GigaEthernet1.1
    encapsulation pppoe
    auto-connect
    ppp binding isp2
    ip address ipcp
    ip napt enable
    no shutdown

interface GigaEthernet2.0
    description LAN
    ip address 192.168.0.254/24
    linkmgr enable
    no shutdown
```

2.48.9 アクション実行

以下の処理が実行できます。

- ファームウェア更新
- コンフィグ取得
- 装置情報一括取得
- 装置削除
- 設定引継ぎ
- コンフィグ保存　（Ver10.1 以降）
- コマンド実行　（Ver10.1 以降）
- 再起動　（Ver10.1 以降）
- ライセンス　（Ver10.3 以降）
- Find Your Device　（Ver10.6 以降）

2.48.10 デバイスリスト

接続機器の情報を表示することができます。

2.48.11 UTM 統計レポート

UTM 機能で収集した統計レポートを表示することができます。

2.48.12 URL オフロード拡張

URL オフロードの URL を編集・管理することができます。
※設定に url netmeister(URL オフロードコンフィグモード) が必要です
※IPv6（NGN 閉域網を含む）に未対応です。

2.48.13 他機種収容

他機種を NetMeister 接続子機として収容できます。
また、接続した子機の死活監視も可能です。ネットワークモニタ通知アラームで通知されます。
VRF インタフェースからは接続子機として収容できません。
※設定に http-server ip enable が必要です。
死活監視は、NetMeister 上からの設定が必要です。

2.48.14 UTM 脅威分析

UTM 機能で収集したセキュリティログ情報から分析を容易にします。

2.48.15 リモートログイン

外部のクライアントから自装置や子機への HTTPS/SSH サーバサービスへのアクセスを一時的に許可することができます。

※同じグループ内に IPv4 グローバルアドレスが付与されている必要があります。

※設定に http-server ip enable や ssh-server ip enable が必要です。
設定を変更した場合、nm update が必要です。

※Ver.10.6 以降、system information コマンドで WAN 側と LAN 側のインタフェース指定が行えます。

※Ver.10.5 以前では、web-console system information コマンドで WAN 側と LAN 側のインタフェースの指定が行えます。

show nm information で HTTPS/SSH の有効/無効が確認できます。

【設定例】

```
interface GigaEthernet2.0
   description LAN
   ssh-server ip enable
   http-server ip enable

system information lan 1 GigaEthernet2.0
system information wan 1 GigaEthernet0.1
```

【表示例】

```
Router(config)# show nm information
   :
API-GW:
   :
  Detail      :
    wanif     : GigaEthernet0.1
    lanif     : GigaEthernet2.0
    https     : enable
    ssh       : enable
   :
```

2.48.16 ダイナミック VPN 設定

NetMeister に接続された対応装置を選択し、ダイナミック VPN を構築することができます。

※IPv6（NGN 閉域網を含む）に未対応です。
WebUI では、NGN 閉域網でのダイナミック VPN の設定が可能です。

2.48.17 メトリクス

トラフィックや、CPU 使用率・メモリ使用率・装置温度のグラフを表示することができます。

2.48.17.1 SW-HUB ポートの統計情報通知

SW-HUB ポートの統計は、全てのポートの情報は、各ポートの合計値が通知されます。

Ver.10.8 以降、ポート VLAN を利用することにより、各ポートの統計情報を通知することができます。

ポート VLAN を設定している場合は、ポートが含まれているポート VLAN のインタフェースの情報を通知します。

【設定例】

```
bridge irb enable

device GigaEthernet2
   vlan-group 1 port 1
   vlan-group 2 port 2
   vlan-group 3 port 3
   vlan-group 4 port 4

interface GigaEthernet2:1.0
   no ip address
   bridge-group 1
   no shutdown

interface GigaEthernet2:2.0
   no ip address
   bridge-group 1
   no shutdown

interface GigaEthernet2:3.0
   no ip address
   bridge-group 1
   no shutdown

interface GigaEthernet2:4.0
   no ip address
   bridge-group 1
   no shutdown

interface BVI1
   ip address 192.168.1.254/24
   bridge-group 1
   no shutdown
```

【動作】
ポート 1 の情報は GigaEthernet2:1.0 の情報を通知
ポート 2 の情報は GigaEthernet2:2.0 の情報を通知
ポート 3 の情報は GigaEthernet2:3.0 の情報を通知
ポート 4 の情報は GigaEthernet2:4.0 の情報を通知

2.48.18 ポート情報

ポートの UP/DOWN 情報や、LED を表示することができます。

2.48.19 Find Your Device

現地での実機装置の特定を容易にするため、対応する IX の LED ランプを一定時間点滅させることができます。

2.48.20 NetMeister Prime

NetMeister Prime とは NetMeister の有償サービスです。Wake on LAN や任意 IP アドレスの死活監視などがご利用できるようになります。

詳細は

https://www.necplatforms.co.jp/product/netmeister/prime.html

をご覧ください。

2.48.21 イベントログ送信機能

Ver10.7 以降、イベントログ送信機能を利用することで、IX に記録していたイベントログ情報を NetMeister で確認することができます。

イベントログ送信機能は、NetMeister と接続後に動作を開始します。

利用には NetMeister Prime（有償サービス）が必要となります。

2.48.21.1 基本設定

イベントログ送信機能を有効化する場合、以下のコマンドを設定する必要があります。

グローバルコンフィグモード	
nm logging enable	イベントログ送信機能を有効化します。 オプションを指定することにより、送信対象のログレベルの範囲を指定することができます。指定したレベル以上の全てのレベルのイベントログが送信対象となります。 なお、大量のイベントログ送信が発生することを防止するため、本オプションで debug レベルを指定することはできません。

運用中に設定を追加した場合は、設定追加時に必ず nm update コマンドを実行してください。
nm update による設定更新後からイベントログ送信機能が有効となります。
オプションでイベントログレベルを変更した場合は、記録するログレベルは即時反映されます。

また、イベントログを記録するために以下の設定が必要になります。
設定がない場合、イベントログの記録ができません。

グローバルコンフィグモード	
logging subsystem	サブシステムメッセージ表示の設定

【設定例】

1：warn レベル以上のログを記録する場合
logging subsystem all warn

nm logging enable

2：notice レベル以上のログを記録する場合
logging subsystem utm debug
logging subsystem nmc warn

nm logging enable level notice

設定例 2 の場合、イベントログ送信機能では utm は notice 以上のログが記録され、
info 以下のイベントログは記録されません。

※NetMeister と接続するための基本設定は省略しています。

※ logging subsystem include/ exclude 設定時の動作は以下の通りになります。

設定	動作
logging subsystem include	設定対象のログレベルが nm logging enable で設定しているログレベル以上である場合、記録される。
logging subsystem exclude	設定対象のログレベルに関係なく記録対象外となります。

2.48.21.2 注意事項

- 記録するレベルを上げた場合、記録するログが多くなるため必要な情報が埋もれる、またはオーバフローで損失する可能性があります。
- イベントログ以外で表示されるログは記録されません。

2.48.21.3 送信周期と送信サイズ

NetMeister へ記録したイベントログを送信する周期と、記録できるサイズは以下になります。

送信周期	5 分
記録サイズ	最大 100KB※
記録ログ数	最大 2000 件※

※どちらかが上限に達した場合、NetMeister へイベントログが送信されるまでイベントログは記録されません。

・再送処理タイミングについて
NetMeister へ記録したイベントログを送信に失敗した場合、再送処理を行います。
次回の送信周期のタイミングまでに再送が成功しなかった場合、再送を諦め次の送信を行います。
この時、再送に失敗したデータは廃棄されます。

2.48.21.4 アラーム

発生条件は NetMeister のアラーム通知（イベント欠落）を確認してください。

■2.49 アプリケーション解析機能の設定

2.49.1 アプリケーション解析機能概要

IX ルータのアプリケーション解析機能を利用することで、特定のアプリケーション通信（Zoom など）に対して様々なトラフィック制御と解析をすることができます。
アプリケーション解析機能は、NetMeister と接続後に動作を開始します。
また、この機能は一部の詳細設定を除き NetMeister サービスから設定や管理を行います。

NetMeister での画面表示や設定方法につきましては、NetMeister のマニュアルを参照してください。
<https://support.necplatforms.co.jp/netmeister/manual/index.html>

2.49.2 機能一覧

通信のパケットを解析して利用されているアプリケーションを識別します。特定のアプリケーションが利用されていた場合、以下の機能を適用することができます。

機能	対応バージョン	説明
トラフィックの ローカルブレイクアウト	Ver10.6 ～	送信先の WAN 側インタフェースをアプリケーションごとに指定することで、アプリケーション単位の負荷分散を実現することが可能です。 Ver.10.9 以降、ネクストホップの指定が可能です。
UTM 透過機能	Ver10.6 ～	U TM スキャンを行うかどうかを、アプリケーション単位で設定可能です。 UTM のセキュリティチェックをせずに動作します。設定は NetMeister サービスで制御します。
トラフィックグラフ	Ver10.6 ～	時間帯ごとの通信量をアプリケーションごとにグラフ等で確認可能です。 グラフの確認は NetMeister サービスで可能です。
トラフィック制限機能	Ver10.7 ～	アプリケーションごとに帯域制御をすることができます。特定のアプリケーションによる通信帯域の圧迫を防止することが可能です。 設定は NetMeister サービスで制御します。

2.49.3 注意事項

2.49.3.1 NetMeister との接続について

アプリケーション解析を利用するには、NetMeister との接続を常時維持する必要があります。
NetMeister との接続状況は、NetMeister サービス上で確認可能です。

2.49.3.2 解析対象について

- 対象トラフィック

IPv6 トラフィックには対応しておりません。

- プロキシ環境での解析

インターネットアクセスにプロキシサーバを使用している場合、プロキシサーバ宛へのパケットは解析対象外になります。

2.49.3.3 URL オフロード併用について

- 併用できない機能

URL オフロードデータベースの指定コマンド(url)で、”NetMeister”以外のデータベースを指定した場合、アプリケーション解析機能はご利用いただけません。

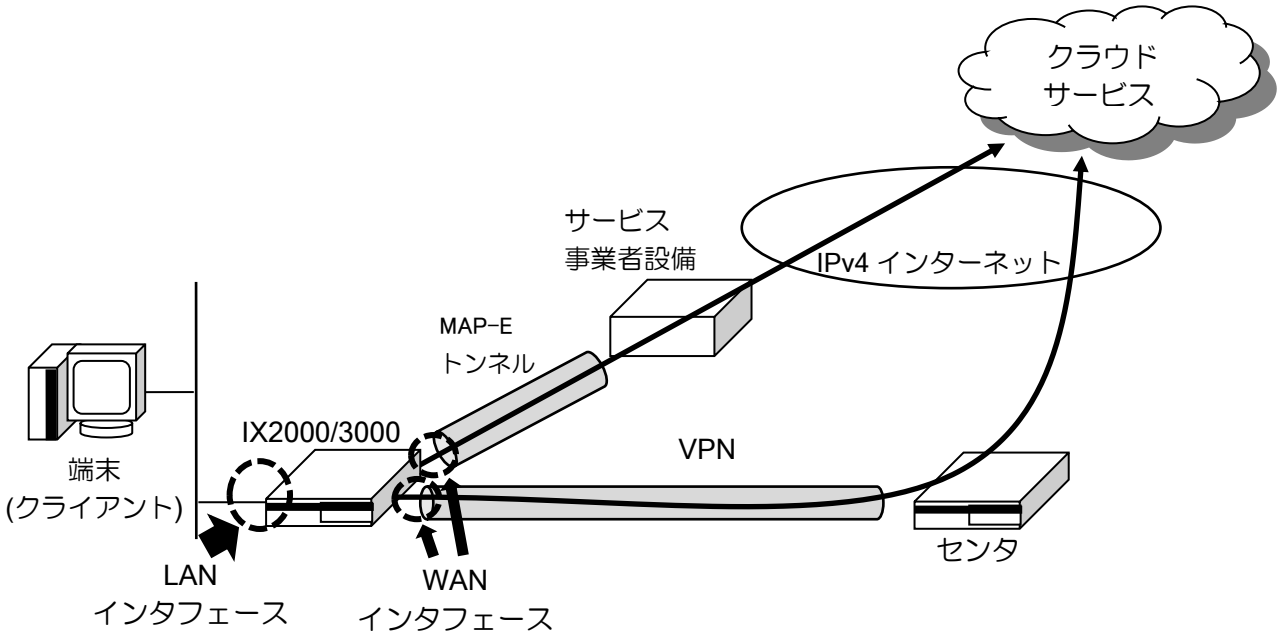
- 設定値の決定

アドレスキャッシュや更新周期など一部設定はアプリケーション解析機能の設定のどちらかの値を使用して動作します。

詳細は、「URL オフロード併用」の項目をご確認ください。

2.49.4 WAN・LAN インタフェースの指定

2.49.4.1 アプリケーション解析機能における WAN・LAN インタフェース



図のように、アプリケーション解析機能において WAN インタフェースと LAN インタフェースは以下のように定義します。WAN・LAN インタフェースはそれぞれ複数設定することができます。

- WAN インタフェース

IPv4 インターネットとの通信に使用するインタフェース。

NetMeister で指定したアプリケーションのローカルブレイクアウト先インタフェースとして利用します。全ての送信先となるインタフェースを WAN インタフェースとして指定する必要があります。

Tunnel インタフェースを利用してインターネット接続する場合、WAN インタフェースとして Tunnel インタフェースを指定する必要があります。例えば、VPN や IPoE（MAP-E、DS-Lite など）のような、Tunnel インタフェースを経由してクラウドサービスと接続する場合、WAN インタフェースはそれらの Tunnel インタフェースを全て指定する必要があります。

- LAN インタフェース

クライアントとの通信に使用するインタフェース。

指定したインタフェースを通過するトラフィックに対してアプリケーション種別の判定を実施し、各種アプリケーション解析機能を利用できるようになります。

2.49.4.2 WAN・LAN インタフェースの確認方法

装置のどのインタフェースが WAN・LAN に指定されているかは、show running-config コマンドで表示される system information 情報で確認が可能です。

デフォルト設定の場合、system information の設定は表示されません。

2.49.4.3 WAN・LAN 対象インタフェース

- デフォルト設定

デフォルト設定では WAN・LAN インタフェースは以下のインタフェースが割り当てられます。
個別にインタフェースを指定する場合、system information コマンドで設定が必要になります。

	対象インタフェース	備考
WAN	GigaEthernet0.0	IP アドレスが振られている場合に WAN として割り当て
	GigaEthernet0.1	
	USB0.0	
LAN	GigaEthernetX.0	X:対象プラットフォームで一番大きいインタフェース番号

- 個別設定

system information コマンド設定することで、個別に対象インタフェースを設定することができます。詳細な設定については次項「設定方法」を参照してください。

2.49.4.4 設定方法

アプリケーション解析機能の対象にする場合、以下のコマンドで設定する必要があります。
設定可能な WAN・LAN インタフェース番号はそれぞれ最大 20 までになります。

グローバルコンフィグモード	
system information	WAN、LAN インタフェース割り当て設定

```
【表示例】
(config)# show running-config
                ;
system information lan 1 GigaEthernet2.0
system information wan 1 GigaEthernet0.0
```

構成により WAN として指定するインタフェースが異なります。
主な構成例で WAN として指定するインタフェースを以下に示します。

構成	WAN インタフェース (WAN アドレスが割り当てられているインタフェース)
DS-Lite	Tunnel インタフェース
DHCP	ip address dhcp を設定しているインタフェース
PPP	ip address ipcp を設定しているインタフェース
MAP-E	Tunnel インタフェース

注意事項

- Web コンソール利用時

Web コンソールで設定をしている場合、以下の system information コマンドが設定されている場合があります。

```
system information lan 1
system information wan 1
system information wan 2
```

この設定を変更した場合、Web コンソールが動作しなくなる可能性がありますのでご注意ください。設定を追加する場合、上記のコマンドで設定されている番号とインタフェースに重複しないような番号とインタフェースを設定してください。

- NetMeister サービス利用時

一部の NetMeister サービスでは以下の system information コマンドの設定を参照して機能が動作しています。

NetMeister サービス機能	該当コマンド
ダイナミック VPN	system information wan 1 system information lan 1
リモートログイン	system information lan 1

そのため、手動設定する際は使用する環境に合わせて system information コマンドの設定をしてください。設定を追加する場合、上記のコマンドで設定されている番号とインタフェースに重複しないような番号とインタフェースを設定してください。

2.49.5 トラフィックのローカルブレイクアウトについて

NetMeister で指定したアプリケーションを WAN へローカルブレイクアウトします。

NetMeister サービスにて任意のインタフェースをローカルブレイクアウト先とする場合、system information コマンドで wan 側インタフェースとして設定する必要があります。

また、ロールブレイクアウト先に関係なく送信先となるインタフェースは wan 側インタフェースとして設定する必要があります。

2.49.6 URL オフロード併用

2.49.6.1 共有する設定

以下の設定は、アプリケーション解析機能の設定と比較して設定値が大きい方を使用します。

- アドレスキャッシュ設定（url-offload address-cache）
  - 最大キャッシュ数
  - ネガティブキャッシュの保持時間
  - ポジティブキャッシュの保持時間
- 更新周期設定（update-interval）

アプリケーション解析機能では、それぞれ以下の固定値が設定されています。

設定値	アプリケーション解析
最大保キャッシュ数	65535
ネガティブキャッシュの保持時間	1800
ポジティブキャッシュの保持時間	600
更新周期	24

2.49.6.2 判定の優先度

以下の順序でオフロード判定が行われます。
最初にヒットした条件で処理は実施され、以降の条件は無視されます。

1. ルートマップ設定　※
2. 外部定義ファイル（NetMeister サービスより取得）

※ルートマップが同一名で複数ある場合、優先度の高いルートマップから判定を行います。

2.49.7 情報の確認

2.49.7.1 CLI 表示

以下のコマンドでアプリケーション解析機能関連の状態を確認できます。

グローバルコンフィグモード	
show app-analytics status	アプリケーション解析機能の状態表示
show app-analytics database	アプリケーション解析データベースの表示
show app-analytics address-cache	アプリケーション解析アドレスキャッシュの表示
show app-analytics session-cache	アプリケーション解析セッションキャッシュの表示
show app-analytics statistics	アプリケーション解析機能の統計情報表示

状態表示では、アプリケーション解析機能の統計が確認できます。

【表示例】

```
(config)# show app-analytics status
DataBase Information:
   Update: 1636096669
   Total 168 entries, URL 46 entries, IPv4 122 entries
   Total 0 packets analyzed, 0 packets matched.
---以下の表示は ver10.7 以降に表示されます----
Setting Information:
   Update: 2022/08/01 13:03:18
   Setting data:
      Application          Transmit Interface   UTM exclude   Rate(Mbps)
      Office365             ---                  disable          ---
      Skype/Teams           ---                  disable          ---
      WindowsUpdate         ---                  disable          ---
      Box                   ---                  disable          ---
      GSuite                ---                  disable          ---
      AdobeCreativeCloud    ---                  disable          ---
      Salesforce            ---                  disable          ---
      Zoom                  ---                  disable          ---
      WebEX                 ---                  disable          ---
      UserDefined           ---                  disable          ---
```

表示	内容
DataBase Infomation	
Update:	更新時間
Total　xx entries	合計エントリ数
URL　xx entries	URL エントリ数
IPv4 xx entries	IPv4 アドレスエントリ数
Total　xx packets analyzed	アプリケーション解析機能で解析した packet 数
xx packets matched.	Database にヒットしたパケット数

Setting Information	
Update	更新時間
Setting data	Application：アプリ名 Transmit Interface：送信先インタフェース UTM exclude：UTM 除外設定 Rate：トラフィック制限設定

データベース表示では、アプリケーション解析機能で使用しているデータベースの詳細情報を確認できます。

【表示例】

```
(config)# show app-analytics database
DataBase Information:
   Update: 1636096669
   Total 168 entries, URL 46 entries, IPv4 122 entries
DataBase entries : Application
   Office365
   Skype/Teams
   UserDefined
DataBase entries : URL
   *.example.com(Skype/Teams)
   *.example1.com(Office365)
   example2.com(Skype/Teams)
   *.example2.com(Skype/Teams)
   *.officeapps.live.com(Office365)
DataBase entries : IPv4
   203.0.113.0/24 (tcp, 80, Office365)
   198.51.100.0/24 (udp, 3478-3481, Skype/Teams)
```

表示	内容
DataBase Information:	
Update	更新時間
Total　xx entries	合計エントリ数
URL　xx entries	URL エントリ数
IPv4 xx entries	IPv4 アドレスエントリ数
DataBase entries:Application	データベースで保持しているアプリケーション名
DataBase entries : URL	データベースで保持している URL 集
DataBase entries : IPv4	データベースで保持している IPv4 アドレス集

アドレスキャッシュ表示では、アドレスキャッシュエントリに紐づくアプリケーション名を確認することができます。

【表示例】

```
(config)# show app-analytics address-cache
Address-Cache - 56 entries, 56 max entries, 0 overflows
Codes: p - positive, n - negative
   Prot   Destination Addr:Port   Remain Time   Reference Source
n tcp     192.0.2.1:443                0:09:59   ---
p tcp     203.0.113.1:443              0:19:49   203.0.113.0/24 (tcp, 443, Office365)
```

表示	内容
Address-Cache	アドレスキャッシュ情報
xx entries	エントリ数
xx max entries	最大エントリ数
xx overflows	オーバフロー数

セッションキャッシュ表示では、セッションキャッシュエントリに紐づくアプリケーション名を確認することができます。

【表示例】

```
(config)# show app-analytics session-cache
Session-Cache - 1 entries, 4 max entries, 0 overflows, 0 drops
Prot    Source Addr:Port          Destination Addr:Port    Remain Time    Reference Source
tcp     192.0.2.3:51232           203.0.113.1:443          0:00:47    203.0.113.0/24 (tcp, 443, Office365)
```

表示	内容
Session-Cache	セッションキャッシュ情報
xx entries	エントリ数
xx max entries	最大エントリ数
xx overflows	オーバフロー数
xx drops	廃棄数

■2.50 ゼロコンフィグの設定

2.50.1 ゼロコンフィグ

ゼロコンフィグは、IX2000/IX3000 シリーズのゼロコンフィグモデルで実現される機能の総称です。IX2000/IX3000 シリーズのゼロコンフィグは、SMF を使用して自動コンフィグレーションやリモートメンテナンス機能、死活監視・運用監視等を実現します。

ゼロコンフィグを利用する場合、ゼロコンフィグモデルの IX2000/IX3000 シリーズを購入する必要があります。また、別途サービス事業者様との契約（またはサーバの構築）が必要となります。

2.50.2 SMF とは？

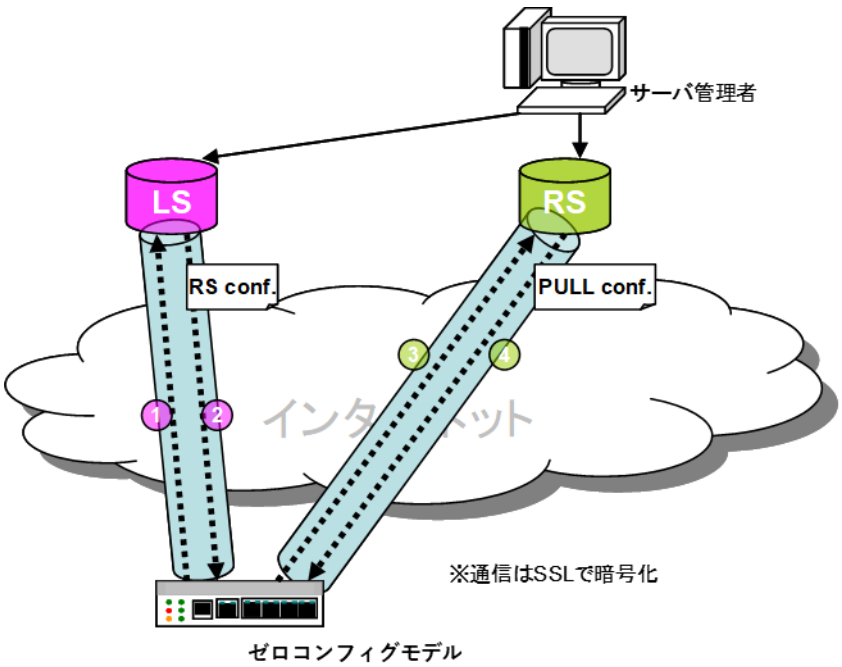
SEIL Management Framework の略称で、自動コンフィグレーション機能やリモート管理など、ゼロコンフィグモデルで実現できるサービスのフレームワークです。IX2000/IX3000 シリーズのゼロコンフィグモデルでは、SMF のバージョン２である SMFv2 をサポートしています。

※ 「SEIL は株式会社インターネットイニシアティブの登録商標または商標です。」

2.50.3 自動コンフィグレーション機能（ゼロコンフィグ機能）

ゼロコンフィグモデルの IX ルータをインターネットなどの回線に接続することにより、LS（ロケーションサーバ）と RS（リソースサーバ）より運用コンフィグを自動的に設定し動作します。

IX ルータの設置場所でコンフィグ設定などを実施する必要が無く、LS・RS からの情報取得も SMF によって SSL で暗号化され自動的に取得できるため、設置する人を選ばず、情報漏洩の心配なく安全に機器導入することが可能となります。

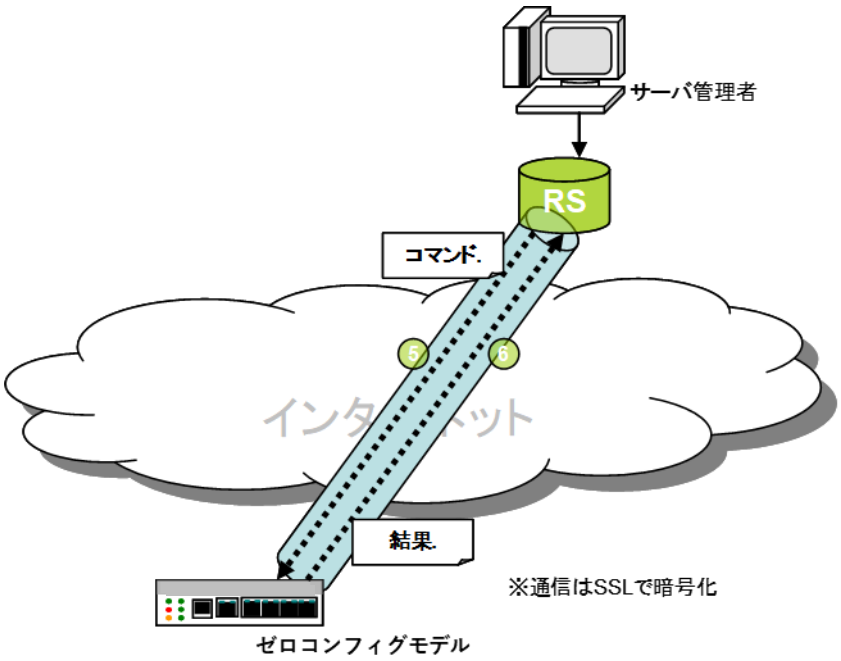


- IX ルータをインターネット回線に接続
- IX ルータにあらかじめ登録された LS へ接続するための情報から、PPPoE/DHCP で自動的にインターネットに接続①、LS から RS 接続情報（RS conf.）を取得②
- LS から取得した RS 接続情報（RS conf.）により RS に接続して③、RS から運用コンフィグ（PULL conf.）を取得④

- IX ルータを設置した場所では何も設定することなく運用開始。

2.50.4 リモートメンテナンス

ゼロコンフィグモデルのメンテナンスはすべて RS の Web ベースの GUI などから実行できます。SMF により SSL で暗号化されたプロトコルで安全に、コンフィグ変更、運用状態把握、バージョンアップができます。



- RS より任意のコマンド実行⑤、結果取得⑥が可能
- 完全２面化された、ファームウェア構造により安全にバージョンアップ可能（たとえバージョンアップ中に電源が落ちても、機器故障が発生しない限り前回起動していたファームウェアより起動可能）

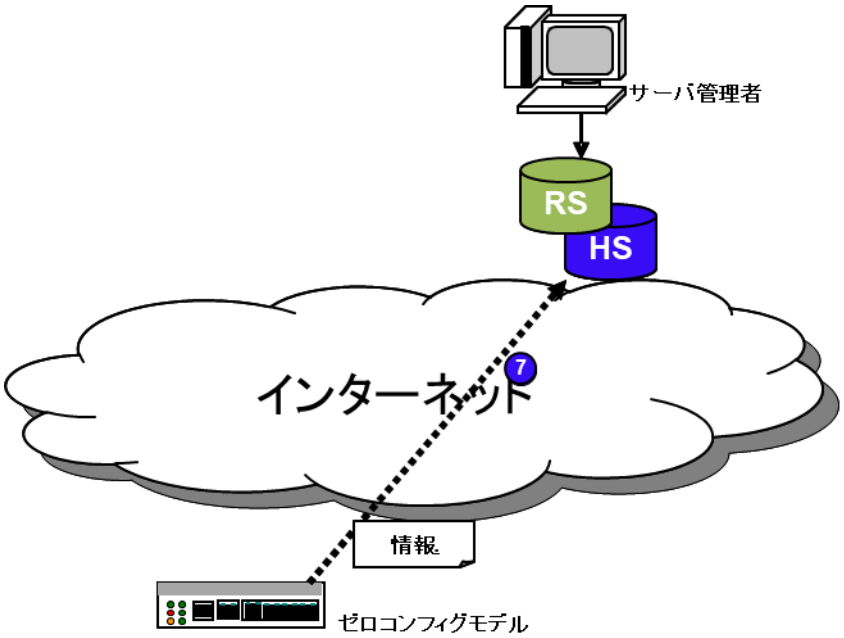
※　実際にリモートから実行可能な操作は、サービス事業者様のサービス内容によって異なります。

2.50.5 起動時バージョン固定（PULL バージョンアップ・ダウン）（Ver.8.4 以降）

ゼロコンフィグモデルのルータを起動時に RS に設定したバージョンに自動バージョンアップ・バージョンダウンすることができます。これにより、リモートメンテナンス機能を使用して運用者が手動でバージョンダウンなどを実施しなくても、使用したいバージョンに固定した運用が可能となります。

2.50.6 死活監視・運用監視（Heartbeat）

ゼロコンフィグモデルのルータを接続すると、Heartbeat サーバに対して、Heartbeat パケットを定期的に送信するようになります。サーバ管理者は、RS を介してこの Heartbeat サーバの情報を参照することにより、各ルータの状況を把握することができます。



- 装置情報の確認⑦
  - CPU 使用率（ロードアベレージ）
  - メモリ使用率
  - デバイス単位のトラフィック情報

※ 実際に確認可能な内容は、サービス事業者様のサービス内容によって異なります。
※ Ver.8.4 以降では、各ゼロコンフィグモデルの IX ルータに対して、Heartbeat パケットの送信や送信オプション制御が可能となっています。

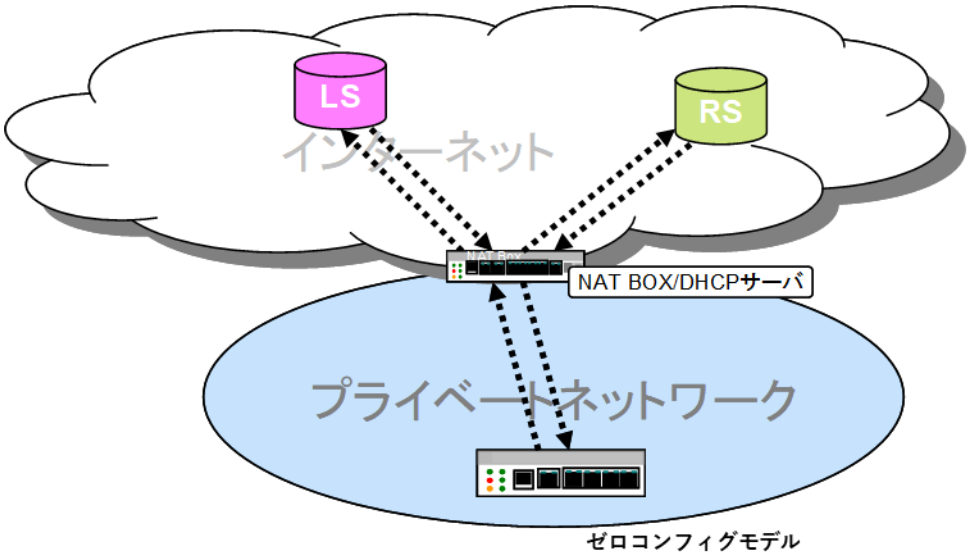
2.50.7 ゼロコンフィグ適用環境

ゼロコンフィグモデルでは、適用環境として下記の制限があります。（今後、適用範囲拡大予定）

- ゼロコンフィグによるコンフィグ取得時に、PPPoE（NTT フレッツ）または DHCP 経由で IX ルータから直接インターネットに接続できる必要があります。（Ver.8.3 以降では、NAT ボックスを介したプライベートネットワークでの利用が可能となりました。下記を参照してください）
- ゼロコンフィグによるコンフィグ取得時に、インターネットに接続するためにタグ VLAN・ポート VLAN 等の設定が必要となる接続形態では使用できません。
- ゼロコンフィグによるコンフィグ取得時に、SFP モジュール（光モジュール）は使用できません。

2.50.7.1 NAT ボックスを介したプライベートネットワークでの利用（Ver.8.3 以降）

RS とゼロコンフィグモデルの IX ルータの間に、NAT/NAPT を行うルータ（NAT ボックス）などが存在するプライベートネットワーク環境においてもゼロコンフィグモデルの使用が可能です。



- ゼロコンフィグモデルの IX ルータは、DHCP で NAT ボックスからインターネットへ接続される経路が自動設定される必要があります。
- インターネット接続にプロキシサーバ等を中継する必要のあるプライベートネットワーク環境では使用できません。

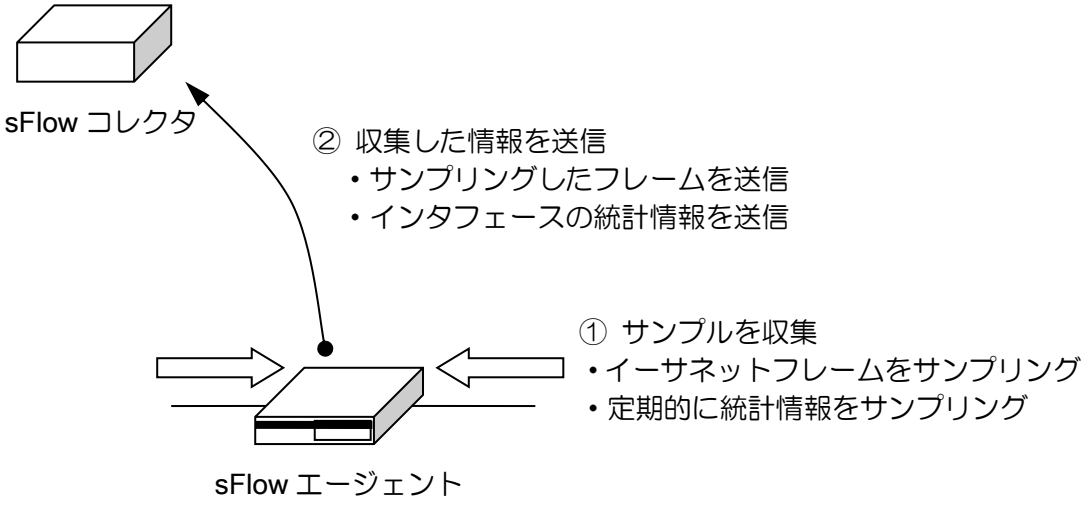
■2.51 sFlow の設定

sFlow は InMon 社が開発し RFC3176 および http://www.sflow.org/で公開されている、トラフィックをリアルタイムにモニタリングするためのプロトコルです。sFlow はトラフィックのごく一部をサンプリングして統計的手法で解析するため、ネットワークや装置に負荷をかけずにモニタリングすることができます。

IX ルータでは、Ver8.9 から sFlow ver5 の sFlow エージェント機能をサポートしています。この機能の利用には sFlow コレクタが別途必要です。

2.51.1 sFlow エージェント機能概要

sFlow エージェント機能として、フローサンプルと、カウンタサンプルの送信機能に対応しています。通常、必要なデバイスごとに両方設定して sFlow コレクタに通知します。



2.51.1.1 フローサンプル

指定したデバイス上で受信したフレーム（Ver9.6 以降は送信フレームも対応）を、指定した頻度でサンプリングする機能です。実際に流れているトラフィックをサンプリング的に収集して、低負荷でリアルタイムにモニタリングすることができます。

サンプリングレートの調整については、後述のフローサンプルの調整の項目を参照してください。

sFlow ver5 のフローサンプルにはいくつかの形式がありますが、対応しているのは基本データ形式のヘッダ型のみで、受信したフレームを先頭から指定したサイズだけ収集してコレクタに送ります。また、フレームを廃棄した場合に要因を記録する機能は対応しておりません。

なお、送信方向のサンプリング機能については、コレクタによって正しく動作しない場合もありますので、事前に動作確認をお願いいたします。

2.51.1.2 カウンタサンプル

指定したデバイス上の統計情報を一定周期で通知する機能です。イーサネットのデバイスでは Generic Interface Counters と Ethernet Inteface Counters のカウンタを、その他のデバイスは Generic Interface Counters のカウンタのみを送信します。

Generic Interface Counters

ifIndex	インタフェース番号※
ifType	インタフェースの種類
ifSpeed	回線速度 (64bit)
ifDirection	Duplex（1 = full, 2 = half）
ifStatus	インタフェースの状態
ifInOctets	受信バイト数 (64bit)
ifInUcastPkts	受信ユニキャストパケット数
ifInMulticastPkts	受信マルチキャストパケット数
ifInBroadcastPkts	受信ブロードキャストパケット数
ifInDiscards	受信破棄パケット数
ifInErrors	受信エラーパケット数
ifInUnknownProtos	受信プロトコル不明パケット数
ifOutOctets	送信バイト数 (64bit)
ifOutUcastPkts	送信ユニキャストパケット数
ifOutMulticastPkts	送信マルチキャストパケット数
ifOutBroadcastPkts	送信ブロードキャストパケット数
ifOutDiscards	送信破棄パケット数
ifOutErrors	送信エラーパケット数

※0x3FFFFFFF は自生成パケット（RFC ではなく、IX 独自仕様）

Ethernet Interface Counters

dot3StatsAlignmentErrors	アライメントエラー
dot3StatsFCSErrors	FCS エラー
dot3StatsSingleCollisionFrames	シングルコリジョン
dot3StatsMultipleCollisionFrames	マルチプルコリジョン
dot3StatsSQETestErrors	SQE テストエラー
dot3StatsDeferredTransmissions	送信延期指示の検出回数
dot3StatsLateCollisions	レイトコリジョン
dot3StatsExcessiveCollisions	リトライオーバー
dot3StatsInternalMacTransmitErrors	内部 MAC 送信エラー
dot3StatsCarrierSenseErrors	キャリアセンスエラー
dot3StatsFrameTooLongs	ロングフレーム
dot3StatsInternalMacReceiveErrors	内部 MAC 受信エラー
dot3StatsSymbolErrors	シンボルエラー

2.51.2 sFlow エージェント設定

sFlow の設定および確認は次のコマンドを使用します。

sflow collector	sFlow コレクタの設定
sflow agent	sFlow エージェントの設定
sflow max-datagram-size	sFlow データグラムの最大サイズ設定
sflow sampling-rate	フローサンプリングレート設定
sflow max-header-size	フローサンプルの最大ヘッダサイズ設定
sflow polling-interval	カウンタサンプルの送信間隔設定
show sflow information	sFlow 情報の表示
clear sflow statistics	sFlow 統計情報の消去

```
【設定例】
Ver9.6 以降
sflow collector ip 192.168.100.100
sflow agent ip 192.168.1.1

device GigaEthernet0
   sflow polling-interval 30
   sflow sampling-rate 200 in    // 受信側のフローサンプリングレート設定
   sflow sampling-rate 400 out    // 送信側のフローサンプリングレート設定

device GigaEthernet1
   sflow polling-interval 30
   sflow sampling-rate 200 in
   sflow sampling-rate 400 out

interface GigaEthernet0.0
   ip address 192.168.0.1/24
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.1.1/24
   no shutdown

Ver9.5 以前の sflow sampling-rate  は in/out 指定がありません(in のみ)
device GigaEthernet0
   sflow polling-interval 30
   sflow sampling-rate 200
```

フローサンプルの動作条件は sflow collector と sflow sampling-rate が設定されていることで、カウンタサンプルの動作条件は sflow collector と sflow polling-interval が設定されていることです。

また、sFlow はデフォルトで UDP の 6343 番ポートを利用します。

2.51.3 sFlow エージェントの設定調整

2.51.3.1 フローサンプルの調整

IX ルータではサンプリングレートを逆数で登録します。N を設定した場合のサンプリングレートは 1/N で、平均 N 回に 1 回パケット情報を通知します。

サンプリングレートを低くすると（設定値を大きくすると）、パケットの収集頻度が低下するため装置負荷が小さくなりますが、統計的に予測するトラフィック量の誤差は大きくなり、低帯域のフローは監視しにくくなります。サンプリングレートを高くすると（設定値を小さくすると）、トラフィックの誤差は小さくなりますが、装置の負荷が上昇し、帯域の占有率が増えます。

サンプリングレートは求める精度や許容される負荷によって異なるため、利用環境ごとに調整する必要があります。目安が必要な場合は以下の値を参考にしてください。精度が十分であればサンプリングレートはなるべく低く（設定値をなるべく大きく）設定してしてください。

- 回線速度が 100Mbps で数 Mbps 以上のトラフィックを監視したい
  - ✧ サンプリングレートは 1/200 以下（設定値 200 以上）を設定してください。
- 回線速度が 1Gbps で数十 Mbps 以上のトラフィックを監視したい
  - ✧ サンプリングレートは 1/2000 以下（設定値 2000 以上）を設定してください。

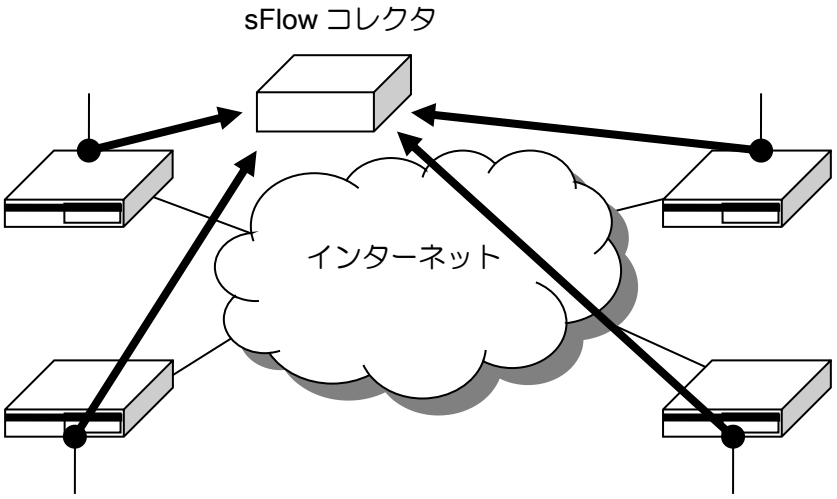
2.51.3.2 カウンタサンプルの調整

カウンタサンプルは指定した送信間隔ごとに統計情報を収集します。sFlow の仕様により、設定よりも早く収集することがあります。カウンタサンプルは統計情報を収集するだけで装置負荷への影響は比較的小さいですが、過剰な頻度で収集しないようにしてください。

2.51.4 IPsec 利用時の監視方法

sFlow はトラフィックをそのまま通知するため、VPN 区間のデバイスで動作させても暗号化されていてトラフィックを区別することができません。

Ver9.5 のように受信方向だけ動作させる場合、それぞれの拠点の LAN 側デバイスを監視してください。全トラフィックはいずれかの装置の LAN 側デバイスで受信されるため、監視可能です。



Ver9.6 以降では、送信方向のサンプリングも可能となっているため、センタルータの設定のみでネットワーク全体を監視できます（センタルータの LAN 側デバイスで送信と受信の両方を有効にする）。ただし、この方法では拠点間の通信を監視することはできません。

■2.52 アクセスリストの設定

2.52.1 IPv4/IPv6 アクセスリスト

アクセスリストは、トラフィックを様々な条件で識別する機能です。フィルタや QoS、ポリシールーティングなど多数の機能で利用し、トラフィック種別ごとに異なる条件でパケットを転送することができます。アクセスリストは設定を登録順（show running-config の表示順）に評価し、一致した条件の結果を返します。permit なら許可、deny なら拒否となります。

- Ver10.2 以降、アクセスリスト機能のシーケンス番号指定に対応しました。
- Ver9.6 以降、アクセスリスト機能の最適化による高速化に対応しました。アクセスリスト内にエントリが多数含まれる場合に転送性能が低下する場合がありましたが、高速化機能によって性能低下を抑制します。
- Ver9.6 以降、アクセスリストごとにキャッシュを無効化する機能に対応しました。IPsec や NAPT などでアクセスリストを設定する場合、無効化したほうが効率よくキャッシュを利用できます。

2.52.1.1 基本設定

アクセスリストは、次のコマンドで設定します。

ip access-list	IPv4 アクセスリストの設定
ipv6 access-list	IPv6 アクセスリストの設定
show ip access-list	IPv4 アクセスリストの表示
show ipv6 access-list	IPv6 アクセスリストの表示
show ip access-list cache	IPv4 アクセスリストのキャッシュ表示
show ipv6 access-list cache	IPv6 アクセスリストのキャッシュ表示

現在、アクセスリストで判定可能な項目は以下のようになります。

- プロトコル
- 送信元/送信先アドレス（プレフィックス指定 / マスク指定 / ドメイン名指定）
- 送信元/送信先ポート
- TCP ヘッダ制御フラグ
- TOS / TRAFFIC-CLASS フィールド（PRECEDENCE / DSCP / TOS）
- ICMP / ICMPv6 メッセージ
- フラグメント
- リンクマネージャのグループ情報（MG / SG）（Ver.9.6 以降）

2.52.1.2 TOS / TRAFFIC-CLASS フィールドの評価

TOS / TRAFFIC-CLASS フィールドを precedence および TOS、または DSCP の値で参照することができます。それぞれの設定は以下のとおりです。

- RFC791 / RFC1349 で定義されている TOS（Type of Service）フィールド

Precedence 3bits	D	T	R	M	0

precedence（=優先度）：
111 - Network Control
110 - Internetwork Control
101 - CRITIC/ECP
100 - Flash Override
011 - Flash
010 - Immediate
001 - Priority
000 - Routine

D（Delay=遅延）：
0 = Normal Delay
1 = Low Delay
T（Throughput=スループット）：
0 = Normal Throughput
1 = High Throughput
R（Reliability=信頼度）：
0 = Normal Reliability
1 = High Reliability
M（Money=コスト）
0 = Normal money cost
1 = Minimum money cost

- RFC2474 で Diffserv 用に定義されている TOS（Type of Service）フィールド

DSCP（Diffserv codepoint） 6bits	未使用

DSCP	
Default PHB 0（000000）	ベストエフォート（優先制御なし）
EF（Expedited Forwarding PHB） 46（101110） cf. RFC3246	パケットを最優先で転送 仮想専用線（低損失 低遅延 低ジッタ）
AF（Assured Forwarding PHB） 12 種類 cf. RFC2597	輻輳時に確率的にパケット廃棄 輻輳時の最低帯域を保証可能

2.52.1.3 ワイルドカードビット指定

アドレスはワイルドカードビット指定（マスク指定）でも設定可能です。ワイルドカードのビットが“1”の時は、そのビットは判定しません。

【設定例】

ip access-list list1 permit ip src 10.10.10.10 0.0.0.255 dest any

上記の場合、10.10.10.0 - 10.10.10.255 が許可されます。

2.52.1.4 フラグメントパケットの評価

IPv4 のフラグメントパケットは、2 番目以降のフラグメントパケットがポート番号を含まないため、ポート番号を指定したアクセスリストにマッチしません。フラグメントパケットの 2 番目以降にのみマッチする条件を記述できるため、フラグメントパケットを受信する環境でも、指定したポートの通信だけを許可できます。

※ ここではフラグメントの 2 番目以降のパケットのみをフラグメントパケットと呼びます。

【設定例 1】フラグメントオプションを利用しない場合の動作

```
ip access-list list1 permit tcp src any dest 192.168.0.10/32 dport eq 80
ip access-list list1 deny ip src any dest any
```

- 送信先が 192.168.0.10 のポート 80 の通信が permit になる設定ですが、ポート番号が取得できないフラグメントパケットは、元がポート 80 の通信でも 1 行目にはマッチできないため、2 行目で deny となります。

【設定例 2】フラグメントオプションを利用する場合の動作

```
ip access-list list2 permit tcp src any dest 192.168.0.10/32 dport eq 80
ip access-list list2 permit tcp src any dest 192.168.0.10/32 fragments
ip access-list list2 deny ip src any dest any
```

- 送信先が 192.168.0.10 のポート 80 の通信はフラグメントかどうかによらず、必ず permit になります。
- ただし、送信先が 192.168.0.10 のポート 80 以外の通信がフラグメントされていても先頭パケット以外は 2 行目にマッチして permit になるので注意が必要です。（フィルタで利用の場合、先頭はポート 80 以外が deny なので、ポート 80 以外の通信が成立することはありません）。

fragments を設定するアクセスリストは、プロトコル、IP アドレスのみ記述してください。ポート番号等のレイヤ 4 情報を設定しても無視されます。

なお、アクセスリストをフィルタで使用する場合は、フラグメントパケットを正確に判定するために、フィルタの「ip filter forced-reassembly」の機能を利用して、リアセンブルしてから判定処理を行うことも可能です。ただし、リアセンブルを行うのでルータの負荷は高くなる可能性があります。

TCP の通信については mss 調整機能でフラグメントの発生を抑制できます。TCP が分割される環境では極力 mss 調整機能を利用してください。

2.52.1.5 アクセスリストの高速化

Ver9.6 以降では、内部データベースを最適化し、アクセスリストの検索を高速化することができます。アクセスリストごとに以下のコマンドで設定可能です。

ip access-list NAME option optimize	IPv4 アクセスリストの高速化
ipv6 access-list NAME option optimize	IPv6 アクセスリストの高速化

1 つのアクセスリストに多数のエントリがある場合の検索を高速化します。

高速に処理するために、アクセスリストは以下の条件を満たす必要があります。

- 送信元、送信先アドレスに、ワイルドカードビット指定やドメイン指定を利用しない。
- permit や deny の行がなるべく連続するように記述する。
  - ✧ 上から permit または deny のブロック 4 つ目までが高速化対象

【設定例】

```
ip access-list list1 option optimize
ip access-list list1 permit ip src 192.168.0.0/24 dest 10.0.0.0/24          ↑
ip access-list list1 permit ip src 192.168.1.0/24 dest 10.0.1.0/24        ブロック(1)
                              :                                            |
ip access-list list1 permit ip src 192.168.9.0/24 dest 10.0.9.0/24        ↓
ip access-list list1 deny ip src 192.168.10.0/24 dest any                   ↑
                              :                                          ブロック(2)
ip access-list list1 deny ip src 192.168.19.0/24 dest any                   ↓
ip access-list list1 permit ip src 192.168.20.1/32 dest 10.0.20.1/32        ↑
                              :                                          ブロック(3)
ip access-list list1 permit ip src 192.168.29.1/32 dest 10.0.29.1/32        ↓
ip access-list list1 deny ip src 192.168.30.0/24 dest 10.0.30.0/24          ↑
                              :                                          ブロック(4)
ip access-list list1 deny ip src 192.168.39.0/24 dest 10.0.39.0/24          ↓
ip access-list list1 permit ip src 192.168.40.0/24 dest 10.0.40.0/24      以下の行は
                              :                                          高速化されない
ip access-list list1 permit ip src 192.168.255.0/24 dest 10.0.255.0/24
ip access-list list1 deny ip src any dest any
```

なお、最適化によってアクセスリストの評価結果が変わることはありません。最適化の都合上 permit や deny のブロックの中での評価順序が変更になる場合はあります。

2.52.1.6 アクセスリストのシーケンス番号指定

Ver10.2 以降、既存のアクセスリスト登録方式に加え、アクセスリストの各行にシーケンス番号を加えたコンフィグができます。（※ デフォルトはシーケンス番号なしのアクセスリスト設定）

ip access-list NAME sequence-mode	IPv4 アクセスリストのシーケンス番号指定
ipv6 access-list NAME sequence-mode	IPv6 アクセスリストのシーケンス番号指定
access-list NAME sequence-mode	MAC アクセスリストのシーケンス番号指定

※ ダイナミックアクセスリストではシーケンス番号指定はできません。

※ 従来のシーケンス番号なしのアクセスリストを「通常モード」のアクセスリスト、シーケンス番号ありのアクセスリストを「シーケンス番号指定モード」のアクセスリストとここでは呼びます。

アクセスリスト名単位で、通常モードとシーケンス番号指定モードのアクセスリストを混在させることができます。

【コンフィグ例】

```
ip access-list name1 permit ip src 192.168.0.0/24 dest 10.0.0.0/24
ip access-list name1 permit ip src 192.168.1.0/24 dest 10.0.1.0/24
ip access-list name1 permit ip src 192.168.9.0/24 dest 10.0.9.0/24
ip access-list name1 deny ip src 192.168.10.0/24 dest any
ip access-list name1 deny ip src 192.168.11.0/24 dest any
ip access-list name1 deny ip src 192.168.19.0/24 dest any
ip access-list name1 permit ip src any dest any

ip access-list name2 sequence-mode 100
ip access-list name2 100 permit ip src 192.168.20.1/32 dest 10.0.20.1/32
ip access-list name2 200 permit ip src 192.168.21.1/32 dest 10.0.21.1/32
ip access-list name2 300 permit ip src 192.168.29.1/32 dest 10.0.29.1/32
ip access-list name2 400 deny ip src 192.168.30.0/24 dest 10.0.30.0/24
ip access-list name2 500 deny ip src 192.168.31.0/24 dest 10.0.31.0/24
ip access-list name2 600 deny ip src 192.168.39.0/24 dest 10.0.39.0/24
ip access-list name2 700 permit ip src any dest any
```

通常モードのコンフィグに対し、シーケンス番号指定オプションを設定すると、シーケンス番号の自動付与間隔に従ってシーケンス番号が自動的に付与されます。

※ アクセスリスト高速化設定時は、高速化のブロック単位でシーケンス番号が自動的に付与されます。（シーケンス番号指定で追加されたコンフィグによりブロックが変更になった場合に自動的に番号が振りなおされるものではありません）

- ✧ ブロック(1): 0～
- ✧ ブロック(2): 1000000～
- ✧ ブロック(3): 2000000～
- ✧ ブロック(4): 3000000～
- ✧ 最適化対象外: 4000000～

2.52.1.7 アクセスリストキャッシュの無効化

Ver9.6 以降では、アクセスリストごとにキャッシュの生成・参照を無効化できます。

ip access-list NAME option nocache	IPv4 アクセスリストキャッシュの無効化
ipv6 access-list NAME option nocache	IPv6 アクセスリストキャッシュの無効化

以下のような機能での利用に効果があります。

IKEv1/IPSec 機能

IPsec で設定するアクセスリストは通常 any を 1 行設定するのみのため、キャッシュなしで高速判定可能です。アクセスリストキャッシュを無効化し、キャッシュの消費を抑制することで、キャッシュのオーバーフロー発生頻度を抑制できます。

【設定例】

```
ip access-list sec-list option nocache
ip access-list sec-list permit ip src any dest any
!
ipsec autokey-map ipsec-policy sec-list peer 20.20.20.20 ipsec-prop
```

2.52.1.8 アクセスリストキャッシュのタイムアウト指定

Ver9.6 以降では、アクセスリストキャッシュのタイムアウト時間を変更可能です。

ip access-list cache timeout	キャッシュのタイムアウト時間変更
ipv6 access-list cache timeout	キャッシュのタイムアウト時間変更

タイムアウト時間を短く変更することで、アクセスリストキャッシュのオーバーフロー発生頻度を抑制できる場合があります。あまり短く設定すると、キャッシュ生成回数が増えて負荷が上昇する可能性もあります。

2.52.2 ドメイン名指定

アクセスリストのドメイン名指定は不具合のため、現在使用を制限しています。

(a) 逆引きができない場合の動作

逆引きが正常にできない場合（ネガティブキャッシュに該当する場合）に、次のアクセスリストの評価を行うか、アクセスリストの評価を終了するかを指定することができます。

ip access-list disregard-case dns negative-cache	IPv4 アクセスリスト DNS ネガティブキャッシュ評価の設定
ipv6 access-list disregard-case dns negative-cache	IPv6 アクセスリスト DNS ネガティブキャッシュ評価の設定

上記のコマンドを設定した場合は、逆引きができない場合でも次のアクセスリストの評価を行います。設定しない場合（デフォルト）は、それ以降のアクセスリストの評価は行わず deny となります。

Ver7.1 以降は、DNS キャッシュのアドレスデータベースを使用できます。端末が最初に正引きした結果をデータベースとして保存することで逆引きできない環境でも動作可能になります。ただし、端末が正引きしない場合やアドレスデータベースが端末のキャッシュ保持時間より短く先にタイムアウトした場合などに正常動作しなくなるため、利用については十分ご注意ください。

(b) その他注意事項

また、逆引きの結果が複数存在する場合は、全てについて設定しないと正しく動作しません。逆引きの応答パケットの Answers に CNAME が 10 以上つながる場合でもホスト名の獲得ができないため、これらに該当する IP アドレスは、直接アクセスリストに設定してください。

2.52.3 ダイナミックアクセスリスト

ダイナミックアクセスリストは、ダイナミックフィルタ機能で利用されます。ダイナミックフィルタの詳細についてはパケットフィルタの章を参照してください。

2.52.4 MAC アクセスリスト

MAC アクセスリストは、レイヤ 2 情報により許可／拒否の判定を行います。判定条件が異なる以外は通常のアクセスリストと同様な動作となります。

現在、MAC アクセスリストを利用する機能（サブシステム）には以下のようなものがあります。機能毎のアクセスリストの利用方法については、各機能の項目を参照してください。

- MAC フィルタ
- QoS（ブリッジ）

アクセスリストは、次のコマンドで設定します。

access-list	MAC アクセスリストの設定
show access-list	MAC アクセスリストの表示
show access-list cache	MAC アクセスリストのキャッシュ表示

現在アクセスリストで判定可能な項目は以下のようになります。

- 送信元/送信先 MAC アドレス指定
- Ethernet ヘッダの Type フィールド指定
- VLAN タグの COS フィールド指定
- VLAN タグの CFI フィールド指定
- VLAN タグの VLAN-ID 指定
- 任意の位置（オフセット）指定
- リンクマネージャのグループ情報 (Ver.9.6 以降)

(a)ワイルドカードビット指定

MAC アドレスの指定には、ワイルドカードビット指定を行うことができます。”1”のビットの位置が任意の値となります。

【設定例】

access-list list1 permit src 00:11:22:33:44:00 00:00:00:00:00:ff dest any

上記の場合、00:11:22:33:44:00 - 00:11:22:33:44:ff が許可されます。

(b)オフセット指定

オフセット指定を使用することにより、任意の位置の値を条件とすることができます。MAC アクセスリストでは通常は IP アドレスを条件とすることはできませんが、オフセット指定で IP アドレスの位置を指定することにより、IP アドレスを条件とすることが可能です。オフセットはゼロオリジンなので、パケットの先頭を指定する場合のオフセットは 0 になります。

【設定例】

access-list list1 permit src any dest any offset 26 4 0a000001

上記の場合、先頭から 26byte の位置（VLAN タグなしの場合送信元アドレス）からの値が 0x0a000001（10.0.0.1）のパケットが許可されます。

■2.53ルートマップの設定

ルートマップは、ポリシールーティングもしくは、ダイナミックルーティングプロトコルにおける経路再配信設定など、特にルートに関する高度な設定を必要とする場合において使用します。

ルートマップは、シーケンス番号順（登録時に設定）に評価し、match 指定にルートやアドレスが一致した場合に、set 指定にしたがって各機能（各サブシステム）に結果を返し実行されます。

現在、ルートマップを利用する各機能（各サブシステム）には以下のようなものがあります。各機能のルートマップの利用方法については、各機能の項目を参照してください。

- ポリシールーティング
- RIP/RIPng
- OSPFv2/v3
- BGP4

ルートマップは、次のコマンドで設定します。

route-map	ルートマップ
match interface	出先インタフェースを条件とします。
match ip address	IPv4 アドレスを条件とします。
match ip next-hop	IPv4 ネクストホップを条件とします。
match ipv6 address	IPv6 アドレスを条件とします。
match ipv6 next-hop	IPv6 ネクストホップを条件とします。
match metric	メトリック値を条件とします。
match tag	タグ値を条件とします。
match community	コミュニティ値を条件とします。（Ver.8.9 以降）
match ip url-offload	URL オフロード対象を条件とします。（Ver.9.4 以降）
set interface	送信インタフェースを設定します。
set default interface	デフォルト送信インタフェースを設定します。
set ip next-hop	IPv4 ネクストホップを設定します。
set ip default next-hop	デフォルト IPv4 ネクストホップを設定します。
set ipv6 next-hop	IPv6 ネクストホップを設定します。
set ipv6 default next-hop	デフォルト IPv6 ネクストホップを設定します。
set metric	メトリック値を設定します。
set metric-type	メトリックタイプを設定します。
set tag	タグ値を設定します。
set as-path prepend	BGP の AS パス属性に AS をプリペンドします。
set local-preference	BGP のローカルプリファレンス属性を設定します。
set origin	BGP のオリジン属性を設定します。
set community	コミュニティ値を設定します。（Ver.8.9 以降）
show route-map	ルートマップを表示します。
clear route-map	統計情報をクリアします。

■2.54 プレフィックスリストの設定

プレフィックスリストは、ダイナミックルーティングプロトコルのパケットをパケット単位もしくはルート単位でアクセス制限指定するために使用します。

プレフィックスリストは、シーケンス番号順（登録時に設定）に評価し、一致するものが検索できた場合には、その時点の結果（permit または deny）を各機能（各サブシステム）に返し評価されます。それ以降のリストは評価しません。

現在、プレフィックスリストを利用する機能（サブシステム）には以下のようなものがあります。機能毎のプレフィックスリストの利用方法については、各機能の項目を参照してください。

- RIP/RIPng
- OSPFv2/v3
- BGP
- ルートマップ

プレフィックスリストは、次のコマンドで設定します。

ip prefix-list	IPv4 プレフィックスリストの設定
ipv6 prefix-list	IPv6 プレフィックスリストの設定
show ip prefix-list	IPv4 プレフィックスリストの表示
show ipv6 prefix-list	IPv6 プレフィックスリストの表示

現在、プレフィックスリストで判定可能な項目には以下があります。

- プレフィックス
- プレフィックス長

【設定例 1】

10.0.0.0/24 のみ許可
```
ip prefix-list list1 10 permit 10.0.0.0/24
```

【設定例 2】
10.0.0.0/16～10.0.255.0/24 の経路を許可
```
ip prefix-list list 10 permit 10.0.0.0/16 max 24
```

■2.55 UFS キャッシュの設定

UFS キャッシュ（Unified Forwarding Service Cache）は、フィルタ、NAT/NAPT、IPsec などのサービスを使用している場合に有効な高速フォワーディングキャッシュメカニズムであり、IX2000/IX3000 の独自機能です。UFS キャッシュにより、フィルタの多段設定、IPsec の複数設定等におけるスケーラビリティを向上させます。

2.55.1 概要

フィルタや IPsec では、パケットに応じてどの設定を有効にするかを決定するために、それぞれにパケット検索処理やその結果を保持するキャッシュを持っています。通常これらは機能毎にそれぞれ独立に動作し、その検索結果に基づいて処理が行われています。

ここで、パケットの受信から送信までの間に各サービスで行われていた検索処理を 1 回で済ませることができれば、検索時間を大幅に短縮することができると考えられます。UFS キャッシュは、複数のサービスで行っていた検索を一元化し、複数サービスの検索結果を統合します。フォワーディング処理における複数サービスの統合したキャッシュを用いることから、UFS キャッシュ（Unified Forwarding Service Cache）と呼んでいます。

以下の機能が UFS キャッシュに対応しています。

- スタティックフィルタの検索結果（通過 or 廃棄）
- NAT/NAPT キャッシュ（変換アドレスなど）
- IPsec の各種検索結果（SA など）
- ルーティングキャッシュ情報（出力インタフェースなど）
- ポリシールーティング情報　（出力インタフェースなど）
- QoS 情報　（クラス、キュー、カラーリング情報など）
- ダイナミックフィルタ情報　（通過キャッシュ情報など）
- NGN データコネクト対応（送信先アドレス、ポートなど）（Ver.8.6 以降）
- GRE トンネル対応（キー情報など）（Ver.8.11 以降）
- ダイナミック VPN 情報（Ver.9.2 以降）
- UTM ファーストパス情報（Ver.10.0 以降）

2.55.2 動作原理

UFS キャッシュでは、プロトコルごとに下記の条件に基づきパケットを分別します。

※ 以下で、IPv6 の場合には TOS ではなく Traffic class です。

・TCP

プロトコル	送信元アドレス /ポート	送信先アドレス /ポート	TOS	TCP-flag	

・UDP

プロトコル	送信元アドレス /ポート	送信先アドレス /ポート	TOS	

・AH/ESP（IPsec）

プロトコル	送信元アドレス	送信先アドレス	TOS	SPI	

・GRE

プロトコル	送信元アドレス	送信先アドレス	TOS	GRE-flag	GRE-Key

・TCP/UDP/AH/ESP/GRE/ICMP 以外

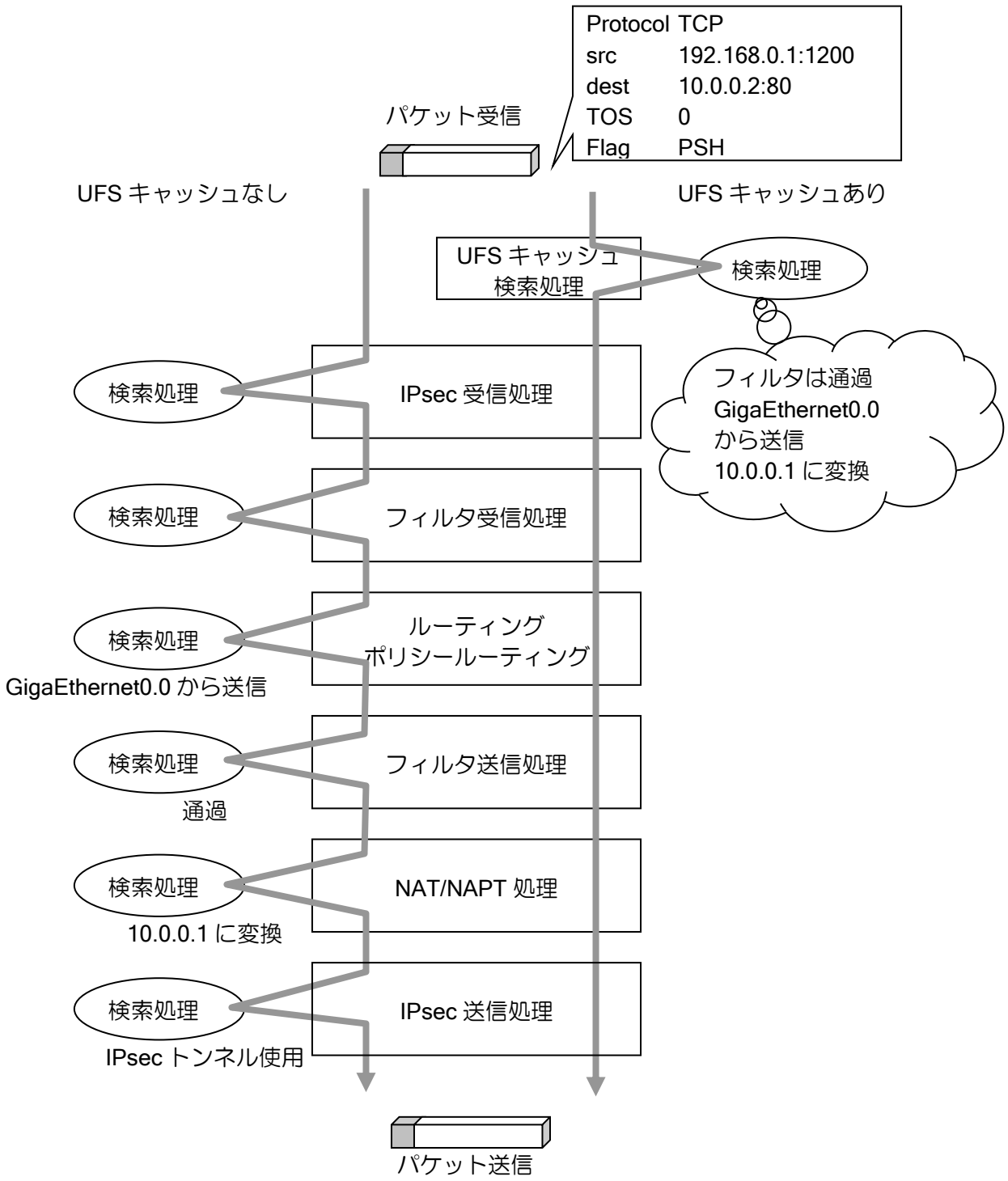
プロトコル	送信元アドレス	送信先アドレス	TOS	

・ICMP
使われません（判定処理の増加に対する効果が小さいため）

・COS
・qos-group（QoS の項を参照してください）

フローごとに上記のサービスの情報を 1 つの UFS キャッシュに登録するため、パケット受信時に最初に 1 度だけ検索処理を行えば、その時点でパケットがどのように処理されるかが決定されます。UFS キャッシュを使用しない場合には、それぞれのサービスで繰り返しキャッシュを検索する必要が生じます。

以下に UFS キャッシュが有効/無効の場合のフォワーディング処理を図示します。



※ UFS キャッシュは、自装置が送信元となるパケットには適用されません。IPsec はトランスポートの場合には適用されませんので、ご注意ください。

2.55.3 UFS キャッシュの設定

UFS キャッシュの設定は次のコンフィグを使用します。IPv4/IPv6 は個別に設定します。

IPv4 コンフィグ

ip ufs-cache enable	IPv4 UFS キャッシュの有効 （グローバルコンフィグモード）
ip ufs-cache hash	IPv4 UFS キャッシュのハッシュサイズ変更 （インタフェースコンフィグモード）
ip ufs-cache max-entries	IPv4 UFS キャッシュの最大エントリ数設定 （グローバルコンフィグモード）
ip ufs-cache timeout	IPv4 UFS キャッシュのタイムアウト設定 （インタフェースコンフィグモード）
show ip ufs-cache	IPv4 UFS キャッシュの表示
clear ip ufs-cache	IPv4 UFS キャッシュの消去

IPv6 コンフィグ

ipv6 ufs-cache enable	IPv6 UFS キャッシュの有効 （グローバルコンフィグモード）
ipv6 ufs-cache hash	IPv6 UFS キャッシュのハッシュサイズ変更 （インタフェースコンフィグモード）
ipv6 ufs-cache max-entries	IPv6 UFS キャッシュの最大エントリ数設定 （グローバルコンフィグモード）
ipv6 ufs-cache timeout	IPv6 UFS キャッシュのタイムアウト設定 （インタフェースコンフィグモード）
show ipv6 ufs-cache	IPv6 UFS キャッシュの表示
clear ipv6 ufs-cache	IPv6 UFS キャッシュの消去

【設定例】

```
ip ufs-cache enable
ipv6 ufs-cache enable

interface GigaEthernet0.0
   ip address 10.0.0.1/24
   ipv6 address 2001:db8:1::1/64
   no shutdown
```

2.55.4 UFS キャッシュの表示

Ver.8.2 以降 UFS キャッシュの表示方法が拡張されています。

show ip ufs-cache show ipv6 ufs-cache	有効なキャッシュのみを簡易表示します。
show ip ufs-cache verbose show ipv6 ufs-cache verbose	無効となったキャッシュを含め、詳細に表示します。
show ip ufs-cache entries show ipv6 ufs-cache entries	インタフェース毎のキャッシュ表示数を制限します。 ※ 0 を指定時はヘッダ情報のみ表示します。

※表示内容については、統計情報一覧を参照してください

2.55.4.1 無効キャッシュ

Ver.8.2 以降では、タイムアウトもしくは、UFS キャッシュを利用している機能から無効と宣言されたキャッシュは即時に削除せず、無効キャッシュとなります。無効キャッシュは約 2 分を周期とした UFS キャッシュクリア機構によって順次削除されます。無効キャッシュ時のキャッシュには、以下の特徴があります。

- show ip/ipv6 ufs-cache verbose で UFS キャッシュを表示させたとき、「Codes: D - Scheduled to delete」で表示されます。
- 無効キャッシュに対し、パケットが検索マッチした場合、そのキャッシュに含まれるすべての情報をクリアした上で、有効なキャッシュになります。ただし、ヒットカウントやアップタイムはクリアしません。（show ip ufs-cache では、無効キャッシュ時は表示されないため、有効キャッシュに戻ることによって、アップタイムの大きなキャッシュが突然表示されるように見えますが、問題ではありません。）

2.55.5 消費メモリ量

UFS キャッシュは各種サービスの情報を保存するため、メモリを大量に消費します。特に ip/ipv6 ufs-cache max-entries 等でキャッシュサイズを変更する際には、システムの残りメモリに注意して設定する必要があります。

バージョン	IPv4 UFS キャッシュ	IPv6 UFS キャッシュ
7.2 まで	768 bytes/entry	512 bytes/entry
7.3～8.1	1024 bytes/entry	768 bytes/entry

Ver.8.2 以降では、UFS キャッシュ有効時や、ip/ipv6 ufs-cache max-entries による設定変更時には UFS キャッシュエントリのメモリを確保しません。実際にキャッシュが必要となった時点で、128KB 単位でメモリを確保します。（一度確保した UFS キャッシュで使用するメモリは、clear ip/ipv6 ufs-cache をグローバルコンフィグで実行しない限り解放されません。）

バージョン	IPv4 UFS キャッシュ	IPv6 UFS キャッシュ
8.2～8.5	約 825 bytes/entry	約 600 bytes/entry
8.6～8.10	約 860 bytes/entry	約 600 bytes/entry
8.11～9.1	約 900 bytes/entry	約 635 bytes/entry
9.2～9.7	約 930 bytes/entry	約 670 bytes/entry
10.0～10.3	約 716 bytes/entry	約 537 bytes/entry
10.4～	約 760 bytes/entry	約 552 bytes/entry

UFS キャッシュで必要となるメモリは、キャッシュエントリのほかに、インタフェースあたりのハッシュテーブルがあります。Ver.8.2 以降では、「show ip/ipv6 ufs-cache verbose」にて、現在 UFS キャッシュで使用しているメモリのサイズを確認することができます。（今後必要となるメモリのサイズを含みません。）

2.55.6 ハッシュテーブルサイズの拡張について

ip ufs-cache hash	IPv4 UFS キャッシュのハッシュサイズ変更 （インタフェースコンフィグモード）
ipv6 ufs-cache hash	IPv6 UFS キャッシュのハッシュサイズ変更 （インタフェースコンフィグモード）

UFS キャッシュの最大エントリ数をデフォルト値以上に拡張する場合において、特定のインタフェースで生成されるキャッシュが下記に記載のキャッシュ数を超えている場合、該当インタフェースのハッシュサイズを拡張すると性能向上することがあります。（IX3315 などで特定のインタフェースに入力するフローが倍の 10 万エントリになる場合は、ハッシュテーブルサイズも倍の 4096 などにすることで効果が得られる場合があります。）

ハッシュテーブルサイズ	インタフェースあたりのメモリサイズ	インタフェースあたりのキャッシュ拡張目安
1024	8,192 bytes/interface	32,768 caches/interface
2048	16,384 bytes/interface	65,536 cashs/interface
4096	32,768 bytes/interface	100,000 caches/interface
8192	65,536 bytes/interface	200,000 caches/interface

※本設定は、ハッシュサイズを変更しないと特に問題が発生するものではなく、最大キャッシュサイズ付近で運用時のパフォーマンス改善の参考となります。
※ハッシュサイズ拡張の目安は、IX2000/IX3000 シリーズで特に区別はありません。
※IX2000 シリーズで最大キャッシュ数を仕様制限内で利用する限りは設定変更の必要はありません。（最大キャッシュ数を最大値の 40,000 に設定していてもインタフェースあたりのキャッシュ数が 25,000 を超えることはほぼ無いため）
※IPsec などトンネルインタフェースが大量に存在する場合に、一律にハッシュテーブルサイズを拡張するとメモリ枯渇の原因となります。あくまでも該当インタフェースに上記を目安とした多くのフローが同時に入力される場合にのみ拡張してください。

■2.56 OpenFlow の設定

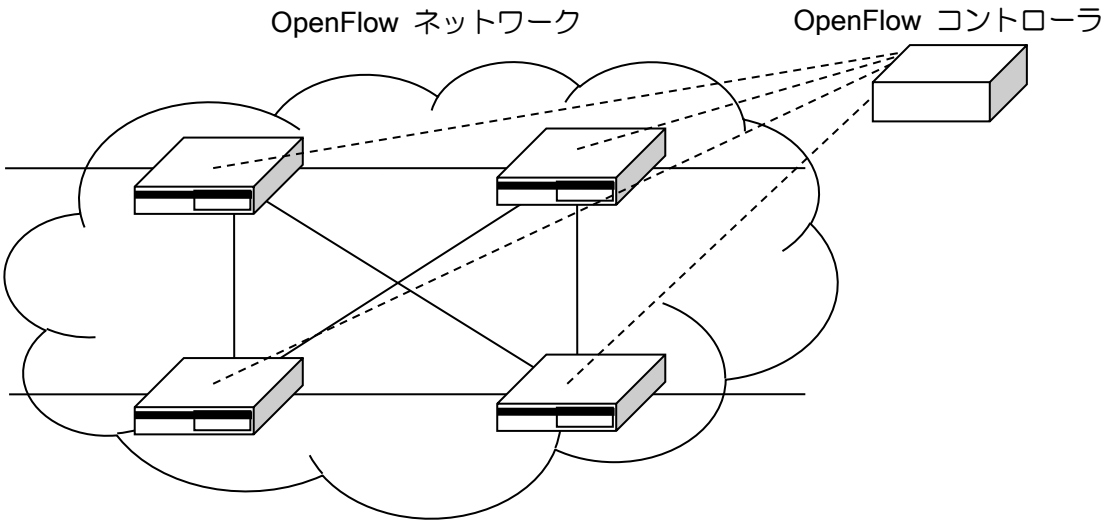
IX2000/IX3000 シリーズルータは OpenFlow Switch Specification 1.3.1 に準拠した OpenFlow スイッチとして動作します。

Ver.9.0 以降に対応します。IX3015 は未対応です。

また、Ver.9.0.54 以降では NEC の ProgrammableFlow 制御に正式対応しており、OpenFlow を利用して WAN ソリューションを実現することができます。ProgrammableFlow の詳細や対応状況については、PF6800 等のマニュアルを参照してください。

2.56.1 OpenFlow 機能概要

OpenFlow のネットワークは、OpenFlow コントローラと OpenFlow スイッチの 2 種類の装置から構成されます。従来のスイッチでは経路制御とパケット転送の両方をスイッチ自身が行っていましたが、OpenFlow では経路制御を OpenFlow コントローラが行い、OpenFlow スイッチはコントローラの指示に従ってパケットを転送します。



OpenFlow スイッチは、パケット転送をフローテーブルで行います。フローテーブルにはパケットのマッチ条件とマッチしたパケットに適用するインストラクション（アクション）などから構成されたフローエントリを登録します。パケット転送やパケットの書き換え、VLAN タグの付与/除去、QoS のキュー指定等も可能で、コントローラから自由にパケットを制御することができます。

コントローラは管理下の全ての OpenFlow スイッチを制御し、設定変更や情報収集、イベント通知の受信などにより、ネットワーク全体を集中管理することが可能です。

ただし、コントローラとの通信に障害が発生すると制御不能になるため、制御通信の管理が重要であること、通信開始時にコントローラに処理を問い合わせる必要があること、多数のフローを高速転送するためにはフローエントリの仕組みを理解しておく必要があるなど、障害や性能に配慮したネットワーク設計および制御が必要です。

2.56.2 注意事項・制限事項

- OpenFlow Switch Specification 1.3.1 の必須機能をサポートしており、同機能をサポートしている任意のコントローラから OpenFlow プロトコルで制御することが可能です。なお、特定のコントローラとの接続を保証するものではないため、事前にコントローラ側のプロトコル仕様の確認、および接続検証の実施をお願いします。
- IX のルータ機能では転送に関わる情報の内部構造を工夫することにより高性能を実現していますが、OpenFlow 機能では転送にかかわる情報の制御をコントローラが行います。このため、IX が高速処理できる形式でフローエントリを登録するようにコントローラから制御しなければ、十分な転送性能を得られない場合があります。IX ルータの高速化の仕組みをご確認いただき、十分な動作検証を行ったうえでご利用ください。
- ブロードキャスト、マルチキャストなどのトラフィックは、送信先が多くなると性能の大幅低下につながります。ARP や VRRP などのプロトコルに注意してください。
- コントローラとの接続は IPv4 のみに対応しています。
- Flow-Mod の CHECK_OVERLAP 機能のみ、本来の実装と異なります。詳細は Flow-Mod の項目を参照してください。

2.56.3 OpenFlow ポート機能

OpenFlow でパケットを送受信するインタフェースを OpenFlow ポートと呼びます。OpenFlow で制御するためには、OpenFlow で送受信を制御したいインタフェース全てに OpenFlow ポートの設定を行い、任意のポート番号と名前を割り当てる必要があります。

OpenFlow ポートに割り当てることができるインタフェースは以下の通りです。なお、IX ルータでは、OpenFlow ポート番号として使用できる値を 1～65535 に制限しています。

- 物理ポート/論理ポート

イーサネットポートのほか、以下のように L2 のトンネルインタフェースも利用可能です。WAN の VPN を通して OpenFlow で制御することができます。

  - Ethernet インタフェース（ポート VLAN を含む。タグ VLAN や PPPoE の I/F は指定不可）
  - Ethernet over GRE インタフェース
  - Ethernet over GRE over IPsec インタフェース
  - BVI インタフェース

※GRE トンネルは IP パケットと Ethernet フレームを同時にカプセル化できるため、コントローラとの制御用通信と、OpenFlow で転送するユーザトラフィックを 1 つのトンネルで送信することができます。

※BVI インタフェースを OpenFlow ポートに割り当てることで、ルータ機能と OpenFlow 機能を併用することができます。

※SW-HUB は、全体を 1 つの OpenFlow ポートとして割り当てることも、ポート VLAN を設定して物理ポート毎にそれぞれ OpenFlow ポートを設定することも可能です。

- 予約済みポート対応状況

パケット転送は、特定のポートを指定して送信するほか、予約済みのポートを利用することが可能です。予約済みポートの対応状況は以下の通りです。

予約済みポート	対応	説明
IN PORT	○	入力ポート（パケットを受信ポートに送信）
TABLE	○	テーブル指定（Packet-Out で送信先をテーブルで決定）
NORMAL	×	従来機能での転送（OpenFlow で制御しない）
FLOOD	×	ブロックされたポートと受信ポート以外の全ポート
ALL	○	受信ポート以外の全ポート
CONTROLLER	○	コントローラ
LOCAL	×	ローカルポート
ANY	○	指定なし（入出力ポートとしては利用しません）

2.56.4 OpenFlow テーブル機能

2.56.4.1 フローテーブル

OpenFlow 機能がパケットを転送するときに参照するテーブルです。パケットの種類ごとに送信先や書き換えなどの指示を行うフローエントリをコントローラから自由に登録・削除して制御します。フローエントリはプライオリティ順に参照され、全てのフローエントリに該当しないパケットは廃棄します。

フローテーブルは 0～254 の 255 個全て利用可能です。受信フレームが最初に参照するのはフローテーブル 0 で、テーブル 1 以降はフローエントリのインストラクションに Goto-Table を指定して使います。

なお、IX ルータのフローテーブルは、高速転送のために独自のハッシュ機能を実装しています。詳細は後述のハッシュ機能を参照してください。

2.56.4.2 フローエントリ

フローテーブルに登録されるフローエントリは主に以下の要素を持っています。

マッチフィールド	パケットをマッチさせる条件を記述するフィールド
プライオリティ	フローエントリの優先度（数値の大きい順に判定）
カウンター	統計情報
インストラクション	マッチしたパケットの動作を記述するフィールド
タイムアウト	フローエントリの保持時間

コントローラから Flow-Mod というメッセージで、フローエントリの登録・削除・変更を行います。フローエントリの削除は明示的な命令のほか、2 種類のタイムアウト（無通信時間または固定時間）で自動的に消去させることも可能です。

パケット転送の際には、プライオリティ順にフローエントリを参照し、マッチフィールドに合致した場合、指定のインストラクション（アクション）を実行することで動作します。

プライオリティが 0 のフローエントリを特にテーブルミスエントリと呼び、他の全てのフローエントリにマッチしなかった場合の動作を指定します。このエントリも存在しない場合、パケットは廃棄します。

マッチ条件の対応状況は以下の通りです。

マッチ条件	対応	説明
OFPXMT_OFB_IN_PORT	○	受信ポート
OFPXMT_OFB_IN_PHY_PORT	×	受信物理ポート
OFPXMT_OFB_METADATA	○	メタデータ
OFPXMT_OFB_ETH_DST	○	送信先イーサネットアドレス
OFPXMT_OFB_ETH_SRC	○	送信元イーサネットアドレス
OFPXMT_OFB_ETH_TYPE	○	イーサタイプ
OFPXMT_OFB_VLAN_VID	○	VID（VLAN Identifier）
OFPXMT_OFB_VLAN_PCP	○	PCP（Priority Code Point）
OFPXMT_OFB_IP_DSCP	○	DSCP（Differentiated Service Code Point）
OFPXMT_OFB_IP_ECN	○	ECN（Explicit Congestion Notification）
OFPXMT_OFB_IP_PROTO	○	IPv4/IPv6 プロトコル
OFPXMT_OFB_IPV4_SRC	○	IPv4 送信元アドレス
OFPXMT_OFB_IPV4_DST	○	IPv4 送信先アドレス
OFPXMT_OFB_TCP_SRC	○	TCP 送信元ポート番号
OFPXMT_OFB_TCP_DST	○	TCP 送信先ポート番号
OFPXMT_OFB_UDP_SRC	○	UDP 送信元ポート番号
OFPXMT_OFB_UDP_DST	○	UDP 送信先ポート番号
OFPXMT_OFB_SCTP_SRC	×	SCTP 送信元ポート番号
OFPXMT_OFB_SCTP_DST	×	SCTP 送信先ポート番号
OFPXMT_OFB_ICMPV4_TYPE	○	IPv4 ICMP タイプ
OFPXMT_OFB_ICMPV4_CODE	○	IPv4 ICMP コード
OFPXMT_OFB_ARP_OP	○	ARP オペレーションコード
OFPXMT_OFB_ARP_SPA	○	ARP 送信元 IP アドレス
OFPXMT_OFB_ARP_TPA	○	ARP 送信先 IP アドレス
OFPXMT_OFB_ARP_SHA	○	ARP 送信元 MAC アドレス
OFPXMT_OFB_ARP_THA	○	ARP 送信先 MAC アドレス
OFPXMT_OFB_IPV6_SRC	○	IPv6 送信元アドレス
OFPXMT_OFB_IPV6_DST	○	IPv6 送信先アドレス
OFPXMT_OFB_IPV6_FLABEL	○	IPv6 フローラベル
OFPXMT_OFB_ICMPV6_TYPE	○	IPv6 ICMP タイプ
OFPXMT_OFB_ICMPV6_CODE	○	IPv6 ICMP コード
OFPXMT_OFB_IPV6_ND_TARGET	○	ND ターゲット IPv6 アドレス
OFPXMT_OFB_IPV6_ND_SLL	○	ND 送信元リンクレイヤアドレス
OFPXMT_OFB_IPV6_ND_TLL	○	ND ターゲットリンクレイヤアドレス
OFPXMT_OFB_MPLS_LABEL	×	MPLS ラベル
OFPXMT_OFB_MPLS_TC	×	MPLS TC
OFPXMT_OFB_MPLS_BOS	×	MPLS BOS
OFPXMT_OFB_PBB_ISID	×	PBB I-SID
OFPXMT_OFB_TUNNEL_ID	×	トンネル ID
OFPXMT_OFB_IPV6_EXTHDR	×	IPv6 拡張ヘッダ

なお、bitmask の利用が定義されていないタイプに対しても、独自に全てのフィールドで bitmask を利用可能としています。

インストラクションの対応状況は以下の通りです。
Apply-Actions は Ver.9.0.54 以降、Clear-Actions は Ver.9.3 以降の対応です。

インストラクション	対応	説明
Meter	×	メーターの設定
Apply-Actions	○	アクションの適用（即時）
Clear-Actions	○	登録されたアクションを消去
Write-Actions	○	アクションの登録（パイプライン終了時に適用）
Write-Metadata	○	メタデータの登録
Goto-Table	○	指定のテーブルに飛ぶ

アクションの対応状況は以下の通りです。

アクション	対応	説明
Output	○	パケットを指定ポートに送信
Set-Queue	○	QoS のキュー指定（※ qos-group 値として利用）
Drop	○	廃棄
Group	○	指定したグループエントリのアクションを適用
Push-Tag/Pop-Tag	○	タグの付与/除去（VLAN タグのみ対応）
Set-Field	○	パケットのヘッダ書き換え（送信元/送信先イーサネットアドレス、イーサタイプ、VID、PCP のみ対応）
Change-TTL	×	TTL の書き換え

Set-Queue で指定する qos-group の設定は QoS の項目を参照してください。

2.56.4.3 グループエントリ

フローエントリでは直接記述できないアクションを設定する場合に利用します。フローエントリの Group アクションで Group ID を指定することで利用できます。

グループタイプの対応状況は以下の通りです。

グループタイプ	対応	説明
all	○	全てのアクションバケツを実行します。
select	×	複数のアクションバケツを選択して実行します。
indirect	○	単一のアクションバケツを実行します。
fast failover	○	最初の LIVE 状態のアクションバケツを実行します。（指定ポートが link-up なら LIVE です）

グループエントリには複数のアクションバケツを登録することができ、それぞれにアクションを登録することができます。グループから別のグループを指定するチェーン機能は未対応です。

グループを利用することで、複数のフローエントリのアクションを一括で変更することができます。また、fast failover では、障害発生時にコントローラからフローを変更することなく、自律的に迂回経路に切り替えるなどの利用が可能です。

OpenFlow 1.3 の仕様により、グループエントリを削除すると利用しているフローエントリは全て削除されます。

2.56.4.4 カウンタ

カウンタの対応状況と説明は以下の通りです。

Per Flow Table	対応	説明
Reference Count (active entries)	○	テーブルに存在するフローエントリ数
Packet Lookups	○	パケットが参照した回数
Packet Matches	○	パケットがマッチした回数

Per Flow Entry	対応	説明
Received Packets	○	マッチしたパケット数
Received Bytes	○	マッチしたパケットの合計サイズ
Duration (seconds)	○	テーブルに登録してからの経過時間（秒）
Duration (nanoseconds)	×	経過時間（ナノ秒）

Per Port	対応	説明
Received Packets	○	受信パケット数
Transmitted Packets	○	送信パケット数
Received Bytes	○	受信パケットの合計サイズ
Transmitted Bytes	○	送信パケットの合計サイズ
Receive Drops	○	受信廃棄したパケットのサイズ
Transmit Drops	○	送信廃棄したパケットのサイズ
Receive Errors	×	受信エラーパケット数
Transmit Errors	×	送信エラーパケット数
Receive Frame Alignment Errors	×	受信アライメントエラー
Receive Overrun Errors	×	受信オーバーランエラー
Receive CRC Errors	×	受信 CRC エラー
Collisions	×	コリジョン数
Duration (seconds)	○	ポートを登録してからの経過時間（秒）
Duration (nanoseconds)	×	経過時間（ナノ秒）

Per Group	対応	説明
Reference Count (flow entries)	○	グループを参照しているフローエントリ数
Packet Count	○	マッチしたパケット数
Byte Count	○	マッチしたパケットの合計サイズ
Duration (seconds)	○	テーブルに登録してからの経過時間（秒）
Duration (nanoseconds)	×	経過時間（ナノ秒）

Per Group Bucket	対応	説明
Packet Count	○	マッチしたパケット数
Byte Count	○	マッチしたパケットの合計サイズ

2.56.5 OpenFlow Channel 機能

OpenFlow Channel は OpenFlow コントローラが OpenFlow スイッチを制御するための TCP セッションで、デフォルトでポート番号 6653 を利用します。接続は常にスイッチ側から行われ、コントローラからスイッチへの設定変更や情報取得、スイッチからコントローラへの通知、双方の死活監視などは全て OpenFlow Channel を介して OpenFlow メッセージで行われます。

※OpenFlow Channel は、従来は Secure Channel と呼ばれ、ポート番号も 6633 が推奨されていました。必要に応じて設定を変更してください。

2.56.5.1 接続動作

OpenFlow Channel は、装置起動後 60 秒経過後にスイッチ側から接続し、接続を維持します。接続が切断された場合は、プライオリティの最も高いコントローラから順に接続を試みます。

コントローラとの接続に関して、以下の機能はサポートしていません。

- 複数コントローラへの同時接続
- OpenFlow ポートを介した OpenFlow Channel 接続（In-Band 接続 ※）
- TLS 対応
- 単一コントローラとの複数 OpenFlow Channel 接続

※In-Band 接続とは、フローテーブルで OpenFlow Channel の通信を転送することを指します。GRE トンネルを利用して、1 つのトンネルに OpenFlow Channel と OpenFlow のデータパスの通信を通すことは可能です。また、OpenFlow ポートに OpenFlow Channel 通信用のタグ VLAN を設定することで、1 つの物理ポートに OpenFlow Channel と OpenFlow のデータパスの通信を通すことも可能です。

2.56.5.2 対応メッセージ

OpenFlow メッセージの対応状況と説明は以下の通りです。

OpenFlow メッセージ	対応	説明
OFPT_HELLO	○	接続開始メッセージ
OFPT_ERROR	○	エラーメッセージ
OFPT_ECHO_REQUEST	○	ECHO 要求メッセージ
OFPT_ECHO_REPLY	○	ECHO 応答メッセージ
OFPT_EXPERIMENTER	×	拡張メッセージ
OFPT_FEATURES_REQUEST	○	スイッチ情報の取得要求
OFPT_FEATURES_REPLY	○	スイッチ情報の応答
OFPT_GET_CONFIG_REQUEST	×	GET_CONFIG 要求メッセージ
OFPT_GET_CONFIG_REPLY	×	GET_CONFIG 応答メッセージ
OFPT_SET_CONFIG	×	SET_CONFIG メッセージ
OFPT_PACKET_IN	○	受信パケットをコントローラへ転送 （バッファリングは未対応）
OFPT_FLOW_REMOVED	○	フローエントリの削除通知
OFPT_PORT_STATUS	○	ポートの状態変更通知
OFPT_PACKET_OUT	○	コントローラからのパケット送信 （バッファリングは未対応）
OFPT_FLOW_MOD	○	フローエントリの追加・変更・削除
OFPT_GROUP_MOD	○	グループエントリの追加・変更・削除
OFPT_PORT_MOD	○	ポートの設定変更 （Port Down のみ対応）
OFPT_TABLE_MOD	×	テーブルの設定変更

OFPT_MULTIPART_REQUEST	○	スイッチの各種統計情報の取得要求
OFPT_MULTIPART_REPLY	○	スイッチの各種統計情報の応答
OFPT_BARRIER_REQUEST	○	処理完了の確認要求
OFPT_BARRIER_REPLY	○	処理完了の確認応答
OFPT_QUEUE_GET_CONFIG_REQUEST	×	QUEUE_GET_CONFIG 要求メッセージ
OFPT_QUEUE_GET_CONFIG_REPLY	×	QUEUE_GET_CONFIG 応答メッセージ
OFPT_ROLE_REQUEST	×	Role 要求メッセージ
OFPT_ROLE_REPLY	×	Role 応答メッセージ
OFPT_GET_ASYNC_REQUEST	×	GET_ASYNC 要求メッセージ
OFPT_GET_ASYNC_REPLY	×	GET_ASYNC 応答メッセージ
OFPT_SET_ASYNC	×	SET_ASYNC メッセージ
OFPT_METER_MOD	×	メーターの追加・変更・削除

スイッチ内の各種情報を取得する Multipart メッセージの対応は以下の通りです。

Multipart	対応	説明
OFPMP_DESC	○	OpenFlow スイッチ情報
OFPMP_FLOW	○	フローエントリの個別の統計情報
OFPMP_AGGREGATE	○	フローエントリの集約した統計情報
OFPMP_TABLE	○	フローテーブルの統計情報
OFPMP_PORT_STATS	○	ポートの統計情報
OFPMP_QUEUE	×	キューの統計情報
OFPMP_GROUP	○	グループエントリの統計情報
OFPMP_GROUP_DESC	○	グループエントリ情報
OFPMP_GROUP_FEATURES	○	グループテーブルの情報
OFPMP_METER	×	メーターの統計情報
OFPMP_METER_CONFIG	×	メーターの設定
OFPMP_METER_FEATURES	×	メーターの情報
OFPMP_TABLE_FEATURES	○	フローテーブルの情報
OFPMP_PORT_DESC	○	ポート情報
OFPMP_EXPERIMENTER	×	拡張メッセージ

2.56.5.3 Echo メッセージ

コントローラとスイッチは、Echo メッセージで通信路を死活監視します。

IX ルータでは、コントローラから Echo-Request を受信している場合、Echo-Request は送信しません。また、Echo-Request に対して、何らかのメッセージを受信した場合、Echo-Reply が受信できなくても OpenFlow Channel は切断しません。

2.56.5.4 Packet-In メッセージ

受信パケットをコントローラへ転送するためのメッセージです。フローエントリで送信先を controller と設定すると送信されます。バッファリング機能には対応していないため、受信フレームは常にパケット全体を転送します。Output アクションで max_len を指定しても無視します。

Packet-In は大量のメッセージを生成する可能性があるため、以下の優先度で処理されます。また、各 Packet-In のキューは 64 に制限しています。

- LLDP の Packet-In
- OpenFlow メッセージ（Packet-In 以外）
- Set queue 命令付きの Packet-In
- ARP 等の非ユニキャストフレームの Packet-In
- 通常の Packet-In

2.56.5.5 Flow-Mod メッセージ

パケットの条件と適用するアクションおよびタイムアウト等から構成されるフローエントリを登録します。対応状況は前述のフローエントリの項目を参照してください。

OFPFMFC_OVERLAP フラグのみ定義上の仕様と異なります。このフラグを有効にした場合、本来は同一プライオリティでマッチ条件に重なる部分があるフローエントリが既に登録済みか検出する機能ですが、IX ルータでは完全に同一のエントリのみを OVERLAP として判定します。

また、buffer_id はサポートしていないため、OFP_NO_BUFFER（0xffffffff）以外の値を利用しないでください。

2.56.5.6 Port-status メッセージ

OpenFlow ポートをコンフィグで追加、変更、削除した場合、および linkup、linkdown の状態が変化した場合に送信されます。なお、advertised, supported, peer の各 feature についてはサポートしていないため、常に 0 を送信します。

また、Tunnel インタフェースを OpenFlow ポートとしている場合には Current feature には値が設定されません。インタフェースの速度は curr_speed, max_speed で取得してください。

max_speed は全てのポートで 1Gbps 固定です。curr_speed はインタフェース速度が設定されますが、bandwidth コマンドで任意の値に変更することもできます。

2.56.5.7 その他注意事項

OpenFlow Channel 上での大量のメッセージの送受信は、スイッチ（IX ルータ）、コントローラの双方にとって高い負荷となります。ネットワーク設計時、運用時には下記のような事象がなるべく発生しないように配慮してください。

- Packet-In、Packet-Out メッセージの大量発生
- 大量の Flow-Removed の一斉通知
- 大量の応答が必要な Multipart の情報取得

Packet-In の負荷は、Ver.9.2 以降 Packet-In 抑止機能により抑止可能です。

Flow-Removed などの OpenFlow メッセージは、Ver.9.1 までは 10000 以上同時に送信することはできません。Ver.9.2 以降は上限なしがデフォルトで、上限を設定することも可能です。

Multipart の情報取得は、できるだけ分割して取得するなどの仕組みを検討する必要がありますが、GROUP_DESC など仕様上一括取得しかできないメッセージもあり、大量にグループを設定する場合にはご注意ください。

2.56.6 OpenFlow 機能の基本設定

OpenFlow の設定は以下のコマンドで行います。

グローバルコンフィグモード

openflow enable	OpenFlow 機能の有効化
openflow dpid	DPID の設定（スイッチ識別用 Datapath ID）
openflow controller	OpenFlow コントローラとの接続設定
openflow flow-table	フローテーブルの設定 （フローテーブルコンフィグモードに遷移）
openflow table	テーブル ID の最大値を設定

インタフェースコンフィグモード

openflow port	OpenFlow ポートの設定
openflow ip tcp adjust-mss	OpenFlow ポートの IPv4 TCP MSS 調整
openflow ipv6 tcp adjust-mss	OpenFlow ポートの IPv6 TCP MSS 調整

フローテーブルコンフィグモード

table-name	フローテーブル名の設定
hash	ハッシュの設定（ハッシュキー、ハッシュサイズ）

表示コマンド

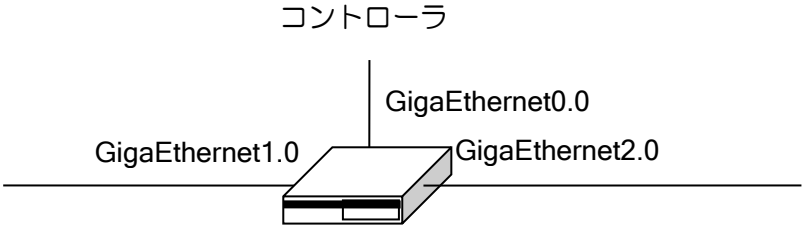
show openflow switch	スイッチ情報の表示
show openflow controller	コントローラ情報の表示
show openflow table	フローテーブル機能の表示
show openflow flow-entry	フローエントリ情報の表示
show openflow group-entry	グループエントリの表示
show openflow flow-cache	フローキャッシュの確認
show openflow port	ポート情報の表示

イベントログ

logging subsystem opfc	OpenFlow Channel のログ取得 （コントローラ関連）
logging subsystem opft	OpenFlow Datapath のログ取得 （トラフィック制御関連）

2.56.6.1 基本設定

OpenFlow スイッチの基本設定です。



OpenFlow スイッチとして動作させるための最低限の設定は以下のとおりです。

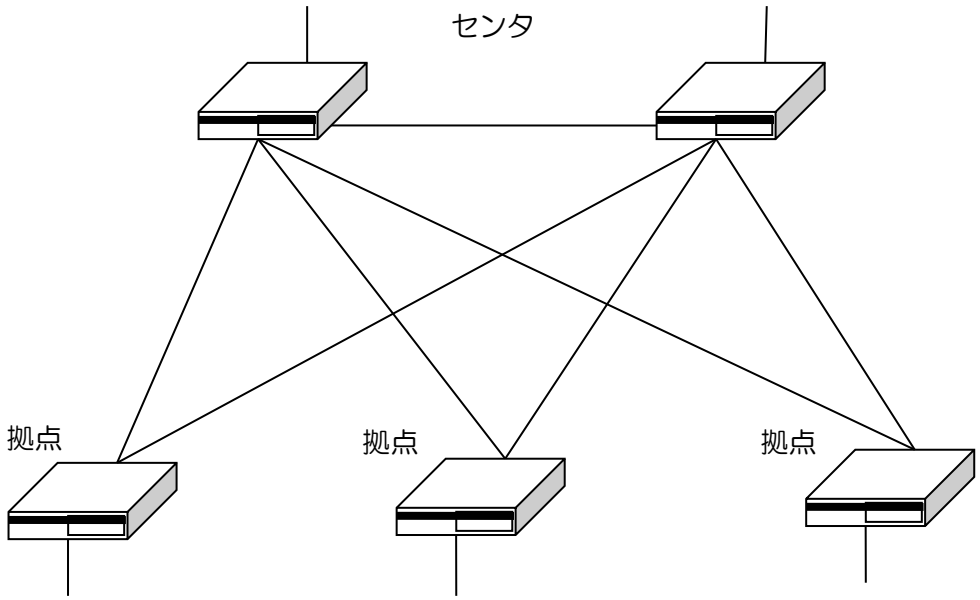
- ✧ OpenFlow 機能の有効化（openflow enable）
- ✧ DPID の設定（openflow dpid）。
- ✧ コントローラがスイッチを識別するための ID です。省略時は GE0 の MAC アドレスになりますが、管理しやすい番号を設定してください。
- ✧ コントローラの登録（openflow controller）
- ✧ OpenFlow ポートの割り当て（openflow port）

【設定例】

```
openflow enable
openflow dpid 0000000000000001
openflow controller priority 100 ipv4 10.0.0.1
!
interface GigaEthernet0.0
   ip address 10.0.0.254/24
   no shutdown
!
interface GigaEthernet1.0
   no ip address
   openflow port number 1 name GE1
   no shutdown
!
interface GigaEthernet2.0
   no ip address
   openflow port number 2 name GE2
   no shutdown
!
```

2.56.6.2 IPsec トンネルを利用した接続

WAN 回線を使って OpenFlow の制御を行う設定です。センタと拠点は IPsec トンネルで接続し、センタ内のコントローラから IPsec トンネルを介して VPN 全体を制御します。



拠点とセンタは GRE IPsec トンネルで接続し、OpenFlow Channel（制御通信）とデータパス（ユーザトラフィック）の両方を 1 つのトンネルで収容します。

コントローラのアドレスは 192.168.0.1、センタ側 IX の WAN 側アドレスは 172.16.1.251 と 172.16.1.252 とします。ハッシュテーブル等の高速化の設定は省略します。制御方法にあわせて設定してください。

【設定例 - センタ 1（拠点 1 台の例。センタ 2 は同様なので省略）】

```
ip route 192.168.1.1/32 Tunnel0.0

ip access-list list-any permit ip src any dest any
ike proposal ike-prop encryption aes hash sha
ike policy ike-policy1 peer any key secret mode aggressive ike-prop
ike remote-id ike-policy1 keyid site1

ipsec autokey-proposal ipsec-prop esp-aes esp-sha
ipsec dynamic-map ipsec-policy1 list-any ipsec-prop
ipsec remote-id ipsec-policy1 192.168.1.1

openflow enable
openflow dpid 0000000000001001
openflow controller priority 1 ipv4 192.168.0.1

interface GigaEthernet0.0
   ip address 172.16.1.251/24
   no shutdown

interface GigaEthernet1.0
   no ip address
   openflow port number 1 name LAN1
   no shutdown
```

```
interface GigaEthernet2.0
   no ip address
   openflow port number 1 name LAN2
   no shutdown

interface GigaEthernet3.0
   ip address 192.168.0.254/24
   no shutdown

interface Loopback0.0
   ip address 192.168.254.1/32

interface Tunnel0.0
   tunnel mode gre ipsec
   tunnel keepalive period 5 retries 5 recoveries 5
   ip unnumbered Loopback0.0
   ipsec policy transport ipsec-policy1 with-id-payload
   openflow port number 101 name WAN1
   no shutdown
```

【設定例 - 拠点 1】

```
ip route 192.168.0.1/32 Tunnel0.0
ip route 192.168.0.1/32 Tunnel1.0 distance 200

ip access-list list-any permit ip src any dest any

ike proposal ike-prop encryption aes hash sha

ike policy ike-policy1 peer 172.16.1.251 key secret mode aggressive ike-prop
ike local-id ike-policy1 keyid site1

ike policy ike-policy2 peer 172.16.1.252 key secret mode aggressive ike-prop
ike local-id ike-policy2 keyid site1

ipsec autokey-proposal ipsec-prop esp-aes esp-sha

ipsec autokey-map ipsec-policy1 list-any peer 172.16.1.251 ipsec-prop
ipsec local-id ipsec-policy1 192.168.1.1

ipsec autokey-map ipsec-policy2 list-any peer 172.16.1.252 ipsec-prop
ipsec local-id ipsec-policy2 192.168.1.1

openflow enable
openflow dpid 0000000000000001
openflow controller priority 1 ipv4 192.168.0.1

interface GigaEthernet0.0
   ip address dhcp receive-default
   no shutdown

interface GigaEthernet1.0
   no ip address
   openflow port number 1 name LAN1
   no shutdown

interface Loopback0.0
   ip address 192.168.1.1/32

interface Tunnel0.0
```

```
   tunnel mode gre ipsec
   tunnel keepalive period 5 retries 5 recoveries 5
   ip unnumbered Loopback0.0
   ipsec policy transport ipsec-policy1 with-id-payload
   openflow port number 101 name WAN1
   no shutdown

interface Tunnel1.0
   tunnel mode gre ipsec
   tunnel keepalive period 5 retries 5 recoveries 5
   ip unnumbered Loopback0.0
   ipsec policy transport ipsec-policy2 with-id-payload
   openflow port number 102 name WAN2
   no shutdown
```

2.56.6.3 ルータ機能との併用設定

前述の例で、拠点 1 の IX にルータ機能を持たせた場合の例です。

全拠点およびセンタにルータが設定されており、WAN 側のネットワークは 10.0.0.0/16 とします。拠点 1 の LAN 側のサブネットは 10.1.1.0/24 です。

【設定例 - 拠点 1（BVI 併用版）】

```
ip route 192.168.0.1/32 Tunnel0.0
ip route 192.168.0.1/32 Tunnel1.0 distance 200

ip access-list list-any permit ip src any dest any

ike proposal ike-prop encryption aes hash sha

ike policy ike-policy1 peer 172.16.1.251 key secret mode aggressive ike-prop
ike local-id ike-policy1 keyid site1

ike policy ike-policy2 peer 172.16.1.252 key secret mode aggressive ike-prop
ike local-id ike-policy2 keyid site1

ipsec autokey-proposal ipsec-prop esp-aes esp-sha

ipsec autokey-map ipsec-policy1 list-any peer 172.16.1.251 ipsec-prop
ipsec local-id ipsec-policy1 192.168.1.1

ipsec autokey-map ipsec-policy2 list-any peer 172.16.1.252 ipsec-prop
ipsec local-id ipsec-policy2 192.168.1.1

openflow enable
openflow dpid 0000000000000001
openflow controller priority 1 ipv4 192.168.0.1

interface GigaEthernet0.0
   ip address dhcp receive-default
   no shutdown

interface GigaEthernet1.0
   ip address 10.1.1.254/24
   no shutdown

interface BVI0
   ip address 10.0.0.1/16
   openflow port number 1 name LAN1
   no shutdown
```

```
interface Loopback0.0
   ip address 192.168.1.1/32

interface Tunnel0.0
   tunnel mode gre ipsec
   tunnel keepalive period 5 retries 5 recoveries 5
   ip unnumbered Loopback0.0
   ipsec policy transport ipsec-policy1 with-id-payload
   openflow port number 101 name WAN1
   no shutdown

interface Tunnel1.0
   tunnel mode gre ipsec
   tunnel keepalive period 5 retries 5 recoveries 5
   ip unnumbered Loopback0.0
   ipsec policy transport ipsec-policy2 with-id-payload
   openflow port number 102 name WAN2
   no shutdown
```

BVI でルータ機能を併用する場合、ユーザトラフィックの制御と OpenFlow Channel や IPsec 接続の制御が同じルーティングテーブルで制御されます。このため、管理用の通信とユーザの通信で同じ IP アドレスを設定することはできません。また、フィルタやポリシールーティング等で、ユーザ通信と管理用の通信を分離する必要があります。

2.56.7 ProgrammableFlow 対応

コントローラに PF6800 を使用し、センタと多数の拠点からなる WAN ソリューションを実現する場合、ProgrammableFlow の制御にあわせた設定が必要になります。ProgrammableFlow の利用可能な構成や設定例については PF6800 の製品サポートを通じてご確認ください。

ProgrammableFlow 機能には Ver.9.0.54 以降で対応していますが、今後は Ver.9.2 で追加した機能を推奨設定として利用します。特に理由がない限り Ver.9.2 以降を利用してください。

なお Ver.9.4 以降では、ProgrammableFlow の制御によって発生する MPLS パケットのブリッジインタフェースでの MSS 調整に対応しています。

2.56.8 高速転送機能

OpenFlow では、フローエントリのマッチ条件をプライオリティ順に評価する必要があります。OpenFlow スイッチは一般的には高性能なハードウェアスイッチが利用されますが、IX ルータは検索処理をハードウェアでアシストする機能を持ちません。このため、何も考慮せずにフローテーブルを構築すると、数百エントリ程度でも大幅に性能が低下する可能性があります。

実用的な性能を確保するために、以下のような検討が必要です。

- フローテーブルを分割し、検索回数を削減する。
- 通信量の多いエントリのプライオリティを高くして、平均検索回数を削減する。
- ハッシュテーブル機能を利用する。
- キャッシュ転送機能を利用する（Ver.9.2 以降）。

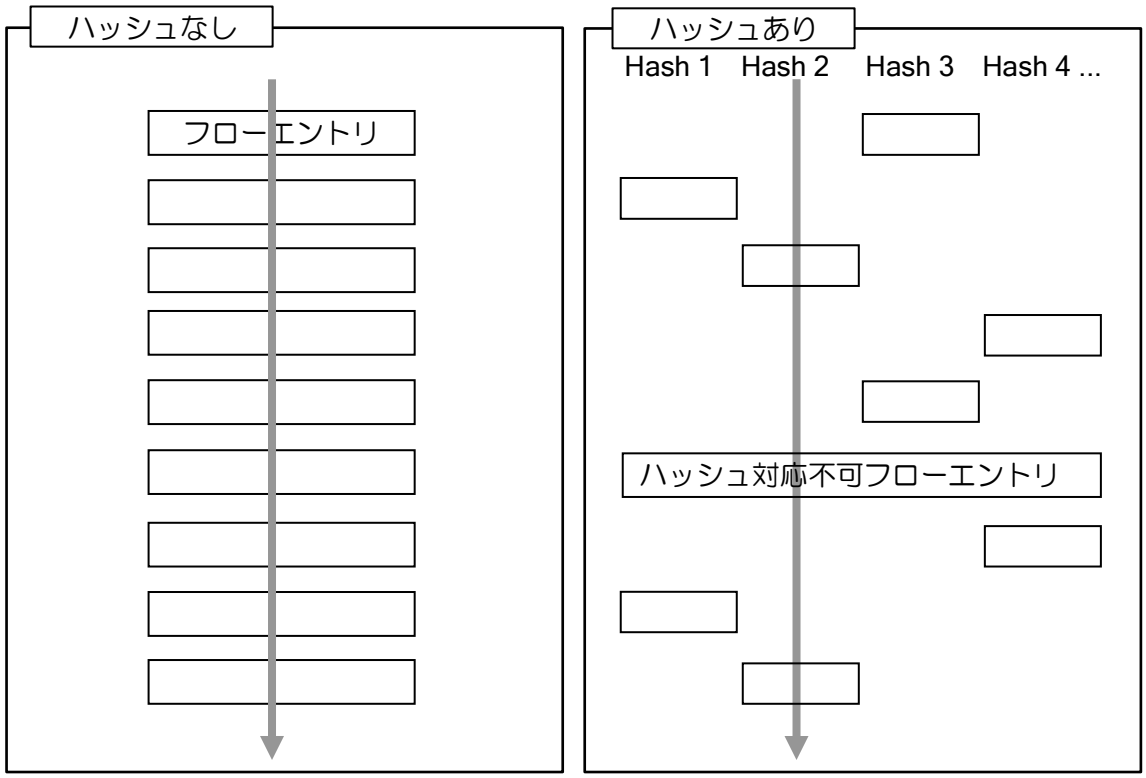
ここでは、IX 独自機能であるハッシュテーブル機能とキャッシュ転送機能について説明します。それぞれ利用するために簡単な制約等がありますが、適切に利用することで、フローエントリが大量に存在する環境でも高い転送性能を実現できます。

2.56.8.1 ハッシュテーブル機能

ハッシュテーブル機能は、フローエントリのいくつかのフィールドをハッシュキーとすることで、フローテーブルをハッシュテーブル化する機能です。宛先 MAC アドレスや宛先 IP アドレスなど、いくつかのフィールドを 1 つまたは複数組み合わせてキーにすることができます。

動作概要

通常、フローエントリの検索は下の左図のようにフローエントリをマッチするまで順番に参照しますが、ハッシュテーブルでは右図のようにハッシュ値が一致しないフローエントリは検索対象になりません。このため数千から数万のフローが登録されても、数個～数十個のフローエントリが登録されているのと同程度の速度で転送することが可能になります。



ハッシュキーの動作

- ハッシュキーを「宛先 IP アドレス/32」と設定した場合

マッチ条件が「宛先 IP アドレス/32」のフローエントリには全てハッシュ値が設定されます。また受信パケットも宛先 IP アドレスでハッシュ値が設定されます。

具体的にはマッチ条件が 192.168.0.2 であるフローエントリも 192.168.0.2 宛のパケットも同じハッシュ値が設定されますので、例えば 2 と計算されたとすると、ハッシュ値が 2 でないフローエントリは全て検索せずに転送できます。

ただし、ハッシュに設定したフィールドに Wildcard を含むフローエントリがある場合（宛先が 192.168.0.0/30 や宛先 any など）は、ハッシュ値が 1 つに決まらないので、このようなエントリは全てのパケットで従来通り参照されます。

- ハッシュキーを「宛先 IP アドレス/24」と設定した場合

マッチ条件が「宛先 IP アドレス/24～32」のフローエントリには全てハッシュ値が設定されます。/25 や/32 のマッチ条件もハッシュ計算のフィールドに Wildcard がないので問題ありません。

例えば 192.168.0.0/24 の拠点宛のフローエントリを作る場合、192.168.0.0/24～32 のマッチ条件が必ず付与されることになりますので、大多数のフローエントリをハッシュテーブルに乗せることができます。

ただし送信する拠点ごとにハッシュ値が固まってしまうため、拠点分のフロー検索数は減少しません。それでも「拠点数×拠点ごとのフロー数」から「拠点ごとのフロー数」まで大幅に検索回数は抑制されます。

設定方法

以下のコマンドでフローテーブルごとに設定します。

フローテーブルコンフィグモード

hash	ハッシュの設定（ハッシュキー、ハッシュサイズ）

ハッシュ値を広く分布させるため、なるべく多くの値が設定されるフィールドを選択する必要があります。また、範囲を広く設定するとハッシュ値が散らばりませんし、狭く設定するとハッシュ計算できないフローエントリが増えます。適切な値の設定が必要です。

フローテーブルを目的別に分割するなどするとハッシュテーブルは設定しやすくなります。詳細は具体的な利用例を参照してください。

利用例

1）L2 スイッチ制御

主に宛先 MAC アドレスで転送先を制御する場合、ハッシュキーを宛先 MAC アドレスにしてください。異なる MAC アドレスのエントリは、ほとんど検索対象にならないことが期待されるので、大量にフローエントリを処理することができます。設定例は以下の通りです。

```
openflow flow-table 0
  hash key mac-dest size 65536
```

2）多拠点ネットワークのセンタ装置利用（L3 / L4 制御）

センタと多数の拠点がそれぞれ複数の IPsec トンネルで接続されているネットワークのセンタ装置を制御する場合、ハッシュキーを「IPv4 宛先アドレス/24」とした IPv4 パケット専用のフローテーブルを用意する方法が有効です（拠点のサブネットが/24～/32 の場合）。

拠点ごとにハッシュ値が決まるので、拠点数が増えても 1 拠点分の検索速度で転送可能です。ただし拠点内のフローエントリは全て衝突するので、1 拠点あたりのフロー数が多いと性能は劣化します。

```
openflow flow-table 0
  hash key ipv4-dest-prefix 24 size 16384
```

3）ProgrammableFlow のコアスイッチ利用

ProgrammableFlow のコアスイッチ利用の場合の設定例です。宛先 MAC アドレスを変換して転送するため、以下の設定で効率的に分散されます。

```
  hash key mac-dest-mask ff:ff:ff:f8:00:00 size 65536
```

4）ProgrammableFlow のエッジスイッチ利用

ProgrammableFlow のエッジスイッチ利用の場合の設定例です。エッジスイッチの場合は、条件が利用環境によって異なります。通常は IP アドレスの/32 の設定が多く負担になりますので、以下の設定が適しています。

```
  hash key ipv4-src-prefix 32 ipv4-dest-prefix 32 size 16384
```

2.56.8.2 キャッシュ転送機能

キャッシュ転送機能は、新規の通信が発生するたびに受信したパケットがどのフローエントリにマッチしたかを記録し、次回以降のフローエントリの検索を省略することで高速転送する仕組みです。Ver.9.2 以降利用可能です。

なお、通信開始時の転送性能には効果がありませんので、ハッシュテーブル機能と併用して運用してください。また、ARP と ND はキャッシュ転送機能の対象外です。

設定方法

以下のコマンドでフローテーブルごとに設定・確認ができます。デフォルトは無効です。

フローテーブルコンフィグモード

flow-cache	キャッシュ転送機能の設定
show openflow flow-cache	キャッシュ情報の表示

設定コマンドでエントリ数とタイムアウトを設定することができます。タイムアウトは 2 種類の方式に対応しており、通信があっても指定時間で必ずキャッシュを削除する hard-timeout と、無通信になってから指定時間でキャッシュを削除する idle-timeout を選択することができます。

注意事項

- フローテーブル変更時のキャッシュ動作

キャッシュ転送を利用した場合、フローテーブルに変更があっても即座に切り替わらないケースがあります。Flow-Mod の Modify や Delete は即時反映されますが、Add のみで切り替えを行った場合に即時反映されません。

以下のフローエントリで 192.168.0.1 宛の通信をキャッシュ転送している場合

Pri	マッチ条件	インストラクション
100	宛先 IP アドレス：192.168.0.1/32	Port 1 から送信

Pri 200 のフローエントリが登録されると、本来は廃棄ですがキャッシュ転送が優先されます。

Pri	マッチ条件	インストラクション
200	宛先 IP アドレス：192.168.0.0/24	廃棄
100	宛先 IP アドレス：192.168.0.1/32	Port 1 から送信

Add と同時に Pri 100 のフローエントリを削除する、あるいは Pri 100 のフローエントリのインストラクションを廃棄に変更するなど、Modify や Delete による変更を伴う場合には、フローエントリの変更は即時反映されます。

- 総エントリ数の制限
  複数のフローテーブルで有効化する場合は、メモリの消費量が大きいためキャッシュの総エントリ数が 65535 を超えないようにテーブルごとのエントリ数を調整してください。

2.56.8.3 その他の対策

- フローテーブルの分割
  ハッシュテーブル機能は、ハッシュが上手く分散できるようにフローエントリを投入することが重要になります。目的別にフローテーブルを活用したり、アドレスやポートの集約条件を決まったルールで運用することが、ハッシュによる高速検索に向いた制御です。
  多拠点ネットワークの設定で、多数の拠点が/24 で一部/16 の拠点があるといった場合に、ハッシュキーを「IPv4 宛先アドレス/16」としてしまうと、同一ハッシュ値となるエントリが増加してしまい、十分な効果が得られません。この場合はテーブルを分割するか、キャッシュ機能の利用を検討してください。

- ブロードキャスト、マルチキャストの抑止
  多拠点ネットワークで利用する場合、ARP などのブロードキャストパケットやマルチキャストパケットをコピーして全拠点に送信すると性能が著しく劣化します。
  ルータを挟んで ARP の通信を抑制する、ARP_TPA のマッチ条件を使って端末が存在するネットワークのみに ARP パケットを送信する、OpenFlow Channel のみで制御するなどが効果的です。

2.56.9 Packet-In 抑止機能

Packet-In により新規の通信を検出し、コントローラがフローエントリを登録する制御方式の場合、フローエントリが登録されるまでの間 Packet-In が大量に送信され続ける可能性があります。
Ver.9.2 以降、本機能を有効にすることで、不要な Packet-In の発生を抑止できます。

2.56.9.1 設定方法

以下のコマンドでフローテーブルごとに設定・確認が可能です。

フローテーブルコンフィグモード

openflow channel rate-limit packet-in	Packet-In 抑止機能
show openflow controller	抑止状態の確認

同一のフローに対して、指定した時間内に指定したパケット数のみ Packet-In を行う機能です。以下のマッチフィールドがすべて一致する場合に同一フローとして扱います。

- In-port, eth-dst, eth-src, eth-type, vlan-vid
- ip-proto, ipv4-src, ipv4-dst, ipv6-src, ipv6-dst
- tcp-dst, tcp-src, udp-dst, udp-src, arp-tpa

2.56.10 QoS 対応

OpenFlow では QoS 機能を利用することができます。既存のブリッジで動作する QoS 機能のほか、OpenFlow 1.3 の Set Queue の命令に対応しています。

2.56.10.1 Set-Queue 対応

OpenFlow の Set queue 機能は、QoS のキュー番号を指定する機能です。IX ルータでは、set-queue で命令されたキュー番号を qos-group として扱います。あらかじめ、ルータの設定として CBQ やシェーピング等の QoS 設定を行い、qos-group の対応付けを設定しておくことで、任意の QoS 設定を利用することができます。

qos-group が OpenFlow 機能で付与される以外は、ブリッジ機能の QoS 設定と同一となるため、ブリッジの設定や QoS の設定を参照してください。

2.56.10.2 ToS/CoS 値の書き換え

OpenFlow には Set-Filed の命令で ToS や CoS の値を書き換える機能がありますが、ToS の書き換えには対応しておりません。CoS 値の書き換えは可能です。

2.56.10.3 OpenFlow Channel の優先設定

OpenFlow Channel のパケットが廃棄されると正常に通信ができないため、優先設定を行う必要があります。

Ver.9.2 以降では以下のコマンドで ToS 値を付与できますので、これを利用してください。Ver.9.1 以前の場合は宛先ポート番号等でマッチさせて QoS を適用してください。

ip type-of-service openflow	OpenFlow Channel の ToS 設定

IKE や GRE keepalive、OSPF などを利用する場合は、これらも優先設定する必要があります。同じ ToS 値を設定すればまとめて制御可能です。

2.56.11 ルータ機能との併用

OpenFlow 機能は既存のルータ機能と併用可能です。構成によりますが、WAN ソリューションの場合、「IPsec 接続用の VPN ルータ」、「OpenFlow スイッチ」、「ユーザルータ」の 3 台の動作を 1 台で実現することも可能です。

2.56.11.1 IPsec 機能との併用

複数の WAN 回線上で IPsec 接続し、OpenFlow で送信先を制御したい場合は、Ether over GRE over IPsec のトンネルを使用して keepalive 機能を有効化してください。接続区間で障害があると OpenFlow ポートがダウンするので、OpenFlow の制御上は通常の物理ポート同士でケーブル接続している状態と同様に扱えます。

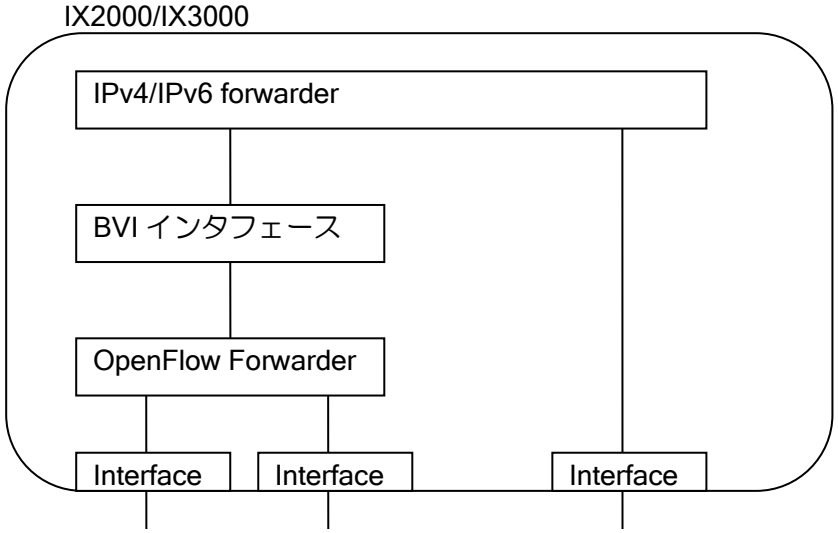
また GRE トンネルは OpenFlow の通信と OpenFlow channel の制御通信を同時に 1 つのトンネルに通すことができます。制御用のトンネルを別途用意する必要はありません。

2.56.11.2 ユーザルータとの併用

BVI インタフェースを利用することで、LAN 側からの通信をルータ機能で処理したあとに OpenFlow 機能で経路制御することができます。ルータ機能が BVI から送信すると OpenFlow 機能が BVI で受信し、逆も同様です。Ver.9.0.54 以降では BVI インタフェースに VLAN タグを設定することができます。

Ver.9.3 で複数 BVI に、Ver.9.5 で VRF に対応しているため、ユーザルータ部分を含めて複数 VTN を構築できます。複数の BVI インタフェースに異なる VLAN タグをそれぞれ設定することで、複数 VTN に対応することができます。VRF を併用すればネットワークも分離されます。

OpenFlow 機能と BVI インタフェース使用時のブロック図



2.56.11.3 サブインタフェースの利用

サブインタフェースを併用することで、1 つの物理ポート上で OpenFlow 機能と既存のブリッジ機能やルータ機能を併用して動作させることも可能です。

OpenFlow のデータトラフィックと OpenFlow Channel の通信を 1 つの物理ポートに通す場合などに利用できます。

2.56.12 VLAN タグ制御補助機能

Ver.9.4 以降ではイーサネットポートに VLAN ID を指定できます。VLAN ID を指定した場合、当該ポートで受信したイーサネットフレームは、VLAN タグを付与したうえで OpenFlow 転送します。また、送信時には指定された VLAN ID と一致するイーサネットフレームのみを VLAN タグを外して送信します。

インタフェースコンフィグモード

openflow port	OpenFlow ポートの設定

```
【設定例】
device GigaEthernet2
  vlan-group 1 port 1
  vlan-group 2 port 2
!
interface GigaEthernet2:1.0
  openflow port number 1 name LAN1 access vlan 10
  no shutdown
!
interface GigaEthernet2:2.0
  openflow port number 2 name LAN2 access vlan 20
  no shutdown
```

ポート 1 の場合

- 受信フレームにタグ 10 をつけてから、OpenFlow 機能で受信する。
- 送信フレームはタグ 10 のみ、タグを外して送信する。

ポート 2 の場合

- 受信フレームにタグ 20 をつけてから、OpenFlow 機能で受信する。
- 送信フレームはタグ 20 のみ、タグを外して送信する。

2.56.13 フローエントリ コンフィグ制御機能

OpenFlow スイッチを制御するフローエントリおよびグループエントリは、通常コントローラから登録を行いますが、Ver.9.2 以降では同時に CLI で制御することも可能です。

In-Band 接続の実現など、コントローラと接続する前にフローエントリで転送制御したい場合や、コントローラの制御方式を変更せずに経路制御したい場合に利用することができます。

設定内容がコントローラと競合してしまうと通信異常などが発生する場合があるので注意してください。特にコントローラに PF6800 を利用する場合、指定された設定以外は本機能によるフローテーブルの設定は行わないでください。

2.56.13.1 設定方法

以下のコマンドで設定可能です。

グローバルコンフィグモード

openflow match	マッチ条件の設定
openflow instructions	インストラクションの設定
openflow group	グループエントリの設定

グループエントリコンフィグモード

action-buckets	アクションバケツの設定

フローテーブルコンフィグモード

flow-entry	フローエントリの設定
tablemiss-entry	テーブルミスエントリの設定

flow-entry コマンドは、別コマンドで設定したマッチ条件、インストラクションを選択する仕組みです。tablemiss-entry も同様にインストラクションを指定して登録します。

なお、コンフィグで登録したフローエントリはコントローラに対して隠ぺいします（Multipart で全フローエントリを要求されても CLI 設定分は載せません）。コントローラがフローエントリの設定不一致を検出し、削除命令を発行するケースがあるためです。CLI で転送した通信はコントローラ側で認識できないことに注意してください。

```
【設定例（マッチ条件）】
openflow match web_server1 ipv4-src 192.168.0.0 255.255.255.0 ipv4-dst 10.0.0.1
送信元が 192.168.0.0/24、宛先が 10.0.0.1 の通信にマッチ。範囲指定はマスクで指定。

【設定例（インストラクション）】
openflow instructions out-port1_2 write-actions group 1
Group1 のルールで送信

【設定例（グループエントリ）】
openflow group 1 fast-failover
  action-buckets watch-port 1 action out-port 1
  action-buckets watch-port 2 action out-port 2
上から順に、Port 1 が up なら Port 1 に送信、Port 2 が up なら Port2 に送信する。

【設定例（フローエントリ、テーブルミスエントリ）】
openflow flow-table 0
  flow-entry priority 10000 match web_server1 instruction out-port1_2
  tablemiss-entry goto-table 1
フローエントリはマッチ条件とインストラクションを選択したもので登録
```

テーブルミスエントリは、インストラクションの選択か goto-table を記述可能

2.56.13.2 コントローラとの設定の競合

CLI によるフローの制御はコントローラ側に認識されないため、コントローラの制御との競合は極力回避する必要があります。

フローエントリやグループエントリの設定が競合して片方しか有効にならない場合、以下のようにコントローラの指示を優先します。

- CLI で登録したフローエントリと同じマッチ条件のフローエントリがコントローラから登録された場合(Add)、コントローラの設定で上書きします。コンフィグは削除しませんが、コントローラが登録したフローエントリが削除されても CLI のフローエントリは再登録されません。グループエントリも同様です。
- CLI で登録したフローエントリ、グループエントリはコントローラから変更・削除できません。例えば接続直後に全フローエントリを削除する命令を受けることがありますが、そのような場合にも CLI の設定は残ります。

2.56.14 表示コマンド

いくつかの表示コマンドの表示内容について説明します。

2.56.14.1 show openflow flow-entry コマンド

登録されたフローエントリの内容を表示します。

【表示例】

```
# show openflow flow-entry table-id 0
Flow Table 0 (table0) - 3 entries, 1 lookups
Codes: R - send flow removed, P - no send pkt count, B - no send byte count
Pri 1000, serial 108, cookie 0, code -
   Match field:
      ipv4 src 192.168.11.0/24, dest 192.168.10.0/24
   Instruction:
      group 1 (bucket 2, out-port Tunnel1)
   Timer:
      duration 7
      idletime 7
   0 packets, 0 bytes
Pri 999, serial 109, cookie 0, code R
   Match field:
      ipv4 src 192.168.11.0/24, dest any
   Instruction:
      out-port Tunnel2
   Timer:
      duration 7
      idletime 7, idle-timeout 30
   0 packets, 0 bytes
         :
```

- タイトル行
  テーブル ID（テーブル名）、フローエントリ数、フローテーブル参照回数を表示します。
- Pri 行
  フローエントリの先頭行です。
  プライオリティ、内部管理用のシリアル番号、クッキー、フラグ情報を順に表示します。
- Match field
  設定されたマッチ条件です。ワイルドカード指定は可読性の高い表示形式で表示します。
- Instruction
  設定されたインストラクションです。
  fast-failover のグループを指定している場合、現在選択されているバケツと送信先も表示します。
- Timer
  duration（エントリ生成からの時間）、idletime（無通信時間）を表示します。
  idle-timeout, hard-timeout が設定されている場合には、その値も表示します。
- 統計情報
  フローエントリで転送したパケット数とパケットサイズを表示します。

Ver.9.2 以降ではフローエントリを 1 行で表示するサマリ表示にも対応しています。プライオリティ、シリアル番号、転送パケット数、Info（マッチ条件）のみ表示します。

2.56.14.2 show openflow group-entry コマンド

show openflow group-entry コマンドは、グループエントリを表示します。

【表示例】

```
# show openflow group-entry
Group 0
   Group type is fast-failover
   Bucket 1 is selected
   Duration is 0:00:16
   Reference count is 1
   Statistics:
      0 packets, 0 bytes
   Action buckets:
      Bucket 1:
         watch-port PORT1
         out-port PORT1
      Bucket 2:
         watch-port PORT2
         out-port PORT2
```

- Group
  グループエントリの先頭行でグループ ID を表示します。
- Group type
  グループタイプを表示します。
- Bucket 1 is selected（fast-failover のみ）
  現在選択しているバケツを表示します。
  例では PORT1 が LIVE（up）で、Bucket 1 を使って転送していることを示しています。
- Duration
  グループが設定されてからの経過時間です。
- Reference count
  このグループをインストラクションに設定して参照しているフローエントリの数です。
- Action buckets
  アクションバケツを登録順に表示します。
- watch-port（fast-failover のみ）
  監視するポートをポート名で表示します。

2.56.15 イベントログの設定

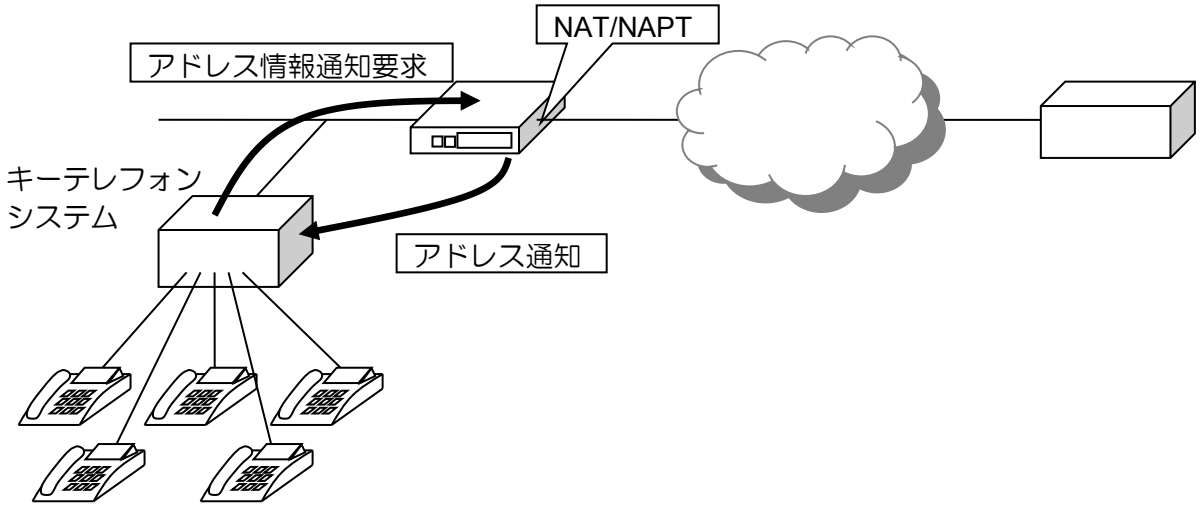
OpenFlow 機能のイベントログは、以下の 2 種類です。
詳細はイベントログリファレンスを参照してください。

- 制御通信のログ表示：opfc
- トラフィックのログ表示: opft

■2.57 キーテレフォンシステム連携機能の設定

2.57.1 機能概要

本機能は、日本電気製キーテレフォンシステムと IX2000/IX3000 シリーズを組み合わせて使用するための機能です。それ以外の装置に対しては、本機能を使用することはできません。



2.57.2 インタフェースの設定

2.57.2.1 IP アドレスの設定

固定アドレス設定の他に、DHCP サーバからの払い出し、IPCP による動的なアドレス取得も可能です。コマンドは以下のとおりです。

ip address	IP アドレス設定 （インタフェースコンフィグモード）
no shutdown	インタフェースを運用状態へ変更 （インタフェースコンフィグモード）

【設定例 1】
固定アドレス設定

```
interface GigaEthernet0.0
  ip address 10.0.0.1/24
  no shutdown
```

【設定例 2】
DHCP による動的アドレス設定

```
interface GigaEthernet0.0
  ip address dhcp
  no shutdown
```

【設定例 3】
IPCP による動的アドレス設定
（次の PPPoE の設定も参照してください）

```
interface GigaEthernet0.1
  encapsulation pppoe
  ppp binding pppoe1
  ip address ipcp
  no shutdown
```

2.57.2.2 PPPoE の設定

PPPoE を使用する場合、サブインタフェース（インタフェースの後ろの数字が 0 以外）を使用します。PPP 用のプロファイルにユーザ名,パスワードを設定し、作成したプロファイルをインタフェースに割り当てます。

コマンドは以下のとおりです。詳細については、PPP，PPPoE の項を参照してください。

ppp profile	PPP プロファイルの作成 （グローバルコンフィグモード）
authentication myname	ユーザ名の設定 （PPP コンフィグモード）
authentication password	パスワードの設定 （PPP コンフィグモード）
encapsulation	カプセル化タイプの設定 （インタフェースコンフィグモード）
ppp binding	PPP プロファイルの割り当て （インタフェースコンフィグモード）

【設定例】

```
ppp profile pppoe1
  authentication myname ix@nec.co.jp
  authentication password ix@nec.co.jp ix-router

interface GigaEthernet0.1
  encapsulation pppoe
  ppp binding pppoe1
  ip address ipcp
  no shutdown
```

2.57.3 グローバルアドレス通知機能の設定

キーテレフォンシステムにグローバルアドレスを通知する機能です。

NAT/NAPT 配下のキーテレフォン装置は、外部の装置と通信する際に NAT/NAPT で使用するインタフェースのアドレス（グローバルアドレス）が必要となります。本機能は、キーテレフォンシステムからのアドレス情報通知要求に対して、指定したインタフェースのアドレスを通知する機能です。

2.57.3.1 グローバルアドレス通知機能コマンドの有効化

最初にグローバルアドレス通知機能のコマンドを有効にする設定を行う必要があります。コマンドを有効にしていない場合、グローバルアドレス機能のコマンドは表示されません。コマンドは以下のとおりです。

service kts-addressing	グローバルアドレス通知機能コマンドの有効化 （グローバルコンフィグモード）

2.57.3.2 グローバルアドレス通知の有効化

キーテレフォンシステムからの要求を受信するインタフェースにおいて、アドレス通知機能を有効にします。1 つのインタフェースにのみ設定可能です。コマンドは以下のとおりです。

kts-addressing enable	グローバルアドレス通知の有効化 （インタフェースコンフィグモード）

2.57.3.3 通知インタフェースの設定

グローバルアドレスを持つインタフェースを指定します。指定したインタフェースのアドレスがキーテレフォンシステムに通知されます。Ver.8.6 以降 NGN モードの設定が可能です。NGN モードに設定した場合、アドレス通知に加えて NGN 網の情報を通知します。コマンドは以下のとおりです。

kts-addressing external	通知インタフェースの設定 （グローバルコンフィグモード）

【設定例 1】
PPPoE に接続する場合

```
kts-addressing external GigaEthernet0.1
```

【設定例 2】
NGN 回線に接続する場合

```
kts-addressing external GigaEthernet0.0 ngn-mode
```

2.57.3.4キーテレフォンシステムのアドレス設定

グローバルアドレスの通知は、指定したキーテレフォンシステムに対して行います。設定可能な装置数は 1 台のみです。コマンドは以下のとおりです。

kts-addressing allowed-host	キーテレフォンシステムのアドレス設定 （グローバルコンフィグモード）

2.57.3.5 IX 情報更新時の通知設定（Ver.8.6 以降）

IX の情報が更新された場合にキーテレフォンシステムに通知を行います。コマンドは以下のとおりです。

kts-addressing notify	IX 更新時の通知設定 （グローバルコンフィグモード）

2.57.3.6 状態／統計の表示，クリア

以下のコマンドで、状態／統計情報の表示，クリアを行うことができます。

show kts-addressing	状態／統計情報の表示
clear kts-addressing statistics	状態／統計情報のクリア

2.57.4 NAT/NAPT の設定

グローバルアドレスを持つインタフェースに NAPT の設定を行います。

コマンドは以下のとおりです。詳細は、ネットワークアドレス変換の設定の項を参照してください。

ip napt enable	NAPT の有効化 （インタフェースコンフィグモード）
ip napt address	NAPT アドレスの設定 （インタフェースコンフィグモード）
ip napt service	サーバサービスの設定 （インタフェースコンフィグモード）

IP フォンサービスで複数の電話番号を取得している場合には、それらの電話番号間での通話を可能とするために、キーテレフォンシステムを接続しているインタフェース（LAN 側）にも NAPT の設定を行います。

```
【設定例 1】
基本設定

!WAN 側の設定
interface GigaEthernet0.1
  ip address ipcp
  ip napt enable
  ip napt static 192.168.0.20 udp 10020-10051
  ip napt static 192.168.0.10 udp 5060
  no shutdown

【設定例 2】
複数の電話番号を取得している場合
設定例 1 の WAN 側に加えて、LAN 側の設定も行います。

ip access-list alist_napt permit ip src 192.168.0.0/24 dest any

!LAN 側の設定
interface GigaEthernet1.0
  ip address 192.168.0.1/24
  no ip redirects
  ip napt enable
  ip napt address GigaEthernet0.1
  ip napt inside list alist_napt
  ip napt static 192.168.0.20 udp 10020-10051
  ip napt static 192.168.0.10 udp 5060
  no shutdown
```

2.57.5 フィルタの設定

特定パケットのみ通過を許可する場合、フィルタを使用します。

フィルタには、固定の条件を設定するスタティックフィルタと、通過したパケットに対応するパケットのみ受信を許可するダイナミックフィルタがあります。フィルタ条件をアクセスリスト、ダイナミックアクセスリストで設定し、フィルタコマンドで割り当てます。アクセスリストに該当しないパケットは deny の扱いとなり、廃棄されます。

コマンドは以下の通りです。詳細はパケットフィルタの項を参照してください。

ip filter	フィルタの設定 （インタフェースコンフィグモード）
ip access-list	アクセスリストの設定 （グローバルコンフィグモード）
ip access-list dynamic	ダイナミックアクセスリストの設定 （グローバルコンフィグモード）

【設定例 1】
静的フィルタ
送信元 100.0.0.0/24、送信先 any のパケットのみ受信可。

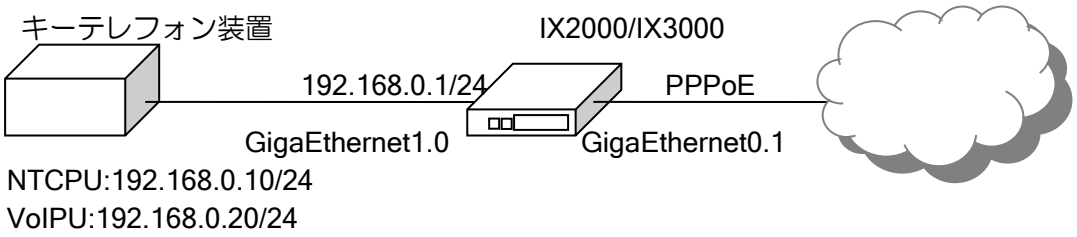
```
ip access-list flt-acl permit ip src 100.0.0.0/24 dest any

interface GigaEthernet0.1
   ip address ipcp
   ip filter flt-acl 10 in
   no shutdown
```

【設定例 2】
動的フィルタ
送信したパケットに対応するパケットのみ受信可。

```
ip access-list deny-all deny ip src any dest any
ip access-list permit-all permit ip src any dest any

ip access-list dynamic dym-flt access permit-all

interface GigaEthernet0.1
   ip address ipcp
   ip filter deny-all 10 in
   ip filter dym-flt 20 out
   no shutdown
```

2.57.6 設定例

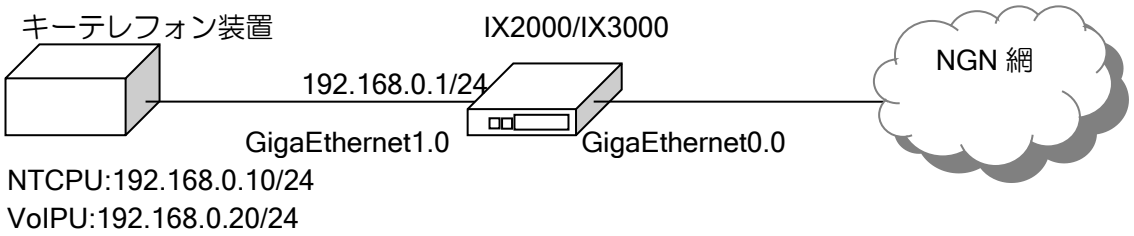
2.57.6.1 PPPoE 回線に接続



【設定例】
アクセス回線として PPPoE（GigaEthernet0.1）を使用
PPPoE のアドレスは動的（IPCP）に取得
GigaEthernet0.1 のアドレスをグローバルアドレスとして通知
GigaEthernet1.0 からアドレス情報通知要求を受信
キーテレフォンシステムのアドレスは 192.168.0.10,192.168.0.20
IP フォンサービスで複数の電話番号を取得

```
service kts-addressing

ip route default GigaEthernet0.1

kts-addressing external GigaEthernet0.1
kts-addressing allowed-host 192.168.0.10

ip access-list alist_napt permit ip src 192.168.0.0/24 dest any

ppp profile pppoe1
  authentication myname ix@nec.co.jp
  authentication password ix@nec.co.jp ix-router

interface GigaEthernet0.1
  encapsulation pppoe
  auto-connect
  ppp binding pppoe1
  ip address ipcp
  ip napt enable
  ip napt service rtp 192.168.0.20 none udp 10020-10051
  ip napt service sip 192.168.0.10 none udp 5060
  no shutdown

interface GigaEthernet1.0
  ip address 192.168.0.1/24
  no ip redirects
  ip napt enable
  ip napt address GigaEthernet0.1
  ip napt inside list alist_napt
  ip napt service rtp 192.168.0.20 none udp 10020-10051
  ip napt service sip 192.168.0.10 none udp 5060
  kts-addressing enable
  no shutdown
```

2.57.6.2 NGN 回線に接続（Ver.8.6 以降）

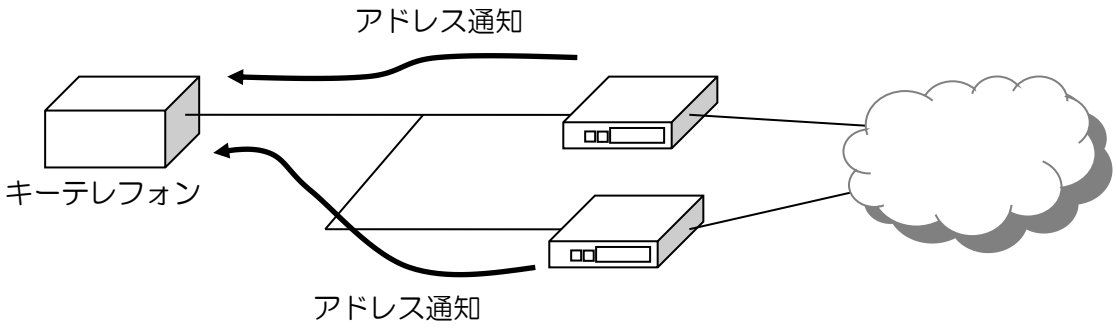


【設定例】
アクセス回線として NGN 回線（データコネクト）（GigaEthernet0.0）を使用
GigaEthernet0.0 のアドレスをグローバルアドレスとして通知
GigaEthernet1.0 からアドレス情報通知要求を受信
キーテレフォンシステムのアドレスは 192.168.0.10,192.168.0.20
IP フォンサービスで複数の電話番号を取得

```
service kts-addressing

kts-addressing external GigaEthernet0.0 ngn-mode
kts-addressing allowed-host 192.168.0.10
kts-addressing notify

ip access-list alist_napt permit ip src 192.168.0.0/24 dest any

interface GigaEthernet0.0
   ip address dhcp
   ip napt enable
   ip napt service rtp 192.168.0.20 none udp 10020-10051
   ip napt service sip 192.168.0.10 none udp 5060
   no shutdown

interface GigaEthernet1.0
   ip address 192.168.0.1/24
   no ip redirects
   ip napt enable
   ip napt address GigaEthernet0.0
   ip napt inside list alist_napt
   ip napt service rtp 192.168.0.20 none udp 10020-10051
   ip napt service sip 192.168.0.10 none udp 5060
   kts-addressing enable
   no shutdown
```

2.57.7 制限事項

- SIP-NAT との併用はできません。
- IX ルータを複数台使用した冗長構成を行うことはできません。
  キーテレフォンシステムでは、1 つのグローバルアドレスのみ対応しています。そのため、複数の IX ルータからアドレスを通知された場合、正常に動作しません。



■2.58 設定パラメータの一覧

標準的に使用されているパラメータ名と、IX2000/IX3000 シリーズの変更コマンドとの対応は、次のとおりです。

基本設定で説明したコマンドに対応する変数以外は、通常、デフォルト値で問題ありません。特に必要がない場合は、変更しないでください。

以下の表では、次の省略文字を使用しております。

m	モード
b	ブートモニタモード
o	オペレーションモード
g	グローバルコンフィグモード
d	デバイスコンフィグモード
i	インタフェースコンフィグモード

System

RFC1213	m	変更コマンド
sysDescr	-	機種ごと、バージョンごとに固定
sysObjectID	-	IX2215: .1.3.6.1.4.1.119.1.84.16.1（Ver.8.8 以降） IX2105: .1.3.6.1.4.1.119.1.84.14.1（Ver.8.5 以降） IX2106: .1.3.6.1.4.1.119.1.84.22.1 (Ver.9.6 以降) IX2107: .1.3.6.1.4.1.119.1.84.27.1 (Ver.10.6 以降) IX2207: .1.3.6.1.4.1.119.1.84.18.1（Ver.9.0 以降） IX2235: .1.3.6.1.4.1.119.1.84.25.1（Ver.10.4 以降） IX2310: .1.3.6.1.4.1.119.1.84.26.1（Ver.10.5 以降） IX3015: .1.3.6.1.4.1.119.1.84.20.1（Ver.9.1 以降） IX3110: .1.3.6.1.4.1.119.1.84.10.1（Ver.8.0 以降） IX3315: .1.3.6.1.4.1.119.1.84.21.1（Ver.9.4 以降）
sysContact	g	snmp-agent contact
sysName	g	hostname
sysLocation	g	snmp-agent location

Interfaces

RFC1213	m	変更コマンド
ifDescr	i	snmp-agent mib-2 ifdescr ※description コマンドでは変更されません
ifType	i	snmp-agent mib-2 iftype
ifMtu	i	ip mtu 未設定時はインタフェースが持つ MTU サイズ
ifSpeed	d	speed
	i	snmp-agent mib-2 ifspeed
ifPhysicalAddress	-	インタフェースが持つ物理アドレス固定
ifAdminStatus	i	shutdown
ifOperStatus	-	変更不可 インタフェースの運用状態

address-translation

RFC1213	m	変更コマンド
atPhysAddress	-	インタフェースが持つ物理アドレス固定
atNetAddress	i	ip address

IPv4

RFC1213	m	変更コマンド
ipForwarding	-	Forwarding 固定
ipDefaultTTL	-	64 固定
ipReasmTimeout	-	30 固定
ifPhysicalAddress	-	下位インタフェースが持つ物理アドレス固定
ipAddrTable	i	ip address
ipRouteTable	g	ip route
IX2000/IX3000 特有		変更コマンド
Reassemble Buffer Size	g	ip reassemble-buffer（Ver.8.4 以前） ip reassembly buffers（Ver.8.5 以降）
Max Route	g	ip max-route
Max Route Cache	g	ip cache-size

TCP

RFC1213	m	変更コマンド
tcpRtoAlgorithm	-	4(vanj)固定
tcpRtoMin	-	15000 固定
tcpRtoMax	-	1800000 固定
tcpMaxConn	-	-1 固定

IPv6

RFC2465	m	変更コマンド
ipv6Forwarding	-	Forwarding 固定
ipv6DefaultHopLimit	i	ipv6 hop-limit
ipv6IfEffectiveMtu	-	ipv6 mtu 未設定時はインタフェースが持つ MTU サイズ
ipv6IfReasmMaxSize	g	ipv6 reassemble-buffer（Ver.10.2 以前） ipv6 reassembly buffers（Ver.10.3 以降）
ipv6IfIdentifier	i	ipv6 interface-identifier
ipv6IfIdentifierLength	i	ipv6 interface-identifier
ipv6IfPhysicalAddress	-	下位インタフェースが持つ物理アドレス固定
ipv6IfAdminStatus	i	shutdown
ipv6AddrPrefixTable	i	ipv6 address および ipv6 prefix
ipv6AddrAddressTable	i	ipv6 address
IX2000/IX3000 特有		変更コマンド
Max Route	g	ipv6 max-route

ND

RFC2462	m	変更コマンド
DupAddrDetectTransmits	I	ipv6 nd dad-transmit
IX2000/IX3000 特有		変更コマンド
Garbage Time	i	ipv6 nd garbage-time
Static Cache	i	ipv6 nd static-neighbor
Cache Size	g	ipv6 nd max-neighbors

RA

RFC2461	m	変更コマンド
AdvSendAdvertisements	i	ipv6 nd ra enable
MaxRtrAdvInterval	i	ipv6 nd ra max-interval
MinRtrAdvInterval	i	ipv6 nd ra min-interval
AdvManagedFlag	i	ipv6 nd ra managed-config-flag
AdvOtherConfigFlag	i	ipv6 nd ra other-config-flag
AdvLinkMTU	i	ipv6 nd ra linkmtu
AdvReachableTime	i	ipv6 nd ra reachable-time
AdvRetransTimer	i	ipv6 nd ra retrans-timer
AdvCurHopLimit	i	ipv6 hop-limit
AdvDefaultLifetime	i	ipv6 nd ra lifetime
AdvPrefixList	i	ipv6 nd ra prefix-advertisement

IGMP

RFC2236	m	変更コマンド
Robustness Variable	-	2 固定
Query Interval	i	ip igmp query-interval
Query Response Interval	i	ip igmp query-max-response-time
Group Membership Interval	-	2*[Query Interval]+[Query Response Interval]
Other Querier Present Interval	-	2*[Query Interval]+[Query Response Interval]/2
Startup Query Interval	-	[Query Interval]/4
Startup Query Count	-	2 固定
Last Member Query Interval	-	1 秒固定
Last Member Query Count	-	2 固定
Unsolicited Report Interval	-	10 秒固定

MLD

RFC2710	m	変更コマンド
Robustness Variable	-	2 固定
Query Interval	-	125 秒固定
Query Response Interval	-	10 秒固定
Multicast Listener Interval	-	1 秒固定
Other Querier Present Interval	-	255 秒固定
Startup Query Interval	-	125/4 秒固定
Startup Query Count	-	2 固定
Last Listener Query Interval	-	1 秒固定
Last Listener Query Count	-	2 固定
Unsolicited Report Interval	-	10 秒固定
optimization done message	-	未サポート

VRRP

RFC2338	m	変更コマンド
VRID	i	vrrp ip
Priority	i	vrrp priority
IP_Addresses	i	vrrp ip
Advertisement_Interval	i	vrrp timers
Preempt_Mode	i	vrrp preempt
Authentication_Type	i	vrrp authentication
Authentication_Data	i	vrrp authentication

IPsec - Security Protocol Identifiers

RFC2407	m	変更コマンド
PROTO_ISAKMP	-	フェーズ 1 固定
PROTO_IPSEC_AH	g	ipsec autokey-proposal フェーズ 2
PROTO_IPSEC_ESP	g	ipsec autokey-proposal フェーズ 2
PROTO_IPCOMP	-	フェーズ 2（未サポート）

IPsec - Transform Identifiers

RFC2407	m	変更コマンド
KEY_IKE	-	フェーズ 1 固定
AH_MD5	g	ipsec autokey-proposal フェーズ 2
AH_SHA	g	ipsec autokey-proposal フェーズ 2
AH_DES	-	フェーズ 2（未サポート）
ESP_DES	g	ipsec autokey-proposal フェーズ 2
ESP_3DES	g	ipsec autokey-proposal フェーズ 2
ESP_NULL	g	ipsec autokey-proposal フェーズ 2
ESP_DES_IV64	-	フェーズ 2（未サポート）
ESP_RC5	-	フェーズ 2（未サポート）
ESP_IDEA	-	フェーズ 2（未サポート）
ESP_CAST	-	フェーズ 2（未サポート）
ESP_BLOWFISH	-	フェーズ 2（未サポート）
ESP_3IDEA	-	フェーズ 2（未サポート）
ESP_DES_IV32	-	フェーズ 2（未サポート）
ESP_RC4	-	フェーズ 2（未サポート）

IPsec - Identification Type Value

RFC2407	m	変更コマンド
ID_IPV4_ADDR	g	ike local-id, ike remote-id
ID_IPV4_ADDR_SUBNET	g	ike local-id, ike remote-id
ID_IPV6_ADDR	g	ike local-id, ike remote-id
ID_IPV6_ADDR_SUBNET	g	ike local-id, ike remote-id
ID_FQDN	g	ike local-id, ike remote-id
ID_USER_FQDN	g	ike local-id, ike remote-id
ID_IPV4_ADDR_RANGE	-	未サポート
ID_IPV6_ADDR_RANGE	-	未サポート
ID_DER_ASN1_DN	-	未サポート
ID_DER_ASN1_GN	-	未サポート
ID_KEY_ID	g	ike local-id, ike remote-id

IPsec - Encryption Algorithm

RFC2409	m	変更コマンド
DES-CBC	g	ike proposal
3DES-CBC	g	ike proposal
IDEA-CBC	-	未サポート
Blowfish-CBC	-	未サポート
RC5-R16-B64-CBC	-	未サポート
CAST-CBC	-	未サポート

IPsec - Hash Algorithm

RFC2409	m	変更コマンド
MD5	g	ike proposal
SHA	g	ike proposal
Tiger	-	未サポート

IPsec - Authentication Method

RFC2409	m	変更コマンド
DSS signatures	-	未サポート
RSA signatures	-	未サポート
Encryption with RSA	-	未サポート
Revised encryption with RSA	-	未サポート

IPsec - Group Description

RFC2409	m	変更コマンド
MODP768	g	ike policy,ipsec autokey-map
MODP1024	g	ike policy,ipsec autokey-map
EC2N155	-	未サポート
EC2N185	-	未サポート
MODP1536	g	ike policy,ipsec autokey-map

IPsec - Group Type

RFC2409	m	変更コマンド
MODP	-	固定
ECP	-	未サポート
EC2N	-	未サポート

IPsec - Life Type

RFC2409	m	変更コマンド
Seconds	g	ipsec autokey-map
Kilobytes	g	ipsec autokey-map

IPsec - Additional Exchange Type

RFC2409	m	変更コマンド
Quick Mode	-	固定
New Group Mode	-	未サポート

3章 UTM 機能の設定

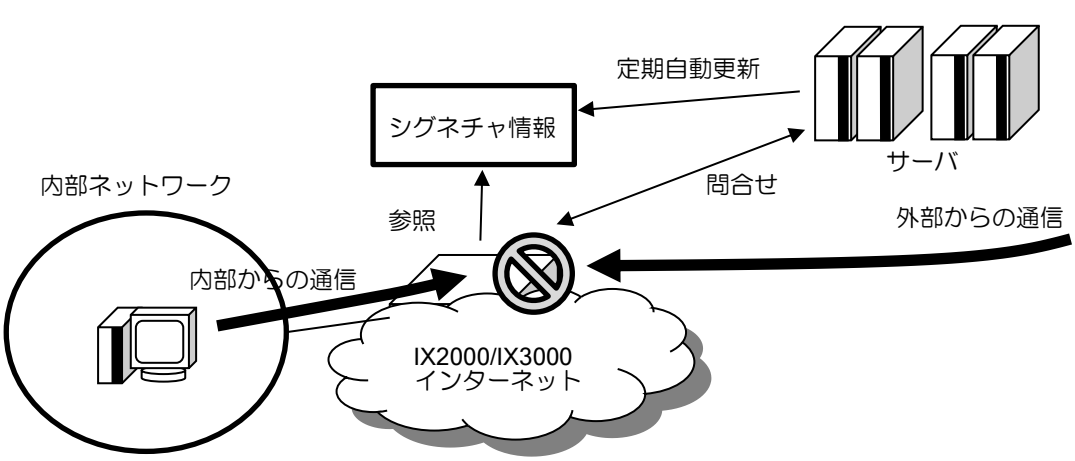
本章では、IX2000/IX3000 シリーズの UTM 機能（セキュリティ・スキャン機能）について説明します。

■3.1 はじめに

3.1.1 UTM 概要

IX ルータの UTM 機能を利用することで、従来のルータ機能を使用しながらセキュリティ・スキャン機能が利用できます。これにより、IX2000/IX3000 シリーズ 1 台でルータ機能とセキュリティ機能が実現できます。

セキュリティ・スキャンの実行結果をセキュリティログとして記録し、NetMeister や syslog サーバに通知できます。



3.1.2 機能一覧

IX2000/IX3000 シリーズの UTM 機能の一覧は以下のとおりです。

セキュリティ・スキャン機能

各トラフィックに対してセキュリティ・スキャンを実行し、脅威度を分類するとともに、通信の遮断、無害化などの対処を行います。

機能	対応バージョン	説明
アンチウイルス（AV）	Ver10.0 ～	通信内のウイルスファイルを検出および無害化
不正侵入防止（IPS）	Ver10.0 ～	不正アクセスなどの悪意のある通信を検出および遮断
Web ガード（WG）	Ver10.0 ～	端末が Web アクセスした URL が特定の危険な Web サイトと判断した場合にアクセスをブロック 個別に指定した URL を許可することも可能
URL フィルタリング（UF）	Ver10.0 ～	端末がアクセスした Web ページのカテゴリを分類し、カテゴリごとにアクセスを許可または遮断 各カテゴリに対する動作はユーザでカスタマイズ可能

運用・保守

セキュリティ・スキャン機能で分類された脅威度に応じてログの収集や通知を行います。

機能	対応バージョン	説明
セキュリティログ	Ver10.0 ～	脅威検出時の詳細なセキュリティ・スキャン結果 イベントログおよび脅威レポートとして通知可能
エラーログ	Ver10.0 ～	脅威検出およびライセンス切れをエラーログに記録
LED 通知	Ver10.0 ～	脅威検出とライセンス切れを装置の LED で通知
統計情報	Ver10.0 ～	セキュリティ・スキャンの実行回数や最新の脅威検出情報を表示

NetMeister 連携

NetMeister 連携機能の詳細な内容については NetMeister サービスのマニュアルを参照してください。

機能	対応バージョン	説明
アラーム通知	Ver10.0 ～	セキュリティ・スキャンで脅威を検出した際や、装置に登録している UTM ライセンスの有効期限が近づいた際に、NetMeister サービス上でアラームを通知 NetMeister サービス登録メールアドレスへの通知も可能
UTM 脅威レポート通知	Ver10.1 ～	日時ごとのセキュリティ・スキャンの実行結果を NetMeister サービス上からグラフィカルに確認可能
UTM 脅威分析通知	Ver10.2 ～	セキュリティ・スキャンで検出した個々の脅威についてのセキュリティログを、NetMeister サービス上から検索可能
UTM ライセンス自動設定機能	Ver10.9 ～	UTM ライセンスの自動設定、自動延長に対応。有効期限や延長処理を意識せずに UTM を利用することができます。 ※NetMeister サービスとの連携が必要になります。

その他機能

機能	対応バージョン	説明
ホワイトリスト設定	Ver10.0 ～	UTM スキャンの対象とせず無条件に許可する通信を設定できます (対象通信の判定にはアクセスリストを利用します)
UTM WebGUI	Ver10.1 ～	WebGUI から UTM のライセンス設定、スキャン設定が行えます WebGUI 上で UTM 脅威レポート情報を表示できます
機能別ホワイトリスト設定	Ver10.2 ～	各セキュリティ・スキャン機能ごとに、スキャンの対象とせず無条件に許可する通信を設定できます
グループ別ポリシー設定	Ver10.2 ～	通信をグループ分けし、セキュリティ・スキャン機能のポリシーを各グループに対して別々に適用できます。 (グループの判別にはアクセスリストを利用します)
証明書自動更新機能	Ver10.3 ～	UTM サーバとの接続で使用する証明書やアドレス情報の自動更新に対応。失効期限や更新手続きを意識せずご利用いただけます。

3.1.3 UTM ライセンス

UTM 機能を使用するためには UTM ライセンスキーが必要です。

別途 UTM ライセンスキーを購入してください。(UNIVERGE IX2000/IX3000 シリーズ UTM ライセンスシート)

UTM ライセンス自動設定機能を使用する場合、別途の NetMeister Partner Portal Service の契約およびオプション契約が必要となります。

- UTM 機能を動作させるためには装置にライセンスキー登録を行い、サーバからライセンス

情報を取得する必要があります。
- ✧ サーバから取得したライセンス情報は装置 FLASH メモリに保存されます。（ユーザがこのライセンス情報を参照することはできません。）

- ➢ ライセンスには有効期限があります。有効期限が近付くと、イベントログや NetMeister により通知されます。有効期限までにライセンスの延長を行ってください。
- ➢ ライセンスの有効期限を超えた場合は、UTM 機能は停止します。新規ライセンスを購入し、再度ライセンス登録を行ってください。
- ➢ ライセンスの有効期限の判定は、装置の時刻を元に行われます。IX ルータとライセンスサーバとの時刻の差が大きい場合、自動的にライセンスサーバの時刻と同期します。
  - ✧ ライセンスサーバとの時刻同期における精度は保証されませんので、NTP などによる時刻同期を推奨します。
- ➢ ライセンス未登録時でも、UTM 関連のコマンドは設定できます。

■3.2 注意事項

3.2.1 IPv4 インターネット接続の必要性

UTM が動作するためには、IX ルータが IPv4 インターネット上のライセンスサーバと通信できる必要があります。

3.2.2 セキュリティ・スキャン対象外のトラフィック

以下のパケットはセキュリティ・スキャンを行いません。

- ➢ トンネルによるカプセル化されたパケットおよび IPsec 暗号化されたパケット
  - ➢ 本装置で IPsec やトンネルの終端となっている場合は、IPsec やカプセル化されていないパケットが通過する LAN 側インタフェースや Tunnel インタフェースを指定することで UTM のセキュリティスキャンが行われます。
- ➢ TLS/SSL 暗号化された内容
  - ➢ WEB アクセスに対する URL フィルタおよび WEB ガード以外は暗号化された通信内容はスキャンの対象外となります。
- ➢ セッションの片方向通信パケットのみスキャンされるような構成
- ➢ マルチキャストアドレス宛のパケット
- ➢ 自装置（IX ルータ）宛のパケット
- ➢ ヘアピン NAT 変換されたパケット
  - ➢ Ver10.0 では自動的に UTM 対象外とならないため、ヘアピン NAT のパケットが折り返し通過する LAN インタフェースは UTM スキャン対象にしないようにしてください。
- ➢ Ver10.2 以前では IPv6 フラグメントパケットのスキャンは行われません。

3.2.3 メモリについて

UTM 利用時には UTM 有効前の状態で最低 50MB 以上の空きメモリが必要となります。

さらに、運用設定に応じてセキュリティログのメモリ保持や UFS キャッシュなどのメモリが追加で必要となります。

UTM 機能の利用を中止する場合、no utm license key および no utm enable 実行後、装置を再起動してください。

no utm license key や no utm enable のみの場合、UTM で確保されたメモリは解放されません。

3.2.4 UTM と併用できない機能

以下の機能が有効の場合は、UTM はご利用いただけません。

- ゼロコンフィグ機能

3.2.5 UTM が動作しないインタフェース

以下のインタフェースでは UTM をご利用いただけません。

- ブリッジ機能を有効にしたインタフェース（BVI インタフェースでの利用は可能）
- VRF 機能を有効にしたインタフェース

3.2.6 内蔵 SSL 証明書について

ライセンスサーバおよび、AV、UF サーバとの暗号化通信のため、IX ルータにはあらかじめ証明書が組み込まれています。証明書の期限が切れると UTM の動作安定性と有効性に問題が生じるため、証明書の失効前に適切な IX ルータのバージョンへの変更が必要です。

- Ver10.0、Ver10.1、Ver10.2 の UTM に組み込まれている証明書の期限は、2028 年 1 月 24 日までとなります。
- 証明書の更新時期や脆弱性対策により、装置に組み込まれている証明書の期限より前に失効させることがあります。（この場合、リリース通知等による事前通知を予定しています。）
- Ver10.3 以降、証明書および各種サーバアドレスの自動更新機能に対応しました。これにより、ユーザが意識することなく証明書等が更新されます。（コマンドによる手動更新にも対応）

3.2.7 最大セッション数に達した場合の動作について

最大セッション数を超過した場合、ver により超過した際の処理が異なります。

- Ver.10.3 以前：超過した通信のパケットは廃棄されます。
- Ver.10.4 以降：超過した通信のパケットは透過されます。

■3.3 基本設定

UTM 有効化，ライセンス、インタフェース指定等の最低限動セキュリティ・スキャンを動作させるための共通設定です。この他、UTM サーバとの通信のため IX ルータが IPv4 インターネットに接続できる必要があります。

- 共通設定（セキュリティ・スキャン対象のインタフェースに GigaEthernet1.0 を指定する場合）

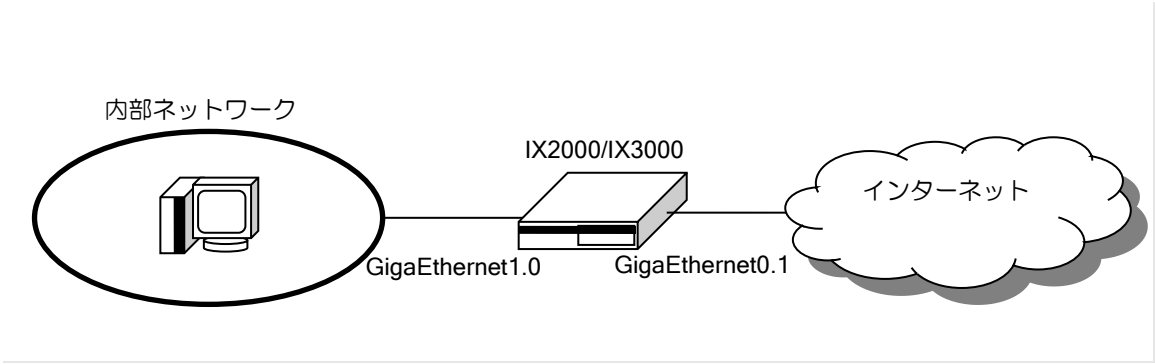
```
utm license key XXXXXXXXXXXXXXXX
utm enable
utm interface GigaEthernet1.0

ip ufs-cache enable

logging buffered
logging subsystem utm notice
logging timestamp datetime
```

- コマンドの説明

グローバルコンフィグモード	
utm license key	UTM ライセンスキーを登録します。
utm enable	UTM 機能を有効化します。 一部のセキュリティ・スキャン機能のみ有効化することもできます。
utm security-log	UTM セキュリティログを有効化、又は無効化します。 無効にした場合は、脅威検出時に一切通知がされなくなります。 デフォルトでは有効化の設定となるため通常は変更不要です。
utm interface	UTM 機能の監視対象のインタフェースの設定を行います。 指定したインタフェースを通過して送受信されるトラフィックに対してセキュリティ・スキャンを実行します。 複数のインタフェースを指定することも可能です。 ※暗号化やカプセル化されたパケットを監視することはできません。VPN 等のトンネルインタフェースを経由するトラフィックに対してキュリティ・スキャンを実行する場合は、トンネルインタフェース、もしくは LAN 側インタフェースを指定する必要があります。
ip ufs-cache enable	UFS キャッシュ機能を有効化することで、セキュリティ・スキャンの負荷を低減し通信速度の低下を抑止します。
logging subsystem utm warn	UTM のセキュリティログ等のイベントをイベントログとして出力します。 ※脅威度の低いセキュリティログも含めたイベントログが必要な場合は、logging subsystem utm notice を設定してください
logging buffered	発生したイベントログを装置上に保存します。
logging timestamp datetime	イベントログの発生時刻を保存します。 イベントログ有効時、セキュリティスキャンで脅威を検出した時刻をイベントログに残すことができます。

- 構成例

  IX2000/IX3000 を直接インターネットに接続する構成です。



WAN 回線を通過する通信に対してセキュリティ・スキャンを実行します
本構成は IPv4 PPPoE を WAN 回線とした設定例になりますが、MAP-E や
DS-Lite などの IPoE インターネット接続でもご利用いただけます。

設定条件	
接続構成	PPPoE インターネット接続
セキュリティスキャン機能	すべて有効
運用・保守機能	イベントログ有効(UTM ログレベル:notice) セキュリティログ有効(デフォルト有効) syslog サーバへの通知有効
NetMeister 連携	連携 UTM 脅威レポート通知(デフォルト有効) UTM 脅威分析通知
UTM スキャンインタフェース	WAN 側インタフェース指定(GigaEthernet0.1)

【設定】

```
logging buffered
logging subsystem utm notice
logging timestamp datetime
!
syslog ip host 192.168.1.253
!
ip route default GigaEthernet0.1
!
ip ufs-cache enable
!
nm ip enable
nm account “グループ ID”　password plain “グループパスワード”
!
utm license key XXXXXXXXXXXXXXXX
utm enable
utm interface GigaEthernet0.1
utm security-log-analytics enable

ppp profile pppoe1
   authentication myname xxx
   authentication password xxx xxxxxx

interface GigaEthernet0.1
   encapsulation pppoe
```

```
  auto-connect
  ppp binding pppoe1
  ip address ipcp
  ip napt enable
  no shutdown

interface GigaEthernet1.0
  ip address 192.168.1.254/24
  no shutdown
```

■3.4 脅威検出の通知と情報の取得について

UTM で脅威を検出した場合、設定に応じて以下のような方法での通知、情報の取得が可能です。
※セキュリティログ設定を無効化している場合、脅威を検出しても以下の機能は動作しません。

- 脅威レポート
- LED 通知
  - IPS 機能、および UF 機能では通知を行いません。
  - 脅威検出時の動作設定が「ログ表示のみ」の場合は通知を行いません。
- エラーログ
  - IPS 機能、および UF 機能では表示しません。
  - 脅威検出時の動作設定が「ログ表示のみ」の場合は表示しません。
- イベントログ
  - 別途、UTM のイベントログ設定が必要です。
- NetMeister へのアラーム通知
  - セキュリティ機能検出時動作設定を、透過(検出時ログ出力) (log-only)に設定している場合はアラーム通知を行いません。
  - UF 機能では通知を行いません。
  - IPS 機能では重要度の高い脅威を検出した場合にのみ通知を行います。
- NetMeister への脅威レポート通知
  - 別途、NetMeister への接続設定が必要です。
- NetMeister への脅威分析通知
  - 別途、脅威分析通知機能の有効化と NetMeister への接続設定が必要です。

NetMeister サービスと連携している場合、脅威検出時に指定したメールアドレスにアラーム通知するようサービス側で設定しておくことが可能です。

検出した脅威については NetMeister サービス上で詳細情報を確認することができます。詳しくは NetMeister サービスのマニュアルをご覧ください。

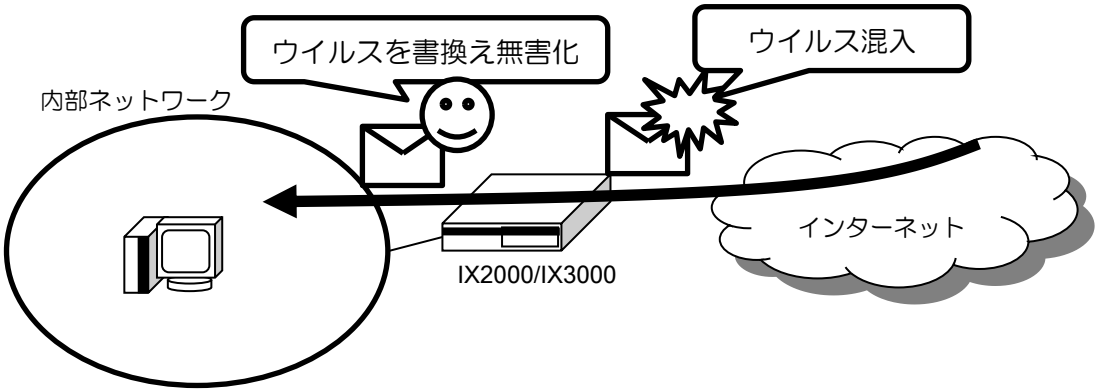
NetMeister サービスと連携していない場合、以下のコマンドで検出した脅威の情報を取得することができます。

コマンド	取得できる情報
show utm security-report	脅威の種類ごとに検出数を表示
show utm statistics	最後に検出した脅威の種類、アクセス元 IP、アクセス先 IP などの情報を表示
show logging	検出した脅威の種類、アクセス元 IP、アクセス先 IP などのセキュリティログ情報をイベントログ中に表示 (UTM のイベントログ設定の有効化が必要)

■3.5 セキュリティ・スキャン

3.5.1 アンチウイルス（AV）

3.5.1.1機能説明



Web サイトへのアクセスやメールの送受信などで転送されるファイルの内容を監視します。有害なファイルを検出した場合、データの一部を書換えることでファイルを破壊し、無害化することができます。アンチウイルス機能ではセキュリティ・スキャンの都度クラウドサーバに問い合わせを行っており、常に最新のシグネチャを参照しているため、脅威に対して柔軟に対応することができます。

アンチウイルス機能が検出できる脅威の例として以下のものがあります。
・ウイルス
・スパイウェア
・トロイの木馬
・ワーム

アンチウイルス機能のセキュリティ・スキャン対象とできるプロトコルは以下の通りです。

- セキュリティ・スキャン対象となる通信プロトコル

プロトコル	対象
HTTP	検出対象ポート　：全ポート 検出対象メソッド　：GET,POST
FTP	検出対象ポート　：20,21
SMTP	検出対象ポート　：25,587 検出対象エンコード　：base64,quoted-printable,Uuencode 検出対象ファイル形式：eml
POP3	検出対象ポート　：110 検出対象エンコード　：base64,quoted-printable,Uuencode 検出対象ファイル形式：eml
IMAP4	検出対象ポート番号　：143 検出対象エンコード　：base64,quoted-printable,Uuencode

アンチウイルス機能のセキュリティ・スキャンの対象とできるファイル形式は以下の通りです。特定の形式で圧縮されたファイルもセキュリティ・スキャン対象とすることができます。ファイルが複数のパケットに分割・フラグメントされた場合もスキャン対象とすることができます。

- 検出対象ファイル

プロトコル	対象
ファイル形式	exe(dll,scr), com, elf, js, pdf, bat, cmd, vbs, wsf, doc(docx), ppt(pptx), xls(xlsx), msi
圧縮形式	gz, zip, jar, apk

3.5.1.2 注意事項

UTM サービスに脅威として登録されているウイルスがアンチウイルス機能の検出対象となります。検出対象の脅威はクラウドサーバから配信され、随時更新されます。

転送ファイルが以下に該当する場合、セキュリティ・スキャンの対象とすることはできません。
・複数のファイルがアーカイブされている場合

パスワード付きファイルや暗号化されたファイルをセキュリティ・スキャンの対象とすることはできません。

アンチウイルス機能ではセキュリティ・スキャンの実行時にクラウドサーバへの問い合わせを行うため、環境によっては通信性能が低下する可能性があります。

3.5.1.3 アンチウイルス（AV）の設定

初期状態では以下の設定となっています。

機能	初期値
検出時の動作	対象ファイルを無害化し透過
個別解除設定	なし
対象プロトコル	HTTP,FTP,POP3,SMTP,IMAP4
圧縮ファイルのスキャン機能	有効
高圧縮ファイルのスキャン機能	無効
スキャン可能サイズ	2MB
セキュリティログ	有効

設定変更は以下のコマンドで行います。

グローバルコンフィグモード	
utm　enable anti-virus	スキャンの個別指定
utm anti-virus	アンチウイルス機能の設定 （UTM アンチウイルスコンフィグモードに移行）

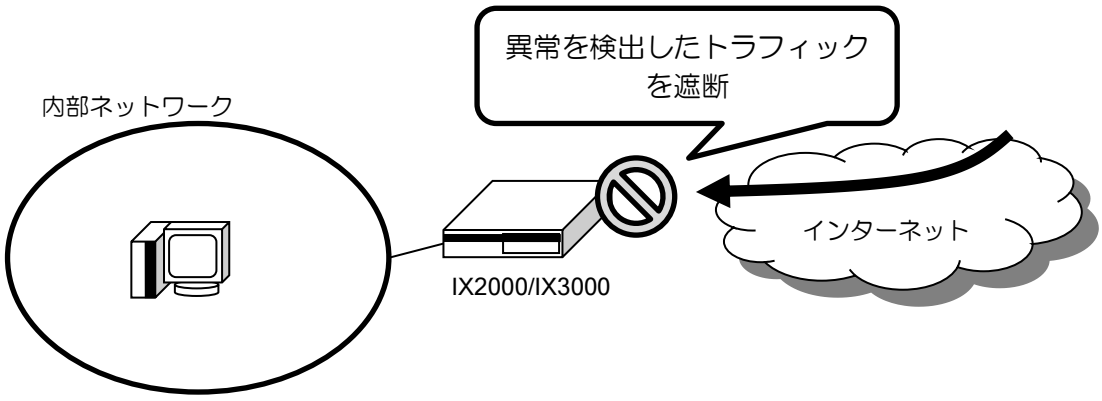
UTM アンチウイルスコンフィグモード	
action	脅威検出時の動作設定 block　（対象ファイルを無害化して透過） log-only（対象ファイルを無害化せず透過） ※ どちらの動作も脅威検出時にセキュリティログを出力します。
ignore id {VID}	VID 個別解除設定 VID：ウイルス ID セキュリティログ等で通知されるウイルスに割り当てられた ID です。特定のウイルス検出を無効化する場合、該当する VID を指定してください。
protocol	監視対象のプロトコル設定
scan compress-file	圧縮ファイルのスキャン機能の有効化
scan decomp-bomb	高圧縮ファイル（※）のスキャン機能の有効化 ※100 倍以上のサイズに解凍されるファイル （1MB の zip ファイルを解凍すると 100MB 以上のファイルになるような場合）
scan-size	スキャン可能サイズの設定

デフォルト動作から変更する設定例

utm anti-virus 　action log-only 　scan-size 10	異常検出時に無害化せず透過 圧縮ファイルのスキャン対象ファイルサイズ上限 10MB

3.5.2 不正侵入防止（IPS）

3.5.2.1 機能説明



ネットワークへの不正侵入を試みる攻撃パターンを検出します。

既知の侵入手口のパターンとマッチングさせることにより検出し、 通信を防止することで、ファイアウォール(ダイナミックフィルタ)では検知できないネットワークに対する 攻撃を認識、防止する機能になります。

IPS 機能は UTM サーバから定期的にダウンロードするシグネチャ情報を参照し、攻撃パターンと一致する通信や脆弱性のある通信を脅威として検出します。拡張機能で検出する一部の脅威を除き、脅威が検出された通信は廃棄されます。

既存の IDS 機能を併用することもできます。併用している場合は、IDS 機能で廃棄されなかったパケットが対象となります。

3.5.2.2 注意事項

UTM サービスに登録されている攻撃パターンが IPS 機能の検出対象となります。検出対象の攻撃パターンはクラウドサーバから配信され、随時更新されます。

3.5.2.3 拡張機能

拡張機能を有効化することにより、IX ルータに組み込まれたシグネチャ情報による脅威検出を行うことができます。拡張機能として設定できる脅威検出にはプロトコル不正検出とポートスキャン検出があります。

プロトコル不正検出

プロトコルで取り決められた形式に完全に従っていない通信を検出します。

拡張機能のプロトコル不正検出では、通信は廃棄されません。セキュリティログおよび統計情報に脅威検出情報が記録されます。

- プロトコル不正（URI）検出内容

SID	概要	検出条件
80300001	ASCII-ENCODING ATTACK	ASCII によるエンコードを検出した場合
80300002	DOUBLE-DECODING ATTACK	二重デコードを検出した場合
80300003	U-ENCODING ATTACK	Unicode によるエンコードを検出した場合
80300004	BARE-BYTE-UNICODING-ENCODING ATTACK	ベアバイトの Unicode によるエンコードを検出した場合
80300005	UTF-8-ENCODING ATTACK	UTF-8 によるエンコードを検出した
80300006	IIS-UNICODE-CODEPOINT-ENCODING ATTACK	IIS から Unicode へのエンコードを検出した場合
80300007	MULTI-SLASH-ENCODING ATTACK	マルチスラッシュのエンコードを検出した場合
80300008	IIS-BACKSLASH-EVASION ATTACK	IIS によるバックスラッシュ攻撃を検出した場合
80300009	SELF-DIRECTORY-TRAVERSAL ATTACK	自己ディレクトリへのトラバーサル攻撃を検出した場合
80300010	DIRECTORY-TRAVERSAL ATTACK	ディレクトリへのトラバーサル攻撃を検出した場合
80300011	APACHE-WHITESPACE ATTACK	Apache Web サーバへのスペースを含む URI 検出時
80300012	NON-RFC-HTTP-DELIMITER ATTACK	RFC 非準拠の区切り記号を含む HTTP プロトコル検出時
80300013	NON-RFC-DEFINED-CHAR ATTACK	RFC 非準拠定義の検出時
80300014	OVERSIZE-REQUEST-URI-DIRECTORY ATTACK	指定された長さより長い URL の要求を検出した場合
80300015	OVERSIZE-CHUNK-ENCODING ATTACK	エンコードされたリクエストの使用を検出した場合
80300016	UNAUTHORIZED-PROXY-USE-DETECTED ATTACK	不正なプロキシの検出時
80300017	WEBROOT-DIRECTORY-TRAVERSAL ATTACK	Web サーバのルートディレクトリへのトラバーサル攻撃を検出した場合

- プロトコル不正（パケット）検出内容

SID	概要	検出条件
80400003	IP header length < 20	IP ヘッダが 20byte 以下の場合
80400004	IP header length exceeds packet length.	IP ヘッダがパケット長を超えている場合
80400005	Bad IP checksum.	IP でチェックサムエラーを検出した場合

80400006	IP Option Truncated found.	IP ヘッダのオプションが切り捨てられた場合
80400007	IP Option found with bad lengths.	IP ヘッダのオプションが不正な長さの場合
80400009	Short TCP packet, length is less than header length.	TCP パケットがヘッダより短い場合
80400010	TCP header length < 20	TCP ヘッダが 20byte 以下の場合
80400011	TCP Header length exceeds packet length.	TCP ヘッダがパケット長を超えている場合
80400012	Bad TCP checksum.	TCP でチェックサムエラーを検出した場合
80400013	TCP Options found with bad lengths.	TCP オプションが不正な長さの場合
80400014	TCP Options Truncated found.	TCP ヘッダのオプションが切り捨てられた場合
80400015	TCP Options T/TCP Detected.	TCP オプションで T/TCP を検出した場合
80400016	TCP Options Obsolete found.	廃止された TCP オプションを検出した場合
80400017	TCP Options Experimental found.	実験的な TCP オプションを検出した場合
80400018	Short UDP packet, length is less than header length.	UDP パケットがヘッダ長より短い場合
80400019	Invalid UDP header.	UDP ヘッダが不正の場合
80400020	Short UDP packet, length field > payload length.	短い UDP パケットのフィールド長がペイロードよりも大きい場合
80400021	Bad UDP checksum.	UDP でチェックサムエラーを検出した場合
80400022	ICMP Header Truncated.	ICMP でヘッダサイズのエラーを検出した場合
80400023	ICMP Timestamp Header Truncated.	ICMP でタイムスタンプのエラーを検出した場合
80400024	ICMP Address Header Truncated.	ICMP でアドレスのエラーを検出した場合
80400025	Bad ICMP checksum.	ICMP でチェックサムエラーを検出した場合
80400026	Short ICMP packet, length is less than header length.	ICMP パケットがヘッダ長よりも短い場合
80400027	Invalid ICMP type.	ICMP のタイプが無効な場合

ポートスキャン検出

ネットワーク上の装置の複数のポートに接続要求を行い、利用可能なポートを特定しようとするポートスキャン攻撃を検出します。

拡張機能のポートスキャンに該当する脅威を検出した際は、該当する通信を一定時間遮断します。ポートスキャン検出が通信を遮断する時間（ブロックタイマ）は設定により指定することが可能です。

- ポートスキャン検出内容

SID	概要	検出条件
80600001	TCP RST Scan	ホスト IP から 1 分間に 30 ポート以上の接続を 1 対多、多対 1、多対多の TCP ポートでスキャンを検出した場合。 SID:80200001-80200008, 80200017-8020002 を含む
80600002	TCP Flood Scan	同ホスト IP から 1 分間に 60 回以上の同ポートへの多重接続を検出した場合。(TCP プロトコルによる DoS 攻撃) SID:80200028, 80200031 を含む
80600003	UDP Scan	同ホスト IP から 1 分間に 30 ポート以上のスキャンを UDP・ICMP ポートで検出した場合。 SID:80200009-80200016,80200017-80200024,80200025-80200027,80200029,80200031 を含む

3.5.2.4 不正侵入防止（IPS）の設定

初期状態では以下が設定されています。

機能	初期値
検出時の動作	遮断
プロトコル不正検出	無効
ポートスキャン検出	無効
個別解除設定	なし
セキュリティログ	有効

設定変更は以下のコマンドで行います。

グローバルコンフィグモード	
utm ips	IPS 機能の設定 （UTM IPS コンフィグモード移行）
utm security-log	セキュリティログの有効化

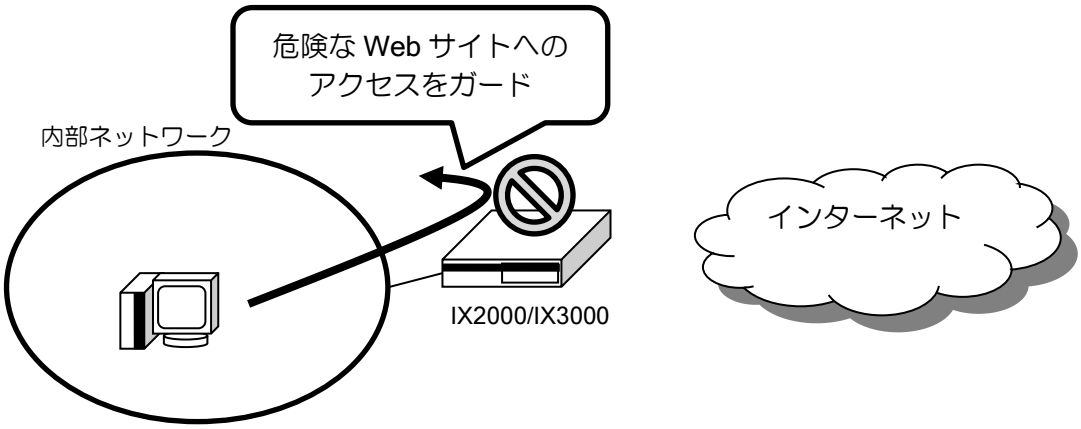
UTM IPS コンフィグモード	
basic-inspection	不正侵入検出時の動作設定（拡張機能を除く） block　（対象トラフィックを遮断） log-only（対象トラフィックを透過） ※ どちらの動作も異常検出時にセキュリティログを出力しますが、logging subsystem utm および utm security-log が設定されていない場合、セキュリティログは出力されません。
extended-inspection protocol-anomaly	プロトコル不正検出設定（拡張機能） • 検出ログ出力のみ行い透過 • 無効
extended-inspection traffic-anomaly	ポートスキャン検出設定（拡張機能） • 遮断 • 無効
extended-inspection traffic-anomaly block-period	ポートスキャン検出時のブロックタイマ設定 ※共通ポリシーでのみコンフィグ可能で、すべてのグループ別ポリシーにも適用されます。
ignore id {SID}	SID 個別解除設定 SID：シグネチャ ID セキュリティログ等で通知される IPS の脅威に割り当てられた ID で、特定の脅威検出を無効化する場合に指定します。

デフォルト動作から変更する設定例

utm ips basic-inspection block extended-inspection protocol-anomaly log-only extended-inspection traffic-anomaly block extended-inspection traffic-anomaly block-period 3600	脅威検出した通信をブロックする。 拡張機能のプロトコル不正で検出した脅威はログのみを記録し、ブロックしない。 拡張機能のポートスキャン検出時は該当する通信を 3600 秒間ブロックする。

3.5.3 Web ガード（WG）

3.5.3.1 機能説明



Web サイトへのアクセスを検出した場合にパケットに含まれる URL をシグネチャと照合し、フィッシングサイトや閲覧によってウイルス感染を起こす既知の危険な Web サイトなどへのアクセスをガードします。

ブロック対象の URL に対して透過設定をすることで、アクセスを個別に許可することもできます。

HTTP の Web アクセスがブロックされた場合、利用者のブラウザにブロックした旨を表示します。設定により別のページにリダイレクトすることもできます。

【Web ガードによりアクセスがブロックされた際の表示例】

```
Access intercepted by UTM filter.
URL: xxxxxx.com/download/xxx
Type : 2
Category : 50000
```

Web ガードによるブロックは「Type : 2」となります。

※ HTTPS の Web アクセスがブロックされた場合、ブラウザで用意されているアクセス不能のページが表示されます。ブラウザご利用中、アクセス不能の画面が表示された場合は、必要に応じてセキュリティログをご確認ください。

Web サイトアクセスとして検出するプロトコルは以下となります。

- 検出対象

プロトコル	対象
HTTP	URL のホスト名・パス名 検出対象のポート番号　：全ポート 検出対象のメソッド　：GET,POST
HTTPS	URL のホスト名 検出対象のポート番号　：443 検出対象のメソッド　：GET,POST

※ プロキシサーバの利用などにより HTTPS で 443 以外のポート番号が利用される場合「utm https-port」コマンドで HTTPS 判定されるポートを追加する必要があります。

3.5.3.2 注意事項

HTTPS の Web アクセスをブロックした場合に、その旨を表示するページを表示したりリダイレクトすることは出来ません。

3.5.3.3 Web ガード（WG）の設定

初期状態では以下が設定されています。

機能	初期値
検出時の動作	遮断
個別解除設定	なし
セキュリティログ	有効

設定変更は以下のコマンドで行います。

グローバルコンフィグモード	
utm web-guard	WG 機能の設定 （UTM WG コンフィグモード移行）
utm security-log	セキュリティログの有効化

UTM IPS コンフィグモード	
action	対象 URL 検出機能の動作設定 block　（対象トラフィックを遮断） log-only（対象トラフィックを透過） ※ どちらの動作も異常検出時にセキュリティログを出力しますが、logging subsystem utm および utm security-log が設定されていない場合、セキュリティログは出力されません。
ignore url {URL}	URL 個別解除設定 URL：URL 文字列 特定の URL について脅威検出を無効化する場合に指定します。

デフォルト動作から変更する設定例

utm web-guard action block ignore url www.example.jp/test	検出時は廃棄 www.example.jp/test は Web ガード機能から除外

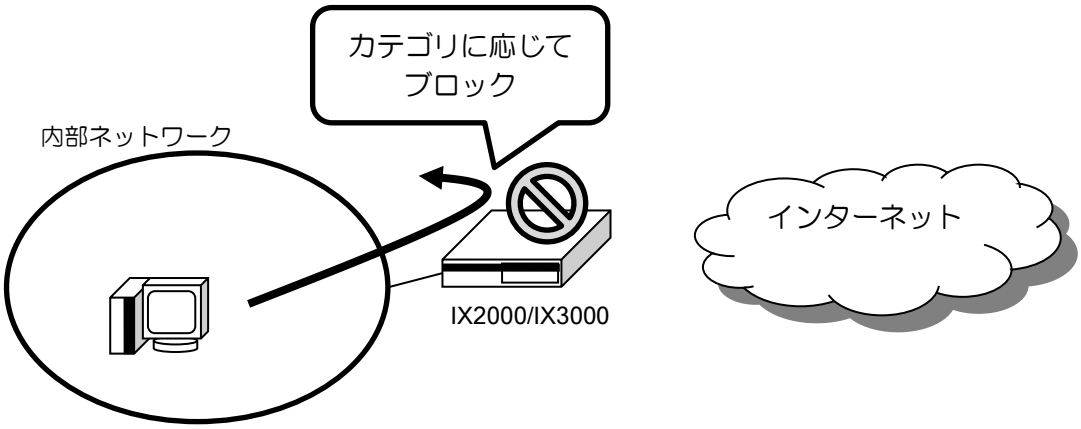
個別除外の URL を設定した場合、ホスト名は完全一致、パス名は前方一致となります。HTTP はホスト名とパス名、HTTPS はホスト名のみで判定します。

utm https-port 8080 utm proxy http://proxy.example.co.jp:8080	HTTP スキャン対象とする TCP ポートに 8080 番を追加

プロキシサーバの利用などにより HTTPS で 443 以外のポート番号が利用される場合、「utm https-port」コマンドで HTTPS 判定されるポートを追加する必要があります。

3.5.4 URL フィルタリング（UF）

3.5.4.1 機能説明



Web サイトへのアクセスを検出した場合にパケットに含まれる URL を解析し、外部サーバへ問い合わせを行うことで Web サイトのカテゴリ分類を行います。アクセス先の Web サイトのカテゴリがブロック対象のカテゴリに該当した場合、Web アクセスをブロックします。カテゴリごとの許可・ブロックは個別に設定することができます。

HTTP の Web アクセスがブロックされた場合、利用者のブラウザにブロックした旨を表示します。 設定により別途用意されたブロックページにリダイレクトすることもできます。

【URL フィルタリングの表示例】

```
Access intercepted by UTM filter.
URL: xxxxxx.com/
Type : 1
Category : 62000
```

URL フィルタリングによるブロックは「Type : 1」となります。

※ HTTPS の Web アクセスがブロックされた場合、ブラウザで用意されているアクセス不能のページが表示されます。ブラウザご利用中、アクセス不能の画面が表示された場合は、必要に応じてセキュリティログをご確認ください。

指定可能なカテゴリは以下になります。複数の個別カテゴリをまとめたスタンダードカテゴリと、個別カテゴリの指定ができます。

- 個別カテゴリー覧

カテゴリ ID	カテゴリ
10000	ポルノ
11000	アダルトサイト
12000	ギャンブル・宝くじ
13000	アルコール・たばこ
14000	ドラッグ
15000	過激論・人種差別

16000	中絶
17000	犯罪行為
18000	暴力的なサイト
19000	気持ち悪いサイト
20000	ゲーム
21000	インスタントメッセージ
22000	出会い系サイト
23000	ソーシャルネットワーク
24000	Web チャットルーム
25000	ショッピング・オークション
26000	ミュージック
27000	コミック・アニメ
28000	エンターテインメント・芸術
29000	ストリーミング・VoIP
30000	P2P
31000	マルチメディアダウンロード
32000	オンライン共有・ストレージ
33000	シェアウェア・フリーウェア
34000	Web メール
35000	システム更新
36000	コンテンツ配信サーバ
37000	Web サービス API
38000	ネットワークサービス
39000	リモートコントロール
40000	プロキシ・アノニマイザー
41000	フィッシング詐欺
42000	マルウェア
43000	ブラックハット SEO サイト
44000	危険アプリケーション
45000	広告
46000	ポータル・検索サイト
47000	輸送機関
48000	不動産
49000	金融・保険
50000	コンピュータ・IT
51000	ビジネス・サービス
52000	参考文献・研究
53000	教育機関
54000	軍隊・兵器
55000	政治・政府
56000	協会・慈善団体
57000	旅行
58000	飲食物
59000	家・庭
60000	健康・医学
61000	宗教・数秘術
62000	スポーツ
63000	自動車
64000	求人情報
65000	ニュース・メディア
66000	フォーラム・ニュースグループ
67000	ブログと個人サイト
68000	不明なサイト
69000	ドメインパーキング

70000	デッドサイト
71000	プライベート IP アドレス

- スタンダードカテゴリー覧

スタンダードカテゴリ	カテゴリ名称	対象カテゴリ ID
all	全てのカテゴリ	10000～71000
adult	アダルトサイトカテゴリ	10000～19000,22000
malicious	危険サイトカテゴリ	41000～44000
sns	SNS サイトカテゴリ	21000,23000,24000,66000,67000
entertainment	エンターテインメント サイトカテゴリ	20000,25000～29000

Web サイトアクセスとして検出するプロトコルは以下となります。

- 検出対象

プロトコル	対象
HTTP	URL のホスト名・パス名 検出対象のポート番号　：80 検出対象のメソッド　：GET,POST
HTTPS	URL のホスト名 検出対象のポート番号　：443 検出対象のメソッド　：GET,POST

※ HTTP でドメインが IP アドレスで指定された場合、IP アドレスとしてカテゴリに一致しない限りは未定義カテゴリに分類されます。

※ HTTPS でドメインが IP アドレスで指定された場合、検出の対象となりません。

プロキシサーバの利用などにより HTTPS で 443 以外のポート番号が利用される場合「utm https-port」コマンドで HTTPS 判定されるポートを追加する必要があります。

3.5.4.2 注意事項

特定の URL アクセスをブロックしたい場合は内部 URL フィルタリング(ルータの設定•URL フィルタリングを参照してください)を併用してください。

特定の URL アクセスを許可する場合は UTM の URL フィルタ URL 個別除外で設定してください。

外部 URL フィルタリングとの併用はセッション性能が著しく低下する恐れがあるため非推奨です。

3.5.4.3 URL フィルタリング（UF）設定

初期状態では以下が設定されています。

機能	初期値	備考
廃棄カテゴリ指定	アダルトサイトカテゴリ (adult 10000-19000 22000) 危険サイトカテゴリ (malicious 41000-44000)	
未定義カテゴリの廃棄設定	透過	
サーバ未応答時の廃棄設定	透過	
URL 個別解除設定	なし	
セキュリティログ	有効	

設定変更、確認は以下のコマンドで行います。

グローバルコンフィグモード	
utm url-filter	URL フィルタリング機能の設定 （UTM URL フィルタコンフィグモード）
utm security-log	セキュリティログの有効化
utm https-port	HTTPS ポート番号追加設定 プロキシポート番号設定
utm query url-category	URL カテゴリ問合わせコマンド(Ver10.1 以降) ※ サーバへ問合せをするコマンドであるため、 show running-config には反映されません。

UTM URL フィルタコンフィグモード	
reject category	廃棄カテゴリの設定
reject no-category	未定義カテゴリの廃棄設定 （カテゴリ不明サイトをブロックする）
reject no-response	サーバ未応答時の廃棄設定 （カテゴリ判定不可能時にブロックする）
reject dry-run enable	URL フィルタリング試験運用設定 廃棄カテゴリにマッチした通信のログを記録しますが、 実際に廃棄はしない設定となります。(Ver10.2 以降)
ignore url {UTM}	URL 個別解除設定 ※ 先頭文字に*(ワイルドカード)を設定した場合は、ホスト名およびサブドメインについても、ワイルドカードとして判定されます。

■3.6 運用・保守

3.6.1 イベントログ

UTM イベントログでは、UTM 機能にて検出したセキュリティ脅威やその他 UTM 関連のログ情報を記録します。

イベントログには以下の内容が記録されます。

イベントログ	ログ内容	イベント出力条件
セキュリティログ	Json 形式のセキュリティログ（セキュリティログの内容は後述の章を参照してください）	logging subsystem utm が有効（UTM.001～UTM.016） イベントログ内容については、イベントログ・リファレンスを参照してください。 設定したログレベルに応じたセキュリティログが出力されます。 脅威度の低いセキュリティログも出力する場合は logging subsystem utm notice を設定してください。 脅威検出されなかったセキュリティ・スキャン結果を含め、全てのセキュリティログを出力する場合は logging subsystem utm info を設定してください。
その他ログ	UTM 機能のイベントログ（UTM起動失敗、メモリ枯渇エラーなど）	logging subsystem utm が有効（UTM.021～）

3.6.2 エラーログ

UTM 機能で発生した特に重要なログ情報をエラーログとして記録します。

エラーログには以下の内容が記録されます。

エラーログ	ログ内容
ALERT:Security Scan LED control Start	AV/WG での脅威検出による LED 通知の開始
ALERT:Security Scan LED control End	AV/WG での脅威検出による LED 通知の終了
ALERT:Security Scan License Warning	ライセンス期限切れ間近の警告
ALERT:Security Scan License Expiration	ライセンス期限切れ

※　IPS/UF による脅威検出では LED 表示は行われません。

3.6.3 統計情報

UTM 機能の統計情報を表示します。

以下の統計情報を記録します。

機能	統計情報	説明
アンチウイルス（AV）	スキャンしたセッション数	AV 機能でスキャンしたセッションの数
	検出したセッション数	AV 機能で脅威検出したセッションの数
不正侵入防止（IPS）	スキャンしたフロー数	IPS 機能でスキャンしたトラフィックフローの数
	検出したフロー数	IPS 機能で脅威検出したトラフィックフローの数
	ブロックしたフロー数	IPS 機能で遮断したトラフィックフローの数
Web ガード（WG）	スキャンした URL 数	WG 機能でスキャンした URL の数
	検出した URL 数	WG 機能で脅威検出した URL の数
	ブロックした URL 数	WG 機能で遮断した URL の数
URL フィルタリング（UF）	スキャンした URL 数	UF 機能でスキャンした URL の数
	ブロックした URL 数	UF 機能で遮断した URL の数

3.6.4 LED 通知

UTM 機能で脅威検出時およびライセンス切れを装置の LED ランプによりユーザに通知します。

通知開始契機	LED 状態	通知停止契機
UTM 起動失敗 ライセンス認証失敗	ALM：点滅（遅） VPN：点滅（遅） PPP：点滅（遅） BAK：点滅（遅）	・通知停止コマンド実行 ・UTM ライセンス削除
AV 異常検出 WG 異常検出	ALM：点滅（遅） VPN：点滅（遅） PPP：消灯 BAK：消灯	・最新の検出から一定時間後自動停止 (時間はコンフィグ設定可) ・通知停止コマンド実行 ・UTM ライセンス削除
ライセンス期限満了間近になった時	ALM：点滅（遅） VPN：消灯 PPP：消灯 BAK：点滅（遅）	・ライセンス更新 ・通知停止コマンド実行 ・UTM ライセンス削除
ライセンス切れ	ALM：点滅（遅） VPN：消灯 PPP：消灯 BAK：点灯	・ライセンス更新 ・通知停止コマンド実行 ・UTM ライセンス削除

※　点滅（遅）：2 秒周期点滅

※　IPS/UF による脅威検出では LED 表示は行われません。
※　UTM 機能で LED 表示中は、本来の VPN、PPP、BAK 機能での LED 表示は行われません。
※　UTM 機能で同時に複数の LED 表示が発生した場合は、点灯＞点滅（遅）＞消灯の優先順位の OR 条件で各 LED が表示されます。
※　LED 消灯コマンド「clear utm led」を実行しても、新たに脅威検出やライセンス期限切れ通知が行われるタイミングで再度 LED 表示が発生します。
※　UTM ライセンス自動設定機能が有効の場合、ライセンス期限満了間近の LED 表示は行われません。

■3.7 NetMeister 連携

UTM 機能にて検出したイベントを NetMeister に通知することができます。

※ 通知の種類ごとに NetMeister へ送信する情報は異なります。構築する環境のセキュリティポリシーに従っていずれの通知を有効化するか判断してください。
※ 設定の詳細は「NetMeister の設定」を参照してください。

3.7.1 アラーム通知

通知内容	通知契機
アンチウイルス(AV)ガード	AV 脅威検出時
不正侵入防止(IPS)ガード	IPS 脅威検出時 （重要度の高い脅威のガード時のみ通知）
Web ガード(WG)ガード	WG 脅威検出時
ライセンス期限満了間近になった	ライセンス切れ警告発生時 （ライセンス切れ数日前に通知。日数は設定可能） （1 日 1 回通知）
ライセンス切れ	ライセンスの有効期間が満了したとき（1 日 1 回通知）

※ セキュリティ機能検出時動作設定を、透過(検出時ログ出力) (log-only)に設定している場合はアラーム通知を行いません。
※ URL フィルタリングはアラーム通知されません。
※ UTM ライセンス自動設定機能が有効の場合、ライセンス期限満了間近のアラーム通知は行いません。

NetMeister への UTM 情報は以下のルールで通知されます。

（1） 最初に検出した脅威は、重要度に関わらず即時通知。
（2） 前回と同じ重要度、または、前回より低い重要度の脅威を検出した場合は、30 分の間隔を空けて通知する。
（3） 前回よりも重要度の高い脅威を検出した場合は、即時通知する。
（4） 前回通知から 30 分以上脅威を検出していなければ即時通知する。

UTM 機能で検出した脅威の情報が NetMeister に通知されます。NetMeister サービス上では以下のアラーム情報が確認できます。

検出したスキャンの種類(AV、IPS、WG)
重要度
検出時のアクション
検出時刻
検出した脅威の内容・通信情報(IP、ポート)

3.7.2 UTM 脅威レポート通知

Ver10.1 以降では、UTM で検出した脅威情報を、NetMeister や、IX ルータの CLI や Web コンソールから確認できます。

Web コンソールや CLI

IX ルータの Web コンソール上で、UTM で検出した脅威レポートを累計、もしくは 3 日間合計で表示確認できます。また、CLI でも確認できます。

NetMeister

NetMeister で、UTM で検出した脅威を月次のレポートとしてグラフ表示で確認できます。

NetMeister へは、1 時間に 1 回、検出した脅威情報が送信されます。送信内容には以下の情報が含まれます。

- 送信時タイムスタンプ
- アンチウイルスのスキャン数、検出数、ブロック数（合計）
- アンチウイルスで検出した脅威毎のウイルス ID、ウイルス名、検出数、ブロック数（最新 100 件）
- IPS のスキャン数、検出数、ブロック数（合計）
- IPS で検出した脅威毎のシグネチャ ID、検出数、ブロック数（最新 100 件）
- Web ガードのスキャン数、検出数、ブロック数（合計）
- URL フィルタリングのスキャン数、検出数、ブロック数（合計）
- URL フィルタリングのカテゴリ毎の検出数、ブロック数

3.7.3 UTM 脅威分析通知

Ver10.2 以降では、セキュリティログを NetMeister に送信します（デフォルトは無効）。
送信したセキュリティログは、NetMeister 上で確認・分析できます。

NetMeister へのセキュリティログの送信は、5 分毎もしくは 1MB 毎に行われます。1 時間毎に送信されるセキュリティログの上限は 10MB です（最大 10MB を超えたセキュリティログは送信されません）。

3.7.4 UTM ライセンス自動設定機能

Ver10.9 以降、UTM ライセンスを自動で取得し更新することができます。
UTM ライセンス自動設定機能を使用する場合、別途の NetMeister Partner Portal Service の契約およびオプション契約が必要となります。
有効化は、以下のコマンドで設定が必要になります。

グローバルコンフィグモード	
utm license key netmeister	UTM ライセンス自動設定機能有効化(Ver10.9)

3.7.4.1 ライセンスの自動延長について

UTM ライセンス自動設定機能が有効の場合、自動でライセンスの延長が行われます。
自動延長を停止する場合は、NetMeister サービスで設定を行ってください。

3.7.4.2 注意事項

- NetMeister のグループを入れ替える場合、設定変更後に IX ルータを再起動してください。再起動を行わないまま IX ルータを動作させた場合、一時的に設定変更前のグループの UTM ライセンス情報で動作する可能性があります。
- NetMeister 自動延長機能をご利用される場合、Ver.10.7、Ver.10.8 に実装されている自動延長機能では動作しません。Ver.10.9 以降を使用してください。

■3.8 詳細設定

3.8.1 UTM サーバとの接続

UTM 機能ではインターネット上の UTM サーバに HTTPS でアクセスを行います。ルータ自身がインターネット通信（ (HTTPS/TCP443） できるよう、装置設定（フィルタ、ルーティング等）や環境構築（ファイアウォール等）を行ってください。

Ver10.4 以降、UTM サーバとの通信は IP フィルタでは廃棄されなくなりました。

その他、環境に応じて以下の設定を行ってください。

グローバルコンフィグモード	
utm proxy	UTM サーバとの通信に用いるプロキシサーバの設定 UTM サーバとの通信をプロキシ経由させたい場合に設定してください。
utm outgoing-interface	UTM サーバとの通信の送信インタフェース指定（Ver10.3 以降）
utm source-address	UTM サーバとの通信の送信元アドレス指定（Ver10.2 以降）

※ アカウント・パスワードの必要なプロキシサーバや、ルート証明書による認証を別途必要とするプロキシサーバの利用はできません。

3.8.2 UFS キャッシュ

UTM 機能では、UFS キャッシュを利用した転送処理の高速化が行われています。UFS キャッシュが未設定の場合、性能が極端に遅くなるなどの影響があるため必ず設定してください。

グローバルコンフィグモード	
ip ufs-cache enable ipv6 ufs-cache enable	UFS キャッシュの有効化
ip ufs-cache max-entries ipv6 ufs-cache max-entries	UFS キャッシュ最大エントリ数の設定

UTM 機能では、TCP 通信 1 セッションに対して最大 4 つ程度の UFS キャッシュが生成されます。このため、利用するセッション数を考慮した UFS キャッシュ最大エントリ数の調整を行ってください。

3.8.3 ライセンス登録・ライセンス延長

ライセンスの登録、確認は以下のコマンドで行います。
ライセンス認証は、UTM サーバとの接続性が確保された時点で行われます。
ライセンス認証が成功すると UTM 機能が使用できるようになります。

グローバルコンフィグモード	
utm license key	ライセンスキーの登録
utm license days-before-alert	ライセンス期限切れ通知日数設定
utm license validate-immediately	ライセンス有効期限の即時チェック ※サーバへ問合せをするコマンドであるため、show running-config には反映されません。 ※UTM ライセンス自動設定機能を利用時には NetMeister サーバへの問合せも行います。
show utm license	ライセンス状態の確認

ライセンスの延長、確認は以下のコマンドで行います。
延長コマンドを入力時には UTM サーバとの接続性が取れた状態で実施してください。
※UTM ライセンス自動設定機能を利用している場合はコマンドでの延長はできません。

グローバルコンフィグモード	
utm license update	ライセンス延長キーの登録
show utm license	ライセンス状態の確認

ライセンス状態の確認は以下の様に行います。
ライセンスが認証成功していること(UTM License is Validated)を確認してください。
ライセンスが延長されていること(Expire Date)を確認してください。

```
(config)# show utm license
UTM License is Validated
   Active Key       : XXXX-XXXX-XXXX-XXXX-XXXX
   Product Name     : IX2000
   Model            : IX2000-Y1
   Device ID        : ABCD-EFGH-IJKL-MNOP
   Expire Date      : 2019/08/26 14:51:17
   Last Check       : 2018/08/28 14:33:12
   Status           : In-service

UTM Signature is Active
   Last Update      : 2018/08/28 14:52:23
   Last Check       : 2018/08/28 14:52:23
   Current Version
      IPS           : 2018/08/27 14:10:23 4.6.290
      Web Guard     : 2018/08/27 14:14:30 1.0.1282
```

ライセンスの延長が成功したことは、ライセンス状態の確認表示にて「ライセンス満了日時」が延長されていることで確認します。

表示	内容	補足
UTM License is	ライセンスの状態	Activated （ライセンス有効状態） Validated （ライセンス有効かつ認証成功） Inactive （ライセンス未取得/初期状態） Invalid （ライセンス認証エラー） Expired （ライセンス期限切れ）
Active Key	有効ライセンスキー	ライセンス取得時に使用したライセンスキー netmeister （UTM ライセンス自動設定機能利用時）
Product Name	ライセンスの種類	ライセンスキーの製品名
Model	プロダクト名	ライセンス取得時にサーバから取得したプロダクト名
Device ID	デバイス識別番号	ライセンス取得時にサーバから取得したデバイス識別 ID
Expire Date	ライセンス満了日時	
Last Check	ライセンス認証日時	サーバから認証結果を受信した日時
Status	UTM 動作状態	In-service （動作中） Out-of-service （ライセンス期限切れ、もしくは シグネチャ更新中など UTM 停止中） Startup-failed （UTM 機能起動失敗）
UTM Signature is	シグネチャ更新状態	None （シグネチャ未取得／初期状態） Active （シグネチャ適用中） Downloading （シグネチャダウンロード中）
Last Update	シグネチャダウンロード日時	最新のシグネチャをダウンロードした日時
Last Check	シグネチャバージョン確認日時	最新のシグネチャバージョンをサーバに確認した日時
Current Version	シグネチャバージョン	ダウンロード済みシグネチャのリリース日時およびバージョン ※ コマンドにより無効化されている機能のシグネチャはダウンロードされません。

Ver10.9 以降、UTM ライセンス自動設定機能を有効にした場合、show utm license に以下の表示が追加されます。

```
UTM License Auto Configuration is Inactive
        Expire Date   : ----/--/-- --:--:--
        Last Check    : ----/--/-- --:--:--
```

表示	内容	補足
UTM License Auto Configuration is	UTM ライセンス自動設定機能の状態	Activated （有効状態） Inactive （無効状態/初期状態） Expired （期限切れ）
Expire Date	満了日時	
Last Check	認証日時	

3.8.4 リダイレクトページ設定

URL フィルタリングおよび Web ガードでブロック時に任意のブロックページにリダイレクトして表示させることができます。デフォルトでは、リダイレクトはせずに簡易なブロックページに応答パケットを直接書き換えます。

グローバルコンフィグモード	
utm redirect	リダイレクトページの設定

※ HTTPS で Web サイトをアクセスしていた場合にブロックされた場合、ブラウザで用意されているアクセス不能のページが表示されます。（HTTPS は通信が暗号化されているため応答をブロックページに書き換えることができないため、通信のリセットのみが行われます。）

IX ルータの Web コンソールを有効にすることで、Web コンソール内に用意されている UTM ブロックページにリダイレクトすることも可能です。

【設定例】

```
http-server ip enable
utm redirect http://<ix-router address>/utm/block.html
```

※ IX ルータの Web コンソールを利用する場合、外部からの不正アクセスを防止するため、適切なセキュリティ設定を行ってください。

3.8.5 グループ別ポリシーの設定

IPv4/IPv6 アクセスリストで分割したユーザ PC やグループ毎に、UTM 機能のポリシーを設定できます。

(Ver10.2 以降)

UTM グループの設定で指定したアクセスリストにマッチした通信について、それぞれの UTM 機能で個別のポリシー設定を行います。

※ UTM グループ指定をしない UTM 機能の設定は共通ポリシーの設定と呼びます。

※ UTM グループの設定が行われていて、グループ別の UTM 機能設定が行われていない UTM 機能は、共通ポリシーの UTM 機能設定で動作します。

グローバルコンフィグモード	
utm group <1-10>	UTM グループの設定 UTM グループプロファイルコンフィグモードへ移行
utm anti-virus group <1-10>	グループ別ポリシーのアンチウイルス機能の設定
utm ips group <1-10>	グループ別ポリシーの不正侵入防止機能の設定
utm web-guard group <1-10>	グループ別ポリシーの Web ガード機能の設定
utm url-filter group <1-10>	グループ別ポリシーの URL フィルタリング機能の設定
utm anti-virus	共通ポリシーのアンチウイルス機能の設定
utm ips	共通ポリシーの不正侵入防止機能の設定
utm web-guard	共通ポリシーの Web ガード機能の設定
utm url-filter	共通ポリシーの URL フィルタリング機能の設定
ip access-list ipv6 access-list	アクセスリストの設定
ip access-list NAME option nocache ipv6 access-list NAME option nocache	アクセスリストキャッシュの無効化設定

UTM グループプロファイルコンフィグモード	
match	アクセスリストの設定
description	グループのコメント設定

※ 以下の設定は、共通ポリシーの UTM 機能設定が、すべてのグループにも適用されます。

UTM IPS コンフィグモード	
extended-inspection traffic-anomaly block-period	ポートスキャン検出時のブロックタイマ設定

※ UTM グループは最大 10 個（1～10）まで設定できます。

※ 複数の UTM グループを設定した場合、1 パケット流れただけでも多数のアクセスリストキャッシュが生成されキャッシュ枯渇を引き起こす可能性があります。このため、アクセスリストキャッシュの無効化設定が推奨されます。（UTM グループで生成されたアクセスリストキャッシュは、同時に生成される UFS キャッシュにマッチする限り利用されません。）

【設定例】
192.168.0.11 と 192.168.0.12 の端末の URL フィルタリングの条件をそれ以外の端末と異なる設定にする。

```
ip access-list utm-g1 option nocache       // アクセスリストキャッシュの無効化
ip access-list utm-g1 permit ip src 192.168.0.11/32 dest any
ip access-list utm-g1 permit ip src 192.168.0.12/32 dest any

utm group 1
   description ascii Group1
   match ip access-list utm-g1
```

```
utm url-filter                  // URL フィルタリングの共通ポリシー
  reject category 10000-20000 22000 25000-29000 41000-44000

utm url-filter group 1       // URL フィルタリングの UTM グループ 1 ポリシー
  reject category 41000-44000
```

3.8.6 ホワイトリスト設定

UTM 機能を通さず、無条件で許可、廃棄するトラフィックを設定することができます（ホワイトリスト設定）。

UTM 機能を通さず、無条件でトラフィックを廃棄する場合は、既存のスタティックフィルタ・ダイナミックフィルタによる廃棄設定を入力インタフェースに設定してください（ブラックリスト設定）。

Ver10.2 以降、各セキュリティ・スキャン機能別にホワイトリストを設定することもできます。

アクセスリストを使用して、特定の通信を UTM 機能のチェック対象から除外する設定を行います。

Ver10.2 以降、個別の UTM 機能に対してホワイトリスト設定を行うこともできます。

グローバルコンフィグモード	
utm ignore utm ignore	ホワイトリスト設定（すべての UTM 機能）
utm ignore anti-virus	ホワイトリスト設定（アンチウイルス）
utm ignore ips	ホワイトリスト設定（不正侵入防止）
utm ignore web-guard	ホワイトリスト設定（Web ガード）
utm ignore url-filter	ホワイトリスト設定（URL フィルタリング）
ip access-list ipv6 access-list	アクセスリストの設定
ip access-list NAME option nocache ipv6 access-list NAME option nocache	アクセスリストキャッシュの無効化設定

```
【設定例】
192.168.0.11 と 10.0.0.11 間の通信は UTM の処理を行わない
192.168.0.21 の端末は URL フィルタリングを行わない

ip access-list utm-white-list option nocache
ip access-list utm-while-list permit ip src 192.168.0.11/32 dest 10.0.0.11/32

ip access-list uf-white-list option nocache
ip access-list uf-white-list permit ip src 192.168.0.21/32 dest any

utm ignore ip access-list utm-while-list
utm ignore url-filter ip access-list uf-white-list
```

設定したアクセスリストは src/dest を反転させた逆方向でも評価を行います。

- 上記設定の場合は、送信元 192.168.0.11、送信先 10.0.0.11 と、逆向きの通信となる、送信元 10.0.0.11、送信先 192.168.0.11 のパケットも UTM 処理では除外されます。

※ ホワイトリスト設定で使用するアクセスリストでは、プロトコル、アドレス、ポート番号以外の指定はサポート外です。

※ UTM 処理の前に、受信インタフェースのトラフィックフィルタが動作します。また、受信フィルタは UTM 処理より前に動作するため、フィルタ機能を設定することにより、ブラックリスト設定として UTM 処理を除外したパケット廃棄ができます。フィルタ設定の詳細については、フィルタの項を参照してください。

※ 個別の UTM 機能でホワイトリストの設定した場合、1 パケット流れただけでも多数のアクセスリストキャッシュが生成されキャッシュ枯渇を引き起こす可能性があります。このため、アクセスリストキャッシュの無効化設定が推奨されます。（ホワイトリストで生成されたアクセスリストキャッシュは、同時に生成される UFS キャッシュにマッチする限り利用されません。）

3.8.7 通知の設定

3.8.7.1 セキュリティログの設定

IX ルータでは UTM のセキュリティログはイベントログとして出力されます。電源断やイベントログバッファの上限により、装置内のセキュリティログは消えるため syslog サーバに送信するなどの対応が推奨されます。

グローバルコンフィグモード	
utm security-log	機能毎のログ設定
logging subsystem utm	UTM 機能のイベントログ設定
logging buffered	イベントログの装置への保存
syslog	syslog サーバ設定 ※ utm-security-log オプションを指定することで、UTM セキュリティログを異なる syslog ホストに送信することもできます。(Ver10.2 以降)

【設定例】
UTM notice レベルのログを出力
UTM セキュリティログはアンチウイルスのログのみ出力

```
logging buffered 1000000
logging subsystem utm notice

utm security-log anti-virus
```

3.8.7.2 LED 通知の設定

脅威検出時の、LED 通知の設定を行います。
初期状態では全ての条件で通知を行います。

グローバルコンフィグモード	
utm led enable	LED 通知の有効化
utm led alert-time	LED 通知時間設定（脅威検出時）

【設定例】
脅威検出時のみ、LED の点灯により通知。
点灯後は 5 時間点灯

```
utm led enable alert
utm led alert-time 5
```

3.8.8 NetMeister 連携

NetMeister を有効にすることで、UTM の脅威通知が NetMeister にも通知されます。
設定の詳細は「NetMeister の設定」を参照してください。

3.8.8.1 UTM 脅威レポート通知の設定

NetMeister でグラフィカルな脅威レポート表示ができるようになります。
また、CLI や Web コンソールで検出した脅威や URL フィルタリングのカテゴリ毎の内容および utm security-report 統計情報が表示できます。（Ver10.1 以降）

グローバルコンフィグモード	
utm security-report disable	UTM 脅威レポート通知設定 （デフォルトでは有効）
show utm security-report	UTM 脅威レポート情報表示

3.8.8.2 UTM 脅威分析通知の設定

NetMeister で UTM 脅威分析表示ができるようになります。（Ver10.2 以降）

グローバルコンフィグモード	
utm security-log-analytics enable	UTM 脅威分析通知設定 （デフォルトでは無効）

■3.9 情報の確認

3.9.1 CLI 表示

以下のコマンドで UTM 関連の状態を確認できます。

グローバルコンフィグモード	
show utm status	UTM 状態・統計情報の確認
show utm statistics	UTM 統計情報の確認
show utm security-report	UTM 脅威レポート情報表示
show logging	ログ情報の確認
clear utm statistics	UTM 統計情報のクリア
clear utm led	UTM 機能で点灯した LED をクリアします

状態表示では、UTM の情報が表示されます。

【表示例】

```
(config)# show utm status
UTM Status: on
   Security-log: anti-virus, ips, url-filter, web-guard
   Redirect page: none
   LED: alert, license, startup-failed
   LED alert-time: 1
   IPS Status: on
      Signature version: 4.6.290
      Action: block
      Extended-inspection protocol-anomaly: ignore
      Extended-inspection traffic-anomaly: ignore
      Traffic-anomaly block-period: 600
      Ignore Security ID list:
         none
   Anti-Virus Status: on
      Server status: active
      Action: block
      Scan protocol: ftp, http, imap, pop3, smtp
      File size threshold (MB): 2
      Compress file scan: off
      Ignore Virus ID list:
         none
   URL-Filter Status: on
      Server status: active
      Reject category ID list:
         10000, 11000, 12000, 13000, 14000, 15000, 16000, 17000
         18000, 19000, 22000, 41000, 42000, 43000, 44000
      No category: pass
      No response: pass
      Ignore URL list:
         none
   Web-Guard Status: on
      Signature version: 1.00.1282
      Action: block
      Ignore URL list:
         none
```

```
UTM Statistics:
  Anti-Virus:
    Connections blocked/infected/scanned = 0/0/12233
  IPS:
    Flows blocked/identified/scanned = 4/4/29983
  Web-Guard:
    URLs blocked/scanned = 0/29726
  URL-Filter:
    URLs blocked/identified/scanned = 0/29726/29726
  Anti-Virus latest detected:
    none
  IPS latest detected:
    Sequence Number: 3
      date 2018/08/28 15:15:38
      act Drop
      mac 00:60:B9:00:00:02
      src 203.0.113.2:80
      dst 192.0.2.2:39846
      protocol 6
      msg JSIG-RAT GH0ST-Activity-9
      sid 8050779
      severity 0
  Web-Guard latest detected:
    none
  URL-Filter latest detected:
    Sequence Number: 29725
      date 2018/08/28 15:31:35
      act Block
      mac 00:60:B9:00:00:01
      src 192.0.2.1:52382
      dst 203.0.113.1:8080
      protocol 6
      url ix-router.example.com/success.txt
      cid 50000
      uid 15
UTM Cache:
  URL-Filter category cache 6 entries, 16644/1048576 bytes
UTM Queue Status:
  System buffer:
    0/0 (curr/peak), 0/0 (queued/overflow)
  GigaEthernet0 buffer:
    0/0 (curr/peak), 0/0 (queued/overflow)
  GigaEthernet1 buffer:
    0/0 (curr/peak), 0/0 (queued/overflow)
```

表示	内容	補足
UTM Status	UTM の状態	on （動作中） off （停止中）
Security-log	セキュリティログ有効機能	disable anti-virus ips url-filter web-guard
Redirect page	リダイレクトページ設定	
LED	LED 表示機能設定	
LED alert-time	UTM 脅威検出時 LED 点灯時間	Hours
IPS Status	IPS 機能の状態	on （動作中） off （停止中）
Signature version	IPS 機能シグネチャバージョン	

Action	IPS 機能検出時動作(basic-inspection)	block log
Extended-inspection protocol-anomaly	IPS 機能プロトコル不正検出機能	ignore log
Extended-inspection traffic-anomaly	IPS 機能トラフィック不正検出機能	ignore block
Traffic-anomaly block-period	IPS 機能トラフィック不正検出時ブロック時間	秒
Ignore Security ID list	IPS 機能の除外 SID リスト	
Anti-Virus Status	アンチウイルス機能の状態	on （動作中） off （停止中）
Server status	AV クラウドサーバ接続状態	active （接続可） inactive （接続不可）
Action	アンチウイルス機能検出時動作	block log
Scan protocol	スキャン対象プロトコル	none http ftp pop3 smtp imap
File size threshold (MB)	ファイルスキャンサイズ	MB
Compress file scan	圧縮ファイルスキャン	on off
Ignore Virus ID list	アンチウイルス機能の除外 VID リスト	
URL-Filter Status	URL フィルタリング機能の状態	on （動作中） off （停止中）
Server status	UF クラウドサーバ接続状態	active （接続可） inactive （接続不可）
Reject category ID list	URL フィルタリング機能廃棄カテゴリリスト	カテゴリ番号
No category	カテゴリなし応答動作	reject pass
No response	サーバ応答なし動作	reject pass
Ignore URL list	URL フィルタリング機能除外 URL リスト	URL
Web-Guard Status	Web ガード機能の状態	on （動作中） off （停止中）
Signature version	Web ガード機能シグネチャバージョン	
Action	Web ガード機能検出時動作	block log
Ignore URL list	Web ガード機能除外 URL リスト	URL
UTM Statistics		下記統計情報表示例を参照してください
UTM Cache		
URL-Filter category cache	URL フィルタリング機能カテゴリキャッシュ	エントリ数（entries） キャッシュサイズ（bytes）
UTM Queue Status	UTM 処理待ち滞留パケット数および統計	
{デバイス名}	受信デバイスのパケットバッファ滞留数および統計	現在の滞留数(curr) 過去最大滞留数(peak) 過去滞留数の累計(queued) 廃棄数の累計(overflow)
System buffer	フラグメントのパケットバッファ滞留数および統計	一連のフラグメントパケットを 1 つとしてカウント 内容は上記のデバイス毎の補足を参照してください

統計情報では、各機能でスキャンした回数、脅威を検出した回数等を確認できます。
また、各機能の最新の脅威検出結果を確認できます。

【表示例】

```
(config)# show utm statistics
UTM Statistics:
  Anti-Virus:
    Connections blocked/infected/scanned = 0/0/12233
  IPS:
    Flows blocked/identified/scanned = 4/4/29983
  Web-Guard:
    URLs blocked/scanned = 0/29726
  URL-Filter:
    URLs blocked/identified/scanned = 0/29726/29726
  Anti-Virus latest detected:
    none
  IPS latest detected:
    Sequence Number: 3
      date 2018/08/28 15:15:38
      act Drop
      mac 00:60:B9:00:00:02
      src 203.0.113.2:80
      dst 192.0.2.2:39846
      protocol 6
      msg JSIG-RAT GH0ST-Activity-9
      sid 8050779
      severity 0
  Web-Guard latest detected:
    none
  URL-Filter latest detected:
    Sequence Number: 29725
      date 2018/08/28 15:31:35
      act Block
      mac 00:60:B9:00:00:01
      src 192.0.2.1:52382
      dst 203.0.113.1:8080
      protocol 6
      url ix-router.example.com/success.txt
      cid 50000
      uid 15
```

表示	内容	補足
UTM Statistics		
Anti-Virus	アンチウイルス機能の統計情報	
Connections blocked/infected/scanned	コネクション毎のスキャンカウンタ	ブロック数 感染検出数 スキャン数
IPS	IPS 機能の統計情報	
Flows blocked/identified/scanned	トラフィックフロー毎のスキャンカウンタ	ブロック数 識別数 スキャン数
Web-Guard	Web ガード機能の統計情報	
URLs blocked/scanned	URL 毎のスキャンカウンタ	ブロック数 スキャン数
Anti-Virus latest detected	アンチウイルス機能の最新セキュリティログ	

IPS latest detected	IPS 機能の最新セキュリティログ	
Web-Guard latest detected	Web ガード機能の最新セキュリティログ	
URL-Filter latest detected	URL フィルタリング機能の最新セキュリティログ	

脅威レポートとして、これまでの累計、もしくは 3 日間で検出した脅威をまとめて表示することができます。

【表示例】

```
(config)# show utm security-report
        UTM Security-Report(total):
   Summary:
      Anti-Virus:
         blocked/infected/scanned = 9/9/93
         latest detected date 2019/02/12 15:57:36
      IPS:
         blocked/identified/scanned = 1/1/150
         latest detected date 2019/02/12 15:52:36
      Web-Guard:
         blocked/scanned = 9/135
         latest detected date 2019/02/12 15:57:35
      URL-Filter:
         blocked/identified/scanned = 0/135/135
         latest detected date 2019/02/12 15:58:01
   Details:
      Anti-Virus:
         vid:903380613 (Test.File.EICAR.y)
            blocked/infected/scanned = 9/9/93
            latest detected date 2019/02/12 15:57:36
      IPS:
         sid:80600001 (TCP RST Scan)
            blocked/identified/scanned = 1/1/150
            latest detected date 2019/02/12 15:52:36
      URL-Filter:
         cid:23000 (Social Network)
            blocked/identified/scanned = 0/2/135
            latest detected date 2019/02/12 15:57:58
         cid:31000 (Multimedia Download)
            blocked/identified/scanned = 0/2/135
            latest detected date 2019/02/12 15:57:56
         cid:36000 (Content Delivery Network)
            blocked/identified/scanned = 0/2/135
            latest detected date 2019/02/12 15:57:58
```

3.9.2 セキュリティログ

UTM セキュリティログは UTM.001～UTM.016 のイベントログで表示され、イベントログヘッダと JSON 形式のログ情報を組み合わせたフォーマットで表記されます。

装置イベントログ例:

UTM.003: WG-h seq 2, {"type":"WG","src":"192.0.2.40:54505",...,"act":"Block","time":"1516337068"}

イベントログヘッダ　　JSON 形式のログ情報

syslog 送信時例:

<132> UTM[003]: WG-h seq 2, {"type":"WG","src":"192.0.2.40:54505",...,"act":"Block","time":"1516337068"}

【表示例】（見やすくするため、適宜改行を入れています。）

```
(config)# show logging
2018/02/06 18:19:51 UTM.001:AV-h seq 10,

{"type":"AV","src":"203.0.113.10:80","dst":"192.0.2.10:43515","mac":"00:60:B9:01:49:10","proto":"6","L7_proto":"
HTTP",
 "virus":"IX-Test-File","vid":"2053","file":"ix-router.example1.com.txt","severity":"0","act":"
Destroy","time":"1442476129"}
 2018/02/06 18:19:51 UTM.002: IPS-l seq 11,
  {"type":"IPS","src":"203.0.113.20:443","dst":" 192.0.2.20:54176","mac":"00:60:B9:01:49:20","proto":"6",
 "msg":"TCP RST Scan","sid":"80600001","severity":"0","act":"Drop","time":"1516336933"}
 2018/02/06 18:19:51 UTM.004: UF-l seq 12,
  {"type":"UF","src":"192.0.2.30:54521","dst":"203.0.113.30:443","mac":"00:60:B9:01:49:30","proto":"6",
 "url":" ix-router.example2.jp","cid":"46000","gid":"15","act":"Block","time":"1516337351"}
 2018/02/06 18:19:51 UTM.003: WG-h seq 13,
  {"type":"WG","src":"192.0.2.40:54505","dst":"203.0.113.40:80","mac":"00:60:B9:01:49:40","proto":"6",
 "url":"www. ix-router.example3.org/download/example3.zip","act":"Block","time":"1516337068"}
```

セキュリティログ内容

表示	内容	補足
type	UTM 機能 AV : アンチウイルス IPS : IPS UF : URL フィルタリング WG : Web ガード	全機能
src	送信元アドレス:ポート	全機能
dst	送信先アドレス:ポート	全機能
mac	MAC アドレス	全機能
proto	プロトコル番号	全機能
msg	セキュリティログ付加情報	
act	Destroy : アンチウイルスによるデータ無害化 Pass : 透過もしくは IPS で検出 Block : ブロック Drop : 廃棄	全機能
time	イベント発生時刻のタイムスタンプ (UNIX タイムスタンプ)	全機能
L7_proto	レイヤ 7 プロトコル情報	AV
virus	ウイルス情報	AV
vid	アンチウイルス ウイルス ID	AV
charset	SMTP もしくは POP3 の charset	AV
subject	SMTP もしくは POP3 の subject	AV
date	SMTP もしくは POP3 の date	AV
sid	IPS シグネチャ ID	IPS
url	URL フィルタリング、Web ガードで検出時の URL	UF、WG
cid	URL フィルタリングのカテゴリ ID	UF
gid	URL フィルタリングのカテゴリグループ ID	UF
xff	HTTP X-Forward-For ヘッダ	全機能
severity	緊急度 （0: 未定義、1: 低、2: 中、3: 高） ※Ver10.1 以前は 0 固定	全機能

※ Ver10.1 以降、セキュリティログ UTM.006 は以下のように分割表示となります。
UTM.006（URL フィルタリングのブロック指定カテゴリでの判定時に notice レベルで表示）
UTM.007（URL フィルタリングの UTM.006 以外の判定結果を info レベルで表示）

※ Ver10.1 以降、セキュリティログ UTM.011、UTM.012、UTM.013、UTM.014、UTM.015、UTM.016 は、それぞれ、UTM.001、UTM.002、UTM.003、UTM.004、UTM.005、UTM.006 もしくは UTM.007 に統合して表示されます。

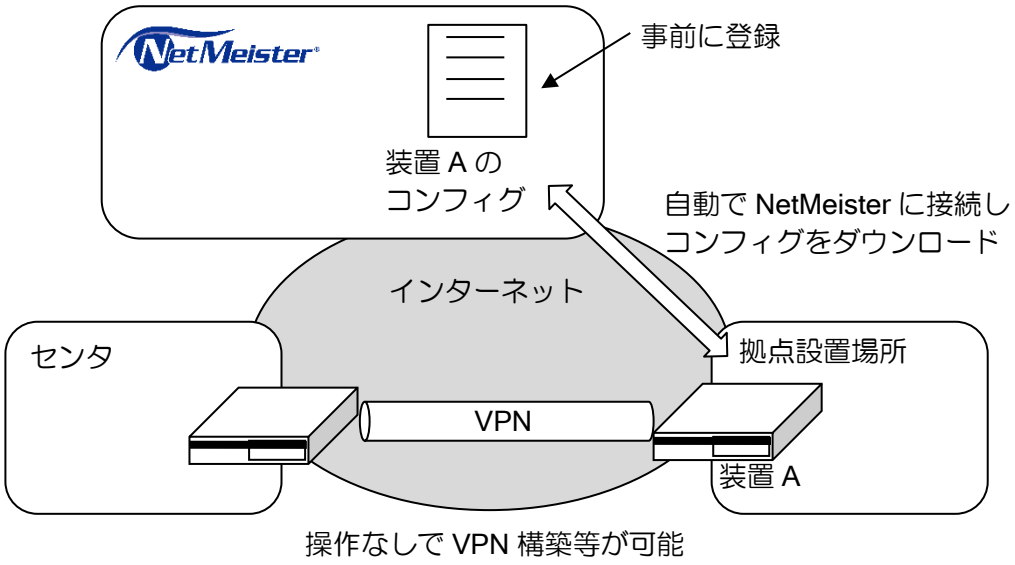
4章 ゼロタッチプロビジョニング

■4.1 はじめに

4.1.1 ゼロタッチプロビジョニング（ZTP）概要

ゼロタッチプロビジョニング（以下「ZTP」）機能は、NetMeister との連携により装置コンフィグのプロビジョニング（ネットワーク接続環境の構築）を設置場所でのコンフィグ操作なしで実現する機能です（Ver.10.4 以降）。事前に NetMeister にコンフィグ等を登録することで、設置場所では ZTP 機能を有効にして起動することで、自動で NetMeister に接続を行い、登録されたコンフィグをダウンロード・適用して動作させることができます。

NetMeister での設定等は NetMeister Ver.6.0 対応 以降のマニュアルをご確認ください。



4.1.2 用語の定義

ゼロタッチプロビジョニング、ZTP、ゼロタッチ

本機能の名称で使用。IX ルータではすべて同じ意味で記載しています。

ZTP 接続 ID

NetMeister で登録したコンフィグと装置を結びつけるために、既存の情報を組み合わせた ID です。

MODE スイッチ

装置前面に MODE と書かれたスイッチです。ZTP を有効/無効にする場合に使用します。

MODE スイッチ LED

MODE スイッチありの装置は、ZTP 処理状況により MODE スイッチ部分が LED によって点灯・点滅します。

ダウンロードコンフィグ

ZTP により NetMeister から装置に適用するためのコンフィグ。NetMeister の Web 画面で設定します。

4.1.3 適用範囲

適用ソフトウェアバージョン

ソフトウェアは Ver.10.4 以降で使用できます。

適用装置

- MODE スイッチあり装置
  IX2107、IX2235、IX2310
- MODE スイッチなし装置
  IX2106、IX2207、IX2215、IX3315

それ以外の装置は ZTP 未対応です。

適用環境

- フレッツ光ネクスト等の IPv6 NGN 閉域網
- IPv4 (DHCP)

※　NGN 閉域網以外の IPv6 はサポートしません。
※　ZTP 機能による起動時の NetMeister 接続は GE0（GigaEthernet0）を利用します。

4.1.4 制限事項

※　ゼロコンフィグ（SMF）機能とは同時に使用できません。
※　イントラネット内などからの接続で、プロキシ越しにネットワークに接続する場合、ZTP 開始時の startup-config にプロキシ設定をしておく必要があります。
※　起動時コンフィグダウンロード機能とは同時に使用できません。

■4.2 設定の流れ

4.2.1 NetMeister への装置登録

ZTP を利用するには NetMeister に以下の情報を登録する必要があります。

① 装置に設定するコンフィグ
② 装置の MAC アドレス、シリアル番号（装置のゼロタッチプロビジョニング装置登録用 QR コード読み取りで簡単登録可能）
③ ①と②の情報の紐づけ

NetMeister に登録後、設定した有効期間以内に ZTP により装置にコンフィグをダウンロードする必要があります。有効期間を過ぎた場合は再度 NetMeister に登録してください。

4.2.1.1 ZTP 接続 ID の確認

ZTP 接続 ID は ZTP で利用する装置識別 ID です。ZTP 機能による NetMeister サーバ接続時に認証用データとして ZTP 接続 ID を送信します。ZTP 接続 ID は IX ルータに固有に割り振られており、次の方法で確認することができます。

show hardware コマンド

ZTP 機能の有効無効に関わらず常に表示されます。

nm provisioning enable コマンド入力時

入力後に CLI に表示されます。

4.2.1.2 IX ルータの MAC アドレスとシリアル番号の登録

現品の MAC アドレスとシリアル番号を確認し、紐づけ情報に MAC アドレスとシリアル番号を NetMeister に登録します。装置にゼロタッチプロビジョニング装置登録用 QR コードが貼っていれば、スマートフォンで読み取ることでそのまま NetMeister へアクセスして登録することができます。

4.2.2 ZTP の有効化設定

ZTP を有効にします。装置によって有効化の方法が異なります。

MODE スイッチがある装置の場合

MODE スイッチのある装置の場合、MODE スイッチを ON にすることで ZTP が有効になります。装置に CLI や WebGUI でのコンフィグ設定は必要ありません。

その状態で装置を起動すると ZTP が起動します。

※ MODE スイッチが OFF でも、装置のコンフィグに nm provisioning enable コマンドが設定されている場合は ZTP が有効になります。

MODE スイッチがない装置の場合

MODE スイッチのない装置の場合、CLI から下記のコマンドを設定、または WebGUI からの設定で装置の ZTP を有効にする必要があります。

CLI の設定では下記コマンドを設定した後、保存・再起動することにより ZTP が起動します。

nm provisioning enable	ZTP を有効 （グローバルコンフィグモード）

※ZTP の無効化
CLI から下記のコマンドの設定により、ZTP が動作しません。
MODE スイッチが ON の場合でも、ZTP は動作しません。

nm provisioning disable	ZTP を無効（Ver.10.9 以降） （グローバルコンフィグモード）

4.2.3 子機 ZTP の有効化設定

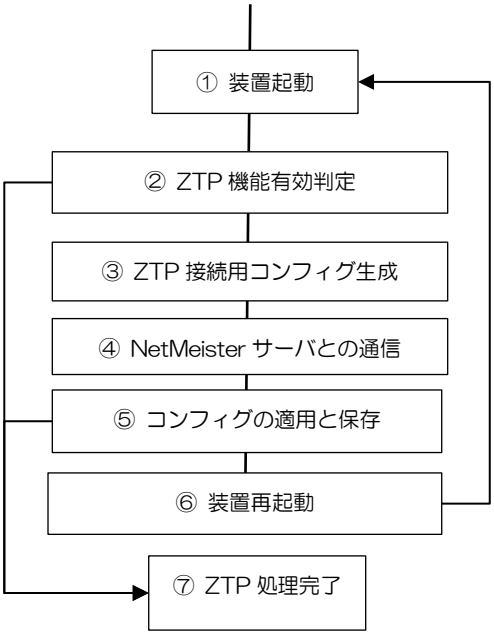
子機の ZTP を行う場合、親機である IX ルータから DHCP サーバの機能にて ZTP 有効を通知する必要があります。子機の ZTP を行う際は以下の設定例を参考に DHCP サーバの設定をしてください。

【設定例】

```
nm ip enable
nm account <グループ ID> password plain <グループ PW>
ip dhcp enable
ip dhcp profile dhcp-prof
   provisioning ip enable
```

4.2.4 ZTP 起動後の動作

ZTP を有効にし装置を起動すると、NetMeister サーバへ接続するためのコンフィグが一時的に設定され、NetMeister サーバに接続します。認証に成功すると NetMeister サーバから登録済のコンフィグをダウンロードし反映します。



① 装置を起動します。
② ZTP 機能が有効であるか判定します。無効であれば通常通りに起動します。
③ NetMeister サーバと通信するためのコンフィグを自動で設定します。
④ NetMeister サーバへの認証およびコンフィグのダウンロードを行います。
⑤ ダウンロードしたコンフィグを装置の startup-config に差し替え・保存します。コンフィグに

差分がなければ再起動を行いません。

⑥ 装置を再起動します。

※ NetMeister サーバへの接続に使用するポートは GE0 です。
※ 装置のコンフィグで既に、GE0 または GE0 配下のいずれかのサブインタフェースに no shutdown が設定されている場合、既に設定されているコンフィグ情報で NetMeister に接続します。
※ NetMeister サーバへの接続設定は startup-config/default-config のものを使用します。startup-config/default-config に NetMeister の接続設定がない場合は、「IPv6 NGN 閉域網接続、IPv4 接続」の順に繰り返し NetMeister に接続試行します。
※ ZTP 処理中に startup-config が変更された場合、ZTP 処理がキャンセルされます。
※ ユーザがコンフィグにログインした場合 ZTP 処理は一時停止し、コンフィグからログアウトすると再開します。

4.2.5 ZTP の動作パターン

4.2.5.1 最初の起動時のみコンフィグをダウンロード

最初の起動時のみに ZTP 機能が動作し、それ以降の起動には ZTP 機能を使用しない動作パターンです。この方法を行うには以下の状態である必要があります。

- NetMeister で「初回コンフィグダウンロード後、無効にする」を設定。
- MODE スイッチを ON またはコンフィグに nm provisioning enable を設定する。

起動後は、MODE スイッチを OFF、または、ダウンロードコンフィグに nm provisioning disable を設定してください（Ver.10.9 以降）。

4.2.5.2起動時毎回ダウンロード

起動時に毎回 ZTP 機能が動作するパターンです。以下の設定を行う必要があります。

- NetMeister で「初回コンフィグダウンロードに成功した装置は、初回 DL 期限後もダウンロード可能とする」を設定。
- MODE スイッチを ON またはダウンロードコンフィグに nm provisioning enable を設定する。

4.2.5.3 ダウンロードしたコンフィグを装置に保存しない

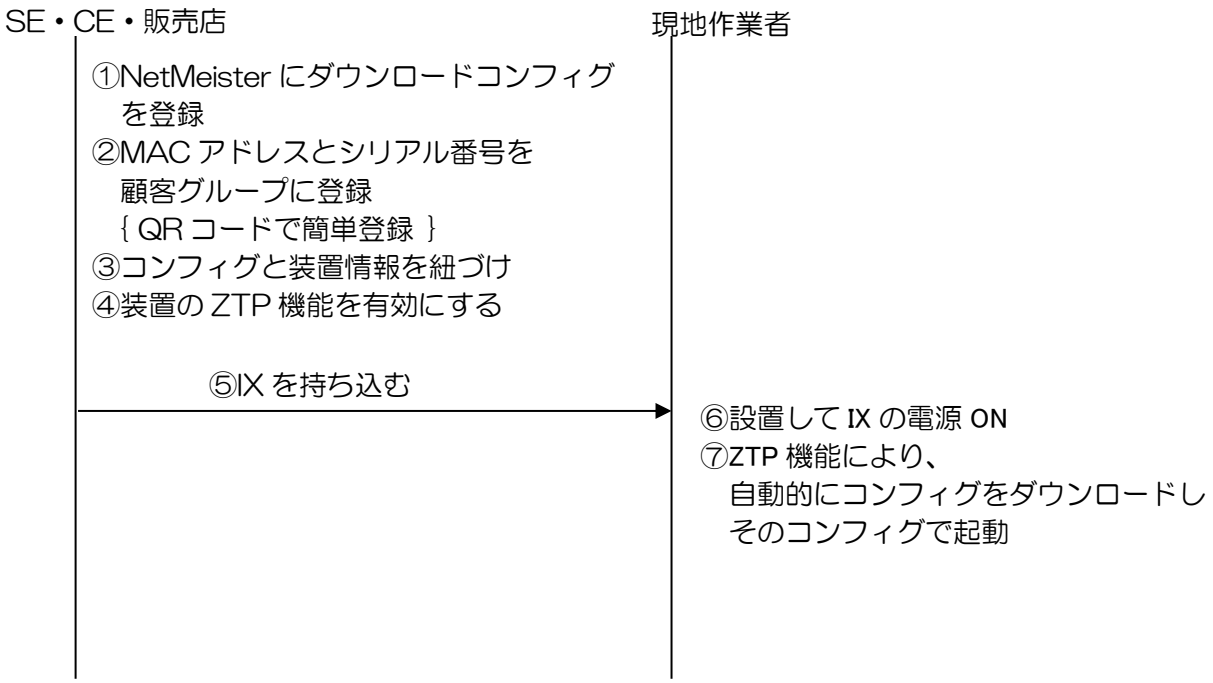
通常は NetMeister からダウンロードしたコンフィグを装置に保存しますが、コンフィグを保存せずに運用することもできます。その場合の運用は、装置を起動するたびに毎回 NetMeister からコンフィグをダウンロードし適用します。この方法を行うには以下の設定が必要です。

- ダウンロードコンフィグに nm provisioning enable no-saveconfig を設定します。

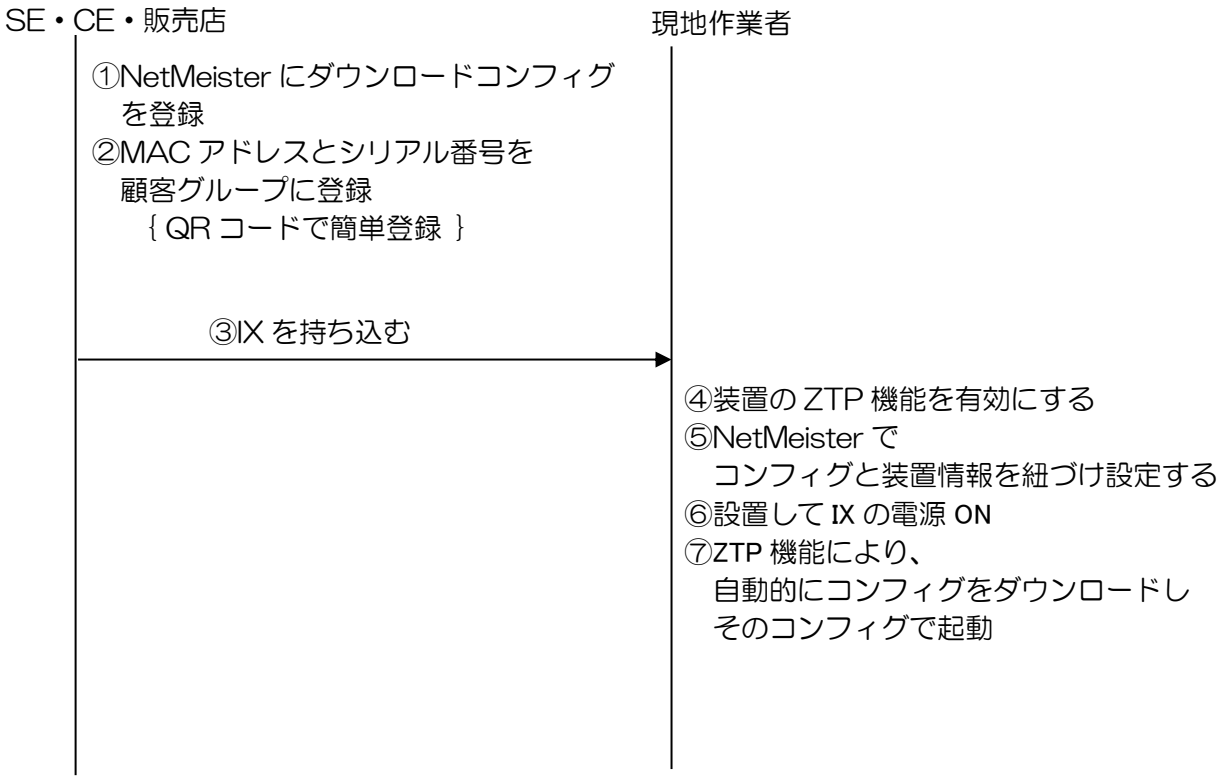
※ 装置のコンフィグに nm provisioning enable no-saveconfig を設定しても、保存する動作になるので注意してください。
※ 以下のコマンドは startup-config に保存されます。
  - terminal speed コマンド
  - nm provisioning enable no-saveconfig コマンド
  - 要再起動コマンド(暗号化されて保存されます。)

4.2.6 ZTP の運用フロー

4.2.6.1 コンフィグ設定や装置情報を事前に紐づけ済の運用準備フロー



4.2.6.2 コンフィグを事前登録し、装置情報の紐づけを現地で行う運用準備フロー



4.2.6.3 直接現地で ZTP を使用する場合の運用準備フロー

現地作業者

①NetMeister にダウンロードコンフィグを登録
②装置の ZTP 機能を有効にする
③NetMeister で MAC アドレスとシリアル番号により検索し、
顧客グループへ紐づけ
④コンフィグと装置情報を紐づけ
⑤設置して IX の電源 ON
⑥ZTP 機能により、
自動的にコンフィグをダウンロードし
そのコンフィグで起動

■4.3LED

4.3.1 MODE スイッチ LED

MODE スイッチがある装置は、MODE スイッチの LED により状態を通知します。
ZTP 機能が有効の場合、MODE スイッチの LED の状態は以下の通りです。

	装置運用可能	装置運用不可能
装置起動～ ZTP 初期化	緑点滅 （1 秒周期）	緑点滅 （1 秒周期）
ZTP 処理中	緑点滅 （2 秒周期※1）	緑点滅 （2 秒周期※1）
ZTP 処理時間超過	橙点滅 （2 秒周期）	赤点滅 （2 秒周期）
ZTP 正常終了	緑点灯	緑点灯
ZTP 異常終了	橙点灯	赤点灯
ZTP 処理キャンセル	消灯	消灯
再起動時	※2	※2

※1 処理開始時は点滅周期が短いことがあります。
※2 下記の再起動時を参照してください。

- 装置運用可能/不可能
  起動時に使用したコンフィグファイル(startup-config または default-config)で
  GE0 の全てのインタフェースが shutdown なら運用不可能、
  GE0 のいずれかのインタフェースが no shutdown なら運用可能。

- 装置起動中～ZTP 初期化
  装置起動からソフトウェア起動まで。
  MODE スイッチ OFF の場合、緑点滅を開始するのは BOOT 起動時から
  となる。ZTP 初期化処理実行時に無条件で一旦消灯状態となる。

- ZTP 処理中
  ZTP 処理中の状態。通信エラーやコンフィグモードログインによる処理中断中も含む。

- ZTP 処理時間超過
  ZTP 処理開始から 10 分経過した状態。
  正常終了/キャンセル/異常終了となるまで継続する。

- ZTP 正常終了
  ZTP 処理が最後まで正常に終了した状態。

- ZTP 異常終了
  内部エラー(メモリ取得エラー等)で ZTP 処理の継続が不可能になった状態。

- ZTP 処理キャンセル
  ZTP 処理中のコンフィグ変更や startup-config 書き換えで、
  ユーザ操作により ZTP 処理が終了した状態。

- 再起動時
  再起動時の LED 制御は、以下のように動作します。
  - MODE スイッチが ON、または nm provisioning enable が設定されている場合、
    緑点滅（1 秒周期）。
  - MODE スイッチが OFF、かつ nm provisioning enable が未設定の場合、
    消灯

4.3.2 VPN、PPP、BAK、の LED

ZTP 処理中は VPN、PPP、BAK の LED によって ZTP の状態を表します。
WAN 接続モード、接続フェーズ、接続エラーを通知します。

	NetMeister 認証中&リトライ中			NetMeister ダウンロード中&リトライ中		
回線設定(nm ip/ipv6 enable)	VPN	PPP	BAK	VPN	PPP	BAK
IPv6 (NGN 閉域網経由)	点滅	点灯	点灯	点灯	点灯	点灯
IPv4 (DHCP)	点滅	点滅	点滅	点灯	点滅	点滅

処理内容	LED 動作
コンフィグを保存中	BSY が点灯
ZTP 処理開始から 10 分以上経過 かつ装置運用不可能	ALM が点滅（2 秒周期）
ZTP 異常終了、 かつ装置運用不可能	ALM が点灯

■4.4 統計情報・メッセージ

4.4.1 エラーログ

ZTP 処理による startup-config 更新時、および再起動時、正常終了時、キャンセル時、異常終了時に、それぞれエラーログへの記録を行います。

■startup-config 更新時(Erase/ Modify)
INFO: Erase startup-config cmd:erase state:succeeded from:@ZTP
INFO: Modify startup-config cmd:write state:succeeded from:@ZTP

■再起動時
INFO: ZTP requested reboot

■正常終了時
INFO: ZTP process has succeeded

■異常終了時
INFO: ZTP process has abnormal terminated by CAUSE

CAUSE:
“download configuration save failed”(ダウンロードコンフィグの保存失敗)
“download configuration apply failed”(ダウンロードコンフィグの適用失敗)
“internal data save failed”(ZTP 関連情報の書き込み失敗)
“internal memory get failed”(内部メモリ取得失敗)
“config process occupy failed”(コンフィグ権限占有失敗)
“command execution failed”(コマンド実行失敗)
“internal error”(上記以外の内部エラー)

■キャンセル時
INFO: ZTP process has been canceled

なお、同じ種別のエラーログは最新のログで上書きされます。
(特に startup-config 更新は ZTP 以外の機能で更新された場合も上書きされるので注意してください)

4.4.2 ZTP 処理中の無条件表示ログ

以下のログを無条件でコンソール表示する。

- ZTP 機能開始メッセージ
  IX/ZTP: Start ZTP process. (ID: 000022076500#IX#IX2207#45SNU80001)

- IP アドレス設定メッセージ
  IX/ZTP: Address-Family address has been assigned by Type, Interface

  ※Address-Family：IPv4 / IPv6
  Type：User config / DHCP / PD / RA
  Interface：GigaEthernet0.x

両方接続時はそれぞれのログが出力される。
IP アドレスを取得するタイミングによっては ZTP 処理の途中で表示される場合もあり。

- NetMeister 接続開始メッセージ
  IX/ZTP: Start connecting to NetMeister server with Connection-Type.

  ※Connection-Type： IPv4 / IPv6(Closed NGN)

- 認証完了メッセージ
  IX/ZTP: Authentication succeeded with Connection-Type.

  ※Connection-Type： IPv4 / IPv6(Closed NGN)

- コンフィグダウンロード開始メッセージ
  IX/ZTP: Start configuration download from NetMeister server.

- コンフィグダウンロード完了メッセージ
  IX/ZTP: Configuration download completed.

- ダウンロードコンフィグの保存成功メッセージ
  IX/ZTP: Configuration has been saved.

- コンフィグ保存ありモード時の装置再起動メッセージ
  IX/ZTP: Reboot router.

- コンフィグ保存なしモード時の装置再起動メッセージ
  IX/ZTP: Configuration requires reboot.

- ダウンロードコンフィグの適用成功メッセージ
  IX/ZTP: Configuration has been applied.

- ZTP 機能正常終了メッセージ
  IX/ZTP: ZTP process has succeeded.

- 認証エラーメッセージ
  IX/ZTP: Authentication failed (Cause).

  ※Cause：
  code XXX(NetMeister サーバからのエラーステータス)
  timeout(無応答タイムアウト)
  invalid data received(不正なデータ受信)
  cert verify error(証明書インストール失敗又は、証明書検証 NG)

- コンフィグダウンロードエラーメッセージ
  IX/ZTP: Configuration download failed (Cause).

  ※Cause：
  code XXX(NetMeister サーバからのエラーステータス)
  timeout(無応答タイムアウト)
  invalid data received(不正なデータ受信)
  cert verify error(証明書検証 NG)

- 処理一時停止メッセージ
  IX/ZTP: ZTP process has been suspended.

- 処理再開メッセージ
  IX/ZTP: ZTP process has been resumed.

- ZTP 機能異常終了メッセージ
  IX/ZTP: ZTP process has abnormal terminated by Cause.

  ※Cause：
  download configuration save failed(ダウンロードコンフィグの保存失敗)
  download configuration apply failed(ダウンロードコンフィグの適用失敗)
  internal data save failed(ZTP 関連情報の書き込み失敗)
  internal memory get failed(内部メモリ取得失敗)
  config process occupy failed(コンフィグ権限占有失敗)
  command execution failed(コマンド実行失敗)
  internal error(上記以外の内部エラー)

- ZTP 機能キャンセルメッセージ
  IX/ZTP: ZTP process has been canceled.

- ZTP 処理時間超過メッセージ
  IX/ZTP: ZTP process delays.

- NetMeister に「初回コンフィグダウンロード後、無効にする」を設定してダウンロード後に ZTP 有効で再起動した場合のメッセージ
  IX/ZTP: ZTP process has finished since configuration is already applied and saved.

5章 保守・運用

本章では、IX2000/IX3000 シリーズの設定の変更、保存について説明します。

■5.1 設定の変更

設定コマンドは通常はコマンド入力時に反映されますが、一部コマンドは再起動等が必要となる場合があります。本項では、即時反映されないコマンドについて説明します。

5.1.1 再起動が必要なコマンド

設定を反映させるために再起動が必要なコマンドは、コマンド実行後次のようなメッセージが表示されます。

```
% You must restart the router for this configuration to take effect.
```

該当するコマンドは次のとおりです。

項目	備考
service-policy enable	FastEthernet,GigaEthernet のみ不要
isdn switch-type	
encapsulation	dot1q の VLAN-ID 変更時は不要
ip cache-size	
ipv6 cache-size	
ip max-route	
rib max-entries	
scheduler poller rotor-preference	
t1 pri-group	
snmp-agent mib-2 conceal-unconfigured-ifstack	
snmp-agent mib-2 ifindex	
default-console	
no interface	
receive-buffers	
tunnel mode	Ver.8.10 以降。L2TPv2 使用時のみ。
system interfaces	Ver.8.11 以降
system qos	Ver.9.3 以降
system subinterfaces	Ver.9.4 以降
usbmem revert-config	Ver.9.0 以降
poller rotor-preference	
nhrp nhs no utm https-port	NBMA アドレスのプロトコル変更後
utm max-session	UTM 起動後のみ
nm provisioning enable	

5.1.2 操作が必要なコマンド

設定を反映させるために、セッションのリセット等が必要な場合があります。
該当するコマンドは次のとおりです。

- QoS 関連コマンド

項目	備考
class-map policy-map	（1）service-policy output を削除後再設定 （2）clear policy-map interface（Ethernet のみ）

- BGP 関連コマンド

項目	備考
cluster-id	clear ip bgp * を実行
default-local-preference	clear ip bgp * を実行
default-metric	clear ip bgp * を実行
router-id	clear ip bgp * を実行
timers	clear ip bgp * を実行
neighbor connect-interval	clear ip bgp [該当ピアのアドレス]を実行
neighbor distribute-list	clear ip bgp [該当ピアのアドレス]を実行
neighbor next-hop-self	clear ip bgp [該当ピアのアドレス]を実行
neighbor receive-capability	clear ip bgp [該当ピアのアドレス]を実行
neighbor route-map	clear ip bgp [該当ピアのアドレス]を実行
neighbor route-reflector-client	clear ip bgp [該当ピアのアドレス]を実行
neighbor send-capability	clear ip bgp [該当ピアのアドレス]を実行
neighbor send-default	clear ip bgp [該当ピアのアドレス]を実行
neighbor timers	clear ip bgp [該当ピアのアドレス]を実行

- OSPF 関連コマンド

項目	備考
router-id	clear ip ospf process を実行
distribute-list	clear ip ospf process を実行
distance	clear ip ospf process を実行

- RIP 関連コマンド

項目	備考
distance	clear ip route を実行

- IKE/IKEv2 関連コマンド

項目	備考
全コマンド	SA クリア後有効になります。

- PPP/ISDN 関連コマンド

項目	備考
ppp profile	clear interface を実行
idle-time	clear interface を実行

5.1.3 インタフェース一括設定

Ver9.5 以降では多数のトンネルインタフェースのコンフィグを一括設定することができます。Ver9.7 以降ではイーサネットのサブインタフェースも一括設定することができます。全てのインタフェースに同様のコンフィグを設定する場合に利用可能です。

設定は以下のコマンドで行います。

interface range	インタフェースの一括設定
show running-config interface all	インタフェース設定の全表示 （一括設定したインタフェースも個別表示）

interface range コマンドで一括設定したいインタフェースの範囲を指定して、インタフェース一括コンフィグモードに移行します。

なお、インタフェース一括コンフィグモードで<INTERFACE>と入力すると、<INTERFACE>の部分を各インタフェースの番号に展開してコンフィグを設定することができ、全く同一の設定でなくても利用可能です。

```
【トンネルの設定例】
interface range Tunnel 0-9
  tunnel mode ipsec
  ip unnumbered GigaEthernet1.0
  ipsec policy tunnel ipsec-pol<INTERFACE> df-bit ignore pre-fragment out
  no shutdown

【参考】上記の設定例で interface Tunnel5.0 に設定されるコンフィグ
  tunnel mode ipsec
  ip unnumbered GigaEthernet1.0
  ipsec policy tunnel ipsec-pol5 df-bit ignore pre-fragment out
  no shutdown
```

```
【イーサネットの設定例】
interface range GigaEthernet0 sub 1-9
  bridge-group <INTERFACE>
  no shutdown

【参考】上記の設定例で interface GigaEthernet0.5 に設定されるコンフィグ
  bridge-group 5
  no shutdown
```

インタフェース一括コンフィグモードは、通常のコマンド入力と振舞いが大きく異なります。基本的な使い方として、確定しているコンフィグを一括設定して運用を開始し、運用中に一括設定は変更しないことを想定しているため、以下の動作概要と注意事項があります。内容をよく確認の上ご利用ください。

動作概要

- 1 行設定するたびに、指定した全てのインタフェースに対して当該コマンドが設定されます。
- 一度設定したコマンドの変更や削除はできません。設定変更、設定削除のコマンドも含めて、1 行設定するたびに入力した順にコマンド行が追加されます。例えば no shutdown を設定したあとで shutdown を設定した場合、両方のコマンドが設定されます（show running-config で表示した場合、no shutdown と shutdown の 2 行が表示されます）。
- コマンドを省略形で設定した場合、そのままの形で設定されます（補完されません）。
- interface range コマンドを削除しても、各トンネルインタフェースに設定されたコンフィグは削除されません。
- 一括設定したあと、個別のインタフェースのみ設定を変更することも可能です。設定変更したインタフェースは、show running-config で表示されるようになります。
- トンネルやイーサネットで利用可能な全ての設定コマンドが利用できます。

注意事項

- インタフェース一括コンフィグモードでは設定したコンフィグを修正、削除することができません。インタフェース一括コンフィグモード内でコマンドを試行錯誤せず、あらかじめ確認済みの設定を投入してください。
- インタフェース一括コンフィグモードで設定したコマンドを削除、変更したい場合は、interface range コマンドを削除したうえで設定を保存し、再起動してから改めて設定してください。再起動が困難な場合は、interface range コマンドを削除したあと、show running-config interface all コマンドを実行して、トンネルインタフェースに不要なコマンドが設定されていないことを確認してください。
- 一括コンフィグモードでは、対象インタフェースの数が多い場合、コマンド投入時に負荷が高くなる可能性があります。運用中に設定追加・変更を行うことは非推奨ですが、必要な場合は負荷に配慮して利用してください。
- <INTERFACE>を使用している行では TAB 補完やヘルプを実行しないでください。実行した場合、<INTERFACE>文字列が変換されてしまいますので、改めて編集してください。
- コマンドは省略せずに設定してください。設定したときに問題は発生しませんが、今後のバージョンアップで省略形が同じになるコマンドが追加されると、当該コマンドが設定されなくなります。
- 指定した全てのインタフェースに設定済みの設定（変更がない場合）は投入できません。

■5.2 設定の保存

すべての設定は、装置の揮発性メモリ上で変更が行われているだけです。
装置のリロード（reload），リスタート（restart）または電源 OFF を行うと、設定内容が消えてしまいます。
装置起動後も設定内容を有効にしたい場合、設定データを内部の不揮発性メモリ（フラッシュ）上に保存する必要があります。また、設定を不揮発性メモリ（フラッシュ）にファイルとして保存することにより、設定を複数保存することができます。

5.2.1 スタートアップコンフィグ

スタートアップコンフィグに設定を保存するためのコマンドは次のとおりです。

```
write memory
```

また、以下のコマンドによる設定保存もサポートされています。内部動作は、write memory コマンドと同じ動作を行います。

```
copy running-config startup-config
```

設定未保存状態の場合、以下のメッセージが表示されます。保存が必要な場合は、上記の設定の保存を行ってください。

```
% Warning: current running-configuration is not saved yet.
```

上記のメッセージは、次の場合に表示されます。

- reload 実行時

装置の設定情報をネットワーク上の他のホストにテキスト形式で設定を保存することも可能です。ただし送信には tftp を使用しますので、保存先のホストが tftp サーバである必要があります。tftp サーバには記録したいファイル名のファイルを予め作成し、書き込み可能にしておく必要がありますので、注意してください。
アドレスを指定しない場合、フラッシュ上にファイルとして保存できます。

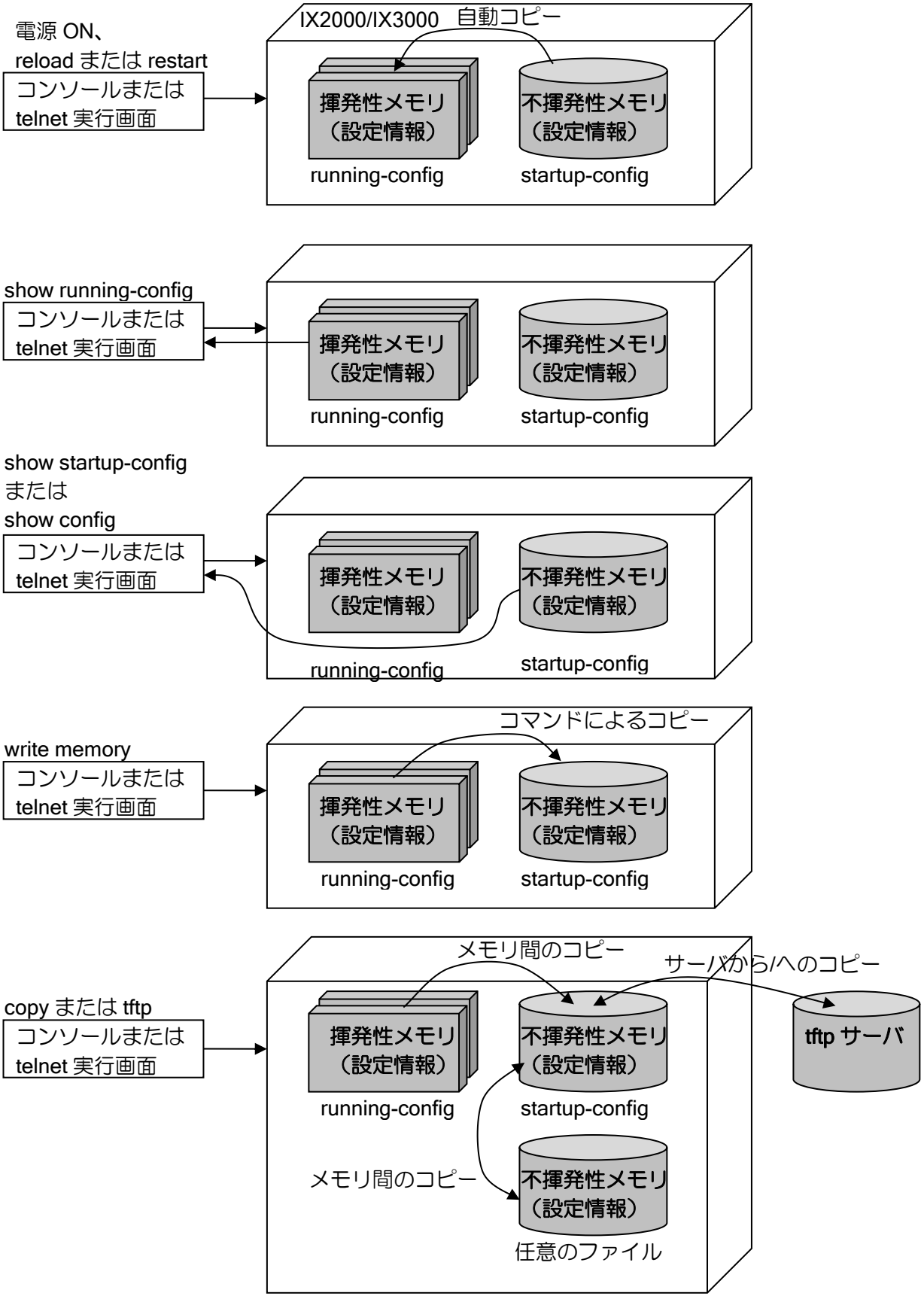
```
copy startup-config address:filename
```

※tftp サーバに保存したテキスト形式の設定ファイルを IX2000/IX3000 の起動時に自動的に読み出す手段はありません。起動時に設定を読み込ませるためには上記の write memory コマンドで設定を保存しておく必要があります。

スタートアップコンフィグは、以下のコマンドで消去することができます。

```
erase startup-config
```

次に設定情報の格納の動作原理を示します。

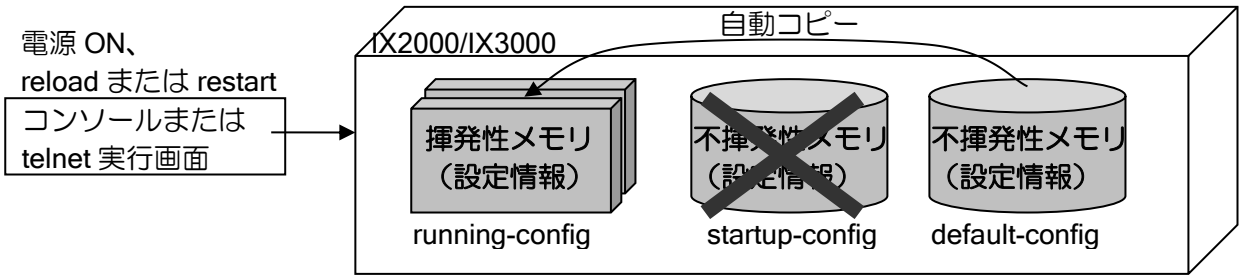


5.2.2 デフォルトコンフィグ

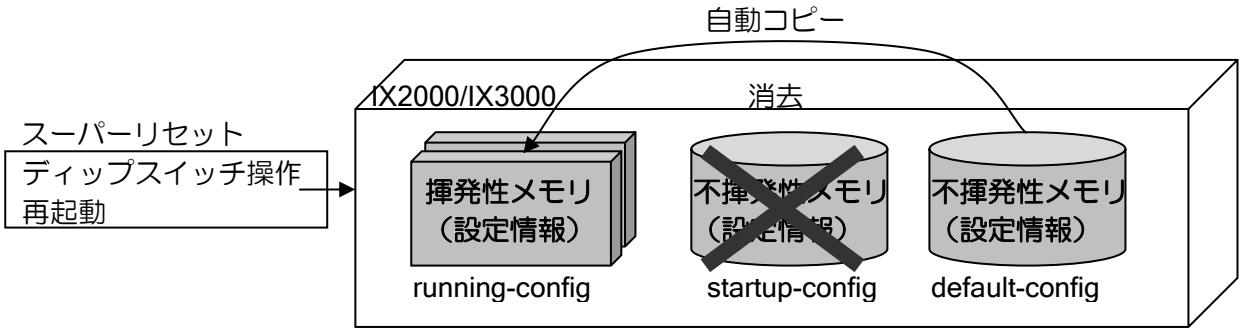
IX2000/IX3000 では、不慮の事故等でスタートアップコンフィグが破壊された場合などにデフォルトコンフィグの内容で起動することができます。（IX1000 シリーズでは、デフォルトコンフィグの利用はできません）

5.2.2.1 デフォルトコンフィグの特徴

- デフォルトコンフィグは、スタートアップコンフィグが存在しない場合に、起動時にランニングコンフィグに読み出されます。



- スーパーリセット（ディップスイッチによるコンフィグ消去）で消去されません。



✧ スーパーリセットにより、スタートアップコンフィグは消去されます。
✧ デフォルトコンフィグは消去されず、次回起動時にはデフォルトコンフィグで起動します。

※デフォルトコンフィグにログインパスワード設定を行い、かつパスワードを忘れた場合には、スーパーリセットでコンフィグを消去できないため注意が必要です。（ブートモニタコマンドで消去する必要があります）
※スーパーリセットの詳細については、取り扱い説明書を参照してください。

- コピーコマンドで上書きできません。

※デフォルトコンフィグに設定を保存する場合には、一度 erase default-config にてデフォルトコンフィグを消去する必要があります。

5.2.2.2 デフォルトコンフィグの設定

デフォルトコンフィグは、以下のコマンドにより保存することができます。

```
copy running-config default-config
copy startup-config default-config
copy address:filename default-config
```

デフォルトコンフィグは、以下のコマンドにより消去することができます。

```
erase default-config
```

ブートモニタで、デフォルトコンフィグを消去するには、以下のコマンドを使用します。

dc	デフォルトコンフィグの消去 （ブートモニタモード）

```
Router# reload
Notice: The router will be RELOADED. This is to ensure that
        the peripheral devices are properly initialized.
Are you sure you want to reload the router? (Yes or [No]): yes


NEC Bootstrap Software
Copyright (c) NEC Corporation 2001-2004. All rights reserved.

%BOOT-INFO: No boot records found, attempting flash load.
%BOOT-INFO: Trying flash load, exec-image [ix2010-xx-xx.xx.xx.ldc].
Loading: ###### <CTRL-C>
NEC Bootstrap Software, Version x.x
Copyright (c) NEC Corporation 2001-2004. All rights reserved.
boot>
boot> dc
Enter "Y" to clear default configuration: Y
% Default configuration is cleared.
```

■5.3 設定値の調整

IX2000/IX3000 シリーズでは、性能を最大限に引き出すために、効率的な稼動状態にする調整機構があります。利用環境によっては調整を実施した方が良い場合があります。本項では調整が必要な項目について、設定値を決定するための目安を説明します。

変更可能な項目には、次の項目があります。

項目	内容
送受信処理のスケジューリング	Serial インタフェースと Ethernet インタフェースを使用する場合の送受信処理のスケジューリングの設定を行います。
ルートキャッシュ数	ルートキャッシュ数の設定を行います。
ルートエントリ数	ルートエントリ数の設定を行います。
OSPF ルートエントリ数	OSPF のルートエントリ数の設定を行います。
NAT/NAPT エントリ数	NAT/NAPT のエントリ数の設定を行います。
UFS キャッシュエントリ数	UFS キャッシュのエントリ数の設定を行います。

5.3.1 送受信処理のスケジューリング

IX3015 において、Serial インタフェースと Ethernet インタフェースを使用する環境では、送信するデータサイズ, レートによっては、Serial の送信レートが期待通りにならない場合があります。Serial と Ethernet の送受信処理のスケジューリングを調整することにより Serial の送信レートを上げることができます。ただし、この場合 Ethernet のスループットが低下しますので、使用環境に応じて適切な値に調整する必要があります。

Serial のみ，または Ethernet のみの場合は調整の必要はありません。

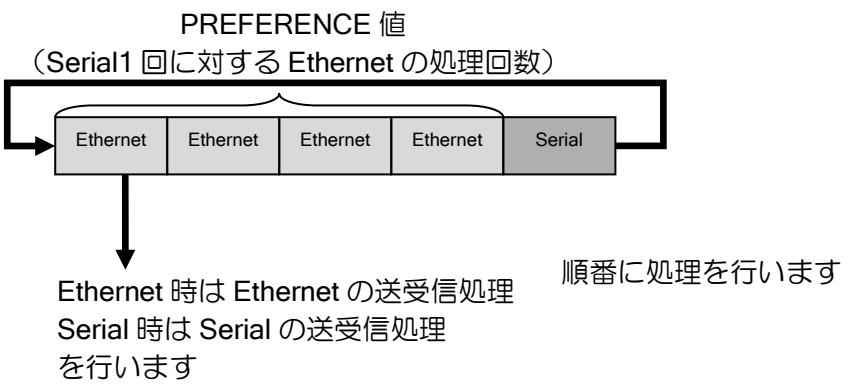
設定コマンドは以下の通りです。

scheduler poller rotor-preference （Ver.8.7 以前） poller rotor-preference （Ver.8.8 以降）	送受信処理のスケジューリング設定 （グローバルコンフィグモード）

【設定例】

```
scheduler poller rotor-preference 10
```

設定コマンドでは、PREFERENCE 値を設定します。Ethernet と Serial の送受信処理のスケジューリング動作と PREFERENCE 値は以下のように関連します。



PREFERENCE 値は、Serial1 回の処理に対して Ethernet を何回処理するかを表します。値を変更することによって、Serial の処理の割合を増やすか Ethernet の処理の割合を増やすかを決定します。これにより、どちらを優先するかの調整が可能となります。

Serial のみ, または Ethernet のみの場合はどちらか一方のみ処理を行いますので、PREFERENCE 値の変更により動作は変わりません。

設定値	効果
↑大きい	Ethernet の処理回数が増えます。 Serial の送信レートが低下します。 Ethernet のスループットが低下しません。
23：デフォルト	
↓小さい	Serial の処理回数が増えます。 Serial の送信レートが低下しません。 Ethernet のスループットが低下します。

送信レートは、PREFERENCE 値と 1 チャンネル当たりの最大 TimeSlot 割り当て数に影響します。最大 TimeSlot 数が大きくなるとデフォルト値のままでは Serial の送信レートが低下しますので、スケジューリングの調整が必要になります。

ver5.1 での PREFERENCE 値の推奨値とその時の送信レートは以下のようになります。以下の内容は構成，バージョンにより異なる場合がありますので、設定の際の目安として使用してください。

条件		結果		
TS アサイン数	PREFERENCE	Serial（pps）（双方向）	Ethernet（pps）（双方向）	総 pps 値（双方向）
24（1536Kbps）	6	7000	47400	54400
23（1472Kbps）	6	7000	45600	52600
22（1408Kbps）	6	7000	46600	53600
21（1344Kbps）	6	7000	46800	53800
20（1280Kbps）	6	7000	46400	53400
19（1216Kbps）	6	7000	46000	53000
18（1152Kbps）	6	7000	45960	52960
17（1088Kbps）	6	7000	45800	52800
16（1024Kbps）	6	7000	45600	52600
15（960Kbps）	6	7000	45400	52400
14（896Kbps）	6	7000	45200	52200
13（832Kbps）	6	7000	45000	52000
12（768Kbps）	6	7000	44800	51800
11（704Kbps）	6	7000	44800	51800
10（640Kbps）	6	7000	44200	51200
9（576Kbps）	6	7000	44280	51280
8（512Kbps）	6	7000	44000	51000
7（448Kbps）	6	7000	44000	51000
6（384Kbps）	8	7000	44000	51000
5（320Kbps）	10	7000	44600	51600
4（256Kbps）	12	7000	44400	51400
3（192Kbps）	16	7000	44400	51400
2（128Kbps）	23	7000	45200	52200
1（64Kbps）	23	7000	44800	51800

5.3.2 ルートキャッシュ数

ルートキャッシュはパケットを転送するためのキャッシュで、以下の項目でキャッシュを作成します。

- 宛先アドレス
- 送信元アドレス
- プロトコル

ルートキャッシュは最初のパケット転送時に作成され、以降の通信はキャッシュを使用することにより、高速にパケットを転送することが可能となります。作成されたキャッシュは、経路情報に変更がある（インタフェースの down, ネクストホップの変更等）まで保持されます。指定のキャッシュ数を超えた場合は、使用していないキャッシュがあれば削除しますが、削除するキャッシュが無い場合、キャッシュが作成されず、ルーティングテーブルを使用して転送先を検索するため、転送処理に時間がかかります。

キャッシュサイズはデフォルトは装置毎に異なります（以下の表を参照）。これ以上のキャッシュが必要な場合は、ルートキャッシュ数を変更してください。キャッシュ数を増やすことにより、メモリの消費量が増えます。メモリはエントリ作成時に確保しますので、残りのメモリ容量にはご注意ください。
起動時の残りメモリが 30%以下の場合、キャッシュサイズはデフォルト値に戻ります。更にメモリが不足する場合は、キャッシュサイズは 256 になります。

設定コマンドは以下の通りです。

ip cache-size	IPv4 ルートキャッシュの設定 Ver.9.5 以前 デフォルト:4096,IX3315 のみ 10000 Ver.9.6 以降のデフォルト IX3315 : 200000 IX3110 / IX2235 / IX2310 : 100000 IX2215 / IX2207 / IX2106 / IX2107 : 65535 IX3015 / IX2105 : 4096 （グローバルコンフィグモード）
ipv6 cache-size	IPv6 ルートキャッシュの設定 （デフォルト:4096,IX3315 のみ 20000） （グローバルコンフィグモード）
show ip cache	IPv4 ルートキャッシュの表示
show ipv6 cache	IPv6 ルートキャッシュの表示
show memory	メモリの確認

【設定例】

```
ip cache-size 6000
```

5.3.3 ルートエントリ数

ルートエントリはルータが持つ経路情報を格納するテーブルとなります。

- 宛先ネットワークアドレス
- ネクストホップ

ルートエントリは、スタティックに設定した経路，ルーティングプロトコルにより学習した経路が含まれます。ルートエントリ数を超えると、それ以上経路情報は作成されません。また、ルートエントリは、スタティックの経路の場合は削除されません。ルーティングプロトコルから学習した経路はルーティングプロトコルから学習している間は削除されません。

ルートエントリ数はデフォルトでは、IPv4 は 2048，IPv6 は無限大（システムのメモリがある限り確保）となります。IPv4 ではサイズを指定した場合は、指定したサイズ分のメモリを確保します。IPv4 で無限大（unlimited）を指定した場合と IPv6 の場合は、エントリが増える毎にメモリを確保します。値を増やすとメモリの消費量も増えますので、値を変更する場合は、メモリの容量にご注意ください。

IPv4,IPv6 ともに設定可能です。設定コマンドは以下の通りです。

ip max-route	最大ルートエントリ数設定 （デフォルト:2048,IX3315 のみ 100000） （グローバルコンフィグモード）
ipv6 max-route	最大動的ルート数の設定 （デフォルト:unlimited） （グローバルコンフィグモード）
show ip route	IPv4 ルート情報の表示
show ipv6 route	IPv6 ルート情報の表示
show memory	メモリの確認

【設定例】

IPv4 の場合
ip max-route unlimited

IPv6 の場合
ipv6 max-route 4000

5.3.4 OSPFv2 ルートエントリ数

OSPFv2 が学習したルートエントリの数になります。

- 宛先ネットワークアドレス
- ネクストホップ

ルータのルートエントリと同様に経路を学習した時に作成し、経路が無くなると削除されます。
ただし、Ver.9.4 以前では、ネットワーク構成変更等で古いルートエントリが未使用になった場合でも、エントリ情報は内部で保持しています。そのため、実際のエントリ数が上限を超えていない場合でも、エントリ数のオーバーフローが発生することがあります。Ver.9.5 以降では、未使用の内部エントリを削除しています。
デフォルトではエントリ数は 2048 となります。使用する値は、ip max-route の設定と関連します。

	rib max-entries 設定あり	rib max-entries 設定なし
ip max-route 設定あり	rib max-entries で設定した値を使用します。	ip max-route で設定した値を使用します。
ip max-route 設定なし	rib max-entries で設定した値を使用します。	デフォルト値を使用します。

メモリは、エントリが増える毎に確保されます。値を増やすとメモリの消費量も増えますので、値を変更する際は残りのメモリ量にご注意ください、
設定コマンドは以下の通りです。

rib max-entries	OSPF ルートエントリ数の設定(デフォルト:2048) （OSPF コンフィグモード）
show memory	メモリの確認

【設定例】

```
ip router ospf 1
  rib max-entries 3000
```

5.3.5 NAT/NAPT エントリ数

NAT/NAPT のアドレス変換用に使用するキャッシュとなります。以下の項目でキャッシュを作成します。

- 宛先アドレス
- 宛先ポート（NAPT 時）
- 送信元アドレス
- 送信元ポート（NAPT 時）
- プロトコル

NAT/NAPT エントリは、最初にアドレス変換を行う際に作成され、一定時間通信が無ければ削除されます。エントリ数の上限を超えると、新しいエントリが作成できず通信は破棄されます。デフォルト値では不足する場合もありますので、必要に応じて設定変更してください。
なお、特にデフォルトで不足しやすいNAPTエントリは、Ver9.3 以降一部の装置（IX2025, IX3015）を除きデフォルト値を 65535 に変更しました。

設定値を増やす場合はメモリの消費量が増えることにご注意ください。メモリはエントリ作成時に確保されます。

設定コマンドは以下の通りです。

ip nat translation max-entries	NAT エントリ数の設定 （インタフェースコンフィグモード）
ip napt translation max-entries	インタフェース単位での NAPT エントリ数の設定 （インタフェースコンフィグモード）
ip napt translation max-entries per-address	ホスト単位での NAPT エントリ数の設定 （デフォルト: ホスト単位制限なし） （インタフェースコンフィグモード）
show ip nat translation	NAT エントリ数の確認
show ip napt translation	NAPT エントリ数の確認
show memory	メモリの確認

【設定例】

```
interface FastEthernet0/0.0
  ip napt translation max-entries 10000
  ip napt translation max-entries per-address 1000
```

■5.4 LED 状態

対応する装置に関しては、ハードウェア諸元の項を参照してください。
Ver9.3 以降 show hardware コマンドでも点灯状態を確認できます。

LED	状態	条件
PWR	緑点灯	電源が ON の場合
ALM	赤点灯	障害が発生した場合
BUSY（BSY）	橙点灯	フラッシュメモリにアクセス中 LED 点灯中は装置の電源を OFF にしないでください。 以下のような場合、フラッシュメモリにアクセスを行います。 • write memory 実行中 • ロードモジュール更新中 • copy,tftp コマンド実行中 • show tech-support のフラッシュメモリ出力中
VPN	緑点灯	送受信の IPsec-SA が存在する場合 IPsec 設定が複数存在する場合は、いずれか SA が存在している場合
PPP	消灯	PPPoE が接続していない状態 この状態が継続する場合、物理接続,ケーブル等の確認を行ってください。
	緑点滅	PPP 接続処理中、または直前の PPP 接続で失敗した状態 PPPoE が OPEN して、IPCP が OPEN していない状態 または、直前の PPP 接続で、PPPoE が OPEN して、IPCP が OPEN しなかった状態 この状態が継続する場合、PPP のコンフィグに誤りが無いか確認してください。
	緑点灯	通信が可能な状態 IPCP が OPEN している場合 複数 PPP 設定が存在する場合は、いずれかが通信可能となった場合
BAK	緑点灯	ネットワークモニタのイベントが発生時のアクションとして指定 複数のネットワークモニタで設定している場合は、いずれかのアクションが実行されている場合。 コマンドはネットワークモニタの項を参照してください。

(a) ALM

アラームが点灯する障害は以下の通りです。

障害内容	点灯条件
ハードウェア異常	装置起動時の POST（電源投入時のハードウェア自己診断）で Fail を検出した場合に障害となります。
温度異常	温度アラーム検出時に点灯します。 *IX2003,IX2004 は温度異常を検出しません
電圧異常	電圧障害時に点灯します。 *IX2003,IX2004 は電圧異常を検出しません
電源モジュール異常	電源モジュールの二重化運用時に、一方の電源が供給されなくなった場合障害となります。
FAN 異常	5 秒間隔でポーリングし、3 回連続 5294 回転/分以下を検出すると障害となります。

■5.5 IX3315 の注意事項

IX3315 を利用する場合の注意事項と、IX3315 特有のチューニング方法について説明します。IX3315 を最適な状態で動作させるためには、状況にあわせて設定変更が必要となる場合がありますので、各項目を参照して、必要に応じて設定してください。

以下の項目について説明します。

項目	内容
10G インタフェースについて	10G ポートを 1G で使う場合の注意事項です。
インタフェース数の調整	不要なインタフェースを削減します。
受信パケット優先制御の設定	受信パケットの優先制御を行います。
IPsec の設定	1024 対地以上を利用する場合の注意事項です。
QoS クラス数の設定	QoS の不要なクラス数を削減します。
レイテンシ制限機能の無効化	輻輳時のレイテンシ増加時のパケット廃棄を無効化します。
SW-HUB 送信レート制限の無効化	イーサネットコントローラ（CPU）から SW-HUB に送信するパケットのレート制限を無効化します。

5.5.1 10G インタフェースについて

10Gbps 対応のインタフェースが 10Gbps 以外のリンク速度でリンクアップしたとき、最大スループットが帯域の 90%～97%程度になります。[理由]Ether デバイスの制限事項により、パケット間の間隔(IPG：Inter-Packet Gap)を通常よりも 32byte 多く挿入しているためです。【回避策】IX3315 で 1Gbps のリンク速度でご利用する場合、GE0,GE1 ポートをお使いください。

5.5.2 インタフェース数の調整

IX3315 ではトンネルインタフェース 5000, イーサネットのサブインタフェース 1000 など、多数のインタフェースを利用できますが、インタフェースの総数は装置全体の負荷への影響が大きく、コンフィグしていないインタフェースも装置の負荷要因となっています。
このため、以下のような条件の場合には、トンネルインタフェース数を削減してください。

- イーサネットのサブインタフェースを増加させる場合
- IPv6 インタフェースを多数設定する場合（IPv4 over IPv6 トンネルは IPv4 なので対象外）

これ以外でも、負荷が高いと思われる設定で利用する場合には、利用予定のないトンネルインタフェースを削減すると装置全体の負荷軽減になります。

5.5.2.1 トンネルインタフェース数の設定

トンネルインタフェース数の初期値は最大値の 5000 です。
設定変更後は装置の再起動が必要となります。設定コマンドは以下の通りです。

system interfaces	インタフェース数の設定

【設定例】
トンネルインタフェース数を 500 に設定

```
system interfaces tunnel 500
```

5.5.2.2 サブインタフェース数の設定

イーサネットのサブインタフェース数の初期値は 32 で、設定により 1 デバイスあたり 1000 まで拡張できます（タグ VLAN の利用を想定しています）。

ただし、サブインタフェースを増やす場合は、トンネルインタフェースを同数以上削減し、インタフェースの総数が増えないように設定してください。また、サブインタフェースの総数は以下が推奨です。

サブインタフェースの総数：（搭載 Ethernet デバイス[6 個]-1）×32+1000＝1160

サブインタフェース設定変更後は装置の再起動が必要となります。
設定コマンドは以下の通りです。

system subinterfaces	サブインタフェース数の設定 （グローバルコンフィグモード）

【設定例】
GigaEthernet0 のサブインタフェース数を 500 に設定

```
system subinterfaces GigaEthernet0 500
```

5.5.3 受信パケットの優先制御

IX3315 は受信パケットの優先制御が可能です。高負荷時に制御パケットが受信できず障害と検出されることを極力防止することができます。いくつかのプロトコルは自動的に優先しますが、TOS や COS の条件を設定することで任意のパケットを優先することも可能です。

デフォルトで優先されるパケットは以下のとおりです。

- ARP、LLDP、ループ検出パケット
- ICMP、PIM、IGMP、VRRP、OSPF
- telnet/SSH、BGP、RIP、DNS、IKE（ESP を除く）

設定コマンドは以下の通りです。

system input-priority-queue	受信パケット優先制御の設定 （グローバルコンフィグモード）

【設定例】
DSCP が 1～63 の場合に優先パケットとして受信
（TOS または Traffic-Class フィールドの上位 6bit の何れかが”1”）

```
system input-priority-queue high tos mask 0xfc
```

5.5.4 IPsec の注意事項

IPsec の通信で 1024 対地を超えて利用する場合は、以下の条件で利用してください。

- IKEv1 を利用せず、IKEv2 を利用する。
- DPD を利用せず、ネットワークモニタを利用する（拠点側のみ設定を推奨）
- 受信パケットの優先制御でネットワークモニタの通信を優先する。
- DH グループは可能なら 1024-bit や 768-bit を利用する。
- DH グループを 3072-bit を 3000 対地以上で使用する場合は、再送間隔を 10 秒以上に設定

する。

5.5.5 QoS クラス数の設定

Ver9.7 以降では、以下の作業は不要です。

QoS クラス数は初期値では最大値の 5002 個（local クラス,default クラスを含む）となります。
QoS を設定すると利用するクラス数に関係無く最大クラス数分のメモリを確保するため、多数のインタフェースに QoS を設定する場合には、最大クラス数を減少させることでメモリの使用量を抑制することができます。
設定変更後は装置の再起動が必要となります。設定コマンドは以下の通りです。

system qos max-classes	QoS 最大クラス数の設定

【設定例】
QoS のクラス数を 100 に設定

```
system qos max-classes 100
```

5.5.6 レイテンシ制限機能の無効化

輻輳制御によるパケット廃棄を無効化します。通常設定を変更する必要はありません。
受信時と送信時に輻輳している場合は、パケットが処理されるまで装置内部で滞留し、遅延が発生します。初期状態では、装置内の遅延時間が一定時間を超えるとパケットを廃棄します。
無効化により、輻輳時にも受信バッファが枯渇するまでパケットを廃棄しなくなりますが、遅延は大きくなります。
設定コマンドは以下の通りです。

system latency-control disabled	レイテンシ制限機能の無効化の設定

【設定例】

```
system latency-control disabled
```

5.5.7 SW-HUB での送信レート制限無効化

IX3315 では、SW-HUB とイーサネットコントローラ（CPU）との接続は 10Gbps で、SW-HUB の各ポートは最大 1Gbps となっています。このため、イーサネットコントローラから SW-HUB へのパケット送信をポート VLAN グループごとにリンク速度に制限することにより、SW-HUB 内での廃棄を抑止しています。
ポート VLAN が設定されていない場合、全体で送信を 1Gbps に制限します。ポート VLAN が設定されている場合は、ポート VLAN ごとに送信を 1Gbps に制限します。
送信レート制限の無効化により、1Gbps 以上の送信が可能となります。ただし、通信が特定のポートに偏る場合、リンク速度を超えるため SW-HUB でパケット廃棄が発生します。
設定コマンドは以下の通りです。

system swhub-shaping disabled	シェーピング機能の無効化

【設定例】

```
system swhub-shaping disabled
```

■5.6 起動時コンフィグダウンロード

指定したサーバからダウンロードしたコンフィグで起動することができます（Ver.8.8 以降 IPv4 対応、Ver.8.9 以降 IPv6 対応）。

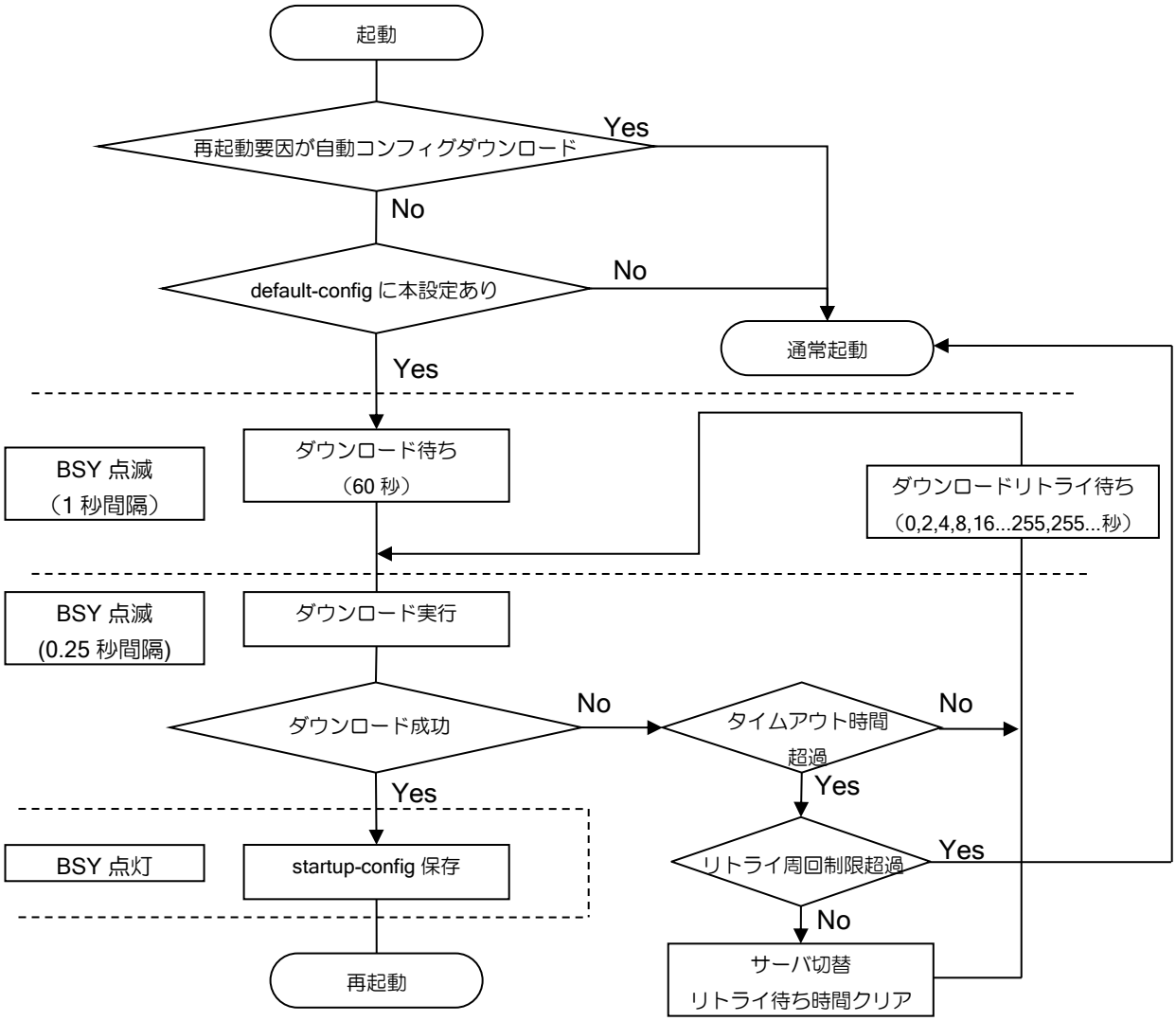
起動時コンフィグダウンロードを使用している場合、起動時は必ず指定したサーバからコンフィグのダウンロードを行います。状態は LED で確認することができます。

5.6.1 動作

default-config に起動時コンフィグダウンロードの設定を行っている場合、装置起動時は設定されたサーバからコンフィグのダウンロードを行います。起動直後のダウンロードは 60 秒後に実行します。ダウンロードが失敗した場合は、成功するまでコンフィグのダウンロードを繰り返します。Ver.10.2 以降、リトライ周回数の上限を設定することでダウンロードを中断し通常起動することができます。複数サーバ設定時は、設定順にダウンロードするサーバを切り替えます。応答が無い場合は、タイムアウト時間経過後、サーバを切り替えます。応答がエラーの場合、リトライを行います。リトライ毎にリトライ間隔を延長し、リトライ間隔がタイムアウト時間を超える場合、次のサーバに切り替えます。

ダウンロードが成功すると、startup-config に保存し再起動を行います。再起動時にはダウンロードしたコンフィグで起動します。

起動時コンフィグダウンロード機能の処理の流れは以下の通りです。



コンフィグダウンロード時でもコンソールは通常通り使用可能です。ダウンロード処理を中断する場合は、コンソールから svintr-config を入力してください。また、enable-config ではコンフィグモードへの遷移はできません。svintr-config により処理を中断し、コンフィグモードへ遷移することができます。

動作結果は、show crashinfo により確認することができます。

【表示例】
正常に更新した場合の表示例

```
(config)# show crashinfo
Latest Occurrence Time       Event Description
2012/06/18 16:42:33 +0900 INFO: Start logging fault and crash errorlog_information
2012/06/18 16:44:10 +0900 INFO: Start bootstrap from this side [0].
2012/06/18 16:44:05 +0900 INFO: Modify startup-config cmd:config-download
state:succeeded from:system
2012/06/18 16:44:05 +0900 INFO: Download startup-config from tftp://10.0.0.1
/con09TNU000001.txt state:succeeded
```

起動時コンフィグダウンロードの結果として以下のメッセージが表示されます。
その他のメッセージに関しては、付録の「ルータメッセージ一覧」を参照してください。

メッセージ	内容
Download startup-config from	コンフィグダウンロードを実行しました。 ・succeeded：成功しました ・failed(communication error)： 　サーバにアクセスできなかった 　ファイルが存在しなかった ・failed(timeout)：転送がタイムアウトした ・failed(file too big)： 　転送したファイルがコンフィグサイズの上限を超えている ・failed(internal error)：内部エラー ・failed(retry count exceeded)： 　リトライ周回制限に達した（Ver.10.2 以降）

注意事項

- enable-config によるオペレーションモードからコンフィグモードへの遷移は行えません。
- ダウンロードしたファイルについては、サイズ（最大コンフィグサイズ）のチェックのみ行います。内容の確認は行いません。
- default-config に起動時自動バージョンアップ機能を設定している場合、バージョンアップ機能は動作しません。起動時自動バージョンアップ機能は、ダウンロードする運用コンフィグ側に設定してください。
- 起動時コンフィグダウンロード機能動作中は、スケジューラ機能は動作しません。

5.6.2 設定

default-config に起動時ダウンロードの設定を行います。startup-config に起動時コンフィグダウンロードを設定した場合は設定は無視され、起動時のコンフィグのダウンロードは行いません。

起動時コンフィグダウンロード設定では、ファイル名に<SN>を指定することにより装置のシリアル番号を自動で取得しファイル名を作成します。<SN>指定を行うことにより、同じ default-config を使用しても、装置に対応したファイルをダウンロードすることが可能です。

default-config には、起動時コンフィグダウンロードの設定以外に、インタフェースの IP アドレスやサーバへのルーティング等、サーバへ接続するための設定が必要になります。

startup config-download	起動時コンフィグダウンロードサーバ指定
startup config-download-timeout	起動時コンフィグダウンロードタイムアウト設定
startup config-download-retry	自動コンフィグダウンロードのリトライ周回数設定

【設定例】
default-config に以下を設定

```
startup config-download https://10.0.0.10/con<SN>.txt account user1 password pass1

interface GigaEthernet0.0
  ip address dhcp
  no shutdown
```

【動作例】
シリアル番号が 01TNU00001 の場合、10.0.0.10 のサーバから con01TNU00001.txt をダウンロードします。

※2006 年以前製造の IX3010（show hardware のシリアル表示未対応）では、<SN>指定によりシリアル番号は取得できません。

■5.7 USB メモリの利用

Ver9.0 以降では、USB ポートで USB メモリが利用可能となります。また、IX2207 では、かんたん操作ボタン（SEL／ENT ボタン）を使用した USB メモリへのコピー、リストアなどの機能が利用可能です。

※ゼロコンフィグ（SMFv2）利用時には USB メモリは利用できません。

5.7.1 対応機能

かんたん操作ボタン（USB ボタン機能）（※1）

- かんたん操作ボタンによる USB ボタン機能の実行
- USB メモリの安全な取り外し（EJCT）
- USB メモリへの装置コンフィグ、ログのコピー（COPY）
- USB メモリからの装置コンフィグのリストア、ソフトウェアのアップデート（RSTR）
- USB メモリに用意した、コマンドバッチファイルの実行

（※1） コマンドによる USB ボタン機能の実行は、SEL/ENT ボタンの無い機種でも可能です。

工場出荷状態装置のリストア機能

- コンフィグが入っていない装置に USB メモリを挿して起動させることで、装置コンフィグのリストア、ソフトウェアのアップデートが可能

USB メモリ対応コマンド（コピーコマンド、情報取得、ソフトウェアアップデート）

- 装置コンフィグと USB メモリのファイル間のコピー
- 装置フラッシュメモリのファイルと USB メモリのファイル間のコピー
- show tech-support 情報の USB メモリのファイルへの書き込み
- show logging 情報の USB メモリのファイルへの書き込み
- software-update コマンドでの USB メモリの利用
- USB メモリのファイル削除

USB メモリ認証機能

- 利用可能な USB メモリの制限
- USB メモリのベンダ ID、プロダクト ID、シリアルナンバーによる認証
- USB メモリに保存したパスワードファイルによる認証

5.7.2 対応 USB メモリ

- FAT32 でフォーマットされた USB メモリ
- 32 キロバイト以下のアロケーションユニットサイズ
- Windows アプリケーション等を必要とする暗号化機能付きの USB メモリは利用不可

※ NTFS や exFAT など FAT32 以外でフォーマットされた USB メモリは利用できません。
※ FAT16、FAT12 でフォーマットされた USB メモリも利用可能ですが非推奨です。
※ 64 キロバイト以上のアロケーションユニットサイズでフォーマットされた USB メモリは利用できません。（例: 高速化ツールなどでフォーマットされた USB メモリ）
※ Windows のクイックフォーマットを利用すると、予期しない不具合が発生する可能性があり

ます。通常フォーマットを行った USB メモリを使用してください。

※ USB メモリによっては、正しくフォーマットされていても利用できない可能性があります。（運用前に利用可能か確認してください。）

※ サポート機器以外の接続はしないでください。（外付け USB-HUB 等）

※ 未サポートのデバイスを接続している状態でのルータ動作の正常性は保証できません。

※ 未サポートのデバイスを挿入した場合、抜去した後においてもルータ動作の正常性は保証できません。

※ USB メモリの 1 つのディレクトリに大量にファイルを保存された状態で使用すると、著しく装置負荷が上がることがあります。1 つのディレクトリ内のファイル数は 100 個程度を上限として、極力少ない数となるようにしてください。

5.7.3 USB メモリのマウント

USB メモリをコピーコマンドや USB ボタン機能で利用可能な状態にすることを、USB のマウントと呼びます。USB メモリを利用するためには、以下の設定を行い FAT32 でフォーマットされた USB メモリを挿します。

usbmem enable	USB メモリの有効化（デフォルト無効） （グローバルコンフィグモード）
no shutdown shutdown	USB ポートの有効化 USB ポートの無効化（USB ポートの電源供給断） （USB デバイスコンフィグモード）

```
【設定例】
!
usbmem enable
!
device USB0
   no shutdown
!
device USB1
   no shutdown
```

USB メモリがマウントされると、対応する USB の LED が点灯します。

状態	点灯パターン
USB メモリがマウントされている（利用可能状態）	3 ○（点灯） 2 ●（消灯） 1 ○（点灯）
USB メモリのファイルアクセス中 ※ USB メモリの抜去には特に注意してください	3 ◎（点滅） 2 ●（消灯） 1 ○（点灯）

5.7.4 USB メモリデバイスの確認

マウントされた USB メモリの USB メモリデバイス名、デバイス情報は、show hardware コマンドで確認できます。
USB メモリ機能で使用する、装置シリアル番号も、show hardware コマンドで確認できます。

```
【表示例】
Router(config)# show hardware
IX Series IX2215 Hardware Platform

S/N: XXXXXXXXXX                          ... 装置シリアル番号
                    :

Option interface unit USB0:
  USB Mass Storage Device (usbmem0)      ... USB メモリデバイス名（usbmem0）
    Model name is <MODEL 名>             ... 製品名、モデル名
    Vendor ID is 0xXXXX                  ... ベンダ ID（16 進数）
    Product ID is 0xXXXX                 ... プロダクト ID（16 進数）
    Serial number is XXXXXXXXXXXXXXX     ... シリアルナンバー（文字列）
```

※ USB1 ポートの USB メモリデバイス名は、usbmem1 などになります。
※ シリアルナンバーの無い USB メモリでは、該当項目が表示されません。

5.7.5 USB メモリのファイル、ディレクトリ指定方法

コマンドでの USB メモリの指定は、以下のようなフォーマットを使用します。USB メモリデバイス名は、USB メモリがマウントされた状態で、show usbmem や、show hardware で確認することができます。

```
usbmemX[.Y]:PATH/[FILENAME]

        usbmemX[.Y] ... USB メモリデバイス名
          X  -  USB ポート番号（範囲 0-1）
          Y  -  論理ユニット番号（範囲 0-3、0 の場合は省略可能）
        PATH ... ディレクトリ名
        FILENAME ... ファイル名
```

※ 省略可能なオプションなど詳細は、コマンドリファレンスマニュアルを参照してください。
※ 日本語ファイル名、ディレクトリ名は使用できません。

【指定例】

USB メモリのディレクトリ指定

```
Router(config)# show usbmem usbmem0:/
Directory is /
2014/06/29   20:21:26   <DIR>          LOG                LOG
2014/06/29   20:21:26   <DIR>          COPY               COPY
2014/06/29   20:21:28            1238   STARTU~1.CFG   startup-config.cfg
1 files 1238 bytes
2 directories
```

USB メモリのファイル指定

```
Router(config)# show usbmem usbmem0:/startup-config.cfg
! NEC Portable Internetwork Core Operating System Software
! IX Series IX2215 (magellan-sec) Software, Version 9.0.X, RELEASE SOFTWARE
! Compiled Jun 20-Fri-2014 13:30:46 JST #2
! Last updated Jun 29-Sun-2014 20:14:09 JST
!
                                :
```

5.7.6 USB メモリが使用可能なコマンド

USB メモリは以下のコマンドで利用可能です。詳細はコマンドリファレンスマニュアルを参照してください。

copy <flash> <USB メモリ> copy <USB メモリ> <flash>	装置フラッシュメモリのファイルと USB メモリのファイル間のコピー
copy startup-config <USB メモリ> copy <USB メモリ> startup-config copy default-config <USB メモリ> copy <USB メモリ> default-config	装置コンフィグと USB メモリのファイル間のコピー
copy tech-support <USB メモリ> show tech-support output <USB メモリ>	show tech-support の結果を USB メモリのファイルに出力
copy logging <USB メモリ> show logging output <USB メモリ>	show logging の結果を USB メモリのファイルに出力
software-update <USB メモリ>	USB メモリのファイルを使用して、ソフトウェアアップデート
erase <USB メモリ>	USB メモリのファイルを削除 ※USB メモリのディレクトリは削除できません。（不要なディレクトリは PC 等で削除してください）
show usbmem [<USB メモリ>]	USB メモリ情報を表示

※ TFTP によるリモートファイルから USB メモリのファイルへのコピーはできません。
※ USB メモリのファイルから USB メモリのファイルへのコピーはできません。（PC 等で実施してください）
※ USB メモリのファイル書き込み時に、すでに同一ファイルがあった場合は上書きされます。（装置フラッシュメモリへのファイル書き込み時に、同一ファイルがあった場合は書き込みできません。）

5.7.7 かんたん操作ボタン（SEL／ENT ボタン）

IX2207 は、かんたん操作ボタン（SEL／ENT ボタン）を持っており、コンソールやリモートログインを行わずに、USB メモリの USB ボタン機能（イジェクト機能、コピー機能、リストア機能、コマンドバッチ機能）を利用することができます。

USB メモリがマウントされた状態で、SEL ボタンを押すと、各 USB ボタン機能を示す LED が点灯し、ENT ボタンを押すことで対応する USB ボタン機能を実行することができます。

5.7.7.1 状態遷移と LED 表示

	状態	点灯パターン
①	マウント状態 ↓ SEL ボタンを押す ②へ	3 ○ RSTR（点灯） 2 ● COPY（消灯） 1 ○ EJCT （点灯）
②	イジェクト機能選択中 ↓ SEL ボタンを押す　↓ ENT ボタンを押す ③へ　実行（次項以降を参照してください）	3 ● RSTR（消灯） 2 ● COPY（消灯） 1 ○ EJCT （点灯）
③	コピー機能選択中 ↓ SEL ボタンを押す　↓ ENT ボタンを押す ④へ　実行（次項以降を参照してください）	3 ● RSTR（消灯） 2 ○ COPY（点灯） 1 ● EJCT （消灯）
④	リストア機能選択中 ↓ SEL ボタンを押す　↓ ENT ボタンを押す ⑤へ　実行（次項以降を参照してください）	3 ○ RSTR（点灯） 2 ● COPY（消灯） 1 ● EJCT （消灯）
⑤	コマンドバッチ機能選択中 ↓ SEL ボタンを押す　↓ ENT ボタンを押す ②へ　実行（次項以降を参照してください）	3 ○ RSTR（点灯） 2 ○ COPY（点灯） 1 ○ EJCT （点灯）

※ 機能選択中のまま、30 秒経過すると機能選択中が解除されマウント状態の LED①に戻ります。
※ USB0 と USB1 の両方に USB メモリがマウントされている場合は、USB0（②→③→④→⑤）→USB1（②→③→④→⑤）→USB0（②→③→④→⑤）→... のように交互に選択されます。
※ USB メモリがマウントされていない場合は、SEL ボタンを押しても機能選択はされません。
※ USB ボタン機能を実行すると（コマンドラインからの USB ボタン機能の実行も同じ）、コンソールなどでコンフィグモードに入っていた場合、USB ボタン機能の実行中はコンフィグにロックがかかり、完了後グローバルコンフィグモードに自動的に遷移されます。

5.7.8 イジェクト機能（USB ボタン機能）

USB メモリを利用中のアプリケーションを終了させ、USB メモリを安全に抜去できる状態にします。

※ USB メモリにアクセス中に抜去すると、USB メモリ内のファイルやファイルシステムが破壊され、USB メモリが読み書きできなくなる可能性もありますので、USB メモリは必ずイジェクト機能を実行してから抜去してください。

コマンドから、イジェクト機能を実行することもできます。

usbmem eject <USB デバイス名>	USB ボタン機能のイジェクト機能を実行する。 （グローバルコンフィグモード）

※ スケジューラ機能からこのコマンドを呼び出すことはできません。

5.7.8.1 USB メモリに保存されるファイル

実行ログ

/LOG/<装置シリアル番号>/<実行日時>_eject-result.log

※ USB メモリの容量不足などでログファイルが作成できなくても処理は継続されます。

5.7.8.2 状態遷移と LED 表示

	状態	点灯パターン
①	イジェクト機能実行中 ↓（最低 10 秒間 LED 表示） ②へ ※USB メモリを利用中のアプリケーションがあった場合、完了に時間がかかることがあります。	3 ● RSTR（消灯） 2 ● COPY（消灯） 1 ◎ EJCT （点滅）
②	イジェクト機能完了 USB メモリを抜去可能	3 ● RSTR（消灯） 2 ● COPY（消灯） 1 ● EJCT （消灯）

※イジェクトされた USB メモリを再度マウントするには、USB メモリを抜き挿しするか、USB デバイスモードで reset を行ってください。

5.7.9 コピー機能（USB ボタン機能）

装置コンフィグ（startup-config、default-config）や、装置ログ（show tech-support、show logging）を USB メモリにコピーします。

コマンドから、コピー機能を実行することもできます。

usbmem copy <USB デバイス名>	USB ボタン機能のコピー機能を実行する。 （グローバルコンフィグモード）

※ スケジューラ機能からこのコマンドを呼び出すことはできません。

5.7.9.1 USB メモリに保存されるファイル

装置コンフィグ

※ 装置シリアル番号のディレクトリとルートディレクトリの両方に保存されます。
※ ルートディレクトリに保存されたファイルを利用して、そのまま、工場出荷状態装置へのリストアを行うことができます。

startup-config のバックアップ

/COPY/<装置シリアル番号>/<実行日時>_startup-config.cfg
/startup-config.cfg

default-config のバックアップ

/COPY/<装置シリアル番号>/<実行日時>_default-config.cfg
/default-config.cfg

装置ログ

show tech-support の出力

/COPY/<装置シリアル番号>/<実行日時>_tech-support.log

show logging の出力

/COPY/<装置シリアル番号>/<実行日時>_logging.log

実行ログ

/LOG/<装置シリアル番号>/<実行日時>_copy-result.log

※ USB メモリの容量不足などで開始時に実行ログファイルが作成できない場合は処理を終了します。
※ USB メモリの容量不足などで処理の途中で実行ログファイルへの書き込みができなくなっても、コピー処理は継続されます。（以降、実行ログファイルへの出力は行われません。）

5.7.9.2 状態遷移と LED 表示

	状態	点灯パターン
①	コピー機能実行中 startup-config のコピー default-config のコピー show tech-support の出力をコピー show logging の出力をコピー → ③ ↓（最低 10 秒間 LED 表示） エラー発生時 ②へ	3 ● RSTR（消灯） 2 ◎ COPY（点滅） 1 ● EJCT （消灯）
②	コピー機能完了	3 ○ RSTR（点灯） 2 ● COPY（消灯） 1 ○ EJCT （点灯）
③	実行エラー ↓（最低 30 秒間 LED 表示） ②へ	3 ◎ RSTR（点滅） 2 ○ COPY（点灯） 1 ◎ EJCT （点滅） ◎ ALM （赤点滅）

※ 実行エラーの代表的な発生要因は、USB メモリ不良などによる書き込みエラー、容量不足等となります。
※ 書き込み時に USB メモリに同一ファイル名があった場合は上書きされます。
※ 書き込み終了時にファイルサイズが 0 バイトだった場合、ファイルは削除されます。
※ コピー処理がエラーとなった場合でも他のコピー処理は実行されます。最終的にいずれかのコピー処理でエラーが発生していた場合には実行エラーとなります。

5.7.10 リストア機能（USB ボタン機能）

USB メモリ内にあらかじめ保存してあるコンフィグやソフトウェアから、装置のコンフィグの変更や、ソフトウェアアップデートを行います。

コマンドから、リストア機能を実行することもできます。

usbmem restore <USB デバイス名>	USB ボタン機能のリストア機能を実行する。 （グローバルコンフィグモード）

※ スケジューラ機能からこのコマンドを呼び出すことはできません。

5.7.10.1 USB メモリのファイル配置

リストア機能では、更新するコンフィグ、ソフトウェアを USB メモリの該当ファイルを上から順番に検索し、ファイルがあった場合にコンフィグのリストア、もしくはソフトウェアアップデートを実行します。
装置シリアル番号のディレクトリにファイルを配置することで、1 つの USB メモリで複数の装置に対して個別のコンフィグを配置することができます。（装置シリアル番号は、show hardware などであらかじめ取得しておきます。）

リストア前の装置のコンフィグに拠らず、リストア後のコンフィグを一意に確定させるためには、startup-config と default-config の両方のリストア用のファイルを配置しておく必要があります。

※ startup-config、default-config、ソフトウェアに対して個別にリストアが実施されます。（更新ファイルの検索できなかった対象は変更されません。）
※ リストア時に装置内の startup-config、default-config を削除する必要がある場合は、erase-startup-config.cfg、erase-default-config.cfg など、削除用の空のファイルを配置しておきます。

装置リストアコンフィグ

startup-config のリストア（上から順番に検索）

/RESTORE/<装置シリアル番号>/startup-config.cfg
/RESTORE/<装置シリアル番号>/erase-startup-config.cfg（削除用）
/startup-config.cfg
/erase-startup-config.cfg（削除用）

default-config のリストア（上から順番に検索）

/RESTORE/<装置シリアル番号>/default-config.cfg
/RESTORE/<装置シリアル番号>/erase-default-config.cfg（削除用）
/default-config.cfg
/erase-default-config.cfg（削除用）

ソフトウェアアップデート

RAP ファイル（上から順番に検索）

/RESTORE/<装置シリアル番号>/software-update.rap
/software-update.rap

5.7.10.2 USB メモリに保存されるファイル

実行ログ

/LOG/<装置シリアル番号>/<実行日時>_restore-result.log

※ USB メモリの容量不足などで開始時に実行ログファイルが作成できない場合は処理を終了します。
※ USB メモリの容量不足などで処理の途中で実行ログファイルへの書き込みができなくなっても、リストア処理は継続されます。（以降、実行ログファイルへの出力は行われません。）

5.7.10.3 装置フラッシュメモリに保存されるファイル

バックアップファイル（装置フラッシュメモリ）

startup-config のバックアップ

BACKUP-STARTUPCONFIG

default-config のバックアップ

BACKUP-DEFAULTCONFIG

※ バックアップファイルを保存することにより装置フラッシュメモリが不足する場合、以下のファイルを除く装置フラッシュメモリのすべてのファイルが削除されます。

- ファームウェア
- SYSTEM-PRIVATE-KEY
- SYSTEM-CERT-BUNDLE

5.7.10.4 コンフィグの切り戻し

リストア機能実行時に既存コンフィグを、装置フラッシュメモリにバックアップします。もし、リストアに問題があった場合、コンフィグ切り戻し機能でリストア前のコンフィグに戻すこともできます。

usbmem revert-config	バックアップファイルからコンフィグを元に戻す。 （グローバルコンフィグモード） （要再起動）

5.7.10.5 エラーログへの記録

リストア機能の実行は、装置エラーログ（show error-log）に記録されます。

INFO: System restore completed.	リストア機能の正常完了
INFO: System restore failed(Copy startup-config).	リストア失敗（startup-config のコピーに失敗）
INFO: System restore failed(Copy default-config).	リストア失敗（default-config のコピーに失敗）
INFO: System restore failed(Software update).	リストア失敗（ソフトウェアアップデートに失敗）
INFO: System restore failed(Log file).	リストア失敗（ログファイルの書き込み失敗）
INFO: Modify startup-config by system restore.	リストア機能により startup-config が書き換えられました。
INFO: Modify default-config by system restore.	リストア機能により default-config が書き換えられました。
INFO: Erase startup-config by system restore.	リストア機能により startup-config が削除されました。

INFO: Erase default-config by system restore.	リストア機能により default-config が削除されました。
INFO: System revert-config completed.	リストア機能のコンフィグ切り戻しを実行しました。
INFO: System revert-config failed.	リストア機能のコンフィグ切り戻しに失敗しました。

5.7.10.6 状態遷移と LED 表示

	状態	点灯パターン
①	リストア機能実行中 USB メモリにリストアファイルがあるかチェック ｜あり　　｜なし「File not found.」 ｜　　↓（最低 1 秒間 LED 表示） ｜　　②へ ↓ USB メモリへのログファイルを作成　　→ ③ ↓ 既存コンフィグを装置フラッシュメモリにバックアップ ↓ startup-config を更新　　→ ③ default-config を更新　　→ ③ ソフトウェアアップデート　　→ ③ ｜　　エラー発生時 ↓ コンフィグの更新、ソフトウェアアップデートが実施された ｜変更あり　　｜変更なし ↓（最低 10 秒間 LED 表示）　　↓ 自動的に再起動　　②へ	3 ◎ RSTR（点滅） 2 ● COPY（消灯） 1 ● EJCT （消灯）
②	通常動作	3 ○ RSTR（点灯） 2 ● COPY（消灯） 1 ○ EJCT （点灯）
③	実行エラー ↓（最低 30 秒間 LED 表示） ②へ	3 ◎ RSTR（点滅） 2 ○ COPY（点灯） 1 ◎ EJCT （点滅） ◎ ALM （赤点滅）

5.7.11 コマンドバッチ機能（USB ボタン機能）

USB メモリ内のバッチファイルを使用して、ファイルに記載されているコンフィグ・コマンドを 1 行ずつ実行します。

コマンドから、コマンドバッチ機能を実行することもできます。

usbmem command <USB デバイス名> usbmem command file <USB ファイル名>	USB ボタン機能のコマンドバッチ機能を実行する。 （グローバルコンフィグモード）

※ USB メモリの容量不足などで、実行ログファイルが作成できない場合は処理を終了します。
※ USB メモリの容量不足などで、実行ログファイルがバッチ処理実行中に追加書き込みできなくなった場合は処理を継続します。（ただし、以降の実行ログファイルへの出力は行われません。）
※ バッチファイルがバイナリデータのファイルであった場合はエラー終了します。
※ スケジューラ機能からこのコマンドを呼び出すことはできません。

※ バッチファイルから以下のコマンドは実行できません。
- usbmem eject
- usbmem copy
- usbmem restore
- usbmem command
- no usbmem enable
- usb host-reset
- event-terminal
- clear event
- shutdown （USB デバイスコンフィグモード）
- reset （USB デバイスコンフィグモード）
- scheduler execute（スケジューラの即時実行）
- scheduler resume（スケジューラの一時停止解除）
- scheduler suspend（スケジューラの一時停止）

5.7.11.1 USB メモリのファイル配置

コマンドバッチ機能では、USB メモリの該当ファイルを上から順番に検索します。

装置シリアル番号のディレクトリにファイルを配置することで、1 つの USB メモリで複数の装置に対して個別のコンフィグを配置することができます。（装置シリアル番号は、show hardware などであらかじめ取得しておきます。）

バッチファイル

/COMMAND/<装置シリアル番号>/command.cmd
/command.cmd

※ 両方のディレクトリにバッチファイルが配置されている場合は、装置シリアル番号ディレクトリに配置されているファイルのみ実行されます。

5.7.11.2 USB メモリに保存されるファイル

以下の USB のファイルに、バッチ処理実行時のログが保存されます。

実行ログ

/LOG/<装置シリアル番号>/<実行日時>_command-result.log

※ USB メモリの容量不足などで開始時に実行ログファイルが作成できない場合は処理を終了します。
※ USB メモリの容量不足などで処理の途中で実行ログファイルへの書き込みができなくなっても、バッチ処理は継続されます。（以降、実行ログファイルへの出力は行われません。）

5.7.11.3 状態遷移と LED 表示

	状態	点灯パターン
①	コマンドバッチ機能実行中 コマンド・コンフィグ読み出し ｜なし　↓あり　　↑次の行 ｜　　コマンド・コンフィグ実行　　→ ③ ｜　　エラー発生時 ↓（最低 10 秒間 LED 表示） ②へ	3 ○ RSTR（点灯） 2 ◎ COPY（点滅） 1 ○ EJCT （点灯）
②	コマンドバッチ機能完了	3 ○ RSTR（点灯） 2 ● COPY（消灯） 1 ○ EJCT （点灯）
③	実行エラー ↓（最低 30 秒間 LED 表示） ②へ	3 ◎ RSTR（点滅） 2 ○ COPY（点灯） 1 ◎ EJCT （点滅） ◎ ALM （赤点滅）

※ 大量のコマンドバッチファイルや、終了しないコマンドの実行など、10 分以内でコマンドバッチ機能が完了しない場合、エラー終了となります。

5.7.11.4 コマンドバッチ機能の強制終了

実行時間が長時間になるコマンドなどを行った場合に、コマンドバッチを強制終了させることができます。

usbmem command stop-request	コマンドバッチ機能に停止要求を送信します。（オペレーションモード）

※ コマンドバッチ機能で途中まで実行されたコマンド・コンフィグを元に戻す機能ではありません。

5.7.12 工場出荷状態装置のリストア機能

装置コンフィグの入っていない工場出荷状態の装置に、コンフィグやソフトウェアをあらかじめ入れた USB メモリを挿して装置起動させることで、自動的に USB メモリに保存してあるコンフィグを startup-config や default-config に書き込み、ソフトウェアアップデートを行います。

装置導入時における、PC レスでのコンフィグ書き込み、ソフトウェアバージョン固定などの要望に応えることができます。

※ 工場出荷装置のリストア機能で使用可能な USB ポートは USB0 のみです。（USB1 では動作しません）

5.7.12.1 USB メモリのファイル配置

工場出荷装置のリストア機能では、各コンフィグ、ソフトウェアに対して、あらかじめ USB メモリに保存しておいた、該当ファイルを上から順番に検索し、ファイルがあった場合にリストア、もしくはソフトウェアアップデートを実行します。

※ 装置シリアル番号のディレクトリにファイルを配置することで、1 つの USB メモリで複数の装置に対して個別のコンフィグを配置することができます。（装置シリアル番号は、show hardware などであらかじめ取得しておきます。）

装置リストアコンフィグ

startup-config へのリストア（上から順番に検索）

/RESTORE/<装置シリアル番号>/startup-config.cfg
/startup-config.cfg

default-config へのリストア（上から順番に検索）

/RESTORE/<装置シリアル番号>/default-config.cfg
/default-config.cfg

ソフトウェアアップデート

RAP ファイル（上から順番に検索）

/RESTORE/<装置シリアル番号>/software-update.rap
/software-update.rap

5.7.12.2 USB メモリに保存されるファイル

リストア時のログは以下のファイルに保存されます。

実行ログ

/LOG/<装置シリアル番号>/<実行日時>_restore-result.log

※ USB メモリの容量不足などで開始時に実行ログファイルが作成できない場合は処理を終了します。
※ USB メモリの容量不足などで処理の途中で実行ログファイルへの書き込みができなくなっても、リストア処理は継続されます。（以降、実行ログファイルへの出力は行われません。）

5.7.12.3 エラーログへの記録

リストア機能の実行ログは、装置エラーログ（show error-log）にも記録されます。

※ リストア機能（USB ボタン機能）を参照してください

5.7.12.4 状態遷移と LED 表示

	状態	点灯パターン USB0
①	電源 ON ↓ 装置コンフィグの存在チェック → ③ ↓ USB0 に USB メモリが挿さっているかチェック → ③ ↓（最大 20 秒間） ②へ	3 ● RSTR（消灯） 2 ● COPY（消灯） 1 ● EJCT （消灯）
②	USB メモリにリストアファイルがあるかチェック → ③ ↓ USB メモリへのログファイルを作成 ↓ startup-config リストア default-config リストア ソフトウェアアップデート ｜ ↓（最低 10 秒間 LED 表示） 自動的に再起動	3 ◎ RSTR（点滅） 2 ● COPY（消灯） 1 ● EJCT （消灯）
③	通常起動	3 ● RSTR（消灯） 2 ● COPY（消灯） 1 ● EJCT （消灯）
④	実行エラー ↓（5 分間表示） ③へ ※エラーLED 点滅状態で電源 OFF、USB 抜去が可能です。	3 ◎ RSTR（点滅） 2 ○ COPY（点灯） 1 ◎ EJCT （点滅） ◎ ALM （点滅）

※ USB メモリが挿さっているかチェックしている間（最大 20 秒間）に、ユーザがコンフィグモードに入った場合、リストア機能は終了し、通常起動となります。

5.7.13 USB メモリ認証・セキュリティ

USB メモリを有効にすると、誰でも USB ボタン機能を利用して装置情報を簡単に取得・変更することが可能となります。便利になる反面、外部からの不正アクセスに対して、無防備になります。
ここでは、かんたん操作ボタンの無効化や、使用可能な USB メモリを制限する方法、USB メモリの利用状況、不正アクセスの確認方法を記載します。

5.7.13.1 かんたん操作ボタン（SEL／ENT ボタン）の無効化

USB メモリを有効にすると、デフォルトでかんたん操作ボタン（SEL／ENT ボタン）も有効となります。USB メモリは使用したいが、かんたん操作ボタンは使用されたくない場合は以下のコマンドで無効にします。

no usbmem button enable	かんたん操作ボタンを無効化する。 （グローバルコンフィグモード）

※ USB ボタンを無効化しても、コマンドによる USB ボタン機能自体は利用可能です。

5.7.13.2 利用可能な USB メモリの制限

USB メモリの固有の、ベンダ ID、プロダクト ID、シリアルナンバー、USB メモリにあらかじめ保存しておいたパスワードファイルにより利用可能な USB メモリを制限することができます。

usbmem authentication	利用可能な USB メモリを制限します。 （グローバルコンフィグモード） ※16 個までの設定をサポート

USB メモリのベンダ ID、プロダクト ID、シリアルナンバーは、show hardware、もしくは、USB メモリ挿入時のイベントログで確認することができます（次項を参照してください）。

【設定例】

コンフィグ例
```
!
usbmem authentication vendor-id 0000 product-id 0000 serial-number 00000000000
usbmem authentication password-file usb_auth.dat plain abcdefghijklmnopqrstuvwxyz
!
```

パスワードファイル例（/usb_auth.dat）
```
abcdefghijklmnopqrstuvwxyz
```

※USB メモリのルートディレクトリに設定したパスワードファイルを作り、コマンドで指定したパスワードを 1 行目に記載しておく。

※ USB メモリによっては、シリアルナンバーが入っていないことがあります。
※ USB メモリによっては、複数の製品で同じシリアルナンバーが登録されていることがあります。
※ service password-encryption を使用すると、パスワードファイルによる認証において、show running-config で表示されるパスワード部分が暗号化されます。パスワードファイルには、暗号化される前のパスワードを指定する必要があります。

5.7.13.3 USB 認証失敗時の LED 表示

	状態	点灯パターン
①	USB メモリ認証失敗 ↓（最低 30 秒間 LED 表示） ②へ	3 ◎ RSTR（点滅） 2 ○ COPY（点灯） 1 ◎ EJCT （点滅） ◎ ALM （赤点滅）
②	USB はマウントされていない状態（利用不可能状態）	3 ● RSTR（消灯） 2 ● COPY（消灯） 1 ● EJCT （消灯）

5.7.13.4 USB メモリのログ確認

USB メモリの挿入・抜去、USB ボタン機能の実行は、イベントログの warn で表示されます。必要に応じて syslog などで運用情報を記録することができます。

logging subsystem usb <LEVEL>	USB のイベントログを設定します。 （グローバルコンフィグモード）

【イベントログ表示例】

<USB メモリ認証失敗>

USB.022: USB memory authentication failure on USB0, vendor id is <ベンダ ID>, product id is <プロダクト ID>, serial number is <シリアルナンバー>

<USB メモリの挿入>

USB.023: USB memory has been inserted on USB0, vendor id is <ベンダ ID>, product id is <プロダクト ID>, serial number is <シリアルナンバー>

<USB メモリの抜去>

USB.024: USB memory has been ejected on USB0, vendor id is <ベンダ ID>, product id is <プロダクト ID>, serial number is <シリアルナンバー>

<USB ボタン機能の実行>

USB.025: USB button copy is executed on USB0
USB.025: USB button restore is executed on USB0
USB.025: USB button command is executed on USB0
USB.025: USB button eject is executed on USB0

5.7.14 スケジューラ機能と連携したログの保存

スケジューラ機能と連携することで USB メモリに定期的なログの保存ができます。Ver9.1 以降では、スケジューラ機能のマクロ文字列の展開により、保存ディレクトリやファイル名、作成時間などを含めたログの保存が可能となっています。

command	スケジューラ実行コマンドの設定 （アクションリストコンフィグモード） 使用可能なマクロ文字列 <HOSTNAME> ... 装置のホスト名 <SN> ... 装置のシリアル番号 <YEAR> ... コマンド実行の年（2015 など） <MONTH> ... コマンド実行の月（01 など） <DATE> ... コマンド実行の日（27 など） <TIME> ... コマンド実行の時分秒（131203 など）

【設定例】一時間に 1 回、USB メモリの/log/<SN>/<YEAR><MONTH><DATE>/ に、show tech-support と show logging のログを保存する。

```
!
usbmem enable
!
scheduler timetable usbmem interval hour 1
command-action list usbmem
   command 10 show tech-support output usbmem0:/log/<SN>/
<YEAR><MONTH><DATE>/<YEAR><MONTH><DATE><TIME>_tech.log
   command 20 show logging output usbmem0:/log/<SN>/
<YEAR><MONTH><DATE>/<YEAR><MONTH><DATE><TIME>_logging.log
!
device USB0
   no shutdown
!
```

※ マクロ文字の展開機能は、スケジューラの機能となりますので、グローバルコンフィグモードなどで show tech-support や show logging のコマンドとしてマクロ文字を指定しても、文字列展開はされません。

※ USB メモリの 1 つのディレクトリに大量にファイルを保存された状態で使用すると、著しく装置負荷が上がることがあります。1 つのディレクトリ内のファイル数は 100 個程度を上限として、分散保存されるよう調整してください。

※ show tech-support output は、FLASH メモリも指定可能であるため、本機能の連携実行が可能となりますが、FLASH メモリは格納可能なファイル数、容量、書込速度などにより利用が大幅に制限されます。

■5.8 コンフィグ引継ぎ

5.8.1 IX2004/IX2005 コンフィグ引継ぎ

Ver10.4 以降、IX2106/IX2107 へ IX2004 および IX2005 のコンフィグを引き継ぐことができます。

5.8.1.1インタフェース/デバイス名変換

IX2106/IX2107 に IX2004/IX2005 のインタフェース名・デバイス名を含む設定コンフィグを入力した場合、以下の対応表のように置換され設定されます。

デバイス名対応表

物理ポート名称	IX2004/IX2005 デバイス名	IX2106/IX2107 デバイス名
FE0.0 ポート （基本インタフェース）	FastEthernet0	GigaEthernet0
FE1.0 ポート （基本インタフェース）	FastEthernet1	GigaEthernet1

インタフェース名対応表

物理ポート名称	IX2004/IX2005 インタフェース名	IX2106/IX2107 インタフェース名
FE0.0 ポート （基本インタフェース）	FastEthernet0.0	GigaEthernet0.0
FE0.0 ポート （サブインタフェース）	FastEthernet0.[1-32]	GigaEthernet0.[1-32]
FE1.0 ポート （基本インタフェース）	FastEthernet1.0	GigaEthernet1.0
FE1.0 ポート （サブインタフェース）	FastEthernet1.[1-32]	GigaEthernet1.[1-32]
FE1.0 ポート （VLAN インタフェース）	FastEthernet1:[0-4].[0-8]	GigaEthernet1:[0-4].[0-8]

5.8.1.2注意事項

以下のコマンドは設定を引き継ぐことはできません。

- ipv6 スコープ識別子((ipv6 アドレス%インタフェース名)の設定を含むコマンド
- http-server wol-username
- webcon upload-refresh

コマンド一覧

コマンド	設定例
ipv6 route	ipv6 route 2001:db8:1::/64 fe80::1%FastEthernet0.0 ipv6 route default fe80::1%FastEthernet0.0
ipsec autokey-map	ipsec autokey-map auto1 alist1 peer fe80::1%FastEthernet0.0
ipsec manualkey-map	ipsec manualkey-map kotei1 alist1 peer fe80::1%FastEthernet0.0 none mkey4/800/
ike policy	ike policy ipolicy1 peer fe80::1%FastEthernet0.0 key pkey1234 default
action ipv6 resume-route	action 30 ipv6 resume-route 2001:db8::/64 fe80::1%FastEthernet0.0
action ipv6 shutdown-route	action 40 ipv6 shutdown-route 2001:db8::/64 fe80::1%FastEthernet0.0
event ipv6 reach-host	event 10 ipv6 reach-host fe80::1%FastEthernet0.0 Tunnel0.0 event 20 ipv6 reach-host 2001:db8:1::1 Tunnel0.0 fe80::1%FastEthernet0.0
event ipv6 reach-route	event 10 ipv6 reach-route 2001:db8:1::1/24 fe80::1%FastEthernet0.0
event ipv6 unreach-host	event 10 ipv6 unreach-host fe80::1%FastEthernet0.0 Tunnel0.0 event 20 ipv6 unreach-host 2001:db8:1::1 Tunnel0.0 fe80::1%FastEthernet0.0
event ipv6 unreach-route	event 10 ipv6 unreach-route 2001:db8:1::1/24 fe80::1%FastEthernet0.0
snmp-agent ipv6 host	snmp-agent ipv6 host fe80::1%FastEthernet0.0 com_pub version 2
proxy-dns server	proxy-dns server fe80::1%FastEthernet0.0
ipv6 name-server	ipv6 name-server fe80::1%FastEthernet0.0
syslog ipv6 host	syslog ipv6 host fe80::1%FastEthernet0.0
ping6	ping6 fe80::1%FastEthernet0.0
traceroute6	traceroute6 fe80::1%FastEthernet0.0
http-server wol-username	http-server wol-username test
webcon upload-refresh	webcon upload-refresh 600

6章 ルーティング状態確認

本章では、IX2000/IX3000 シリーズのルーティング設定、動作状態の確認方法について説明します。

■6.1 物理/リンクレイヤの状態確認

下記に示すコマンドにより、デバイスやインタフェースの状態が確認できます。

コマンド	確認項目
show devices	デバイス状態 ・デバイス名 ・運用の状態 ・動作情報 ・設定情報　など

コマンド	確認項目
show interfaces	インタフェース状態 ・インタフェース名 ・管理/運用の状態 ・動作情報 ・設定情報　など

■6.2 IPv4 レイヤの状態確認

IPv4 のレイヤ情報として確認可能な項目を示します。

6.2.1 IPv4 レイヤの状態確認

下記に示すコマンドにより、IPv4 レイヤの状態を確認することができます。

コマンド	確認項目
show ip interface	IPv4 インタフェース状態
show ip address	IPv4 アドレス状態 ・IPv4 インタフェース状態 ・IPv4 アドレス

6.2.2 ARP 情報の確認

下記に示すコマンドにより、ARP 情報を確認できます。

コマンド	確認項目
show arp entry show arp neighbors	近隣探索情報

■6.3 IPv6 レイヤの状態確認

IPv6 のレイヤ情報として確認可能な項目を示します。

6.3.1 IPv6 レイヤの状態確認

下記に示すコマンドにより、IPv6 レイヤの状態を確認することができます。

コマンド	確認項目
show ipv6 interface	インタフェース状態
show ipv6 address	IPv6 アドレス状態 ・インタフェース状態 ・IPv6 アドレス

6.3.2 近隣探索情報の確認

下記に示すコマンドにより、近隣探索情報を確認することができます。

コマンド	確認項目
show ipv6 neighbor-discovery	近隣探索情報
show ipv6 neighbors	近隣キャッシュの情報

6.3.3 マルチキャストリスナ情報の確認

下記に示すコマンドにより、同一リンク上のマルチキャストアドレスを用いた送受信が可能な装置（マルチキャストリスナ）を確認することができます。

コマンド	確認項目
show ipv6 mld status show ipv6 multicast-listener-discovery	マルチキャストリスナ情報
show ipv6 mld listeners show ipv6 multicast-listeners	マルチキャストリスナキャッシュの情報

■6.4 ルーティング情報の状態確認

IPv4/IPv6 のルーティング情報として確認可能な項目を示します。

6.4.1 ルーティングテーブルの確認

下記に示すコマンドにより、ルーティング情報の状態を確認することができます。

コマンド	確認項目
show ip route	IPv4 ルーティングテーブル ・経路種別 ・送信先アドレスまたはネットマスク長 （プレフィックス長） ・メトリック値 ・ネクストホップアドレス ・出力インタフェース　など
show ip cache	IPv4 ルートキャッシュ情報 ・送信元アドレス ・送信先アドレス ・プロトコル ・ネクストホップアドレス ・出力インタフェース　など
show ip protocols	IPv4 ルーティング情報 ・ルートエントリ数 ・ルーティングプロトコル状態
show ipv6 route	IPv6 ルーティングテーブル ・経路種別 ・送信先アドレスまたはプレフィックス長 ・メトリック値 ・ネクストホップアドレス ・出力インタフェース　など
show ipv6 cache	IPv6 ルートキャッシュ情報 ・送信元アドレス ・送信先アドレス ・プロトコル ・ネクストホップアドレス ・出力インタフェース　など
show ipv6 protocols	IPv6 ルーティング情報 ・ルートエントリ数 ・ルーティングプロトコル状態

6.4.2 RIPv1/v2 プロトコルの状態確認

下記に示すコマンドにより、RIP プロトコルの状態を確認することができます。

コマンド	確認項目
show ip rip	RIP で運用されている情報（サマリ） ・有効無効 ・送信先アドレスまたはネットマスク長 （プレフィックス長）

show ip rip interface	RIP で運用されている詳細情報 ・RIP バージョン ・認証タイプ ・スプリットタイプ　など
show ip rip peer-information	隣接ルータに関する情報 ・インタフェース ・隣接ルータのアドレス ・統計情報　など
show ip rip database	インタフェース毎の経路情報 ・送信している経路の確認

6.4.3 RIPng プロトコルの状態確認

下記に示すコマンドにより、RIPng プロトコルの状態を確認することができます。

コマンド	確認項目
show ipv6 rip	RIPng で運用されている情報（サマリ） ・有効無効 ・送信先アドレスまたはネットマスク長 （プレフィックス長）
show ipv6 rip interface	RIPng で運用されている詳細情報 ・インタフェース状態 ・統計情報　など
show ipv6 rip peer-information	隣接ルータに関する情報 ・インタフェース ・隣接ルータのアドレス ・統計情報　など
show ipv6 rip database	インタフェース毎の経路情報 ・送信している経路の確認

6.4.4 OSPFv2 プロトコルの状態確認

下記に示すコマンドにより、OSPF プロトコルの状態を確認することができます。

コマンド	確認項目
show ip ospf area	OSPF で使用されているエリア情報
show ip ospf database	OSPF で使用されている リンクステートデータベース情報 ・Router-LSA 情報 ・Network-LSA 情報 ・Summary-LSA 情報 ・AS-external-LSA 情報
show ip ospf interface	OSPF で設定されている詳細情報 ・有効無効 ・インタフェース ・プロセス ID ・エリア ID ・DR/BDR 情報　など

show ip ospf neighbor	隣接ルータに関する情報 ・インタフェース ・隣接ルータのアドレス ・状態情報　など

6.4.5 OSPFv3 プロトコルの状態確認

下記に示すコマンドにより、OSPF プロトコルの状態を確認することができます。

コマンド	確認項目
show ipv6 ospf area	OSPF で使用されているエリア情報
show ipv6 ospf border-routers	ABR,ASBR 情報
show ipv6 ospf database	OSPF で使用されている リンクステートデータベース情報 ・Router-LSA 情報 ・Network-LSA 情報 ・Summary-LSA 情報 ・AS-external-LSA 情報
show ipv6 ospf interface	OSPF で設定されている詳細情報 ・有効無効 ・インタフェース ・プロセス ID ・エリア ID ・DR/BDR 情報　など
show ipv6 ospf neighbor	隣接ルータに関する情報 ・インタフェース ・隣接ルータのアドレス ・状態情報　など
show ipv6 ospf process	OSPF プロセスに関する情報 ・エリア数 ・LSA 数　など

6.4.6 BGP4 プロトコルの状態確認

下記に示すコマンドにより、BGP プロトコルの状態を確認することができます。

コマンド	確認項目
show ip bgp	BGP で学習した経路情報 ・ネットワーク ・ネクストホップ ・メトリック　など
show ip bgp neighbors	BGP ピア情報 ・ピアのアドレス ・ピアのケイパビリティ ・統計情報　など
show ip bgp summary	BGP ピア情報の要約 ・ピアのアドレス ・状態　など
show ip bgp paths	BGP のパス情報

■6.5 到達および経路確認

IPv4 の到達可能性確認は、ping コマンドを使用し、IPv6 の到達可能性確認は、ping6 コマンドを使用することにより行います。

また、IPv4 のパケット送信経路確認は、traceroute コマンドを使用し、IPv6 のパケット送信経路確認は、traceroute6 コマンドを使用することにより行います。

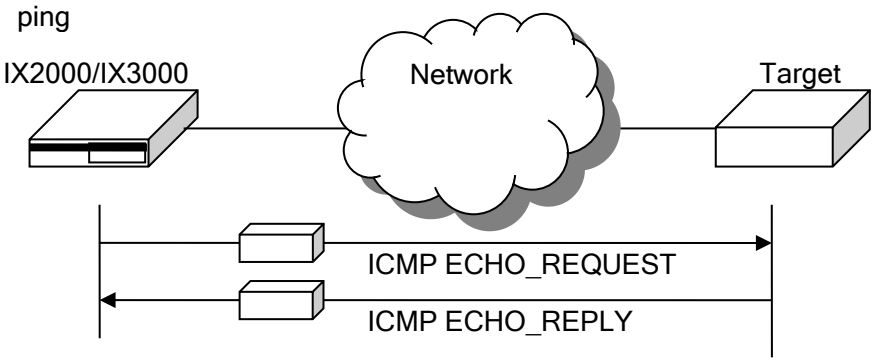
IPv4/IPv6 ともに、これらのコマンドは宛先指定にホスト名を使用することができます。DHCP や IPCP 等で自動的に DNS サーバを取得していない場合には、ip name-server コマンドで DNS サーバを指定する必要があります。詳細は DNS の節を参照してください。

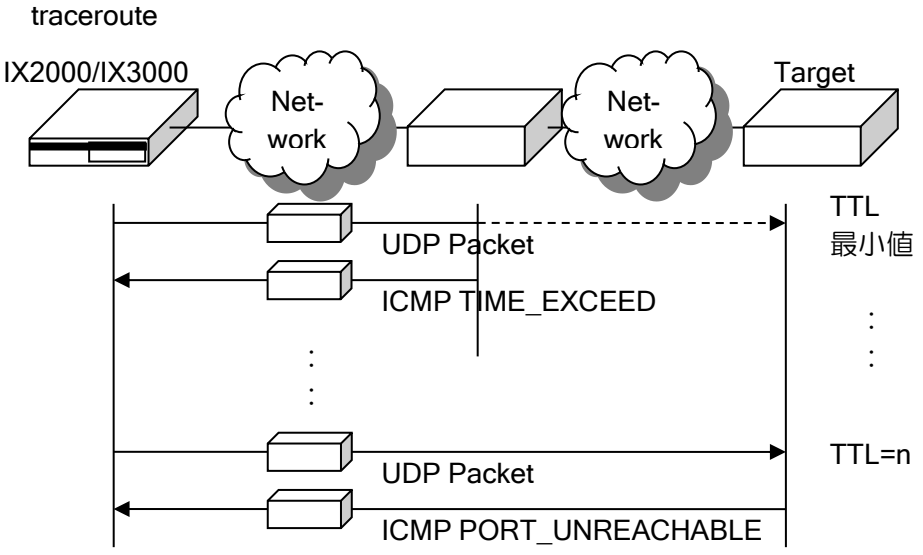
6.5.1 IPv4 到達および経路確認

IPv4 の到達可能性確認は、ping コマンドを使用し、ICMP ECHO_REQUEST パケットを送出することにより行います。

また、IPv4 の経路確認は、traceroute コマンドを使用します。TTL（Time To Live）を最小値でターゲットノードまで UDP のデータパケットを送出し、途中経路から ICMP TIME_EXCEED を受信します。徐々に TTL 値を増加させ同じように ICMP TIME_EXCEED を受信します。最終的に、ターゲットノードから ICMP PORT_UNREACHABLE を受信することにより判定します。

以下に、ping、traceroute の基本操作について説明します。





(a) ping 基本操作

ping コマンド実行時には送信先とともに下記を設定することができます。また送信先にはアドレスのほか、ドメイン名を指定することも可能です。(ip name-server コマンドでサーバを指定しておく必要があります。)

- リクエスト回数
- 転送するデータサイズ
- 送信元アドレス
- タイムアウト時間
- ホップリミット値

【設定例】

次の条件で到達確認を行います。

```
到達先ノード          : 192.168.24.3
リクエスト回数        : 256 回
送信データサイズ      : 128 バイト
タイムアウト時間      : 2 秒
ホップリミット値      : 64

ping 192.168.24.3 count 256 hop-limit 64 size 128 wait 2
```

(b) traceroute 基本操作

traceroute コマンド実行時には送信先とともに下記を設定することができます。また送信先にはアドレスのほか、ドメイン名を指定することも可能です。(ip name-server コマンドでサーバを指定しておく必要があります。)

- 最初に表示するルートまでのホップ数
- ホップリミット値

【設定例】

次の条件で到達確認を行います。

```
到達先ノード                        : 192.168.24.3
最初に表示するルートまでのホップ数  : 10
ホップリミット値                    : 64

traceroute 192.168.24.3 firsthop 10 hop-limit 64
```

UDP の送信先ポートは 33436～33690 を使用します。初期値が 33436 でホップ数が増えるごとに 1 加算されます。送信元ポートは不定のランダム値を使用します。

途中の経路からの応答に記号が表示される場合があります。

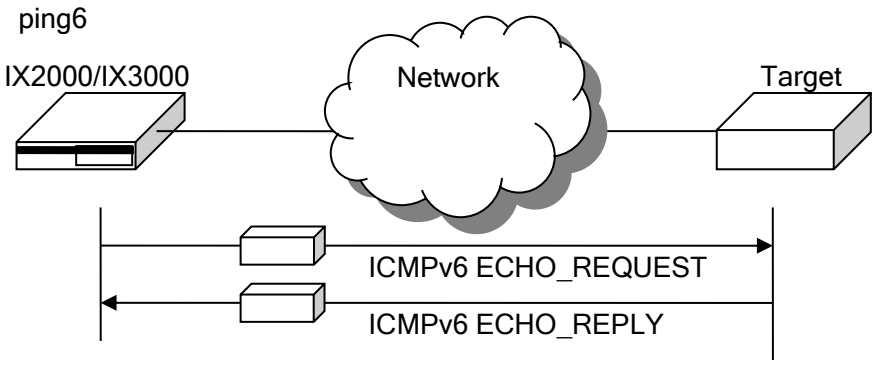
!N	Net Unreachable の ICMP Error 応答がありました。
!H	Host Unreachable の ICMP Error 応答がありました。
!P	Protocol Unreachable の ICMP Error 応答がありました。
!	Port Unreachable の ICMP Error 応答がありました。

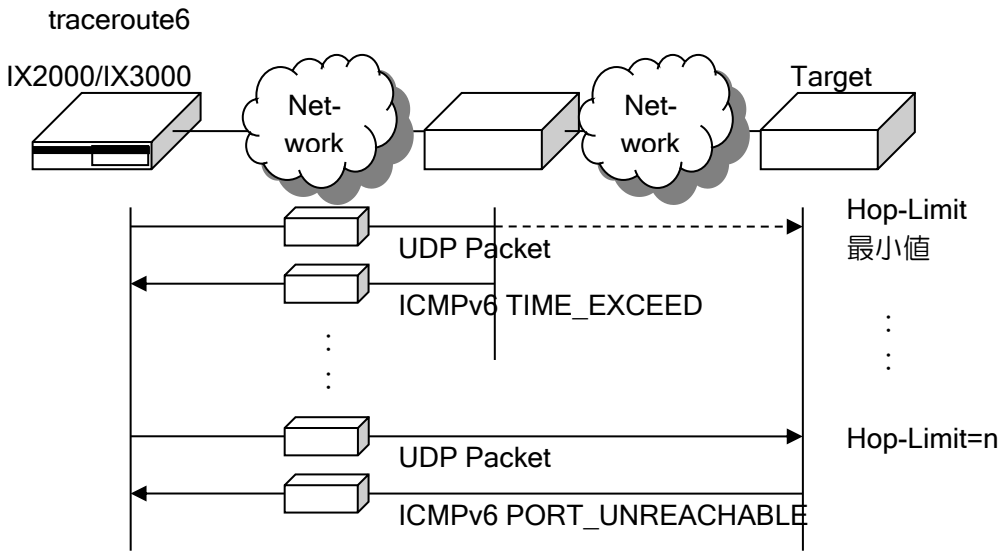
6.5.2 IPv6 到達および経路確認

IPv6 の到達可能性確認は、ping6 コマンドを使用し、ICMPv6 ECHO_REQUEST パケットを送出することにより行います。

また、IPv6 の経路確認は、traceroute6 コマンドを使用します。Hop-Limit を最小値でターゲットノードまで UDP のデータパケットを送出し、途中経路から ICMPv6 TIME_EXCEED を受信します。徐々に Hop-Limit 値を増加させ同じように ICMPv6 TIME_EXCEED を受信します。最終的に、ターゲットノードから ICMPv6 PORT_UNREACHABLE を受信することにより判定します。

以下に、ping6、traceroute6 の基本操作について説明します。





(a) ping6 基本操作

ping6 コマンド実行時には送信先とともに下記を設定することができます。また送信先にはアドレスのほか、ドメイン名を指定することも可能です。（ipv6 name-server コマンドでサーバを指定しておく必要があります。）

- リクエスト回数
- 転送するデータサイズ
- 送信元アドレス
- タイムアウト時間
- ホップリミット値

【設定例】

次の条件で到達確認を行います。

到達先ノード　　: FastEthernet0/0.0 の fe80::200:4cff:fe00:1501
リクエスト回数　　: 256 回
送信データサイズ　　: 256 バイト
タイムアウト時間　　: 2 秒
ホップリミット値　　: 64

```
ping6 fe80::200:4cff:fe00:1501%FastEthernet0/0.0 count 256
        hop-limit 64 size 256 wait 2
```

(b) traceroute6 基本操作

traceroute6 コマンド実行時には送信先とともに下記を設定することができます。また送信先にはアドレスのほか、ドメイン名を指定することも可能です。（ipv6 name-server コマンドでサーバを指定しておく必要があります。）

- 最初に表示するルートまでのホップ数
- ホップリミット値

【設定例】

次の条件で到達確認を行います。

到達先ノード　　: 2001:db8::1
最初に表示するルートまでのホップ数　: 10
ホップリミット値　　: 64

```
traceroute6 2001:db8::1 firsthop 10 hop-limit 64
```

途中の経路からの応答に記号が表示される場合があります。

!N	no route to destination の ICMP Error 応答がありました。
!H	address unreachable の ICMP Error 応答がありました。
!	port unreachable の ICMP Error 応答がありました。

■6.6 隣接ノードのアドレス調査方法

隣接ノードのアドレスの調査は、IPv6 のみで使用することができます。

隣接ノードの IPv6 リンクローカルアドレスの調査方法
隣接ノードのリンクローカルアドレスは、送信先アドレスにマルチキャストアドレスを指定した ping6 コマンドを実行することにより調査できます。

【設定例】

(1) リンク上の全ノードのリンクローカルアドレス調査
全ノードのマルチキャストアドレスを送信先アドレスとして使用します。

対象となるリンク
インタフェース名　　: FastEthernet0/0.0

ping6 ff02::1%FastEthernet0/0.0

(2) リンク上の全ルータのリンクローカルアドレス調査
全ルータのマルチキャストアドレスを送信先アドレスとして使用します。

対象となるリンク
インタフェース名　　: FastEthernet0/0.0

ping6 ff02::2%FastEthernet0/0.0

7章 遠隔設定と監視

本章では、IX2000/IX3000 シリーズの遠隔設定と監視方法について説明します。

■7.1 telnet を利用した遠隔設定

IX2000/IX3000 シリーズでは、telnet 機能による遠隔からの設定ができます。
詳細なログデータを telnet クライアントに出力することで、ネットワークトラブル等の解析ができるようになります。

Ver.9.5 以前では telnet の機能を装置全体でしか有効に出来ませんでしたが、Ver.9.6 以降ではインタフェースコンフィグモードに enable コマンドを設定することで特定のインタフェースでのみ機能を有効にすることができます。
意図しないインタフェースへの telnet を防止することが可能です。

Ver.10.2 からログインセキュリティ機能強化のため、装置にユーザ名とパスワードを設定していない場合、telnet による接続ができません。そのため、telnet を使用して装置に接続する場合は、あらかじめ装置にログインするためのユーザ名とパスワードを設定しておく必要があります。

telnet サーバの設定および確認は次のコマンドを使用します。

telnet-server ip enable	IPv4 用 telnet サーバの起動
telnet-server ip access-list	IPv4 用 telnet サーバへのアクセス制限
telnet-server ip port	IPv4 用 telnet サーバの受信ポートを変更

telnet-server ipv6 enable	IPv6 用 telnet サーバの起動
telnet-server ipv6 access-list	IPv6 用 telnet サーバへのアクセス制限
telnet-server ipv6 port	IPv6 用 telnet サーバの受信ポートを変更

次に、192.168.10.10 の telnet クライアントのみ、telnet サーバへのアクセスを許可する場合の例を示します。telnet サーバでは、アクセスリストは src のみ判定の対象にしていますので、dest は無視して動作します。

【設定例】

```
ip access-list telnet4 permit ip src 192.168.10.10/32 dest any
telnet-server ip enable
telnet-server ip access-list telnet4
```

- telnet 送信パケットサイズ

show コマンドなどでデータを表示させると、約 500 バイトに到達するか、あるいは約 1/60 秒間の時間が経た際にデータがまとめて送信されます。

■7.2 SSH を利用した遠隔設定

7.2.1 SSH サーバの設定

Ver.8.7 以降 IX2000/IX3000 シリーズでは、SSH サーバ機能に対応しています。
SSH では通信が暗号化されるため、より安全に遠隔からの操作ができるようになります。

Ver.9.5 以前では SSH の機能を装置全体でしか有効に出来ませんでしたが、Ver.9.6 以降ではインタフェースコンフィグモードに enable コマンドを設定することで特定のインタフェースでのみ機能を有効にすることができます。
意図しないインタフェースへの SSH を防止することが可能です。

Ver.10.2 からログインセキュリティ機能強化のため、装置にユーザ名とパスワードを設定していない場合、SSH による接続ができません。そのため、SSH を使用して装置に接続する場合は、あらかじめ装置にログインするためのユーザ名とパスワードを設定しておく必要があります。

SSH サーバの設定および確認は次のコマンドを使用します。

ssh-server ip enable	IPv4 用 SSH サーバの起動
ssh-server ip access-list	IPv4 用 SSH サーバへのアクセス制限
ssh-server ip port	IPv4 用 SSH サーバの受信ポートを変更
ssh-server ipv6 enable	IPv6 用 SSH サーバの機能 (Ver8.9 以降)
ssh-server ipv6 access-list	IPv6 用 SSH サーバへのアクセス制限 (Ver8.9 以降)
ssh-server ipv6 port	IPv6 用 SSH サーバの受信ポートを変更 (Ver8.9 以降)
ssh-server key-exchange compatibility	旧鍵交換アルゴリズム有効化設定 (Ver9.4 以降)
ssh-server encryption compatibility	旧暗号アルゴリズム有効化設定 (Ver10.6 以降)
ssh-server mac compatibility	旧 MAC アルゴリズム有効化設定 (Ver10.6 以降)

次に、192.168.10.10 の SSH クライアントのみ、SSH サーバへのアクセスを許可する場合の例を示します。SSH サーバでは、アクセスリストは src のみ判定の対象にしていますので、dest は無視して動作します。

【設定例】
SSH サーバを有効化し、192.168.10.10 からのアクセスのみ許可する。

```
ip access-list ssh4 permit ip src 192.168.10.10/32 dest any
ssh-server ip enable
ssh-server ip access-list ssh4
```

7.2.2 秘密鍵の操作

SSH サーバ機能では、サーバ認証には公開鍵認証を使用します。このため、秘密鍵が必要となります。SSH サーバ機能を使用する前に、IX2000/IX3000 において秘密鍵を生成します。装置交換等の場合は、再度鍵を生成するか、または、エクスポート、インポートにより鍵の保存、復元を行います。

pki private-key generate	秘密鍵の生成
pki private-key erase	秘密鍵の削除

秘密鍵は、秘密鍵の生成コマンドにより生成します。

生成した鍵は” SYSTEM-PRIVATE-KEY ”という名称でフラッシュメモリに書き込まれます。

” SYSTEM-PRIVATE-KEY ”ファイルは通常のコマンドにより操作することはできません。削除する場合は秘密鍵の削除コマンドを使用してください。

Ver10.1 以降では、ssh-server ip/ipv6 enable を設定した際に秘密鍵が存在しなければ、自動で秘密鍵の生成を行います。

【操作例】
秘密鍵の生成

```
(config)# pki private-key generate rsa
Generating RSA private key .....
(config)# show flash
Codes: M - Main-side, B - Backup-side, N - Newfile, R - Runnable
           A - Active-file, + - Next-boot, * - Bootmode-entry
Length       Name                                Status
8169726       ix2207-ms-10.2.21.ldc              MA
1766          SYSTEM-PRIVATE-KEY
```

- 注意事項

秘密鍵はフラッシュメモリに保存されています。このため、装置交換時は再度秘密鍵を生成する必要があります。装置交換後も同じ秘密鍵を使用する場合は、秘密鍵をエクスポートし、交換後の装置にインポートを行ってください。

pki private-key export	秘密鍵のエクスポート
pki private-key import	秘密鍵のインポート

秘密鍵の保存はエクスポートコマンドを使用します。エクスポートコマンドにより、秘密鍵をファイルまたは、画面への出力を行うことができます。ファイルに出力した場合は TFTP、copy コマンドにより、別ホストへ転送します。画面に出力した場合は出力内容を記録してください。

【操作例】
鍵をファイルに出力

```
(config)# pki private-key export bundle crypto test file key-file
(config)#
```

RSA の鍵を画面に出力

```
(config)# pki private-key export pem rsa crypto test
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,C88D0E3BE455D7D5A26E4DEB57025E9B

y8RdxHKX3DTx1/4g1qLNnRPhHswIdzRhHztr3W6giRFOt5+iyxxeDCtP3eaSddOy
```

```
+g3cM6oXmtyEcV9SFuX3UmeBezzrSoKEg1WfPTZmHRyvbcb5QkpQIBsf29L0YUKb
      :
k5qVfOkMKxuFJKe8/kYl5E33XbtNIQ5S6TKNdehNmxvej+bnKIEXUpWjC2Xbrs8K
Aetg25hZRt5QzcmMcd62SrUofG2WHIJ8HHgCRJ0MiwscA3YBMAbp8J3iJqNQvN8P
-----END RSA PRIVATE KEY-----
(config)#
```

秘密鍵の復元にはインポートコマンドを使用します。エクスポートにより出力したファイルを IX2000/IX3000 へ転送し、転送したファイルをインポートコマンドで指定するか、エクスポートで出力した内容をインポートコマンド実行時に指定することにより、秘密鍵を復元できます。

```
【操作例】
バンドルファイル形式のファイルを使用して鍵を復元
(config)# pki private-key import bundle crypto test file key-file
(config)#

コマンドを実行し、予めテキストに保存した鍵を画面上に貼り付け鍵を復元
(config)# pki private-key import pem rsa crypto test
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-256-CBC,C88D0E3BE455D7D5A26E4DEB57025E9B

y8RdxHKX3DTx1/4g1qLNnRPhHswIdzRhHztr3W6giRFOt5+iyxxeDCtP3eaSddOy
+g3cM6oXmtyEcV9SFuX3UmeBezzrSoKEg1WfPTZmHRyvbcb5QkpQIBsf29L0YUKb
      :
k5qVfOkMKxuFJKe8/kYl5E33XbtNIQ5S6TKNdehNmxvej+bnKIEXUpWjC2Xbrs8K
Aetg25hZRt5QzcmMcd62SrUofG2WHIJ8HHgCRJ0MiwscA3YBMAbp8J3iJqNQvN8P
-----END RSA PRIVATE KEY-----
(config)#
```

7.2.3 仕様

SSH サーバ仕様		
対応バージョン	SSHv2	
鍵交換アルゴリズム	Ver.9.2 以降	diffie-hellman-group-exchange-sha256
	Ver.9.1 以前	diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1
暗号アルゴリズム	Ver.10.6 以降	aes256-ctr,aes192-ctr,aes128-ctr
	Ver.10.5 以前	aes256-ctr,aes192-ctr,aes128-ctr, aes256-cbc,aes192-cbc,aes128-cbc, 3des-cbc
MAC アルゴリズム	Ver.10.6 以降	hmac-sha2-512,hmac-sha2-256
	Ver.10.5 以前	hmac-sha1,hmac-sha1-96, hmac-md5,hmac-md5-96
認証方式	サーバ認証	RSA／DSA
	クライアント認証	認証なし／パスワード認証
秘密鍵仕様		
鍵長	RSA（2048bit）／DSA（1024bit）	

■7.3 SNMP を利用した監視

IX2000/IX3000 シリーズでは、IPv4、IPv6 管理オブジェクトを実装しています。

したがって、SNMP（Simple Network Management Protocol）を使用することにより、IPv4 および IPv6 の動作状態を遠隔監視することができます。IX2000/IX3000 の機種ごとの sysObjectID については設定パラメータの一覧を参照してください。

IPv6 での管理オブジェクトへのアクセスにも対応しています

7.3.1 Trap と管理オブジェクト

IX2000/IX3000 シリーズで監視可能な Trap と管理オブジェクトを下記に示します。

(a) Trap

generic-trap

Trap-ID	内容	備考
0	cold-start	RFC1215
1	warm-start	RFC1215
2	link-down	RFC1215
3	link-up	RFC1215
4	authentication-failure	RFC1215

※ warm-start は SNMP で送信されません。

enterpriseSpecific

Trap-ID		内容	備考
vrrpNotifications	1	vrrpTrapNewMaster	RFC2787
vrrpNotifications	2	vrrpTrapAuthFailure	RFC2787
pico （*1）	3	temperature-fault	温度アラーム発生
pico （*1）	4	temperature-restoration	温度アラーム復旧
pico （*1）	5	voltage-fault	電圧異常発生
pico （*1）	6	voltage-restoration	電圧異常復旧
pico （*1）	7	picoFanFault	ファン異常発生 (IX3000 シリーズ、IX2310)
pico （*1）	8	picoFanRestoration	ファン異常復旧 (IX3000 シリーズ、IX2310)
pico （*1）	9	picoPowerSupplyFault	電源異常発生 (IX3000 シリーズ)
pico （*1）	10	picoPowerSupplyRestoration	電源異常復旧 (IX3000 シリーズ)
pico （*1）	11	picoPowerSupplyInserted	電源実装 (IX3000 シリーズ)
pico （*1）	12	picoPowerSupplyRemoved	電源未実装 (IX3000 シリーズ)
pico （*1）	13	picoLoginSession	ログイン
pico （*1）	14	picoLoginFailure	ログイン失敗
pico （*1）	15	picoConfigMode	モード変更

pico （*1）	16	picoConfigModified	コンフィグ変更
pico （*1）	17	picoExtIfLinkDown	4P SW-HUB ポートダウン
pico （*1）	18	picoExtIfLinkUp	4P SW-HUB ポートアップ
pipSecMIBNotificationPrefix	1	pikeTunnelStart	IKE Phase1 接続生成
pipSecMIBNotificationPrefix	2	pikeTunnelStop	IKE Phase1 接続終了
pipSecMIBNotificationPrefix	7	pipSecTunnelStart	IPsec トンネル生成
pipSecMIBNotificationPrefix	8	pipSecTunnelStop	IPsec トンネル終了
pipSecMIBNotificationPrefix	11	pipSecEarlyTunTerm	IPsec トンネル異常終了
picoNetmonMIBNotificationPrefix	1	picoNetMonWatchGroupStatusChange	ネットワークモニタ状態変更
picoIsdnMIBNotificationPrefix	1	picoIsdnLapdOperStatusChange	LAPD 状態変更（Ver.8.6 以降）
picoPostMIBNotificationPrefix	1	picoPostFailMessage	起動時自己診断 NG（Ver.8.11 以降）
picoMobileMIBNotificationPrefix	1	picoMobileDeviceDown	ポートダウン（Ver.9.3 以降）
picoMobileMIBNotificationPrefix	2	picoMobileDeviceUp	ポートアップ（Ver.9.3 以降）
picoMobileMIBNotificationPrefix	3	picoMobileSignalStatusChange	電波状態変更（Ver.9.3 以降）

- *1：Ver.7.1 以前は、sysObjectID が使用されます。Ver.7.2 以降は、pico が使用されますが、snmp-agent ip/ipv6 host コマンドを設定することにより、Ver.7.1 以前と同じ Trap-ID の値に変更することができます。

(b) 管理オブジェクト

IPv4 管理オブジェクト

MIB-II	RFC1213	mib-2
Ethernet MIB	RFC1643	dot3
The Interfaces Group MIB	RFC2863	ifStackTable ifXTable
IGMP MIB	RFC2933	igmpStdMIB
IP Forwarding Table MIB	RFC2096	ipCidrRouteNumber (Ver.9.7 以降) ipCidrRouteTable (Ver.9.7 以降)

IPv6 管理オブジェクト

General グループ	RFC2465	ipv6MIB
ICMP グループ	RFC2466	ipv6IcmpMIB
TCP MIB	RFC2452	ipv6TcpConnTable
UDP MIB	RFC2454	ipv6UdpTable
MIB for MLD	RFC3019	mldMIB

VRRP 管理オブジェクト

VRRP グループ	RFC2787	vrrpMIB（一部未実装）

ISDN 管理オブジェクト

isdnBearerChannelType	RFC2127	isdnMIB
isdnBearerOperStatus	RFC2127	isdnMIB
isdnLapdOperStatus	RFC2127	isdnMIB（Ver.8.6 以降）

BGP 管理オブジェクト

bgpPeerState	RFC4273	bgpPeerTable（Ver.8.7 以降）
bgpPeerRemoteAddr	RFC4273	bgpPeerTable（Ver.8.7 以降）

プライベート管理オブジェクト

システム	―	picoSystem
IPsec/IKE	―	picoIpSecFlowMonitorMIB

※　プライベート管理オブジェクトの詳細については付録を参照してください。

7.3.1.1 sysObjectID

装置毎に sysObjectID が設定されています。
値は以下のとおりです。

装置名（IX2000 シリーズ）	sysObjectID
IX2105	1.3.6.1.4.1.119.1.84.14.1
IX2106	1.3.6.1.4.1.119.1.84.22.1
IX2107	1.3.6.1.4.1.119.1.84.27.1
IX2207	1.3.6.1.4.1.119.1.84.18.1
IX2215	1.3.6.1.4.1.119.1.84.16.1
IX2235	1.3.6.1.4.1.119.1.84.25.1
IX2310	1.3.6.1.4.1.119.1.84.26.1

装置名（IX3000 シリーズ）	sysObjectID
IX3015	1.3.6.1.4.1.119.1.84.20.1
IX3110	1.3.6.1.4.1.119.1.84.10.1
IX3315	1.3.6.1.4.1.119.1.84.21.1

7.3.1.2 interfaceMIB/ifMIB

(a) 未使用インタフェースの隠蔽

未使用インタフェースの MIB はデフォルトでは出力されません。全てのインタフェースを出力する場合は、未使用インタフェースの隠蔽設定を無効化してください。

snmp-agent mib-2 conceal-unconfigured-ifstack	未使用インタフェースの隠蔽

(b) ifIndex の設定

任意の ifIndex が設定可能です。ただし、コンフィグ可能な device と interface のみ設定でき、内部用インタフェースの ifIndex は設定できません。また、設定を有効にするには再起動が必要です。Dialer と Tunnel には、範囲を指定して連番を設定することができます。

設定コマンド（グローバルコンフィグモード）

snmp-agent mib-2 ifindex	ifIndex の設定

【設定例】
(1) device FastEthernet0/0 の ifIndex を 1000 に設定
(2) interface FastEthernet0/0.0 の ifIndex を 2000 に設定
(3) interface Tunnel0.0 から Tunnel127.0 の ifIndex を 3000 から 3127 に連番設定
(4) interface Dialer0 の ifIndex を 4000 に設定
(5) interface Dialer90 から Dialer95 の ifIndex を 4090 から 4095 に連番設定

```
snmp-agent mib-2 ifindex device FastEthernet0/0 1000
snmp-agent mib-2 ifindex interface FastEthernet0/0.0 2000
snmp-agent mib-2 ifindex interface range Tunnel 0-127 3000
snmp-agent mib-2 ifindex interface Dialer0 4000
snmp-agent mib-2 ifindex interface range Dialer 90-95 4090
```

新たに投入した設定がすでに投入されている設定と重複するとき、すでに投入されている設定は削除され、新たに投入した設定が有効になります。上記の (1)～(5) に対して以下の (6) を設定すると、(1) は ifIndex、(4) と (5) はインタフェースが重複するため削除されます。

(6) interface Dialer0 から Dialer90 の ifIndex を 1000 から 1090 に連番設定

```
snmp-agent mib-2 ifindex interface range Dialer 0-90 1000
```

【注意事項】
※ 設定可能な ifIndex は 1～10000 です。ifIndex が設定されているとき、設定されていないインタフェースの ifIndex は 10001 以上になります。
※ show devices/interfaces に ifIndex が表示されます。

(c) ifDescr と ifType

インタフェースのスタック情報は、以下のように ifType および ifDescr に対応付けされております。ifTable を参照することで、スタックの情報を参照することができます。

Ver.5.1 以降

デバイス、 またはインタフェース	備考	ifType	ifDescr	参照 RFC
GigaEthernet*		ethernetCsmacd(6)	GigaEthernet*	3635
GigaEthernet*/*		ethernetCsmacd(6)	GigaEthernet*/*	3635
FastEthernet*		ethernetCsmacd(6) fastEther(62)	FastEthernet*	2665
FastEthernet*/*		ethernetCsmacd(6) （Ver.7.3 以降） fastEther(62)	FastEthernet*/*	2665
Ethernet*		ethernetCsmacd(6)	Ethernet*	1573
GigaEthernet*	内部用	propMultiplexor(54)	GigaEthernet*-Multiplexor	
GigaEthernet*/*	内部用	propMultiplexor(54)	GigaEthernet*-Multiplexor	—
FastEthernet*	内部用	propMultiplexor(54)	FastEthernet*-Multiplexor	—
FastEthernet*/*	内部用	propMultiplexor(54)	FastEthernet*/*-Multiplexor	—
Ethernet*	内部用	propMultiplexor(54)	Ethernet*-Multiplexor	—
GigaEthernet*.0	基本	propVirtual(53)	GigaEthernet*.0	2665
GigaEthernet*/*.0	基本	propVirtual(53)	GigaEthernet*/*.0	2665
FastEthernet*.0	基本	propVirtual(53)	FastEthernet*.0	2665
FastEthernet*/*.0	基本	propVirtual(53)	FastEthernet*/*.0	2665
Ethernet*.*	基本	propVirtual(53)	Ethernet*.*	1573
GigaEthernet*.1	PPPoE /タグ VLAN	propVirtual(53)	GigaEthernet*.1	1573
GigaEthernet*/*.1	PPPoE /タグ VLAN	propVirtual(53)	GigaEthernet*/*.1	1573
FastEthernet*.1	PPPoE /タグ VLAN	propVirtual(53)	FastEthernet*.1	1573
FastEthernet*/*.1	PPPoE /タグ VLAN	propVirtual(53)	FastEthernet*/*.1	1573
Ethernet*.1	PPPoE /タグ VLAN	propVirtual(53)	Ethernet*.1	1573
GigaEthernet1:*.0	ポート VLAN Ver.8.5 以降	propVirtual(53)	GigaEthernet1:*.0	3635
GigaEthernet1:*.1	PPPoE /タグ VLAN Ver.8.5 以降	propVirtual(53)	GigaEthernet1:*.1	3635
FastEthernet*/*:*.0	ポート VLAN	propVirtual(53)	FastEthernet*/*:*.0	2665
FastEthernet*/*:*.1	PPPoE /タグ VLAN	propVirtual(53)	FastEthernet*/*:*.1	1573
BRI*		isdns(75)	BRI*-Physical	2127
BRI*		lapd(77)	BRI*	2127
BRI*.0		ds0(81) （専用線モードの場合 ds0 は 1 つしか存在せず、ISDN モードの場合 ds0 は 2 つ存在します）	BRI*:0-Bearer Channel	2494
BRI*.0	PPP	propVirtual(53)	BRI*.0	—
Dialer*	PPP	propVirtual(53)	Dialer*	—
Serial*	T1	ds1(18)	Serial*	1573
Serial*	E1	ds1(18)	Serial*	1573
Serial*/*	T1	ds1(18)	Serial*/*	1573
Serial*.0	PPP	propVirtual(53)	Serial*.0	1573
Serial*/*.0	PPP	propVirtual(53)	Serial*/*.0	1573
Serial*/*:*.0	PPP	propVirtual(53)	Serial*/*:*.0	1573
USB-Serial*.0	PPP	propVirtual(53)	USB-Serial*.0	—
USB*		other(1)	USB*	—
BVI*		propVirtual(53)	BVI*	—
AutoTunnel0.0		propVirtual(53)	AutoTunnel0.0	2667
Tunnel*.0		propVirtual(53)	Tunnel*.0	2667
Loopback*.0		propVirtual(53)	Loopback*.0	1573
Null0.0		propVirtual(53)	Null0.0	1573
Translator0.0		other（1）	Translator0.0	—

ISDN デバイスの ifDescr は「デバイス名-Physical」(BRI1/0-Physical、Serial1/0-Physical など)です。D チャネルの ifDescr がデバイス名と同一になります。
インタフェースの ifType,ifDescr を変更することが可能です。

snmp-agent mib-2 iftype	ifType の変更 （インタフェースコンフィグ） （デバイスコンフィグ Ver.8.1 以降）
snmp-agent mib-2 ifdescr	ifDescr の変更 （インタフェースコンフィグ）

(d) ifAdminStatus と ifOperStatus

インタフェース設定および状態と、ifAdminStatus および ifOperStatus の関係を以下に示します。

インタフェース設定	インタフェース状態	ifAdminStatus	ifOperStatus
shutdown	リンクダウン	down(2)	down(2)
shutdown	正常状態	down(2)	down(2)
no shutdown	リンクダウン	up(1)	down(2) または testing(3)
no shutdown	正常状態	up(1)	up(1)

(e) ifSpeed

インタフェースの ifSpeed を変更することができます。
設定は以下のとおりです。

bandwidth	インタフェース帯域幅情報の変更 （インタフェースコンフィグ）
snmp-agent mib-2 ifspeed	インタフェース帯域幅情報の変更 （インタフェースコンフィグ）

snmp-agent mib-2 ifspeed コマンドにて設定した値は、ifSpeed にのみ使用します。
Bandwidth にて設定した値は、ifSpeed 以外にも、以下の機能においてインタフェースの帯域幅情報として使用します。詳細については、各機能の項を参照してください。

- OSPF
- QoS

両方を設定した場合は、ifSpeed は snmp-agent mib-2 ifspeed にて設定した値となります。
何も設定しない場合は、インタフェースの速度となります。

(f) ポート VLAN

VLAN グループの設定を行ったインタフェースの MIB の値は以下のようになります。MIB はインタフェース単位となります。物理ポート単位の MIB はプライベート MIB でサポートしています。

Object	値
ifSpeed	同一 VLAN グループ内において各ポートの設定が異なる場合、最も速いインタフェーススピード
ifAdminStatus	インタフェース単位（no shutdown で up）
ifOperStatus	同一 VLAN グループ内の全ポート Down 時に Down

7.3.2 SNMP バージョン

IX2000/IX3000 シリーズでは、SNMPv1、SNMPv2c、SNMPv3(Ver.10.4 以降)に対応しています。それぞれ、以下の機能に対応しています。

機能	SNMPv1	SNMPv2	SNMPv3
Get	○	○	○
Getnext	○	○	○
Getbulk	×	○	○
Trap	○	×	×
SNMPv2-Trap	×	○	○

Get/Getnext/Getbulk については、SNMP マネージャからの要求が SNMPv1 であれば SNMPv1 で、SNMPv2 であれば SNMPv2、SNMPv3 であれば SNMPv3 で応答を返します。

SNMP マネージャから SNMPv1 を使用し、SNMPv1 ではサポートしていない MIB をアクセスしようとした場合は、そのオブジェクトがサポートされていない場合と同様な動作となります。Get の場合は、“No Such Name（2）”を返し、Getnext の場合は、次のアクセス可能なオブジェクトを返します。

SNMPv2 および SNMPv3 で、獲得できる MIB のタイプは以下のとおりです。

SYNTAX	使用している主なオブジェクト
Counter64	ifXTable の ifHCInOctets など

バージョンによって、対応しているエラーコードが異なります。SNMPv1,SNMPv2c,SNMPv3 でサポートしているエラー種別は以下の通りです。

SNMPv1 のエラーコード

エラーステータス	エラーコード	内容
no Error	0	エラーがありません
too Big	1	SNMP メッセージに応答が入りきりません
no such Name	2	指定したオブジェクトが存在しません
gen Err	5	受信したパケットにて異常を検出しました

SNMPv2c のエラーコード

エラーステータス	エラーコード	内容
no Error	0	エラーがありません
too Big	1	SNMP メッセージに応答が入りきりません
no such Name	2	指定したオブジェクトが存在しません
gen Err	5	受信したパケットにて異常を検出しました
no Access	6	アクセスできないオブジェクトです。
Not Writable	17	セットできないオブジェクトです。

SNMPv3 のエラーコード

エラーステータス	エラーコード	内容
no Error	0	エラーがありません
too Big	1	SNMP メッセージに応答が入りきりません
no such Name	2	指定したオブジェクトが存在しません
gen Err	5	受信したパケットにて異常を検出しました
no Access	6	アクセスできないオブジェクトです。
authorization Error	16	認証に失敗しました。
Not Writable	17	セットできないオブジェクトです。

Trap は設定したバージョンで送信します。ホストとコミュニティの組み合わせ毎に SNMPv1 で送信するか、SNMPv2c で送信するかを指定することができます。

7.3.3 SNMP の設定

SNMP を使用した監視を行うためには、装置側にコミュニティ名とトラップ送信先の設定を事前に行うことが必要です。以下にその設定概要を示します。

SNMP を利用した監視を行わない場合は、設定は必要ありません。

Ver.9.5 以前では SNMP の機能を装置全体でしか有効に出来ませんでしたが、Ver.9.6 以降ではインタフェースコンフィグモードに enable コマンドを設定することで特定のインタフェースでのみ機能を有効にすることができます。

(a) SNMP の有効化

SNMP を使用した監視を行うために、SNMP 機能を有効にする必要があります。

SNMP データの転送（SNMP マネージャからのアクセス、トラップの送信）に IPv4/IPv6 ともに使用可能です。有効化は IPv4/IPv6 で別々に行うことができます。

SNMP 設定を有効にすることで、SNMPv1,SNMPv2c,SNMPv3 すべてが有効となります。いずれか 1 つのみ有効にすることはできません。

設定は以下のとおりです。

snmp-agent ip enable	SNMP（IPv4）の有効化
snmp-agent ipv6 enable	SNMP（IPv6）の有効化

(b) コミュニティ名の設定

コミュニティ名の設定を行います。

下記の手順にしたがって、設定を行ってください。

i) アクセスを許可する SNMP マネージャを制限する

アクセスリストを使用して、アクセスを許可する SNMP マネージャを登録してください。制限する必要がなければ設定は不要です。アクセスリストは src アドレスのみ設定し、dest は any としてください。

ip access-list <アクセスリスト名> permit ip src <SNMP マネージャアドレス> dest any ipv6 access-list <アクセスリスト名> permit ip src <SNMP マネージャアドレス> dest any

ii) アクセスを許可するビュー名を制限する

特定のオブジェクト ID のみアクセスを許可したい場合に設定してください。通常設定する必要はありません。設定しない場合は全てのオブジェクトのアクセスを許可します。

snmp-agent view	アクセス制限するビュー（ObjectID）の設定

iii)コミュニティ名を指定する

ビューとアクセスリストによる制限を行う場合は、ここで登録します。

snmp-agent ip community	アクセスを許可する SNMP マネージャの設定
snmp-agent ipv6 community	アクセスを許可する SNMP マネージャの設定

【設定例】
コミュニティ名 test。10.0.0.1/32 から ifTable（1.3.6.1.2.1.2.2）のみアクセス可能

```
ip access-list snmp-manager permit ip src 10.0.0.1/32 dest any

snmp-agent ip enable
snmp-agent view test-view 1.3.6.1.2.1.2.2
snmp-agent ip community test view test-view snmp-manager
```

(c) トラップ送信先の設定

トラップの送信先 SNMP マネージャとして、送信先アドレスとコミュニティ名、送信 SNMP バージョンを設定します。

snmp-agent ip trap	送信するトラップの選択
snmp-agent ip host	送信先 SNMP マネージャの設定
snmp-agent ip trap-source	送信元インタフェースの設定
snmp-agent ipv6 trap	送信するトラップの選択
snmp-agent ipv6 host	送信先 SNMP マネージャの設定
snmp-agent ipv6 trap-source	送信元インタフェースの設定
snmp-agent trap	送信するトラップの選択
snmp-agent host	送信先 SNMP マネージャの設定
snmp-agent trap-source	送信元インタフェースの設定

トラップの送信元アドレスの設定で、エージェントアドレス（Trap PDU Source Address Field）も任意に設定することができます。

IPv6 を使用する場合、エージェントアドレスは IPv4 アドレス形式となっています。エージェントアドレスを指定しない場合は、ルータ ID 選択と同様の論理でエージェントアドレスが設定されます。IPv4 アドレスが 1 つも設定されていない場合は、0.0.0.0 が設定されます。

SNMPv2c で送信する場合は、エージェントアドレスは送信されません。

インタフェース単位にトラップの送信設定が可能です。これは、該当インタフェースのトラップの送信設定となります。トラップの送信はルーティング情報に従って出力されますので、該当インタフェースからトラップの送信設定を行う訳ではありません。

【設定例】
認証エラーのトラップを出力しない
BRI1/0.0 の link-up/down のトラップを送信しない

```
no snmp-agent ip trap com_pub snmp auth-fail

interface BRI1/0.0
  no snmp-agent ip trap com_pub link-status
```

Link-up/down のトラップに ifDescr を追加して送信することできます。

【設定例】
Link-up トラップに ifDescr を追加して送信

```
snmp-agent ip trap com_pub snmp link-up add-option
```

(d) トラップ送信タイマ設定

トラップの送信タイマを変更することができます。

IPv4/IPv6 共通となります。

snmp-agent trap-timeout	トラップ送信タイマ設定

(e) SNMP メッセージサイズ設定

SNMP メッセージサイズを変更することができます。

snmp-agent message-size	SNMP メッセージサイズ設定

(f) 設定例

```
【設定例】

snmp-agent ip enable
snmp-agent ip community com_pub
snmp-agent ip host 192.168.1.1 com_pub
snmp-agent ip trap-source FastEthernet0/0.0
snmp-agent contact NEC
snmp-agent location Floor1
```

Ver10.4 以降、SNMPv3 対応に伴い以下の設定ができます。

(g) グループの設定

ユーザごとの MIB の参照範囲を設定可能にするため、MIB ビューとユーザを繋ぐためのグループを作成することができます。グループは最大 253 件作成できます。

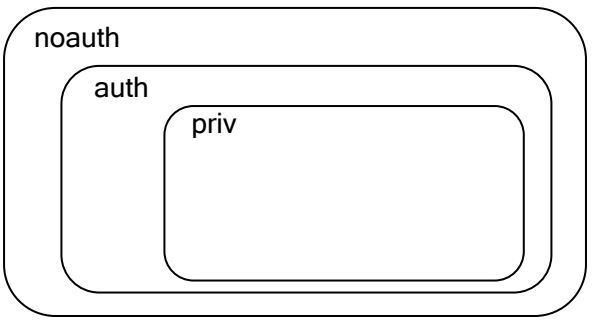
snmpv3 group	SNMPv3 セキュリティグループの設定

グループには以下のパラメータを設定することができます。

- 認証レベル

グループに所属するユーザが必要とするセキュリティレベルを noauth/auth/priv から設定できます。設定したレベルに満たないユーザが所属する場合、そのユーザは全ての MIB オブジェクトに対してアクセスすることができず、全ての MIB オブジェクトに関するトラップも発送されません。

セキュリティレベルは以下のような包含関係で設定されることになります。例えば、noauth を設定した場合、auth/priv レベルのユーザも条件を満たします。priv を設定した場合、noauth/auth レベルのユーザは条件を満たしません。



包含関係

- Read ビュー

所属ユーザは設定された MIB ビューの範囲内で MIB を読み出すことができます。
存在しないビュー名を設定することはできません。

設定を省略した場合、ユーザはすべての MIB を読み出し可能となります。

- Notify ビュー

所属ユーザにトラップ(PDU タイプが SNMPv2-Trap の SNMP パケット)を送信する際に、設定された MIB ビューの範囲内でのみ MIB の通知を送信することができます。
存在しないビュー名を設定することはできません。
設定を省略した場合、ユーザへすべての MIB についてトラップにより通知可能となります。

- アクセスリスト

ユーザの認証を許可/拒否する IP アドレスのアクセスリストを設定することができます。
ユーザ名/パスワードが正しくても、アクセスリストで許可されない IP アドレスの場合は認証を拒否します。
設定を省略した場合、IP アドレスの確認は行われません。

(h) ユーザの設定

USM に必要となるユーザ名および認証/暗号化アルゴリズムを設定することができます。
ユーザのセキュリティレベルはユーザの認証/暗号化アルゴリズムの設定に有無に応じて決定します。
“snmpv3 user”コマンドでは所属するグループの設定が必須となりますが、作成されていないグループ名に設定することはできないため「(g) グループの設定」で先にグループの作成をしてください。

snmpv3 user	SNMPv3 ユーザの設定

認証の設定	暗号化の設定	セキュリティレベル
設定しない	設定しない	Noauth
設定する	設定しない	auth
設定する	設定する	priv

認証/暗号化では以下のアルゴリズムをサポートしています。

認証アルゴリズム	MD5 SHA-1,SHA-224,SHA-256,SHA-384,SHA-512
暗号化アルゴリズム	DES AES-128

noauth/auth レベルのユーザはデフォルトでは設定が正しい場合でも無条件で認証に失敗します。
noauth/auth レベルのユーザでの認証を許可する場合、以下の設定が必要です。

snmpv3 no-password enable	SNMPv3 パスワード省略による認証の許可の設定

(i) エンジン ID の設定

SNMP エンジンの識別、および暗号化の共通鍵生成に使われるエンジン ID を設定することができます。このエンジン ID はエンティティとは 1 対 1 の関係にあるため、1 つのみ設定することができます。
マネージャ側がエンジン ID によりエージェントを識別する必要がない場合、エンジン ID はユーザが任意の値を設定する必要はありません。
コマンド未設定の場合、エンジン ID は装置の GE0 の MAC アドレスをベースとした固定のエンジン ID が装置に設定されます。
現在のエンジン ID は” show snmp-agent statistics”コマンドで確認することができます。

snmpv3 engine-id	SNMPv3 エンジン ID の設定

エンジン ID のフォーマットは以下になります。

	コマンド未設定	コマンド設定済み
1～4 オクテット	80000077	
5 オクテット	03	04
6 オクテット以降	GE0 の MAC アドレス	設定値(ASCII コード)

(j) トラップの設定

トラップ送信先のアドレス設定および送信するトラップの設定ができます。

- トラップ送信先アドレスの設定

ユーザごとにトラップ送信先の IP アドレスを設定することができます。

snmpv3 ip host	SNMPv3 トラップ送信先の IP アドレスの設定
snmpv3 ipv6 host	SNMPv3 IPv6 用トラップ送信先の IP アドレスの設定

存在しないユーザ名を指定することはできません。「(h) ユーザの設定」で先にユーザ名の作成をしてください。

- 送信するトラップの選択

ユーザ毎に送信可能なトラップの種別を設定することができます。

snmpv3 trap	SNMPv3 トラップの設定

存在しないユーザ名を指定することはできません。「(h) ユーザの設定」で先にユーザ名の作成をしてください。

(k) 設定例（SNMPv3）

```
【設定例】
snmp-agent ip enable
snmpv3 group admin_group priv
snmpv3 user admin_user admin_group auth md5 plain auth_pass priv des plain priv_pass
snmpv3 ip host 192.168.1.1 admin_user
```

■7.4 ロギング

IX2000/IX3000 シリーズのロギング機能は、機能ごとに詳細なログデータを採取することができます。ネットワークトラブルの解析に重要な情報を取得することができますので、なるべく設定するようにしてください。

7.4.1 ロギングの取得

7.4.1.1 ロギングの設定

ロギングは次のコマンドで設定できます。解除は no コマンドで行います。時刻表示も可能で、（1）日時（2）時刻のみ（3）起動してからの時間、の 3 種類が選択できます。その場で表示しながら解析をする場合以外は設定するようにしてください。

logging subsystem <機能名> <レベル>	ログを取得する機能と取得レベルの設定
logging timestamp	ログにタイムスタンプの表示を追加

【設定例】

```
logging subsystem all warn
logging timestamp datetime
```

【表示例】
（1）日時[datetime]

```
2012/12/12 13:54:55     IP.006: Packet 10.0.0.1 > 10.0.0.10 discarded for ...
```

（2）時刻のみ[timeofday]

```
13:54:49     IP.006: Packet 10.0.0.1 > 10.0.0.10 discarded for ...
```

（3）起動してからの時間[uptime]

```
05:22:23     IP.006: Packet 10.0.0.1 > 10.0.0.10 discarded for ...
```

設定可能な機能の種類やレベルの設定については後述の項を参照してください。設定によっては膨大な数のログが取得されることがあり、性能が激しく劣化します。そちらを参照して必要十分な設定を行ってください。

Ver.10.3 以降のコンフィグ表示について

Ver.10.3 以降、all の設定と異なるレベルで logging subsystem コマンド、または no logging subsystem コマンドが設定された場合、コンフィグ上には all の設定と上記設定したコマンドの両方が表示されます。この場合のイベントログの出力について、設定された個別サブシステム以外は all の設定で動作します。

【設定例 1】
サブシステム IP のみ debug レベルで出力、それ以外全て warn レベルで出力する場合

```
logging subsystem all warn
logging subsystem ip debug
```

【設定例 2】
サブシステム IP のみロギング出力なし、それ以外全て warn レベルで出力する場合

```
logging subsystem all warn
no logging subsystem ip
```

7.4.1.2 ロギング可能な機能の種類とレベル

ログは以下のように、機能ごとにレベルを設定して取得することができます。
次のコマンドでも一覧表示することができます。

```
logging subsystem ?
```

サブシステム名	機能名	補足
all	全機能	
aaa	Authentication Authorization and Accounting	
acl	アクセスリスト	
apa	アプリケーション解析機能	Ver.10.6 以降
arp	Address Resolution Protocol	
bgp	Border Gateway Protocol	
bri	Basic Rate ISDN	
brs	QoS	
circ	インタフェース内部動作	
cmda	コマンドアクション	Ver.9.3 以降
cnfg	コンフィグプロセス	
crtp	Compression RTP	
d1x	IEEE802.1x	
ddns	ダイナミック DNS	Ver.8.8 以降
dh6	DHCP for IPv6	
dhc	DHCP クライアント for IPv4	
dhr	DHCP リレーエージェント for IPv4	
dhs	DHCP サーバ for IPv4	
dial	ダイアラ	Ver.8.6 以降
dns	Domain Name System	
dqos	ダイナミック QoS	Ver.10.0 以降
e1	E1	日本国内向けは未実装
eap	Extensible Authentication Protocol	
env	Environment Monitor	電圧,温度等
eth	Ethernet	
flt	トラフィックフィルタ	
gptl	トンネル	
gw	ルータベース機能	
hrdf	URL リダイレクト機能	Ver.9.0 以降
http	Hypertext Transfer Protocol (HTTP)	
icmp	ICMP for IPv4	
icp6	ICMP for IPv6	
ids	Intrusion Detection System	Ver.8.10 以降
igmp	IGMP for IPv4	
ike	IKEv1	
ike2	IKEv2	Ver.8.7 以降
ip	IPv4	
ip6	IPv6	
ipwc	ネットワークモニタ	
irb	ブリッジ	
isdn	ISDN	
key	Key マネージャ（IKEv1）	
ktsa	キーテレフォンシステム連携機能	
l2tp	L2TP	Ver.8.10 以降
ldf	ループ検出機能	Ver.8.9 以降
lnkm	リンクマネージャ機能	Ver.9.5 以降

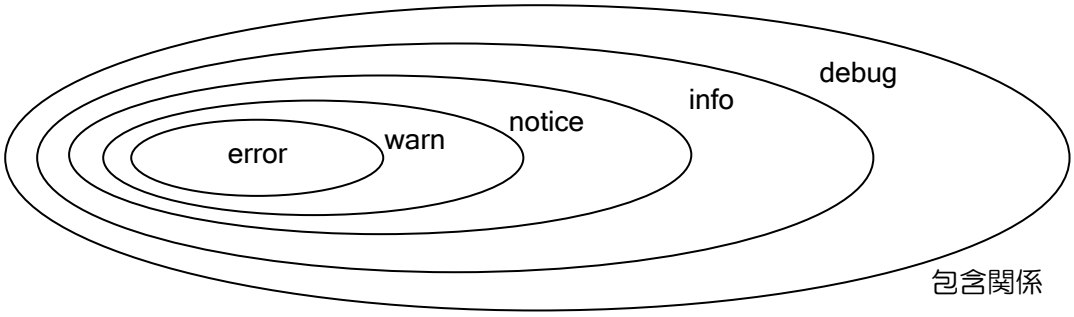
maca	MAC 認証	
macl	MAC アクセスリスト	
mape	MAP-E	
mflt	MAC フィルタ	
modm	モデムコマンド（USB）	Ver.8.8 以降
nat	NAT/NAPT	
ngna	NGN アクセス機能	Ver.8.6 以降
ngns	NGN サービス機能	Ver.8.6 以降
ngnt	NGN トンネル機能	Ver.8.6 以降
nhrp	Next Hop Resolution Protocol	Ver.9.2 以降
nmc	NetMeister クライアント	Ver.9.7 以降
ntp	NTP	
opfc	OpenFlow Protocol	Ver.8.11 以降
opft	OpenFlow DataPath	Ver.8.11 以降
ospf	OSPFv2	
pdn6	プロキシ DNS for IPv6	
pdns	プロキシ DNS for IPv4	
pim	PIM	Ver.8.4 以降
ppoe	PPPoE	
ppp	PPP	
pri	PRI	
prte	ポリシールーティング	
rad	RADIUS クライアント	
rip	RIP	
rip6	RIPng	
rmap	Route Map	
schd	スケジューラ	Ver.8.8 以降 Ver.9.2 まで （Ver.9.3 以降は cmda）
sec	IPsec traffic	
snmp	SNMP	
spf6	OSPFv3	
ssh	SSH サーバ	Ver.8.7 以降
t1	T1	
tcp	TCP	
tels	Telnet サーバ	
tftp	TFTP	
udp	UDP for IPv4	
udp6	UDP for IPv6	
urlf	URL フィルタリング機能	Ver.9.5 以降
urll	URL リスト	Ver.9.5 以降
urlo	URL オフロード機能	Ver.9.4 以降
usb	USB	Ver.8.8 以降
utm	UTM	Ver.10.0 以降
v6pv	IPv6 標準プロビジョニング機能	Ver.10.8 以降
vrrp	VRRP	
weba	Web 認証	Ver.9.5 以降
webc	Web コンソール	
wol	Wake on LAN	Ver.8.9 以降
ztp	ゼロタッチ機能	Ver.10.4 以降

IX2000/IX3000 シリーズでは、重要度を以下のように分類しています。

重要度	意味	イベントログリファレンス対応表*

		Ver.7.3 以降	Ver.7.2 以前
error	エラー状態レベル	ERROR	UI-ERROR,UE-ERROR
warn	警告状態レベル	WARNING	CI-ERROR,CE-ERROR
notice	注意レベル	NOTICE	U-INFO
info	情報レベル	INFO	C-INFO
debug	デバッグレベル	DEBUG	P-TRACE,U-TRACE,C-TRACE

また、上記の重要度は、以下のような包含関係で設定されることになります。例えば、warn を設定すると、error も同時にロギングできます。



7.4.1.3 メッセージの表示例

IP.006: Packet 192.168.100.1 > 192.168.200.1 discarded for <REASON> FastEthernet0/0.0
（SEC.025 なども同様）

<REASON>の領域に理由として表示される内容の原因

- LINK-FRMWRK: NO ENTRY IN LOOKUP TABLE TO COMPLETE OPERATION
  - ARP 解決ができない、または ARP 解決中にさらにパケットの転送要求が来た場合で、送信先が見つからないので廃棄したことを示します。
  - arp auto-refresh で改善することがあります。
- LINK-FRMWRK: PACKET NOT ACCEPTED FOR FLOW CONTROL REASONS
  - QoS の制御によりパケットが廃棄されました。意図しない廃棄のログでしたら設定を見直してください。
  - Ver7.2 まではキュー長の不足が原因となることも多いので、設定で大きくとることで改善する場合があります。

IKE.007: Send notification data to 192.168.100.1, type <type>:<REASON>, protocol ISAKMP
IKE.009: Receive notification data from 192.168.200.1, type <type>:<REASON>, protocol ISAKMP

<type>:<REASON>の領域に理由として表示される内容の原因

- 9:INVALID-MESSAGE-ID
- 14:NO-PROPOSAL-CHOSEN
  - Send の場合は自装置が異常を検出したことを相手に通知し、Receive の場合は異常を検出したとの通知を相手装置から受信したことを示します。
  - ほとんどの場合は設定の不一致が原因です。

SEC.001: Drop invalid packet from 192.168.100.1, protocol 4, error 61

- protocol 4 は IPv4 の IPsec, protocol 41 は IPv6 の IPsec の廃棄を意味します。
- error 番号は内部値ですので無視してください。前後のメッセージに理由があります。

SEC.008: Invalid ICV from Tunnel, 192.168.100.1

- パケットの認証に失敗したことを示します。
- 「データの改ざん」「回線の異常」が考えられます。

BRI.004: ConnID 0x6 Q.931 Cause Info Element (Call Rejected) cause (0x5:0x15) on device BRI1/0

- 切断理由などのメッセージが表示されます。
- cause は NTT の勧告または本マニュアルの「ISDN 切断理由コード一覧」を参照してください。

ETH.048: Maintenance failed: FastEthernet0

- 回線のチェックに異常があったことを示します。
- 対向装置の電源断やケーブルを抜いたときに表示されるのは問題ありませんが、それ以外で表示される場合は、回線またはケーブルに異常があると考えられます。

7.4.1.4 注意事項

debug レベルはパケットトレースを行うものが多いので、運用時には表示量が多く性能が激しく劣化することがありますので注意してください。

特に telnet 中に event-terminal start コマンドを使用してロギング情報を表示させる場合に、logging subsystem ip debug を行うと、ロギングを表示するためのパケットに反応して、ロギングが次々と表示されるため、正常に動作しなくなります。

7.4.2 ロギングの出力

設定したロギング情報は、次の 3 種類の方法で出力することができます。

- ターミナル画面への直接出力
- 内部バッファへ保存した情報の出力
- syslog による出力

7.4.2.1 ターミナル画面への出力

ロギング情報をリアルタイムにターミナル画面へ出力します。

event-terminal	取得ログのターミナル画面への直接出力

```
【動作例】
(config)# event-terminal start
IP006: Packet 10.0.0.1 > 10.0.0.11 discarded for LINK-FRMWRK: NO ENTRY IN LOOKUP TABLE TO COMPLETE OPERATION, FastEthernet0.0
  :
(config)# event-terminal stop
```

開始の設定を行うと、リアルタイムにロギング情報が表示されます。停止設定を行うとロギングの表示は停止します。ロギング表示の状態でも、他のコマンドを実行することが可能です。ただし、show コマンド実行時にロギングが表示された場合、コマンド結果表示途中にロギング情報が表示される場合があります。また、大量のロギングが表示された場合は、一部のロギング情報が表示されない場合があります。

ログをターミナル画面に表示していない状態でもログは保存されますが、ロギング情報最大保持件数は 128 件です。128 件を超えた場合は、古い情報から廃棄されていきます。表示開始時に保存されているログが表示され、保存されている情報はクリアされます。

7.4.2.2 内部バッファへの保存と出力

ロギング情報を内部バッファへ保存し、show コマンドにより保存した情報を表示します。

logging buffered	ログの保存領域サイズ設定
show logging	取得ログのコマンドでの表示
show logging output <USB メモリ> copy logging <USB メモリ>	取得ログを USB メモリのファイルに書き込む（Ver9.0 以降）

```
【設定例】

logging buffered 1000000
```

ロギング保存設定のパラメータはバイト数になります。1 行あたり 80 バイト程度となりますので、show memory で残りのメモリ量，何行程度ログを保存するかを確認の上、サイズを決定してください。ただし、残りメモリが 1Mbyte 以下になる場合は、運用に支障がないように新規にメモリ確保を行いません。それまで確保できた範囲内でログの保存を行ないます。

7.4.2.3 syslog への出力

ロギング情報を syslog サーバへ送信します。設定方法等については、syslog の項を参照してください。

7.4.3 ロギングの出力制御

Ver.10.1 以降、logging subsystem コマンドで設定したレベル内で表示不要なログの出力を抑止することができます。また、logging subsystem コマンドで設定したレベル外のログを追加で出力することができます。

7.4.3.1 ロギングの出力抑止

機能名とログ番号を設定することでログの出力を抑制することができます。

logging subsystem <機能名> exclude <ログ番号>	指定したログ番号のメッセージ表示を無効 ※ ログ番号は複数設定可能

【設定例】
IP.006（error レベル）と IP.015（debug レベル）を出力せず、
debug レベル以下の IP ログを出力する場合

```
logging subsystem ip debug
logging subsystem ip exclude 6 15
```

7.4.3.2 ロギングの出力追加

機能名とログ番号を設定することでログを追加出力することができます。

logging subsystem <機能名> include <ログ番号>	指定したログ番号のメッセージ表示を有効 ※ ログ番号は複数設定可能

【設定例】
warn レベルの IP ログの出力と、IP.015（debug レベル）を出力する場合

```
logging subsystem ip warn
logging subsystem ip include 15
```

7.4.3.3 設定の追加・削除

(a) 設定の追加

既に設定がある状態で、出力抑止（exclude） / 出力追加（include）した場合、
設定は上書きされます。
また、ログ番号を重複して指定した場合、重複している番号はまとめて表示します。

【動作例 1】
既に logging subsystem ip exclude 1 2 3 が設定済みの状態で
"logging subsystem ip exclude 7 8 15 20"を再設定した場合。

```
(再設定前)
(config)# show running-config
                :
logging subsystem ip exclude 1 2 3

(再設定後)
(config)# logging subsystem ip exclude 7 8 15 20
(config)# show running-config
                :
logging subsystem ip exclude 7 8 15 20
```

【動作例 2】
重複するログ番号を設定した場合。

```
(config)# logging subsystem ip include 1 2 2 3 3 3
(config)# show running-config
                :
logging subsystem ip include 1 2 3
```

なお、logging subsystem all コマンドでは出力抑止（exclude） / 出力追加（include）の設定をすることはできません。

(b) 設定の削除

設定を削除する場合、no logging subsystem コマンドのオプションの有無で動作が異なります。

【設定】

```
(config)# show running-config
                :
logging subsystem arp warn
logging subsystem arp include 1 2 3
logging subsystem arp exclude 4 5 6
logging subsystem ip warn
logging subsystem ip include 1 2 3
logging subsystem ip exclude 4 5 6
```

【動作例 1】
no logging subsystem <機能名> コマンドを実行した場合、
該当する機能名の全ての設定を削除します。

```
(config)# no logging subsystem ip
(config)# show running-config
                :
logging subsystem arp warn
logging subsystem arp include 1 2 3
logging subsystem arp exclude 4 5 6
```

【動作例 2】
no logging subsystem <機能名> <レベル>コマンドを実行した場合、
logging subsystem <機能名> <レベル>コマンドの設定を削除します。

```
(config)# no logging subsystem ip error
(config)# show running-config
                :
logging subsystem arp warn
logging subsystem arp include 1 2 3
logging subsystem arp exclude 4 5 6
logging subsystem ip include 1 2 3
logging subsystem ip exclude 4 5 6
```

【動作例 3】
no logging subsystem <機能名> include（exclude）コマンドを実行した場合、
該当する機能名の include（exclude）設定を削除します。
(config)# no logging subsystem ip include
(config)# show running-config
:
logging subsystem arp warn
logging subsystem arp include 1 2 3
logging subsystem arp exclude 4 5 6
logging subsystem ip warn
logging subsystem ip exclude 4 5 6

※ ログ番号を指定して設定を削除することはできません。

なお、no logging subsystem all コマンドを実行した場合、logging subsystem の設定をすべて削除します。

7.4.3.4 注意事項

- ログ番号ごとのログ内容はバージョンによって変更される可能性があります。
- 別のログ番号と関連付けが行われているログ番号では、出力の抑止や追加の設定と異なる動作となることがあります。
- 1 行あたり文字数 629 文字(スペース含む)以上になるコンフィグは投入できません。
  - ✧ 上記文字数まで設定を投入した状態で、no コマンドによるコンフィグ全削除は数を超えることになる為投入できなくなります。
- 同じ機能名のログ番号を 出力抑止（exclude）と 出力追加（include）の両方に設定した場合、抑止（exculde）処理が動作します。
- VRF 機能有効時の拡張されたログ番号(IP と BGP)は設定できません。
- VRF 有効時に出力するログ番号を抑制・追加する場合は、VRF 無効時のログ番号で設定をする必要があります。

7.4.3.5 統計情報の表示

ロギングの統計情報（show logging statistics）の表示とログのカウント方法は以下のとおりです。

	show logging statistics 表示	ログのカウント
出力抑止設定あり	非表示	※1
出力追加設定あり	表示	

※ 同じ機能名のログ番号が出力抑止（exclude）と 出力追加（include）の両方に設定されている場合は、抑止（exculde）処理が動作します。

※1 出力抑止・追加に関わらず装置起動時からカウントを行います。
抑制設定時や追加設定時にカウントの停止・開始およびリセットは行いません。

■7.5 syslog を利用した監視

IX2000/IX3000 シリーズでは、ロギング機能による詳細なログデータをコンソールに出力だけではなく、syslog サーバへ転送することで、syslog サーバ側にデータを保存することができます。

これにより、syslog サーバ側でのデータを基に、ネットワークトラブル等の解析ができるようになります。

ただし、予めロギングの設定を実施しておく必要があります。

syslog は、次のコマンドにより設定することができます。syslog は、event-terminal コマンドと独立して動作しますので、syslog のみ使用する場合は、event-terminal コマンドによる開始は不要です。Ver.7.2 以降は、送信先サーバを複数設定することができます。

Ver.7.2 以降

syslog facility	送信するファシリティ設定
syslog ip host	送信先 IPv4 syslog サーバの設定
syslog ipv6 host	送信先 IPv6 syslog サーバの設定
syslog ip source	送信元 IPv4 アドレスの設定
syslog ipv6 source	送信元 IPv6 アドレスの設定
syslog ip enable	IPv4 syslog 送信有効化（デフォルト有効）
syslog ipv6 enable	IPv6 syslog 送信有効化（デフォルト有効）
logging subsystem	ロギング設定

Ver.7.1 以前

syslog facility	送信するファシリティ設定
syslog host	送信先 syslog サーバの設定
syslog source-address	送信元 IPv4 または IPv6 アドレスの設定
logging subsystem	ロギング設定

syslog のメッセージ部分にロギングにて出力される内容が出力されます。
ログ番号の出力フォーマットが syslog とロギングでは異なります。

【出力例】

syslog 出力
IP[021]: Interface GigaEthernet0.0, link up

ロギング出力
IP.021: Interface GigaEthernet0.0, link up

ファシリティは、IX2000/IX3000 シリーズから syslog パケットを送信する際に付加するラベルのようなもので、syslog サーバ側での判断のために使用します。デフォルトでは、local0（16）が割り当てられています。

ファシリティは、すべてのイベントに対して、1 つのファシリティを選択します。

kern	0
user	1
mail	2
daemon	3
auth	4
syslog	5
lpr	6
news	7
uucp	8
cron	9
authpriv	10
ftp	11

ntp	12
security	13
console	14
local0	16
local1	17
local2	18
local3	19
local4	20
local5	21
local6	22
local7	23

セビリティ（重要度）については、ロギングの重要度と以下のように対応します。

セビリティ	値	イベントログリファレンス対応表*	
		Ver.7.3 以降	Ver.7.2 以前
error	3	ERROR	UI-ERROR,UE-ERROR
warn	4	WARNING	CI-ERROR,CE-ERROR
notice	5	NOTICE	U-INFO
info	6	INFO	C-INFO
debug	7	DEBUG	P-TRACE,U-TRACE,C-TRACE

※ syslog は、イベント発生時に送信されます。syslog 送信を停止している状態でのロギング情報最大保持件数は、0 件です。

※ info や debug を利用する場合は、syslog パケット送信ログで syslog が生成されるなどによる大量パケット送信に注意してください。

(a) syslog 抑止設定

Ver.8.1 以降、syslog が大量に送信された場合、送信が抑止されます。デフォルトでは、1 秒間に 10 個に制限されます。送信レートはセビリティ毎に設定できます。

設定コマンドは以下のとおりです。

syslog rate-limit	syslog 送信抑止設定

【設定例】
Error は 1 秒間に 20 個に制限
Warning は 1 秒間に 15 個に制限

```
syslog rate-limit error rate 20
syslog rate-limit warn rate 15
```

(b) タイムスタンプとホスト名付与設定

syslog メッセージ内にタイムスタンプとホスト名を設定できます。タイムスタンプは Ver8.10 以降、ホスト名は Ver9.4 以降で対応しています。設定コマンドは以下のとおりです

設定コマンドは以下のとおりです。

syslog timestamp	syslog タイムスタンプ設定
syslog id hostname	syslog ホスト名設定

```
【設定例】
hostname Host1

syslog ip host 192.168.0.100
syslog timestamp datetime
syslog id hostname
```

タイムスタンプとホスト名は、この順番に空白(スペース)区切りで付与します。ホスト名は hostname コマンドで設定してください。

```
【出力例】
Jul 12 13:10:50 Host1     IP[021]: Interface GigaEthernet0.0, line protocol up
```

8章 統計情報

本章では、IX2000/IX3000 シリーズで収集できる統計情報について説明します。

■8.1 統計情報一覧

統計情報の収集コマンドを一覧にて示します。

コマンド	内容
show devices	デバイス情報
show interfaces	インタフェース情報
show ppp	PPP 情報
show ppp lcp	PPP LCP 情報
show ppp ipcp	PPP IPCP 情報
show ppp pap	PPP PAP 情報
show ppp chap	PPP CHAP 情報
show ppp ip	PPP IPv4 情報
show ppp ipv6	PPP IPv6 情報
show ppp ipv6cp	PPP IPv6CP 情報
show ppp multilink	PPP multilink 情報
show ppp errors	PPP エラー情報
show pppoe statistics	PPPoE 情報
show bridge traffic	ブリッジ情報
show arp statistics	ARP 情報
show ip traffic	IPv4 情報
show ip nat statistics	NAT 情報
show ip napt statistics	NAPT 情報
show ip nat translation	NAT エントリ情報
show ip napt translation	NAPT エントリ情報
show ip napt record	NAPT キャッシュ情報
show ip dhcp-client statistics	DHCP クライアント情報
show ip dhcp server	DHCP サーバ情報
show proxy-dns	プロキシ DNS 情報
show ip route	IPv4 ルーティング情報
show ip cache	IPv4 キャッシュ情報
show ipv6 traffic	IPv6 情報
show ipv6 cache	IPv6 キャッシュ情報
show ip rip	RIP サマリ情報
show ip rip interface	RIP インタフェース情報
show ip rip peer-information	RIP 隣接ルータ情報
show ip rip statistics	RIP その他統計情報
show ipv6 rip	RIPng 情報
show ipv6 rip interface	RIPng インタフェース情報
show ipv6 rip peer-information	RIPng 隣接ルータ情報
show ipv6 rip statistics	RIPng その他統計情報
show ip ospf statistics	OSPFv2 情報
show ipv6 ospf statistics	OSPFv3 情報
show ip bgp	BGP 情報

show ip bgp neighbors advertise-routes	BGP 送信経路情報
show ip bgp neighbors receive-routes	BGP 受信経路情報
show ip bgp routes	BGP 経路情報
show ip bgp neighbors	BGP ピア情報
show ip bgp summary	BGP ピアのサマリ情報
show ip bgp paths	BGP パス情報
show ip pim statistics	PIM 統計情報（Ver.8.4 以降）
show tunnel status	トンネル情報
show ike statistics	IKE 情報
show ipsec statistics	IPsec 情報
show ikev2 statistics	IKEv2 情報（Ver.8.7 以降）
show policy-map interface	QoS 情報
show bandwidth-policy-map interface	QoS 情報（帯域ポリシーマップ）
show ip rtp header-compression	CRTP 情報
show ip rtp tcp-header-compression	CRTP（CTCP）情報
show vlans	VLAN 情報
show vrrp	VRRP 情報
show vrrp statistics	VRRP 統計情報
show watch-group	ネットワークモニタ情報
show ip watch	ネットワークモニタ情報
show access-list	MAC アクセスリスト情報
show access-list cache	MAC アクセスリストキャッシュ情報
show ip access-list	IPv4 アクセスリスト情報
show ip access-list cache	IPv4 アクセスリストキャッシュ情報
show ip access-list dynamic	IPv4 ダイナミックアクセスリスト情報
show ipv6 access-list	IPv6 アクセスリスト情報
show ipv6 access-list cache	IPv6 アクセスリストキャッシュ情報
show ipv6 access-list dynamic	IPv6 ダイナミックアクセスリスト情報
show ip filter statistics	IPv4 トラフィックフィルタ情報
show ipv6 filter statistics	IPv6 トラフィックフィルタ情報
show ip prefix-list	IPv4 プレフィックスリスト情報
show ipv6 prefix-list	IPv6 プレフィックスリスト情報
show snmp-agent statistics	SNMP エージェント情報
show snmpv3 user	SNMPv3 ユーザ情報（Ver.10.4 以降）
show logging statistics	ロギング情報
show ip ufs-cache	IPv4 UFS キャッシュ情報
show ipv6 ufs-cache	IPv6 UFS キャッシュ情報
show sip	SIP-ALG システム情報表示
show sip access-list	SIP アクセスリスト情報表示
show sip dynamic-filter	SIP ダイナミックフィルタシステム情報表示
show sip dynamic-filter dialog	SIP ダイナミックフィルタダイアログ情報表示
show sip dynamic-filter register	SIP ダイナミックフィルタレジスタ情報表示
show sip dynamic-filter transaction	SIP ダイナミックフィルタトランザクション情報表示
show sip filter	SIP フィルタ情報表示
show sip nat	SIP NAT システム情報

show sip nat register	SIP NAT ユーザキャッシュ情報
show sip nat dialog	SIP NAT ダイアログキャッシュ情報
show sip nat transaction	SIP NAT トランザクションキャッシュ情報
show dot1x interface	IEEE802.1X インタフェース情報
show dot1x statistics	IEEE802.1X 統計情報
show dot1x supplicant	IEEE802.1X Supplicant 情報
show http-server	HTTP サーバ統計情報
show kts-addressing statistics	グローバルアドレス通知機能統計
show ngn statistics	NGN 統計情報（Ver.8.6 以降）
show loop-detection information	ループ検知統計情報（Ver.8.9 以降）
show sflow information	sFlow 統計情報（Ver.8.9 以降）
show ids statistics	IDS 統計情報（Ver.8.10 以降）
show l2tp statistics	L2TP 統計情報（Ver.8.10 以降）
show l2tp active	L2TP 接続情報（Ver.8.10 以降）
show l2tp history	L2TP 接続履歴（Ver.8.10 以降）
show http-redirect information	URL リダイレクト端末情報（Ver.9.0 以降）
show openflow controller	OpenFlow コントローラ情報（Ver.9.0.54 以降）
show openflow port	OpenFlow ポート情報（Ver.9.0.54 以降）
show url-offload status	URL オフロード情報（Ver.9.4 以降）
show url-filter statistics	URL フィルタリング統計情報（Ver.9.5 以降）
show url-filter server	URL フィルタリングサーバ情報（Ver.9.5 以降）
show url-filter cache	URL フィルタキャッシュ情報（Ver.9.5 以降）
show utm statistics	UTM 統計情報（Ver.10.0 以降）

■8.2 統計情報詳細

統計情報の表示内容の詳細をコマンド別に示します。
内容の [ ] 内は該当する MIB になります。

8.2.1 デバイス関連

show devices
*は detail 指定時のみ表示します。

Ethernet 共通
※記載の無い項目については、装置毎を参照してください。

項目	内容
link-up*	リンクアップ数（Ver8.5 以降）
link-down*	リンクダウン数（Ver8.5 以降）
since*	リンク状態が変化してからの経過時間（Ver8.5 以降）
input frames	受信フレーム数（64 ビット）
input octets	受信オクテット数（64 ビット）※1
input good frames*	正常な受信フレーム数（64 ビット）※1
input good octets*	正常な受信オクテット数（64 ビット）※1
output frames	送信フレーム数（64 ビット）
output octets	送信オクテット数（64 ビット）※1
output requests	送信要求回数（64 ビット）
output good frames*	正常な送信フレーム数（64 ビット）※1
output good octets*	正常な送信オクテット数（64 ビット）※1
Rx errors	受信時のエラー統計情報※4
alignment errors	8bit の整数倍でないフレームの受信回数 [dot3StatsAlignmentErrors]
CRC errors	CRC 値が正しくないフレームの受信回数 [dot3StatsFCSErrors]
long frames	最大フレーム長以上のフレームの 受信回数 [dot3StatsFrameTooLongs]
short frames	ショートフレームの受信回数 [dot3StatsInternalMacReceiveErrors （overflows 分を含む）]
overflows	オーバーフローの検出回数 [dot3StatsInternalMacReceiveErrors （short frames 分を含む）]
Tx errors	送信時のエラー統計情報※4
single collision	リトライ（１回）の検出回数 [dot3StatsSingleCollisionFrames]
multiple collision	リトライ（複数回）の検出回数 [dot3StatsMultipleCollisionFrames]
excessive collisions	リトライオーバーの検出回数 [dot3StatsExcessiveCollisions]
late collisions	レイト・コリジョンの合計検出回数 [dot3StatsLateCollisions]
deferred transmissions	送信延期指示の検出回数 [dot3StatsDeferredTransmissions]
carrier sense errors	キャリア・センス・ロストの検出回数 [dot3StatsCarrierSenseErrors]※2
heart beat errors	ハートビートエラーの検出回数 [dot3StatsSQETestErrors]※2

underflows	アンダーフローの検出回数 [dot3StatsInternalMacTransmitErrors]
truncations	サイズオーバーを切り捨てて送信した数

※1 GigaEthernet のみ表示

※2 FastEthernet,の場合に表示

※3 IX3110 では 1537 バイト以上の CRC 値が正常なフレームでも計上

※4 IX3315 は「IX3315 GigaEthernet」の「Controller statistics」、「PHY statistics」を参照してください

IX3015 FastEthernet

項目	内容
Controller statistics*	装置固有の統計情報
rx-bufdesc exhausted*	受信時のフレーム破棄の検出回数
stall detected*	FCC ストールの検出回数
RMON statistics*	RMON 統計情報
received octets counter*	受信オクテット数
received good frames of broadcast address*	受信フレーム数(ブロードキャスト)
received good frames of multicast address*	受信フレーム数(マルチキャスト)
received frames of unicast address*	受信フレーム数(ユニキャスト)
received frames shorter than 64 octets*	受信フレーム数 (ユニキャスト:64 オクテット以下)
received frames of ＊＊ octets*	フレーム長毎の受信フレーム数
received frames longer than 1518 octets*	受信フレーム数 (ユニキャスト:1518 オクテット以上)
estimated number of collisions*	コリジョン検出数
as uspc + bad frames* received bad frames shorter than 64 octets	無効 FCS を持つ 64 オクテットより短いフレーム数
as ospc + bad frames* received bad frames longer than 1518 octets	無効 FCS を持つ 1518 オクテットより長いフレーム数

IX2105/IX2106/IX2107/IX2207/IX2215/IX2235 GigaEthernet

項目	内容
Rx errors	受信時のエラー統計情報
misc errors	バッファ不足による廃棄、内部エラー ※1
Tx errors	送信時のエラー統計情報
misc errors	内部エラー※1
Other errors:	装置固有の統計情報
internal bus errors*	内部のシステムバスエラー発生数
internal parity errors*	内部のパリティエラー発生数
busy conditions*	受信空きバッファ不足回数
graceful stop timeout*	デバイスリセットのタイムアウト回数
stall detected*	送信停止検出回数
Controller statistics*	装置固有の統計情報
received frames*	受信フレーム数
transmitted frames*	送信フレーム数
transmitted/received frames of * octets*	フレームサイズ毎の送受信フレーム数
received good pause frames*	受信した正常なポーズフレーム数

transmitted good pause frames*	送信した正常なポーズフレーム数
Rx errors:*	受信エラー
received bad short frames*	64 バイト以下の受信異常フレーム数
received bad long frames*	1519 バイト以上(VLAN タグ付きの場合は 1523 バイト以上)の受信異常フレーム数 ※1537 バイト以上のフレームは常に CRC エラーでカウントされます。
Tx errors:*	送信エラー
transmitted bad short frames*	64 バイト以下の送信異常フレーム数
transmitted bad long frames*	1519 バイト以上(VLAN タグ付きの場合は 1523 バイト以上)の送信異常フレーム数

※1 IX2105/IX2106/IX2107 のみ表示

IX3000 GigaEthernet

項目	内容
Controller statistics*	装置固有の統計情報
transmitted octets counter*	送信オクテット数（64 ビット）
transmitted good octets counter*	正常送信オクテット数
transmitted frames of broadcast address*	ブロードキャストフレーム送信数
transmitted frames of multicast address*	マルチキャストフレーム送信数
transmitted frames of unicast address*	ユニキャストフレーム送信数
transmitted good frames*	送信フレーム数
transmitted frames of ＊＊ octets*	フレーム長毎の送信フレーム数
transmitted XON*	XON フレーム送信数
transmitted XOFF*	XOFF フレーム送信数
transmitted TCP segmentation context*	未使用
TCP segmentation context Tx fail*	未使用
received octets counter*	受信オクテット数（64 ビット）
received good frames*	（64 ビット）
received frames of broadcast address*	受信フレーム数(ブロードキャスト)
received frames of multicast address*	受信フレーム数(マルチキャスト)
received frames of unicast address*	受信フレーム数(ユニキャスト)
received frames shorter than 64 octets*	受信フレーム数 (ユニキャスト:64 オクテット以下)
received frames of ＊＊ octets*	パケット長毎の受信パケット数
received frames longer than 1518 octets*	受信フレーム数 (ユニキャスト:1518 オクテット以上)
Fragment*	フラグメントエラーフレーム受信数
received XON*	XON フレーム受信数
received XOFF*	XOFF フレーム受信数
management frames*	未使用
FC received unsupported*	未使用
receive length errors*	64byte 未満または 1522byte 超の フレーム数
symbol errors*	IEEE 802.3x のシンボル以外の検出回数
sequence errors*	受信シーケンスエラーの検出回数
no buffers*	受信バッファ枯渇の検出回数
Jabber*	受信ジャバーの検出回数
carrier extension errors*	受信キャリアエクステンションエラー 検出回数
management frame drop errors*	未使用

rx errors*	PHY 受信エラー検出回数
data errors*	バッファディスクリプタ受信エラー検出回数
IP checksum errors*	未使用
TCP/UDP checksum errors*	未使用

IX3100 GigaEthernet

項目	内容
Other errors:	装置固有の統計情報
internal bus errors	内部のシステムバスエラー発生数
internal parity errors	内部のパリティエラー発生数
busy conditions	受信空きバッファ不足回数
SFP tx faults	SFP 出力信号低下検出回数
graceful stop timeout	デバイスリセットのタイムアウト回数
stall detected	送信停止検出回数
Controller statistics*	装置固有の統計情報（デバイス情報）
received frames	受信フレーム数
transmitted frames	送信フレーム数
transmitted/received frames of ＊ octets	フレームサイズ毎の送受信フレーム数
received good pause frames	受信した正常なポーズフレーム数
transmitted good pause frames	送信した正常なポーズフレーム数
Rx errors:	受信エラー
received bad short frames	64 バイト以下の受信異常フレーム数
received bad long frames	1519 バイト以上(VLAN タグ付きの場合は 1523 バイト以上)の受信異常フレーム数 ※1537 バイト以上のフレームは常に CRC エラーでカウントされます。
Tx errors:	送信エラー
transmitted bad short frames	64 バイト以下の送信異常フレーム数
transmitted bad long frames	1519 バイト以上(VLAN タグ付きの場合は 1523 バイト以上)の送信異常フレーム数

IX3315 IX2310 GigaEthernet

項目	内容
Rx traffic statistics:	
high group packet input	高優先パケット（受信パケット優先制御に該当）受信数
low group packet input	低優先パケット（受信パケット優先制御に非該当）受信数
high group packet drop	高優先パケット受信廃棄数
low group packet drop	低優先パケット受信廃棄数
Rx high/low group packet drop statistics:	
allocate failure	高/低優先パケット割当失敗による廃棄数
latency exceeded	待機時間オーバーによる廃棄数
Rx errors:	受信時のエラー統計情報
frame errors	壊れたフレーム、サイズ異常フレーム受信による廃棄数
internal errors	frame errors を除く受信エラー数
no buffers	バッファ枯渇による廃棄数

FMan queueing errors:*	FMan での廃棄
internal errors*	QMan 内部エラーによる廃棄
Rx Core queueing errors:*	受信コアでの廃棄数
busy errors*	コア間転送コントローラビジーによる廃棄数
internal errors*	コア間転送コントローラ内部エラーによる廃棄数
Tx traffic statistics:	
high group packet output	高優先パケット（受信時に受信パケット優先制御に該当、QoS に該当、自生成パケット）送信数
low group packet output	低優先パケット（受信時に受信パケット優先制御に非該当）送信数
high group packet drop	高優先パケット送信廃棄数
low group packet drop	低優先パケット送信廃棄数
Tx high/low group packet drop statistics:	
latency exceeded	待機時間オーバーによる廃棄数
Tx errors:	送信時のエラー統計情報
frame errors	壊れたフレーム、サイズ異常フレーム送信による廃棄数
internal errors	frame errors を除く送信廃棄数
Main Core queueing errors:*	メインコアでの廃棄数
busy errors*	コア間転送コントローラビジーによる廃棄数
internal errors*	コア間転送コントローラ内部エラーによる廃棄数
Tx Core queueing errors:*	送信コアでの廃棄数
busy errors*	コア間転送コントローラビジーによる廃棄数
internal errors*	コア間転送コントローラ内部エラーによる廃棄数
Other errors:*	装置固有の統計情報
SFP tx faults*	SFP 出力レベルが低下した回数
internal errors*	イーサネットコントローラ内部エラー数
Controller statistics:*	装置固有の統計情報
received frames*	受信フレーム数
received frames of ＊＊ octets*	パケット長毎の受信パケット数
received good pause frames*	受信した正常なポーズフレーム数
Rx errors:*	
alignment errors*	アライメントエラーフレーム数 [dot3StatsAlignmentErrors]
CRC errors*	CRC エラーフレーム数 [dot3StatsFCSErrors]
long frames*	最大フレーム長をオーバーした正常 FCS の受信フレーム数 [dot3StatsFrameTooLongs] (PHY statistics の long frames を含む)
short frames*	64Byte 未満の正常 FCS 受信フレーム数 [dot3StatsInternalMacReceiveErrors] (overflows と PHY Statistics の short frames を含む)

overflows*	受信 FIFO オーバーフローが発生し、内部エラーにより廃棄したフレーム数 [dot3StatsInternalMacReceiveErrors] (short frames と PHY Statistics の short frames を含む
bad short frames*	64Byte 未満の FCS エラー受信フレーム数
bad long frames*	最大フレーム長をオーバーした FCS エラー受信フレーム数
transmitted frames*	送信フレーム数
transmitted frames of ＊＊ octets*	フレーム長毎の送信フレーム数
transmitted good pause frames*	送信した正常なポーズフレーム数
Tx errors:*	送信エラー
CRC errors*	CRC エラーフレーム数 [dot3StatsInternalMacTransmitErrors] (other errors を含む)
other errors*	CRC エラー以外で発生したエラー数 [dot3StatsInternalMacTransmitErrors] (other errors を含む)
PHY statistics:	
Rx statistics:	
input frames	受信フレーム数
Rx errors:	
phys errors	受信エラーを検出したフレーム数
CRC errors	CRC 値が正しくないフレームの受信数
long frames	2048 バイト以上のフレーム受信数 [dot3StatsFrameTooLongs] (Controller statistics の long frames を含む)
short frames	64 バイト未満のフレーム受信数 [dot3StatsInternalMacReceiveErrors] (short frames と overflows 含む)
jabbers	2048 バイト以上で CRC 値が異常なフレーム受信数
fragments	64 バイト未満で、CRC 値が異常なフレーム受信数
Tx statistics:	
output frames	送信フレーム数
Tx errors:	
single collisions	リトライ（1 回）の検出回数 [dot3StatsSingleCollisionFrames]
multiple collisions	リトライ（複数回）の検出回数 [dot3StatsMultipleCollisionFrames]
excessive collisions	リトライオーバーの検出回数 [dot3StatsExcessiveCollisions]
late collisions	レイトコリジョンの検出回数 [dot3StatsLateCollisions]
deferred transmissions	送信延期指示の検出回数 [dot3StatsDeferredTransmissions]
collisions	コリジョン発生回数
internal CRC errors	送信時の CRC エラー検出回数

SWHUB

項目	内容
Extended card is switching hub	
CRC errors	CRC 値が正しくないフレームの受信数
collisions	コリジョン発生回数
link-up*	リンクアップ数（Ver8.5 以降）
link-down*	リンクダウン数（Ver8.5 以降）
since*	リンク状態が変化してからの経過時間（Ver8.5 以降）
SWHUB information:	
Global:	
free queue*	フリーキュー数 （IX2025 のみ表示されます）
SWHUB statistics:	
input frames	受信フレーム数
output frames	送信フレーム数
Rx errors*	
discards	受信バッファ不足による廃棄数
phys errors	受信エラーを検出したフレーム数
CRC errors	CRC 値が正しくないフレームの受信数
long frames	2048 バイト以上のフレーム受信数
short frames	64 バイト未満のフレーム受信数
jabbers	2048 バイト以上で CRC 値が異常なフレーム受信数
fragments	64 バイト未満で、CRC 値が異常なフレーム受信数
Tx errors:	
single collisions	リトライ（1 回）の検出回数 （IX2215 以外）
multiple collisions	リトライ（複数回）の検出回数 （IX2215 以外）
excessive collisions	リトライオーバーの検出回数 （IX2215 以外）
late collisions	レイトコリジョンの検出回数 （IX2215 以外）
deferred transmissions	送信延期指示の検出回数 （IX2215 以外）
collisions	コリジョン発生回数
internal CRC errors	送信時の CRC エラー検出回数 （IX2215 以外）
discards	リトライオーバーの検出回数と レイトコリジョンの検出回数の合計 （IX2215 のみ）

BRI 共通（IX2215 以外）

項目	内容
interrupts*	割込み発生回数
INFO0(F3) interrupts*	L1 down 検出
INFO2(F6) interrupts*	INFO2 signal 検出
INFO4(F7) interrupts*	L1 up 検出
INFOX(F5) interrupts*	Any signal 検出
INFOX(F8) interrupts*	Lost framing 検出
unknown interrupts*	その他の割込み検出
INFO4(invalid F7) interrupts*	不正な L1 up 検出
Internal call control statistics:	
disconnect requests discarded*	切断要求廃棄の検出数
wait inbound calls	保留中の受信呼設定メッセージ数
max wait inbound calls	保留となった受信呼設定メッセージの最大数
Local buffer statistics:	
allocated	割り付けられているバッファ数
inuse	現在使用中のバッファ数
highest inuse	過去に使用したバッファの最大数
Statistics summary	統計情報概要
＊ch	Ch 毎の統計情報
input/output frames	受信/送信フレーム数
bytes	受信/送信バイト数
errors	受信/送信エラーの合計数
alignment errors	8bit の整数倍でないフレームの受信回数
CRC errors	CRC 値が正しくないフレームの受信回数
long frames	最大受信フレーム長以上のフレームの受信回数
overruns	バッファは足りているが、受信処理時にエラーの発生したフレーム数
buffer overflows	受信バッファが足りずオーバーフローしたフレーム数
overflows	受信オーバーフロー検出回数
aborts	受信中にアボートの発生したフレーム数
CTS lost	送信中に同期が失われたフレーム数
underruns	送信アンダーラン検出回数
buffer underflows	ドライバがオーバーフローによって破棄したフレーム数
Hardware errors	ハードウェアで検出したエラー情報
interrupt queue overflows	送信割り込みキューのオーバーフロー検出回数
global underflows	発生チャネルが特定できないアンダーフローの検出回数
global overflows	発生チャネルが特定できないオーバーフローの検出回数

IX2215 BRI

項目	内容
BRI status	
system errors*	フレーマのシステムエラー発生回数 ・回復不能なエラー ・フレームを大量に受信
initialization failed*	初期化失敗回数
interrupts*	割り込み合計回数
active*	L1 ダウン→アップ 割り込み回数
inactive*	L1 アップ→ダウン 割り込み回数
sync*	フレーム非同期→同期 割り込み回数
async*	フレーム同期→非同期 割り込み回数
connect*	S/T インタフェース部に電源供給開始 割り込み回数
disconnect*	S/T インタフェース部に電源供給停止 割り込み回数
Internal call control statistics:*	
disconnect requests discarded*	切断要求が破棄された回数
wait inbound calls*	待機中の着呼数
max wait inbound calls*	待機中の着呼数の最大数
Local buffer statistics:*	
allocated*	保有しているバッファ数
inuse*	使用中のバッファ数
highest inuse*	使用中バッファ数の最大値
HDLC Controller status:/*ch	各 Ch 統計の合計/Ch 毎の統計
input/output frames	送信/受信フレーム数
bytes	送信/受信バイト数
errors	送信/受信のエラーの合計
alignment errors*	8bit の整数倍でない受信フレーム数
CRC errors*	CRC 値が正しくない受信フレーム数
aborts*	アボート（7bit 以上連続した"1"）検出数 （Dch 以外）
long frames*	2048byte 以上のフレーム受信
overruns*	受信オーバーラン発生回数
buffer overflows*	受信バッファオーバーフロー発生回数
underruns*	送信アンダーラン発生回数
buffer underflows*	送信バッファアンダーフロー発生回数

T1

項目	内容
input/output frames	受信/送信フレーム数
bytes	受信/送信バイト数
Current 15-minute interval time statistics	15 分毎の統計 (15 分間で最大 65535 までカウント)
24 hour statistics	一日毎の統計
line code violations	Line Code Violation（LCV）数
path code violations	Path Code Violation（PCV）数
unavailable seconds	SES 状態が 10 秒間続いた場合にカウント（US）
errored seconds	通信可で OOF を検出した場合にカウント（ES）

bursty errored seconds	通信可で PCV のカウント値が 320 より小さい場合にカウント（BES）
severely errored seconds	通信可の状態で OOF を検出した場合、又は PCV のカウント値が 320 以上の場合にカウント（SES）
severely errored framing seconds	通信可で OOF を検出した場合にカウント（SEFS）
line errored seconds	LCV がカウントされた場合にカウント（LES）
controlled slip seconds	Controlled Slip を検出した場合にカウント（CSS）

Channelized-T1

項目	内容
input/output frames	受信/送信フレーム数
bytes	受信/送信バイト数
errors	受信/送信エラーの合計数
alignment errors	8bit の整数倍でないフレームの受信回数
CRC errors	CRC 値が正しくないフレームの受信回数
long frames	最大フレーム長以上のフレームの受信回数
incomplete frames	不完全なフレームの受信回数
Overflows	受信オーバーフローの検出回数
Aborts	受信中にアボートの発生したフレーム数
Underflows	送信アンダーフローの検出回数
Hardware errors	ハードウェアで検出したエラー
rx interrupt queue0-3 overflows	受信割り込みキュー0-3 のオーバーフロー検出回数
tx interrupt queue overflows	送信割り込みキューのオーバーフロー検出回数
global underflows	発生チャネルが特定できないアンダーフローの検出回数
global overflows	発生チャネルが特定できないオーバーフローの検出回数

USB

項目	内容
link-up	リンクアップ回数
link-down	リンクダウン回数
Modem statistics:	
input commands	受信したモデムコマンドの総数
frcs	受信した最終リザルト数
ircs	受信した中間リザルト数
urcs	受信した非請求リザルト数
echos	受信したエコー数
errors	受信したリザルトエラー数
illegals	受信した不正データ数
output commands	送信したモデムコマンドの総数
connects	接続回数
cancels	接続キャンセル回数
disconnects	切断回数

registers	ネットワーク登録状態が登録となった回数（※）
unregisters	ネットワーク登録状態が登録以外となった回数（※）
GPRS registers	GPRS ネットワーク登録状態が登録となった回数（※）
GPRS unregisters	GPRS ネットワーク登録状態が登録以外となった回数（※）
EPS registers	EPS ネットワーク登録状態が登録となった回数（※）
EPS unregisters	EPS ネットワーク登録状態が登録以外となった回数（※）
in-ranges	電波状態が圏内、かつ基地局登録状態が登録となった回数
out-ranges	電波状態が圏外、または基地局登録状態が登録以外となった回数
QMI statistics:	
input messages	受信した QMI メッセージ総数
responses	受信した QMI 応答数
indications	受信した QMI 通知数
illegals	解読できなかった QMI メッセージ数
output messages	送信した QMI メッセージ総数
Statistics:	
input frames	受信フレーム数
input good frames	正常受信したフレーム数
input good octets	正常受信したバイト数
output frames	送信したフレーム数
output octets	送信したバイト数
output requests	送信要求したフレーム数
Rx errors:	
cancel errors	キャンセルになったフレーム数
unknown frames	予期しないフォーマットのフレーム数
oversize frames	予期しないサイズのフレーム数
other errors	その他のエラーとなったフレーム数
stuffing errors	octet stuffing アルゴリズムでエラーとなったフレーム数
reassemble errors	PPP パケットのリアセンブルでエラーとなったフレーム数
disassemble discards	PPP パケットのディスアセンブルで廃棄となったフレーム数
Tx errors	
cancel errors	キャンセルとなったフレーム数
other errors	その他のエラーとなったフレーム数
overflow errors	オーバーフローによる廃棄フレーム数
stuffing errors	octet stuffing アルゴリズムでエラーとなったフレーム数
Wireless adaptor reset cause:	
transmit timeouts	回線確立後の無応答によるリセット数
modem timeouts	モデムコマンド無応答によるリセット数
startup timeouts	データ通信端末の初期化未完了によるリセット数
terminate timeouts	回線切断時の無応答によるリセット数

coverage timeouts	圏外が 30 分以上継続によるリセット数
connecting errors	回線接続の連続 10 回失敗によるリセット数
signal information errors	電波状態読み出しに連続して失敗したため、データ通信端末をリセットした回数。（Ver9.0.54 以降）
Device reset cause:	
mount timeouts	データ通信端末未検出によるリセット数
Host controller reset cause:	
reset failures	Port Reset 実施不可による USB ホストコントローラのリセット数
HUB power on failures	内蔵 USB ハブポートの電源 ON 失敗によるリセット数
HUB power off failures	内蔵 USB ハブポートの電源 OFF 失敗によるリセット数
HUB health check failures	内蔵 USB ハブの定期的な状態チェック失敗によるリセット数

※データ通信端末が IX で認識された後に基地局で登録状態が変更されたときの非請求リザルト応答通知回数。（例えば、データ通信端末が基地局に登録された状態で IX を再起動した場合、通常は基地局の状態は変更されないため、カウントされません。）

8.2.2 インタフェース関連

show interfaces

※show devices と重複する項目については省略しています。

共通項目

項目	内容
packets input	データリンクレイヤの受信パケット数（64 ビット）
bytes	受信バイト数（64 ビット） [ifInOctets]（下位 32 ビット分）
errors	下記の受信エラーの合計 （drops,misc errors を含む）
unicasts	ユニキャストパケット （64 ビット） [ifInUcastPkts] （下位 32 ビット分）
non-unicasts	ユニキャスト以外のパケット [ifInNUcastPkts]
unknown protos	プロトコル不明パケット数 （IP/ARP/IPv6/Dot1x 以外のパケット数。 ブリッジ未設定時のみ） [ifInUnknownProtos]
drops	受信エラーによる廃棄数（Ver8.6 以降） 送信先のバッファオーバーフローのため 廃棄したパケット数（Ver8.5 以前） [ifInDiscards]
misc errors	レイヤ２以下でエラーを検出した パケット数 PPP 使用時は - 不正なコントロールフィールド受信数 - 不正なプロトコルフィールド受信数 [ifInErrors]
output requests	ネットワークレイヤがデータリンクレイヤに対して送信要求を行なったパケット数（64 ビット）
bytes	送信要求バイト数 （64 ビット） [ifOutOctets] （下位 32 ビット分）
errors	下記の送信エラーの合計 （overflows, neighbor unreachable, misc errors）
unicasts	ユニキャストパケット （64 ビット） [ifOutUcastPkts] （下位 32 ビット分）
non-unicasts	ユニキャスト以外のパケット [ifOutNUcastPkts]
overflows	送信パケットキューオーバーフロー回数 [ifOutDiscards]
neighbor unreachable	アドレス解決失敗 [ifOutError:misc error との合計]

misc errors	レイヤ２以下でエラーを検出した パケット数 ・インタフェース down ・ハードウェア障害 ・発信抑止中 [ifOutErrors: neighbor unreachable との合計]
link-up detected	リンクアップ検出回数
link-down detected	リンクダウン検出回数

Tunnel

項目	内容
packets input/output	受信/送信パケット数
bytes	バイト数
errors	トンネル送信/受信時のエラー数 [送信時のエラー] ・トンネルのネスト数の制限オーバー ・トンネルが up 以外 ・フラグメント不可 [受信時のエラー] ・送信先のバッファオーバーフロー
Received ICMP messages	ICMP メッセージの受信数
network unreachable	ネットワークへの到達不可
host unreachable	ホストへの到達不可
protocol unreachable	プロトコルに到達不可
fragmentation needed	フラグメントが必要
TTL exceeded	TTL が 0 になった
parameter problem	パラメータ異常

PPP 関連は show ppp *** と同様になりますので、PPP 関連の項を参照してください。

BRI

項目	内容
transmit error	送信エラー＋送信同期外れエラー
receive error	受信エラー＋アライメントエラー
transmit/receive overflow	送信/受信オーバーフローの発生回数
transmit/receive underrun	送信/受信アンダーランの発生回数
transmit/receive abort	送信/受信中にアボートの発生した回数
receive crc error	CRC の正しくないフレームの受信回数

8.2.3 PPP 関連

show ppp

下記のすべての情報を表示

- show ppp lcp
- show ppp ipcp
- show ppp ipv6cp
- show ppp pap
- show ppp chap
- show ppp ip
- show ppp ipv6
- show ppp errors

show ppp lcp

項目	内容
packets	LCP パケット送受信数
octets	LCP パケットの総オクテット数
cfg reqs	Configure-Request 回数
cfg acks	Configure-Ack 回数
cfg naks	Configure-Nak 回数
cfg rejs	Configure-Reject 回数
term reqs	Terminate-Request 回数
term acks	Terminate-Ack 回数
echo reqs	Echo-Request 回数
echo reps	Echo-Reply 回数
disc reqs	Discard-Request 回数
code rejs	Code-Reject 回数

show ppp ipcp

項目	内容
packets rcvd	IPCP 受信パケット数
octets	IPCP 受信パケットの総オクテット数
proto rejects	IPCP パケットに対する Protocol-Reject 回数
packets send	IPCP 送信パケット数
octets	IPCP 送信パケットの総オクテット数

show ppp ipv6cp

項目	内容
packets rcvd	IPv6CP 受信パケット数
octets	IPv6CP 受信パケットの総オクテット数
proto rejects	IPv6CP パケットに対する Protocol-Reject 回数
packets send	IPv6CP 送信パケット数
octets	IPv6CP 送信パケットの総オクテット数

show ppp pap

項目	内容
packets rcvd/sent	PAP パケット受信数
octets	PAP パケット総受信オクテット数
auth reqs	Authenticate-Request 受信回数
auth acks	Authenticate-Ack 受信回数
auth naks	Authenticate-Nak 受信回数
packets sent	PAP パケット送信数
octets	PAP パケット総送信オクテット数
auth reqs	Authenticate-Request 送信回数
auth acks	Authenticate-Ack 送信回数
auth naks	Authenticate-Nak 送信回数

show ppp chap

項目	内容
packets rcvd	CHAP パケット受信数
octets	CHAP パケット総受信オクテット数
challenges	Challenge 受信回数
responses	Response 受信回数
successes	Success 受信回数
failures	Failure 受信回数
packets sent	CHAP パケット送信数
octets	CHAP パケット総送信オクテット数
challenges	Challenge 送信回数
responses	Response 送信回数
successes	Success 送信回数
failures	Failure 送信回数

show ppp ip

項目	内容
packets rcvd	IP 受信パケット数
octets	IP 受信パケットの総オクテット数
prot rej	IP パケットに対する Protocol-Reject 回数
packets send	IP 送信パケット数
octets	IP 送信パケットの総オクテット数

show ppp ipv6

項目	内容
packets rcvd	IPv6 受信パケット数
octets	IPv6 受信パケットの総オクテット数
proto rejects	IPv6 パケットに対する Protocol-Reject 回数
packets sent	IPv6 送信パケット数
octets	IPv6 送信パケットの総オクテット数

show ppp errors

項目	内容
bad controls	制御部が 3 でない PPP フレームの受信数
last one is	前回の制御部の値
unknown protocols	Protocol-Reject した PPP フレーム数
last one is	前回のプロトコル識別値
invalid protocols	プロトコル識別値の最下位ビットが 1 でない PPP フレームの受信数
last one is	前回のプロトコル識別値
config timeouts	リンク設定パケットの最大再送回数オーバーの回数
terminate timeouts	Terminate-Request の最大再送回数オーバーの回数

show ppp multilink

項目	内容
MP Statistics	バンドル全体の統計情報
fragments rcvd	受信 MP フラグメント数
fragments sent	送信 MP フラグメント数
bytes	バイト数
complete pkts	MP 分割したパケット数（送信） MP 分割から組み立てたパケット数（受信）
lost frgs	MP フラグメントを受信できなかった数
discarded frgs	リンク設定パケットの最大再送回数オーバーの回数
LCP 1:	各 LCP の統計情報
fragments rcvd	受信フラグメント数
fragments sent	送信フラグメント数
bytes	バイト数

show pppoe statistics

項目	内容
PADI	PADI 送信パケット数
PADO	PADO 送信パケット数
PADR	PADR 送信パケット数
PADS	PADS 送信パケット数
PADT	PADT 送信パケット数
Discard Packet	エラーにより廃棄したパケット数
Retry	リトライ情報
PADI retrys	PADI のリトライ回数
PADO retrys	PADO リトライ回数（Ver9.7 以降）
PADR retrys	PADR のリトライ回数
PADT timeout	PADT のタイムアウト数 （PADT 送信後に、ピアから PADT を受信しなかった回数）

8.2.4 ブリッジ関連

show bridge traffic

項目	内容
RX count	インタフェース受信フレーム数
TX count	インタフェース送信フレーム数
statistics:	プロトコル種別毎の統計
receives	受信フレーム数
bytes	受信バイト数
discards	受信時の廃棄 ・受信バッファのオーバーフロー
forwards	送信フレーム数
bytes	送信バイト数
discards	送信時の廃棄 ・送信バッファのオーバーフロー ・デバイスでの送信エラー

8.2.5 IPv4 関連

show arp statistics

項目	内容
Entries	エントリ数
Overflows	受信パケットキューオーバーフロー回数
Refresh	エントリリフレッシュ回数
Timeouts	タイムアウトによるエントリ消失回数

show ip traffic

項目	内容
Recv	受信統計情報
receives	インタフェース経由で受信したパケット数 （IPsec、フィルタ、NAT 等で廃棄されたパケットは計上されません）
hdr errors	IP ヘッダエラーパケット数（バージョンエラー、ヘッダ長異常, パケット長異常、チェックサム異常, TTL が 0 のパケット）
addr errors	宛先アドレスエラーパケット数 （クラス A/B/C、マルチキャスト、ブロードキャスト以外のアドレス）
unknown protos	プロトコル不明パケット数
discards	その他の受信廃棄数 （転送無効時のダイレクトブロードキャスト受信、受信アドレスがダウン、スローパスキューのオーバーフローなど）
delivers	自局宛パケットのうちレイヤ 4 以上のサービスに渡されたパケット数 （宛先プロトコル不明パケットは計上されません）

reasm reqs	自局宛フラグメントパケット数
reasm oks	リアセンブル成功回数
reasm fails	リアセンブル失敗回数
Sent	送信統計情報
forwards	転送パケット数（自局宛パケット、自局生成パケットは対象外）
requests	自局で生成されたパケット数
discards	データリンク送信に失敗したパケット数（IPsec、フィルタ、NAT、NAPT 等で廃棄されたパケットは計上されません）
frag oks	フラグメント成功回数
frag fails	フラグメント失敗回数（DF（Don't Fragment）フラグ がセットされていた場合にのみ計上されます）
frag creates	フラグメント処理の結果、生成されたパケット数
no routes	経路検索失敗回数（宛先アドレス異常パケットは計上されません）
Mcast	マルチキャスト統計情報
in pkts	入力マルチキャストパケット
out pkts	出力マルチキャストパケット

ICMP 情報

項目	内容
Rcvd	受信 ICMP 統計情報
msgs	受信 ICMP パケット数
errors	受信 ICMP エラーパケット数 （パケットサイズ異常、チェックサムエラー等）
dest unreachs	destination unreachable 受信数
time excds	time exceeded 受信数
parm problems	parameter problem 受信数
echos	echo request 受信数
echo replies	echo reply 受信数
redirects	redirect 受信数
quenches	source quench 受信数
timestamps	time stamp request 受信数
timestamp replies	time stamp reply 受信数
mask requests	address mask request 受信数
mask replies	address mask reply 受信数
Sent	送信 ICMP 統計情報
msgs	送信 ICMP パケット数
errors	ICMP パケット送信失敗回数（メモリリソース枯渇等）
dest unreachs	destination unreachable 送信数
time excds	time exceeded 送信数
parm problems	parameter problem 送信数
echos	echo request 送信数
echo replies	echo reply 送信数
redirects	redirect 送信数
quenches	source quench 送信数
timestamps	time stamp request 送信数

timestamp replies	time stamp reply 送信数
mask requests	address mask request 送信数
mask replies	address mask reply 送信数

IGMP 情報

項目	内容
Rcvd	受信 IGMP 統計情報
v1 queries	IGMP version1 クエリ受信数
v2 queries	IGMP version2 クエリ受信数
unknown ver queries	未サポート version クエリ受信数
v1 reports	IGMP version1 レポート受信数
v2 reports	IGMP version2 レポート受信数
unknown ver reports	未サポート version レポート受信数
leaves	リーブ受信数
errors	不正な IGMP パケット受信数
Sent	送信 IGMP 統計情報
queries	クエリ送信数
reports	レポート送信数
leaves	リーブ送信数

UDP 情報

項目	内容
Rcvd	受信 UDP 統計情報 （Ver.8.0.50 以前は IPv6 との合計）
datagrams	受信 UDP データグラム総数
no ports	宛先ポートを使用するアプリケーションが起動されていなかった UDP データグラム数
errors	受信 UDP データグラムのうち、宛先ポートでアプリケーションが起動されていないという理由以外で上位のプロトコルに渡すことができなかったデータグラム数
Sent	送信 IPv4 UDP 統計情報
datagrams	送信 UDP データグラム総数

TCP 情報

項目	内容
active opens	TCP コネクションが CLOSE 状態から SYN-SENT 状態に直接状態遷移した回数
passive opens	TCP コネクションが LISTEN 状態から SYN-RCVD 状態に直接状態遷移した回数
attempt fails	TCP コネクションが SYN-SENT 状態かまたは SYN-RCVD 状態から CLOSED 状態へ直接状態遷移した回数と、SYN-RCVD 状態から LISTEN 状態へ直接状態遷移した回数との和。 （TCP コネクションの確立中に RST（Reset）ビットがセットされた "ConnectionRefused" パケットが相手側から 返ってきたとき、この状態遷移が起こり得ます。

established resets	TCP コネクションが ESTABLISHED 状態かまたは CLOSE-WAIT 状態から CLOSED 状態へ直接状態遷移した回数。（上位のプロトコルから中止するよう依頼されたとき、RST ビットがセットされたセグメントが送られ、この 状態遷移が起こり得ます。）
in segments	受信セグメント数。エラーも含む。現在確立されているコネクションで受信したセグメントを含む。
out segments	送信セグメント数。現在確立されているコネクション上のセグメントは含むが、再送データのみのセグメントは含まず。
retransmit segments	再送セグメント数。即ち、送出されたセグメントのうちで、以前一度以上送出されたことのあるオクテットを含んだセグメントの個数を表します。
in errors	受信エラー（TCP チェックサムエラー）セグメント数
out resets	RST フラグを含んで送信したセグメント数
checksum errors	チェックサムエラー検出回数
bad MD5 authentications	MD5 認証失敗検出回数
ack challenge sent	Ack challenge 送信数

show ip nat/napt statistics

項目	内容
Processing packets	パケット処理を行った回数
receives	パケットを受信した回数
forwards	パケットを転送した回数
discards	パケットを廃棄した回数
Translation failure packets	変換の失敗によるパケットの廃棄回数
Reassemble packets	リアセンブルパケットの処理回数
reasm reqs	リアセンブル要求パケットの処理回数
reasm oks	リアセンブル成功数
Memory allocation failures	メモリ確保失敗数
Static NAT cache entries	静的 NAT 累積変換回数
Dynamic NAT cache entries	動的 NAT 累積変換回数
NAPT cache entries	NAPT 累積変換回数
Static NAPT cache entries	静的 NAPT 累積変換回数
Service NAPT cache entries	サービス NAPT 累積変換回数
ALG Service NAPT cache entries	ALG サービス NAPT 累積変換回数
NAPT cache ALG counter	ALG 累積変換回数
forwards	パケット転送回数
drops	パケット廃棄回数
creates	キャッシュ生成回数

cache 情報

項目	内容
Prot	プロトコルタイプ
Inside Address:Port	変換される内側アドレス、およびポート
Outside Address:Port	変換される外側アドレス、およびポート
InPkt	受信パケット数
OutPkt	送信パケット数

show ip nat/napt translation

項目	内容
entry	現在のエントリ数
free	現在の残り生成可能エントリ数
peak	同時に存在した最大エントリ数
create	累計エントリ生成数
overflow	累計エントリ生成不可数
Codes	キャッシュの追加情報 (コードの優先順位 A > S)
A - ALG	ALG 処理対象キャッシュ
S - Static、Service	スタティック NAPT、又はサービス NAPT から生成されたキャッシュ

show ip nat/napt translation verbose

項目	内容
flag	フラグ
static	スタティック NAPT から生成
service	サービス NAPT から生成
ALG service	ALG サービスから生成
ALG	ALG 処理対象パケット
creator	クリエイター
ALG	ALG から生成された Cache
NAT	NAT から生成された Cache
NAPT	NAPT から生成された Cache
ALG type	本 Cache にヒットすることで適用される ALG のタイプ
None	ALG 処理なし
FTP	FTP コントロールセッション
FTP(data)	FTP データセッション
TFTP	TFTP コントロールセッション
TFTP(data)	TFTP データセッション
SIP	SIP
SIP(RTP)	SIP 用 RTP
SIP(RTCP)	SIP 用 RTCP
Dir	ディレクション
IN	内向きのパケットで生成された Cache
OUT	外向きのパケットで生成された Cache
-	ALG から生成されたため向き情報なし
uptime	Cache が生成されてからの時間
outbound	外向きの統計情報

inbound	内向きの統計情報
forwards	累計転送数
drops	累計廃棄数

show ip napt record

項目	内容
NAPT Record	
entry	インタフェース単位での NAPT キャッシュ数
overflow	インタフェース単位での NAPT キャッシュオーバーフロー発生数
エントリ	
Inside Address	ホストの IP アドレス
curr	現在の NAPT キャッシュ数
peak	過去最大の NAPT キャッシュ数
overflow	NAPT キャッシュのオーバーフロー発生数
last overflow time	オーバーフローが発生した直近の時刻

show ip dhcp-client statistics

項目	内容
Number of clients bound	アドレス取得したクライアント数
Bad packets received	不正なパケットの受信数
Buffer allocation failures	バッファ取得エラー数
Memory allocation failures	メモリ確保エラー数

show ip dhcp server

項目	内容
Global	グローバル
Leased to x clients in all	グローバル、ローカルに割り当てたクライアント合計数
Interface	インタフェース名
Leased to x clients	ローカルに割り当てたクライアント数

show proxy-dns

項目	内容
DNS server(s)	手動で登録、あるいは動的に取得した DNS サーバアドレス
Session list(s)	セッション情報
entry	セッション数
servers	問い合わせを行ったサーバ数
fails	Failure メッセージの受信数

show ip route

項目	内容
IP Routing Table	
entries	現在の経路情報数
hidden	表示していない経路情報数 - クラスフルの経路 - 内部で使用されるデフォルトルート - ネットワークモニタ機能で隠蔽された経路
frees	現在の残り経路情報数数
Entries:	
Connected	Connected の経路数
Static	Static ルーティングの経路数
RIP	RIP の経路数
OSPF	OSPF の経路数
BGP	BGP の経路数

show ip cache

項目	内容
busy	現在のキャッシュエントリ数 [picoIPv4CacheEntries]
frees	現在の残りキャッシュエントリ数
peaks	有効キャッシュ数が最も多かった時点の有効キャッシュ数(Ver.9.6 以降) [picoIPv4CachePeaks]
garbage	フラッシュされて無効になったエントリ数（Ver.8.2 以降）
multicasts	マルチキャストエントリ数 （Ver.8.2 以降） （使用できる最大数は、ユニキャストとマルチキャストの合計になります。）
flybys	キャッシュを使用せずに送信した回数
creates	キャッシュを作成した回数(Ver.9.6 以降) [picoIPv4CacheCreates]
overflows	残りエントリ数が不足し、キャッシュを作成できなかった回数 [picoIPv4CacheOverflows]

8.2.6 IPv6 関連

show ipv6 traffic

IPv6 情報

項目	内容
IP statistics	IPv6 パケット情報
Rcvd	受信 IPv6 統計情報
receives	インタフェース経由で受信したパケット数（エラーを含む）

hdr errors	IP ヘッダエラーパケット数（チェックサムエラー、バージョン番号エラー、フォーマットエラー、TTL エラー、IP オプションエラーなど）
too big errors	受信した過大パケット数
no routes	経路が判明しなかったために廃棄されたデータグラムの数を表します。
addr errors	IP ヘッダの宛先フィールドのアドレスが不正となっている受信パケット数
unknown protos	未知かまたはサポートしていないプロトコルが指定されていたために廃棄したパケット数
truncated pkts	切詰検出パケット数
discards	廃棄パケット数
delivers	ユーザプロトコル（ICMP も含む）に正常に渡された受信パケット数
reasm reqds	リアセンブルする必要があるパケット数
reasm oks	リアセンブル成功回数
reasm fails	リアセンブル失敗回数
Sent	送信 IPv6 統計情報
forwd datagrams	転送パケット数（自局宛パケット、自動生成パケットは対象外）
requests	生成したパケット数
discards	データリンク送信に失敗したパケット数
frag oks	フラグメント成功回数
frag fails	フラグメント失敗回数
frag creates	フラグメント処理の結果、生成されたパケット数
Mcast:	マルチキャスト
in pkts	受信マルチキャストパケット数
out pkts	送信マルチキャストパケット数

ICMP 情報

項目	内容
msgs	受信 ICMP パケット総数（icmp[In/Out]Errors でカウントされるものも含む）
errors	受信 ICMP エラーパケット数（ICMP チェックサムエラーや長さのエラーなど）
dest unreachs	destination unreachable 受信数
admin prohibs	admin prohibs 受信数（管理者によってアクセスが拒否されているため配送が失敗したとき）
time excds	time exceeded 受信数（time-to-live=0 を検出したとき、このパケットを廃棄し、送信元ホストにこのメッセージを送信）
parm problems	parameter problem 受信数（処理中にヘッダにエラーを発見したとき、このパケットを廃棄し、送信元ホストにこのメッセージを送信）
pkt too bigs	pkt too bigs 受信数（パケット長が長い）

echos	echo request 受信数
echo replies	echo reply 受信数
router solicits	近隣要請メッセージパケット数
router advertisements	近隣通知メッセージパケット数
neighbor solicits	ルータ要請メッセージパケット数
neighbor advertisements	ルータ通知メッセージパケット数
redirects	redirect パケット受信数
group memb queries	マルチキャスト聴取問い合わせメッセージパケット数
group memb responses	マルチキャスト聴取報告メッセージパケット数
group memb reductions	マルチキャスト聴取終了メッセージパケット数

UDP 情報

項目	内容
Rcvd	受信 UDP 統計情報 （Ver.8.0.50 以前は IPv4 との合計）
datagrams	受信 UDP データグラム総数
no ports	宛先ポートを使用するアプリケーションが起動されていなかった UDP データグラム数
errors	受信 UDP データグラムのうち、宛先ポートでアプリケーションが起動されていないという理由以外で上位のプロトコルに渡すことができなかったデータグラム数
Sent	送信 IPv6 UDP 統計情報
datagrams	送信 UDP データグラム総数

TCP 情報

項目	内容
active opens	TCP コネクションが CLOSE 状態から SYN-SENT 状態に直接状態遷移した回数
passive opens	TCP コネクションが LISTEN 状態から SYN-RCVD 状態に直接状態遷移した回数
attempt fails	TCP コネクションが SYN-SENT 状態かまたは SYN-RCVD 状態から CLOSED 状態へ直接状態遷移した回数と、SYN-RCVD 状態から LISTEN 状態へ直接状態遷移した回数との和。 （TCP コネクションの確立中に RST（Reset）ビットがセットされた "ConnectionRefused" パケットが相手側から 返ってきたとき、この状態遷移が起こり得ます。
established resets	TCP コネクションが ESTABLISHED 状態かまたは CLOSE-WAIT 状態から CLOSED 状態へ直接状態遷移した回数。 （上位のプロトコルから中止するよう依頼されたとき、RST ビットがセットされたセグメントが送られ、この 状態遷移が起こり得ます。）

in segments	受信セグメント数。エラーも含む。現在確立されているコネクションで受信したセグメントを含む。
out segments	送信セグメント数。現在確立されているコネクション上のセグメントは含むが、再送データのみのセグメントは含まず。
retransmit segments	再送セグメント数。即ち、送出されたセグメントのうちで、以前一度以上送出されたことのあるオクテットを含んだセグメントの個数を表します。
in errors	受信エラー（TCP チェックサムエラー）セグメント数
out resets	RST フラグを含んで送信したセグメント数
checksum errors	チェックサムエラー検出回数
bad MD5 authentications	MD5 認証失敗検出回数
ack challenge sent	Ack challenge 送信数

show ipv6 cache

項目	内容
busy	現在のキャッシュエントリ数 [picoIPv6CacheEntries]
frees	現在の残りキャッシュエントリ数
peaks	有効キャッシュ数が最も多かった時点の有効キャッシュ数(Ver.9.6 以降) [picoIPv6CachePeaks]
garbage	フラッシュされて無効になったエントリ数（Ver.8.2 以降）
multicasts	マルチキャストエントリ数 （Ver.8.2 以降） （使用できる最大数は、ユニキャストとマルチキャストの合計になります。）
flybys	キャッシュを使用せずに送信した回数
creates	キャッシュを作成した回数(Ver.9.6 以降) [picoIPv6CacheCreates]
overflows	残りエントリ数が不足し、キャッシュを作成できなかった回数 [picoIPv6CacheOverflows]

8.2.7 ルーティング関連

show ip rip

以下を参照してください。

- show ip rip interface
- show ip rip peer-information
- show ip rip statistics

show ip rip interface

項目	内容
Interface	インタフェース名
RIP	RIP インタフェース状態
Source Address	送信パケットの送信元アドレス
neighbors	RIP 隣接ルータ数
uptime	RIP インタフェース作成経過時間
send	送信バージョン
receive	受信バージョン
authentication type	RIP 認証タイプ
split type	スプリットタイプ
metric offset	メトリックオフセット値
packets input	インタフェースより受信した RIP パケット数
bad packets	インタフェースより受信した不正な RIP パケット数
bad port	不正な port の受信パケット数
bad command	不正な command の受信パケット数
bad version	不正な version の受信パケット数
bad mustbezero	不正な must-be-zero の受信パケット数
bad length	不正な length の受信パケット数
bad authentication	不正な authentication の受信パケット数
bad metric	不正な metric の受信パケット数
routes receive	インタフェースより受信した RIP ルート数
bad routes	インタフェースより受信した不正な RIP ルート数
bad mustbezero	不正な must-be-zero の受信ルート数
bad family	不正な family の受信ルート数
bad nexthop	不正な nexthop の受信ルート数
bad address	不正な address の受信ルート数
bad mask	不正な mask の受信ルート数
bad metric	不正な metric の受信ルート数
packets output	インタフェースより送信した RIP パケット数
routes advert	インタフェースより送信した RIP ルート数
triggered update	トリガードアップデート送信回数

show ip rip peer-information

項目	内容
Neighbor	隣接ルータアドレス
age	RIP 受信後の経過時間
Interface	インタフェース名
Version	隣接ルータの送信 RIP バージョン
packets input	隣接ルータより受信した RIP パケット数
bad packets	隣接ルータより受信した不正な RIP パケット数
bad port	不正な port の受信パケット数
bad command	不正な command の受信パケット数
bad version	不正な version の受信パケット数
bad mustbezero	不正な must-be-zero の受信パケット数
bad length	不正な length の受信パケット数
bad authentication	不正な authentication の受信パケット数
bad metric	不正な metric の受信パケット数
routes receive	隣接ルータより受信した RIP ルート数
bad routes	隣接ルータより受信した不正な RIP ルート数
bad mustbezero	不正な must-be-zero の受信ルート数
bad family	不正な family の受信ルート数
bad nexthop	不正な nexthop の受信ルート数
bad address	不正な address の受信ルート数
bad mask	不正な mask の受信ルート数
bad metric	不正な metric の受信ルート数

show ip rip statistics

項目	内容
memory allocation failures	メモリ確保エラー数
I/O buffer allocation failures	パケットバッファ取得エラー数
timer scheduler failures	RIP スケジューラエラー発生数
responses sent to neighbors queries	RIP 要求メッセージ受信数
changes routing information bases	ルーティングテーブル変更数

show ipv6 rip

以下を参照してください。

- show ipv6 rip interface
- show ipv6 rip peer-information
- show ipv6 rip statistics

show ipv6 rip interface

項目	内容
Interface	インタフェース名
Interface address	インタフェースアドレス
RIPng	インタフェース状態（IPv6 状態） RIPng の状態ではありません。
Number of neighbors	隣接ルータ数

packets input	受信パケット数
bad packets	エラーパケット受信数
bad routes	エラー経路受信数
packets output	送信パケット数

show ipv6 rip peer-information

項目	内容
Neighbor	隣接ルータのアドレス
uptime	隣接ルータから最初にパケットを受信してからの経過時間
Age	前回の応答パケット受信からの経過時間
Interface	隣接ルータが存在するインタフェース名
packets input	受信パケット数
bad packets	エラーパケットを受信した回数
bad routes	エラー経路を受信した回数
bad format	パケットフォーマットが不正
bad command	コマンドコードが不正
bad version	バージョン番号が不正
bad mustbezero	Must be zero フィールドが0でない
no route entry	パケットに経路が含まれていない
bad prefix	プレフィックスが不正
bad prefixlen	プレフィックス長が不正
bad metric	メトリックの値が不正

show ipv6 rip statistics

項目	内容
memory allocation failures	メモリ獲得エラー発生回数
I/O buffer allocation failures	I/O バッファ獲得エラー発生回数
responses sent to neighbors queries	要求パケットに応答した回数
changes made to the routing database	経路を更新した回数（定期更新を含む）

show ip ospf statistics

項目	内容
OSPF router ID	ルータ ID
AS boundary capability	AS 境界ルータかどうか
Import external routes	再配信する外部経路
Orig. default route	デフォルトルートを生成する
FA for Type-7 LSA	Type-7 LSA フォワーディングアドレス
Attached areas	接続されているエリアの数
Estimated # external routes	外部経路の最大数
OSPF packets rcvd	OSPF パケット受信数
OSPF packets rcvd w/ errs	エラーパケット受信数
Transit nodes allocated	生成したルータ情報数
Transit nodes freed	解放したルータ情報数
LS adv. allocated	生成した LSA 数
LS adv. freed	解放した LSA 数
Queue headers alloc	生成したキューの数
Queue headers avail	使用可能なキューの数

# Dijkstra runs	SPF パスツリー計算を実行した回数
Incremental summ. updates	Summary Link の更新回数
Incremental VL updates	Transit Area の Sum Link の更新回数
Buffer alloc failures	メモリ獲得失敗回数
Multicast pkts sent	マルチキャスト送信回数
Unicast pkts sent	ユニキャスト送信回数
LS adv. aged out	LSA タイムアウト回数
LS adv. flushed	LSA フラッシュ回数
OSPF current entries	現在の OSPF 経路数
Incremental ext. updates	外部経路更新回数
OSPF max entries	最大 OSPF 経路数
External LSA database	外部 LSA 情報
Current state	外部経路の状態
Number of LSAs	外部 LSA 数
Number of overflows	オーバーフローした回数

show ipv6 ospf statistics

項目	内容
Process ID	プロセス ID
Router ID	ルータ ID
Areas	エリア数
Interfaces	インタフェース数
Neighbors	ネイバ数
Current number of LSAs	LSA 数
LSA allocated	LSA 作成数
LSA freed	LSA 解放数
Memory allocation errors	メモリ確保失敗
Packet sent	OSPF パケット送信数
Packet received	OSPF パケット受信数
Packet received with errors	OSPF 受信エラー情報
Checksum error	チェックサムエラー
Version mismatch	バージョンエラー
Area-ID mismatch	エリア ID が異なる
Hello interval mismatch	Hello インターバルが異なる
Dead interval mismatch	Dead インターバルが異なる
Stub area mismatch	エリア設定が異なる
DD packet sequence number mismatch	DD シーケンス番号エラー
Bad LS-Request received	異常な LSRequest を受信
Bad LS-Update received	異常な LSUpdate を受信
Interface state change	インタフェースの状態が変化した回数

show ip bgp
show ip bgp neighbors advertised-routes
show ip bgp neighbors received-routes
show ip bgp neighbors routes

項目	内容
Network	ネットワークアドレス
Next Hop	ネクストホップ
Metric	MED

LocPrf	ローカルプリファレンス
Path	AS パス

show ip bgp neighbors

*は detail 指定時のみ表示します。

項目	内容
BGP neighbor	ピアのアドレス
remote AS	ピアの AS 番号
local AS	自 AS 番号
BGP version	BGP のバージョン
remote router ID	ピアのルータ ID
BGP state	ピアの状態
up for	状態が変更してからの経過時間
Last read	最後に BGP メッセージを受信してからの経過時間
last sent	最後に BGP メッセージを送信してからの経過時間
Received/Sent	受信/送信
messages	BGP メッセージ数
notifications	Notification 数
Minimum time between advertisement	最小広告間隔
Minimum time between origination	最小生成間隔
Neighbor capabilities	ケイパビリティ情報
Address family IPv4 Unicast	IPv4 ユニキャスト
Address family IPv6 Unicast	IPv6 ユニキャスト
Route Refresh capability	ルートリフレッシュ
For address family	アドレスファミリ情報
BGP table version	BGP ルーティングテーブルの版数
advertised table version	広告したルーティングテーブルの版数
accepted prefixes	受信経路数
Connections	コネクション状態
established	接続回数
dropped	切断回数
Active connection*	自装置から接続
Passive connection*	相手装置から接続
TCB*	テーブルアドレス
state*	ピアの状態
hold time	ホールドタイム
keepalive interval	キープアライブ送信間隔
Local host	自アドレス
local port	自ポート番号
Foreign host	ピアのアドレス
foreign port	ピアのポート番号
TTL	接続可能なホップ数
Messages*	BGP メッセージ統計
Received/ Sent	送信/受信情報
messages	BGP メッセージ数の合計
opens*	Open メッセージ数
updates*	Update メッセージ数

keepalives*	Keep alive メッセージ数
route refreshs*	Route Refresh メッセージ数
notifications	Notification メッセージ数
Message header errors*	BGP メッセージヘッダエラー統計
header errors*	ヘッダエラーの合計
connection not synchronized*	接続の同期が取れていない
bad message length*	メッセージ長不正
bad message type*	メッセージ種別不正
OPEN message errors*	Open メッセージエラー統計
open message errors*	Open メッセージエラーの合計
unsupported version number*	未サポートのバージョン番号
bad peer as*	ピアの AS 番号が不正
bad bgp identifier*	BGP 識別子が不正
unsupported optional parameter	未サポートのオプションパラメータ
authentication failure*	認証エラー
unacceptable hold time*	ホールドタイムが合っていない
unsupported capability*	サポートしていないケイパビリティ
UPDATE message errors*	Update メッセージエラー統計
update message errors*	Update メッセージエラーの合計
malformed attribute list*	属性リストが不正
unrecognized well-known attribute*	周知属性が識別できない
missing well-known attribute*	周知属性がない
attribute flags error*	属性フラグエラー
attribute length error*	属性長エラー
invalid origin attribute*	オリジン属性が無効
as routing loop*	AS 番号のルーティングループを検出
invalid next-hop attribute*	ネクストホップ属性が不正
optional attribute error*	オプション属性エラー
invalid network field*	ネットワークフィールドが不正
malformed as-path*	AS パスが不正
Other errors*	その他のエラー
hold timer expired*	ホールドタイマの時間切れ検出
finite state machine errors*	状態遷移の異常検出
cease notifications*	切断要求

show ip bgp summary

項目	内容
Neighbor	ピアのアドレス
V	BGP バージョン
AS	ピアの AS 番号
MsgRcvd	受信メッセージ数
MsgSent	送信メッセージ数
Up/DownTime	経過時間
State	ピアの状態
Total number of neighbors	ピアの数

show ip bgp paths

項目	内容
Address	パス情報格納アドレス
Refcnt	パス情報参照経路数
Next hop	ネクストホップ
MED	MED 情報
LocPrf	ローカルプリファレンス
Path	AS パス情報

8.2.8 マルチキャスト関連

show ip pim statistics（Ver.8.4 以降）

項目	内容
PIM system statistics	
null register sent	Null regsiter 送信数
null register received	Null register 受信数
register received from PMBR	PMBR からの Register 受信数
register encapsulated	カプセル化した Register 数
register decapsulated	カプセル化解除した Register 数
register dropped by rate-limiting	Rate-limit 機能により廃棄した Register 数
registering failed because RP is not configured	Register を失敗した回数
PIM message statistics	on system :システム全体の統計 on インタフェース名 :インタフェース単位の統計
hello sent	Hello メッセージ送信数
hello received	Hello メッセージ受信数
register sent	Register メッセージ送信数
register received	Register メッセージ送信数
register-stop sent	Register-stop メッセージ送信数
register-stop received	Register-stop メッセージ送信数
join/prune sent	Join/Prune 送信数
join/prune received	Join/Prune 受信数
bootstrap sent	Bootstrap メッセージ送信数
bootstrap received	Bootstrap メッセージ受信数
assert sent	Assert メッセージ送信数
assert received	Assert メッセージ受信数
graft sent	Graft メッセージ送信数
graft received	Graft メッセージ受信数
graft-ack sent	Graft-ack メッセージ送信数
graft-ack received	Graft-ack メッセージ受信数
c-rp-adv sent	Candidate-RP-Advertisement メッセージ送信数
c-rp-adv received	Candidate-RP-Advertisement メッセージ受信数
unknown received	不明なメッセージの受信数
dropped in sending	送信時の廃棄数
dropped in receiving	受信時の廃棄数

8.2.9 トンネル関連

show tunnel status

項目	内容
Total statistics	全体情報
packets input	トンネルパケット受信総数
bytes	トンネルパケット受信総バイト数
errors	トンネルパケット受信エラー総数
packets output	トンネルパケット送信総数
bytes	トンネルパケット送信総バイト数
errors	トンネルパケット送信エラー総数
Interface	トンネルインタフェース名
Tunnel mode	トンネル種別
Tunnel status	状態の詳細が表示されます。 （終端への経路がない場合は Down となる） Tunnel is ready 運用可能な状態 Tunnel mode is not specified:mode モードが設定されていない Source address selection failed ソースアドレス自動選択に失敗 IPv6 scope-zone selection failed IPv6 スコープゾーン自動選択に失敗 Destination is unreachable 宛先へ到達するための経路が無い Destination is never reachable via loopback interface 宛先へ到達するための経路がループバックインタフェースを向いている Destination address is not configured 宛先アドレスが設定されていない Source address is not configured on specified interface 指定されたインタフェースにアドレスが割り当てられていない Source address is not assigned to local interface 指定されたソースアドレスがどのインタフェースにも割り当てられていない Destination address is assigned to local interface 指定された宛先アドレスがインタフェースに割り当てられている Number of nested encapsulations is over limit ネスト数が制限値を超えている Invalid destination address 宛先アドレスが間違っている Invalid IPv6 scope-zone IPv6 スコープゾーン名が間違っている IPsec is not ready IPsec が通信を開始する準備が整っていない
Destination address	トンネル終端先アドレス
Source address	トンネル送信元アドレス
Outgoing interface	下位レイヤインタフェース
Interface MTU	インタフェース MTU

Path MTU	トンネル区間パス MTU
Statistics	インタフェース別統計情報
packets input	トンネルパケット受信数
bytes	トンネルパケット受信バイト数
errors	トンネルパケット受信エラー数
packets output	トンネルパケット送信数
bytes	トンネルパケット送信バイト数
errors	トンネルパケット送信エラー数
Received ICMP messages	
errors	トンネル区間 ICMP エラー受信数 （項目は IPv4 と IPv6 で異なる）

IPv4 でカプセル化する Tunnel,Auto Tunnel 情報

項目	内容
network unreachable	network unreachable 受信数
host unreachable	host unreachable 受信数
protocol unreachable	protocol unreachable 受信数
fragmentation needed	fragmentation needed and DF bit set 受信数
TTL exceeded	TTL exceeded 受信数
parameter problem	parameter problem 受信数

IPv6 でカプセル化する Tunnel,Auto Tunnel 情報

項目	内容
no route to destination	no route to destination 受信数
administratively prohibited	administratively prohibited 受信数
beyond scope of source address	beyond scope of source address 受信数
address unreachable	address unreachable 受信数
port unreachable	port unreachable 受信数
packet too big	packet too big 受信数
hop limit exceeded in transit	hop limit exceeded in transit 受信数
parameter problem	parameter problem 受信数

GRE 統計情報

項目	内容
GRE statistics	GRE 統計情報（Ver.8.9 以降）
GRE option statistics	GRE 統計情報（Ver.8.8 以前）
incorrect key received	不正なキー受信数
incorrect checksum received	不正なチェックサム受信数
keepalive sent	キープアライブ送信数
reply received	キープアライブ応答受信数
keepalive received	キープアライブ受信数
reply sent	キープアライブ応答送信数
Last sent sequence number	最後に送信したシーケンス番号
Last received sequence number	最後に受信したシーケンス番号
Bridged packets	Ether フレームを処理
IPv4 packets	IPv4 パケットを処理
IPv6 packets	IPv6 パケットを処理
encaps	カプセル化数
decaps	カプセル化解除数

8.2.10 IKE/IPsec 関連

show ike statistics

項目	内容
Phase1 Statistics	フェーズ 1 ネゴシエーション統計情報
success	成功数
failure	失敗数
hash errors	ハッシュエラー数
config errors	コンフィグミスによるエラー数
timeout errors	タイムアウト回数
resend packet	再送パケット数
Phase2 Statistics	フェーズ 2 ネゴシエーション統計情報
success	成功数
failure	失敗数
request errors	要求失敗数
hash errors	ハッシュエラー数
config errors	コンフィグミスによるエラー数
timeout errors	タイムアウト回数
resend packet	再送パケット数
Notify message type	Notify メッセージ情報
Rcvd/Sent	送信/受信統計情報
invalid payload type	不正なペイロードタイプ
doi not supported	サポートしていない DOI 番号
situation not supported	サポートしていない situation
invalid cookie	不正なクッキー
invalid major version	不正なメジャーバージョン
invalid minor version	不正なマイナーバージョン
invalid exchange type	不正な交換タイプ
invalid flags	不正なフラグ
invalid message id	不正なメッセージ ID
invalid protocol id	不正なプロトコル ID
invalid spi	不正な SPI
invalid transform id	不正な Transform 番号
attributes not supported	サポートしていない属性
no proposal chosen	プロポーザル不一致
bad proposal syntax	プロポーザルシンタックス不正
payload malformed	不正なペイロード
invalid key information	未サポート
invalid id information	不正な ID 情報
invalid cert encoding	未サポート
invalid certificate	未サポート
cert type unsupported	未サポート
invalid cert authority	未サポート
invalid hash information	不正なハッシュ情報
authentication failed	未サポート
invalid signature	未サポート
address notification	未サポート
notify sa lifetime	未サポート
certificate unavailable	未サポート

unsupported exchange type	未サポートの交換タイプ
unequal payload lengths	ペイロード長不正
connected	COMMIT ビット connected 送受信数
responder lifetime	responder lifetime 送受信数
replay status	replay status 送受信数
initial contact	イニシャルコンタクト送受信数
keepalive	キープアライブ送受信数
keepalive ack	キープアライブ応答送受信数
unknown type	上記以外のエラー
Delete protocol type	デリートメッセージ
isakmp	ISAKMP
ah	AH
esp	ESP
unknown type	上記以外の種別

show ipsec statistics

Rcvd

項目	内容
Rcvd	受信統計情報
process switching	遅いパスでパケットが処理された回数 - キャッシュ登録前・ホスト受信時・フラグメント等
esp encap history des	ESP DES パケット受信数
esp encap history 3des	ESP 3DES パケット受信数
esp encap history aes	ESP AES パケット受信数
esp encap history null	ESP NULL パケット受信数
esp auth history md5	ESP MD5 パケット受信数
esp auth history sha1	ESP SHA-1 パケット受信数
esp auth history sha2-*	ESP SHA-2 パケット受信数
ah auth history　md5	AH MD5 パケット受信数
ah auth history　sha1	AH SHA1 パケット受信数
ah auth history sha2-*	AH SHA2 パケット受信数
succeeded	正常受信した IPsec パケット数
以下は失敗理由を示す統計情報	
sp errors	SP 検索エラー数 - 解除したパケットが SP 対象外の場合
not found esp sa	受信 ESP パケットの SPI に該当する SA が存在しない回数
not found ah sa	受信 AH パケットの SPI に該当する SA が存在しない回数
esp errors	ESP パケットの解除失敗数 理由は decrypt failure 以下を参照してください
ah errors	AH パケットの解除失敗数 理由は decrypt failure 以下を参照してください
ahesp errors	AHESP パケットの解除失敗数 理由は decrypt failure 以下を参照してください

decrypt failure	受信 ESP パケットの復号失敗数 - ESP ヘッダレングス不正 - 暗号ペイロードレングス不正 - アライメント不正
auth failure	受信 AH/ESP パケットの認証データ不正検出数
invalid icv	SA 無効時の送信エラー数
invalid key	受信 AH/ESP パケット解除時の鍵情報不正検出数 - 内部データベースに鍵情報が無い - 内部データベースの鍵情報が間違い
invalid pkt	復号後の IP ヘッダサイズ不正数
replay errors	リプレイ攻撃検出数
seq over	受信 IPsec パケットのシーケンス番号が最大値(0xffffffff)に達した回数
seclevel miss	セキュリティレベルが require のとき、IPsec されないパケットを受信して廃棄した回数
other errors	上記以外のエラー数 - 内部データベース不正など
failed	エラーによるパケット廃棄回数

Sent

項目	内容
Sent	送信統計情報
process switching	遅いパスでパケットが処理された回数 - キャッシュ登録前・ホスト受信時・フラグメント等
esp encap history des	ESP DES パケット送信数
esp encap history 3des	ESP 3DES パケット送信数
esp encap history aes	ESP AES パケット受信数
esp encap history null	ESP NULL パケット送信数
esp auth history md5	ESP MD5 パケット送信数
esp auth history sha1	ESP SHA-1 パケット送信数
esp auth history sha2-*	EPS SHA-2 パケット送信数
ah auth history　md5	AH MD5 パケット送信数
ah auth history　sha1	AH SHA1 パケット送信数
ah auth history sha2-*	AH SHA2 パケット送信数
succeeded	正常送信した IPsec パケット数
以下は失敗理由を示す統計情報	
key exchg req	SA がない場合の IKE による鍵作成回数
unavailable sa	IPsec 送信時の SA 無効によるパケット廃棄回数 - 自動鍵 　SA 確立前に送信した場合 - 固定鍵 　SA の設定がない場合
esp errors	ESP パケットの送信失敗数 理由は decrypt failure 以下を参照してください
ah errors	AH パケットの送信失敗数 理由は decrypt failure 以下を参照してください

ahesp errors	AHESP パケットの送信失敗数 理由は decrypt failure 以下を参照してください
encrypt failure	送信 ESP パケットの暗号化失敗数 - 鍵情報のレングス不正
auth failure	AH/ESP パケットの認証データ付与失敗数 - 鍵情報のレングス不正
seq over	送信 IPsec パケットのシーケンス番号が最大値(0xffffffff)に達した回数
invalid key	暗号化/認証時の鍵情報不正数 - 内部データベースに鍵情報が無い - 内部データベースの鍵情報が間違い
invalid pkt	
endpoint unreach	SA 終点への到達性がなかった回数 - ルーティングテーブルに経路がない
encap size over	MTU 超過によるパケット廃棄数
nest over	IPsec 又は IPIP トンネルのネストが 3 段を超過して適用されたことによるパケット廃棄数 - 内部でループする設定がある場合など
no buffer	バッファを確保できなかった回数 - グローバルバッファ枯渇時が該当
other errors	上記以外のエラー発生数 - 出力インタフェースがダウンしている - 下位レイヤで、何らかのエラー(ARP 未解決等)が発生したため IPsec パケットの送信に失敗した
failed	エラーによるパケット廃棄回数

show ikev2 statistics

項目	内容
Initial Exchange	イニシャルエクスチェンジ
IKE rekey	IKE-SA リキー
Child rekey	Child-SA リキー
IKE delete	IKE-SA delete
Child delete	Child-SA delete
Initiator/ Responder	イニシエータ・レスポンダ
success	成功回数
fail	失敗回数
Error	
no proposal chosen	プロポーザルが選択できなかった回数
auth fail	認証失敗回数
invalid KE	KE ペイロード不一致検出
invalid syntax	予期しない IKE パケット検出
decrypt error	復号エラー回数
ICV error	ICV エラー回数
config error	ネゴシエーションが不可能な設定でのネゴシエーション開始エラー検出
memory error	メモリ確保失敗
other error	その他エラー検出
Exchange	
SA-INIT	IKE_SA_INIT Type での Exchange

AUTH	IKE_AUTH Type での Exchange
CREATE-CHILD-SA	CREATE_CHILD_SA Type での Exchange
INFORMATIONAL	INFORMATIONAL Type での Exchange
SESSION-RESUME	IKE_SESSION_RESUME Type での Exchange
unknown	未定義な Type での Exchange
send request	要求送信回数
recv response	応答受信回数
recv request	要求受信回数
send response	応答送信回数
resend	再送回数
timeout	タイムアウト回数
Notify status	
initial contact	Initial contact 通知
set window size	Window サイズ通知
additional ts possible	TS 追加可能通知
ipcomp supported	IPCOMP サポート通知
nat detection source ip	Source IP アドレスでの NAT 検出
nat detection destination ip	Destination IP アドレスでの NAT 検出
cookie	Cookie の通知
use transport mode	Transport mode 利用の通知
http cert lookup supported	HTTP による証明書取得サポート通知
rekey sa	Child SA のリキー通知
esp tfc padding not supported	ESP での TFC パディング未サポート通知
non first fragment also	フラグメントパケット送受信の通知
mobike supported	MOBIKE サポートの通知
additional ip4 address	追加 IPv4 アドレス
additional ip6 address	追加 IPv6 アドレス
no additional address	アドレス追加できないことを通知する
update sa addresses	SA のアドレス更新
cookie2	Cookie2 の通知
no nats allowed	NAT の不許可の通知
auth lifetime	認証期間設定
multiple auth supported	複数認証サポート通知
another auth follows	複数認証サポート時、他の認証を使いたいことを通知する。
redirect supported	Redirect のサポート通知
Redirect	Redirect の通知
redirect from	Redirect でオリジナル VPN GW の通知
ticket lt opaque	Session Resumption 利用時での TICKET_LT_OPAQUE の通知（LifeTime 付き Ticket）
ticket request	Session Resumption Ticket リクエストの通知
ticket ack	Session Resumption Ticket Ack の通知
ticket nack	Session Resumption Ticket Nack の通知
ticket opaque	Session Resumption Ticket が opaque の通知
link id	VirtualLink での SA 生成通知
use wesp mode	Wrapped Encapsulating Security Payload モード使用の通知
rohc supported	Rohc サポートの通知
Other	
send	送信回数

recv	受信回数
Notify error	Notity 受信
unsupport critical payload	Critical bit が立ったペイロードの未サポート
invalid ike spi	不正な IKE SPI 番号検出
invalid major version	不正メジャーバージョン検出
invalid syntax	不正なシンタックスを検出
invalid message id	不正なメッセージ ID 検出回数
invalid spi	不正な SPI 番号検出回数
no proposal chosen	プロポーザル選択
invalid ke	KE ペイロード検証失敗
authentication failed	認証失敗
single pair required	1 ペアのみを要求することを通知
no additional sas	SA 追加失敗
internal address failure	内部アドレス不正
failed cp required	コンフィグペイロードの要求
ts unacceptable	TS の受け入れ拒否
invalid selectors	不正セレクタ検出
unacceptable addresses	アドレスの更新不可の通知
unexpected nat detected	予期しない NAT 検出
use assigned HoA	Home Address アサインの使用
temporary failure	受信しても成功できない状態を通知
child sa not found	Child-SA が存在しない
other	その他エラー

show ikev2 child-sa

項目	内容
Statistics	
Outbound	送信側統計
packets	送信パケット数
octets	送信オクテット数
cipher failure	暗号化失敗
out of memory	メモリエラー
ts unacceptable	トラフィックセレクタ適用外パケット数
misc error	上記以外のエラー
Inbound	受信側統計
packets	受信パケット数
octets	受信オクテット数
invalid sa	SA が不正な受信パケット数
replay detected	リプレイ検出回数
integrity failure	認証失敗
cipher failure	暗号化失敗
packet truncated	パケット長不正
invalid padding	不正なパディング
unknown protocol	未知のプロトコル
out of memory	メモリエラー
ts unacceptable	トラフィックセレクタ受入れ不可
misc error	その他のエラー

show dmvpn detail（Ver9.2 以降）

項目	内容
Statistics	（現在の接続のみの統計情報）
packets input	受信パケット数
errors	受信エラー数 （不明な送信元・プロトコル異常など）
packets output	送信パケット数
errors	送信エラー数 （送信先アドレス解決失敗・GRE カプセル化失敗など
Total statistics	（過去の接続も含めた統計情報）
packets input	総受信パケット数
errors	総受信エラー数
packets output	総送信パケット数
errors	総送信エラー数
DMVPN statistics:	-
up	ダイナミック VPN 機能 up 回数
down	ダイナミック VPN 機能 down 回数
Down reasons:	-
IKE peer down	対向先からの切断通知受信数
IKE timeout	IKE タイムアウト数
other IKE reason	他の IKE 要因切断数（コマンド等）
NHRP cache expired.	キャッシュタイムアウト数
NHRP retry out	再送タイムアウト数
NHRP NAK received	NAK 応答受信数
NHRP error indication received	エラー通知受信数
NHRP unknown reply received	不明応答受信数
NHRP cache removed	NHRP キャッシュ削除数（コマンド等）
NHRP interface down	インタフェースダウン数
NHRP unexpected	不正応答受信数 （不明な送信元からの応答・解決アドレスが自装置など）
NHRP no cie payload	cie ペイロードなしの解決応答数
too many connections	接続超過数

8.2.11 QoS 関連

show policy-map interface（Ethernet 以外）

項目	内容
Current processing	キューイングされているパケット数
Threshold for tail drop	パケット用キューの最大キュー長 （パケット数）
Total input	キューイングされた総パケット数
Tail drops	キュー長オーバーで破棄したパケット数 （最大キュー長を超える等）
high	優先度が high のパケット数
medium	優先度が medium のパケット数
normal	優先度が normal のパケット数
low	優先度が low のパケット数
sub-a	優先度が sub-a のパケット数
sub-b	優先度が sub-b のパケット数
sub-c	優先度が sub-c のパケット数
sub-d	優先度が sub-d のパケット数

show policy-map interface（Ethernet）

Device 項目	デバイス単位の統計情報
Device buffer packets, bytes peak packets, bytes	デバイスのキュー情報 現在の総パケット数、サイズ 最大パケット数、サイズ
Queued packets, bytes peak packets, bytes	デバイス配下の全 I/F のキュー情報 現在の総パケット数、サイズ 最大パケット数、サイズ
Interface 項目	インタフェース単位のキュー情報
Queued packets, bytes peak packets, bytes	I/F 配下の全クラスのキュー情報 現在の総パケット数、サイズ 最大パケット数、サイズ
Burst size	全クラスのバーストサイズの合計値 （LLQ 設定時のみ）
Class 項目	クラス単位のキュー情報
Queued packets, bytes peak packets, bytes	クラス配下の全 Queue のキュー情報 現在の総パケット数、サイズ 最大パケット数、サイズ
LLQ 項目（priority 設定時のみ）	LLQ 情報
Traffic policing is enabled, activated	ポリシング動作回数
CIR / Bc / Be / Tc	ポリシングの各設定値
Current token	内部計算用トークン値
CBQ 項目（bandwidth 設定時 / デフォルト）	CBQ 情報
Bandwidth percent, weight	CBQ 情報 割合、計算された重み値
シェーピング項目（shape 設定時のみ）	クラスシェーピング情報
Traffic shaping is enabled, activated	シェーピング動作回数
CIR / Bc / Be / Tc	シェーピングの各設定値

Current token	内部計算用トークン値
Queue 項目	内容（未使用の優先キューは表示なし）
normal packets limit peak	優先度（high / medium / normal / low / sub-a / sub-b / sub-c / sub-d） キューイングされたパケット数 キューの上限数（queue-limit 設定時のみ） キューイングされた最大パケット数
Output packets, bytes	送信パケット数、送信パケットサイズ
tail drops	オーバーフローによる廃棄数
excess bandwidth	帯域を超えたため廃棄したパケット数（LLQ で有効）
buffer exhausted	パケットバッファ枯渇による廃棄数
Local fragments	ルータ内でフラグメントしたパケット
output	送信数
discarded	廃棄数

show bandwidth-policy-map interface（Ethernet 以外）

項目	内容
Service policy unity is	基本 I/F 上でサブ I/F もまとめて BRS/PQ されているかどうかを表示
Priority control between interfaces is	I/F 間 PQ が有効かどうかを表示
Bandwidth-class	帯域クラス名
Bandwidth	最小予約帯域
Belonging interfaces	帯域クラスに属するインタフェース
Total input	キューイングされた総パケット数
Current processing	現在キューイングされているパケット数
tail drops	キュー長オーバーで破棄したパケット数（最大キュー長を超える等）
Bandwidth-class priority queues	I/F 間 PQ のキューにキューイングされている I/F の数
high	優先度が high のパケット数
medium	優先度が medium のパケット数
normal	優先度が normal のパケット数
low	優先度が low のパケット数
sub-a	優先度が sub-a のパケット数
sub-b	優先度が sub-b のパケット数
sub-c	優先度が sub-c のパケット数
sub-d	優先度が sub-d のパケット数

8.2.12 CRTP 関連

show ip rtp header-compression

項目	内容
Full Header Packets	Full Header パケットの圧縮伸張数
Compressed UDP Packets	Compressed UDP パケットの圧縮伸張数
Compressed RTP Packets	RTP パケットの圧縮伸張数
TCP Full Header Packets	Compressed TCP(UDP)パケットの圧縮伸張数
Non TCP Full Header Packets	Non TCP(UDP) Full Header パケットの圧縮伸張数
Compressed Non TCP Packets	Compressed Non TCP(UDP)パケットの圧縮伸張数
Compressed	圧縮したパケット数
Decompressed	伸張したパケット数
Context State Packets	Context State パケット
sent	送信数
rcvd	受信数
Total	圧縮伸張パケット総数
Error	エラー数
connection limit over(compress)	圧縮時に圧縮接続数を超えた回数
connection limit over(decompress)	伸張時に圧縮接続数を超えた回数
resource busy(compress)	圧縮時に圧縮接続最大数（256）を超えた回数
resource busy(decompress)	伸張時に圧縮接続最大数（256）を超えた回数
packet size error(decompress)	受信パケットの内容に誤りがありパケットサイズが正しくなかった回数
compressed packet type error (decompress)	受信パケットの種別が違っていた回数
Sequence no. error(decompress)	受信パケットのシーケンス番号が違っていた回数
Unsupported context type(decompress)	受信パケットの Context ID が 8 ビットでなかった回数
Unsupported protocol(decompress)	受信 Full Header パケットが TCP/UDP（RTP）でなかった回数

show ip rtp tcp-header-compression

項目	内容
Full Header Packets	Full Header パケットの圧縮伸張回数
Compressed TCP Packets	Compressed TCP パケットの圧縮伸張回数
Compressed TCP Nodelta Packets	Compressed TCP Nodelta パケットの伸張回数
Compressed	圧縮したパケット数
Decompressed	伸張したパケット数
Context State Packets	Context State パケット送受信数
sent	送信数
recv	受信数

Total	圧縮伸張パケット総数
Error	エラー数
connection limit over(compress)	圧縮時に圧縮接続数を超えた回数
connection limit over(decompress)	伸張時に圧縮接続数を超えた回数
resource busy(compress)	圧縮時に圧縮接続最大数（256）を超えた回数
resource busy(decompress)	伸張時に圧縮接続最大数（256）を超えた回数
packet size error(decompress)	受信したパケットの内容に誤りがありパケットサイズが正しくなかった回数

8.2.13 VLAN 関連

show vlans

項目	内容
Virtual LAN ID	802.1Q Encapsulation インタフェースの VLAN ID
TPID	VLAN-ID インタフェースの TPID 値
vLAN Trunk Interface	VLAN-ID インタフェースの名称
Protocols	ネットワーク層プロトコル名称（IPv4/IPv6）
Address	稼働中の IP アドレス
Received	受信パケット数 show ip(v6) traffic コマンドの IP Statistics-Rcvd として表示するものと同内容
Transmitted	送信パケット数 show ip(v6) traffic コマンドの IP Statistics-Sent として表示するものと同内容
Virtual Bridged LAN	ポート VLAN を使用するインタフェース名
Group	VLAN グループ値
Assigned ports	割り当てられたポート番号
Input frames	受信フレーム数
Output frames	送信フレーム数

8.2.14 VRRP 関連

show vrrp（Ver.8.2 以降）

※Statistics 以降は show vrrp <ID> statistics と同じ内容になります。

項目	内容
サマリ情報	
Interface	インタフェース
Grp（～Ver8.5）、VRID（Ver8.6～）	Virtual Router グループ ID
Pri	プライオリティ
Pre	プリエンプトモード
State	VRRP 状態
Master addr	Master の IP アドレス
Group addr（Ver8.5 以前）	仮想 IP アドレス
詳細情報（detail，ID 指定）	
Virtual router group	Virtual Router グループ ID
Virtual router status	
State	VRRP 状態
Virtual router IP address	仮想 IP アドレス
Virtual router IPv6 address	仮想 IPv6 アドレス（Ver8.6 以降）
Master IP address	Master の IP アドレス
Master IPv6 address	Master の IPv6 アドレス（Ver8.6 以降）
MAC address	仮想 MAC アドレス
Priority	プライオリティ
History	過去 10 件の履歴情報
time	状態が変化した時間
state	VRRP 状態
Statistics	
Become master	マスタに遷移した回数 (vrrpStatsBecomeMaster)
Advertise	広告パケット送信/受信数 (vrrpStatsAdvertiseRcvd)
Priority zero	0プライオリティ（shutdown） 送信/受信数 (vrrpStatsPriorityZeroPktsRcvd) (vrrpStatsPriorityZeroPktsSent)
Errors	
advertise interval errors	広告送信間隔エラー (vrrpStatsAdvertiseIntervalErrors)
authentication failures	認証エラー (vrrpStatsAuthFailures)
address list errors	受信アドレスリストエラー (vrrpStatsAddressListErrors)
invalid authentication type	無効な認証タイプ (vrrpStatsInvalidAuthType)
authentication type mismatch	認証タイプミスマッチ (vrrpStatsAuthTypeMismatch)
length errors	パケット長エラー (vrrpStatsPacketLengthErrors)
invalid type packets	パケット種別エラー (vrrpStatsInvalidTypePktsRcvd)
IP TTL errors	TTL エラー (vrrpStatsIpTtlErrors)

show vrrp statistics（Ver.8.2 以降）

※show vrrp <ID> statistics は show vrrp detail と同じ内容になります。

項目	内容
Virtual router statistics	仮想ルータ統計情報
Errors	
checksum errors	チェックサムエラー (vrrpRouterChecksumErrors)
version errors	バージョンエラー (vrrpRouterVersionErrors)
VR-ID errors	Virtual Router ID エラー (vrrpRouterVrIdErrors)

show vrrp（Ver.8.1 以前）

*Become Master 以降は show vrrp statistics と同じ内容になります。

項目	内容
Virtual Router Group	Virtual Router グループ ID
Virtual MAC address	Virtual Router MAC アドレス
Virtual Router Status	Virtual Router ステータス
Virtual Router Priority	Virtual Router プライオリティ
Virtual IP Address Count	Virtual Router アドレスの数
Associated IP Address	Virtual Router アドレス
Master IP Address	現在の MASTER の IP アドレス
Authentication Type	認証タイプ
Advertisement Interval	広告パケット送信間隔
Preempt Mode	プリエンプトモード
Virtual Router Protocol	Virtual Router サポートプロトコル
Virtual-Host	Virtual-Host 設定の有無
Become Master	マスタになった回数
Advertise Received	広告パケット受信数
Advertise Interval Errors	広告送信間隔エラー
Authentication Failures	認証エラー
Priority Zero Received	0プライオリティ（shutdown）受信数
Priority Zero Sent	0プライオリティ（shutdown）送信数
Address List Errors	受信アドレスリストエラー
Invalid Authentication Type	無効な認証タイプ
Authentication Type Mismatch	認証タイプミスマッチ
Packet Length Errors	パケット長エラー

show vrrp statistics（Ver.8.1 以前）

項目	内容
Virtual Router Statistics	仮想ルータ統計情報
Checksum Errors	チェックサムエラー (vrrpRouterChecksumErrors)
Version Errors	バージョンエラー (vrrpRouterVersionErrors)
VR-ID Errors	Virtual Router ID エラー (vrrpRouterVrIdErrors)

Invalid Type Packets	パケットタイプエラー (vrrpStatsInvalidTypePktsRcvd)
IP TTL Errors	TTL エラー (vrrpStatsIpTtlErrors)
VR Session	仮想ルータセッション統計情報
Become Master	マスタになった回数 (vrrpStatsBecomeMaster)
Advertise Received	広告パケット受信数 (vrrpStatsAdvertiseRcvd)
Advertise Interval Errors	広告送信間隔エラー (vrrpStatsAdvertiseIntervalErrors)
Authentication Failures	認証エラー (vrrpStatsAuthFailures)
Priority Zero Received	0プライオリティ（shutdown）受信数 (vrrpStatsPriorityZeroPktsRcvd)
Priority Zero Sent	0プライオリティ（shutdown）送信数 (vrrpStatsPriorityZeroPktsSent)
Address List Errors	受信アドレスリストエラー (vrrpStatsAddressListErrors)
Invalid Authentication Type	無効な認証タイプ (vrrpStatsInvalidAuthType)
Authentication Type Mismatch	認証タイプミスマッチ (vrrpStatsAuthTypeMismatch)
Packet Length Errors	パケット長エラー (vrrpStatsPacketLengthErrors)

8.2.15 ネットワークモニタ関連

show watch-group（サマリ表示）

項目	内容
Total	Watch グループ名
Normal	障害未検出状態のプロファイル数
Stand	障害検出中のプロファイル数
Group name	Watch グループ名
Sequence	シーケンス番号
Status	状態（normal/stand）
Variance	障害発生検出回数
Wait	起動待ち時間

show watch-group detail/プロファイル名指定（Ver.8.5 以降）

項目	内容
Watch-group	Watch グループ名
Sequence	シーケンス番号
Status: normal/stand/ -	プロファイル状態（未発生/発生/未起動） 抑止の場合は suppress も表示
Elapsed variance time	プロファイルの現在の障害の経過時間 （障害検出中のみ表示）
Profile variance counts	プロファイルの障害検出回数
Profile restore counts	プロファイルの障害復旧回数
Suppress variance counts	イベント発生抑止回数
Suppress restoration counts	イベント復旧抑止回数

Profile history Time: Event: variance/resotorer Status: normal/stand	プロファイル単位の履歴 発生日時 イベントの発生/復旧 プロファイルの状態（未発生/発生）
Event	イベント単位の情報
Status: normal/stand/ -	イベントの状態（未発生/発生/未起動）
Elapsed variance time	イベントの現在の障害の経過時間 （障害検出中のみ表示）
Event variance counts	イベント発生回数
Event restore counts	イベント復旧回数
Probe success counts	監視パケットの成功応答回数
Probe failure counts	監視パケットの失敗応答回数
Probe history Time: Result: success/failure Round Trip: round-trip (ms)　min/avg/max	監視パケットの送信履歴 発生日時 応答あり/なし 応答時間 応答時間の最小/平均/最大
Action	アクション単位の情報
Status	restoration：アクション未実行 executing　：アクション実行中

show watch-group detail/プロファイル名指定（Ver8.4 以前）

項目	内容
Watch-group	Watch グループ名
Sequence	シーケンス番号
Event	設定したイベント
Status	イベントの状態 normal：イベント未発生 stand　：イベント発生中 -　　：停止中
Last start time	最終実行時間
Elapsed watch time	開始からの経過時間
Last stop time	最終停止時間
Last variance time	最後のイベント発生時刻
Elapsed variance time	発生中のイベント発生からの経過時間
Last restore time	最後のイベント復旧時刻
Time in variance	前回のイベント発生時間
Event variance counts	イベント発生回数
Event restore counts	イベント復旧回数
packets sent.	ICMP echo 送信数
packets failed.	ICMP echo 送信失敗数
packets received.	ICMP echo reply 受信数
packets lost	ICMP echo reply が戻らなかった回数
Action	設定したアクション
Status	アクションの状態 restoration：アクション未実行 executing　：アクション実行中
Summarized variance seconds	合計イベント発生時間
Summarized variance counts	合計イベント発生回数
Summarized restore counts	合計イベント復旧回数

Event History	イベント履歴
Sequence	シーケンス番号
Time	時刻
event	イベント種別

show ip watch

項目	内容
type	監視タイプ（ホスト監視/ルート監視）
status	ステータス（-/normal/failure）
last start time	監視開始時刻
last stop time	監視停止時刻
elapsed watch time	現在の監視経過時間
elapsed failure time	現在の障害経過時間
packets sent.	送信パケット数（ホスト監視のみ）
packets received.	受信パケット数（ホスト監視のみ）
total failure seconds	合計障害時間
total failure counts	合計障害回数

8.2.16 アクセスリスト関連

show access-list

項目	内容
Entries	MAC アクセスリストに登録されているエントリ数
Hits	MAC アクセスリストにヒットした回数
Refs	MAC アクセスリストを参照した回数

ACCESS-LIST-NAME が指定された場合、そのアクセスリストのエントリ毎にヒットカウントが表示されます。

show access-list cache

項目	内容
entries	現在の MAC アクセスリストキャッシュエントリ数
free	現在の残り MAC アクセスリストキャッシュエントリ数
overflow	残りエントリ数が無くなった回数 （残りエントリがなくなった場合、登録されている MAC アクセスリストエントリを 1 回ごと参照する必要があるため、性能に影響を与えます。）
p (Codes)	Permit キャッシュ
d (Codes)	Deny キャッシュ
n (Codes)	Not Found キャッシュ （MAC アクセスリストを参照して、マッチするエントリがなかった場合、Not Found でキャッシュされます。）
hits	キャッシュヒット回数

show ip/ipv6 access-list

項目	内容
entries	アクセスリストに登録されているエントリ数
hits	アクセスリストにヒットした回数
refs	アクセスリストを参照した回数

ACCESS-LIST-NAME が指定された場合、そのアクセスリストのエントリ毎にヒットカウントが表示されます。

show ip/ipv6 access-list cache

項目	内容
entries	現在のアクセスリストキャッシュエントリ数
free	現在の残りアクセスリストキャッシュエントリ数
overflow	残りエントリ数が無くなった回数 （残りエントリがなくなった場合、登録されているアクセスリストエントリを 1 回ごと参照する必要があるため、性能に影響を与えます。）
p (Codes)	Permit キャッシュ
d (Codes)	Deny キャッシュ
n (Codes)	Not Found キャッシュ （アクセスリストを参照して、マッチするエントリがなかった場合、Not Found でキャッシュされます。）
hits	キャッシュヒット回数

show ip/ipv6 access-list dynamic

項目	内容
entries	ダイナミックアクセスリストに登録されているエントリ数
hits	ダイナミックアクセスリストにヒットした回数
refs	ダイナミックアクセスリストを参照した回数

ACCESS-LIST-NAME が指定された場合、そのアクセスリストのエントリ毎にヒットカウントが表示されます。

8.2.17 トラフィックフィルタ関連

show ip/ipv6 filter statistics

項目	内容
Traffic filter process counter	トラフィックフィルタサブシステムを通過したパケット数
receives	受信パケット数
Static filter process counter	スタティックフィルタで処理を行ったパケット数
receives	受信パケット数
passes	通過パケット数
drops	廃棄パケット数
seeks	アクセスリストにドメインが指定されていたが、名前の解決を行えなかった数(※1)
Dynamic filter process counter	ダイナミックフィルタで処理を行ったパケット数
receives	受信パケット数
passes	通過パケット数
fails	廃棄パケット数
seeks	アクセスリストにドメインが指定されていたが、名前の解決を行えなかった数(※1)
None process counter	トラフィックフィルタで処理を行わなかったパケット数
packets	受信パケット数
Implicit deny counter	暗黙の deny ヒット数(※2)
packets	暗黙の deny で廃棄したパケット数
Memory allocation failure counter	メモリ確保失敗数
failures	メモリ確保に失敗した回数
Reassembly counter	リアセンブリカウンタ(※3)
requests	フラグメントパケット受信数
oks	リアセンブリパケット生成数

※1 厳密には、「DNS サーバへクエリを送信したが、応答を得られなかった」場合にカウントされます。これには DNS サーバ自身の不良、DNS サーバへの経路不良、ルータに DNS サーバのアドレスを指定していない、などが考えられます。但し、トラフィックフィルタでのドメイン指定されたアクセスリストの使用はサポート対象外です。

※2 インタフェースに設定された全てのフィルタにマッチしなかった場合、パケットは廃棄され、これを暗黙の deny と呼びます。

※3 強制リアセンブリ機能が有効化されている場合のみカウントされます。例えば、元々 3500byte のパケットが 3 つのフラグメントパケットに分割されており、これをトラフィックフィルタの強制リアセンブリで 1 つのパケットにリアセンブリした場合、requests が 3、oks が 1、カウントされます。

8.2.18 プレフィックスリスト関連

show ip/ipv6 prefix-list

項目	内容
Statistics	プレフィックスリスト統計情報
refs	全エントリの検索累積数
hits	全エントリのヒット累積数
entry	エントリ統計情報
hits	対象エントリのヒット回数

8.2.19 SNMP 関連

show snmp-agent statistics

項目	内容
System statistics	MIB-II によるシステムの統計情報
Descr	装置情報
Object ID	装置固有番号 sysObjectID を表示します
Engine ID	IX のエンジン ID（Ver10.4 以降）
Uptime	装置の起動時間 show uptime の System uptime と同じ
Name	hostname コマンドの設定名
SNMP statistics	SNMP エージェント統計情報
Authen traps	認証トラップの可否
Rcvd	受信パケット情報
pkts	受信パケット数
bad versions	不正なバージョンのパケット数
bad community names	不正なコミュニティ名の数
bad community uses	不正なコミュニティの使用数
asn parse errs	パケット整合性チェックにおける異常数
too bigs	シーケンスが大きすぎるパケットの数
no such names	一致しない名前の数
bad values	不正な値を含んだパケット数
read onlys	読み込み専用のパケット数
gen errs	一般的なエラー数
total reqvars	変数の request 総数
total setvars	変数の set 総数
get requests	get request パケット数
get nexts	get next パケット数
set requests	set request パケット数
get responses	get response パケット数
traps	trap パケット数
Sent	送信パケット情報
pkts	送信パケット数
too bigs	シーケンスが大きすぎるパケットの数
no such names	一致しない名前の数
bad values	不正な値を含んだパケット数
gen errs	一般的なエラー数

authorization errs	認証エラー数（Ver10.4 以降）
get requests	get request パケット数
get nexts	get next パケット数
set requests	set request パケット数
get responses	get response パケット数
traps	trap パケット数

show snmpv3 user

項目	内容
User name	ユーザ名
Security level	ユーザの認証レベル
Auth protocol	認証用プロトコル
Priv protocol	暗号化用プロトコル
Group name	ユーザと紐づくグループ名
Read View	グループの Read ビュー設定
Notify View	グループの Notify ビュー設定
Access-list	グループのアクセスリスト設定
Traps	トラップ送信設定
Interface link trap is disabled on	LinkUP/LinkDown をした際にトラップを送信しないインタフェース
Trap host	トラップ送信先アドレス

8.2.20 NTP 関連

show ntp

項目	内容
[synchronized | not synchronized]	時刻同期の有無
reference is ADDRESS	同期中のタイムサーバのアドレス
Rcvd:/ Sent:	受信数／送信数
requests	要求数
responses	応答数
NTP server	コンフィグしたタイムサーバのアドレス
VRF name	VRF 設定がある場合の VRF 名
St	コンフィグしたタイムサーバの階層
Ver	コンフィグしたタイムサーバのバージョン
Timeout	コンフィグしたタイムサーバのタイムアウト時間
Last Receive	コンフィグしたタイムサーバからの最終受信日時

8.2.21 ロギング

show logging statistics

項目	内容

Event	logging subsystem コマンドで有効になっているサブシステムのログメッセージのカウント数。

8.2.22 UFS キャッシュ

show ip/ipv6 ufs-cache（8.2 以降）

項目	内容
entries	現在の UFS キャッシュエントリ数 [picoIPv4UFSCacheEntries] ※IPv4 [picoIPv6UFSCacheEntries] ※IPv6
frees	現在の残り UFS キャッシュエントリ数
peaks	有効キャッシュ数が最も多かった時点の有効キャッシュ数(Ver.9.6 以降) [picoIPv4UFSCachePeaks] ※IPv4 [picoIPv6UFSCachePeaks] ※IPv6
creates(Ver.9.6 以降) flybys(Ver.9.5 以前)	UFS キャッシュエントリを作成した回数（今までに UFS キャッシュを通過したフロー数の目安となります。） [picoIPv4UFSCacheCreates] ※IPv4 [picoIPv6UFSCacheCreates] ※IPv6
overflows	残りエントリ数が無くなった回数（キャッシュエントリが無かった場合でも、キャッシュ効果はでませんがパケットロス等の実害はありません。このカウンタが著しく増加する場合、最大 UFS キャッシュエントリ数の追加を検討する必要があります。） [picoIPv4CacheOverflows] ※IPv4 [picoIPv6CacheOverflows] ※IPv6
* (Codes)	L3 キャッシュ検索結果登録済み L3 キャッシュは show ip/ipv6 cache で確認できます。
p (Codes)	ポリシルーティングの結果登録済み
f (Codes)	IPv4/IPv6 フィルタの通過結果登録済み フィルタのカウンタは、show ip/ipv6 access-list NAME で確認できます。
n (Codes)	NAT/NAPT の検索処理結果登録済み NAT/NAPT のカウンタは、show ip nat/napt statistics で確認できます。
s (Codes)	IPsec の SP または SA の検索結果登録済み
v (Codes)	SIP フィルタの通過結果登録済み
q (Codes)	QoS の通過結果登録済み
g (Codes)	NGN の通過結果登録済み
Uptime	まとめて表示している UFS キャッシュの中で最大のアップタイム
Hits	まとめて表示している UFS キャッシュの検索にマッチした総数
Ents	まとめて表示している UFS キャッシュの数

show ip/ipv6 ufs-cache verbose（8.2 以降）

項目	内容
allocs/maxents	メモリ確保済みの UFS キャッシュ/最大 UFS キャッシュ数
bytes used	UFS キャッシュとして確保したメモリのサイズ（UFS キャッシュとハッシュテーブルのすべて）
D (Codes)	無効キャッシュ（削除待ちキャッシュ）
entries (Interface)	該当インタフェースで作成された UFS キャッシュの数
hash-size (Interface)	インタフェースの UFS キャッシュハッシュサイズ
max-depth	1 つのハッシュにつながっている最大 UFS キャッシュ数（常に大きい場合、hash-size を大きくすると性能改善する可能性があります。）
Timeout	無効キャッシュになるまでの時間
Uptime	キャッシュが生成されてからの時間
Hits	UFS キャッシュでマッチした回数

8.2.23 SIP-NAT 関連

show sip dynamic-filter

項目	内容
Memory	メモリ運用情報
bytes requires	キャッシュ最大利用時の予想必要メモリ
bytes uses	現在使用中のメモリサイズ
Cache	キャッシュ運用情報
Register	ユーザキャッシュ運用情報
Dialog	ダイアログキャッシュ運用情報
Transaction	トランザクションキャッシュ運用情報
SDP	SDP/RTP/RTCP キャッシュ運用情報
Detect-server	サーバキャッシュ運用情報
User-contact	Contact キャッシュ運用情報
Relation-of-I/F	インタフェースキャッシュ運用情報
curr	現在使用中のキャッシュエントリ数
free	利用可能な残りキャッシュエントリ数
peak	ピークキャッシュエントリ数
overflows	キャッシュオーバーフロー回数
Permit Server	送信許可サーバ情報（設定時のみ）
refs	評価パケット数
hits	許可パケット数
drops	廃棄パケット数
Statistics	統計情報
Outside requests	Outside 側のリクエスト回数
Outside responses	Outside 側のレスポンス回数
Inside requests	Inside 側のリクエスト回数
Inside responses	Inside 側のレスポンス回数
receives	受信数
sends	送信数
	detail を指定すると、メソッド/ステータスごとにも表示します
RTP	RTP パケットフォワード数
RTCP	RTCP パケットフォワード数
inside forwards	内部→外部方向のフォワード数
outside forwards	外部→内部方向のフォワード数
Internal failure	SIP-ALG パケットドロップなど
parses	SIP パケットの解析ができない
transaction searches	該当トランザクションキャッシュが無い
transaction updates	トランザクションキャッシュの更新ができない

show sip filter-dynamic register

項目	内容
SIP dynamic filter Register	レジスタユーザキャッシュ情報
curr	現在使用中のキャッシュ数
free	残りキャッシュ数
peak	ピークキャッシュエントリ数
overflows	オーバーフロー回数
allocs	メモリ確保数（detail）
alloc errors	メモリ確保エラー数（detail）
errors	エラー数（detail） peak が最大キャッシュエントリ数の 2 倍を超えるとカウント
Terminal-detection	`terminal-detection'機能で端末障害を検出した回数（detail）
Contact	Contact 情報
Uptime	Contact 情報生成からの経過時間
Timer	設定されたタイマ値
expires	キャッシュ残り時間
Authenticated server	REGISTER 先のサーバ情報
Uptime	サーバ情報生成からの経過時間
Statistics	統計情報※1
Outside requests	Outside 側のリクエスト回数
Outside responses	Outside 側のレスポンス回数
Inside requests	Inside 側のリクエスト回数
Inside responses	Inside 側のレスポンス回数
	detail を指定すると、メソッド/ステータスごとにも表示します
Receives	受信数
Sends	送信数
Internal failures	SIP パケットドロップなど
parses	SIP パケットの解析ができない
transaction searches	該当トランザクションキャッシュが無い
transaction updates	トランザクションキャッシュの更新ができない

※1　detail 指定時は REGISTER 送信先サーバごとの統計と、ユーザ単位の統計を表示します。

show sip dynamic-filter dialog

項目	内容
SIP dynamic filter Dialog	ダイアログキャッシュ情報
curr	現在使用中のキャッシュ数
free	残りキャッシュ数
peak	ピークキャッシュエントリ数
overflows	オーバーフロー回数
allocs	メモリ確保数（detail）
alloc errors	メモリ確保エラー数（detail）
errors	エラー数（detail） peak が最大キャッシュエントリ数の 2 倍を超えるとカウント
Uptime	ダイアログキャッシュ生成からの経過時間
history	ヒストリ番号
Timer	設定されたタイマ値
expires	キャッシュ残り時間
Call-ID	Call-ID 情報
From	From 情報
(inside) or (outside)	発信側位置
Contact	発信側 Contact 情報
To	To 情報
(inside) or (outside)	発信先位置
Contact	発信先 Contact 情報
SDP	SDP 情報
Statistics	統計情報
Outside requests	Outside 側のリクエスト回数
Outside responses	Outside 側のレスポンス回数
Inside requests	Inside 側のリクエスト回数
Inside responses	Inside 側のレスポンス回数
receives	受信数
ends	送信数
	detail を指定すると、メソッド/ステータスごとにも表示します
RTP	RTP パケットフォワード数
RTCP	RTCP パケットフォワード数
inside forwards	内部→外部方向のフォワード数
outside forwards	外部→内部方向のフォワード数
Internal failures	SIP パケットドロップなど
parses	SIP パケットの解析ができない
transaction searches	該当トランザクションキャッシュが無い
transaction updates	トランザクションキャッシュの更新ができない

show sip dynamic-filter transaction

項目	内容
SIP dynamic filter Transaction	トランザクションキャッシュ情報
curr	現在使用中のキャッシュ数
free	残りキャッシュ数
peak	ピークキャッシュエントリ数
overflows	オーバーフロー回数
allocs	メモリ確保数（detail）
alloc errors	メモリ確保エラー数（detail）
errors	キャッシュ生成エラー数（detail） peak が最大キャッシュエントリ数の 2 倍を超えるとカウント
Uptime	トランザクションキャッシュ生成からの経過時間
history	ヒストリ番号
Timer	設定されたタイマ値
expires	キャッシュ残り時間
Call-ID	Call-ID 情報
Cseq	Cseq 情報
From	From 情報
To	To 情報
Via-NoAck/Ack	Via ブランチ情報(detail)

show sip nat

項目	内容
Memory	メモリ運用情報
bytes requires	キャッシュ最大利用時の予想必要メモリ
bytes uses	現在使用中のメモリサイズ
Cache	キャッシュ運用情報
Register	ユーザキャッシュ運用情報
Dialog	ダイアログキャッシュ運用情報
Transaction	トランザクションキャッシュ運用情報
SDP	SDP/RTP/RTCP キャッシュ運用情報
Temporary-service	外部 SIP パケット受信用キャッシュ運用情報
curr	現在使用中のキャッシュエントリ数
free	利用可能な残りキャッシュエントリ数
peak	ピークキャッシュエントリ数
overflows	キャッシュオーバーフロー回数
Reassemble buffer	SIP-NAT 変換用バッファ情報 (Ver7.2 のみ)
bytes	変換可能な最大ペイロードサイズ
entries	現在使用中のバッファ数
frees	利用可能な残りバッファ数
overflows	バッファオーバーフロー回数
Server filter	サーバフィルタ運用情報※1
entries	フィルタ設定数

refs	評価パケット数
hits	許可パケット数
drops	廃棄パケット数
Statistics	統計情報
Outside requests	Outside 側のリクエスト回数
Outside responses	Outside 側のレスポンス回数
Inside requests	Inside 側のリクエスト回数
Inside responses	Inside 側のレスポンス回数
receives	受信数
sends	送信数
	detail を指定すると、メソッド/ステータスごとにも表示します
RTP	RTP パケットフォワード数
RTCP	RTCP パケットフォワード数
inside forwards	内部→外部方向のフォワード数
outside forwards	外部→内部方向のフォワード数
Internal failure	SIP パケットドロップなど
parses	SIP パケットの解析ができない
converts	SIP パケットの変換ができない
reassembles	SIP パケットの再構成ができない
transaction searches	該当トランザクションキャッシュが無い
transaction updates	トランザクションキャッシュの更新ができない

show sip nat register

項目	内容
SIP-NAT/ALG Register	レジスタユーザキャッシュ情報
curr	現在使用中のキャッシュ数
free	残りキャッシュ数
peak	ピークキャッシュエントリ数
overflows	オーバーフロー回数
allocs	メモリ確保数（detail）
alloc errors	メモリ確保エラー数（detail）
errors	エラー数（detail） peak が最大キャッシュエントリ数の 2 倍を超えるとカウント
Terminal-detection	`terminal-detection'機能で端末障害を検出した回数
Contact	Contact キャッシュ情報
Packet src	SIP パケットの変換前、変換後の IP アドレスとポート番号
Registration to	REGISTER 先サーバ情報
Timer	設定されたタイマ時間
expires	キャッシュ残り時間
Statistics	統計情報※1
Outside requests	Outside 側のリクエスト回数
Outside responses	Outside 側のレスポンス回数
Inside requests	Inside 側のリクエスト回数
Inside responses	Inside 側のレスポンス回数
receives	受信数
sends	送信数
	detail を指定すると、メソッド/ステータスごとにも表示します
Internal failures	SIP-ALG パケットドロップなど
parses	SIP パケットの解析ができない
converts	SIP パケットの変換ができない
reassembles	SIP パケットの再構成ができない
transaction searches	該当トランザクションキャッシュが無い
transaction updates	トランザクションキャッシュの更新ができない

※1　detail 指定時は REGISTER 送信先サーバごとの統計と、ユーザ単位の統計を表示します。

show sip nat dialog

項目	内容
SIP-NAT/ALG Dialog	ダイアログキャッシュ情報
curr	現在使用中のキャッシュ数
free	残りキャッシュ数
peak	ピークキャッシュエントリ数
overflows	オーバーフロー回数
allocs	メモリ確保数（detail）
alloc errors	メモリ確保エラー数（detail）
errors	エラー数（detail） peak が最大キャッシュエントリ数の 2 倍を超えるとカウント
Uptime	ダイアログキャッシュ生成からの経過時間
history	ヒストリ番号
Timer	設定されたタイマ値
expires	キャッシュ残り時間
Call-ID	Call-ID 情報
From	From 情報
(inside) or (outside)	発信側位置
Contact	発信側 Contact 情報
To	To 情報
(inside) or (outside)	発信先位置
Contact	発信先 Contact 情報
SDP	SDP 情報
Statistics	統計情報
Outside requests	Outside 側のリクエスト回数
Outside responses	Outside 側のレスポンス回数
Inside requests	Inside 側のリクエスト回数
Inside responses	Inside 側のレスポンス回数
receives	受信数
sends	送信数
	detail を指定すると、メソッド/ステータスごとにも表示します
RTP	RTP パケットフォワード数
RTCP	RTCP パケットフォワード数
inside forwards	内部→外部方向のフォワード数
outside forwards	外部→内部方向のフォワード数
Internal failures	SIP パケットドロップなど
parses	SIP パケットの解析ができない
converts	SIP パケットの変換ができない
reassembles	SIP パケットの再構成ができない
transaction searches	該当トランザクションキャッシュが無い
transaction updates	トランザクションキャッシュの更新ができない

show sip nat transaction

項目	内容
SIP-NAT/ALG Transaction	トランザクションキャッシュ情報
curr	現在使用中のキャッシュ数
free	残りキャッシュ数
peak	ピークキャッシュエントリ数
overflows	オーバーフロー回数
allocs	メモリ確保数（detail）
alloc errors	メモリ確保エラー数（detail）
errors	キャッシュ生成エラー数（detail） peak が最大キャッシュエントリ数の 2 倍を超えるとカウント
Uptime	トランザクションキャッシュ生成からの経過時間
history	ヒストリ番号
Timer	設定されたタイマ値
expires	キャッシュ残り時間
Call-ID	Call-ID 情報
Cseq	Cseq 情報
(within a dialog)	ダイアログ内トランザクションを示す
From	From 情報
To	To 情報
Via-NoAck/Ack	Via ブランチ情報(detail)

show sip

項目	内容
Parse buffer	解析用バッファ情報
Reassemble buffer	再構築用バッファ情報
bytes	最大ペイロード長
entries	使用バッファ数
frees	フリーバッファ数
overflows	オーバーフロー発生数
Internal failure	SIP パケットドロップなど
parses	SIP パケットの解析ができない
parse buffers	バッファ取得に失敗
reassemble buffers	バッファ取得に失敗
transaction searches	該当トランザクションキャッシュが無い
transaction updates	トランザクションキャッシュの更新ができない

8.2.24 IEEE802.1X 関連

show dot1x interface

表示項目	内容
Quarantine is	検疫の状態（Ver.8.2 以降）
Quarantine attribute	検疫に使用する RADIUS のアトリビュート名（Ver.8.2 以降）
Access control mode	現在の認証単位
Maximum supplicants	インタフェースで処理可能な Supplicant の最大数
Current	
Supplicant entries	インタフェースで現在処理中の Supplicant 数
Authorized entries	インタフェースで認証済みの Supplicant 数
Interface	
AUTHSM	Authenticator PAE State Machine の状態
BACKSM	Backend Authentication State Machine の状態
EAP	EAP の状態
Port control mode	現在の認証動作
Direction	現在の制御方向
no logging ～	ログ抑止設定時に抑止内容を表示（Ver8.2 以降）
EAPoL version code	ルータが送信する EAPoL フレームのバージョンコード
AAA	AAA の設定
Maximum request	ルータから送信する EAP-Request/Identity の送信回数の設定
reAuthentication	再認証の設定の表示
Supplicant detection	Supplicant 検出動作のモード
Timeout	タイマに関する設定

show dot1x statistics

*は detail 指定時のみ表示します。

表示項目	内容
Rcvd	インタフェース単位の受信フレームに関する統計情報
eapol	全 EAPoL フレーム数
start	EAPoL-Start 数
logoff	EAPoL-Logoff 数
response/Id	EAP-Response/Identity 数
response	Response/Identity 以外のレスポンスフレーム数
invalid type	認識しないタイプの EAPoL フレーム数
length errors	Length フィールドの値が異常なフレーム数
Sent	インタフェース単位の送信フレームに関する統計情報
eapol	全 EAPoL フレーム数
request/Id	EAP-Request/Identity 数
request	EAP-Request/Identity、EAP-Request/Notification 以外のリクエストフレーム数
success	EAP-Success 数
failure	EAP-Failure 数

other	EAP-Request、EAP-Success、EAP-Failure 以外のリクエストフレーム数
errors	送信に失敗したフレーム数
Authorized packets	認証済み端末に関して送受信したパケットの情報
UnAuthorized packets	非認証済み端末に関して送受信したパケットの情報
Quarantine Passed packets	検疫で設定したフィルタを通過したパケットの情報（Ver.8.2 以降）
Quarantine Dropped packets	検疫で設定したフィルタで廃棄されたパケットの情報（Ver.8.2 以降）
Quarantine Dropped error packets	検疫で異常を検出したパケット数（Ver.8.2 以降）
Internal error*	内部的なエラー情報
allocation errors*	メモリ確保エラー
supplicant*	Supplicant 情報追加の際に発生したエラー数
auth supp*	認証済み Supplicant エントリの追加の際に発生したエラー数
misc*	その他のメモリ確保エラー
EAP statistics*	EAP に関する情報
Rcvd from supplicant*	Supplicant から受信したパケットに関する情報
packets*	全 EAP パケット数
responses*	EAP-Response パケット数
code errors*	不正なコード番号を持つ EAP パケット数
length errors*	Length フィールドの値が異常な EAP パケット数
id errors*	不正な ID 番号を持つ EAP パケット数。
unexpected errors*	状態に合わない EAP パケット数
Sent to supplicant*	Supplicant へ送信したパケットに関する情報
packets*	全 EAP パケット数
requests*	EAP-Request パケット数
success*	EAP-Success 数
failure*	EAP-Failure 数
Rcvd from authentication server*	認証サーバから受信したパケットに関する情報
packets*	全 EAP パケット数
requests*	EAP-Request パケット数
success*	EAP-Success 数
failure*	EAP-Failure 数
server timeout*	タイムアウト数
empty packets*	EAP 情報が入っていなかった数
code errors*	不正なコード番号持つパケット数
length errors*	レングスエラー数
id errors*	不正な ID 番号を持つパケット数
unexpected errors*	EAP の状態に合わないパケット数
Sent to authentication server*	認証サーバへ送信したパケットに関する情報
Internal errors*	内部的なエラー数
Supplicant	Supplicant 単位での統計情報
entries	インタフェースで現在処理中の Supplicant 数
authorized	インタフェースで認証済みの Supplicant 数
frees	インタフェースで処理可能な残り Supplicant 数
Supplicant(IDENTITY)	
MAC	MAC アドレス
uptime	ルータが検出してからの経過時間
Rcvd	受信フレームに関する統計情報
Sent	送信フレームに関する統計情報

LastEapolVersion	最後に受信した EAPoL フレームのバージョン番号
EntersConnecting*	ステートマシンが CONNECTING に遷移した回数
EapLogoffsWhileConnecting*	ステートマシンが CONNECTING の間に EAPoL-Logoff を受信した回数
EntersAuthenticating*	ステートマシンが AUTHENTICATING に遷移した回数
AUTHSM statistics*	Authenticator PAE State Machine に関する統計情報
SuccessWhileAuthenticating*	認証成功回数
TimeoutsWhileAuthenticating*	認証中のタイムアウト発生回数
FailWhileAuthenticating*	認証失敗回数
EapStartsWhileAuthenticating*	認証中に EAPoL-Start を受信した回数
EapLogoffWhileAuthenticating*	認証中に EAPoL-Logoff を受信した回数
ReauthsWhileAuthenticated*	認証期限切れによる再認証の発生回数
EapStartsWhileAuthenticated*	認証された状態で EAPoL-Start を受信した回数
EapLogoffWhileAuthenticated*	認証された状態で EAPoL-Logoff を受信した回数
BACKSM statistics*	Backend Authentication State Machine に関する統計情報
Responses*	ステートマシンが RESPONSE に遷移した回数
AccessChallenges*	認証サーバから Access-Challenge を受信した回数
OtherRequestsToSupplicant*	EAP-Request/Identity 以外の EAP-Request 送信回数
AuthSuccesses*	認証成功回数(EAP-Success 受信回数)
AuthFails*	認証失敗回数(EAP-Failure 受信回数)
EAP statistics*	Supplicant 単位の EAP 関連情報
Authorized packets	認証された状態で送受信されたパケット情報
Quarantine Passed packets	検疫で設定したフィルタを通過したパケットの情報（Ver.8.2 以降）
Quarantine Dropped packets	検疫で設定したフィルタで廃棄されたパケットの情報（Ver.8.2 以降）
Quarantine Dropped error packets	検疫で異常を検出したパケット数（Ver.8.2 以降）

show dot1x supplicant

*は detail 指定時のみ表示します。

表示項目	内容
Supplicant	
entries	インタフェースで現在処理中の Supplicant 数
authorized	インタフェースで認証済みの Supplicant 数
frees	インタフェースで処理可能な残り Supplicant 数
Interface Base State Machine	インタフェース単位で動作しているステートマシンに関する状態情報
AUTHSM	Authenticator PAE State Machine の状態
BACKSM	Backend Authentication State Machine の状態
EAP	EAP の状態
Supplicant(guest)	Supplicant の状態情報
MAC	Supplicant の MAC アドレス
uptime	Supplicant がルータに検出されてからの経過時間
Status	Supplicant の認証状態 (Authorized/Unauthorized)
AUTHSM	Authenticator PAE State Machine の状態
BACKSM	Backend Authentication State Machine の状態
EAP	EAP の状態

8.2.25 HTTP サーバ関連

show http-server

*は detail 指定時のみ表示します。
（各項目の中で何れかがカウントされた場合のみ表示されます）

表示項目	内容
HTTP(S) status*	接続中のセッション情報 ※ HTTPS は Ver10.1 以降
requests received	要求を受信した数の合計
GET*	GET 要求を受信した数
POST*	POST 要求を受信した数
HEAD*	HEAD 要求を受信した数
unknown*	上記以外の要求を受信した数
responses sent	応答を送信した数の合計 ※以下、[ ]内はステータスコードを示す
oks*	要求が成功したことを示す応答を送信した数[200]
founds*	リダイレクト(一時的な URI へのアクセス指示)を示す応答を送信した数［302］
see others*	リダイレクト(別要求での URI アクセス指示)を示す応答を送信した数［303］
bad reqs*	要求が不正だったことを示す応答を送信した数［400］
unauths*	認証が失敗または必要であることを示す応答を送信した数［401］
not founds*	要求されたページが見つからなかったことを示す応答を送信した数［404］
not allows*	許可されていないメソッドでページにアクセスした事を示す応答を送信した数［405］
not accepts*	提示されたリソースが受け入れられないことを示す応答を送信した数［406］
too longs*	URL が長すぎることを示す応答を送信した数［414］
server errors*	内部エラーが発生したことを示す応答を送信した数［500］
not supports*	未サポート HTTP バージョンで要求されたことを示す応答を送信した数［505］
unknowns*	上記以外の応答を送信した数
errors	WEB コンソールで検出されたエラー数の合計
denies*	アクセス制限(アクセスリスト)による接続拒否数
over hosts*	既定ホスト数超過エラー数
over sessions*	既定セッション数超過エラー数
too bigs*	既定リクエストサイズ超過エラー数
over requests*	リクエスト数の規定値超過エラー数
parse errors*	パケットの構文解析エラー数
allocation errors*	内部メモリ確保エラー数
https accept errors	セッション確立失敗数 ※ Ver10.1 以降(HTTPS のみ)
Terminal statistics	
logins	ログイン回数の合計
normals*	通常ログイン回数
forces*	強制ログイン回数
logouts	ログアウト回数の合計
normals*	通常ログアウト回数
autos*	タイムアウトによるログアウト回数

forces*	強制ログアウト回数
Buffer status	
free acbq	空きセッション用保持メモリ数
active mcbq	処理中メッセージ用保持メモリ数 ※ Ver10.1 以降
free mcbq	空きメッセージ用保持メモリ数
free mcbq_sbuf	空きメッセージ送信用保持メモリ数
active hostq	ホスト情報のカレント数 ※ Ver10.1 以降
free hostq	ホスト情報のフリー数 ※ Ver10.1 以降

8.2.26 グローバルアドレス通知機能関連

show kts-addressing statistics

*は値が 0 以外の場合に表示されます。

表示項目	内容
HTTPU statistics:	
message received:	要求を受信した数の合計
M-SEARCH request*	M-SEARCH 要求を受信した数
unsupported*	M-SEARCH 以外の要求を受信した数
message sent:	応答を送信した数の合計
OK(200)*	成功したことを示す応答を送信した数
HTTP statistics:	
message received:	要求を受信した数の合計
GET request*	GET 要求を受信した数
POST request*	POST 要求を受信した数
unsupported*	上記以外の要求を受信した数
message sent:	応答を送信した数の合計
OK(200)*	要求が成功したことを示す応答を送信した数
Bad Request(400)*	要求が不正だったことを示す応答を送信した数
Not Found(404)*	要求されたページが見つからなかったことを示す応答を送信した数
Method Not Allowed(405)*	許可されていないメソッドでページにアクセスした事を示す応答を送信した数
Internal Server Error(500)*	内部エラーが発生したことを示す応答を送信した数
UDP statistics:	
not allows	不許可端末から UDP パケットを受信した数
ignores	応答が不要な M-SEARCH を受信した数
parse errors	解析エラー数
internal errors	内部エラー数
TCP statistics:	
accepts	TCP コネクション要求を受け入れた数
received segments	受信セグメント数
overflows	既定バッファ長を超えたメッセージを受信した数
timeouts	セッションタイマがタイムアウトした数
not allows	不許可端末からのコネクション要求数
parse errors	解析エラー数
internal errors	内部エラー数

8.2.27 NGN 機能関連

show ngn statistics（Ver.8.6 以降）

表示項目	内容
Registration statistics:	
initializing bindings	登録初期化数
refreshing bindings	登録/更新数
Session statistics:	
Outgoing:	
outgoings	発信回数
Incoming:	
incomings	着信回数
Disconnect:	
disconnects	切断回数
Other:	
force releases	リンクダウンやコマンドによる強制切断数
expires	セッション強制解放数
Filter statistics:	
drops	NGN 網に許可されていない送信パケットの廃棄数

8.2.28 ループガード関連機能

show loop-detection information detail（Ver.8.9 以降）

表示項目	内容
Loop detection statistics:	
Interface	インタフェース名
Send	
packets	送信フレーム数（エラー含む）
errors	送信フレームのエラー合計数
buffer exhaust errors	パケットバッファ枯渇による廃棄数
Rcvd:	
packets	受信フレーム数（エラー含む）
invalid id	無効な ID の受信フレーム廃棄数
errors	受信フレームのエラー合計数
version errors	LDF 機能の Version と一致しない受信フレームの合計数
payload errors	Data 部 MAC アドレスの不一致やサイズ不足なフレームの受信回数
CRC errors	CRC 値が正しくないフレームの受信回数
invalid port	ルータのポート数を超えるポート番号を持つフレームの受信回数
invalid address	無効な宛先 MAC アドレスを持つフレームの受信回数

8.2.29 sFlow 関連機能

show sflow information（Ver.9.6 以降）

表示項目	内容
sFlow information	
Statistics	
outputs	コレクタへ送信した sFlow パケット数
errors	コレクタへ送信失敗したパケット数
flow samples	コレクタへ送信したフローサンプル数の合計
counter samples	コレクタへ送信したカウンタサンプル数の合計
Data source information:	
Device	デバイス名
Flow sampling:	
In:	受信側情報
inputs	受信したパケット数
samples	コレクタへ送信したフローサンプル数
drops	リソース不足により廃棄したフローサンプル数
single dest packets	送信先がシングルのフローサンプル数
multiple dest packets	送信先がマルチのフローサンプル数
received packets	自装置宛のフローサンプル数
discarded packets	送信処理されなかったフローサンプル数
unknown packets	宛先不明のフローサンプル数
Out:	送信側情報
outputs	送信したパケット数
samples	コレクタへ送信したカウンタサンプル数
drops	リソース不足により廃棄したフローサンプル数
single dest packets	送信先がシングルのフローサンプル数
multiple dest packets	送信先がマルチのフローサンプル数
generated packets	自装置生成されたフローサンプル数
Counter sampling:	
samples	コレクタへ送信したカウンタサンプル数

show sflow information（Ver.8.9 以降）

表示項目	内容
sFlow information	
Statistics	
outputs	コレクタへ送信した sFlow パケット数
errors	コレクタへ送信失敗したパケット数
flow samples	コレクタへ送信したフローサンプル数の合計
counter samples	コレクタへ送信したカウンタサンプル数の合計
Data source information:	
Device	デバイス名
Flow sampling:	
inputs	受信したパケット数
samples	コレクタへ送信したフローサンプル数
drops	リソース不足により廃棄したフローサンプル数
single dest packets	送信先がシングルのフローサンプル数
multiple dest packets	送信先がマルチのフローサンプル数
received packets	自装置宛のフローサンプル数
discarded packets	送信処理されなかったフローサンプル数

unknown packets	宛先不明のフローサンプル数
Counter sampling:	
samples	コレクタへ送信したカウンタサンプル数

8.2.30 IDS 関連機能

show ids statistics（Ver.8.10 以降）

表示項目	内容
ip-header	タイプが IP ヘッダの統計情報
ip-option	タイプが IP オプションの統計情報
icmp	タイプが ICMP の統計情報
udp	タイプが UDP の統計情報
tcp	タイプが TCP の統計情報
ftp	タイプが FTP の統計情報
[検出条件]	検出条件については IDS の項を参照してください
detected	検出数
discarded	廃棄数
last detected	最後に検出したパケットの情報

8.2.31 L2TP 関連

show l2tp statistics（Ver.8.10 以降）

表示項目	内容
Elapsed time after clear counters	統計情報クリア時からの経過時間
Control connection statistics	コントロールコネクション統計情報
total tunnels	コネクション確立総数
failed tunnels	失敗総数
disconnect requests	コネクション切断総数
disconnect accepts	切断受諾総数
Session statistics	L2TP セッション統計情報
total sessions	セッション確立総数
failed sessions	失敗総数
disconnect accepts	セッション切断受諾総数
Control message statistics	コントロールメッセージ統計情報
packets input	コントロールメッセージ受信数
errors	受信エラー数
SCCRQ	SCCRQ メッセージ受信数
SCCRP	SCCRP メッセージ受信数
SCCCN	SCCCN メッセージ受信数
StopCCN	StopCCN メッセージ受信数
Hello	Hello メッセージ受信数
ICRQ	ICRQ メッセージ受信数
ICRP	ICRP メッセージ受信数
ICCN	ICCN メッセージ受信数
CDN	CDN メッセージ受信数
ZLB	ZLB メッセージ受信数
header errors	L2TP ヘッダ異常検出数
id errors	不明なトンネル ID 検出数
seq errors	シーケンス番号異常検出数
unknowns	不明なタイプ検出数
packets output	コントロールメッセージ送信数
errors	送信エラー数
SCCRQ	SCCRQ メッセージ送信数
SCCRP	SCCRP メッセージ送信数
SCCCN	SCCCN メッセージ送信数
StopCCN	StopCCN メッセージ送信数
Hello	Hello メッセージ送信数
ICRQ	ICRQ メッセージ送信数
ICRP	ICRP メッセージ送信数
ICCN	ICCN メッセージ送信数
CDN	CDN メッセージ送信数
ZLB	ZLB メッセージ送信数
buffer errors	送信バッファ確保失敗数
send errors	メッセージ送信失敗数

show l2tp active（Ver.8.10 以降）

表示項目	内容
L2TP information	接続中 L2TP トンネル情報
active tunnels	接続中トンネル数
active sessions	接続中セッション数
Interface	インタフェース名
L2TP mode	トンネルタイプ（LNS または LAC）
Tunnel is	トンネル状態 idle ：未接続 wait-ctl-conn ：接続処理中 established ：接続 disconnecting：切断処理中
Local Ns, Nr	送信シーケンス番号、受信シーケンス番号
Remote Ns, Nr	対応装置送信シーケンス番号、受信シーケンス番号
CWND	輻輳ウィンドウサイズ
SSTHRESH	スロースタートスレッショルド
Retransmit count	再送回数
timer	再送タイマ
Local id	自装置 L2TP トンネル ID
remote id	対向装置 L2TP トンネル ID
Remote address	対向装置 IP アドレス
Remote window size	対向装置ウィンドウサイズ
Remote host name	対向装置ホスト名
Remote vendor name	対向装置ベンダ名
Session Information	LAC のみ表示
Client ID	クライアント ID（LAC 時のみ）
Interface is	インタフェース情報（LAC 時のみ）
Session is	セッション状態（LAC 時は経過時間も表示） idle ：未接続 wait-connect：接続処理中 established ：接続
Idle time	無通信時間（LAC 時のみ表示）
Local id	自装置セッション ID
remote id	対向装置セッション ID

show l2tp history（Ver.8.10 以降）

表示項目	内容
L2TP information	接続中 L2TP トンネル情報（show l2tp active を参照してください）
L2TP history	L2TP 接続履歴
Used time	L2TP 接続時間
Remote address	対向装置アドレス
Remote host name	対向装置ホスト名
Remote vendor name	対向装置ベンダ名
Disconnect reason	切断要因
Result Code	リザルトコード

8.2.32 URL リダイレクト関連

show http-redirect information（Ver.9.0 以降）

表示項目	内容
recodes	端末数
overflow	オーバーフロー発生回数
MAC address	端末の MAC アドレス
Uptime	端末情報の生存時間
Expires	リダイレクト抑止残り時間

8.2.33 OpenFlow 関連

show openflow controller（Ver.9.0.54 以降）

表示項目	内容
connected	コントローラとの接続回数
disconnected	コントローラとの切断回数
message received	コントローラからのメッセージ受信数
hello	hello メッセージ受信数
echo	echo メッセージ受信数
echo replies	echo 応答メッセージ受信数
experimenter	experimenter メッセージ受信数
features	features メッセージ受信数
get-config	get-config メッセージ受信数
set-config	set-config メッセージ受信数
packet-out	packet-out メッセージ受信数
flow-mod	flow-mod メッセージ受信数
group-mod	group-mod メッセージ受信数
port-mod	port-mod メッセージ受信数
table-mod	table-mod メッセージ受信数
multipart	multipart メッセージ受信数
desc	desc メッセージ受信数
flow	flow メッセージ受信数
aggregate	aggregate メッセージ受信数
table	table メッセージ受信数
port-status	port-status メッセージ受信数
queue	queue メッセージ受信数
group	group メッセージ受信数
group-desc	group-desc メッセージ受信数
group-features	group-features メッセージ受信数
meter	meter メッセージ受信数
meter-config	meter-config メッセージ受信数
meter-features	meter-features メッセージ受信数
table-features	table-features メッセージ受信数
port-desc	port-desc メッセージ受信数
experimenter	experimenter メッセージ受信数
unknown	multipart の種別が不明なメッセージ受信集
barrier	barrier メッセージ受信数

queue-get-config	queue-get-config メッセージ受信数
role	role メッセージ受信数
get-async	get-async メッセージ受信数
set-async	set-async メッセージ受信数
meter-mod	meter-mod メッセージ受信数
unknown	種別が不明なメッセージ受信数
message sent	コントローラへのメッセージ送信数
hello	Hello メッセージ送信数
error	error メッセージ送信数
echo	echo メッセージ送信数
echo replies	echo 応答メッセージ送信数
experimenter	experimenter メッセージ送信数
features replies	features 応答メッセージ送信数
get-config replies	get-config 応答メッセージ送信数
packet-in	packet-in メッセージ送信数
flow-removed	flow-removed メッセージ送信数
port-status	port-status メッセージ送信数
multipart replies	multipart 応答メッセージ送信数
desc	desc メッセージ送信数
flow	flow メッセージ送信数
aggregate	aggregate メッセージ送信数
table	table メッセージ送信数
port-status	port-status メッセージ送信数
queue	queue メッセージ送信数
group	group メッセージ送信数
group-desc	group-desc メッセージ送信数
group-features	group-features メッセージ送信数
meter	meter メッセージ送信数
meter-config	meter-config メッセージ送信数
meter-features	meter-features メッセージ送信数
table-features	table-features メッセージ送信数
port-desc	port-desc メッセージ送信数
experimenter	experimenter メッセージ送信数
barrier replies	barrier 応答メッセージ送信数
queue-get-config replies	queue-get-config 応答メッセージ送信数
role replies	role 応答メッセージ送信数
get-async replies	get-async 応答メッセージ送信数
OpenFlow Channel Message Queue:	（Ver9.2 以降)
Output packets	メッセージ送信数
overflows	キュー長を超えたメッセージの破棄数
excess rate-limit	PacketIn 抑止機能で抑止したメッセージ数

show openflow port（Ver.9.0.54 以降）

表示項目	内容
received packets	受信パケット数
bytes	受信バイト数
drops	受信廃棄数
transmitted packets	送信パケット数
bytes	送信バイト数
drops	送信廃棄数
link-up detected	ポート up 回数
link-down detected	ポート down 回数

8.2.34 URL オフロード関連

show url-offload status（Ver.9.4 以降）

表示項目	内容
XML-List Information:	XML リスト情報
Last Request	最終取得要求時刻
Last Update	最終更新時刻
Request	取得要求送信回数
Success	取得成功回数
Failure	取得失敗回数
format error	取得ファイルフォーマット異常
DataBase Information:	データベース情報
Total	合計エントリ数
URL	URL エントリ数
IPv4	IPv4 アドレスエントリ数
PAC-File Information:	PAC ファイル情報(Ver.9.6 以降)
URL	パックファイルの URL
Last Request	最終取得要求時間
Last Update	最終更新時間
Request	取得要求送信回数
Success	取得成功回数
Failure	取得失敗回数
Internal PAC-File Information:	内部パックファイル情報(Ver.9.6 以降)
Last Request	最終取得要求時刻
Last Update	最終更新時刻
Request	取得要求送信回数
Success	取得成功回数
Failure	取得失敗回数

show url-offload status（Ver.10.5 以降）

表示項目	内容
Internal:	URL list 設定を条件としたオフロード動作情報
input packets	受信 IF でオフロード判定対象となったパケット数
offload	マッチ(オフロード対象となった)パケット数
passes	アンマッチ(オフロード対象とならなかった)パケット数

output packets	送信 IF でオフロード判定対象となったパケット数
passes	discard(破棄)しなかったパケット数
discard	discard(破棄)したパケット数
External:	XML または NetMeister による設定を条件としたオフロード動作情報
input packets	受信 IF でオフロード判定対象となったパケット数
offload	マッチ(オフロード対象となった)パケット数
passes	アンマッチ(オフロード対象とならなかった)パケット数
output packets	送信 IF でオフロード判定対象となったパケット数
passes	discard(破棄)しなかったパケット数
discard	discard(破棄)したパケット数
Other:	Internal External 以外の条件によるオフロード動作情報
input packets	受信 IF でオフロード判定対象となったパケット数
offload	マッチ(オフロード対象となった)パケット数
passes	アンマッチ(オフロード対象とならなかった)パケット数
output packets	送信 IF でオフロード判定対象となったパケット数
passes	discard(破棄)しなかったパケット数
discard	discard(破棄)したパケット数
Address-Cache:	アドレスキャッシュ情報
max entries	キャッシュの最大数
overflows	キャッシュの上限に達し、キャッシュが作成されなかった数
Session-Cache:	セッションキャッシュ情報
max entries	キャッシュの最大数
overflows	キャッシュの上限に達し、キャッシュが作成されなかった数

8.2.35 URL フィルタリング関連

show url-filter statistics（Ver.9.5 以降）

表示項目	内容
Internal:	内部 URL フィルタリング情報
input packets	受信パケット数
passes	内部フィルタによる透過パケット数
blocks	内部フィルタによる廃棄パケット数
External:	外部 URL フィルタリング情報
input packets	受信パケット数
passes	外部フィルタによる透過パケット数
blocks	外部フィルタによる廃棄パケット数
drops	問い合わせ中にユーザから再送されたパケットの廃棄数
overflows	問い合わせのオーバーフローで廃棄したパケット数
Internal Filter List:	内部 URL フィルタリング機能の URL リスト情報
Seqnum	URL リストのシーケンス番号 no-match:URL リストに該当しないパケットの情報
Hits	URL リストに該当したパケット数
Blocks	URL リストに該当し、廃棄したパケット数
External Category List:	外部 URL フィルタリング機能のカテゴリ情報
Category	カテゴリ ID no-category: カテゴリ ID 未定義 no-response: 事業者サーバ無応答
Hits	カテゴリ ID に該当したパケット数
Blocks	カテゴリ ID に該当し、廃棄したパケット数

show url-filter server（Ver9.5 以降）

表示項目	内容
Sessions:	セッション情報
curr	現在問い合わせ中セッション数
peak	問い合わせセッション過去最大数
max	問い合わせセッション受付最大数
Statistics:	統計情報
requests	事業者サーバ問い合わせ要求数
responses	事業者サーバ問い合せ応答数
timeouts	事業者サーバ無応答によるタイムアウト数
errors	事業者サーバからのエラー応答による失敗数

show url-filter cache（Ver.9.5 以降）

表示項目	内容
entries	キャッシュ登録数
frees	キャッシュ空き数
overflows	キャッシュオーバーフロー数
category	カテゴリ ID
hits	キャッシュヒット数
sec	キャッシュ登録後の経過時間

8.2.36 UTM 関連

UTM 関連は、UTM の章を参照してください。

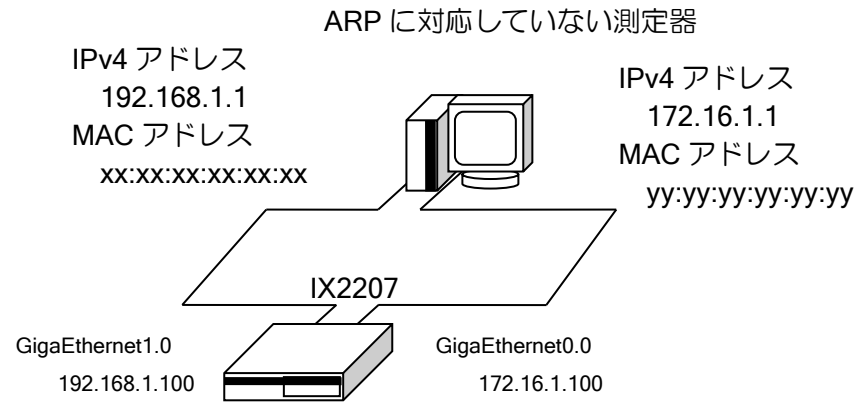
9章 ベンチマークテストのための設定

本章では、IX2000/IX3000 シリーズをベンチマークテストに使用する場合の設定について説明します。

測定器を用いてベンチマークテストを実施する場合、測定器側が、ARP に対応していない、ND に対応していないといった可能性があります。
このときにはスタティック（パーマネント）な ARP エントリあるいは近隣エントリを固定設定することで、測定器側を IX2000/IX3000 シリーズに登録することができます。

■9.1 ARP エントリの固定設定

ARP エントリへの固定設定方法は次のとおりです。



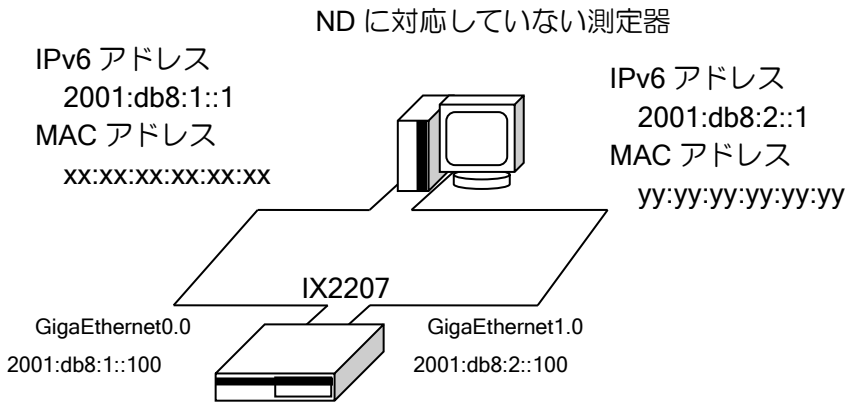
【設定例】

```
interface GigaEthernet0.0
  ip address 172.16.1.100/24
  arp entry 172.16.1.1 yy:yy:yy:yy:yy:yy
interface GigaEthernet1.0
  ip address 192.168.1.100/24
  arp entry 192.168.1.1 xx:xx:xx:xx:xx:xx
```

ARP エントリへの固定設定は保存対象です。したがって、write memory にて保存した後は、再起動しても設定が保存されます。

■9.2 近隣エントリの固定設定

近隣エントリへの固定設定方法は次のとおりです。



【設定例】

```
interface GigaEthernet0.0
  ipv6 address 2001:db8:1::100/64
  ipv6 nd static-neighbor 2001:db8:1::1 xx:xx:xx:xx:xx:xx
interface GigaEthernet1.0
  ipv6 address 2001:db8:2::100/64
  ipv6 nd static-neighbor 2001:db8:2::1 yy:yy:yy:yy:yy:yy
```

近隣エントリへの固定設定は保存対象です。したがって、write memory にて保存した後は、再起動しても設定が保存されます。

NA(Neighbor Advertisement)パケットを IX2000/IX3000 シリーズに送信するだけの測定器の場合でも、RFC2461 によって近隣エントリ固定設定が必要となります。

10章 ファームウェアインストール

本章では、IX2000/IX3000 シリーズのファームウェアバージョンアップ方法、インストール方法を説明します。また、コンフィグファイルのインストール方法も説明します。

■10.1 2 面管理対応版でのバージョンアップ方法

ブートおよび ldc ファイルのロードモジュールを、メイン領域とバックアップ領域の２箇所に保存できるファームウェアは、安全なバージョンアップが可能です。対応する装置、バージョンは以下のとおりです。

装置名	対応バージョン
IX3110	Ver.8.3 以降
上記以外の全機種	全バージョン

10.1.1 格納されているプログラムの確認方法

show flash により、格納されているファームフェアを確認できます。

Status の表示が“M”はメインのファームウェア、”B”はバックアップのファームウェアになります。”A”は現在起動しているファームウェアになります。

【表示例】

```
(config)# show flash
Codes: M - Main-side, B - Backup-side, N - Newfile, R - Runnable
           A - Active-file, + - Next-boot, * - Bootmode-entry
Length        Name                                  Status
7279799       ix2207-ms-10.1.22.ldc                 B
8169726       ix2207-ms-10.2.21.ldc                 MA
1766          SYSTEM-PRIVATE-KEY

[15718080 bytes used, 11264514 available, 26982594 total]
26368 Kbytes of processor board System flash (Read/Write)

ix2207-ms-10.2.21.ldc がメイン領域に格納され、現在使用中
ix2207-ms-10.1.22.ldc がバックアップ領域に格納
```

10.1.2 バージョンアップの手順

software-update コマンドを使用して rap ファイルでバージョンアップを行ってください。

2 面化対応版では、現在使用しているブートと ldc ファイルを削除せずにバージョンアップを行うため、バージョンアップが電源断等で失敗してもブートに失敗する問題が発生しません。

software-update	ファームウェアの更新

【実行例】

```
(config)# software-update tftp://192.168.1.1/ ix2207-boot-10.2-gate-ms-10.1.22.rap
% Downloading ..........................................................................
.....................................................................................
TFTP transfer complete, 8523785 bytes, MD5 = 6aa29e4dd4b43a1772692e479ecc57ca
% Check ..... done
% Update file name is ix2207-ms-10.1.22.ldc
```

```
% Writing ..........................................................................................
.......................................................................... done
% Software update completed.
(config)#
```

※ HTTP/HTTPS サーバ指定時は、Ver.8.9 以降 IPv6 に対応しています。
※ パスワード設定は、Basic 認証のみのサポートとなります。

コマンドが終了した時点で、ファームウェアの展開が完了します。この時点で show flash を実行すると Status に”N+”が表示されます。”N”は更新した新しいファームウェアであること、”+”は再起動後に起動するファームウェアであることを示しています。software-update コマンド終了後、再起動することにより、更新したファームウェアで起動します。

```
【表示例】
(config)# show flash
Codes: M - Main-side, B - Backup-side, N - Newfile, R - Runnable
          A - Active-file, + - Next-boot, * - Bootmode-entry
Length       Name                                  Status
7279799      ix2207-ms-10.1.22.ldc             MA
8169726      ix2207-ms-10.2.21.ldc             N+
1766         SYSTEM-PRIVATE-KEY

[15718080 bytes used, 11264514 available, 26982594 total]
26368 Kbytes of processor board System flash (Read/Write)

ix2207-ms-10.1.22.ldc が現在動作しているファームウェア
ix2207-ms-10.2.21.ldc が再起動後に起動するファームウェア
```

ファームウェアの 2 面管理機能を使用した後は、ファームウェアのバージョンアップは software-update コマンドを使用してください。また、バージョンアップ時には rap ファイルを使用してください。

2 面管理機能使用後、未対応のバージョンに変更する場合、software-update コマンドに bootmode-update オプションを指定してください。software-update コマンド実行後、show flash を実行すると転送したファームウェアの Status に実行可能なファイルであることを示す”R*”が表示され、再起動することにより、ファームウェアの更新を行います。

```
【実行例】

(config)# software-updatetftp://192.168.2.254/ix2207-boot-10.2-gate-ms-1
          0.1.22.rap bootmode-update
%Downloading ..........................................................................................
.....................................................................................
TFTP transfer complete, 8523785 bytes, MD5 = 6aa29e4dd4b43a1772692e479ecc57ca
% Check ... done
% Update file name is ix2207-boot-10.2-gate-ms-10.1.22.rap
%Writing ..............................................................................................
.......................................................................... done
% Software update completed.
(config)#
(config)# show flash
Codes: M - Main-side, B - Backup-side, N - Newfile, R - Runnable
          A - Active-file, + - Next-boot, * - Bootmode-entry
Length       Name                                  Status
7279799      ix2207-ms-10.1.22.ldc             B+
8169726      ix2207-ms-10.2.21.ldc             MA
8523785      ix2207-boot-10.2-gate-ms-10.1.22.rap R*
1766         SYSTEM-PRIVATE-KEY
```

```
[24363024 bytes used, 2619570 available, 26982594 total]
26368 Kbytes of processor board System flash (Read/Write)
(config)# reload
Notice: The router will be RELOADED. This is to ensure that
        the peripheral devices are properly initialized.
Are you sure you want to reload the router? (Yes or [No]): y

NEC Bootstrap Software
Copyright (c) NEC Corporation 2001-2019. All rights reserved.

%BOOT-INFO: Trying flash load, exec-image [ix2207-boot-10.2-gate-ms-10.1.22.rap].
Loading:
################################################################################
############################################################ [OK]


Starting at 0x20000

NEC Bootstrap Software, Version 10.2
Copyright (c) NEC Corporation 2001-2019. All rights reserved.

***** FLASH MEMORY IMAGE UPDATER *****

%UPDATE-INFO: Update Information [0a011620156ca456]
%UPDATE-INFO: Starting update.
%UPDATE-INFO: [Bootstrap Software] [Main Bootstrap Software] [Diagnostic Software]
[Gateway Software]
%UPDATE-INFO: Cleanup all FLASH area, please wait for a while.
%UPDATE-INFO: 0x00100274 > 0xfffe0000 update done.
%UPDATE-INFO: 0x00120294 > 0xffdc0000 update done.
    :
```

bootmode-update オプションを使用しない場合、ダウンロード後にエラーとなります。

```
【実行例】

(config)# software-update tftp://192.168.1.1/ix3100-boot-3.1-gate-ms-8.2.19.rap
% Downloading ..........................................................................................
.....................................................................................
TFTP transfer complete, 3955078 bytes, MD5 = aaff6124c7907f08434810f5aa5e86fe
% Check
% Invalid file
```

また、ldc ファイルを指定した場合は bootmode-update を指定すればエラーとはなりませんが、2 面化管理情報が更新されないため、通常は rap ファイルを使用してください。

10.1.3 起動ファームウェアの選択

software-select コマンドにより、起動するファームウェアを選択できます。コマンド実行後、再起動により、選択したファームウェアで起動します。software-select コマンドでは、メインまたはバックアップ領域のファームウェアのみ指定可能です。

software-select	ファームウェアの選択

```
【実行例】
(config)# software-select ix2207-ms-10.1.22.ldc
% ix2207-ms-10.1.22.ldc is selected as system file.
(config)# show flash
Codes: M - Main-side, B - Backup-side, N - Newfile, R - Runnable
           A - Active-file, + - Next-boot, * - Bootmode-entry
Length        Name                                  Status
7279799       ix2207-ms-10.1.22.ldc                 B+
8169726       ix2207-ms-10.2.21.ldc                 MA
1766          SYSTEM-PRIVATE-KEY

[15718080 bytes used, 11264514 available, 26982594 total]
26368 Kbytes of processor board System flash (Read/Write)
```

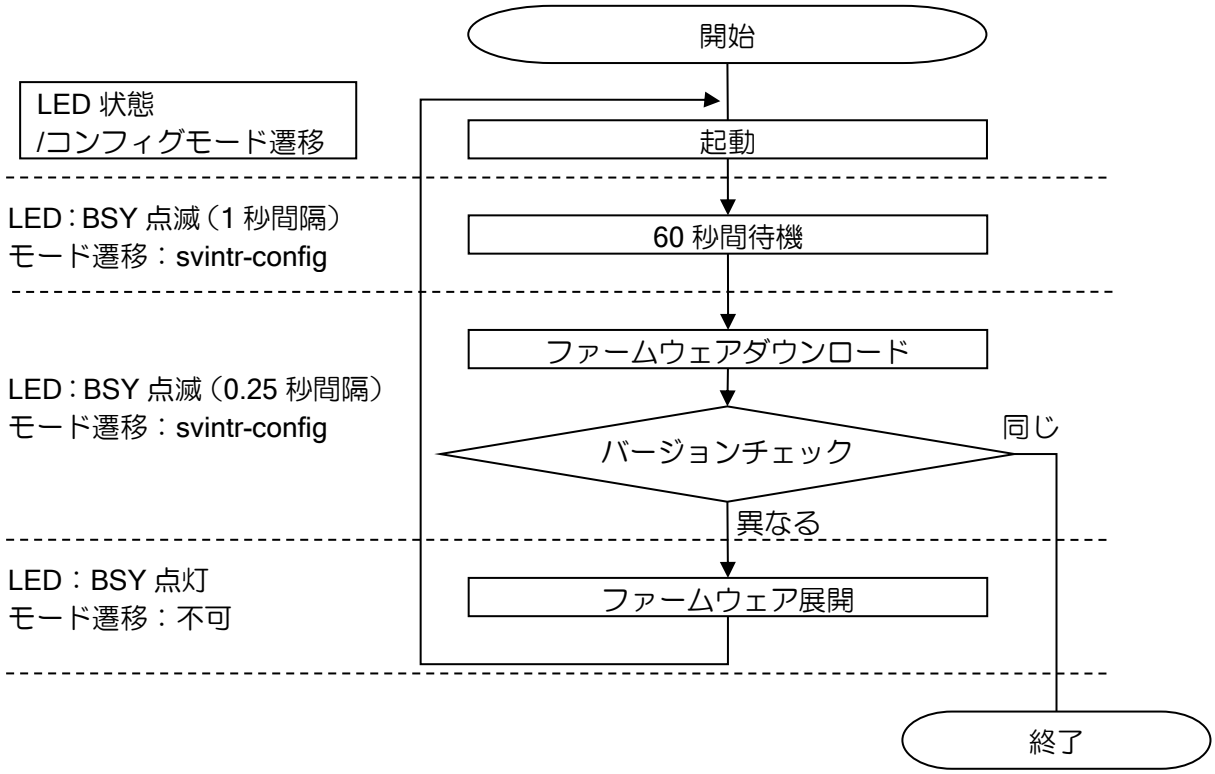
■10.2 2 面管理対応版以外のバージョンアップ方法

従来のブートが 2 面管理されていないファームウェアの場合は、現在のファームウェアを削除しないとバージョンアップできません。バージョンアップ中に電源が落ちるとブートできなくなくなる場合がありますので、十分注意してください。

バージョンアップ方法につきましては、該当するバージョンの取扱説明書の「管理と保守」の項を参照してください。

■10.3 起動時の自動バージョンアップ

Ver.8.7 以降、起動時に、指定したサーバからファームウェアをダウンロードし、バージョンアップすることができます。自動バージョンアップの処理の流れは以下の通りです。



インタフェースや経路状態の安定のため、起動から 60 秒経過後、ファームウェアのダウンロードを開始します。ファームウェアをダウンロードし、展開後、自動で再起動を行います。再起動後も自動バージョンアップが動作します。ファームウェアを一部ダウンロードし、装置のプログラムと同じバージョンであることを確認し、終了となります。

コマンドは以下のとおりです。

startup software-update	起動時の自動ファームウェア更新

【設定例】
TFTP を使用して転送を行う場合の設定例

```
startup software-update tftp://192.168.0.100/xxx.rap
```

※ HTTP/HTTPS サーバ指定時は、IPv4 のみのサポートとなります。
※ パスワード設定は、Basic 認証のみのサポートとなります。

設定には固定のファイル名を指定します。最新のファームウェアの名前を、設定したファイル名と同じ名前に変更し、サーバへ格納してください。これにより、設定を変更せずに最新ファームウェアのダウンロードが可能となります。

バージョンアップ処理実行時、コンソール画面には何も表示されません。処理の状態は LED により確認できます。

また、バージョンアップ処理実行中は、コンフィグモードへの遷移はできません。svintr-config により、バージョンアップ処理を中断し、強制的にコンフィグモードへの遷移が可能です。ただし、動作状態によって、コンフィグモードへ遷移できない場合があります。各動作状態における、LED 状態とコンフィグモード遷移の可否はバージョンアップの流れを参照してください。

次の場合、バージョンアップは実行せずに処理を終了します。

- 使用中のバージョンと同じ場合
- ファームウェアの転送に失敗した場合
  （転送のリトライは行いません）
  - ダウンロード開始から 10 分以上経過した場合
  - サーバからの応答が無い場合
  - サーバにファイルが存在しない場合
  - ダウンロードしたファームフェアが異常だった場合
  - フラッシュメモリの空き容量が不足していた場合

また、以下の場合には自動バージョンアップ機能は動作しません。

- boot entry コマンドを設定した場合
- ゼロコンフィグモードで動作している場合

処理結果は、show crashinfo により確認することができます。

【表示例】
正常に更新した場合の表示例

```
(config)# show crashinfo
Latest Occurrence Time       Event Description
2010/10/20 20:15:10 +0900 INFO: Start logging fault and crash errorlog_information
2010/10/20 20:25:58 +0900 INFO: Start bootstrap from this side [1].
2010/10/20 20:27:13 +0900 INFO: Software update not needed.
2010/10/20 20:25:53 +0900 INFO: Auto software update completed.(xx-x.x.x.ldc)
```

自動バージョンアップの結果として以下のメッセージが表示されます。
その他のメッセージに関しては、付録の「ルータメッセージ一覧」を参照してください。

メッセージ	内容
Software update not needed.	ファームウェアの更新が必要ありませんでした ・バージョンが同じ
Software update failed.	ファームウェア更新に失敗しました ・ファームウェア転送失敗
Auto software update completed.	ファームウェアの更新が正常に完了しました
Auto software update canceled.	ファームウェア更新を中断しました ・svintr-config によるモード遷移

ソフトウェア更新後の再起動時にも、ソフトウェア更新が動作します。この場合、サーバのプログラムのバージョンと装置のソフトウェアバージョンが同じとなるため、最新のログ情報は”Software update not needed.”となります。

ロギング設定を行うことにより、詳細な結果を確認することができます。
ロギングの詳細については、「遠隔設定と監視」の項を参照してください。

logging subsystem	ロギング設定
logging buffered	ログ保存サイズ指定
logging timestamp datetime	ログのタイムスタンプ設定
show logging	ログ情報表示

【設定例】
ログの設定例

```
logging buffered 131072
logging subsystem gw warn
logging timestamp datetime
```

ログの表示例（処理中断の場合）

```
(config)# show logging
Buffer logging enabled, 131072 bytes, type cyclic
   2 messages (1-2), 123 bytes logged, 0 messages dropped

Log Buffer (1-2):
2010/10/20 21:05:20     GW.038: User admin@ has logged on
2010/10/20 21:05:30     GW.085: Software update canceled by user
```

自動バージョンアップに関するログは、以下が表示されます。

No	Level	メッセージ	内容
80	info	Software update not needed	ファームウェア更新が不要です
81	error	Software update internal error	内部エラーが発生しました ・格納ファイル数の最大(19)を超えている
82	warn	Software update communication error	通信に問題がありました ・サーバとの通信異常 ・サーバにファイルが存在しない
83	warn	Software update timeout error	転送がタイムアウトしました ・転送に 10 分以上経過
84	warn	Software update invalid file	ファイルが不正です
85	warn	Software update canceled by user	ファームウェア更新が中断されました
86	warn	Software update flash too small	フラッシュメモリに空きがありません

■10.4 正常に立ち上がらない場合のファームウェアインストール

IX2000/IX3000 シリーズでは、万一正常に立ち上がらなくなった場合でも、ネットワーク立ち上げによるファームウェアインストール方法を提供しております。
以下に正常に立ち上がらない場合のファームウェアインストール方法を示します。

※IPv4 により経路到達可能な tftp サーバが別途必要です。IPv6 には対応しておりません。
※事前に tftp サーバ上にファームウェアを置いておく必要があります。

(1) ルータにコンソールを接続します。

(2) ルータの電源を落とします。

(3) ルータの電源を再度投入し、ロード中に ctrl キーを押しながら c キーを入力（ctrl + c）することで、ブートモニタモードに移ります。

```
Ver.6.0 以降

      :
      :
%BOOT-INFO: No boot records found, attempting flash load.
%BOOT-INFO: Trying flash load, exec-image [ix2215-ms-1.0.1.ldc].
Loading: ##########
                    ↑途中で、ctrl + c で停止させてください。
                      うまくいかない場合は、何度でも試行できます
```

(4) 実行プロンプトが表示されますので、以下のように入力します。

```
【実行例】

bm
```

(5) 以下のように、コンソールクエリーが表示されます。

```
Device types available:

        Flash
        GigaEthernet0.0
        GigaEthernet1.0
              :
        Device type:
```

以下、コンソールクエリーにしたがって設定しますが、誤って入力しても、ctrl + c を入力すると、プロンプト表示にもどることができます。

(6) ロードするデバイスを入力します。

```
【実行例】

fastethernet
```

(7) 以下のように表示されます。

```
Connector Type (AUI/RJ45) [AUTO_CONFIG]:
```

(8) 変更の必要がありませんので、単にリターンキーを入力します。

(9) 以下のように表示されます。

```
Interface IP address:
```

(10) IX2000/IX3000 シリーズ側に付与する IPv4 アドレスを入力します。

```
【実行例】

192.168.1.1
```

(11) 以下のように表示されます。

```
IP mask [FFFFFF00]:
```

(12) IX2000/IX3000 シリーズ側に付与した IPv4 アドレスのネットマスク（プレフィックス）を入力します。変更の必要がない場合は、単にリターンキーでも構いません。

```
【実行例】

ffffff00
```

(13) 以下のように表示されます。

```
Boot from host:
```

(14) tftp サーバ側の IPv4 アドレスを入力します。

```
【実行例】

192.168.1.2
```

(15) tftp サーバが同一リンクに存在しない場合は、以下のように表示されます。

```
Via gateway:
```

(16) "Via gateway:"が表示された場合は、ゲートウェイの IPv4 アドレスを入力します。

```
【実行例】

192.168.1.254
```

(17) 以下のように表示されます。

```
Boot file name:
```

(18) tftp サーバ側に置いたファームウェアを入力します。

【実行例】

ix2215-1.1.1.ldc

(19) 正常に設定できれば、ドットが連続して表示され、外部のファームウェアによる立ち上げが可能となります。ドットが表示されている間、tftp get が動作しています。

正常にドットが表示されず、コンソールクエリーが再度表示された場合は、ネットワーク上に何らかの問題がある可能性があります。ネットワークを確認し、再度設定してください。

(20) 以上で立ち上げまで完了しましたが、ファームウェアは フラッシュ上にダウンロードされておりませんので、引き続き、通常のファームウェアバージョンアップの方法を実行します。

■10.5 コンフィグファイルのダウンロード方法

コンフィグを記述したテキストファイルを tftp サーバ上に置いておき、そのファイルをダウンロードしてコンフィグを設定する手順を説明します。コンフィグファイルは、制御コード以外の ASCII 文字のみで記述されている必要があります。それ以外の文字を使用した場合、正常に起動しなくなることがありえますので注意が必要です。

(1) 到達可能な経路上に tftp サーバを用意し、コンフィグファイルを置いておきます。

(2) IX2000/IX3000 シリーズに、Administrator 権限でログインします。

```
login: username
password: password
```

(3) 必要に応じて、tftp サーバへのルーティング情報を設定します。

【実行例】

IPv4 の場合
```
ip route 192.168.10.1/32 FastEthernet0/0.1
```

IPv6 の場合
```
ipv6 route fec0:1000:100::/64 FastEthernet0/0.1
```

(4) tftp サーバへの到達確認（IPv4 または IPv6）を行います。

【実行例】

IPv4 の場合
```
ping 192.168.10.1
```

IPv6 の場合
```
ping6 fec0:1000:100::1
```

(5) copy コマンドにより、コンフィグのテキストファイルをダウンロードします。

【実行例】

IPv4 の場合
```
copy 192.168.10.1:ix1000-config startup-config
```

IPv6 の場合
```
copy [fec0:1000:100::1]:ix1000-config startup-config
```

(6) exit コマンドでオペレーションモードに移り、リロードを行います。

```
exit
reload y
```

(7) 正常に立ち上がったら、動作確認を実施します。

■10.6 工場出荷値設定へのもどし方

IX2000/IX3000 シリーズを、工場出荷値にもどす方法を説明します。この手順は、ディップスイッチによるスーパーリセット手順とは異なり、ソフトウェアで工場出荷値にもどす手順を示しています。

以下の手順により、工場出荷値にもどすことができます。

(1) IX2000/IX3000 シリーズに、Administrator 権限でログインします。

```
login: username
password: password
```

(2) startup-config, default-config（使用時）を削除します。

```
erase startup-config
erase default-config
```

注 1：このコマンドを実行しても、ファイルは削除されません。
ファイルは、show flash コマンドにより確認し、
必要なプログラムファイル以外を、erase コマンドにより削除します。

注 2：このコマンドを実行しても、オプションソフトのライセンス情報は削除されません。
ライセンス情報は、show license コマンドにより確認し、
erase license コマンドにより削除します。

注 3：このコマンドを実行しても、エラーログ情報は削除されません。
エラーログ情報は、show error-log コマンドにより確認し、
clear error-log コマンドにより削除します。

(3) ctrl と z キーを入力（ctrl + z）する（exit コマンドも利用可能）ことで、オペレーションモードに移り、リスタートを行います。

```
reload y
```

以上で工場出荷値にもどす処置は完了です。

■10.7 ブートできない場合の処置

ブートできないときは、お買い上げの販売店、または、担当のサービスセンターにご連絡ください。

11章 障害発生時の処置ガイドライン

本章では、IX2000/IX3000 シリーズに障害が発生した場合の対処方法を説明します。

■11.1 イベント表示による解析

IX2000/IX3000 シリーズでは､イベント情報を表示することで障害の解析を行うことができます。設定方法等は、ロギングの設定および syslog の設定の節を参照してください。また、各イベント情報については、イベントログリファレンスを参照してください。

■11.2 システムロードアベレージ

11.2.1 システムロードアベレージ

IX2000/IX3000 シリーズでは、システムロードアベレージを下記のコマンドで確認できます。

show utilization	システムロードアベレージの確認
show processes	プロセス毎のロードアベレージの確認

※Ver.8.8 以降システムロードアベレージの計測方法が変更となっています。Ver.8.8 以降では CPU 実行時間を計測して算出しているため CPU 使用率と同等となります。（便宜上、Ver8.8 以降でもロードアベレージという名称を利用します。）
※Ver.8.8 以降では実行プロセス毎のロードアベレージが show processes で確認することができます。
※システムロードアベレージは MIB で確認することができます。詳しくは付録のプライベート MIB 詳細を参照してください。
※システムロードアベレージは 1 秒間の平均値となります。つまり表示上 99%にならなくとも、瞬間的に高負荷となっている場合にはパケット廃棄などの原因となります。

Ver.8.8 以降の計測方法

システムロードアベレージの内部演算方式は、以下のようになっています。

$$\text{CPU 使用率（%）} = \frac{\text{プロセス毎の CPU 実行時間の合計}}{\text{1 秒間の割り込みで実際に進んだ CPU 時間}} \times 100$$

プロセス毎の CPU 実行時間の合計
＝ 1 秒間の割り込みで実際に進んだ CPU 時間 － システム idle 処理時間

Ver.8.8 以降では、システム idle 処理時間（主にルータ無負荷時のポーリング処理時間）を除いたプロセス毎の CPU 実行時間の総和と計測した 1 秒間の割り込み間隔の間に実際に進んだ CPU 実行時間の割合から算出します。

システムロードアベレージの計測は 1 秒間隔で行われ、コマンド実行時には過去の計測した最新の結果を表示します。

CPU 時間は、CPU 内部にある CPU クロックから計測できる命令を利用した差分時間により計測されます。（RTC や NTP の時間とは無関係です。）

Ver.8.7 以前の計測方法

Ver8.7 以前のシステムロードアベレージの内部演算方式は、以下のようになっています。

$$\frac{\text{最大スレッド数} \quad - \quad \text{現在のスレッド数}}{\text{最大スレッド数}} \times \quad 100$$

※常時測定を行い、コマンド実行時に過去に計測した最新の 1 秒間の結果を表示します。

スレッド数は、装置で動作した処理の数となります。IX2000/IX3000 シリーズでは、装置が何もしていない状態でも、短時間で終了する処理が動作します。したがって、何も処理していない状態が最大スレッド数となります。最大スレッド数は固定値となります。現在のスレッド数は、最新の 1 秒間に処理した数になります。時間がかかる処理を実行した場合、現在のスレッド数が少なくなり、システムロードアベレージは上昇します。

Ver8.7 以前のシステムロードアベレージは、一定時間に行った処理の回数から上記演算式に基づき計算を行ったスレッド実行偏差となりますので、CPU 使用率を表すものではありません。精度はあまり高くありませんが、負荷状態のおよその目安として利用することができます。

11.2.2 システムロードアベレージ履歴表示

システムロードアベレージの履歴を確認することができます。

show utilization history	システムロードアベレージの履歴表示

履歴は、以下の 3 種類があります。

- 過去 5 秒間の値の 5 分間の履歴
- 過去 1 分の値の 1 時間の履歴
- 過去 1 時間の値の 72 時間の履歴

1 秒毎にロードアベレージの収集を行い、測定期間（5 秒間，1 分間，1 時間）での平均値をその期間の値として保存します。それぞれの値は、履歴保存期間（5 分，1 時間，72 時間）分を保存します。

表示項目	表示の意味
peak	履歴保存期間の中の最大値
low	履歴保存期間の中の最小値
average	履歴保存期間の平均値
*	測定期間の測定値
|	測定期間での最大値／最小値

【表示例】

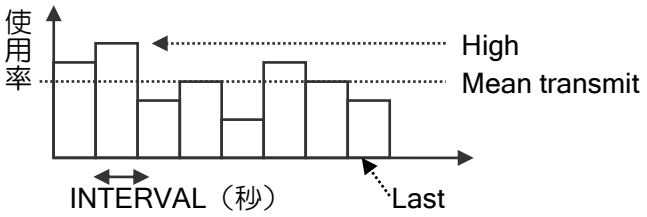
```
Router(config)# show utilization history
System utilization per 5 seconds(last 5 minutes): 42/16/20 (peak/low/average)
  (* = average, | = maximum and minimum)
      22224222222122222222222222222222222222222222222222222222222
      10102031030600000000000000001000000000000000000000000000000
  100      |
   90      |
   80      |
   70      |
   60      |
   50      |
   40      *
   30      | |  |
   20 ****|***********************************************************
   10             |
     +-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
     0s    30s   60s   90s   120s  150s  180s  210s  240s  270s  300s
```

■11.3 回線使用率の解析

IX2000/IX3000 シリーズでは、下記のコマンドで回線使用率を確認することができます。

show utilization	回線使用率の確認
clear utilization	回線使用率の消去

回線使用率表示は起動時または clear utilization コマンド投入後から測定され、
次のように使用率を測定し、測定値を表示します。INTERVAL の値は 60 秒です。
計算に使用するインタフェース速度は、実際に動作している速度となります。



表示項目	表示の意味
Mean transmit util	デバイス単位の送信使用率平均値
last transmit util	デバイス単位の送信使用率最新値
high transmit util	デバイス単位の送信使用率最大値
Mean receive util	デバイス単位の受信使用率平均値
last receive util	デバイス単位の受信使用率最新値
high receive util	デバイス単位の受信使用率最大値

■11.4 送受信パケットの解析

IX2000/IX3000 シリーズでは、送受信パケットをレイヤ 2 レベルでコンソールにダンプ出力（最大 128byte 分）することができ、パケット解析に役立ちます。下記に示すコマンドにより、パケットを確認することができます。

logging packet	レイヤ 2 レベルダンプ設定
event-terminal	コンソールまたは telnet クライアント表示

パケットをダンプ表示している際、ルータ性能は著しく低下します。また、パケットすべてをダンプできる保証はありません。

また、ダンプ情報は syslog 転送できません。

■11.5 装置異常時の解析

IX2000/IX3000 シリーズで装置異常が発生した場合、システムの状態を確認することで障害原因を解析することができます。

11.5.1 装置電圧状態の確認

下記に示すコマンドにより、電圧状態を確認することができます。

show environment	電圧状態の確認

電圧状態は、MIB で確認することができます。また、異常値となった場合に、SNMP マネージャに SNMP トラップを送信することができます。詳しくは SNMP を利用した監視の節を参照してください。

11.5.2 装置温度状態の確認

下記に示すコマンドにより、温度状態を確認することができます。

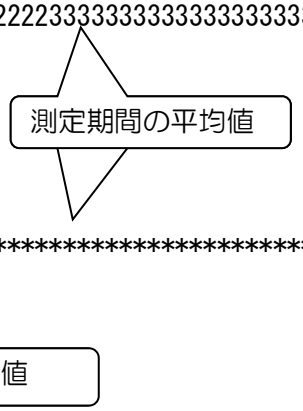
Ver.8.3.39 以降は、起動後の最高温度、最低温度および過去 1 時間の値の 72 時間分、Ver.8.7 以降は 72 週分の履歴を確認することができます。

show environment	温度状態の確認

表示項目	表示の意味
maximum	起動後からの最大値
minimum	起動後からの最小値
total fault time	起動後からの温度アラーム累積継続時間
peak	履歴保存期間の中の最大値
low	履歴保存期間の中の最小値
average	履歴保存期間の平均値
*	測定期間の測定値
|	測定期間での最大値／最小値

【表示例】

```
(config)# show environment history
System hardware information:
      :
    maximum  61.0C 20XX/0X/XX 10:28:14
    minimum  43.0C 20XX/0X/XX 08:02:00
    total fault time 0d0h0m

    Internal temperature per 1 hour(last 2 days): 54/47/52 (peak/low/average)
      (* = average, X = detected fault, | = maximum and minimum)

      445555555555555555555555555555555555555555555555555555555555554555
    C 883444444434444433333333333333333333222223333333333333333333329000
  100
   90
   80
   70
   60              |
   50 ***************  ************************************************
   40  |
   30
   20
   10
    0
  -10
```



温度状態は、MIB で確認することができます。また、異常値となった場合に、SNMP マネージャに SNMP トラップを送信することができます。詳しくは SNMP を利用した監視の節を参照してください。

11.5.3 装置 FAN 状態の確認

下記に示すコマンドにより、FAN 状態を確認することができます。

show environment	FAN 状態の確認（IX3000 シリーズのみ） 正常値（5295rpm 以上） 5294rpm 以下の場合は全て 5294 となります。

FAN 状態は、MIB で確認することができます。また、異常値となった場合に、SNMP マネージャに SNMP トラップを送信することができます。詳しくは SNMP を利用した監視の節を参照してください。

11.5.4 メモリの状態確認

下記に示すコマンドにより、メモリ使用状態を確認することができます。

show memory	メモリ状態の確認

【表示例】
Ver.8.7 以降

```
ipsec(config)# show memory
Calculating configuration memory size...
Heap memory:
   48% memory used, 52% memory avail
   Total 54799528 bytes
      28041028 bytes free (27928484 clean, 112544 dirty)
      26758500 bytes busy (10102128 dynamic, 16656372 permanent)
Configuration memory:
   0% memory used, 100% memory avail
   Total 524288 bytes, 522572 bytes free

Storage statistics:
   Embodiments: 50045/49838/207 (total/busy/idle)
   Exhausts: 0/0/0 (desc/area/sysiob)
Scope: 0x04000000/0x02263fbc/0x00a4f708 (head/curr/tail)
    Size(b)     Busy-list     Idle-list   Ref(alloc)     Ref(free)
         32         24165            52        76385         52220
         48         14444           117        25782         11338
         64           962             5         2732          1770
         96          3502            10         7487          3985
        128           712             5         2039          1327
          :
```

Ver5.0～Ver8.1

```
Router(config)# show memory
Heap memory
   Total 11710823 bytes, 8385472 bytes reserved (23616 bytes for heap)
   1349399 bytes free (1213623 clean, 135776 dirty), 1975952 bytes busy
Configuration memory
   Total 64512 bytes, 58483 bytes free
```

ヒープメモリでは、運用中に使用しているメモリ量を確認することができ、コンフィグレーションメモリは、コンフィグとして設定しているサイズを確認することができます。

Ver.8.2 以降の表示項目（ヒープメモリ）

表示項目	表示の意味
memory used	使用中のメモリ量（パーセント）
memory avail	使用可能なメモリ量（パーセント）
Total	メモリ量の合計
free	未使用のメモリ量。 clean と dirty の合計になります。
clean	一度も使用していないメモリ量。 残りサイズ分までメモリ確保できます。

dirty	使用されていたが解放され使用可能なメモリ量。 フラグメンテーションの状態により残りサイズ分はメモリ確保ができない場合があります。
busy	使用中のメモリ量。
dynamic	解放可能だが同一サイズでのみ再利用可能なメモリ
permanent	ヒープとして使用しないメモリ量
temporary	解放可能でサイズに関係なく再利用可能なメモリ

Ver8.1 以前の表示項目（ヒープメモリ）

表示項目	表示の意味
Total	メモリ量の合計
reserved	ヒープとして使用しないメモリ量
free	未使用のメモリ量。 clean と dirty の合計になります。
clean	一度も使用していないメモリ量。 残りサイズ分までメモリ確保できます。
dirty	使用されていたが解放され使用可能なメモリ量。 フラグメンテーションの状態により残りサイズ分はメモリ確保ができない場合があります。
busy	使用中のメモリ量

コンフィグレーションメモリ

表示項目	表示の意味
Total	メモリ量の合計
free	未使用のメモリ量

サイズ毎の統計

表示項目	表示の意味
Size(b)	サイズ
Busy-list	使用中のメモリ数
Idle-list	未使用のメモリ数
Ref(alloc)	確保した回数
Ref(free)	解放した回数

MIB でも確認することができます。詳しくは付録のプライベート MIB 詳細を参照してください。

フリーサイズが少量になってきている場合は、ネットワーク設計の見直しやコンフィグの見直しが必要です。

あるいは、バージョンアップによるコンフィグ自動継承により、コンフィグレーションメモリの未使用エリアが確保されていることも考えられます。コンフィグ継承のしくみの節を参照してください。

11.5.5 バッファの状態確認

下記に示すコマンドにより、デバイス単位のバッファ使用状態を確認することができます。

show buffers	バッファ状態の確認

システムバッファは、装置内でパケットを生成する場合、そのバッファに一旦プールします。そのバケットの転送処理が完了すると、バッファから削除されます。

一方、インタフェースに属するバッファは、外部から受信したパケットをプールします。システムバッファと同様に、そのパケットの転送処理が完了すると、バッファから削除されます。

付録のキューイング処理も参照してください。

11.5.6 キューの状態確認

下記に示すコマンドにより、デバイス単位のキュー状態を確認することができます。

show queue	キュー状態の確認

付録のキューイング処理を参照してください。

11.5.7 uptime の確認

下記に示すコマンドにより、uptime を確認することができます。

show uptime	uptime の確認

uptime は、reload や restart した直後から測定した運用時間を表します。

11.5.8 エラーログの確認

IX2000/IX3000 シリーズでは異常が発生した場合にログ情報を不揮発性メモリ上に保存しています。下記に示すコマンドにより、エラーログを確認・消去することができます。

show error-log	エラーログの確認
clear error-log	エラーログ、エラーカウンタの消去

エラーログは、最も新しい情報のみが上書きで保存されています。したがって前回発生した異常情報は削除されます。ただし、異常を確認した回数を示すエラーカウンタが含まれていますので、過去に生じた異常回数は確認することができます。このエラーカウンタは、clear error-log コマンドにて初期値 0 にもどすことができます。

11.5.9 プログラムおよびハードウェア情報の確認

下記に示すコマンドにより、プログラムバージョンおよびハードウェア情報を確認することができます。

show version	プログラムバージョン情報の確認
show hardware	ハードウェア情報の確認

■11.6テクニカルサポートのための状態収集

IX2000/IX3000 シリーズでは、ご自身では解析できない問題が生じた場合に、テクニカルサポートに送るための情報を収集することができます。通常、下記に示す 2 つのコマンドにより、情報を収集してください。

show tech-support	テクニカルサポート送付用情報の収集
show logging	ログの表示

11.6.1 テクニカルサポート送付用情報の確認

以下のコマンドでテクニカルサポートに送るための情報を一括収集することができます。

show tech-support	テクニカルサポート送付用情報の収集

表示内容が非常に多いため、more で中断されないようにしておくと収集が容易になります。Ver8.4 以降の場合は show tech-support no-pausing コマンドで停止せずに収集できます。それ以前のバージョンは、グローバルコンフィグで terminal length 0 コマンドを入力することで同様に停止せず収集することができます。

またテクニカルサポート情報をファイルとして書き込むことができます。ファイルに書き込み後は copy または tftp コマンドで、装置から PC 等にファイルを転送してください。なお、通常 TFTP サーバへのアップロードは、アップロード先に同名のファイルが存在している必要があります（上書きしかできません）。

【実行例】
tech.txt というファイル名で保存し、10.0.0.1 のサーバに転送。

```
Router(config)# show tech-support output tech.txt
% Warning: do NOT enter CNTL/Z while writing to avoid information corruption.
Calculating configuration memory size...
.............[OK]
Written 110794 bytes
Router(config)# tftp put tech.txt 10.0.0.1:tech.txt
.......
TFTP transfer complete
Router(config)#
```

11.6.2 ロギング情報の確認

下記に示すコマンドにより、ログ情報を確認することができます。装置のログ情報を表示しますので、必要に応じて情報を収集してください。

ログの設定に関しては、「遠隔設定と監視」の項を参照してください。

show logging	ログの表示

【表示例】

```
Router(config)# show logging
Buffer logging enabled, 131072 bytes, type cyclic
   1395 messages (116163-117557), 131056 bytes logged, 116162 messages dropped

Log Buffer (116163-117557):
```

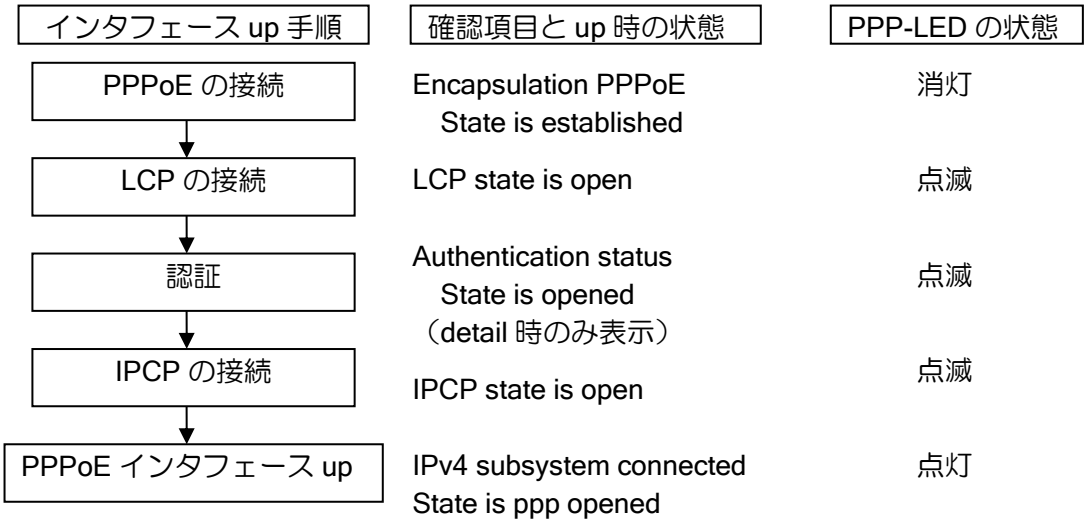
以下に問い合わせの多いログについて説明します。

<table>
<tr><th>番号</th><th colspan="2">内容</th></tr>
<tr><td rowspan="4">IP.006</td><td colspan="2">パケット送信に失敗し廃棄しました。</td></tr>
<tr><td>廃棄要因</td><td>内容</td></tr>
<tr><td>LINK-FRMWRK: PACKET NOT ACCEPTED FOR FLOW CONTROL REASONS</td><td>オーバーフローによる廃棄</td></tr>
<tr><td>LINK-FRMWRK: NO ENTRY IN LOOKUP TABLE TO COMPLETE OPERATION</td><td>ARP 解決失敗による廃棄</td></tr>
<tr><td>SEC.025</td><td colspan="2">IPsec 使用時に、パケット送信に失敗し廃棄しました。
廃棄要因は、IP.006 と同様になります。</td></tr>
<tr><td>TCP.007</td><td colspan="2">ルータ宛の TCP パケットを廃棄しました。
TCP により再送されるので、問題はありません。</td></tr>
</table>

■11.7 インタフェースの確認

11.7.1 PPPoE インタフェースの状態確認

PPPoE インタフェースは以下の手順で up します。
show interfaces コマンドにより、各段階でどのような状態になっているか確認できます。



【表示例】

状態をわかりやすくするため、他の情報は省略しています。

```
(config)# show interfaces FastEthernet0.1
Interface FastEthernet0.1 is up
   Fundamental MTU is 1492 octets
   Current bandwidth 100M b/s, QoS is disabled
   Datalink header cache type is ppp-over-ethernet: 0/0 (standby/dynamic)
           IPv4 subsystem connected, physical layer is up, 0:00:57
   Dialer auto-connect is enabled
      :
   Encapsulation PPP:
              PPP state is ppp opened , prev state is ppp closed
              LCP state is open, prev state is ack sent, since 0:00:57
              IPCP state is open, prev state is ack sent, since 0:00:57
      IPV6CP state is closed
   Encapsulation PPPoE:
      Session ID is 9026
              State is established, prev state is PAD session confirmation wait
      Connected access concentrator is Cisco-1
      Host unique tag: 00711c78
           :
```

PPPoE インタフェースの通信ができない場合、以下のコマンドで状態を確認することで、原因を推測することができます。

“Interface ** is”はインタフェースの状態を示します。

“prev-state”は失敗している処理を示します。インタフェースが up しない場合は、この状態を確認することで、どの処理で失敗しているかわかります。

“PPP state”は現在の状態を示します

【表示例】
```
(config)# show interfaces FastEthernet0.1
Interface FastEthernet0.1 is up
   Fundamental MTU is 1492 octets
   Current bandwidth 100M b/s, QoS is disabled
   Datalink header cache type is ppp-over-ethernet: 0/0 (standby/dynamic)
   IPv4 subsystem connected, physical layer is up, 0:00:57
   Dialer auto-connect is enabled
      :
   Encapsulation PPP:
            PPP state is ppp opened , prev state is ppp closed
      :
```

Interface ** is	状態	推測される原因/対処
up	リンクが up している	
down	リンクが down している	ケーブルを確認してください。
administratively down	管理状態が down している	インタフェースの no shutdown を設定してください。
prev state	**状態**	**推測される原因/対処**
ppp close（Ver.8.2 以降）	LCP が起動していない	以下を確認してください。 物理的な接続 ケーブル ADSL モデムとの接続
pppoe timeout（Ver.8.1 以前）	PPPoE サーバからの応答がない	
lcp failure	LCP が接続できない	対向装置と ppp profile のコンフィグが合っているか確認してください。（LCP,認証関連の設定）
lcp timeout	LCP の応答が返らない	プロバイダに確認してください。
chap receive failure chap send failure pap receive nak pap send nak	認証が失敗	ppp profile の authentication myname authentication password の設定を確認してください。 RADIUS 利用時は、RADIUS の設定を確認してください。
chap failure pap failure chap timeout pap timeout	認証中に処理失敗	応答のタイムアウトまたは、PPP の設定を確認してください。 RADIUS 利用時は、RADIUS の設定を確認してください。
chap close pap close（Ver.8.2 以降）	認証終了後、IPCP/IPv6CP が起動しなかった	IP,IPv6 の設定を確認してください
PPP state	**状態**	**推測される原因/対処**
ppp opened	正常に接続しています。	
ppp opened (address negotiation failed)（Ver8.2 以降）	接続しているが、アドレス情報がもらえていない	対向装置と IPCP 関連,アドレスの設定があっているか確認してください。
ppp opened w/ failure（Ver.8.1 以前）	接続しているが、何らかの情報がもらえていない。	対向装置とコンフィグがあっているか確認してください。 （IPCP 関連,アドレスの設定） サーバからアドレスがもらえていない場合は、プロバイダ（または、対向装置）に確認してください。

11.7.2 トンネルインタフェースの確認

Tunnel インタフェースの状態は、以下のコマンドで確認できます。

【表示例】

```
(config)# show tunnel status
Total statistics
   0 packets input, 0 bytes, 0 errors
   0 packets output, 0 bytes, 0 errors
Interface Tunnel11.0
   Tunnel mode is ipsec (4-over-4)
   Tunnel is ready
   Destination address is 192.168.160.2
   Source address is 192.168.160.1
   Outgoing interface is FastEthernet1/0.0
         :
```

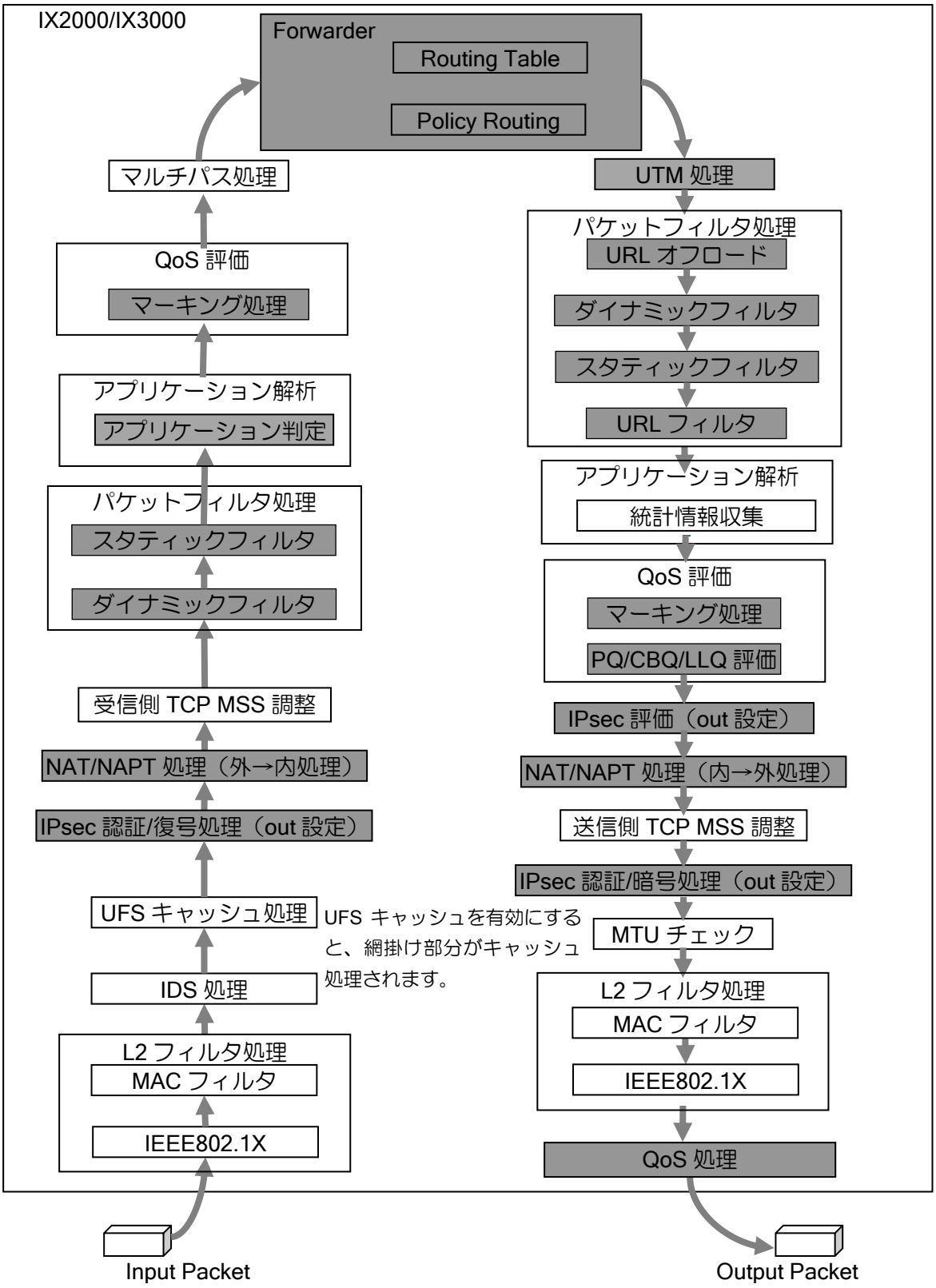
Tunnel 状態	状態/推測される原因
Tunnel is ready	使用可能な状態です。
Tunnel mode is not specified	tunnel mode が設定されていません。 コンフィグを確認してください。
Source address selection failed	ソースアドレスの選択に失敗しました。 インタフェースの状態を確認してください。
Destination is unreachable	あて先への経路がありません。 経路情報を確認してください。
Destination is never reachable via loopback interface	あて先への経路が Loopback インタフェースとなっています。経路情報を確認してください。
Destination address is not configured	あて先アドレスが設定されていません。 コンフィグを確認してください。
Source address is not configured on specified interface	指定されたインタフェースにアドレスが設定されていません。コンフィグを確認してください。
Source address is not assigned to local interface	指定されたソースアドレスがどのインタフェースにも設定されていません。 コンフィグを確認してください。
Destination address is assigned to local interface	指定されたあて先アドレスが装置のインタフェースに設定されています。 コンフィグを確認してください。
Number of nested encapsulations is over limit	トンネルネスト数の制限（3）を超えています。 コンフィグを確認してください。
IPsec is not ready	IPsec の開始のための準備ができていません。 IPsec のコンフィグを確認してください。

12章 パケット評価フロー

■12.1 IPv4 パケット評価

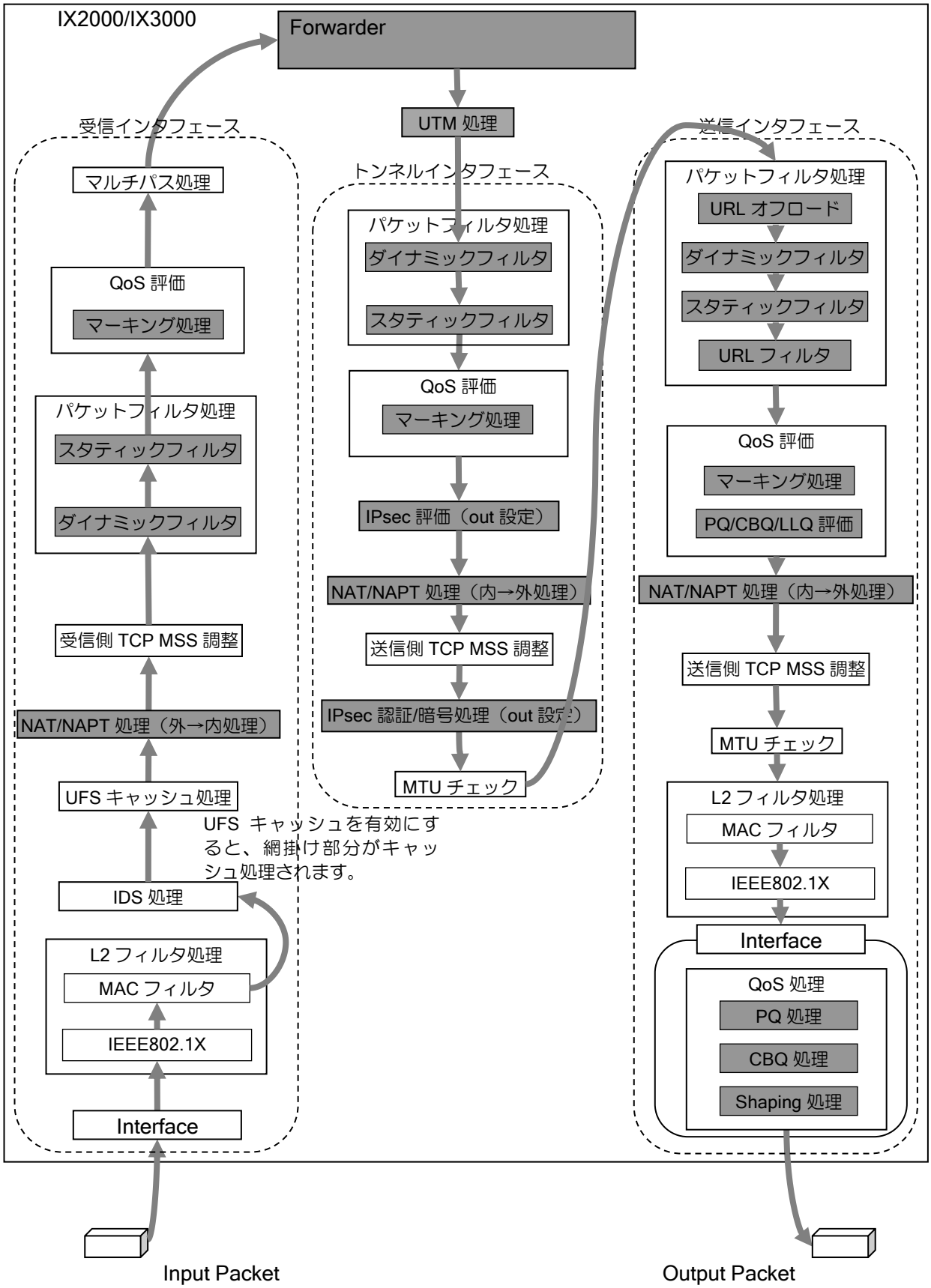
IPv4 Forwarder 配下のパケット評価順を説明します。

入力インタフェース処理・フォワーディング・出力インタフェース処理は、以下の順序で行われます。



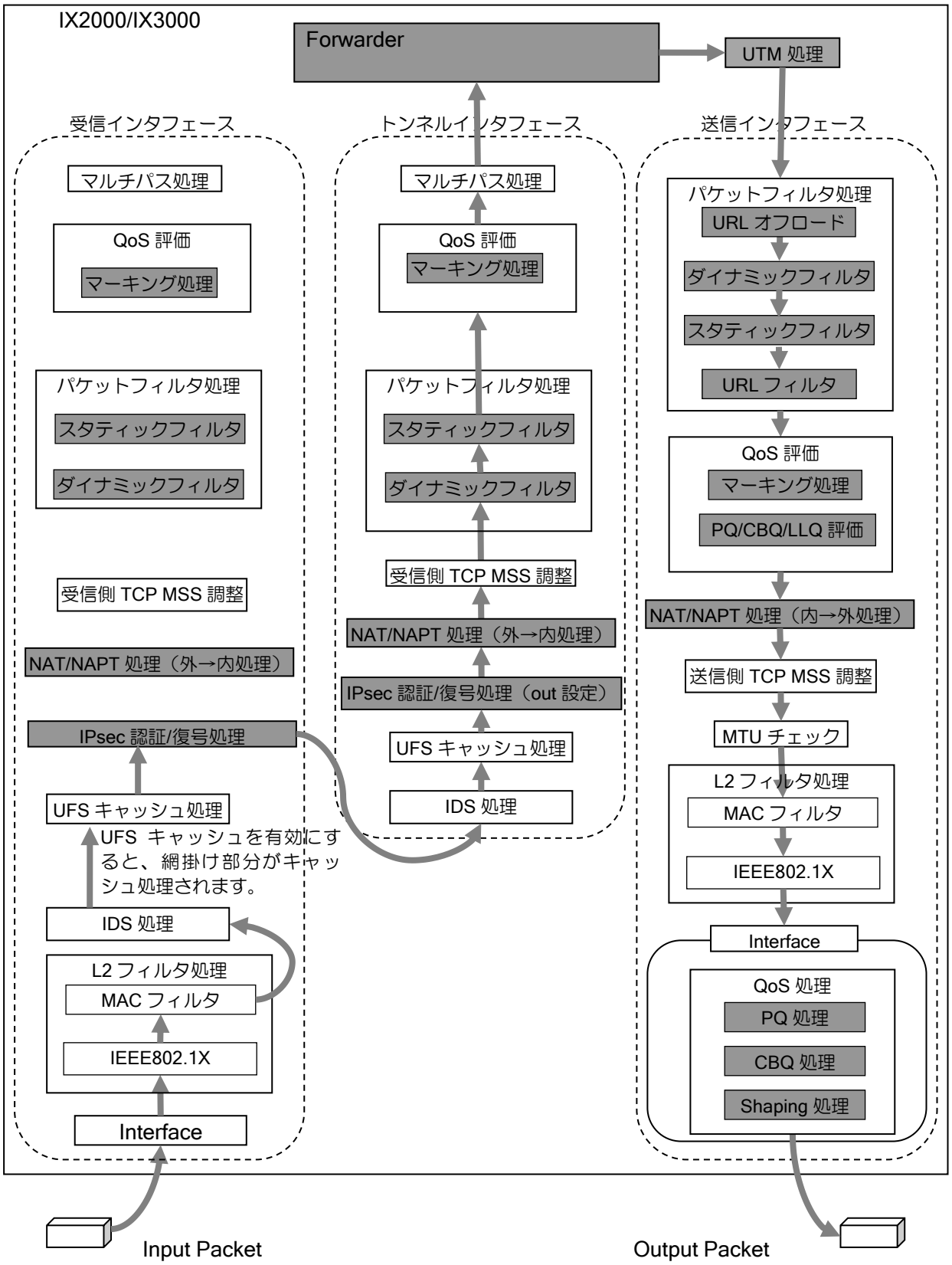
■12.2 IKEv1/IPsec 送信評価フロー

- IKEv1/IPsec（トンネルモード）送信時の評価フロー
- IKEv1 では IPsec でカプセル化したパケットに対して IP フィルタ、NAT 等は適用しません。



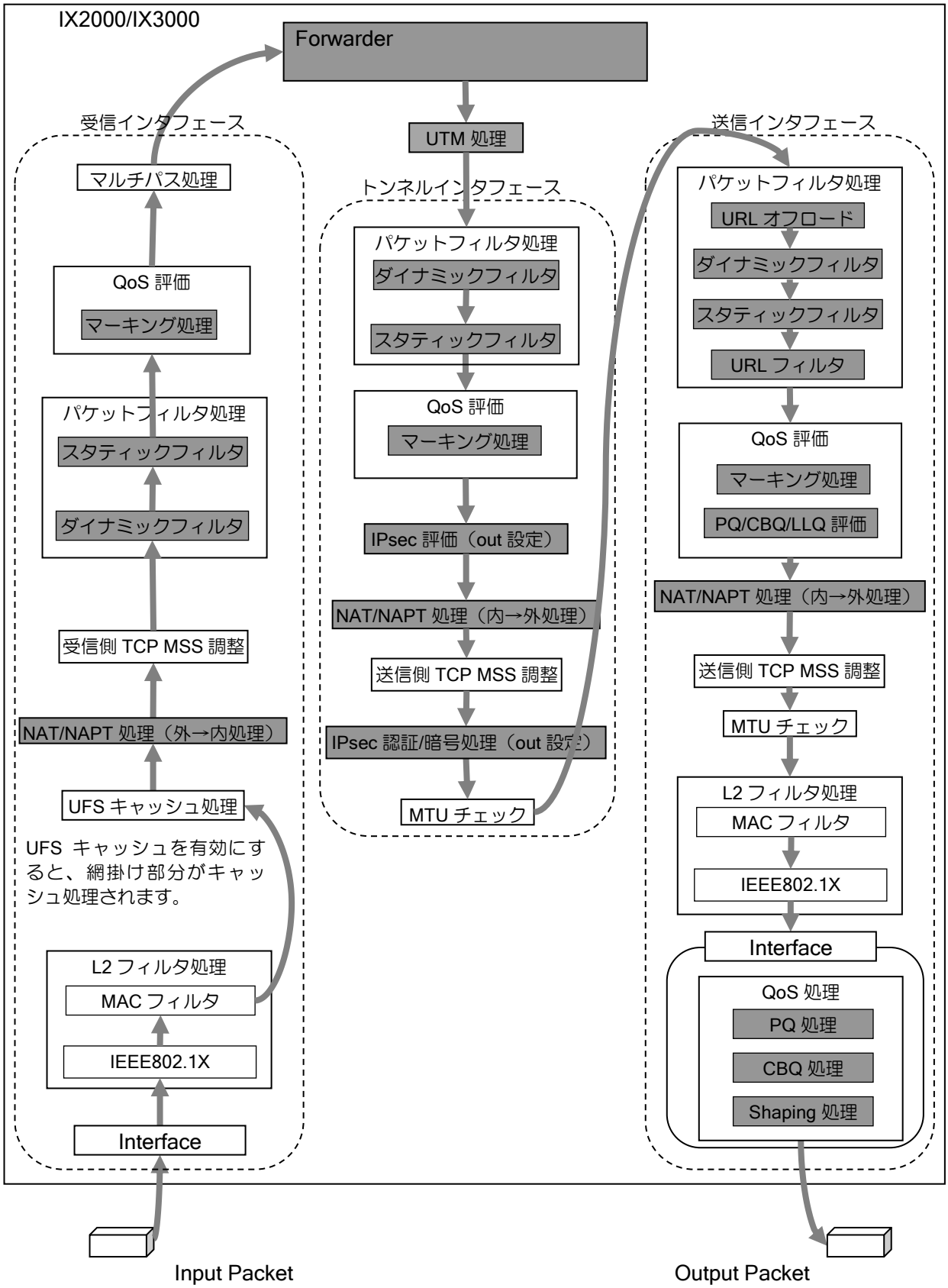
■12.3 IKEv1/IPsec 受信評価フロー

- IKEv1/IPsec（トンネルモード）受信時の評価フロー
- IKEv1 では IPsec でカプセル化されたパケットに対して IP フィルタ、NAT 等は適用しません。



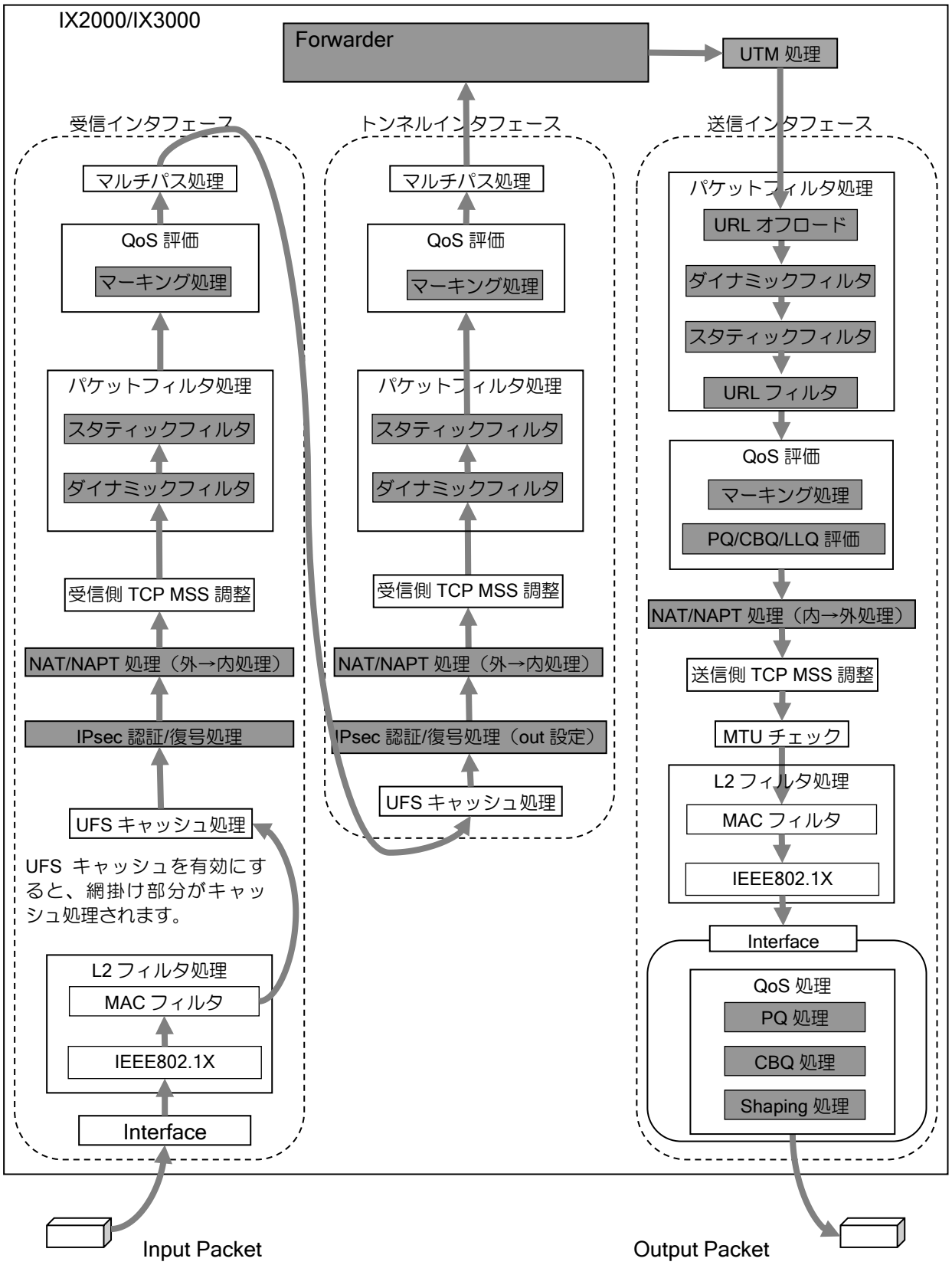
■12.4 IKEv2/IPsec 送信評価フロー

- IKEv2/IPsec（トンネルモード）送信時の評価フロー
- IKEv2 の場合は、通常どおり受信インタフェースの全ての設定を参照します。



■12.5 IKEv2/IPsec 受信評価フロー

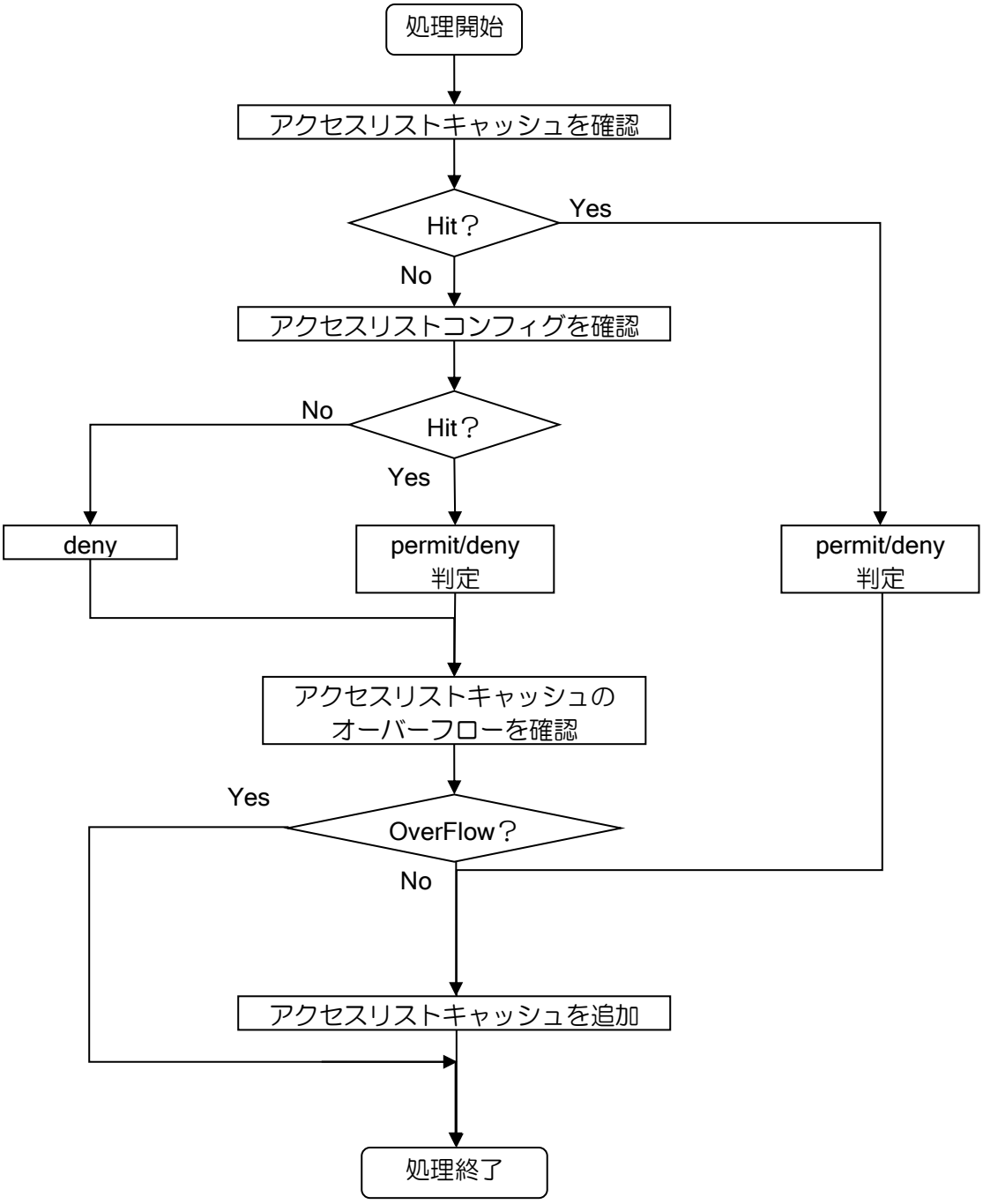
- IKEv2/IPsec（トンネルモード）受信時の評価フロー
- IKEv2 の場合は、通常どおり送信インタフェースの全ての設定を参照します。



機能	対応バージョン
Forwarder	Ver.1～
スタティックフィルタ	Ver.1～
NAT/NAPT 処理（外→内処理）	Ver.1～
IPsec 認証/暗号/復号処理（in 設定）	Ver.1～
MTU チェック	Ver.1～
ダイナミックフィルタ	Ver.2～
マーキング	Ver.2～
PQ	Ver.2～
CBQ	Ver.2～
LLQ	Ver.7.3～
IPsec 認証/暗号処理（out 設定）	Ver.2～
IPsec 認証/復号処理（out 設定）	Ver.2～
ポリシールーティング	Ver.2～
Shaping	Ver.3～
マルチパス処理	Ver.4.0～
TCP MSS 調整	Ver.4.0～
IPsec 評価（out 設定）	Ver.4.0～
UFS キャッシュ	Ver.4.2～
MAC フィルタ	Ver.6.2～
IEEE802.1X	Ver.7.4～
UTM	Ver.10.0～

■12.6 アクセスリスト評価フロー

アクセスリストのパケット評価順を説明します。



13章 バージョンアップにおける諸注意

IX2000/IX3000 シリーズでは、プログラムのバージョンアップの際に自動的に旧バージョンのコンフィグ情報を引き継ぐように設計されています。しかし、新機能の追加や旧機能の大幅な変更に伴い、完全には引き継げない項目が存在します。それらはバージョンアップ後に適切な設定を行う必要があります。

Ver8.0 以降でソフトウェアをバージョンアップした際の注意事項について説明します。Ver8.0 以前については説明を割愛します。

※なお、バージョンアップは提供している rap ファイルで実施してください。ブートとソフトウェアのバージョンは、提供している rap ファイルの組み合わせのみサポートします。バージョンの不一致が発生した場合、動作不良や装置故障の原因となることがあります。

■13.1 Ver.8.1 コンフィグ

Ver.8.1 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.1.1 自動コンフィグ継承

Ver.8.1 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.1.2 コンフィグ継承の注意事項

Ver.8.1 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
BGP	Ver.8.1 以降、デフォルトでは、デフォルトルート送信設定は、デフォルトルートが存在する場合にデフォルトルートを広告します。デフォルトルートを常に送信する場合は、パラメータに always を追加して設定しなおしてください。	originate-default
	Ver.8.1 以降、ピア毎のデフォルトルート送信設定は削除しました。特定のピアのみデフォルトルートを広告したい場合は、デフォルトルートを広告しないピアに対して、no neighbor send-default を設定してください。	neighbor originate-default

■13.2 Ver.8.2 コンフィグ

Ver.8.2 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.2.1 自動コンフィグ継承

Ver.8.2 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.2.2 コンフィグ継承の注意事項

Ver.8.2 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
UFS キャッシュ	キャッシュ数のデフォルト値が 4096 から 8192 に変更になっています。影響がある場合は、キャッシュ数を変更してください。	ip ufs-cache max-entries

■13.3 Ver.8.3 コンフィグ

Ver.8.3 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.3.1 自動コンフィグ継承

Ver.8.3 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
IPv6	RA のパラメータを設定する複数のコマンドが変更になりました。古いコマンドは新しいコマンドに引き継がれます。	ipv6 nd ra
Access-list	アクセスリストの src/dest にアドレス以外が設定された場合、ドメイン名と判断し新しいパラメータに引き継がれます。	ip access-list ipv6 access-list

13.3.2 コンフィグ継承の注意事項

Ver.8.3 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
AutoTunnel	AutoTunnel 機能を削除しました。	
IPv6	ipv6 scope-zone コマンドを削除しました。	ipv6 scope-zone

■13.4 Ver.8.4 コンフィグ

Ver.8.4 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.4.1 自動コンフィグ継承

Ver.8.4 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.4.2 コンフィグ継承の注意事項

Ver.8.4 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.5 Ver.8.5 コンフィグ

Ver.8.5 へバージョンアップでは注意事項はありません。
を行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.5.1 自動コンフィグ継承

Ver.8.5 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.5.2 コンフィグ継承の注意事項

Ver.8.5 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.6 Ver.8.6 コンフィグ

Ver.8.6 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.6.1 自動コンフィグ継承

Ver.8.6 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.6.2 コンフィグ継承の注意事項

Ver.8.6 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
ARP	ARP エントリのデフォルト数が拡張されています。 Ver8.5 以前のデフォルト値（1024）で使用する場合は、コマンドにより設定を変更してください。	arp max-neighbors

■13.7 Ver.8.7 コンフィグ

Ver.8.7 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.7.1 自動コンフィグ継承

Ver.8.7 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.7.2 コンフィグ継承の注意事項

Ver.8.7 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
DNS	ip6.int をデフォルトでは使用しません。 ip6.int を使用する場合は、コマンドにより設定を変更してください。	dns interoperability support-ip6.int
プロキシ DNS	DNS キャッシュ有効時、デフォルトでは応答に DNS キャッシュを使用しません。応答に DNS キャッシュを使用する場合は、コマンドにより設定を変更してください。	proxy-dns ip/ipv6 enable

■13.8 Ver.8.8 コンフィグ

Ver.8.8 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.8.1 自動コンフィグ継承

Ver.8.8 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.8.2 コンフィグ継承の注意事項

Ver.8.8 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.9 Ver.8.9 コンフィグ

Ver.8.9 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.9.1 自動コンフィグ継承

Ver.8.9 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.9.2 コンフィグ継承の注意事項

Ver.8.9 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
BGP	Ver.8.9 以降、未対応の受信ケーパビリティの確認は行いません。これに伴い、neighbor receive-capability コマンドは無効となります。設定時はコンフィグから削除されます。	neighbor receive-capability

■13.10 Ver.8.10 コンフィグ

Ver.8.10 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.10.1 自動コンフィグ継承

Ver.8.10 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
PPP	ipcp request-ip-address コマンドの名称が変更になりました。ipcp provide-ip-address コマンドに引継がれます。	ipcp provide-ip-address

13.10.2 コンフィグ継承の注意事項

Ver.8.10 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.11 Ver.8.11 コンフィグ

Ver.8.11 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.11.1 自動コンフィグ継承

Ver.8.11 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.11.2 コンフィグ継承の注意事項

Ver.8.11 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.12 Ver.9.0 コンフィグ

Ver.9.0 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.12.1 自動コンフィグ継承

Ver.9.0 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.12.2 コンフィグ継承の注意事項

Ver.9.0 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
ダイナミック DNS/ PKI 関連/ ソフトウェア更新	Ver9.0.14a 以降、HTTPS の使用プロトコルのデフォルトが SSLv3.0 から TLS1.0 に変更となります。SSLv3.0 を使用する場合は ssl-protocol に SSLv3.0 を指定してください（非推奨です）。	

■13.13 Ver.9.1 コンフィグ

Ver.9.1 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.13.1 自動コンフィグ継承

Ver.9.1 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.13.2 コンフィグ継承の注意事項

Ver.9.1 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.14 Ver.9.2 コンフィグ

Ver.9.2 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.14.1 自動コンフィグ継承

Ver.9.2 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
ダイナミック DNS	source コマンドの名称が変更になりました。 source-interface コマンドに引継がれます。	source-interface
Web コンソール	webcon コマンドの名称が変更になりました。 web-console コマンドに引き継がれます。	
Web コンソール	自動ログアウトの設定をデフォルト 60 分に変更します。 従来のデフォルト設定では自動ログアウトはしません。	

13.14.2 コンフィグ継承の注意事項

Ver.9.2 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.15 Ver.9.3 コンフィグ

Ver.9.3 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.15.1 自動コンフィグ継承

Ver.9.3 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
スケジューラ	scheduler list コマンド名称が変更になりました。 command-action list コマンドに引き継がれます。	command-action list

13.15.2 コンフィグ継承の注意事項

Ver.9.3 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
ダイナミック VPN	Ver.9.3 以降、センタ（ハブ）側の接続数を制限し、初期値は最大接続数となっています。最大接続数は、諸元値を参照してください。接続数を変更する場合は、nhrp max-connections コマンドにて変更してください。	nhrp max-connections
napt	キャッシュサイズのデフォルト数が拡張されています。※IX2025, IX3015 以外の機種 Ver.9.2 以前のデフォルト値（4096）で使用する場合は、コマンドにより設定を変更してください。	ip napt translation max-entries

■13.16 Ver.9.4 コンフィグ

Ver.9.4 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.16.1 自動コンフィグ継承

Ver.9.4 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.16.2 コンフィグ継承の注意事項

Ver.9.4 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。以下は、バージョンアップ後に適切な設定を行う必要が生じる場合があります。

分類	設定内容	参照
SNMP	Ver.9.4 以降、SNMPv2 のリンク up/down トラップに ifAdminStatus、ifOperStatus が付与されます。Ver.9.3.11 以前の動作にする場合は、snmp-agent ip trap コマンドにて変更してください。	snmp-agent ip trap

■13.17 Ver.9.5 コンフィグ

Ver.9.5 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.17.1 自動コンフィグ継承

Ver.9.5 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.17.2 コンフィグ継承の注意事項

Ver.9.5 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.18 Ver.9.6 コンフィグ

Ver.9.6 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.18.1 自動コンフィグ継承

Ver.9.6 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
Proxy-DNS	proxy-dns ip enable、proxy-dns ipv6 enable のオプション request がコマンドとして独立します。 proxy-dns ip request、proxy-dns ipv6 request コマンドに引き継がれます。	
sFlow	sflow sampling-rate コマンドにサンプリング方向(in/out)のパラメータ指定が必要になります。 Ver.9.5 以前の sflow sampling-rate 設定は、受信(in)方向の設定として引き継がれます。	
Web コンソール	http-server wol-username コマンドが変更になりました。 http-server monitor-username コマンドに引き継がれます。	

13.18.2 コンフィグ継承の注意事項

Ver.9.6 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。

分類	設定内容	参照
IP ルートキャッシュ	エントリ数のデフォルト数が拡張されています。 Ver.9.5 以前のデフォルト値（4096）で使用する場合は、コマンドにより設定を変更してください。 (対象機種 IX2105 以外)	ip cache-size

■13.19 Ver.9.7 コンフィグ

Ver.9.7 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.19.1 自動コンフィグ継承

Ver.9.7 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
LNS の設定	tunnel mode l2tp ipsec は、 tunnel mode l2tp-lns ipsec に変更しました。	

13.19.2 コンフィグ継承の注意事項

Ver.9.7 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。

分類	設定内容	参照
BGP	connected 経路の redistribute 時の MED 値は Ver9.7 以降では 0 に変更します。 Ver9.6 以前は 1 を通知していました。	

■13.20 Ver.10.0 コンフィグ

Ver.10.0 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.20.1 自動コンフィグ継承

Ver.10.0 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.20.2 コンフィグ継承の注意事項

Ver.10.0 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。

分類	設定内容	参照
QoS	クラス名に” class-dynamic”を使用している場合は別なクラス名に変更してください。	

■13.21 Ver.10.1 コンフィグ

Ver.10.1 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.21.1 自動コンフィグ継承

Ver.10.1 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.21.2 コンフィグ継承の注意事項

Ver.10.1 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.22 Ver.10.2 コンフィグ

Ver.10.2 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.22.1 自動コンフィグ継承

Ver.10.2 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
UTM	extended-inspection traffic-anomaly block のオプション block-period がコマンドとして独立します。 extended-inspection traffic-anomaly block-period コマンドに引き継がれます。	

13.22.2 コンフィグ継承の注意事項

Ver.10.2 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。

分類	設定内容	参照
セキュリティ機能	telnet や SSH を使用してリモートコンソールから本製品にアクセスするには、ユーザ登録がされている必要があります。ユーザ登録がされていない場合、ログインすることができません。	

■13.23 Ver.10.3 コンフィグ

Ver.10.3 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.23.1 自動コンフィグ継承

Ver.10.3 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
IPv6	ipv6 reassemble-buffer コマンドが ipv6 reassembly buffers コマンドに引き継がれます。	

13.23.2 コンフィグ継承の注意事項

Ver.10.3 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.24 Ver.10.4 コンフィグ

Ver.10.4 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.24.1 自動コンフィグ継承

Ver.10.4 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.24.2 コンフィグ継承の注意事項

Ver.10.4 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.25 Ver.10.5 コンフィグ

Ver.10.5 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.25.1 自動コンフィグ継承

Ver.10.5 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.25.2 コンフィグ継承の注意事項

Ver.10.5 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.26 Ver.10.6 コンフィグ

Ver.10.6 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.26.1 自動コンフィグ継承

Ver.10.6 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
Web コンソール	web-console system information コマンドの内 o wan、 o lan 設定が system information コマンドに引き継がれます。	

13.26.2 コンフィグ継承の注意事項

Ver.10.6 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目について説明します。

分類	設定内容	参照
SSH サーバ機能	Ver.10.6 以降、暗号アルゴリズムは aes256-ctr,aes192-ctr,aes128-ctr 、 MAC アルゴリズムは hmac-sha2-512,hmac-sha2-256 が使用されます。Ver.10.5 以前で使用されていたアルゴリズムを使用する場合、ssh-server encryption compatibility コマンド、 ssh-server mac compatibility コマンドを設定してください。	

■13.27 Ver.10.7.17 コンフィグ

Ver.10.7.17 へバージョンアップを行った際に、自動的にコンフィグ変更される項目および自動的には継承されない項目および自動的には継承されない項目について説明します。

13.27.1 自動コンフィグ継承

Ver.10.7.17 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
Web コンソール	web-console system information コマンドの内 o wan、 o lan 設定が system information コマンドに引き継がれます。	

13.27.2 コンフィグ継承の注意事項

【DNS リゾルバの仕様変更】

Ver.10.7.17 から、下記の対象機能において DNS 問い合わせの際には outgoing-interface で設定されているインタフェースから取得した DNS サーバを優先に使用する機能がデフォルトで動作します。

対象機能：IKEv2/NHRP/UTM/NetMeister/Tunnel(IPoE)

動作に影響があった場合【dns transport-routing】のコンフィグを投入することにより、Ver10.6 以前の仕様に戻すことができます。

【Ver10.6 以前から 10.7.17 へのバージョンアップによる NetMeister 接続不可】

以下の条件に全て合致する場合、10.6 以前から 10.7.17 にバージョンアップした場合に NetMeister への接続が不可となります

【条件】

1.IPv6 による NetMeister 接続が設定されている。

「nm ipv6 enable」

2. NetMeister の出力先インタフェースを設定している

「nm outgoing-interface [INTERFACE] auto」

3.上記出力先インタフェースに IPv6 のアドレスがない

[a] Ver10.6 以前から Ver10.7.17 にバージョンアップする場合

【アップデート前の回避策】

バージョンアップ前に以下のいずれかを実行してください。

[a-1] IPv4 にてプロバイダ契約下回線に可能な場合は、接続されている IX の場合は、NetMeister の接続に IPv6 を使用せず、IPv4 を使用してください。

[a-2] "nm outgoing-interface"設定が無くても IPv4 にて NetMeister との接続性が確保でき、また利用している機能に影響が無い場合は、

"nm outgoing-interface"設定を削除してください。

「no nm outgoing-interface」

[a-3] Ver10.7.17 にバージョンアップ後は NetMeister からの操作ができなくなるため、NetMeister 以外の方法で復旧できるようバージョンアップ前にあらかじめ Web コンソール、ssh または telnet によるリモート接続を設定してください。
(ローカルコンソールによる接続が可能な場合は、リモート接続設定は不要です。)

バージョンアップ後は、あらかじめ設定した接続方法にて IPv4 および IPv6 それぞれに適切な送信インタフェースを設定してください。

nm outgoing-interface [インタフェース指定] [nexthop 指定] protocol ip
nm outgoing-interface [インタフェース指定] [nexthop 指定] protocol ipv6

■13.28Ver.10.7.18 コンフィグ

Ver.10.7.18 へバージョンアップを行った際に、自動的にコンフィグ変更される項目および自動的には継承されない項目および自動的には継承されない項目について説明します。

13.28.1 自動コンフィグ継承

Ver.10.7.18 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
NetMeister	nm outgoing-interface [INTERFACE] コマンド が nm outgoing-interface [INTERFACE] protocol ip に引き継がれます。	

13.28.2 コンフィグ継承の注意事項

以下の条件に全て合致する場合、10.7.17 から 10.7.18 にバージョンアップした場合に NetMeister への接続が不可となります。

※ Ver10.6 以前からのバージョンアップに影響はございません

1. IPv6 による NetMeister 接続が設定されている。
nm ipv6 enable

2. NetMeister の出力先インタフェースを設定し、プロトコル指定を行っていない。
nm outgoing-interface [インタフェース] auto

3.IPv6 デフォルトルートの送信先が、NetMeister に接続できないインタフェースが設定されている。

【アップデート前対応策】

Ver10.7.17 へのバージョンアップ後は NetMeister からの操作が不可となるために NetMeister を利用せずに復旧策の設定を実行できるよう、バージョン アップ前にあらかじめ telnet/ssh/web のリモート接続設定を有効化してください。

バージョンアップ後に、次の復旧策をリモート接続にて実行してください。
以下のように IPv4、IPv6 それぞれに適切な送信インタフェースを設定してく ださい。
nm outgoing-interface [インタフェース指定] [nexthop 指定] protocol ip
nm outgoing-interface [インタフェース指定] [nexthop 指定] protocol ipv6

※ IX へのローカルコンソールの直接接続による操作が可能な場合にはリモート接続設定は不要となります。

■13.29 Ver.10.8 コンフィグ

Ver.10.8 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.29.1 自動コンフィグ継承

Ver.10.8 へのバージョンアップ時に自動的にコンフィグが変更される項目について示します。

分類	設定内容	参照
Tunnel	tunnel mode map-e にて jpne を指定している場合は、 jpix に変更されます。	

13.29.2 コンフィグ継承の注意事項

Ver.10.8 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

■13.30 Ver.10.9 コンフィグ

Ver.10.9 へバージョンアップを行った際に、自動的にコンフィグが変更される項目および自動的には継承されない項目について説明します。

13.30.1 自動コンフィグ継承

Ver.10.9 へのバージョンアップ時に自動的にコンフィグが変更される項目はありません。

13.30.2 コンフィグ継承の注意事項

Ver.10.9 へのバージョンアップにおいてコンフィグが継承できないか、あるいは注意が必要な項目はありません。

14章 付録

■14.1 関連 RFC 一覧

- 実装 RFC／Internet Draft

実装 RFC および Internet Draft の一覧（一部参照のみ）を下表に示します。

PPPoE

RFC / Internet Draft	備考
RFC2516 A Method for Transmitting PPP Over Ethernet (PPPoE)	一部実装

PPP

RFC / Internet Draft	備考
RFC1661 The Point-to-Point Protocol (PPP)	LCP
RFC1334 PPP Authentication Protocols	
RFC1994 PPP Challenge Handshake Authentication Protocol (CHAP)	
RFC1332 The PPP Internet Protocol Control Protocol (IPCP)	
RFC1990 The PPP Multilink Protocol (MP)	
RFC2472 IP Version 6 over PPP	一部実装

RFC 1570 については、以下をサポートしておりません。

- コード（パケット種別）
  - ID 通知要求（Identification:12）
  - 残余時間通知（Time-Remaining:13）

このコードを受信した場合、コード拒否（Code-Reject:7）を送信せずパケットを廃棄します。

- LCP 設定オプション
  - 自己記述パディング（Self-Describing-Padding:10）
  - 複合フレーム（Compound-Frames:15）

このオプションを受信した場合、設定拒否（Conf-Reject:4）を送信します。

ARP

RFC / Internet Draft	備考
RFC826　An Ethernet Address Resolution Protocol	

IPv4 Specification

RFC / Internet Draft	備考
RFC791　Internet Protocol	
RFC950　IP Subnet Extension	
RFC919　IP Broadcast Datagrams	
RFC922　IP Broadcast Datagrams with Subnets	
RFC1042 Internet Protocol on IEEE 802	
RFC1812 Requirements for IP Version 4 Routers	一部未実装

ICMP

RFC / Internet Draft	備考
RFC792　Internet Control Message Protocol	
RFC950　Internet Standard Subnetting Procedure	

IGMP

RFC / Internet Draft	備考
RFC1112 Host Extensions for IP Multicasting	
RFC2236 Internet Group Management Protocol,Version2	

TCP

RFC / Internet Draft	備考
RFC793 Transmission Control Protocol	
draft-ietf-tcpm-tcpsecure-00.txt TransmissionControlProtocol security considerations	
draft-ietf-tcpm-tcpsecure-01.txt TransmissionControlProtocol security considerations	

UDP

RFC / Internet Draft	備考
RFC768 User Datagram Protocol	

RIPv1

RFC / Internet Draft	備考
RFC1058 Routing Information Protocol	特定ルートのリクエストは対応せず。

RIPv2

RFC / Internet Draft	備考
RFC2453 RIP Version 2	特定ルートのリクエストは対応せず。

OSPFv2

RFC / Internet Draft	備考
RFC2328 OSPF Version 2	
RFC3101 The OSPF Not-So-Stubby Area (NSSA) Option	

BGP4

RFC / Internet Draft	備考
RFC1771 A Border Gateway Protocol 4（BGP4）	
RFC1772 Application of the Border Gateway Protocol in the Internet	
RFC2385 Protection of BGP Sessions via the TCP MD5 Signature Option	
RFC2545 Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing	
RFC2796 BGP Route Reflection - An Alternative to Full Mesh IBGP	
RFC2918 Route Refresh Capability for BGP-4	

PIM

RFC / Internet Draft	備考
RFC2362 Protocol Independent Multicast-Sparse Mode (PIM-SM): Protocol Specification	Ver.8.4 以降
RFC4601 Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)	一部実装 Ver.8.4 以降

NAT

RFC / Internet Draft	備考
RFC1631 The IP Network Address Translator (NAT)	
RFC2663 IP Network Address Translator (NAT) Terminology and Considerations	destination address の変換には対応せず。
RFC3022 Traditional IP Network Address Translator (Traditional NAT)	

NAPT

RFC / Internet Draft	備考
RFC3022 Traditional IP Network Address Translator (Traditional NAT)	

DHCP

RFC / Internet Draft	備考
RFC2131 Dynamic Host Configuration Protocol	

DNS

RFC / Internet Draft	備考
RFC1034 DOMAIN NAMES - CONCEPTS AND FACILITIES	Proxy-DNS DNS リゾルバ
RFC1035 DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION	Proxy-DNS DNS リゾルバ

IPv6 Specification

RFC / Internet Draft	備考
RFC1924 A Compact Representation of IPv6 Addresses	
RFC1981 Path MTU Discovery for IP version 6	
RFC2080 RIPng for IPv6	
RFC2185 Routing Aspects of IPv6 Transition	
RFC4291 IP Version 6 Addressing Architecture	Ver.8.3 以降
RFC2373 IP Version 6 Addressing Architecture	
RFC3879 Deprecating Site Local Addresses	Ver.8.3 以降
RFC2374 An IPv6 Aggregatable Global Unicast Address Format	
RFC2375 IPv6 Multicast Address Assignments	
RFC2460 Internet Protocol, Version 6 (IPv6) Specification	
RFC4861 Neighbor Discovery for IP Version 6 (IPv6)	Ver.8.3 以降
RFC2461 Neighbor Discovery for IP Version 6 (IPv6)	
RFC4862 IPv6 Stateless Address Autoconfiguration	Ver.8.3 以降
RFC2462 IPv6 Stateless Address Autoconfiguration	
RFC4443 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	Ver.8.3 以降

RFC2463 Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification	
RFC2464 Transmission of IPv6 Packets over Ethernet Networks	
RFC2472 IP Version 6 over PPP	一部実装
RFC2473 Generic Packet Tunneling in IPv6 Specification	
RFC2526 Reserved IPv6 Subnet Anycast Addresses	
RFC2675 IPv6 Jumbograms	
RFC2710 Multicast Listener Discovery (MLD) for IPv6	
RFC2711 IPv6 Router Alert Option	
RFC2893 Transition Mechanisms for IPv6 Hosts and Routers	
RFC3513 Internet Protocol Version6 Addressing Architecture	
RFC3810 Multicast Listener Discovery Version 2 (MLDv2) for IPv6	
RFC5952 A Recommendation for IPv6 Address Text Representation	Ver.8.3 以降
draft-ietf-ipngwg-p2p-pingpong-00.txt Avoiding ping-pong packets on point-to-point links	
draft-savola-ipv6-rtheader-00.txt IPv6 Type 0 Routing Header Processing	

RIPng

RFC / Internet Draft	備考
RFC2080 RIPng for IPv6	

OSPFv3

RFC / Internet Draft	備考
RFC2740 OSPF for IPv6	

DHCPv6

RFC / Internet Draft	備考
RFC3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)	一部実装
RFC3633 IPv6 Prefix Options for DHCPv6 (PD)	
RFC3646 DNS Configuration Options for DHCPv6	一部実装
RFC4075 Simple Network Time Protocol (SNTP) Configuration Option for DHCPv6	

Packet Tunneling

RFC / Internet Draft	備考
RFC2003 IP Encapsulation within IP	IPv4-over-IPv4 のみ
RFC2473 Generic Packet Tunneling in IPv6 Specification	Nested Option を除く
RFC2784 Generic Routing Encapsulation (GRE)	
RFC2890 Key and Sequence Number Extensions to GRE	
RFC2893 Transition Mechanisms for IPv6 Hosts and Routers	一部のみ

EtherIP

RFC / Internet Draft	備考
RFC3378 EtherIP: Tunneling Ethernet Frames in IP Datagrams	

IPsec/IKE

RFC / Internet Draft	備考
RFC2401 Security Architecture for the Internet Protocol	Appendix B Path MTU Discovery は未実装
RFC2402 IP Authentication Header	
RFC2406 IP Encapsulating Security Payload (ESP)	
RFC2451 The ESP CBC-Mode Cipher Algorithms	
RFC2405 The ESP DES-CBC Cipher Algorithm With Explicit IV	
RFC2403 The Use of HMAC-MD5-96 within ESP and AH	
RFC2404 The Use of HMAC-SHA-1-96 within ESP and AH	
RFC2410 The NULL Encryption Algorithm and Its Use With IPsec	
RFC2407 The Internet IP Security Domain of Interpretation for ISAKMP	
RFC2408 Internet Security Association and Key Management Protocol (ISAKMP)	
RFC2409 The Internet Key Exchange (IKE)	
RFC3602 The AES-CBC Cipher Algorithm and Its Use with IPsec	鍵長 128bit 鍵長 192,256bit （Ver.8.1 以降）
RFC4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec	Ver.8.6 以降
RFC3706 A Traffic-Based Method of Detecting Dead IKE Peers	
RFC3947 Negotiation of NAT-Traversal in the IKE	一部未対応
RFC3948 UDP Encapsulation of IPsec ESP Packets	一部未対応
draft-knight-ppvpn-ipsec-dynroute-02.txt A Method to Provide Dynamic Routing in IPsec VPNs	Tunnel Mode "Tunnel Link"のみ準拠
draft-ietf-ipsec-nat-t-ike-02/03.txt	
draft-ietf-ipsec-udp-encaps-02/03.txt	

IKEv2（Ver.8.7 以降）

RFC / Internet Draft	備考
RFC5996 Internet Key Exchange Protocol Version 2 (IKEv2)	
RFC4307 Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)	
RFC4303 IP Encapsulating Security Payload (ESP)	

L2TPv2（LNS：Ver.8.10 以降、LAC：Ver.9.7 以降）

RFC / Internet Draft	備考
RFC2661 Layer Two Tunneling Protocol "L2TP"	
RFC2809 Implementation of L2TP Compulsory Tunneling via RADIUS	
RFC3193 Securing L2TP using IPsec	

Network Management

RFC / Internet Draft	備考
RFC1157 Simple Network Management Protocol (SNMP)	
RFC1212 Concise MIB Definitions	
RFC1213 Management Information Base for Network Management of TCP/IP-based internets:MIB-II	MIB-II
RFC1214 OSI Internet Management: Management Information Base	
RFC1215 A Convention for Defining Traps for use with the SNMP	
RFC1643 Definitions of Managed Objects for the Ethernet-like Interface Types	dot3
RFC2863 The InterfaceGroup MIB	ifStack（一部実装）
RFC2127 ISDN Management Information Base using SMIv2	isdnMIB（一部実装）
RFC2452 IP Version 6 Management Information Base for the Transmission Control Protocol	
RFC2454 IP Version 6 Management Information Base for the User Datagram Protocol	
RFC2465 Management Information Base for IP Version 6: Textual Conventions and General Group	ipv6MIB
RFC2466 Management Information Base for IP Version 6: ICMPv6 Group	ipv6IcmpMIB
RFC2787 Definitions of Managed Objects for the Virtual Router Redundancy Protocol	vrrpMIB（一部未実装）
RFC3019 IP Version 6 Management Information Base for The Multicast Listener Discovery Protocol	mldMIB
RFC1901 Introduction to Community-based SNMPv2	
RFC2576 Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	（一部未実装）
RFC2578 Structure of Management Information Version 2 (SMIv2)	
RFC2579 Textual Conventions for SMIv2	
RFC2580 Conformance Statements for SMIv2	
RFC3416 Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)	
RFC3417 Transport Mappings for the Simple Network Management Protocol (SNMP)	
RFC3418 Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)	
RFC4273 Definitions of Managed Objects for BGP-4	Ver.8.7 以降（bgpPeerTable の一部のみ）
RFC2096 IP Forwarding Table MIB	ipCidrRouteTable のみ Ver9.7 以降
RFC3411 An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks	Ver.10.4 以降

RFC3412 Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	Ver.10.4 以降
RFC3413 Simple Network Management Protocol (SNMP) Applications	Ver.10.4 以降
RFC3414 User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)	Ver.10.4 以降
RFC3415 View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)	Ver.10.4 以降

VRRP

RFC / Internet Draft	備考
RFC2338 Virtual Router Redundancy Protocol	
RFC5798 Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6	IPv6 のみ（Ver.8.6 以降）

CRTP

RFC / Internet Draft	備考
RFC2507 IP Header Compression	
RFC2508 Compressing IP/UDP/RTP Headers for Low-Speed Serial Links	
RFC2509 IP Header Compression over PPP	

※CRTP は接続性の問題から、一部 RFC に準拠しておりません。

telnet

RFC / Internet Draft	備考
RFC854 TELNET PROTOCOL SPECIFICATION	

SSH サーバ（Ver.8.7 以降）

RFC / Internet Draft	備考
RFC4250 The Secure Shell (SSH) Protocol Assigned Numbers	
RFC4251 The Secure Shell (SSH) Protocol Architecture	
RFC4252 The Secure Shell (SSH) Authentication Protocol	
RFC4253 The Secure Shell (SSH) Transport Layer Protocol	
RFC4254 The Secure Shell (SSH) Connection Protocol	
RFC4344 The Secure Shell (SSH) Transport Layer Encryption Modes	
RFC4419 Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol	

sntp

RFC / Internet Draft	備考
RFC2030 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	一部実装
RFC4330 Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	Ver.8.3 以降

tftp client

RFC / Internet Draft	備考
RFC1350 THE TFTP PROTOCOL (REVISION 2)	クライアントのみ

syslog

RFC / Internet Draft	備考
RFC3164 The BSD Syslog Protocol	Authentication Problem を除く

RADIUS client

RFC / Internet Draft	備考
RFC2865 Remote Authentication Dial In User Service (RADIUS)	クライアントのみ
RFC2866 RADIUS Accounting	

Multicast

RFC / Internet Draft	備考
RFC4605 Internet Group Management Protocol (IGMP)/ Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")	

HTTP（Ver.7.5 以降）

RFC / Internet Draft	備考
RFC2616 Hypertext Transfer Protocol -- HTTP/1.1	
RFC2617 HTTP Authentication: Basic and Digest Access Authentication	
RFC2045 Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies	
RFC2965 HTTP State Management Mechanism	Cookie2 は未サポート
RFC3548 The Base16, Base32, and Base64 Data Encodings	

- 参照 RFC／Internet Draft

参照 RFC および Internet Draft の一覧を下表に示します。

PPP

RFC / Internet Draft	備考
RFC1570 PPP LCP Extensions	下記参照
RFC1661 The Point-to-Point Protocol (PPP)	LCP

IPv4 Specification

RFC / Internet Draft	備考
RFC1122 Host Requirements-Communications	参照
RFC1123 Host Requirements-Applications	参照

NAT

RFC / Internet Draft	備考
RFC2993 Architectural Implications of NAT	参照

IPv6 Specification

RFC / Internet Draft	備考
RFC1809 Using the Flow Label Field in IPv6	参照
RFC1881 IPv6 Address Allocation Management	参照
RFC1887 An Architecture for IPv6 Unicast Address Allocation	参照
RFC2292 Advanced Sockets API for IPv6	参照
RFC2450 Proposed TLA and NLA Assignment Rule	参照
RFC2471 IPv6 Testing Address Allocation	参照
RFC2553 Basic Socket Interface Extensions for IPv6	参照
RFC2928 Initial IPv6 Sub-TLA ID Assignments	参照
RFC2991 Multipath Issues in Unicast and Multicast Next-Hop Selection	参照
RFC3056 Connection of IPv6 Domains via IPv4 Clouds	参照
draft-ietf-ipngwg-scoping-arch-02.txt IP Version 6 Scoped Address Architecture	参照
draft-ietf-ipngwg-default-addr-select-05.txt Default Address Selection for IPv6	参照

DHCPv6

RFC / Internet Draft	備考
draft-ietf-dhc-dhcpv6-interop-01.txt Results from Interoperability Tests of DHCPv6 Implementations	参照

IPsec/IKE

RFC / Internet Draft	備考
RFC2412 The OAKLEY Key Determination Protocol	参照
RFC2709 Security Model with Tunnel-mode IPsec for NAT Domains	参照
draft-ietf-ipsec-flow-monitoring-mib-01.txt IPsec Flow Monitoring MIB	参照

IGMP/MLD Proxying

RFC / Internet Draft	備考
draft-ietf-idmr-igmp-proxy-01.txt IGMP-based Multicast Forwarding ('IGMP Proxying')	参照

sntp

RFC / Internet Draft	備考
RFC1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis	参照

RADIUS client

RFC / Internet Draft	備考
RFC3162 RADIUS and IPv6	参照

SIP-NAT

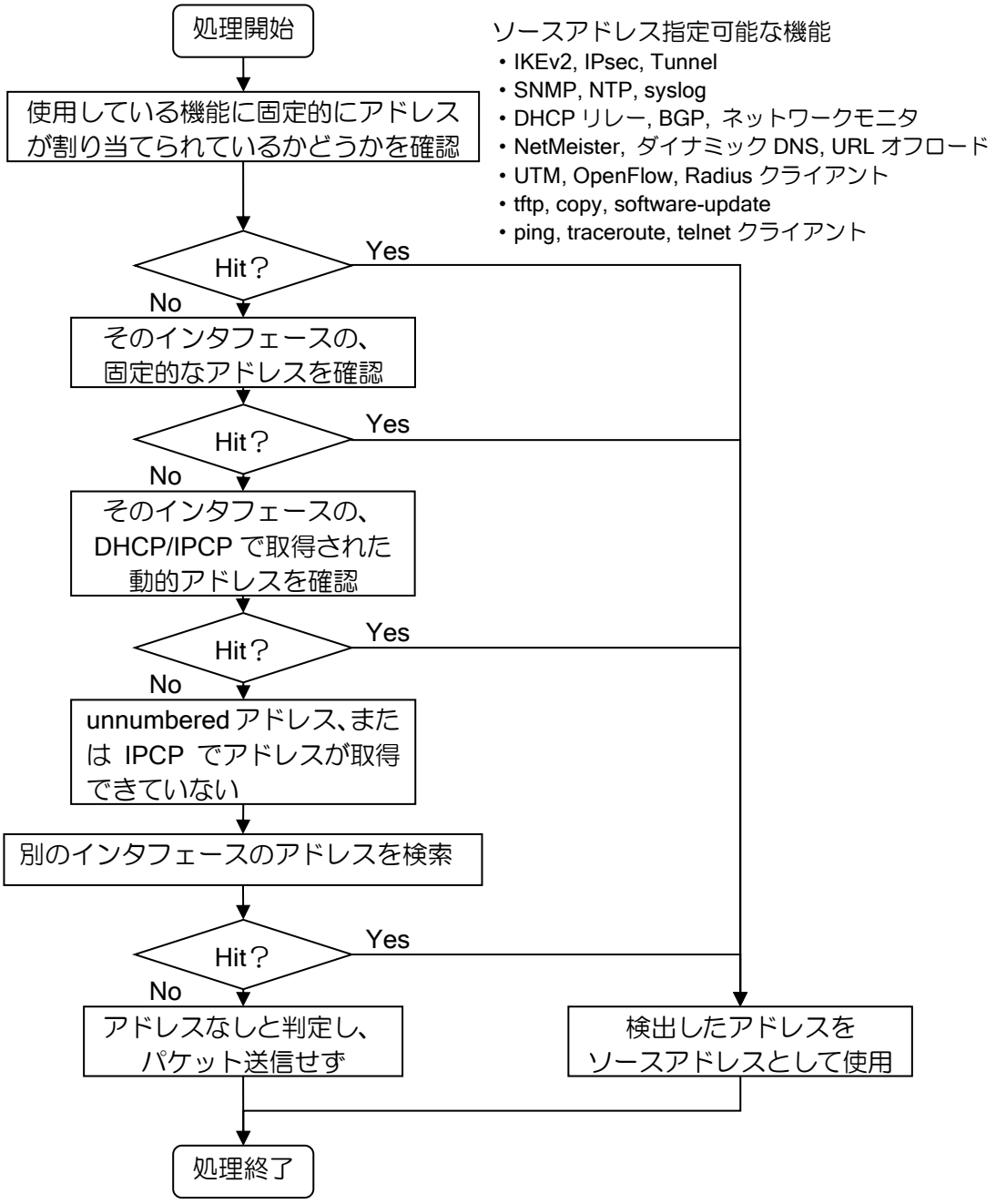
RFC / Internet Draft	備考
RFC3261 SIP: Session Initiation Protocol	参照
RFC2327 SDP: Session Description Protocol	参照
RFC2046 Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types	参照
RFC3264 An Offer/Answer Model with the Session Description Protocol (SDP)	参照
RFC3265 Session Initiation Protocol (SIP)-Specific Event Notification	参照
RFC3515 The Session Initiation Protocol (SIP) Refer Method	参照

■14.2 ソースアドレスセレクション

IX2000/IX3000 シリーズからパケットを送信する場合の、ソース（送信元）アドレスをどのように決定するか、ソースアドレスセレクションの一連の動作について説明します。

(a) IPv4 ソースアドレスセレクション

IPv4 ソースアドレスセレクションの一連の動作について説明します。



詳細な判定順序は以下のようになります。
セカンダリアドレスもソースアドレスセレクションの対象になります。

- 動的アドレス（IPCP または DHCP）の場合
  または
- unnumbered でソースアドレスインタフェースが指定されていない場合

  1. 送信インタフェースのプライマリアドレス
  2. 送信インタフェースのセカンダリアドレス
  3. 16 進表記したときに最も大きい有効（ホスト受信可能）アドレス

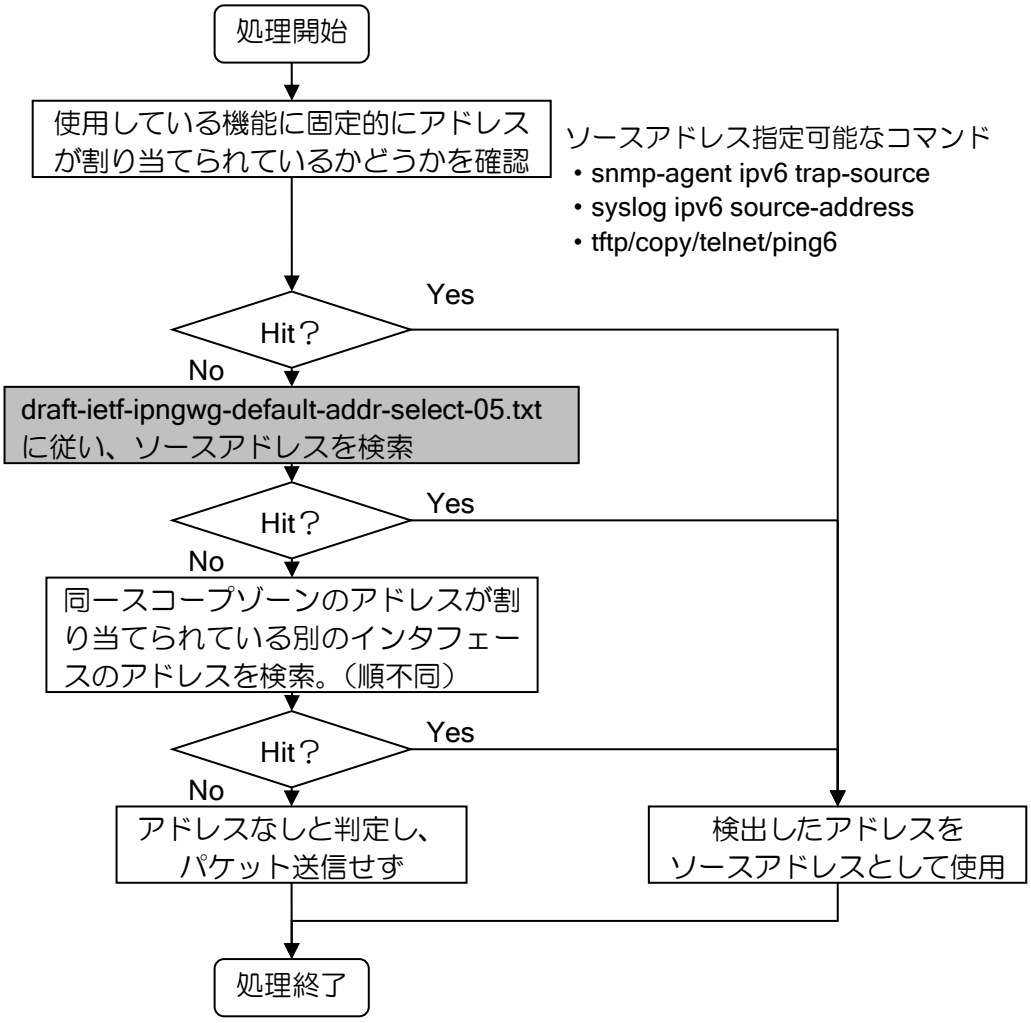
- unnumbered でソースアドレスインタフェースが指定されている場合

  1. 送信インタフェースのプライマリアドレス
  2. 指定したインタフェースのプライマリアドレス
  3. 送信インタフェースのセカンダリアドレス
  4. 16 進表記したときに最も大きい有効（ホスト受信可能）アドレス

  ※インタフェース指定したインタフェースのセカンダリアドレスは優先されません。
  ※NAPT アドレスの場合には、指定インタフェースの検索のみ行います。

(b) IPv6 ソースアドレスセレクション

IPv6 ソースアドレスセレクションの一連の動作について説明します。

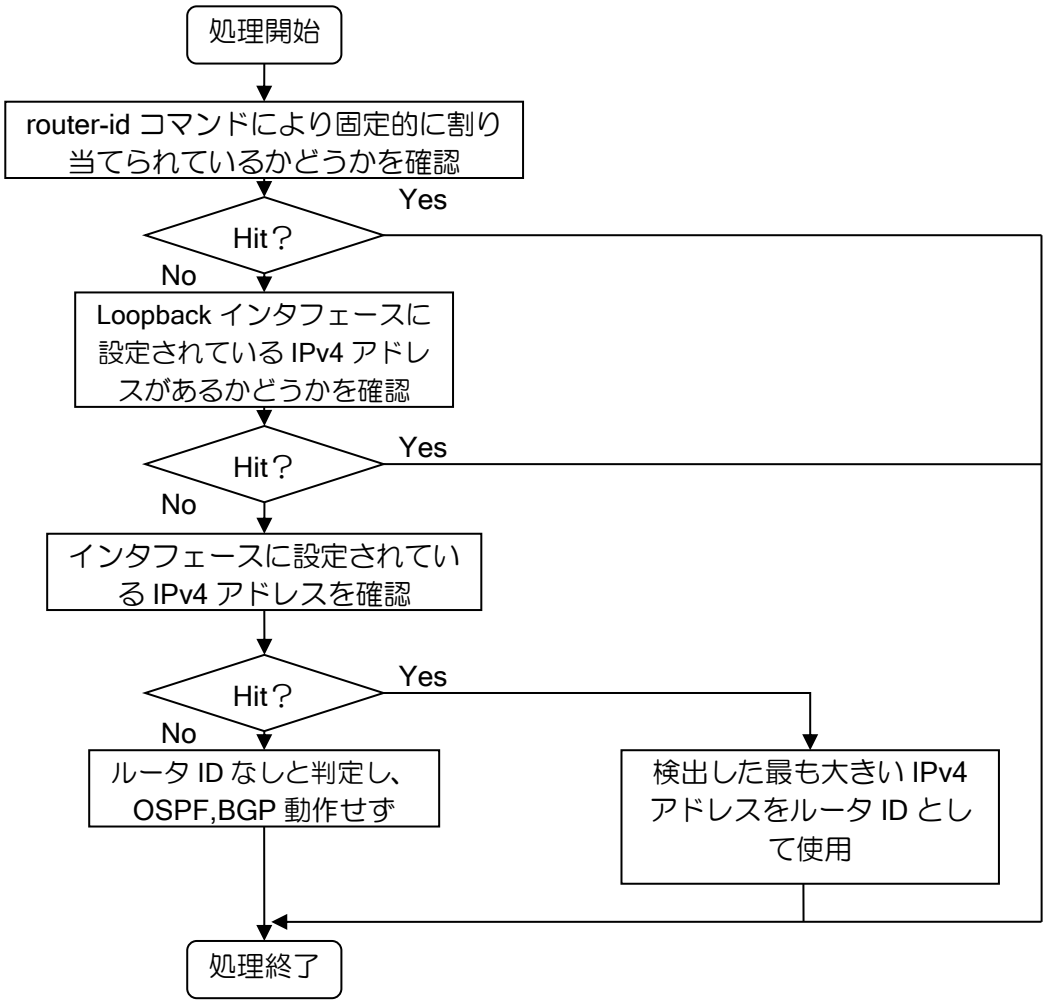


■14.3 ルータ ID セレクション

OSPF，BGP4 で使用するルータ ID をどのように決定するか、ルータ ID セレクションの一連の動作について説明します。

(a) OSPFv2,BGP4

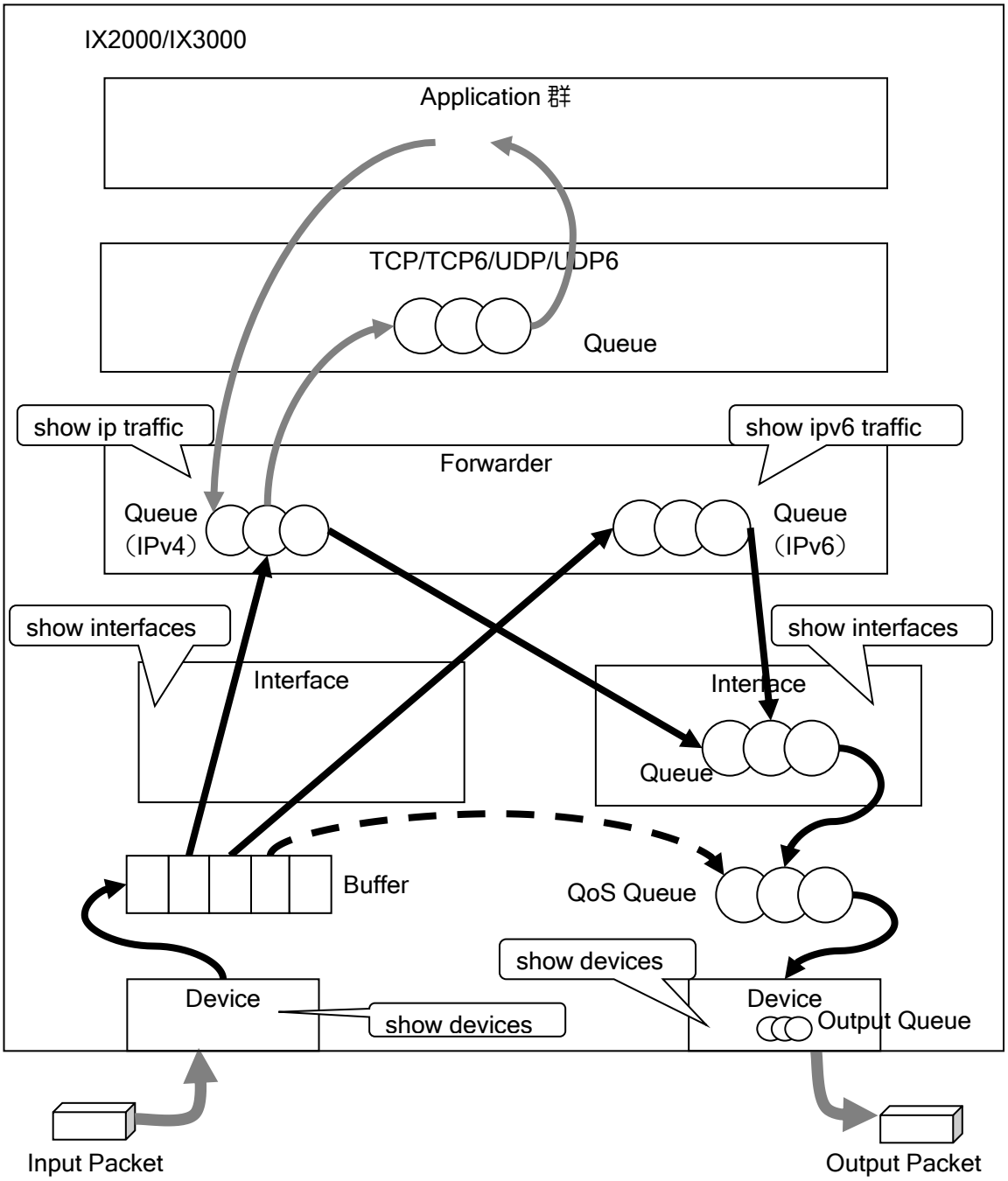
OSPFv2,BGP4 ルータ ID セレクションの一連の動作について説明します。



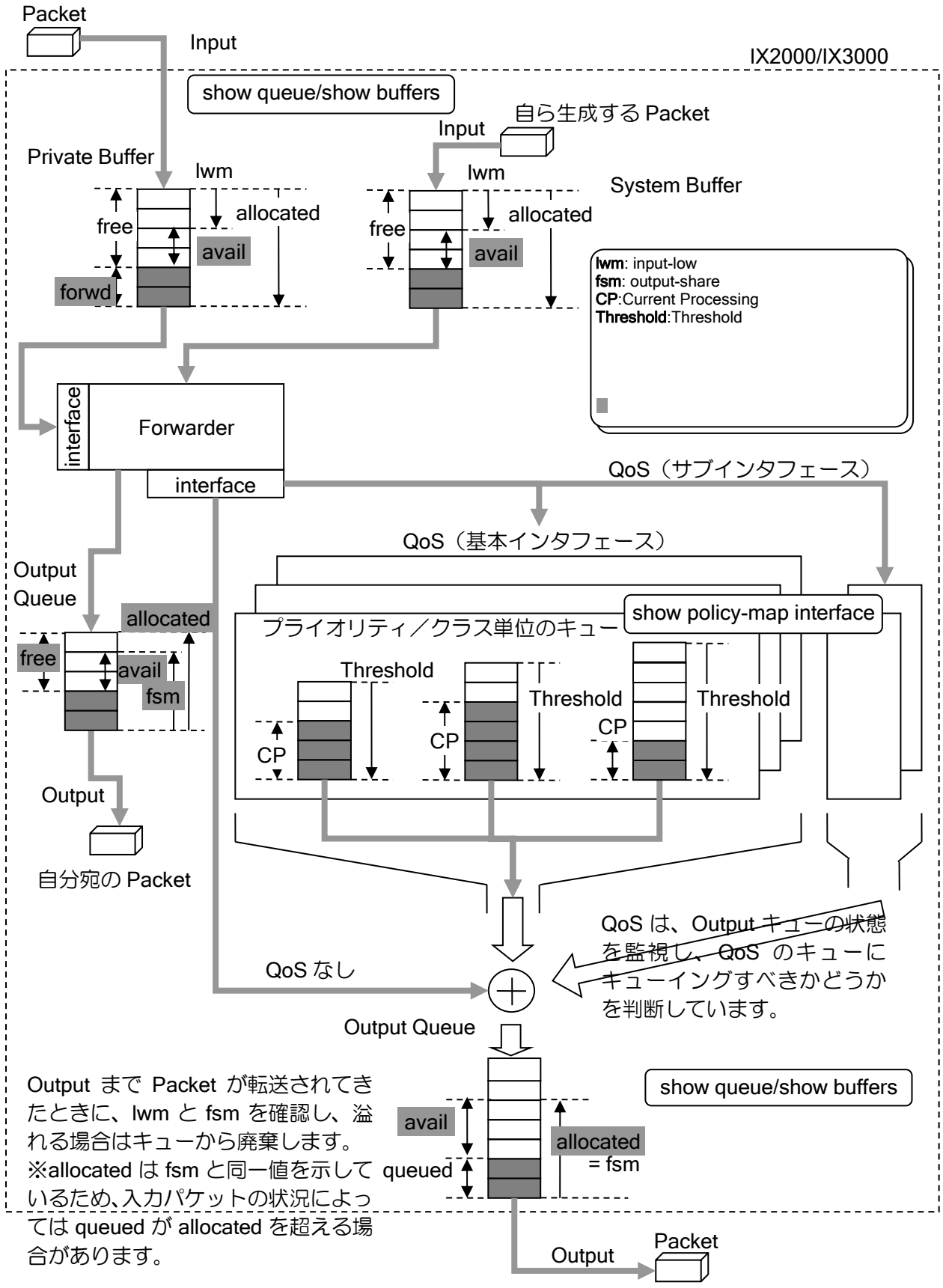
■14.4 キューイング処理

IX2000/IX3000 シリーズでのパケットフォワーディング処理の、キューイングメカニズムについて説明します。下記は、キューがどこに存在するかを示しています。キューが存在する部分では、転送処理に時間がかかります。

また IX2000/IX3000 では、濃い矢印にて記述している部分について、優先的に処理を実行する仕組みを取り入れております。さらに、一旦パケット転送のパスができあがると、点線に示すような最短処理（Fast-Path）が構成され、そのパスを通るようになります。



QoS キューとデバイス単位に所持しているキューの関連を以下に示します。



■14.5 インタフェースの特性

IX2000/IX3000 シリーズのインタフェースには、ベース（主）のインタフェースと、サブ（副）のインタフェースが存在します。ベースインタフェースは、インタフェース識別子がドットゼロ（.0）で示されるインタフェースで、サブインタフェースは、ドットゼロ以外で示されるインタフェースです。

各サブインタフェースでは、それぞれ PPP などの encapsulation の設定を行うことができます。設定に応じて特性が異なりますので、IPv4、IPv6 それぞれについて、以下に説明します。

(a) 論理インタフェース一覧

ベースインタフェースとサブインタフェースの特性を以下に説明します。

インタフェース種類	種別	デバイス	用途
Ethernet	ベース	あり	データ送受信
Ethernet	サブ	あり	データ送受信（カプセル化対応）
FastEthernet	ベース	あり	データ送受信
FastEthernet	サブ	あり	データ送受信（カプセル化対応）
GigaEthernet	ベース	あり	データ送受信
GigaEthernet	サブ	あり	データ送受信（カプセル化対応）
Serial	ベース	あり	データ送受信（カプセル化対応）
Serial	サブ	あり	データ送受信（カプセル化対応）
BRI	ベース	あり	データ送受信（カプセル化対応）
Dialer	ベース	なし	データ送受信（カプセル化対応）
USB-Serial （Ver.8.8 以降）	ベース	あり	データ送受信（カプセル化対応）
BVI	ベース	なし	データ送受信
Tunnel	ベース	なし	カプセル化
Loopback	ベース	なし	IPv6 ルーティング ホスト受信他 （shutdown 不可）
Null	ベース	なし	不要パケット対処用 （shutdown 不可）

(b) 論理インタフェース特性（IPv4 関連）

○：コマンド投入可および動作可
×：コマンド投入不可または動作不可

interface	encapsulation	IPv4	ICMP	ARP	NAT	DHCP	RIP	OSPF
Ethernet	-	○	○	○	○	○	○	○
	PPP	○	○	×	○	×	○	○
	VLAN-tagging	○	○	○	○	○	○	○
Serial	PPP	○	○	×	○	×	○	○
BRI	-	○	○	×	○	×	○	○
Dialer	-	○	○	×	○	×	○	○
USB-Serial	-	○	○	×	○	×	○	○
BVI	-	○	○	○	○	○	○	○
	VLAN-tagging	○	○	○	○	○	○	○
Tunnel	-	○	○	×	○	×	○	○
Loopback	-	○	○	×	×	×	○	○
Null	-	○	○	×	×	×	×	×

BVI の VLAN-tagging は Ver9.3 以降可能です。

interface	encapsulation	Filter	VRRP	IPsec	QoS	CRTP	CTCP	Policy Routing
Ethernet	-	○	○	○	○	×	×	○
	PPP	○	×	○	○	×	×	○
	VLAN-tagging	○	○	○	○	×	×	○
Serial	PPP	○	×	○	○	○	○	○
BRI	-	○	×	○	○	○	○	○
Dialer	-	○	×	○	○	○	○	○
USB-Serial	-	○	×	○	○	○	○	○
BVI	-	○	○※2	○	○※1	×	×	○
	VLAN-tagging	○	○	○	○※1	×	×	○
Tunnel	-	○	×	○	○※1	×	×	○
Loopback	-	×	×	×	×	×	×	×
Null	-	×	×	×	×	×	×	×

BVI の VLAN-tagging は Ver9.3 以降可能です。
※1 は、マーキングのみ可能です。
※2 は、Ver.8.8 以降可能です。

(c) 論理インタフェース特性（IPv6 関連）

○：コマンド投入可および動作可
×：コマンド投入不可または動作不可

interface	encapsulation	IPv6	ICMP v6	ND	MLD	RIPng	PD※3
Ethernet	-	○	○	○	○	○	○※4
	PPP	○	○	○	○	○	○
	VLAN-tagging	○	○	○	○	○	○※4
Serial	PPP	○	○	○	○	○	○
BRI	-	○	○	○	○	○	○
Dialer	-	○	○	○	○	○	○
USB-Serial	-	×	×	×	×	×	×
BVI	-	○	○	○	○	○	○
	VLAN-tagging	○	○	○	○	○	○
Tunnel	-	○	○	○	○	○	○※4
Loopback	-	○	○	×	×	○	×
Null	-	○	○	×	×	○	×

※3 PD はリクエスタの仕様です。アドレスは全インタフェースに割り当てられます。
※4 動作はしますが、サポート対象にはなりません。

interface	encapsulation	Filter	IPsec	QoS	CRTP	CTCP	Policy Routing
Ethernet	-	○	○	○	×	×	○
	PPP	○	○	○	×	×	○
	VLAN-tagging	○	○	○	×	×	○
Serial	PPP	○	○	○	×	×	○
BRI	-	○	○	○	×	×	○
Dialer	-	○	○	○	×	×	○
USB-Serial	-	×	×	×	×	×	×
BVI	-	○	○	○	×	×	○
	VLAN-tagging	○	○	○	×	×	○
Tunnel	-	○	○	○	×	×	○
Loopback	-	×	×	×	×	×	×
Null	-	×	×	×	×	×	×

■14.6 インタフェースの MTU 値

IX2000/IX3000 シリーズの、各インタフェースにおける MTU の最大値は次の通りです。

インタフェース	MTU 最大値
Ethernet	1500
VLAN	1500
PPPoE	1492

✧ 各種仮想トンネルインタフェースの MTU サイズの最大値は Lower インタフェースの MTU サイズからカプセル化するヘッダサイズを引いたサイズに自動的に調整されます。

■14.7 TCP-MSS 調整値

TCP-MSS 調整の設定値は出力インタフェースの MTU や暗号化の種別によって異なります。自動調整を行わない場合の設定値は、以下を参考にしてください。

(a) IPv4

カプセル化方式	出力 I/F の MTU 長	Tunnel I/F の MTU 長	Tunnel I/F の MSS 値
IPv4	1500	-	1460
	1492	-	1452
	1454	-	1414
IPsec（transport） + ESP-3DES/DES + ESP-SHA1/MD5	1500	-	1426
	1492	-	1418
	1454	-	1378
IPsec（transport） + ESP-AES + ESP-SHA1/MD5	1500	-	1418
	1492	-	1410
	1454	-	1350
IPsec（tunnel） + ESP-3DES/DES + ESP-SHA1/MD5	1500	1446	1406
	1492	1438	1398
	1454	1398	1358
IPsec（tunnel） + ESP-AES + ESP-SHA1/MD5	1500	1438	1398
	1492	1430	1390
	1454	1390	1350

(b) IPv6

カプセル化方式	出力 I/F の MTU 長	Tunnel I/F の MTU 長	Tunnel I/F の MSS 値
IPv6	1500	-	1440
	1492	-	1432
	1454	-	1394
IPsec（transport） + ESP-3DES/DES + ESP-SHA1/MD5	1500	-	1410
	1492	-	1402
	1454	-	1362
IPsec（transport） + ESP-AES + ESP-SHA1/MD5	1500	-	1402
	1492	-	1394
	1454	-	1354
IPsec（tunnel） + ESP-3DES/DES + ESP-SHA1/MD5	1500	1430	1370
	1492	1422	1362
	1454	1382	1322
IPsec（tunnel） + ESP-AES + ESP-SHA1/MD5	1500	1422	1362
	1492	1406	1346
	1454	1374	1314

(c) EtherIP

カプセル化方式	出力 I/F の MTU 長	Tunnel I/F の MTU 長	Tunnel I/F の MSS 値
EtherIP（IPv4）	1500	1464	1424
	1492	1456	1416
	1454	1418	1378
EtherIP（IPv4） + ESP-3DES/DES + ESP-SHA1/MD5	1500	1430	1390
	1492	1422	1382
	1454	1382	1342
EtherIP（IPv4） + ESP-AES + ESP-SHA1/MD5	1500	1422	1382
	1492	1406	1366
	1454	1374	1334
EtherIP（IPv6）	1500	1444	1384
	1492	1436	1376
	1454	1398	1338
EtherIP（IPv6） + ESP-3DES/DES + ESP-SHA1/MD5	1500	1414	1354
	1492	1406	1346
	1454	1366	1306
EtherIP（IPv6） + ESP-AES + ESP-SHA1/MD5	1500	1406	1346
	1492	1390	1330
	1454	1358	1298

※ EtherIP なしの場合と比較して、EtherIP ヘッダ（2） + MAC ヘッダ（通常 14）の分だけ MSS は小さくなります。ただし MAC ヘッダがタグ等の機能により長くなる場合は、さらに小さくする必要がありますので、適宜設定を変更してください。

(d) Ether over GRE

カプセル化方式	出力 I/F の MTU 長	Tunnel I/F の MTU 長	Tunnel I/F の MSS 値
Ether over GRE （IPv4）	1500	1450	1410
	1492	1442	1402
	1454	1402	1364
Ether over GRE + ESP-3DES/DES + ESP-SHA1/MD5	1500	1416	1376
	1492	1408	1368
	1454	1368	1328
Ether over GRE + ESP-AES + ESP-SHA1/MD5	1500	1408	1368
	1492	1392	1352
	1454	1360	1320

※上記の値は GRE のオプションを全て有効化したときの値です。

■14.8 ソフトウェア起動プロセス

ルータ起動時の初期化処理と、外部出力の関係です。次のように初期化処理が順番に行われます。

事象	外部出力
電源投入	LED 点灯
Power On Self Test	診断メッセージ表示
Boot 起動開始	なし
Boot 初期化完了	コピーライト表示
ローダ起動	Loading …表示
Gateway 起動開始	Starting at <address>表示
Gateway 初期化完了	コピーライト表示
Subsystem 起動開始	特になし

■14.9 マルチパス

イコールコストマルチパスの動作は、IPv4,IPv6 の章をそれぞれ参照してください。ただし、バージョンごとに対応状況やデフォルト動作が異なりますので、詳細について説明します。

(a) IPv4、IPv6 のマルチパス仕様

IX2000/IX3000 では、Per-Session には対応しておりません。その他の項目については設定で選択可能です。

マルチパス数は、IPv4 で 4、IPv6 で 16 になります。これらの値は変更できません。

	Best-Path	Per-Packet	Per-Flow	Per-Session
IPv4	○	◎	○	×
IPv6	○	◎	○	×

◎：デフォルト設定　○：設定可能　×：設定不可能

※IPv6 ではサイト境界となった場合には複数のパスのうちサイト境界をまたがないパスが選択されます。

(b) 各ルーティングプロトコルのベストパス選択

(1) IPv4 スタティックルート

ユーザ設定によりマルチパス可能です。

```
【設定例】

ip route default FastEthernet0/0.1 metric 10
ip route default Tunnel0.0 metric 10
```

(2) IPv6 スタティックルート

ユーザ設定によりマルチパス可能です。

(3) RIP/RIPng

プロトコルはマルチパスに未対応です。最初に学習したパスをベストパスと判断します。

(4) OSPFv2/OSPFv3

コスト計算の結果、宛先へのコストが同じだった場合に、イコールコストマルチパスとして動作します。

(5) BGP

Ver.10.0 以降、コマンドによりマルチパスに対応しています。マルチパスの条件については、ルータ設定の BGP の項を参照してください。

デフォルトでは、最適経路決定手順によりベストパスを選択します。

■14.10　FIB と RIB

ルータの経路情報を格納するテーブルとして FIB（Forwarding Information Base）と RIB（Routing Information Base）が存在します。以下にこれらの情報の役割を説明します。

なお、バージョンごとに対応状況が異なりますので、加えて説明します。

(a) FIB（Forwarding Information Base）

IPv4/IPv6 パケットを転送するために必要な情報を含むテーブルを FIB と呼んでいます。これは各々の到達可能な宛先ネットワークプレフィクスに対して、インタフェース識別子とネクストホップ情報を含みます。

FIB は、フォワーディングエンジンが使用するテーブルであり、ルータはそのテーブルにしたがってパケットを転送します。（RFC1812 に概要が記載されています。）

(b) RIB（Routing Information Base）

RIB は、ルーティングプロトコルで得た経路情報だけを格納するテーブルです。RIB の内容は、最終的に FIB に適用され、パケット転送する際に使用されます。

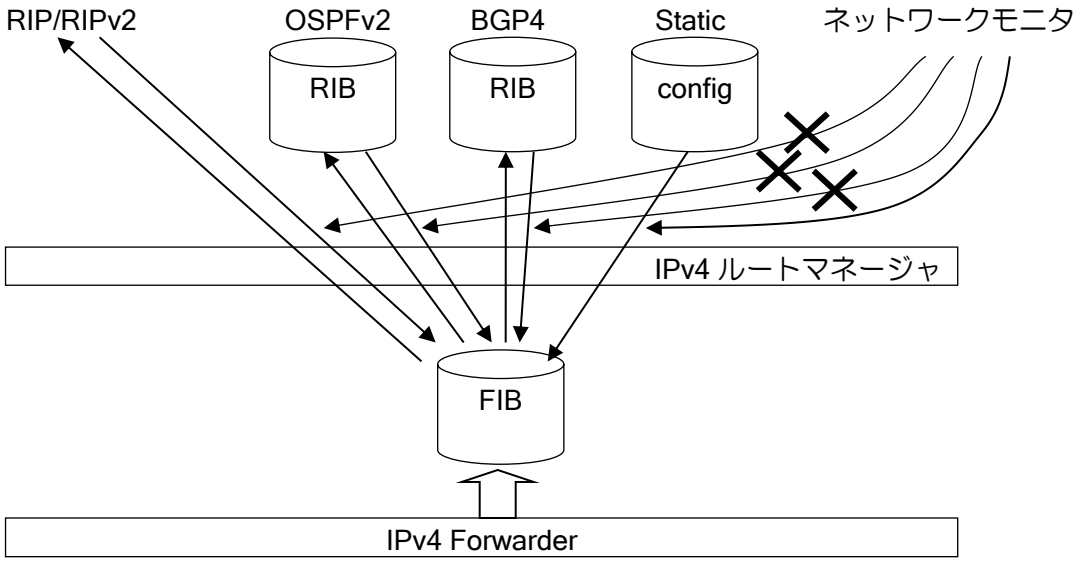
(c) ルートマネージャ

ルートマネージャは、RIB と FIB 間の経路情報の管理を行います。

(d) IPv4 経路情報

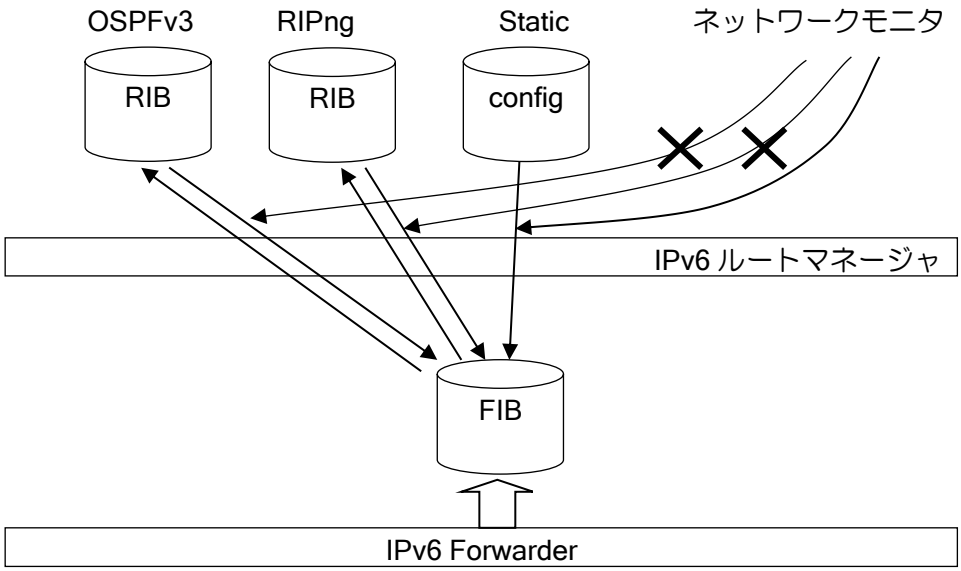
IX2000/IX3000 の IPv4 経路情報の関係は以下のようになっています。

ネットワークモニタのルート監視は、ダイナミックルーティングプロトコルと関連付けされた動作はおこないませんので、ダイナミックルーティングプロトコルと同時に使用する場合は、FIB に予期せぬ情報が書き込まれる場合があります。



(e) IPv6 経路情報

IX2000/IX3000 の IPv6 経路情報の関係は以下のようになっています。



(f) 経路再配信

直接接続しているネットワークや、スタティックルート、ダイナミックルートなど、他の RIB の経路情報を RIP や OSPF に再配信することも可能です。それぞれのルーティングプロトコルの設定で redistribute コマンドを使用します。設定の詳細は、それぞれのルーティングプロトコルの項を参照してください。

■14.11 デフォルト開設ポート番号

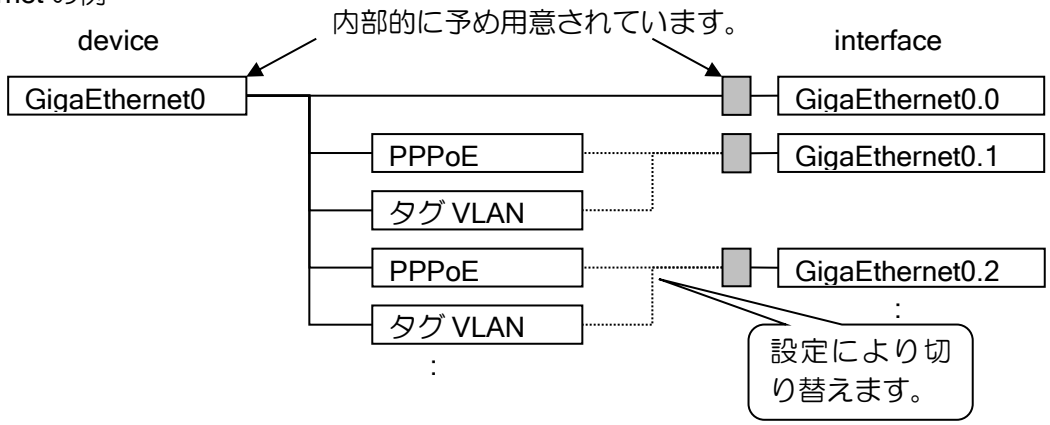
IX2000/IX3000 シリーズソフトウェアでは、デフォルト開設ポート番号はありません。

■14.12 インタフェース内部構成

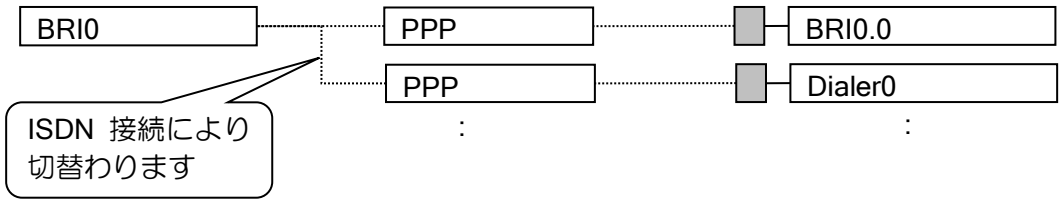
IX2000/IX3000 シリーズでは、内部的に予め L2 構造体が用意されており、この L2 構造体をインタフェースとして外部に見せるかどうかで、あたかも新たに L2 構造体が生成されたかのように動作しています。

あらかじめ用意されている L2 構造体を encapsulation コマンドでインタフェースに関連付け、あるいは新たに interface コマンドを使用して表示するなどによって、そのインタフェースが利用できるようになります。

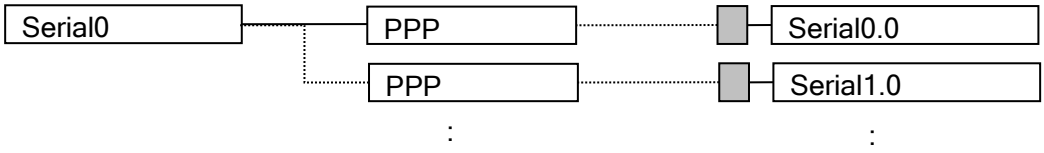
Ethernet の例



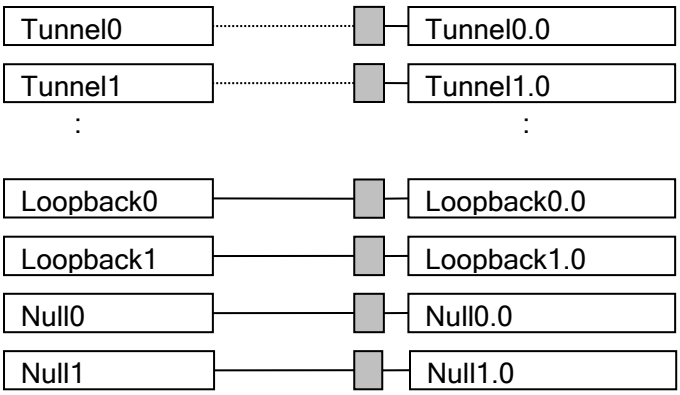
BRI の例



Serial の例



ソフトウェア I/F の例



以下に、内部インタフェース割当を示します。（ポート VLAN は SW-HUB のみ使用可能です）

IX3315 / IX3110 / IX3015

インタフェース	IX3315	IX3110	IX3015	備考
GigaEthernet	*.0	*.0	-	Ethernet （Ver.7.3 以降）
	:1.0～:8.0	-	-	Ethernet （ポート VLAN）
GigaEthernet	*.1～*.1000	*.1 ～*.32	-	PPPoE/タグ VLAN
	:.1～*:*.8	-	-	PPPoE/タグ VLAN （ポート VLAN）
FastEthernet	-	-	0/0.0 0/1.0	Ethernet
	-	-	1/0.0	Ethernet （拡張カード）
	-	-	1/0:1.0～1/0:4.0	Ethernet （ポート VLAN）
FastEthernet	-	-	0/*.1～0/*.32	PPPoE/タグ VLAN
	-	-	1/0.1～1/0.32	PPPoE/タグ VLAN （拡張カード）
	-	-	1/0:*.1～1/0:*.8	PPPoE/タグ VLAN （ポート VLAN）
Serial	-	-	*/0:1.0 ～*/0:23.0	PPP
BRI	-	-	*/0.0～*/3.0	PPP
Dialer	-	-	0～511	PPP（Ver5.0 以降）
BVI	0～63	0～7 0～63(Ver.8.11～)	0～7 0～63(Ver.8.11～)	Software （Ver.6.2 以降）
Tunnel	0.0～4999.0	0.0～1023.0	0.0～511.0	Software
Loopback	0.0～1.0	0.0～1.0	0.0～1.0	Software
	0.0～64.0 （Ver9.5～）	-	0.0～64.0 （Ver9.5～）	Software （拡張設定）
Null	0.0～1.0	0.0～1.0	0.0～1.0	Software
	0.0～64.0 （Ver9.5～）	0.0～64.0 （Ver9.5～）	0.0～64.0 （Ver9.5～）	Software （拡張設定）

IX2105 / IX2106 /IX2107/ IX2215 / IX2207 / IX2235

インタフェース	IX2105 IX2106 IX2107	IX2215	IX2207	備考
GigaEthernet	0.0	0.0 1.0	0.0 1.0	Ethernet
	1:1.0～1:4.0	2:1.0～2:8.0	2:1.0～2:4.0	Ethernet （ポート VLAN）
GigaEthernet	0.1～0.32	0.1～0.32 1.1～1.32	0.1～0.32 1.1～1.32	PPPoE/タグ VLAN
	1.1～1.32	2.1～2.32	2.1～2.32	PPPoE/タグ VLAN （SW-HUB）
	1:*.1～1:*.8	2:*.1～2:*.8	2:*.1～2:*.8	PPPoE/タグ VLAN （ポート VLAN）
BRI	-	0.0	-	PPP
Dialer	-	0～95	-	PPP
USB-Serial	-	0.0	0.0 1.0	PPP
BVI	0～7	0～7	0～7	Software
Tunnel	0.0～127.0	0.0～127.0	0.0～127.0	Software
Loopback	0.0～1.0	0.0～1.0	0.0～1.0	Software
	0.0～64.0 （Ver9.5～）	0.0～64.0 （Ver9.5～）	0.0～64.0 （Ver9.5～）	Software（拡張設定）
Null	0.0～1.0	0.0～1.0	0.0～1.0	Software
	0.0～64.0 （Ver9.5～）	0.0～64.0 （Ver9.5～）	0.0～64.0 （Ver9.5～）	Software（拡張設定）

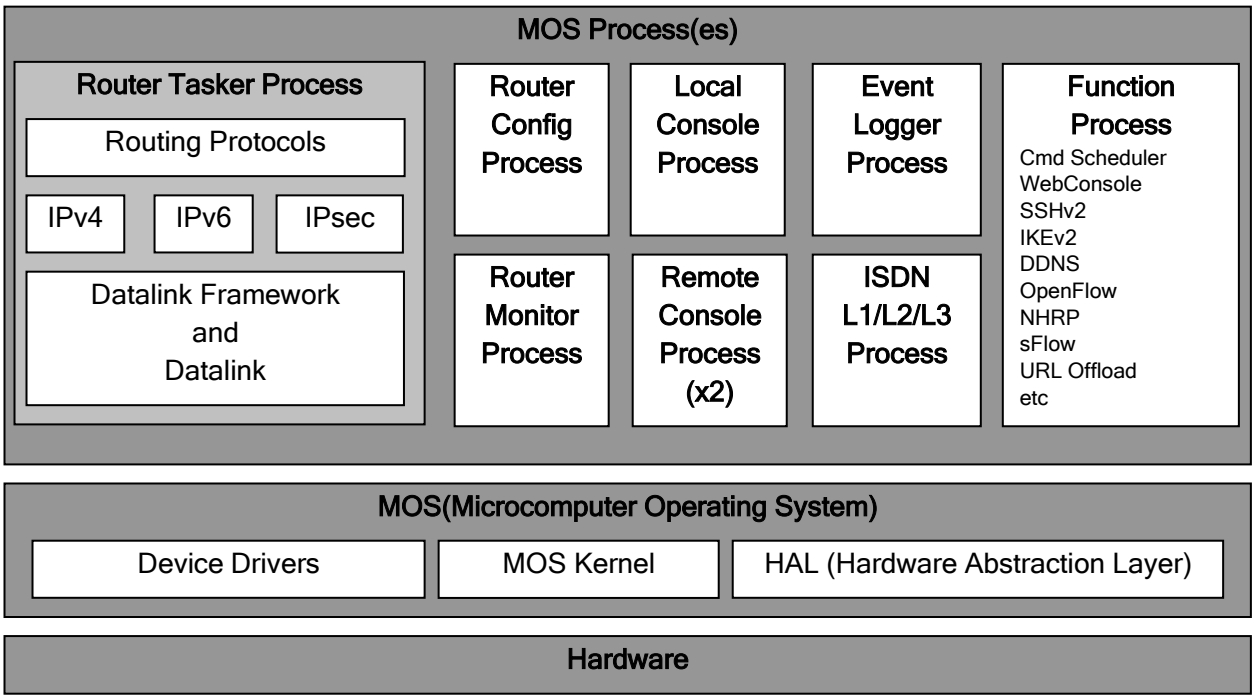
IX2235/IX2310

インタフェース	IX2235	IX2310	備考
GigaEthernet	0.0 1.0	0.0～3.0	Ethernet
	2:1.0～2:8.0	-	Ethernet（ポート VLAN）
GigaEthernet	0.1～0.32 1.1～1.32	0.1～0.32 1.1～1.32 2.1～2.32 3.1～3.32	PPPoE/タグ VLAN
	2.1～2.32	-	PPPoE/タグ VLAN （SW-HUB）
	2.*.1～2.*.8	-	PPPoE/タグ VLAN （ポート VLAN）
BRI	-	-	PPP
Dialer	-	-	PPP
USB-Serial	0.0	0.0	PPP
BVI	0～31	0～31	Software
Tunnel	0.0～127.0	0.0～255.0	Software
Loopback	0.0～1.0	0.0～1.0	Software
	0.0～64.0	0.0～64.0	Software（拡張設定）
Null	0.0～1.0	0.0～1.0	Software
	0.0～64.0	0.0～64.0	Software（拡張設定）

■14.13 ソフトウェア構造

IX2000/IX3000 シリーズのソフトウェア構造を説明します。ソフトウェア構造は、おおよそ下記の構成になっております。IX2000/IX3000 シリーズのソフトウェアは、MOS と呼ぶオペレーティングシステムと MOS 上で動作するいくつかのプロセスから構成されています。

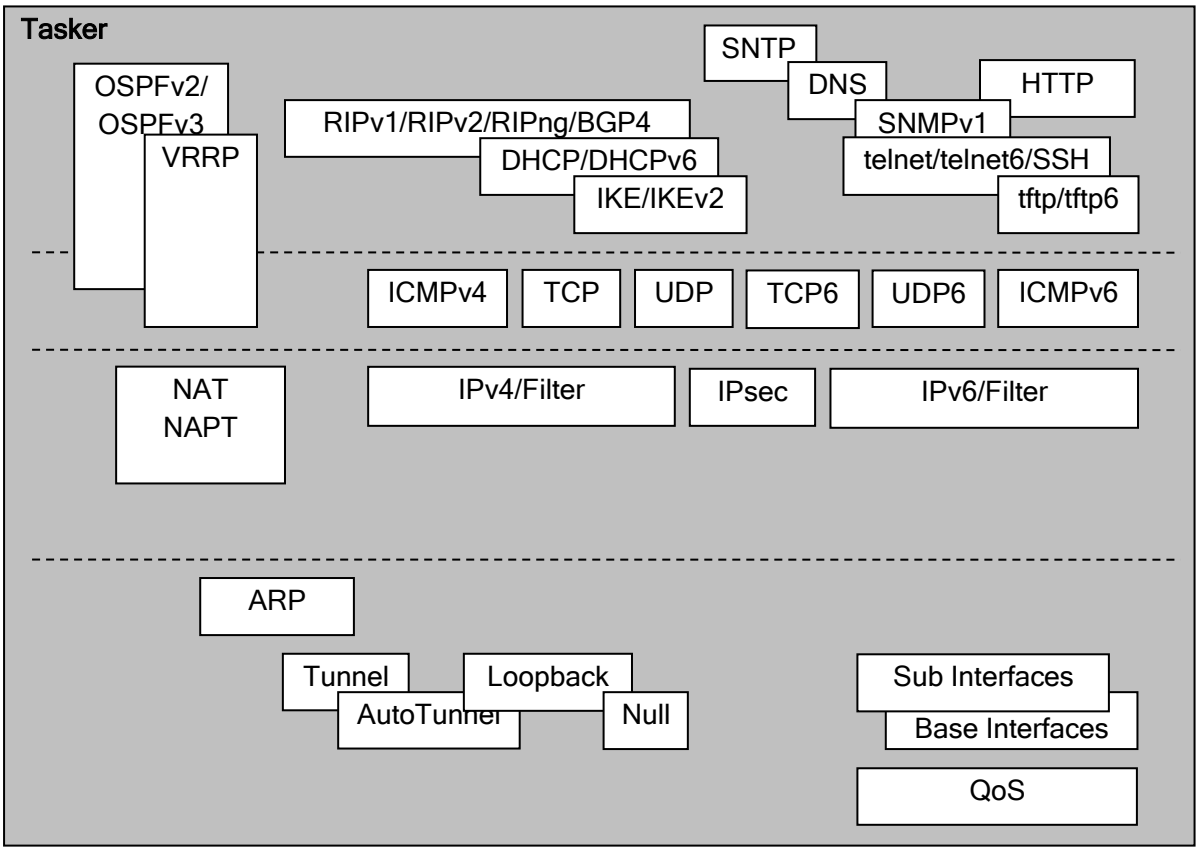
MOS はシンプルなオペレーティングシステムです。MOS は、ノンプリエンプティブスケジューラおよびリソース（ヒープメモリ、タイマ他）マネージャを実装する MOS カーネル、各種デバイスを制御するデバイスドライバ群、およびハードウェアを抽象化しソフトウェアの移植性を高める HAL から構成されています。



(a) プロセス構造

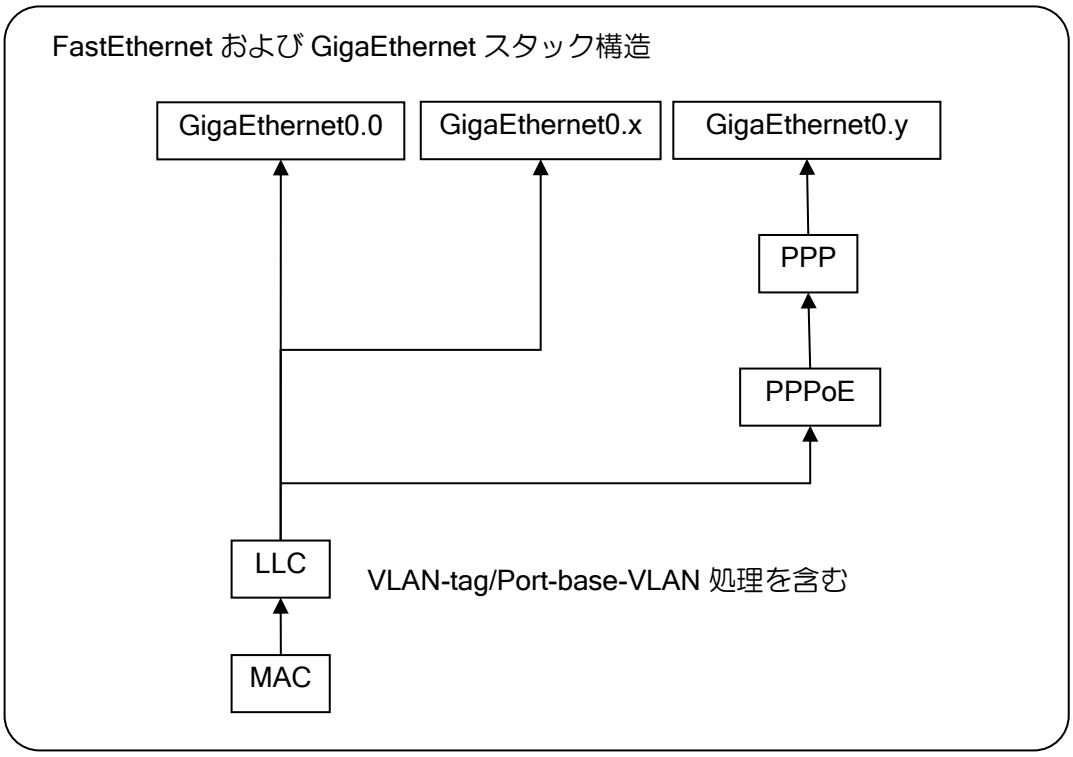
- Router Tasker Process
  - 主にルータ機能全般を実現するプロセスです。ルータタスカプロセスは、リンクレイヤ機能からルーティングプロトコルまで、ほぼ全てのルータ機能を実装しています。また、複数の機能を高速に動作させるために、特殊なサブスケジューラを実装しています。このため、ルータタスカプロセスは他の MOS プロセスより優先してスケジューリングされます。
- Router Config Process
  - 主にコマンドおよび設定データ保存関連を実現するプロセスです。
- Local Console Process
  - コンソールを司るプロセスです。
- Remote Console Process
  - telnet サーバを実現するプロセスです。
- Router Monitor Process
  - 動作しておりません。
- ISDN Process
  - ISDN D チャネルを司るプロセスです。
- Function Process
  - 機能毎のプロセスです。主な機能のプロセスのみ記載しています。

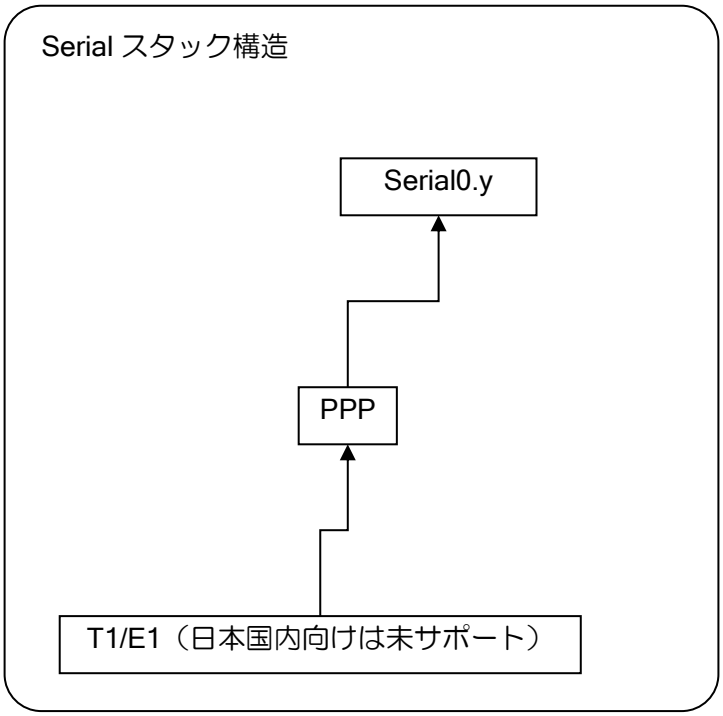
(b) プロトコルスタック

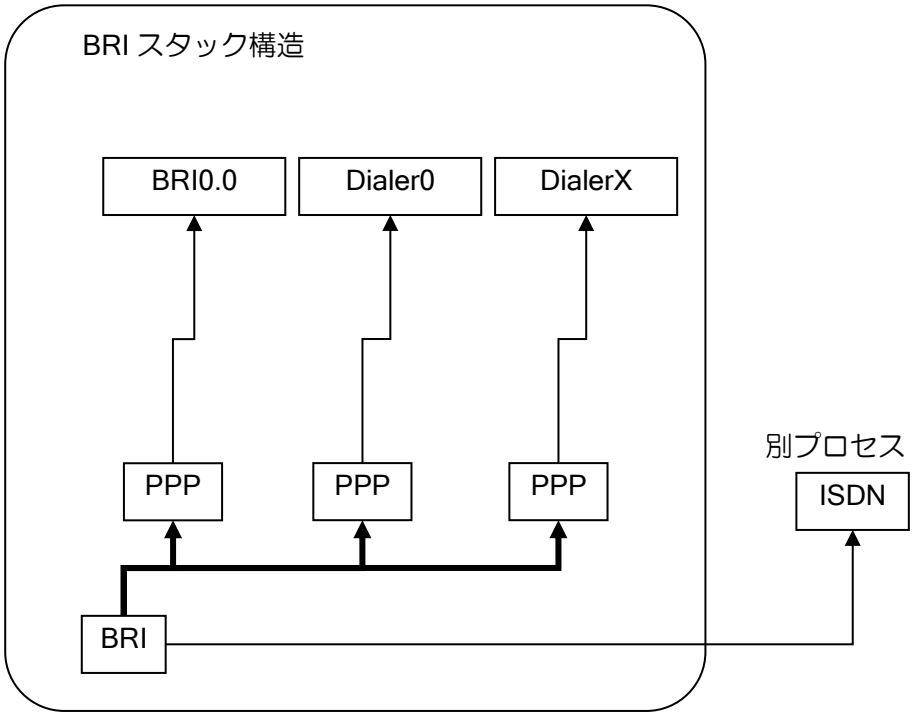


プロトコルスタックは、厳密には異なりますが、おおよそ上記の構成になっております。

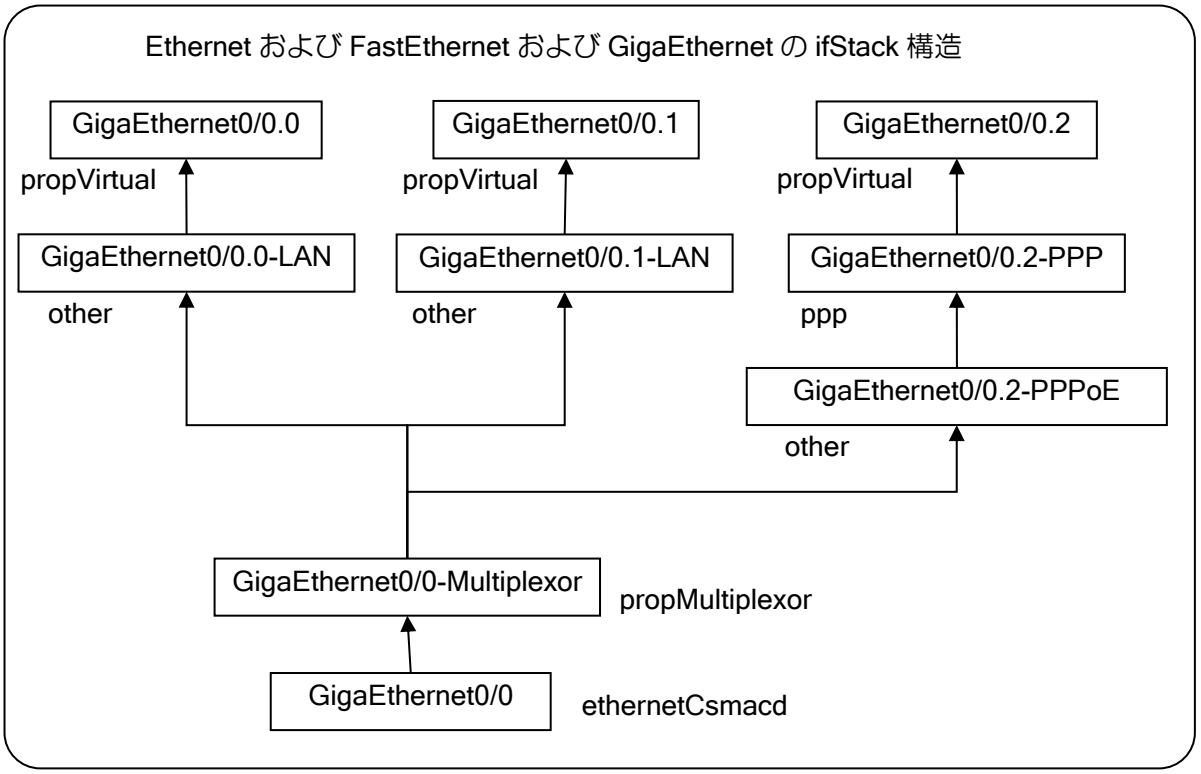
(c) リンクレイヤスタック

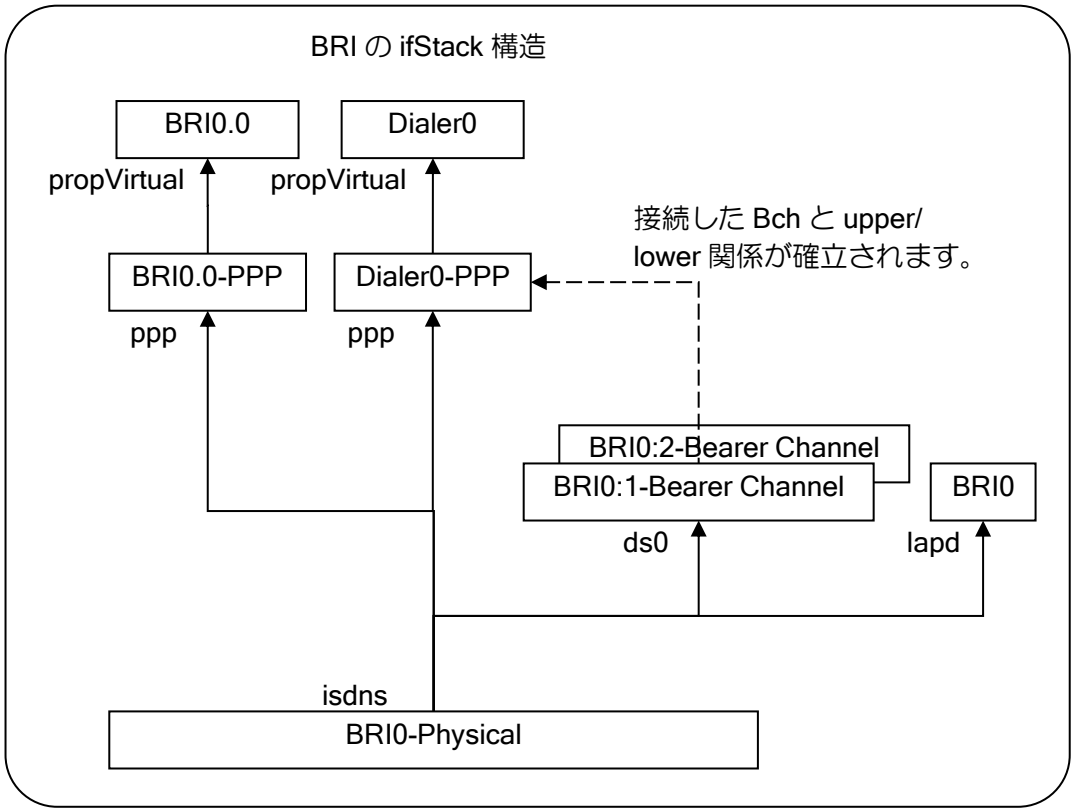


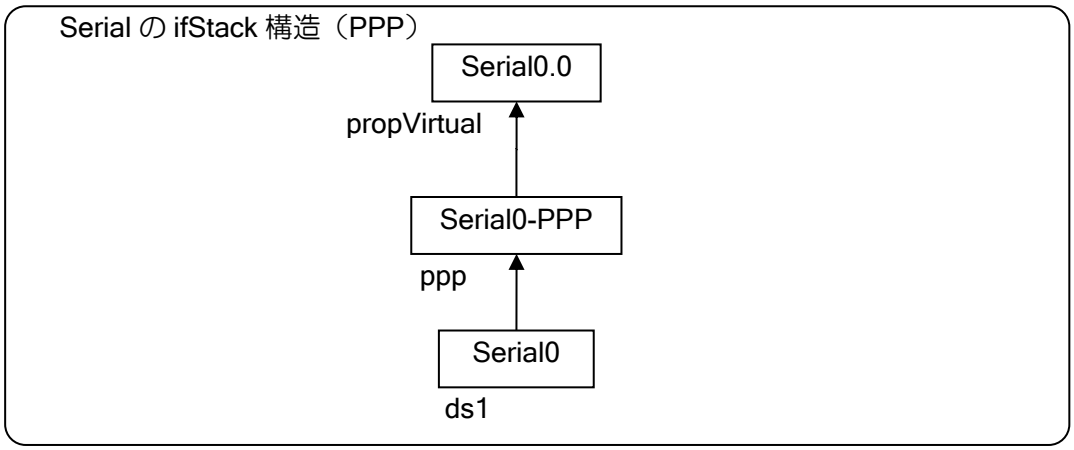


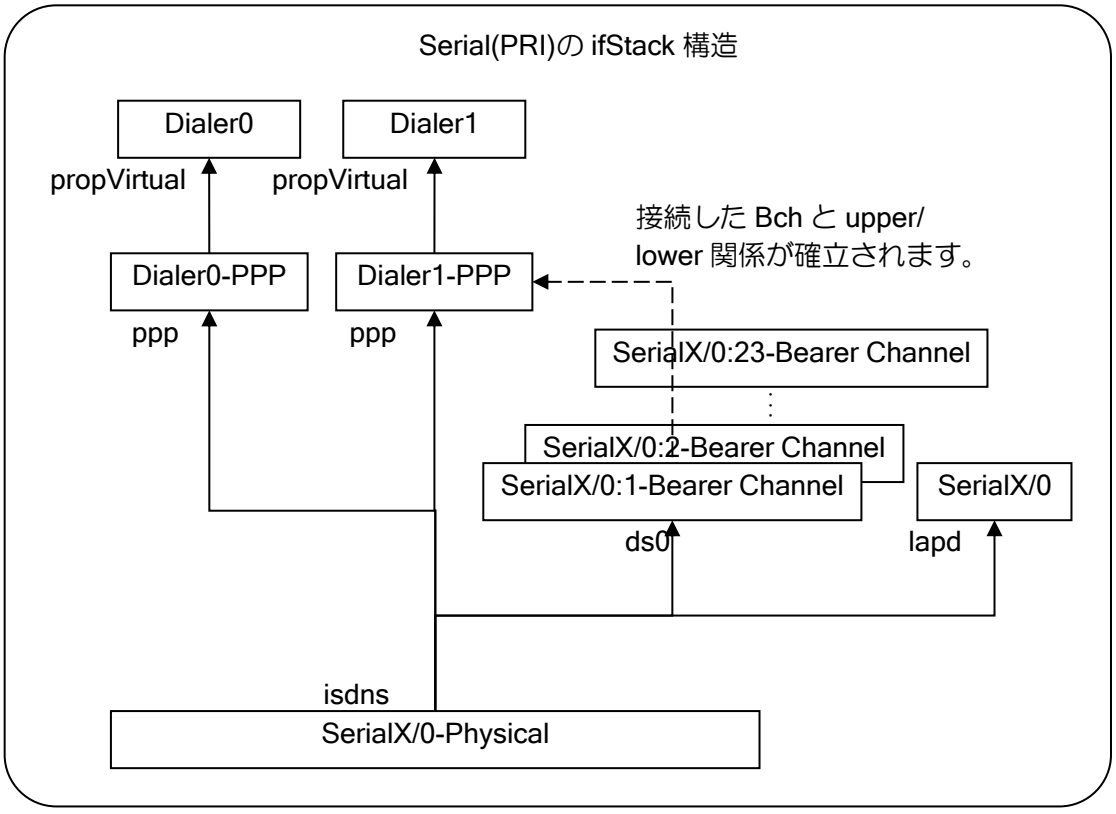

BRI スタック構造
BRI0.0
Dialer0
DialerX
PPP
PPP
PPP
別プロセス
ISDN
BRI

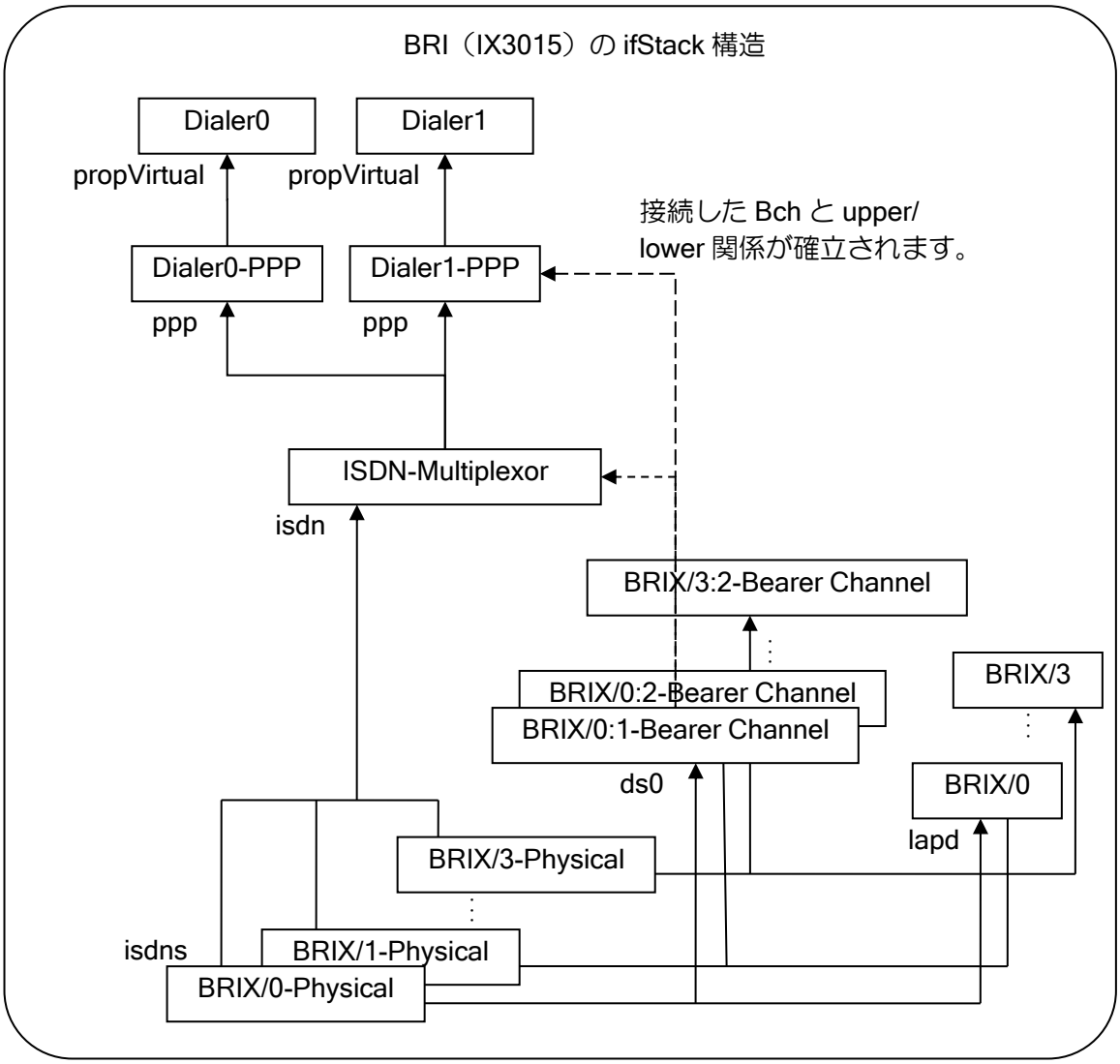
(d) ifStack

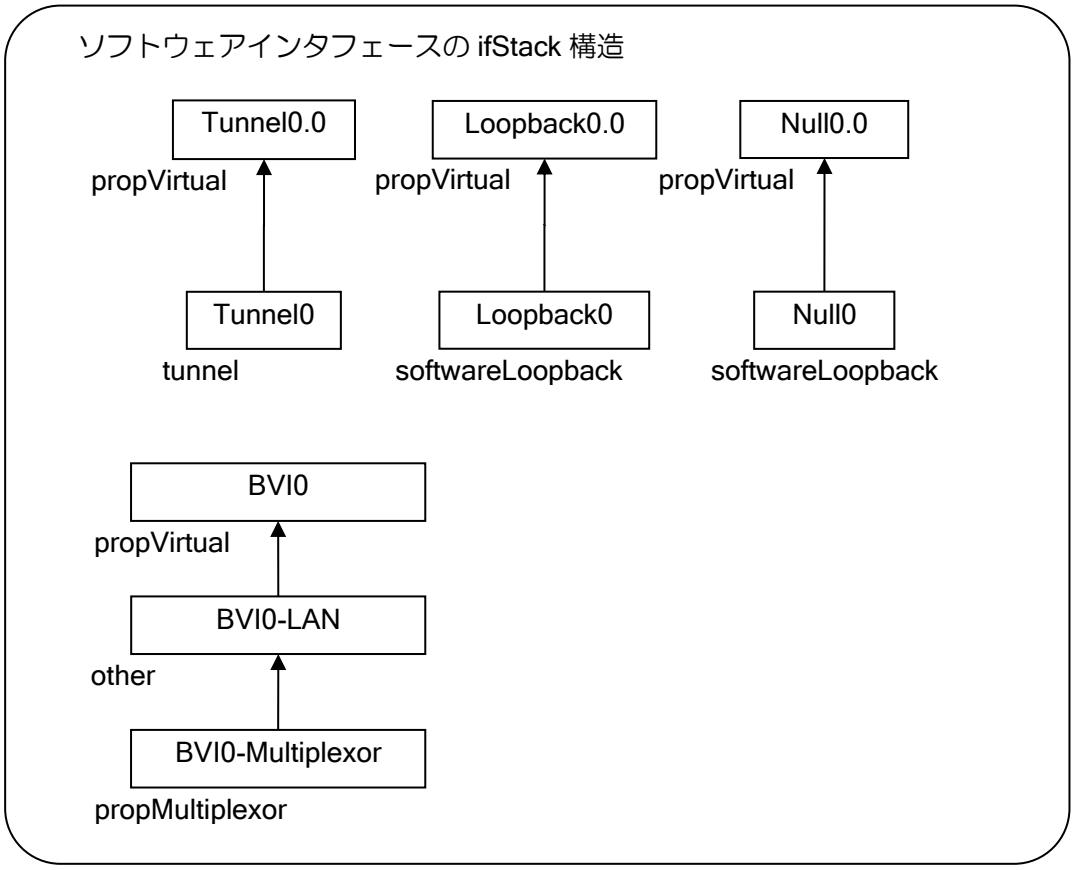

Ethernet および FastEthernet および GigaEthernet の ifStack 構造
GigaEthernet0/0.0
GigaEthernet0/0.1
GigaEthernet0/0.2
propVirtual
propVirtual
propVirtual
GigaEthernet0/0.0-LAN
GigaEthernet0/0.1-LAN
GigaEthernet0/0.2-PPP
other
other
ppp
GigaEthernet0/0.2-PPPoE
other
GigaEthernet0/0-Multiplexor
propMultiplexor
GigaEthernet0/0
ethernetCsmacd

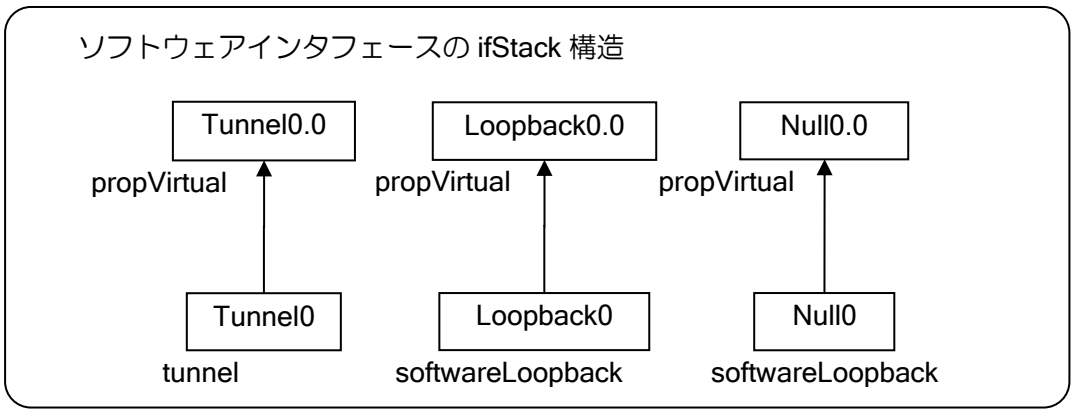

BRI の ifStack 構造
BRI0.0
Dialer0
propVirtual
propVirtual
接続した Bch と upper/
lower 関係が確立されます。
BRI0.0-PPP
Dialer0-PPP
ppp
ppp
BRI0:2-Bearer Channel
BRI0:1-Bearer Channel
BRI0
ds0
lapd
isdns
BRI0-Physical


Serial の ifStack 構造（PPP）
Serial0.0
propVirtual
Serial0-PPP
ppp
Serial0
ds1


Serial(PRI)の ifStack 構造
Dialer0
Dialer1
propVirtual
propVirtual
接続した Bch と upper/
lower 関係が確立されます。
Dialer0-PPP
Dialer1-PPP
ppp
ppp
SerialX/0:23-Bearer Channel
SerialX/0:2-Bearer Channel
SerialX/0:1-Bearer Channel
SerialX/0
ds0
lapd
isdns
SerialX/0-Physical


BRI（IX3015）の ifStack 構造
Dialer0
Dialer1
propVirtual
propVirtual
接続した Bch と upper/
lower 関係が確立されます。
Dialer0-PPP
Dialer1-PPP
ppp
ppp
ISDN-Multiplexor
isdn
BRIX/3:2-Bearer Channel
BRIX/3
BRIX/0:2-Bearer Channel
BRIX/0:1-Bearer Channel
ds0
BRIX/0
lapd
BRIX/3-Physical
isdns
BRIX/1-Physical
BRIX/0-Physical


ソフトウェアインタフェースの ifStack 構造
Tunnel0.0
Loopback0.0
Null0.0
propVirtual
propVirtual
propVirtual
Tunnel0
Loopback0
Null0
tunnel
softwareLoopback
softwareLoopback
BVI0
propVirtual
BVI0-LAN
other
BVI0-Multiplexor
propMultiplexor

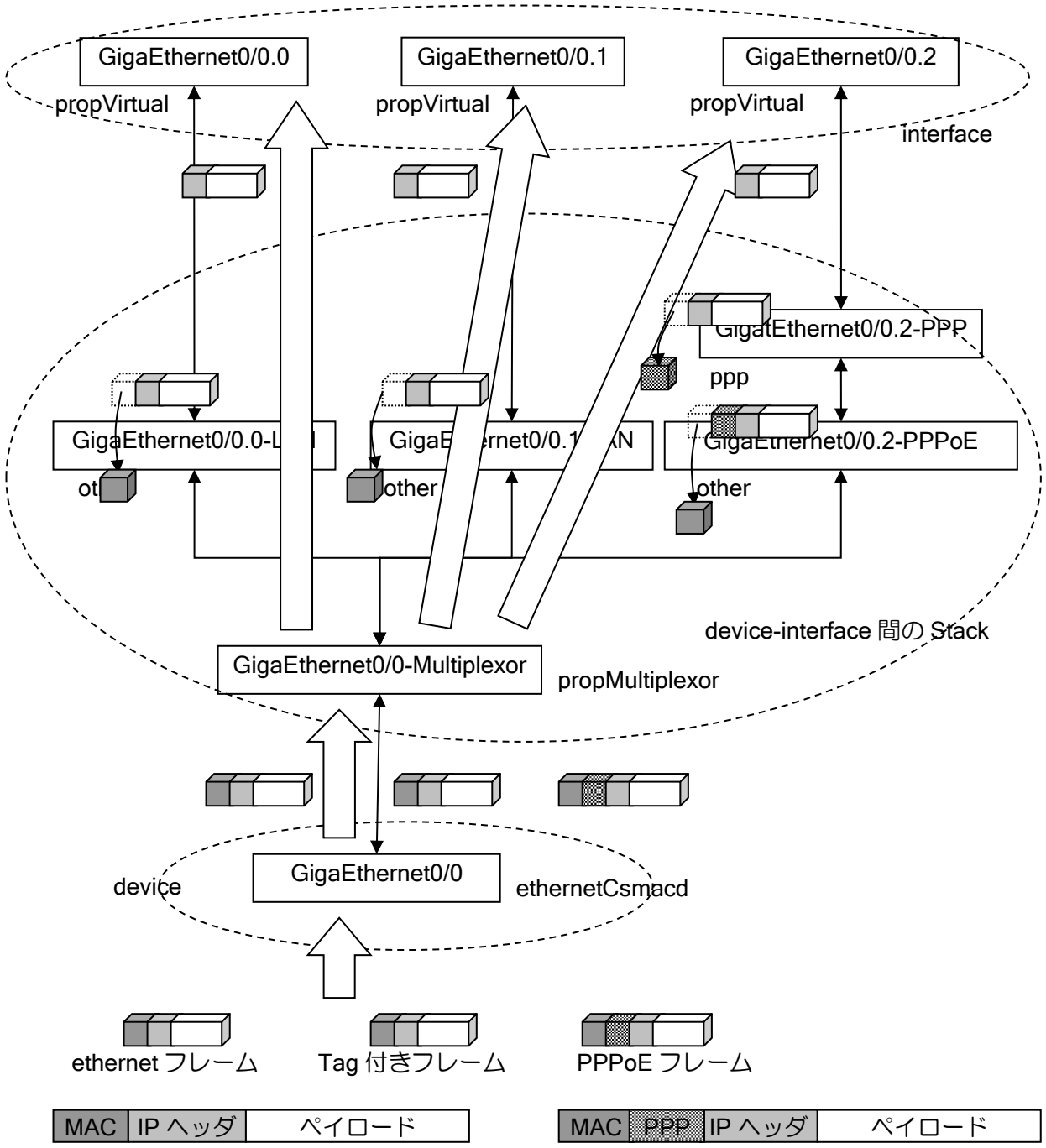

ソフトウェアインタフェースの ifStack 構造
Tunnel0.0
Loopback0.0
Null0.0
propVirtual
propVirtual
propVirtual
Tunnel0
Loopback0
Null0
tunnel
softwareLoopback
softwareLoopback

(e) interface と device の統計

ifStack 構造を基に、interface と device で収集する統計の違いを説明します。

フレームは device で受信し、それぞれのスタックで適切に処理された後、さらに上位にパケットが渡されます。device から上位に渡されるパケットは、IPv4、IPv6、ARP のみです。パケットが異常な場合や、壊れている場合などは、それぞれのスタックで適切に廃棄されます。

Gigathernet の場合



厳密には device、interface 間での相違を表す計算式を生成することはできません（device、interface では扱っているレイヤが異なるため）が、おおよそ以下のような形で表すことができます。

ifInUcastPkts［device］
－（IPv4 でも IPv6 でも ARP でもないユニキャストフレーム数）
－（廃棄されたユニキャストフレーム数）
＝Σ｛ifInUcastPkts［interface］－（マルチキャストパケット数）｝

ifOutUcastPkts［device］
＝Σ｛ifOutInUcastPkts［interface］－（廃棄フレーム数）
－（マルチキャストパケット数）｝

ifInNucastPkts［device］＝MAC レイヤのユニキャスト以外のフレーム数

ifInNucastPkts［interface］＝未対応

ifOutNucastPkts［device］＝MAC レイヤのユニキャスト以外のフレーム数

ifOutNucastPkts［interface］＝未対応

ifInOctets［device］－（IPv4 でも IPv6 でも ARP でもないフレームのオクテット数）
－（廃棄フレームのオクテット数）－（MAC ヘッダ、PPP ヘッダのオクテット数）
＝Σ｛ifInOctets［interface］｝

ifOutOctets［device］－（MAC ヘッダ、PPP ヘッダのオクテット数）
＝Σ｛ifOutOctets［interface］－（廃棄パケットのオクテット数）｝

廃棄フレームおよび廃棄パケットは、device-interface 間で処理されるときに廃棄されたフレームおよびパケットを表します。

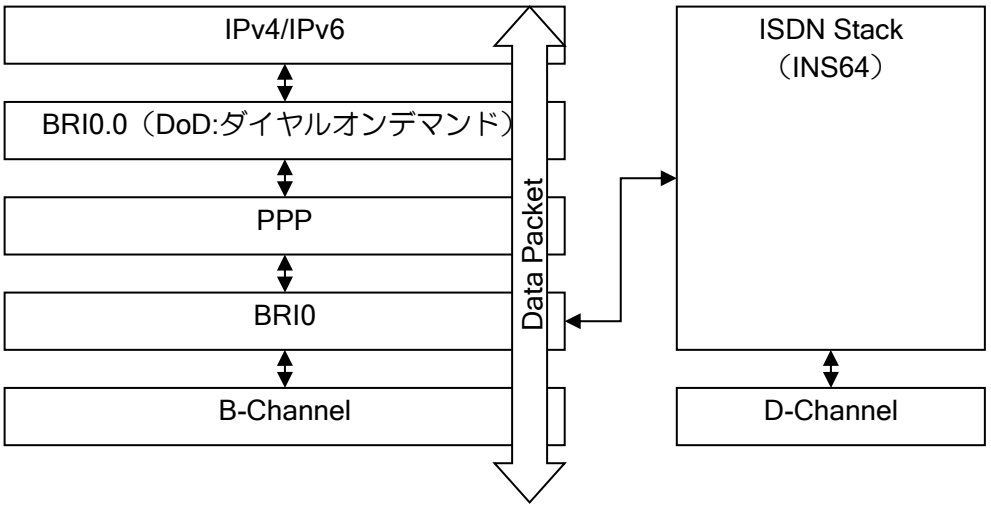
■14.14 ISDN 発信シーケンス

IX2000/IX3000 シリーズの ISDN 機能について、発信シーケンスを説明します。

ただし、以下のシーケンス等は、INS64 サービスにおける例を示しています。したがって、再発信規制のない日本国外仕様は、このシーケンスと異なります。

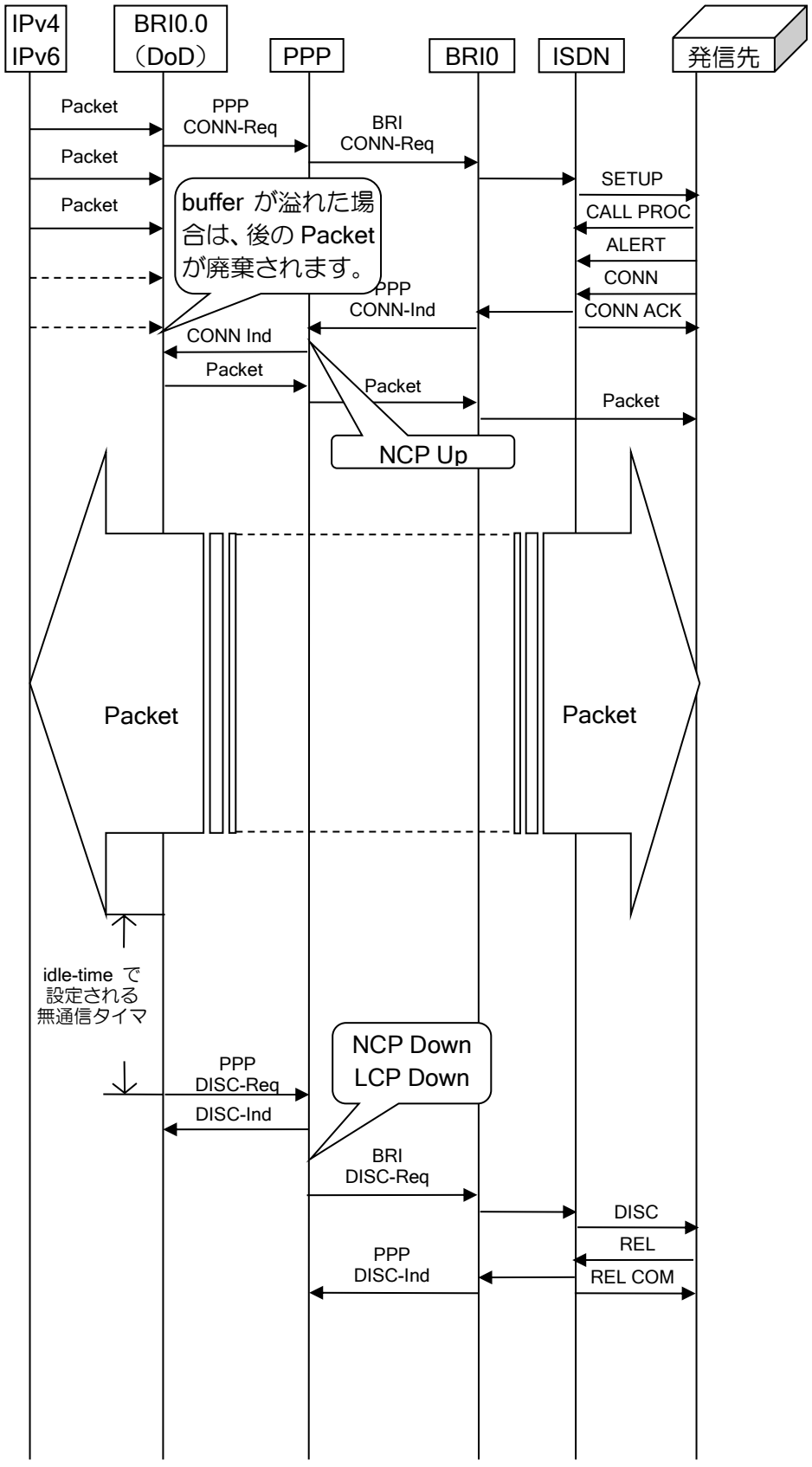
(a) BRI スタック構造

BRI のプロトコルスタック（BRI0.0 の例）を示します。



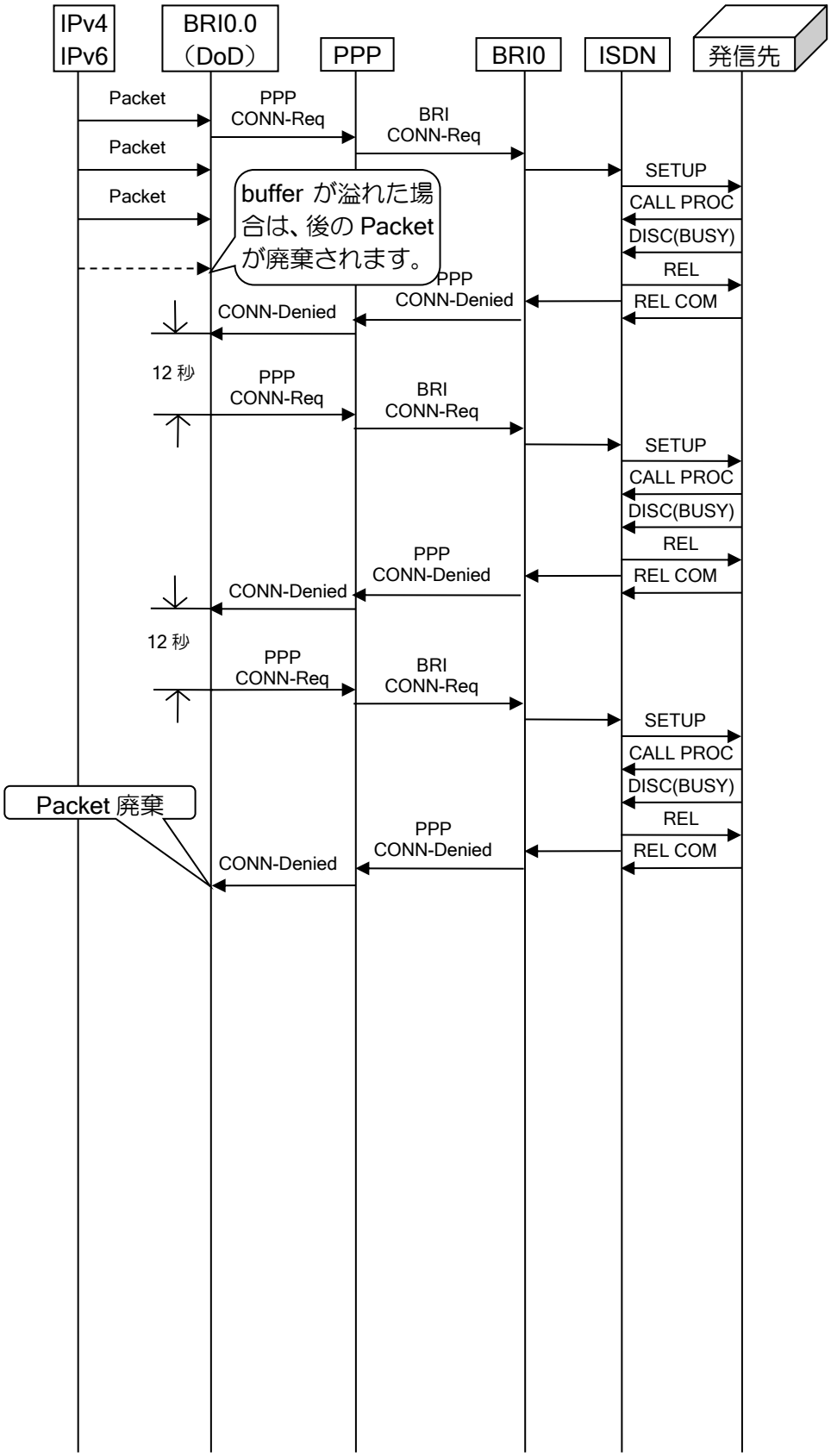
(b) 正常に ISDN 接続できる場合の例

正常に ISDN 接続できる場合のシーケンス例を示します。



(c) 発信先が１つで、ビジーとなってしまう場合の例

発信先が１つの設定で、発信してもビジーとなってしまう場合の例を示します。
ただし、以下の例では再発信規制のタイマは省略して記述しております。

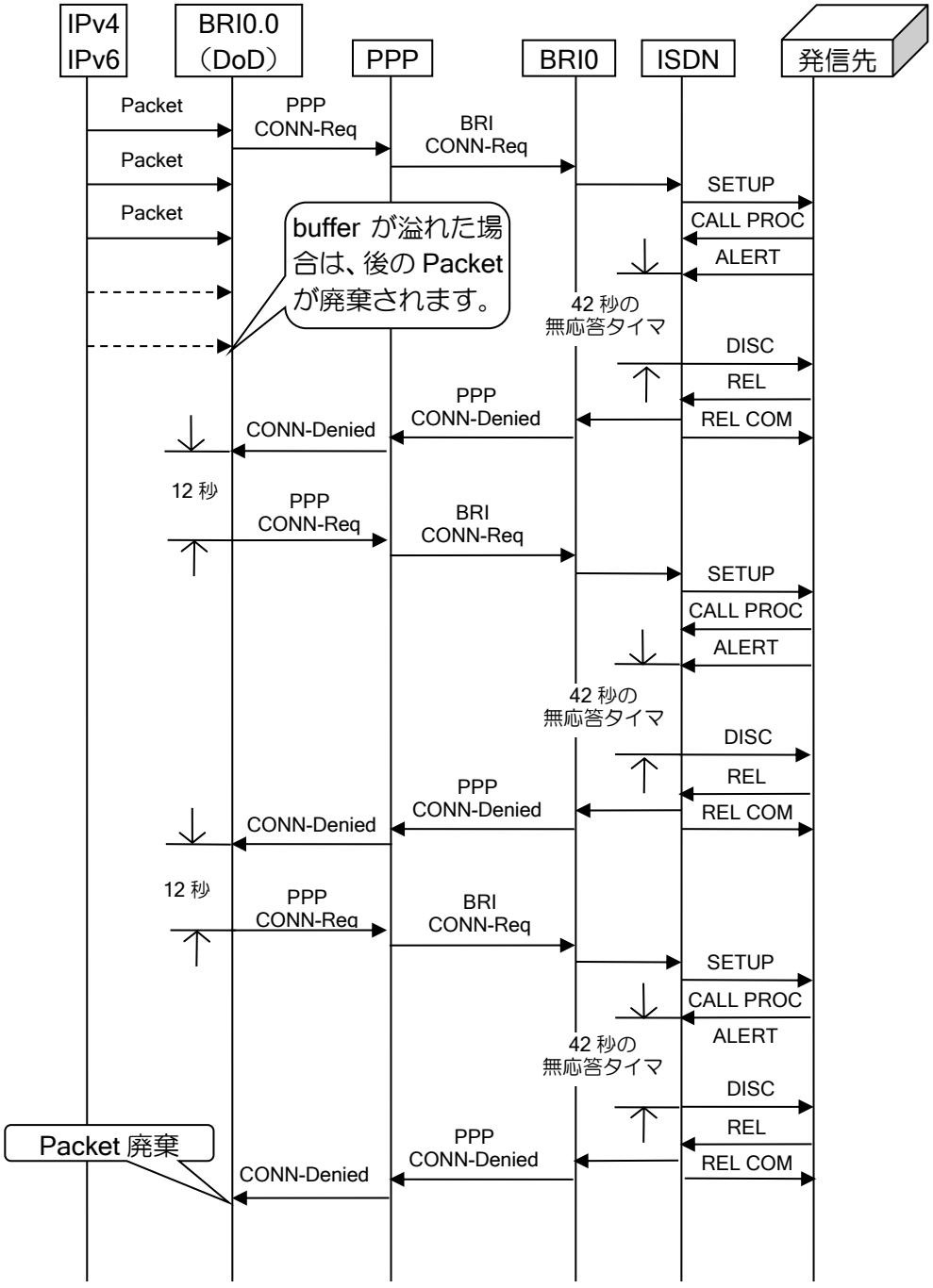


(d) 発信先が 1 つで、無応答となってしまう場合の例

発信先が 1 つの設定で、発信しても無応答となってしまう場合の例を示します。

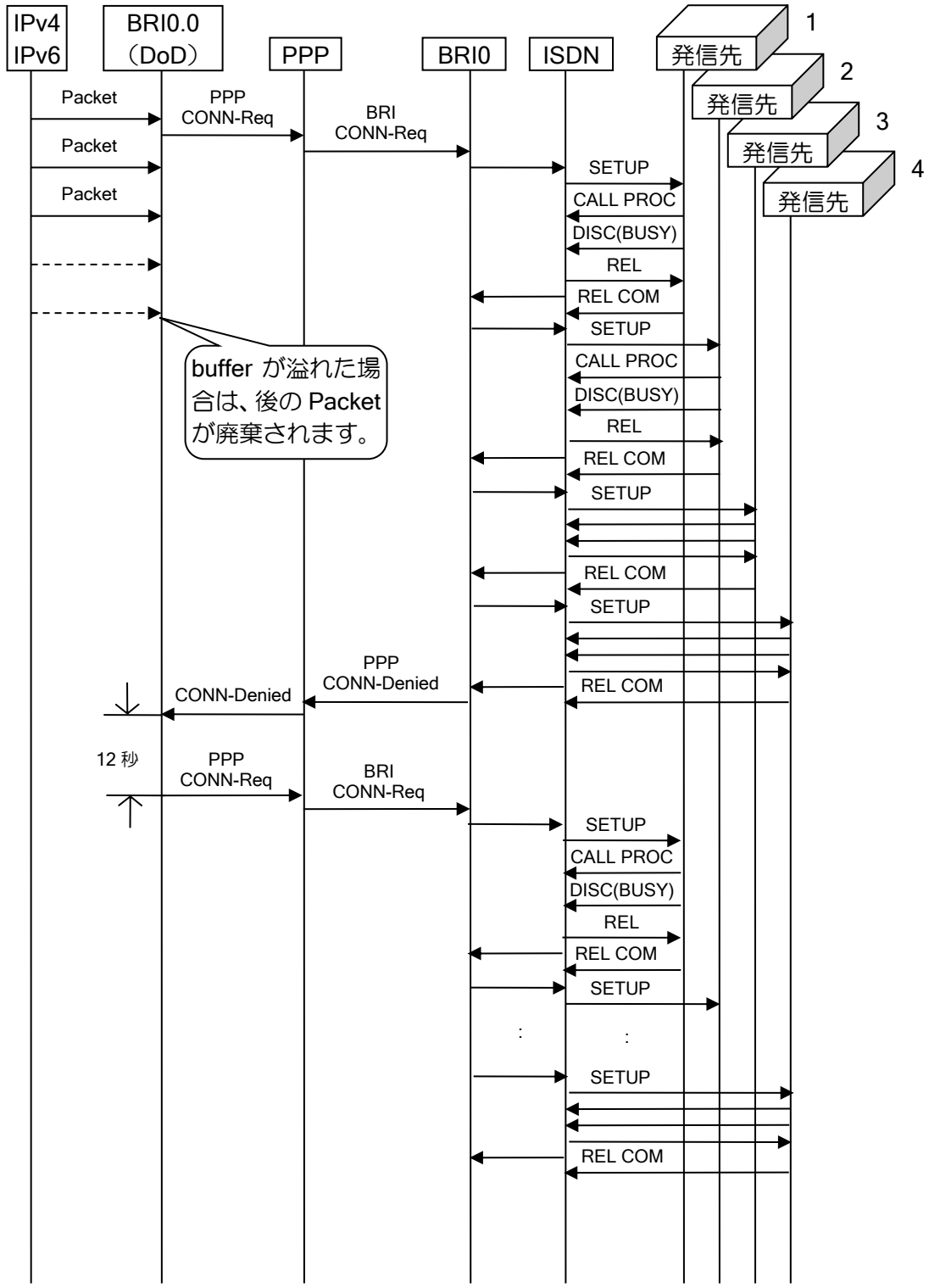
ここで示す無応答とは、呼び出し中のまま応答が返されない状態（SETUP に対して CALL_PROC および ALERT は返されるが、CONN が返されない状態）を表しており、発信先が回線断、電源 OFF 等の状態（SETUP に対して CALL_PROC が返されない状態）ではありません。

また、以下の例では再発信規制のタイマは省略して記述しております。

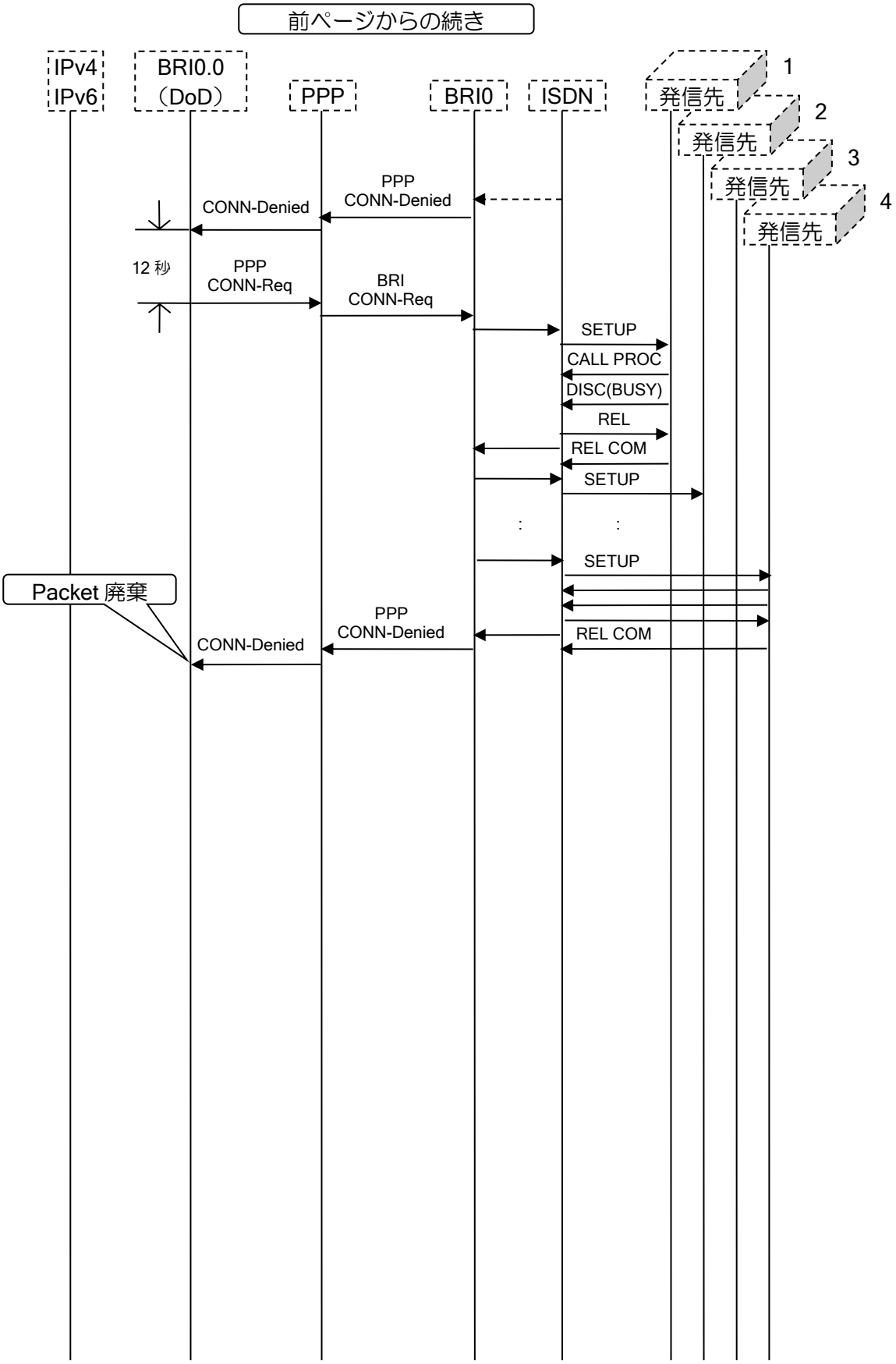


(e) 発信先が複数で、すべてがビジーとなってしまう場合の例

発信先が複数の設定で、発信してもすべてがビジーとなってしまう場合の例を示します。
ただし、以下の例では再発信規制のタイマは省略して記述しております。



次ページに続く

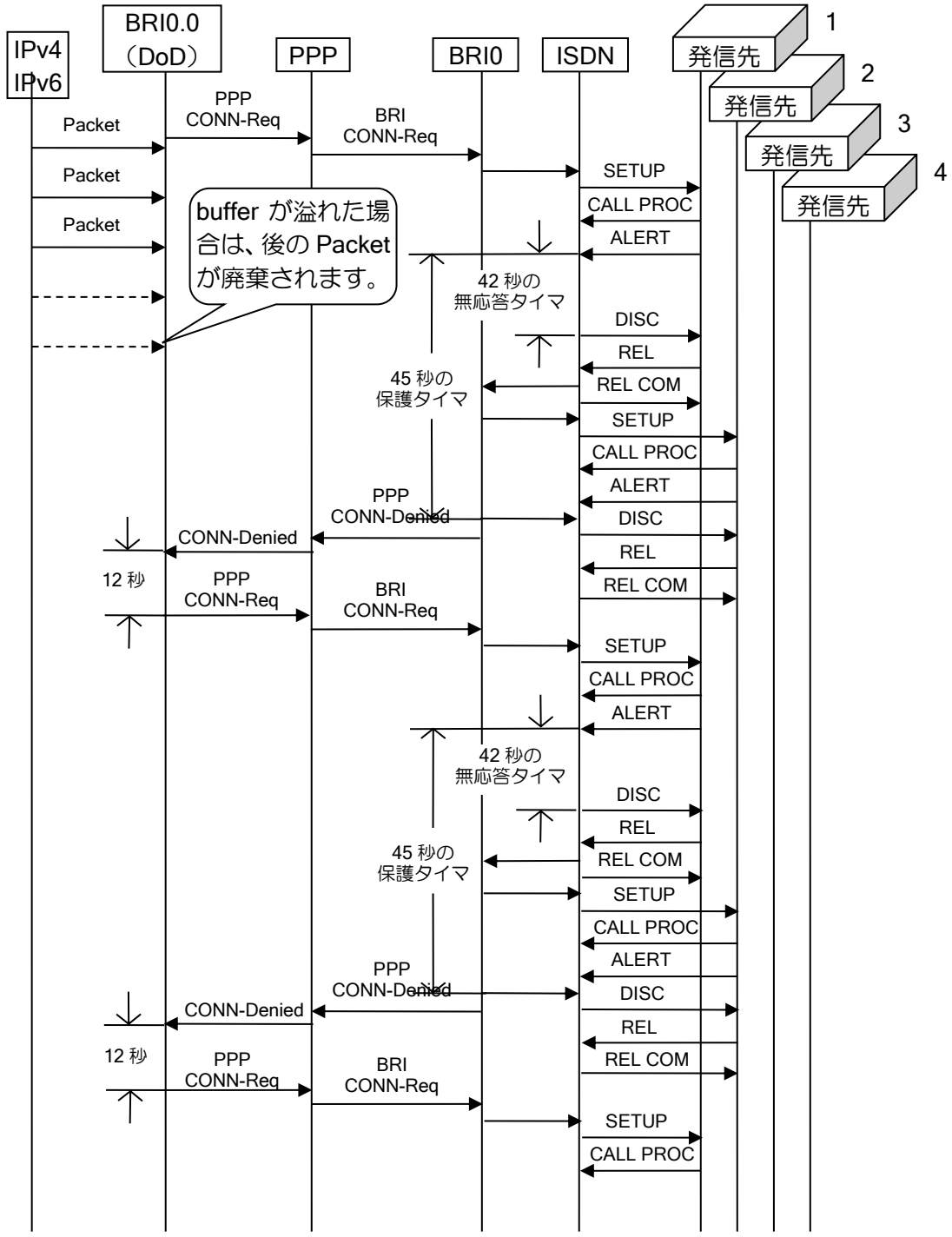

前ページからの続き
IPv4
IPv6
BRI0.0
（DoD）
PPP
BRI0
ISDN
発信先
1
発信先
2
発信先
3
発信先
4
PPP
CONN-Denied
CONN-Denied
12 秒
PPP
CONN-Req
BRI
CONN-Req
SETUP
CALL PROC
DISC(BUSY)
REL
REL COM
SETUP
:
:
SETUP
Packet 廃棄
PPP
CONN-Denied
REL COM
CONN-Denied

(f) 発信先が複数で、すべてが無応答となってしまう場合の例

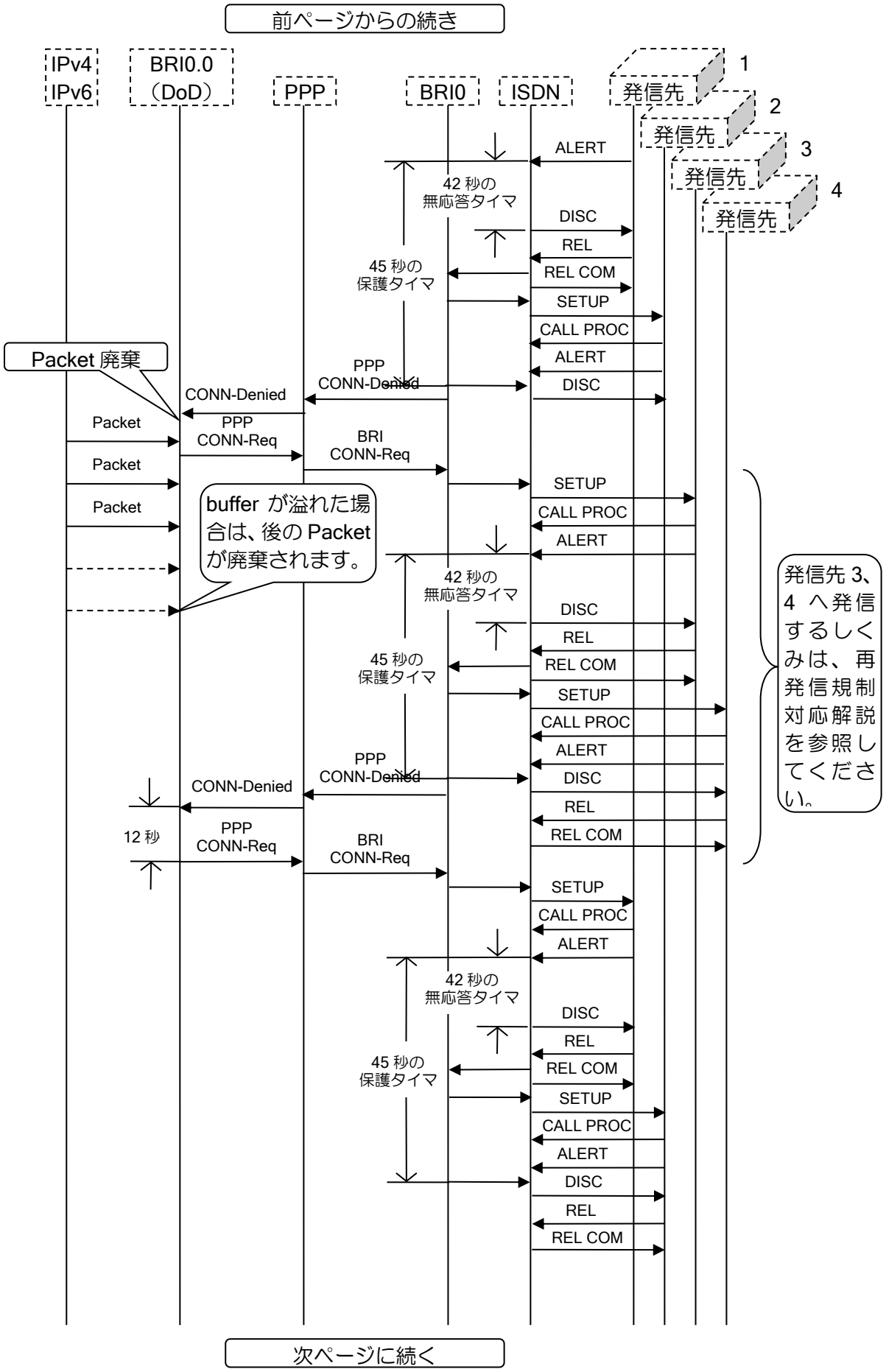
発信先が複数の設定で、発信してもすべてが無応答となってしまう場合の例を示します。

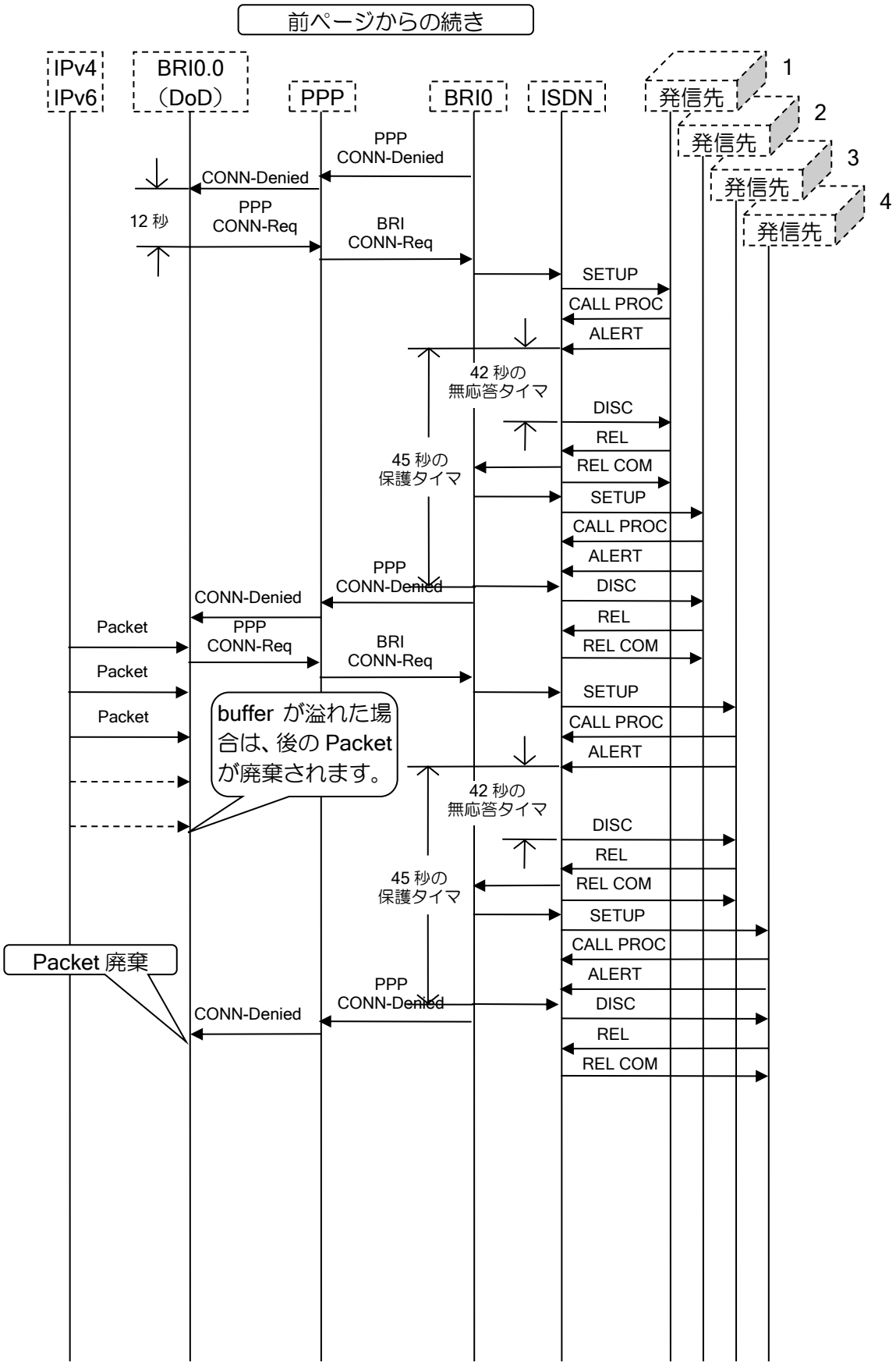
ここで示す無応答とは、呼び出し中のまま応答が返されない状態（SETUP に対して CALL PROC および ALERT は返されるが、CONN が返されない状態）を表しており、発信先が回線断、電源 OFF 等の状態（SETUP に対して CALL_PROC が返されない状態）ではありません。

また、以下の例では再発信規制のタイマは省略して記述しております。



次ページに続く


前ページからの続き
IPv4
IPv6
BRI0.0
（DoD）
PPP
BRI0
ISDN
発信先
1
2
3
4
ALERT
42 秒の
無応答タイマ
DISC
REL
REL COM
45 秒の
保護タイマ
SETUP
CALL PROC
ALERT
DISC
Packet 廃棄
PPP
CONN-Denied
CONN-Denied
Packet
PPP
CONN-Req
BRI
CONN-Req
Packet
Packet
buffer が溢れた場合は、後の Packet が廃棄されます。
SETUP
CALL PROC
ALERT
42 秒の
無応答タイマ
DISC
REL
REL COM
45 秒の
保護タイマ
SETUP
CALL PROC
ALERT
PPP
CONN-Denied
DISC
REL
REL COM
CONN-Denied
12 秒
PPP
CONN-Req
BRI
CONN-Req
SETUP
CALL PROC
ALERT
42 秒の
無応答タイマ
DISC
REL
REL COM
45 秒の
保護タイマ
SETUP
CALL PROC
ALERT
DISC
REL
REL COM
発信先 3、4 へ発信するしくみは、再発信規制対応解説を参照してください。
次ページに続く


前ページからの続き
IPv4
IPv6
BRI0.0
（DoD）
PPP
BRI0
ISDN
発信先
1
2
3
4
PPP
CONN-Denied
CONN-Denied
12 秒
PPP
CONN-Req
BRI
CONN-Req
SETUP
CALL PROC
ALERT
42 秒の
無応答タイマ
DISC
REL
45 秒の
保護タイマ
REL COM
SETUP
CALL PROC
ALERT
PPP
CONN-Denied
DISC
CONN-Denied
REL
Packet
PPP
CONN-Req
REL COM
BRI
CONN-Req
Packet
SETUP
Packet
CALL PROC
buffer が溢れた場合は、後の Packet が廃棄されます。
ALERT
42 秒の
無応答タイマ
DISC
REL
45 秒の
保護タイマ
REL COM
SETUP
CALL PROC
Packet 廃棄
ALERT
PPP
CONN-Denied
DISC
CONN-Denied
REL
REL COM

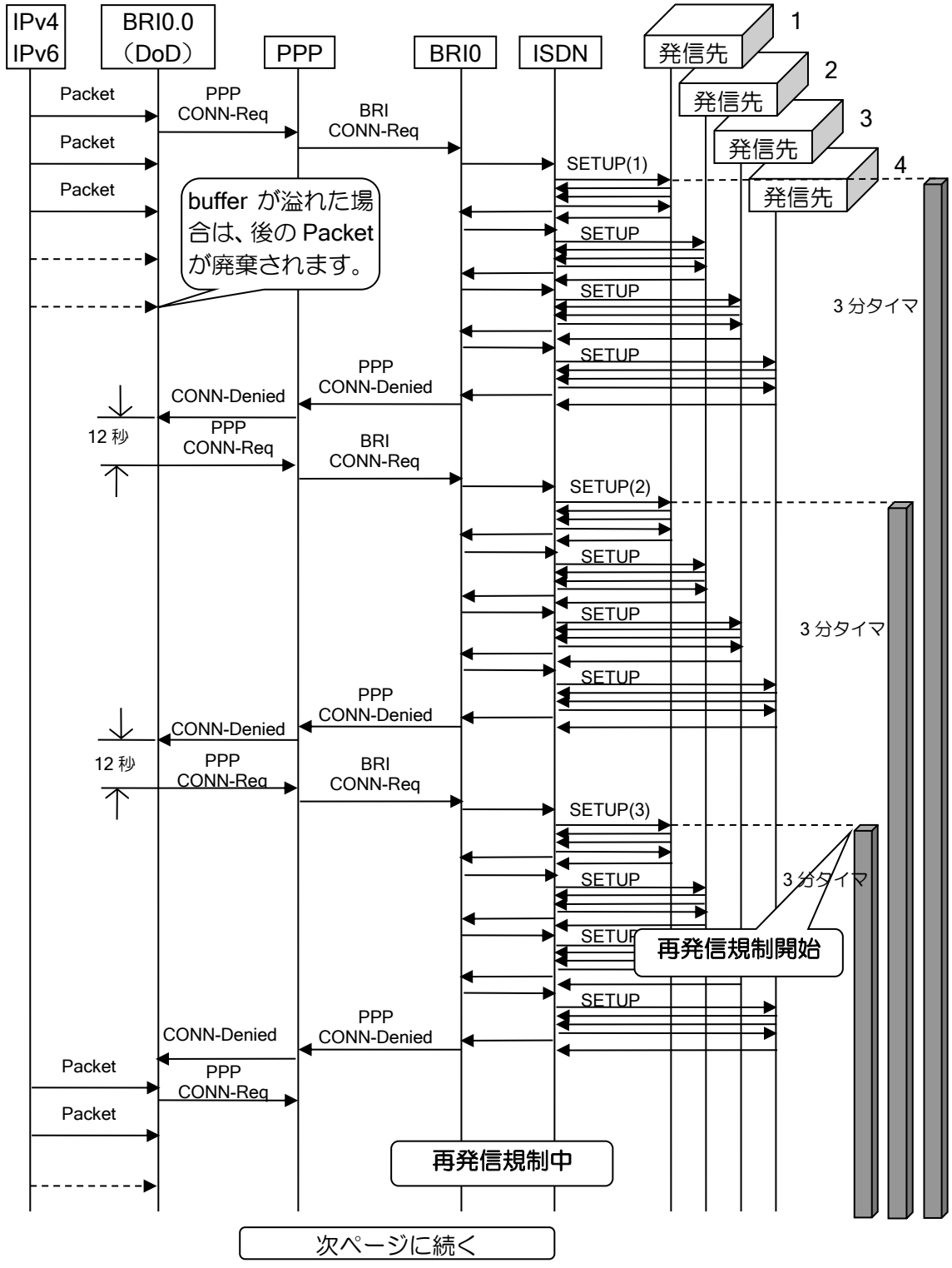
(g) 3 分間に 2 回以内の再発信規制対応の解説

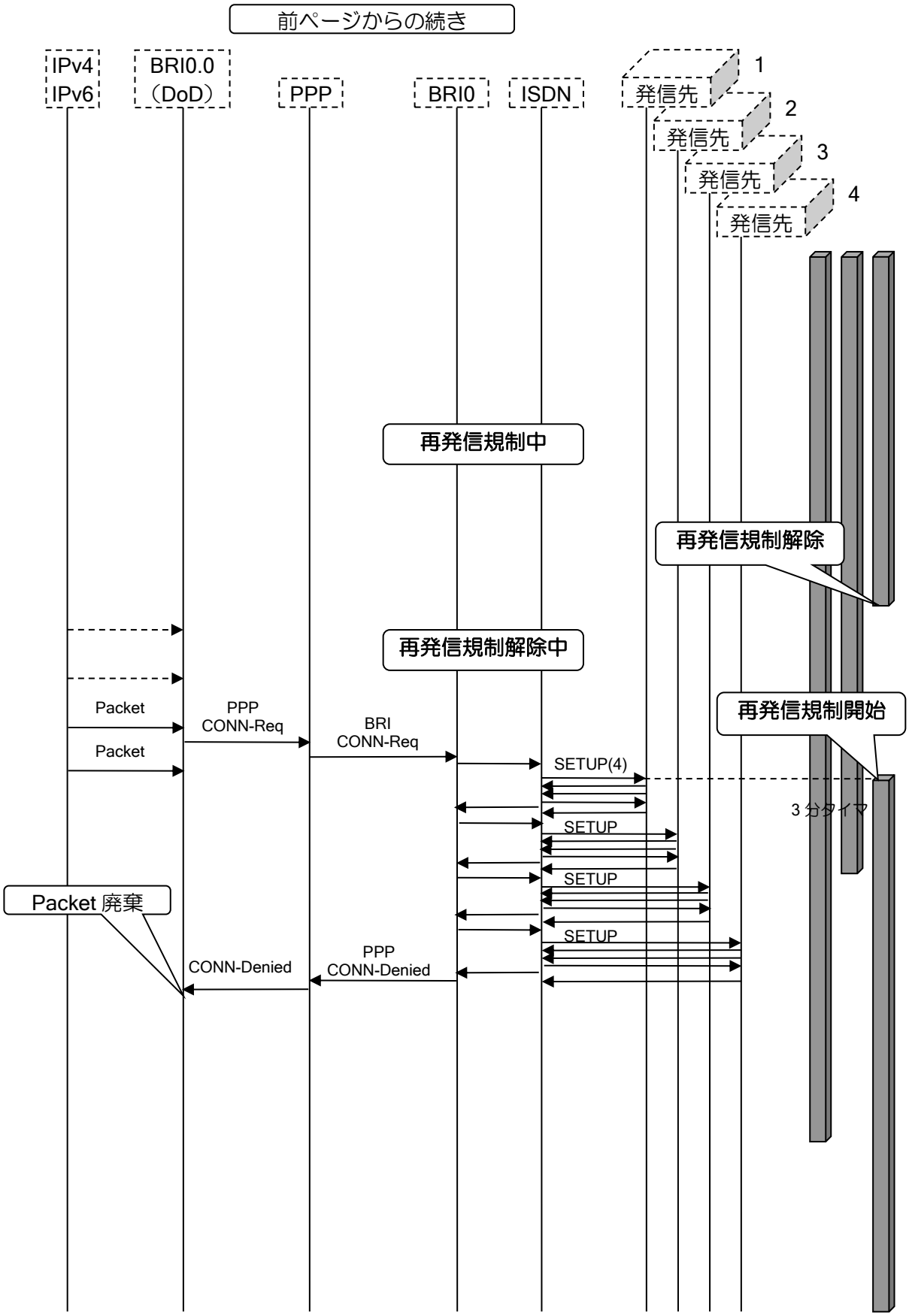
同一発信先に対して 3 分以内に 2 回以内の再発信規制機構が備えられています。
そのしくみを以下に説明します。

i) 発信先が複数で、すべてがビジーとなってしまう場合の例

発信先が複数の設定で、発信してもビジーとなってしまう場合の例を示します。

ここでは、発信先 1 に着目して説明しますが、実際には、発信先 2、発信先 3、発信先 4 についても同様のタイマが適用されます。



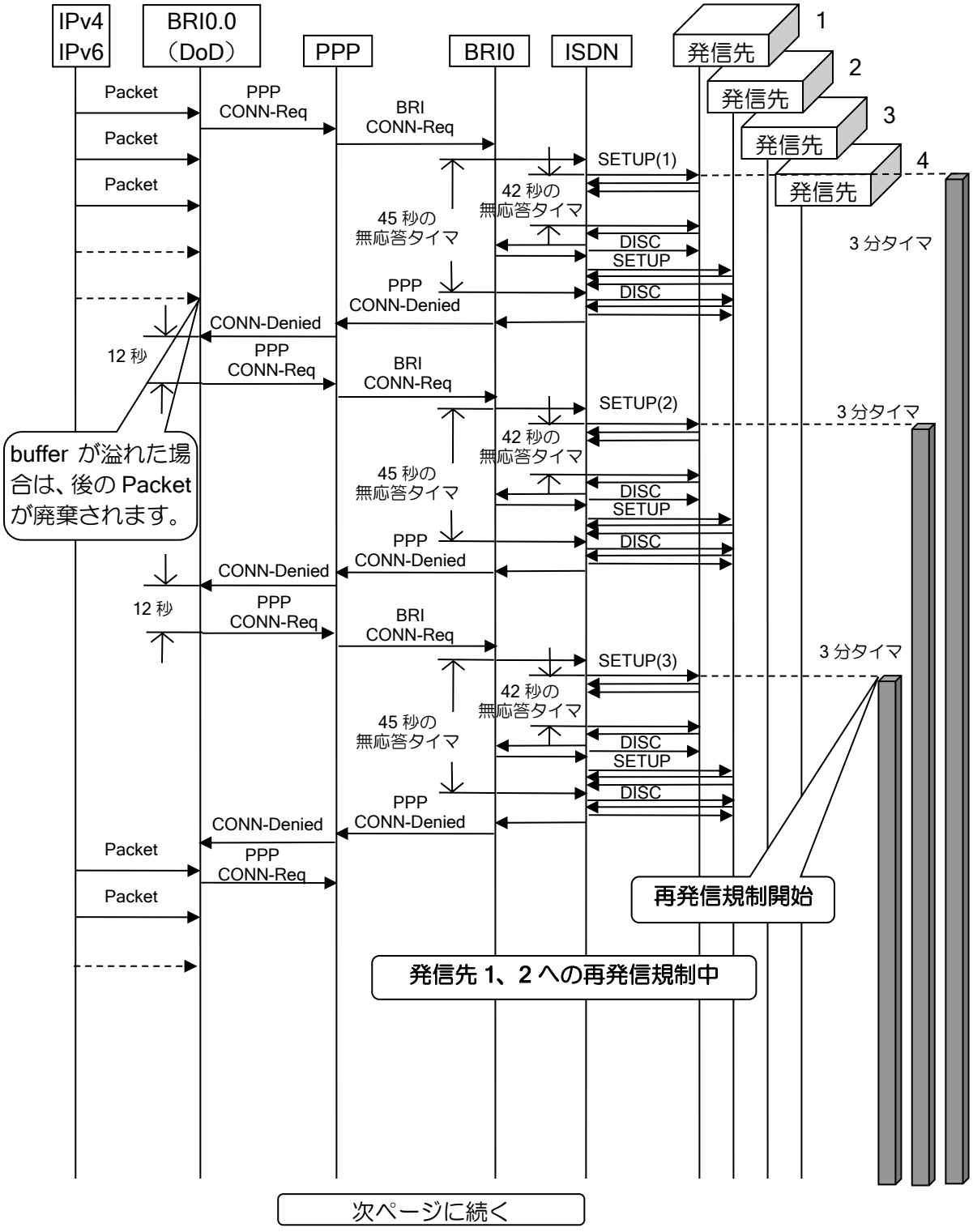

前ページからの続き
IPv4
IPv6
BRI0.0
（DoD）
PPP
BRI0
ISDN
発信先
1
発信先
2
発信先
3
発信先
4
再発信規制中
再発信規制解除
再発信規制解除中
再発信規制開始
Packet
Packet
PPP
CONN-Req
BRI
CONN-Req
SETUP(4)
3 分タイマ
SETUP
SETUP
SETUP
Packet 廃棄
CONN-Denied
PPP
CONN-Denied

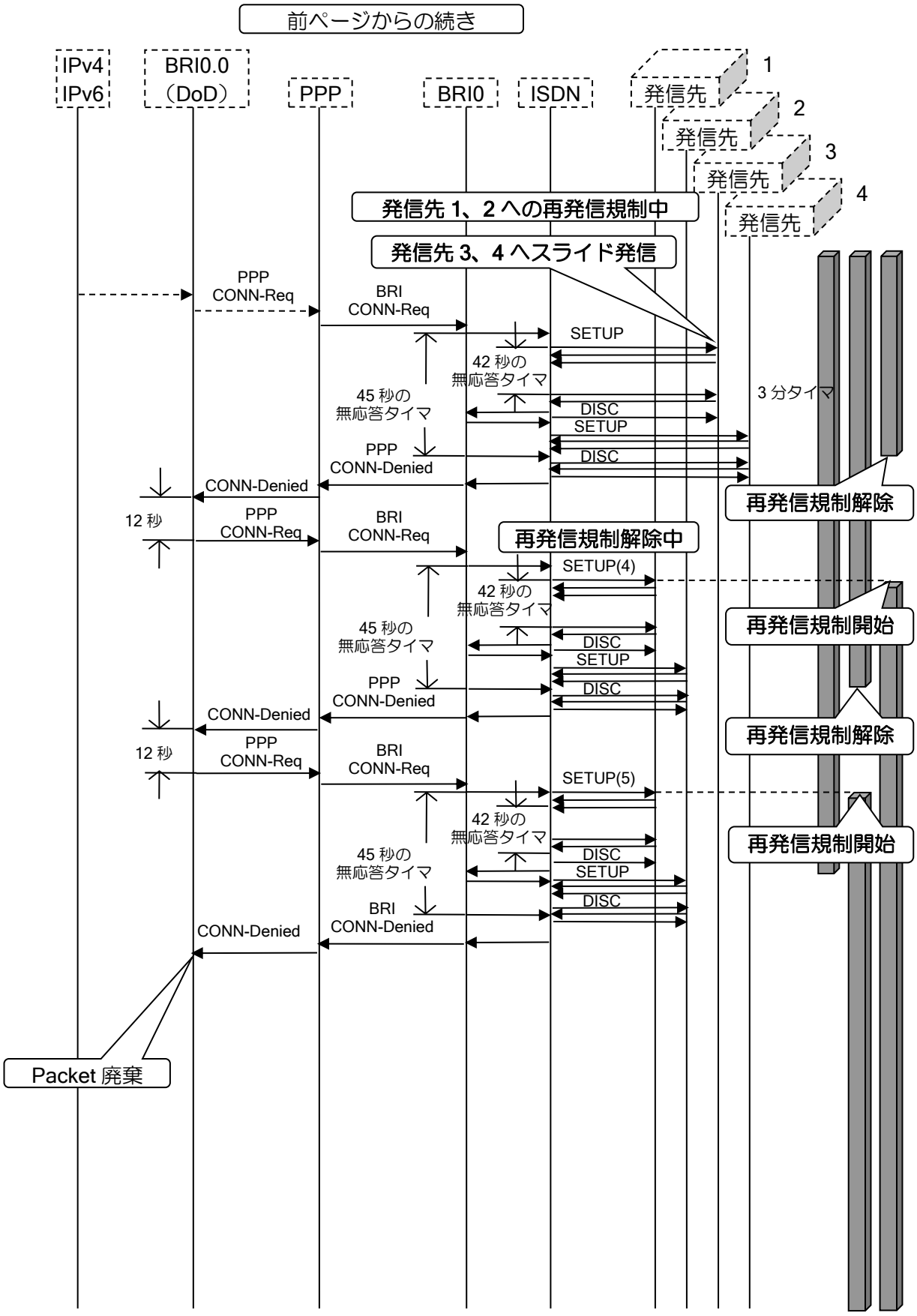
ii) 発信先が複数で、すべてが無応答となってしまう場合の例

発信先が複数の設定で、発信しても無応答となってしまう場合の例を示します。

ここで示す無応答とは、呼び出し中のまま応答が返されない状態（SETUP に対して CALL PROC および ALERT は返されるが、CONN が返されない状態）を表しており、発信先が回線断、電源 OFF 等の状態（SETUP に対して CALL_PROC が返されない状態）ではありません。

また、以下では、発信先 1 に着目して説明しますが、実際には、発信先 2、発信先 3、発信先 4 についても同様のタイマが適用されます。




前ページからの続き
IPv4
IPv6
BRI0.0
（DoD）
PPP
BRI0
ISDN
発信先
1
発信先
2
発信先
3
発信先
4
発信先 1、2 への再発信規制中
発信先 3、4 へスライド発信
PPP
CONN-Req
BRI
CONN-Req
SETUP
42 秒の
無応答タイマ
45 秒の
無応答タイマ
DISC
SETUP
3 分タイマ
PPP
CONN-Denied
DISC
CONN-Denied
再発信規制解除
12 秒
PPP
CONN-Req
BRI
CONN-Req
再発信規制解除中
SETUP(4)
42 秒の
無応答タイマ
再発信規制開始
45 秒の
無応答タイマ
DISC
SETUP
PPP
CONN-Denied
DISC
CONN-Denied
再発信規制解除
12 秒
PPP
CONN-Req
BRI
CONN-Req
SETUP(5)
42 秒の
無応答タイマ
再発信規制開始
45 秒の
無応答タイマ
DISC
SETUP
BRI
CONN-Denied
DISC
CONN-Denied
Packet 廃棄

(h) 同一電話番号で異なるサブアドレスを持つ場合の解説

同一電話番号で異なるサブアドレスを持つ場合、同一電話番号への発信と見なして、自動再発信規制を行います。

【動作例】

発信先 1 電話番号=123
発信先 2 電話番号=123:01
発信先 3 電話番号=567
発信先 4 電話番号=890

の場合でビジーのときは、

発信先 1
発信先 2
発信先 3
発信先 4
発信先 1
発信先 3
発信先 4
発信先 3
発信先 4
：
：

のように発信されます。

■14.15 プライベート MIB 詳細

System MIB

(a) 温度

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84). picoSystem(2).picoTemperature(1)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoCelsius(1)	温度（単位：摂氏［℃］）	INTEGER	RO	
picoFahrenheit(2)	温度（単位：華氏［F］）	INTEGER	RO	

(b) 電圧

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84). picoSystem(2)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoVoltage(2)	電圧　単位：mV	INTEGER	RO	取得する電圧値は 3.3V

(c) FAN 状態（IX3000 シリーズ、IX2310）

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoSystem(2).picoFanTable(3).picoFanEntry(1)

- インデックス：picoFanIndex(1)：ファン番号

オブジェクト名	内容	SYNTAX	R/W	備考
picoFanIndex(1)	ファン番号	INTEGER	RO	
picoFanStatus(2)	ファン状態 1.正常 2.異常	INTEGER	RO	
picoFanRpm(3)	ファン回転数（回転数/分） 0.異常（5295 以下は全て 0） 5295～.正常	INTEGER	RO	

(d) 電源ユニット状態（IX3000 シリーズ）

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoSystem(2).picoPowerSupplyTable (4).
  picoPowerSupplyEntry (1)

- インデックス：picoPowerSupplyIndex (1)：電源ユニット番号

オブジェクト名	内容	SYNTAX	R/W	備考
picoPowerSupplyIndex (1)	電源ユニット番号	INTEGER	RO	
picoPowerSupplyType (2)	電源ユニット種別 0.未実装 1.通常電源 2.PoE 電源	INTEGER	RO	
picoPowerSupplyStatus (3)	電源ユニット状態 0.未実装 1.正常 2.異常	INTEGER	RO	

(e) システム utilization

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoSystem(2). picoSched (5)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoSchedRtUtl1Sec (1)	過去 1 秒間の utilization （単位：%）	Gauge	RO	
picoSchedRtUtl5Sec (2)	過去 5 秒間の utilization （単位：%）	Gauge	RO	
picoSchedRtUtl1Min (3)	過去 1 分間の utilization （単位：%）	Gauge	RO	
picoSchedRtUtl1Hour (4)	過去 1 時間の utilization （単位：%）	Gauge	RO	Ver.7.4 以降

(f) Heap メモリ

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoSystem(2). picoHeap (6)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoHeapSize (1)	トータル Heap メモリサイズ （単位：byte）	INTEGER	RO	
picoHeapUtil (2)	メモリの使用率 （単位：%）	Gauge	RO	

IPsec MIB

(a) IPsec MIB バージョン

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecLevels(1)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
pipSecMibLevel(1)	IPsec MIB のバージョン	INTEGER	RO	

(b) Phase1 統計情報（全体）

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecPhaseOne (2).pikeGlobalStats(1)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
pikeGlobalActiveTunnels(1)	有効な IKE Phase1 接続数	Gauge	RO	
pikeGlobalInNotifys(6)	Notify 受信数	Counter	RO	
pikeGlobalInP2Exchgs(7)	Phase2 交換受信数	Counter	RO	
pikeGlobalInP2ExchgInvalids(8)	不正な Phase2 交換受信数	Counter	RO	
pikeGlobalInP2ExchgRejects(9)	自装置で拒絶した Phase2 交換受信数	Counter	RO	
pikeGlobalInP2SaDelRequests(10)	Phase2 SA 削除要求受信数	Counter	RO	
pikeGlobalOutNotifys(14)	Notify 送信数	Counter	RO	
pikeGlobalOutP2Exchgs(15)	Phase2 交換送信数	Counter	RO	
pikeGlobalOutP2ExchgInvalids(16)	相手装置で不正とされた Phase2 交換送信数	Counter	RO	
pikeGlobalOutP2ExchgRejects(17)	相手装置で拒絶された Phase2 交換送信数	Counter	RO	
pikeGlobalOutP2SaDelRequests(18)	Phase2SA 削除要求送信数	Counter	RO	
pikeGlobalInitTunnels(19)	自装置から開始した Phase1 接続数	Counter	RO	
pikeGlobalInitTunnelFails(20)	自装置からの開始で接続が失敗した Phase1 接続数	Counter	RO	
pikeGlobalRespTunnelFails(21)	相手装置からの開始で接続が失敗した Phase1 接続数	Counter	RO	
pikeGlobalAuthFails(23)	認証失敗数	Counter	RO	
pikeGlobalDecryptFails(24)	復号化失敗数	Counter	RO	
pikeGlobalHashValidFails(25)	ハッシュ確認失敗数	Counter	RO	
pikeGlobalRespTunnels(27)	相手装置から開始した Phase1 接続数	Counter	RO	
pikeGlobalInP1SaDelRequests(30)	Phase1 SA 削除要求受信数	Counter	RO	
pikeGlobalOutP1SaDelRequests(31)	Phase1 SA 削除要求送信数	Counter	RO	

(c) Phase1 ピア情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecPhaseOne (2).pikePeerTable(2). pikePeerEntry(1)

- インデックス
  pikePeerLocalType(1)　:自装置のピア識別の種別
  pikePeerLocalValue(2)　:自装置のピア識別の値
  pikePeerRemoteType(3)　:相手装置のピア識別の種別
  pikePeerRemoteValue(4)　:相手装置のピア識別の値
  pikePeerIntIndex(5)　:Phase1 インデックス

オブジェクト名	内容	SYNTAX	R/W	備考
pikePeerLocalType(1)	自装置のピア識別の種別 1.IPv4 アドレス 4.IPv6 アドレス	IkePeerType	不可	
pikePeerLocalValue(2)	自装置のピア識別の値	DisplayString	不可	
pikePeerRemoteType(3)	相手装置のピア識別の種別 1.IPv4 アドレス 4.IPv6 アドレス	IkePeerType	不可	
pikePeerRemoteValue(4)	相手装置のピア識別の値	DisplayString	不可	
pikePeerIntIndex(5)	Phase1 インデックス	INTEGER	不可	
pikePeerLocalAddr(6)	自装置のアドレス（IPv4/IPv6）	IPSIpAddress	RO	
pikePeerRemoteAddr(7)	相手装置のアドレス （IPv4/IPv6）	IPSIpAddress	RO	
pikePeerActiveTime(8)	Phase1 SA の接続時間	TimeInterval	RO	
pikePeerActiveTunnelIndex(9)	Phase1 インデックス	INTEGER	RO	

(d) Phase1 トンネル情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecPhaseOne (2).pikeTunnelTable (3). pikeTunnelEntry (1)

- インデックス
  pikeTunIndex (1) :トンネルのインデックス

オブジェクト名	内容	SYNTAX	R/W	備考
pikeTunIndex(1)	Phase1 インデックス	INTEGER	不可	
pikeTunLocalType(2)	自装置のピア識別の種別 1.IPv4 アドレス 4.IPv6 アドレス	IkePeerType	RO	
pikeTunLocalValue(3)	自装置のピア識別の値	DisplayString	RO	
pikeTunLocalAddr(4)	自装置のアドレス（IPv4/IPv6）	IPSIpAddress	RO	
pikeTunRemoteType(6)	相手装置のピア識別の種別 1.IPv4 アドレス 4.IPv6 アドレス	IkePeerType	RO	
pikeTunRemoteValue(7)	相手装置のピア識別の値	DisplayString	RO	
pikeTunRemoteAddr(8)	相手装置のアドレス （IPv4/IPv6）	IPSIpAddress	RO	
pikeTunNegoMode(10)	Phase1 の接続モード 1.メインモード 2.アグレッシブモード	IkeNegoMode	RO	

pikeTunDiffHellmanGrp(11)	Diffie Hellman グループ 1.無し 2.768 ビット 3.1024 ビット 4.1536 ビット 5.2048 ビット	DiffHellmanGrp	RO	
pikeTunEncryptAlgo(12)	暗号化アルゴリズム 1.無し 2.DES 3.3DES 4.AES	EncryptAlgo	RO	
pikeTunHashAlgo(13)	ハッシュアルゴリズム 1.無し 2.MD5 3.SHA-1	IkeHashAlgo	RO	
pikeTunAuthMethod(14)	認証方法 1.無し 2.pre-sharedkey	IkeAuthMethod	RO	
pikeTunLifeTime(15)	Phase1 SA のライフタイム（単位：秒）	INTEGER	RO	
pikeTunActiveTime(16)	Phase1 SA がアクティブな時間（単位：1/100 秒）	TimeInterval	RO	
pikeTunSaRefreshThreshold(17)	ライフタイム満了時に実行する Re-key タイミングの閾値（単位：秒）	INTEGER	RO	
pikeTunInNotifys(22)	Notify の受信数	Counter	RO	
pikeTunInP2Exchgs(23)	Phase2 交換の受信数	Counter	RO	
pikeTunInP2ExchgInvalids(24)	不正な Phase2 交換受信数	Counter	RO	
pikeTunInP2ExchgRejects(25)	自装置で拒絶した Phase2 交換受信数	Counter	RO	
pikeTunInP2SaDelRequests(26)	Phase2 SA 削除要求受信数	Counter	RO	
pikeTunOutNotifys(30)	Notify の送信数	Counter	RO	
pikeTunOutP2Exchgs(31)	Phase2 交換の送信数	Counter	RO	
pikeTunOutP2ExchgInvalids(32)	相手装置で不正とされた Phase2 交換送信数	Counter	RO	
pikeTunOutP2ExchgRejects(33)	相手装置で拒絶された Phase2 交換送信数	Counter	RO	
pikeTunOutP2SaDelRequests(34)	Phase2 SA 削除要求送信数	Counter	RO	
pikeTunStatus(35)	Phase1 接続状態 1.active 2. down	TunnelStatus	RO	

(e) Phase2 トンネル統計情報（全体）

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecPhaseTwo(3).pipSecGlobalStats (1)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
pipSecGlobalActiveTunnels(1)	有効な IPsec トンネル数	Gauge	RO	
pipSecGlobalInOctets(3)	受信オクテット数	Counter	RO	
pipSecGlobalInPkts(9)	受信パケット数	Counter	RO	
pipSecGlobalInDrops(10)	受信時のパケット廃棄数（Anti-Replay による廃棄は除く）	Counter	RO	
pipSecGlobalInReplayDrops(11)	Anti-Replay によるパケット廃棄数	Counter	RO	
pipSecGlobalInAuths(12)	受信時の認証回数	Counter	RO	
pipSecGlobalInAuthFails(13)	受信時の認証失敗回数	Counter	RO	
pipSecGlobalInDecrypts(14)	受信時の復号回数	Counter	RO	
pipSecGlobalInDecryptFails(15)	受信時の復号失敗回数	Counter	RO	

pipSecGlobalOutOctets(16)	送信オクテット数	Counter	RO	
pipSecGlobalOutPkts(22)	送信パケット数	Counter	RO	
pipSecGlobalOutDrops(23)	送信時の廃棄数	Counter	RO	
pipSecGlobalOutAuths(24)	送信時の認証回数	Counter	RO	
pipSecGlobalOutAuthFails(25)	送信時の認証失敗回数	Counter	RO	
pipSecGlobalOutEncrypts(26)	送信時の暗号回数	Counter	RO	
pipSecGlobalOutEncryptFails(27)	送信時の暗号失敗回数	Counter	RO	
pipSecGlobalNoSaFails(33)	SA が存在しないため失敗した送受信回数	Counter	RO	

(f) Phase2 トンネル情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecPhaseTwo(3).pipSecTunnelTable (2). pipSecTunnelEntry(1)

- インデックス：
  pipSecTunIndex(1)　:トンネルのインデックス

オブジェクト名	内容	SYNTAX	R/W	備考
pipSecTunIndex(1)	トンネルのインデックス	INTEGER	不可	
pipSecTunIkeTunnelIndex(2)	Phase2 接続時に使用した Phase1 のインデックス	INTEGER	RO	
pipSecTunIkeTunnelAlive(3)	Phase2 接続時に使用した Phase1 SA の有無	TruthValue	RO	
pipSecTunLocalAddr(4)	自装置の IP アドレス（IPv4/IPv6）	IPSIpAddress	RO	
pipSecTunRemoteAddr(5)	相手装置の IP アドレス（IPv4/IPv6）	IPSIpAddress	RO	
pipSecTunKeyType(6)	鍵種別 1.自動鍵 2.固定鍵	KeyType	RO	
pipSecTunEncapMode(7)	カプセル化モード 1.トンネル 2.トランスポート	EncapMode	RO	
pipSecTunLifeSize(8)	トンネルのライフサイズ（単位：キロバイト）	INTEGER	RO	
pipSecTunLifeTime(9)	トンネルのライフタイム（単位：秒）	INTEGER	RO	
pipSecTunActiveTime(10)	トンネルがアクティブな時間（単位：1/100 秒）	TimeInterval	RO	
pipSecTunSaLifeSizeThreshold(11)	ライフサイズ満了時に実行する Re-key タイミングの閾値（単位：キロバイト）	INTEGER	RO	
pipSecTunSaLifeTimeThreshold(12)	SA のライフタイム満了時に実行する Re-key タイミングの閾値（単位：秒）	INTEGER	RO	
pipSecTunTotalRefreshes(13)	SA のリフレッシュ回数	COUNTER	RO	
pipSecTunExpiredSaInstances(14)	期限満了になった SA 数	Gauge	RO	
pipSecTunCurrentSaInstances(15)	現在の SA 数	Gauge	RO	
pipSecTunInSaDiffHellmanGrp(16)	受信方向 DH グループ 1.無し 2.768 ビット 3.1024 ビット 4.1536 ビット 5.2048 ビット	DiffHellmanGrp	RO	
pipSecTunInSaEncryptAlgo(17)	受信方向暗号化方法 1.無し 2.DES 3.3DES 4.AES	EncryptAlgo	RO	

pipSecTunInSaAhAuthAlgo(18)	受信方向 AH 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	
pipSecTunInSaEspAuthAlgo(19)	受信方向 ESP 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	
pipSecTunOutSaDiffHellmanGrp(21)	送信方向 DH グループ 1.無し 2.768 ビット 3.1024 ビット 4.1536 ビット 5.2048 ビット	DiffHellmanGrp	RO	
pipSecTunOutSaEncryptAlgo(22)	送信方向暗号化方法 1.無し 2.DES 3.3DES 4.AES	EncryptAlgo	RO	
pipSecTunOutSaAhAuthAlgo(23)	送信方向 AH 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	
pipSecTunOutSaEspAuthAlgo(24)	送信方向 ESP 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	
pipSecTunPmtu(26)	パス MTU サイズ	INTEGER	RO	
pipSecTunInOctets(27)	受信オクテット数	Counter	RO	
pipSecTunInPkts(33)	受信パケット数	Counter	RO	
pipSecTunInDropPkts(34)	受信時の廃棄パケット数（Anti-Replay による廃棄は除く）	Counter	RO	
pipSecTunInReplayDropPkts(35)	受信時の Anti-Replay による廃棄	Counter	RO	
pipSecTunInAuths(36)	受信時の認証回数	Counter	RO	
pipSecTunInAuthFails(37)	受信時の認証失敗回数	Counter	RO	
pipSecTunInDecrypts(38)	受信時の復号回数	Counter	RO	
pipSecTunInDecryptFails(39)	受信時の復号失敗回数	Counter	RO	
pipSecTunOutOctets(40)	送信オクテット数	Counter	RO	
pipSecTunOutPkts(46)	送信パケット数	Counter	RO	
pipSecTunOutDropPkts(47)	送信時の廃棄パケット数（Anti-Replay による廃棄は除く）	Counter	RO	
pipSecTunOutAuths(48)	送信時の認証回数	Counter	RO	
pipSecTunOutAuthFails(49)	送信時の認証失敗回数	Counter	RO	
pipSecTunOutEncrypts(50)	送信時の復号回数	Counter	RO	
pipSecTunOutEncryptFails(51)	送信時の復号失敗回数	Counter	RO	
pipSecTunStatus(56)	トンネル状態 1.active 2.down	TunnelStatus	RO	

(g) Phase2 SPI 情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecPhaseTwo(3).pipSecSpiTable (4). pipSecSpiEntry(1)

- インデックス：
  pipSecSpiIndex(1)　:トンネルのインデックス

オブジェクト名	内容	SYNTAX	R/W	備考
pipSecSpiIndex(1)	SPI のインデックス	INTEGER	不可	
pipSecSpiDirection(2)	SPI の方向	INTEGER	RO	
pipSecSpiValue(3)	SPI 値	Gauge	RO	

pipSecSpiProtocol(4)	SPI のプロトコル 1: AH, 2:ESP, 3:IPCOMP	INTEGER	RO	
pipSecSpiStatus(5)	SPI の状態 1: active, 2:expiring	INTEGER	RO	

(h) Phase1 履歴情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecHistory(4). pipSecHistPhaseOne(2). pikeTunnelHistTable(1). pikeTunnelHistEntry(1)

- インデックス：
  pikeTunHistIndex(1) :IKE ヒストリインデックス

オブジェクト名	内容	SYNTAX	R/W	備考
pikeTunHistIndex(1)	インデックス	INTEGER	不可	
pikeTunHistTermReason(2)	トンネル終了理由 1.その他（下記以外） 2.正常終了 3.コマンドによる終了 4.相手装置からの削除	INTEGER	RO	
pikeTunHistActiveIndex(3)	Phase1 インデックス	INTEGER	RO	
pikeTunHistPeerLocalType(4)	自装置のピア識別の種別 1.IPv4 アドレス 4.IPv6 アドレス	IkePeerType	RO	
pikeTunHistPeerLocalValue(5)	自装置のピア識別値	DisplayString	RO	
pikeTunHistPeerIntIndex(6)	Phase1 インデックス	INTEGER	RO	
pikeTunHistPeerRemoteType(7)	相手装置のピア識別の種別 1.IPv4 アドレス 4.IPv6 アドレス	IkePeerType	RO	
pikeTunHistPeerRemoteValue(8)	相手装置のピア識別値	DisplayString	RO	
pikeTunHistLocalAddr(9)	自装置のアドレス（IPv4/IPv6）	IPSIpAddress	RO	
pikeTunHistRemoteAddr(11)	相手装置のアドレス （IPv4/IPv6）	IPSIpAddress	RO	
pikeTunHistNegoMode(13)	Phase1 の接続モード 1.メインモード 2.アグレッシブモード	IkeNegoMode	RO	
pikeTunHistDiffHellmanGrp(14)	Diffie Hellman グループ 1.無し 2.768 ビット 3.1024 ビット 4.1536 ビット 5.2048 ビット	DiffHellmanGrp	RO	
pikeTunHistEncryptAlgo(15)	暗号化アルゴリズム 1.無し 2.DES 3.3DES 4.AES	EncryptAlgo	RO	
pikeTunHistHashAlgo(16)	ハッシュアルゴリズム 1.無し 2.MD5 3.SHA-1	IkeHashAlgo	RO	
pikeTunHistAuthMethod(17)	認証方法 1.無し 2.pre-sharedkey	IkeAuthMethod	RO	
pikeTunHistLifeTime(18)	Phase1 SA のライフタイム （単位：秒）	INTEGER	RO	
pikeTunHistStartTime(19)	Phase1 SA の開始時間 （sysUpTime）	TimeStamp	RO	
pikeTunHistActiveTime(20)	Phase1 SA の接続時間 （単位：1/100 秒）	TimeInterval	RO	
pikeTunHistInNotifys(26)	Notify 受信数	Counter	RO	
pikeTunHistInP2Exchgs(27)	Phase2 交換受信数	Counter	RO	
pikeTunHistInP2ExchgInvalids(28)	不正な Phase2 交換受信数	Counter	RO	

pikeTunHistInP2ExchgRejects(29)	自装置で拒絶した Phase2 交換受信数	Counter	RO	
pikeTunHistInP2SaDelRequests(30)	SA 削除要求受信数	Counter	RO	
pikeTunHistOutNotifys(34)	Notify 送信数	Counter	RO	
pikeTunHistOutP2Exchgs(35)	Phase2 交換送信数	Counter	RO	
pikeTunHistOutP2ExchgInvalids(36)	不正な Phase2 交換送信数	Counter	RO	
pikeTunHistOutP2ExchgRejects(37)	相手装置で拒絶された Phase2 交換送信数	Counter	RO	
pikeTunHistOutP2SaDelRequests(38)	SA 削除要求送信数	Counter	RO	

(i) Phase2 履歴情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIpSecFlowMonitorMIB(3).pipSecMIBObjects(1).
  pipSecHistory(4). pipSecHistPhaseTwo(3). pipSecTunnelHistTable(1).
  pipSecTunnelHistEntry(1)

- インデックス：
  pipSecTunHistIndex(1):IPsec ヒストリインデックス

オブジェクト名	内容	SYNTAX	R/W	備考
pipSecTunHistIndex (1)	インデックス	INTEGER	不可	
pipSecTunHistTermReason (2)	トンネル終了理由 1.その他（下記以外） 2.正常終了 3.コマンドによる終了 4.相手装置からの削除	INTEGER	RO	
pipSecTunHistActiveIndex (3)	Phase2 インデックス	INTEGER	RO	
pipSecTunHistIkeTunnelIndex(4)	Phase2 接続時に使用した Phase1 インデックス	INTEGER	RO	
pipSecTunHistLocalAddr(5)	自装置の IP アドレス（IPv4/IPv6）	IPSIpAddress	RO	
pipSecTunHistRemoteAddr(6)	相手装置の IP アドレス（IPv4/IPv6）	IPSIpAddress	RO	
pipSecTunHistKeyType(7)	鍵種別 1.自動鍵 2.固定鍵	KeyType	RO	
pipSecTunHistEncapMode(8)	カプセル化モード 1.トンネル 2.トランスポート	EncapMode	RO	
pipSecTunHistLifeSize(9)	トンネルのライフサイズ（単位：キロバイト）	INTEGER	RO	
pipSecTunHistLifeTime(10)	トンネルのライフタイム（単位：秒）	INTEGER	RO	
pipSecTunHistStartTime(11)	トンネルの開始時間（sysUpTime）	TimeStamp	RO	
pipSecTunHistActiveTime(12)	トンネルの接続時間（単位：1/100 秒）	TimeInterval	RO	
pipSecTunHistTotalRefreshes(13)	SA のリフレッシュ回数	Counter	RO	
pipSecTunHistInSaDiffHellmanGrp(15)	受信方向 DH グループ 1.無し 2.768 ビット 3.1024 ビット 4.1536 ビット 5.2048 ビット	DiffHellmanGrp	RO	
pipSecTunHistInSaEncryptAlgo(16)	受信方向暗号化方法 1.無し 2.DES 3.3DES 4.AES	EncryptAlgo	RO	
pipSecTunHistInSaAhAuthAlgo(17)	受信方向 AH 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	

pipSecTunHistInSaEspAuthAlgo(18)	受信方向 ESP 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	
pipSecTunHistOutSaDiffHellmanGrp (20)	送信方向 DH グループ 1.無し 2.768 ビット 3.1024 ビット 4.1536 ビット 5.2048 ビット	DiffHellmanGrp	RO	
pipSecTunHistOutSaEncryptAlgo (21)	送信方向暗号化方法 1.無し 2.DES 3.3DES 4.AES	EncryptAlgo	RO	
pipSecTunHistOutSaAhAuthAlgo(22)	送信方向 AH 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	
pipSecTunHistOutSaEspAuthAlgo(23)	送信方向 ESP 認証方法 1.無し 2.HMAC-MD5 3.HMAC-SHA-1	AuthAlgo	RO	
pipSecTunHistPmtu(25)	パス MTU サイズ	INTEGER	RO	
pipSecTunHistInOctets(26)	受信オクテット数	Counter	RO	
pipSecTunHistInPkts(32)	受信パケット数	Counter	RO	
pipSecTunHistInDropPkts(33)	受信時のパケット廃棄数（Anti-Replay による廃棄は除く）	Counter	RO	
pipSecTunHistInReplayDropPkts(34)	Anti-Replay によるパケット廃棄数	Counter	RO	
pipSecTunHistInAuths(35)	受信時の認証回数	Counter	RO	
pipSecTunHistInAuthFails(36)	受信時の認証失敗回数	Counter	RO	
pipSecTunHistInDecrypts(37)	受信時の復号回数	Counter	RO	
pipSecTunHistInDecryptFails(38)	受信時の復号失敗回数	Counter	RO	
pipSecTunHistOutOctets(39)	送信オクテット数	Counter	RO	
pipSecTunHistOutPkts(45)	送信パケット数	Counter	RO	
pipSecTunHistOutDropPkts(46)	送信時のパケット廃棄数	Counter	RO	
pipSecTunHistOutAuths(47)	送信時の認証回数	Counter	RO	
pipSecTunHistOutAuthFails(48)	送信時の認証失敗回数	Counter	RO	
pipSecTunHistOutEncrypts(49)	送信時の暗号回数	Counter	RO	
pipSecTunHistOutEncryptFails (50)	送信時の暗号失敗回数	Counter	RO	

ログイン状態 MIB

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib (84). picoLoginMIB (4). picoLoginSessionTable (1).
  picoLoginSessionEntry(1)

- インデックス：picoLoginSessionIndex(1)：ログイン ID

オブジェクト名	内容	SYNTAX	R/W	備考
picoLoginSessionIndex(1)	ログイン ID(1- 2147483647)	INTEGER	N/A	
picoLoginSessionStatus(2)	ログイン状態 1. ログイン 2. ログアウト 3. ログイン失敗	INTEGER	RO	
picoLoginSessionPrivilege(3)	ユーザ権限 1. administrator 2. monitor 3. operator 4. unknown	INTEGER	RO	
picoLoginSessionProcessMode(4)	モード状態 1. operation 2. configure	INTEGER	RO	
picoLoginSessionTerminalType(5)	ターミナル種別 1. unknown 2. console/local(*1) 3. telnet/remote(*1) *1 MIB ファイル R10.1 以降	INTEGER	RO	
picoLoginSessionPeerIpAddress(6)	接続元アドレス（IPv4）	IpAddress	RO	
picoLoginSessionPeerIpv6Address(7)	接続元アドレス（IPv6）	Ipv6Address	RO	

コンフィグ状態 MIB

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib (84). picoConfigEventMIB (5)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoConfigType (1)	コンフィグ種別 1. default-config 2. startup-config 3. unknown	INTEGER	N/A	
picoConfigEventType (2)	イベント種別 1. 変更 2. 削除	INTEGER	N/A	

SW-HUB カード用 MIB

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib (84). picoExtIfMIB (6). picoExtIfTable(1). picoExtIfEntry(1)

- インデックス：picoExtIfInstalledSlot(1)：スロット番号
  picoExtIfIndex(2)　　：ポート番号

オブジェクト名	内容	SYNTAX	R/W	備考
picoExtIfInstalledSlot(1)	スロット番号	INTEGER	N/A	
picoExtIfIndex(2)	ポート番号	INTEGER	N/A	
picoExtIfDescr(3)	属するインタフェース名	DisplayString	RO	
picoExtIfUpperLayer(4)	属するインタフェースの ifIndex	INTEGER	RO	
picoExtIfType(5)	インタフェース種別	INTEGER	RO	
picoExtIfSpeed(6)	ポートスピード	INTEGER	RO	
picoExtIfDuplex(7)	Duplex 1. halfduplex 2. fullduplex	INTEGER	RO	
picoExtIfEffectiveMtu(8)	属するインタフェースの MTU	INTEGER	RO	
picoExtIfPhysicalAddress(9)	MAC アドレス	PhysAddress	RO	
picoExtIfAdminStatus(10)	管理状態 1. up 2. down 3. testing	INTEGER	RO	
picoExtIfOperStatus(11)	運用状態 1. up 2. down 3. testing	INTEGER	RO	
picoExtIfLastChange(12)	ステータス変更時間	TimeStamp	RO	

ネットワークモニタ MIB

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib (84). picoNetworkMonitorMIB (7). picoNetmonMibObjects(1).
  picoNetmonWatchgroupTable(1). picoNetmonWatchgroupEntry(1)

- インデックス：picoNetmonWatchgroupIndex(1)：Watch グループインデックス

オブジェクト名	内容	SYNTAX	R/W	備考
picoNetmonWatchgroupIndex (1)	インデックス	INTEGER	N/A	
picoNetmonWatchgroupName (2)	Watch グループ名	DisplayString	RO	
picoNetmonWatchgroupSequenceNumber (3)	シーケンス番号	INTEGER	RO	
picoNetmonWatchgroupStatus (4)	状態 1.正常 2.障害中 3.停止中	INTEGER	RO	
picoNetmonWatchgroupVarianceCounts (5)	障害発生回数	INTEGER	RO	

NGN MIB（Ver.8.7 以降）

(a) UNI 情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib(84). picoNgnMIB(9). picoNgnMIBObjects (1).
  picoNgnTable (1). picoNgnEntry (1)

- インデックス：picoNgnIfIndex (1)：

オブジェクト名	内容	SYNTAX	R/W	備考
picoNgnIfIndex (1)	インデックス	INTEGER	N/A	
picoNgnType (2)	NGN 回線種別 1.通常回線 2.ナンバーゲート回線	INTEGER	RO	
picoNgnIfType (3)	NGN インタフェース種別 1.グローバル接続 2.プライベート接続	INTEGER	RO	
picoNgnStatus (4)	状態 1.NGN サービス未作動 2.初期化中 3.登録中 4.登録完了	INTEGER	RO	
picoNgnSipServerIpAddress (5)	SIP サーバアドレス(IPv4)	IpAddress	RO	
picoNgnSipUri(6)	SIP URI	DisplayString	RO	
picoNgnUpTime (7)	SIP 登録経過時間	TimeTicks	RO	

(b) VPN 接続情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib(84). picoNgnMIB(9). picoNgnMIBObjects (1).
  picoNgnVpnTable (2). picoNgnVpnEntry (1)

- インデックス：picoNgnVpnIfIndex (1)：

オブジェクト名	内容	SYNTAX	R/W	備考
picoNgnVpnIfIndex (1)	インデックス	INTEGER	N/A	
picoNgnVpnStatus (2)	セッション状態 1.切断 2.接続処理中 3.接続完了	INTEGER	RO	
picoNgnVpnPeerAddress (3)	接続先電話番号	DisplayString	RO	
picoNgnVpnBandwidth (4)	接続帯域情報	INTEGER	RO	
picoNgnVpnUsedTime (5)	接続経過時間	TimeTicks	RO	
picoNgnVpnSbcIpAddress (6)	SBC IPv4 アドレス	IpAddress	RO	
picoNgnVpnSbcPort(7)	SBC ポート番号	INTEGER	RO	

起動時ハードウェア自己診断 MIB（Ver.8.11 以降）

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib(84).picoPostMIB(10).picoPostMIBObjects(1)
  picoPostTable (1). picoPostEntry (1).

- インデックス：picoPostIndex (1)：

オブジェクト名	内容	SYNTAX	R/W	備考
picoPostIndex (1)	インデックス	INTEGER	RO	
picoPostFail (2)	診断 NG 内容	DisplayString	RO	

無線 WAN MIB（Ver.9.2 以降）

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3). pico-mib(84). picoMobileMIB (11). picoMobileMIBObjects (1).
  picoMobileDeviceTable (1). picoMobileDeviceEntry (1)

- インデックス：picoMobileDeviceIndex (1)：

オブジェクト名	内容	SYNTAX	R/W	備考
picoMobileDeviceIndex (1)	インデックス（1,2）	INTEGER	不可	
picoMobileDeviceVendorName (2)	端末製造会社名	DisplayString	RO	
picoMobileDeviceName (3)	データ通信端末名	DisplayString	RO	
picoMobileDeviceProductID (4)	データ通信端末製造番号	DisplayString	RO	
picoMobileDeviceSoftwareVersion (5)	端末ファームウェア バージョン	DisplayString	RO	
picoMobileDeviceSignalBar (6)	アンテナ本数	INTEGER	RO	
picoMobileDeviceSignalStrength (7)	電波強度 -1.不明 0. 圏外（電波強度 0） 1. 微弱（電波強度 1） 2. 弱　（電波強度 2） 3. 強　（電波強度 3）	INTEGER	RO	
picoMobileDeviceSignalQuality (8)	電波強度値	DisplayString	RO	
picoMobileDeviceSignalElapsedTime (9)	電波状態読出後経過時間	TimeTicks	RO	
picoMobileDeviceRadioInterface (10)	接続回線種別	DisplayString	RO	
picoMobileDeviceCarrier (11)	キャリア名	DisplayString	RO	
picoMobileDeviceDialerString (12)	自局電話番号	DisplayString	RO	
picoMobileDeviceDialStatus (13)	ダイヤル接続状態 0. 未接続 1. 接続手続き中 2. 接続中断中 3. 通信中 4. 切断処理中	INTEGER	RO	
picoMobileDeviceInRangeCounts (14)	圏内になった回数	Gauge	RO	
picoMobileDeviceOutRangeCounts (15)	圏外状態になった回数	Gauge	RO	
picoMobileDeviceResetCounts (16)	端末リセット回数	Gauge	RO	

キャッシュ MIB（Ver.9.6 以降）

(a) IPv4 ルートキャッシュ情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIPv4MIB(12).picoIPv4Cache(1)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoIPv4CacheEntries (1)	有効キャッシュ数	Gauge	RO	
picoIPv4CachePeaks (2)	キャッシュピーク値	Gauge	RO	
picoIPv4CacheCreates (3)	キャッシュ作成数	Counter	RO	
picoIPv4CacheOverflows (4)	キャッシュオーバフロー数	Counter	RO	

(b) IPv4 UFS キャッシュ情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIPv4MIB(12).picoIPv4UFSCache(2)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoIPv4UFSCacheEntries (1)	有効 UFS キャッシュ数	Gauge	RO	
picoIPv4UFSCachePeaks (2)	UFS キャッシュピーク値	Gauge	RO	
picoIPv4UFSCacheCreates (3)	UFS キャッシュ作成数	Counter	RO	
picoIPv4UFSCacheOverflows (4)	UFS キャッシュオーバフロー数	Counter	RO	

(c) IPv6 ルートキャッシュ情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIPv6MIB(13).picoIPv6Cache(1)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoIPv6CacheEntries (1)	有効キャッシュ数	Gauge	RO	
picoIPv6CachePeaks (2)	キャッシュピーク値	Gauge	RO	
picoIPv6CacheCreates (3)	キャッシュ作成数	Counter	RO	
picoIPv6CacheOverflows (4)	キャッシュオーバフロー数	Counter	RO	

(d) IPv6 UFS キャッシュ情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoIPv6MIB(13).picoIPv6UFSCache(2)

- インデックス：無し

オブジェクト名	内容	SYNTAX	R/W	備考
picoIPv6UFSCacheEntries (1)	有効 UFS キャッシュ数	Gauge	RO	
picoIPv6UFSCachePeaks (2)	UFS キャッシュピーク値	Gauge	RO	
picoIPv6UFSCacheCreates (3)	UFS キャッシュ作成数	Counter	RO	
picoIPv6UFSCacheOverflows (4)	UFS キャッシュオーバフロー数	Counter	RO	

QoS MIB（Ver.10.2 以降）

(a) QoS Policy-map 情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoQoSMIB(14).qosPolicyTable(1).qosPolicyEntry(1)

- インデックス：qosPolicyIfIndex (1)

オブジェクト名	内容	SYNTAX	R/W	備考
qosPolicyIfIndex (1)	インタフェースの ifIndex	INTEGER	N/A	
qosPolicyName (2)	Policy-map 名	DisplayString	RO	

(b) QoS Class-map 情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoQoSMIB(14).qosClassTable(2).qosClassEntry(1)

- インデックス：qosClassIfIndex (1)
  qosClassIndex (2)

オブジェクト名	内容	SYNTAX	R/W	備考
qosClassIfIndex (1)	インタフェースの ifIndex	INTEGER	N/A	
qosClassIndex (2)	通し番号（自動採番）	INTEGER	N/A	
qosClassName (3)	Class 名	DisplayString	RO	
qosClassType (4)	Class タイプ	INTEGER	RO	
qosClassBandwidth (5)	Class 帯域	INTEGER	RO	
qosClassBandwidthUnit (6)	Class 帯域形式	INTEGER	RO	
qosClassBitRate (7)	Class の Shaping 値	INTEGER	RO	
qosClassEnqPkts (8)	Class 内の Queue に積まれたパケット数の合計	Counter64	RO	
qosClassEnqBytes (9)	Class 内の Queue に積まれたバイト数の合計	Counter64	RO	
qosClassDeqPkts (10)	Class 内の Queue から送信したパケット数の合計	Counter64	RO	
qosClassDeqBytes (11)	Class 内の Queue から送信したバイト数の合計	Counter64	RO	
qosClassDropPkts (12)	Class 内の破棄したパケット数の合計	Counter64	RO	
qosClassDropBytes (13)	Class 内の破棄したバイト数の合計	Counter64	RO	

(c) QoS Queue 情報

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).picoQoSMIB(14).qosQueueTable(3).qosQueueEntry(1)

- インデックス：qosQueueIfIndex (1)
  qosQueueClassIndex (2)
  qosQueueQueueIndex (3)

オブジェクト名	内容	SYNTAX	R/W	備考
qosQueueIfIndex (1)	インタフェースの ifIndex	INTEGER	N/A	
qosQueueClassIndex (2)	通し番号（自動採番）	INTEGER	N/A	
qosQueueQueueIndex (3)	Queue の優先度 1: high 2: medium 3: normal	INTEGER	N/A	

	4: low 5: sub-a 6: sub-b 7: sub-c 8: sub-d			
qosQueueEnqPkts (4)	Queue に積まれたパケット数の合計	Counter64	RO	
qosQueueEnqBytes (5)	Queue に積まれたバイト数の合計	Counter64	RO	
qosQueueDeqPkts (6)	Queue から送信したパケット数の合計	Counter64	RO	
qosQueueDeqBytes (7)	Queue から送信したバイト数の合計	Counter64	RO	
qosQueueDropPkts (8)	Queue で破棄したパケット数の合計	Counter64	RO	
qosQueueDropBytes (9)	Queue で破棄したバイト数の合計	Counter64	RO	

NAPT キャッシュ MIB（Ver.10.2 以降）

- オブジェクトツリー
  .iso(1).org(3).dod(6).internet(1).private(4).enterprise(1).nec(119).nec-mib(2).
  necProductDepend(3).pico-mib(84).
  picoNAPTMIB(15).picoNAPTMIBObjects(1).naptCacheTable(1).naptCacheEntry(1)

- インデックス：naptCacheIfIndex (1)

オブジェクト名	内容	SYNTAX	R/W	備考
naptCacheIfIndex (1)	インタフェースの ifIndex	INTEGER	N/A	
naptCacheEntries (2)	有効キャッシュ数	Gauge	RO	
naptCachePeak (3)	キャッシュピーク値	Gauge	RO	
naptCacheCreates (4)	キャッシュ作成数	Counter	RO	
naptCacheOverflows (5)	キャッシュオーバフロー数	Counter	RO	

■14.16 Trap 詳細

Generic Trap

- SNMPv1

ID	Trap 名	VARIABLES	発行契機
0	cold-start	無し	電源投入 再起動（reload） リスタート（restart） ライセンス期限切れ クラッシュ
2	link-down	ifIndex ifDescr（設定時、Ver.7.4 以降）	インタフェースダウン
3	link-up	ifIndex ifDescr（設定時、Ver.7.4 以降）	インタフェースアップ
4	authentication-failure	無し	Community 名が間違っている

- SNMPv2c/SNMPv3
  - (1.3.6.1.6.3.1.1.5.)

ID	Trap 名	VARIABLES	発行契機
1	cold-start	無し	電源投入 再起動（reload） リスタート（restart） ライセンス期限切れ クラッシュ
3	link-down	ifIndex ifAdminStaus※1 ifOperStatus※1 ifDescr（設定時、Ver.7.4 以降）	インタフェースダウン ※1 Ver.9.4 以降
4	link-up	ifIndex ifAdminStatus※1 ifOperStatus※1 ifDescr（設定時、Ver.7.4 以降）	インタフェースアップ ※1 Ver.9.4 以降
5	authentication-failure	無し	Community 名が間違っている

Specific Trap

(a) システムトラップ

- SNMPv1
  - ENTERPRISE:pico（1.3.6.1.4.1.119.1.84）
- SNMPv2c/SNMPv3
  - ENTERPRISE:pico（1.3.6.1.4.1.119.1.84.0）

ID	Trap 名	VARIABLES	発行契機
3	picoTemperatureFault	無し	温度アラーム発生時
4	picoTemperatureRestoration	無し	温度アラーム復旧時
5	picoVoltageFault	無し	電圧が±10%の範囲外になった時
6	picoVoltageRestoration	無し	電圧が±10%の範囲内に復旧した時
7	picoFanFault	picoFanIndex	5 秒間隔でポーリングし 3 回連続 5294 回転/分以下になった時
8	picoFanRestoration	picoFanIndex	5295 回転/分以上に復旧した時
9	picoPowerSupplyFault	picoPowerSupplyIndex picoPowerSupplyType	電源障害発生時 電源 OFF 時
10	picoPowerSupplyRestoration	picoPowerSupplyIndex picoPowerSupplyType	電源障害復旧時 電源 ON 時
11	picoPowerSupplyInserted	picoPowerSupplyIndex picoPowerSupplyType	電源ユニットを挿入した時
12	picoPowerSupplyRemoved	picoPowerSupplyIndex picoPowerSupplyType	電源ユニットを抜去した時
13	picoLoginSession	picoLoginSessionStatus picoLoginSessionPrivilege picoLoginSessionTerminalType picoLoginSessionPeerIpAddress picoLoginSessionPeerIpv6Address	ログイン/ログアウト時
14	picoLoginFailure	picoLoginSessionStatus picoLoginSessionPrivilege picoLoginSessionTerminalType picoLoginSessionPeerIpAddress picoLoginSessionPeerIpv6Address	ログイン失敗時
15	picoConfigMode	picoLoginSessionProcessMode picoLoginSessionTerminalType picoLoginSessionPeerIpAddress picoLoginSessionPeerIpv6Address	モード変更時 configure termial,enable exit（オペレーションモード移行時)
16	picoConfigModified	picoConfigType picoConfigEventType picoLoginSessionTerminalType picoLoginSessionPeerIpAddress picoLoginSessionPeerIpv6Address	コンフィグ変更/削除時 write memory,erase
17	picoExtIfLinkDown	picoExtIfAdminStatus picoExtIfOperStatus	SW-HUB ポート down
18	picoExtIfLinkUp	picoExtIfAdminStatus picoExtIfOperStatus	SW-HUB ポート up

(b)IPsec トラップ

- SNMPv1
  - ENTERPRISE:pipSecMIBNotificationPrefix（1.3.6.1.4.1.119.2.3.84.3.2）
- SNMPv2c/SNMPv3
  - ENTERPRISE: pipSecMIBNotifications（1.3.6.1.4.1.119.2.3.84.3.2.0）

ID	Trap 名	VARIABLES	発行契機
1	pikeTunnelStart	pikePeerLocalAddr pikePeerRemoteAddr pikeTunLifeTime	IKE-SA(Phase1 SA)確立時
2	pikeTunnelStop	pikeTunHistTermReason pikePeerLocalAddr pikePeerRemoteAddr pikeTunActiveTime	IKE-SA(Phase1 SA)削除時 1.下記 2～4 以外 - キープアライブのフェイルアウト - インタフェースのアドレス変更 2.LifeTime 満了時 3.CLI による削除時 4.DELETE メッセージ受信時

7	pipSecTunnelStart	pipSecTunLifeTime pipSecTunLifeSize	IPSEC-SA(Phase2 SA)確立時 （注）リキーによる再接続時は未発行
8	pipSecTunnelStop	pipSecTunHistTermReason pipSecTunActiveTime	IPSEC-SA(Phase2 SA)削除時 1.下記 2～5 以外 - キープアライブのフェイルアウト - インタフェースのアドレス変更 - INITIAL-CONTACT 受信 - シーケンス番号が 1 周した時 - ネットワークモニタ等外部からの削除 2.LifeTime 満了時 3.CLI による削除時 4.DELETE メッセージ受信時 5. IPsec SA のリキー失敗時 ※リキー時は発行しません。
11	pipSecEarlyTunTerm	pipSecTunActiveTime pipSecSpiProtocol	IPSEC-SA(Phase2 SA)の異常削除時 - キープアライブのフェイルアウト - インタフェースのアドレス変更 - INITIAL-CONTACT 受信 - シーケンス番号が 1 周した時 - DELETE メッセージ受信時 - IPsec SA のリキー失敗時 ※リキー時は発行しません

(c) ネットワークモニタトラップ（Ver.7.1 以降）

- SNMPv1
  - ENTERPRISE: picoNetmonMIBNotificationPrefix（1.3.6.1.4.1.119.2.3.84.7.2）
- SNMPv2c/SNMPv3
  - ENTERPRISE: picoNetmonMIBNotifications（1.3.6.1.4.1.119.2.3.84.7.2.0）

ID	Trap 名	VARIABLES	発行契機
1	picoNetMonWatchGroupStatusChange	picoNetmonWatchgroupName picoNetmonWatchgroupSequenceNumber picoNetmonWatchgroupStatus	ネットワークモニタの状態が変更になった時

(d) VRRP トラップ

- SNMPv1
  - ENTERPRISE: vrrpNotifications（1.3.6.1.2.1.68.0）
- SNMPv2c/SNMPv3
  - ENTERPRISE: vrrpNotifications（1.3.6.1.2.1.68.0.0）

ID	Trap 名	VARIABLES	発行契機
1	vrrpTrapNewMaster	vrrpOperMasterIpAddr	新しく MASTER になった時
2	vrrpTrapAuthFailure	vrrpTrapPacketSrc vrrpTrapAuthErrorType	VRRP の認証失敗時

(e) ISDN トラップ（Ver.8.6 以降）

- SNMPv1
  - ENTERPRISE: picoIsdnMIBNotificationPrefix（1.3.6.1.4.1.119.2.3.84.8.2）
- SNMPv2c/SNMPv3
  - ENTERPRISE: picoIsdnMIBNotifications（1.3.6.1.4.1.119.2.3.84.8.2.0）

ID	Trap 名	VARIABLES	発行契機
1	picoIsdnLapdOperStatusChange	ifIndex isdnLapdOperStatus	ISDN LAPD 状態が変更になった時

(f) 起動時ハードウェア自己診断 NG トラップ（Ver.8.11 以降）

- SNMPv1
  - ENTERPRISE: picoPOSTNotificationPrefix（1.3.6.1.4.1.119.2.3.84.10.2）
- SNMPv2c/SNMPv3
  - ENTERPRISE: picoPOSTNotifications（1.3.6.1.4.1.119.2.3.84.10.2.0）

ID	Trap 名	VARIABLES	発行契機
1	picoPostFailMessage	picoPostFail	起動時の自己診断で NG があった場合

(g) USB 無線 WAN トラップ（Ver.9.3 以降）

- SNMPv1
  - ENTERPRISE: picoMobileMIBNotificationPrefix（1.3.6.1.4.1.119.2.3.84.11.2.0）
- SNMPv2c/SNMPv3
  - ENTERPRISE: picoMobileMIBNotifications（1.3.6.1.4.1.119.2.3.84.11.2.0）

ID	Trap 名	VARIABLES	発行契機
1	picoMobileDeviceDown	picoMobileDeviceIndex picoMobileDeviceName	データ通信端末が USB ポートから抜去
2	picoMobileDeviceUp	picoMobileDeviceIndex picoMobileDeviceName	データ通信端末が USB ポートに挿入
3	picoMobileSignalStatusChange	picoMobileDeviceIndex picoMobileDeviceSignalBar picoMobileDeviceSignalStrength picoMobileDeviceSignalQuality picoMobileDeviceRadioInterface	以下の状態が変化 電波状態 電波強度 接続回線種別

■14.17 ISDN 切断理由コード一覧

ISDN 関連の show コマンド（show dialer device、show isdn history 等）では、ISDN 切断時の切断理由として Q.931 で定義されているコードが表示されます。

Ver.8.6 以降、独自の拡張切断要因も表示されます。

(a) 切断理由コード

code		表示	規約の内容	補足
DEC	HEX			
1	0x1	Unassigned number	未使用番号	
2	0x2	No route to specified transit network	指定中継網へのルートなし	
3	0x3	No route to destination	相手へのルートなし	
6	0x6	Channel unacceptable	チャンネル利用不可	
7	0x7	Call awarded in an established channel	呼が設定済のチャンネルへ着呼	
16	0x10	Normal call clearing	正常切断	
17	0x11	User busy	着ユーザビジー	
18	0x12	No user responding	着ユーザレスポンスなし 一定時間内に"呼出中","応答"が返ってこない	
19	0x13	User alerting, no answer	着ユーザ応答なし "呼出"の通知はあったがその後の応答が返ってこない	
20	0x14	Unknown	加入者不在	
21	0x15	Call Rejected	通信拒否 呼の受付が可能であるにもかかわらず、呼を受け付けない	発信者番号認証失敗、 発信専用の設定時に着信した場合などに発生
22	0x16	Number changed	相手加入者番号変更 着信番号が使用されていない	
26	0x1a	Non-selected user clearing	選択されなかったユーザの切断復旧 着信呼を得られなかった	
27	0x1b	Destination out of order	着側インタフェース起動不可 着信側インタフェースが正常でないため着信できない	
28	0x1c	Invalid number format	無効番号フォーマット 着信番号が無効なフォーマットのため着信できない	
29	0x1d	Facility rejected	ファシリティ拒否 要求されたファシリティが、網で提供できない	
30	0x1e	Response to STATUS ENQUIRY	状態問い合わせの応答	
31	0x1f	Destination is out of order	その他の正常クラス	
34	0x22	No channel/circuit available	利用可回線／チャネルなし 利用可能な回線／チャネルが現在ない	
38	0x26	Network out of order	網故障 正常でない状態が長時間は継続しそう	
41	0x29	Temporary Failure	一時的失敗 正常でない状態が長時間は継続しそうもない	
42	0x2a	Switching Equipment Congestion	交換機輻輳 交換装置が輻輳している	
43	0x2b	Access information discarded	アクセス情報廃棄 要求したアクセス情報が相手に届けられなかった	
44	0x2c	Requested channel not available	要求回線／チャネル利用不可 通知された回線／チャネルが相手側インタフェースで提供できない	
47	0x2f	Resource unavailable, unspecified	その他のリソース使用不可クラス	

49	0x31	Unknown	サービス品質（QOS）利用不可 要求された QOS が提供されない	
50	0x32	Requested facility not subscribed	要求ファシリティ未契約 手続きが終了していないため要求された付加サービスが提供されない	
57	0x39	Bearer Capability not authorized	伝達能力不許可 メッセージを送信した装置が、許可していない伝達能力を要求した	
58	0x3a	Bearer capability not presently available	現在利用不可伝達能力 メッセージを送信した装置が現在利用不可の伝達能力を要求した	
63	0x3f	Service not available, unspecified	その他のサービスまたはオプションの利用不可クラス	
65	0x41	Bearer Capability not implemented	未提供伝達能力指定 メッセージを送信した装置が要求された伝達能力をサポートしていない	
66	0x42	Channel type not implemented	未提供チャンネル種別指定 メッセージを送信した装置が要求されたチャンネル種別をサポートしていない	
69	0x45	Requested facility not implemented	未提供ファシリティ要求 メッセージを送信した装置が要求された付加サービスを提供していない	
70	0x46	Only restricted digital information is available	制限ディジタル情報伝達能力のみ可能 メッセージを送信した装置が、要求された伝達能力のうち制限ディジタル情報伝達能力のみをサポートしている	
79	0x4f	Service not implemented, unspecified	その他のサービスまたはオプションの未提供クラス	
81	0x51	Invalid Call Reference Value	無効呼番号値使用 メッセージを送信した装置が使用中のものと異なる呼番号のメッセージを受信した	
82	0x52	Identified channel does not exist	無効チャネル番号使用 活性化していないチャネル番号の使用要求を受信	
83	0x53	A suspended call exists, but call identity does not	指定された中断呼識別番号未使用 中断された呼に用いられていた呼識別番号と異なる呼識別番号を持つ呼の再開が試された	
84	0x54	Call identity in use	中断呼識別番号使用中 網が呼の中断要求を受信したが、すでに使用中の呼識別を含んでいる	
85	0x55	No call suspended	中断呼なし 網が呼の再開要求を受信	
86	0x56	Requested call identity has been cleared	指定中断呼切断復旧済 網が再開要求を受信したが既に切断復旧している	
87	0x57	Unknown	ユーザは CUG のメンバでない	
88	0x58	Incompatible destination	端末属性不一致 適合しない整合性属性をもつ呼設定の要求を受信した	音声着信の場合などに発生
91	0x5b	Invalid transit network selection	無効中継網選択 中継網識別のフォーマットが正しくない	
95	0x5f	Invalid message , unspecified	その他の無効メッセージクラス	
96	0x60	Mandatory Information Element is missing	必須情報要素不足 メッセージを送信した装置が必要な情報が不足するメッセージを受信した	
97	0x61	Message type non-existent	メッセージ種別未定義または未提供 メッセージを送信した装置が未定義のメッセージを受信した	
98	0x62	Message not compatible with call state or message type non-existent	呼状態とメッセージ不一致又はメッセージ種別未定義または未提供 メッセージを送信した装置が整合していない呼状態になっている	
99	0x63	Information element non-existent	情報要素未定又は未提供 受信した情報要素識別子が未定義	

100	0x64	Invalid information element contents	情報要素内容無効 受信した情報要素が提供していないコード	
101	0x65	Message not compatible with call state	呼状態とメッセージ不一致 受信したメッセージと呼状態が不一致	
102	0x66	Recovery on time expiry	タイマ満了による回復	
111	0x6f	Protocol Error, Unspecified	その他の手順誤りクラス	
127	0x7f	Interworking, Unspecified	その他のインタワーキングクラス レイヤ 1 ダウン	

(b) 拡張切断要因

code	表示	内容	補足
10	L1 Down	自装置の L1Down による切断/接続失敗	
11	L2 Down	自装置の L2Down による切断/接続失敗	
12	ISDN net disconnected	網からの切断/接続失敗	
13	Calling address auth failed	発信者番号認証 NG による切断/接続失敗	
14	Device internal error	内部エラーによる切断/接続失敗	
15	Channel unavailable	自装置側のチャネル利用不可による切断/接続失敗	
16	Invalid message	受信メッセージエラーによる切断/接続失敗	
17	No resources	自装置側リソース無しによる切断/接続失敗	
18	Unexpected message	期待しないメッセージ受信による切断/接続失敗	
19	Dest phone number error	自装置からの発信時、宛先電話番号エラーによる切断/接続失敗	
20	Redial restriction	再発信規制による発信拒否	
21	Disconnect timer expired	切断処理中の切断応答待ちタイマ満了 (T305 タイマ満了)	
22	Disconnect response timer expired	解放処理中の解放応答待ちタイマ満了 (T308 タイマ満了)	
23	Outbound call timer expired	発呼処理中の発呼応答待ちタイマ満了	
24	Inbound call timer expired	着呼処理中の着呼完了応答待ちタイマ満了	
25	Inbound call timer expired(T313)	着呼処理中の着呼完了応答待ちタイマ満了 (T313 タイマ満了)	
26	Upper layer call rejected	上位レイヤへの着信認証で着信拒否	
27	Dialer call rejected	Dialer で着信拒否	
79	Request from upper layer	上位レイヤからの要求	
80	MUXISDN disconnected	MUXISDN で切断	
81	MUXISDN call failed	MUXISDN で接続失敗	
82	Dialer disconnected for priority-call	優先呼による切断	
83	PPP call cancel(no lcp link)	接続中の LCP がなくなったので、発呼中の呼をキャンセル	
99	Request from upper layer (MUXISDN)	上位レイヤからの要求	
100	PPP disconnected	PPP(LCP)で切断	
101	PPP call failed	PPP(LCP)で接続失敗	
102	PPP disconnected(timeout)	PPP(LCP)のタイムアウトによる切断	
103	PPP Send CONF-REQ retry over	コンフィグリクエストの再送オーバーによる切断	
104	PPP call failed (auth error)	PPP(LCP)の認証失敗による切断	
105	PPP call failed (internal error)	PPP(LCP)の内部エラーによる切断	
106	PPP Receive TERM-REQ	PPP(LCP)の TERM-REQ 受信による切断	
107	PPP Receive CODE-REJ	PPP(LCP)の CODE-REJ 受信による切断	
108	PPP Receive PROT-REJ	PPP(LCP)の PROT-REJ 受信による切断	
109	Dialer on-demand disconnected	オンデマンド接続による切断	
110	PPP echo keepalive failed	エコーキープアライブによる切断	
111	PPP call failed (bundle error)	PPP のバンドル失敗による切断	
112	PPP Receive	PPP(LCP)の不正なタイミングでの CONFIGURE 受信による切断	
113	PPP call failed (nego error)	PPP(LCP)のネゴシエーション失敗による切断	
149	Request from upper	上位レイヤからの要求	
150	PPP disconnected	PPP(NCP)で切断	

151	PPP call failed	PPP(NCP)で接続失敗	
152	PPP disconnected (timeout)	PPP(NCP)のタイムアウトによる切断	
153	PPP Send CONF-REQ retry over	PPP(NCP)のネゴシエーション失敗による切断	
154	PPP call failed (auth error)	PPP(NCP)の認証失敗による切断	
155	PPP call failed (internal error)	PPP(NCP)の内部エラーによる切断	
156	PPP Receive TERM-REQ	PPP(NCP)の TERM-REQ 受信による切断	
157	PPP Receive CODE-REJ	PPP(NCP)の CODE-REJ 受信による切断	
158	PPP Receive PROT-REJ	PPP(NCP)の PROT-REJ 受信による切断	
159	PPP unset ip address disconnected	IP アドレス未取得による切断	
160	PPP Receive unexpected message	PPP(NCP)の不正なタイミングでの CONFIGURE 受信による切断	
199	Request from upper layer (PPP NCP)	上位レイヤからの要求	
200	Dialer disconnected	Dialer で切断	
201	Dialer call rejected	Dialer で接続失敗	
203	Dialer idle-time disconnected	無通信時間による切断 idle-time	
204	Dialer force-time disconnected	強制切断タイマによる切断 forced-disconnect-time	
205	Dialer total-time disconnected	接続時間積算による切断 dialer total-time ～ disconnect	
206	Dialer restraint disconnected	自動発信抑止による切断 dialer restraint ～ disconnect	
254	Request from upper layer (Dialer)	上位レイヤからの要求	

■14.18 アカウンティングリスト

RADIUS サーバにアカウンティングを行った場合の出力内容を記述します。
項目名は RFC にて定義されている名称ですので、サーバの種類によって項目名は異なります。

項目名	内容	アカウンティング種別				
		exec	network	fail	resource	system
User-Name(1)	ユーザ名	○	○	○		
Acct-Status-Type(40)	状態	○	○	○	○	
Start(1)	開始	○	○		○	
Stop(2)	終了	○	○	○	○	
account-on(7)	システム起動					○
account-off(8)	システム終了					○
NAS-Port-Type(61)	インタフェース種別	○	○	○	○	
async(0)	ローカルコンソール	○		○		
sync(1)	専用線		○			
ISDN-sync(2)	ISDN		○		○	
virtual(5)	telnet	○		○		
Ethernet(15)	PPPoE		○			
NAS-Port(5)	ポート番号 telnet：TTY 番号 その他：最上位 bit='1'+ifIndex	○	○			
Acct-Terminate-Cause(49)	終了要因	○	○	○	○	
UserRequest(1)	ユーザからの要求	○	○		○	
LostCarrier(2)	回線断				○	
LostService(3)	対向装置からの終了		○			
Idle Timeout(4)	タイマのタイムアウト ログインタイマ 無通信タイマ	○	○			
Session Timeout(5)	ISDN 発信抑止		○			
User Error(17)	認証失敗			○		
Calling-Station-Id (30)	発信元番号 接続元 IP アドレス 発信元電話番号	○	○	○	○	
Called-Station-Id (31)	発信先電話番号		○		○	
Framed-IP-Address(8) Framed-Interface-Id(96)	対向装置 IP アドレス（IPv4） 対向装置インタフェース ID （IPv6）		○			
Acct-Session-Id (44)	セッション ID	○	○	○	○	○
Acct-Authentic(45)	認証方法	○	○			
RADIUS(1)	RADIUS サーバ	○	○			
Local(2)	装置内データベース	○	○			
Remote(3)						
Acct-Delay-Time (41)	ネットワークの転送時間			○		
Acct-Session-Time(46)	開始から終了までの時間	○	○		○	○
Acct-Input-Octets(43)	受信オクテット数		○			
Acct-Output-Octets(44)	送信オクテット数		○			
Acct-Input-Packets(47)	受信パケット数		○			
Acct-Output-Packets(48)	送信パケット数		○			

ローカルでアカウンティングを行った場合の項目名は RADIUS サーバに送信する場合とは異なります。ローカルでの項目名,RADIUS サーバ送信時の項目名の対応は以下の通りです。

ローカルの項目名		サーバ送信の項目名	補足
User		User-Name	
Type		ー（ローカルのみ）	アカウンティング種別
	exec	ー（ローカルのみ）	シェルサービス
	network	ー（ローカルのみ）	ネットワークサービス
	send	ー（ローカルのみ）	接続失敗
	resource	ー（ローカルのみ）	呼接続，切断
	system	ー（ローカルのみ）	システムイベント
Status		Acct-Status-Type	
Interface		NAS-Port-Type, NAS-Port	telnet 以外は実際のインタフェース名
Cause		Acct-Terminate-Cause	
Calling		Calling-Station-Id	電話番号の場合
Called		Called-Station-Id	
Remote Access		Calling-Station-Id	IP アドレスの場合
Session ID		Acct-Session-Id	
Delay		Acct-Delay-Time	
Elapsed		Acct-Session-Time	

■14.19 INS1500 サービスの利用可否

INS1500 サービスの利用可否は、以下のとおりです。
付加機能をご利用の際には、事前に実機と実回線を用いた接続試験を行うことを推奨いたします。

(a) 必須項目

項目	契約内容	利用可否
インタフェース形態	23B+D	利用可（必須）
	24B	利用不可
発信者番号通知サービス	呼毎通知許可	利用可（推奨）
	呼毎通知拒否	利用不可
	常時通知拒否	利用不可
ユーザー間情報通知サービス	着信許可	利用不可
	着信拒否	利用可（推奨）

(b) 付加機能等項目（使用料 無料）

項目		契約内容	利用可否
代表取扱サービス	代表選択	親	利用可
		子	利用可
	代表選択方式	順次サーチ方式	利用可
		ラウンドロビン方式	利用可
通信中着信通知サービス			利用不可
任意チャネル着信サービス			利用不可
発信専用制御機能		契約者回線単位	条件付きで利用可※1
		B チャネル単位	利用不可
でんわ会議サービス			利用不可

※1 発信専用制御機能を利用する場合、着信は行えませんので、該当する装置には発呼しないようにする必要があります。

(c) 付加機能等項目（使用料 有料）

項目	契約内容	利用可否
384Kb/s 通信モード		利用不可
1.5Mb/s 通信モード		利用不可
ダイヤルインサービス	グローバル着信利用	条件付きで利用可※2
	グローバル着信利用しない	条件付きで利用可※2
フレックスホン	コールウェイティング機能	利用不可
	三者通話機能	利用不可
	通信中転送機能	利用不可
	着信転送機能	利用不可
でんわばん/W サービス		利用不可
メッセージインサービス		利用不可
#ダイヤルサービス		利用不可
グループセキュリティサービス		利用不可
テレドームサービス		利用不可
ファクシミリ通信網サービス		利用不可

※2 ダイヤルインサービスを利用する場合、着信時に設定されてくる着番号が契約回線番号、追加番号、番号設定無しのいずれかになりますので、用途に合わせた設定が IX3000 側にも必要になります。

■14.20 ルータメッセージ一覧

再起動要因一覧

show uptime,show version コマンドで再起動の要因の詳細が表示されます。

【表示例】

```
ix2010(config)# show uptime
System uptime is ** minutes
System woke up by reload, caused by command execution    <<  再起動要因
System started at Jun **-Mon-2005 **:**:** JST

Statistics: 1 start, 0 known crashes
Last reload: ** minutes ago
Last restart: ** minutes ago

ix2010(config)# show version
NEC Portable Internetwork Core Operating System Software
IX Series IX2010 (magellan-sec) Software, Version 7.2.XX, RELEASE SOFTWARE
Compiled Jun **-Fri-2005 **:**:** JST #2 by *****, coregen-7.2(*)

ROM: System Bootstrap, Version 15.*
System Diagnostic, Version 13.*

System uptime is 45 minutes
System woke up by reload, caused by command execution      <<  再起動要因
System started at Jun **-Mon-2005 **:**:** JST
System image file is "ix2010-ms-7.2.**.ldc"
Processor board ID <0>
IX2010 (MPC8250A) processor with 65536K bytes of memory.
3 FastEthernet/IEEE 802.3 interfaces
512K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Current configuration is based on "startup-configuration"
Configuration register is 0x11000020, last changed 29 Jun 2004 08:53:52 (UTC)
```

＊表示例ですので、バージョンにより一部内容が異なる場合があります。

メッセージ	内容
System woke up by reload, caused by command execution	コマンドによる再起動
System woke up by restart, caused by command execution	コマンドによる再起動
System woke up by reload, caused by power-on	電源 ON による起動
System woke up by reload, caused by license invalidation	ライセンス削除による再起動
System woke up by reload, caused by temporary license expiration	テンポラリライセンス期限切れ による再起動
System woke up by reload, caused by crash	クラッシュによる再起動

クラッシュ情報

show crashinfo コマンドで表示される Exception Type の内容と主な要因について説明します。

```
(config)# show crashinfo
2005/07/XX XX:XX:XX +0900 INFO: Start logging fault and crash informations
2005/07/XX XX:XX:XX +0900 CRASH: Number of the crash 1
2005/07/XX XX:XX:XX +0900 CRASH: IX Series IX2010 (magellan-sec) Software, Version 7.2.XX, RELEASE
SOFTWARE
2005/07/XX XX:XX:XX +0900 CRASH: Compiled Jun XX-XXX-2005 XX:XX:XX JST #2 by XXXXX, coregen-7.2(XX)
2005/07/XX XX:XX:XX +0900 CRASH:

******** C R A S H   D U M P ********
Time: 2005/07/XX XX:XX:XX +0900

CPU is MPC8270: PVR = 0x80822013, IMMR[16:31] = 0x0a01

CPU Register Context:
R00    = 0x0000000e   R01    = 0x007eefa8   R02    = 0xfe00ed68   R03    = 0x0000000e
R04    = 0xffffffff   R05    = 0x0017097c   R06    = 0x00613ee4   R07    = 0x00504efe
R08    = 0x00610000   R09    = 0x00000000   R10    = 0x012f5dd8   R11    = 0xffffaa39
R12    = 0x00610000   R13    = 0x00000000   R14    = 0x00000000   R15    = 0x00000000
R16    = 0x00000000   R17    = 0x00000000   R18    = 0x00000000   R19    = 0x00000000
R20    = 0x00000000   R21    = 0x00000000   R22    = 0x00000000   R23    = 0x00000000
R24    = 0x00000000   R25    = 0x00000000   R26    = 0x007eefb0   R27    = 0x0017097c
R28    = 0x012f4a5c   R29    = 0x007eefb4   R30    = 0x012e517c   R31    = 0x012f7994
CR     = 0x427e2289   MSR    = 0x00001030   LR     = 0x00000704   SRR0   = 0x00025b08
SRR1   = 0x00021032   SPRG0 = 0x03000000   SPRG1 = 0x00000000   SPRG2 = 0x00000000
SPRG3 = 0x00000000   XER    = 0x00000000   CTR    = 0x00429bec   DAR    = 0x00000000
DSISR = 0x00000000   ESR    = 0x08000000   EMR    = 0xff1f0000   ECR    = 0x00000000

SIUMCR    = 0x4060c000   TESCR1    = 0x00004000   TESCR2    = 0x00000000
PCI_EACR = 0x00008000   PCI_EDCR = 0x00000000   PCI_ECCR = 0x03a0113f
SIPNR_H   = 0x00200001   SIPNR_L   = 0x00009004   SIVEC      = 0x38000000
PDTEA     = 0x0091a4d0   LDTEA     = 0x00000000

SDMR       = 0x00          PDTEM      = 0x22          LDTEM      = 0x00

IPSEC_PCI_STS          = 0x0146       IU_PCI_STS              = 0xffff

Exception Type: program (0x00000700)    << クラッシュ要因
Exception Stack: PC(SRR0) = 0x00025b08, SP(R01) = 0x007eefa8

Stack Trace:
Frame 00: SP = 0x012f70dc
Frame 01: SP = 0x0015e150
Frame 02: SP = 0x0015e684
Frame 03: SP = 0x0016ead0
Frame 04: SP = 0x0016e9f8
Frame 05: SP = 0x0042d35c
Frame 06: SP = 0x0042d2d4
Frame 07: SP = 0x0042d35c

＊表示例のため、バージョンにより一部内容が異なる場合があります。
```

- エラーメッセージ一覧

メッセージ	内容	備考
INFO: Start logging fault and crash informations	ログクリア時刻	
INFO: Erase ***-config cmd:*** state:*** from:***	startup-config/default-config 削除	
INFO: Modify ***-config cmd:*** state:*** from:***	startup-config/default-config 修正	
INFO: Start bootstrap from this side [*].	ロードモジュール 2 面化使用時の起動面	Ver.8.2 以降
INFO: Software update *** (*******)	ソフトウェア更新結果	Ver.8.2 以降
CRASH: IX Series IX**** (**) Software, Version *.*.**, RELEASE SOFTWARE	クラッシュの発生したソフトウェアバージョン	
CRASH: Compiled Jun **-***-**** **:**:** JST #2 by *****, coregen-*.*(**)	クラッシュの発生したソフトウェア作成日時	
CRASH: Number of the crash *	クラッシュ発生回数（Bughalt 発生回数を含む）	
CRASH: Number of the bughlt *	Bughalt 発生回数	

CRASH: Bughlt, ********	Bughalt の要因	
ALERT: Voltage fault	電圧障害発生	電源電圧確認
ALERT: Voltage restore	電圧障害復旧	
ALERT: Temperature fault	温度アラーム発生	周囲温度確認
ALERT: Temperature restore	温度アラーム復旧	
ALERT: Fan failed	FAN 異常発生	本体交換
ALERT: Fan recovered	FAN 異常復旧	
ALERT: Power module *: System AC Power Supply failed	電源モジュール異常発生	電源の確認 電源交換
ALERT: Power module *: System AC Power Supply recovered	電源モジュール異常復旧	
ALERT: Power module *: System AC Power Supply inserted	電源モジュール実装	
ALERT: Power module *: System AC Power Supply removed	電源モジュール削除	
ALERT: Diagnostic	診断異常（詳細は以下）	
POST DRAM TEST 1: failed	DRAM 診断異常	本体交換
POST DRAM TEST 2: failed	DRAM 診断異常	本体交換
POST NVRAM TEST: failed	NVRAM 診断異常	本体交換
POST CPU TEST: failed	CPU 診断異常	本体交換
POST PLD TEST: failed	PLD 診断異常	本体交換
POST LAN1(FE0/0) TEST: failed	LAN1 ポート診断異常	本体交換
POST LAN2(FE0/1) TEST: failed	LAN2 ポート診断異常	本体交換
POST FE＊/＊ TEST: failed	FE ポート診断異常	本体交換
POST GE0-3(＊＊＊) TEST: failed	GE ポート診断異常（IX3110）	本体交換
POST GE＊TEST: failed	GE ポート診断異常	本体交換
POST GE＊[1G] TEST: failed	GE ポート診断異常（IX3115）	本体交換
POST GE＊[10G] TEST: failed	GE ポート診断異常（IX3115）	本体交換
POST ＊＊(SW-HUB)1-4 TEST:failed	SW-HUB ポート診断異常	本体交換
POST GE＊(SW-HUB)1-8 TEST:failed	SW-HUB ポート診断異常（IX3315）	本体交換
POST BRI TEST: failed	BRI ポート診断異常	本体交換
POST USB TEST: failed	USB ポート診断異常	本体交換
POST SECURITY TEST: failed	暗号化チップ診断異常	本体交換
POST ＊.＊ VOLTAGE STATUS: failed	電源診断異常	電源電圧確認
POST TEMPERATURE STATUS: failed	温度診断異常	周囲温度確認
POST FAN REVOLUTION STATUS: failed	FAN 診断異常	本体交換
POST SYSTEM AC POWER 0 STATUS: failed	電源モジュール 0 診断異常	電源交換
POST SYSTEM AC POWER 1 STATUS: failed	電源モジュール 1 診断異常	電源交換
POST ** 10/100BASE-TX TEST: failed	拡張スロット 10/100BASE-TX ポート診断異常	カード交換
POST ** HUB(SW)1-4 TEST: failed	拡張スロット HUB ポート診断異常	カード交換
POST ** T1 TEST: failed	拡張スロット T1 ポート診断異常	カード交換
POST ** DI TEST: failed	拡張スロット DI ポート診断異常	カード交換
POST ** T1 * TEST: failed	拡張スロット 2T1 ポート*診断異常	カード交換
POST ** BRI * TEST: failed	拡張スロット BRI ポート診断異常	カード交換
DUMP:	使用バージョンでは未対応のメッセージ	

- 主なクラッシュ要因一覧

(a) IX2015/IX3015

メッセージ	意味	一般的被疑箇所
unknown	未定義	HW
machine check (watchdog)	ウォッチドック タイムアウト	主に SW
machine check (pci error)	PCI バスエラー	HW,SW
machine check (bus monitor address only)	バスモニタタイムアウト (アドレスのみ)	HW,SW
machine check (bus monitor timeout)	バスモニタタイムアウト	HW,SW
machine check (internal bus error)	内部バスエラー	HW,SW
machine check (external bus error)	外部バスエラー	HW

machine check (unexpected error)	その他のエラー	HW,SW
DSI	DSI 例外	HW
ISI	ISI 例外	HW
alignment	アライメント例外	HW,SW
program	ソフトウェアによる強制リブート	SW
system call	システムコール	HW
inst. TLB miss	命令変換ミス	主に SW
data load TLB miss	データロード変換ミス	主に SW
data store TLB miss	データストア変換ミス	主に SW

(b)IX3315/IX3110/IX/2106/IX2107/IX2215/IX2207/IX2235/IX2310

メッセージ	意味	一般的被疑箇所
Unknown	未定義	HW
Watchdog Timer Interrupt	ウォッチドックタイムアウト	主に SW
Machine Check (Data cache parity error)	データキャッシュパリティエラー	HW,SW
Machine Check (Bus read data bus error)	バスデータ読み込みエラー	HW,SW
Machine Check (Bus write bus error)	バス書き込みエラー	HW,SW
Machine Check (Bus read parity error)	バスパリティエラー	HW,SW
Alignment	アライメント例外	HW,SW
Program	ソフトウェアによる強制リブート	SW
System Call	システムコール	HW
Instruction TLB error	命令変換エラー	主に SW
Data TLB error	データ変換エラー	主に SW
Processor doorbell critical	他 CPU 要因（IX3315,IX2310 のみ）	他 CPU

(c)IX2105

メッセージ	意味	一般的被疑箇所
unknown	未定義	HW
machine check (watchdog)	ウォッチドックタイムアウト	主に SW
machine check (pci error)	PCI バスエラー	HW,SW
machine check (data time out)	データタイムアウト	HW,SW
machine check (data parity error)	データパリティエラー	HW,SW
machine check (bus error)	バスエラー	HW,SW
DSI	DSI 例外	HW
ISI	ISI 例外	HW
alignment	アライメント例外	HW,SW
program	ソフトウェアによる強制リブート	SW
system call	システムコール	HW
inst. TLB miss	命令変換ミス	主に SW
data load TLB miss	データロード変換ミス	主に SW
data store TLB miss	データストア変換ミス	主に SW

■14.21 Ver.9.5 以前のソフトウェア諸元値

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
VLAN タギング	VLAN 設定数 （1 物理インタフェース当たり）	32	32	32	32	1000 ※5	- 32※6	同左 1000※6
	VLAN 設定数 （1 ポート VLAN インタフェース当たり）	8	8	8	-	8	-	同左
PPP※4	マルチリンク PPP 最大リンク数	2	2	46※3	-	-	2	同左
PPPoE	PPPoE 同時接続数 （1 物理インタフェース当たり）	8	8	8	8	8	-	32
ISDN （INS64・NI-1 サービス）※1, （INS1500,NI- PRI）※2	自己電話番号設定数	-	2	2	-	-	-	2
	SPID 設定数	-	2	-	-	-	-	2
	宛先/発信者番号認証用電話番号設定数 （1 対地当たり）	-	8	8	-	-	-	8
	登録対地数	-	96	512	-	-	-	同左
	同時接続対地数	-	2	46 ※3	-	-	-	同左
	無通信時間の設定最大値	-	86400	86400	-	-	120	86400
NGN	設定インタフェース数	1	1	1※4	1	1	-	1
	対地数（同時接続数）	16	16 32（IX2215）	24	200	300	-	なし
	対地数（設定数）（Ver.8.7 以降）	16	100	100	1000	5000	-	なし
	対地数（設定数）（Ver.8.6）	16	16	-	100	-	-	なし

（注）PPPoE と VLAN タギングの制限値は両方合わせた値となります。

※1 NI-1 は海外向け、INS64 は国内向けサービスとなります。

※2 NI-PRI は北米向け、INS1500 は国内向けとなります。

※3 PRI の複数ポートサポートは INS1500 のみとなります。

※4 Ver.8.7 以降

※5 システム全体で 1000 まで

※6 IX3315 のみ

分類	項目 （Ver.8.0 以降のソフトウェア諸元）		IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
ブリッジ	グループ当たりのインタフェース数		10	10	50※1	200※1	200	-	なし
	ブリッジグループ数		255	255	255	255	1000	-	同左
	BVI インタフェース数（Ver.8.11 以降）		64	64	64	64	64	8	64
	BVI インタフェース数（Ver.8.10 以前）		8	8	8	8	-	8	8
	学習アドレスエントリ数		4096	4096	4096	4096	20000	4096	なし
EtherIP Ether over GRE （ブリッジ機能）	対地数 （ブリッジグループ当たり）		10	10	50※1	200※1	300※1	-	Tunnel 数
	対地数 （全ブリッジ合計）		10	10	50※1	200※1	1000※1	-	Tunnel 数
IEEE802.1X	サプリカント数 （インタフェース当たり）※2	EAP-MD5 使用時	64	64	128	128	128	32	256
		EAP-PEAP/TLS 使用時	32	32	64	64	64	32	256
	検疫許可フィルタ ID 設定数 （インタフェース当たり）		3	3	3	3	3	-	なし
MAC 認証	収容端末数（インタフェース当たり）		512	512	512	512	512	-	なし
Web 認証	認証端末数		2048	2048	2048	2048	2048	-	65535
	認証パスワード設定数		32	32	32	32	32	-	なし
リンク マネージャ機能	登録端末数		4096	4096	4096	4096	4096	-	4096

※1 使用する条件によって、最大値は異なります。Ether over IP の項を参照してください。

※2 IEEE802.1X の認証確立時間は主に Supplicant と認証サーバの性能に依存します。特に電子証明書を利用する認証方式でその特性が顕著に現れるため、注意してください。

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
IPv4	ARP エントリ数（Ver.8.6 以降）	2048	2048	2048	2048	2048	2048	65536
	ARP エントリ数（Ver.8.5 以前）	1024	1024	1024	1024	-	1024	65536
	インタフェースアドレス数（セカンダリ）	2	2	2	2	2	-	2
	スタティックルート数	1024	1024	1024	2048	10000	-	なし
	ルート数	4096	4096	8192	20000	100000	2048 100000※4	なし
	ルートキャッシュエントリ数	10000	10000	10000	20000	100000	4096 100000※4	※1
	マルチパス数	4	4	4	4	4	-	4
	マルチキャストスタティックルート数	64	64	128	256	256	-	なし
VRF	VRF 数	32	32	32	32	32	-	なし
NAT	静的 NAT 数	2048	2048	16384	16384	16384	-	なし
	静的 NAT 設定数（Ver.9.1 以降）	256	1024	2048	2048	2048	-	なし
	静的 NAT 設定数（Ver9.0 以前）	256	256	1024	1024	-	-	なし
	動的 NAT 数	2048	2048	2048	2048	2048	-	なし
	キャッシュサイズ	2048	2048	16384	16384	16384	512	65535
NAPT	キャッシュサイズ	65535	65535	65535	65535	65535	4096 65535※3	65535
	静的 NAPT/サービス数	255	255	255	255	255	-	なし
	アクセスログの保存サイズ（Ver9.2 以降）	32※2 128※2	16※2 128※2	32	128	128	-	128
DHCP サーバ	プロファイル設定数	64	64	64	64	64	-	なし
	インタフェース当たりのプロファイル割り当て数	1	1	1	1	1	-	1
	グローバルでのプロファイル割り当て数	4	4	4	4	4	-	なし
	アドレスプール設定数 （インタフェース当たり）	1	1	1	1	1	-	1
	クライアント設定数（1 プール当たり）	256	256	256	256	-	-	65535
	クライアント設定数 （1 プール・装置当たり）（ver9.1 以降）	512	512	1024	1024	1024	-	65535
	固定クライアント設定数	32	32	32	32	32	-	なし
DHCP リレーエージェント	リレー先サーバ数	4	4	4	4	4	-	なし

※1 機種によって上限が異なります。コマンドリファレンスマニュアルを参照してください。
※2 IX2025 が 16, IX2105 が 32, IX2207 と IX2215 は 128 です。
※3 Ver.9.3 以降 IX2105, IX2207, IX2215, IX3110, IX3315 はデフォルト 65535。それ以外の機種・バージョンは 4096 です。
※4 IX3315 のみ

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 仕様	IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
IPv6	スタティックルート設定数	1024	1024	1024	1024	2048	10000	-	なし
	ルート数	2048	2048	2048	2048	4096	20000	-	なし
	リアセンブルバッファサイズ[byte]	65535	65535	65535	65535	65535	65535	65535	65535
	インタフェースアドレス数 （インタフェース当たり）	16	16	16	16	16	16	-	なし
	ルートキャッシュエントリ数	4096	4096	4096	4096	4096	20000	4096 20000※2	4096 100000※2
	マルチパス数	16	16	16	16	16	16	-	16
ICMPv6	メッセージ送出間隔 [msec]	1000	1000	1000	1000	1000	1000	1000	10000
ND （近隣探索）	ルータ通知用プレフィックス数 （装置当たり）	16	16	16	16	16	16	-	なし
	近隣キャッシュ数 （装置当たり）	512	512	512	512	512	512	1024 ※1	4096 ※1
DHCPv6 サーバ	接続 PD クライアント数 （Ver.8.9 以降）	128	64	256	128	256	256	-	なし
DHCPv6 クライアント	PD 再配布プール設定数 （Ver.8.9 以降）	128	64	256	128	256	256	-	なし

※1 default,制限値はインタフェース当りの値となります。
※2 IX3315 のみ

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
RIP/RIPv2	受信ルート数	2048	2048	4096	4096	4096	-	なし
	ネイバ数	512	512	512	512	512	-	なし
	同時送信経路数（装置当たり）	1000	1000	1000	1000	1000	-	なし
	設定インタフェース数	64	64	64	64	64	-	なし
RIPng	受信ルート数	1000	1000	1000	2048	2048	-	なし
	ネイバ数	64	64	64	64	64	-	なし
	同時送信経路数（装置当たり）	1000	1000	1000	1000	1000	-	なし
OSPFv2	プロセス数	1	1	1	1	1	-	1
	エリア数	16	16	16	16	16	-	なし
	バーチャルリンク数	16	16	16	16	16	-	16
	ネットワーク登録数	64	64	64	64	64	-	同左
	AS 外部 LSA 数	1000	1000	4000	20000	20000	-	65535
	Type7 LSA（NSSA）数	1000	1000	4000	20000	20000	-	65535
	ルートエントリ数	2048	2048	4096	20000	20000	2048	65535
	ネイバ数（Ver.8.7 以降）	128	128	128	128	128	-	なし
	ネイバ数（Ver.8.6 以前）	64	64	64	64	-	-	なし
OSPFv3	プロセス数	4	4	4	4	4	-	なし
	エリア数	16	16	16	16	16	-	なし
	ネットワーク登録数	64	64	64	64	64	-	同左
	AS 外部 LSA 数	1000	1000	1000	1000	1000	-	1000
	ルートエントリ数	2048	2048	2048	2048	2048	2048	65535
	ネイバ数	64	64	64	64	64	-	なし
BGP4	ルートエントリ数（パス数）	4096	4096	8192	20000	100000	-	なし
	ピア数	64	64	128	256	1000	-	なし
	ダイナミックネイバ数（Ver.9.4 以降）	64	64	128	256	1000	64	65535
	ダイナミックネイバ数（Ver.9.3 以前）	64	64	128	256	-	64	256
ポリシー ルーティング	1 インタフェース当たりの条件数 （access-list の場合は行数の和）	96	96	256	256	256	-	なし
VRRPv2 VRRPv3	VRRP グループ設定数 装置当たり）	32	32	32	32	32	-	なし
	参加可能な VRRP ルータ数 （1VR グループ当たり）	4	4	4	4	4	-	なし

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
PIM-SM	ネイバ数	128	128	128	256	256	-	なし
	マルチキャストグループ数	128	128	128	255	255	-	255
	マルチキャストエントリ数	256	256	256	256	256	-	なし
	ダウンストリームインタフェース数	16	16	32	64	64	-	なし
IGMP プロキシ	リスナキャッシュ数	32	32	32	32	32	-	なし
	アップストリームインタフェース	1	1	1	1	1	1	1
	ダウンストリームインタフェース	16※1	16※1	32※1	32※1	32※1	-	なし
MLD プロキシ	リスナキャッシュ数	32	32	32	32	32	-	なし
	アップストリームインタフェース	1	1	1	1	1	1	1
	ダウンストリームインタフェース	16※1	16※1	32※1	32※1	32※1	-	なし
	MLDv2 のソースアドレス数 （マルチキャストグループ当たり）	64	64	64	64	64	-	128
ネットワーク モニタ	監視プロファイル（watch-group）の 最大数	128※2	128※2	512※2	1024※2	5000	-	なし
	1 プロファイル当たりのイベント数	96	96	96	96	96	-	なし
	1 プロファイル当たりのアクション数	16	16	16	16	16	-	なし
	装置全体のイベント数	128	128	512	1024	5000	-	なし

※1 ダウンストリーム数は固定ビットレート、2Mbps のストリーミング時の推奨値です。ストリーミング量により最大値が異なります。詳細はマルチキャストの設定の項を参照してください。

※2 ホスト監視時の対地数が 100 を超える場合は、対地数に応じて ICMP ECHO_REQUEST の送信間隔を延ばし、また、約 100 対地ごとに送信間隔を 1,2 秒程度ずらすことで負荷分散してください。また、監視周期を 1 秒以下に設定する場合は、ネットワークモニタの設定の項の注意事項を参照してください。

分類	項目（Ver.8.0 以降のソフトウェア諸元）			IX2105 IX2207 仕様	IX2025 仕様	IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
トンネル	トンネル数		IPv4 over IPv4 IPv4 over IPv6 IPv4 over GRE, L2TP	128	128	128	512※2	1024※2	5000	-	同左
			IPv6 over IPv4 IPv6 over IPv6 IPv6 over GRE	128	128	128	256	256	256	-	IPv4 overIPv4 トンネル数
	Auto トンネル数（Ver.8.2 まで）			-	1	-	1	1	-	-	1
	多段トンネル終端段数※4,※6			3	3	3	3	3	3	-	3
IKE/IKEv2※1	対地数	MD5 SHA-1		128	128	128	512※2 [24]	1024※2	5000※2	-	なし
		SHA-256（Ver.8.6 以降）		128	[2]※3	128	[2]※3	1024※2	5000※2	-	なし
		SHA-384（Ver.8.6 以降） SHA-512（Ver.8.6 以降）		128	[2]※3	128	[2]※3	[2]	5000	-	なし
IPsec※1	対地数	MD5 SHA-1	トンネル IPv4 over IPv4 IPv4 over IPv6	128	128	128	512※2 [24]※3	1024※2	5000※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	128	128	256 [24]※3	256	256	-	トンネル数
			トランスポート	32	32	32	64	64	64	-	なし
		SHA-256 （Ver.8.6 以降） ※5	トンネル IPv4 over IPv4 IPv4 over IPv6	128	[2]※3	128	[2]※3	1024※2	5000※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	[2]※3	128	[2]※3	256	256	-	トンネル数
			トランスポート	32	[2]※3	32	[2]※3	64	64	-	なし
		SHA-384 SHA-512 （Ver.8.6 以降） ※5	トンネル IPv4 over IPv4 IPv4 over IPv6	128	[2]※3	128	[2]※3	[2]	5000※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	[2]※3	[128	[2]※3	[2]	256	-	トンネル数
			トランスポート	32	[2]※3	32	[2]※3	[2]	64	-	なし
	ポリシーに対応するプロポーザル設定数			4	4	4	4	4	4	-	4
	自動鍵マップに対応する自動鍵プロポーザル設定数			8	8	8	8	8	8	-	8
ダイナミック VPN	接続対地数			128	128	128	512	1024	5000	同左※7	同左※7
	接続対地数（BGP 使用時）			64	64	64	128	256	1000	同上※7	同上※7

※1 [ ]内はソフトウェア暗号認証処理の場合の対地数、[ ]なしはハードウェア暗号認証処理の場合の対地数を表します。IPsec 高速化拡張オプション（ハードウェア暗号認証処理）が必要な機種で、IPsec 高速化拡張オプション用のライセンスを投入していない場合は、ソフトウェア暗号認証処理となります。ソフトウェア暗号認証処理の場合は、IKE の DH グループおよび IPsec の PFS はデフォルト値を使用してください。
※2 トンネル種別が混在する場合の最大数は、以下のトンネル数を 2 として計算してください。
- IPv6 over IPv4, IPv6 over IPv6
- IPv6 over IPv4 IPsec,IPv6 over IPv6 IPsec,EtherIP with IPsec

※3 ISDN ダイヤルアップ回線で IPsec を利用される場合は、IPsec で利用している PRI の場合 1PRI インタフェース当たり 23CH 分、IPsec で利用している BRI の場合 1BRI インタフェース当たり 2CH 分の数を対地数に加算することができます。
※4 SHA-256、SHA-384、SHA-512 のソフトウェア暗号認証処理による IPsec トンネルの場合、最大のトンネル段数は 1 となります。
※5 マルチリンク PPP では利用できません。
※6 L2TP では多段トンネルは利用できません。
※7 拠点間の動的接続は諸元値で制限されます。Ver9.3 以降はセンタでの拠点からの接続数の制限を設定できます。デフォルト値は諸元値となります。

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
AAA/Radius	RADIUS サーバ設定数	4	4	4	4	4	-	なし
SNMP エージェント	TRAP 送信先マネージャ設定数	8	8	8	8	8	-	なし
	コミュニティ登録件数	253	253	253	253	253	-	なし
プロキシ DNS	ipv4 固定/動的サーバ設定数	各 2	各 2	各 2	各 2	各 2	-	なし
	ipv4 セッション数（9.2 以降）※1	254	254	254	254	254	254	1024
	ipv4 セッション数（9.1 以前）※1	32	32	32	32	-	32	254
	ipv6 固定/動的サーバ設定数	各 2	各 2	各 2	各 2	各 2	-	なし
	ipv6 セッション数（9.2 以降）※1	254	254	254	254	254	254	1024
	ipv6 セッション数（9.1 以前）※1	32	32	32	32	-	32	254
DNS リゾルバ	固定/動的サーバ設定数	6	6	6	6	6	-	なし
SNTP クライアント	サーバ設定数	3	3	3	3	3	-	なし
MAC フィルタ	MAC フィルタ設定数 （インタフェース当たり）	in 3 out 3	in 3 out 3	in 3 out 3	in 3 out 3	in 3 out 3	-	なし
MAC アクセスリスト	アクセスリスト名の数	256	256	256	256	256	-	なし
	１アクセスリスト当たりの各エントリ数	256	256	256	256	256	-	なし
	アクセスリスト総エントリ数	256	256	256	256	256	-	なし
	アクセスリストキャッシュ数	2048	2048	2048	2048	2048	8192	65535
トラフィック フィルタ	スタティックフィルタ設定数※2 （インタフェース当たり）	64	64	128	128	128	-	なし
	ダイナミックフィルタ設定数 （インタフェース当たり）	in 8 out 8	in 8 out 8	in 8 out 8	in 8 out 8	in 8 out 8	-	なし
IP アクセス リスト	アクセスリスト名の数	256	256	256	1024	5120	-	なし
	１アクセスリスト当たりの各エントリ数	256	256	256	2048	2048	-	なし
	アクセスリスト総エントリ数	512	512	512	2048	10000	-	なし
	アクセスリストキャッシュ数	8192	8192	8192	20000	100000	8192 20000※3	65535 100000※3
	ダイナミックアクセスリスト名の数	64	64	64	256	256	-	なし
	ダイナミックアクセスリスト１アクセスリスト当たりの各エントリ数	256	256	256	512	512	-	なし
	ダイナミックアクセスリスト キャッシュ数	8192	8192	32768	32768	32768	8192 32768※3	65535
URL フィルタリング	内部 URL フィルタリング数	256	256	256	256	256	-	なし
	登録インタフェース数	4	4	4	4	4	-	なし

※1 IPv4/IPv6 は問い合わせ元のプロトコルとなります。

※2 最大数まで使用する場合は、UFS キャッシュを併用してください。

※3 IX3315 のみ

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
QoS	ポリシーマップ数 （インタフェース当たり）	in 1 out 1	in 1 out 1	in 1 out 1	in 1 out 1	in 1 out 1	-	in 1 out 1
	1 クラス当たりの優先キュー数（8.9 以降）	8	8	8	8	8	8	8
	1 クラス当たりの優先キュー数（8.8 以前）	4	4	4	4	-	4	4
VoIP 関連	RTP ヘッダ圧縮接続数	-	16	16	-	-	-	255
	TCP ヘッダ圧縮接続数	-	16	16	-	-	-	255
クラスマップ ※1 ※2	クラスマップ数 （Ethernet インタフェースのみ）	16	16	62	62 126※4	128	-	128※5 1024※5 5000※6
	クラスマップ数 （データコネクトのみ利用する場合）	16	100	100	1000	1000	-	128※5 1024※5
	クラスマップ数 （上記以外）	-	8	16	-	-	-	62
ルートマップ	ルートマップ数	128※3	128※3	256※3	256※3	256※3	-	なし
プレフィック スリスト	プレフィックスリスト数	1024	1024	1024	1024	1024	-	なし
	1 リストのエントリ数	256	256	256	1024	1024	-	なし
	総エントリ数	512	512	512	2048	2048	-	なし
UFS キャッシュ	最大キャッシュ数（8.2 以降 IPv4）	20000	20000	20000	65535	200000	8192 100000 ※6	100000 500000 ※6
	最大キャッシュ数（8.2 以降 IPv6）	10000	10000	10000	20000	100000	4096 50000※6	65535 500000 ※6
	最大キャッシュ数（8.1 以前）	10000	10000	10000	20000	-	4096	65535
	ハッシュサイズ	8192	8192	8192	8192	8192	1024 2048※6	65536
ロギング	ロギング保持件数 （1 件 80byte とした場合）	100000	100000	100000	100000	500000	1600 10000※6	100000 1000000 ※6
syslog	syslog 送信先設定数	8	8	8	8	8	-	なし

※1 クラスマップの仕様値は帯域制御を含む場合です。カラーリングのみで利用する場合は制限値まで利用可能です。クラスマップ数に class-local, class-default は含みません。
※2 データコネクト利用時は同時利用されるクラスマップが NGN の同時接続数で制限されるため、仕様値まで設定可能となっています。
※3 最大数まで使用する場合は、UFS キャッシュを併用してください。
※4 Ver.8.6 以降。62 以上で使用する場合、設定が必要です。詳細は QoS の項を参照してください。
※5 IX3110 以外が 128, IX3110 のみ 1024、Ver8.7 以前は IX3110 以外が 62, IX3110 のみ 254 となります。
※6 IX3315 のみ

分類	項目 （Ver.8.0 以降のソフトウェア諸元）	IX2105 IX2207 仕様	IX2025 IX2215 仕様	IX3015 仕様	IX3110 仕様	IX3315 仕様	default	制限値
URL リダイレクト	端末登録エントリ数	2048	2048	2048	2048	2048	-	2048
	同時セッション受信数	64	64	64	64	64	-	64
スケジューラ	最大アクションリスト数	128	128	512	1024	1024	-	なし
	最大コマンド数	512	512	1024	1024	1024	-	なし
	最大タイマ数	128	128	512	1024	1024	-	なし
Wake on LAN	端末情報登録数	128	128	256	256	256	-	なし
システム	プログラム世代管理数	2	2	2	2	2	-	なし
	ログインアカウント設定数	8	8	8	8	8	-	50
	ユーザ名長	16	16	16	16	16	-	16
	パスワード長	80	80	80	80	80	-	249
	telnet 同時ログイン数	4	4	4	4	4	-	4
	SSH 同時ログイン数	4	4	4	4	4	-	4
	コンソール同時ログイン数	1	1	1	1	1	-	1
	enable-config 同時操作数	1	1	1	1	1	-	1
	ブートエントリ数	4	4	4	4	4	-	4
	格納ファイル数	19	19	19	19	19	19	19

分類	項目	IX2105 IX2207 仕様	IX2215 仕様	IX3110 仕様	IX3315 仕様	default	制限値
OpenFlow	フローエントリ数※1	8192	8192	65535	65535	-	なし
	フローテーブル数	254	254	254	254	-	なし
	ポート数	128	128	1024	1024	-	なし
	フローキャッシュ数	65536	131072	131072	131072	-	なし
	コントローラ設定数	4	4	4	4	-	なし
	コントローラ同時接続数	1	1	1	1	-	1
Ether over GRE （OpenFlow 機能）	対地数	10	10	100 1024※2	100 1024※2	-	なし

※1 ハッシュ機能の利用が前提です。
※2 フラッディング処理がない場合のみです。

■14.22 Ver.9.6 以降 販売終了製品ソフトウェア諸元値

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
VLAN タギング	VLAN 設定数 （1 物理インタフェース当たり）	32	32	32	32	32
	VLAN 設定数 （1 ポート VLAN インタフェース当たり）	8	8	-	-	同左
PPP	マルチリンク PPP 最大リンク数	-	46	-	2	同左
PPPoE	PPPoE 同時接続数 （1 物理インタフェース当たり）	8	8	8	-	32
ISDN ISDN	PPPoE サーバ同時接続数 （装置あたり）	32	32	32	-	32
	自己電話番号設定数	-	2	-	-	2
	SPID 設定数	-	-	-	-	2
	宛先/発信者番号認証用電話番号設定数 （1 対地当たり）	-	8	-	-	8
	登録対地数	-	512	-	-	同左
	同時接続対地数	-	46	-	-	同左
データコネクト (NGN)	無通信時間の設定最大値	-	86400	-	120	86400
	設定インタフェース数	1	1	1	-	1
	対地数（設定数）	16	100	1000	-	なし

（注）PPPoE と VLAN タギングの制限値は両方合わせた値となります。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）		IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
ブリッジ	グループ当たりのインタフェース数		10	50※1	200※1	-	なし
	ブリッジグループ数		255	255	255	-	同左
	BVI インタフェース数		64	64	64	8	64
	学習アドレスエントリ数		4096	4096	4096	4096	なし
EtherIP Ether over GRE （ブリッジ機能）	対地数 （ブリッジグループ当たり）		10	50※1	200※1	-	Tunnel 数
	対地数 （1対地当たり1ブリッジグループの場合）		10	50※1	200※1	-	Tunnel 数
IEEE802.1X	サプリカント数 （インタフェース当たり）※2	EAP-MD5 使用時	64	128	64	256	256
		EAP-PEAP/TLS 使用時	64	64	3	256	256
	検疫許可フィルタ ID 設定数 （インタフェース当たり）		3	3	3	-	256
MAC 認証	収容端末数（インタフェース当たり）		512	512	512	-	なし
Web 認証	認証端末数		2048	2048	2048	-	65535
	認証パスワード設定数		32	32	32	-	なし
リンク マネージャ機能	登録端末数		4096	4096	4096	-	4096
MAP-E	収容回線数		1	1	1	-	-

※1 使用する条件によって、最大値は異なります。Ether over IP の項を参照してください。

※2 IEEE802.1X の認証確立時間は主に Supplicant と認証サーバの性能に依存します。特に電子証明書を利用する認証方式でその特性が顕著に現れるため、注意してください。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
IPv4	ARP エントリ数（Ver.8.6 以降）	2048	2048	2048	2048	65536
	インタフェースアドレス数（セカンダリ）	16	16	16	-	16
	スタティックルート数	1024	1024	2048	-	なし
	ルート数	4096	8192	20000	2048 100000※5	なし
	ルートキャッシュエントリ数	10000	65535	100000	4096※2 100000※3	65535 100000※1
	マルチパス数	4	4	4	-	4
	マルチキャストスタティックルート数	64	128	256	-	なし
VRF	VRF 数	32	32	32	-	なし
NAT	静的 NAT 数	2048	16384	16384	-	なし
	静的 NAT 設定数	256	2048	2048	-	なし
	動的 NAT 数	2048	2048	2048	512	なし
	キャッシュサイズ	2048	16384	16384	65535 4096※4	65535
NAPT	キャッシュサイズ	65535	65535	250000	-	諸元値と 同じ
	静的 NAPT/サービス数	255	255	255	-	なし
	アクセスログの保存サイズ	32	32	128	-	128
DHCP サーバ	プロファイル設定数	64	64	64	-	なし
	インタフェース当たりのプロファイル 割り当て数	1	1	1	-	1
	グローバルでのプロファイル割り当て数	4	4	4	-	なし
	アドレスプール設定数 （インタフェース当たり）	1	1	1	-	1
	クライアント設定数 （装置当たり）	512	1024	1024	-	65535
	固定クライアント設定数	32	32	32	-	なし
DHCP リレー エージェント	リレー先サーバ数	4	4	4	-	なし

※1 IX3110 のみ

※2 IX2105/IX3015

※3 IX3110

※4 IX3015 のみ

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
IPv6	スタティックルート設定数	1024	1024	2048	-	なし
	ルート数	2048	2048	4096	-	なし
	リアセンブルバッファサイズ[byte]	65535	65535	65535	65535	65535
	インタフェースアドレス数 （インタフェース当たり）	16	16	16	-	なし
	ルートキャッシュエントリ数	4096	4096	4096	4096	※2
	マルチパス数	16	16	16	-	16
ICMPv6	メッセージ送出間隔 [msec]	1000	1000	1000	1000	10000
ND （近隣探索）	ルータ通知用プレフィックス数 （装置当たり）	16	16	16	-	なし
	近隣キャッシュ数 【Ver9.6】 （装置当たり）	1024	1024	1024	1024 ※1	8192 ※1
	近隣キャッシュ数 【Ver9.7】 （装置当たり）	1024	16384	16384	1024 ※1	16384 ※1
DHCPv6 サーバ	接続 PD クライアント数	128	128	256	-	なし
DHCPv6 クライアント	PD 再配布プール設定数	128	128	256	-	なし

※1 default,制限値はインタフェース当りの値となります。
※2 機種によって上限が異なります。コマンドリファレンスマニュアルを参照してください。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
RIP/RIPv2	受信ルート数	2048	4096	4096	-	なし
	ネイバ数	512	512	512	-	なし
	同時送信経路数（装置当たり）	1000	1000	1000	-	なし
	設定インタフェース数	64	64	64	-	なし
RIPng	受信ルート数	1000	1000	2048	-	なし
	ネイバ数	64	64	64	-	なし
	同時送信経路数（装置当たり）	1000	1000	1000	-	なし
OSPFv2	プロセス数	1	1	1	-	1
	エリア数	16	16	16	-	なし
	バーチャルリンク数	16	16	16	-	16
	ネットワーク登録数	64	64	64	-	同左
	AS 外部 LSA 数	1000	4000	20000	-	65535
	Type7 LSA（NSSA）数	1000	4000	20000	-	65535
	ルートエントリ数	2048	4096	20000	2048	65535
	ネイバ数	128	128	128	-	なし
OSPFv3	プロセス数	4	4	4	-	なし
	エリア数	16	16	16	-	なし
	ネットワーク登録数	64	64	64	-	同左
	AS 外部 LSA 数	1000	1000	1000	-	1000
	ルートエントリ数	2048	2048	2048	2048	65535
	ネイバ数	64	64	64	-	なし
BGP4	ルートエントリ数（パス数）	4096	8192	20000	-	なし
	ピア数	64	128	256	-	なし
	ダイナミックネイバ数	64	128	256	64	65535
ポリシー ルーティング	1 インタフェース当たりの条件数 （参照する access-list の行数）※1	96	256	256	-	なし
VRRPv2 VRRPv3	VRRP グループ設定数 装置当たり）	32	32	32	-	なし
	参加可能な VRRP ルータ数 （1VR グループ当たり）	4	4	4	-	なし

※1 Ver9.6 以降はアクセスリストの最適化コマンドにより、より多くの条件を指定可能です。詳細はアクセスリストの章を参照してください。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
PIM-SM	ネイバ数	128	128	256	-	なし
	マルチキャストグループ数	128	128	255	-	255
	マルチキャストエントリ数	256	256	256	-	なし
	ダウンストリームインタフェース数	16	32	64	-	なし
IGMP プロキシ	リスナキャッシュ数	32	32	32	-	なし
	アップストリームインタフェース	1	1	1	1	1
	ダウンストリームインタフェース	16※1	32※1	32※1	-	なし
MLD プロキシ	リスナキャッシュ数	32	32	32	-	なし
	アップストリームインタフェース	1	1	1	1	1
	ダウンストリームインタフェース	16※1	32※1	32※1	-	なし
	MLDv2 のソースアドレス数 （マルチキャストグループ当たり）	64	64	64	-	128
ネットワーク モニタ	監視プロファイル（watch-group）の 最大数	128	512	1024	-	なし
	1 プロファイル当たりのイベント数	96	96	96	-	なし
	1 プロファイル当たりのアクション数	16	16	16	-	なし
	装置全体のイベント数	128	512	1024	-	なし

※1 ダウンストリーム数は固定ビットレート、2Mbps のストリーミング時の推奨値です。ストリーミング量により最大値が異なります。詳細はマルチキャストの設定の項を参照してください。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）			IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
トンネル	トンネル数		IPv4 over IPv4 IPv4 over IPv6 IPv4 over GRE, L2TP	128	512※2	1024※2	-	同左
			IPv6 over IPv4 IPv6 over IPv6 IPv6 over GRE	128	256	256	-	IPv4 overIPv4 トンネル数
	多段トンネル終端段数※4,※6			3	3	3	-	3
IKE/IKEv2※1	対地数	MD5 SHA-1		128	512※2 [24]	1024※2	-	なし
		SHA-256（Ver.8.6 以降）		128	[2]※3	1024※2	-	なし
		SHA-384（Ver.8.6 以降） SHA-512（Ver.8.6 以降）		128	[2]※3	[2]	-	なし
IPsec※1	対地数	MD5 SHA-1	トンネル IPv4 over IPv4 IPv4 over IPv6	128	512※2	1024※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	256	256	-	トンネル数
			トランスポート	32	64	64	-	なし
		SHA-256 ※5	トンネル IPv4 over IPv4 IPv4 over IPv6	128	[2]※3	1024※2	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	[2]※3	256	-	トンネル数
			トランスポート	32	[2]※3	64	-	なし
		SHA-384 SHA-512 ※5	トンネル IPv4 over IPv4 IPv4 over IPv6	128	[2]※3	[2]	-	トンネル数
			トンネル IPv6 over IPv4 IPv6 over IPv6	128	[2]※3	[2]	-	トンネル数
			トランスポート	32	[2]※3	[2]	-	なし
	ポリシーに対応するプロポーザル設定数			4	4	4	-	4
	自動鍵マップに対応する自動鍵 プロポーザル設定数			8	8	8	-	8
ダイナミック VPN	接続対地数			128	512	1024	同左※7	同左※7
	接続対地数（BGP 使用時）			64	128	256	同上※7	同上※7

※1 [ ]内はソフトウェア暗号認証処理の場合の対地数、[ ]なしはハードウェア暗号認証処理の場合の対地数を表します。IPsec 高速化拡張オプション（ハードウェア暗号認証処理）が必要な機種で、IPsec 高速化拡張オプション用のライセンスを投入していない場合は、ソフトウェア暗号認証処理となります。ソフトウェア暗号認証処理の場合は、IKE の DH グループおよび IPsec の PFS はデフォルト値を使用してください。
※2 トンネル種別が混在する場合の最大数は、以下のトンネル数を 2 として計算してください。
- IPv6 over IPv4, IPv6 over IPv6
- IPv6 over IPv4 IPsec,IPv6 over IPv6 IPsec,EtherIP with IPsec

※3 ISDN ダイヤルアップ回線で IPsec を利用される場合は、IPsec で利用している PRI の場合 1PRI インタフェース当たり 23CH 分、IPsec で利用している BRI の場合 1BRI インタフェース当たり 2CH 分の数を対地数に加算することができます。
※4 SHA-256、SHA-384、SHA-512 のソフトウェア暗号認証処理による IPsec トンネルの場合、最大のトンネル段数は 1 となります。
※5 マルチリンク PPP では利用できません。
※6 L2TP では多段トンネルは利用できません。
※7 拠点間の動的接続は諸元値で制限されます。Ver9.3 以降はセンタでの拠点からの接続数の制限を設定できます。デフォルト値は諸元値となります。

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
AAA/Radius	RADIUS サーバ設定数	4	4	4	-	なし
SNMP エージェント	TRAP 送信先マネージャ設定数	8	8	8	-	なし
	コミュニティ登録件数	253	253	253	-	なし
	グループ登録件数 ※4	253	253	253	-	なし
	ユーザ登録件数 ※4	253	253	253	-	なし
プロキシ DNS	ipv4 固定/動的サーバ設定数	各 2	各 2	各 2	-	なし
	ipv4 セッション数 ※1	254	254	254	254	1024
	ipv6 セッション数 ※1	各 2	各 2	各 2	-	なし
	ipv4 固定/動的サーバ設定数	254	254	254	254	1024
DNS リゾルバ	固定/動的サーバ設定数	6	6	6	-	なし
SNTP クライアント	サーバ設定数	3	3	3	-	なし
MAC フィルタ	MAC フィルタ設定数 （インタフェース当たり）	in 3 out 3	in 3 out 3	in 3 out 3	-	なし
MAC アクセスリスト	アクセスリスト名の数	256	1024	1024	-	なし
	１アクセスリスト当たりの各エントリ数	256	1024	1024	-	なし
	アクセスリスト総エントリ数	256	1024	1024	-	なし
	アクセスリストキャッシュ数	8192	8192	8192	8192	65535
トラフィック フィルタ	スタティックフィルタ設定数※2 （インタフェース当たり）	64	128	128	-	なし
	ダイナミックフィルタ設定数 （インタフェース当たり）	in 8 out 8	in 8 out 8	in 8 out 8	-	なし
IP アクセスリスト	アクセスリスト名の数	256	256	1024	-	なし
	１アクセスリスト当たりの各エントリ数	256	256	2048	-	なし
	アクセスリスト総エントリ数	512	512	2048	-	なし
	アクセスリストキャッシュ数	8192	8192	20000	8192	65535
	ダイナミックアクセスリストの数	64	64	256	-	なし
	ダイナミックアクセスリスト １アクセスリスト当たりの各エントリ数	256	256	512	-	なし
	ダイナミックアクセスリスト キャッシュ数	65535	65535	65535 100000 ※4	8192	諸元地と同じ
URL フィルタリング	内部 URL フィルタリング数	256	256	256	-	なし
	登録インタフェース数	4	4	4	-	なし

※1 IPv4/IPv6 は問い合わせ元のプロトコルとなります。

※2 最大数まで使用する場合は、UFS キャッシュを併用してください。

※3 Ver.10.3 以降

※4 Ver10.4 以降

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
QoS	ポリシーマップ数 （インタフェース当たり）	in 1 out 1	in 1 out 1	in 1 out 1	-	in 1 out 1
	1 クラス当たりの優先キュー数	8	8	8	8	8
VoIP 関連	RTP ヘッダ圧縮接続数	-	16	-	-	255
	TCP ヘッダ圧縮接続数	-	16	-	-	255
クラスマップ ※1 ※2	クラスマップ数 （Ethernet インタフェースのみ）	16	62	62 126※4	-	128 1024※5
	クラスマップ数 （データコネクトのみ利用する場合）	16	100	1000	-	128 1024※5
	クラスマップ数 （上記以外）	-	16	-	-	62
ルートマップ	ルートマップ数	128※3	256※3	256※3	-	なし
プレフィックスリスト	プレフィックスリスト数	1024	1024	1024	-	なし
	1 リストのエントリ数	256	256	1024	-	なし
	総エントリ数	512	512	2048	-	なし
UFS キャッシュ	最大キャッシュ数（8.2 以降 IPv4）	20000	20000	65535	8192	100000
	最大キャッシュ数（8.2 以降 IPv6）	10000	10000	20000	4096	65535
	ハッシュサイズ	8192	8192	8192	1024	65536
ロギング	ロギングバッファサイズ（byte） （保持件数：1 件 80byte の場合）	8000000 （100000）	8000000 （100000）	8000000 （100000）	131072 （1638）	8388608 （104857）
syslog	syslog 送信先設定数	8	8	8	-	なし

※1 クラスマップの仕様値は帯域制御を含む場合です。カラーリングのみで利用する場合は制限値まで利用可能です。クラスマップ数に class-local, class-default は含みません。
※2 データコネクト利用時は同時利用されるクラスマップが NGN の同時接続数で制限されるため、仕様値まで設定可能となっています。
※3 最大数まで使用する場合は、UFS キャッシュを併用してください。
※4 62 以上で使用する場合、設定が必要です。詳細は QoS の項を参照してください。
※5 IX3110 のみ

分類	項目 （Ver.9.6 以降のソフトウェア諸元）	IX2105 仕様	IX3015 仕様	IX3110 仕様	default	制限値
URL リダイレクト	端末登録エントリ数	2048	2048	2048	-	2048
	同時セッション受信数	64	64	64	-	64
スケジューラ	最大アクションリスト数	128	512	1024	-	なし
	最大コマンド数	512	1024	1024	-	なし
	最大タイマ数	128	512	1024	-	なし
Wake on LAN	端末情報登録数	128	256	256	-	なし
システム	プログラム世代管理数	2	2	2	-	なし
	ログインアカウント設定数	8	8	8	-	50
	ユーザ名長	16	16	16	-	16
	パスワード長	80	80	80	-	249
	telnet 同時ログイン数	4	4	4	-	4
	SSH 同時ログイン数	4	4	4	-	4
	コンソール同時ログイン数	1	1	1	-	1
	enable-config 同時操作数	1	1	1	-	1
	ブートエントリ数	4	4	4	-	4
	格納ファイル数	19	19	19	19	19

分類	項目	IX2105 IX2207 仕様	IX2215 仕様	IX3110 仕様	IX3315 仕様	default	制限値
OpenFlow	フローエントリ数※1	8192	8192	65535	65535	-	なし
	フローテーブル数	255	255	255	255	-	なし
	ポート数	128	128	1024	1024	-	なし
	フローキャッシュ数	65536	65535	65535	65535	-	65535
	コントローラ設定数	4	4	4	4	-	なし
	コントローラ同時接続数	1	1	1	1	-	1
Ether over GRE （OpenFlow 機能）	対地数	10	10	100 1024※2	100 1024※2	-	なし

※1 ハッシュ機能の利用が前提です。
※2 フラッディング処理がない場合のみです。

■14.23 Ver.9.6 以降 販売終了製品ハードウェア仕様

分類	項目		IX2105 IX2105-Z 仕様	IX3015 仕様	IX3110 IX3110-Z 仕様
インタフェース	GigaEthernet（10G:RJ45/SFP）		-	-	-
	GigaEthernet（10G:RJ45）		-	-	-
	GigaEthernet		1	-	-
	GigaEthernet（RJ45/SFP）		-	-	4
	GigaEthernet（HUB ポート）		4	-	-
	FastEthernet		-	2	-
	FastEthernet（HUB ポート）		-	4	-
	BRI		-	※1	-
	T1		-	※1	-
	USB		-	-	-
メモリ	ヒープメモリ		128MB	128MB	256MB
	コンフィグメモリ		512KB	1024KB	2048KB
電源ユニット			-	2※2	2※2
FAN			-	1	1
装置監視	温度	アラーム発生（高温）	76	66	66
		アラーム発生（低温）	-1	-1	-1
		アラーム復旧（高温）	70	60	60
		アラーム復旧（低温）	5	5	5
	監視電圧（正常範囲：±10%）		+1.0V +1.8V +2.5V +3.3V +5V	+3.3V	+1.1V +1.8V +2.5V +3.3V +5V
LED	PWR		○	○	○
	ALM		○	○	○
	BUSY/BSY		○	○	○
	VPN		○	○	○
	PPP		○	○	○
	BAK		○	○	○
	1		-	-	-
	2		-	-	-
	3		-	-	-
MODE スイッチ, MODE LED			-	-	-
暗号/認証処理	DES/3DES/AES(128,192,256) MD5/SHA		○	○	○
	SHA2	256	○	-	○
		384,512	○	-	-

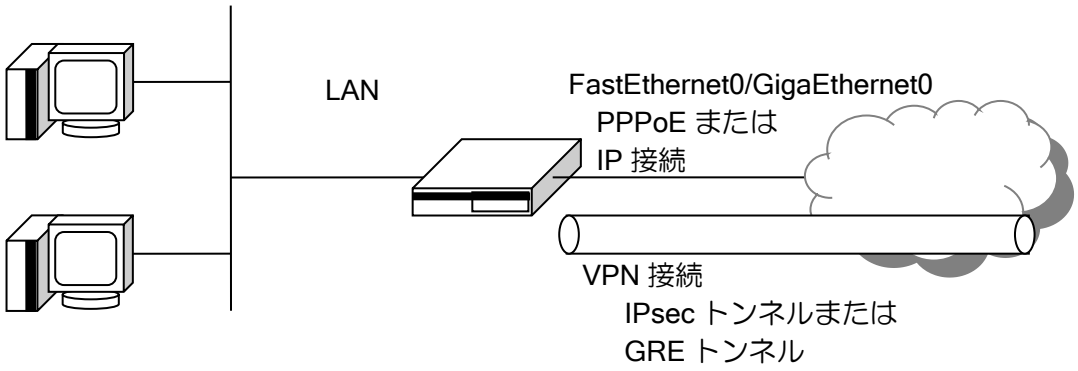
※1：オプションカードにより対応可

■14.24 Ver.9.1 以前の Web コンソールの設定

Web コンソール機能は Ver9.2 以降大幅に仕様変更しており、機能も順次追加しています。このため、Web コンソール機能を利用したい場合は、Ver9.2 以降のできるだけ最新版を利用するようにしてください。

1. Web コンソールの対応構成

Ver9.1 以前の Web コンソールは、下図に示すネットワーク構成で使用します。下図に示す構成以外では、正しく情報が表示されない場合があります。



WAN インタフェースは FE0 または GE0 のデバイスのみ対応、LAN インタフェースは SWHUB のデバイスのみ対応です。
IP 接続と PPPoE 接続のプロバイダに対応しています。
VPN 接続は、IPsec トンネルと GRE トンネルが設定可能です。

作成可能なコンフィグ例

以下のようなコンフィグを作成します。

【設定例】
PPPoE，IPsec（動的アドレス）を使用。
Web コンソールの設定は省略します。次項を参照してください。

```
ip route default Tunnel1.0
ip route 10.0.0.1/32 FastEthernet0.1

ip access-list any-list permit ip src any dest any

ike proposal ike_prop encryption aes hash sha

ike policy ike_policy peer 10.0.0.1 key KEY mode aggressive ike_prop
ike local-id ike_policy keyid ix-router

ipsec autokey-proposal ipsec_prop esp-aes esp-sha
ipsec autokey-map sec-map any-list peer 10.0.0.1 ipsec_prop
ipsec local-id sec-map 192.168.0.0/24

ppp profile ppp1
  authentication myname ix@nec.co.jp
  authentication password ix@nec.co.jp ix-router
```

```
interface FastEthernet0.1
   encapsulation pppoe
   ip address ipcp
   ppp binding ppp1
   no shutdown

interface FastEthernet1.0
   ip address 192.168.0.1/24
   no shutdown

interface Tunnel1.0
   description To center
   tunnel mode ipsec
   ip unnumbered FastEthernet1.0
   ipsec policy tunnel sec-map out
   no shutdown
```

2. Web コンソールの操作

Ver9.2 以降の Web コンソールと同様ですので、そちらを参照してください。

3. Web コンソールによるコンフィグ設定

各値を入力後「設定ボタン」を押すと設定が反映されます。
設定変更時は、「!!注意!! 設定が変更されています。」のメッセージが表示されます。設定終了後、トップページに戻り設定の保存を行ってください。
※以下の設定コマンドのインタフェース名はギガ対応装置の場合、GigaEthernet となります。

装置の設定

「装置名とログインの設定」では以下の設定を行うことができます。

装置名とログインの設定	
装置名	装置名を設定します。
ログイン ID	初期状態では admin となります。 変更する場合は CLI で変更してください。
ログインパスワード	ログインパスワードを設定します。
Telnet サーバ機能	telnet サーバの有効無効を設定します。（Ver.8.1 以降）

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

hostname [装置名]
username [ログイン ID] password plain [ログインパスワード] administrator

telnet-server ip enable
```

「装置時刻の設定」では以下の設定を行うことができます。

装置時刻の設定	
装置時刻	装置の時刻，タイムゾーンを設定します。
NTP サーバ アドレス	NTP サーバアドレスを設定します。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

clock [設定時刻]
timezone [タイムゾーン]

ntp server [NTP サーバアドレス]
```

ネットワークの設定

LAN 側ネットワークの設定を行います。

LAN 側ネットワークの設定	
IP アドレス	IP アドレス，セカンダリ IP アドレスを設定します
DHCP サーバ機能	LAN インタフェースで DHCP サーバの使用を設定します。
割り当て範囲	DHCP サーバで割り当てるアドレスの範囲を設定します。

設定時は、以下のコンフィグが設定されます。

```
【設定コマンド】

ip dhcp enable   : DHCP サーバ有効時

ip access-list web_console permit ip src any dest [IP アドレス]/32
ip access-list web_console permit ip src any dest [セカンダリ IP アドレス]/32

proxy-dns ip enable
proxy-dns ip query-interval 1

http-server ip access-list web_console

! DHCP プロファイル名は web_[LAN インタフェース名]となります。
ip dhcp profile web_fastethernet1.0
   assignable-range [割り当て範囲]
   dns-server [IP アドレス] [セカンダリ IP アドレス]

interface FastEthernet1.0
   ip address [IP アドレス]
   ip address [セカンダリ IP アドレス] secondary
   ip dhcp binding web_fastethernet1.0   : DHCP サーバ有効時
   no shutdown
```

現在の IP アドレスを変更すると、設定実行時にアドレスが変更され、装置へのアクセスができなくなります。設定後は、変更後の IP アドレスで再度ログインしてください。

プロバイダ接続の設定

WAN 側インタフェースの設定を行います。PPPoE 接続または、IP 接続のいずれかの設定が可能です。接続方法を変更する場合は、現在の設定を削除後、新しい設定を行ってください。

PPPoE 接続は 2 つまで設定可能です。1 つ目の接続の場合、「PPPoE 基本接続」を選択してください。2 つ目の接続は、1 つ目の接続を設定後、「PPPoE 追加接続」を選択してください。

PPPoE 基本接続の設定/PPPoE 追加接続	
接続名	Web コンソールの画面表示に使用します。
ユーザ ID	PPPoE 接続のためのユーザ ID を設定します。
パスワード	PPPoE 接続のためのパスワードを設定します。
IP アドレス	IPCP で設定する場合は自動設定を選択してください 手動の場合は IP アドレスを入力してください。
DNS アドレス	IPCP で設定する場合は自動設定を選択してください。 手動の場合は IP アドレスを入力してください。
ルーティング	追加接続の場合のみ設定します。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】

ip route default FastEthernet0.1
ip route [ルーティング] FastEthernet0.2　: 追加接続の場合

proxy-dns interface FastEthernet0.1 priority 254　: DNS アドレス自動設定時

proxy-dns server [DNS アドレス 1] priority 254　　: DNS アドレス手動設定時
proxy-dns server [DNS アドレス 2] priority 254　　: DNS アドレス手動設定時

!PPP プロファイル名は GigaEthernet の装置の場合 web_gigaethernet0.1 となります。
!追加接続は web_fastethernet0.2 となります。
ppp profile web_fastethernet0.1
  authentication myname [ユーザ名]
  authentication password [ユーザ名] [パスワード]

!追加接続は FastEthernet0.2 となります。
interface FastEthernet0.1
  description [接続名]
  encapsulation pppoe
  auto-connect
  ppp binding web_fastethernet0.1
  ip address ipcp
  ip mtu 1454
  ip tcp adjust-mss auto
  ip napt enable
  ip napt static FastEthernet0.1 udp 500
  no shutdown
```

直接 IP アドレスを設定する場合、および DHCP でアドレスを付与する場合は、「IP 接続の設定」から設定を行います。

IP 接続の設定	
接続名	Web コンソールの画面表示に使用します。
DHCP クライアント機能	DHCP でアドレスを付与する場合に使用します。
IP アドレス	IP アドレスを設定します。 DHCP クライアントを使用しない場合に設定します。
デフォルトルート	デフォルトルートのネクストホップを設定します。 DHCP クライアントを使用しない場合に設定します。
DNS アドレス	DNS サーバを設定します。2 個まで設定可能です。 DHCP クライアントを使用しない場合に設定します。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】

ip route default [デフォルトルート]

proxy-dns interface FastEthernet0.0 priority 254 :DHCP クライアント使用時
proxy-dns server [DNS アドレス 1] priority 254   :DNS アドレス指定時
proxy-dns server [DNS アドレス 2] priority 254   :DNS アドレス指定時

interface FastEthernet0.0
  description [接続名]
  ip address dhcp receive-default   :DHCP クライアント使用時
  ip address [IP アドレス]          :IP アドレス指定時
  ip napt enable
  ip napt static FastEthernet0.0 udp 500
  no shutdown
```

VPN 接続（IPsec 接続）の設定

IPsec 接続の場合は、「IPsec 接続の設定」を選択します。Tunnel インタフェースは、接続番号―1 の番号のインタフェースを使用します。接続番号が#1 の場合、Tunnel0.0 を使用します。

IPsec トンネル接続の設定		
接続名		Web コンソールの画面表示に使用します。
接続元 WAN 側アドレス		固定アドレスまたは動的アドレスを選択します。
接続先	WAN 側アドレス	IPsec の接続先のアドレスを設定します。 接続先が動的アドレスの場合、アドレスは設定不要です。
	LAN 側ネットワーク	接続先装置の LAN 側ネットワークを設定します。
ルーティング		スタティックルートの宛先を設定します。
IKE	事前共有鍵	事前共有鍵を設定します。
	アルゴリズム	暗号化アルゴリズム：AES,３DES,DES 認証アルゴリズム　：SHA,MD5
	ID	アグレッシブモード時の ID を設定します。 Initiator の場合は自分の ID（Local-ID） Responder の場合は相手の ID（Remote-ID）
IPsec	アルゴリズム	暗号化アルゴリズム：AES,３DES,DES 認証アルゴリズム　：SHA,MD5

いくつかの動作、設定値は、接続先と接続元の WAN 側 IP アドレスの固定 IP アドレス，動的 IP アドレスの組み合わせによって決定します。

IPsec ローカル ID/リモート ID は、接続先装置にて対応する値を設定する必要があります。

接続元 WAN	固定 IP アドレス	動的 IP アドレス	固定 IP アドレス	動的 IP アドレス
接続先 WAN	固定 IP アドレス	固定 IP アドレス	動的 IP アドレス	動的 IP アドレス
モード	メイン	アグレッシブ	アグレッシブ	設定できません
動作	―	Initiator	Responder	設定できません
IPsec ローカル ID	0.0.0.0/0	接続元 LAN 側	0.0.0.0/0	設定できません
IPsec リモート ID	0.0.0.0/0	0.0.0.0/0	接続先 LAN 側	設定できません

設定時は以下のコンフィグが設定されます。

【設定コマンド】
Tunnel は接続番号-1 を使用します。
ポリシー名等は接続番号を使用します。

以下は接続番号#1 の場合になります。

```
ip route [接続先 LAN 側ネットワーク] Tunnel0.0
ip route [ルーティング] Tunnel0.0

ip access-list web_vpnlist permit ip src any dest any

webcon remote-lan 20.0.0.0/24 Tunnel0.0

ike proposal web_vpn1ikeprop encryption [IKE 暗号アルゴリズム]
                                        hash [IKE 認証アルゴリズム]
ipsec autokey-proposal web_vpn1secprop [IPsec 暗号アルゴリズム]
                                                [IPsec 認証アルゴリズム]

!接続元固定―接続先固定
ike policy web_vpn1ikepolicy peer [接続先 WAN 側アドレス] key [事前共有鍵]
                                        mode main web_vpn1ikeprop
ipsec autokey-map web_vpn1secpolicy web_vpnlist peer [接続先 WAN 側アドレス]
                                                        web_vpn1secprop

!接続元動的―接続先固定
ike policy web_vpn1ikepolicy peer [接続先 WAN 側アドレス] key [事前共有鍵]
                                        mode aggressive web_vpn1ikeprop
ike keepalive web_vpn1ikepolicy 30 6
ike local-id web_vpn1ikepolicy fqdn [IKE ID]
ike suppress-dangling web_vpn1ikepolicy
!
ipsec autokey-map web_vpn1secpolicy web_vpnlist peer [接続先 WAN 側アドレス]
                                                        web_vpn1secprop
ipsec local-id web_vpn1secpolicy [接続元 LAN 側ネットワーク]

!接続元固定―接続先動的
ike policy web_vpn1ikepolicy peer any key [事前共有鍵]mode aggressive
                                                        web_vpn1ikeprop
ike remote-id web_vpn1ikepolicy fqdn [IKE ID]
ipsec dynamic-map web_vpn1secpolicy web_vpnlist web_vpn1secprop
                                                        ike web_vpn1ikepolicy
ipsec remote-id web_vpn1secpolicy [接続先 LAN 側ネットワーク]


interface Tunnel0.0
  description [接続名]
  tunnel mode ipsec
  ip unnumbered FastEthernet1.0
  ip tcp adjust-mss auto
  ipsec policy tunnel web_vpn1secpolicy out
  no shutdown
```

VPN 接続（IP トンネル接続）の設定

IP トンネル接続では、GRE トンネルによる接続を行います。「IP トンネル接続設定」から設定します。

IP トンネル接続の設定		
接続名		Web コンソールの画面表示に使用します。
接続元	WAN 側アドレス	使用している WAN インタフェースを選択します。
接続先	WAN 側アドレス	トンネル接続先のアドレスを設定します。
	LAN 側ネットワーク	接続先装置の LAN 側ネットワークを設定します。
ルーティング		スタティックルートの宛先を設定します。

設定時は以下のコンフィグが設定されます。

【設定コマンド】
Tunnel は接続番号-1 を使用します。

以下は接続番号#1 の場合になります。

```
ip route [接続先 LAN 側ネットワーク] Tunnel0.0
ip route [ルーティング] Tunnel0.0

interface Tunnel0.0
  description [接続名]
  tunnel mode gre ip
  tunnel destination [接続先 WAN 側アドレス]
  tunnel source [接続元 WAN 側アドレス]
  tunnel keepalive
  ip unnumbered FastEthernet1.0
  ip tcp adjust-mss auto
  no shutdown
```

IPv4 スタティックフィルタの設定

IPv4 スタティックフィルタの設定を行います。

[詳細設定]から、[IPv4 スタティックフィルタの設定]を選択します。インタフェース毎にメニューが表示されますので、フィルタを設定するインタフェースの設定追加を選択します。

IPv4 スタティックフィルタの設定		
シーケンス番号		シーケンス番号を選択します。
方向/動作		in/out と通過（permit）/廃棄（deny）を選択します。
プロトコル		プロトコル：TCP,UDP,IP,ICMP,その他 その他を選択した場合はプロトコル番号を設定します。
送信元	IP アドレス	すべてまたは、IP アドレスを設定します。
	ポート番号	すべてまたは、ポート番号を設定します。 プロトコルが TCP,UDP の場合に設定します。
送信先	IP アドレス	すべてまたは、IP アドレスを設定します。
	ポート番号	すべてまたは、ポート番号を設定します。 プロトコルが TCP,UDP の場合に設定します。
ログ		廃棄ログの記録のする/しないを選択します。

[詳細設定]から[IPv4 スタティックフィルタの設定]を選択すると、設定したフィルタの一覧が表示されます。変更する場合は、各リストの[編集]を選択してください。削除する場合は、[削除]を選択してください。

シーケンス番号は使用済みの番号は使用できません。設定済みの内容を変更するか、または、一旦削除後、新規に登録してください。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
アクセスリスト名等はシーケンス番号を使用します。
設定されるコマンドのみ表示しています。

ip access-list web_f_[インタフェースの番号部分]_[方向(i/o)]_[シーケンス番号] [動作] [プロトコル] src [送信元 IP アドレス] sport [送信元ポート番号] dest [送信先 IP アドレス] dport [送信先ポート番号]

interface [インタフェース]
  ip filter [アクセスリスト名] [シーケンス番号] [方向]
```

静的 NAPT の設定

WAN インタフェースへ静的 NAPT の設定を行います。

[詳細設定]から、[静的 NAPT の設定]を選択します。インタフェース毎にメニューが表示されますので、静的 NAPT を設定するインタフェースの設定追加を選択します。

静的 NAPT の設定		
プロトコル		プロトコル：
ポート番号		プロトコルでポート指定を選択した場合に設定します。
プライベート側	IP アドレス	プライベート側の IP アドレスを設定します。
	ポート番号	変換なしまたは、ポート番号を設定します。

[詳細設定]から[静的 NAPT の設定]を選択すると、設定した静的 NAPT の一覧が表示されます。変更する場合は、各リストの[編集]を選択してください。削除する場合は、[削除]を選択してください。

設定時は以下のコンフィグが設定されます。

```
【設定コマンド】
設定されるコマンドのみ表示しています。

interface [インタフェース]
  ip napt service web_[通し番号] [プライベート側アドレス] [プライベート側ポート番号] [プロトコル番号] [ポート番号]
```

4. Web コンソールの表示項目

Web コンソールで表示する項目は以下のとおりです。

- トップページ

装置	
装置	装置名を表示します。 hostname コマンドで設定した名前を表示します。
バージョン	ソフトウェアバージョンを表示します。 show version の Software バージョンを表示します。
稼働時間	装置の起動時間を表示します。 show uptime の System uptime を表示します。
稼働率	システムの Utilization を表示します。 show utilization の System utilization を表示します。
メモリ	メモリの使用量をパーセントで表示します。 show memory の Heap memory の memory used を表示します。
内部温度	装置内部温度を表示します。 正常範囲の場合は青、アラーム発生時は赤で表示されます。 show environment の Internal temperature を表示します。
内部電圧	装置内部電圧を表示します。 正常範囲の場合は青、異常の場合は赤で表示されます。 show environment の 3.3 volt line measured を表示します。
NTP	NTP の状態を表示します。 show ntp の NTP status を表示します。 同期済み：サーバと同期がとれています 非同期　：サーバと同期がとれていません 未設定　：NTP が設定されていません

ネットワーク	
デバイス	デバイス名を表示します。 設定可能な機種 WAN 側(FE0)：FastEthernet0（IX2005） WAN 側(GE0)：GigaEthernet0（その他の装置） LAN 側(FE1)：FastEthernet1（IX2005） LAN 側(GE1)：GigaEthernet1（IX2105） LAN 側(GE2)：GigaEthernet2（IX2207） GE1　　：GigaEthernet1（IX2207） USB0　　（IX2207） USB1　　（IX2207） 表示のみの機種 デバイス名を表示します。 ただし、T1 カード、4BRI-ST カード実装時は、デバイス名は表示されません。
接続状態	デバイスの状態を表示します。 show devices の情報を表示します。 up の場合は、speed と duplex を表示します。 また、SW-HUB の場合、ポート毎の状態を表示します。
送信量	現在のデバイスの送信の使用率を表示します。 show utilization の last transmit util を表示します。
受信量	現在のデバイスの受信の使用率を表示します。 show utilization の last receive util を表示します。

プロバイダ接続（設定可能な機種）	
プロバイダ接続	ネットワークの接続形態を表示します。 IP 接続：基本インタフェースに IP アドレスが設定 PPPoE 基本接続：PPPoE1 つ目を使用 PPPoE 追加接続：PPPoE2 つ目を使用 未接続：インタフェース未設定または、上記 3 種類以外の設定の場合。構成の詳細は前項の対応構成を参照してください。
接続名	接続名を表示します。 show interfaces の Description（description で設定した内容）を表示します。 PPPoE 使用で description 未設定の場合は PPP プロファイル名が表示されます。
状態	接続状態を表示します。 接続： 通信可能です。 IP 接続の場合は、リンク up している状態です。 PPPoE の場合は、IPCP まで OPEN している状態です。 アドレス取得中： DHCP の場合のみ表示されます。 DHCP サーバからアドレス取得を行っている状態です。 IPCP 確立中： PPPoE の場合のみ表示されます。 認証が終了し、IPCP の接続を行っている状態です。 認証中： PPPoE の場合のみ表示されます。 LCP が OPEN し、認証中の状態です。 この状態のまま接続できない場合は、ppp profile のユーザ ID、パスワードや ppp profile 名などの設定に誤りがある可能性があります。 接続されていません： PPPoE が確立できない状態です。 この状態のまま接続できない場合は、物理的な接続に問題がある可能性があります。

IP 接続（表示機能のみの機種）	
インタフェース名	インタフェース名を表示します。
接続名	接続名を表示します。 show interfaces の Description（description で設定した内容）を表示します。 PPPoE 使用で description 未設定の場合は PPP プロファイル名が表示されます。
状態	接続状態を表示します。 接続： 通信可能です。 IP 接続の場合は、リンク up している状態です。 PPPoE の場合は、IPCP まで OPEN している状態です。 アドレス取得中： DHCP の場合のみ表示されます。 DHCP サーバからアドレス取得を行っている状態です。 IPCP 確立中： PPPoE の場合のみ表示されます。 認証が終了し、IPCP の接続を行っている状態です。 認証中： PPPoE の場合のみ表示されます。 LCP が OPEN し、認証中の状態です。 この状態のまま接続できない場合は、ppp profile のユーザ ID、パスワードや ppp profile 名などの設定に誤りがある可能性があります。 接続されていません： PPPoE が確立できない状態です。 この状態のまま接続できない場合は、物理的な接続に問題がある可能性があります。

VPN 接続	
接続番号	Tunnel インタフェースの番号+1 となります。
接続名	接続名を表示します。 description で設定した内容を表示します。
接続種別	接続種別を表示します。 IPsec　　：IPsec トンネルで接続 IP トンネル：GRE トンネルで接続
状態	接続状態を表示します。 接続：通信可能です。 IPsec の場合、IPsec-SA が作成された状態です。 GRE の場合、Tunnel インタフェースが Up した状態です。 接続されていません：通信できません。

- 装置のメンテナンス

装置の稼動状態	
起動日時	装置の起動日時を表示します。 show uptime の System started を表示します。
稼働時間	装置の起動時間を表示します。 show uptime の System uptime を表示します。
稼働率	システムの Utilization を表示します。 show utilization の System utilization を表示します。
メモリ使用量	メモリ使用量をパーセントで表示します。 show memory の Heap memory の memory used を表示します。

ソフトウェアバージョン	
ソフトウェアバージョン	ルータソフトのソフトウェアバージョンを表示します。 show version のソフトウェアバージョンを表示します。
ブートストラップ バージョン	ブートストラップのバージョンを表示します。 show version のブートストラップバージョンを表示します。

- 装置のログ

装置のログ	
ログ	show tech-support を表示します。

※文字列を表示する項目の場合、設定内容に”<”が含まれると正しく表示されません。設定の内容には”<”は使用しないでください。

IX2000/IX3000 シリーズ機能説明書

GYS-077528-001-00

2023 年　12 月　10.9（第 1.0 版）　発行

発行元　日本電気株式会社