NEC

UNIVERGE IX-V シリーズ
機能説明書

日本電気株式会社

ご注意

- 本マニュアル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。
- 本マニュアルの内容については、将来予告なしに変更することがあります。
- 本マニュアル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。

商標について

- Oracle® および Java は、オラクルおよびその関連会社の登録商標です。
- 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。

- UNIVERGE IX-V100

医療機関等での使用について

- 本製品は、医療機器、原子力設備や機器、航空宇宙機器、輸送設備や機器など、人命にかかわるシステムに組み込んでの使用は意図されておりません。
- これら設備や機器、制御システムなどに本製品を使用され、当社製品の故障により、人身事故、火災事故、社会的な損害などが生じても、当社ではいかなる責任も負いかねます。

輸出に関する注意事項

- 本製品は日本国内仕様であり、外国の規制などには準拠しておりません。
- 本製品は日本国外で使用された場合、当社は一切責任を負いかねます。
- また、当社は本製品に関し海外での保守サービスおよび技術サポートなどは行っておりません。
- 本製品は外国為替、外国貿易法の規定および米国輸出管理規則により規制役務に該当する可能性があります。
- 本製品の日本国外への持ち出し、および日本居住者以外の使用はできません。

ユーザーズガイドの案内

- UNIVERGE IX-V シリーズが起動までの準備（クラウドの設定およびライセンス）は、別紙のユーザーズガイドを参照してください。

目次

1章 機能概要

本章では、UNIVERGE IX-V 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 UNIVERGE IX-V シリーズの機能の特徴

UNIVERGE IX-V 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

ルーティングプロトコル

- スタティックルーティング
- BGP4
- ポリシールーティング

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

信頼性向上

- 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
- IPsec トンネル冗長化機能

■1.2 諸元

1.2.1 UNIVERGE IX-V シリーズ ソフトウェア仕様

分類	機能	備考
サポートプロトコル	IPv4	
ルーティング プロトコル	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 プロキシ DNS NAT/NAPT PPTP マルチパススルー TCP MSS 調整	
トンネル機能	L2TPv2（LNS）	
IPsec 機能	IPsec(ESP) IKE(メインモード/アグレッシブモード) IKEv2 IPsec 高速処理対応 NAT トラバーサル機能	
FireWall 機能	IPv4 スタティックフィルタ IPv4 ダイナミックフィルタ	
冗長構成	ネットワークモニタ	
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 SSHv2 サーバ	
NetMeister	DDNS 設定 NetMeister 対応	

1.2.2 UNIVERGE IX-V シリーズ 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。

分類	項目	IX-V100 仕様	default	制限値
IPv4	ARP エントリ数	2048	2048	65536
	スタティックルート数	10000	-	なし
	ルート数	100000 1000 ※2	100000	100000
NAT	静的 NAT 数	8192	-	なし
	静的 NAT 設定数	2048	-	なし
	動的 NAT 数	2048	-	なし
	キャッシュサイズ	8192	512	65535
NAPT	キャッシュサイズ	250000	65535	250000
	静的 NAPT/サービス数	255	-	なし
	アクセスログの保存サイズ	128	-	128
DHCP サーバ	プロファイル設定数	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
	グローバルでのプロファイル割り当て数	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
	クライアント設定数（装置当たり）	1024	-	65535
	固定クライアント設定数	32	-	なし
BGP4	ピア数	1000	-	なし
	BGP 広告経路数（ピア数×ルート数）	1000000	-	1000000
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	256	-	なし
プロキシ DNS	ipv4 固定サーバ設定数	2	-	なし
	ipv4 動的サーバ設定数	1	-	なし
	ipv4 セッション数	254	254	1024
DNS リゾルバ	固定/動的サーバ設定数	3	-	なし
SNTP クライアント	サーバ設定数	3	-	なし
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）	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	-	なし
IP アクセスリスト	アクセスリスト名の数	5120	-	なし
	１アクセスリスト当たりの各エントリ数	2048	-	なし
	アクセスリスト総エントリ数	10000	-	なし
	アクセスリストキャッシュ数	50000	20000	50000
	ダイナミックアクセスリスト名の数	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	512	-	なし
	ダイナミックアクセスリストキャッシュ数	250000	32768	250000

※1 アクセスリストの最適化有効時は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。

※2 BGP ピア数 1000 の場合

分類	項目	IX-V100 仕様	default	制限値
IKE/IKEv2/IPsec	対地数	1000	-	1000
	ポリシーに対応するプロポーザル設定数	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
ルートマップ	ルートマップ数	256 ※1	-	なし
プレフィックスリスト	プレフィックスリスト数	1024	-	なし
	1 リストのエントリ数	1024	-	なし
	総エントリ数	2048	-	なし
UFS キャッシュ	最大キャッシュ数（IPv4）	200000	100000	500000
	ハッシュサイズ	8192	2048	65536
システム	ログインアカウント設定数	8	-	50
	ユーザ名長	16	-	16
	パスワード長	80	-	249
	SSH 同時ログイン数	8	-	8
	コンソール同時ログイン数	1	-	1
	コンフィグモード同時操作数	1	-	1

※1 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。

■1.3 制限事項

UNIVERGE IX-V 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

- ポリシールーティング、フィルタ等でアクセスリストを大量に設定する場合は、アクセスリストの最適化を有効化してください。詳細はアクセスリストの章を参照してください。
- VRF 機能には対応していません。
- マルチパス機能には対応しておりません。

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。
- 経路集約機能には対応しておりません。
- 動的ピア機能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。
- 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。
- L2TP(LNS)機能は IPsec（IKEv1）との併用が必須です。
- L2TP(LAC)機能には対応しておりません。
- ダイナミック VPN 機能には対応しておりません。

DNS 関連

- ローカル DNS サーバ機能による 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。

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。

GigaEthernet 関連

- 10Gbps の転送性能には、ハードウェア支援(SR-IOV)の利用が必要です。

2章 ルータの設定

本章では、UNIVERGE IX-V 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

ルータが正常に起動すると login プロンプトが表示されます。
初期状態でログインすると初期ユーザ登録モードになり、ユーザ登録と保存、再起動のみが行えます。

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# co [TAB]
Router# configure

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# s [TAB]
  svintr-config   -- Enters global configuration mode (supervisor interrupt)
  show            -- Show running system information
```

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# co [Enter]
configure を実行

Router# sh ver [Enter]
show version 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	EXEC モードに遷移（後述）

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。

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 24」で元に戻ります。

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。

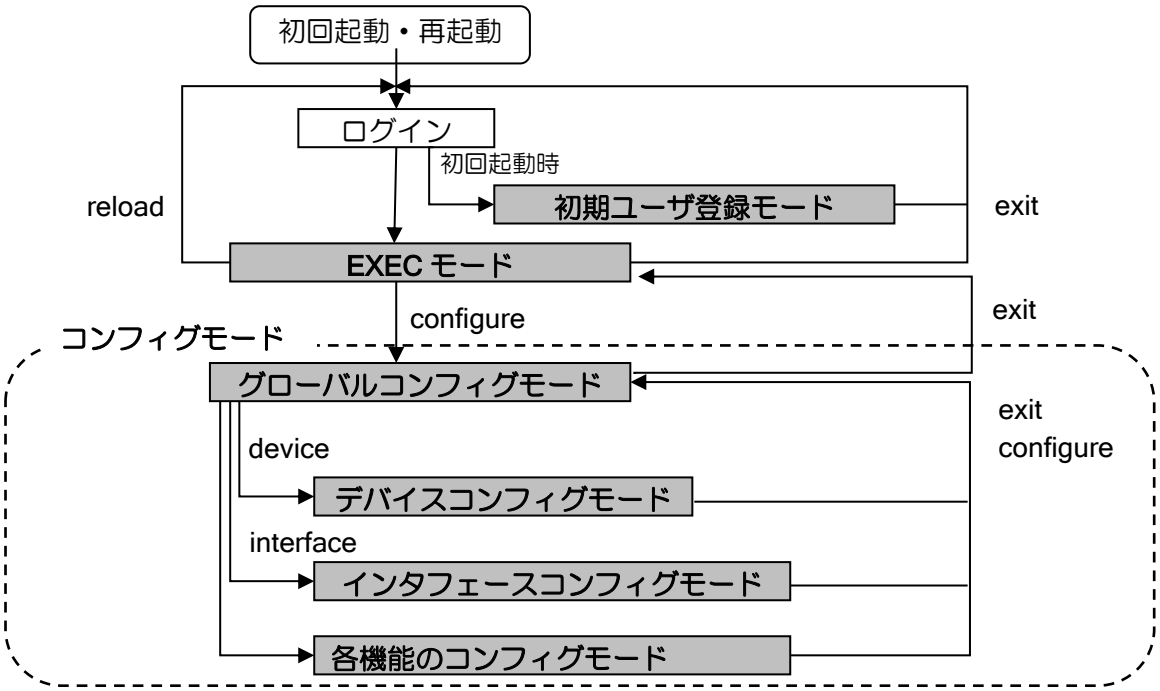
- 初期ユーザ登録モード
  - 初回起動時に入るモードです。ユーザの追加コマンドを利用できます。
  - プロンプトは「Router(init)# 」です。

- EXEC 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 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（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。

- 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、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 EXEC 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。

2.1.3.1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、インタフェースへの設定は、

以下のインタフェースモードで行います。

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。

interface GigaEthernet0.0	GigaEthernet0.0 インタフェース設定 IPv4 アドレス設定や NAT アドレス変換設定等の特定インタフェースに関連する設定を行います。

このほかにも、Loopback や Null、Tunnel 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。

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 IX-V Series IX-Vxxx Software, Version X.X.X, RELEASE SOFTWARE
      :
```

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。

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
! NEC IX-V Series IX-Vxxx Software, Version X.X.X, RELEASE SOFTWARE
      :
```

初期状態では設定は保存されていないため、以下のように表示されます。

```
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、再起動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。
保存中は再起動したり、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
Building configuration...
% Warning: do NOT enter CNTL/Z while saving to avoid config corruption.
Router(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。
初期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 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# configure
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# username admin password plain *********
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

初期導入時に、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。
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

初期状態ではログインすると初期ユーザ登録モードになり、アカウント設定のみが行えます。Administrator レベルのアカウントを作成後に再ログインすることで EXEC モードに遷移できます。
初期ユーザ登録モード以外でもアカウント設定は可能です。

username	アカウント設定

【設定例】

username USERNAME password plain 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
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

IKE の事前共有鍵等を 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
ikev2 authentication	IKEv2 認証設定

※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 tech-support	テクニカルサポート情報の表示
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

■2.3物理、リンクレイヤの設定

物理、リンクレイヤについて必要なコマンドは次のとおりです。

2.3.1 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。

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】
IX-V100 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】
IX-V100 の GE2 基本ポート：GigaEthernet2.0

2.3.2 GigaEthernet インタフェースの設定

UNIVERGE IX-V シリーズでは、デバイスの設定は自動で行われ、変更することはできません。

デバイス・インタフェース情報の表示

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	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

2.3.3 Loopback インタフェースの設定

UNIVERGE IX-V 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。

2.3.4 Null インタフェースの設定

UNIVERGE IX-V 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。

2.3.5 トンネルインタフェースの設定

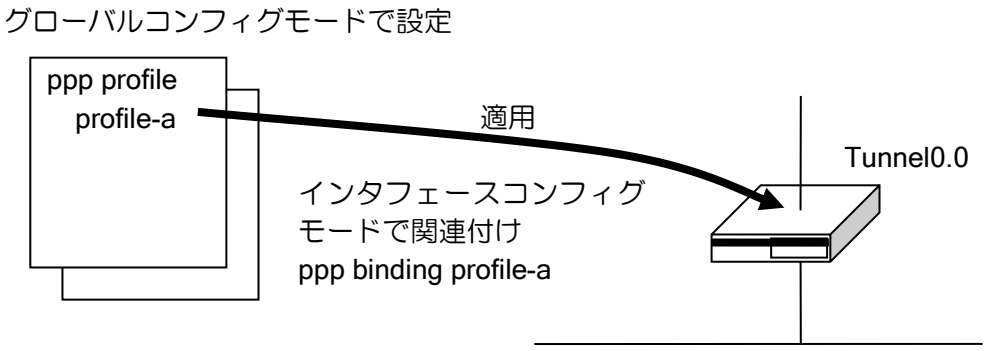
UNIVERGE IX-V シリーズでは、トンネル機能をサポートしています。詳細はトンネルの節にて説明します。トンネルも、通常のインタフェースのひとつとして振舞います。

■2.4 PPP の設定

UNIVERGE IX-V シリーズでは、L2TP LNS 機能で使用します。

2.4.1 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。



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

2.4.2 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 acfc	Address-and-Control-Field-Compression の有効設定
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 pfc	Protocol-Field-Compression の有効設定

2.4.2.1 LCP 認証プロトコルの設定

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 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】L2TP LNS 機能で使用する場合
ppp profile lns
   authentication request chap
   authentication password user1 pass1
   authentication password user2 pass2
   authentication password user3 pass3
!
```

UNIVERGE IX-V 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。

(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。

(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。

2.4.2.2 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 provide-remote-dns	相手からの DNS アドレス要求の有効設定
ipcp request-ip-address ipcp provide-ip-address	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

2.4.3 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

■2.5 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.）

2.5.1 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。

ip address	IPv4 アドレスの登録

【設定例】

ip address 192.168.0.254/24
※設定変更時はインタフェースが一旦 down します。

2.5.2 unnumbered アドレスの設定

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は動作が停止します。

2.5.3 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。

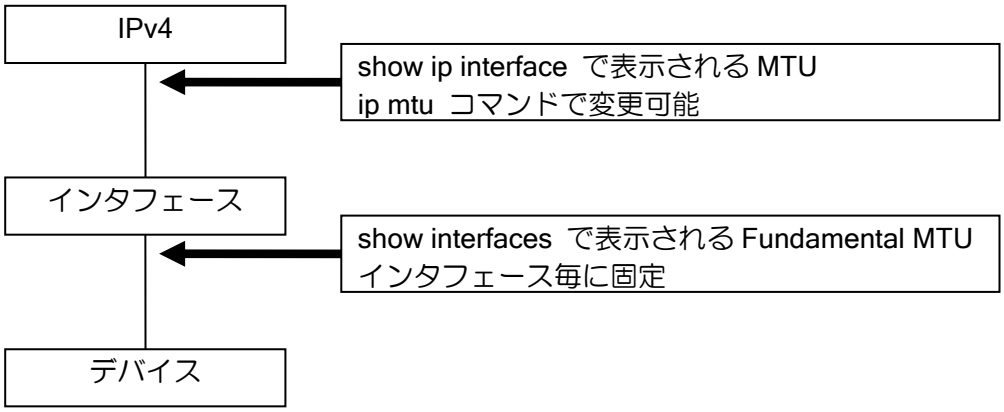
ip mtu	MTU の変更 （インタフェースコンフィグモード）

【設定例】

```
ip mtu 1000
ip tcp adjust-mss auto
```

※ 「ip mtu」コマンドを設定している場合は、「ip tcp adjust-mss auto」の設定もして下さい

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。



2.5.4 TCP MSS 調整

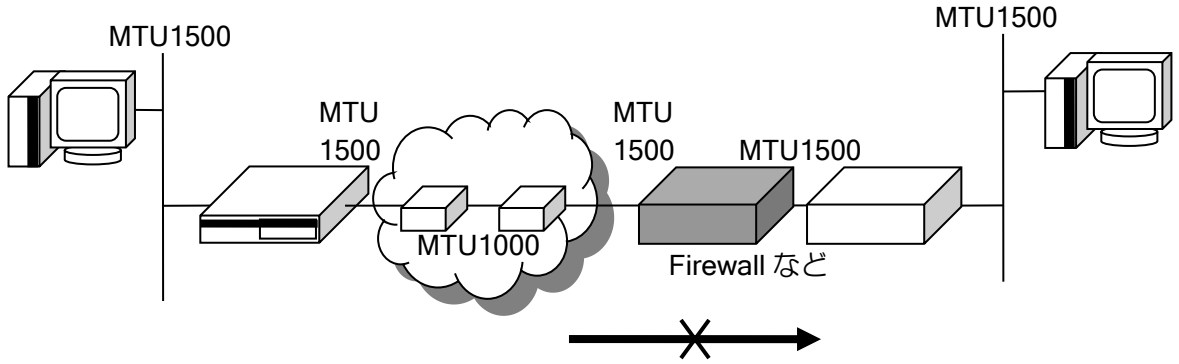
トンネルや PPPoE など MTU が 1500 でないインタフェースを利用する場合に、TCP のパケットサイズの上限をフラグメントされないサイズに制限し、性能低下を抑止する機能です。

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。

インタフェースコンフィグモード	
ip tcp adjust-mss	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。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)

【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	3DES + SHA1	1390
				AES + SHA1	1382
		なし	ー	ー	1424
	なし	あり	トランスポート	3DES + SHA1	1426
				AES + SHA1	1418
			トンネル	3DES + SHA1	1406
				AES + SHA1	1398
		なし	ー	ー	1460

2.5.5 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
```

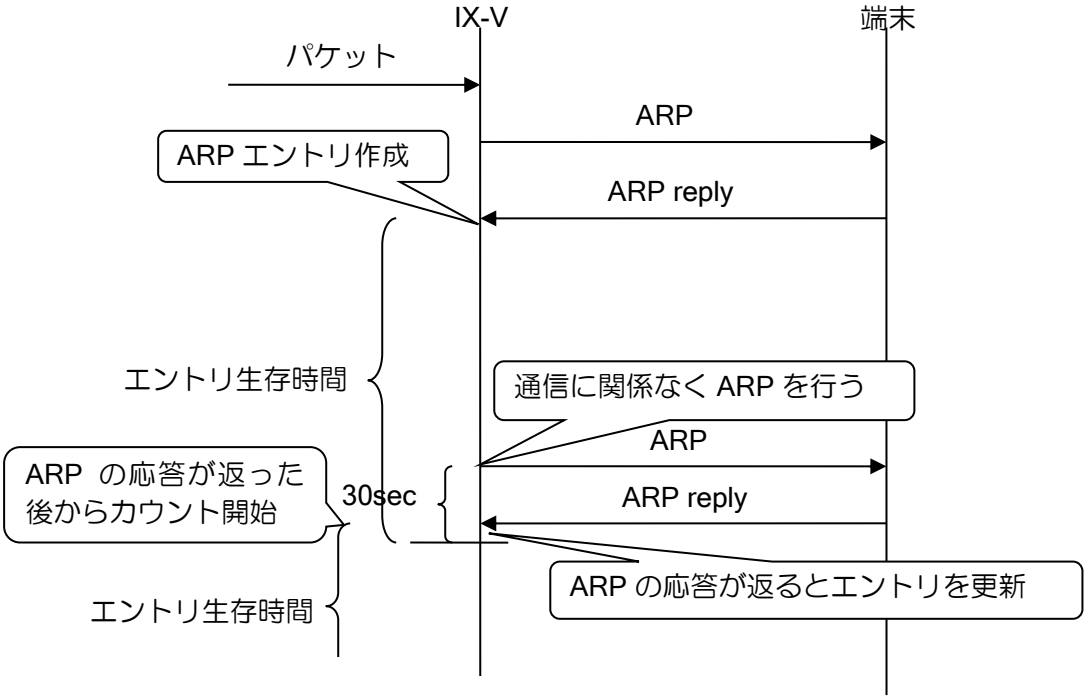
2.5.6 ARP の設定

ARP に関して、以下の設定を行うことができます。

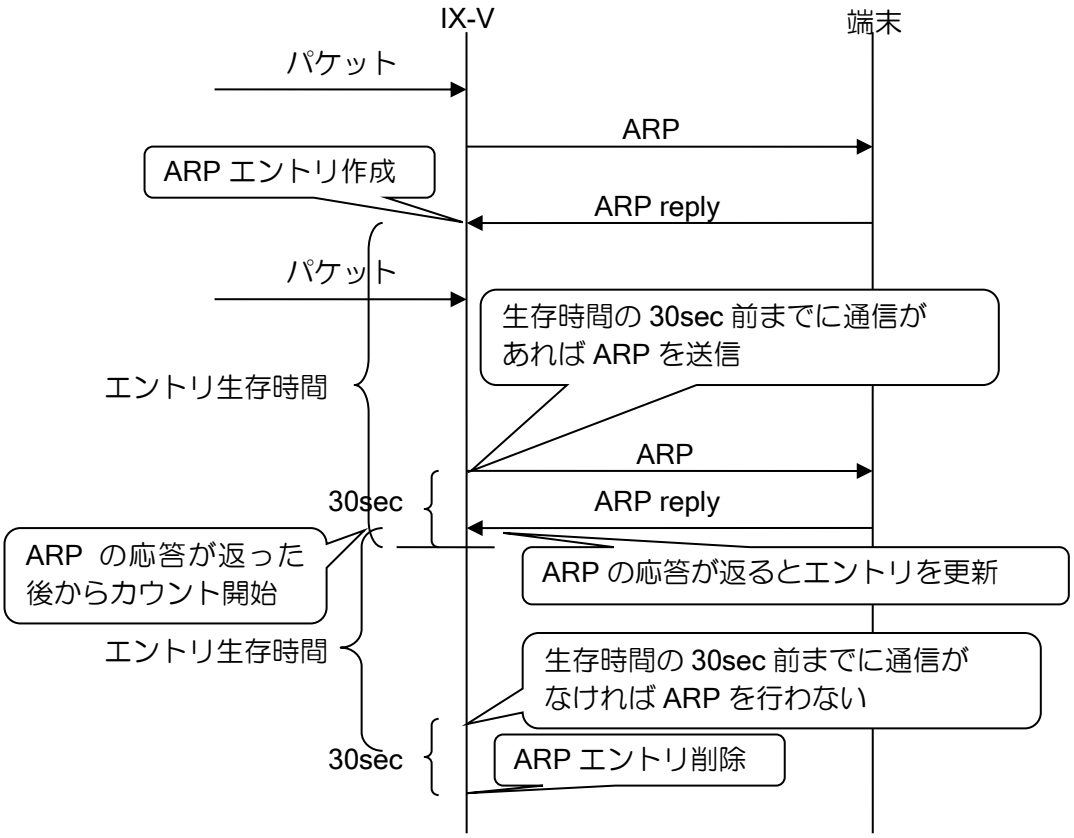
arp auto-refresh	ARP エントリ自動更新
arp timeout	ARP エントリ生存時間
arp entry	ARP エントリのスタティック登録

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、UFS キャッシュの情報から判断します。以下の場合は、UFS 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。

- 自装置から送信する通信
- ICMP 通信

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。

2.5.7 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 169.254.1.251/24
  ip directed-broadcast
  no shutdown
```

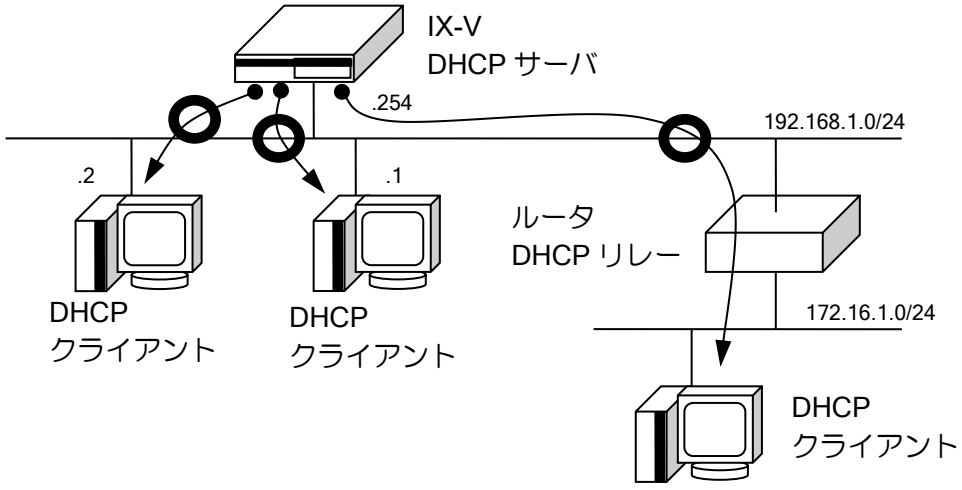
上記の設定を行うと、ダイレクトブロードキャストを設定した GigaEthernet1.0 のネットワーク
(192.168.0.0/24)のブロードキャストアドレスとなる 192.168.0.255 宛のパケットを、
GigaEthernet1.0 に転送するようになります。
ダイレクトブロードキャストを設定していない場合は、パケットを破棄します。
なお、それ以外のセグメント宛のブロードキャストパケットについては、ダイレクトブロードキャスト
設定の有無にかかわらず、ユニキャストパケットと同様に転送を行います。

■2.6 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。
DHCP のサーバ機能、クライア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。

2.6.1 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。



●⟶ DHCP によるアドレス割り当て方向

2.6.1.1 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ネットワーク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。

クラウド仮想ネットワーク上で動作する IX-V シリーズは、遠隔ネットワークに対してアドレスを払い出す方法のみが利用可能です。

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
default-gateway	デフォルトルータの通知設定

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。
subnet-mask	サブネットマスクの設定
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

- 遠隔ネットワーク上のクライアントを管理する場合

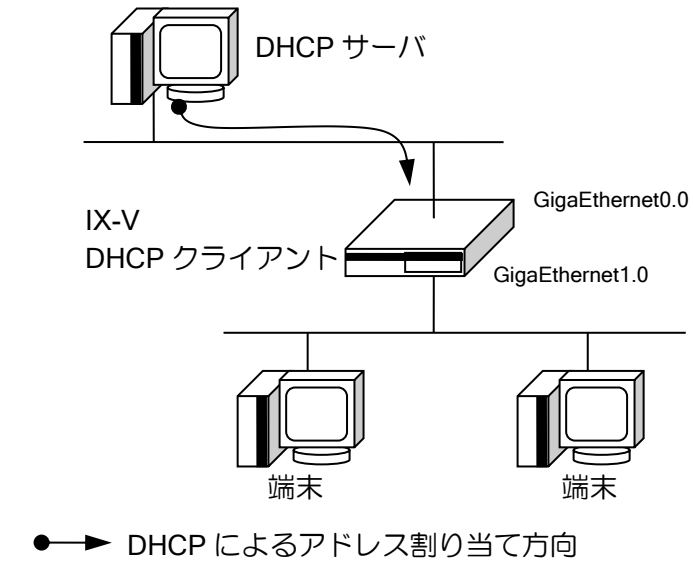
【設定例】

```
ip dhcp profile profile1
   assignable-range 192.168.1.1 192.168.1.10
   subnet-mask 255.255.255.0

ip dhcp binding profile1

interface Tunnel.0
   ip address 192.168.1.254/24
   ip dhcp enable
   no shutdown
```

2.6.2 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 GigaEthernet0.0
  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

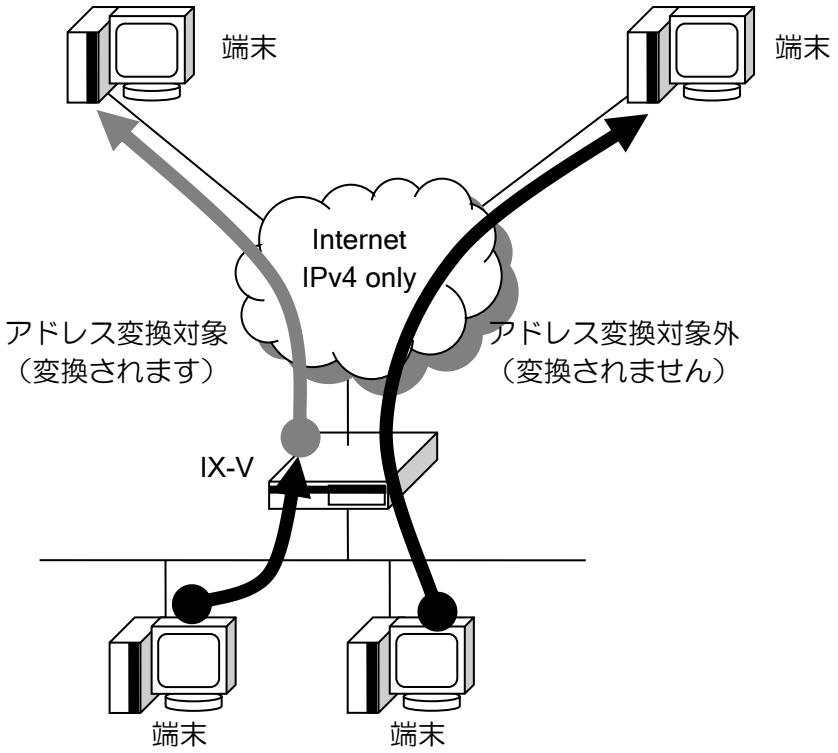
```
ip route 10.0.0.0/24 GigaEthernet0.0 dhcp

interface GigaEthernet0.0
  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 GigaEthernet0.0
   ip address dhcp receive-default distance 200 metric 10
   no shutdown
```

■2.7 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)

Oracle Cloud Infrastructure(OCI)の様なクラウド環境においては VNIC 等のイーサネットインタフェースに割り当てられたアドレス以外のアドレスに変換されたパケットは正常に転送されません。そのため、NAT/NAPT 設定で指定する変換先アドレス全てを、事前に VNIC にセカンダリ・プライベート IP アドレスとして割り当てておく必要があります。

2.7.1 NAT の設定

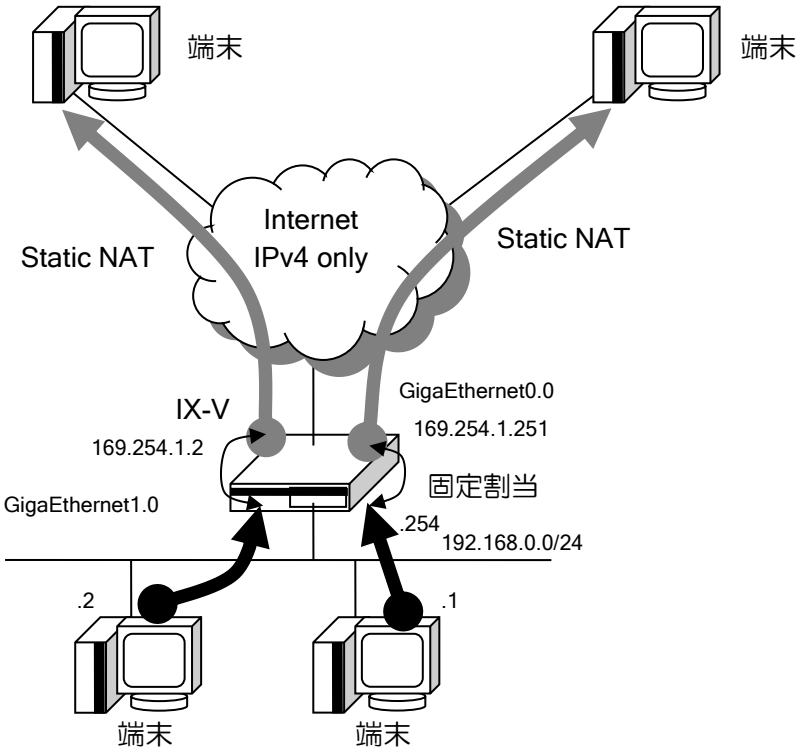
ネットワークアドレス変換（NAT）は、内部ネットワークの IPv4 アドレスを、外部ネットワークの IPv4 アドレスに変換する機能です。NAT の登録は、次のように大別することができます。

- 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。

2.7.1.1 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。



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 169.254.1.200/24
   ip nat enable
   ip nat static 192.168.0.1 169.254.1.251
   ip nat static 192.168.0.2 169.254.1.252
   no shutdown
```

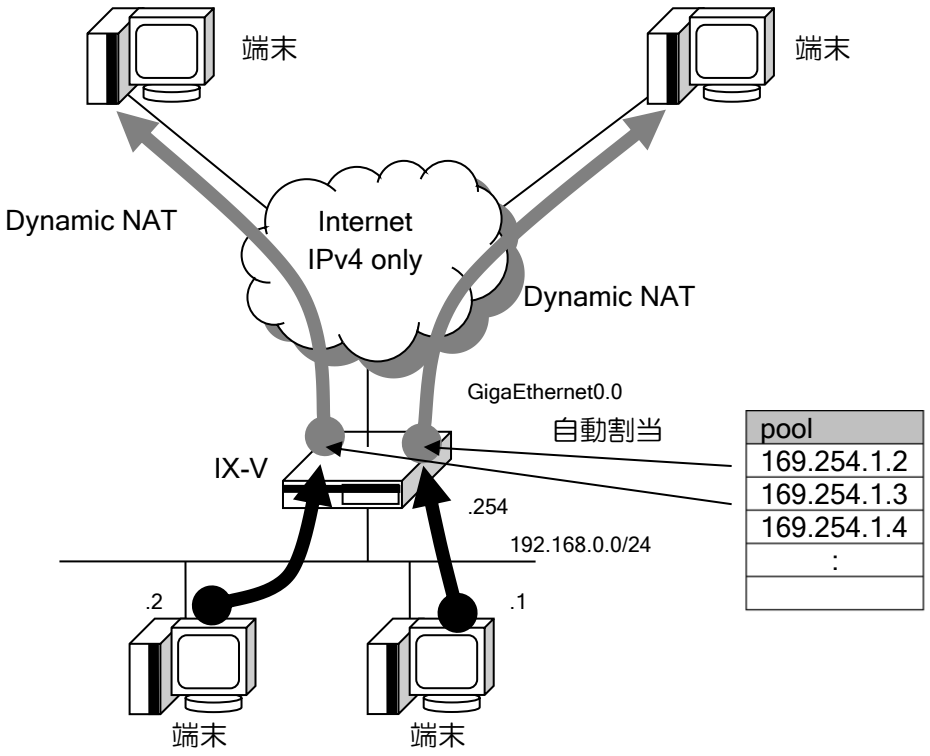
ネットワーク単位で静的 NAT の指定を行うことができます。この場合、アドレス部分は同じ値となります。複数の設定が重なっている場合は、プレフィックス長の長い方が優先されます。

```
【設定例】
192.168.0.x を 169.254.1.x に変換（x は 0～127）

interface GigaEthernet0.0
   ip address 169.254.1.200/24
   ip nat enable
   ip nat static network 192.168.0.0/25 169.254.1.0/25
   no shutdown
```

2.7.1.2 動的 NAT（Dynamic NAT）の設定

動的 NAT は、外部アドレスの数が限定されている場合に有効です。複数の IPv4 アドレスを予めプールに格納しておくことで、内部ネットワーク側の端末から外部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	外部 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】

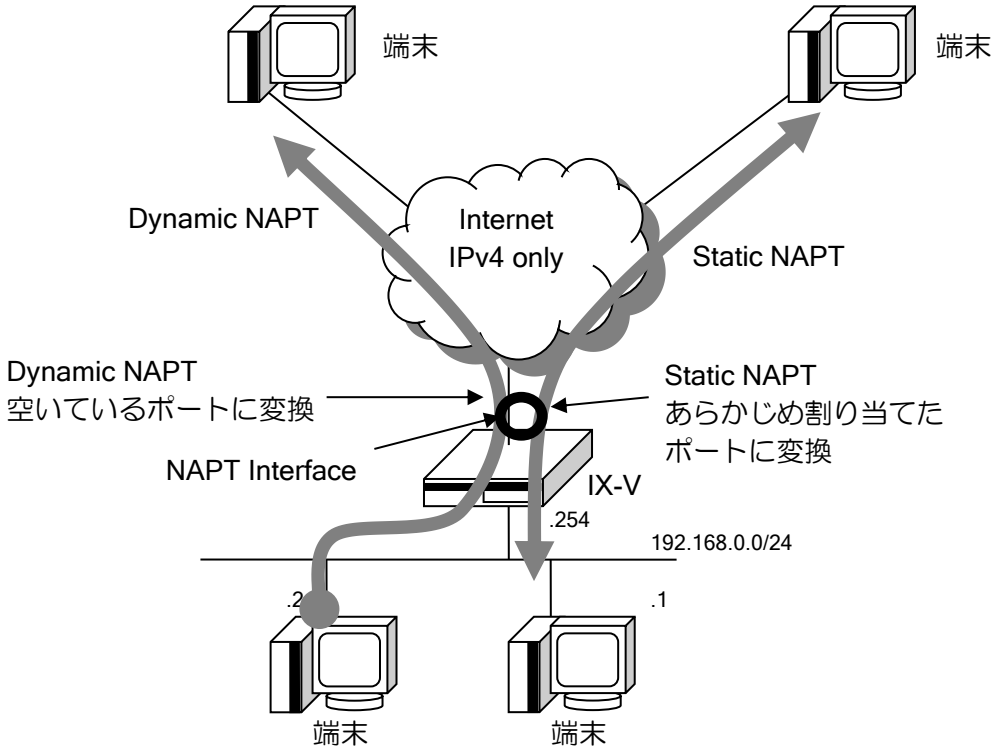
```
ip access-list access-1 permit ip src 192.168.0.0/24 dest any
ip nat pool pool-1 169.254.1.2 169.254.1.10
interface GigaEthernet0.0
   ip address 169.254.1.200/24
   ip nat enable
   ip nat dynamic list access-1 pool pool-1
   no shutdown
```

2.7.2 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 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 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（Dynamic 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（ひとつの 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、特定の内部アドレス空間に存在するサーバを外部アドレス空間に提供する場合に使用します。



2.7.2.1 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、省略時にはインタフェースアドレスが利用されます。
ip napt inside ...	内部ネットワークの端末アドレス範囲をアクセスリストによって指定します。
ip napt inside ... outside ...	NAPT 変換アドレスの複数設定、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及び保持時間設定

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>

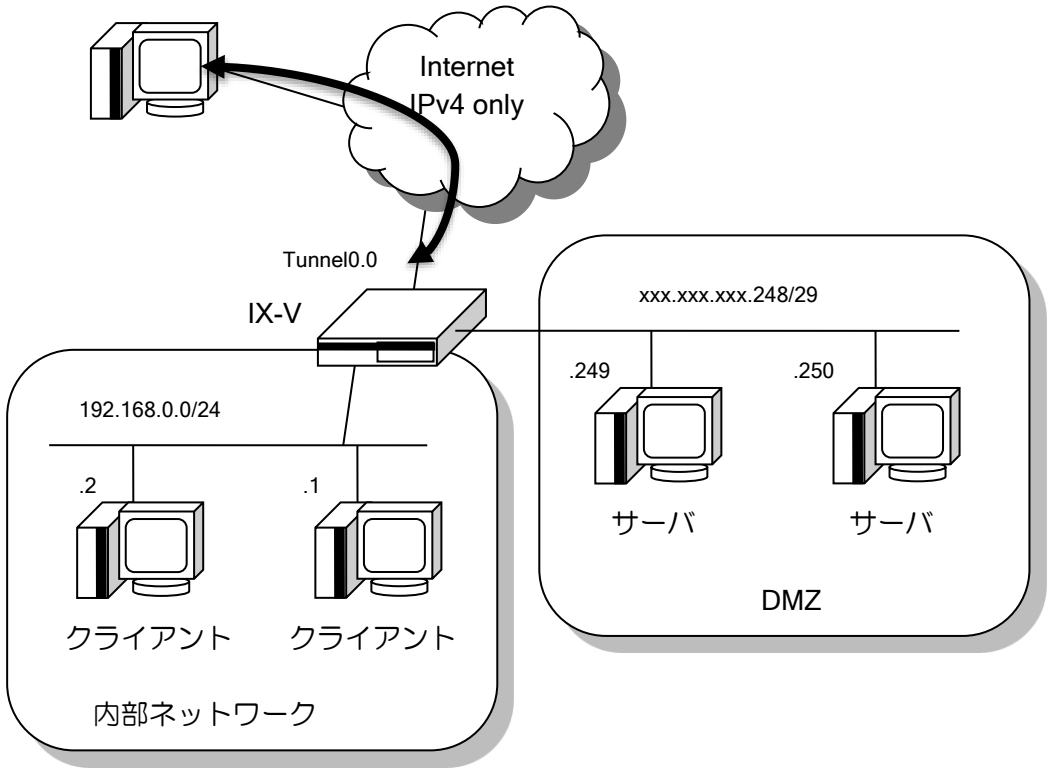
【設定例】

・端末及び外部アドレスを指定しない場合

```
interface GigaEthernet0.0
  ip address 169.254.1.200/24
  ip napt enable
  no shutdown
```

2.7.2.2 NAPT 範囲指定（DMZ の設定）

NAPT 配下の内部ネットワークを変換対象アドレス空間と変換対象外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 Tunnel0.0
  ip address 192.168.10.2/24
  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。

2.7.2.3 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 169.254.1..2 を使用
送信元が 10.10.20.0/24 の場合は NAPT アドレスに 169.254.1..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 169.254.1.251/24
   ip napt enable
   ip napt address 169.254.1.2
   ip napt inside list access-1
   ip napt inside list access-2 outside 169.254.1..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 169.254.1.2 を使用
送信元が 10.10.20.0/24 の場合は NAPT アドレスに 169.254.1.3 を使用
送信元がそれ以外の場合は、NAPT アドレスに 169.254.1.251 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 169.254.1.251/24
   ip napt enable
   ip napt inside list access-1 outside 169.254.1.2
   ip napt inside list access-2 outside 169.254.1.3
   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 169.254.1.251 で変換されます。

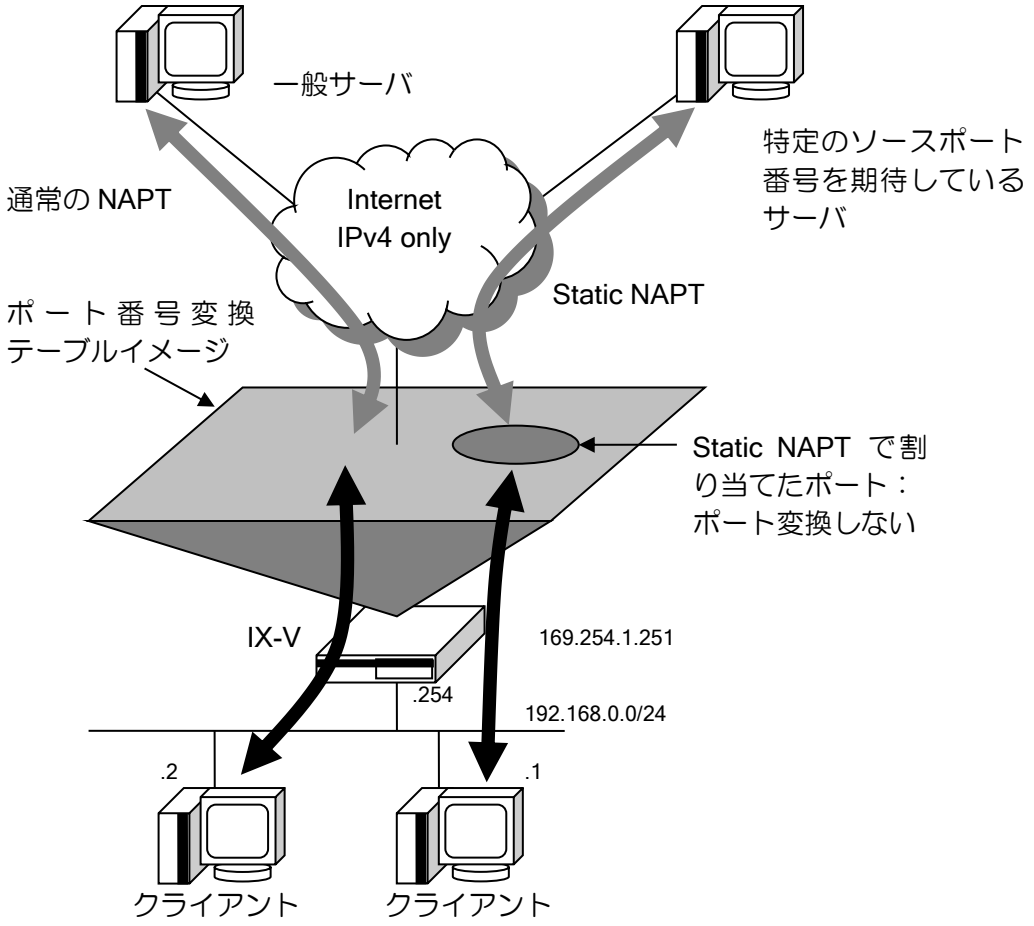
【設定例 3】
送信元が 10.10.10.0/24 の場合は NAPT アドレスに 169.254.1.2 を使用
送信元が 10.10.20.0/24 または自発パケットの場合は NAPT アドレスに 169.254.1.251 を使用
送信元がそれ以外の場合は、NAPT しない

```
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 169.254.1.251/32 dest any

interface GigaEthernet0.0
  ip address 169.254.1.251/24
  ip napt enable
  ip napt address 169.254.1.2
  ip napt inside list access-1
  ip napt inside list access-2 outside 169.254.1.251
  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 169.254.1.251)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。

2.7.2.4 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

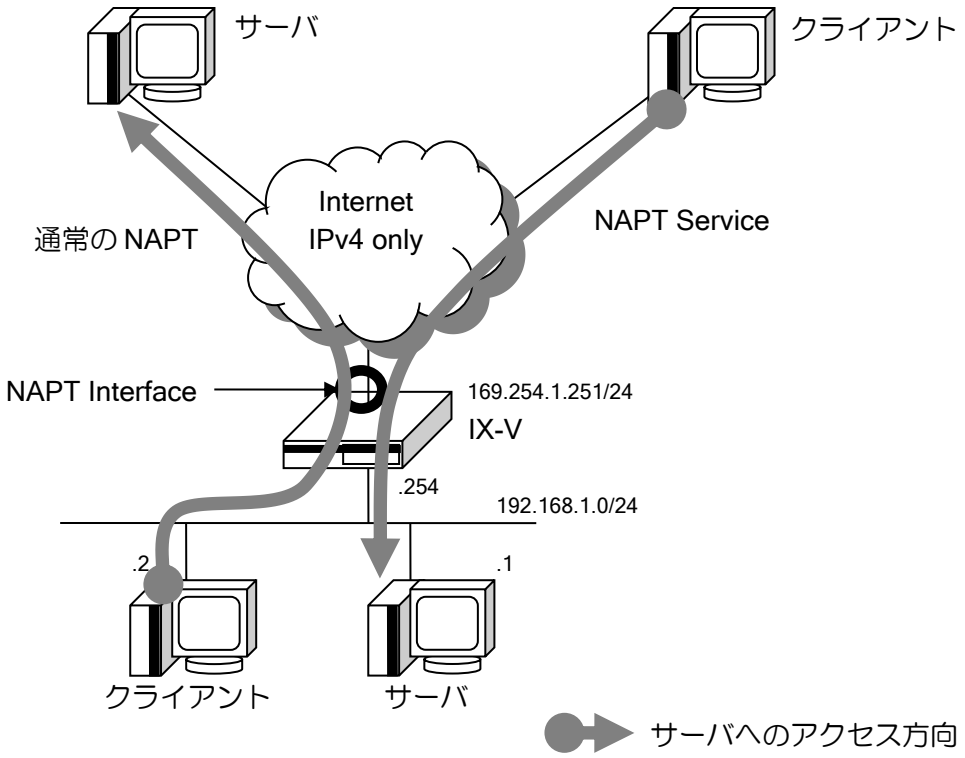
```
interface GigaEthernet0.0
   ip address 169.254.1.251/24
   ip napt enable
   ip napt static 192.168.0.1 tcp 1000-1010
   no shutdown
```

TCP,UDP 以外のプロトコルの場合

```
interface GigaEthernet0.0
   ip address 169.254.1.251/24
   ip napt enable
   ip napt static 192.168.0.1 41
   no shutdown
```

2.7.2.5 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 169.254.1.251/24
  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 169.254.1.251/24
  ip napt enable
  ip napt service tftp 192.168.1.1 none udp 69
  no shutdown
```

2.7.2.6 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 169.254.1.251/24
  ip napt enable
  ip napt translation max-entries 16384
  no shutdown
```

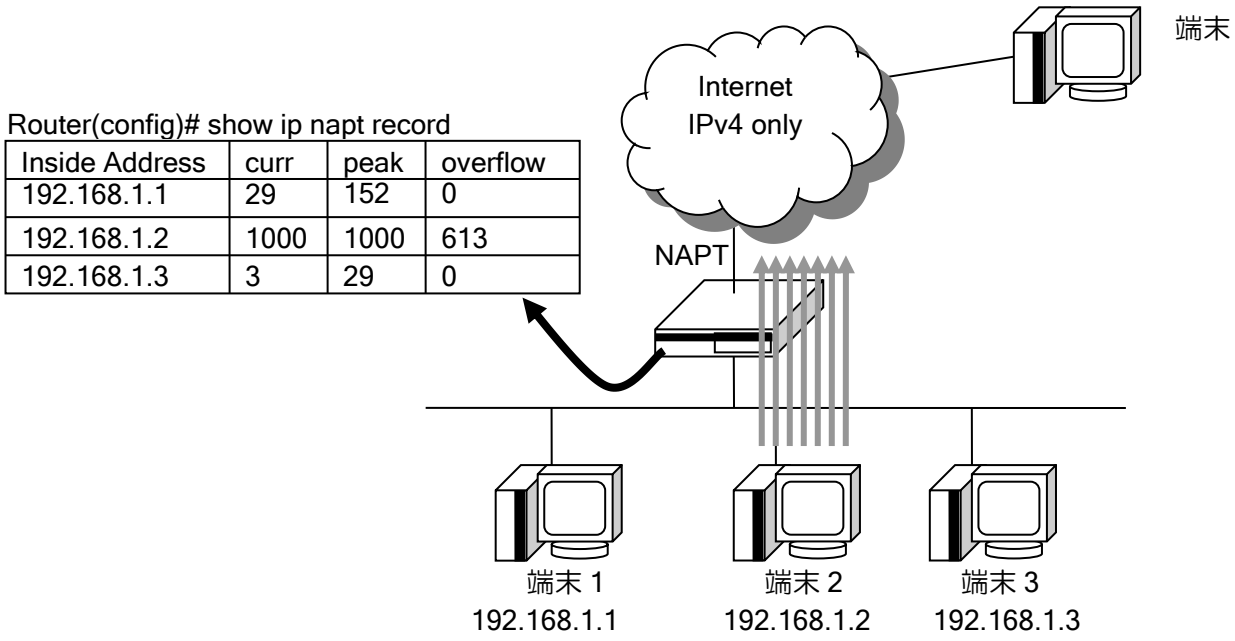
2.7.2.7 NAPT キャッシュ数の制限の設定 - ホスト単位での制限

「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 169.254.1.251/24
  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。

2.7.2.8 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]
- 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]
- 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]

2.7.3 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(ip napt alg コマンドでポート番号を指定できます)
- TFTP
- ICMP
- PPTP

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

2.7.4 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することができます。

2.7.4.1 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。

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
```

2.7.4.2 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 2023 7 7
  2023/7/7 00:00:00～2023/7/7 23:59:59 のログを表示

年月日時を指定
  show ip napt access-log datetime 2023 7 7 17
  2023/7/7 17:00:00～2023/7/7 17:59:59 のログを表示

年月日時分を指定
  show ip napt access-log datetime 2023 7 7 17 50
  2023/7/7 17:50:00～2023/07/07 17:50:59 のログを表示

2.7.5 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。

2.7.5.1 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。

2.7.5.2 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）

■2.8 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、IX-V シリーズ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）
  - BGP を使用し外部から学習したルート

複数の同一ルートが存在した場合は、各ルーティングプロトコル（ダイレクト、スタティックルートを含む）の最適経路計算やルーティングプロトコル間の優先度に基づいて最適と判断されたものが選択されルーティングテーブルへの登録されます。

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。

2.8.1 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、以下の種類があります。

- Connected（ダイレクトルート）
- Static（スタティックルート）
- BGP external
- BGP internal

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	
BGP internal	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	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

【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
```

2. 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
```

2.8.2 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
show ip static-routes	IPv4 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
```

2.8.3 BGP4

BGP（Border Gateway Protocol）は AS（Autonomous System）間で動作する EGP（Exterior Gateway Protocol）のひとつで、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。

2.8.3.1 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。

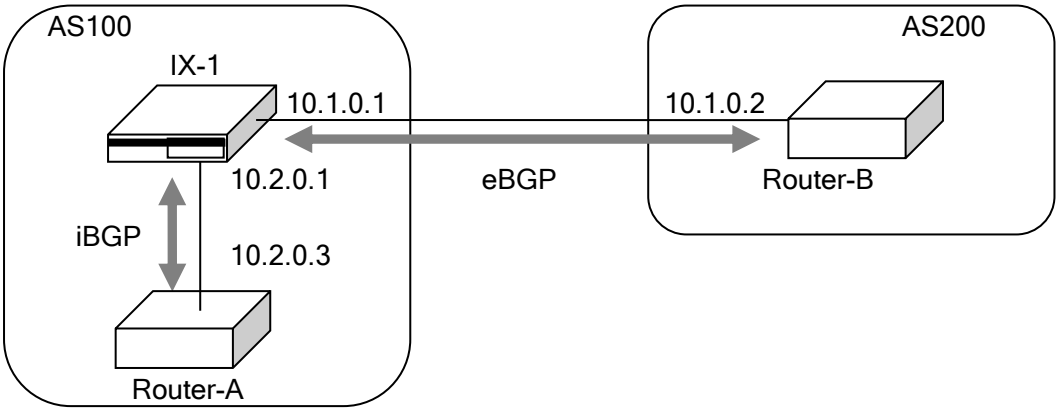
- eBGP（外部ピア）
  異なる AS 間での接続を eBGP（external-BGP）と呼びます。
  eBGP では、ピアは直接接続しているネットワークに接続している必要があります。
  直接接続していないネットワーク間で eBGP ピアを確立する場合は、マルチホップの設定が必要となります。

- 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、スタティックルートなどの 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 ID

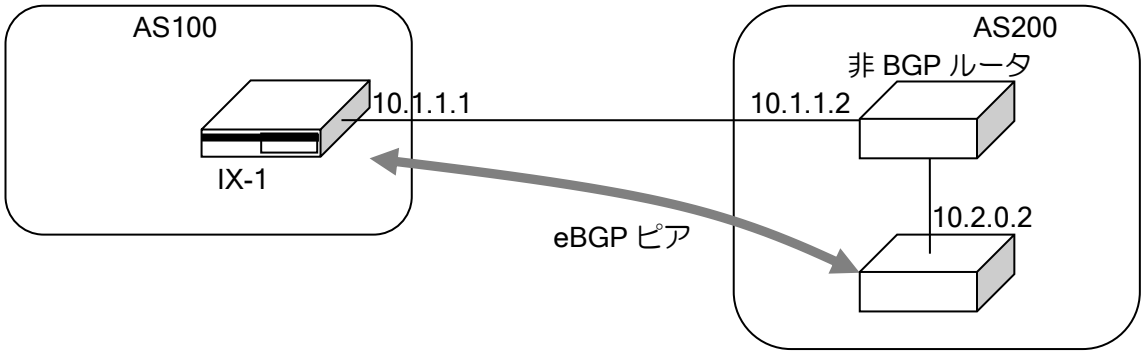
BGP では、ルータを一意に識別できるようにルータ ID を持ちます。ルータ ID はインタフェースに割り当てられている IP アドレスのうちのいずれかになります。ルータ ID の選択の方法については、付録のルータ ID セレクションの節を参照してください。ルータ ID を任意の値に設定するには、以下のコマンドを使用します。

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】

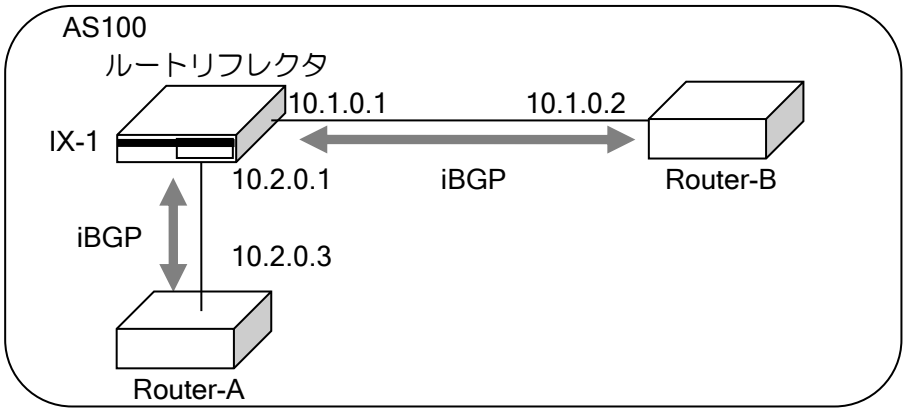
ソースアドレス指定の設定
ソースアドレスとして、GigaEthernet0.0 のアドレスを使用

```
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。



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)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
```

(f)ケイパビリティの設定

BGP4 では、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、サポートしているケイパビリティに対応する機能みを使用します。

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、接続開始時にピアルータのケイパビリティを知ることができます。

UNIVERGE IX-V シリーズでは IPv4 unicast，route-refresh ケイパビリティが送信されます。

- IPv4 unicast：IPv4 ユニキャスト広告
- route-refresh：ルートの再広告要求

2.8.3.2 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。

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。

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 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）

【設定例 1】
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。

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
```

(b)経路再配信

スタティックルート等の 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。

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。
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。

```
【設定例】

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 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）

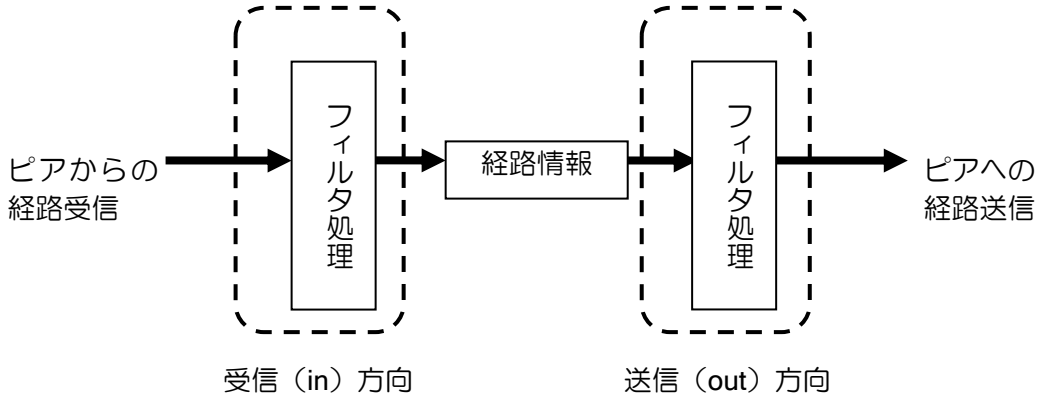
【設定例】

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）

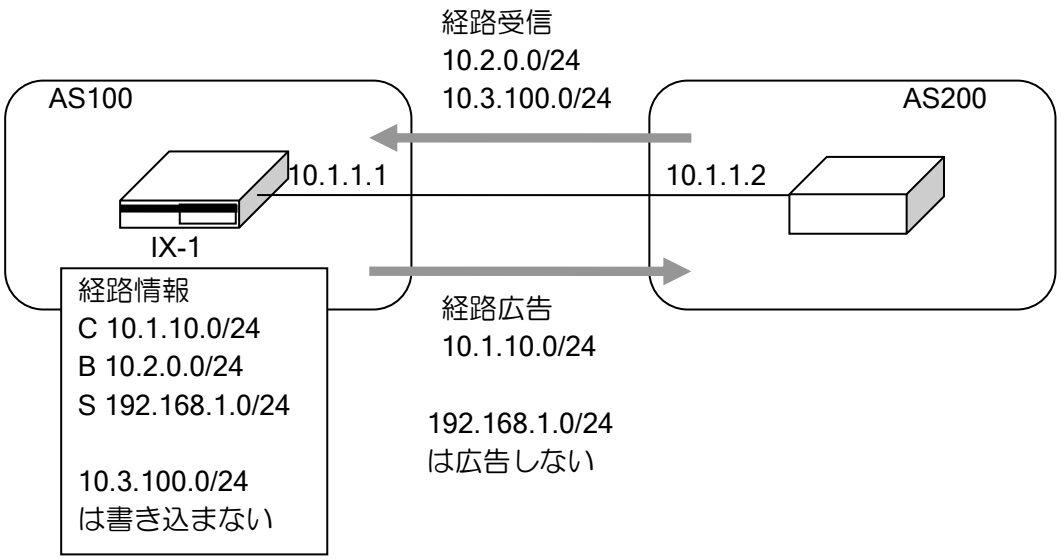
経路フィルタを使用することにより、受信する経路，送信する経路を制御することが可能です。フィルタはピア毎に、受信（in）方向，送信（out）方向それぞれ別に設定が可能です。



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】

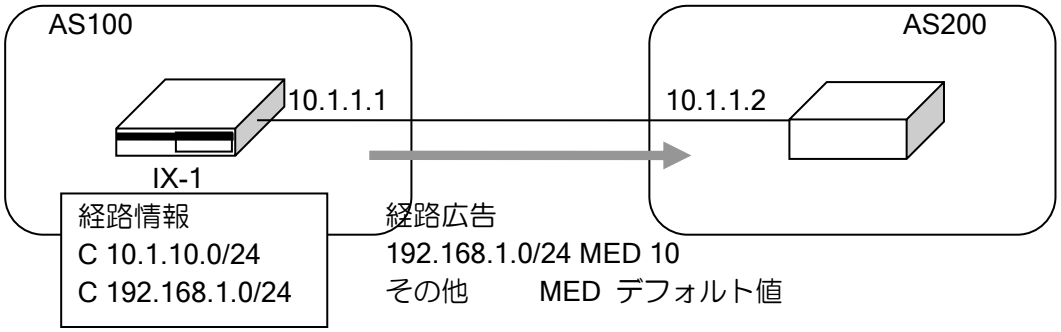
経路フィルタの設定

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 static
```

(e)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。
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。

【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
```

2.8.3.3 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	サポート
1	ORIGIN	○
2	AS_PATH	○
3	NEXT_HOP	○
4	MED（MULTI-EXIT-DISC）	○
5	LOCAL_PREFERENCE	○
6	ATOMIC_AGGREGATE	○
7	AGGREGATOR	○
9	ORIGINATOR	○
10	CLUSTER_LIST	○

14	MP_REACH_NLRI	×
15	MP_UNREACH_NLRI	×
16	EXT_COMMUNITY	×

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。

サポート対象外の属性は経路情報受信時に無視され、経路情報広告時に含まれません。

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。

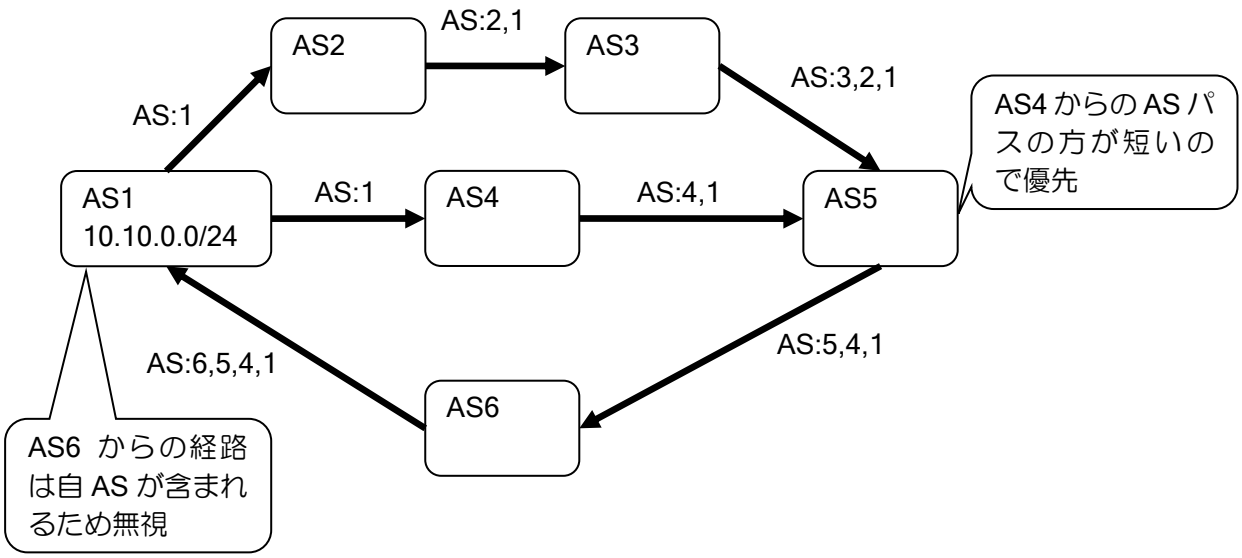
- IGP（タイプ 0）：IGP を通して学習した経路
- EGP（タイプ 1）：EGP を通して学習した経路
- INCOMPLETE（タイプ 2）：上記以外の別の手段で学習した経路

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。

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

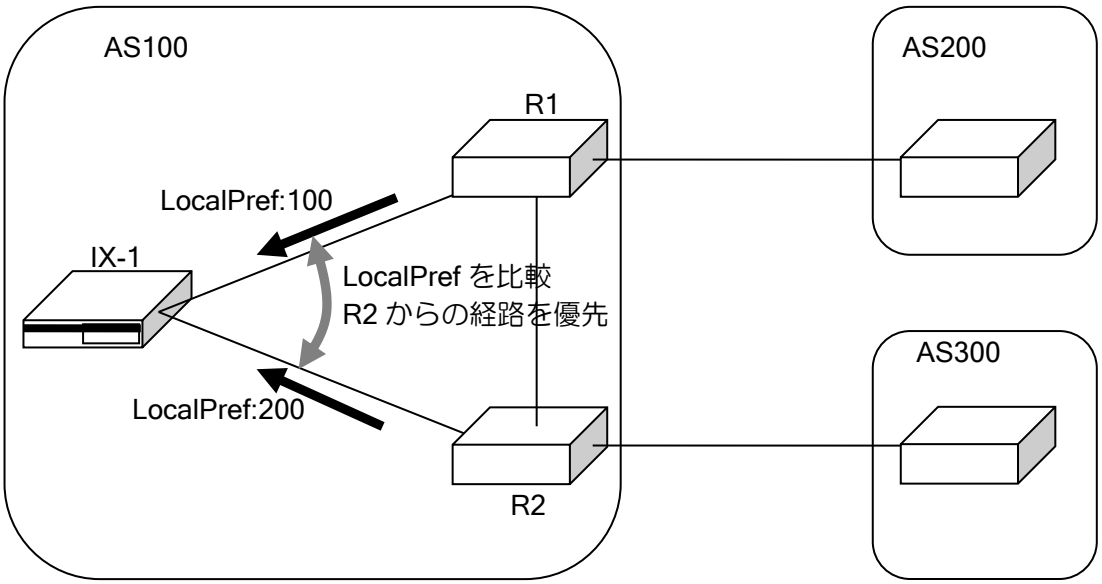
【設定例】
iBGP への経路広告時、ネクストホップに自アドレスを設定します。

```
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

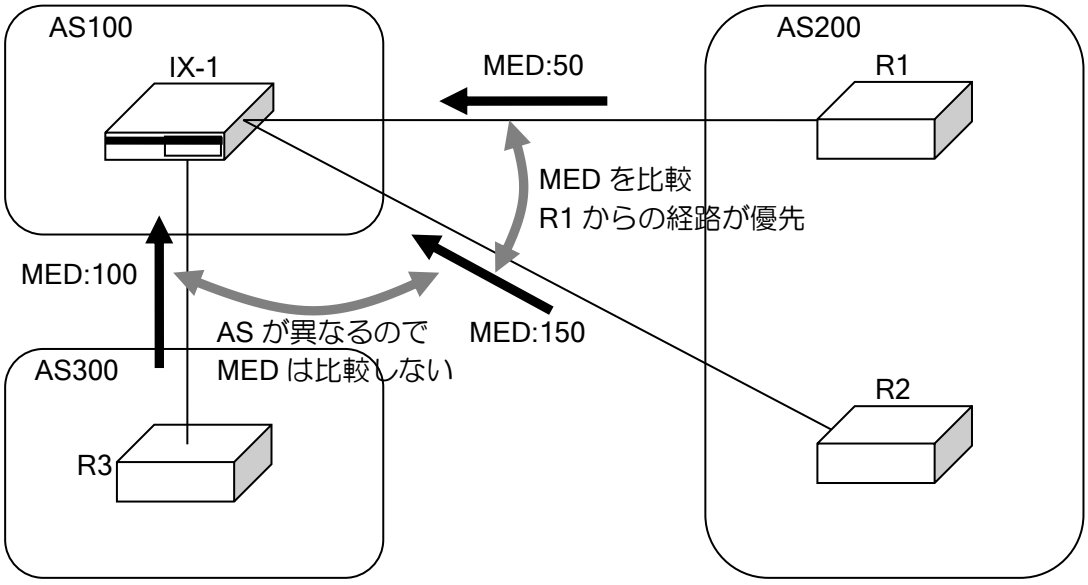
【設定例】
デフォルトローカルプリファレンスを 50 に設定します。

```
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】

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 static metric 6
```

(f)コミュニティ属性

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ひとつにまとめます。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、ひと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

2.8.3.4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）隣接したネクストホップの経路が優先される。
（9）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。
（10）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。
（11）アドレスが最も小さい BGP ルータからの経路が優先される。（※）
　　（※）同一装置間で複数 BGP セッションを設定した場合

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。

2.8.3.5 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		備考
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	IX-V シリーズでは検出しません
		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	IX-V シリーズでは検出しません
		0	上記以外のエラー	不正なオプションサイズ 不正なケーパビリティサイズ
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	IX-V シリーズでは検出しません
		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	IX-V シリーズでは検出しません
		8	ネクストホップ属性が無効	IX-V シリーズでは検出しません
		9	オプション属性エラー	IX-V シリーズでは検出しません
		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	1	OPENSENT 状態からの状態遷移が異常	
		2	OPENCONFIRM 状態からの状態遷移が異常	
		3	ESTABLISHED 状態からの状態遷移が異常	
6	コマンドによる切断要求 上記以外のエラー			

2.8.4 ポリシールーティング

UNIVERGE IX-V 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。

但し、IPsec 等のトンネルインタフェースを経由するパケットはポリシールーティングの対象外となります。

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。

- 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

【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 next-hop	IPv4 ネクストホップ指定
set ip default next-hop	IPv4 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 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
```

- ローカルパケットに対するポリシールーティング

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
```

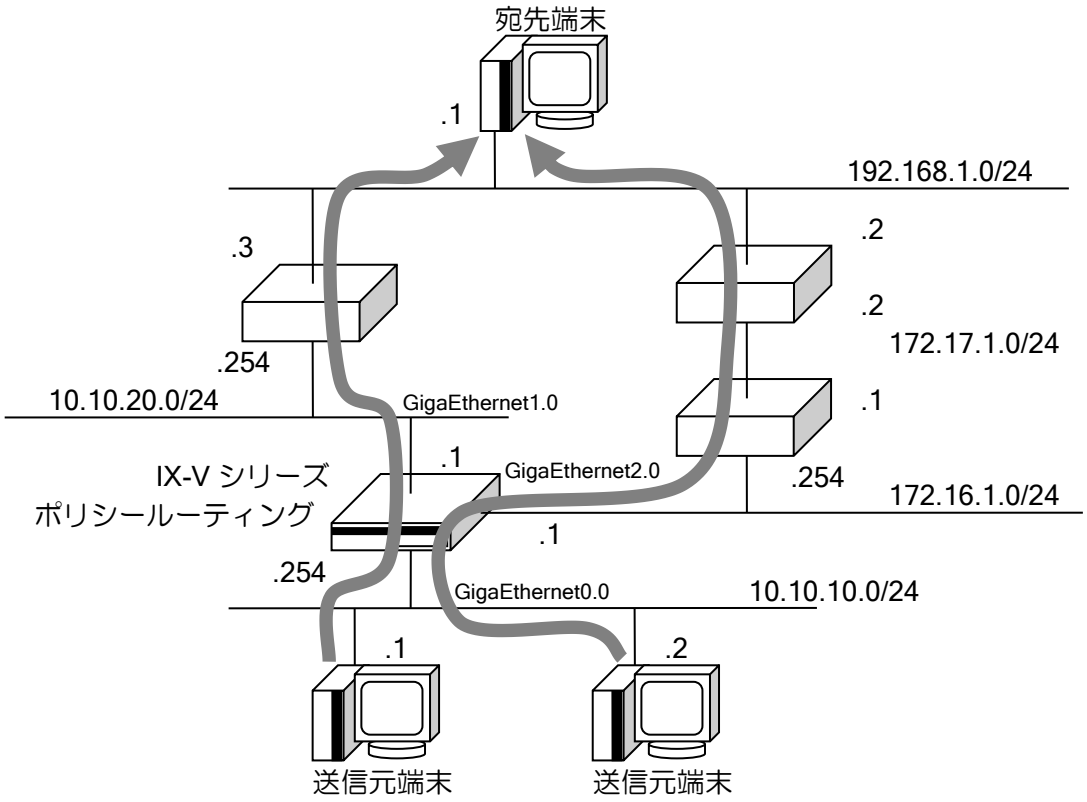
(c) ポリシールーティング設定時の経路選択の優先順位

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 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 default next-hop（経路が存在しない場合に適用）	↓低

2.8.4.1 ポリシールーティングの構成例

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
```

■2.9 DNS の設定

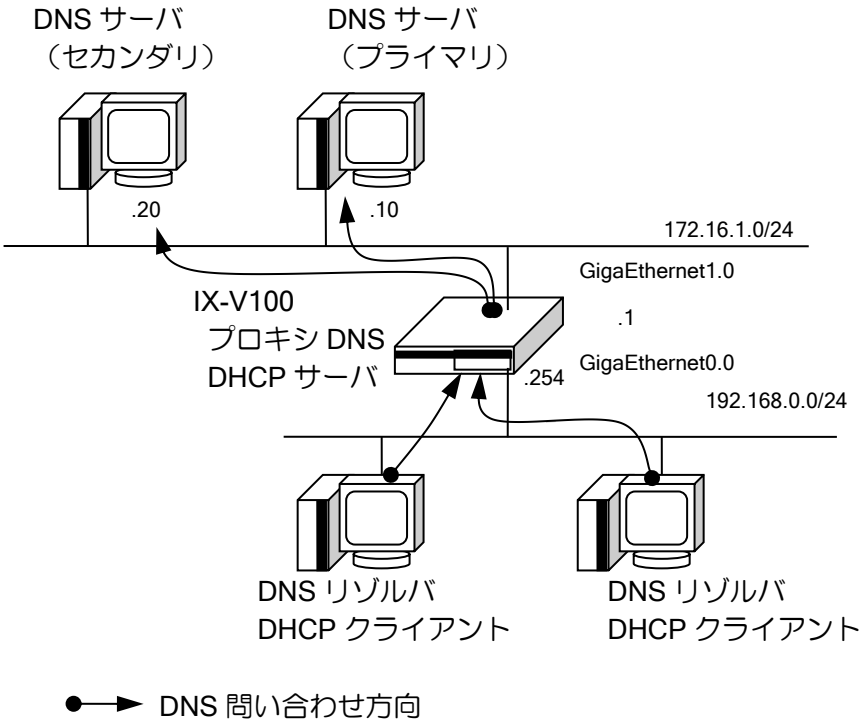
UNIVERGE IX-V シリーズは、プロキシ DNS および、DNS リゾルバ機能をサポートしています。

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す。

DNS リゾルバからの UDP と TCP 両方の問い合わせに対応しています。

DNS サーバへの問い合わせは UDP のみとなり、512byte を超える応答パケットに対応しています。

2.9.1 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 enable	プロキシ DNS の有効設定
proxy-dns ip max-sessions	最大セッション数の設定
proxy-dns ip query-interval	DNS 要求パケット送信間隔の設定
proxy-dns ip query-response	DNS 応答パケット待ち時間の設定
proxy-dns ip query-retries	DNS 要求パケット再送回数
proxy-dns ip access-list	DNS リゾルバのアクセス制限
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

```
ip dhcp 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
   proxy-dns ip enable
   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。

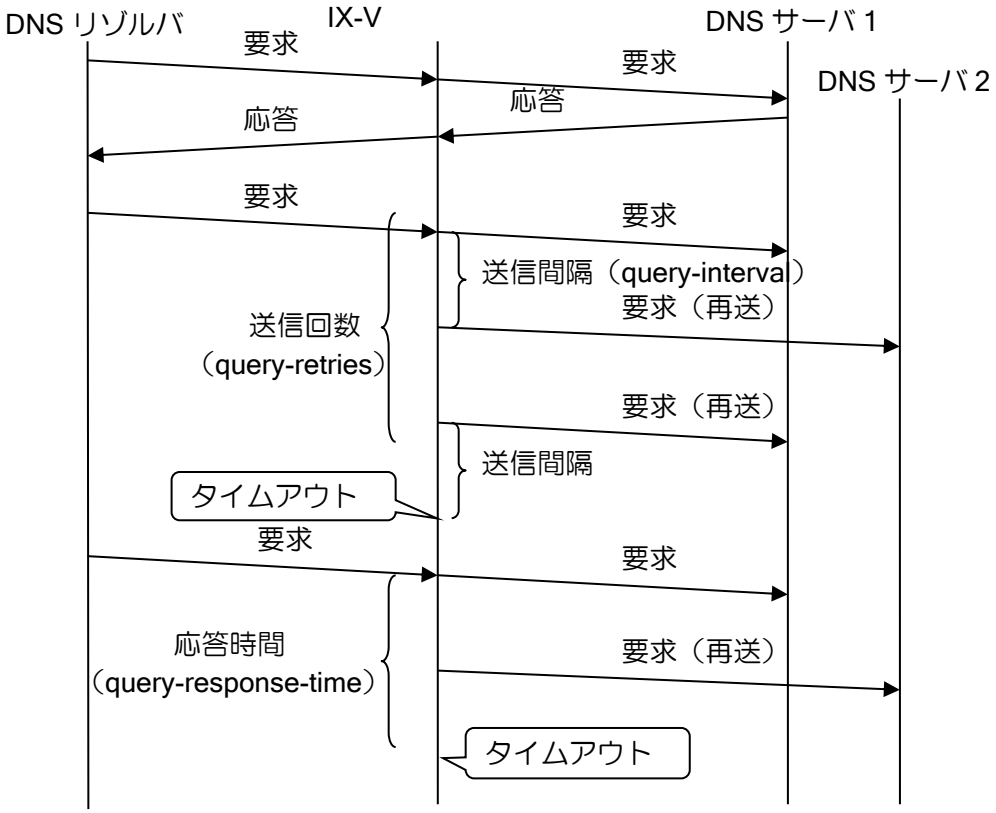
【設定例】

```
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

- 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。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
  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 access-list resolver-acl
proxy-dns server 10.0.0.1
interface GigaEthernet1.0
   proxy-dns ip enable
```

- DNS 問合せ出力先指定
  DNS リゾルバ、Proxy-DNS 共に 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下さい。

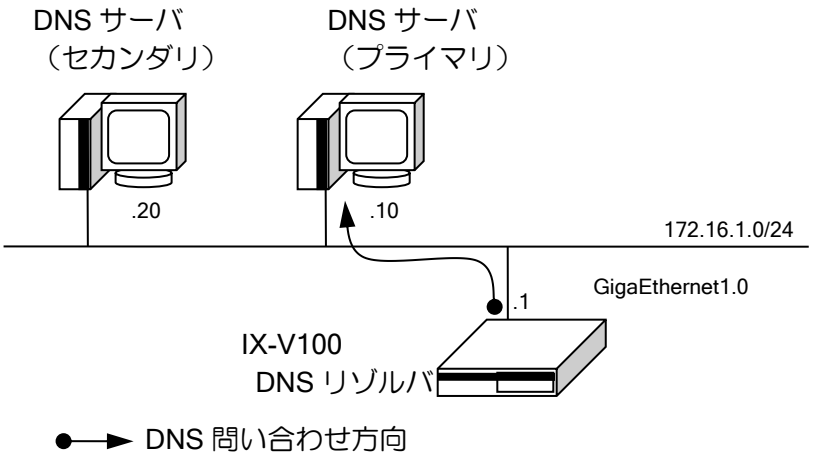
  また、DNS リゾルバ、Proxy-DNS 共に IPCP/DHCP で動的に取得した DNS サーバへの問合せは取得したインタフェースから送信されます。DNS リゾルバだけは、以下のコマンドによってこの動作を変更しルーティングテーブルに従って問い合わせを行うことが可能です。

no ip name-server dynamic fixed-interface	IPv4 動的取得 DNS の送信インターフェース固定動作の無効化

2.9.2 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。

DNS リゾルバは、ping, traceroute, nslookup コマンド及び IPsec の接続先等で使用することができます。EDNS0 と 512byte 以上の応答に対応しています。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 で自動取得されたものを使用しますが、手動で固定設定することも出来ます。

ip name-server	DNS のアドレスを固定的に設定

DNS サーバを複数設定している場合、DNS の問い合わせ順番は以下となります。

- 固定で設定した IPv4 の DNS サーバ(登録順)
- DHCPv4、IPCP で学習した DNS サーバ(学習順)

各機能では outgoing-interface で指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

【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
```

2.9.3 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。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）

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。

2.9.4 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。

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。

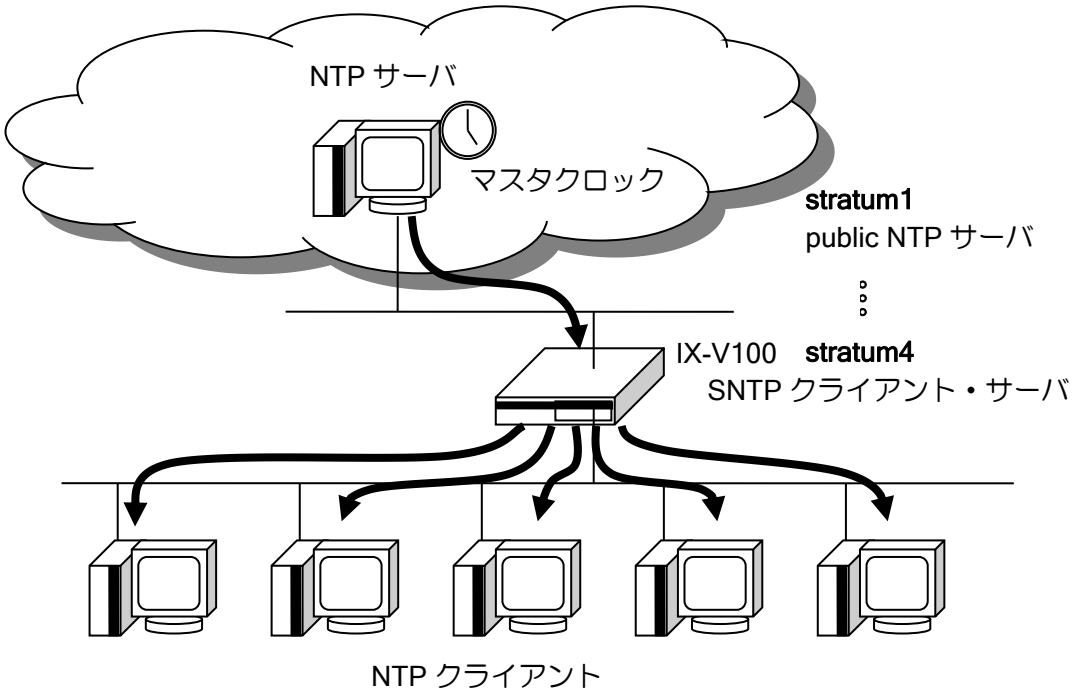
【設定例】
・example.com ドメインへの DNS 問い合わせをルータが A レコード(192.168.0.200)で応答し、それ以外の DNS 問い合わせを外部 DNS サーバへ行う。

```
ip route default GigaEthernet0.0

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 dchp enable
   ip dhcp binding gigaethernet2.0
   proxy-dns ip enable
   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。

■2.10 NTP の設定

UNIVERGE IX-V シリーズでは、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。



2.10.1 NTP クライアントの設定

UNIVERGE IX-V シリーズでは、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

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 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
```

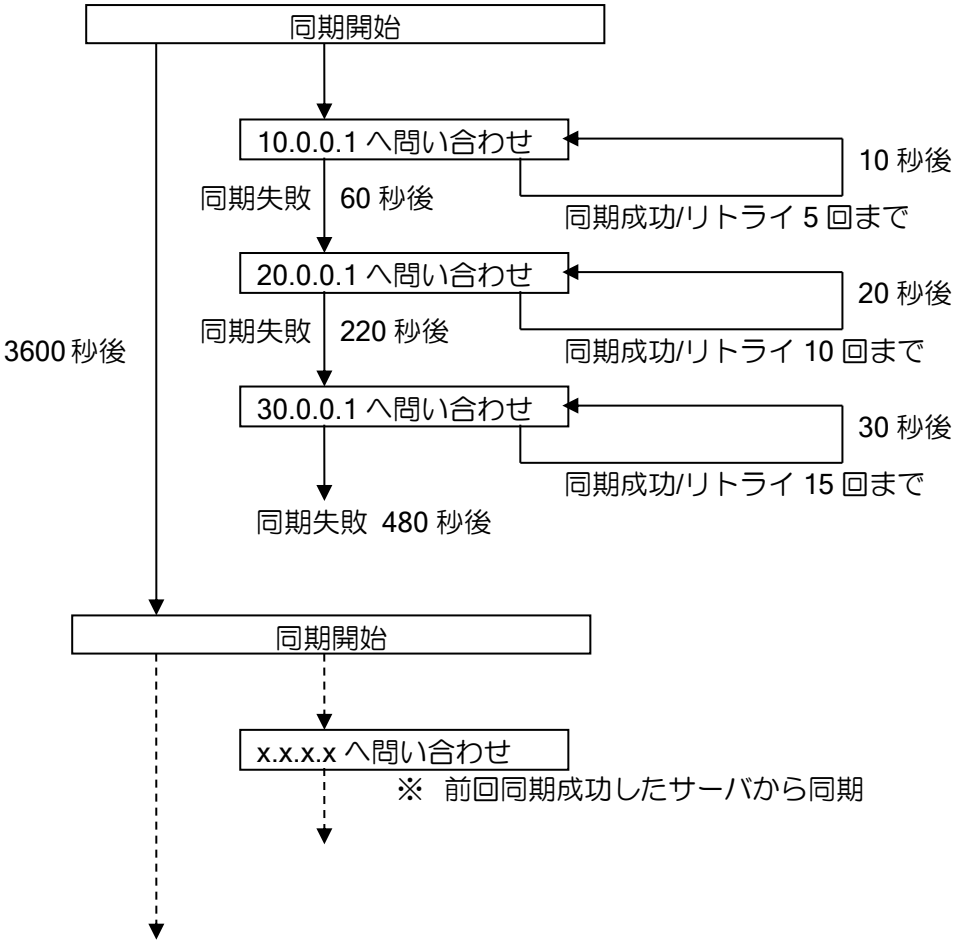
2.10.1.1 複数 NTP サーバ登録時の動作

- 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。

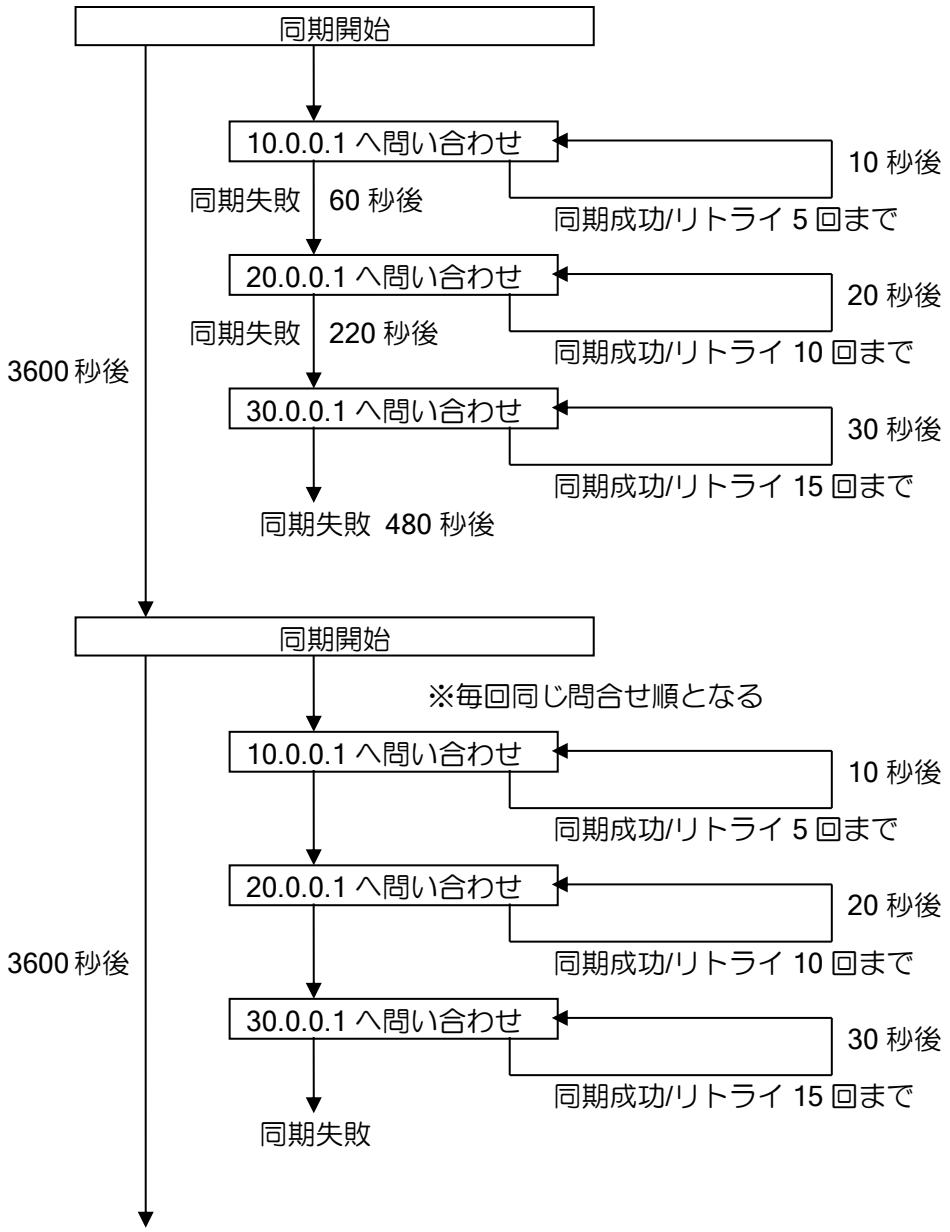
※時刻同期周期（ntp interval）は同期失敗となる時間よりも長く設定する必要があります。同期失敗する前に次の同期時刻となった場合、前回の同期はリセットされ新たに同期プロセスを開始します。

- 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
```



2.10.2 NTP サーバの設定

UNIVERGE IX-V シリーズでは、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

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 enable	NTP サーバの有効化
ntp master	ローカル NTP サーバの設定
ntp ip 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 server 10.0.0.1
```

UNIVERGE IX-V シリーズの時刻をマスタクロックとします。

```
ntp ip 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。

2.10.3 NTP アクセスリスト

UNIVERGE IX-V シリーズの 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 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
```

■2.11 ネットワークモニタの設定

2.11.1 ネットワークモニタ機能の概要

UNIVERGE IX-V 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。

※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。

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 （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
event ip unreach-host	端末到達不可監視の設定
event ip reach-host	端末到達監視の設定
event ip unreach-route	経路到達不可監視の設定
event ip reach-route	経路到達監視の設定
event watch-group-status	Watch グループ状態監視の設定
event always	常時発生イベントの設定
event interface-up	インタフェース up 監視の設定
event interface-down	インタフェース down 監視の設定
action ip shutdown-route	隠蔽経路の設定
action ip resume-route	可視経路の設定
action ip shutdown-policy	ポリシールーティングの無効設定
action ip resume-policy	ポリシールーティングの有効設定
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 netmeister-alarm	NetMeister アラームの設定

clear watch-group session	watch グループの全てのアクションの復旧

2.11.2 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 GigaEthernet0.0
  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。

2.11.3 イベントの設定

2.11.3.1 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。

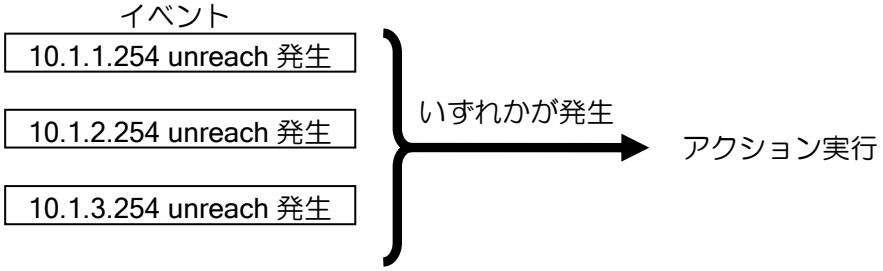
複数のイベントを設定した場合、以下のいずれかの条件でアクションを実行します。

- 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）

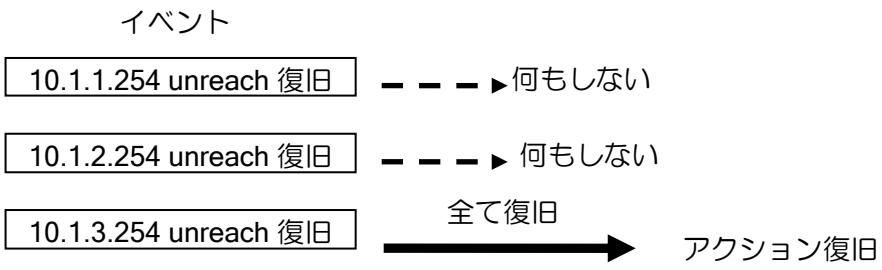
  シーケンス番号が異なるイベントはいずれかが発生した場合にアクションを実行します。

  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】

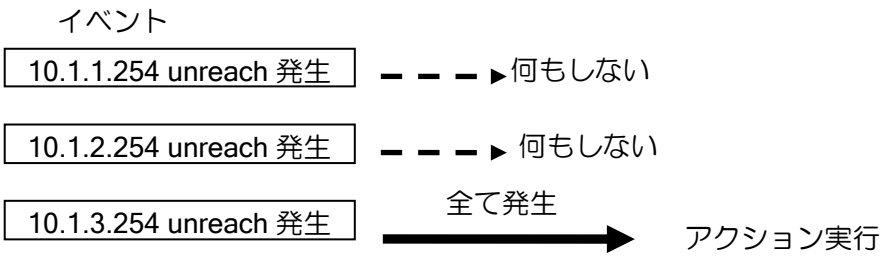



```
【設定例】

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
```

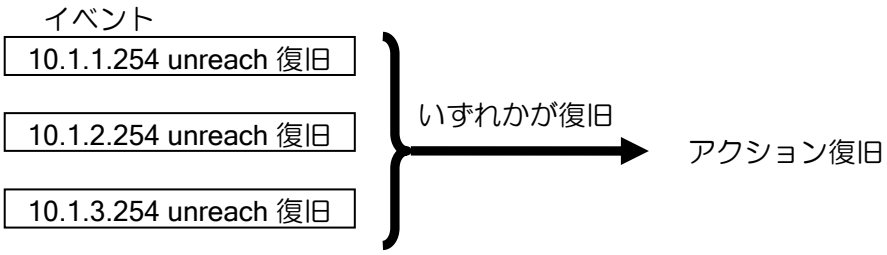
➢ 全てのイベントが発生した場合（AND 条件）

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】

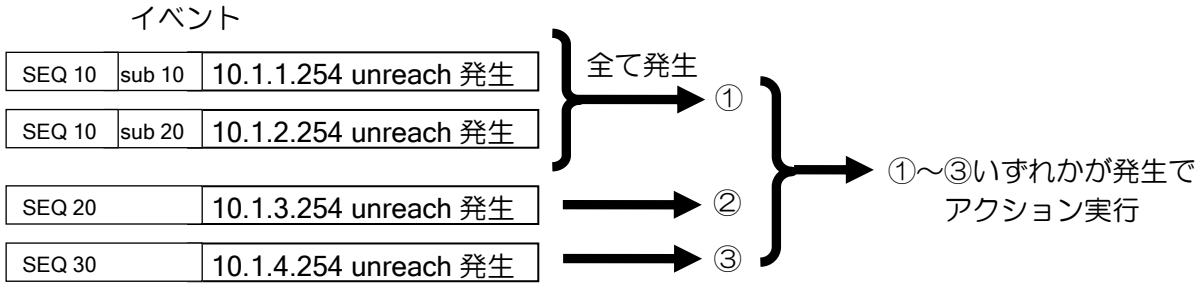



```
【設定例】

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
```

2.11.3.2 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。

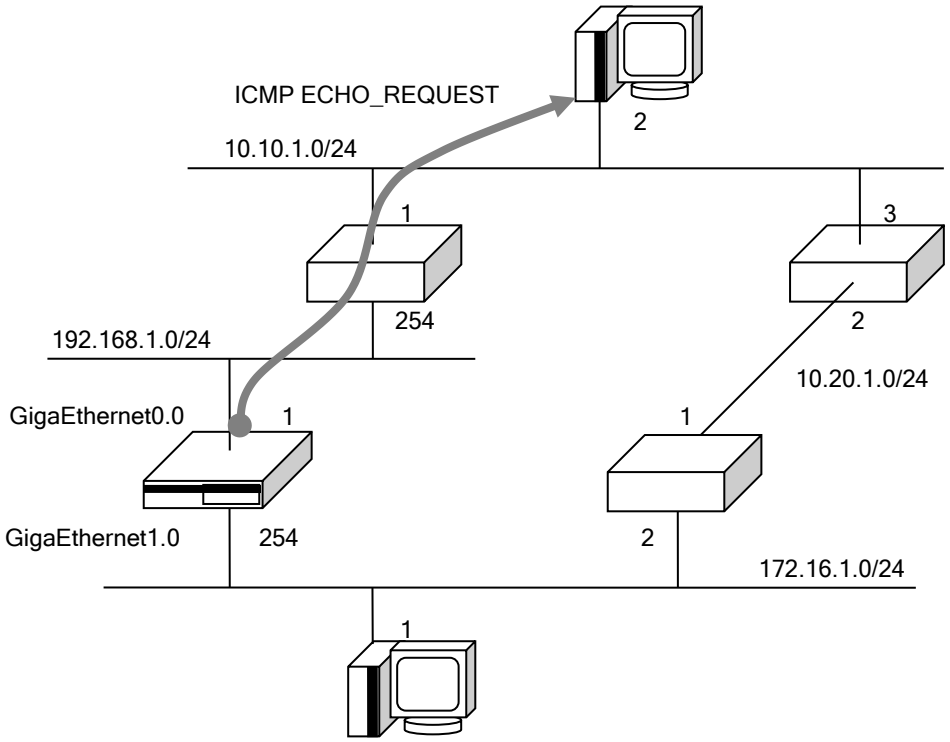
(a)ホスト監視の基本動作

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。

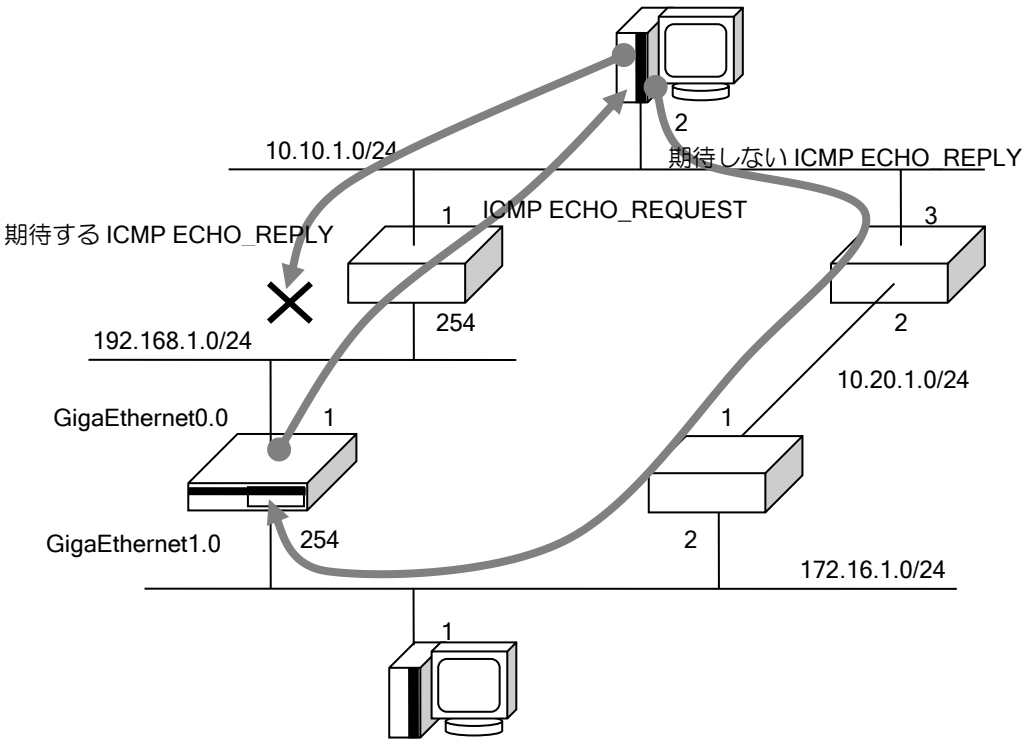


【設定例】

```
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-V 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。 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 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 　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） 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） 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） 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】

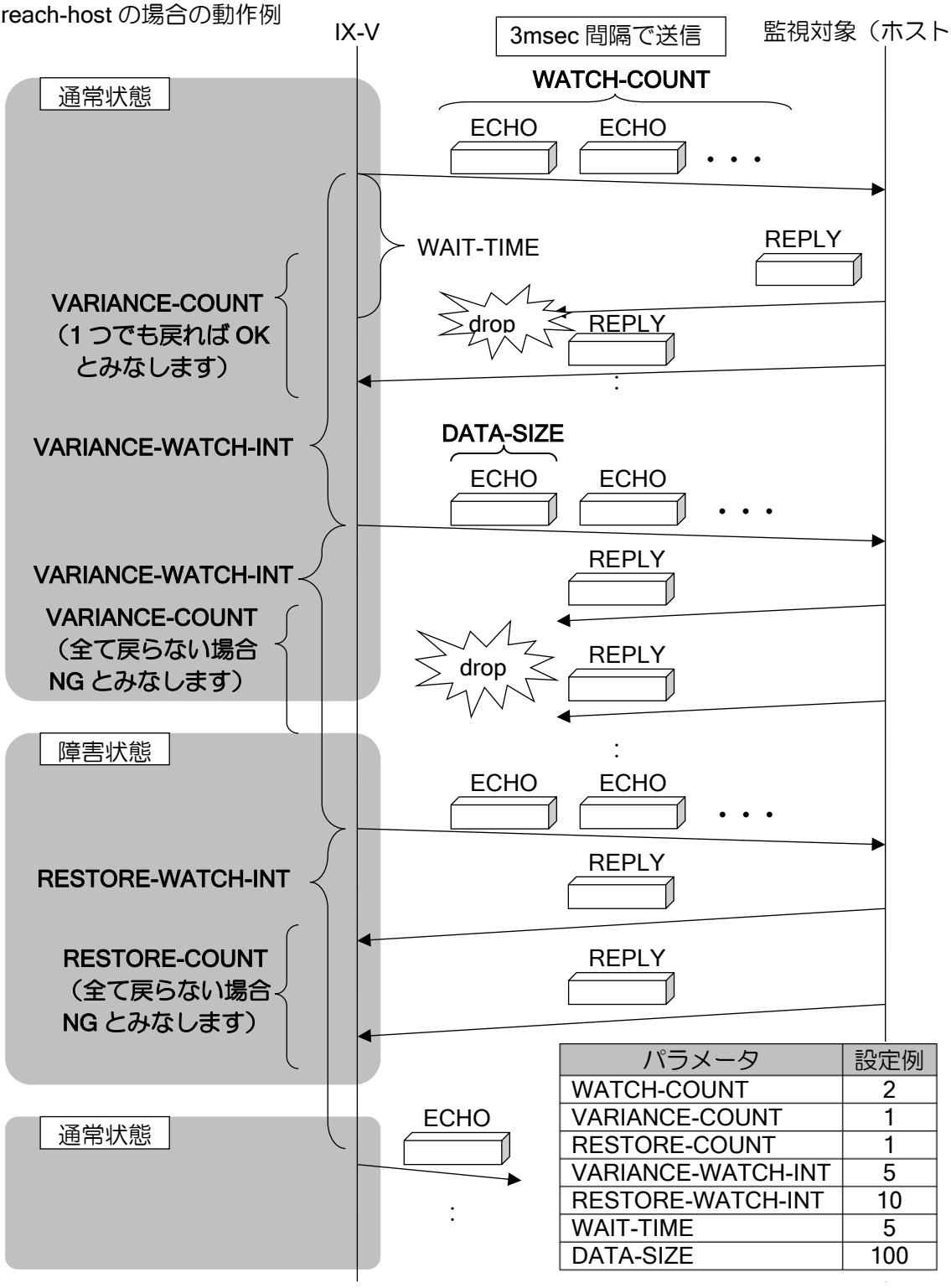
```
watch-group router-1 10
   probe-counter watch WATCH-COUNT
   probe-counter variance VARIANCE-COUNT percent VARIANCE-PERCENT
   probe-counter restorer RESTORE-COUNT percent RESTORE-PERCENT

   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

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。

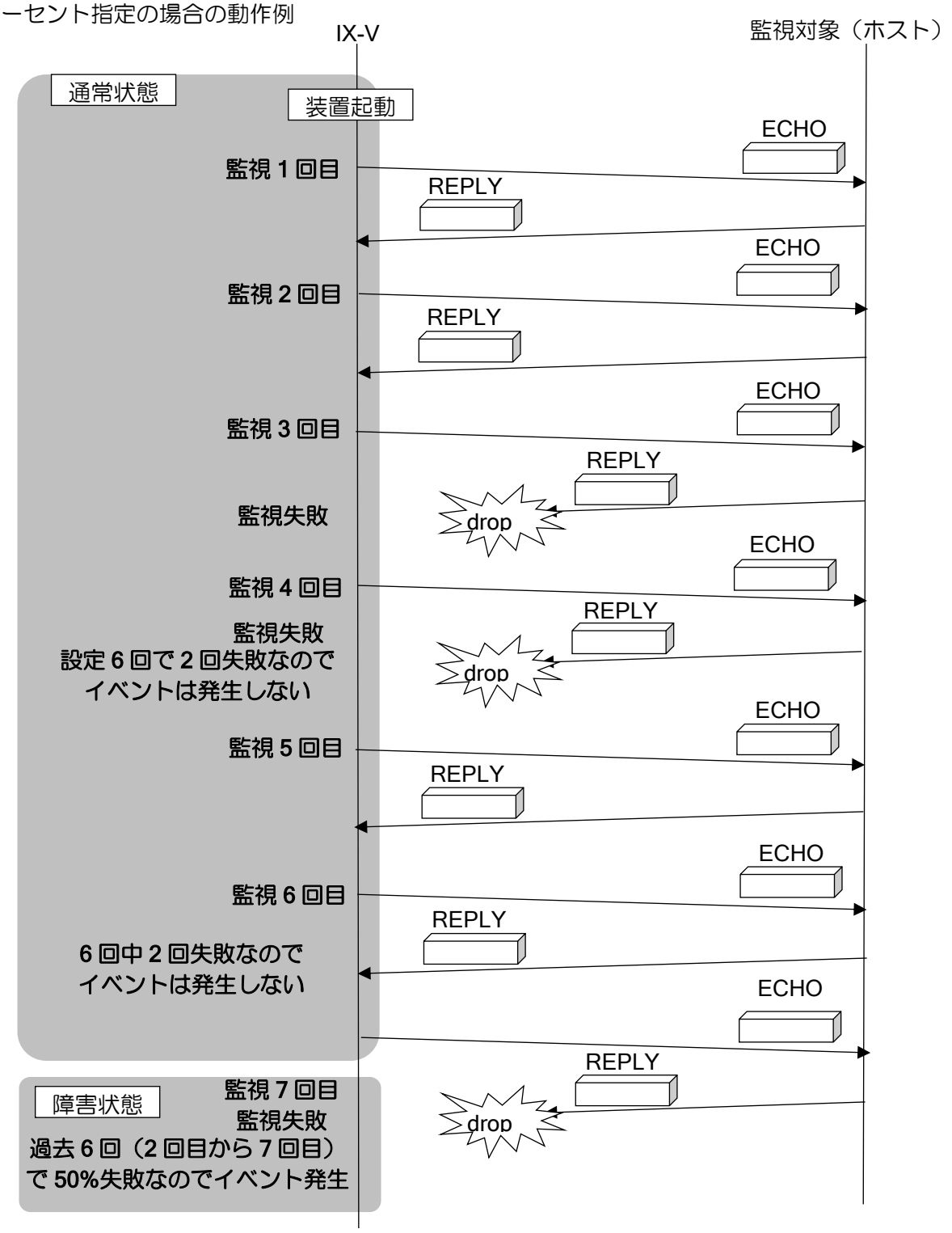
unreach-host の場合の動作例



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

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。

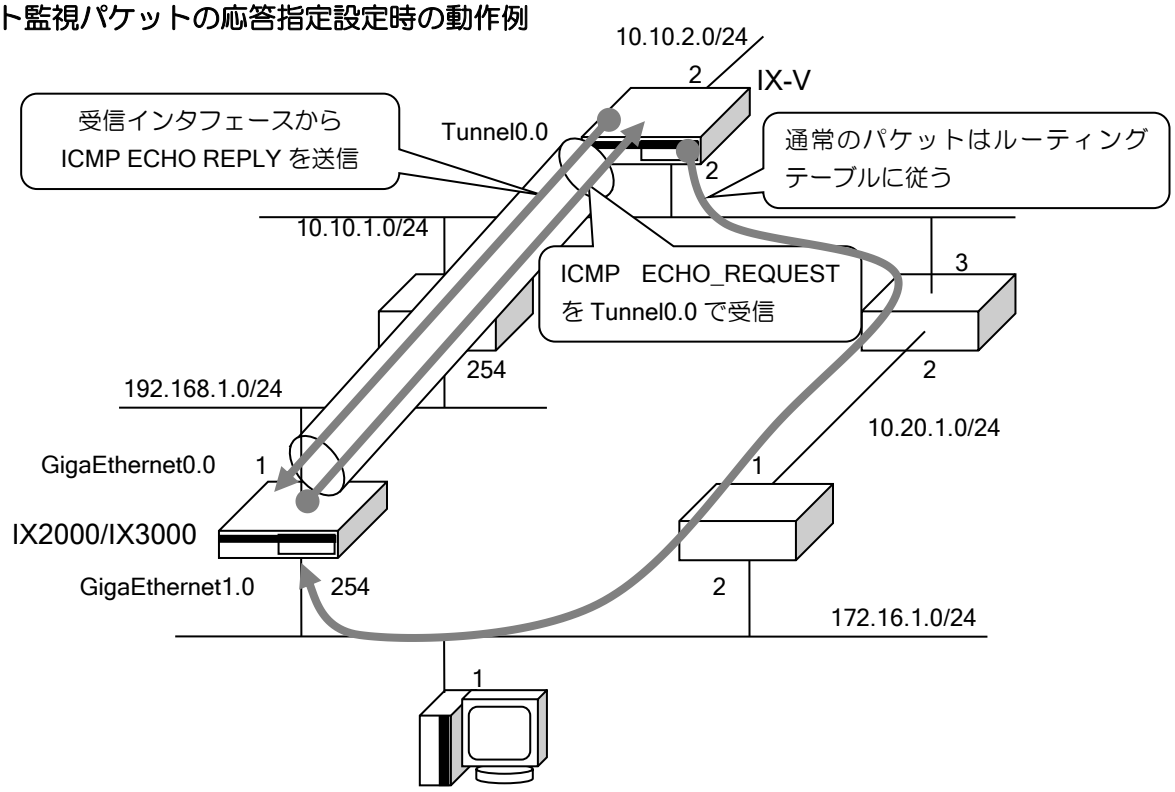
ネットワークモニタの監視用 ICMP ECHO REQUEST を送信するインタフェースから受信した ICMP ECHO REQUEST に対する ICMP ECHO REPLY は、ルーティングテーブルには依存せず、受信したインタフェースから送信することにより、往復で同じ経路を監視することができます。

UNIVERGE IX-V シリーズと UNIVERGE 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-V 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
```

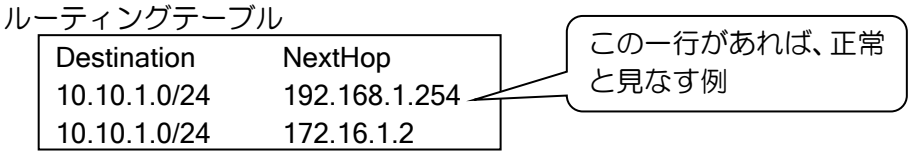
```
!
interface GigaEthernet0.0
   ip address 10.10.2.2/24
   no shutdown
!
interface GigaEthernet1.0
   ip address 10.10.1.2/24
   no shutdown


[IX2000/IX3000 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
```

2.11.3.3 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） 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） 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
```

2.11.3.4 watch グループ状態監視イベントの設定

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
```

2.11.3.5 常時発生／復旧イベントの設定

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。

2.11.3.6 インタフェース状態監視の設定

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
```

2.11.4 アクションの設定

2.11.4.1 アクション共通の動作

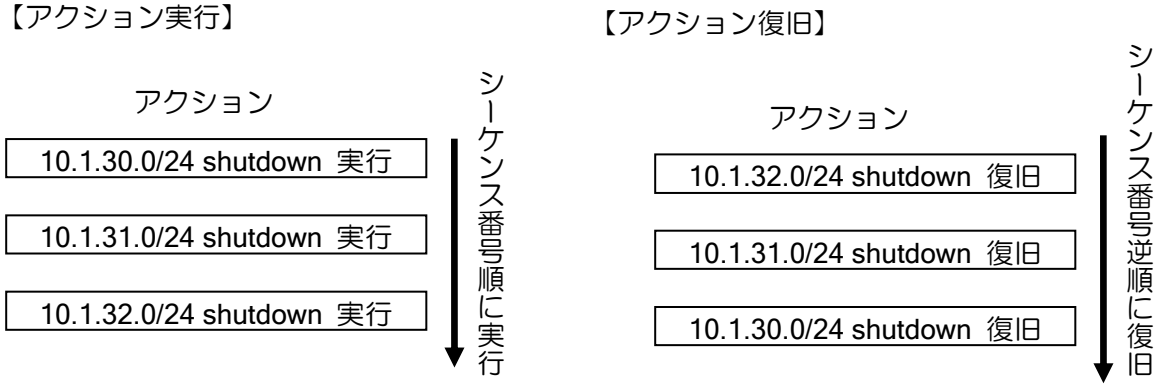
アクションは、イベント（ホスト/ネットワーク不到達等）発生時に実行され、イベント復旧時に元の状態に復旧します。action コマンドのパラメータに suppress-restoration オプションを指定することにより、イベント復旧時にアクションを復旧させないこともできます。この場合、clear watch-group session コマンドを実行することにより、アクションを復旧させることができます。

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
```

2.11.4.2 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 GigaEthernet0.0
   action 10 ip shutdown-route 10.1.31.0/24 suppress-restoration
```

2.11.4.3 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。

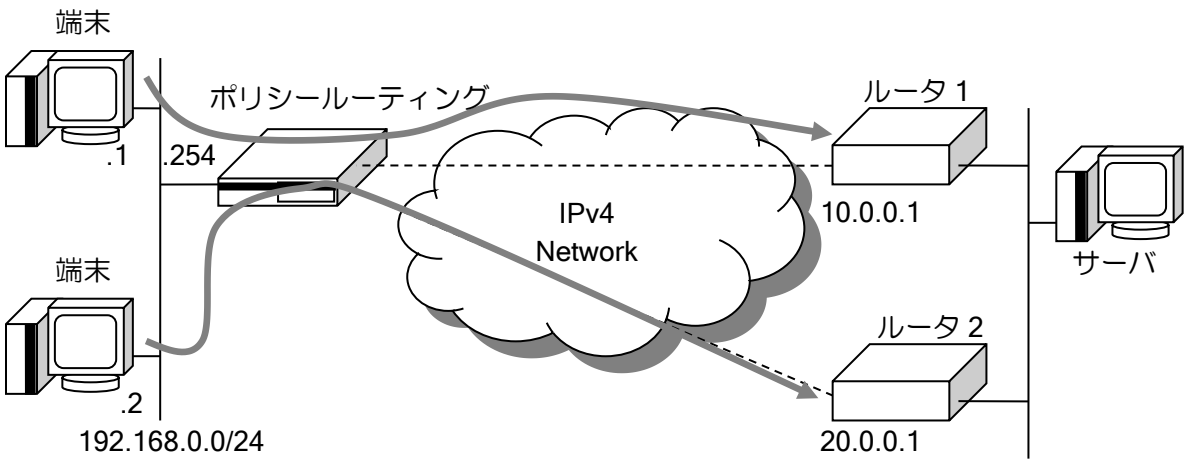
ポリシールーティングの詳細については、ポリシールーティングの項を参照してください。

【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
```

2.11.4.4 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
```

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。

2.11.4.5 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
```

2.11.4.6 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 GigaEthernet0.0
  action 20 turn-BAK-LED-on
```

2.11.4.7 NetMeister アラーム通知

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
```

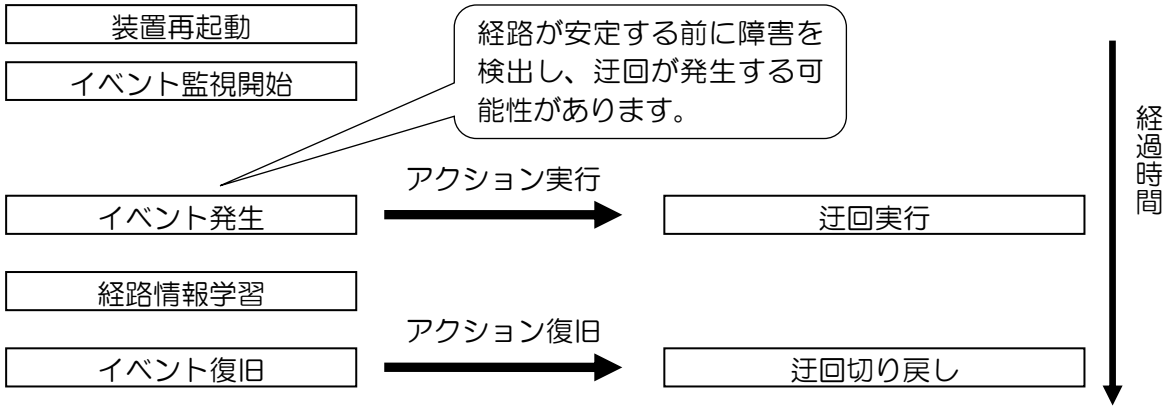
2.11.5 watch グループ毎の設定

2.11.5.1 watch グループ監視起動遅延時間設定

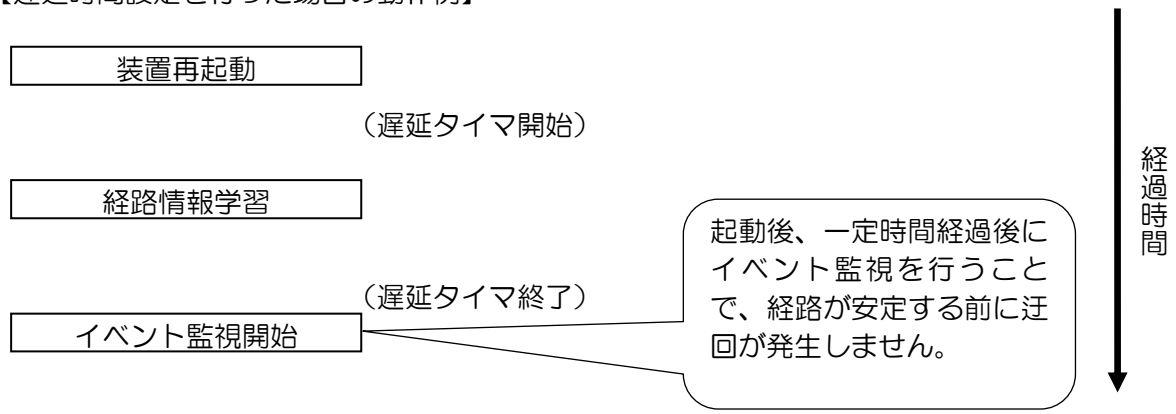
装置の再起動の際に watch グループによる監視の開始を遅らせることができます。装置起動から設定した遅延時間の間は、イベントの監視を行いません。これにより、装置起動直後の経路情報が安定していない状態のときに迂回が発生することを回避することができます。

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】



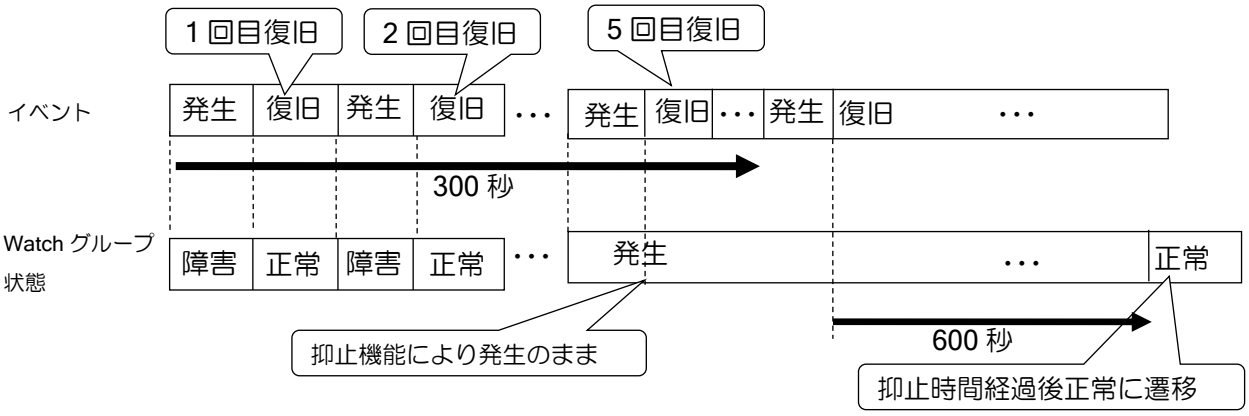
【設定例】
起動開始後、200 秒後にイベント監視を開始します。

```
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
```

2.11.5.2 状態変更抑止

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
```

2.11.5.3 複数の watch グループの連動

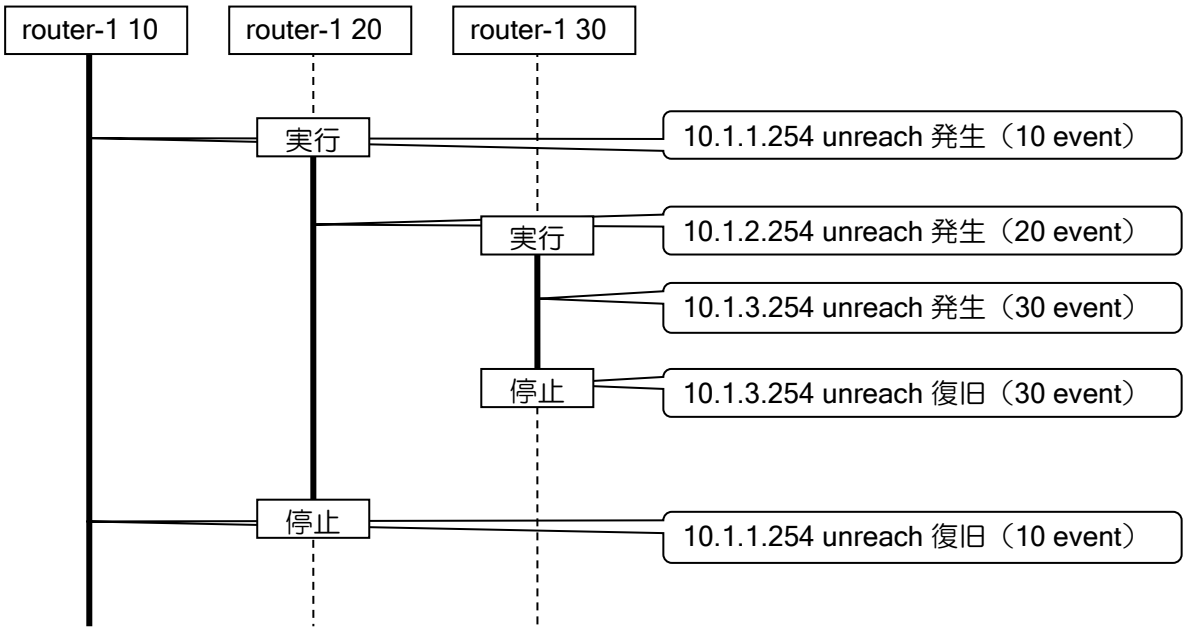
シーケンス番号の設定により、複数の watch グループをひとつの watch グループとして管理することができます。

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
```

2.11.6 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。

2.11.6.1 パッシブモード

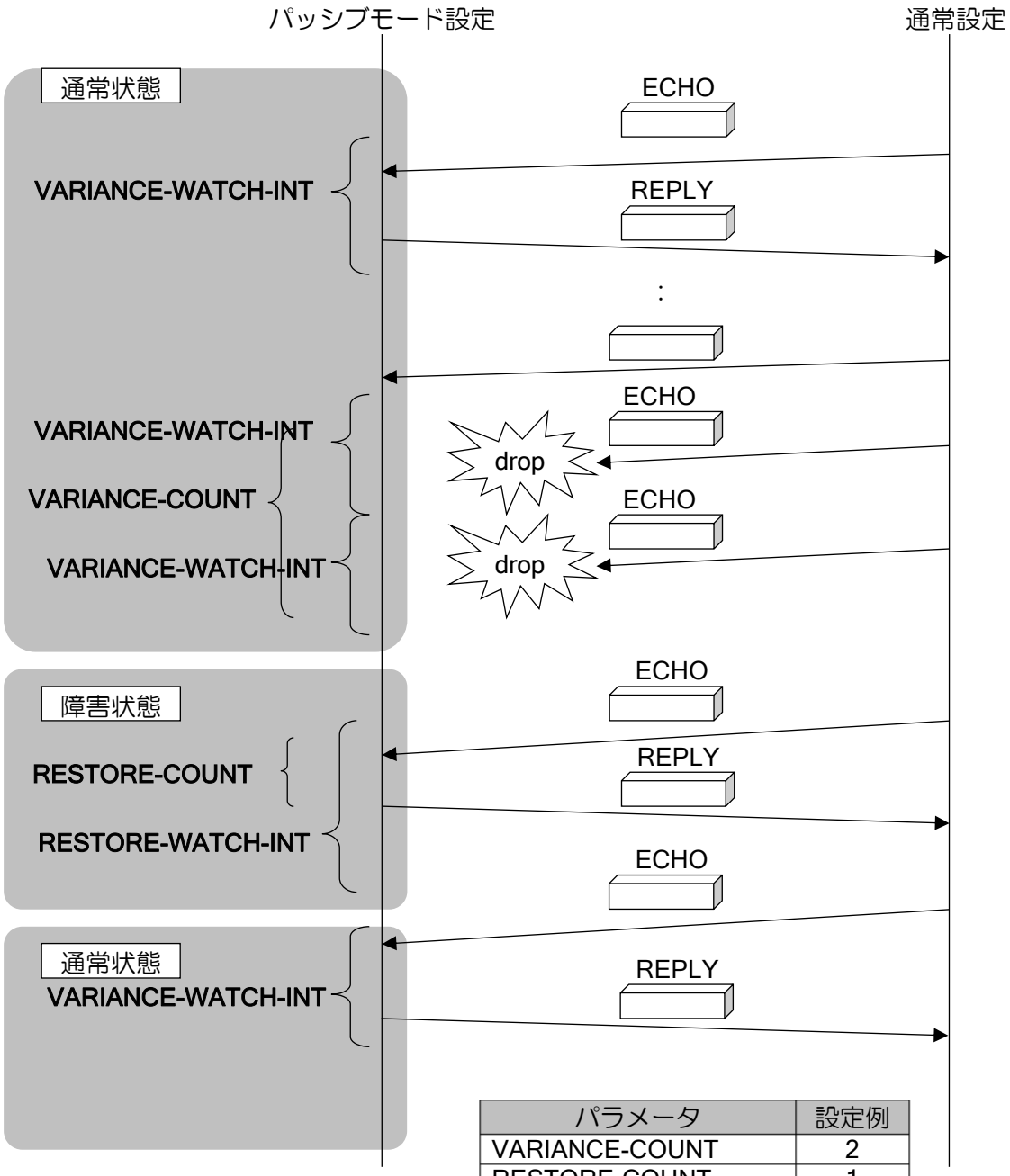
パッシブモードでは、相手からの ICMP ECHO パケットの監視を行います。通常の ICMP ECHO を送信する間隔で、相手装置から ICMP ECHO が届いているかの監視を行い、パケットが届いている場合は通信可能と判断します。最初に相手からパケットを受信するまでは、ready 状態となり、障害状態にはなりません。パッシブモードを設定した場合、自装置からは、ICMP ECHO の送信は行いません。

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。

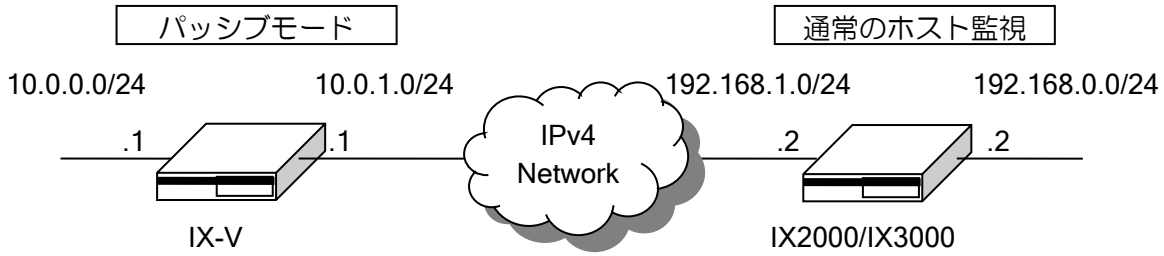
- 片方の監視先アドレスと、もう一方のソースアドレス
- 障害監視の間隔（VARIANCE-WATCH-INT,RESTORE-WATCH-INT）

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



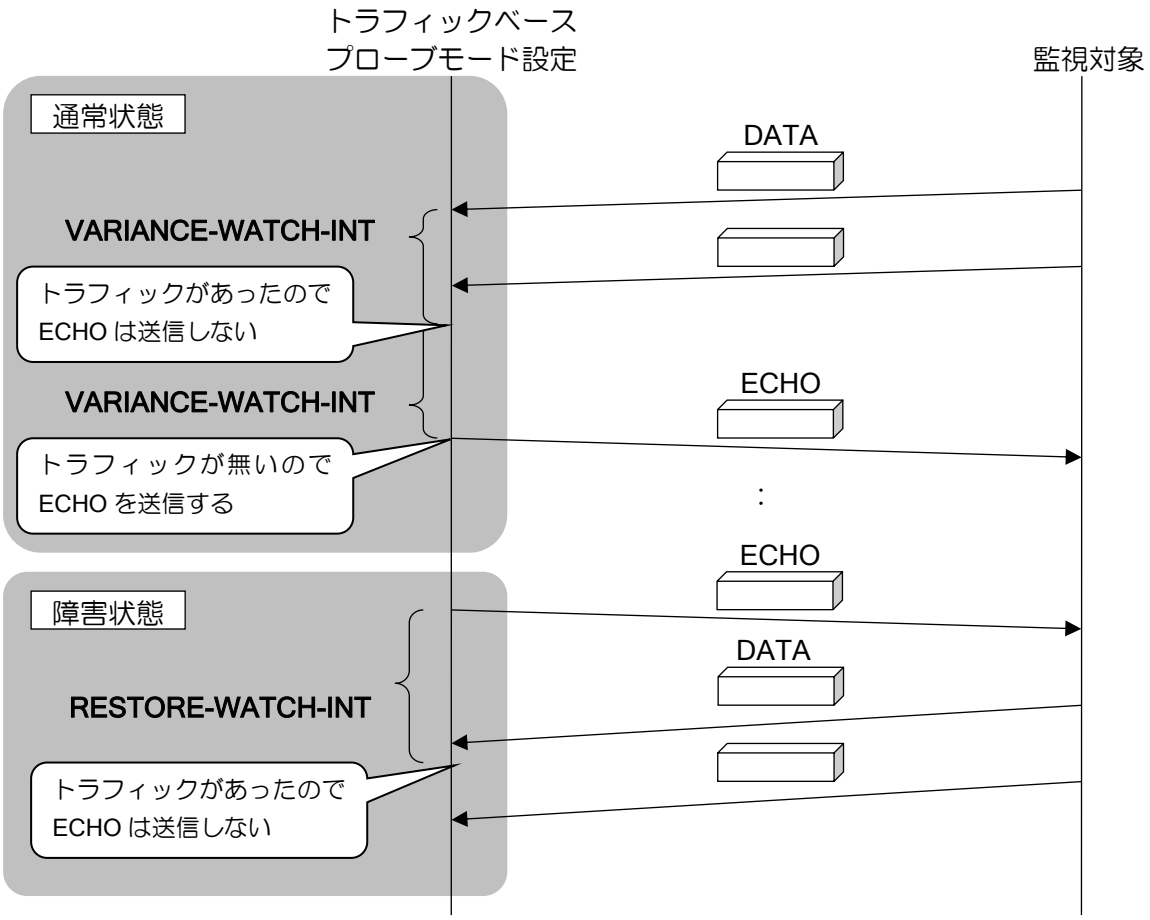
【設定例】

```
[IX-V 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

[IX2000/IX3000 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
```

2.11.6.2 トラフィックベースプローブモード

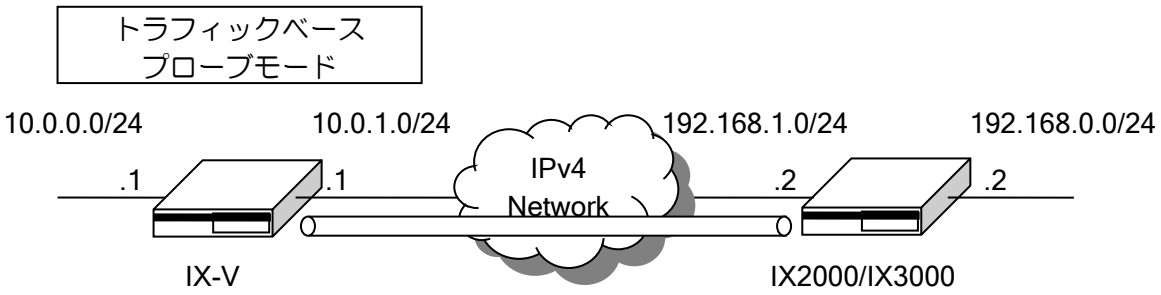
トラフィックベースプローブモードでは、ICMP ECHO を送信する周期で、ICMP ECHO を送信インタフェースからデータを受信している場合は、インタフェースの到達性があると判断し、ICMP ECHO の送信を行いません。ICMP ECHO/ECHO REPLY はデータ受信確認の対象外となります。これらのパケットのみ受信している場合は、データを受信していないと判断し、ICMP ECHO の送信を行います。データ受信の有無は統計情報から判断するため、ICMP ECHO を送信するインタフェースがポイントツーポイント（トンネル，PPP 等）以外の場合、受信の統計からはどの装置から受信したデー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-V から IX2000/IX3000 を監視し、IX-V 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 IX2000/IX3000 からトンネルインタフェース経由で送信されるため、IX-V 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-V の設定例]

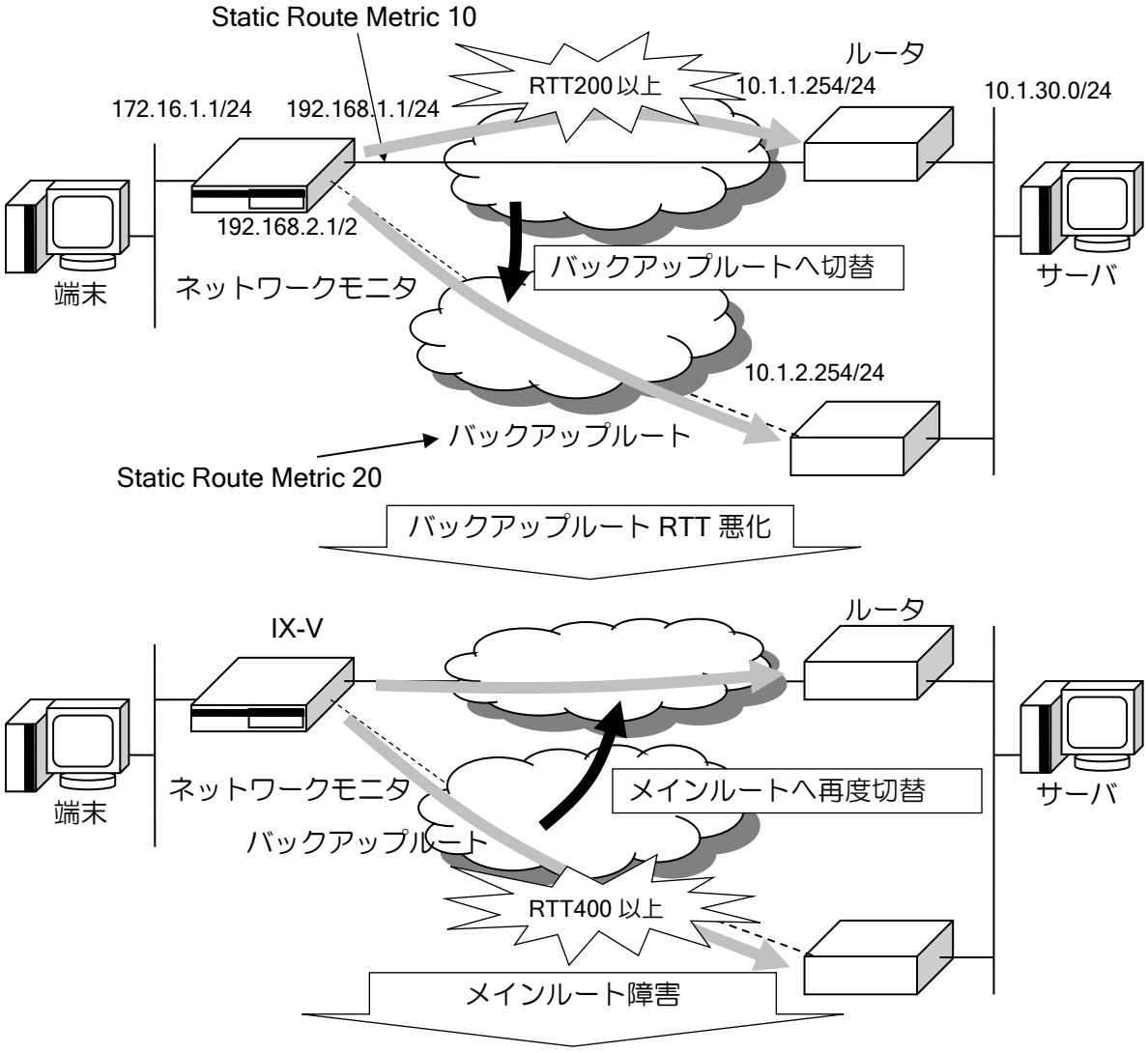
```
ip route default Tunnel0.0
ip route default 10.0.0.254 metric 100
ip route 192.168.1.2/32 10.0.1.254
!
watch-group traffic-watch 10
   event 10 ip unreach-host 192.168.0.2 Tunnel0.0
   probe-mode traffic event 10
   action 10 ip shutdown-route 0.0.0.0/0 Tunnel0.0
   probe-counter variance 1
   probe-timer 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
```

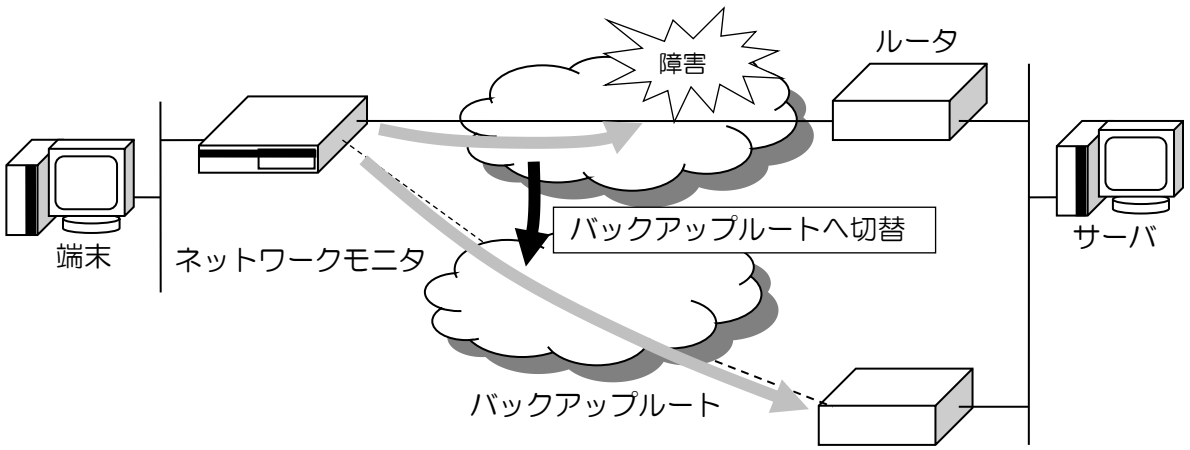
2.11.7 使用例

2.11.7.1 RTT（Round Trip Time）監視の例

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
```

2.11.8 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下さい。

(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。

送信間隔については、以下の値を推奨します。

- 対地数 128：送信間隔　平均 8 秒
- 対地数 256：送信間隔　平均 10 秒
- 対地数 512：送信間隔　平均 15 秒

(d) msec 指定の場合の対地数

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。

■2.12 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。

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。

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。

2.12.1 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 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。

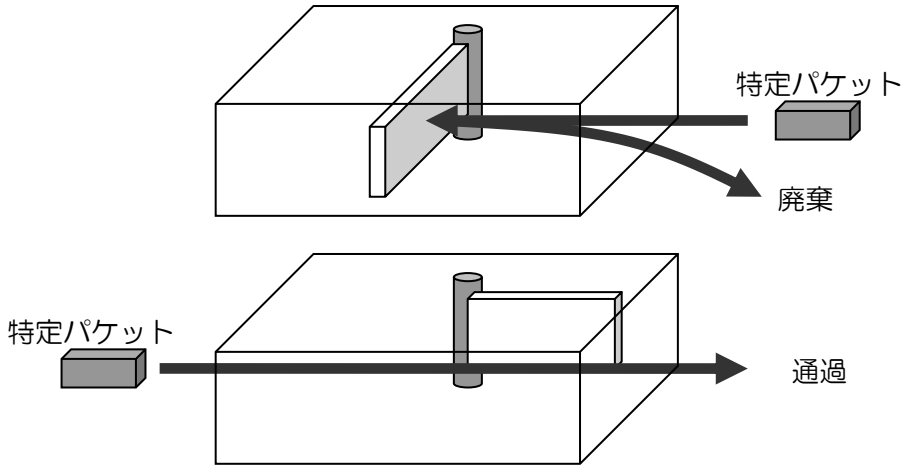
※スタティックフィルタは、UFS キャッシュを利用することにより、転送が高速化します。UFS キャッシュについては、UFS キャッシュの項目を参照してください。

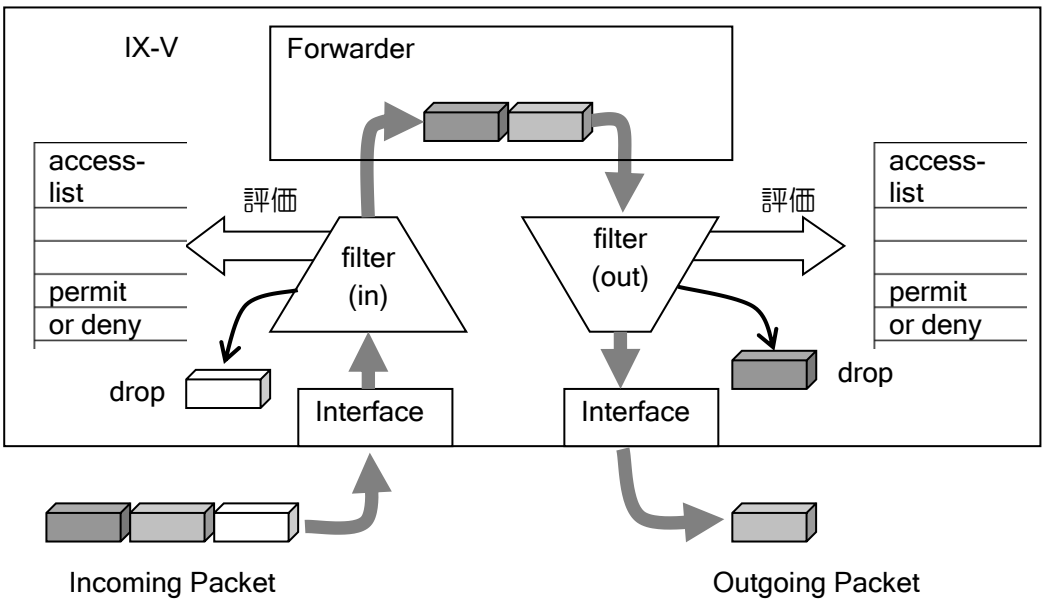
- 評価条件（アクセスリストと同一となります）
  - プロトコル
  - 送信元/送信先アドレス（プレフィックス指定 / マスク指定）
  - 送信元/送信先ポート（TCP、UDP、ICMP のみ）
  - TCP ヘッダ制御フラグ
  - TOS フィールド（Precedence / TOS / DSCP）
  - ICMP メッセージ
  - フラグメント

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。

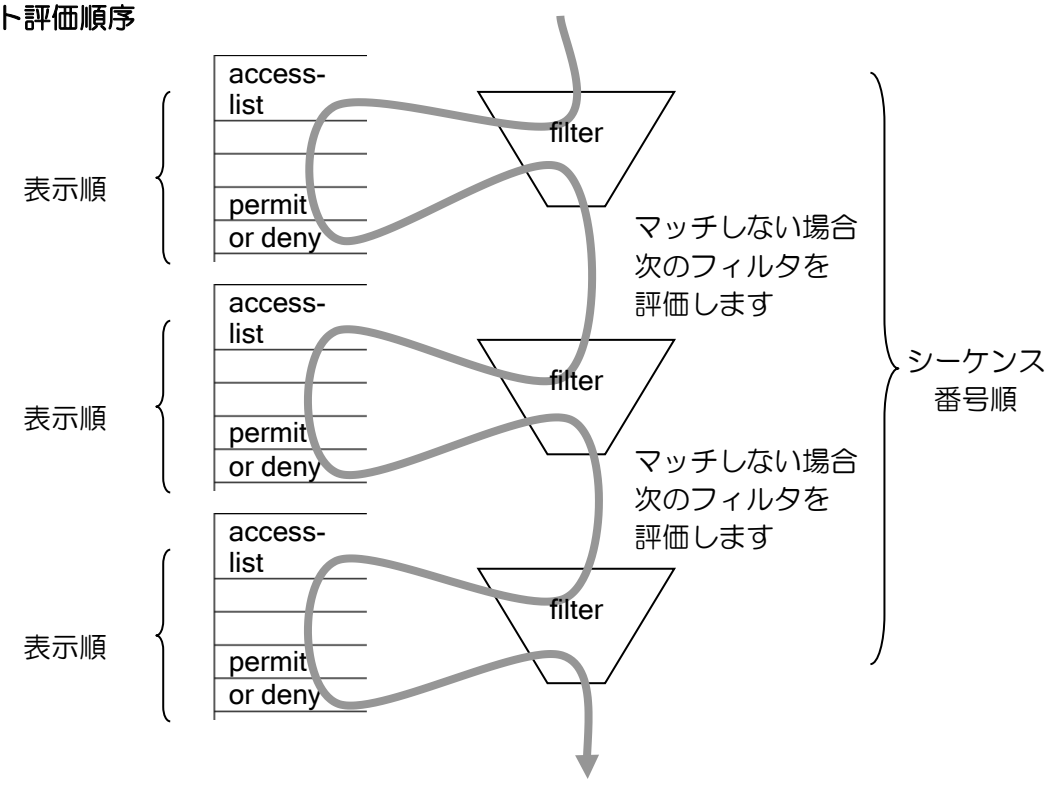
以下にスタティックフィルタの評価ポイントおよび評価ポイントにおける処理を示します。

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ください。

ip filter	IPv4 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

【設定例】

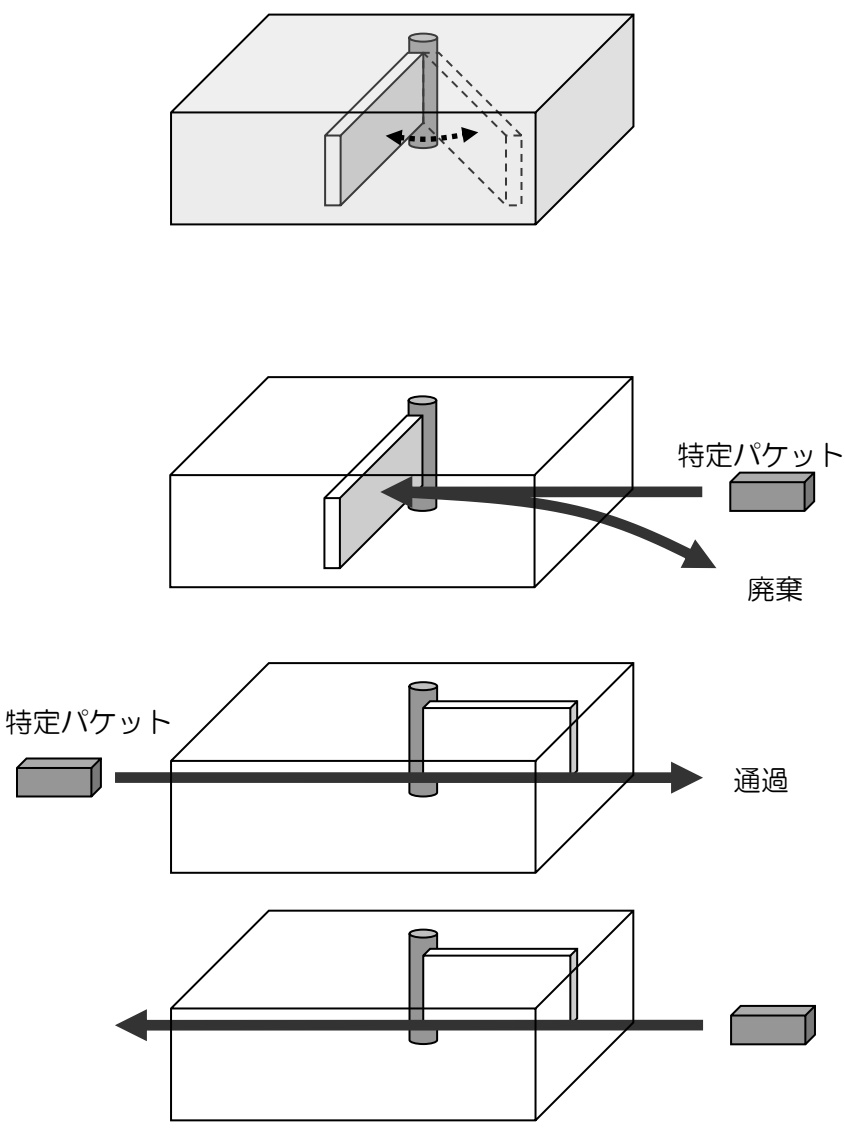
```
ip access-list access-1 permit ip src 192.168.0.0/24 dest any
interface GigaEthernet0.0
   ip address 10.0.0.1/8
   ip filter access-1 100 in
   no shutdown
```

2.12.2 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 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
ip access-list dynamic	IPv4 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

2.12.2.1 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】

```
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
```

2.12.2.2 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）

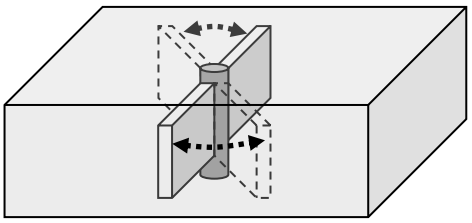
なお、アクセスリストを指定する方法でも FTP のパケットを検知した場合には、自動的に通信可能にします。別途サービス指定で FTP を設定したダイナミックフィルタを用意する必要はありません。FTP で使用する TCP のポート 21 番がトリガの範囲にある必要があります。

【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。

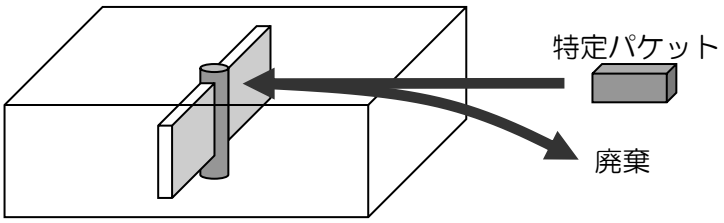
```
ip access-list deny-all deny ip src any dest any
ip access-list access1 permit ip src any dest any
ip access-list dynamic dyn-access access access1
!
interface GigaEthernet1.0
   ip address 10.0.0.1/8
   ip filter dyn-access 100 out
   ip filter deny-all 100 in
   no shutdown
```

(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

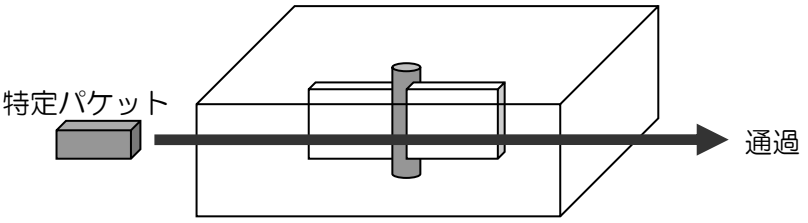
ダイナミックフィルタ（高度な利用）概念図



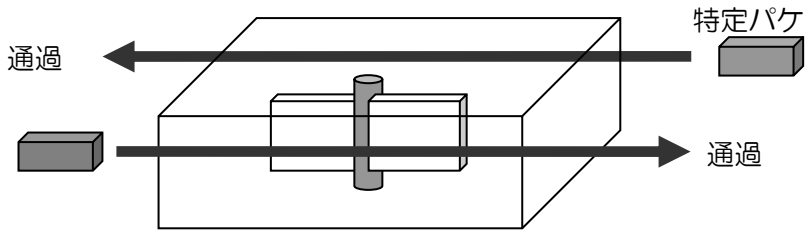
トリガとなるパケットと、トリガパケットの通過に伴って穴を開けたいフィルタを、任意の条件のアクセスリストを使用して、より詳細に設定することができます。



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。

```
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
```

2.12.2.3 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。

2.12.2.4 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。

2.12.3 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）

2.12.4 パケットフィルタのイベントログ

パケットフィルタ機能と SYSLOG 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イベント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。

パケットフィルタのイベントログは SYSLOG 設定時の機能名として ip-flt を指定します。イベントログについての説明は別途遠隔設定と監視の章を参照ください。

【設定例】
フィルタにより廃棄した時のイベントログを表示する。

```
syslog enable 1000000
syslog function ip-flt warn

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】

```
show syslog

2023-02-09T14:52:25.678259+09:00 ip-flt - 007 - BLOCK icmp 10.1.0.2 > 10.10.10.254, match access1, GigaEthernet0.0 in
```

上記の設定例のように、IP トラフィックフィルタの syslog 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より廃棄される環境の場合、遮断イベント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、指定した遮断フィルタによるパケット廃棄イベント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 filter {ACL_NAME} {SEQ_NUM} {in | out} suppress-logging	パケット廃棄いべんとログを出力しない

本装置では、SYSLOG 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)	遮断フィルタにより廃棄	×	○	○	○	○
(d)	暗黙の deny により廃棄	×	○	○	○	○
(e)	各種内部処理(正常系)	×	×	×	○	○
(f)	通過フィルタにより許可	×	×	×	○	○
(g)	フラグメントパケットの正常処理	×	×	×	×	○

○：イベントログが出力される　×：イベントログが出力されない

本設定を行うことで上記「(c) 遮断フィルタにマッチしたので廃棄」に関するイベントログの出

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。

SYSLOG 機能は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。

■2.13 トンネルの設定

2.13.1 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。

UNIVERGE IX-V シリーズは以下のトンネル機能をサポートしています。

- L2TP IPsecモード　（詳細はL2TPの設定の章を参照）

2.13.2 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

2.13.3 フラグメントの設定

トンネルは IPv4 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）のパケットはフラグメントが禁止されているため、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）。

ip forced-fragment コマンドでは、パケットのフラグメント禁止ビットを 0（無効）に書き換えます。ヘッダ情報を書き換えて良い場合に利用してください。

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

■2.14 IKE の設定

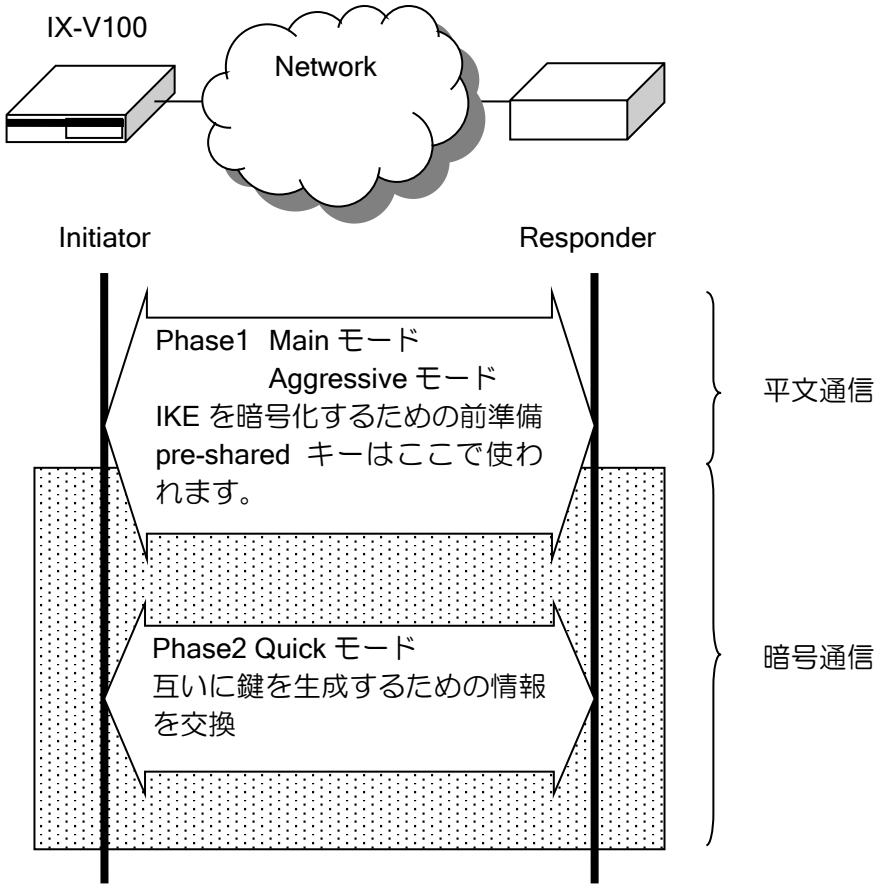
IKE（Internet Key Exchange）は、鍵交換プロトコルのことで、IPsec 通信を行う通信相手（ピア）との鍵を自動的に生成するために使用します。UNIVERGE IX-V シリーズでは、通信相手のアドレスが不定の場合についてもサポートしております。

IKE には IKEv1 と IKEv2 があり、本章では IKEv1 についてを記載いたします。IKEv2 については IKEv2 の章を参照してください。

IKEv1（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、UNIVERGE IX-V シリーズ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、UNIVERGE IX-V シリーズ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。

2.14.1 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	IPv4 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	IPv4 アドレス
ID_IPV4_ADDR_SUBNET	IPv4 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	AES-CBC-256
認証アルゴリズム	SHA2-512
認証手段	pre-shared
PFS	DH グループ: 3072-bit (DH group 15)
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:3072 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

UNIVERGE IX-V 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	Triple DES-CBC AES-CBC 128bit AES-CBC 192bit AES-CBC 256bit
認証アルゴリズム	HMAC-SHA1-96 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512
DH グループ	768-bit (DH group 1) 1024-bit (DH group 2) 1536-bit (DH group 5) 2048-bit (DH group 14) 3072-bit (DH group 15)

2.14.1.1 宛先の FQDN 指定

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

```
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 ipv4 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
   no shutdown
```

2.14.2 対向装置の監視

UNIVERGE IX-V 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

2.14.2.1 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。

UNIVERGE IX-V シリーズの IKE キープアライブ機能は RFC3706 に基づく仕様です。UNIVERGE IX-V シリーズ・UNIVERGE IX2000/IX3000 シリーズで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

UNIVERGE IX-V シリーズの 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。UNIVERGE IX-V 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。

2.14.2.2 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
```

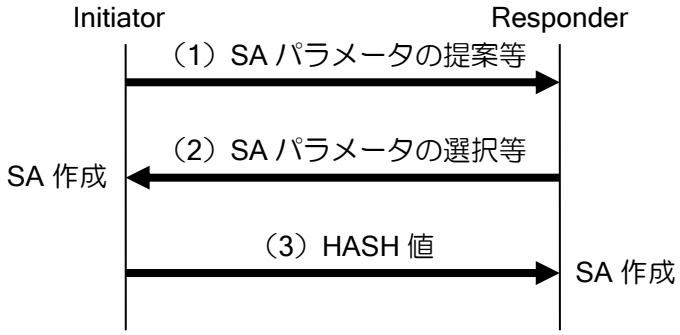
2.14.3 commit-bit 対応

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。

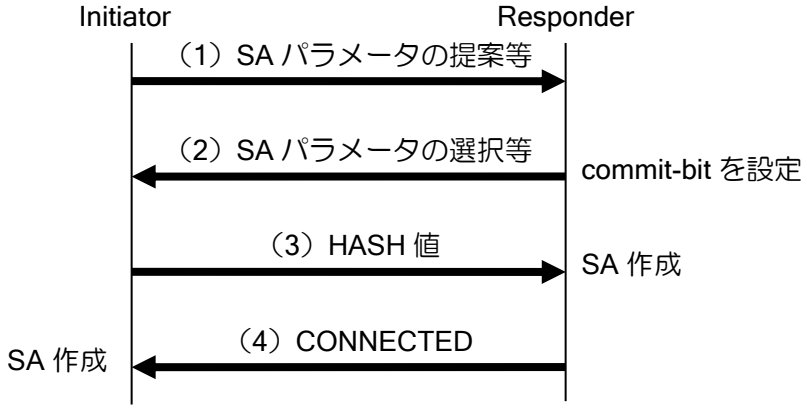
以下に commit-bit の動作を説明します。

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。

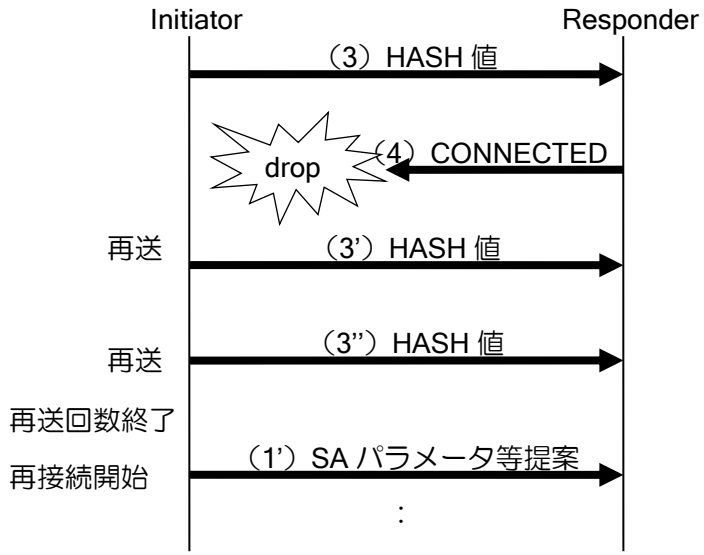
この状態の場合、Initiator は指定回数再送を行いますが、Responder は SA 作成済みなので（4）の再送は行いません。したがって、そのまま再送回数が終了しますので、SA 状態の不一致が発生します。

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

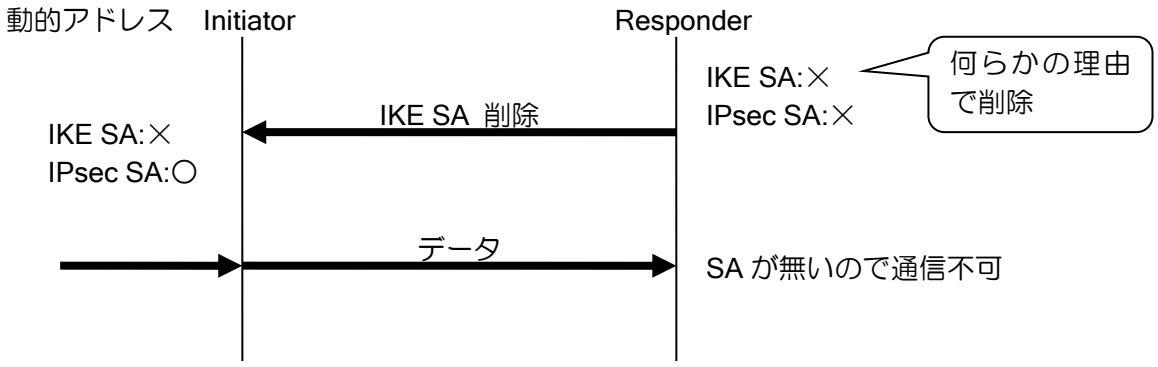
設定はありませんので、自動で再接続を行います。



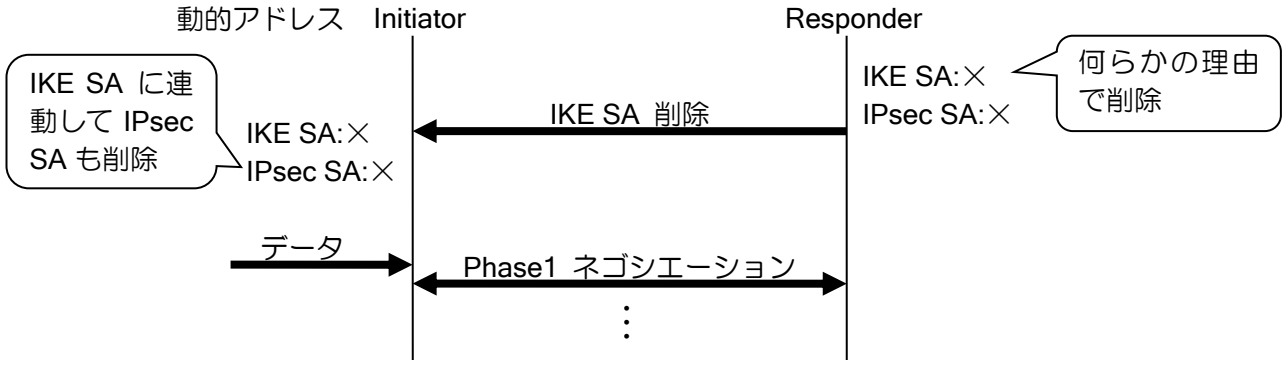
2.14.4 Dangling SA 型/Continuous-channel SA 型

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。UNIVERGE IX-V 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 共に削除され、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
```

2.14.5 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。
リキー開始タイミングの変更ができます。
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
```

2.14.6 DELETE 送信抑止設定

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
```

■2.15 IPsec の設定

IPsec には、データの完全性を保持するための認証機能と、データの機密性を保持するための暗号機能があります。

IPsec の機能は IKE と併用する必要があります。IKE には IKEv1 と IKEv2 がありますが、本章は IKEv1 と併用する場合の IPsec について記載いたします。IKEv2 を利用する場合の IPsec については IKEv2 の章を参照してください。

- 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。
- NAT トラバーサル機能が利用可能です。
- ESP にのみ対応し、AH には対応しません。
- L2TP リモートアクセス機能に対応します。

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
- 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。

2.15.1 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。L2TP リモートアクセス機能等の IKE 以外のプロトコルと併用する場合はトランスポートモードを指定します。IKE プロトコルのみを利用する場合はトンネルモードを選択します。

- インタフェース指定
  - IPsec 処理を実施するトンネルインタフェースを選択します。トンネルインタフェース以外は指定出来ません。

- 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

自動鍵ポリシーは、対向装置毎との自動鍵生成に必要な以下のパラメータを設定します。

- IPsec 通信相手アドレス
- PFS 値
- 自動鍵プロポーザル
-

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	AES-CBC-256
ESP 認証アルゴリズム	HMAC-SHA2-512
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。IKEv1 については、IKEv1 の節に詳細を記述します。

(c) アルゴリズム

UNIVERGE IX-V 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	Triple DES-CBC AES-CBC 128bit AES-CBC 192bit AES-CBC 256bit
ESP 認証アルゴリズム	HMAC-SHA1-96 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512

2.15.1.1 強制フラグメント

DF ビットが設定された IPv4 パケットをフラグメントすることができます。

通常、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が、設定により強制的にフラグメント動作させることが可能です。。

設定は以下のコマンドで行います。

ipsec policy ... mtu ignore	強制フラグメント設定

2.15.1.2 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、IKEv1 の場合と同様ですので、「IKEv1 の設定」の章を参照して下さい。

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 を指定して下さい。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下さい。

【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
```

2.15.1.3 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。

通信経路やインターネット回線上において帯域制御によりパケットの転送順序が変更されるような環境では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
```

2.15.1.4 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。

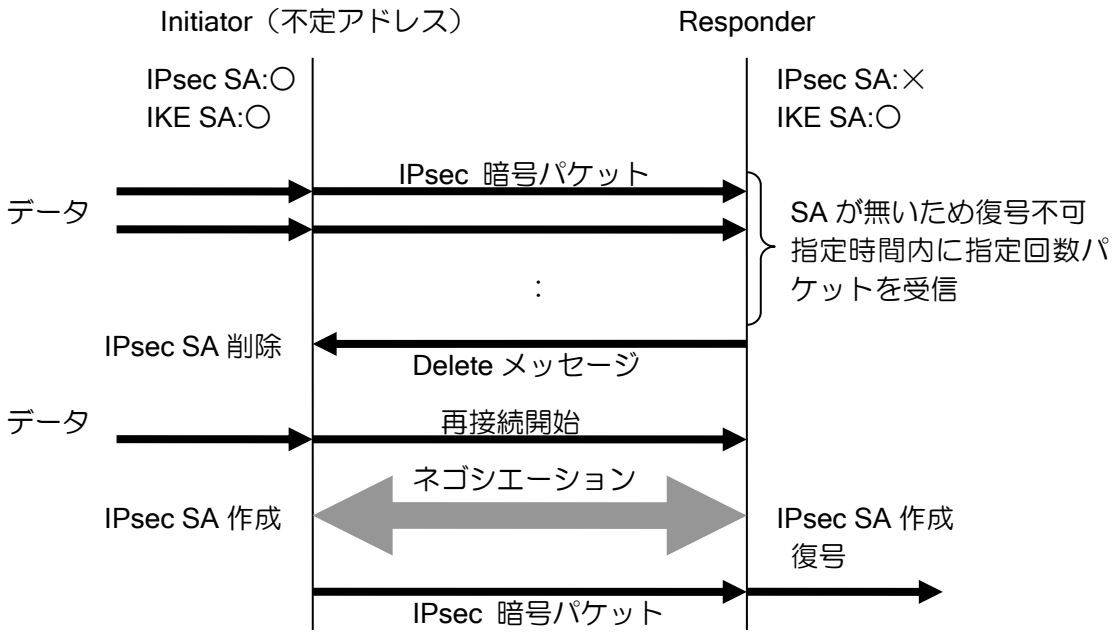
DELETE 送信機能は、相手装置に無効な IPsec SA 情報を削除させる機能です。ただし、DELETE メッセージを送信できるのは IKE SA が存在しているときのみです。

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
```



2.15.1.5 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。

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。

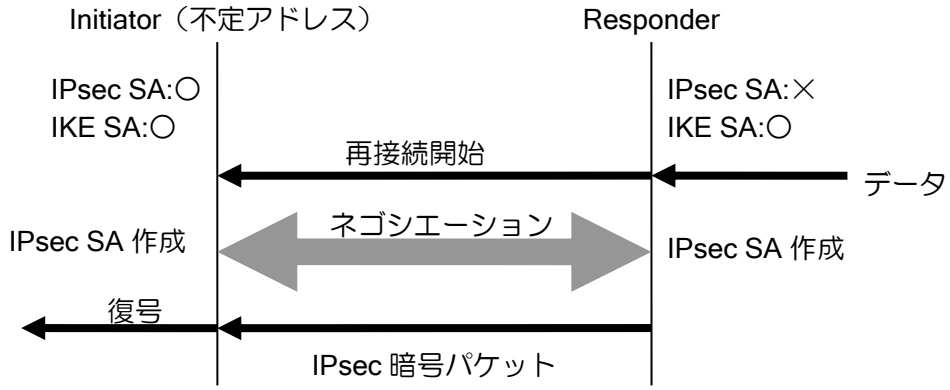
設定は、自動鍵ダイナミックポリシーの設定コマンドを使用します。

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
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

2.15.1.6 リキー設定

IKEv1 は IPsec で使用する鍵を一定期間で更新するリキー(Rekey)機能が利用出来ます。

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。

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。

2.15.1.7 宛先の FQDN 指定

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

```
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 ipv4 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
  no shutdown
```

2.15.1.8 IKE フェーズ2 ID 送信なし機能

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

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
  no shutdown
```

2.15.2 トンネルモード

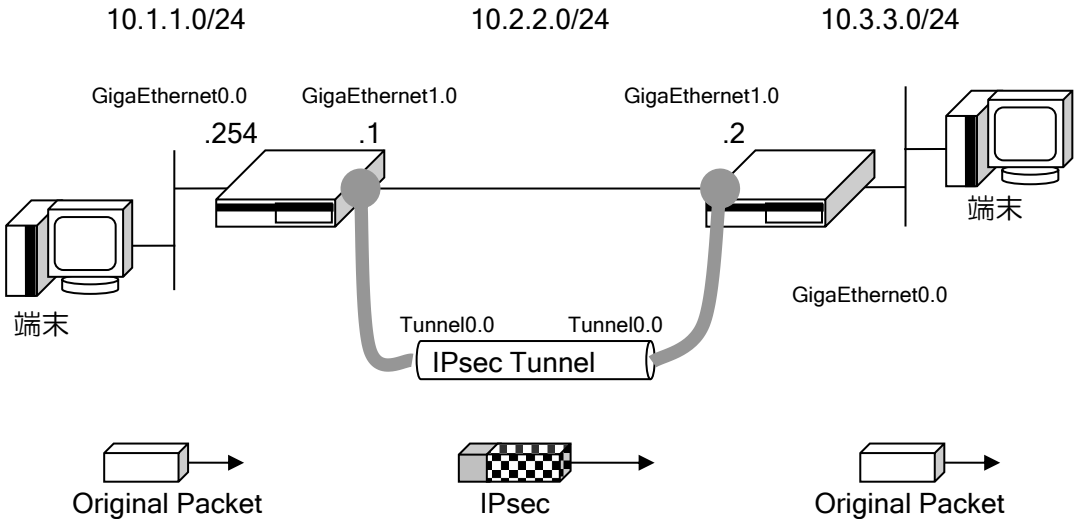
トンネルモードは、L2TP の IPsec 以外のカプセル化プロトコルと併用"しない場合に利用します。。

オリジナルのパケットに対して、暗号化を行い、その後に ESP ヘッダ、IP ヘッダ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。

tunnel mode ipsec	トンネルインタフェース IPsec 適用設定
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イメージと設定例を示します。

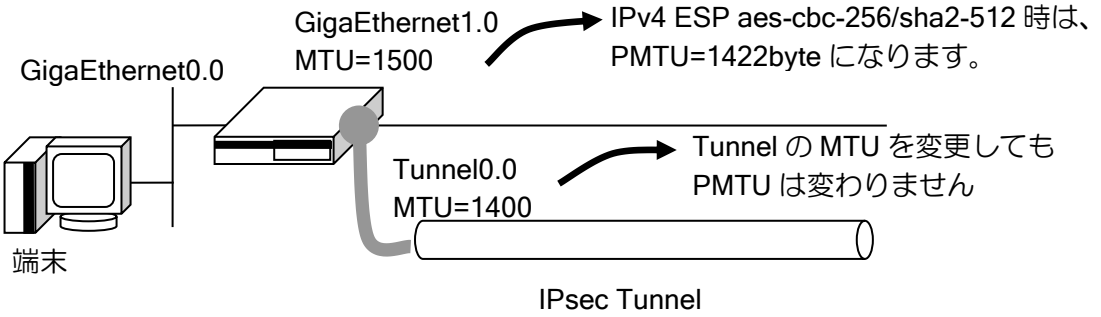


【設定例】

```
ip route 10.3.3.0/24 Tunnel0.0
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 ipv4 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
   no shutdown
```

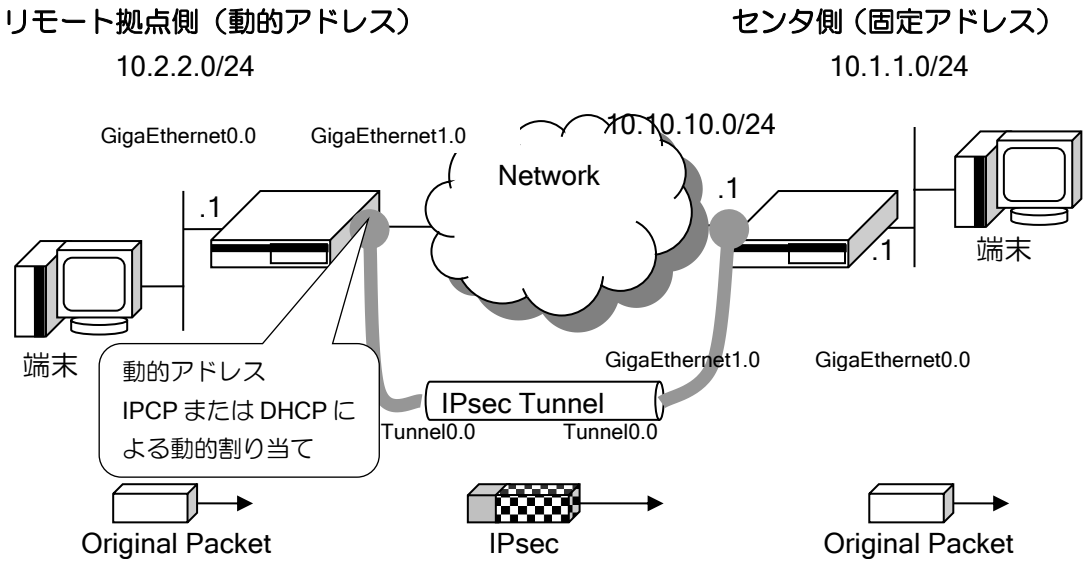
※トンネルモード使用時の MTU に関する注意事項

- ✧ 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。
- ✧ 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。



2.15.3 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（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
!
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 ipv4 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
   no shutdown


センタ側（固定アドレス側）

ip route 10.2.2.0/24 Tunnel0.0
!
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 ipv4 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
   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。

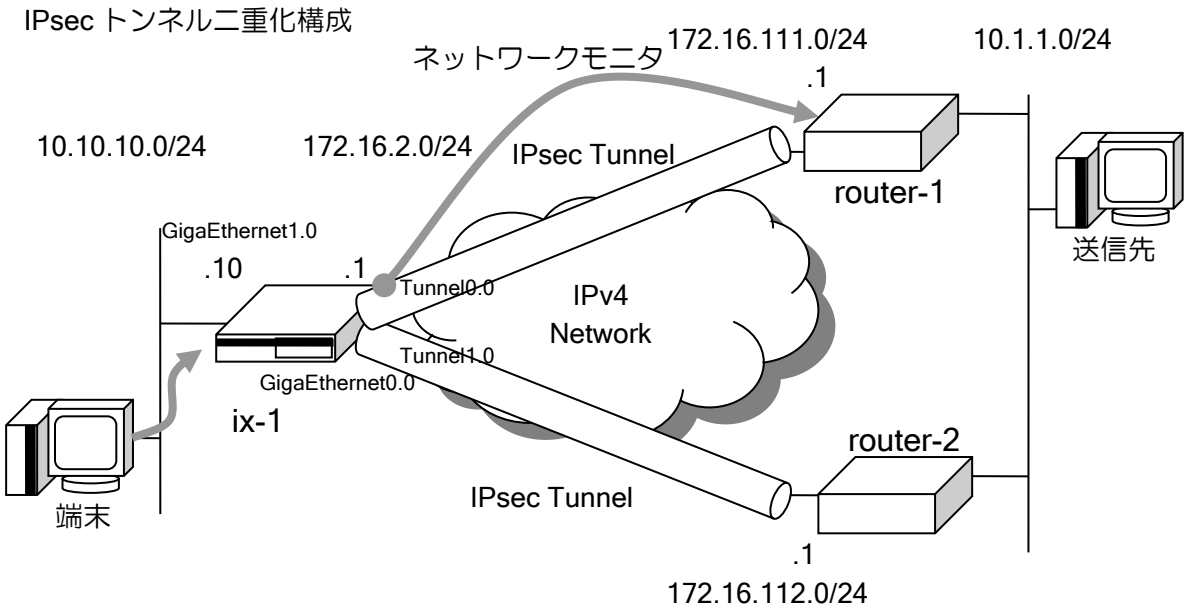
2.15.4 IPsec トンネル二重化対応

IPsec トンネルの二重化構成を組むためには、IPsec と共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】

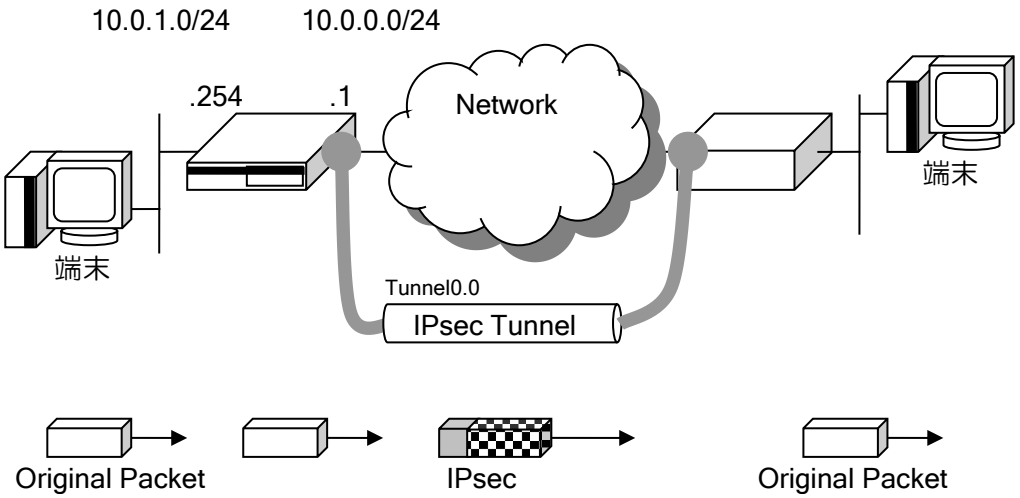
```
ip route default 172.16.2.254
ip route 10.1.1.0/24 Tunnel0.0
ip route 10.1.1.0/24 Tunnel1.0 metric 100
ike proposal ike-pro1 encryption 3des hash sha lifetime 3600
ike policy ike-poli1 peer 172.16.111.1 key key1 mode aggressive ike-pro1
ike policy ike-poli2 peer 172.16.112.1 key key2 mode aggressive 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 ipv4 peer 172.16.111.1 ipsec-pro1
ipsec autokey-map ipsec-poli2 ipv4 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
   no shutdown
!
interface Tunnel1.0
   tunnel mode ipsec
   ip unnumbered GigaEthernet1.0
   ipsec policy tunnel ipsec-poli2
   no shutdown
```

2.15.5 IPsec と NAT/NAPT の連携

IPsec の経路の途中に NAT/NAPT ルータが存在する等、アドレス・ポートが変更されるような環境では 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）



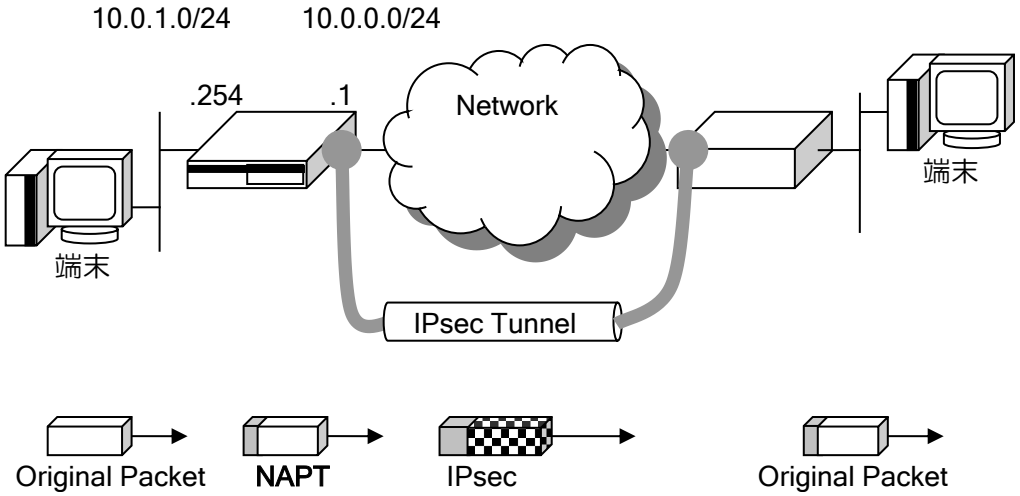
インターネット VPN の設定などで、WAN 側インタフェースで NAT/NAPT を有効にし、IPsec の設定も行う場合、アドレスは変換されないので NAT トラバーサルの設定は不要です。ただし、相手側から通信が開始された場合に、NAT/NAPT でパケットが廃棄されないように、静的 NAPT の設定が必要になります。

【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
   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
   no shutdown
```

2.15.6 トランスポートモード

トランスポートモードは、L2TP 等のカプセル化プロトコルを併用する場合に利用します。オリジナルパケットに対して、L2TP ヘッダ等のヘッダを付加した後に暗号化を行い、その後に ESP ヘッダ、IP ヘッダ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。

tunnel mode l2tp-lns ipsec	トンネルインタフェース L2TP/IPsec 適用設定
ipsec policy transport	トランスポートモードの設定

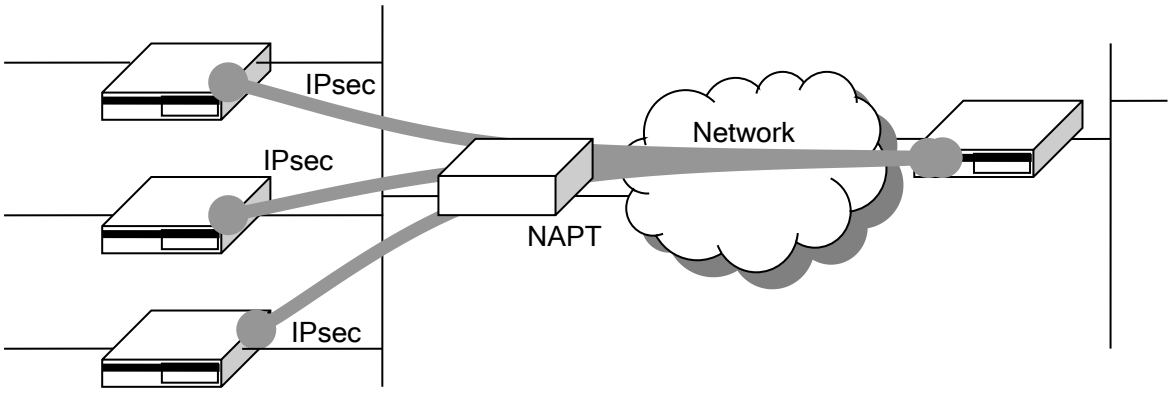
トランスポートモードはトンネルモードと異なりデフォルトでは ID を送信しませんので、ID が必須の対向装置との接続には、with-id-payload を設定してください。

IPsec のトランスポートモードの設定例についてはスマートデバイス対応（L2TP LNS 機能）の章を参照してください。

2.15.7 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 VPN 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

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）

UNIVERGE IX-V シリーズの 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

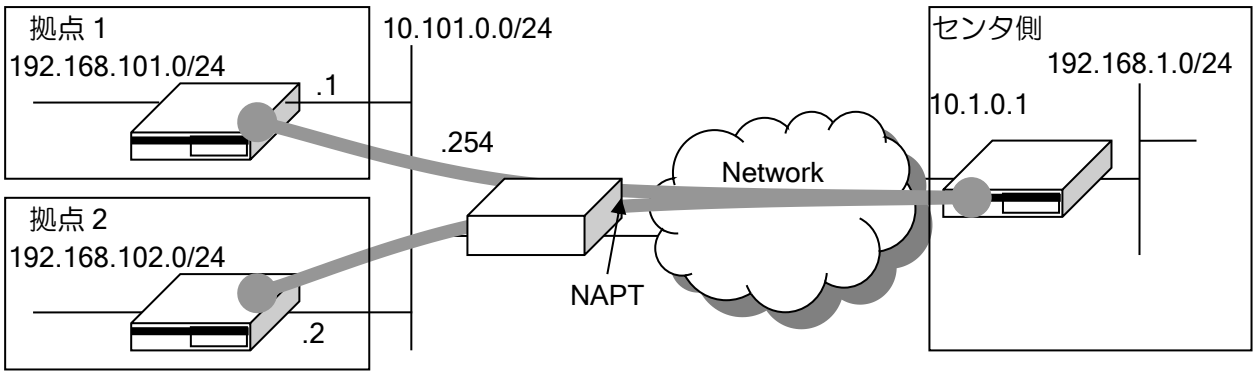
この設定を行わなかった場合、フラグメントパケットが NAT/NAPT ルータで正しく変換されずに廃棄されてしまう可能性があります。

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
!
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 ipv4 ipsecprop ike ike-site1
!
ipsec dynamic-map ipsec-site2 ipv4 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
   no shutdown

interface Tunnel2.0
   tunnel mode ipsec
   ip unnumbered GIgaEthernet1.0
   ipsec policy tunnel ipsec-site2 pre-fragment
   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
!
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 ipv4 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
   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）
        :
```

■2.16 スマートデバイス対応（L2TP LNS 機能）の設定

スマートフォンなどに実装されている L2TP/IPsec のクライアントを利用して、UNIVERGE IX-V シリーズ配下のネットワーク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。

2.16.1 L2TP LNS 機能の概要

UNIVERGE IX-V シリーズ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。
- Radius 連携はサポートしておりません。

2.16.2 動作確認端末

動作確認した端末は以下のとおりです。

- Windows 10
- Windows 11
- iPhone (IOS)

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。

2.16.3 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。

2.16.4 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】

```
ike nat-traversal
!
ike proposal ike-prop1 encryption aes-256 hash sha group 1024-bit
ike proposal ike-prop2 encryption aes hash sha group 2048-bit
ike proposal ike-prop3 encryption aes hash sha group 1024-bit
ike proposal ike-prop4 encryption 3des hash sha group 1024-bit

ike policy ike-policy peer any key SECRET ike-prop1,ike-prop2,ike-prop3,ike-prop4
!
ipsec autokey-proposal ipsec-prop1 esp-aes-256 esp-sha
ipsec autokey-proposal ipsec-prop2 esp-aes esp-sha
ipsec autokey-proposal ipsec-prop3 esp-3des esp-sha
ipsec dynamic-map ipsec-policy ipv4 ipsec-prop1,ipsec-prop2,ipsec-prop3
!
ppp profile lns
   authentication request chap
   authentication password user1 pass1
   authentication password user2 pass2
   authentication password user3 pass3
   lcp pfc
   lcp acfc
!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
```

2.16.4.1 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。

tunnel mode l2tp-lns ipsec	トンネルを L2TP/IPsec 対応に変更

2.16.4.2 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。

2.16.4.3 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

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

2.16.5 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

■2.17 IKEv2/IPsec の設定

UNIVERGE IX-V シリーズでは、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。

2.17.1 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。

2.17.1.1 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。認証方式は、事前共有鍵方式のみになります。

- ID/認証方式

認証方式		
事前共有鍵方式		
ID		
ID_IPV4_ADDR	ID_FQDN	ID_RFC822_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)	ENCR_AES_GCM(256bit)
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		
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		
DH グループ（DH）		
MODP-3072	MODP-2048	MODP-1536
MODP-1024	MODP-768	

- 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。
  - 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。

2.17.1.2 IKEv2/IPsec の未サポート機能一覧

UNIVERGE IX-V 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	AH 認証	

その他の代表的な IKEv2 機能		
コンフィグペイロード	プライベート MIB 対応	デジタル署名クライアント DSS 認証
ESP 拡張シーケンス	ESP TFC パディング	REAUTH

2.17.1.3 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。
- 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。

2.17.2 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。

2.17.2.1 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）
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

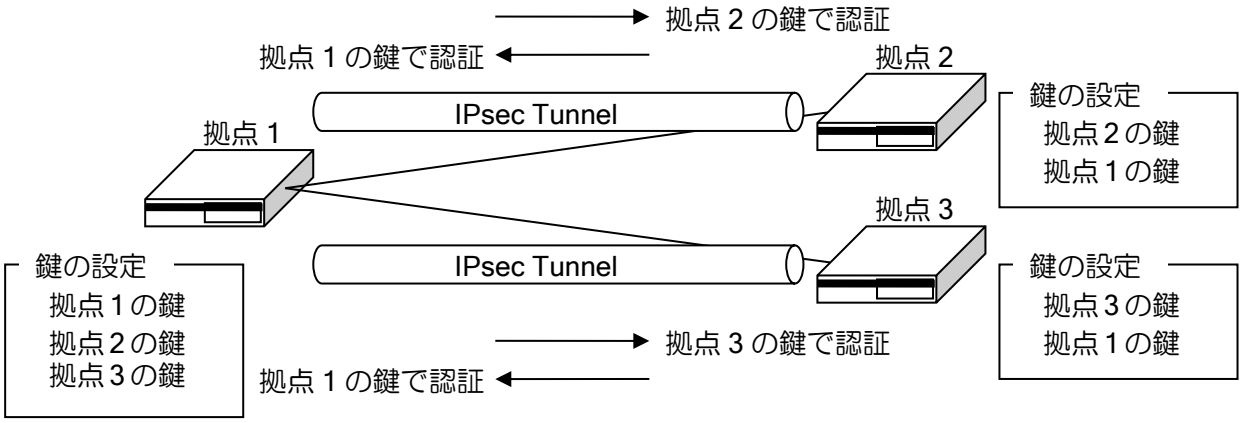
アンチリプレイの機能はデフォルト有効ですが、QoS の影響などでパケットの到着順序が入れ替わる可能性があるネットワークで利用される場合、アンチリプレイ機能が原因でパケットが破棄される可能性があります。そのような環境で利用する場合は、無効化してください。

2.17.2.2 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。

2.17.2.3 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。

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。

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、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

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。設定しない場合は IPv4 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。

2.17.3 NAT トラバーサル機能

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
            :
```

2.17.4 DELETE・REKEY 送信抑止設定

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。

2.17.5 注意事項

フィルタ機能、NAPT 機能

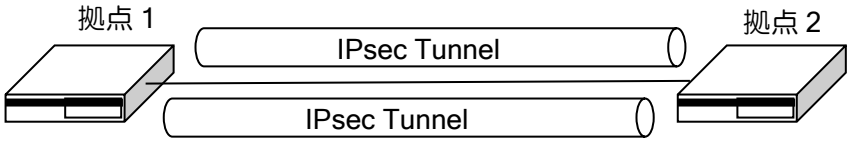
IKEv2 の IPsec を送受信するインタフェースにフィルタや NAPT を設定する場合、IKE（UDP ポート番号：500, 4500）と ESP（プロトコル番号：50）を遮断しないように注意してください。

【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。

2.17.6 複数ポリシーの設定

2.17.6.1 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
```

2.17.6.2 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
```

2.17.6.3 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

2.17.7 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。

2.17.8 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。

2.17.8.1 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
```

2.17.8.2 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。

2.17.8.3 イベントログ

IKEv2 のイベントログは SYSLOG 設定時の機能名として ikev2 を使用しますが、IPsec についてのイベントログは、IKEv1 による IPsec のイベントログと同様に機能名 IPsec を使用します。イベントログ設定についての説明は別途遠隔設定と監視の章を参照ください。

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。

■2.18 NetMeister の設定

NetMeister は、UNIVERGE IX-V 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 については、以下の URL を参照してください。

- 詳細：https://www.necplatforms.co.jp/product/netmeister/
- 操作方法：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
Ver1.0 以降	ダイナミック DNS	ダイナミック DNS
	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	コンフィグ、show tech-support 取得
	コンフィグ管理	コンフィグ情報の管理・反映機能
	メトリクス	トラフィックの表示
	ポート情報	ポート状態や LED の表示
	NetMeister Prime	任意 IP アドレスの死活監視などの有償サービス

2.18.1 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。

2.18.2 利用環境

NetMeister との通信では HTTPS(TCP/443)を使用しています。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。

- 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。

2.18.3 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。一部機能は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

2.18.4 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	NetMeister 機能の有効化
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
hostname	ホスト名（装置名）
nm update	即時更新
show nm status	NetMeister 情報の表示
show nm statistics	NetMeister 統計情報の表示

【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
```

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。

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。

2.18.4.1 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 status コマンドでも確認できます。

【表示例】

```
NetMeister Client:
  Result      : Success (20000)
  Last Request: 2023/04/01 23:59:59
  Next Request: 2023/04/09 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:
  IPv6 Domain :
  ErrorCode1  :
  ErrorCode2  :
  Interval    : 168 hours
API-GW:
  gpid        : sample-id
  stid        : sample-site
  htid        : 771234010101
  Interval    : 3600 sec
  Next Request: 2023/04/02 00:59:59 (remain 2999 sec)
  Status      : Registered
MQTT:
  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。

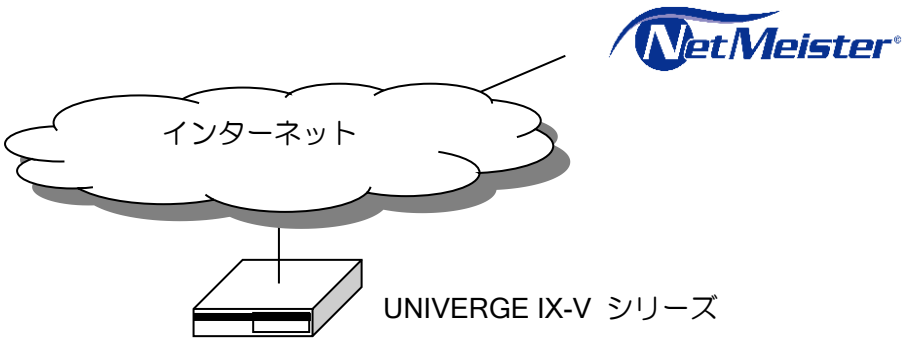
API-GW の Status が Registered でない場合、ダイナミック DNS 以外のサービスが利用できません。
MQTT の Status が Connected でない場合、基本保守機能の一部（アクション実行など）が利用できません。
IPv6 アドレスの DDNS 登録は未対応です。

2.18.5 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。

2.18.5.1 インターネット接続

UNIVERGE IX-V シリーズをインターネットに直接接続する構成です。



【設定例】
UNIVERGE IX-V シリーズ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

interface GigaEthernet0.0
   ip address dhcp receive-default
   ip napt enable
   no shutdown

interface GigaEthernet2.0
   description LAN
   ip address 192.168.0.254/24
   no shutdown
```

2.18.6 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

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

2.18.6.1 ダイナミック DNS の拡張設定

拡張設定が必要なケースと、その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となる OCI のパブリックアドレスのみダイナミック DNS に登録します。
それ以外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。

nm ddns notify interface	ダイナミック DNS 登録インタフェースの設定

【設定例】
IPv4 アドレスの通知インタフェースは GigaEthernet0.0

```
nm ip enable
nm account example-gp1 password plain example-pass1
nm sitename tokyo
nm ddns notify interface GigaEthernet0.0 protocol ip

interface GigaEthernet0.0
  ip address dhcp 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

2.18.7 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	---
CPU 使用率の異常・復旧	※1	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	※1	メモリ使用量が 3 回連続で 95%以上	メモリ使用量が 3 回連続で 80%以下
切断通知	※2	MQTT の切断	MQTT の接続
ネットワークモニタ通知	※3	ネットワークモニタイベント検出時	ネットワークモニタイベント復旧時

※1 監視周期は 1 分となります。
※2 MQTT の通信ができない環境では使用できません。
※3 通知したいイベントの watch グループに NetMeister アラーム通知のアクションを設定する必要があります。

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

2.18.8 アクション実行

以下の処理が実行できます。

- 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
- コマンド実行
- 再起動

2.18.9 メトリクス

トラフィックのグラフを表示することができます。

2.18.10 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。

2.18.11 NetMeister Prime

NetMeister Prime とは NetMeister の有償サービスです。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、以下の URL を参照してください。

・https://www.necplatforms.co.jp/product/netmeister/prime.html

■2.19 アクセスリストの設定

2.19.1 IPv4 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。アクセスリストは基本的に 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。

アクセスリストごとに以下の拡張が利用可能です

- シーケンス番号指定は、表示順の途中に設定を追加可能です。
- 評価最適化は、アクセスリスト内にエントリが多数含まれる場合でも性能低下を抑制できます。
- キャッシュ無効化は、アクセスリスト内にエントリが数行の場合に、効率よくキャッシュを利用できます。

2.19.1.1 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
show ip access-list	IPv4 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

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）
- 送信元/送信先ポート（TCP、UDP、ICMP のみ）
- TCP ヘッダ制御フラグ
- TOS フィールド（Precedence / TOS / DSCP）
- ICMP メッセージ
- フラグメント

2.19.1.2 TOS フィールドの評価

TOS 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

2.19.1.3 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。

2.19.1.4 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。

2.19.1.5 アクセスリストの高速化

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

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。

2.19.1.6 アクセスリストのシーケンス番号指定

アクセスリストの最後に追加する方式に加え、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

※ 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～

2.19.1.7 アクセスリストキャッシュの無効化

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

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
```

2.19.1.8 アクセスリストキャッシュのタイムアウト指定

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

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。

2.19.2 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。

■2.20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
- 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 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。
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 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。
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。

■2.21 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。

- 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
show ip prefix-list	IPv4 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
```

■2.22 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、UNIVERGE IX-V シリーズの独自機能です。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。

2.22.1 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）
- ダイナミックフィルタ情報　（通過キャッシュ情報など）

2.22.2 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。

• 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	

• 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

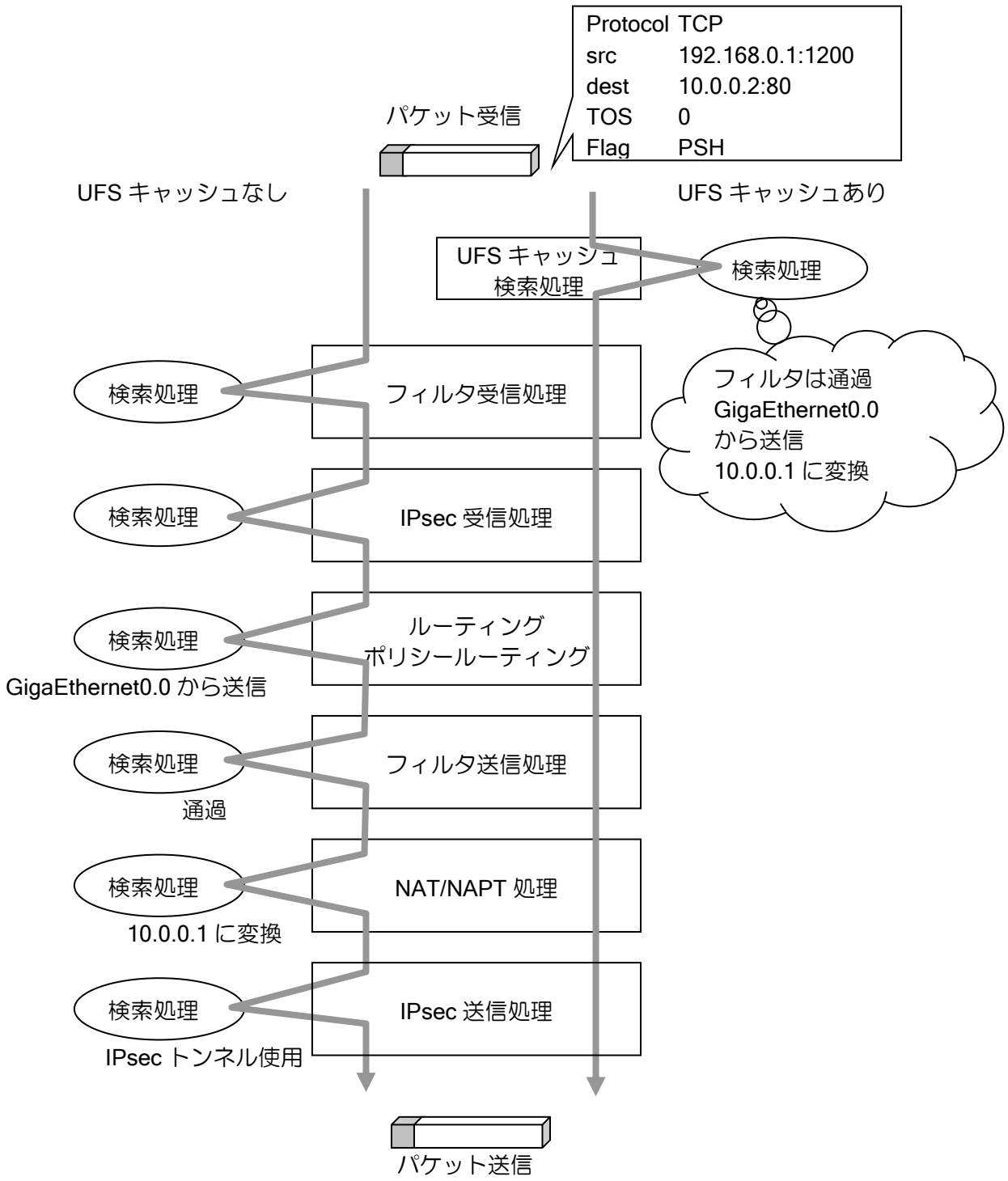
• TCP/UDP/ESP/GRE/ICMP 以外

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）

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。

2.22.3 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。

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

2.22.4 UFS キャッシュの表示

UFS キャッシュの内容表示は以下のコマンドを使用します。

show ip 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	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	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

2.22.4.1 無効キャッシュ

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 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。）

2.22.5 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）

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。

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。
※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。

3章 保守・運用

本章では、UNIVERGE IX-V シリーズの設定の変更、保存について説明します。

■3.1 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や特定のコマンド操作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。

3.1.1 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
no interface	reload を実行し再起動

3.1.2 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。

- 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 ebgp-multihop	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

- 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。

■3.2 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ます。そのため装置の再起動を行うと、設定内容が消えてしまいます。

装置再起動後も設定内容を有効にするためには設定データを内部の不揮発性メモリ上にスタートアップコンフィグとして保存する必要があります。

3.2.1 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
```

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

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
```

■3.3 LED 状態

UNIVERGE IX-V シリーズには仮想の LED があります。
show hardware コマンドや NetMeister 上で点灯状態を確認できます。

LED	状態	CLI 出力	条件
PWR	緑点灯	Green	装置が起動中の場合
VPN	緑点灯	Green	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	Off	PPP 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	Blink Green	PPP 接続処理中、または直前の PPP 接続で失敗した状態 IPCP が OPEN していない状態、または、直前で 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	Green	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	Green	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。

4章 遠隔設定と監視

本章では、UNIVERGE IX-V シリーズの遠隔設定と監視方法について説明します。

■4.1 SSH を利用した遠隔設定

4.1.1 SSH サーバの設定

UNIVERGE IX-V 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。

SSH サーバ機能はインタフェースコンフィグモードにサーバの起動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有効にすることができます。意図しないインタフェースからの SSH アクセスを防止することが可能です。

また、アクセスリストにより不特定アドレスからの SSH アクセスを防止することが可能です。

SSH サーバの設定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

GigaEhternet1.0 経由の 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。

【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 access-list ssh4

interface GigaEthernet1.0
  ip address 192.168.10.254/24
  ssh-server ip enable
  no shutdown
```

4.1.2 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。UNIVERGE IX-V シリーズは初回起動時に秘密鍵を生成します。

バージョンアップ時に新たなバージョンの UNIVERGE IX-V シリーズを起動した場合は秘密鍵も新たに生成されます。

秘密鍵の操作及び確認には以下のコマンドを使用します。

ssh-server host-key regenerate	秘密鍵の更新
show ssh-server host-key fingerprint	秘密鍵の fingerprint の表示

SSH クライアント側において表示される fingerprint と、秘密鍵の fingerprint 表示の内容が一致していることを確認することで、正しく UNIVERGE IX-V シリーズに接続していることを判断できます。。

4.1.3 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	diffie-hellman-group-exchange-sha256, ecdh-sha2-nistp256	
暗号アルゴリズム	aes256-ctr, aes192-ctr, aes128-ctr	
MAC アルゴリズム	hmac-sha2-512, hmac-sha2-256	
認証方式	サーバ認証	RSA
	クライアント認証	パスワード認証
秘密鍵仕様		
鍵長	RSA（2048bit）	

■4.2 SYSLOG によるイベントログ監視

UNIVERGE IX-V シリーズでは各種機能で発生した事象をイベントログとして監視することが出来ます。

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。

4.2.1 SYSLOG 機能

SYSLOG 機能によって本装置の各種機能ごとに指定した取得レベルのイベントログを採取し確認することができます。イベントログ情報は内部バッファに保存され、show コマンドにより保存された情報が表示されます。

4.2.1.1 SYSLOG の設定

イベントログの採取と保存は次の SYSLOG コマンドで設定します。

syslog enable <バッファサイズ>	イベントログの採取と保存の有効化、及び保存バッファサイズの設定
syslog function <機能名> <レベル>	イベントログ採取対象とする機能と取得レベルの設定

【設定例】

```
syslog enable 1000000
syslog function all warn
syslog function ikev2 info
```

バッファサイズの指定単位はバイト数になります。1 行あたり 80 バイト程度が目安となります。

指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、性能が激しく劣化する可能性があります。

機能名 all を指定した場合は全ての機能が対象となります。全機能指定 all と異なるレベルで各機能個別の syslog function または no syslog function が設定された場合、コンフィグ上には all の設定と個別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、設定された個別機能以外は all の設定で動作します。

【設定例 1】
IPv4 機能のみ debug レベルで出力、それ以外全て warn レベルで出力する場合

```
syslog function all warn
syslog function ipv4 debug
```

【設定例 2】
IPv4 機能のみ SYSLOG 出力なし、それ以外全て warn レベルで出力する場合

```
syslog function all warn
no syslog function ipv4
```

4.2.1.2 指定可能な機能と取得レベル

イベントログ収集対象として指定可能な機能は以下の様になります。

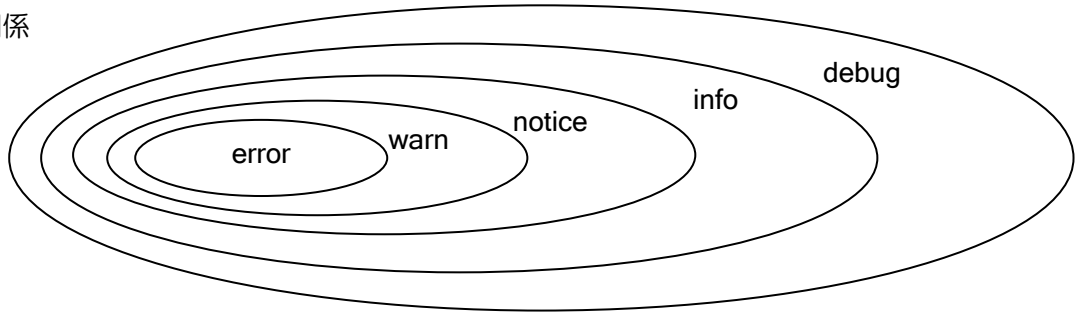
機能名	機能名	補足
all	全機能	個別指定されない機能についてのデフォルト設定となります。
acl	アクセスリスト	
arp	ARP	
bgp4	BGP	
ddns	ダイナミック DNS	
dhcp4c	IPv4 DHCP クライアント	
dhcp4s	IPv4 DHCP サーバ	
dns	DNS	
ether	イーサネット	
icmp4	IPV4 ICMP	
ikev1	IKEv1	
ikev2	IKEv2	
ip-flt	IP トラフィックフィルタ	
ipsec	IPsec	
ipv4	IPv4	
ix-v	IX-V ライセンス	
l2tpv2	L2TPv2	
nat	NAT/NAPT	
netmon	ネットワークモニタ	
nm	NetMeister	
ntp	SNTP	
pbr	ポリシールーティングの	
pdns	プロキシ DNS	
ppp	PPP	
rtmap	ルートマップ	
ssh	SSHv2	
system	システム	個別機能に含まれないイベントログに対する設定となります。
tcp	TCP	
udp	UDP	

イベントログ収集対象として指定可能なレベルは以下の様になります。

レベル	意味
error	エラー状態レベル
warn	警告状態レベル
notice	注意レベル
info	情報レベル
debug	デバッグレベル

レベル指定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 レベルを設定すると、error レベルのイベントログも同時に収集対象となります。

包含関係



4.2.1.3 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。

4.2.1.4 イベントログ確認

保存されたイベントログ情報は以下の SYSLOG コマンドにより確認できます。

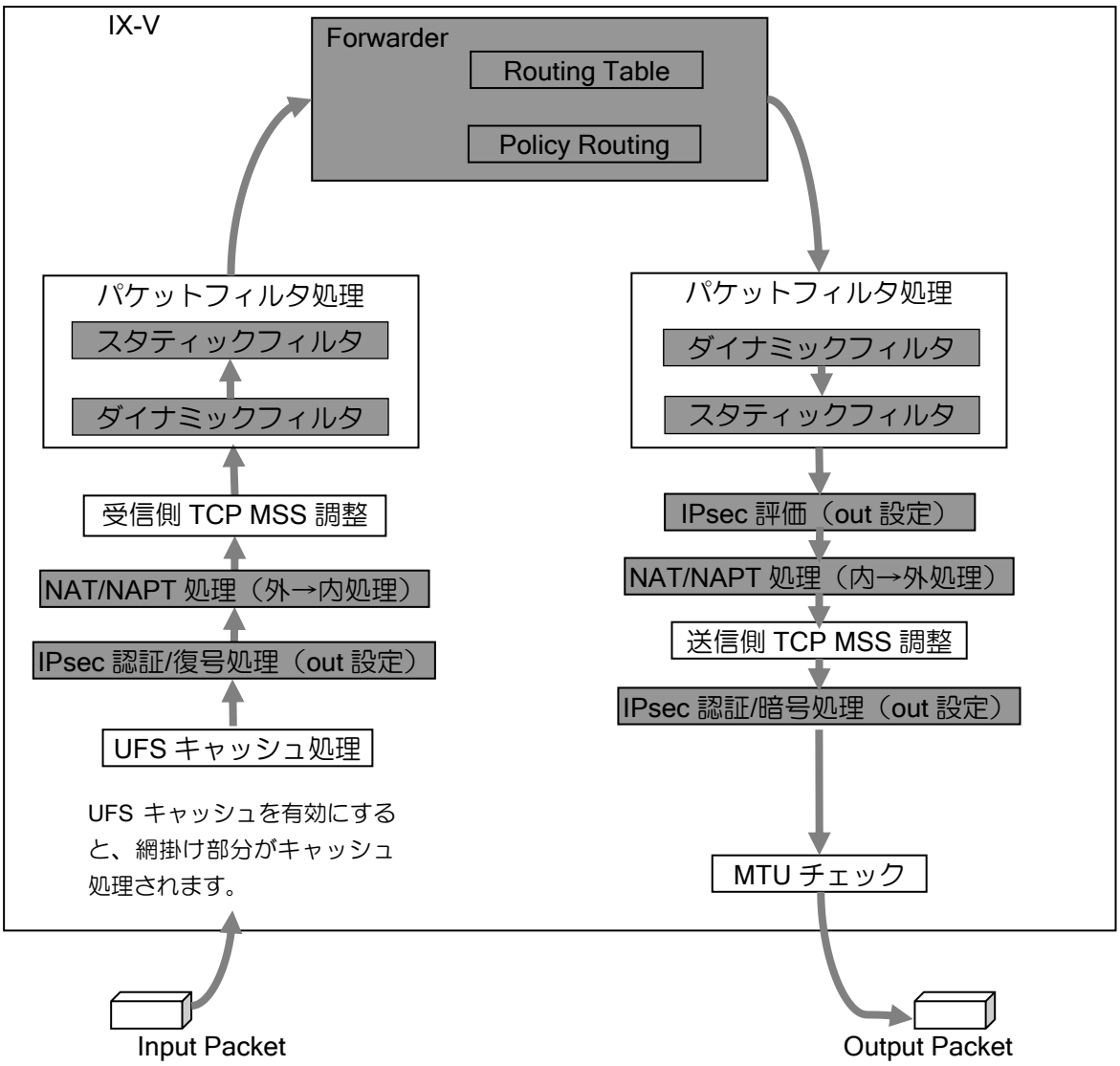
show logging	取得イベントログの表示

5章 パケット評価フロー

■5.1 IPv4 パケット評価

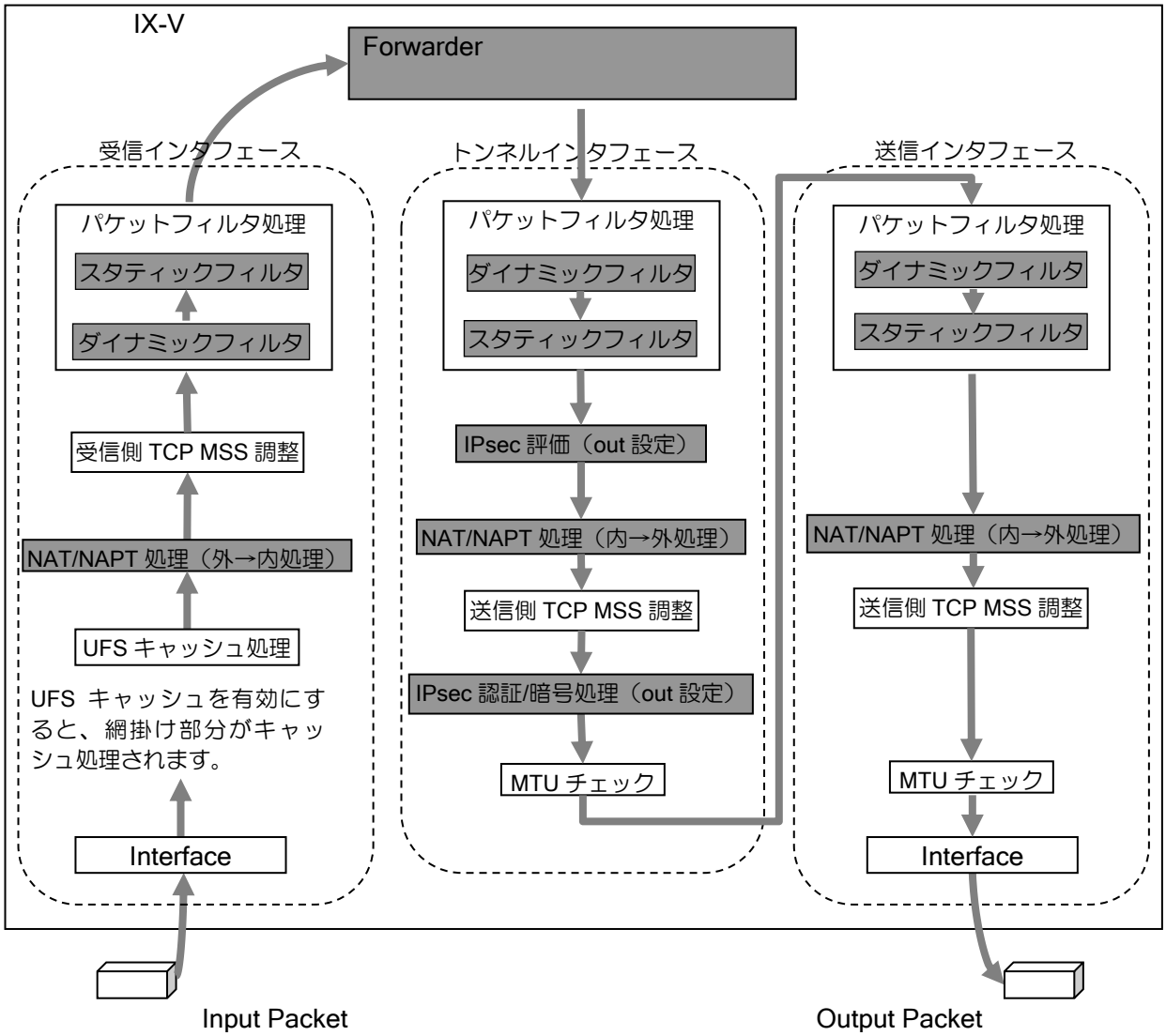
IPv4 Forwarder 配下のパケット評価順を説明します。

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。



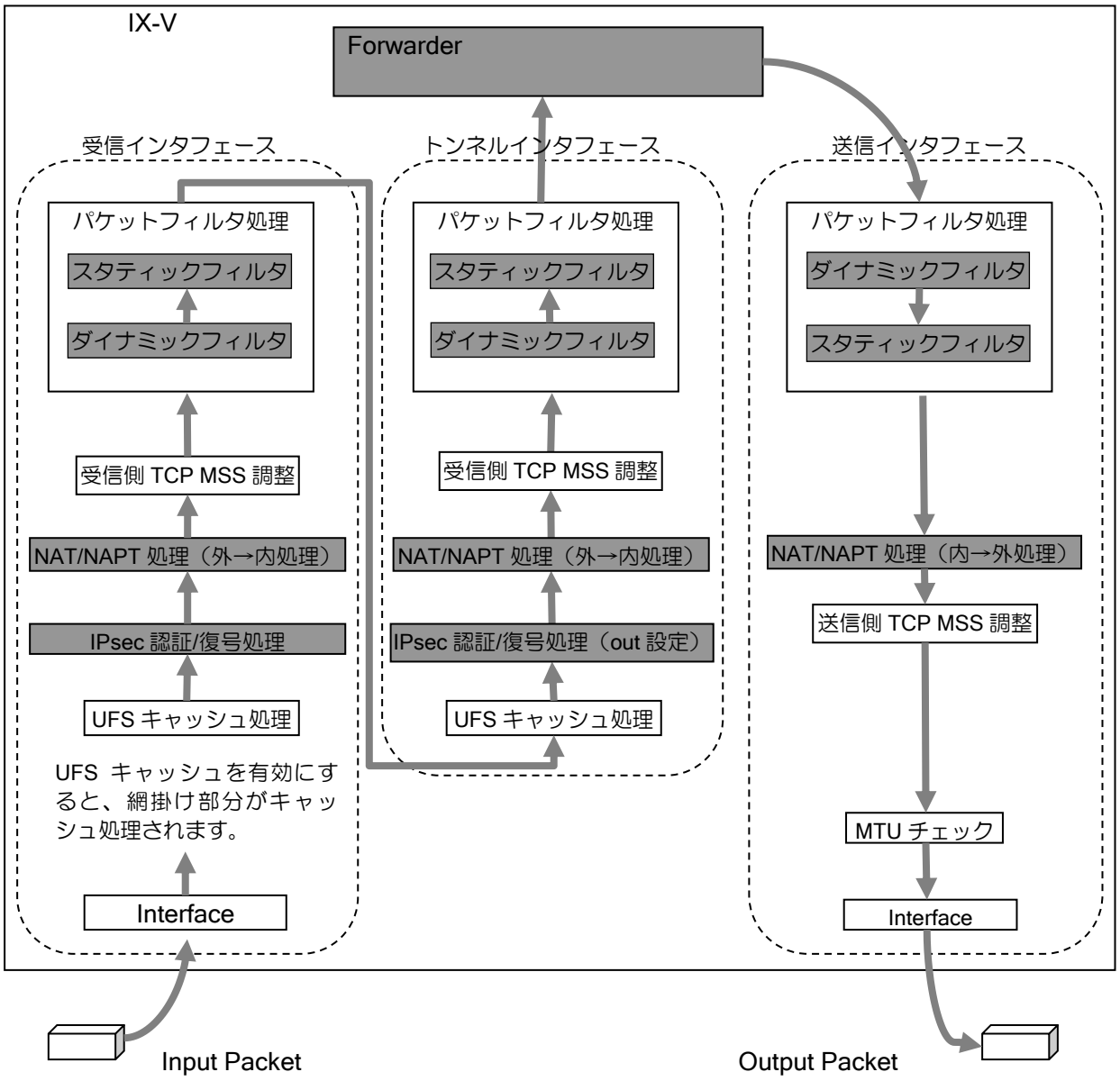
■5.2 IPsec 送信評価フロー

- IKE/IKEv2 の IPsec（トンネルモード）送信時の評価フロー



■5.3 IPsec 受信評価フロー

- IKE/IKEv2 の IPsec（トンネルモード）受信時の評価フロー



6章 付録

■6.1 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。

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)	

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	

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	

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	
RFC2796 BGP Route Reflection - An Alternative to Full Mesh IBGP	
RFC2918 Route Refresh Capability for BGP-4	

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

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 128, 192, 256bit
RFC4868 Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec	
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

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

RFC / Internet Draft	備考
RFC2661 Layer Two Tunneling Protocol "L2TP"	
RFC2809 Implementation of L2TP Compulsory Tunneling via RADIUS	
RFC3193 Securing L2TP using IPsec	

SSH サーバ

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	

syslog

RFC / Internet Draft	備考
RFC3164 The BSD Syslog Protocol	Authentication Problem を除く
RFC5424 The Syslog Protocol	

HTTP

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

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。

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

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

sntp

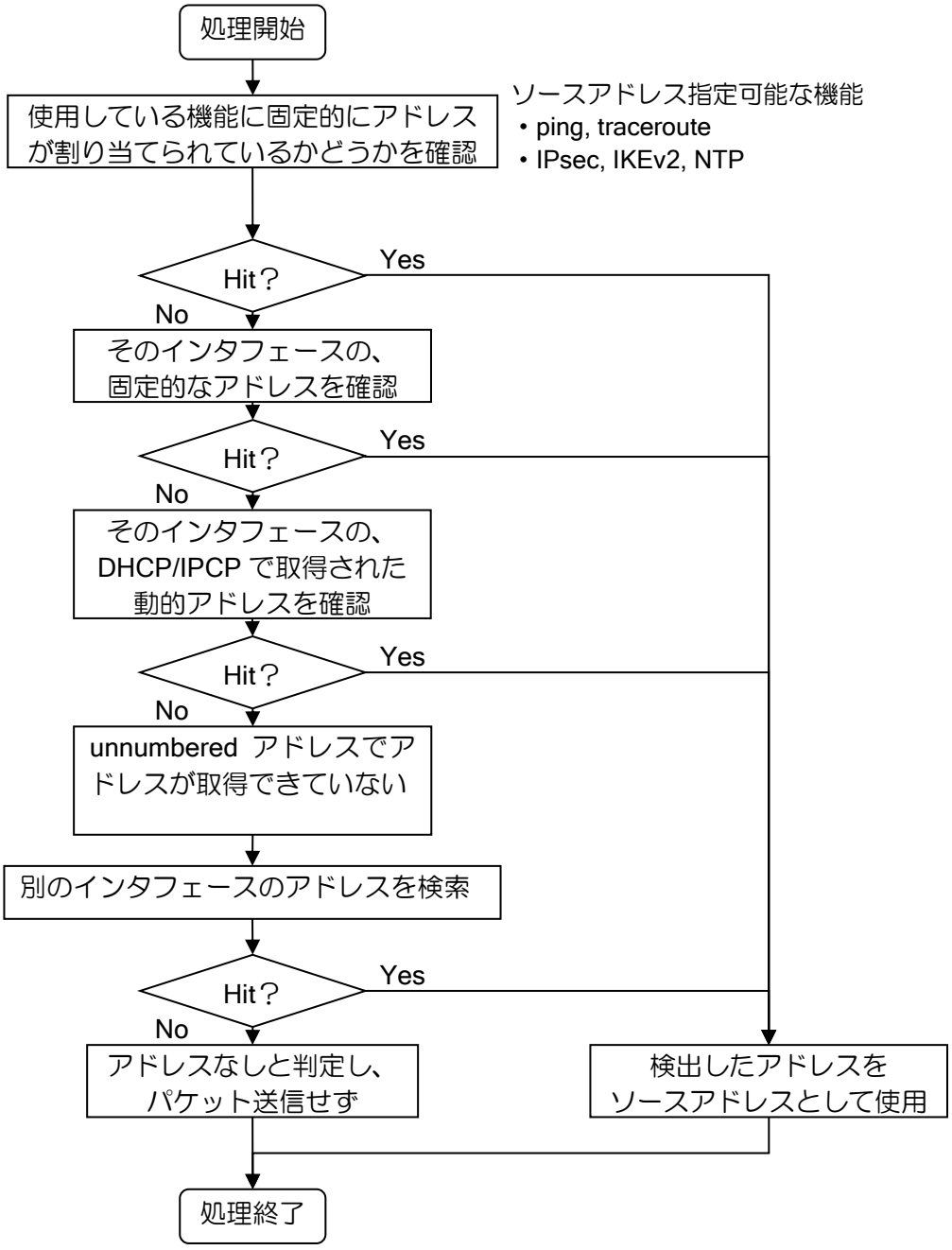
RFC / Internet Draft	備考
RFC1305 Network Time Protocol (Version 3) Specification, Implementation and Analysis	参照

■6.2 ソースアドレスセレクション

UNIVERGE IX-V 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。

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（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

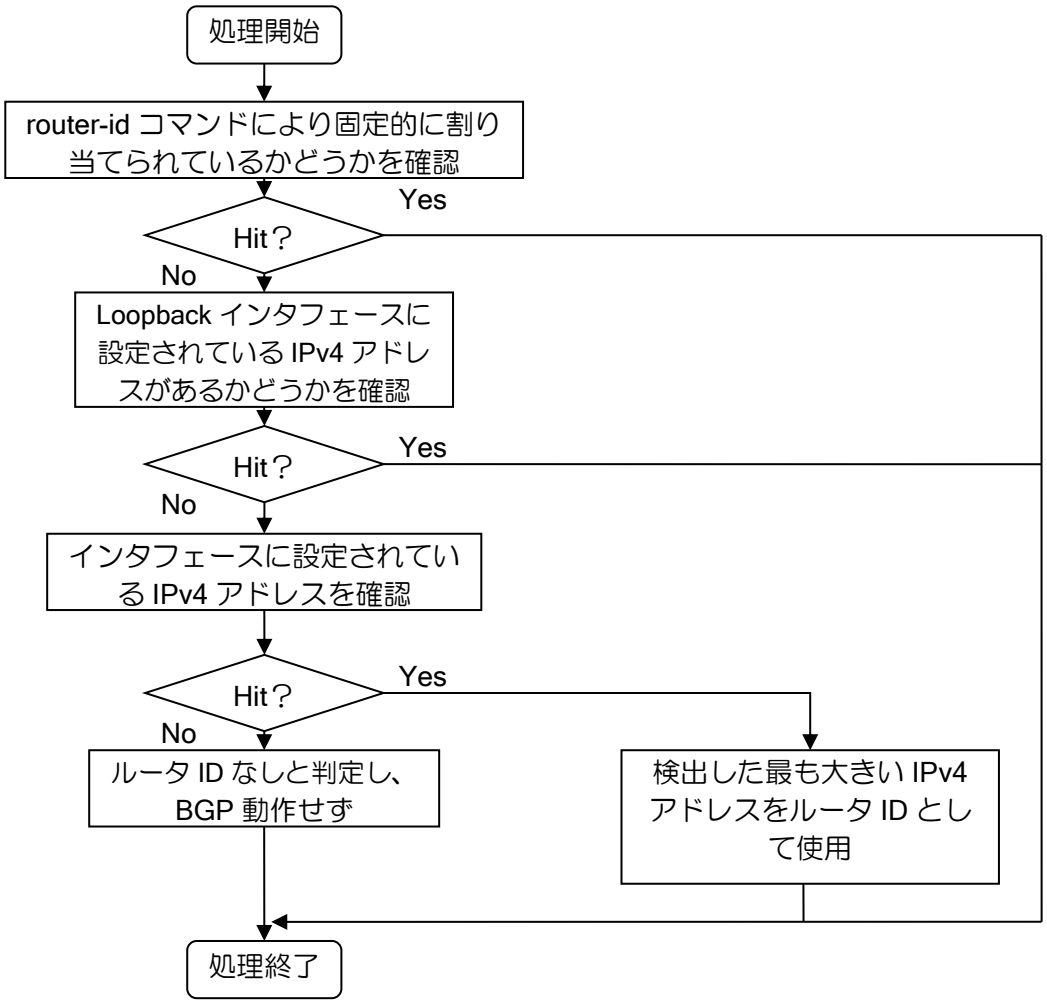
  ※インタフェース指定したインタフェースのセカンダリアドレスは優先されません。
  ※NAPT アドレスの場合には、指定インタフェースの検索のみ行います。

■6.3 ルータ ID セレクション

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) BGP4

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。



UNIVERGE IX-V シリーズ機能説明書

GYS-085944-001-00

2023 年　04 月　ver1.0 （第 1.0 版）　発行

発行元　日本電気株式会社