

# Fujitsu Network Si-R Si-R Gシリーズ

コマンド設定事例集 V3

# はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。  
インターネットやLANをさらに活用するために、本装置をご利用ください。

2015年8月初版

2016年7月第2版

2023年5月第3版

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。  
従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。  
Microsoft Corporationのガイドラインに従って画面写真を使用しています。  
Copyright Fujitsu Limited 2015 - 2023

# 目次

はじめに .....	2
本書の構成と使いかた .....	7
本書の読者と前提知識 .....	7
本書の構成 .....	7
本書における商標の表記について .....	8
本装置のマニュアルの構成 .....	9
<b>第 1 章 導入例 .....</b>	<b>10</b>
1.1 プライベート LAN を構築する .....	11
1.2 CATV インターネットに接続する .....	13
1.3 LAN をネットワーク間接続する .....	16
1.4 IPv4 のネットワークに IPv6 ネットワークを追加する .....	19
1.5 インターネットへ PPPoE で接続する .....	20
1.6 インターネットへデータ通信モジュールを使用して接続する .....	22
1.6.1 データ通信モジュール (wan コマンド) で接続する .....	22
1.6.2 データ通信モジュール (pseudo-ether コマンド) で接続する .....	25
1.7 複数の事業所 LAN を IP-VPN 網を利用して接続する .....	27
1.7.1 ADSL モデムを使用して IP-VPN 網と接続する .....	28
1.8 複数の事業所 LAN を VPN (IPsec) で接続する .....	33
1.8.1 NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換) .....	33
1.8.2 NAT と併用した固定 IP アドレスでの VPN (自動鍵交換) .....	40
1.8.3 NAT と併用した可変 IP アドレスでの VPN (自動鍵交換) .....	46
1.9 IPv6 の事業所 LAN を IPv4 トンネルで接続する .....	52
<b>第 2 章 活用例 .....</b>	<b>56</b>
2.1 RIP の経路を制御する (IPv4) .....	60
2.1.1 特定の経路情報の送信を許可する .....	62
2.1.2 特定の経路情報のメトリック値を変更して送信する .....	63
2.1.3 特定の経路情報の受信を許可する .....	64
2.1.4 特定の経路情報のメトリック値を変更して受信する .....	65
2.1.5 特定の経路情報の送信を禁止する .....	67
2.1.6 特定の経路情報の受信を禁止する .....	68
2.2 RIP の経路を制御する (IPv6) .....	69
2.2.1 特定の経路情報の送信を許可する .....	71
2.2.2 特定の経路情報のメトリック値を変更して送信する .....	72
2.2.3 特定の経路情報の受信を許可する .....	73
2.2.4 特定の経路情報のメトリック値を変更して受信する .....	74
2.2.5 特定の経路情報の送信を禁止する .....	76
2.2.6 特定の経路情報の受信を禁止する .....	77
2.3 OSPFv2 を使用したネットワークを構築する (IPv4) .....	78
2.3.1 スタブエリアを使う .....	82
2.4 OSPF の経路を制御する (IPv4) .....	85
2.4.1 OSPF ネットワークでエリアの経路情報 (LSA) を集約する .....	85
2.4.2 AS 外部経路を集約して OSPF ネットワークに広報する .....	87
2.4.3 エリア境界ルータで不要な経路情報 (LSA) を遮断する .....	88

2.5	OSPF 機能を使う (IPv6)	90
2.5.1	OSPF ネットワークを構築する	90
2.5.2	エリア境界ルータでエリア内部経路を集約する	93
2.5.3	エリア境界ルータで不要な経路情報を遮断する	94
2.6	BGP の経路を制御する (IPv4)	95
2.6.1	特定の経路情報の受信を透過させる	95
2.6.2	特定の AS からの経路情報の受信を遮断する	97
2.6.3	IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する	98
2.6.4	冗長構成の通信経路を使用する	99
2.7	BGP 機能を使う (IPv6)	101
2.7.1	BGP で IPv6 経路情報を交換する	101
2.7.2	特定の経路情報の受信を透過させる	103
2.7.3	特定の AS からの経路情報の受信を遮断する	104
2.7.4	特定の AS から受信した経路情報の送信を遮断する	105
2.7.5	冗長構成の通信経路を使用する	106
2.8	マルチキャスト機能を使う	108
2.8.1	マルチキャスト機能 (PIM-DM) を使う	108
2.8.2	マルチキャスト機能 (PIM-SM) を使う	112
2.8.3	マルチキャスト機能 (スタティックルーティング) を使う	118
2.9	VLAN 機能を使う	121
2.9.1	ポート VLAN 機能を使う	121
2.9.2	タグ VLAN 機能を使う	122
2.10	バックアップポート機能を使う	123
2.11	STP 機能を使う	124
2.11.1	STP を使う	124
2.12	IP フィルタリング機能を使う	125
2.12.1	外部の特定サービスへのアクセスだけを許可する	129
2.12.2	外部から特定サーバへのアクセスだけを許可する	133
2.12.3	外部から特定サーバへのアクセスだけを許可して SPI を併用する	137
2.12.4	外部の特定サービスへのアクセスだけを許可する (IPv6 フィルタリング)	141
2.12.5	外部の特定サーバへのアクセスだけを禁止する	145
2.12.6	利用者が意図しない発信を防ぐ	147
2.12.7	回線が接続しているときだけを許可する	149
2.12.8	外部から特定サーバへの ping だけを禁止する	150
2.13	IPsec 機能を使う	152
2.13.1	IPv4 over IPv4 で固定 IP アドレスでの VPN (手動鍵交換)	159
2.13.2	IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)	163
2.13.3	IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)	167
2.13.4	IPv6 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換)	171
2.13.5	IPv6 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)	175
2.13.6	IPv4 over IPv4 で 1 つの IKE セッションに複数の IPsec トンネル構成での VPN (自動鍵交換)	179
2.13.7	IPsec 機能と他機能との併用	183
2.13.8	テンプレート着信機能 (AAA 認証) を使用した固定 IP アドレスでの VPN	188
2.13.9	テンプレート着信機能 (AAA 認証) を使用した可変 IP アドレスでの VPN	192
2.13.10	テンプレート着信機能 (RADIUS 認証) を使用した固定 IP アドレスでの VPN	197
2.13.11	テンプレート着信機能 (RADIUS 認証) を使用した可変 IP アドレスでの VPN	202
2.13.12	テンプレート着信機能 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	208
2.13.13	テンプレート着信機能 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN (冗長構成)	217
2.13.14	テンプレート着信機能 (動的 VPN) を使用した IPv6 over IPv6 で固定 IP アドレスでの VPN	220
2.13.15	NAT トラバーサルを使用した可変 IP アドレスでの VPN	230



2.13.16	テンプレート着信機能 (AAA 認証) および NAT トラバーサルを使用した可変 IP アドレスでの VPN	234
2.13.17	接続先情報 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	238
2.13.18	RSA デジタル署名認証を使用した固定 IP アドレスでの VPN (自動鍵交換)	249
2.13.19	RSA デジタル署名認証を使用した可変 IP アドレスでの VPN (自動鍵交換)	253
2.13.20	RSA デジタル署名認証で接続先情報 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	257
2.13.21	IPv4 over IPv4 で NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	270
2.13.22	IPv4 over IPv4 で NAT と併用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	274
2.13.23	IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	278
2.13.24	IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	281
2.13.25	IPv6 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	284
2.13.26	IPv6 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	287
2.13.27	IPv4 over IPv4 で 1 つの IKE セッションに複数の IPsec トンネル構成での VPN (自動鍵交換 IKE Version2)	290
2.13.28	NAT トラバーサルを使用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	293
2.13.29	RSA デジタル署名認証を使用した固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	296
2.13.30	RSA デジタル署名認証を使用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	299
2.13.31	EAP 認証を使用した固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	302
2.14	システムログを採取する	305
2.15	マルチ NAT 機能 (アドレス変換機能) を使う	307
2.15.1	プライベート LAN 接続でサーバを公開する	308
2.15.2	PPPoE 接続でサーバを公開する	309
2.15.3	ネットワーク型接続でサーバを公開する	311
2.15.4	サーバ以外のアドレス変換をしないで、プライベート LAN 接続でサーバを公開する	313
2.15.5	複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する	314
2.15.6	NAT あて先変換で双方向のアドレスを変換する	315
2.16	VoIP NAT トラバーサル機能を使う	316
2.17	TOS/Traffic Class 値書き換え機能を使う	318
2.18	VLAN プライオリティマッピング機能を使う	320
2.19	シェーピング機能を使う	322
2.19.1	特定のインタフェースでシェーピング機能を使う	322
2.19.2	送信先ごとにシェーピング機能を使う	323
2.19.3	特定のポートでシェーピング機能を使う	325
2.20	ヘッダ圧縮機能を使う	326
2.21	帯域制御 (WFQ) 機能を使う	327
2.21.1	特定のインタフェースで帯域制御 (WFQ) 機能を使う	327
2.21.2	特定のポートで帯域制御 (WFQ) 機能を使う	329
2.22	DHCP 機能を使う	330
2.22.1	DHCP サーバ機能を使う	331
2.22.2	DHCP スタティック機能を使う	333
2.22.3	DHCP クライアント機能を使う	335
2.22.4	DHCP リレーエージェント機能を使う	337
2.22.5	IPv6 DHCP クライアント機能を使う	341
2.22.6	IPv6 DHCP サーバ機能を使う	343
2.22.7	IPv6 DHCP リレーエージェント機能を使う	345
2.22.8	IPv6 DHCP クライアント機能で取得した情報を IPv6 DHCP サーバ機能で配布する	347
2.22.9	通信事業者からの RA 情報と連携して IPv6 DHCP クライアント機能を使用する	349

2.23	DNS サーバ機能を使う (ProxyDNS)	352
2.23.1	DNS サーバの自動切り替え機能 (順引き) を使う	352
2.23.2	DNS サーバの自動切り替え機能 (逆引き) を使う	354
2.23.3	DNS サーバアドレスの自動取得機能を使う	355
2.23.4	DNS サーバアドレスを DHCP サーバから取得して使う	357
2.23.5	DNS 問い合わせタイプフィルタ機能を使う	359
2.23.6	DNS サーバ機能を使う	360
2.24	特定の URL へのアクセスを禁止する (URL フィルタ機能)	361
2.25	SNMP エージェント機能を使う	363
2.26	ECMP 機能を使う	366
2.27	VRRP 機能を使う	371
2.27.1	簡易ホットスタンバイ機能を使う	372
2.27.2	クラスタリング機能を使う	375
2.28	ポリシールーティング機能を使う	378
2.28.1	Ingress ポリシールーティング機能を使う	378
2.28.2	マルチルーティング機能を使う	380
2.29	クラウドサービスゲートウェイ機能を使う	381
2.29.1	ドメイン名をドメインリストで設定する	383
2.29.2	ドメイン名を構成定義に設定する方法	385
2.30	遠隔地のパソコンを起動させる (リモートパワーオン機能)	386
2.30.1	リモートパワーオン情報を設定する	387
2.30.2	リモートパワーオン機能を使う	387
2.31	スケジュール機能を使う	388
2.31.1	スケジュールを予約する	388
2.31.2	電話番号変更を予約する	390
2.31.3	構成定義情報の切り替えを予約する	390
2.32	ブリッジグループ機能を使う	391
2.32.1	異なる VLAN をグルーピングする	392
2.32.2	IP トンネルで事業所間をブリッジ接続する (Ethernet over IP ブリッジ)	393
2.33	透過モードを使う	398
2.33.1	ブリッジグループ機能と併用する	398
2.34	データ通信モジュールで通信バックアップをする	402
2.35	アプリケーションフィルタ機能を使う	406
2.36	IEEE802.1X 認証機能を使う	408
2.37	不正端末アクセス防止機能 (MAC アドレス認証) を使う	410
2.38	ARP 認証機能を使う	412
2.39	PKI 機能を使う	413
2.39.1	装置に証明書を登録する (自装置証明書を認証局 (CA) で発行する)	413
2.39.2	装置に証明書を登録する (自装置証明書を自己発行する)	417
2.39.3	認証局証明書を設定する	421
2.40	トラッキング機能を使う	423
2.41	装置を保護する	425
2.41.1	設定例	425
<b>索引</b>		<b>427</b>

# 本書の構成と使いかた

本書では、ネットワークを構築するために、代表的な接続形態や本装置の機能を活用した接続形態について説明しています。

## 本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。

本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。






## 本書の構成

以下に、本書の構成と各章の内容を示します。

章タイトル	内容
第1章 導入例	この章では、本装置の代表的な接続形態を紹介します。
第2章 活用例	この章では、本装置の便利な機能の活用方法について説明します。

## マークについて


本書で使用しているマーク類は、以下のような内容を表しています。

-  **ヒント** 本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。
- こんな事に気をつけて
  -  **補足** 操作手順で説明しているもののほかに、補足情報を説明しています。
  -  **参照** 操作方法など関連事項を説明している箇所を示します。
  -  **警告** 製造物責任法（PL）関連の警告事項を表しています。本装置をお使いの際は必ず守ってください。
  -  **注意** 製造物責任法（PL）関連の注意事項を表しています。本装置をお使いの際は必ず守ってください。

## 設定例の記述について

コマンド例では configure コマンドを実行して、構成定義モードに入ったあとのコマンドを記述しています。

また、プロンプトは設定や機種によって変化するため、“#”に統一しています。

-  **参照** マニュアル「コマンドユーザズガイド」

## 本書における商標の表記について

Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

## 製品名の略称について

---

本書で使用している製品名は、以下のように略して表記します。

製品名称	本文中の表記
Microsoft® Windows® 7 64bit Home Premium	Windows 7 または Windows
Microsoft® Windows® 7 32bit Professional	

## 本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
Si-R G110 ご利用にあたって	Si-R G110の設置方法やソフトウェアのインストール方法を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンドリファレンス	構成定義コマンド、運用管理コマンド、およびその他のコマンドの項目やパラメタの詳細な情報を説明しています。
コマンド設定事例集 (本書)	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード/ソフトウェア仕様とMIB/Trap一覧を説明しています。
Si-R 効率化運用ツール使用手引書	Si-R 効率化運用ツールを使用する方法を説明しています。

# 第1章 導入例



この章では、本装置の代表的な接続形態を紹介します。

1.1	プライベートLANを構築する	11
1.2	CATVインターネットに接続する	13
1.3	LANをネットワーク間接続する	16
1.4	IPv4のネットワークにIPv6ネットワークを追加する	19
1.5	インターネットへPPPoEで接続する	20
1.6	インターネットへデータ通信モジュールを使用して接続する	22
1.6.1	データ通信モジュール (wan コマンド) で接続する	22
1.6.2	データ通信モジュール (pseudo-ether コマンド) で接続する	25
1.7	複数の事業所LANをIP-VPN網を利用して接続する	27
1.7.1	ADSL モデムを使用してIP-VPN網と接続する	28
1.8	複数の事業所LANをVPN (IPsec) で接続する	33
1.8.1	NATと併用しない固定IPアドレスでのVPN (自動鍵交換)	33
1.8.2	NATと併用した固定IPアドレスでのVPN (自動鍵交換)	40
1.8.3	NATと併用した可変IPアドレスでのVPN (自動鍵交換)	46
1.9	IPv6の事業所LANをIPv4トンネルで接続する	52

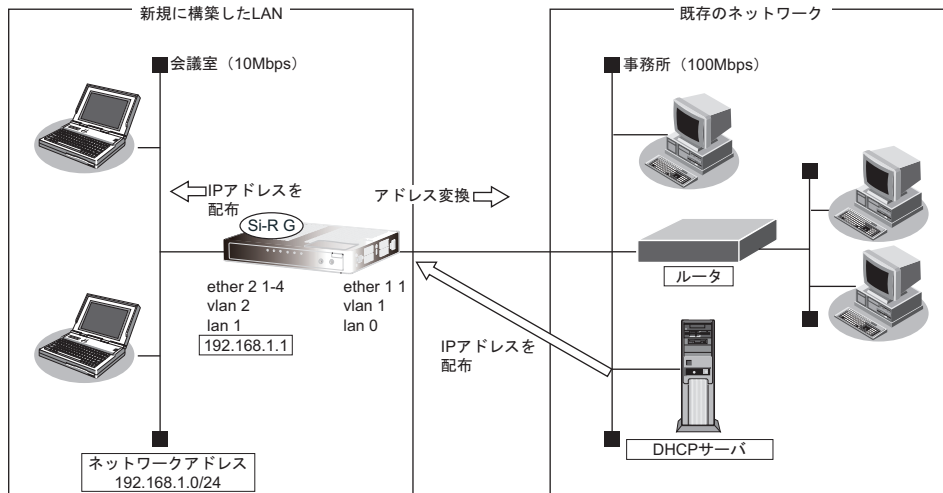
# 1.1 プライベート LAN を構築する

ここでは、以下の条件で会議室 LAN を一時的に構築し、事務所ネットワークと接続する場合を例に説明します。

## こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおり設定しても通信できないことがあります。

☞ 参照 マニュアル「トラブルシューティング」



## ● 設定条件

### [事務所側 LAN]

- ETHER ポート : グループ 1 ポート 1
- VLAN 番号 : 1
- lan 定義番号 : 0
- 転送レート : 自動認識
- IP アドレス : DHCP サーバから自動的に取得
- マルチ NAT を使用する  
グローバルアドレス : 事務所側の DHCP サーバから割り当てられた IP アドレスを使用する  
アドレス个数 : 1  
アドレス割当てタイム : 5分

### [会議室側 LAN]

- ETHER ポート : グループ 2 ポート 1～4
- VLAN 番号 : 2
- lan 定義番号 : 1
- 転送レート : 自動認識
- IP アドレス/ネットマスク : 192.168.1.1/24
- DHCP サーバ機能を使用する  
割当て先頭 IP アドレス : 192.168.1.2  
割当てアドレス数 : 253  
リース期間 : 1日  
デフォルトルータ広報 : 192.168.1.1

### こんな事に気をつけて

- コマンド入力時は、半角文字 (0～9、A～Z、a～z、および記号) だけを使用してください。ただし、空白文字、[ ]、[ < ]、[ > ]、[ & ]、[ % ] は入力しないでください。
  - ☞ 参照 マニュアル「コマンドユーザーズガイド」
- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

## ● コマンド

事務所側の LAN 情報を設定する

```
# ether 1 1 vlan untag 1
```

```
# delete lan 0
```

```
# lan 0 ip dhcp service client
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1
# lan 0 vlan 1
```

会議室側の LAN 情報を設定する

```
# ether 2 1-4 vlan untag 2
```

```
# delete lan 1
```

```
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off
# lan 1 vlan 2
```

設定終了

```
# save
```

再起動

```
# reset
```

本装置の設定が終了したら、設定を有効にするためにパソコンのシステムを終了し、パソコンおよび本装置の電源を切断します。各装置を LAN ケーブルで正しく接続したあと、本装置、パソコンの順に電源を投入します。

### こんな事に気をつけて

本装置の DHCP サーバ機能を使用する場合は、以下の点に注意してください。

- 本装置の DHCP サーバ機能を利用する LAN 側のパソコンは、IP アドレスを自動的に取得する設定にしてください。固定の IP アドレスを設定していると、本装置が配布する IP アドレスと重なり、矛盾が生じる場合があります。
- パソコンに固定の IP アドレスを割り当てる場合は、[\[2.22.2 DHCP スタティック機能を使う\]](#) (P.333) を参考にし、IP アドレスと MAC アドレスを設定してください。



## 1.2 CATVインターネットに接続する

CATVインターネット接続とは、CATV事業者が提供するインターネット接続サービスです。CATVインターネット接続には、ケーブルモデム接続とダイヤルアップ接続の2つの接続形態があります。ケーブルモデム接続は、ケーブルテレビ網を利用したもので、CATV事業者が提供するケーブルモデムに接続する形態です。ダイヤルアップ接続とは、CATV電話サービスを利用したもので、パソコンにモデムを接続する形態です。本装置を使用してCATVインターネット接続する場合は、「ケーブルモデム接続」の形態となり、CATV事業者との契約が必要です。接続にあたっては、CATV事業者の指示に従ってください。

### 💡 ヒント

#### ◆ ケーブルモデムとは？

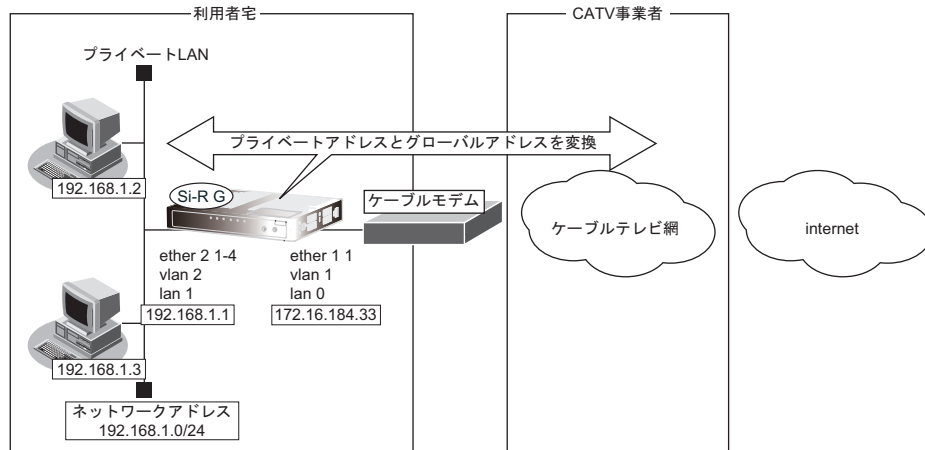
ケーブルテレビ網に接続するための専用モデムで、CATVインターネット接続サービスに必要な機器です。パソコン（LANボード）とはLANケーブルで接続します。通常、CATVサービス加入時にCATV事業者より貸し出され、宅内工事の際に設置されます。

本装置を使ったCATVインターネット接続は、CATV事業者が提供するインターネット接続サービスをプライベートLAN上の複数のパソコンから利用するための接続形態です。本装置とCATV事業者が提供するケーブルモデムを接続することで、プライベートLAN上のパソコンからインターネット接続サービスを利用できます。本装置のアドレス変換機能がCATV事業者側のネットワークと利用者側のプライベートLANとの間で動作し、プライベートLAN側のIPアドレスを外部から隠すため、セキュリティが確保できます。

### こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおり設定しても通信できないことがあります。

☛ 参照 マニュアル「トラブルシューティング」



## ● 設定条件

### [CATV事業者側]

- ETHER ポート : グループ 1 ポート 1
- VLAN 番号 : 1
- lan 定義番号 : 0
- IP アドレス : 172.16.184.33
- ネットワークアドレス/ネットマスク : 172.16.184.0/24
- デフォルトルータ : 172.16.184.100
- DNS サーバ : 192.10.10.10

### [プライベートLAN側]

- ETHER ポート : グループ 2 ポート 1~4
- VLAN 番号 : 2
- lan 定義番号 : 1
- IP アドレス : 192.168.1.1
- ネットワークアドレス/ネットマスク : 192.168.1.0/24
- DHCP サーバ機能を使用する

### こんな事に気をつけて

- 契約したCATV事業者によって設定方法が異なります。実際の設定は、CATV事業者の指示に従ってください。
- 本装置のIPアドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

## ● コマンド

```

CATV事業者側を設定する
# ether 1 1 vlan untag 1

# delete lan

# lan 0 ip address 172.16.184.33/24 3
# lan 0 ip dhcp info time 1d
# lan 0 ip route 0 default 172.16.184.100 1 1
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1 5m
# lan 0 vlan 1

プライベートLAN側を設定する
# ether 2 1-4 vlan untag 2

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.10.10.10
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off
# lan 1 vlan 2

```

ProxyDNS を設定する

```
# proxydns domain 0 any * any static 192.10.10.10
```

```
# proxydns address 0 any static 192.10.10.10
```

設定終了

```
# save
```

再起動

```
# reset
```

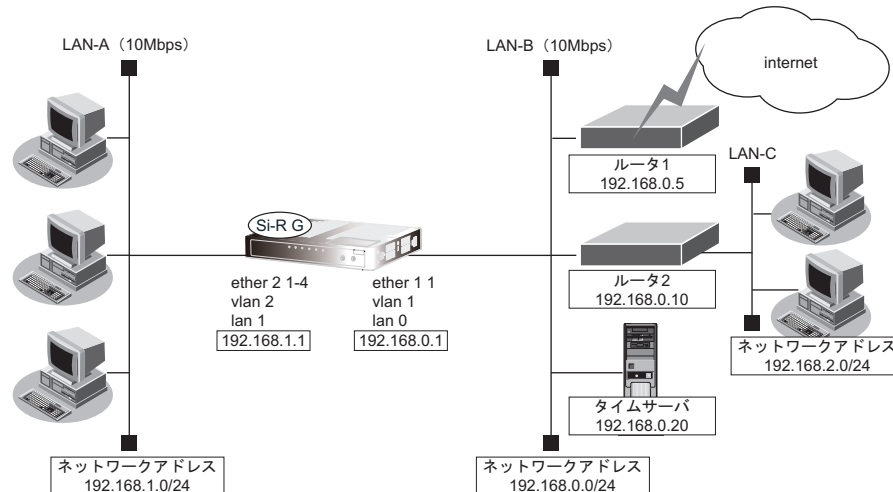
# 1.3 LANをネットワーク間接続する

ここでは、既存のLAN-Bに新規のLAN-Aをネットワーク間接続し、静的に経路情報を設定する場合を例に説明します。

## こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおり設定しても通信できないことがあります。

☞ 参照 マニュアル「トラブルシューティング」



## ● 設定条件

### [LAN-A側]

- ETHER ポート : グループ2 ポート1～4
- VLAN 番号 : 2
- lan 定義番号 : 1
- 本装置のIPアドレス : 192.168.1.1
- ネットワークアドレス/マスク : 192.168.1.0/24
- DHCP 機能 : DHCP サーバ機能を使用する
  - 貸出IPアドレス先頭 : 192.168.1.2
  - 貸出IPアドレス個数 : 253個
  - 貸出IPアドレス有効期限 : 1日
- NAT 機能 : 使用しない
- 経路情報通知 : RIP V1 を使用する

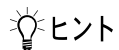
### [LAN-B側]

- ETHER ポート : グループ1 ポート1
- VLAN 番号 : 1
- lan 定義番号 : 0
- 本装置のIPアドレス : 192.168.0.1
- ネットワークマスク : 255.255.255.0
- DHCP 機能 : 使用しない

- NAT 機能 : 使用しない
- ルータ 1 の接続先 : インターネット
- ルータ 1 の IP アドレス : 192.168.0.5
- ルータ 2 の接続先 : LAN-C (事業所内サブネットワーク)
- ルータ 2 の IP アドレス : 192.168.0.10
- LAN-C のネットワークアドレス / マスク : 192.168.2.0/24
- 経路情報通知 : RIP V1 を使用する
- 静的経路情報
  - LAN-C あて : ルータ 2 へ
  - その他すべて (デフォルト) : ルータ 1 へ

**[その他の条件]**

- 自動時刻設定にする
  - タイムサーバ : 使用する
  - サーバ設定 : 設定する
  - プロトコル : TIME プロトコル
  - タイムサーバのアドレス : 192.168.0.20



**◆ TIME プロトコル、SNTP とは？**

TIME プロトコル (RFC868) はネットワーク上で時刻情報を配布するプロトコルです。SNTP (Simple Network Time Protocol、RFC1361、RFC1769) は NTP (Network Time Protocol) のサブセットで、パソコンなど末端のクライアントマシンの時刻を同期させるのに適しています。

**こんな事に気をつけて**

本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。

**● コマンド**

```

LAN-B 側情報を設定する
# ether 1 1 vlan untag 1

# delete lan 0

# lan 0 ip address 192.168.0.1/24 3
# lan 0 ip dhcp service off
# lan 0 ip route 0 192.168.2.0/24 192.168.0.10 1 1
# lan 0 ip route 1 default 192.168.0.5 1 1
# lan 0 ip rip use v1 v1 0 off
# lan 0 vlan 1

LAN-A 側情報を設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off
    
```

```
# lan 1 vlan 2
```

```
自動時刻を設定する
```

```
# time auto server 192.168.0.20 time
```

```
# time auto interval start
```

```
ProxyDNS を設定する
```

```
# proxydns domain 0 any * any static 192.168.0.30
```

```
# proxydns address 0 any static 192.168.0.30
```

```
設定終了
```

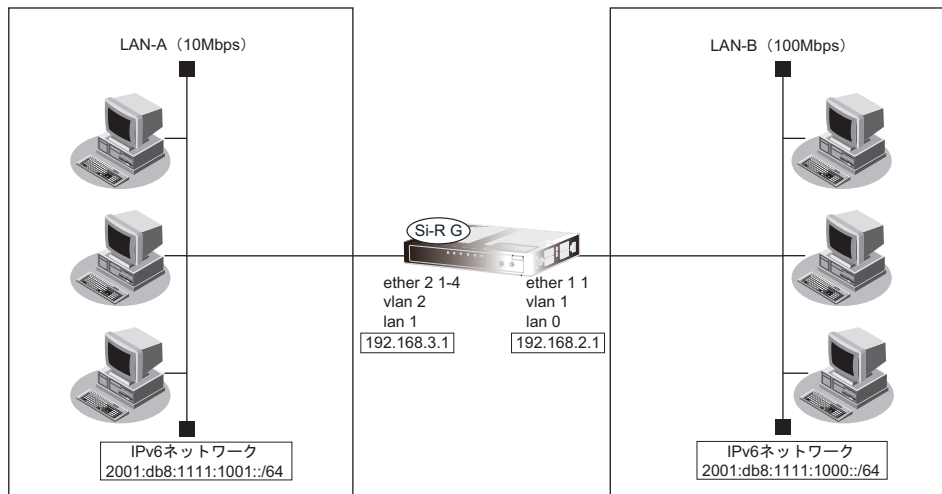
```
# save
```

```
再起動
```

```
# reset
```

# 1.4 IPv4 のネットワークに IPv6 ネットワークを追加する

ここでは、IPv4 で通信しているネットワーク環境に IPv6 通信設定を追加する例について説明します。



## ● 設定条件

### [LAN-A 側]

- ETHER ポート : グループ 2 ポート 1～4
- VLAN 番号 : 2
- lan 定義番号 : 1
- プレフィックス/プレフィックス長 : 2001:db8:1111:1001::/64

### [LAN-B 側]

- ETHER ポート : グループ 1 ポート 1
- VLAN 番号 : 1
- lan 定義番号 : 0
- プレフィックス/プレフィックス長 : 2001:db8:1111:1000::/64

## ● コマンド

```
LAN-B 側情報を設定する
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:1000::/64
# lan 0 ipv6 ra mode send
# lan 0 ipv6 rip use on on 0
# lan 0 ipv6 rip site-local on
```

```
LAN-A 側情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:1001::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 2001:db8:1111:1001::/64 30d 7d 0
# lan 1 ipv6 rip use on on 0
# lan 1 ipv6 rip site-local on
```

```
設定終了
# save
# commit
```

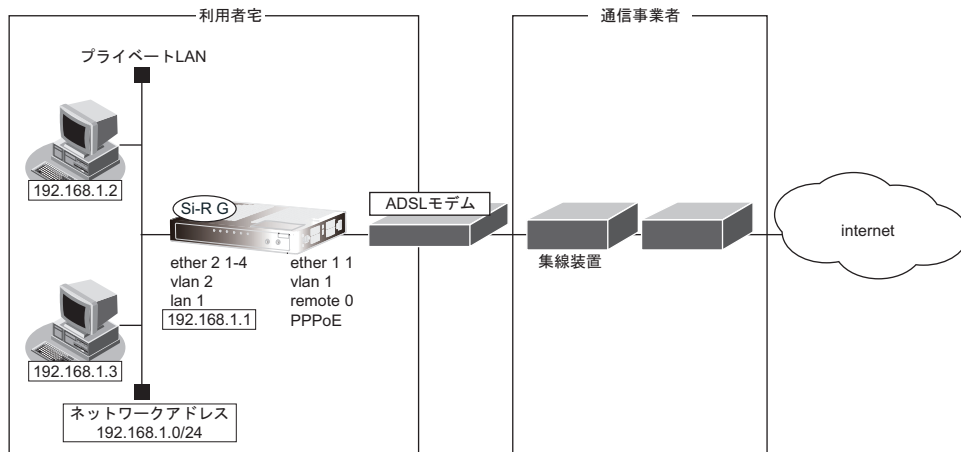
## 1.5 インターネットへ PPPoE で接続する

ここでは、PPPoE 接続を使ってフレッツ・ADSL などのサービスを利用し、インターネットへ接続する場合を例に説明します。

### こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☞ 参照 マニュアル「トラブルシューティング」



### ● 設定条件

#### [通信事業者側]

- ETHER ポート : グループ 1 ポート 1
- VLAN 番号 : 1
- ユーザ認証 ID : userid (プロバイダから提示された内容)
- ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- ETHER ポート : グループ 1 ポート 1

#### [プライベートLAN側]

- ETHER ポート : グループ 2 ポート 1～4
- VLAN 番号 : 2
- lan 定義番号 : 1
- 本装置の IP アドレス : 192.168.1.1
- ネットワークアドレス/ネットマスク : 192.168.1.0/24

### こんな事に気をつけて

- コマンド入力時は、半角文字 (0～9、A～Z、a～z、および記号) だけを使用してください。ただし、空白文字、「\*」、「<」、「>」、「&」、「%」は入力しないでください。

☞ 参照 マニュアル「コマンドユーザズガイド」

- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- PPPoE で利用する相手情報の MTU 値は、接続先から指定された MTU 値を設定します。一般的には、1454 を設定すれば問題ありません。



**● コマンド**

通信事業者側の ETHER ポートを設定する

```
# ether 1 1 vlan untag 1
```

プライベート LAN 側の ETHER ポートを設定する

```
# ether 2 1-4 vlan untag 2
```

LAN 情報を削除する

```
# delete lan
```

本装置の IP アドレスを設定する

```
# lan 1 ip address 192.168.1.1/24 3
```

```
# lan 1 vlan 2
```

DHCP サーバを設定する

```
# lan 1 ip dhcp info dns 192.168.1.1
```

```
# lan 1 ip dhcp info address 192.168.1.2/24 253
```

```
# lan 1 ip dhcp info time 1d
```

```
# lan 1 ip dhcp info gateway 192.168.1.1
```

```
# lan 1 ip dhcp service server
```

```
# lan 1 ip nat mode off
```

通信事業者との接続情報を設定する

```
# remote 0 name internet
```

```
# remote 0 mtu 1454
```

```
# remote 0 ppp ipcp vjcomp disable
```

```
# remote 0 ip route 0 default 1 1
```

```
# remote 0 ip rip use off off 0 off
```

```
# remote 0 ip nat mode multi any 1 5m
```

```
# remote 0 ip msschange 1414
```

```
# remote 0 ap 0 name ISP-1
```

```
# remote 0 ap 0 datalink bind vlan 1
```

```
# remote 0 ap 0 ppp auth send userid userpass
```

```
# remote 0 ap 0 keep connect
```

ProxyDNS を設定する

```
# proxydns domain 0 any * any to 0
```

```
# proxydns address 0 any to 0
```

設定終了

```
# save
```

再起動

```
# reset
```

## 1.6 インターネットヘデータ通信モジュールを使用して接続する

ここでは、データ通信モジュールを使用して、ご購入時の設定のままインターネットへ接続する場合を例に説明します。

### 1.6.1 データ通信モジュール (wan コマンド) で接続する

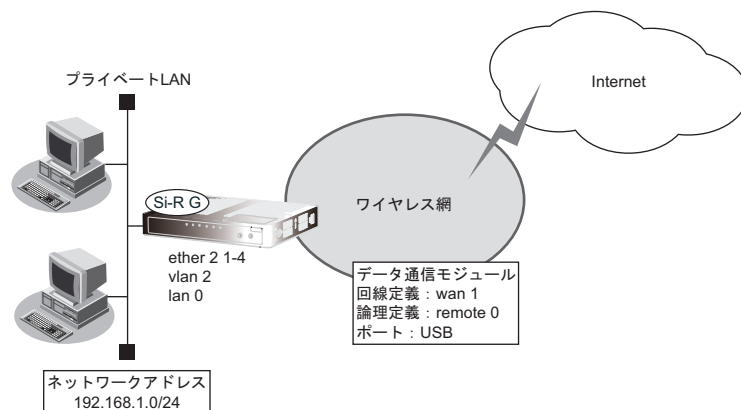
ここでは、データ通信モジュールを wan コマンドを使用して、ご購入時の設定のままインターネットへ接続する場合を例に説明します。

☞ 参照 対応データ通信モジュール (富士通ホームページ)  
<http://fenics.fujitsu.com/products/sir/sirg110/#supportcard>

#### こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかったり手順どおり設定しても通信できないことがあります。

☞ 参照 マニュアル「トラブルシューティング」



#### ● 設定条件

##### [Internet側]

- データ通信モジュール : USB
- 認証 ID : userid (通信事業者から提示された内容)
- 認証パスワード : userpass (通信事業者から提示された内容)
- 電話番号 : \*99\*\*\*1# (通信事業者から提示された内容)
- 無通信監視タイマ : 無通信監視時間を 1 分とする
- 強制切断 : 100000 パケット (128 バイト単位) を超えた場合に回線を切断し、以降自動発信を行わない

##### [プライベート LAN側]

- 利用するポート : ETHERグループ 2 ポート 1～4
- IPアドレス : 192.168.1.1
- ネットワークアドレス/マスク : 192.168.1.0/24

## こんな事に気をつけて

- コマンド入力時は、半角文字 (0～9、A～Z、a～z、および記号) だけを使用してください。ただし、空白文字、「」、「<」、「>」、「&」、「%」は入力しないでください。
- 参照 マニュアル「コマンドユーザズガイド」
- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- データ通信モジュール接続では、以下の機能は動作しません。
  - テンプレート機能
  - 常時接続機能
- データ通信モジュールで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- データ通信モジュールによる発信は従量課金が発生するため、データ通信モジュール接続のアカウント情報を監視して不要な接続が行われていないか、こまめに確認してください。また、異常課金を防止する場合は、強制切断を行う累計接続時間、累計パケット数を設定してください。
- 課金制御機能 (強制切断) による回線切断が発生した場合、以下のシステムログが出力されます。

protocol: [USB] forced disconnection <target> <reason>

■ 参照 マニュアル「メッセージ集」

課金制御機能 (強制切断) により切断した場合、以降の手動および自動発信を禁止します。

接続するにはデータ通信モジュールのアカウント情報のクリア (clear modemmodule account) を実行する必要があります。

- パケット数による強制切断のパケット数は、累計送受信バイト数 (PPP パケット長) を 128 で割った値を用います。パケット数による強制切断のパケット数は目安であり、通信事業者でのパケット数と異なる場合があります。

## ● 設定コマンド

ETHER グループ 2 のポート 1～4 を設定する

```
# ether 2 1-4 vlan untag 10
```

IP アドレスを設定する

```
# delete lan
```

```
# lan 0 ip address 192.168.1.1/24 3
```

```
# lan 0 vlan 10
```

DHCP サーバを設定する

```
# lan 0 ip dhcp info dns 192.168.1.1
```

```
# lan 0 ip dhcp info address 192.168.1.2/24 253
```

```
# lan 0 ip dhcp info time 1d
```

```
# lan 0 ip dhcp info gateway 192.168.1.1
```

```
# lan 0 ip dhcp service server
```

回線情報を設定する

```
# wan 1 use on
```

```
# wan 1 bind usb
```

```
# wan 1 line modemmodule
```

```
# wan 1 description L-03F
```

接続先の情報を設定する

```
# remote 0 description internet
```

```
# remote 0 ppp ipcp vjcomp disable
```

```
# remote 0 ip route 0 default 1 1
```

```
# remote 0 ip nat mode multi any 1 5m
```

```
# remote 0 ap 0 description ISP-1
```

```
# remote 0 ap 0 datalink bind wan 1
```

```
# remote 0 ap 0 ppp auth send userid userpass
```

```
# remote 0 ap 0 dial 0 number *99***1#
```

```
# remote 0 ap 0 idle 1m
```

強制切断を行う累計パケット数を設定する

```
# remote 0 ap 0 disconnect packet 100000 per128
```

```
ProxyDNS を設定する
# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0
```

```
設定終了
# save
# commit
```



各通信事業者の認証 ID、認証パスワード、電話番号を以下に示します。

詳細については、各通信事業者にお問い合わせください。

通信事業者	認証 ID	認証パスワード	電話番号
NTT ドコモ mopera	(任意の文字列)	(任意の文字列)	*99***1#

## 1.6.2 データ通信モジュール (pseudo-ether コマンド) で接続する

ここでは、データ通信モジュールを pseudo-ether コマンドを使用して、ご購入時の設定のままインターネットへ接続する場合を例に説明します。

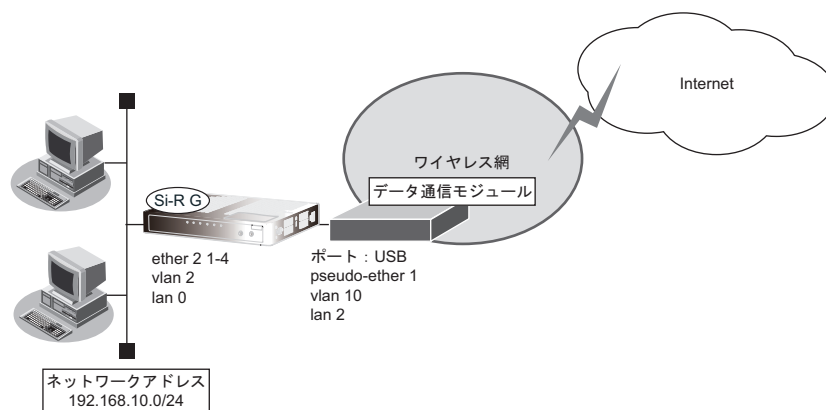
ルータタイプのデータ通信モジュールは、USB 上の ETHER ポート (pseudo-ether) で LAN 接続します。

☛ 参照 対応データ通信モジュール (富士通ホームページ)  
<http://fenics.fujitsu.com/products/sir/sirg110/#supportcard>

### こんな事に気をつけて

この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおり設定しても通信できないことがあります。

☛ 参照 マニュアル「トラブルシューティング」



### ● 設定条件

#### [Internet 側]

- データ通信モジュール : USB
- pseudo-ether : 1
- IP アドレス : DHCP クライアントで獲得する

#### [プライベート LAN 側]

- 利用するポート : ETHER グループ 2 ポート 1～4
- IP アドレス : 192.168.10.1
- ネットワークアドレス/マスク : 192.168.10.0/24

### こんな事に気をつけて

- コマンド入力時は、半角文字 (0～9、A～Z、a～z、および記号) だけを使用してください。ただし、空白文字、「!」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザズガイド」

- 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。
- データ通信モジュールから DHCP で割り当てられるネットワークアドレスがほかの lan アドレスと重複しないように設計してください。
- 本装置からデータ通信モジュール (pseudo-ether) を操作してワイヤレス網に接続・切断することはできません。データ通信モジュールの設定に従ってワイヤレス網に接続します。
- ワイヤレス網との接続が失われても pseudo-ether インタフェースはリンクアップしたままです。
- offline コマンドで pseudo-ether を閉塞してもワイヤレス網とは切断しません。

- pseudo-ether インタフェースでは、以下の機能は利用できません。
  - タグ VLAN 機能
  - バックアップポート機能
  - STP 機能
  - VLAN プライオリティマッピング機能
  - シェーピング機能
  - 優先制御 (WFQ) 機能
  - IEEE802.1X 認証機能
  - 不正端末アクセス防止機能 (MAC アドレス認証)
- pseudo-ether インタフェースに割り当てた LAN では、IPv6 機能は利用できません。
- データ通信モジュール (wan) 接続と比較して電波状態監視機能は利用できません。

## ● 設定コマンド

ETHER グループ 2 のポート 1～4 を設定する

```
# ether 2 1-4 vlan untag 2
```

プライベート LAN 側の IP アドレスを設定する

```
# delete lan  
# lan 0 ip address 192.168.10.1/24 3  
# lan 0 vlan 2
```

プライベート LAN 側の DHCP サーバを設定する

```
# lan 0 ip dhcp info dns 192.168.10.1  
# lan 0 ip dhcp info address 192.168.10.2/24 253  
# lan 0 ip dhcp info time 1d  
# lan 0 ip dhcp info gateway 192.168.10.1  
# lan 0 ip dhcp service server
```

Internet 側の ETHER ポート (pseudo-ether) を設定する

```
# pseudo-ether 1 description DATA_MODULE  
# pseudo-ether 1 use on  
# pseudo-ether 1 bind usb  
# pseudo-ether 1 vlan untag 10
```

Internet 側の LAN の DHCP クライアントを設定する

```
# lan 2 ip dhcp service client  
# lan 2 ip dhcp info time 1d  
# lan 2 ip nat mode multi any 1 5m  
# lan 2 vlan 10
```

ProxyDNS を設定する

```
# proxydns domain 0 any * any dhcp lan2  
# proxydns address 0 any dhcp lan2
```

設定終了

```
# save  
# reset
```

## 1.7 複数の事業所 LAN を IP-VPN 網を利用して接続する

ここでは、プロトコル BGP4 を使用して、IP-VPN 網で複数の事業所を接続する場合の設定方法を説明します。

### こんな事に気をつけて

- この例は、ご購入時の状態からの設定例です。以前の設定が残っていると、設定例の手順で設定できなかつたり手順どおり設定しても通信できないことがあります。

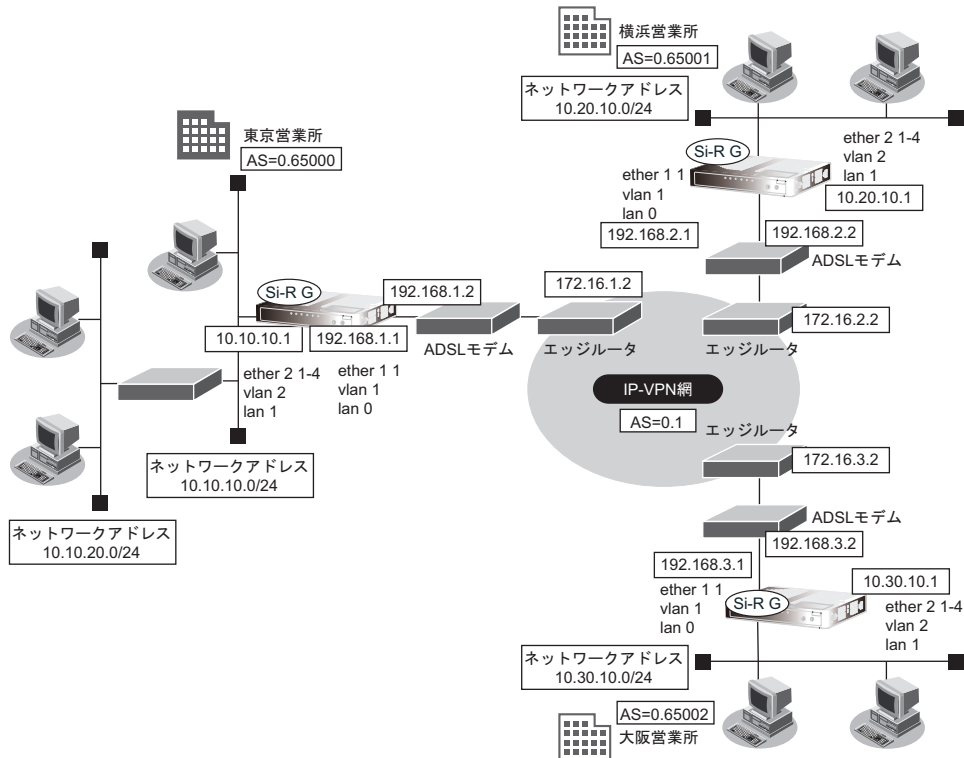
☛ 参照 マニュアル「トラブルシューティング」

- コマンド入力時は、半角文字 (0～9、A～Z、a～z、および記号) だけを使用してください。ただし、空白文字、「[」、[<]、[>]、[&]、[%] は入力しないでください。

☛ 参照 マニュアル「コマンドユーザズガイド」

- NAT 機能と併用することはできません。
- バージョン 4 だけをサポートしています。
- 本装置のグレースフルリスタート機能のサポート範囲は、以下のとおりです。
  - レシーブルータ機能のみ (リスタート機能は、サポートしていません。)
  - アドレスファミリーは IPv4 のみ
- 経路情報を最大値まで保持している状態では、受信した BGP パケットは破棄されます。破棄した BGP パケットの経路情報は、その後、経路情報に空きができた場合でも反映されません。
- BGP 使用中に commit コマンドを実行した場合、接続中のセッションが一度切断されることがあります。

## 1.7.1 ADSL モデムを使用して IP-VPN 網と接続する



### ● 設定条件

- 本装置のETHERグループ1ポート1とADSLモデムのLANポートをLANケーブルで接続する。

#### [IP-VPN 網]

- 東京営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。また、グレースフルリスタートを使用する。
- 横浜営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 大阪営業所との経路交換にBGPを使用し、IPv4ユニキャスト経路を交換する。グレースフルリスタートは使用しない。
- 東京営業所向けIPアドレス : 172.16.1.2
- 横浜営業所向けIPアドレス : 172.16.2.2
- 大阪営業所向けIPアドレス : 172.16.3.2
- AS番号 : 0.1

#### [東京営業所]

##### IP-VPN 網側

- ETHERポート : グループ1ポート1
- VLAN番号 : 1
- IPアドレス : 192.168.1.1
- ネットワークアドレス/マスク : 192.168.1.0/24



**東京営業所内**

- ETHER ポート : グループ2 ポート1～4
- VLAN 番号 : 2
- IP アドレス : 10.10.10.1
- ネットワークアドレス/マスク : 10.10.10.0/24
- ルーティングプロトコル : RIPv2

**BGP 情報**

- AS 番号 : 0.65000
- グレースフルリスタート : 使用する

**[横浜営業所]****IP-VPN 網側**

- ETHER ポート番号 : グループ1 ポート1
- VLAN 番号 : 1
- LAN 定義番号 : 0
- IP アドレス : 192.168.2.1
- ネットワークアドレス/ネットマスク : 192.168.2.0/24

**横浜営業所内**

- ETHER ポート番号 : グループ2 ポート1～4
- VLAN 番号 : 2
- LAN 定義番号 : 1
- IP アドレス : 10.20.10.1
- ネットワークアドレス/ネットマスク : 10.20.10.0/24

**BGP 情報**

- AS 番号 : 0.65001
- グレースフルリスタート : 使用しない

**[大阪営業所]****IP-VPN 網側**

- ETHER ポート番号 : グループ1 ポート1
- VLAN 番号 : 1
- LAN 定義番号 : 0
- IP アドレス : 192.168.3.1
- ネットワークアドレス/ネットマスク : 192.168.3.0/24

**大阪営業所内**

- ETHER ポート番号 : グループ2 ポート1～4
- VLAN 番号 : 2
- LAN 定義番号 : 1
- IP アドレス : 10.30.10.1
- ネットワークアドレス/ネットマスク : 10.30.10.0/24

**BGP 情報**

- AS 番号 : 0.65002
- グレースフルリスタート : 使用しない

## 東京営業所を設定する

### ● コマンド

```
IP-VPN 網側のインタフェースを設定する
# ether 1 1 vlan untag 1

# delete lan 0

# lan 0 ip address 192.168.1.1/24 3
# lan 0 ip route 0 172.16.1.0/24 192.168.1.2 1
# lan 0 vlan 1

東京営業所内のインタフェースを設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 10.10.10.1/24 3
# lan 1 ip rip use v2m v2 0 off
# lan 1 vlan 2

ルーティングプロトコル情報を設定する
# routemanage ip redist rip bgp on
# routemanage ip redist bgp rip on
# bgp as 0.65000
# bgp ip network route 0 10.10.10.0/24
# bgp neighbor 0 address 172.16.1.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2
# bgp neighbor 0 graceful-restart family ipv4

設定終了
# save
# commit
```

## 横浜営業所を設定する

### ● コマンド

```
IP-VPN 網側のインタフェースを設定する
# ether 1 1 vlan untag 1

# delete lan 0

# lan 0 ip address 192.168.2.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# lan 0 ip route 0 172.16.2.0/24 192.168.2.2 1
# lan 0 vlan 1

横浜営業所内のインタフェースを設定する
# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 10.20.10.1/24 3
# lan 1 vlan 2

ルーティングプロトコル情報を設定する
# bgp as 0.65001
# bgp ip network route 0 10.20.10.0/24
# bgp neighbor 0 address 172.16.2.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

## 大阪営業所を設定する

### ● コマンド

```
IP-VPN 網側のインタフェースを設定する
# ether 1 1 vlan untag 1

# lan 0 ip address 192.168.3.1/24 3
# lan 0 ip nat mode off
# lan 0 ip dhcp service off
# lan 0 ip route 0 172.16.3.0/24 192.168.3.2 1
# lan 0 vlan 1

大阪営業所内のインタフェースを設定する
# ether 2 1-4 vlan untag 2

# lan 1 ip address 10.30.10.1/24 3
# lan 1 vlan 2

ルーティングプロトコル情報を設定する
# bgp as 0.65002
# bgp ip network route 0 10.30.10.0/24
# bgp neighbor 0 address 172.16.3.2
# bgp neighbor 0 as 0.1
# bgp neighbor 0 ebgp-multihop 2

設定終了
# save
# commit
```

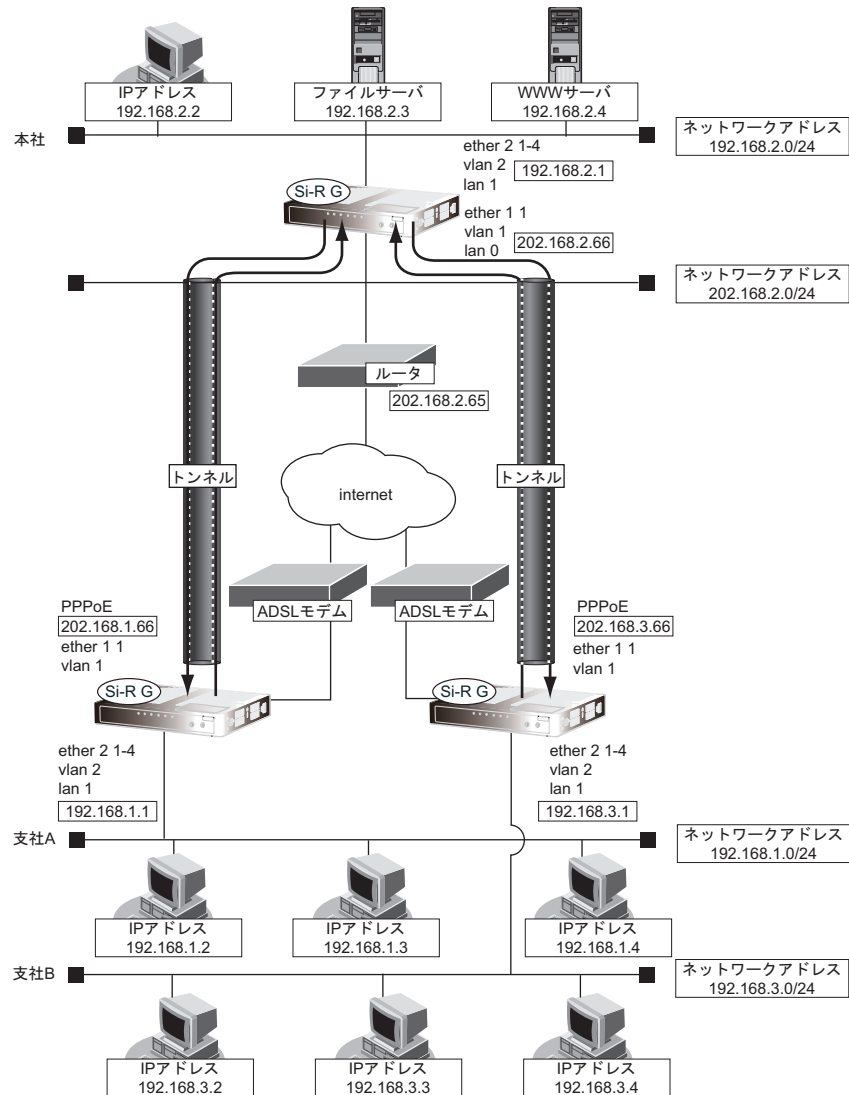
# 1.8 複数の事業所 LAN を VPN (IPsec) で接続する

ここでは、VPN (IPsec) で複数の事業所を接続する場合を例に説明します。

## 1.8.1 NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換)

IPsec 機能を使って自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。



## ● 前提条件

### [支社 A (PPPoE 常時接続)]

#### PPPoE 接続インターネット

- VLAN 番号 : 1
- lan 定義番号 : 0
- ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

#### 支社 A 内ローカルネットワーク

- ETHER ポート : グループ 2 ポート 1~4
- VLAN 番号 : 2
- lan 定義番号 : 1
- プライベート IP アドレス : 192.168.1.1/24
- グローバル IP アドレス : 202.168.1.66 (プロバイダから提示された内容)

### [支社 B (PPPoE 常時接続)]

#### PPPoE 接続インターネット

- VLAN 番号 : 1
- lan 定義番号 : 0
- ユーザ認証 ID : userid3 (プロバイダから提示された内容)
- ユーザ認証パスワード : userpass3 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

#### 支社 B 内ローカルネットワーク

- ETHER ポート : グループ 2 ポート 1~4
- VLAN 番号 : 2
- lan 定義番号 : 1
- プライベート IP アドレス : 192.168.3.1/24
- グローバル IP アドレス : 202.168.3.66 (プロバイダから提示された内容)

### [本社]

#### VPN 終端装置側

- ETHER ポート : グループ 1 ポート 1
- VLAN 番号 : 1
- lan 定義番号 : 0
- IP アドレス : 20.168.2.66/24  
(プロバイダから割り当てられた固定 IP アドレス)
- デフォルトルートの IP アドレス : 202.168.2.65 (プロバイダから指定された IP アドレス)

**本社内ローカルネットワーク**

- Ether ポート : グループ 2 ポート 1~4
- VLAN 番号 : 2
- lan 定義番号 : 1
- IP アドレス : 192.168.2.1/24

**● 設定コマンド****[支社 A (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

**[支社 B (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.3.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

**【本社】**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2
# delete lan
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

**● 設定条件****【支社 A】**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 : 192.168.1.0/24 - any4

**【支社 B】**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.3.66 - 202.168.2.66
- IPsec 対象範囲 : 192.168.3.0/24 - any4

**【本社】**

- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 : any4 - 192.168.1.0/24
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 202.168.2.66 - 202.168.3.66
- IPsec 対象範囲 : any4 - 192.168.3.0/24


**【共通 A】**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768



**[共通B]**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : 3des-cbc
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DH グループ : なし
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321 (文字列)
- IKE 認証方法 : shared
- IKE 暗号アルゴリズム : 3des-cbc
- IKE 認証アルゴリズム : hmac-sha1
- IKE DH グループ : modp1024

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社 A を設定する****● コマンド**

```

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit

```

## 支社 B を設定する

### ● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

## 本社を設定する

### ● コマンド

```
VPN を設定する
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.3.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
```

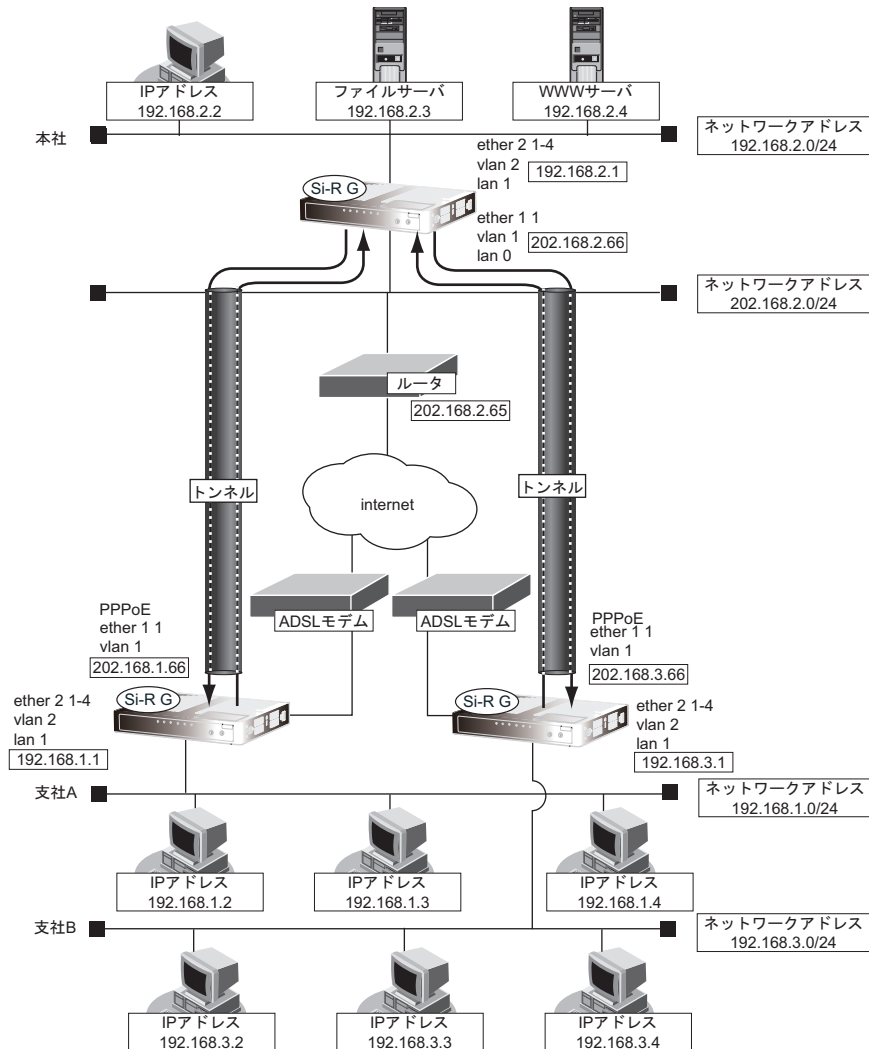
```
# remote 1 ap 0 ike proposal pfs modp1024
```

```
設定終了  
# save  
# commit
```

## 1.8.2 NAT と併用した固定 IP アドレスでの VPN (自動鍵交換)

IPsec 機能を使って自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。



### ● 前提条件

#### [支社 A (PPPoE 常時接続)]

- ローカルネットワーク IP アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.1.66/24
- グローバルネットワーク IP アドレス : 10.0.1.1/24
- PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

**[支社 B (PPPoE 常時接続)]**

- ローカルネットワーク IP アドレス : 192.168.3.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.3.66/24
- グローバルネットワーク IP アドレス : 10.0.3.1/24
- PPPoE ユーザ認証 ID : userid3 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass3 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

**[本社]**

- ローカルネットワーク IP アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス : 202.168.2.65

**● 設定コマンド****[支社 A (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi 202.168.1.66 1 5m
# remote 0 ip msschange 1414
```

**[支社 B (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.3.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid3 userpass3
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.3.66
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi 202.168.3.66 1 5m
# remote 0 ip msschange 1414
```

**[本社]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

**● 設定条件****[支社A]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 10.0.1.1 - 202.168.2.66
- IPsec 対象範囲 : 192.168.1.0/24 - any4

**[支社B]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 10.0.3.1 - 202.168.2.66
- IPsec 対象範囲 : 192.168.3.0/24 - any4

**[本社]**


- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 202.168.2.66 - 10.0.1.1
- IPsec 対象範囲 : any4 - 192.168.1.0/24
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 202.168.2.66 - 10.0.3.1
- IPsec 対象範囲 : any4 - 192.168.3.0/24

**[共通A]**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

**[共通B]**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : 3des-cbc
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DH グループ : なし
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321 (文字列)
- IKE 認証方法 : shared
- IKE 暗号アルゴリズム : 3des-cbc
- IKE 認証アルゴリズム : hmac-sha1
- IKE DH グループ : modp1024

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社 A を設定する****● コマンド**

```

インターネットへIPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.1.66 500 10.0.1.1 500 17
# remote 0 ip nat static 1 202.168.1.66 any 10.0.1.1 any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit

```

## 支社 B を設定する

### ● コマンド

```
インターネットへIPsec/IKE パケットを送信する設定をする
# remote 0 ip nat static 0 202.168.3.66 500 10.0.3.1 500 17
# remote 0 ip nat static 1 202.168.3.66 any 10.0.3.1 any 50
```

VPN を設定する

```
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
```

設定終了

```
# save
# commit
```

## 本社を設定する

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 10.0.1.1
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 10.0.3.1
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
```



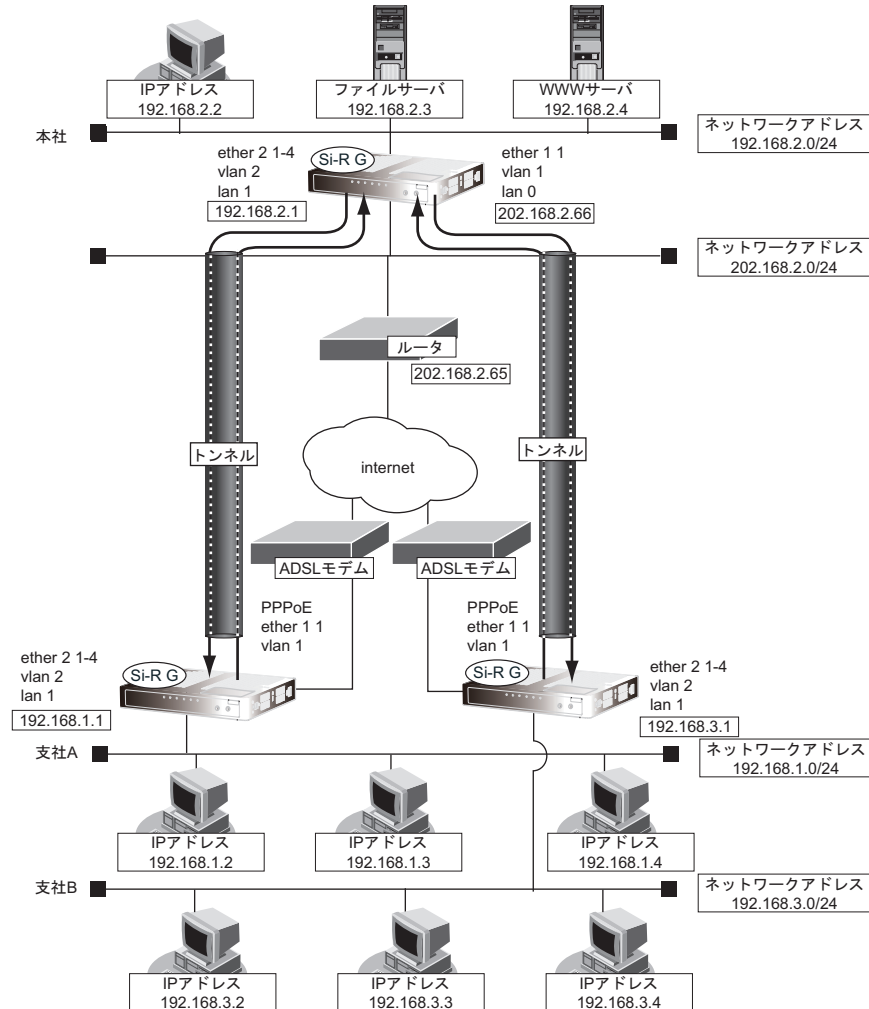
```
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

### 1.8.3 NAT と併用した可変 IP アドレスでの VPN (自動鍵交換)

接続するたびに IP アドレスが変わる環境で VPN を構築する場合の設定方法を説明します。

ここでは、以下のコマンドによって、支社 A および支社 B は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。



#### ● 前提条件

##### [支社 A (PPPoE 接続)]

- ・ ローカルネットワーク IP アドレス : 192.168.1.1/24
- ・ PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- ・ PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- ・ PPPoE ポート : ETHERグループ 1 ポート 1

##### [支社 B (PPPoE 接続)]

- ・ ローカルネットワーク IP アドレス : 192.168.3.1/24
- ・ PPPoE ユーザ認証 ID : userid3 (プロバイダから提示された内容)
- ・ PPPoE ユーザ認証パスワード : userpass3 (プロバイダから提示された内容)
- ・ PPPoE ポート : ETHERグループ 1 ポート 1

**[本社]**

- ローカルネットワーク IP アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス : 202.168.2.65

**● 設定コマンド****[支社 A (PPPoE 接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
```

**[支社 B (PPPoE 接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.3.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid3 userpass3
```

**[本社]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

**● 設定条件****[支社 A (Initiator)]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 A - 202.168.2.66
- IPsec 対象範囲 : 192.168.1.0/24 - any4
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESP のプライベートアドレス : 192.168.1.1

**[支社 B (Initiator)]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 B - 202.168.2.66
- IPsec 対象範囲 : 192.168.3.0/24 - any4
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.3.1
- ESP のプライベートアドレス : 192.168.3.1

**[本社]**


- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 202.168.2.66 - 支社 A
- IPsec 対象範囲 : any4 - 192.168.1.0/24
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 202.168.2.66 - 支社 B
- IPsec 対象範囲 : any4 - 192.168.3.0/24

**[共通 A]**

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 支社 A ID/ID タイプ : shisyaA (自装置名) /FQDN
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

**[共通 B]**

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : 3des-cbc
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DH グループ : なし
- IKE 支社 B ID/ID タイプ : shisyaB (自装置名) /FQDN
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321 (文字列)
- IKE 認証方法 : shared
- IKE 暗号アルゴリズム : 3des-cbc
- IKE 認証アルゴリズム : hmac-sha1
- IKE DH グループ : modp1024

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

**◆ ID タイプとは？**

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

**こんな事に気をつけて**

可変 IP アドレスでの VPN 接続を行うときは、インターネットプロバイダから割り当てられる IP アドレスが不定であるため、ローカルネットワーク IP アドレスで IKE ネゴシエーションを行う場合があります。このような運用では、送出インタフェースで NAT 機能を使用してください。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 A (Initiator) を設定する

### ● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

## 支社 B (Initiator) を設定する

### ● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.3.1 500 any 500 17
# remote 0 ip nat static 1 192.168.3.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

## 本社 (Responder) を設定する

### ● コマンド

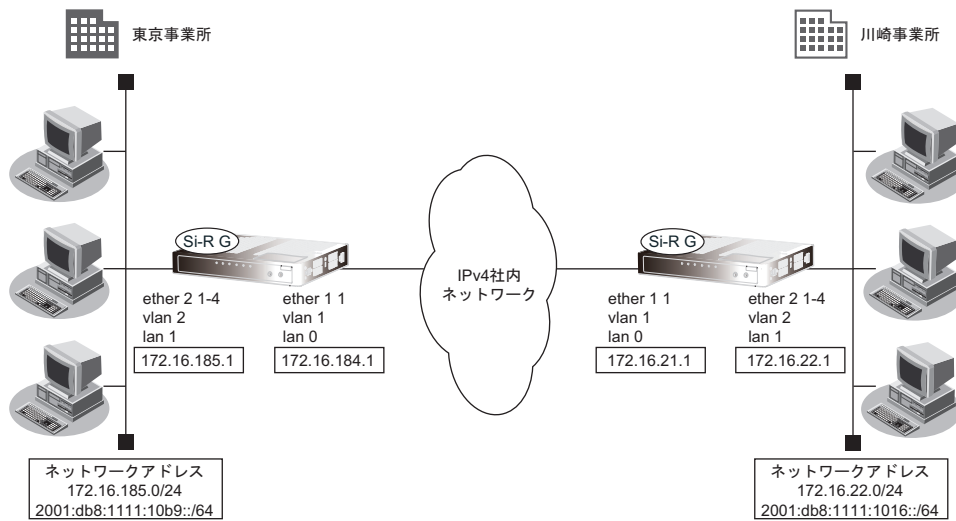
VPN を設定する

```
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024

設定終了
# save
# commit
```

## 1.9 IPv6 の事業所 LAN を IPv4 トンネルで接続する

ここでは、IPv4 で構築されたイントラネットを介して、2つの事業所（東京、川崎）の IPv6 ネットワークどうしを接続（トンネリング）する場合を例に説明します。



### ● 設定条件

#### [東京事業所]

- ・ ダイナミックルーティングを使用する
- ・ イントラネット側の IPv4 アドレス : 172.16.184.1
- ・ 東京事業所側の IPv4 アドレス : 172.16.185.1
- ・ 東京事業所側の IPv6 プレフィックス/プレフィックス長 : 2001:db8:1111:10b9::/64 (※)

#### [川崎事業所]

- ・ ダイナミックルーティングを使用する
- ・ イントラネット側の IPv4 アドレス : 172.16.21.1
- ・ 川崎事業所側の IPv4 アドレス : 172.16.22.1
- ・ 川崎事業所側の IPv6 プレフィックス/プレフィックス長 : 2001:db8:1111:1016::/64 (※)

※) この例では、プライベートアドレス (IPv4) /ドキュメント記述用アドレス (IPv6) を使用しています。

#### こんな事に気をつけて

- ・ コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、[ ]、[ < ]、[ > ]、[ & ]、[ % ] は入力しないでください。

☞ 参照 マニュアル「コマンドユーザズガイド」

- ・ IPv6 over IPv4 トンネルを利用する場合は、カプセル化された IPv4 パケットのフラグメントを防ぐため、トンネルに利用する相手情報の MTU に 1280 を設定してください。
- ・ 本装置の IP アドレスには、ネットワークアドレスまたはブロードキャストアドレスを指定しないでください。



## 東京事業所を設定する

### ● コマンド

```
IPv4 で事業所間を接続する
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 172.16.184.1/24 3
# lan 0 ip rip use v1 v1 0
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 0 vlan 1
# lan 1 ip address 172.16.185.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off
# lan 1 vlan 2

IPv6 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 ifid auto
# lan 1 ipv6 address 0 2001:db8:1111:10b9::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 2001:db8:1111:10b9::/64 30d 7d c0

IP トンネル接続 (川崎事業所) の情報を設定する
# remote 0 name v6kawasa
# remote 0 mtu 1280
# remote 0 ap 0 name tn-kawa
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.184.1
# remote 0 ap 0 tunnel remote 172.16.21.1
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1016::/64 1

設定終了
# save

再起動
# reset
```

## 川崎事業所を設定する

### ● コマンド

```
IPv4 で事業所間を接続する
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan 0
# delete lan 1

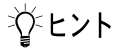
# lan 0 ip address 172.16.21.1/24 3
# lan 0 ip rip use v1 v1 0 off
# lan 0 ip dhcp service off
# lan 0 ip nat mode off
# lan 0 vlan 1
# lan 1 ip address 172.16.22.1/24 3
# lan 1 ip rip use v1 v1 0
# lan 1 ip dhcp service off
# lan 1 ip nat mode off
# lan 1 vlan 2

IPv6 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 ifid auto
# lan 1 ipv6 address 0 2001:db8:1111:1016::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 2001:db8:1111:1016::/64 30d 7d c0

IP トンネル接続 (東京事業所) の情報を設定する
# remote 0 name v6tokyo
# remote 0 mtu 1280
# remote 0 ap 0 name tn-tokyo
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 172.16.21.1
# remote 0 ap 0 tunnel remote 172.16.184.1
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:10b9::/64 1

設定終了
# save

再起動
# reset
```



◆ **NAT と IPv6 over IPv4 トンネルを併用する**

IPv4 環境の NAT と、IPv6 over IPv4 トンネルを利用した IPv6 通信環境を併用する場合は、IPv4 環境の NAT の処理によって、IPv4 アドレスがどのように変換処理されるかを判断して IPv6 over IPv4 トンネル通信の設定を行う必要があります。

本装置では、トンネル処理は NAT 処理の内側（プライベートアドレス側）で行われますので、以下のように設定します。

設定項目	設定内容
自側エンドポイント	以下の IP アドレスのどちらかを設定します。 <ul style="list-style-type: none"> <li>LAN に設定された IP アドレスまたはセカンダリ IP アドレス</li> <li>remote ip address local コマンドで設定した自側 IP アドレス</li> </ul> ※) PPP で割り当てられる IP アドレスは利用できません。
相手側エンドポイント	相手トンネル GW の IP アドレス
静的 NAT	IPv6 over IPv4 トンネル通信が相手トンネル GW 側から開始されることがある場合は、静的 NAT の設定が必要となります。 <ul style="list-style-type: none"> <li>プライベート IP 情報                              IP アドレス 自側エンドポイントに設定したアドレス                              ポート番号 すべて</li> <li>グローバル IP 情報                              IP アドレス 相手トンネル GW に設定された、本装置側のアドレス                              ポート番号 すべて</li> <li>プロトコル IPv6 over IPv4</li> </ul>

具体例を以下に示します。

条件：

- 本装置の NAT 変換で利用するグローバルアドレスに 172.16.0.1 を利用
- 本装置のプライベート LAN 側に 192.168.1.1 を利用
- 相手トンネル GW の IP アドレスに 172.31.0.1 を利用

IPv6 over IPv4 トンネル接続：

- 本装置のトンネル通信の設定：  
 192.168.1.1 と 172.31.0.1 の間でトンネル通信を行うことを前提に、以下のとおり設定します。  
 remote 0 ap 0 tunnel local 192.168.1.1  
 remote 0 ap 0 tunnel remote 172.31.0.1

静的 NAT 設定：

- lan 0 ip nat static 0 192.168.1.1 any 172.16.0.1 any 41

なお、この具体例で、相手トンネル GW の設定は、以下のとおりです。

172.16.0.1 と 172.31.0.1 の間でトンネル通信を行うことを前提とします。

相手トンネル GW に Si-R G シリーズ（NAT 未使用）を利用する場合は、相手側の Si-R G に以下を設定します。

```
remote 0 ap 0 tunnel local 172.31.0.1
remote 0 ap 0 tunnel remote 172.16.0.1
```

## 第2章 活用例

# 2

この章では、本装置の便利な機能の活用方法について説明します。

2.1	RIPの経路を制御する (IPv4)	60
2.1.1	特定の経路情報の送信を許可する	62
2.1.2	特定の経路情報のメトリック値を変更して送信する	63
2.1.3	特定の経路情報の受信を許可する	64
2.1.4	特定の経路情報のメトリック値を変更して受信する	65
2.1.5	特定の経路情報の送信を禁止する	67
2.1.6	特定の経路情報の受信を禁止する	68
2.2	RIPの経路を制御する (IPv6)	69
2.2.1	特定の経路情報の送信を許可する	71
2.2.2	特定の経路情報のメトリック値を変更して送信する	72
2.2.3	特定の経路情報の受信を許可する	73
2.2.4	特定の経路情報のメトリック値を変更して受信する	74
2.2.5	特定の経路情報の送信を禁止する	76
2.2.6	特定の経路情報の受信を禁止する	77
2.3	OSPFv2を使用したネットワークを構築する (IPv4)	78
2.3.1	スタブエリアを使う	82
2.4	OSPFの経路を制御する (IPv4)	85
2.4.1	OSPFネットワークでエリアの経路情報 (LSA) を集約する	85
2.4.2	AS外部経路を集約してOSPFネットワークに広報する	87
2.4.3	エリア境界ルータで不要な経路情報 (LSA) を遮断する	88
2.5	OSPF機能を使う (IPv6)	90
2.5.1	OSPFネットワークを構築する	90
2.5.2	エリア境界ルータでエリア内部経路を集約する	93
2.5.3	エリア境界ルータで不要な経路情報を遮断する	94
2.6	BGPの経路を制御する (IPv4)	95
2.6.1	特定の経路情報の受信を透過させる	95
2.6.2	特定のASからの経路情報の受信を遮断する	97
2.6.3	IP-VPN網からの受信情報の他IP-VPN網への送信を遮断する	98
2.6.4	冗長構成の通信経路を使用する	99
2.7	BGP機能を使う (IPv6)	101
2.7.1	BGPでIPv6経路情報を交換する	101
2.7.2	特定の経路情報の受信を透過させる	103
2.7.3	特定のASからの経路情報の受信を遮断する	104
2.7.4	特定のASから受信した経路情報の送信を遮断する	105
2.7.5	冗長構成の通信経路を使用する	106

2.8	マルチキャスト機能を使う	108
2.8.1	マルチキャスト機能 (PIM-DM) を使う	108
2.8.2	マルチキャスト機能 (PIM-SM) を使う	112
2.8.3	マルチキャスト機能 (スタティックルーティング) を使う	118
2.9	VLAN 機能を使う	121
2.9.1	ポート VLAN 機能を使う	121
2.9.2	タグ VLAN 機能を使う	122
2.10	バックアップポート機能を使う	123
2.11	STP 機能を使う	124
2.11.1	STP を使う	124
2.12	IP フィルタリング機能を使う	125
2.12.1	外部の特定サービスへのアクセスだけを許可する	129
2.12.2	外部から特定サーバへのアクセスだけを許可する	133
2.12.3	外部から特定サーバへのアクセスだけを許可して SPI を併用する	137
2.12.4	外部の特定サービスへのアクセスだけを許可する (IPv6 フィルタリング)	141
2.12.5	外部の特定サーバへのアクセスだけを禁止する	145
2.12.6	利用者が意図しない発信を防ぐ	147
2.12.7	回線が接続しているときだけを許可する	149
2.12.8	外部から特定サーバへの ping だけを禁止する	150
2.13	IPsec 機能を使う	152
2.13.1	IPv4 over IPv4 で固定 IP アドレスでの VPN (手動鍵交換)	159
2.13.2	IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)	163
2.13.3	IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)	167
2.13.4	IPv6 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換)	171
2.13.5	IPv6 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)	175
2.13.6	IPv4 over IPv4 で 1 つの IKE セッションに複数の IPsec トンネル構成での VPN (自動鍵交換)	179
2.13.7	IPsec 機能と他機能との併用	183
2.13.8	テンプレート着信機能 (AAA 認証) を使用した固定 IP アドレスでの VPN	188
2.13.9	テンプレート着信機能 (AAA 認証) を使用した可変 IP アドレスでの VPN	192
2.13.10	テンプレート着信機能 (RADIUS 認証) を使用した固定 IP アドレスでの VPN	197
2.13.11	テンプレート着信機能 (RADIUS 認証) を使用した可変 IP アドレスでの VPN	202
2.13.12	テンプレート着信機能 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	208
2.13.13	テンプレート着信機能 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN (冗長構成)	217
2.13.14	テンプレート着信機能 (動的 VPN) を使用した IPv6 over IPv6 で固定 IP アドレスでの VPN	220
2.13.15	NAT トラバーサルを使用した可変 IP アドレスでの VPN	230
2.13.16	テンプレート着信機能 (AAA 認証) および NAT トラバーサルを使用した可変 IP アドレスでの VPN	234
2.13.17	接続先情報 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	238
2.13.18	RSA デジタル署名認証を使用した固定 IP アドレスでの VPN (自動鍵交換)	249
2.13.19	RSA デジタル署名認証を使用した可変 IP アドレスでの VPN (自動鍵交換)	253
2.13.20	RSA デジタル署名認証で接続先情報 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN	257
2.13.21	IPv4 over IPv4 で NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	270
2.13.22	IPv4 over IPv4 で NAT と併用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	274
2.13.23	IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	278
2.13.24	IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	281
2.13.25	IPv6 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	284
2.13.26	IPv6 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	287
2.13.27	IPv4 over IPv4 で 1 つの IKE セッションに複数の IPsec トンネル構成での VPN (自動鍵交換 IKE Version2)	290
2.13.28	NAT トラバーサルを使用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	293
2.13.29	RSA デジタル署名認証を使用した固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	296
2.13.30	RSA デジタル署名認証を使用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)	299
2.13.31	EAP 認証を使用した固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)	302

2.14	システムログを採取する	305
2.15	マルチ NAT 機能 (アドレス変換機能) を使う	307
2.15.1	プライベート LAN 接続でサーバを公開する	308
2.15.2	PPPoE 接続でサーバを公開する	309
2.15.3	ネットワーク型接続でサーバを公開する	311
2.15.4	サーバ以外のアドレス変換をしないで、プライベート LAN 接続でサーバを公開する	313
2.15.5	複数の NAT トラバーサル機能を使用した IPsec クライアントを同じ IPsec サーバに接続する	314
2.15.6	NAT あて先変換で双方向のアドレスを変換する	315
2.16	VoIP NAT トラバーサル機能を使う	316
2.17	TOS/Traffic Class 値書き換え機能を使う	318
2.18	VLAN プライオリティマッピング機能を使う	320
2.19	シェーピング機能を使う	322
2.19.1	特定のインタフェースでシェーピング機能を使う	322
2.19.2	送信先ごとにシェーピング機能を使う	323
2.19.3	特定のポートでシェーピング機能を使う	325
2.20	ヘッダ圧縮機能を使う	326
2.21	帯域制御 (WFQ) 機能を使う	327
2.21.1	特定のインタフェースで帯域制御 (WFQ) 機能を使う	327
2.21.2	特定のポートで帯域制御 (WFQ) 機能を使う	329
2.22	DHCP 機能を使う	330
2.22.1	DHCP サーバ機能を使う	331
2.22.2	DHCP スタティック機能を使う	333
2.22.3	DHCP クライアント機能を使う	335
2.22.4	DHCP リレーエージェント機能を使う	337
2.22.5	IPv6 DHCP クライアント機能を使う	341
2.22.6	IPv6 DHCP サーバ機能を使う	343
2.22.7	IPv6 DHCP リレーエージェント機能を使う	345
2.22.8	IPv6 DHCP クライアント機能で取得した情報を IPv6 DHCP サーバ機能で配布する	347
2.22.9	通信事業者からの RA 情報と連携して IPv6 DHCP クライアント機能を使用する	349
2.23	DNS サーバ機能を使う (ProxyDNS)	352
2.23.1	DNS サーバの自動切り替え機能 (順引き) を使う	352
2.23.2	DNS サーバの自動切り替え機能 (逆引き) を使う	354
2.23.3	DNS サーバアドレスの自動取得機能を使う	355
2.23.4	DNS サーバアドレスを DHCP サーバから取得して使う	357
2.23.5	DNS 問い合わせタイプフィルタ機能を使う	359
2.23.6	DNS サーバ機能を使う	360
2.24	特定の URL へのアクセスを禁止する (URL フィルタ機能)	361
2.25	SNMP エージェント機能を使う	363
2.26	ECMP 機能を使う	366
2.27	VRRP 機能を使う	371
2.27.1	簡易ホットスタンバイ機能を使う	372
2.27.2	クラスタリング機能を使う	375
2.28	ポリシールーティング機能を使う	378
2.28.1	Ingress ポリシールーティング機能を使う	378
2.28.2	マルチルーティング機能を使う	380
2.29	クラウドサービスゲートウェイ機能を使う	381
2.29.1	ドメイン名をドメインリストで設定する	383
2.29.2	ドメイン名を構成定義に設定する方法	385
2.30	遠隔地のパソコンを起動させる (リモートパワーオン機能)	386
2.30.1	リモートパワーオン情報を設定する	387
2.30.2	リモートパワーオン機能を使う	387
2.31	スケジュール機能を使う	388
2.31.1	スケジュールを予約する	388
2.31.2	電話番号変更を予約する	390
2.31.3	構成定義情報の切り替えを予約する	390

2.32	ブリッジグループ機能を使う	391
2.32.1	異なるVLANをグループ化する	392
2.32.2	IPトンネルで事業所間をブリッジ接続する (Ethernet over IPブリッジ)	393
2.33	透過モードを使う	398
2.33.1	ブリッジグループ機能と併用する	398
2.34	データ通信モジュールで通信バックアップをする	402
2.35	アプリケーションフィルタ機能を使う	406
2.36	IEEE802.1X認証機能を使う	408
2.37	不正端末アクセス防止機能 (MACアドレス認証) を使う	410
2.38	ARP認証機能を使う	412
2.39	PKI機能を使う	413
2.39.1	装置に証明書を登録する (自装置証明書を認証局 (CA) で発行する)	413
2.39.2	装置に証明書を登録する (自装置証明書を自己発行する)	417
2.39.3	認証局証明書を設定する	421
2.40	トラッキング機能を使う	423
2.41	装置を保護する	425
2.41.1	設定例	425

## 2.1 RIPの経路を制御する (IPv4)

本装置を経由して、ほかのルータに送受信する経路情報に対して、IPアドレスや方向を組み合わせで指定することによって、特定のあて先への経路情報だけを広報する、または不要な経路情報を遮断することができます。

### 経路情報のフィルタリング条件

#### 対象となる経路情報

- RIPによる経路情報

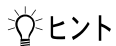
#### 指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件 (IPアドレス/アドレスマスク)
- メトリック値



メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にany以外を指定した場合に有効です。送信方向のメトリック値に1～16を指定した場合、インタフェースに設定したRIPの加算メトリック値は加算されません。



#### ◆ IPアドレスとアドレスマスクの決め方

フィルタリング条件の要素には、「IPアドレス」と「アドレスマスク」があります。制御対象となる経路情報は、経路情報のIPアドレスとアドレスマスクが指定したIPアドレスとアドレスマスクと一致したものです。

例) 指定値 : 172.21.0.0/16の場合  
経路情報 : 172.21.0.0/16は制御対象となる  
172.21.0.0/24は制御対象とならない

また、フィルタリング条件のIPアドレスと指定したIPアドレスが、指定したアドレスマスクまで一致した場合に制御対象とすることもできます。

指定値 : 172.21.0.0/16の場合  
経路情報 : 172.21.0.0/24は制御対象となる  
172.21.10.0/24は制御対象となる

#### こんな事に気をつけて

RIPv1を使用している場合もアドレスマスクの設定が必要です。この場合、インタフェースのアドレスマスクを指定してください。また、アドレスクラスが異なる経路情報を制御する場合は、ナチュラルマスク値を指定してください。

例) `lan 0 ip address 192.168.1.1/24`に`10.0.0.0`の経路情報を制御する場合は、`10.0.0.0/8`を指定します。



## フィルタリングの設計方針

---

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する
- B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針Bの例として、以下の設定例について説明します。

- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

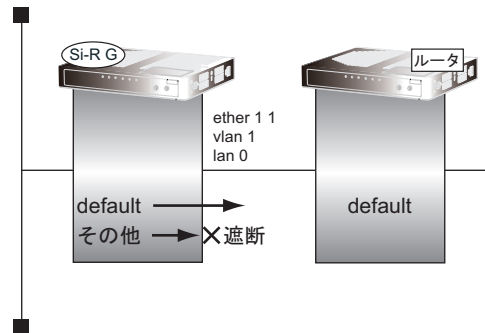
### こんな事に気をつけて

---

- フィルタリング条件には、優先度を示す定義番号があり、小さいほど、より高い優先度を示します。
  - RIP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP経路情報は遮断されます。
  - RIP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP経路情報は遮断されます。
-

## 2.1.1 特定の経路情報の送信を許可する

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明します。



### ● 前提条件

- ETHERグループ1ポート1にlan 0定義が使用されている

### ● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass out
# lan 0 ip rip filter 0 route default
```

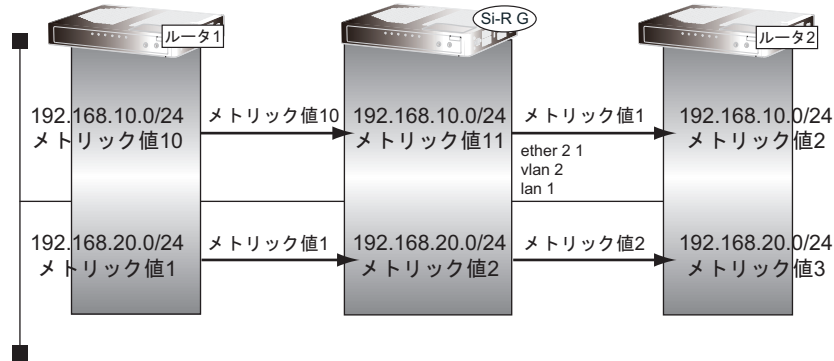
```
その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject out
# lan 0 ip rip filter 1 route any
```

```
設定終了
# save
# commit
```

## 2.1.2 特定の経路情報のメトリック値を変更して送信する

ここでは、本装置がルータ2へ192.168.10.0/24、メトリック値1の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から192.168.10.0/24のメトリック値10と192.168.20.0/24のメトリック値1の経路情報を受信するものとします。



### ● 前提条件

- ETHERグループ2ポート1にlan 1定義が使用されている

### ● フィルタリング設計

- 本装置から192.168.10.0/24の送信を許可する場合、メトリック値1に変更
- 192.168.10.0/24以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

192.168.10.0/24をメトリック値1で送信する

```
# lan 1 ip rip filter 0 act pass out
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 1
```

その他の経路情報はメトリック値を変更しないで送信する

```
# lan 1 ip rip filter 1 act pass out
# lan 1 ip rip filter 1 route any
```

設定終了

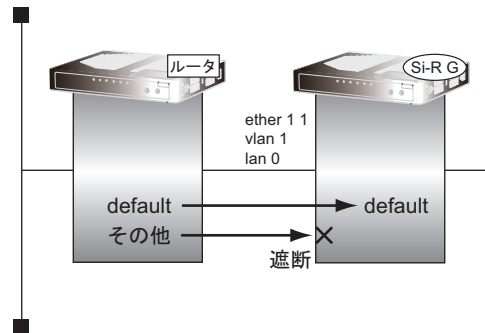
```
# save
# commit
```

### こんな事に気をつけて

- 送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。
- 送信方向でメトリック値が設定されていても、メトリック値16の経路情報のメトリック値は変更されません。

## 2.1.3 特定の経路情報の受信を許可する

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



### ● 前提条件

- ETHERグループ1ポート1にlan 0定義が使用されている

### ● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

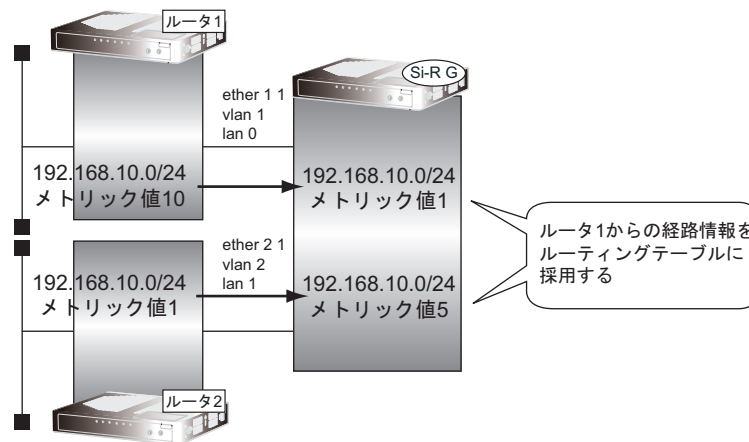
```
デフォルトルートを透過させる
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route default
```

```
その他の経路情報はすべて遮断する
# lan 0 ip rip filter 1 act reject in
# lan 0 ip rip filter 1 route any
```

```
設定終了
# save
# commit
```

## 2.1.4 特定の経路情報のメトリック値を変更して受信する

ここでは、本装置が、ルータ1とルータ2から同じ先へ経路情報 192.168.10.0/24 を受信した場合に、ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている
- ether 2 1 に lan 1 定義が使用されている

### ● フィルタリング設計

- ルータ1から、192.168.10.0/24 の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、192.168.10.0/24 の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```
lan 0 で 192.168.10.0/24 の経路情報を受信した場合、メトリック値1 で受信する
# lan 0 ip rip filter 0 act pass in
# lan 0 ip rip filter 0 route 192.168.10.0/24
# lan 0 ip rip filter 0 set metric 1

lan 0 でのその他の経路情報はすべて受信する
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any

lan 1 で 192.168.10.0/24 の経路情報を受信した場合、メトリック値5 で受信する
# lan 1 ip rip filter 0 act pass in
# lan 1 ip rip filter 0 route 192.168.10.0/24
# lan 1 ip rip filter 0 set metric 5

lan 1 でのその他の経路情報はすべて受信する
# lan 1 ip rip filter 1 act pass in
# lan 1 ip rip filter 1 route any

設定終了
# save
# commit
```

---

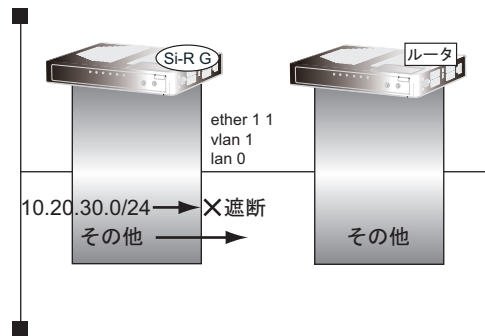
### こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

---

## 2.1.5 特定の経路情報の送信を禁止する

ここでは、本装置からルータへの 10.20.30.0/24 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている

### ● フィルタリング設計

- 本装置からルータへの 10.20.30.0/24 の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

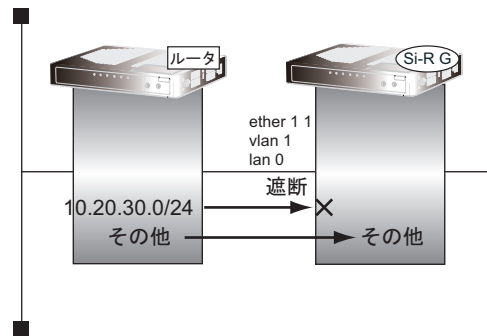
```
10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject out
# lan 0 ip rip filter 0 route 10.20.30.0/24
```

```
その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass out
# lan 0 ip rip filter 1 route any
```

```
設定終了
# save
# commit
```

## 2.1.6 特定の経路情報の受信を禁止する

ここでは、本装置は、ルータから 10.20.30.0/24 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている

### ● フィルタリング設計

- 本装置は 10.20.30.0/24 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```
10.20.30.0/24 を遮断する
# lan 0 ip rip filter 0 act reject in
# lan 0 ip rip filter 0 route 10.20.30.0/24
```

```
その他の経路情報はすべて透過させる
# lan 0 ip rip filter 1 act pass in
# lan 0 ip rip filter 1 route any
```

```
設定終了
# save
# commit
```



## 2.2 RIPの経路を制御する (IPv6)

本装置を経由して、ほかのルータに送信する経路情報や、ほかのルータから受信する経路情報に対して、経路情報や方向を組み合わせて指定することによって、特定のあて先への経路情報だけを広報する、または、不要な経路情報を遮断することができます。

### 経路情報のフィルタリング条件

#### 対象となる経路情報

- RIPによる経路情報 (IPv6)

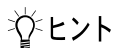
#### 指定条件

本装置では、以下の条件を指定することによって、経路情報を制御することができます。

- 動作
- 方向
- フィルタリング条件 (プレフィックス/プレフィックス長)
- メトリック値



メトリック値は指定メトリック値の経路情報をフィルタリングするのではなく、フィルタリング後の経路情報のメトリック値を変更する場合に指定します。0を指定すると変更は行いません。経路情報のフィルタリング条件にany以外を指定した場合に有効です。送信方向のメトリック値に1～16を指定した場合、インタフェースに設定したRIPの加算メトリック値は加算されません。



#### ◆ プレフィックスとプレフィックス長の決め方

フィルタリング条件の要素には、「プレフィックス」と「プレフィックス長」があります。制御対象となる経路情報は、経路情報のプレフィックスとプレフィックス長が指定したプレフィックスとプレフィックス長と一致したもののだけです。

例) 指定値 : 2001:db8:1111::/32 の場合  
 経路情報 : 2001:db8:1111::/32 は制御対象となる  
           2001:db8:1111::/64 は制御対象とはならない

また、経路情報のプレフィックスと指定したプレフィックスが、指定したプレフィックス長まで一致した場合に制御対象とすることもできます。

指定値 : 2001:db8::/16 の場合  
 経路情報 : 2001:db8::/32 は制御対象となる  
           2001:db8:1111::/32 は制御対象となる

## フィルタリングの設計方針

---

フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A. 特定の条件の経路情報だけを透過させ、その他はすべて遮断する
- B. 特定の条件の経路情報だけを遮断し、その他はすべて透過させる

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 特定の経路情報の送信を許可する
- 特定の経路情報のメトリック値を変更して送信する
- 特定の経路情報の受信を許可する
- 特定の経路情報のメトリック値を変更して受信する

また、設計方針Bの例として、以下の設定例について説明します。

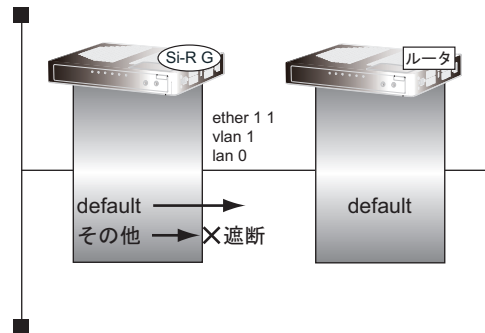
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

### こんな事に気をつけて

- フィルタリング条件には、優先度を示す定義番号があり、小さいほど、より高い優先度を示します。
  - RIP受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しないRIP経路情報は遮断されます。
  - RIP送信時には、優先順位の高い定義から順に送信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、送信方向のすべての条件に一致しないRIP経路情報は遮断されます。
-

## 2.2.1 特定の経路情報の送信を許可する

ここでは、本装置からルータへのデフォルトルートの送信だけを許可し、それ以外の経路情報の送信を禁止する場合の設定方法を説明しています。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている

### ● フィルタリング設計

- 本装置からルータへのデフォルトルートの送信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```

デフォルトルートの経路情報を透過させる
# lan 0 ipv6 rip filter 0 act pass out
# lan 0 ipv6 rip filter 0 route default

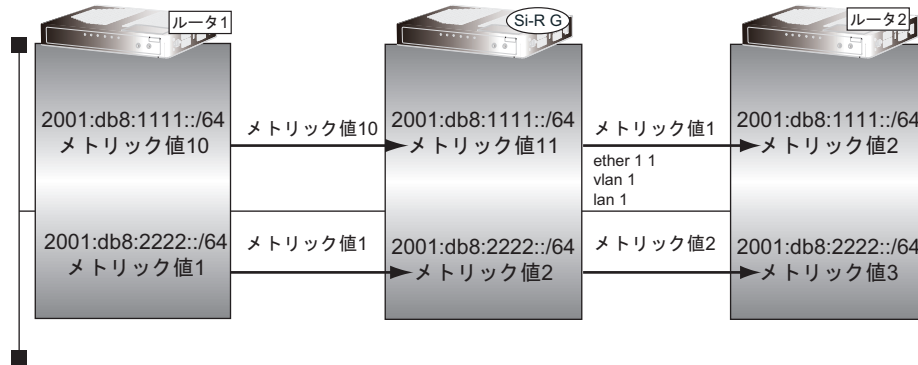
その他の経路情報はすべて遮断する
# lan 0 ipv6 rip filter 1 act reject out
# lan 0 ipv6 rip filter 1 route any

設定終了
# save
# commit
    
```

## 2.2.2 特定の経路情報のメトリック値を変更して送信する

ここでは、本装置がルータ2へ2001:db8:1111::/64、メトリック値1の経路情報を送信する場合の設定方法を説明します。

なお、本装置は、ルータ1から2001:db8:1111::/64のメトリック値10と2001:db8:2222::/64のメトリック値1の経路情報を受信するものとします。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている
- lan 0 に IPv6 の基本情報が定義されている

### ● フィルタリング設計

- 本装置から 2001:db8:1111::/64 の送信を許可する場合、メトリック値 1 に変更
- 2001:db8:1111::/64 以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```

2001:db8:1111::/64 の経路情報をメトリック値 1 で送信する
# lan 1 ipv6 rip filter 0 act pass out
# lan 1 ipv6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ipv6 rip filter 0 set metric 1

その他の経路情報はメトリック値を変更しないで送信する
# lan 1 ipv6 rip filter 1 act pass out
# lan 1 ipv6 rip filter 1 route any

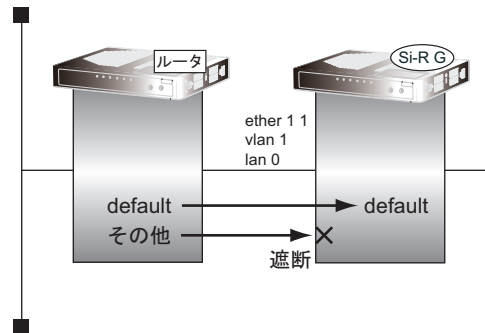
設定終了
# save
# commit
    
```

### こんな事に気をつけて

- 送信方向でメトリック値が設定されている場合、インタフェースのRIP加算メトリック値の加算は行われません。
- 送信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

## 2.2.3 特定の経路情報の受信を許可する

ここでは、本装置はルータからデフォルトルートの受信だけを許可し、それ以外の経路情報の受信を禁止する場合の設定方法を説明します。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている

### ● フィルタリング設計

- 本装置はデフォルトルートの受信だけを許可
- その他はすべて遮断

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```

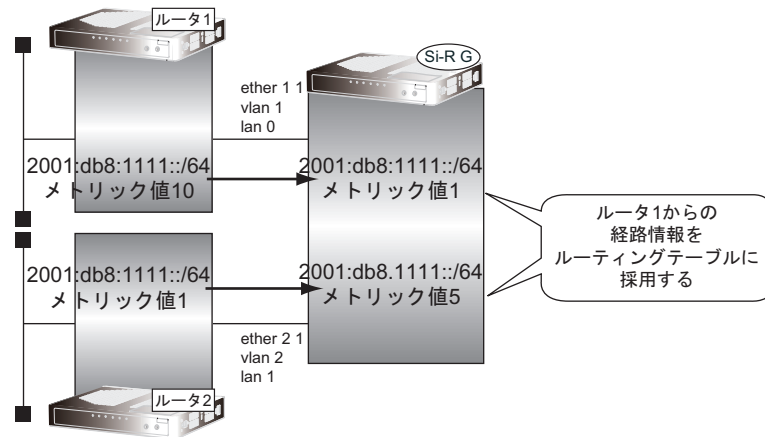
デフォルトルートの経路情報を透過させる
# lan 0 ipv6 rip filter 0 act pass in
# lan 0 ipv6 rip filter 0 route default

その他の経路情報はすべて遮断する
# lan 0 ipv6 rip filter 1 act reject in
# lan 0 ipv6 rip filter 1 route any

設定終了
# save
# commit
    
```

## 2.2.4 特定の経路情報のメトリック値を変更して受信する

ここでは、本装置が、ルータ1とルータ2から同じ先への経路情報 2001:db8:1111::/64 を受信した場合に、ルータ1から受信した経路情報を採用する場合の設定方法を説明します。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている
- ether 2 1 に lan 1 定義が使用されている
- lan0 に IPv6 の基本情報が定義されている
- lan1 に IPv6 の基本情報が定義されている

### ● フィルタリング設計

- ルータ1から、2001:db8:1111::/64 の経路情報を受信した場合、メトリック値1に変更
- ルータ2から、2001:db8:1111::/64 の経路情報を受信した場合、メトリック値5に変更
- 上記以外の経路情報は、メトリック値を変更しない

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```
lan 0 で 2001:db8:1111::/64 の経路情報を受信した場合、メトリック値1で受信する
# lan 0 ipv6 rip filter 0 act pass in
# lan 0 ipv6 rip filter 0 route 2001:db8:1111::/64
# lan 0 ipv6 rip filter 0 set metric 1

lan 0 でのその他の経路情報はすべて受信する
# lan 0 ipv6 rip filter 1 act pass in
# lan 0 ipv6 rip filter 1 route any

lan 1 で 2001:db8:1111::/64 の経路情報を受信した場合、メトリック値5で受信する
# lan 1 ipv6 rip filter 0 act pass in
# lan 1 ipv6 rip filter 0 route 2001:db8:1111::/64
# lan 1 ipv6 rip filter 0 set metric 5

lan 1 でのその他の経路情報はすべて受信する
# lan 1 ipv6 rip filter 1 act pass in
# lan 1 ipv6 rip filter 1 route any

設定終了
# save
# commit
```

---

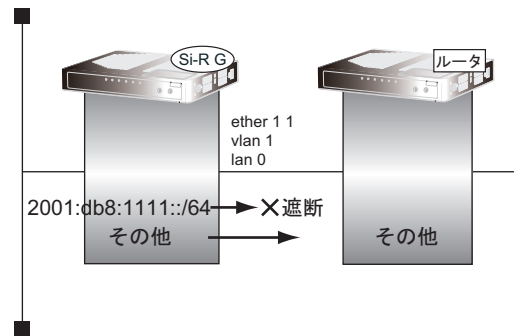
### こんな事に気をつけて

受信方向でメトリック値が設定されていても、メトリック値 16 の経路情報のメトリック値は変更されません。

---

## 2.2.5 特定の経路情報の送信を禁止する

ここでは、本装置からルータへの 2001:db8:1111::/64 の送信を禁止し、それ以外の経路情報の送信を許可する場合の設定方法を説明します。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている

### ● フィルタリング設計

- 本装置からルータへの 2001:db8:1111::/64 の送信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```
2001:db8:1111::/64 の経路情報を遮断する
# lan 0 ipv6 rip filter 0 act reject out
# lan 0 ipv6 rip filter 0 route 2001:db8:1111::/64
```

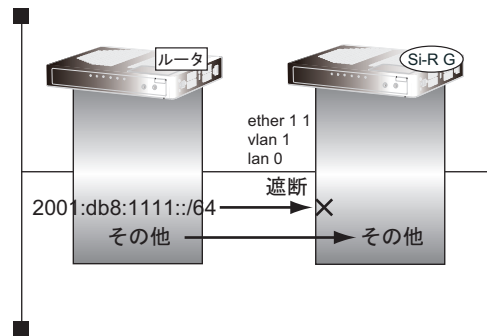
```
その他の経路情報はすべて透過させる
# lan 0 ipv6 rip filter 1 act pass out
# lan 0 ipv6 rip filter 1 route any
```

```
設定終了
# save
# commit
```



## 2.2.6 特定の経路情報の受信を禁止する

ここでは、本装置は、ルータから 2001:db8:1111::/64 の経路情報の受信を禁止し、それ以外の経路情報の受信を許可する場合の設定方法を説明します。



### ● 前提条件

- ether 1 1 に lan 0 定義が使用されている

### ● フィルタリング設計

- 本装置は 2001:db8:1111::/64 の受信を禁止
- その他はすべて透過

上記のフィルタリング設計に従って設定する場合のコマンド例を示します。

### ● コマンド

```
2001:db8:1111::/64 の経路情報を遮断する
# lan 0 ipv6 rip filter 0 act reject in
# lan 0 ipv6 rip filter 0 route 2001:db8:1111::/64
```

```
その他の経路情報はすべて透過させる
# lan 0 ipv6 rip filter 1 act pass in
# lan 0 ipv6 rip filter 1 route any
```

```
設定終了
# save
# commit
```

## 2.3 OSPFv2 を使用したネットワークを構築する (IPv4)

ここでは、OSPFv2 を使用したダイナミックルーティングのネットワークの設定方法について説明します。

OSPF を使用するネットワークは、バックボーンエリアとその他のエリアに分割して管理します。

エリアには、エリアごとにエリア ID を設定します。バックボーンエリアには必ず 0.0.0.0 のエリア ID を設定し、ほかのエリアには重複しないように 0.0.0.0 以外のエリア ID を設定します。

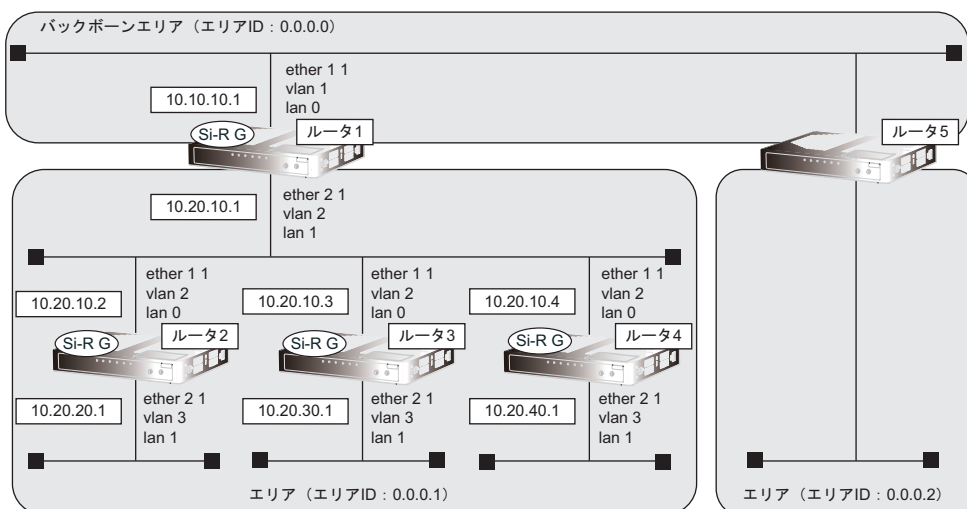
エリア境界ルータでは、エリア内の経路情報を集約して広報することができます。

☛ 参照 マニュアル「機能説明書」

### こんな事に気をつけて

- NAT 機能と併用することはできません。
- OSPF を使用するインターフェースは、それぞれ異なったネットワークに属する IP アドレスを設定する必要があります。同じネットワークに属する IP アドレスを設定した場合、OSPF を使用しないと判断されます。
- ルータは、各エリアに 50 台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2 つ以上のエリアの指定ルータ (Designated Router) とならないように設定してください。
- 隣接する OSPF ルータどうしは、同じ MTU 値を設定してください。
- 経路情報を最大値まで保持した場合、OSPF 以外の経路情報の減少によって経路情報に空きができて、OSPF の経路は、経路情報に反映されません。
- 本装置で保有できる LSA 数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません (LSDB オーバフロー)。また、LSA 生成元のルータの停止などによって、LSA 数が本装置の上限値以下まで減少した場合、本装置の電源再投入、commit/reset コマンド実行にかかわらず、正常に通信ができるまでに最大 60 分かかることがあります。
- OSPF 使用中に commit コマンドを実行した場合、自装置が広報したすべての LSA に対して MaxAge で再広報を行ったあとに、OSPF ネットワークへの経路情報が再作成されることがあります。
- OSPF で使用するインターフェースは、以下の条件で使用してください。

インターフェース数	(30000 ÷ 本装置保有 LSA 数) 未満
通信速度	15Kbps 以上の通信帯域を確保する必要があります。



### ● 前提条件

- すべてのSi-R GでNAT機能およびDHCPクライアント機能を使用しない
- 各装置で経路情報以外の設定がされている

### ● 設定条件

#### [ルータ1でのルーティングプロトコル情報]

- lan 0でのルーティングプロトコル : OSPF
- lan 1でのルーティングプロトコル : OSPF
- lan 0でのOSPFエリアID : 0.0.0.0
- lan 1でのOSPFエリアID : 0.0.0.1
- lan 1でのルータ優先度 : 0
- エリア0.0.0.1への集約経路設定 : 10.20.0.0/16

#### [ルータ2でのルーティングプロトコル情報]

- lan 0でのルーティングプロトコル : OSPF
- lan 1でのルーティングプロトコル : OSPF
- lan 0でのOSPFエリアID : 0.0.0.1
- lan 1でのOSPFエリアID : 0.0.0.1
- lan 0でのルータ優先度 : 1
- lan 1でのpassive-interface設定 : 設定する

#### [ルータ3でのルーティングプロトコル情報]

- lan 0でのルーティングプロトコル : OSPF
- lan 1でのルーティングプロトコル : OSPF
- lan 0でのOSPFエリアID : 0.0.0.1
- lan 1でのOSPFエリアID : 0.0.0.1
- lan 0でのルータ優先度 : 255
- lan 1でのpassive-interface設定 : 設定する

#### [ルータ4でのルーティングプロトコル情報]

- lan 0でのルーティングプロトコル : OSPF
- lan 1でのルーティングプロトコル : OSPF
- lan 0でのOSPFエリアID : 0.0.0.1
- lan 1でのOSPFエリアID : 0.0.0.1
- lan 1でのpassive-interface設定 : 設定する
- lan 0でのルータ優先度 : 1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ルータ1を設定する

---

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1
# lan 1 ip ospf priority 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 range 0 10.20.0.0/16

設定終了
# save
# commit
```

## ルータ2を設定する

---

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

## ルータ3を設定する

---

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 255
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

## ルータ4を設定する

---

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 0 ip ospf priority 1
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1

設定終了
# save
# commit
```

## 2.3.1 スタブエリアを使う

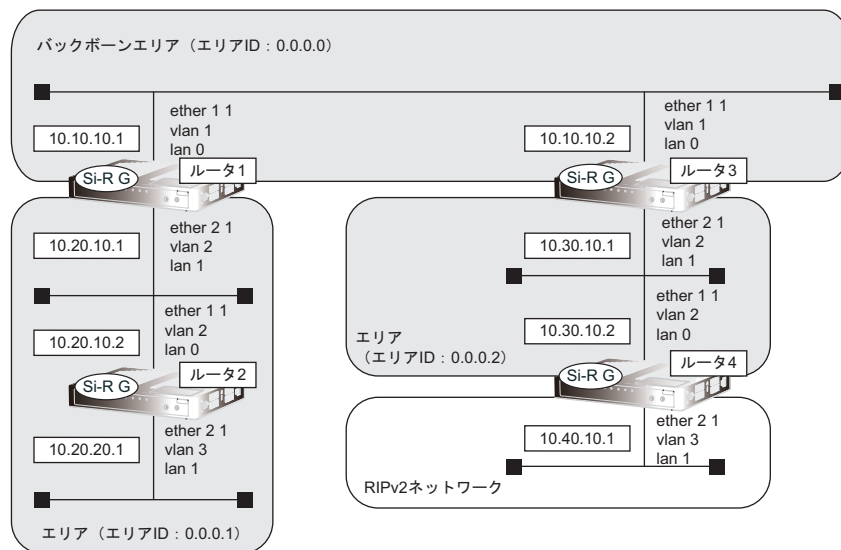
OSPF以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

OSPFは、RIPまたはBGPで受信した経路情報、スタティック経路情報およびインタフェース経路情報をOSPFネットワークに取り入れることができます。また、OSPFの経路情報をRIPおよびBGPで広報することができます。

OSPF以外のネットワークと接続する場合、スタブエリアとして運用すると、OSPFネットワーク外の経路としてデフォルトルートを使用するため、エリア内の経路情報を少なくすることができます。スタブエリアからOSPF以外のネットワークに直接接続することはできません。直接、接続する場合は、準スタブエリア (NSSA)として運用します。

### こんな事に気をつけて

OSPF以外のネットワークと接続する場合、OSPF以外のネットワークで使用するインタフェース経路情報をOSPFネットワークに取り入れるように設定する必要があります。



### ● 前提条件

- すべてのSi-R GでNAT機能およびDHCPクライアント機能を使用しない
- 各装置で経路情報以外の設定がされている

### ● 設定条件

#### [東京営業所]

#### [ルータ1でのルーティングプロトコル情報]

- lan 0でのルーティングプロトコル : OSPF
- lan 1でのルーティングプロトコル : OSPF
- lan 0でのOSPFエリアID : 0.0.0.0
- lan 1でのOSPFエリアID : 0.0.0.1
- エリアID 0.0.0.1のエリアタイプ : stub

**[ルータ2でのルーティングプロトコル情報]**

- lan 0 でのルーティングプロトコル : OSPF
- lan 1 でのルーティングプロトコル : OSPF
- lan 0 での OSPF エリア ID : 0.0.0.1
- lan 1 での OSPF エリア ID : 0.0.0.1
- エリア ID 0.0.0.1 のエリアタイプ : stub

**[ルータ3でのルーティングプロトコル情報]**

- lan 0 でのルーティングプロトコル : OSPF
- lan 1 でのルーティングプロトコル : OSPF
- lan 0 での OSPF エリア ID : 0.0.0.0
- lan 1 での OSPF エリア ID : 0.0.0.2
- エリア ID 0.0.0.2 のエリアタイプ : nssa

**[ルータ4でのルーティングプロトコル情報]**

- lan 0 でのルーティングプロトコル : OSPF
- lan 1 でのルーティングプロトコル : RIP V2,OSPF
- lan 0 での OSPF エリア ID : 0.0.0.2
- lan 1 での passive-interface 設定 : 設定する
- エリア ID 0.0.0.2 のエリアタイプ : nssa
- OSPF 経路の RIP での広報 : 再配布する
- RIP 経路の OSPF での広報 : 再配布する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ルータ1を設定する

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.1
# ospf ip area 1 type stub

設定終了
# save
# commit
```

## ルータ2を設定する

---

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 0

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.1
# ospf ip area 0 type stub

設定終了
# save
# commit
```

## ルータ3を設定する

---

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2
# ospf ip area 1 type nssa

設定終了
# save
# commit
```

## ルータ4を設定する

---

### ● コマンド

```
LAN 情報を設定する
# lan 0 ip ospf use on 0
# lan 1 ip rip use v2m v2 0 off
# lan 1 ip ospf use on 0
# lan 1 ip ospf passive on

ルーティングマネージャ情報を設定する
# routemanage ip redistrib ospf rip on
# routemanage ip redistrib rip ospf on

OSPF 情報を設定する
# ospf ip area 0 id 0.0.0.2
# ospf ip area 0 type nssa

設定終了
# save
# commit
```

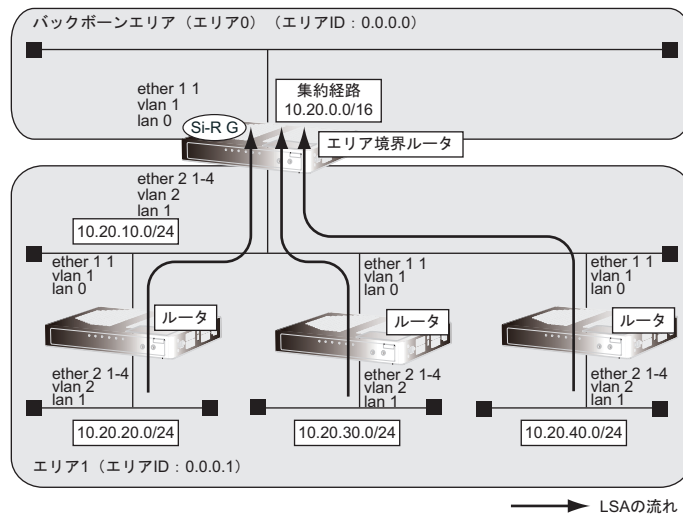


## 2.4 OSPF の経路を制御する (IPv4)

本装置で、ほかのルータから受信する経路情報 (LSA) に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

### 2.4.1 OSPF ネットワークでエリアの経路情報 (LSA) を集約する

エリア内の LSA を、本装置 (エリア境界ルータ) で集約して、バックボーンエリアへ取り込む場合の設定方法を説明します。



#### ● 前提条件

- 各装置で経路情報以外の設定がされている

#### ● 経路情報の設計

- エリア内の LSA を、本装置 (エリア境界ルータ) で集約してバックボーンエリアに取り込む

#### ● 設定条件

- lan 0 でのルーティングプロトコル : OSPF
- lan 1 でのルーティングプロトコル : OSPF
- lan 0 でのエリア ID : 0.0.0.0
- lan 1 でのエリア ID : 0.0.0.1
- バックボーンエリアへの集約経路設定 : 10.20.0.0/16

上記の経路情報に従って設定する場合のコマンド例を示します。

**● コマンド**

OSPF で使用するインタフェースを設定する

```
# lan 0 ip ospf use on 0
```

```
# lan 1 ip ospf use on 1
```

エリア情報を設定する

```
# ospf ip area 0 id 0.0.0.0
```

```
# ospf ip area 1 id 0.0.0.1
```

集約経路を設定する

```
# ospf ip area 1 range 0 10.20.0.0/16
```

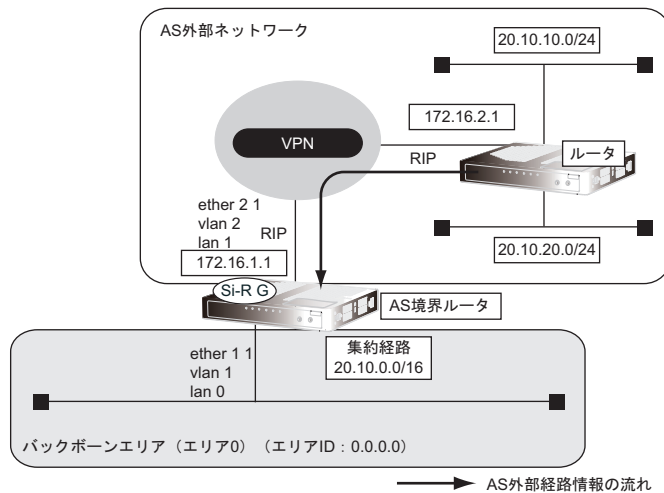
設定終了

```
# save
```

```
# commit
```

## 2.4.2 AS 外部経路を集約して OSPF ネットワークに広報する

AS 外部 (OSPF 以外) のネットワークの経路情報を本装置 (AS 境界ルータ) で集約して、バックボーンエリアに広報する場合の設定方法を説明します。



### ● 前提条件

- すべてのインタフェースに IP アドレスの設定がされている
- lan 1 インタフェースに RIPv2 を使用する設定がされている

### ● 経路情報の設計

- AS 外部経路情報を本装置 (AS 境界ルータ) で集約して OSPF ネットワーク (バックボーンエリア) に広報する

### ● 設定条件

- lan 0 でのルーティングプロトコル : OSPF
- lan 0 でのエリア ID : 0.0.0.0
- バックボーンエリアへの集約経路設定 : 20.10.0.0/16
- OSPF に再配布する RIP 経路 : 20.10.0.0/16 でマスクした結果が一致する経路だけを再配布

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

```
OSPF で使用するインタフェースを設定する
# lan 0 ip ospf use on 0

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0

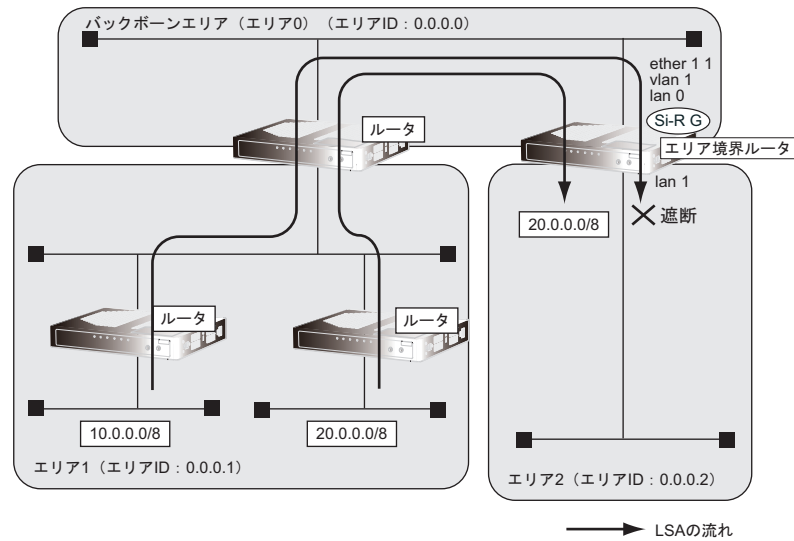
OSPF に広報する AS 外部経路を設定する
# routemanager ip redistrib ospf rip on

集約経路を設定する
# ospf ip summary 0 20.10.0.0/16

設定終了
# save
# commit
```

### 2.4.3 エリア境界ルータで不要な経路情報 (LSA) を遮断する

エリア境界ルータで、通信に使用しないTYPE3 サマリ LSA の経路情報を遮断する設定方法を説明します。



● **経路情報の設計**

- エリア 1 の 10.0.0.0/8 のネットワークとエリア 2 のネットワークでは通信を行わないため、10.0.0.0/8 の経路情報を遮断する
- その他はすべて透過させる

● **前提条件**

- OSPF 以外の lan 0 および remote 0 設定がされている

● **設定条件**

- lan 0 でのルーティングプロトコル : OSPF
- lan 1 でのルーティングプロトコル : OSPF
- lan 0 でのエリア ID : 0.0.0.0
- lan 1 でのエリア ID : 0.0.0.2
- 10.0.0.0/8 の LSA を遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

**● コマンド**

```
OSPF で使用するインタフェースを設定する
# lan 0 ip ospf use on 0
# lan 1 ip ospf use on 1

エリア情報を設定する
# ospf ip area 0 id 0.0.0.0
# ospf ip area 1 id 0.0.0.2

エリア2に注入する経路情報を制限する
# ospf ip area 1 type3-lsa 0 reject 10.0.0.0/8 in exact
# ospf ip area 1 type3-lsa 1 pass any in

設定終了
# save
# commit
```

## 2.5 OSPF 機能を使う (IPv6)

本装置で、ほかのルータから受信する経路情報 (LSA) に変更を加えることで、本装置で保有する経路情報や広報する経路情報の数を制御することができます。

### 2.5.1 OSPF ネットワークを構築する

OSPF (IPv6) を使用したネットワークの構築について説明します。

**⚠注意**

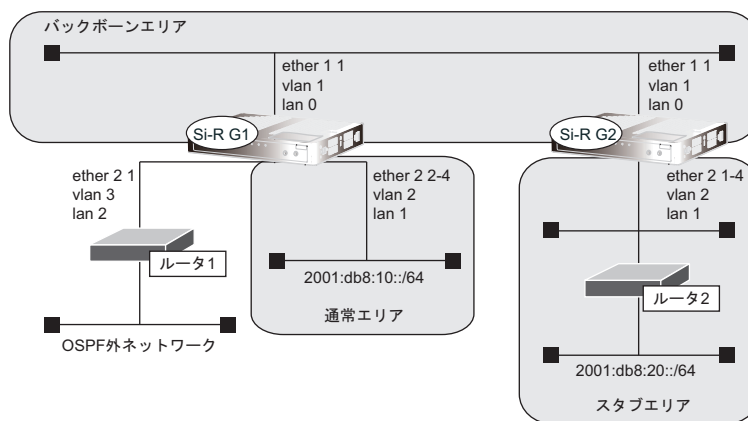
OSPF 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF 機能は使用しないでください。

**こんな事に気をつけて**

- ルータは、各エリアに30台まで設置することができます。ただし、複数のエリアの境界ルータとして使用する場合は、2つ以上のエリアの指定ルータ (DR : Designated Router) とならないように設定してください。
- LAN を使用した隣接 OSPF ルータと MTU 値が一致しない場合は、隣接関係を構築できません。
- 経路情報を最大値まで保持した場合、OSPF 以外の経路情報の減少によって経路情報に空きができて、OSPF の経路は、経路情報に反映されません。
- 本装置で保有できる LSA 数には上限値があります。この上限値を超えるネットワークで本装置を使用した場合、正しく通信することができません (LSDB オーバフロー)。また、LSA 生成元のルータの停止などによって、LSA 数が本装置の上限値以下まで減少した場合、本装置の電源再投入、commit/reset コマンドの実行にかかわらず、正常に通信ができるまでに最大60分かかることがあります。
- OSPF で使用するインターフェースは、以下の条件で使用してください。

本装置が DR を兼務する場合	本装置が DR を兼務しない場合
(10000+ 本装置保有 LSA 数) 未満	(20000+ 本装置保有 LSA 数) 未満

また、通信速度 15Kbps 以上の通信帯域を確保する必要があります。



**● 前提条件**

- 本装置1、2のすべてのインタフェースでIPv6機能を利用する設定 (lan ipv6 use on) がされている
- 本装置1のlan 1には、グローバルアドレスが設定されている
- 本装置1のlan 2には、OSPF外ネットワークへの経路がスタティック設定されている

**● 設定条件**

- 本装置1はバックボーンエリアと通常エリアのエリア境界ルータであり、かつ、OSPF外ネットワークへ到達するためのAS境界ルータとして運用する
- 本装置2はバックボーンエリアとスタブエリアのエリア境界ルータとして運用する。また、バックボーンエリアでは指定ルータとして運用する
- 各エリアIDは、以下のとおり  
バックボーンエリア                   : 0.0.0.0  
通常エリア                            : 0.0.0.1  
スタブエリア                         : 0.0.0.2

**[本装置1]**

- lan 0はバックボーンエリアに属する
- lan 1は通常エリアに属し、ほかにルータが接続されていないため、Passive-interfaceとしてOSPFパケットを送信しないようにする
- OSPFルータIDは100.0.0.1とする
- スタティック経路をOSPFに再配布する

**[本装置2]**

- lan 0はバックボーンエリアに属し、バックボーンエリアの指定ルータとするため、指定ルータ優先度に255を設定する
- lan 1はスタブエリアとする
- OSPFルータIDは100.0.0.2とする

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置1を設定する

**● コマンド**

```
LAN情報を設定する
# lan 0 ipv6 ospf use on 0
# lan 1 ipv6 ospf use on 1
# lan 1 ipv6 ospf passive on

OSPF情報を設定する
# ospf ipv6 id 100.0.0.1
# ospf ipv6 area 0 id 0.0.0.0
# ospf ipv6 area 1 id 0.0.0.1

ルーティングマネージャ情報を設定する
# routemanage ipv6 redist ospf static on

設定終了
# save
# commit
```

## 本装置 2 を設定する

---

### ● コマンド

LAN 情報を設定する

```
# lan 0 ipv6 ospf use on 0  
# lan 0 ipv6 ospf priority 255  
# lan 1 ipv6 ospf use on 1
```

OSPF 情報を設定する

```
# ospf ipv6 id 100.0.0.2  
# ospf ipv6 area 0 id 0.0.0.0  
# ospf ipv6 area 1 id 0.0.0.2  
# ospf ipv6 area 1 type stub
```

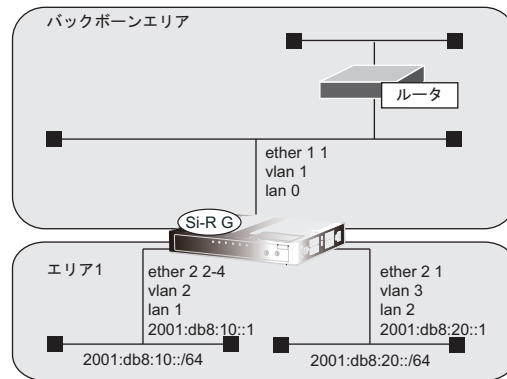
設定終了

```
# save  
# commit
```



## 2.5.2 エリア境界ルータでエリア内部経路を集約する

エリア境界ルータで、エリア内経路を集約してほかのエリアに広報する設定について説明します。



### ● 前提条件

- 本装置のすべてのインタフェースでIPv6機能を利用する設定 (lan ipv6 use on) がされている
- 本装置はバックボーンエリアとエリア1のエリア境界ルータとして運用し、lan 0、lan 1、lan 2でOSPFを使用する
- OSPFルータIDは、100.0.0.1
- 各エリアIDは、以下のとおり  
 バックボーンエリア : 0.0.0.0 (エリア定義番号0)  
 エリア1 : 0.0.0.1 (エリア定義番号1)
- 各インタフェースのIPアドレスは、以下のとおり  
 lan 1 : 2001:db8:10::1/64  
 lan 2 : 2001:db8:20::1/64

### ● 設定条件

- エリア1のエリア内部経路 (2001:db8:10::/64、2001:db8:20::/64) は、集約経路 (2001:db8::/32、コスト100) としてバックボーンエリアに広報する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置を設定する

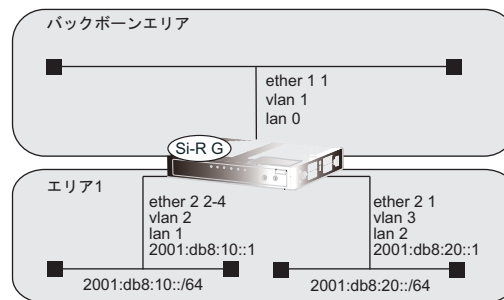
### ● コマンド

```
OSPF 情報を設定する
# ospf ipv6 area 1 range 0 2001:db8::/32 100

設定終了
# save
# commit
```

## 2.5.3 エリア境界ルータで不要な経路情報を遮断する

エリア境界ルータで、ほかのエリアに対し特定のエリア内経路（エリア間プレフィックス LSA）を遮断して広報する設定について説明します。



### ● 前提条件

- 本装置のすべてのインタフェースで IPv6 機能を利用する設定 (lan ipv6 use on) がされている
- 本装置はバックボーンエリアとエリア 1 のエリア境界ルータとして運用し、lan 0、lan 1、lan 2 で OSPF を使用する
- OSPF ルータ ID は、100.0.0.1
- 各エリア ID は、以下のとおり  
 バックボーンエリア : 0.0.0.0 (エリア定義番号 0)  
 エリア 1 : 0.0.0.1 (エリア定義番号 1)
- 各インタフェースの IP アドレスは、以下のとおり  
 lan 1 : 2001:db8:10::1/64  
 lan 2 : 2001:db8:20::1/64

### ● 設定条件

- エリア 1 からバックボーンエリアへの広報で、2001:db8:20::/64 は破棄し、その他のエリア内部経路は透過させる

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置を設定する

### ● コマンド

```
OSPF 情報を設定する
# ospf ipv6 area 1 inter-area-prefix 0 reject 2001:db8:20::/64 out
# ospf ipv6 area 1 inter-area-prefix 1 pass any out

設定終了
# save
# commit
```

## 2.6 BGP の経路を制御する (IPv4)

本装置を経由して、ほかのルータに送受信する経路情報に変更を加えることで、意図的にトラフィックを制御することができます。

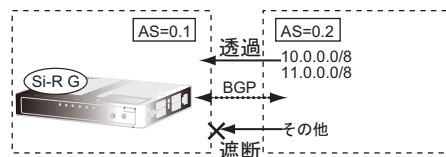
☛ 参照 マニュアル「機能説明書」

### こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- 送信時のフィルタを設定した場合、相手装置に広報する MED メトリック値、AS パスプリペンドはフィルタの設定値が使用されます。
- MED メトリック値の設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- AS パスプリペンドの設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- BGP 使用中に commit コマンドを実行した場合、接続中のセッションが一度切断されることがあります。
- 動的定義反映で BGP IPv4 フィルタを設定した場合、動的定義反映後に送受信する経路情報に対してフィルタリングを実施します。動的定義反映前に送受信した経路情報に対してフィルタリングを実施する場合は、BGP IPv4 セッションのクリア機能を使用してください。

### 2.6.1 特定の経路情報の受信を透過させる

通信が必要なネットワークに限定して経路を透過させる場合の設定方法を説明します。



#### ● 経路情報の設計

- 10.0.0.0/8 のネットワークの経路情報を透過
- 11.0.0.0/8 のネットワークの経路情報を透過
- その他はすべてを遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

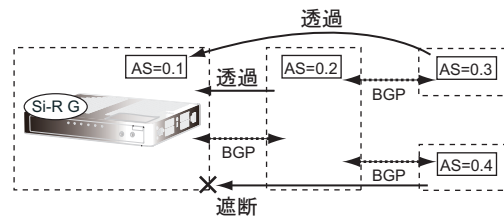
**● コマンド**

```
フィルタリング条件を設定する
# bgp neighbor 0 ip filter 0 act pass in
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 1 act pass in
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 2 act reject in
# bgp neighbor 0 ip filter 2 route any
```

```
設定終了
# save
# commit
```

## 2.6.2 特定のASからの経路情報の受信を遮断する

特定の経路情報を遮断する場合の設定方法を説明します。



### ● 経路情報の設計

- AS0.4からの経路情報を遮断
- その他はすべて透過

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

```

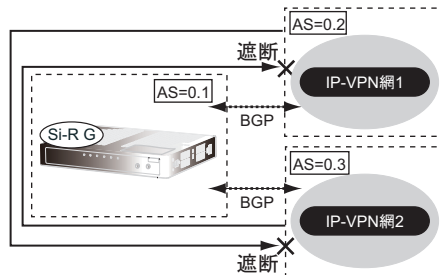
フィルタリング条件を設定する
# bgp neighbor 0 ip filter 0 act reject in
# bgp neighbor 0 ip filter 0 as 0.4
# bgp neighbor 0 ip filter 1 act pass in
# bgp neighbor 0 ip filter 1 route any
    
```

```

設定終了
# save
# commit
    
```

## 2.6.3 IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する

異なる IP-VPN 網を使用し、冗長化ネットワークを構成する場合、IP-VPN 網 1 から受信した経路情報の IP-VPN 網 2 への送信を遮断、および IP-VPN 網 2 から受信した経路情報の IP-VPN 網 1 への送信を遮断する場合の設定方法を説明します。



### ● 経路情報の設計

- AS0.2 から AS0.3 への経路情報を遮断
- AS0.3 から AS0.2 への経路情報を遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

フィルタリング条件を設定する

IP-VPN 網 1 への送信を遮断する

```
# bgp neighbor 0 ip filter 0 act reject out
# bgp neighbor 0 ip filter 0 as 0.3
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route any
```

IP-VPN 網 2 への送信を遮断する

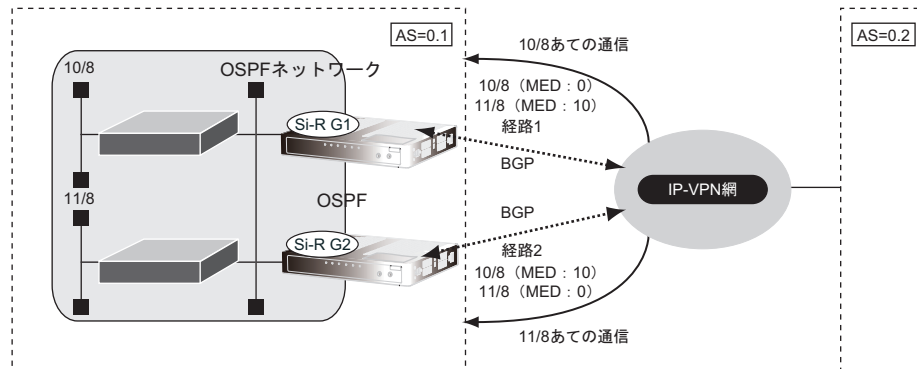
```
# bgp neighbor 1 ip filter 0 act reject out
# bgp neighbor 1 ip filter 0 as 0.2
# bgp neighbor 1 ip filter 1 act pass out
# bgp neighbor 1 ip filter 1 route any
```

設定終了

```
# save
# commit
```

## 2.6.4 冗長構成の通信経路を使用する

IP-VPN 網に接続する経路を2つ使用した冗長構成で、通信の負荷分散および通信網異常による経路切り替えを行う場合の設定方法を説明します。



### ● 経路情報の設計

- OSPF ネットワークである AS0.1 で IP-VPN 網を経由した AS0.2 への通信経路を冗長化する
- 10/8 への通信は経路 1 を優先経路とし、11/8 への通信経路は経路 2 を優先経路とする。それぞれの経路で異常が発生した場合、異常が発生していない経路に切り替わる。優先順位を設定するときは MED メトリック値を使用する
- AS0.1 内の OSPF ネットワークでの経路変更は BGP で AS0.2 に広報する

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

#### [本装置 1]

```

経路情報に MED メトリック値を付加する
# bgp neighbor 0 ip filter 0 act pass out
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 0 set medmetric 0
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 1 set medmetric 10
    
```

```

その他のすべての経路は透過する
# bgp neighbor 0 ip filter 2 act pass out
# bgp neighbor 0 ip filter 2 route any
    
```

```

BGP で OSPF 経路を広報する
# routemanage ip redistrib bgp ospf on
    
```

```

設定終了
# save
# commit
    
```

**[本装置2]**

```
経路情報にMED メトリック値を付加する
# bgp neighbor 0 ip filter 0 act pass out
# bgp neighbor 0 ip filter 0 route 10.0.0.0/8
# bgp neighbor 0 ip filter 0 set medmetric 10
# bgp neighbor 0 ip filter 1 act pass out
# bgp neighbor 0 ip filter 1 route 11.0.0.0/8
# bgp neighbor 0 ip filter 1 set medmetric 0
```

```
その他のすべての経路は透過する
# bgp neighbor 0 ip filter 2 act pass out
# bgp neighbor 0 ip filter 2 route any
```

```
BGP で OSPF 経路を広報する
# routemanage ip redist bgp ospf on
```

```
設定終了
# save
# commit
```



## 2.7 BGP機能を使う (IPv6)

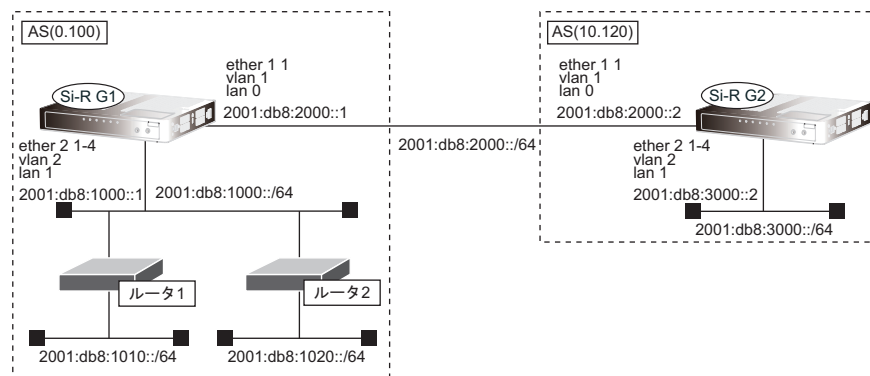
本装置を経由して、ほかのルータに送受信する経路情報に変更を加えることで、意図的にトラフィックを制御することができます。

### こんな事に気をつけて

- すべてのフィルタリング条件に一致しない経路情報は破棄されます。
- 送信時のフィルタを設定した場合、相手装置に広報するMEDメトリック値、ASパスプリペンドはフィルタの設定値が使用されます。
- MEDメトリック値の設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- ASパスプリペンドの設定は、送信時のフィルタでだけ有効となります。受信時のフィルタでは、無効となります。
- BGP使用中にcommitコマンドを実行した場合、接続中のセッションが一度切断されることがあります。
- 動的定義反映でBGP IPv6 フィルタを設定した場合、動的定義反映後に送受信する経路情報に対してフィルタリングを実施します。動的定義反映前に送受信した経路情報に対してフィルタリングを実施する場合は、BGP IPv6 セッションのクリア機能を使用してください。

### 2.7.1 BGPでIPv6経路情報を交換する

BGPを使用したIPv6経路情報の交換について説明します。



#### ● 前提条件

- 本装置1、2間でEBGPを使用し、IPv6経路情報の交換を行う
- 本装置1のlan 0には、2001:db8:2000::1/64のアドレスが設定されている
- 本装置1のlan 1には、2001:db8:1000::1/64のアドレスが設定されている
- 本装置1のlan 1側では、RIP (IPv6) による経路交換が行われている
- 本装置2のlan 0には、2001:db8:2000::2/64のアドレスが設定されている
- 本装置2のlan 1には、2001:db8:3000::2/64のアドレスが設定されている

## ● 設定条件

### [本装置 1]

- RIP (IPv6) 経路情報を BGP で再配布
- BGP (IPv6) 経路情報を RIP で再配布
- AS 番号 (0.100) に属している
- BGP-ID は、1.0.0.0

### [本装置 2]

- AS 番号 (10.120) に属している
- BGP-ID は、2.0.0.0
- BGP ネットワークを使用し、lan 1 のインタフェース経路を BGP で広報

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置 1 を設定する

### ● コマンド

```
ルーティングマネージャ情報を設定する
# routemanage ipv6 redist rip bgp on
# routemanage ipv6 redist bgp rip on

BGP 情報を設定する
# bgp as 0.100
# bgp id 1.0.0.0
# bgp neighbor 0 address 2001:db8:2000::2
# bgp neighbor 0 as 10.120
# bgp neighbor 0 family ipv6
# bgp neighbor 0 source 2001:db8:2000::1

設定終了
# save
# commit
```

## 本装置 2 を設定する

### ● コマンド

```
BGP 情報を設定する
# bgp as 10.120
# bgp id 2.0.0.0
# bgp ipv6 network route 0 2001:db8:3000::/64
# bgp ipv6 network igp on
# bgp neighbor 0 address 2001:db8:2000::1
# bgp neighbor 0 as 0.100
# bgp neighbor 0 family ipv6
# bgp neighbor 0 source 2001:db8:2000::2

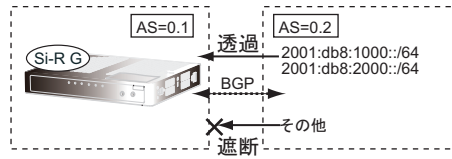
設定終了
# save
# commit
```

### こんな事に気をつけて

IPv6 で BGP を使用する場合は、BGP 自側 IP アドレスを必ず設定してください。

## 2.7.2 特定の経路情報の受信を透過させる

通信が必要なネットワークに限定して経路を透過させる場合の設定方法を説明します。



### ● 経路情報の設計

- 2001:db8:1000::/64のネットワークの経路情報を透過
- 2001:db8:2000::/64のネットワークの経路情報を透過
- その他はすべてを遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

```

フィルタリング条件を設定する
# bgp neighbor 0 ipv6 filter 0 act pass in
# bgp neighbor 0 ipv6 filter 0 route 2001:db8:1000::/64
# bgp neighbor 0 ipv6 filter 1 act pass in
# bgp neighbor 0 ipv6 filter 1 route 2001:db8:2000::/64
# bgp neighbor 0 ipv6 filter 2 act reject in
# bgp neighbor 0 ipv6 filter 2 route any

```

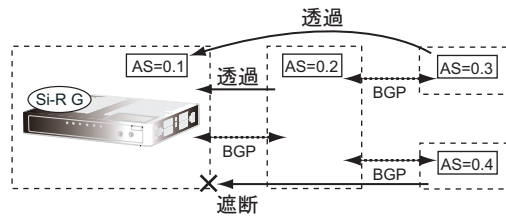
```

設定終了
# save
# commit

```

## 2.7.3 特定のASからの経路情報の受信を遮断する

フルルートを受信するネットワーク（トランジット）に接続されている場合、特定の経路情報を遮断する場合の設定方法を説明します。



### ● 経路情報の設計

- AS0.4からの経路情報を遮断
- その他はすべて透過

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

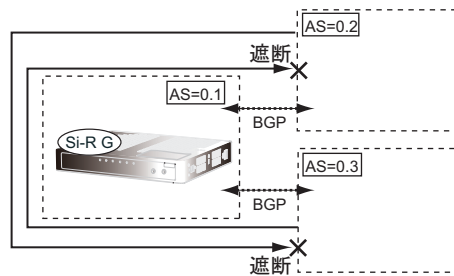
```

フィルタリング条件を設定する
# bgp neighbor 0 ipv6 filter 0 act reject in
# bgp neighbor 0 ipv6 filter 0 as 0.4
# bgp neighbor 0 ipv6 filter 1 act pass in
# bgp neighbor 0 ipv6 filter 1 route any

設定終了
# save
# commit
    
```

## 2.7.4 特定のASから受信した経路情報の送信を遮断する

本装置でAS0.2とAS0.3の通信を中継しないようにする設定方法を説明します。



### ● 経路情報の設計

- AS0.2からAS0.3への経路情報を遮断
- AS0.3からAS0.2への経路情報を遮断

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

フィルタリング条件を設定する

AS0.2への送信を遮断する

```
# bgp neighbor 0 ipv6 filter 0 act reject out
# bgp neighbor 0 ipv6 filter 0 as 0.3
# bgp neighbor 0 ipv6 filter 1 act pass out
# bgp neighbor 0 ipv6 filter 1 route any
```

AS0.3への送信を遮断する

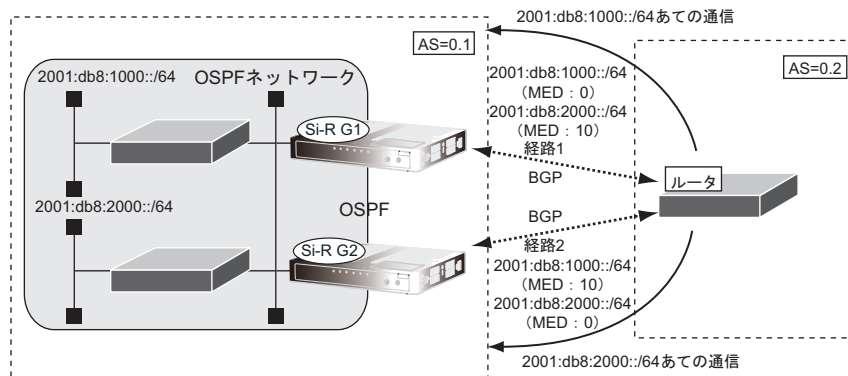
```
# bgp neighbor 1 ipv6 filter 0 act reject out
# bgp neighbor 1 ipv6 filter 0 as 0.2
# bgp neighbor 1 ipv6 filter 1 act pass out
# bgp neighbor 1 ipv6 filter 1 route any
```

設定終了

```
# save
# commit
```

## 2.7.5 冗長構成の通信経路を使用する

ルータに接続する経路を2つ使用した冗長構成で、通信の負荷分散および通信網異常による経路切り替えを行う場合の設定方法を説明します。



### ● 経路情報の設計

- OSPF ネットワークである AS0.1 でルータを経由した AS0.2 への通信経路を冗長化する
- 2001:db8:1000::/64 への通信は経路1を優先経路とし、2001:db8:2000::/64 への通信経路は経路2を優先経路とする。それぞれの経路で異常が発生した場合、異常が発生していない経路に切り替わる。優先順位を設定するときはMEDメトリック値を使用する
- AS0.1内のOSPFネットワークでの経路変更はBGPでAS0.2に広報する

上記の経路情報に従って設定する場合のコマンド例を示します。

### ● コマンド

#### [本装置1]

```

経路情報にMEDメトリック値を付加する
# bgp neighbor 0 ipv6 filter 0 act pass out
# bgp neighbor 0 ipv6 filter 0 route 2001:db8:1000::/64
# bgp neighbor 0 ipv6 filter 0 set medmetric 0
# bgp neighbor 0 ipv6 filter 1 act pass out
# bgp neighbor 0 ipv6 filter 1 route 2001:db8:2000::/64
# bgp neighbor 0 ipv6 filter 1 set medmetric 10

その他のすべての経路は透過する
# bgp neighbor 0 ipv6 filter 2 act pass out
# bgp neighbor 0 ipv6 filter 2 route any

BGPでOSPF経路を広報する
# routemanage ipv6 redist bgp ospf on

設定終了
# save
# commit
    
```

**[本装置2]**

```
経路情報にMED メトリック値を付加する
# bgp neighbor 0 ipv6 filter 0 act pass out
# bgp neighbor 0 ipv6 filter 0 route 2001:db8:1000::/64
# bgp neighbor 0 ipv6 filter 0 set medmetric 10
# bgp neighbor 0 ipv6 filter 1 act pass out
# bgp neighbor 0 ipv6 filter 1 route 2001:db8:2000::/64
# bgp neighbor 0 ipv6 filter 1 set medmetric 0
```

```
その他のすべての経路は透過する
# bgp neighbor 0 ipv6 filter 2 act pass out
# bgp neighbor 0 ipv6 filter 2 route any
```

```
BGP で OSPF 経路を広報する
# routemanage ipv6 redist bgp ospf on
```

```
設定終了
# save
# commit
```

## 2.8 マルチキャスト機能を使う

本装置には、マルチキャスト機能を動作させるために以下の2種類のプロトコルがあります。

- PIM-DMプロトコル
- PIM-SMプロトコル

また、本装置では、ルーティングプロトコルは使用しないで、スタティックにマルチキャスト経路を設定することもできます。

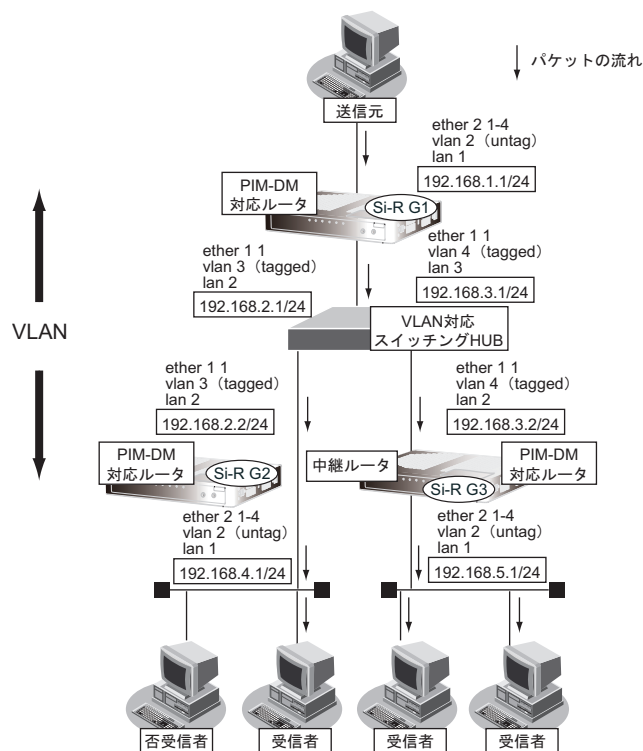
☛ 参照 マニュアル「機能説明書」

### 2.8.1 マルチキャスト機能 (PIM-DM) を使う

マルチキャスト機能 (PIM-DM) を使用すると、会社などのLAN内で、動画や音声などを配送することができます。

こんな事に気をつけて

- マルチキャストでパケットを配送するルータは、すべてPIM-DMに対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- IPアドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側IPアドレスと相手側IPアドレスの両方を正しく設定する必要があります。





ここでは、PIM-DMを利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。

### ● 設定条件

- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける  
VLAN ID : 3                                      ネットワークアドレス : 192.168.2.0/24  
VLAN ID : 4                                      ネットワークアドレス : 192.168.3.0/24
- マルチキャスト・ルーティングプロトコルにはPIM-DMを利用する

#### [本装置 1]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける  
lan 1    : 192.168.1.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1~4  
lan 2    : 192.168.2.1/24、VLAN ID 3 (タグあり)、ETHERグループ1ポート1  
lan 3    : 192.168.3.1/24、VLAN ID 4 (タグあり)、ETHERグループ1ポート1
- ユニキャストのルーティングテーブルの作成にRIPを使用する

#### [本装置 2]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける  
lan 1    : 192.168.4.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1~4  
lan 2    : 192.168.2.2/24、VLAN ID 3 (タグあり)、ETHERグループ1ポート1
- ユニキャストのルーティングテーブルの作成にRIPを使用する

#### [本装置 3]

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける  
lan 1    : 192.168.5.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1~4  
lan 2    : 192.168.3.2/24、VLAN ID 4 (タグあり)、ETHERグループ1ポート1
- ユニキャストのルーティングテーブルの作成にRIPを使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド****[本装置1]**

```
ETHER ポート情報を設定する
# ether 1 1 vlan tag 3,4
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip multicast mode pimdm
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan 3

lan 3 情報を設定する
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimdm
# lan 3 vlan 4

設定終了
# save
# commit
```

**[本装置2]**

```
ether ポートを設定する
# ether 1 1 vlan tag 3
# ether 2 1-4 vlan untag 2

lan 設定を削除する
# delete lan

lan 1 を設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode pimdm
# lan 1 vlan 2

lan 2 を設定する
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimdm
# lan 2 vlan 3

設定終了
# save
# commit
```

**[本装置3]**

ETHER ポート情報を設定する

```
# ether 1 1 vlan tag 4
```

```
# ether 2 1-4 vlan untag 2
```

lan 情報を削除する

```
# delete lan
```

lan 1 情報を設定する

```
# lan 1 ip address 192.168.5.1/24 3
```

```
# lan 1 ip multicast mode pimdm
```

```
# lan 1 vlan 2
```

lan 2 情報を設定する

```
# lan 2 ip address 192.168.3.2/24 3
```

```
# lan 2 ip rip use v2 v2 0 on
```

```
# lan 2 ip multicast mode pimdm
```

```
# lan 2 vlan 4
```

設定終了

```
# save
```

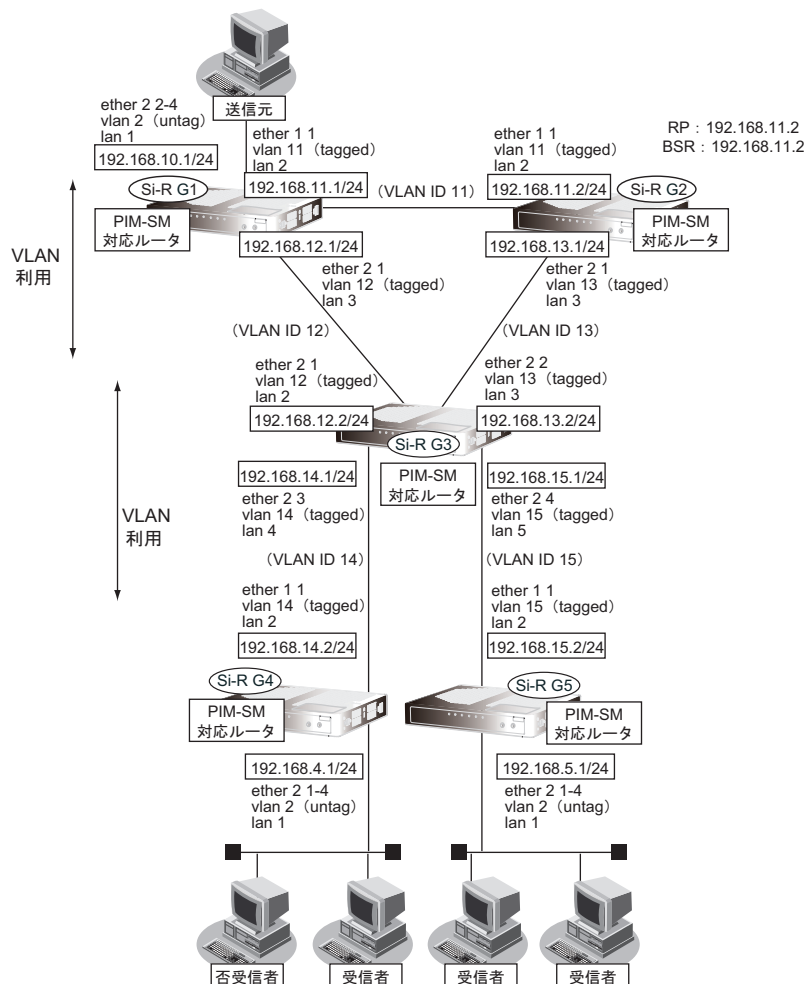
```
# commit
```

## 2.8.2 マルチキャスト機能 (PIM-SM) を使う

マルチキャスト機能 (PIM-SM) を使用すると、インターネットなど、十分な帯域を保証されないネットワーク上で、マルチキャスト・パケットを配送することができます。

### こんな事に気をつけて

- マルチキャスト・パケットを配送するルータは、すべて PIM-SM に対応している必要があります。また、ルータ上ではユニキャストのルーティングテーブルが作成されている必要があります。
- IP アドレスが設定されていないインタフェース上ではマルチキャストを利用することはできません。また、リモートインタフェース上でマルチキャストを動作させる場合は、自側 IP アドレスと相手側 IP アドレスの両方を正しく設定する必要があります。
- ネットワーク内に BSR (Bootstrap Router : ブートストラップルータ) として動作するルータを 1 台以上置く必要があります。BSR は RP (Rendezvous Point : ランデブーポイント) の情報を広報します。
- ネットワーク内に RP として動作するルータを 1 台以上置く必要があります。パケットの配送は、RP を配送樹の頂点として開始され、その後、最短経路 (SPT : Shortest Path Tree) に切り替わります。
- PIM-SM ではマルチキャスト・パケットの配送を、RP を配送樹の頂点として開始するため、RP はネットワークの中心付近に置くことをお勧めします。
- SPT への切り替えは、マルチキャスト・パケットの受信者の直前のルータ (lasthop router) が行います。lasthop router で設定することで SPT への切り替えを無効にすることができます。



ここでは、PIM-SMを利用してマルチキャスト・パケットを転送する場合の設定方法を説明します。

この設定例では、VLANを利用して、上図のネットワークを仮想的に構築します。

マルチキャスト・パケットは、はじめはRPである本装置2を経由して、本装置1→本装置2→本装置3→本装置4の順に配送されます（一度、本装置1から本装置2に送られ、本装置2を配送樹の頂点として配送されます）。本装置4へのパケット転送開始直後に、本装置4はSPTへの切り替えを開始します。切り替えが行われると、本装置1→本装置3→本装置4のように、最短経路を利用して配送されます（本装置1を配送樹の頂点として配送されます）。同様の切り替えが本装置5でも行われます。

### ● 設定条件

- VLAN IDとネットワークアドレスを以下のように対応付ける
 

VLAN ID : 11	ネットワークアドレス : 192.168.11.0/24
VLAN ID : 12	ネットワークアドレス : 192.168.12.0/24
VLAN ID : 13	ネットワークアドレス : 192.168.13.0/24
VLAN ID : 14	ネットワークアドレス : 192.168.14.0/24
VLAN ID : 15	ネットワークアドレス : 192.168.15.0/24
- マルチキャスト・ルーティングプロトコルには PIM-SM を利用する  
ユニキャストのルーティングテーブルの作成に RIP を使用する
 

RP	: 本装置2 (192.168.11.2)
BSR	: 本装置2 (192.168.11.2)
- SPTへの切り替えを行う（初期値）

#### 【本装置1】

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
 

lan 1	: 192.168.10.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート2～4
lan 2	: 192.168.11.1/24、VLAN ID 11 (タグあり)、ETHERグループ1ポート1
lan 3	: 192.168.12.1/24、VLAN ID 12 (タグあり)、ETHERグループ2ポート1

#### 【本装置2】

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
 

lan 2	: 192.168.11.2/24、VLAN ID 11 (タグあり)、ETHERグループ1ポート1
lan 3	: 192.168.13.1/24、VLAN ID 13 (タグあり)、ETHERグループ2ポート1
- RP : 192.168.11.2
- BSR : 192.168.11.2

#### 【本装置3】

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
 

lan 2	: 192.168.12.2/24、VLAN ID 12 (タグあり)、ETHERグループ2ポート1
lan 3	: 192.168.13.2/24、VLAN ID 13 (タグあり)、ETHERグループ2ポート2
lan 4	: 192.168.14.1/24、VLAN ID 14 (タグあり)、ETHERグループ2ポート3
lan 5	: 192.168.15.1/24、VLAN ID 15 (タグあり)、ETHERグループ2ポート4

#### 【本装置4】

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
 

lan 1	: 192.168.4.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1～4
lan 2	: 192.168.14.2/24、VLAN ID 14 (タグあり)、ETHERグループ1ポート1

#### 【本装置5】

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
 

lan 1	: 192.168.5.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1～4
lan 2	: 192.168.15.2/24、VLAN ID 15 (タグあり)、ETHERグループ1ポート1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

### [本装置1]

```
ETHER ポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 11
# ether 2 1 vlan tag 12
# ether 2 2-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.10.1/24 3
# lan 1 ip multicast mode pimsm
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.11.1/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 11

lan 3 情報を設定する
# lan 3 ip address 192.168.12.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan 12

設定終了
# save
# commit
```

**[本装置2]**

```
ETHER ポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 11
# ether 2 1 vlan tag 13

lan 情報を削除する
# delete lan

lan 2 情報を設定する
# lan 2 ip address 192.168.11.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 11

lan 3 情報を設定する
# lan 3 ip address 192.168.13.1/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan 13

マルチキャスト情報を設定する
# multicast ip pimsm candrp mode on
# multicast ip pimsm candrp address 192.168.11.2
# multicast ip pimsm candbsr mode on
# multicast ip pimsm candbsr address 192.168.11.2

設定終了
# save
# commit
```

**[本装置3]**

```
ETHER ポート情報を設定する
# delete ether 2 1-4 vlan untag

# ether 2 1 vlan tag 12
# ether 2 2 vlan tag 13
# ether 2 3 vlan tag 14
# ether 2 4 vlan tag 15

lan 情報を削除する
# delete lan

lan 2 情報を設定する
# lan 2 ip address 192.168.12.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 12

lan 3 情報を設定する
# lan 3 ip address 192.168.13.2/24 3
# lan 3 ip rip use v2 v2 0 on
# lan 3 ip multicast mode pimsm
# lan 3 vlan 13

lan 4 情報を設定する
# lan 4 ip address 192.168.14.1/24 3
# lan 4 ip rip use v2 v2 0 on
# lan 4 ip multicast mode pimsm
# lan 4 vlan 14

lan 5 情報を設定する
# lan 5 ip address 192.168.15.1/24 3
# lan 5 ip rip use v2 v2 0 on
# lan 5 ip multicast mode pimsm
# lan 5 vlan 15

設定終了
# save
# commit
```



**[本装置4]**

```
ETHER ポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 14
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode pimsm
# lan 1 vlan 2

lan 2 を情報設定する
# lan 2 ip address 192.168.14.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 14

設定終了
# save
# commit
```

**[本装置5]**

```
ETHER ポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 15
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode pimsm
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.15.2/24 3
# lan 2 ip rip use v2 v2 0 on
# lan 2 ip multicast mode pimsm
# lan 2 vlan 15

設定終了
# save
# commit
```

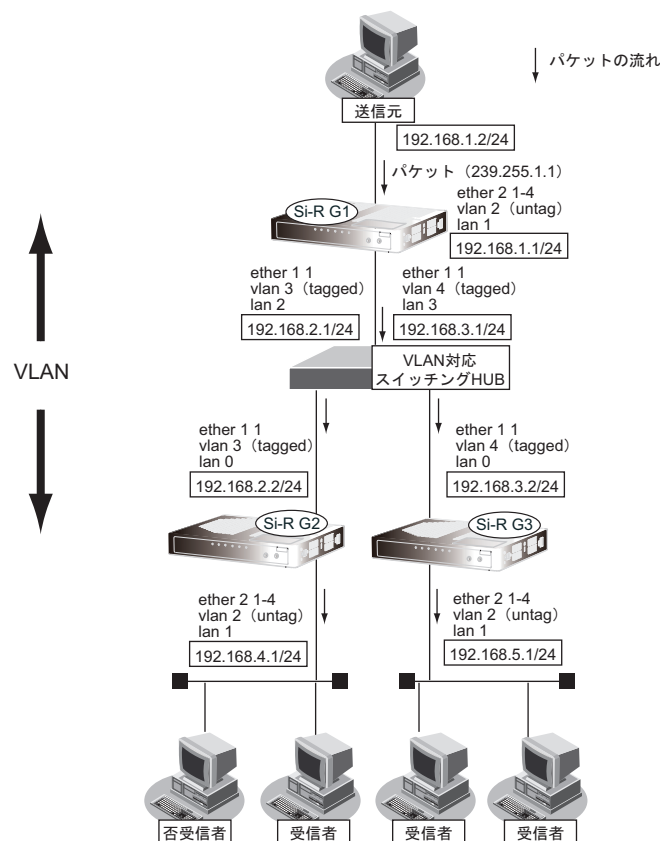
## 2.8.3 マルチキャスト機能（スタティックルーティング）を使う

マルチキャスト機能（スタティックルーティング）を利用すると、マルチキャストパケットが配送される経路を静的に設定することができます。

### こんな事に気をつけて

マルチキャスト・スタティックルーティングでは、入力インターフェイスでのIGMPグループ参加を指定することができます。

上流側にPIM-DMなどのIGMP参加要求を受け付けるマルチキャスト・ルータが存在する場合は、入力インターフェイスでIGMPグループ参加を行うこと、パケットを強制的に転送させることができます。



ここでは、スタティックルーティングを利用してマルチキャストパケットの転送を行う場合を例に説明します。

### ● 設定条件

- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける  
VLAN ID：3                                      ネットワークアドレス：192.168.2.0/24  
VLAN ID：4                                      ネットワークアドレス：192.168.3.0/24
- マルチキャスト・スタティックルーティングを利用する
- マルチキャストパケットの送信元アドレスは 192.168.1.2 とする
- マルチキャストパケットのグループアドレスは 239.255.1.1 とする
- 入力インターフェイスでのIGMPグループ参加は行わない

**[本装置1]**

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  - lan 1 : 192.168.1.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1~4
  - lan 2 : 192.168.2.1/24、VLAN ID 3 (タグあり)、ETHERグループ1ポート1
  - lan 3 : 192.168.3.1/24、VLAN ID 4 (タグあり)、ETHERグループ1ポート1

**[本装置2]**

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  - lan 1 : 192.168.4.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1~4
  - lan 2 : 192.168.2.2/24、VLAN ID 3 (タグあり)、ETHERグループ1ポート1

**[本装置3]**

- lan、IPアドレス、VLAN ID、ETHERポートを以下のように対応付ける
  - lan 1 : 192.168.5.1/24、VLAN ID 2 (タグなし)、ETHERグループ2ポート1~4
  - lan 2 : 192.168.3.2/24、VLAN ID 3 (タグあり)、ETHERグループ1ポート1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド****[本装置1]**

```
ETHERポート情報を設定する
# delete ether 1 1 vlan untag

# ether 1 1 vlan tag 3,4
# ether 2 1-4 vlan untag 2

lan情報を削除する
# delete lan

lan 1情報を設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip multicast mode static
# lan 1 vlan 2

lan 2情報を設定する
# lan 2 ip address 192.168.2.1/24 3
# lan 2 ip multicast mode static
# lan 2 vlan 3

lan 3情報を設定する
# lan 3 ip address 192.168.3.1/24 3
# lan 3 ip multicast mode static
# lan 3 vlan 4

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan1 lan2-lan3 off

設定終了
# save
# commit
```

**[本装置2]**

```
ETHER ポート情報を設定する
# ether 1 1 vlan tag 3
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.4.1/24 3
# lan 1 ip multicast mode static
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.2.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan 3

マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

**[本装置3]**

```
ETHER ポート情報を設定する
# ether 1 1 vlan tag 4
# ether 2 1-4 vlan untag 2

lan 情報を削除する
# delete lan

lan 1 情報を設定する
# lan 1 ip address 192.168.5.1/24 3
# lan 1 ip multicast mode static
# lan 1 vlan 2

lan 2 情報を設定する
# lan 2 ip address 192.168.3.2/24 3
# lan 2 ip multicast mode static
# lan 2 vlan 4

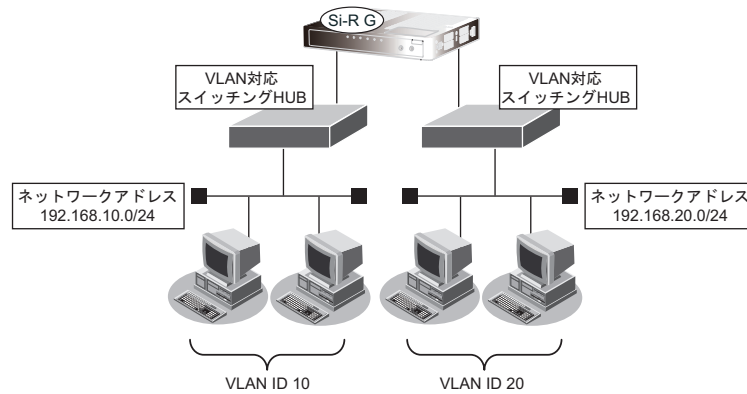
マルチキャスト・スタティックルーティングの設定をする
# multicast ip route 0 192.168.1.2 239.255.1.1 lan2 lan1

設定終了
# save
# commit
```

## 2.9 VLAN機能を使う

### 2.9.1 ポートVLAN機能を使う

ここでは、ポート単位でグループ化したタグなしパケットをポートVLANで送受信する場合の設定方法を説明します。



#### ● 設定条件

- ETHERグループ2ポート1、4を使用する
- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける  
 VLAN ID : 10                      ネットワークアドレス : 192.168.10.0/24  
 VLAN ID : 20                      ネットワークアドレス : 192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

#### ● コマンド

```
ETHERグループ2ポート1を設定する
# ether 2 1 vlan untag 10

ETHERグループ2ポート4を設定する
# ether 2 4 vlan untag 20

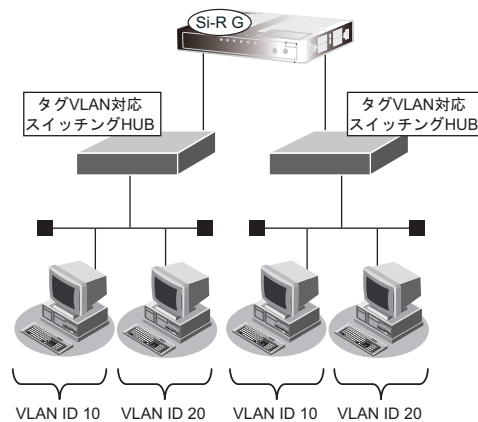
192.168.10.1/24のネットワークを設定する
# delete lan 0
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

192.168.20.1/24のネットワークを設定する
# delete lan 1
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

## 2.9.2 タグVLAN機能を使う

ここでは、1つのポートで、2つのVLANからのタグ付きパケットを、それぞれのVLANで送受信する場合の設定方法を説明します。



### ● 設定条件

- ETHERグループ2ポート1、4を使用する
- VLAN対応スイッチングHUBでVLAN IDとネットワークアドレスを以下のように対応付ける  
 VLAN ID : 10                      ネットワークアドレス : 192.168.10.0/24  
 VLAN ID : 20                      ネットワークアドレス : 192.168.20.0/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
ETHERグループ2ポート1を設定する
# ether 2 1 vlan tag 10,20

ETHERグループ2ポート4を設定する
# ether 2 4 vlan tag 10,20

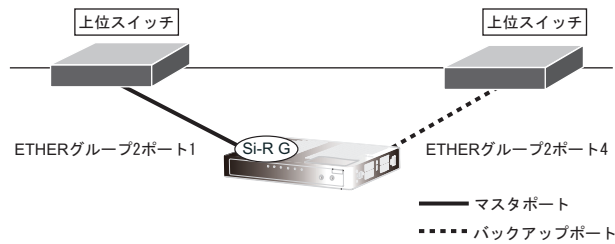
192.168.10.1/24のネットワークを設定する
# delete lan 0
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 10

192.168.20.1/24のネットワークを設定する
# delete lan 1
# lan 1 ip address 192.168.20.1/24 3
# lan 1 vlan 20

設定終了
# save
# commit
```

## 2.10 バックアップポート機能を使う

ここでは、ETHERグループ2をバックアップポートとして利用する場合の設定方法について説明します。アップリンクポートをそれぞれ異なるスイッチに接続することで、冗長アップリンクの形態にできます。



### ● 設定条件

- ETHERグループ2ポート1、4をバックアップポートとして使用する  
(ETHERグループ2ポート1をマスターポート、ETHERグループ2ポート4をバックアップポートとする)
- マスターポートを優先的に使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

#### [本装置1]

```
ETHERグループ2ポート1をバックアップポート (グループ1) のマスターポートに設定する
# ether 2 1 type backup 1 master

ETHERグループ2ポート4をバックアップポート (グループ1) のバックアップポートに設定する
# ether 2 4 type backup 1 backup

バックアップグループ1をマスターポート優先モードに設定する
# backup 1 mode master

設定終了
# save
# commit
```

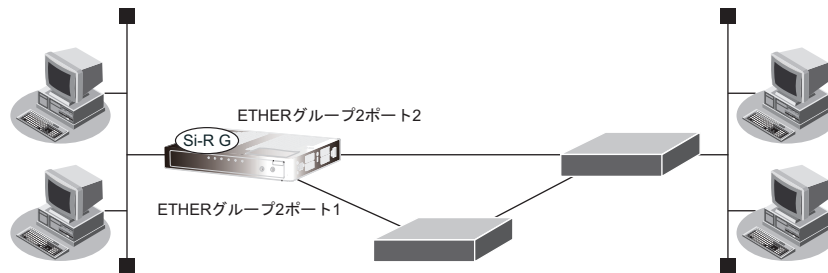
## 2.11 STP 機能を使う

ここでは、STP 機能を使用する場合の設定方法を説明します。

### 2.11.1 STP を使う

STP を使用すると、物理的にループしているネットワークでも、論理的にループしないようにすることができます。これによって、ネットワーク内のデータを円滑に流すことができます。

☞ 参照 マニュアル「機能説明書」



#### ● 設定条件

- STP を使用する
- ETHERグループ2ポート1、ポート2をVID 10のポートVLANとする

上記の設定条件に従って設定を行う場合のコマンド例を示します。

#### ● コマンド

```
VLAN を設定する
# ether 2 1 vlan untag 10
# ether 2 2 vlan untag 10

STP を設定する
# stp mode stp
# ether 2 1 stp use on
# ether 2 2 stp use on

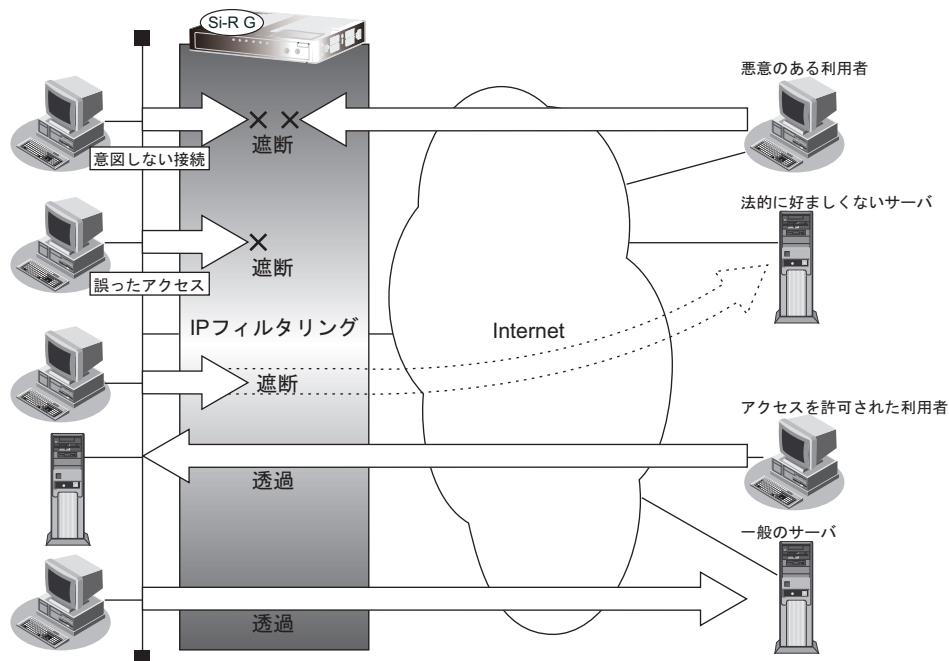
設定終了
# save
# commit
```



## 2.12 IPフィルタリング機能を使う

本装置を経由してインターネットに送出されるパケット、またはインターネットから受信したパケットをIPアドレスとポート番号の組み合わせで制御することによって、ネットワークのセキュリティを向上させたり、回線への超過課金を防止することができます。

☞ 参照 マニュアル「機能説明書」



### IPフィルタリングの条件

本装置では、以下の条件を指定することによって、データの流れを制御できます。

- 動作
- プロトコル
- 送信元情報 (IPアドレス/アドレスマスク/ポート番号)
- あて先情報 (IPアドレス/アドレスマスク/ポート番号)
- TCP接続要求
- TOS値
- 方向

💡 ヒント

◆ TCP 接続要求とは

TCP プロトコルでのコネクション確立要求を、フィルタリングの対象にするかどうか指定するものです。フィルタリングの動作に透過、プロトコルに TCP を指定した場合に有効です。TCP プロトコルはコネクション型であるため、コネクション確立要求を発行し、それに対する応答を受信することによって、コネクションを開設します。したがって、一方からのコネクションを禁止する場合でも、コネクション確立要求だけを遮断し、その他の応答や通常データなどを透過させるように設定しないと通信できません。

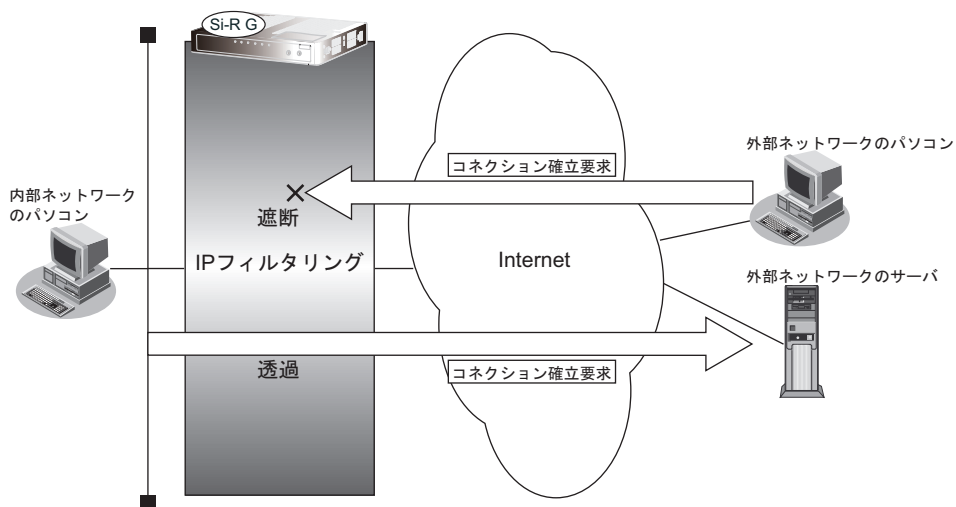
次に、TCP パケットとフラグ設定について説明します。TCP パケット内には SYN フラグと ACK フラグの2つの制御フラグがあります。このフラグの組み合わせによって、TCP パケットの内容が分かります。以下に、対応表を示します。

制御フラグ		TCP パケットの内容
SYN	ACK	
1	0	コネクションの確立要求
1	1	確立後の承認応答
0	1	確認応答、通常のデータ

この表から、制御フラグの組み合わせが SYN = 1、ACK = 0 の場合に、TCP パケットがコネクションの確立要求を行うことが分かります。つまり、IP パケットが禁止されている IP アドレスからの送信を禁止すれば、TCP/IP サービスのフィルタリングを行えます。

以下に、telnet (ポート番号 23) を例に説明します。

- ・外部ネットワークからのコネクション確立要求は遮断
- ・内部ネットワークからのコネクション確立要求は透過



◆ IP アドレスとアドレスマスクの決め方

IP フィルタリング条件の要素には「IP アドレス」と「アドレスマスク」があります。制御対象となるパケットは、本装置に届いたパケットの IP アドレスとアドレスマスクの論理積の結果が、指定した IP アドレスと一致したものに限りません。

◆ IPフィルタリングの方向

IPフィルタリングの方向に「リバース (reverse)」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。

- 送信元IPアドレス/アドレスマスクとあて先IPアドレス/アドレスマスク
- 送信元ポート番号とあて先ポート番号

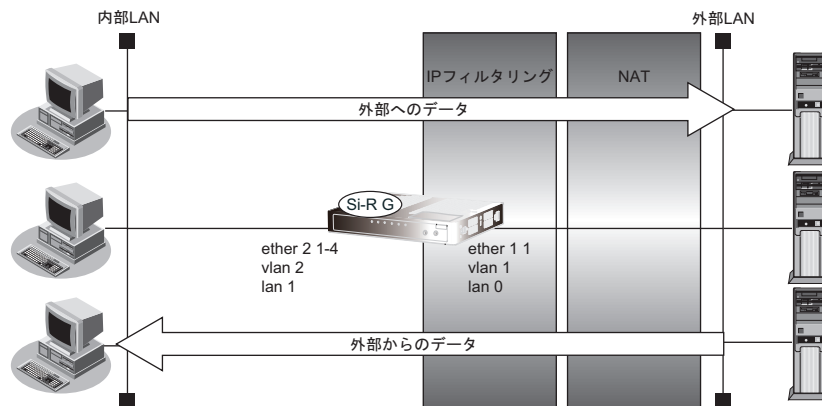


IPフィルタリング機能とNAT機能を併用する場合、回線切断時にNAT機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IPフィルタリング機能によってパケットは破棄されてしまいます。

💡 ヒント

◆ アドレス変換 (NAT) 機能利用時のIPフィルタリングのかかるタイミング

内部LANから外部LANに向かう場合は、アドレス変換でアドレスが変更される前にIPフィルタリング処理を通過します。また、外部LANから内部LANに向かう場合は、アドレス変換でアドレスが変更されたあとで、IPフィルタリング処理を通過します。つまり、IPフィルタリングは「プライベートアドレス」を対象に行います。本装置のIPフィルタリングとアドレス変換の位置付けは以下のとおりです。



## IP フィルタリングの設計方針

---

IP フィルタリングの設計方針には大きく分類して以下の2つがあります。

- A. 基本的にパケットをすべて遮断し、特定の条件のものだけを透過させる
- B. 基本的にパケットをすべて透過させ、特定の条件のものだけを遮断する

ここでは、設計方針Aの例として、以下の設定例について説明します。

- 外部の特定サービスへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけを許可する
- 外部から特定サーバへのアクセスだけ許可してSPIを併用する
- 外部の特定サービスへのアクセスだけを許可する (IPv6 フィルタリング)

また、設計方針Bの例として、以下の設定例について説明します。

- 外部の特定サーバへのアクセスだけを禁止する
- 利用者が意図しない発信を防ぐ
- 回線が接続しているときだけ許可する



TCP 接続要求の設定は、プロトコルにTCPまたはすべてを指定した場合にだけ有効です。それ以外のプロトコルを指定した場合は無効となります。

### こんな事に気をつけて

- IP フィルタリングでWWW (ポート番号 80) でのアクセスを制限する設定を行った場合、外部のWWWブラウザからアクセスができなくなる場合があります。
- IP フィルタリングでDHCP (ポート番号 67、68) でのアクセスを制限する設定を行った場合、DHCP機能が使用できなくなる場合があります。
- IP フィルタリング条件が複数存在する場合、それぞれの条件に優先順位がつき、数値の小さいものから優先的に採用されます。設定内容によっては通信できなくなる場合がありますので、優先順位を意識して設定してください。PPPoEの場合は、remote側にフィルタをかけるようにしてください。
- IP フィルタリングの方向に「reverse」を指定すると、入力パケットと出力パケットの両方がフィルタリング対象になります。ただし、入力パケットについては、以下のものを逆転した条件でフィルタリングします。
  - 送信元IPアドレス/アドレスマスクとあて先IPアドレス/アドレスマスク
  - 送信元ポート番号とあて先ポート番号

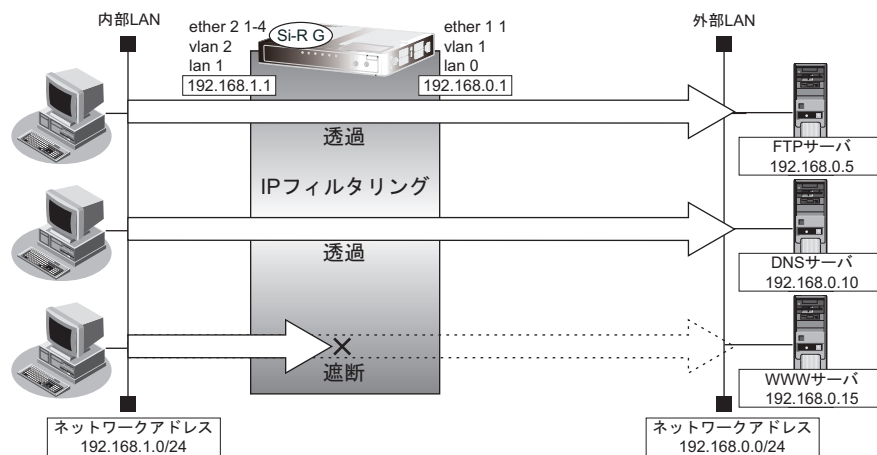
## 2.12.1 外部の特定サービスへのアクセスだけを許可する

### LAN 定義の場合

ここでは、一時的にLANを作成し、外部LANのすべてのFTPサーバに対してアクセスすることだけを許可し、ほかのサーバ（WWWサーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するために、DNSサーバへのアクセスは許可します。



- ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でドメイン名を指定した場合もDNSサーバへの発信が発生します。あらかじめ接続するFTPサーバが決まっている場合は、本装置のDNSサーバ機能を利用することによって、DNSサーバへの発信を抑制することができます。
- 本装置はftp-data転送に関するフィルタリングルールを自動的に作成します。



#### ● フィルタリング設計

- 内部LANのホスト（192.168.1.0/24）から外部LANのFTPサーバへのアクセスを許可
- 内部LANのホスト（192.168.1.0/24）から外部LANへのDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

#### こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

## ● フィルタリングルール

- FTP サーバへのアクセスを許可するには
  - (1) 192.168.1.0/24 の任意のポートから、任意の FTP サーバのポート 21 (ftp) への TCP パケットを透過させる
  - (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  - (1) 192.168.1.0/24 の任意のポートから、DNS サーバのポート 53 (domain) への UDP パケットを透過させる
  - (2) (1) の応答パケットを透過させる
- ICMP の通信を許可するためには
  - (1) ICMP パケットを透過させる
- その他をすべて遮断するには
  - (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

## ● コマンド

```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

FTP サーバからの応答パケットを透過させる
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNS サーバのポート 53 への UDP パケットを透過させる
# acl 2 ip 192.168.1.0/24 192.168.0.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNS サーバからの応答パケットを透過させる
# acl 3 ip 192.168.0.10/32 192.168.1.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

ICMP のパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

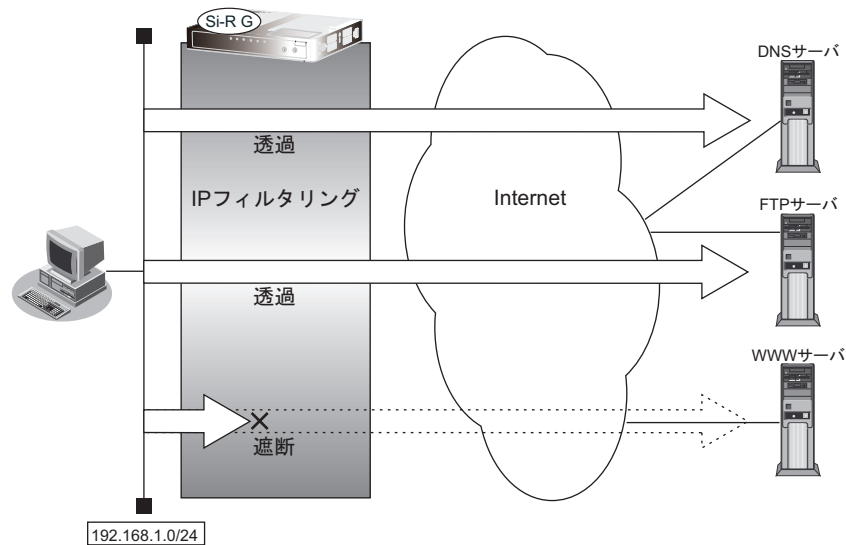
設定終了
# save
# commit
```

## リモート定義の場合

ここでは、LAN上のパソコンからインターネット上のすべてのFTPサーバに対してアクセスすることだけを許可し、ほかのサーバ（WWWサーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するために、DNSサーバへのアクセスは許可します。



- ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でドメイン名を指定した場合もDNSサーバへの発信が発生します。あらかじめ接続するFTPサーバが決まっている場合は、本装置のDNSサーバ機能を利用することによって、DNSサーバへの発信を抑制することができます。
- 本装置は、ftp-dataの転送に関するフィルタリングルールを自動的に作成します。



### ● フィルタリング設計

- LAN上のホスト（192.168.1.0/24）から任意のFTPサーバへのアクセスを許可
- LAN上のホスト（192.168.1.0/24）からWANの先のDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

#### こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

## ● フィルタリングルール

- FTP サーバへのアクセスを許可するには
  - (1) 192.168.1.0/24の任意のポートから、任意のFTPサーバのポート21 (ftp) へのTCPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  - (1) 192.168.1.0/24の任意のポートから、DNSサーバのポート53 (domain) へのUDPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- ICMPの通信を許可するためには
  - (1) ICMPパケットを透過させる
- その他をすべて遮断するには
  - (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

## ● コマンド

任意のFTPサーバのポート21へのTCPパケットを透過させる

```
# acl 0 ip 192.168.1.0/24 any 6
# acl 0 tcp any 21 yes
# remote 0 ip filter 0 pass acl 0 any
```

FTPサーバからの応答パケットを透過させる

```
# acl 1 ip any 192.168.1.0/24 6
# acl 1 tcp 21 any no
# remote 0 ip filter 1 pass acl 1 any
```

DNSサーバのポート53へのUDPパケットを透過させる

```
# acl 2 ip 192.168.1.0/24 any 17
# acl 2 udp any 53
# remote 0 ip filter 2 pass acl 2 any
```

DNSサーバからの応答パケットを透過させる

```
# acl 3 ip any 192.168.1.0/24 17
# acl 3 udp 53 any
# remote 0 ip filter 3 pass acl 3 any
```

ICMPのパケットを透過させる

```
# acl 4 ip any any 1
# acl 4 icmp any any
# remote 0 ip filter 4 pass acl 4 any
```

残りのパケットをすべて遮断する

```
# acl 5 ip any any any
# remote 0 ip filter 5 reject acl 5 any
```

設定終了

```
# save
# commit
```



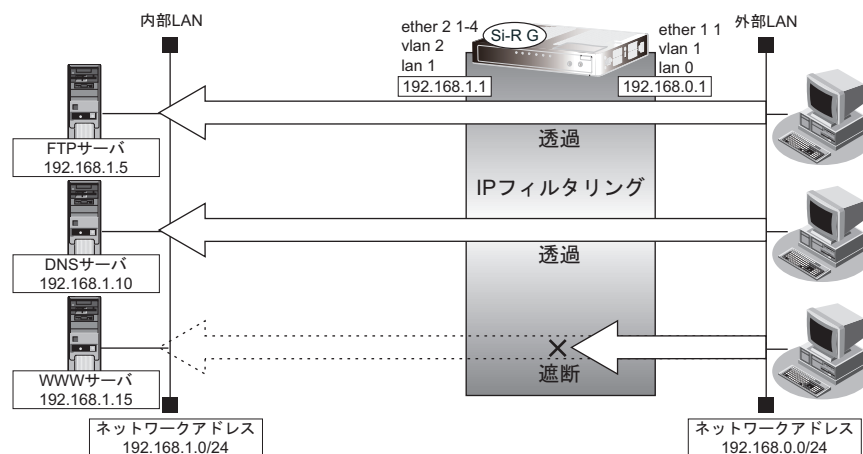
## 2.12.2 外部から特定サーバへのアクセスだけを許可する

### LAN 定義の場合

ここでは、内部LANの特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するためにDNSサーバへのアクセスは許可します。



- ftp でホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されるとDNSサーバへの問い合わせが発生します。あらかじめ接続するftpサーバが決まっている場合は、本装置のDNSサーバ機能を利用することで、DNSサーバへの問い合わせを抑止することができます。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



#### ● フィルタリング設計

- 内部LANのホスト（192.168.1.5/32）をFTPサーバとして利用を許可
- 内部LANのネットワークへのDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

#### こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

## ● フィルタリングルール

- 内部LANのホストのFTPサーバとしての利用を許可するには
  - (1) 192.168.1.5/32のポート21 (ftp) へのTCPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- DNSサーバへのアクセスを許可するには
  - (1) 192.168.0.0/24の任意のポートからDNSサーバのポート53 (domain) へのUDPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- ICMPの通信を許可するためには
  - (1) ICMPパケットを透過させる
- その他をすべて遮断するには
  - (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

## ● コマンド

```
LAN上のホストのポート21へのTCPパケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any

LAN上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any

DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any

DNSサーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any

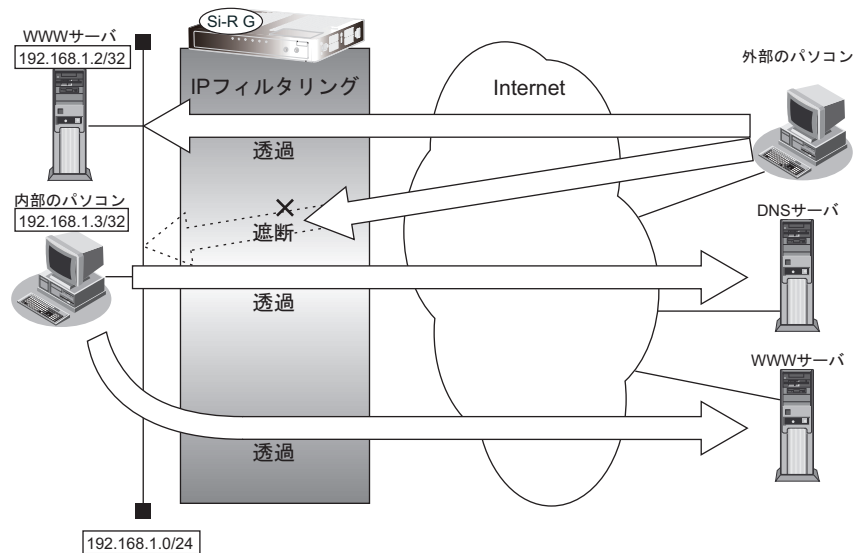
ICMPのパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any

残りのパケットをすべて遮断する
# acl 5 ip any any any
# lan 0 ip filter 5 reject acl 5 any

設定終了
# save
# commit
```

## リモート定義の場合

ここでは、LAN上のWWWサーバに対する外部のパソコンからのアクセスを許可し、LAN上のほかのパソコンへのアクセスは禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上のWWWサーバに対してアクセスすると想定されるため、そのアクセスには制限をつけません。



### ● フィルタリング設計

- LAN上のホスト（192.168.1.2/32）をWWWサーバとして利用することを許可
- LAN上のホスト（192.168.1.3/32）から任意のWWWサーバへのアクセスを許可
- LAN上のホスト（192.168.1.0/24）からWANの先のDNSサーバへのアクセスを許可
- ICMPの通信を許可
- その他はすべて遮断

#### こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

### ● フィルタリングルール

- LAN上のホストのWWWサーバとしての利用を許可するには
  - (1) 192.168.1.2/32のポート80（www-http）へのパケットを透過させる
  - (2) (1)の応答パケットを透過させる
- 任意のWWWサーバへのアクセスを許可するには
  - (1) 192.168.1.3/32の任意のポートから任意のWWWサーバのポート80（www-http）へのパケットを透過させる
  - (2) (1)の応答パケットを透過させる
- DNSサーバへのアクセスを許可するには
  - (1) 192.168.1.0/24の任意のポートからDNSサーバのポート53（domain）へのUDPパケットを透過させる
  - (2) (1)の応答パケットを透過させる
- ICMPの通信を許可するためには
  - (1) ICMPパケットを透過させる
- その他をすべて遮断するには
  - (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

## ● コマンド

```
LAN上のホストのポート80へのパケットを透過させる
# acl 0 ip any 192.168.1.2/32 6
# acl 0 tcp any 80 yes
# remote 0 ip filter 0 pass acl 0 any

LAN上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.2/32 any 6
# acl 1 tcp 80 any no
# remote 0 ip filter 1 pass acl 1 any

任意のWWWサーバのポート80へのパケットを透過させる
# acl 2 ip 192.168.1.3/32 any 6
# acl 2 tcp any 80 yes
# remote 0 ip filter 2 pass acl 2 any

任意のWWWサーバからの応答パケットを透過させる
# acl 3 ip any 192.168.1.3/32 6
# acl 3 tcp 80 any no
# remote 0 ip filter 3 pass acl 3 any

DNSサーバのポート53へのUDPパケットを透過させる
# acl 4 ip 192.168.1.0/24 any 17
# acl 4 udp any 53
# remote 0 ip filter 4 pass acl 4 any

DNSサーバからの応答パケットを透過させる
# acl 5 ip any 192.168.1.0/24 17
# acl 5 udp 53 any
# remote 0 ip filter 5 pass acl 5 any

ICMPのパケットを透過させる
# acl 6 ip any any 1
# acl 6 icmp any any
# remote 0 ip filter 6 pass acl 6 any

残りのパケットをすべて遮断する
# acl 7 ip any any any
# remote 0 ip filter 7 reject acl 7 any

設定終了
# save
# commit
```

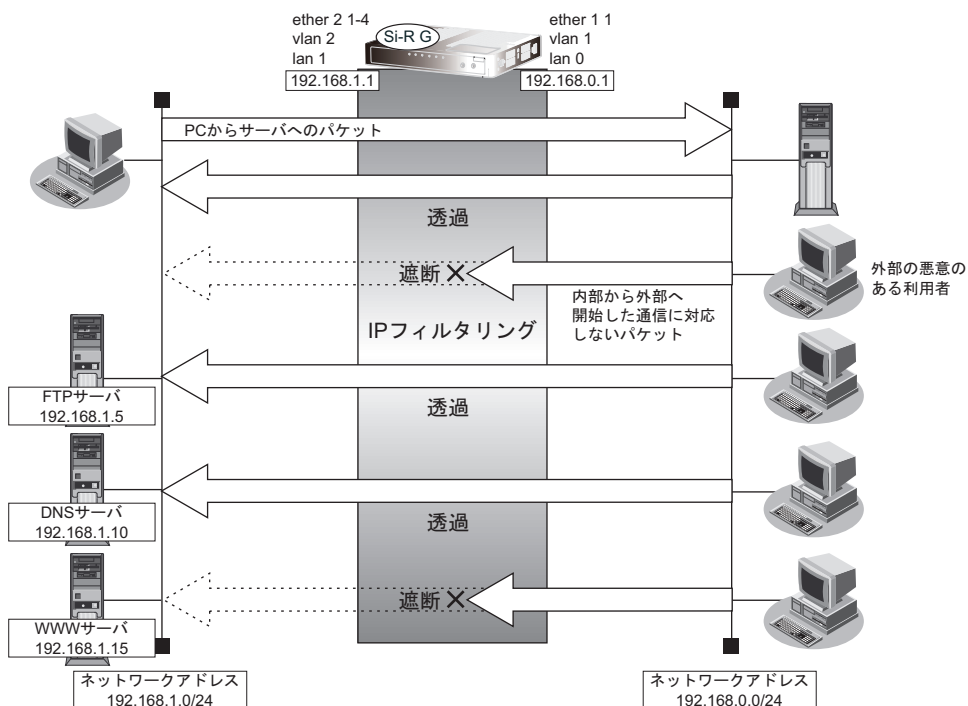
## 2.12.3 外部から特定サーバへのアクセスだけを許可してSPIを併用する

### LAN 定義の場合

ここでは、内部LANの特定サーバに対するアクセスを許可し、ほかのサーバに対するアクセスを禁止し、SPIを利用して外部へアクセスする場合の設定方法を説明します。ただし、FTPサーバ名を解決するためにDNSサーバへのアクセスは許可します。



- ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でもドメイン名で指定されるとDNSサーバへの問い合わせが発生します。あらかじめ接続するftpサーバが決まっている場合は、本装置のDNSサーバ機能を利用することで、DNSサーバへの問い合わせを抑制することができます。
- 本装置はftp-data転送に関するフィルタリングルールを自動的に作成します。



#### ● フィルタリング設計

- 内部LANのホスト (192.168.1.5/32) をFTPサーバとして利用を許可
- 内部LANのネットワークへのDNSサーバへのアクセスを許可
- ICMPの通信を許可
- 内部LANから外部へ開始するアクセスを許可し、その他はすべて遮断

#### こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

## ● フィルタリングルール

- 内部LANのホストのFTPサーバとしての利用を許可するには
  - (1) 192.168.1.5/32のポート21 (ftp) へのTCPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- DNSサーバへのアクセスを許可するには
  - (1) 192.168.0.0/24の任意ポートからDNSサーバのポート53 (domain) へのUDPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- ICMPの通信を許可するためには
  - (1) ICMPパケットを透過させる
- 内部LANから外部へ開始するアクセスは許可し、その他をすべて遮断するには
  - (1) 残りのパケットにSPIを利用してIPフィルタリングを行う

上記のフィルタリングルールに従って設定する場合のコマンド例を示します。

## ● コマンド

```
LAN上のホストのポート21へのTCPパケットを透過させる
# acl 0 ip 192.168.0.0/24 192.168.1.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 pass acl 0 any
```

```
LAN上のホストからの応答パケットを透過させる
# acl 1 ip 192.168.1.5/32 192.168.0.0/24 6
# acl 1 tcp 21 any no
# lan 0 ip filter 1 pass acl 1 any
```

```
DNSサーバのポート53へのUDPパケットを透過させる
# acl 2 ip 192.168.0.0/24 192.168.1.10/32 17
# acl 2 udp any 53
# lan 0 ip filter 2 pass acl 2 any
```

```
DNSサーバからの応答パケットを透過させる
# acl 3 ip 192.168.1.10/32 192.168.0.0/24 17
# acl 3 udp 53 any
# lan 0 ip filter 3 pass acl 3 any
```

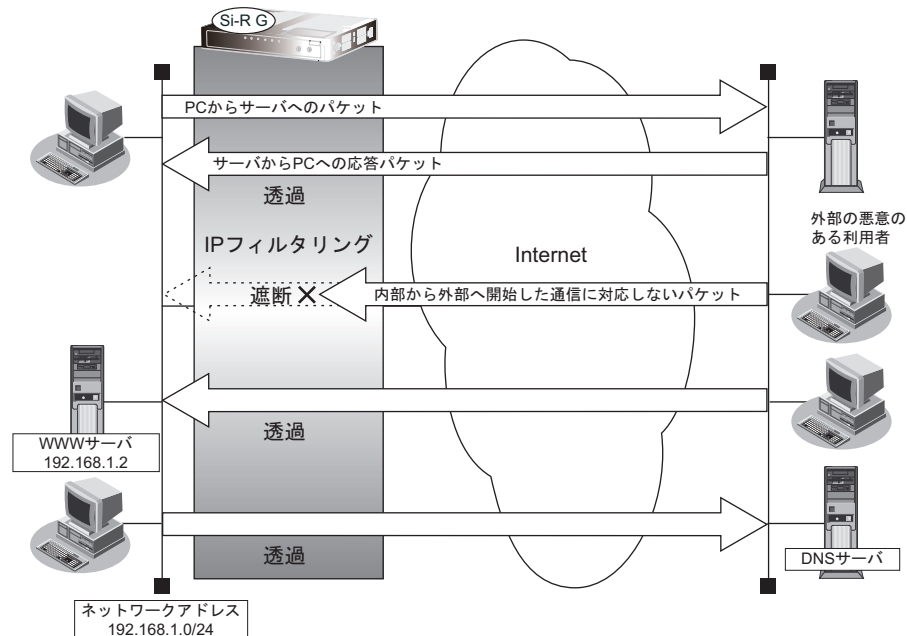
```
ICMPのパケットを透過させる
# acl 4 ip any any 1
# acl 4 icmp any any
# lan 0 ip filter 4 pass acl 4 any
```

```
残りのパケットにSPIを利用してIPフィルタリングを行う
# lan 0 ip filter default spi
```

```
設定終了
# save
# commit
```

## リモート定義の場合

ここでは、外部からLAN上のWWWサーバに対するアクセスを許可し、ほかのLAN上のパソコンへのアクセスを禁止する場合の設定方法を説明します。また、LAN上のほかのパソコンはインターネット上のサーバに対してアクセスしますが、これらのアクセスに対してはSPIによるIPフィルタリングの対象とします。



### ● フィルタリング設計

- LAN上のホスト (192.168.1.2/32) をWWWサーバとして利用を許可
- ICMPの通信を許可
- 内部LANから外部へ開始するアクセスは許可し、その他はすべて遮断

### こんな事に気をつけて

ICMPは、IP通信を行う際にさまざまな制御メッセージを交換します。ICMPの通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPの通信を透過させる設定を行ってください。

### ● フィルタリングルール

- 内部LANのホストのWWWサーバとしての利用を許可するには
  - (1) 192.168.1.2/32のポート80 (www-http) へのTCPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- ICMPの通信を許可するためには
  - (1) ICMPパケットを透過させる
- 内部LANから外部へ開始するアクセスは許可し、その他をすべて遮断するには
  - (1) 残りのパケットにSPIを利用してIPフィルタリングを行う

上記のフィルタリングルールに従って設定する場合のコマンド例を示します。

**● コマンド**

LAN上のホストのポート80へのパケットを透過させる

```
# acl 0 ip any 192.168.1.2/32 6  
# acl 0 tcp any 80 yes  
# remote 0 ip filter 0 pass acl 0 any
```

LAN上のホストからの応答パケットを透過させる

```
# acl 1 ip 192.168.1.2/32 any 6  
# acl 1 tcp 80 any no  
# remote 0 ip filter 1 pass acl 1 any
```

ICMPのパケットを透過させる

```
# acl 2 ip any any 1  
# acl 2 icmp any any  
# remote 0 ip filter 2 pass acl 2 any
```

残りのパケットにSPIを利用してIPフィルタリングを行う

```
# remote 0 ip filter default spi
```

設定終了

```
# save  
# commit
```



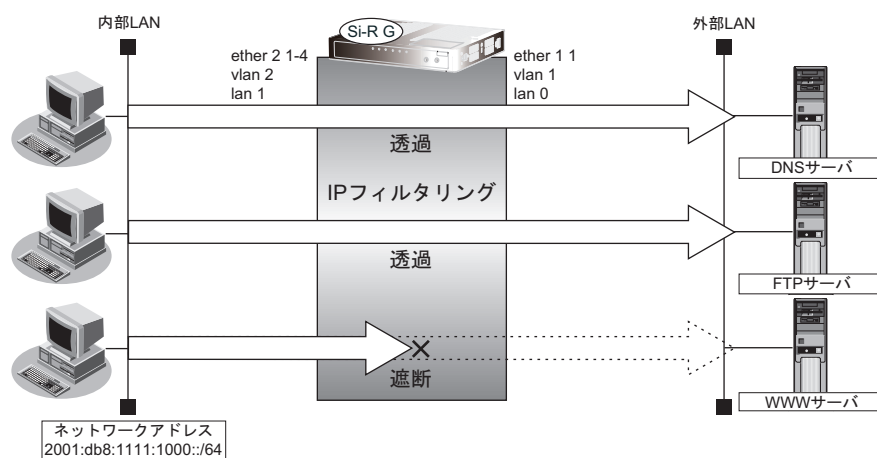
## 2.12.4 外部の特定サービスへのアクセスだけを許可する (IPv6 フィルタリング)

### LAN 定義の場合

ここでは、IPv6 フィルタリングを使って、内部 LAN 上のパソコンから外部 LAN 上のすべての FTP サーバに対してアクセスすることだけを許可し、ほかのサーバ (WWW サーバなど) へのアクセスを禁止する場合の設定方法を説明します。ただし、FTP サーバ名を解決するために DNS サーバへのアクセスを許可する設定にします。



- ftp でホスト名を指定する場合、DNS サーバに問い合わせが発生するため、DNS サーバへのアクセスを許可する必要があります。DNS サーバへのアクセスを許可することによって、ftp サービス以外でもドメイン名で指定されると DNS サーバへの通信が発生します。
- 本装置は ftp-data 転送に関するフィルタリングルールを自動的に作成します。



#### ● フィルタリング設計

- 内部 LAN 上のホスト (2001:db8:1111:1000::/64) から任意の FTP サーバへのアクセスを許可
- 内部 LAN 上のホスト (2001:db8:1111:1000::/64) から外部 LAN の DNS サーバへのアクセスを許可
- ICMPv6 の通信を許可
- その他はすべて遮断

#### こんな事に気をつけて

ICMPv6 は、IPv6 通信を行う際にさまざまな制御メッセージを交換します。ICMPv6 の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6 の通信を透過させる設定を行ってください。

## ● フィルタリングルール

- FTP サーバへのアクセスを許可するには
  - (1) 2001:db8:1111:1000::/64 の任意のポートから、任意のアドレスのポート 21 (ftp) への TCP パケットを透過させる
  - (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  - (1) 2001:db8:1111:1000::/64 の任意のポートから DNS サーバのポート 53 (domain) への UDP パケットを透過させる
  - (2) (1) の応答パケットを透過させる
- ICMPv6 の通信を許可するためには
  - (1) ICMPv6 パケットを透過させる
- その他をすべて遮断するには
  - (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

## ● コマンド

```
任意の FTP サーバのポート 21 への TCP パケットを透過させる
```

```
# acl 0 ipv6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# lan 0 ipv6 filter 0 pass acl 0 any
```

```
FTP サーバからの応答パケットを透過させる
```

```
# acl 1 ipv6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# lan 0 ipv6 filter 1 pass acl 1 any
```

```
DNS サーバのポート 53 への UDP パケットを透過させる
```

```
# acl 2 ipv6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# lan 0 ipv6 filter 2 pass acl 2 any
```

```
DNS サーバからの応答パケットを透過させる
```

```
# acl 3 ipv6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# lan 0 ipv6 filter 3 pass acl 3 any
```

```
ICMPv6 のパケットを透過させる
```

```
# acl 4 ipv6 any any 58
# acl 4 icmp any any
# lan 0 ipv6 filter 4 pass acl 4 any
```

```
残りのパケットをすべて遮断する
```

```
# acl 5 ipv6 any any any
# lan 0 ipv6 filter 5 reject acl 5 any
```

```
設定終了
```

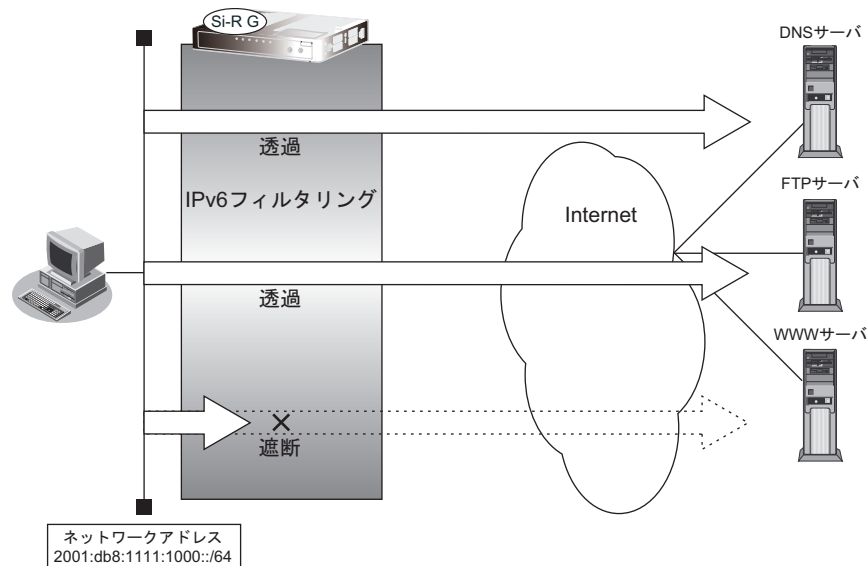
```
# save
# commit
```

## リモート定義の場合

ここでは、IPv6フィルタリングを使って、LAN上のパソコンからイントラネット上のすべてのFTPサーバに対してアクセスすることだけを許可し、ほかのサーバ（WWWサーバなど）へのアクセスを禁止する場合の設定方法を説明します。ただし、FTPサーバ名を解決するためにDNSサーバへのアクセスを許可する設定にします。



- ftpでホスト名を指定する場合、DNSサーバに問い合わせが発生するため、DNSサーバへのアクセスを許可する必要があります。DNSサーバへのアクセスを許可することによって、ftpサービス以外でドメイン名を指定する場合もDNSサーバへの発信が発生します。
- 本装置はftp-data転送に関するフィルタリングルールを自動的に作成します。



### ● フィルタリング設計

- LAN上のホスト（2001:db8:1111:1000::/64）から任意のFTPサーバへのアクセスを許可
- LAN上のホスト（2001:db8:1111:1000::/64）からWANの先のDNSサーバへのアクセスを許可
- ICMPv6の通信を許可
- その他はすべて遮断

### こんな事に気をつけて

ICMPv6は、IPv6通信を行う際にさまざまな制御メッセージを交換します。ICMPv6の通信を遮断すると正常な通信ができなくなる場合がありますので、ICMPv6の通信を透過させる設定を行ってください。

## ● フィルタリングルール

- FTP サーバへのアクセスを許可するには
  - (1) 2001:db8:1111:1000::/64 の任意のポートから、任意のFTPサーバのポート21 (ftp) へのTCPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- DNS サーバへのアクセスを許可するには
  - (1) 2001:db8:1111:1000::/64 の任意のポートからDNSサーバのポート53 (domain) へのUDPパケットを透過させる
  - (2) (1) の応答パケットを透過させる
- ICMPv6の通信を許可するためには
  - (1) ICMPv6パケットを透過させる
- その他をすべて遮断するには
  - (1) すべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

## ● コマンド

任意のFTPサーバのポート21へのTCPパケットを透過させる

```
# acl 0 ipv6 2001:db8:1111:1000::/64 any 6
# acl 0 tcp any 21 yes
# remote 0 ipv6 filter 0 pass acl 0 any
```

FTPサーバからの応答パケットを透過させる

```
# acl 1 ipv6 any 2001:db8:1111:1000::/64 6
# acl 1 tcp 21 any no
# remote 0 ipv6 filter 1 pass acl 1 any
```

DNSサーバのポート53へのUDPパケットを透過させる

```
# acl 2 ipv6 2001:db8:1111:1000::/64 any 17
# acl 2 udp any 53
# remote 0 ipv6 filter 2 pass acl 2 any
```

DNSサーバからの応答パケットを透過させる

```
# acl 3 ipv6 any 2001:db8:1111:1000::/64 17
# acl 3 udp 53 any
# remote 0 ipv6 filter 3 pass acl 3 any
```

ICMPv6のパケットを透過させる

```
# acl 4 ipv6 any any 58
# acl 4 icmp any any
# remote 0 ipv6 filter 4 pass acl 4 any
```

残りのパケットをすべて遮断する

```
# acl 5 ipv6 any any any
# remote 0 ipv6 filter 5 reject acl 5 any
```

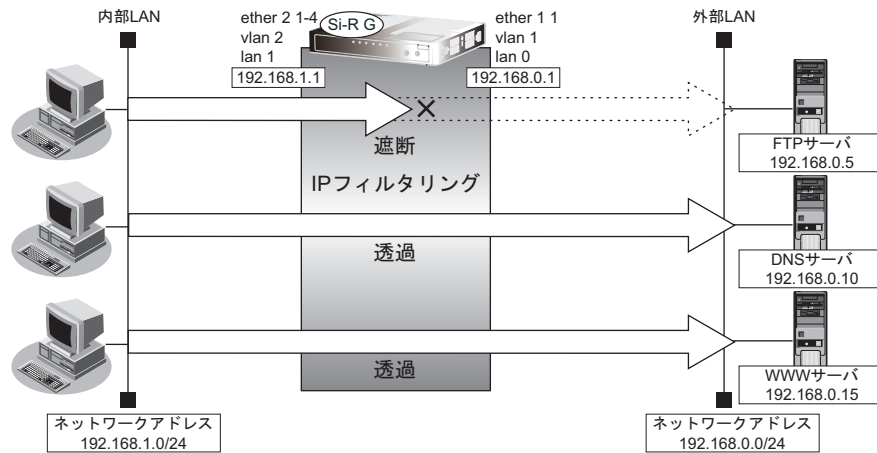
設定終了

```
# save
# commit
```

## 2.12.5 外部の特定サーバへのアクセスだけを禁止する

### LAN 定義の場合

ここでは、外部LANのFTPサーバに対するアクセスを禁止する場合の設定方法を説明します。



#### ● フィルタリング設計

- 内部LANのホスト（192.168.1.0/24）から外部LANのFTPサーバ（192.168.0.5）へのアクセスを禁止

#### ● フィルタリングルール

- FTPサーバへのアクセスを禁止するには
  - 192.168.1.0/24から192.168.0.5のポート21（ftp）へのTCPパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

#### ● コマンド

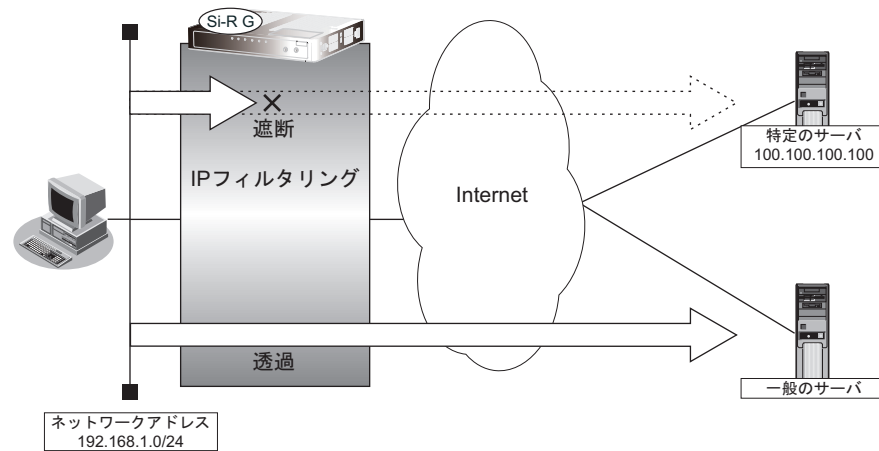
```

内部のLANから192.168.0.5へのFTPパケットを遮断する
# acl 0 ip 192.168.1.0/24 192.168.0.5/32 6
# acl 0 tcp any 21 yes
# lan 0 ip filter 0 reject acl 0 any

設定終了
# save
# commit
  
```

## リモート定義の場合

ここでは、インターネット上の特定のサーバに対するアクセスを禁止する場合の設定方法を説明します。



### ● フィルタリング設計

- LAN上のホスト（192.168.1.0/24）からアドレス 100.100.100.100 へのアクセスを禁止

### ● フィルタリングルール

- 特定アドレスへのアクセスを禁止するには
  - (1) 192.168.1.0/24 から 100.100.100.100 の任意のポートへのすべてのパケットを遮断する

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

### ● コマンド

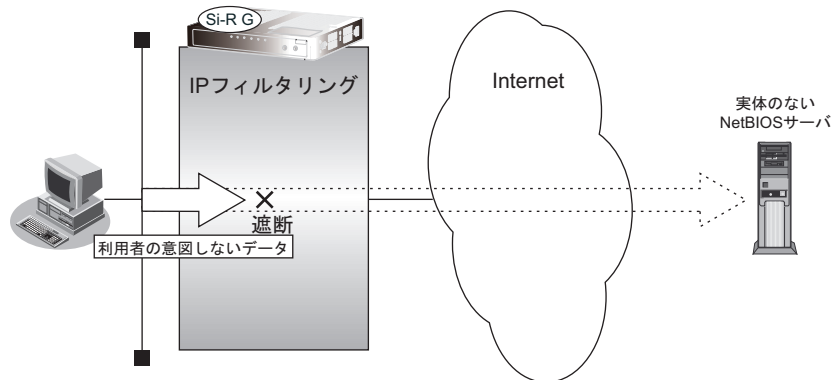
```
アドレス 100.100.100.100 へのすべてのパケットを遮断する
# acl 0 ip 192.168.1.0/24 100.100.100.100/32 any
# remote 0 ip filter 0 reject acl 0 any
```

```
設定終了
# save
# commit
```

## 2.12.6 利用者が意図しない発信を防ぐ

LAN上のパソコンは、利用者の意志とは無関係に、実体のないNetBIOSサーバにアクセスすることがあります。その際、回線が接続され、利用者が意識しないところで通信料金がかかってしまいます。

ここでは、上記のような、回線に対するむだな発信を抑止する場合のフィルタリング設定方法を説明します。



### ● フィルタリング設計

- ポート 137～139 (NetBIOS サービス) へのアクセスを禁止

### ● フィルタリングルール

- ポート 137～139 へのアクセスを禁止するには
  - (1) ポート 137～139 へのすべてのパケットを遮断する
  - (2) ポート 137～139 からのすべてのパケットを遮断する



Windows (TCP 上の NetBIOS) 環境のネットワークでは、セキュリティ上の問題とむだな課金を抑えるために、ポート番号 137～139 の外向きの転送経路をふさいでおく必要があります。

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

**● コマンド**

ポート 137～139 へのすべての TCP パケットを遮断する

```
# acl 0 ip any any 6  
# acl 0 tcp any 137-139 yes  
# remote 0 ip filter 0 reject acl 0 any
```

ポート 137～139 からのすべての TCP パケットを遮断する

```
# acl 1 ip any any 6  
# acl 1 tcp 137-139 any yes  
# remote 0 ip filter 1 reject acl 1 any
```

ポート 137～139 へのすべての UDP パケットを遮断する

```
# acl 2 ip any any 17  
# acl 2 udp any 137-139  
# remote 0 ip filter 2 reject acl 2 any
```

ポート 137～139 からのすべての UDP パケットを遮断する

```
# acl 3 ip any any 17  
# acl 3 udp 137-139 any  
# remote 0 ip filter 3 reject acl 3 any
```

設定終了

```
# save  
# commit
```

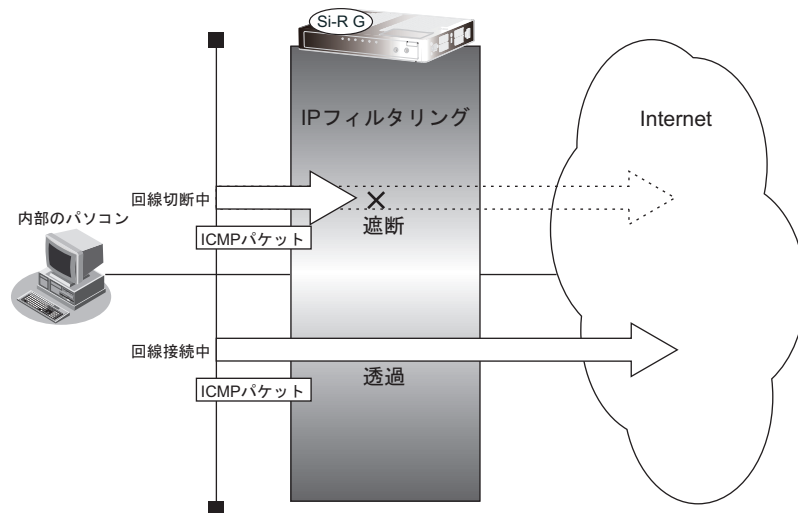


## 2.12.7 回線が接続しているときだけを許可する

一部のパソコンでは、ネットワークの設定によって、ログイン時に自動的にPINGを発行してPPPoE回線を接続してしまうものがあります。回線接続を必要とするICMPパケットを遮断することによって、意図しないPINGによるむだな発信を抑止することができます。ここでは、回線が接続されているときにだけICMPパケットを透過させる場合の設定方法を説明します。



IPアドレスを直接指定せず、DNSによる名前アドレス変換を利用した場合、発信を抑止することはできません。



### ● フィルタリング設計

- すでに回線が接続している場合にだけPINGを許可

### ● フィルタリングルール

- すでに回線が接続している場合にだけPINGを許可するには
  - (1) 回線接続中だけICMPパケットを透過させる

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

### ● コマンド

回線が接続しているときだけICMPパケットを透過させる

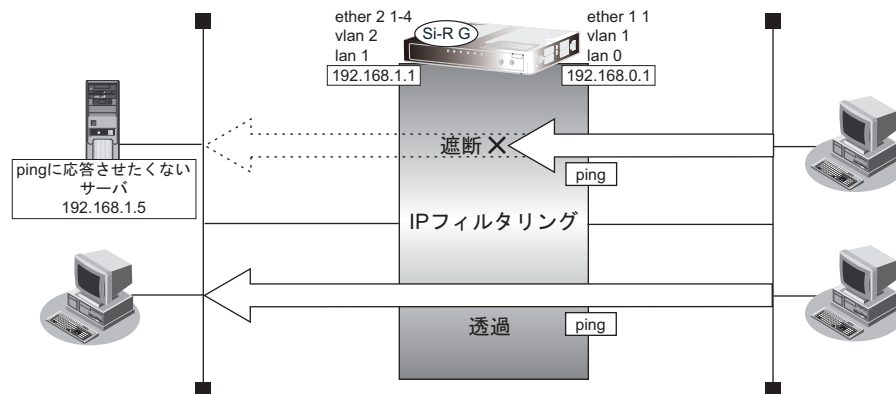
```
# acl 0 ip any any 1
# acl 0 icmp any any
# remote 0 ip filter 0 restrict acl 0 any
```

```
設定終了
# save
# commit
```

## 2.12.8 外部から特定サーバへの ping だけを禁止する

### LAN 定義の場合

ここでは、内部 LAN の特定のサーバに対する ping (ICMP ECHO) を禁止し、この特定のサーバに対するほかの ICMP パケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。



#### ● フィルタリング設計

- 内部 LAN のサーバ (192.168.1.5/32) に対して外部からの ping (ICMP ECHO) を禁止
- その他はすべて通過

#### ● フィルタリングルール

- 内部 LAN のサーバ (192.168.1.5/32) に対して外部からの ping (ICMP ECHO) を禁止するには
  - (1) 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
- その他のパケットを許可する
  - (1) すべてのパケットを透過させる

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

#### ● コマンド

```

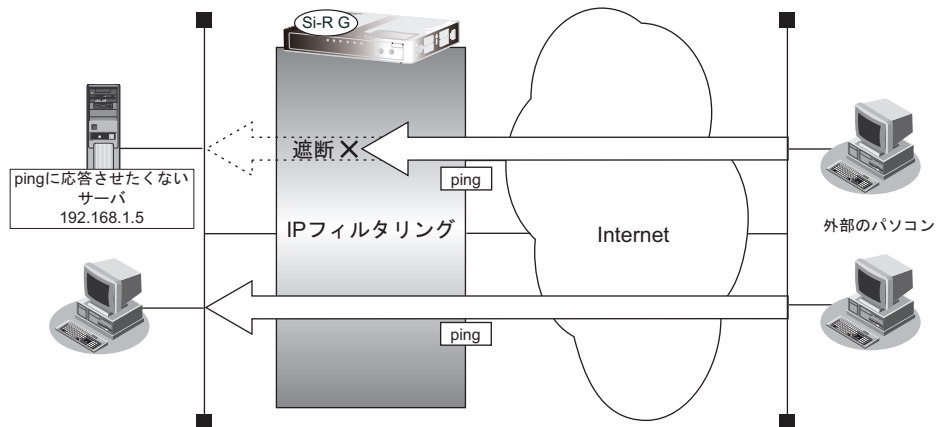
アドレス 192.168.1.5/32 への ICMP TYPE 8 の ICMP パケットを遮断する
# acl 0 ip any 192.168.1.5/32 1
# acl 0 icmp 8 any
# lan 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
# acl 1 ip any any any
# lan 0 ip filter 1 pass acl 1 any

設定終了
# save
# commit
  
```

## リモート定義の場合

ここでは、LAN上の特定のサーバに対するping (ICMP ECHO) を禁止し、この特定のサーバに対するほかのICMPパケット、その他のプロトコルのパケットおよびほかのホストに対するパケットはすべて許可する場合の設定方法を説明します。



### ● フィルタリング設計

- LAN上のサーバ (192.168.1.5/32) に対して外部からのping (ICMP ECHO) を禁止
- その他はすべて通過

### ● フィルタリングルール

- LAN上のサーバ (192.168.1.5/32) に対して外部からのping (ICMP ECHO) を禁止するには
  - (1) 192.168.1.5/32のICMP TYPE 8のICMPパケットを遮断する
- その他のパケットを許可する
  - (1) すべてのパケットを透過させる

上記のフィルタリングルールに従って設定を行う場合のコマンド例を示します。

### ● コマンド

```

アドレス 192.168.1.5/32 へのICMP TYPE 8のICMPパケットを遮断する
# acl 0 ip any 192.168.1.5/32 1
# acl 0 icmp 8 any
# remote 0 ip filter 0 reject acl 0 any

残りのパケットをすべて透過させる
# acl 1 ip any any any
# remote 0 ip filter 1 pass acl 1 any

設定終了
# save
# commit
  
```

## 2.13 IPsec 機能を使う

VPN (Virtual Private Network) は、インターネットを利用して遠隔地の LAN をつなぐと、遠隔地の LAN 上のアプリケーションやデータが、あたかも同じオフィスの LAN のように利用できる機能です。また、認証情報や暗号情報を設定することにより、インターネット上を流れるデータのセキュリティを確保することができます。

本装置では、VPN を実現するために IPsec というプロトコルを使用して、以下の接続形態が利用できます。

- IPv4 over IPv4 で固定 IP アドレスでの VPN (手動鍵交換) (P.159)  
自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は手動で設定します。
- IPv4 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)  
自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。構成例は、[「第1章 導入例」 \(P.10\)](#) を参照してください。
- IPv4 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換)  
自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。構成例は、[「第1章 導入例」 \(P.10\)](#) を参照してください。
- IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換) (P.163)  
自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換) (P.167)  
自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- IPv6 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換) (P.171)  
自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- IPv6 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換) (P.175)  
自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- IPv4 over IPv4 で1つのIKEセッションに複数のIPsecトンネル構成でのVPN (自動鍵交換) (P.179)  
複数のIPsec対象範囲が存在し、IPsec対象範囲をすべて (any) とすることができない環境で、IKEセッション (トンネル) を1つとしてVPN通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode、Aggressive Mode が使用できます。ただし、設定例では Main Mode のみで説明します。
- IPsec 機能と他機能との併用 (P.183)  
IPsec 機能と他機能を併用する場合のいくつかの設定例を説明します。

- テンプレート着信機能 (AAA 認証) を使用した固定 IP アドレスでの VPN (P.188)  
IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使用して VPN 通信を行います。  
認証情報および暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- テンプレート着信機能 (AAA 認証) を使用した可変 IP アドレスでの VPN (P.192)  
相手装置の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能を使用して VPN 通信を行います。  
認証情報および暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- テンプレート着信機能 (RADIUS 認証) を使用した固定 IP アドレスでの VPN (P.197)  
IKE 不特定着信の IKE 認証鍵取得に RADIUS 認証機能を使用して VPN 通信を行います。  
認証情報および暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode を使用します。
- テンプレート着信機能 (RADIUS 認証) を使用した可変 IP アドレスでの VPN (P.202)  
相手装置の IP アドレスが動的に割り当てられる環境で、IKE 不特定着信の IKE 認証鍵取得に RADIUS 認証機能を使用して VPN 通信を行います。  
認証情報および暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- テンプレート着信機能 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN (P.208)  
不特定着信の環境で、動的 VPN 接続契機パケットを監視して動的に VPN 通信を行います。  
自装置の IPv4 トンネルエンドポイントアドレス、IPsec 対象範囲、IPsec 経路情報および接続先監視アドレスは、動的 VPN 情報交換機能で自動的に交換されます。
- テンプレート着信機能 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN (冗長構成) (P.217)  
VRRP 機能を使用した冗長構成環境で、動的 VPN 機能を使用した構成を説明します。
- テンプレート着信機能 (動的 VPN) を使用した IPv6 over IPv6 で固定 IP アドレスでの VPN (P.220)  
不特定着信の環境で、動的 VPN 接続契機パケットを監視して動的に VPN 通信を行います。  
自装置の IPv6 トンネルエンドポイントアドレス、IPsec 対象範囲、IPsec 経路情報および接続先監視アドレスは、動的 VPN 情報交換機能で自動的に交換されます。
- NAT トラバーサルを使用した可変 IP アドレスでの VPN (P.230)  
自装置側の IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、IKE 区間にある NAT を介した IPsec 通信を可能にするために、NAT トラバーサル機能を使用して VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Main Mode、Aggressive Mode が使用できます。ただし、設定例では Aggressive Mode のみで説明します。
- テンプレート着信機能 (AAA 認証) および NAT トラバーサルを使用した可変 IP アドレスでの VPN (P.234)  
相手装置の IP アドレスが動的に割り当てられ、IKE 区間にある NAT を介した環境で、IKE 不特定着信の IKE 認証鍵取得に AAA 認証機能と NAT トラバーサル機能を使用して VPN 通信を行います。  
認証情報および暗号情報の鍵は自動鍵交換 (IKE) を使用して作成し、IKE の鍵交換タイプは Aggressive Mode を使用します。
- 接続先情報 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN (P.238)  
動的 VPN 機能で、送出インタフェースを固定にした場合の構成を説明します。  
また、設定例にはテンプレート着信機能の動的 VPN との併用動作で記載されています。
- RSA デジタル署名認証で接続先情報 (動的 VPN) を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN (P.257)  
動的 VPN 機能で、IKE 認証方式の RSA デジタル署名認証機能を使用します。  
構成例は前述にある構成と同等です。

- IPv4 over IPv4 で NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.270)  
自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「第1章 導入例」 \(P.10\)](#) を参照してください。
- IPv4 over IPv4 で NAT と併用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.274)  
自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「第1章 導入例」 \(P.10\)](#) を参照してください。
- IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.278)  
自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv4 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「2.13.2 IPv4 over IPv6 で固定 IP アドレスでの VPN \(自動鍵交換\)」 \(P.163\)](#) を参照してください。
- IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.281)  
自装置および相手装置の IPv4 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「2.13.3 IPv6 over IPv4 で固定 IP アドレスでの VPN \(自動鍵交換\)」 \(P.167\)](#) を参照してください。
- IPv6 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.284)  
自装置または相手装置のどちらかが IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「2.13.4 IPv6 over IPv4 で可変 IP アドレスでの VPN \(自動鍵交換\)」 \(P.171\)](#) を参照してください。
- IPv6 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.287)  
自装置および相手装置の IPv6 トンネルエンドポイントアドレスが固定で、送信元、送信先が IPv6 アドレス範囲である環境の場合に VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「2.13.5 IPv6 over IPv6 で固定 IP アドレスでの VPN \(自動鍵交換\)」 \(P.175\)](#) を参照してください。
- IPv4 over IPv4 で1つの IKE セッションに複数の IPsec トンネル構成での VPN (自動鍵交換 IKE Version2) (P.290)  
複数の IPsec 対象範囲が存在し、IPsec 対象範囲をすべて (any) とすることができない環境で、IKE セッション (トンネル) を1つとして VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「2.13.6 IPv4 over IPv4 で1つの IKE セッションに複数の IPsec トンネル構成での VPN \(自動鍵交換\)」 \(P.179\)](#) を参照してください。
- NAT トラバーサルを使用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.293)  
自装置側の IPv4 トンネルエンドポイントアドレスが動的に割り当てられる環境で、IKE 区間にある NAT を介した IPsec 通信を可能にするために、NAT トラバーサル機能を使用して VPN 通信を行います。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[「2.13.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN」 \(P.230\)](#) を参照してください。



- EAP 認証を使用した固定 IP アドレスでの VPN (自動鍵交換 IKE Version2) (P.302)  
EAP 認証機能で、IKE 認証方式は事前共有鍵認証機能を使用します。  
認証情報、暗号情報の鍵は自動鍵交換 (IKE Version2) を使用して作成します。  
構成例は、[\[2.13.31 EAP 認証を使用した固定 IP アドレスでの VPN \(自動鍵交換 IKE Version2\)\] \(P.302\)](#) を参照してください。

☞ 参照 マニュアル「機能説明書」

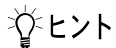
### こんな事に気をつけて

- IPsec は IPv4、IPv6 で使用できます。
- NAT 変換には、IPsec の前の変換と IPsec のあとの変換があります。IPsec 前に変換する場合は IPsec 用の remote ip nat コマンドで設定します。IPsec 後に変換する場合は、プロバイダ接続用の remote ip nat コマンドで設定します。
- インターネット VPN では、VPN 装置どうしがインターネットを介して通信する必要があるため、VPN 装置にはインターネット上で使用可能なグローバルな IP アドレスを使用してください (NAT を使用している場合は、マルチ NAT (静的 NAT) で IP アドレスを割り当てます)。
- VPN 相互接続するアドレスがプライベートアドレスの場合、重複しないように設計してください。
- IPsec では、IPv4、IPv6 パケット通信だけをサポートしています。IPv4、IPv6 パケット以外は VPN の対象とならないため中継されません。
- 暗号パケットが多重に暗号化される形態で使用しないでください。暗号パケットが二重に暗号化され、復号処理が正常に行えないため通信異常となります。
- IPsec と NAT 機能を併用する場合は、マルチ NAT を使用してください。
- IPsec とマルチ NAT を併用する場合は、静的 NAT の設定が必要となることがあります。
- 経路情報を設定する場合、IPsec/IKE ネゴシエーションパケットが VPN のトンネルに入らないように設定してください。
- 複数の接続先情報定義に同じ IPsec トンネルアドレスを定義しないでください。
- IKE セッションに対して複数の IPsec トンネル構成を使用する場合は、同じ IPsec 対象範囲がないように設定してください。
- IPsec 対象範囲が複数ネットワーク存在し、IPsec 対象範囲にすべて (any) を設定できない環境の場合だけ、「IKE セッションに対して複数の IPsec トンネル構成」を使用することをお勧めします。ネットワークごとに IPsec SA を作成する構成や IPsec 対象範囲にすべて (any) を定義できない装置と接続する場合は、「IKE セッションに対して複数の IPsec トンネル構成」を使用してください。
- テンプレート着信機能 (AAA 認証および RADIUS 認証) を使用した IPsec では、以下の点に注意してください。
  - IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
  - 初回 IKE ネゴシエーションは Responder でのみ動作します。
  - 自側トンネルエンドポイントアドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
  - テンプレート定義の接続先監視アドレスに IPv6 DHCP クライアントが取得したプレフィックスを使用することはできません。
  - AAA 設定または RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。
- RADIUS および AAA の登録情報を変更して IPsec が接続できない場合は、手動切断を行い、再度テンプレート着信機能で接続してください。
- 動的 VPN 情報交換機能を使用する場合、システム全体で一意となるユーザ ID を設定してください。
- テンプレート着信機能 (動的 VPN) を使用した IPsec では、以下の点に注意してください。
  - IKE セッションに対して複数の IPsec トンネル構成を使用することはできません。
  - IKE モードは Main Mode で動作します。
  - 動的 VPN で作成されたインタフェースにスタティック経路情報が設定されるように動的 VPN 接続契機パケットを監視するインタフェースの経路情報を設定してください。
  - Si-R シリーズ (V31) 以降のソフトウェアと Si-R シリーズ (V30) ソフトウェアで IPsec を行う場合は、Si-R シリーズ (V31) 以降のソフトウェアの動的 VPN クライアント情報設定で交換情報のエンコードタイプを「off」に指定する必要があります。また、動的 VPN サーバを Si-R シリーズ (V31) 以降のソフトウェアにする必要があります。
- 動的 VPN 機能を使用する場合に経路情報再登録 (clear ip route コマンドまたは clear ipv6 route コマンド) を行うと、経路削除により動的 VPN のセッションが切断されることがあります。
- 動的 VPN で接続する自側ネットワークを異なるアドレスファミリで設定した場合、拡張 IPsec 対象範囲が 1 定義分追加されます。
- 拡張 IPsec 対象範囲機能未対応版数 Si-R シリーズ (V30) の装置と動的 VPN 接続を行う場合、動的 VPN で接続する自側ネットワークに異なるアドレスファミリを設定しないでください。

- 拡張 IPsec 対象範囲機能を使用して IPsec パケットを通過させた場合、IPsec 対象範囲をチェックする相手装置の場合は IPsec が遮断されます。この場合は、拡張 IPsec 対象範囲機能を使用することはできません。
- 拡張 IPsec 対象範囲を使用して双方向通信を行う場合、相手装置側にも同様の設定が必要です。相手装置側に、自側装置と同様の設定が存在しない場合、片側通信のみ暗号化し、折り返しの通信は暗号化されない場合があります。
- NAT トラバーサル機能を利用するときは、以下の点に注意してください。
  - IKE を行う双方の装置で設定してください。片方の装置での利用や NAT トラバーサルのバージョンが異なると、NAT トラバーサルはできません。
  - NAT トラバーサルは、以下の RFC、Internet Draft のバージョンをサポートします。
    - “Negotiation of NAT-Traversal in the IKE”
    - RFC3947
    - draft-ietf-ipsec-nat-t-ike-03
    - draft-ietf-ipsec-nat-t-ike-02
    - “UDP Encapsulation of IPsec ESP Packets”
    - RFC3948
  - IPsec トンネルに存在する NAT 装置の変換テーブルが解放されると、NAT トラバーサルは動作できなくなります。変換テーブルを保持するために、接続先監視機能と併用することを推奨します。
  - IPsec 通信プロトコルは暗号 (ESP) を使用するよう設定してください。IPsec 通信プロトコルが認証 (AH) の場合は動作しません。
  - 自側および相手側トンネルエンドポイントアドレスに IPv6 アドレスを設定した場合は動作しません。
  - IKE モードが Aggressive Mode 設定で、自側および相手側トンネルエンドポイントアドレスに IPv4 アドレスを設定した場合は動作しません。
  - IKE を使用する設定をしてください。動的 VPN (dvpn) および手動鍵 (manual) を設定した場合は動作しません。
  - 初回 IKE ネゴシエーションが、initiator 装置側で NAT される環境でのみ動作します。
  - テンプレート着信機能 (AAA 認証および RADIUS 認証) を使用した IPsec では、IKE モードを Aggressive Mode で設定してください。Main Mode で設定した場合は動作しません。
- 接続優先制御の設定は、IKE ネゴシエーションのすれ違いが頻発する場合にそれぞれ異なる優先方法を設定してください。同じ優先制御を行うと、競合した場合に IKE ネゴシエーションが失敗します。この機能を利用する場合は、以下の設定を奨励します。
  - 一方の装置で Initiator を優先し、一方の装置で Responder を優先する。
- RSA デジタル署名認証を使用した固定 IP アドレスでの VPN を行う設定で、送信 ID を IP アドレスにするには自装置識別情報の設定を削除してください。
- 自装置証明書および相手装置証明書の双方がない場合は、RSA デジタル署名認証は使用できません。
- テンプレート接続を使用した RADIUS/AAA で RSA デジタル署名認証は使用できません。
- 本装置は自装置証明書または相手装置証明書の有効期限が満了しても証明書を使用し続けます。有効期限が満了した場合は、証明書の更新 (保存) を行ってください。
- RSA デジタル署名認証を使用した Aggressive Mode の設定で、IKE セッション用 Proposal 定義を複数設定する場合、PFS と認証情報 (auth-method) の設定はすべて同じ値を設定してください。これは、Aggressive Mode が Diffie-Hellman グループと認証情報について IKE ネゴシエーションができないためです。
- 相手装置から送られて来た証明書の認証局情報が、自装置に設定している認証局情報と異なる場合は、IKE ネゴシエーションが失敗し、通信を行うことができないときがあります。
- 自装置証明書の X.509v3 オプションのサブジェクト代替名称に IPv6 アドレスは使用できません。
- ID タイプが x501\_sbj の場合は、Aggressive モードを使用することはできません。
- 接続先情報の動的 VPN 接続を使用する場合、相手装置の自側ネットワーク設定 (dvpn client localnet) と自装置の相手側ネットワーク設定 (remote ap dvpn remotenet) が異なる場合は、以下に注意してください。
  - 双方の装置で自装置 ID 設定 (dvpn client localid) を設定してください。
  - 接続先情報の動的 VPN 接続を使用する場合は、相手装置 ID 設定 (remote ap dvpn remoteid) に相手装置の自装置 ID (dvpn client localid) を設定してください。
  - 自装置の相手側ネットワーク設定 (remote ap dvpn remotenet) に存在しないネットワーク情報を相手装置の自側ネットワーク設定 (dvpn client localnet) に追加する場合は、必ず後ろの番号に追加してください。
  - 対向装置がテンプレート情報の動的 VPN 接続の場合、自装置の相手側ネットワーク設定 (remote ap dvpn remotenet) に存在しないネットワークからの接続はできません。



- 接続先情報の動的VPN接続で INVITE 自動 ignore 機能を使用する場合は、以下に注意してください。
  - 相手装置側のネットワーク情報に all-0 (0.0.0.0/0または::/0) が含まれている場合は、INVITE 自動 ignore ルール適用の対象外となります。
  - 動的VPNが設定されている接続先情報にセッション監視定義があった場合は、セッション監視パケットも INVITE 自動 ignore 対象となります。
  - INVITE 自動 ignore 機能により作成された ignore ルールの自側アドレス範囲は、any (0.0.0.0/0または::/0) となります。
- IPsec Version3/IKE Version2 機能は、接続先情報のみサポートしています。テンプレート情報使用時は、IPsec Version2/IKE Version1 を使用してください。
- IPsec Version3 は IKE Version2 で動作します。
- IPsec Version3 を使用した手動鍵設定はサポートしていません。
- IPsec Version3/IKE Version2 を使用した動的VPNはサポートしていません。
- IKE Version2 で設定した接続先情報で IKE Version1 を要求してきても接続はできません。また、その逆で IKE Version1 で設定した接続先情報で IKE Version2 を要求してきても接続はできません。
- 自側/相手側 ID タイプに設定する User-FQDN は、RFC822 に対応したチェックは行っていません。RFC822 に対応した対向装置と接続する場合は、正しい User-FQDN 値を設定してください。
- IPsec Version3 の拡張シーケンス番号 (ESN) 機能の設定は、IKE Version2 でネゴシエーションする両方の装置で設定してください。設定されていない場合は、IKE ネゴシエーションで接続に失敗します。
- IKE Version1 で Dead Peer Detection (DPD) 機能を使用する場合、IKE でネゴシエーションする両方の装置で設定してください。設定されていない場合は、IKE ネゴシエーションで接続に失敗します。



## ヒント

### ◆ VPN とは？

暗号化技術や認証技術を使って、インターネットを仮想的な専用線として利用する技術です。また、VPN を使ってつないだルータ間の通信経路のことをトンネルと言います。

### ◆ 自動鍵交換とは？

IPsec の通信に使用される暗号化・認証用の鍵素材を、自動で作成・更新します。鍵素材を定期的に自動更新させることにより、セキュリティの強度を高めることができます。自動鍵交換を使用しない場合は、手動で鍵を設定する必要があります。

### ◆ IPsec Version3 とは？

拡張シーケンス番号 (ESN) を使用することで、高速回線でのシーケンス番号の桁あふれが発生しにくくなります。

◆ NAT と IPsec を併用する

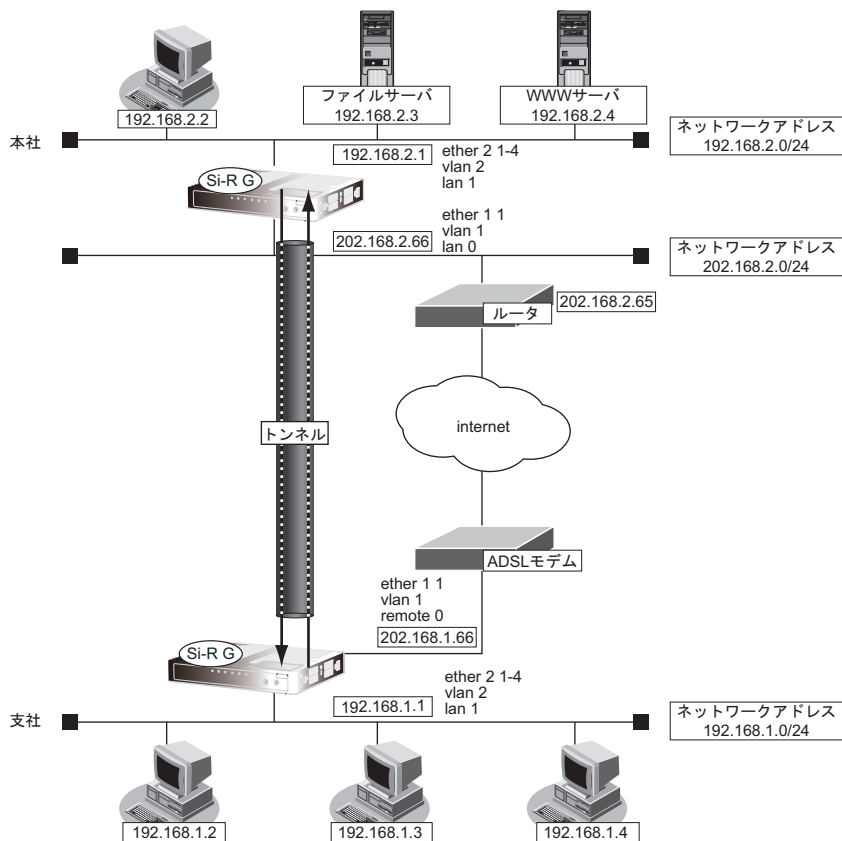
IPsec で使用するグローバルアドレスで NAT を使用している場合 (IPsec 後の NAT 変換後) は、IPsec パケットが NAT を通過できるように、実回線の LAN または remote 定義で、以下の静的 NAT を設定します。

利用形態	設定内容
固定 IP アドレスでの VPN (手動鍵交換)	ESP パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス    自側エンドポイントに設定したアドレス ポート番号    すべて ・グローバル IP 情報 IP アドレス    相手 VPN 装置に設定された本装置側の IP アドレス ポート番号    すべて ・プロトコル    ESP
固定 IP アドレスでの VPN (自動鍵交換)	IKE パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス    自側エンドポイントに設定したアドレス ポート番号    500 ・グローバル IP 情報 IP アドレス    相手 VPN 装置に設定された本装置側の IP アドレス ポート番号    500 ・プロトコル    UDP ESP パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス    自側エンドポイントに設定したアドレス ポート番号    すべて ・グローバル IP 情報 IP アドレス    相手 VPN 装置に設定された本装置側の IP アドレス ポート番号    すべて ・プロトコル    ESP 例) 本装置の WAN の自側 IP アドレスが 202.168.1.66 (固定) であり、202.168.1.66 (自側) と 202.168.2.66 (相手側) の間で IPsec/IKE 通信を行う場合、IPsec/IKE 通信の自側エンドポイントに 202.168.1.66 を設定します。このとき静的 NAT のプライベートアドレスおよびグローバルアドレスには、202.168.1.66 を設定します。
可変 IP アドレスでの VPN (Initiator)	IKE パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス    本装置の LAN 側 IP アドレス ポート番号    500 ・グローバル IP 情報 IP アドレス    指定しない ポート番号    500 ・プロトコル    UDP
可変 IP アドレスでの VPN (Initiator)	ESP パケットの受信を設定します。 ・プライベート IP 情報 IP アドレス    本装置の LAN 側 IP アドレス ポート番号    すべて ・グローバル IP 情報 IP アドレス    指定しない ポート番号    すべて ・プロトコル    ESP

## 2.13.1 IPv4 over IPv4 で固定 IP アドレスでの VPN (手動鍵交換)

IPsec 機能を使って手動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 端末装置として本装置が接続されていることを前提とします。



### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IP アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.1.66/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

#### [本社]

- ローカルネットワーク IP アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IP アドレス : 202.168.2.65

## ● 設定コマンド

### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

### [本社]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

## ● 設定条件

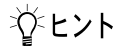
### [支社]

- IPsec 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IPsec プロトコル : esp
- IPsec 送信用 SPI : 100 (16進数)
- IPsec 送信用 SA 暗号アルゴリズムと暗号秘密鍵 : des-cbc、0123456789 (16進数)
- IPsec 送信用 SA 認証アルゴリズムと認証秘密鍵 : hmac-md5、123456789a (16進数)
- IPsec 受信用 SPI : 101 (16進数)
- IPsec 受信用 SA 暗号アルゴリズムと暗号秘密鍵 : des-cbc、23456789ab (16進数)
- IPsec 受信用 SA 認証アルゴリズムと認証秘密鍵 : hmac-md5、3456789abc (16進数)

### [本社]

- IPsec 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IPsec プロトコル : esp
- IPsec 送信用 SPI : 101 (16進数)
- IPsec 送信用 SA 暗号アルゴリズムと暗号秘密鍵 : des-cbc、23456789ab (16進数)
- IPsec 送信用 SA 認証アルゴリズムと認証秘密鍵 : hmac-md5、3456789abc (16進数)
- IPsec 受信用 SPI : 100 (16進数)
- IPsec 受信用 SA 暗号アルゴリズムと暗号秘密鍵 : des-cbc、0123456789 (16進数)

- IPsec受信用SA認証アルゴリズムと認証秘密鍵 : hmac-md5、123456789a (16進数)



#### ◆ SPIとは？

トンネルの識別子です。SPIはトンネルの往路と復路でそれぞれ異なる値を設定します。トンネルをつなぐ本装置を設定するときには、同じ方向のトンネルには同じSPIを設定します。

#### こんな事に気をつけて

- 暗号アルゴリズムに des-cbc を選択する場合、鍵に単純な文字列 (同じ文字だけ、文字列の繰り返しなど) を指定すると、暗号強度が低下するおそれがあるので指定しないでください。暗号アルゴリズムに 3des-cbc を選択する場合は、鍵を 16 桁ごとに 3 つに分割した、それぞれ 3 つの暗号強度が低下する鍵 (弱い鍵) にならないように指定してください。des-cbc で弱い鍵として具体的に知られているものには以下のようなものがあります。本装置は、これらの文字列で始まる鍵で通信できないようにしています。  
0101 0101 0101 0101、1F1F 1F1F E0E0 E0E0、E0E0 E0E0 1F1F 1F1F、FEFE FEFE FEFE FEFE、01FE 01FE 01FE 01FE、1FE0 1FE0 0EF1 0EF1、01E0 01E0 01F1 01F1、FE01 FE01 FE01 FE01、E01F E01F F10E F10E、E001 E001 F101 F101、1FFE 1FFE 0EFE 0EFE、011F 011F 010E 010E、E0FE E0FE F1FE F1FE、FE1F FE1F FE0E FE0E、1F01 1F01 0E01 0E01、FEE0 FEE0 FEF1 FEF1
- 暗号アルゴリズムに 3des を選択する場合は、以下のように鍵を 16 桁ごとに 3 つに分割し、鍵 1 ≠ 鍵 2 ≠ 鍵 3 となるように鍵を設定してください。  
鍵: 1122334455667788 9900aabbccddeeff 1122334455667788  
鍵 1 (16 桁) 鍵 2 (16 桁) 鍵 3 (16 桁)  
鍵 1 = 鍵 3 のように鍵を設定すると、16 バイトの鍵で暗号化すると同じ結果になります。また、鍵 1 = 鍵 2、鍵 2 = 鍵 3 のように鍵を設定すると、それぞれ鍵 3、鍵 1 の des-cbc 暗号と同じ結果になります (鍵 1 = 鍵 2 = 鍵 3 の場合も同様です)。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honten
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type manual

送信用 SA を設定する
# remote 1 ap 0 ipsec send protocol esp
# remote 1 ap 0 ipsec send spi 100
# remote 1 ap 0 ipsec send encrypt des-cbc hex 0123456789
# remote 1 ap 0 ipsec send auth hmac-md5 hex 123456789a

受信用 SA を設定する
# remote 1 ap 0 ipsec receive protocol esp
# remote 1 ap 0 ipsec receive spi 101
# remote 1 ap 0 ipsec receive encrypt des-cbc hex 23456789ab
# remote 1 ap 0 ipsec receive auth hmac-md5 hex 3456789abc

設定終了
# save
# commit
```

## 本社を設定する

---

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shiten
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type manual
```

送信用SAを設定する

```
# remote 0 ap 0 ipsec send protocol esp
# remote 0 ap 0 ipsec send spi 101
# remote 0 ap 0 ipsec send encrypt des-cbc hex 23456789ab
# remote 0 ap 0 ipsec send auth hmac-md5 hex 3456789abc
```

受信用SAを設定する

```
# remote 0 ap 0 ipsec receive protocol esp
# remote 0 ap 0 ipsec receive spi 100
# remote 0 ap 0 ipsec receive encrypt des-cbc hex 0123456789
# remote 0 ap 0 ipsec receive auth hmac-md5 hex 123456789a
```

設定終了

```
# save
# commit
```

## 2.13.2 IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)

IPsec 機能を使って IPv4 ローカルネットワーク間を IPv6 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.1.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス : 2001:db8:1111:1::66/64
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから割り当てられた固定 IPv6 アドレス : 2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートの IPv6 アドレス : 2001:db8:1111:2::65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

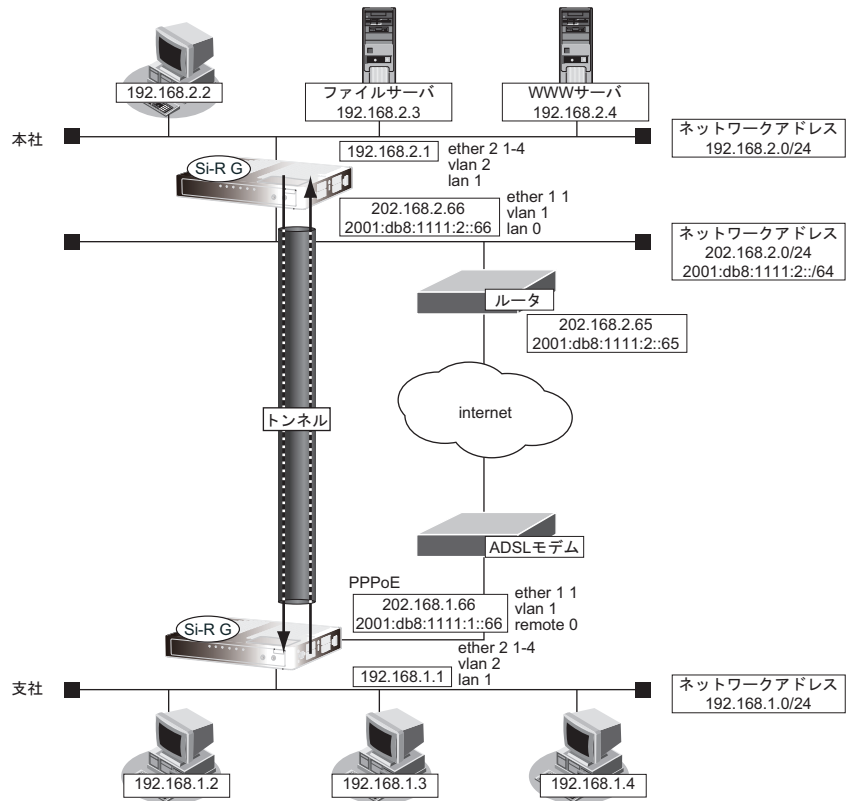
# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::66/64
# remote 0 ipv6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

**【本社】**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:2::66/64
# lan 0 ipv6 route 0 default 2001:db8:1111:2::65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● **設定条件**

**【支社】**

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 2001:db8:1111:1::66 - 2001:db8:1111:2::66
- ・ IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット


**【本社】**

- ・ ネットワーク名 : vpn-shi
- ・ 接続先名 : shisya
- ・ IPsec/IKE 区間 : 2001:db8:1111:2::66 - 2001:db8:1111:1::66
- ・ IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット



**[共通]**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社を設定する****● コマンド**

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit
```

## 本社を設定する

---

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
```

設定終了

```
# save
# commit
```

## 2.13.3 IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)

IPsec 機能を使って IPv6 ローカルネットワーク間を IPv4 インターネットで結び、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- ローカルネットワーク IPv6 アドレス : 2001:db8:1111:1::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.1.66/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- ローカルネットワーク IPv6 アドレス : 2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:1::1/64
# lan 1 vlan 2

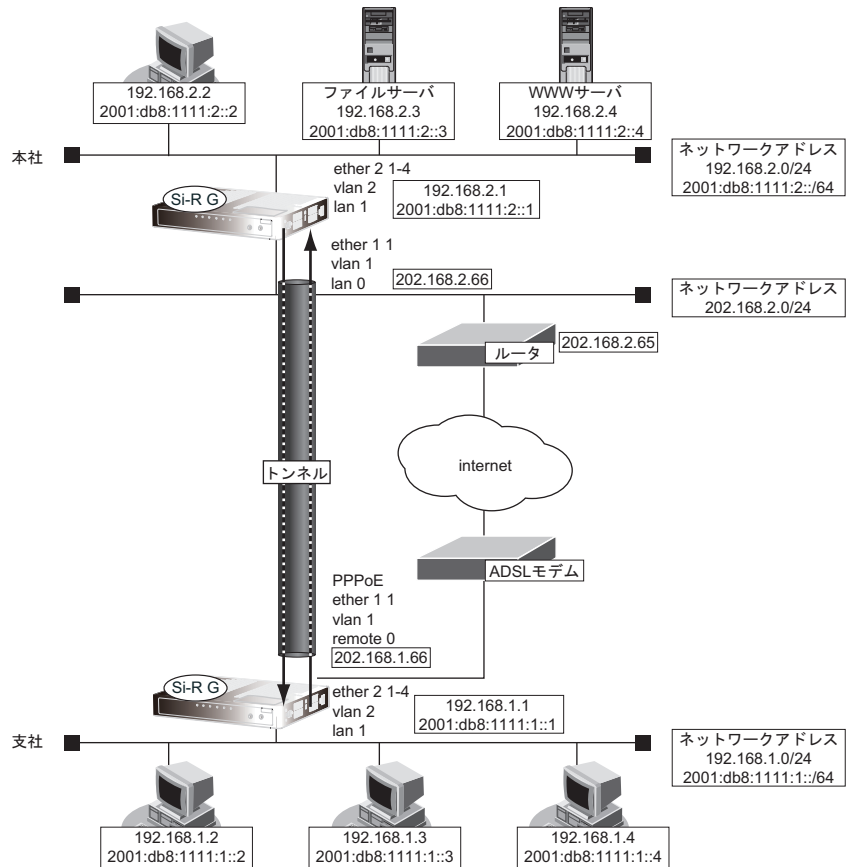
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

**【本社】**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:2::1/64
# lan 1 vlan 2
```



● 設定条件

**【支社】**

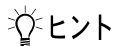
- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**【本社】**

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**[共通]**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

**ヒント****◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社 (Initiator) を設定する****● コマンド**

```

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc

設定終了
# save
# commit

```

## 本社を設定する

---

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
```

設定終了

```
# save
# commit
```

## 2.13.4 IPv6 over IPv4 で可変IPアドレスでのVPN (自動鍵交換)

接続するたびにIPアドレスが変わる環境でVPNを構築する場合の設定方法を説明します。

IPv6 ローカルネットワーク間をIPv4 インターネットで結んでIPsecを行います。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- ローカルネットワーク IPv6 アドレス : 2001:db8:1111:1::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.1.66/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- ローカルネットワーク IPv6 アドレス : 2001:db8:1111:2::1/64
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 2001:db8:1111:1::1/64
# lan 1 vlan 2

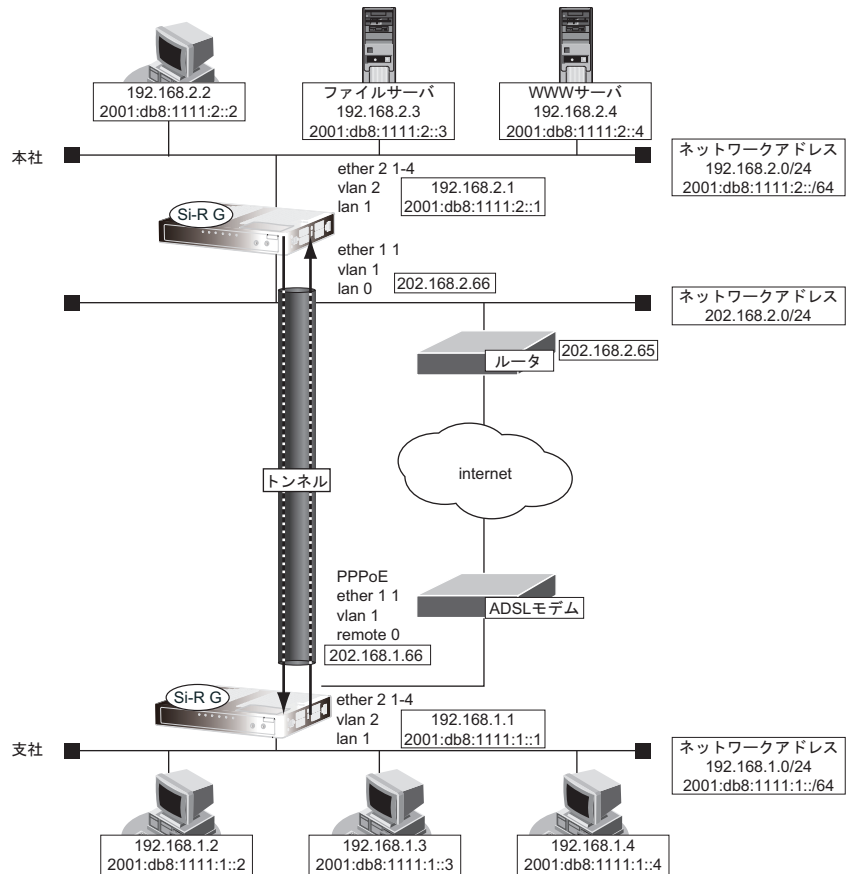
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
```

**[本社]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:2::1/64
# lan 1 vlan 2
```



● **設定条件**

**[支社 (Initiator)]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESPのプライベートアドレス : 192.168.1.1




**【本社】**

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 202.168.2.66 - 支社
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**【共通】**

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

**◆ ID タイプとは？**

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

インターネットから IPsec/IKE パケットを受信する設定をする

```
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
```

VPN を設定する

```
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
```

設定終了

```
# save
# commit
```

## 本社 (Responder) を設定する

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
```

設定終了

```
# save
# commit
```

## 2.13.5 IPv6 over IPv6で固定IPアドレスでのVPN（自動鍵交換）

IPsec機能を使ってIPv6で自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE常時接続)]

- ローカルネットワークIPv4アドレス : 192.168.1.1/24
- ローカルネットワークIPv6アドレス : 2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.1.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス : 2001:db8:1111:1::66/64
- PPPoE ユーザ認証ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1

#### [本社]

- ローカルネットワークIPv4アドレス : 192.168.2.1/24
- ローカルネットワークIPv6アドレス : 2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.2.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス : 2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス : 202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートのIPv6アドレス : 2001:db8:1111:2::65

### ● 設定コマンド

#### [支社 (PPPoE常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ipv6 use on
# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:3::1/64
# lan 1 vlan 2

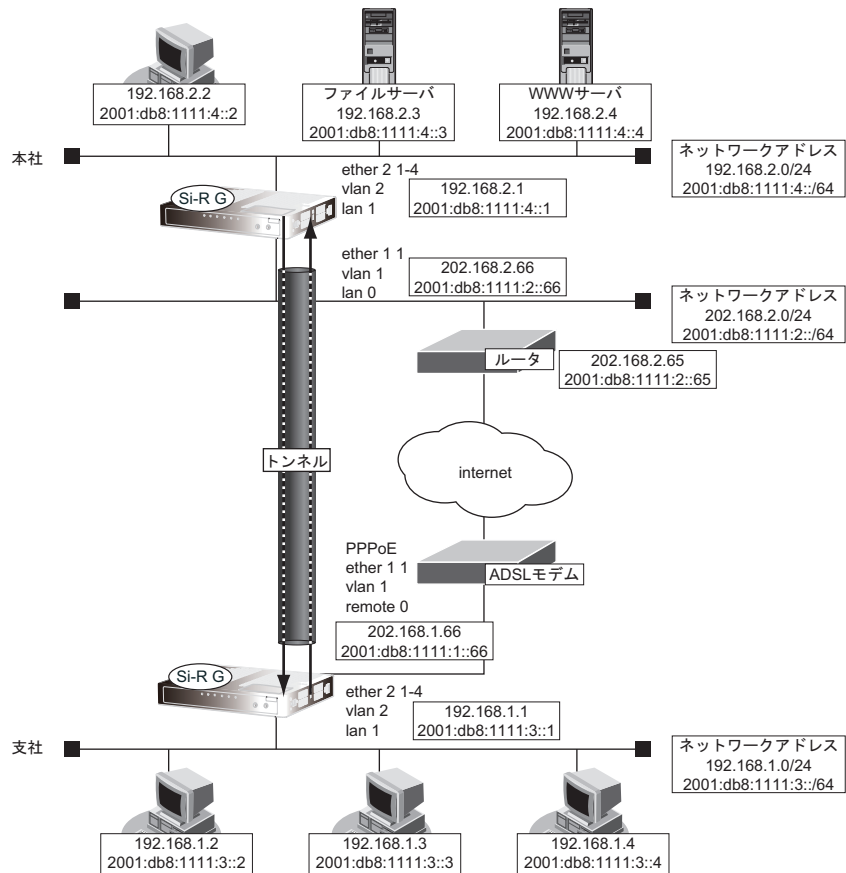
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::66/64
# remote 0 ipv6 route 0 default 1
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

**[本社]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:2::66/64
# lan 0 ipv6 route 0 default 2001:db8:1111:2::65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:4::1/64
# lan 1 vlan 2
```



● 設定条件

**[支社]**

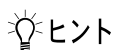
- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 2001:db8:1111:1::66 - 2001:db8:1111:2::66
- ・ IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**【本社】**

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 2001:db8:1111:2::66 - 2001:db8:1111:1::66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**【共通】**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

**ヒント****◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社を設定する****● コマンド**

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
```

```
設定終了  
# save  
# commit
```

## 本社を設定する

### ● コマンド

```
VPNを設定する  
# remote 0 name vpn-shi  
# remote 0 ip route 0 192.168.1.0/24 1 1  
# remote 0 ipv6 use on  
# remote 0 ipv6 route 0 2001:db8:1111:3::/64 1  
# remote 0 ap 0 name shisya  
# remote 0 ap 0 datalink type ipsec  
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66  
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66  
# remote 0 ap 0 ipsec type ike  
# remote 0 ap 0 ipsec ike protocol esp  
# remote 0 ap 0 ipsec ike range any6 any6  
# remote 0 ap 0 ipsec ike encrypt des-cbc  
# remote 0 ap 0 ipsec ike auth hmac-md5  
# remote 0 ap 0 ike mode main  
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890  
# remote 0 ap 0 ike proposal encrypt des-cbc  
  
設定終了  
# save  
# commit
```

## 2.13.6 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN (自動鍵交換)

IPsec機能を使って複数のネットワークにそれぞれのIPsec SAを作成する環境を構築する場合を例に説明します (自動鍵交換の固定IPアドレスを使用した構成です)。

ここでは以下のコマンドにより、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE常時接続)]

- ローカルネットワークIPアドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス : 202.168.1.66/24
- PPPoE ユーザ認証ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1

#### [本社]

- ローカルネットワークIPアドレス1 : 192.168.2.1/24
- ローカルネットワークIPアドレス2 : 192.168.3.1/24
- インターネットプロバイダから割り当てられた固定のIPアドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPアドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

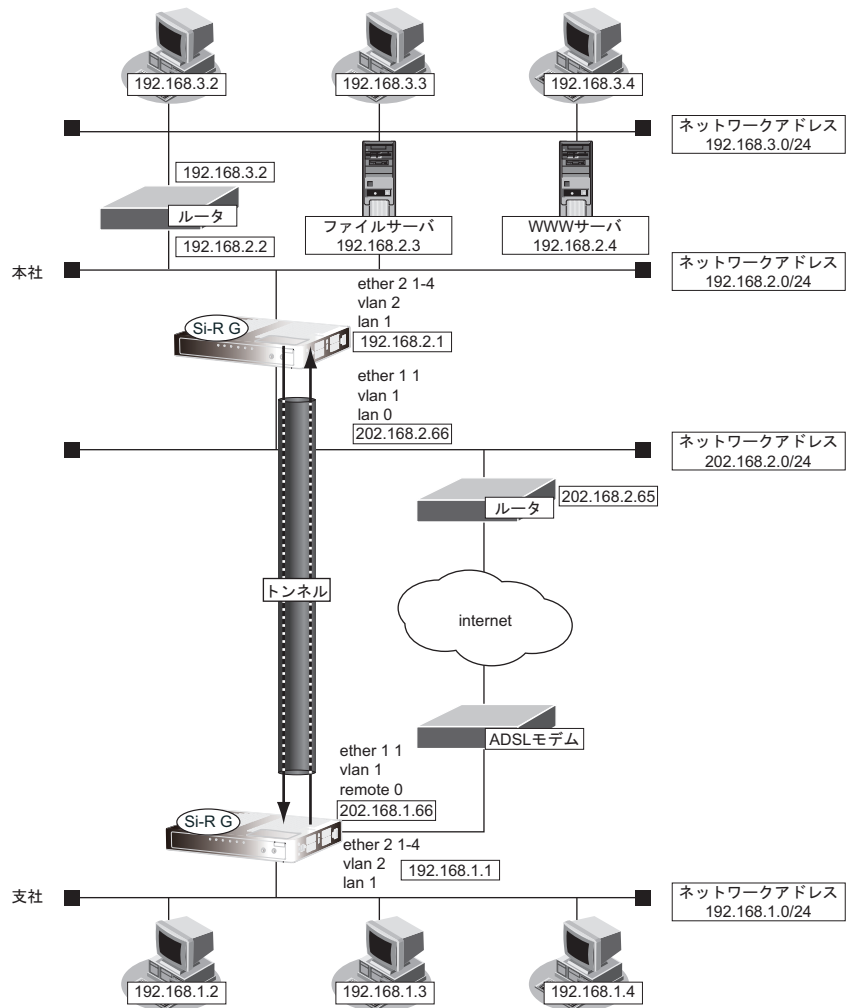
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip address local 202.168.1.66
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
```

**【本社】**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip route 0 192.168.3.0/24 192.168.2.2 1
# lan 1 vlan 2
```



● **設定条件**

**【支社】**

- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 (1) : any - 192.168.2.0/24 (マルチルーティングにも定義する)
- IPsec 対象範囲 (2) : any - 192.168.3.0/24



**[本社]**

- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 (1) : 192.168.2.0/24 - any (マルチルーティングにも定義する)
- IPsec 対象範囲 (2) : 192.168.3.0/24 - any

**[共通]**

- 鍵交換モード : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec PFS 時の DH グループ : なし
- IKE 共有鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方式 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証 (ハッシュ) アルゴリズム : hmac-md5
- IKE DH グループ : modp768 (グループ 1)

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

---

### ● コマンド

```

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ip route 1 192.168.3.0/24 1 1
# remote 1 ap 0 name honten1
# remote 1 ap 0 multiroute pattern 0 use any any 192.168.2.0/24 any 0 any
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.2.0/24
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 1 datalink type ipsec
# remote 1 ap 1 ipsec type ike
# remote 1 ap 1 ipsec ike protocol esp
# remote 1 ap 1 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 1 ipsec ike encrypt des-cbc
# remote 1 ap 1 ipsec ike auth hmac-md5
# remote 1 ap 1 ike bind ap 0

設定終了
# save
# commit

```

## 本社を設定する

### ● コマンド

VPNを設定する

```
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shiten
# remote 0 ap 0 multiroute pattern 0 use 192.168.2.0/24 any any any 0 any
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range 192.168.2.0/24 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 1 datalink type ipsec
# remote 0 ap 1 ipsec type ike
# remote 0 ap 1 ipsec ike protocol esp
# remote 0 ap 1 ipsec ike range 192.168.3.0/24 any4
# remote 0 ap 1 ipsec ike encrypt des-cbc
# remote 0 ap 1 ipsec ike auth hmac-md5
# remote 0 ap 1 ike bind ap 0

設定終了
# save
# commit
```

## 2.13.7 IPsec 機能と他機能との併用

IPsec 機能と他機能を併用する場合のいくつかの設定例を、以下に説明します。

ここでは、「1.8 複数の事業所 LAN を VPN (IPsec) で接続する」(P.33) 相当の設定が行われていることを前提とします。

- IPsec 変換前のマルチ NAT / IP フィルタリング / TOS 値書き換え機能
- IPsec 変換前のシェーピング機能と帯域制御 (WFQ) 機能
- IPsec 変換前の MSS 書き換え機能
- IPsec 変換前の MTU 分割機能
- 接続先監視機能
- 動的経路 (RIP) 機能
- IKE Dead Peer Detection (DPD) 機能



- 以下の機能については、IPv6 アドレスで使用することはできません。
  - IPsec 変換前のマルチ NAT 機能

### IPsec 変換前のマルチ NAT / IP フィルタリング / TOS 値書き換え機能との併用例

#### ● 設定条件

##### [支社]

- NAT の使用 : マルチ NAT を使用する
- グローバルアドレス : 192.168.1.1
- アドレス個数 : 1
- アドレス割当てタイマ : 5分
- IP フィルタリング : 支社 - 本社間の telnet / ftp 通信以外遮断
- TOS 値書き換え : ftp 通信を 0xa0 に変換

##### [本社]

- IP フィルタリング : 支社 - 本社間の telnet / ftp 通信以外遮断
- TOS 値書き換え : ftp 通信を 0xa0 に変換

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

```
# remote 1 ip nat mode multi 192.168.1.1 1

# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 1 ip filter 0 pass acl 0 out
# remote 1 ip filter 1 pass acl 1 in
# remote 1 ip filter 2 reject acl 2 any
# remote 1 ip tos 0 acl 3 a0
```

## 本社を設定する

### ● コマンド

```
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 6 any
# acl 0 tcp any 21,23 yes
# acl 1 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 1 tcp 21,23 any no
# acl 2 ip any any any any
# acl 3 ip 192.168.2.0/24 192.168.1.0/24 6 any
# acl 3 tcp any 20,21 yes

# remote 0 ip filter 0 pass acl 0 in
# remote 0 ip filter 1 pass acl 1 out
# remote 0 ip filter 2 reject acl 2 any
# remote 0 ip tos 0 acl 3 a0
```

## IPsec 変換前のシェーピング機能と帯域制御 (WFQ) 機能の併用例

### ● 設定条件

#### [本社]

- ・ シェーピングレート : 2Mbps
- ・ 帯域制御対象送信元IPアドレス : 192.168.2.0/24
- ・ 帯域制御対象送信元ポート番号 : すべて
- ・ 帯域制御対象あて先IPアドレス : 192.168.1.0/24
- ・ 帯域制御対象あて先ポート番号 : すべて
- ・ 帯域制御対象プロトコル : TCP
- ・ 帯域制御対象TOS値 : すべて
- ・ 割り当て帯域 : 最優先

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本社を設定する

### ● コマンド

```
# remote 0 shaping on 2m
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 6 any
# remote 0 ip priority 0 acl 0 express
```

### こんな事に気をつけて

IPsec機能と帯域制御（WFQ）機能を併用する場合、IPsec前のパケットに対して帯域制御を行うときには、IPsec用のremoteで設定します。この場合、IPsec用のremoteでシェーピングを行うか、または、実回線のremoteでIPsec後のパケットに対して帯域制御を設定する必要があります。

## IPsec変換前のMSS書き換え機能との併用例

### ● 設定条件

#### [共通]

- MSS書き換え値 : 1414Byte

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

```
# remote 1 ip msschange 1414
```

## 本社を設定する

### ● コマンド

```
# remote 0 ip msschange 1414
```

## IPsec変換前のMTU分割機能との併用例

### ● 設定条件

#### [共通]

- MTU長 : 1460Byte

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

```
# remote 1 mtu 1460
```

## 本社を設定する

### ● コマンド

```
# remote 0 mtu 1460
```

## 接続先監視機能との併用例

### ● 設定条件

#### [支社]

- 送信元 IP アドレス : 192.168.1.1
- あて先 IP アドレス : 192.168.2.1
- タイムアウト時間 : 5 秒
- 正常時送信間隔 : 10 秒
- 異常時送信間隔 : 1 分



監視対象装置は、本社側 VPN 装置を指定します。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### 支社を設定する

### ● コマンド

```
# remote 1 ap 0 sessionwatch address 192.168.1.1 192.168.2.1
```

#### こんな事に気をつけて

- 接続先監視のあて先 IP アドレスは、remote ap ipsec ike range コマンドで設定する IPsec 対象パケット範囲に含まれる IP アドレスを指定してください。
- 接続先監視のあて先 IP アドレスに、常時運転している IPsec 対象の装置を指定してください。あて先 IP アドレスに相手 IKE サーバとは異なる装置を指定した場合、あて先 IP アドレスからの応答が受信できなくなります。その場合、相手 IKE サーバが生存していても IPsec/IKE SA は解放されます。そのため通信が不安定にあることがあります。

## 動的経路 (RIP) 機能との併用例

### ● 設定条件

#### [共通]

- RIP 送信 : v1
- RIP 受信 : v1
- RIP 送信時加算メトリック値 : 0

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### 支社を設定する

### ● コマンド

```
# delete remote 1 ip route  
# remote 1 ip rip use v1 v1 0 off
```

### 本社を設定する

### ● コマンド

```
# delete remote 0 ip route  
# remote 0 ip rip use v1 v1 0 off
```

## IKE Dead Peer Detection (DPD) 機能との併用例

---

### ● 設定条件

#### [共通]

- 無通信監視時間 : 10 秒
- 再送時間 : 1 秒
- 再送回数 : 3 回

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### 支社を設定する

#### ● コマンド

```
# remote 1 ap 0 ike dpd use on
# remote 1 ap 0 ike dpd idle 10s
# remote 1 ap 0 ike dpd retry 1s 3
```

### 本社を設定する

#### ● コマンド

```
# remote 0 ap 0 ike dpd use on
# remote 0 ap 0 ike dpd idle 10s
# remote 0 ap 0 ike dpd retry 1s 3
```

### こんな事に気をつけて

- DPD パケットの再送時間と再送回数は、「DPD パケット送信を開始する IPsec 受信パケット無通信監視時間」より短い時間を設定してください。  
再送時間 × (再送回数 + 1) < 無通信監視時間  
その範囲を超えた場合は、定義反映時に設定エラーとなります。
  - IKE Version1 で Dead Peer Detection (DPD) 機能を使用する場合、IKE でネゴシエーションする両方の装置で設定してください。設定されていない場合は、IKE ネゴシエーションで接続に失敗します。
-

## 2.13.8 テンプレート着信機能 (AAA 認証) を使用した 固定IPアドレスでのVPN

IPsec 機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN 終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.1.66/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

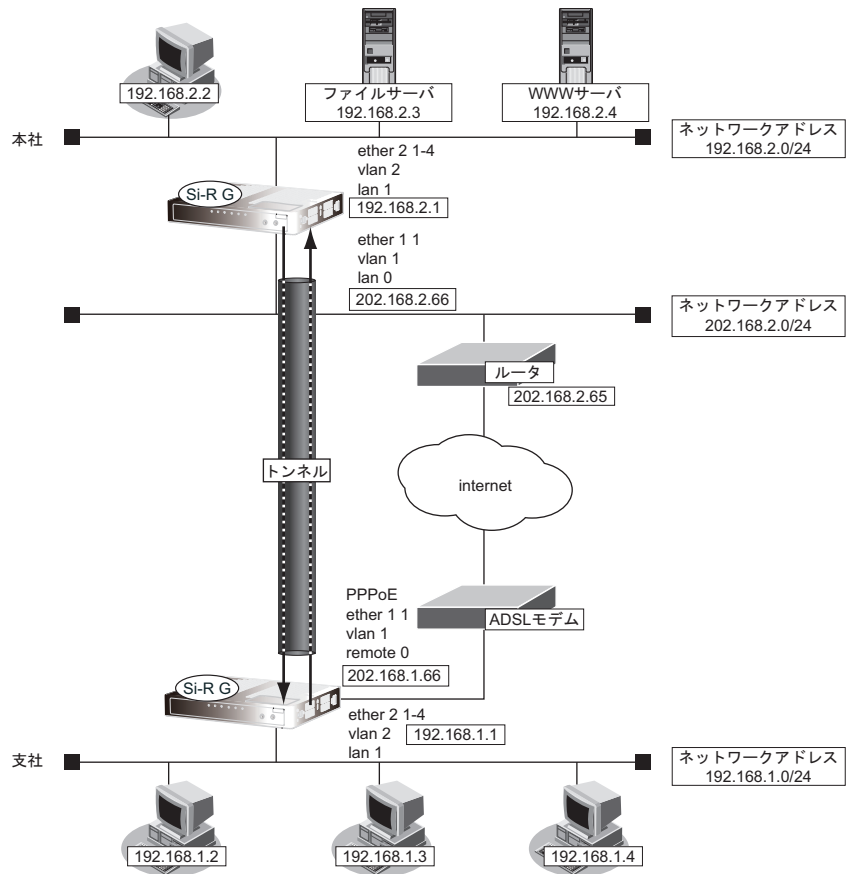


**【本社】**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● **設定条件**

**【支社】**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**【本社】**

- テンプレート名 : vpn-shi
- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

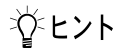
**【共通】**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp

- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DHグループ : なし
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DHグループ : modp768

### こんな事に気をつけて

- テンプレート着信機能 (AAA 認証) を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。  
Main Mode の場合 : 相手側 IPsec トンネルアドレス  
Aggressive Mode の場合 : 相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、  
template ipsec ike newsa responder off 0 の設定を推奨します。



### ヒント

#### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

#### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
```

```
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1
```

```
設定終了
# save
# reset
```

## 本社 (Responder) を設定する

### ● コマンド

VPN (テンプレート) を設定する

```
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode main
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66
```

AAA 情報を設定する

```
# aaa 0 name shisya
# aaa 0 user 0 id 202.168.1.66
# aaa 0 user 0 password 202.168.1.66
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 2
```

```
設定終了
# save
# reset
```

## 2.13.9 テンプレート着信機能 (AAA 認証) を使用した 可変IPアドレスでのVPN

IPsec機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワークIPv4アドレス : 192.168.1.1/24
- PPPoE ユーザ認証ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1

#### [本社]

- ローカルネットワークIPv4アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

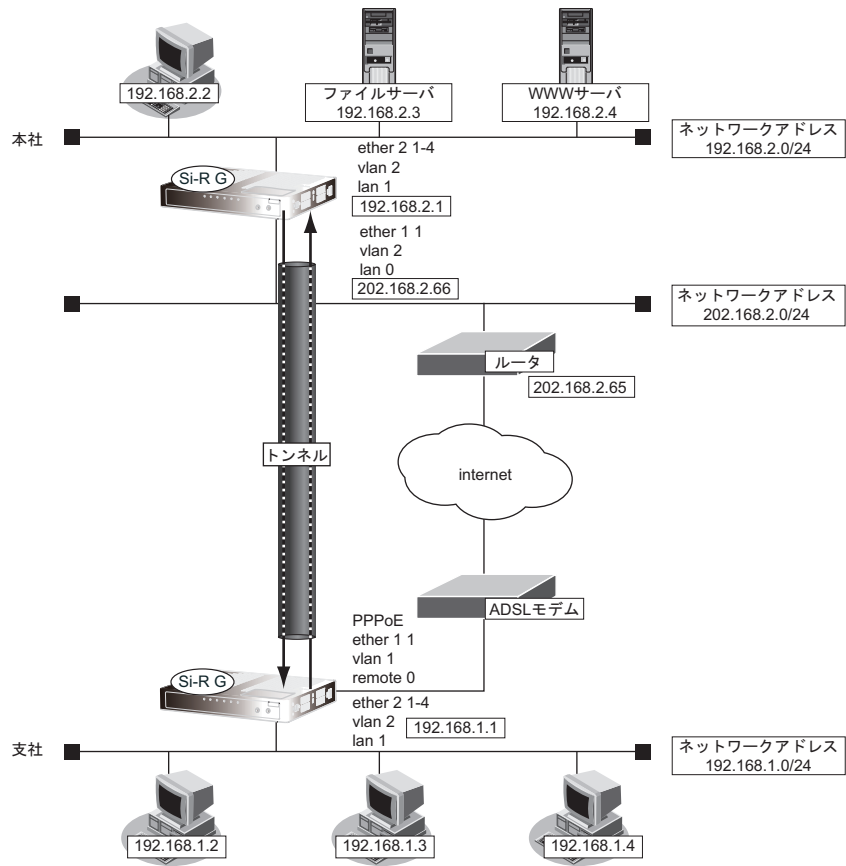
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**【本社】**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● **設定条件**

**【支社】**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**【本社】**


- テンプレート名 : vpn-shi
- IPsec/IKE 区間 : 202.168.2.66 - 支社
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**[共通]**

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

**こんな事に気をつけて**

- テンプレート着信機能 (AAA 認証) を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。  
Main Mode の場合 : 相手側 IPsec トンネルアドレス  
Aggressive Mode の場合 : 相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、  
template ipsec ike newsa responder off 0 の設定を推奨します。

 **ヒント****◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

**◆ ID タイプとは？**

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

インターネットから IPsec/IKE パケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject
```

VPN を設定する

```
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike idtype fqdn
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1
```

設定終了

```
# save
# reset
```

## 本社 (Responder) を設定する

### ● コマンド

VPN (テンプレート) を設定する

```
# template 0 name vpn-hon
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66
```

AAA 情報を設定する

```
# aaa 0 name shisya
# aaa 0 user 0 id shisya
# aaa 0 user 0 password shisya
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 2
```

設定終了

```
# save
# reset
```



## 2.13.10 テンプレート着信機能 (RADIUS 認証) を使用した 固定IPアドレスでのVPN

IPsec 機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN 終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.1.66/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

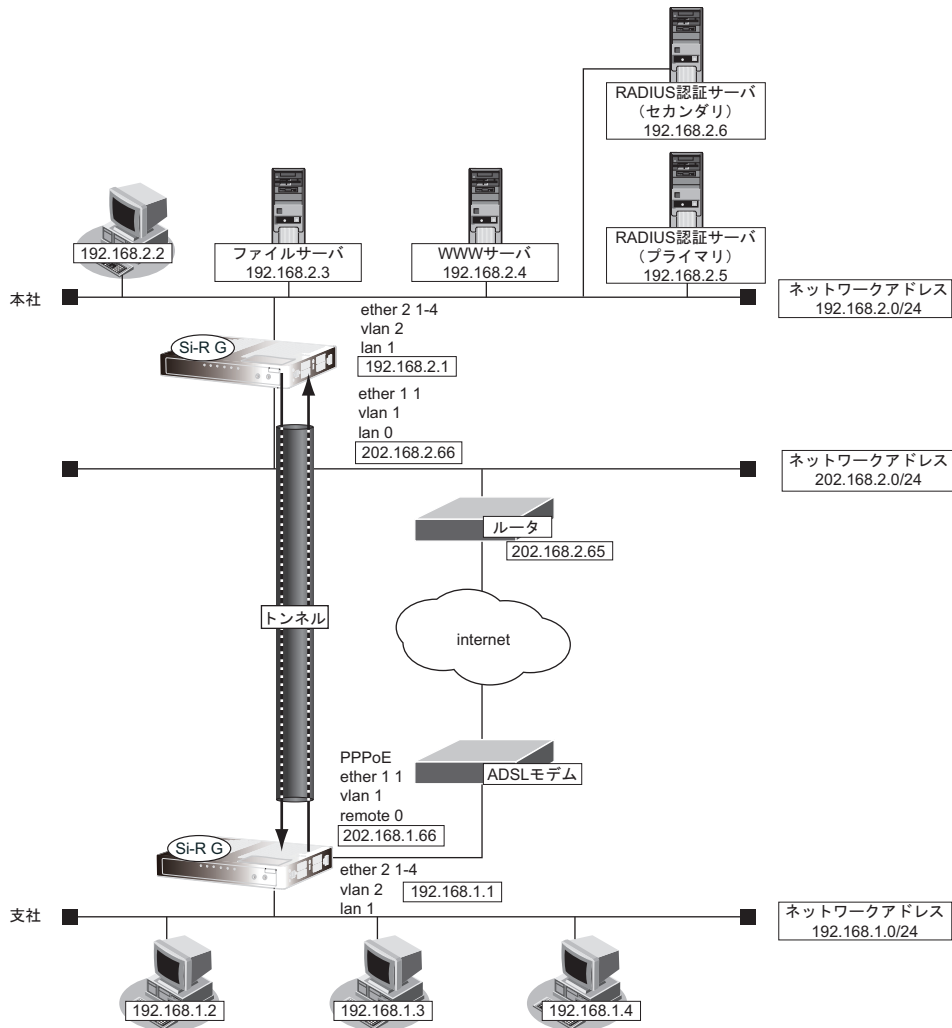
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

**[本社]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● **設定条件**

**[支社]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット

**【本社】**

- テンプレート名 : vpn-shi
- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- RADIUS サービス : クライアント機能  
: 認証、アカウントティング
- 自側認証 IP アドレス : 192.168.2.1
- 自側アカウントティング IP アドレス : 192.168.2.1
- 認証情報 1 (プライマリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.5
  - 復旧待機時間 : 30分
  - 優先度 : 0
- 認証情報 2 (セカンダリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.6
  - 復旧待機時間 : 30分
  - 優先度 : 100
- アカウントティング情報 1 (プライマリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.5
  - 復旧待機時間 : 30分
  - 優先度 : 0
- アカウントティング情報 2 (セカンダリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.6
  - 復旧待機時間 : 30分
  - 優先度 : 100

**【共通】**

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

### こんな事に気をつけて

- テンプレート着信機能 (RADIUS 認証) を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。  
Main Mode の場合 : 相手側 IPsec トンネルアドレス  
Aggressive Mode の場合 : 相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、  
template ipsec ike newsa responder off 0 の設定を推奨します。

### 💡 ヒント

#### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

#### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

```

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset

```

## 本社 (Responder) を設定する

### ● コマンド

VPN (テンプレート) を設定する

```
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode main
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66
```

AAA 情報を設定する

```
# aaa 0 name shisya
```

RADIUS クライアントに関する情報を設定する

```
# aaa 0 radius service client both
# aaa 0 radius auth source 192.168.2.1
# aaa 0 radius accounting source 192.168.2.1
# aaa 0 radius client server-info auth 0 secret 192.168.2.1
# aaa 0 radius client server-info auth 0 address 192.168.2.5
# aaa 0 radius client server-info auth 0 deadtime 30m
# aaa 0 radius client server-info auth 0 priority 0
# aaa 0 radius client server-info auth 1 secret 192.168.2.1
# aaa 0 radius client server-info auth 1 address 192.168.2.6
# aaa 0 radius client server-info auth 1 deadtime 30m
# aaa 0 radius client server-info auth 1 priority 100
# aaa 0 radius client server-info accounting 0 secret 192.168.2.1
# aaa 0 radius client server-info accounting 0 address 192.168.2.5
# aaa 0 radius client server-info accounting 0 deadtime 30m
# aaa 0 radius client server-info accounting 0 priority 0
# aaa 0 radius client server-info accounting 1 secret 192.168.2.1
# aaa 0 radius client server-info accounting 1 address 192.168.2.6
# aaa 0 radius client server-info accounting 1 deadtime 30m
# aaa 0 radius client server-info accounting 1 priority 100
```

設定終了

```
# save
# reset
```

## 2.13.11 テンプレート着信機能 (RADIUS 認証) を使用した 可変IPアドレスでのVPN

IPsec 機能とテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN 終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

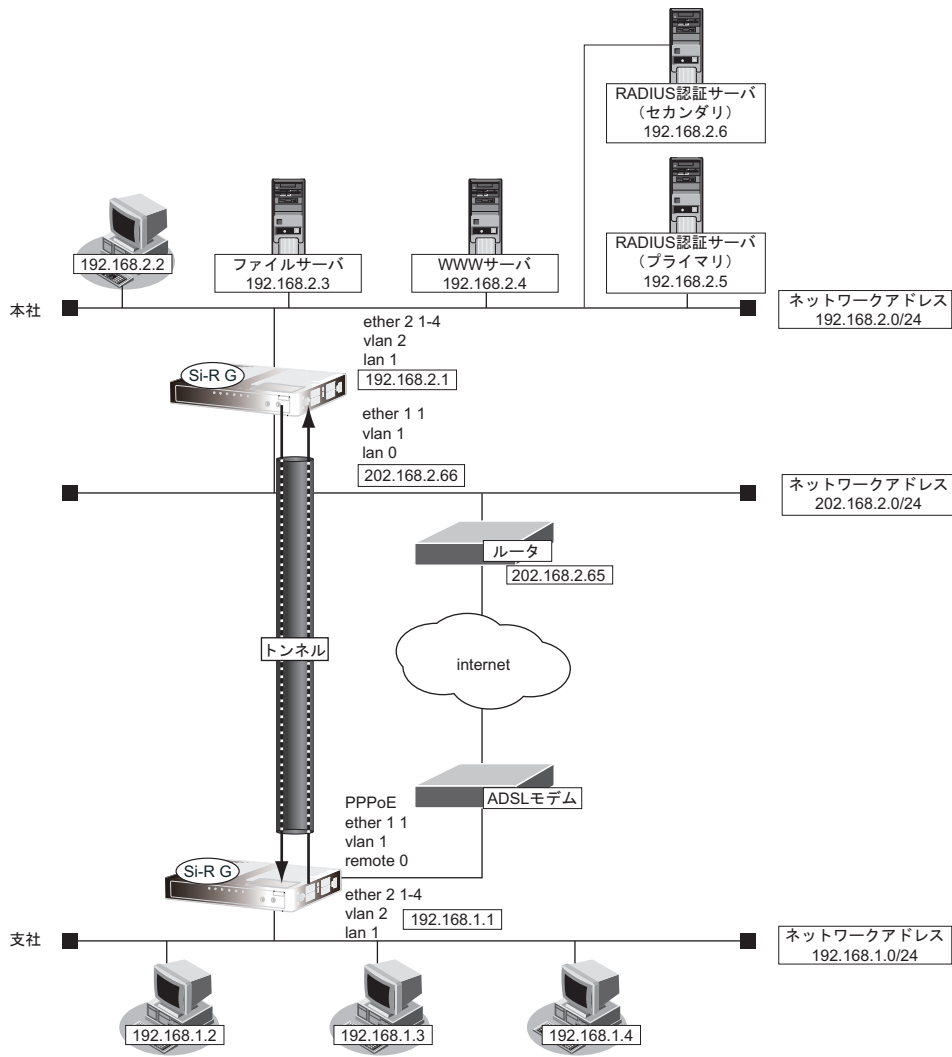
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**【本社】**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● **設定条件**

**【支社】**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**[本社]**

- テンプレート名 : vpn-shi
- IPsec/IKE 区間 : 202.168.2.66 - 支社
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- RADIUS サービス : クライアント機能  
: 認証、アカウントティング
- 自側認証 IP アドレス : 192.168.2.1
- 自側アカウントティング IP アドレス : 192.168.2.1
- 認証情報 1 (プライマリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.5
  - 復旧待機時間 : 30分
  - 優先度 : 0
- 認証情報 2 (セカンダリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.6
  - 復旧待機時間 : 30分
  - 優先度 : 100
- アカウントティング情報 1 (プライマリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.5
  - 復旧待機時間 : 30分
  - 優先度 : 0
- アカウントティング情報 2 (セカンダリ)
  - 共有鍵 : 192.168.2.1
  - サーバ IP アドレス : 192.168.2.6
  - 復旧待機時間 : 30分
  - 優先度 : 100

**[共通]**

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768



### こんな事に気をつけて

- テンプレート着信機能 (RADIUS 認証) を使用した IPsec では、RADIUS 認証サーバ側のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。  
Main Mode の場合 : 相手側 IPsec トンネルアドレス  
Aggressive Mode の場合 : 相手側の装置識別情報
- テンプレート着信側から IKE ネゴシエーションを行う場合、認証しないため、  
template ipsec ike newsa responder off 0 の設定を推奨します。

### 💡 ヒント

#### ◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

#### ◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

#### ◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

```

インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike idtype fqdn
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d

```

```
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

## 本社 (Responder) を設定する

### ● コマンド

```
VPN (テンプレート) を設定する
# template 0 name vpn-hon
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt des-cbc
# template 0 ipsec ike auth hmac-md5
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt des-cbc
# template 0 ike proposal 0 hash hmac-md5
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name shisya

RADIUS クライアントに関する情報を設定する
# aaa 0 radius service client both
# aaa 0 radius auth source 192.168.2.1
# aaa 0 radius accounting source 192.168.2.1
# aaa 0 radius client server-info auth 0 secret 192.168.2.1
# aaa 0 radius client server-info auth 0 address 192.168.2.5
# aaa 0 radius client server-info auth 0 deadtime 30m
# aaa 0 radius client server-info auth 0 priority 0
# aaa 0 radius client server-info auth 1 secret 192.168.2.1
# aaa 0 radius client server-info auth 1 address 192.168.2.6
# aaa 0 radius client server-info auth 1 deadtime 30m
# aaa 0 radius client server-info auth 1 priority 100
# aaa 0 radius client server-info accounting 0 secret 192.168.2.1
# aaa 0 radius client server-info accounting 0 address 192.168.2.5
# aaa 0 radius client server-info accounting 0 deadtime 30m
# aaa 0 radius client server-info accounting 0 priority 0
# aaa 0 radius client server-info accounting 1 secret 192.168.2.1
# aaa 0 radius client server-info accounting 1 address 192.168.2.6
# aaa 0 radius client server-info accounting 1 deadtime 30m
```

```
# aaa 0 radius client server-info accounting 1 priority 100
```

設定終了

```
# save
```

```
# reset
```

## 2.13.12 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4で固定IPアドレスでのVPN

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### 【支社A（PPPoE常時接続）】

- ローカルネットワークIPv4アドレス : 192.168.1.1/24
- PPPoEユーザ認証ID : userid1（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード : userpass1（プロバイダから提示された内容）
- PPPoEポート : ETHERグループ1ポート1
- NAT機能 : マルチNATを使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### 【支社B（PPPoE常時接続）】

- ローカルネットワークIPv4アドレス : 192.168.2.1/24
- PPPoEユーザ認証ID : userid2（プロバイダから提示された内容）
- PPPoEユーザ認証パスワード : userpass2（プロバイダから提示された内容）
- PPPoEポート : ETHERグループ1ポート1
- NAT機能 : マルチNATを使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### 【本社】

- ローカルネットワークIPv4アドレス : 192.168.0.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス : 202.168.2.65

**● 設定コマンド****[支社A (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[支社B (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

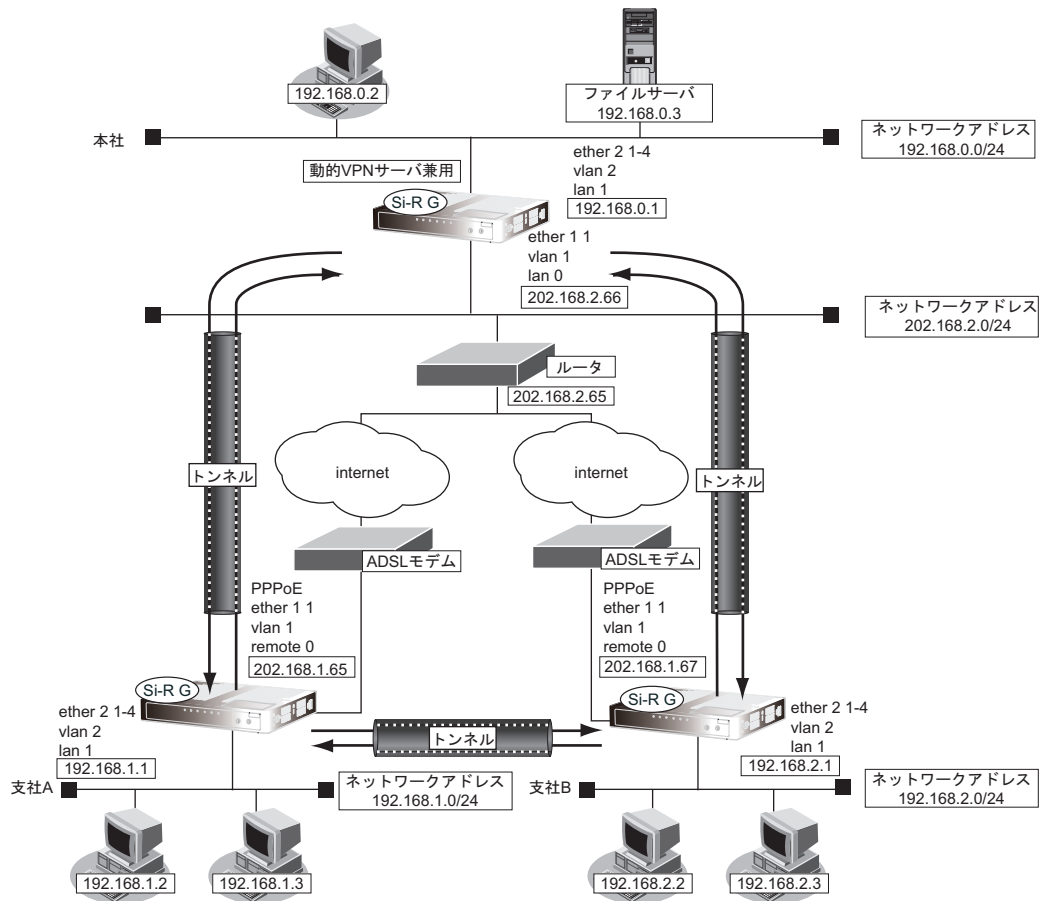
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[本社]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2
```



● 設定条件 (VPN 接続)

[支社 A (Initiator)]

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 支社 A - 202.168.2.66
- ・ IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- ・ IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ・ ESP のプライベートアドレス : 192.168.1.1
- ・ テンプレート名 : vpn-shiB
- ・ IPsec/IKE 始点 : インターネットプロバイダから割り当てられた IPv4 アドレスを使用する
- ・ 接続先監視アドレス : 192.168.1.1

[支社 B (Initiator)]

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 支社 B - 202.168.2.66
- ・ IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- ・ IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.2.1
- ・ ESP のプライベートアドレス : 192.168.2.1
- ・ テンプレート名 : vpn-shiA

- IPsec/IKE 始点 : インターネットプロバイダから割り当てられたIPv4アドレス を使用する
- 接続先監視アドレス : 192.168.2.1

#### **【本社 (Responder)】**

- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 202.168.2.66 - 支社A
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 202.168.2.66 - 支社B
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット

#### **【共通 (本社-支社A、B)】**

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 支社A ID/ID タイプ : shisyaA (自装置識別情報) /FQDN
- IKE 支社B ID/ID タイプ : shisyaB (自装置識別情報) /FQDN
- IKE 支社A IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社B IKE 認証鍵 : 1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

### **● 設定条件 (動的VPN接続)**

#### **【支社A】**

- クライアント情報 : 0
- サーバ情報
  - アドレス : 192.168.0.1
  - ポート番号 : 5070
  - 認証ID : shisyaAid
  - 認証パスワード : shisyaApass
- 有効期間 : 1時間
- セッション更新間隔 : 5分
- クライアントIPアドレス : 192.168.1.1
- ドメイン名 : example.com
- VPN通信
  - 利用インタフェース : rmt0
- 動的VPNクライアントの優先度 : 10
- 動的VPN IPv4 経路情報の優先度 : 1

**[支社B]**


- クライアント情報 : 0
- サーバ情報
  - アドレス : 192.168.0.1
  - ポート番号 : 5070
  - 認証ID : shisyaBid
  - 認証パスワード : shisyaBpass
- 有効期間 : 1時間
- セッション更新間隔 : 5分
- クライアントIPアドレス : 192.168.2.1
- ドメイン名 : example.com
- VPN通信
  - 利用インタフェース : rmt0
- 動的VPNクライアントの優先度 : 10
- 動的VPN IPv4 経路情報の優先度 : 1

**[本社]**

- サーバ機能 : 使用する
  - ドメイン名 : example.com
  - 認証 : 行う
  - AAAグループID : 0
- AAAユーザ情報 (支社A 認証情報)
  - ユーザID : shisyaAid
  - 認証パスワード : shisyaApass
- AAAユーザ情報 (支社B 認証情報)
  - ユーザID : shisyaBid
  - 認証パスワード : shisyaBpass

**[共通 (支社A-支社B)]**

- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : aes-cbc-128
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DH グループ : modp768
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : aes-cbc-128
- IKE 認証アルゴリズム : hmac-sha1
- IKE DHグループ : modp768

 ヒント**◆ DHグループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKEとは？**

自動鍵交換を行うためのプロトコルです。



**◆ IDタイプとは？**

Aggressive Modeの場合に、ネゴシエーションで使用する自装置を識別するIDの種別です。相手VPN装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社 A (Initiator) を設定する****● コマンド**

インターネットからIPsec/IKEパケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject
```

VPNを設定する

```
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 1
# remote 1 ip route 1 192.168.2.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any
```

動的VPN情報を定義する

```
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1
```

```
テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1

設定終了
# save
# reset
```

## 支社 B (Initiator) を設定する

### ● コマンド

```
インターネットから IPsec/IKE パケットを受信するように設定する
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
```

```
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.0.0/24 1 1
# remote 1 ip route 1 192.168.1.0/24 1 2
# remote 1 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any

動的VPN情報を設定する
# dvpn client 0 server 0 address 192.168.0.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

設定終了
# save
# reset
```

## 本社 (Responder) を設定する

### ● コマンド

```
VPNを設定する
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
```

```
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1
```

動的VPNサーバを設定する

```
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# dvpn server auth aaa 0
# aaa name dvpnserver
# aaa user 0 id shisyaAid
# aaa user 0 password shisyaApass
# aaa user 1 id shisyaBid
# aaa user 1 password shisyaBpass
```

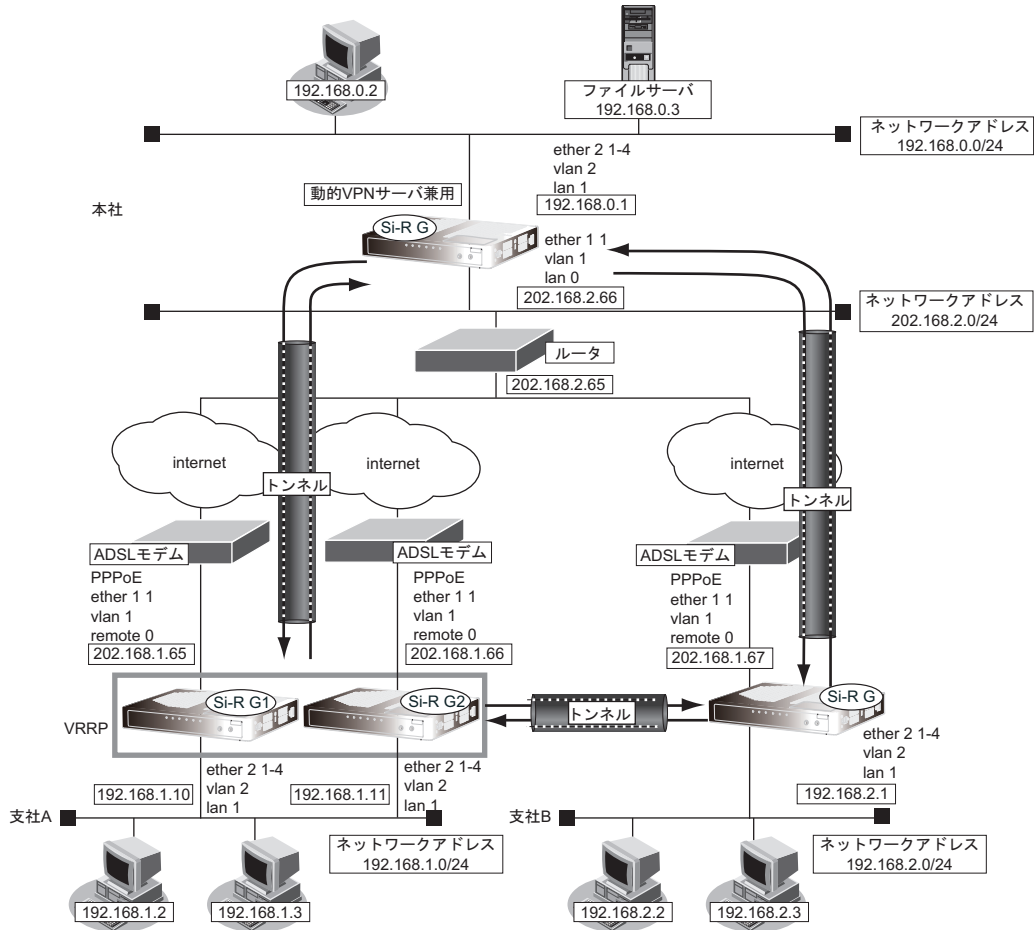
設定終了

```
# save
# reset
```

## 2.13.13 テンプレート着信機能（動的VPN）を使用した IPv4 over IPv4 で固定IPアドレスでのVPN（冗長構成）

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを冗長構成で構築する場合の設定方法を説明します。

ここでは「[2.13.12 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN](#)（P.208）」で説明したネットワーク構成で、支社と本社が動的VPNによって接続されていることを前提とします。ただし、支社AはVRRPによる冗長構成の設定を行います。



### ● 設定コマンド

#### 【支社A (Si-R G1)】

「[2.13.12 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN](#)」（P.208）で説明した支社Aの設定を事前に行います。

#### 【支社A (Si-R G2)】

「[2.13.12 テンプレート着信機能（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN](#)」（P.208）で説明した支社Aの設定を事前に行います。

**● 設定条件 (冗長構成)****[支社A (Si-R G1)]**

- ローカルネットワーク IPv4 アドレス : 192.168.1.10/24
- VRRP 優先度 : 254
- 動的VPNクライアントの優先度 : 1
- ノードダウントリガ : 202.168.2.66

**[支社A (Si-R G2)]**

- ローカルネットワーク IPv4 アドレス : 192.168.1.11/24
- VRRP 優先度 : 100
- 動的VPNクライアントの優先度 : 2

**[支社A (共通)]**

- VRRP 仮想 IP アドレス : 192.168.1.1/24
- VRRP グループ ID : 10

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社A (Si-R G1) を設定する****● コマンド**

```
# lan 1 ip address 192.168.1.10/24 3
# remote 0 ip nat static 0 192.168.1.10 500 any 500 17
# remote 0 ip nat static 1 192.168.1.10 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200
```

VRRP を設定する

```
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 trigger 0 node 202.168.2.66 any
```

動的VPN を設定する

```
# template 0 tunnel local 192.168.1.10
# template 0 sessionwatch address 192.168.1.10
# dvpn client 0 ua 192.168.1.10
# dvpn client priority 1
```

設定終了

```
# save
# reset
```

## 支社A (Si-R G2) を設定する

### ● コマンド

```
# lan 1 ip address 192.168.1.11/24 3
# remote 0 ip nat static 0 192.168.1.11 500 any 500 17
# remote 0 ip nat static 1 192.168.1.11 any any any 50
# remote 1 ip route 1 192.168.2.0/24 1 200
# remote 1 ap 0 ike name local shisyaa
```

VRRP を設定する

```
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 192.168.1.1
```

OSPF を設定する

```
# lan 1 ip ospf use on 0
# routemanage ip redist ospf static on 20 type2
# ospf ip area 0 id 0.0.0.0
```

動的VPNを設定する

```
# template 0 tunnel local 192.168.1.11
# template 0 sessionwatch address 192.168.1.11
# dvpn client 0 ua 192.168.1.11
# dvpn client priority 2
```

設定終了

```
# save
# reset
```

## 本社を設定する

### ● コマンド

```
# remote 0 ip route 0 192.168.1.0/24 1 10
# remote 0 ap 0 sessionwatch address 192.168.0.1 192.168.1.10
# remote 2 name vpn-shia
# remote 2 ap 0 name shisyaa
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaa
# remote 2 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.1.0/24 1 254
```

設定終了

```
# save
# reset
```

## 2.13.14 テンプレート着信機能（動的VPN）を使用した IPv6 over IPv6 で固定IPアドレスでのVPN

IPsec機能、動的VPN情報交換機能およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### 【支社A（PPPoE常時接続）】

- ローカルネットワークIPv4アドレス : 192.168.1.1/24
- ローカルネットワークIPv6アドレス : 2001:db8:1111:3::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.1.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス : 2001:db8:1111:1::66/64
- PPPoE ユーザ認証ID : userid1（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード : userpass1（プロバイダから提示された内容）
- PPPoE ポート : ETHERグループ1ポート1

#### 【支社B（PPPoE常時接続）】

- ローカルネットワークIPv4アドレス : 192.168.2.1/24
- ローカルネットワークIPv6アドレス : 2001:db8:1111:5::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.1.67/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス : 2001:db8:1111:1::67/64
- PPPoE ユーザ認証ID : userid2（プロバイダから提示された内容）
- PPPoE ユーザ認証パスワード : userpass2（プロバイダから提示された内容）
- PPPoE ポート : ETHERグループ1ポート1

#### 【本社】

- ローカルネットワークIPv4アドレス : 192.168.0.1/24
- ローカルネットワークIPv6アドレス : 2001:db8:1111:4::1/64
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.2.66/24
- インターネットプロバイダから割り当てられた固定IPv6アドレス : 2001:db8:1111:2::66/64
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス : 202.168.2.65
- インターネットプロバイダから指定されたデフォルトルートのIPv6アドレス : 2001:db8:1111:2::65



**● 設定コマンド****[支社 A (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:3::1/64
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::66/64
# remote 0 ipv6 route 0 default 1 1
```

**[支社 B (PPPoE 常時接続)]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:5::1/64
# lan 1 vlan 2

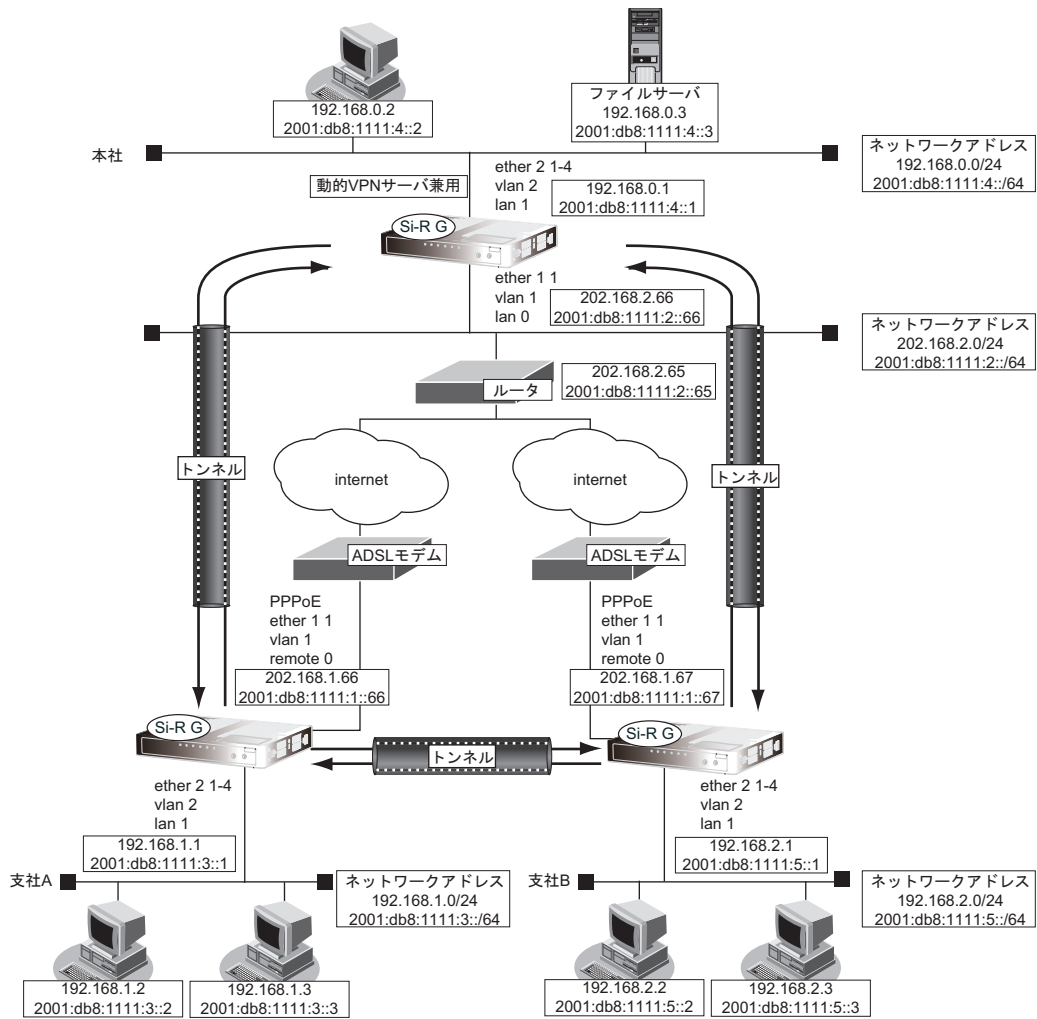
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ipv6 use on
# remote 0 ipv6 address 0 2001:db8:1111:1::67/64
# remote 0 ipv6 route 0 default 1 1
```

**[本社]**

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1111:2::66/64
# lan 0 ipv6 route 0 default 2001:db8:1111:2::65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:1111:4::1/64
```



## ● 設定条件 (VPN 接続)

### [支社A]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 2001:db8:1111:1::66 - 2001:db8:1111:2::66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- テンプレート名 : vpn-shiB
- IPsec/IKE 始点 : インターネットプロバイダから割り当てられた固定IPv6アドレスを使用する
- 接続先監視アドレス : 2001:db8:1111:3::1

### [支社B]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 2001:db8:1111:1::67 - 2001:db8:1111:2::66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- テンプレート名 : vpn-shiA
- IPsec/IKE 始点 : インターネットプロバイダから割り当てられた固定IPv6アドレスを使用する
- 接続先監視アドレス : 2001:db8:1111:5::1

### [本社]

- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 2001:db8:1111:2::66 - 2001:db8:1111:1::66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 2001:db8:1111:2::66 - 2001:db8:1111:1::67
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

### [共通 (本社-支社A、B)]

- 鍵交換タイプ : Main Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 支社 A IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社 B IKE 認証鍵 : 1234567890abcdefghijklmnopqrstuvwxyz
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

**● 設定条件 (動的VPN接続)****[支社A]**

- クライアント情報 : 0
- サーバ情報
  - アドレス : 2001:db8:1111:4::1
  - ポート番号 : 5070
  - 認証ID : shisyaAid
  - 認証パスワード : shisyaApass
- 有効期間 : 1時間
- セッション更新間隔 : 5分
- クライアントIPアドレス : 2001:db8:1111:3::1
- ドメイン名 : example.com
- VPN通信
  - 利用インタフェース : rmt0
- 動的VPNクライアントの優先度 : 10
- 動的VPN IPv6経路情報の優先度 : 1

**[支社B]**


- クライアント情報 : 0
- サーバ情報
  - アドレス : 2001:db8:1111:4::1
  - ポート番号 : 5070
  - 認証ID : shisyaBid
  - 認証パスワード : shisyaBpass
- 有効期間 : 1時間
- セッション更新間隔 : 5分
- クライアントIPアドレス : 2001:db8:1111:5::1
- ドメイン名 : example.com
- VPN通信
  - 利用インタフェース : rmt0
- 動的VPNクライアントの優先度 : 10
- 動的VPN IPv6経路情報の優先度 : 1

**[本社]**

- サーバ機能 : 使用する
  - ドメイン名 : example.com
  - 認証 : 行う
  - AAAグループID : 0
- AAAユーザ情報 (支社A 認証情報)
  - ユーザID : shisyaAid
  - 認証パスワード : shisyaApass
- AAAユーザ情報 (支社B 認証情報)
  - ユーザID : shisyaBid
  - 認証パスワード : shisyaBpass

**[共通 (支社A-支社B)]**

- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : aes-cbc-128
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DHグループ : modp768
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : aes-cbc-128
- IKE 認証アルゴリズム : hmac-sha1
- IKE DHグループ : modp768

 ヒント

## ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

## ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**支社Aを設定する**

## ● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1 1
```

```

# remote 1 ipv6 route 1 2001:db8:1111:5::/64 1 2
# remote 1 ipv6 dvpn 0 invite acl 0 64 0
# acl 0 ipv6 2001:db8:1111:3::/64 2001:db8:1111:5::/64 any any

動的VPN情報を設定する
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:3::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:3::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ipv6 route distance 1

テンプレート情報を設定する
# template 0 name vpn-shiB
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipv6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::66
# template 0 sessionwatch address 2001:db8:1111:3::1

設定終了
# save
# reset

```

## 支社Bを設定する

### ● コマンド

```

VPNを設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0

```

```
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxy
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:1::67
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1 1
# remote 1 ipv6 route 1 2001:db8:1111:3::/64 1 2
# remote 1 ipv6 dvpn 0 invite acl 0 64 0
# acl 0 ipv6 2001:db8:1111:5::/64 2001:db8:1111:3::/64 any any
```

#### 動的VPN情報を設定する

```
# dvpn client 0 server 0 address 2001:db8:1111:4::1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 expire register 1h
# dvpn client 0 expire session 5m
# dvpn client 0 ua 2001:db8:1111:5::1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 2001:db8:1111:5::/64
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ipv6 route distance 1
```

#### テンプレート情報を設定する

```
# template 0 name vpn-shiA
# template 0 mtu 1500
# template 0 idle 0d
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipv6 use on
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 tunnel local 2001:db8:1111:1::67
# template 0 sessionwatch address 2001:db8:1111:5::1
```

#### 設定終了

```
# save
# reset
```

## 本社を設定する

### ● コマンド

VPNを設定する

```
# remote 0 name vpn-shiA
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs off
# remote 0 ap 0 ipsec ike lifetime 8h
# remote 0 ap 0 ipsec ike lifebyte 0
# remote 0 ap 0 ipsec ike newsa initiator 90s 0
# remote 0 ap 0 ipsec ike newsa responder 30s 0
# remote 0 ap 0 ike mode main
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike proposal 0 hash hmac-md5
# remote 0 ap 0 ike proposal 0 pfs modp768
# remote 0 ap 0 ike proposal 0 lifetime 1d
# remote 0 ap 0 ike retry 10s 3
# remote 0 ap 0 ike release on
# remote 0 ap 0 ike initial forward
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:3::/64 1 1
# remote 1 name vpn-shiB
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs off
# remote 1 ap 0 ipsec ike lifetime 8h
# remote 1 ap 0 ipsec ike lifebyte 0
# remote 1 ap 0 ipsec ike newsa initiator 90s 0
# remote 1 ap 0 ipsec ike newsa responder 30s 0
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 hash hmac-md5
# remote 1 ap 0 ike proposal 0 pfs modp768
# remote 1 ap 0 ike proposal 0 lifetime 1d
# remote 1 ap 0 ike retry 10s 3
# remote 1 ap 0 ike release on
# remote 1 ap 0 ike initial forward
# remote 1 ap 0 tunnel local 2001:db8:1111:2::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:1::67
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:5::/64 1 1
```



## 動的VPNサーバを設定する

```
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# dvpn server auth aaa 0
# aaa name dvpnserver
# aaa user 0 id shisyaAid
# aaa user 0 password shisyaApass
# aaa user 1 id shisyaBid
# aaa user 1 password shisyaBpass
```

## 設定終了

```
# save
# reset
```

## 2.13.15 NAT トラバーサルを使用した可変IPアドレスでのVPN

接続するたびにIPアドレスが変わる環境でNATトラバーサルを使って、VPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

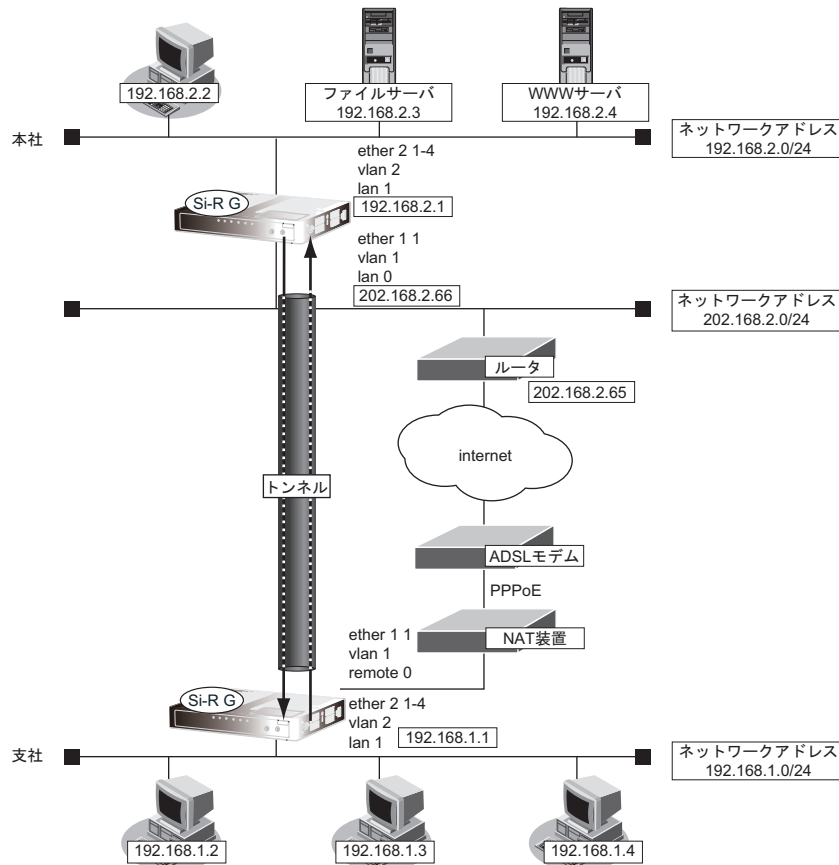
### ● 前提条件

#### 【支社 (PPPoE 常時接続)】

- ローカルネットワークIPv4アドレス : 192.168.1.1/24
- PPPoE ユーザ認証ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1

#### 【本社】

- ローカルネットワークIPv4アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス : 202.168.2.65



## ● 設定条件

### [支社]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 - 202.168.2.66
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット

### [本社]

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 202.168.2.66 - 支社
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット

### [共通]

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : aes-cbc-256
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DH グループ : なし
- IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : aes-cbc-256
- IKE 認証アルゴリズム : hmac-sha1
- IKE DH グループ : modp768
- IKE NAT トラバーサル機能 : 使用する

## 💡 ヒント

### ◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

### ◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

### ◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

```
PPPoE を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip msschange 1414

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike nat-traversal use on
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# commit
```

## 本社 (Responder) を設定する

### ● コマンド

LAN を設定する

```
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2
```

# delete lan

```
# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```

VPN を設定する

```
# remote 0 name vpn-shi
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt aes-cbc-256
# remote 0 ap 0 ipsec ike auth hmac-sha1
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 0 ap 0 ike proposal 0 hash hmac-sha1
# remote 0 ap 0 ike nat-traversal use on
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 1
```

設定終了

```
# save
# commit
```

## 2.13.16 テンプレート着信機能 (AAA 認証) および NAT トラバーサルを使用した可変 IP アドレスでの VPN

IPsec 機能、テンプレート機能および NAT トラバーサルを使って、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

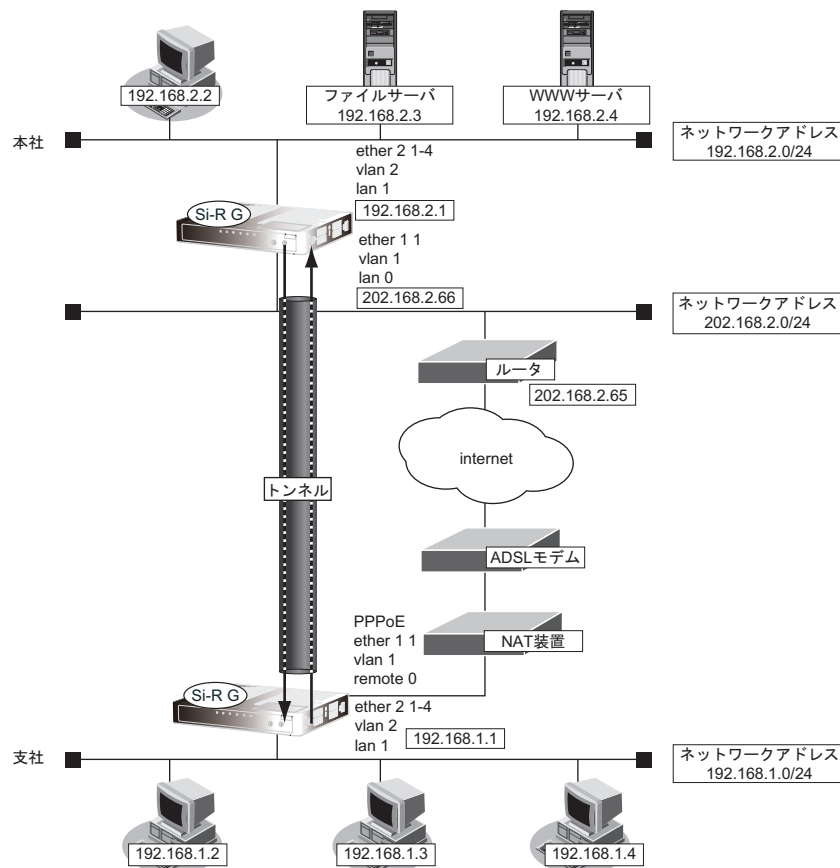
### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65



## ● 設定条件

### [支社]

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 支社 - 202.168.2.66
- ・ IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット

### [本社]

- ・ テンプレート名 : vpn-shi
- ・ IPsec/IKE 区間 : 202.168.2.66 - 支社
- ・ IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット

### [共通]

- ・ 鍵交換タイプ : Aggressive Mode
- ・ IPsec プロトコル : esp
- ・ IPsec 暗号アルゴリズム : aes-cbc-256
- ・ IPsec 認証アルゴリズム : hmac-sha1
- ・ IPsec DH グループ : なし
- ・ IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- ・ IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- ・ IKE 認証方法 : pre-shared (事前共有鍵方式)
- ・ IKE 暗号アルゴリズム : aes-cbc-256
- ・ IKE 認証アルゴリズム : hmac-sha1
- ・ IKE DH グループ : modp768
- ・ IKE NAT トラバーサル機能 : 使用する

### こんな事に気をつけて

- ・ テンプレート着信機能 (AAA 認証) を使用した IPsec では、AAA 設定のユーザ ID とユーザ認証パスワードを同じに設定してください。
- ・ ユーザ ID とユーザ認証パスワードは、テンプレート情報の IKE 情報の交換モードにより以下のように設定します。  
Main Mode の場合 : 相手側 IPsec トンネルアドレス  
Aggressive Mode の場合 : 相手側の装置識別情報

### ヒント

#### ◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

#### ◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

#### ◆ ID タイプとは？

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

```
PPPoE を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip msschange 1414

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike nat-traversal use on
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# commit
```



## 本社 (Responder) を設定する

### ● コマンド

```
LAN を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

VPN (テンプレート) を設定する
# template 0 name vpn-shi
# template 0 combine use aaa
# template 0 datalink type ipsec
# template 0 interface pool 1 1
# template 0 aaa 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-256
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs off
# template 0 ipsec ike lifetime 8h
# template 0 ipsec ike lifebyte 0
# template 0 ipsec ike newsa initiator 90s 0
# template 0 ipsec ike newsa responder off 0
# template 0 ike mode aggressive
# template 0 ike idtype fqdn
# template 0 ike proposal 0 encrypt aes-cbc-256
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike proposal 0 lifetime 1d
# template 0 ike retry 10s 3
# template 0 ike release on
# template 0 ike nat-traversal use on
# template 0 tunnel local 202.168.2.66

AAA 情報を設定する
# aaa 0 name vpn-shi
# aaa 0 user 0 id shisya
# aaa 0 user 0 ipsec ike range any4 any4
# aaa 0 user 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# aaa 0 user 0 ip route 0 192.168.1.0/24 1 2

設定終了
# save
# commit
```

## 2.13.17 接続先情報（動的VPN）を使用したIPv4 over IPv4で固定IPアドレスでのVPN

IPsec機能、動的VPN情報交換機能、接続先およびテンプレート機能を使って、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社および本社はPPPoEでインターネットに接続され、動的VPNサーバはグローバルアドレス空間の終端装置として本装置が接続されていることを前提とします。

### ● 前提条件

#### [本社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.0.1/24
- PPPoE ユーザ認証 ID : userid0 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass0 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1
- NAT 機能 : マルチ NAT を使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### [支社 A (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1
- NAT 機能 : マルチ NAT を使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### [支社 B (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- PPPoE ユーザ認証 ID : userid2 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass2 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1
- NAT 機能 : マルチ NAT を使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### [動的VPNサーバ]

- ローカルネットワーク IPv4 アドレス : 192.168.10.1/24
- ローカルネットワーク ETHER ポート : ETHER グループ 2 ポート 1~4
- ローカルネットワーク ETHER ポート VLAN : 2
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65
- インターネット接続 ETHER ポート : ETHER グループ 1 ポート 1
- インターネット接続 ETHER ポート VLAN : 1

**● 設定コマンド****[本社 (PPPoE 常時接続)]**

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid0 userpass0
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[支社 A (PPPoE 常時接続)]**

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[支社 B (PPPoE 常時接続)]**

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
```

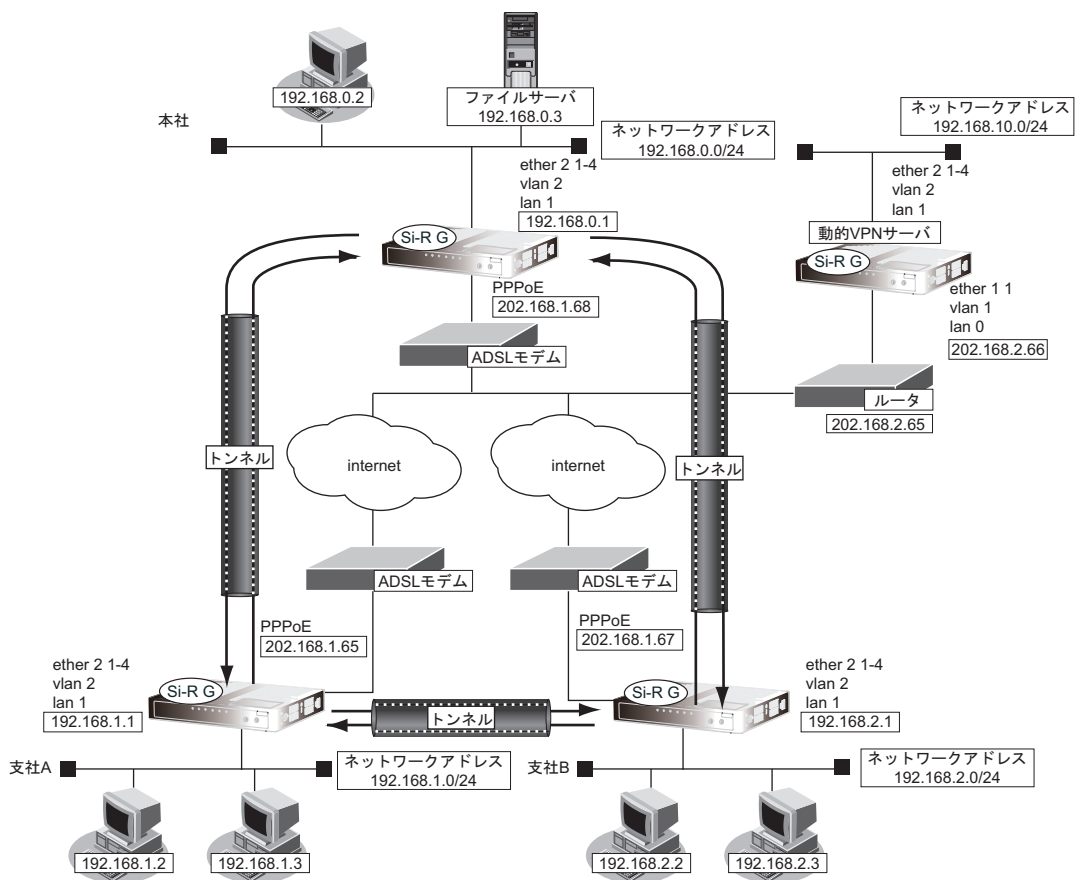
```
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[動的VPNサーバ]**

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.10.1/24 3
# lan 1 vlan 2
```



● 設定条件 (動的VPNサーバ-本社、支社A、B)

**[本社 (Initiator)]**

- ネットワーク名 : vpn-srv
- 接続先名 : dvpn-srv
- IPsec/IKE 区間 : 本社 - 202.168.2.66
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.0.1
- ESPのプライベートアドレス : 192.168.0.1

**【支社A (Initiator)】**

- ネットワーク名 : vpn-srv
- 接続先名 : dvpn-srv
- IPsec/IKE 区間 : 支社A - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESP のプライベートアドレス : 192.168.1.1

**【支社B (Initiator)】**

- ネットワーク名 : vpn-srv
- 接続先名 : dvpn-srv
- IPsec/IKE 区間 : 支社B - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.2.1
- ESP のプライベートアドレス : 192.168.2.1

**【動的VPNサーバ (Responder)】**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.2.66 - 本社
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 202.168.2.66 - 支社A
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 202.168.2.66 - 支社B
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

**【共通 (本社、支社A、B-動的VPNサーバ)】**

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 本社 ID/ID タイプ : honsya (自装置識別情報) /FQDN
- IKE 支社A ID/ID タイプ : shisyaA (自装置識別情報) /FQDN
- IKE 支社B ID/ID タイプ : shisyaB (自装置識別情報) /FQDN
- IKE 本社 IKE 認証鍵 : 1234567890ABCDEFGHIJKLMNQRSTUvwxyz
- IKE 支社A IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890
- IKE 支社B IKE 認証鍵 : 1234567890abcdefghijklmnopqrstuvwxyz

- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DHグループ : modp768

### ● 設定条件 (本社-支社 A、B)

#### [本社]

- テンプレート名 : vpn-shi
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.0.1
- ESPのプライベートアドレス : 192.168.0.1
- テンプレート接続先監視アドレス : 192.168.0.1

#### [支社A]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- テンプレート名 : vpn-shiB
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESPのプライベートアドレス : 192.168.1.1
- 接続先監視アドレス : 192.168.1.1-192.168.0.1
- テンプレート接続先監視アドレス : 192.168.1.1

#### [支社B]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- テンプレート名 : vpn-shiA
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.2.1
- ESPのプライベートアドレス : 192.168.2.1
- 接続先監視アドレス : 192.168.2.1-192.168.0.1
- テンプレート接続先監視アドレス : 192.168.2.1

### ● 設定条件 (動的VPN 接続)

#### [本社-支社 A/B 間の動的VPN 共通設定]

- クライアント情報 : 0
- サーバ情報  
アドレス : 192.168.10.1  
ポート番号 : 5070
- INVITE 自動 ignore 機能 : 使用する
- 有効期間 : 1 時間
- セッション更新間隔 : 5 分
- ドメイン名 : example.com
- VPN通信  
利用インタフェース : rmt0
- 動的VPNクライアントの優先度 : 10

- 動的VPN IPv4 経路情報の優先度 : 1
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : aes-cbc-128
- IPsec 認証アルゴリズム : hmac-sha1
- IPsecDH グループ : modp768
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : aes-cbc-128
- IKE 認証アルゴリズム : hmac-sha1
- IKE DHグループ : modp768

#### [本社の動的VPN設定]

- サーバ情報
  - 認証ID : honsyaId
  - 認証パスワード : honsyapass
- クライアントのIPアドレス (本社) : 192.168.0.1
- ローカルID : honsya

#### [支社Aの動的VPN設定]

- サーバ情報
  - 認証ID : shisyaAid
  - 認証パスワード : shisyaApass
- クライアントのIPアドレス (支社A) : 192.168.1.1

#### [支社Bの動的VPN設定]

- サーバ情報
  - 認証ID : shisyaBid
  - 認証パスワード : shisyaBpass
- クライアントのIPアドレス (支社B) : 192.168.2.1

#### [動的VPNサーバ設定]

- サーバ機能
  - ドメイン名 : example.com
  - 認証 : 行う
  - AAAグループID : 0
- AAAユーザ情報 (本社認証情報)
  - ユーザID : honsyaId
  - 認証パスワード : honsyapass
- AAAユーザ情報 (支社A 認証情報)
  - ユーザID : shisyaAid
  - 認証パスワード : shisyaApass
- AAAユーザ情報 (支社B 認証情報)
  - ユーザID : shisyaBid
  - 認証パスワード : shisyaBpass

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本社を設定する

### ● コマンド

インターネットからIPsec/IKEパケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.0.1 500 any 500 17
# remote 0 ip nat static 1 192.168.0.1 any any any 50
# remote 0 ip nat static default reject
```

本社-動的VPNサーバ間のVPNを設定する

```
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local honsya
# remote 1 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMN0PQRSTUVWXYZ
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1
```

本社-支社A/B間の動的VPNを設定する

```
# remote 0 ip dvpn 0 invite acl 0 24 0
# remote 0 ip dvpn 1 invite acl 1 24 0
# acl 0 ip 192.168.0.0/24 192.168.1.0/24 any any
# acl 1 ip 192.168.0.0/24 192.168.2.0/24 any any
# template 0 name vpn-shi
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMN0PQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.0.1
# template 0 sessionwatch address 192.168.0.1
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth honsyaid honsyapass
# dvpn client 0 ua 192.168.0.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.0.0/24 on
# dvpn client 0 localid honsya
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1
```

設定終了

```
# save
# reset
```



## 支社Aを設定する

### ● コマンド

インターネットからIPsec/IKEパケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject
```

支社A-動的VPNサーバ間のVPNを設定する

```
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1
```

本社-支社A間の動的VPNを設定する

```
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.1.1
# remote 2 ap 0 sessionwatch address 192.168.1.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.2.0/24 1 2
```

支社間の動的VPNを設定する

```
# remote 2 ip dvpn 0 autoignore
# remote 2 ip dvpn 1 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any
# template 0 name vpn-shiB
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
```

```
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1
```

動的VPN（共通部分）を設定する

```
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1
```

設定終了

```
# save
# reset
```

## 支社Bを設定する

### ● コマンド

インターネットからIPsec/IKEパケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject
```

支社B-動的VPNサーバ間のVPNを設定する

```
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxy
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1
```

本社-支社B間の動的VPNを設定する

```
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 tunnel local 192.168.2.1
# remote 2 ap 0 sessionwatch address 192.168.2.1 192.168.0.1
```

```
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.1.0/24 1 2

支社間の動的VPNを設定する
# remote 2 ip dvpn 0 autoignore
# remote 2 ip dvpn 1 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any
# template 0 name vpn-shiA
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

## 動的VPNサーバを設定する

### ● コマンド

VPNを設定する

```
# remote 0 name vpn-hon
# remote 0 ap 0 name honsya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote honsya
# remote 0 ap 0 ike shared key text 1234567890ABCDEFGHIJKLMNQPQRSTUVWXYZ
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.0.0/24 1 1
# remote 1 name vpn-shi
# remote 1 ap 0 name shisyaA
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1
# remote 2 name vpn-shiB
# remote 2 ap 0 name shisyaB
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaB
# remote 2 ap 0 ike shared key text 1234567890abcdefghijklmnopqrstuvwxyz
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.2.0/24 1 1
```

動的VPNサーバを設定する

```
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# aaa 0 name dvpnserver
# aaa 0 user 0 id honsyaid
# aaa 0 user 0 password honsyapass
# aaa 0 user 1 id shisyaAid
# aaa 0 user 1 password shisyaApass
# aaa 0 user 2 id shisyaBid
# aaa 0 user 2 password shisyaBpass
```

設定終了

```
# save
# reset
```

## 2.13.18 RSA デジタル署名認証を使用した固定IPアドレスでのVPN (自動鍵交換)

RSA デジタル署名認証を使用した、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支店はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

また、事前に [\[2.39 PKI機能を使う\] \(P.413\)](#) で証明書関連情報の設定が行われている必要があります。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- ローカルネットワークポート : ETHERグループ2ポート1~4
- ローカルネットワークポート VLAN : 2
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.1.66/24
- PPPoE ユーザ認証ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1
- PPPoE ポート VLAN : 1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス : 202.168.2.65

### ● 設定コマンド

#### [支社 (PPPoE 常時接続)]

```
# delete ether 1
# delete ether 2
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

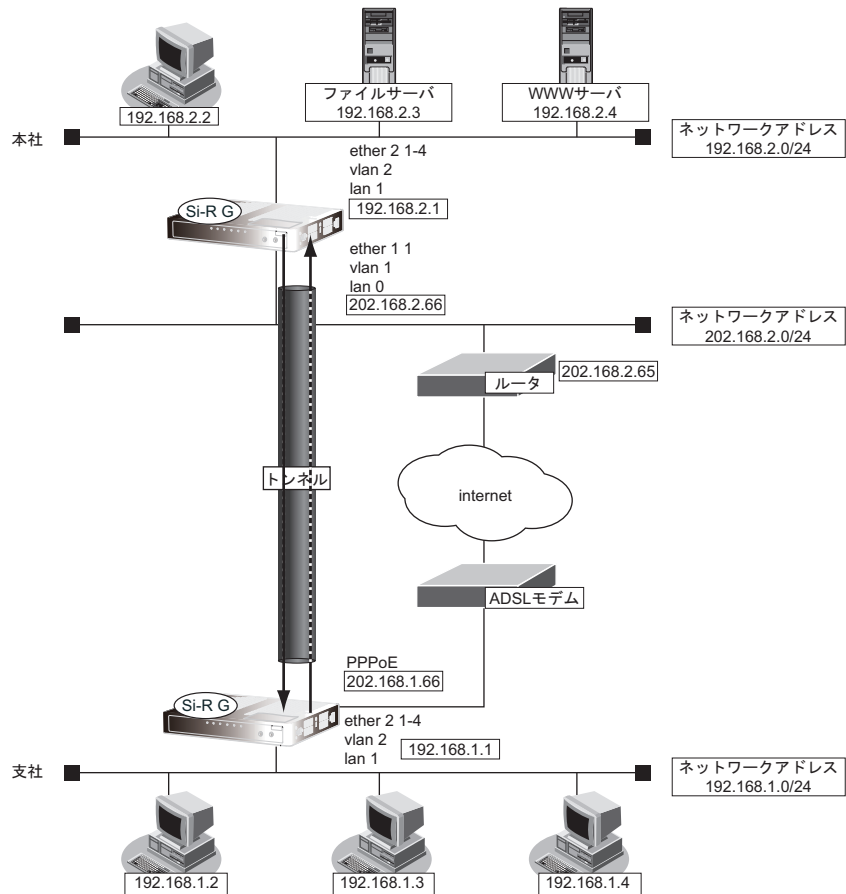
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

**[本社]**

```
# delete ether 1
# delete ether 2
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2
# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● **設定条件**

**[支社]**


- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- 相手装置証明書識別番号 : なし
- 自装置証明書識別番号 : 0
- 秘密識別番号 : 0

**【本社】**

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- 相手装置証明書識別番号 : なし
- 自装置証明書識別番号 : 0
- 秘密識別番号 : 0

**【共通】**

- 鍵交換タイプ : Main Mode
- 自装置証明書情報の送信 : 証明書要求ペイロード受信時
- 証明書要求 : 送信する
- 認証局識別番号 : なし
- 有効期限切れ証明書 : 使用する
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 認証方法 : rsa-signature (RSA デジタル署名)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

---

### ● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# reset
```

## 本社 (Responder) を設定する

---

### ● コマンド

```
VPN を設定する
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.1.66
# remote 1 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# reset
```



## 2.13.19 RSA デジタル署名認証を使用した可変IPアドレスでのVPN (自動鍵交換)

RSA デジタル署名認証を使用した、自動鍵交換でVPNを構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支店はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

また、事前に [\[2.39 PKI機能を使う\] \(P.413\)](#) で証明書関連情報の設定が行われている必要があります。

### ● 前提条件

#### [支社 (PPPoE 接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- ローカルネットワーク接続ポート : ETHERグループ2ポート1~4
- ローカルネットワーク接続ポート VLAN : 2
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループ1ポート1
- PPPoE ポート VLAN : 1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- ローカルネットワークポート : ETHERグループ2ポート1~4
- ローカルネットワークポート VLAN : 2
- インターネットプロバイダから割り当てられた固定IPv4アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートのIPv4アドレス : 202.168.2.65
- インターネット接続ポート : ETHERグループ1ポート1
- インターネット接続ポート VLAN : 1

### ● 設定コマンド

#### [支社 (PPPoE 接続)]

```
# delete ether 1
# delete ether 2
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

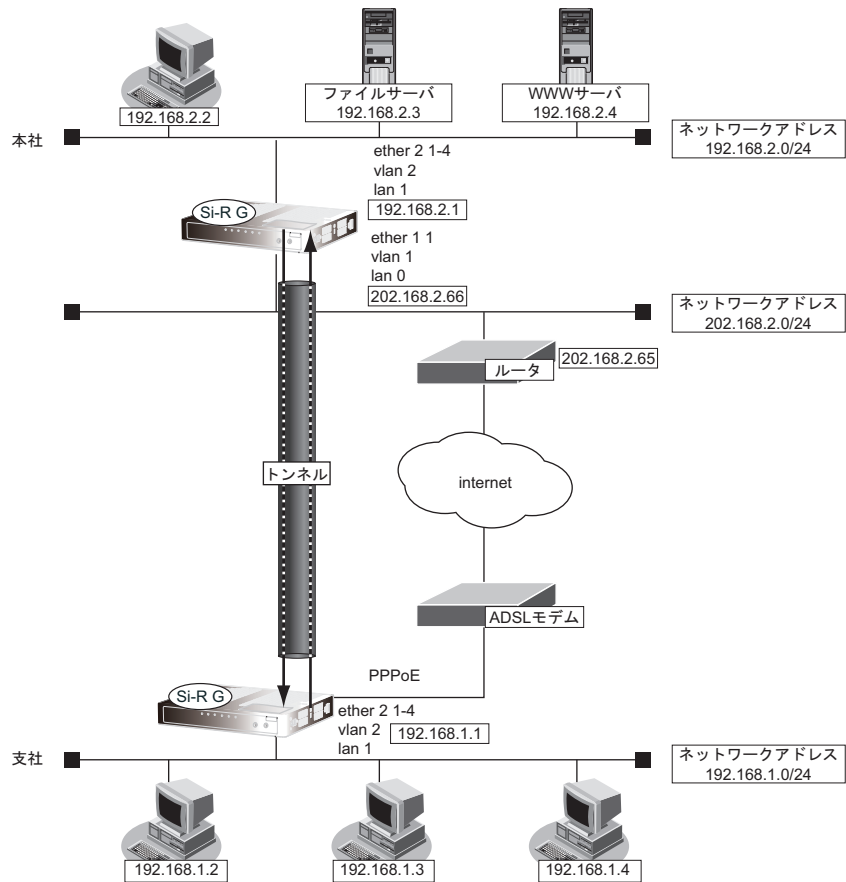
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[本社]**

```
# delete ether 1
# delete ether 2
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2
```



● **設定条件**

**[支社]**


- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- 相手装置証明書識別番号 : なし
- 自装置証明書識別番号 : 0
- 秘密識別番号 : 0

**【本社】**

- テンプレート名 : vpn-shi
- IPsec/IKE 区間 : 202.168.2.66 - 支社
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- 相手装置証明書識別番号 : なし
- 自装置証明書識別番号 : 0
- 秘密識別番号 : 0

**【共通】**

- 鍵交換タイプ : Aggressive Mode
- 自装置証明書情報の送信 : 証明書要求ペイロード受信時
- 証明書要求 : 送信する
- 認証局識別番号 : なし
- 有効期限切れ証明書 : 使用する
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- IKE 認証方法 : rsa-signature (RSA デジタル署名)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

**◆ ID タイプとは？**

Aggressive Mode の場合に、ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

インターネットから IPsec/IKE パケットを受信する設定をする

```
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject
```

VPN を設定する

```
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1
```

設定終了

```
# save
# reset
```

## 本社 (Responder) を設定する

### ● コマンド

VPN を設定する

```
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike name remote shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1
```

設定終了

```
# save
# reset
```

## 2.13.20 RSA デジタル署名認証で接続先情報（動的VPN）を使用した IPv4 over IPv4 で固定 IP アドレスでの VPN

IPsec 機能、動的VPN 情報交換機能、接続先およびテンプレート機能を使って、自動鍵交換でVPN を構築し、RSA デジタル署名認証をする場合の設定方法を説明します。

ここでは以下のコマンドによって、支社および本社は PPPoE でインターネットに接続され、動的VPN サーバはグローバルアドレス空間の終端装置として本装置が接続されていることを前提とします。

また、事前に [\[2.39 PKI 機能を使う\] \(P.413\)](#) で証明書関連情報の設定が行われている必要があります。

### ● 前提条件

#### [本社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.0.1/24
- PPPoE ユーザ認証 ID : userid0 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass0 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1
- NAT 機能 : マルチ NAT を使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### [支社 A (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1
- NAT 機能 : マルチ NAT を使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### [支社 B (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- PPPoE ユーザ認証 ID : userid2 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass2 (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1
- NAT 機能 : マルチ NAT を使用する
- ネットワーク名 : internet
- 接続先名 : ISP-1

#### [動的VPN サーバ]

- ローカルネットワーク IPv4 アドレス : 192.168.10.1/24
- ローカルネットワーク ETHER ポート : ETHER グループ 2 ポート 1~4
- ローカルネットワーク ETHER ポート VLAN : 2
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65
- インターネット接続 ETHER ポート : ETHER グループ 1 ポート 1
- インターネット接続 ETHER ポート VLAN : 1

**● 設定コマンド****[本社 (PPPoE 常時接続)]**

インターネットから IPsec/IKE パケットを受信する設定をする

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.0.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid0 userpass0
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[支社 A (PPPoE 常時接続)]**

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1 userpass1
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[支社B (PPPoE 常時接続)]**

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

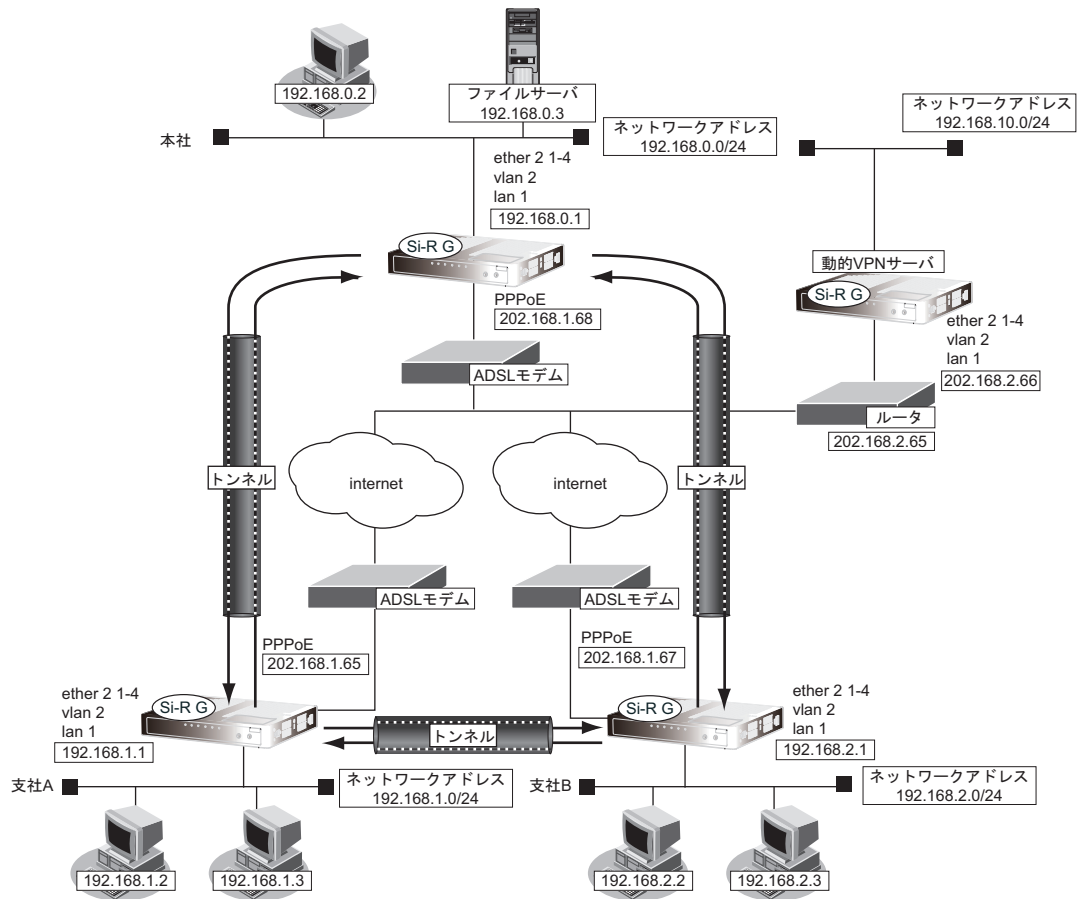
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2 userpass2
# remote 0 ap 0 keep connect
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
# remote 0 ip nat mode multi any 1 5m
```

**[動的VPNサーバ]**

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.10.1/24 3
# lan 1 vlan 2
```



● 設定条件 (動的VPNサーバ-本社、支社A、B)

【本社 (Initiator)】

- ネットワーク名 : vpn-srv
- 接続先名 : dvpn-srv
- IPsec/IKE 区間 : 本社 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.0.1
- ESP のプライベートアドレス : 192.168.0.1

【支社A (Initiator)】

- ネットワーク名 : vpn-srv
- 接続先名 : dvpn-srv
- IPsec/IKE 区間 : 支社A - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESP のプライベートアドレス : 192.168.1.1

【支社B (Initiator)】

- ネットワーク名 : vpn-srv
- 接続先名 : dvpn-srv
- IPsec/IKE 区間 : 支社B - 202.168.2.66



- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.2.1
- ESP のプライベートアドレス : 192.168.2.1

#### [動的VPNサーバ (Responder)]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.2.66 - 本社
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 202.168.2.66 - 支社 A
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 202.168.2.66 - 支社 B
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [共通 (本社、支社 A、B- 動的VPNサーバ)]

- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IKE 本社 ID/ID タイプ : honsya (自装置識別情報) /FQDN
- IKE 支社 A ID/ID タイプ : shisyaA (自装置識別情報) /FQDN
- IKE 支社 B ID/ID タイプ : shisyaB (自装置識別情報) /FQDN
- IKE 認証方法 : rsa-signature
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768
- 自装置証明書情報の送信 : 証明書要求ペイロード受信時
- 証明書要求 : 送信する
- 認証局識別番号 : なし
- 有効期限切れ証明書 : 使用する
- 相手装置証明書識別番号 : なし
- 自装置証明書識別番号 : 0
- 秘密識別番号 : 0

#### ● 設定条件 (本社 - 支社 A、B)

##### [本社]

- テンプレート名 : vpn-shi
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.0.1

- ESPのプライベートアドレス : 192.168.0.1
- テンプレート接続先監視アドレス : 192.168.0.1

**[支社A]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- テンプレート名 : vpn-shiB
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESPのプライベートアドレス : 192.168.1.1
- 接続先監視アドレス : 192.168.1.1 - 192.168.0.1
- テンプレート接続先監視アドレス : 192.168.1.1

**[支社B]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- テンプレート名 : vpn-shiA
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.2.1
- ESPのプライベートアドレス : 192.168.2.1
- 接続先監視アドレス : 192.168.2.1 - 192.168.0.1
- テンプレート接続先監視アドレス : 192.168.2.1

**[支社A]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- テンプレート名 : vpn-shiB
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESPのプライベートアドレス : 192.168.1.1
- 接続先監視アドレス : 192.168.1.1 - 192.168.0.1
- テンプレート接続先監視アドレス : 192.168.1.1

**[支社B]**

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- テンプレート名 : vpn-shiA
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.2.1
- ESPのプライベートアドレス : 192.168.2.1
- 接続先監視アドレス : 192.168.2.1 - 192.168.0.1
- テンプレート接続先監視アドレス : 192.168.2.1

**● 設定条件 (動的VPN接続)****[本社-支社A/B間の動的VPN共通設定]**

- クライアント情報 : 0

- サーバ情報
  - アドレス : 192.168.10.1
  - ポート番号 : 5070
- 有効期間 : 1時間
- セッション更新間隔 : 5分
- ドメイン名 : example.com
- VPN通信
  - 利用インタフェース : rmt0
- 動的VPNクライアントの優先度 : 10
- 動的VPN IPv4 経路情報の優先度 : 1
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : aes-cbc-128
- IPsec 認証アルゴリズム : hmac-sha1
- IPsecDH グループ : modp768
- IKE 認証方法 : rsa-signature
- IKE 暗号アルゴリズム : aes-cbc-128
- IKE 認証アルゴリズム : hmac-sha1
- IKE DH グループ : modp768

**[本社の動的VPN設定]**

- サーバ情報
  - 認証ID : honsyaid
  - 認証パスワード : honsyapass
- クライアントのIPアドレス (本社) : 192.168.0.1
- ローカルID : honsya

**[支社Aの動的VPN設定]**

- サーバ情報
  - 認証ID : shisyaAid
  - 認証パスワード : shisyaApass
- クライアントのIPアドレス (支社A) : 192.168.1.1

**[支社Bの動的VPN設定]**

- サーバ情報
  - 認証ID : shisyaBid
  - 認証パスワード : shisyaBpass
- クライアントのIPアドレス (支社B) : 192.168.2.1

**[動的VPNサーバ設定]**

- サーバ機能 : 使用する
- ドメイン名 : example.com
- 認証 : 行う
- AAAグループID : 0
- AAA ユーザ情報 (本社認証情報)
  - ユーザID : honsyaid
  - 認証パスワード : honsyapass

- AAAユーザ情報 (支社A 認証情報)
  - ユーザID : shisyaAid
  - 認証パスワード : shisyaApass
- AAAユーザ情報 (支社B 認証情報)
  - ユーザID : shisyaBid
  - 認証パスワード : shisyaBpass

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本社を設定する

### ● コマンド

インターネットからIPsec/IKEパケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.0.1 500 any 500 17
# remote 0 ip nat static 1 192.168.0.1 any any any 50
# remote 0 ip nat static default reject
```

本社-動的VPNサーバ間のVPNを設定する

```
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local honsya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1
```

本社-支社A/B間の動的VPNを設定する

```
# remote 0 ip dvpn 0 invite acl 0 24 0
# remote 0 ip dvpn 1 invite acl 1 24 0
# acl 0 ip 192.168.0.0/24 192.168.1.0/24 any any
# acl 1 ip 192.168.0.0/24 192.168.2.0/24 any any
# template 0 name vpn-shi
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike proposal 0 auth-method rsa-signature
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike certificate local 0
# template 0 ike certificate key 0
# template 0 tunnel local 192.168.0.1
# template 0 sessionwatch address 192.168.0.1
# dvpn client 0 server 0 address 192.168.10.1 5070
```

```
# dvpn client 0 server 0 auth honsyaid honsyapass
# dvpn client 0 ua 192.168.0.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.0.0/24 on
# dvpn client 0 localid honsya
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

## 支社Aを設定する

### ● コマンド

インターネットからIPsec/IKEパケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject
```

支社A-動的VPNサーバ間のVPNを設定する

```
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1
```

本社-支社A間の動的VPNを設定する

```
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike proposal 0 auth-method rsa-signature
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 ike certificate local 0
# remote 2 ap 0 ike certificate key 0
# remote 2 ap 0 tunnel local 192.168.1.1
# remote 2 ap 0 sessionwatch address 192.168.1.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.2.0/24 1 2
```

## 支社間の動的VPNを設定する

```
# remote 2 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.1.0/24 192.168.2.0/24 any any
# template 0 name vpn-shiB
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike proposal 0 auth-method rsa-signature
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike certificate local 0
# template 0 ike certificate key 0
# template 0 tunnel local 192.168.1.1
# template 0 sessionwatch address 192.168.1.1
```

## 動的VPN（共通部分）を設定する

```
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaAid shisyaApass
# dvpn client 0 ua 192.168.1.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.1.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1
```

## 設定終了

```
# save
# reset
```

## 支社Bを設定する

### ● コマンド

インターネットからIPsec/IKEパケットを受信するように設定する

```
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip nat static default reject
```

支社B-動的VPNサーバ間のVPNを設定する

```
# remote 1 name vpn-srv
# remote 1 ap 0 name dvpn-srv
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.10.0/24 1 1
```

本社-支社B間の動的VPNを設定する

```
# remote 2 name vpn-hon
# remote 2 ap 0 name honsya
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 dvpn client 0
# remote 2 ap 0 dvpn remotenet 0 192.168.0.0/24 off
# remote 2 ap 0 dvpn remoteid honsya
# remote 2 ap 0 ipsec type dvpn
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt aes-cbc-128
# remote 2 ap 0 ipsec ike auth hmac-sha1
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike proposal 0 auth-method rsa-signature
# remote 2 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 2 ap 0 ike proposal 0 hash hmac-sha1
# remote 2 ap 0 ike proposal 0 pfs modp768
# remote 2 ap 0 ike certificate local 0
# remote 2 ap 0 ike certificate key 0
# remote 2 ap 0 tunnel local 192.168.2.1
# remote 2 ap 0 sessionwatch address 192.168.2.1 192.168.0.1
# remote 2 ip route 0 192.168.0.0/24 1 1
# remote 2 ip route 1 192.168.1.0/24 1 2
```

支社間の動的VPNを設定する

```
# remote 2 ip dvpn 0 invite acl 0 24 0
# acl 0 ip 192.168.2.0/24 192.168.1.0/24 any any
# template 0 name vpn-shiA
# template 0 interface pool 10 10
# template 0 datalink type ipsec
# template 0 combine use dvpn
# template 0 dvpn client 0
# template 0 ipsec ike protocol esp
# template 0 ipsec ike encrypt aes-cbc-128
# template 0 ipsec ike auth hmac-sha1
# template 0 ipsec ike pfs modp768
# template 0 ike proposal 0 auth-method rsa-signature
```

```
# template 0 ike proposal 0 encrypt aes-cbc-128
# template 0 ike proposal 0 hash hmac-sha1
# template 0 ike proposal 0 pfs modp768
# template 0 ike certificate local 0
# template 0 ike certificate key 0
# template 0 tunnel local 192.168.2.1
# template 0 sessionwatch address 192.168.2.1

動的VPN（共通部分）を設定する
# dvpn client 0 server 0 address 192.168.10.1 5070
# dvpn client 0 server 0 auth shisyaBid shisyaBpass
# dvpn client 0 ua 192.168.2.1
# dvpn client 0 domain example.com
# dvpn client 0 localnet 0 192.168.2.0/24 on
# dvpn client 0 interface rmt 0
# dvpn client 0 priority 10
# dvpn client 0 ip route distance 1

設定終了
# save
# reset
```

## 動的VPNサーバを設定する

### ● コマンド

```
VPNを設定する
# remote 0 name vpn-hon
# remote 0 ap 0 name honsya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike mode aggressive
# remote 0 ap 0 ike name remote honsya
# remote 0 ap 0 ike proposal 0 auth-method rsa-signature
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 ike certificate local 0
# remote 0 ap 0 ike certificate key 0
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.0.0/24 1 1
# remote 1 name vpn-shi
# remote 1 ap 0 name shisyaA
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike name remote shisyaA
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1
# remote 2 name vpn-shiB
# remote 2 ap 0 name shisyaB
# remote 2 ap 0 datalink type ipsec
```



```
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ike mode aggressive
# remote 2 ap 0 ike name remote shisyaB
# remote 2 ap 0 ike proposal 0 auth-method rsa-signature
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 ike certificate local 0
# remote 2 ap 0 ike certificate key 0
# remote 2 ap 0 tunnel local 202.168.2.66
# remote 2 ip route 0 192.168.2.0/24 1 1
```

動的VPNサーバを設定する

```
# dvpn server use on
# dvpn server domain example.com
# dvpn server auth use on
# aaa 0 name dvpnsver
# aaa 0 user 0 id honsyaid
# aaa 0 user 0 password honsyapass
# aaa 0 user 1 id shisyaAid
# aaa 0 user 1 password shisyaApass
# aaa 0 user 2 id shisyaBid
# aaa 0 user 2 password shisyaBpass
```

設定終了

```
# save
# reset
```

## 2.13.21 IPv4 over IPv4 で NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)

「1.8.1 NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換)」(P.33) を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は「1.8.1 NAT と併用しない固定 IP アドレスでの VPN (自動鍵交換)」(P.33) と同じです。そちらを参照してください。

### ● 設定条件

#### 【支社 A】

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- ・ IPsec 対象範囲 : 192.168.1.0/24 - any4

#### 【支社 B】

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 202.168.3.66 - 202.168.2.66
- ・ IPsec 対象範囲 : 192.168.3.0/24 - any4

#### 【本社】

- ・ ネットワーク名 : vpn-shiA
- ・ 接続先名 : shisyaA
- ・ IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- ・ IPsec 対象範囲 : any4 - 192.168.1.0/24
- ・ ネットワーク名 : vpn-shiB
- ・ 接続先名 : shisyaB
- ・ IPsec/IKE 区間 : 202.168.2.66 - 202.168.3.66
- ・ IPsec 対象範囲 : any4 - 192.168.3.0/24


#### 【共通 A】

- ・ IKE Version : ikev2
- ・ IPsec プロトコル : esp
- ・ IPsec 暗号アルゴリズム : des-cbc
- ・ IPsec 認証アルゴリズム : hmac-md5
- ・ IPsec DH グループ : なし
- ・ IPsecV3 ESN : あり
- ・ IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- ・ IKE 認証方法 : pre-shared (事前共有鍵方式)
- ・ IKE 暗号アルゴリズム : des-cbc
- ・ IKE 認証アルゴリズム : hmac-md5
- ・ IKE DH グループ : modp768
- ・ IKE PRF アルゴリズム : hmac-md5

- IKE 支社 A ID タイプ : address
- IKE 本社 ID タイプ : address

**[共通 B]**

- IKE Version : ikev2
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : 3des-cbc
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DH グループ : なし
- IPsecV3 ESN : あり
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321 (文字列)
- IKE 認証方法 : shared
- IKE 暗号アルゴリズム : 3des-cbc
- IKE 認証アルゴリズム : hmac-sha1
- IKE DH グループ : modp1024
- IKE PRF アルゴリズム : hmac-sha1
- IKE 支社 B ID タイプ : address
- IKE 本社 ID タイプ : address

 ヒント**◆ DH グループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKE とは？**

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社Aを設定する

### ● コマンド

VPNを設定する

```
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5
```

設定終了

```
# save
# commit
```

## 支社Bを設定する

### ● コマンド

VPNを設定する

```
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.3.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1
```

設定終了

```
# save
# commit
```

## 本社を設定する

### ● コマンド

VPNを設定する

```
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.3.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1

設定終了
# save
# commit
```

## 2.13.22 IPv4 over IPv4 で NAT と併用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)

「1.8.3 NAT と併用した可変 IP アドレスでの VPN (自動鍵交換)」(P.46) を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は「1.8.3 NAT と併用した可変 IP アドレスでの VPN (自動鍵交換)」(P.46) と同じです。そちらを参照してください。

### ● 設定条件

#### 【支社 A (Initiator)】

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 A - 202.168.2.66
- IPsec 対象範囲 : 192.168.1.0/24 - any4
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESP のプライベートアドレス : 192.168.1.1

#### 【支社 B (Initiator)】

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 B - 202.168.2.66
- IPsec 対象範囲 : 192.168.3.0/24 - any4
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.3.1
- ESP のプライベートアドレス : 192.168.3.1

#### 【本社 (Responder)】

- ネットワーク名 : vpn-shiA
- 接続先名 : shisyaA
- IPsec/IKE 区間 : 202.168.2.66 - 支社 A
- IPsec 対象範囲 : any4 - 192.168.1.0/24
- ネットワーク名 : vpn-shiB
- 接続先名 : shisyaB
- IPsec/IKE 区間 : 202.168.2.66 - 支社 B
- IPsec 対象範囲 : any4 - 192.168.3.0/24

#### 【共通 A】

- IKE Version : ikev2
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IPsecV3 ESN : あり

- IKE 支社 A ID/ID タイプ : shisyaA (自装置名) /FQDN
- IKE 本社 ID タイプ : address
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768
- IKE PRF アルゴリズム : hmac-md5

#### [共通 B]

- IKE Version : ikev2
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : 3des-cbc
- IPsec 認証アルゴリズム : hmac-sha1
- IPsec DH グループ : なし
- IPsecV3 ESN : あり
- IKE 支社 B ID/ID タイプ : shisyaB (自装置名) /FQDN
- IKE 本社 ID タイプ : address
- IKE 認証鍵 : ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321 (文字列)
- IKE 認証方法 : shared
- IKE 暗号アルゴリズム : 3des-cbc
- IKE 認証アルゴリズム : hmac-sha1
- IKE DH グループ : modp1024
- IKE PRF アルゴリズム : hmac-sha1

#### 💡 ヒント

##### ◆ DH グループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

##### ◆ IKE とは？

自動鍵交換を行うためのプロトコルです。

##### ◆ ID タイプとは？

ネゴシエーションで使用する自装置を識別する ID の種別です。相手 VPN 装置の設定に合わせます。

#### こんな事に気をつけて

可変 IP アドレスでの VPN 接続を行うときは、インターネットプロバイダから割り当てられる IP アドレスが不定であるため、ローカルネットワーク IP アドレスで IKE ネゴシエーションを行う場合があります。このような運用では、送出インタフェースで NAT 機能を使用してください。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 A (Initiator) を設定する

### ● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisyaA
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

## 支社 B (Initiator) を設定する

### ● コマンド

```
インターネットから IPsec/IKE パケットを受信する設定をする
# remote 0 ip nat static 0 192.168.3.1 500 any 500 17
# remote 0 ip nat static 1 192.168.3.1 any any any 50

VPN を設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range 192.168.3.0/24 any4
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1

設定終了
# save
# commit
```



## 本社 (Responder) を設定する

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shiA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisyaA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 192.168.1.0/24
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype fqdn
# remote 0 ap 0 ike name remote shisyaA
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
# remote 1 name vpn-shiB
# remote 1 ip route 0 192.168.3.0/24 1 1
# remote 1 ap 0 name shisyaB
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype fqdn
# remote 1 ap 0 ike name remote shisyaB
# remote 1 ap 0 ike shared key text ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
# remote 1 ap 0 ike proposal encrypt 3des-cbc
# remote 1 ap 0 ike proposal hash hmac-sha1
# remote 1 ap 0 ike proposal pfs modp1024
# remote 1 ap 0 ike proposal prf hmac-sha1

設定終了
# save
# commit
```

## 2.13.23 IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)

[2.13.2 IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)] (P.163) を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [2.13.2 IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)] (P.163) と同じです。そちらを参照してください。

### ● 設定条件

#### [支社]

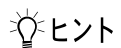
- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 2001:db8:1111:1::66 - 2001:db8:1111:2::66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [本社]

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 2001:db8:1111:2::66 - 2001:db8:1111:1::66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [共通]

- IKE Version : ikev2
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IPsec V3 ESN : あり
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768
- IKE PRF アルゴリズム : hmac-md5
- IKE 支社 ID タイプ : address
- IKE 本社 ID タイプ : address



### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

## 本社を設定する

---

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
```

設定終了

```
# save
# commit
```

## 2.13.24 IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)

[2.13.3 IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)] (P.167) を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [2.13.3 IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)] (P.167) と同じです。そちらを参照してください。

### ● 設定条件

#### [支社]

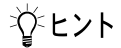
- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [本社]

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [共通]

- IKE Version : ikev2
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsecDH グループ : なし
- IPsecV3 ESN : あり
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768
- IKE PRF アルゴリズム : hmac-md5
- IKE 支社 ID タイプ : address
- IKE 本社 ID タイプ : address



### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

## 本社を設定する

---

### ● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

## 2.13.25 IPv6 over IPv4 で可変IPアドレスでのVPN (自動鍵交換 IKE Version2)

[2.13.4 IPv6 over IPv4 で可変IPアドレスでのVPN (自動鍵交換)] (P.171) を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [2.13.4 IPv6 over IPv4 で可変IPアドレスでのVPN (自動鍵交換)] (P.171) と同じです。そちらを参照してください。

### ● 設定条件

#### [支社 (Initiator)]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 - 202.168.2.66
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット
- IKE (UDP : 500 番ポート) のプライベートアドレス : 192.168.1.1
- ESP のプライベートアドレス : 192.168.1.1

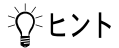
#### [本社 (Responder)]

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 202.168.2.66 - 支社
- IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [共通]

- IKE Version : ikev2
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IPsecV3 ESN : あり
- IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- IKE 本社 ID タイプ : address
- IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DH グループ : modp768
- IKE PRF アルゴリズム : hmac-md5



**◆ DHグループとは？**

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

**◆ IKEとは？**

自動鍵交換を行うためのプロトコルです。

**◆ IDタイプとは？**

ネゴシエーションで使用する自装置を識別するIDの種別です。相手VPN装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

**● コマンド**

```
インターネットからIPsec/IKEパケットを受信する設定をする
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

VPNを設定する
# remote 1 name vpn-hon
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:2::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

## 本社 (Responder) を設定する

### ● コマンド

VPN を設定する

```
# remote 0 name vpn-shi
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:1::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype fqdn
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
```

設定終了

```
# save
# commit
```

## 2.13.26 IPv6 over IPv6で固定IPアドレスでのVPN (自動鍵交換 IKE Version2)

[2.13.5 IPv6 over IPv6で固定IPアドレスでのVPN (自動鍵交換)] (P.175) をIKE Version2を使ってVPNを構築する場合の設定方法を説明します。

支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [2.13.5 IPv6 over IPv6で固定IPアドレスでのVPN (自動鍵交換)] (P.175) と同じです。そちらを参照してください。

### ● 設定条件

#### [支社]

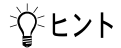
- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 2001:db8:1111:1::66 - 2001:db8:1111:2::66
- IPsec対象範囲 : IPsec相手情報を使用するすべてのパケット

#### [本社]

- ネットワーク名 : vpn-shi
- 接続先名 : shisya
- IPsec/IKE 区間 : 2001:db8:1111:2::66 - 2001:db8:1111:1::66
- IPsec対象範囲 : IPsec相手情報を使用するすべてのパケット

#### [共通]

- IKE Version : ikev2
- IPsecプロトコル : esp
- IPsec暗号アルゴリズム : des-cbc
- IPsec認証アルゴリズム : hmac-md5
- IPsec DHグループ : なし
- IPsecV3 ESN : あり
- IKE認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE認証方法 : pre-shared (事前共有鍵方式)
- IKE暗号アルゴリズム : des-cbc
- IKE認証アルゴリズム : hmac-md5
- IKE DHグループ : modp768
- IKE PRFアルゴリズム : hmac-md5
- IKE支社IDタイプ : address
- IKE本社IDタイプ : address



### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

VPN を設定する

```
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ipv6 use on
# remote 1 ipv6 route 0 2001:db8:1111:4::/64 1
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 2001:db8:1111:1::66
# remote 1 ap 0 tunnel remote 2001:db8:1111:2::66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any6 any6
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5
```

設定終了

```
# save
# commit
```

## 本社を設定する

### ● コマンド

```
VPN を設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 2001:db8:1111:3::/64 1
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 2001:db8:1111:2::66
# remote 0 ap 0 tunnel remote 2001:db8:1111:1::66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any6 any6
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5

設定終了
# save
# commit
```

## 2.13.27 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN (自動鍵交換 IKE Version2)

[2.13.6 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN (自動鍵交換)] (P.179) をIKE Version2を使ってVPNを構築する場合の設定方法を説明します。

支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [2.13.6 IPv4 over IPv4で1つのIKEセッションに複数のIPsecトンネル構成でのVPN (自動鍵交換)] (P.179) と同じです。そちらを参照してください。

### ● 設定条件

#### [支社]

- IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- IPsec 対象範囲 (1) : any - 192.168.2.0/24 (マルチルーティングにも定義する)
- IPsec 対象範囲 (2) : any - 192.168.3.0/24

#### [本社]

- IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- IPsec 対象範囲 (1) : 192.168.2.0/24 - any (マルチルーティングにも定義する)
- IPsec 対象範囲 (2) : 192.168.3.0/24 - any

#### [共通]

- IKE Version : ikev2
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec PFS 時の DH グループ : なし
- IPsecV3 ESN : あり
- IKE 共有鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- IKE 認証方式 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証 (ハッシュ) アルゴリズム : hmac-md5
- IKE DH グループ : modp768 (グループ 1)
- IKE PRF アルゴリズム : hmac-md5
- IKE 支社 ID タイプ : address
- IKE 本社 ID タイプ : address

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社を設定する

### ● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ip route 0 192.168.2.0/24 1 1
# remote 1 ip route 1 192.168.3.0/24 1 1
# remote 1 ap 0 name honten1
# remote 1 ap 0 multiroute pattern 0 use any any 192.168.2.0/24 any 0 any
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 192.168.2.0/24
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
# remote 1 ap 0 ike proposal prf hmac-md5
# remote 1 ap 1 datalink type ipsec
# remote 1 ap 1 ipsec type ikev2
# remote 1 ap 1 ipsec ike protocol esp
# remote 1 ap 1 ipsec ike range any4 192.168.3.0/24
# remote 1 ap 1 ipsec ike encrypt des-cbc
# remote 1 ap 1 ipsec ike auth hmac-md5
# remote 1 ap 1 ike bind ap 0

設定終了
# save
# commit
```

## 本社を設定する

### ● コマンド

```
VPNを設定する
# remote 0 name vpn-shi
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ap 0 name shiten
# remote 0 ap 0 multiroute pattern 0 use 192.168.2.0/24 any any any 0 any
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ap 0 tunnel remote 202.168.1.66
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range 192.168.2.0/24 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ike bind self
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype address
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal encrypt des-cbc
# remote 0 ap 0 ike proposal prf hmac-md5
# remote 0 ap 1 datalink type ipsec
# remote 0 ap 1 ipsec type ikev2
```

```
# remote 0 ap 1 ipsec ike protocol esp
# remote 0 ap 1 ipsec ike range 192.168.3.0/24 any4
# remote 0 ap 1 ipsec ike encrypt des-cbc
# remote 0 ap 1 ipsec ike auth hmac-md5
# remote 0 ap 1 ike bind ap 0
```

設定終了

```
# save
```

```
# commit
```



## 2.13.28 NAT トラバーサルを使用した可変 IP アドレスでの VPN (自動鍵交換 IKE Version2)

[2.13.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN] (P.230) を IKE Version2 を使って VPN を構築する場合の設定方法を説明します。

支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [2.13.15 NAT トラバーサルを使用した可変 IP アドレスでの VPN] (P.230) と同じです。そちらを参照してください。

### ● 設定条件

#### [支社 (Initiator)]


- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 支社 - 202.168.2.66
- ・ IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [本社 (Responder)]

- ・ ネットワーク名 : vpn-shi
- ・ 接続先名 : shisya
- ・ IPsec/IKE 区間 : 202.168.2.66 - 支社
- ・ IPsec 対象範囲 : IPsec 相手情報を使用するすべてのパケット

#### [共通]

- ・ IKE Version : ikev2
- ・ IPsec プロトコル : esp
- ・ IPsec 暗号アルゴリズム : aes-cbc-256
- ・ IPsec 認証アルゴリズム : hmac-sha1
- ・ IPsec DH グループ : なし
- ・ IPsecV3 ESN : あり
- ・ IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- ・ IKE 本社 ID タイプ : address
- ・ IKE 認証鍵 : abcdefghijklmnopqrstuvwxyz1234567890 (文字列)
- ・ IKE 認証方法 : pre-shared (事前共有鍵方式)
- ・ IKE 暗号アルゴリズム : aes-cbc-256
- ・ IKE 認証アルゴリズム : hmac-sha1
- ・ IKE DH グループ : modp768
- ・ IKE PRF アルゴリズム : hmac-sha1
- ・ IKE NAT トラバーサル機能 : 使用する

 ヒント

## ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

## ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

## ◆ IDタイプとは？

ネゴシエーションで使用する自装置を識別するIDの種別です。相手VPN装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

## ● コマンド

```
VPNを設定する
# delete remote 1
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt aes-cbc-256
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike proposal 0 prf hmac-sha1
# remote 1 ap 0 ike nat-traversal use on
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save
# commit
```

## 本社 (Responder) を設定する

### ● コマンド

```
LAN を設定する
# delete ether
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

# delete lan

# lan 0 ip address 202.168.2.66/24 3
# lan 0 ip route 0 default 202.168.2.65 1 1
# lan 0 vlan 1
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 2

VPN を設定する
# remote 0 name vpn-shi
# remote 0 ap 0 name shisya
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 ipsec type ikev2
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike encrypt aes-cbc-256
# remote 0 ap 0 ipsec ike auth hmac-sha1
# remote 0 ap 0 ike local-idtype address
# remote 0 ap 0 ike remote-idtype fqdn
# remote 0 ap 0 ike name remote shisya
# remote 0 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 0 ap 0 ike proposal 0 encrypt aes-cbc-256
# remote 0 ap 0 ike proposal 0 hash hmac-sha1
# remote 0 ap 0 ike proposal 0 prf hmac-sha1
# remote 0 ap 0 ike nat-traversal use on
# remote 0 ap 0 tunnel local 202.168.2.66
# remote 0 ip route 0 192.168.1.0/24 1 1

設定終了
# save
# commit
```

## 2.13.29 RSA デジタル署名認証を使用した固定IPアドレスでのVPN (自動鍵交換 IKE Version2)

[\[2.13.18 RSA デジタル署名認証を使用した固定IPアドレスでのVPN \(自動鍵交換\)\] \(P.249\)](#) を IKE Version2 を使ってVPNを構築する場合の設定方法を説明します。

支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [\[2.13.18 RSA デジタル署名認証を使用した固定IPアドレスでのVPN \(自動鍵交換\)\] \(P.249\)](#) と同じです。そちらを参照してください。

また、事前に [\[2.39 PKI機能を使う\] \(P.413\)](#) で証明書関連情報の設定が行われている必要があります。

### ● 設定条件

#### 【支社 (Initiator)】

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 202.168.1.66 - 202.168.2.66
- ・ IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット
- ・ 相手装置証明書識別番号 : なし
- ・ 自装置証明書識別番号 : 0
- ・ 秘密識別番号 : 0

#### 【本社 (Responder)】

- ・ ネットワーク名 : vpn-shi
- ・ 接続先名 : shisya
- ・ IPsec/IKE 区間 : 202.168.2.66 - 202.168.1.66
- ・ IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット
- ・ 相手装置証明書識別番号 : なし
- ・ 自装置証明書識別番号 : 0
- ・ 秘密識別番号 : 0

#### 【共通】

- ・ IKE Version : ikev2
- ・ 自装置証明書情報の送信 : 証明書要求ペイロード受信時
- ・ 証明書要求 : 送信する
- ・ 認証局識別番号 : なし
- ・ 有効期限切れ証明書 : 使用する
- ・ IPsec プロトコル : esp
- ・ IPsec 暗号アルゴリズム : des-cbc
- ・ IPsec 認証アルゴリズム : hmac-md5
- ・ IPsec DH グループ : なし
- ・ IKE 認証方法 : rsa-signature (RSA デジタル署名)
- ・ IKE 暗号アルゴリズム : des-cbc
- ・ IKE 認証アルゴリズム : hmac-md5
- ・ IKE DH グループ : modp768
- ・ IKE PRF アルゴリズム : hmac-md5

- IKE 支社 ID タイプ : address
- IKE 本社 ID タイプ : address

### 💡 ヒント

#### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

#### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

```
VPN を設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

設定終了
# save

再起動
# reset
```

## 本社 (Responder) を設定する

### ● コマンド

VPN を設定する

```
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.1.66
# remote 1 ip route 0 192.168.1.0/24 1 1
```

設定終了

```
# save
```

再起動

```
# reset
```

## 2.13.30 RSA デジタル署名認証を使用した可変IPアドレスでのVPN (自動鍵交換 IKE Version2)

[2.13.19 RSA デジタル署名認証を使用した可変IPアドレスでのVPN (自動鍵交換)] (P.253) を IKE Version2 を使ってVPNを構築する場合の設定方法を説明します。

支社はPPPoEでインターネットに接続され、本社はグローバルアドレス空間のVPN終端装置として本装置が接続されていることを前提とします。

前提条件の設定および構成例は [2.13.19 RSA デジタル署名認証を使用した可変IPアドレスでのVPN (自動鍵交換)] (P.253) と同じです。そちらを参照してください。

また、事前に [2.39 PKI機能を使う] (P.413) で証明書関連情報の設定が行われている必要があります。

### ● 設定条件

#### [支社 (Initiator)]

- ネットワーク名 : vpn-hon
- 接続先名 : honsya
- IPsec/IKE 区間 : 支社 - 202.168.2.66
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット
- 相手装置証明書識別番号 : なし
- 自装置証明書識別番号 : 0
- 秘密識別番号 : 0

#### [本社 (Responder)]

- テンプレート名 : vpn-shi
- IPsec/IKE 区間 : 202.168.2.66 - 支社
- IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット
- 相手装置証明書識別番号 : なし
- 自装置証明書識別番号 : 0
- 秘密識別番号 : 0

#### [共通]

- IKE Version : ikev2
- 自装置証明書情報の送信 : 証明書要求ペイロード受信時
- 証明書要求 : 送信する
- 認証局識別番号 : なし
- 有効期限切れ証明書 : 使用する
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : des-cbc
- IPsec 認証アルゴリズム : hmac-md5
- IPsec DH グループ : なし
- IPsecV3 ESN : あり
- IKE 支社 ID/ID タイプ : shisya (自装置名) /FQDN
- IKE 本社 ID タイプ : address
- IKE 認証方法 : rsa-signature (RSA デジタル署名)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5

- IKE DHグループ : modp768
- IKE PRF アルゴリズム : hmac-md5

### 💡 ヒント

#### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

#### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

#### ◆ IDタイプとは？

ネゴシエーションで使用する自装置を識別するIDの種別です。相手VPN装置の設定に合わせます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

インターネットからIPsec/IKEパケットを受信する設定をする

```
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50
# remote 0 ip nat static default reject
```

VPNを設定する

```
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype address
# remote 1 ap 0 ike name local shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1
```

設定終了

```
# save
```

再起動

```
# reset
```



## 本社 (Responder) を設定する

### ● コマンド

VPN を設定する

```
# remote 1 name vpn-shi
# remote 1 ap 0 name shisya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype address
# remote 1 ap 0 ike remote-idtype fqdn
# remote 1 ap 0 ike name remote shisya
# remote 1 ap 0 ike proposal 0 auth-method rsa-signature
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate local 0
# remote 1 ap 0 ike certificate key 0
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ip route 0 192.168.1.0/24 1 1
```

設定終了

```
# save
```

再起動

```
# reset
```

## 2.13.31 EAP 認証を使用した固定 IP アドレスでの VPN (自動鍵交換 IKE Version2)

EAP 認証機能を使用した、自動鍵交換で VPN を構築する場合の設定方法を説明します。

ここでは以下のコマンドによって、支社は PPPoE でインターネットに接続され、本社はグローバルアドレス空間の VPN 終端装置が接続されていることを前提とします。

また、事前に [\[2.39.3 認証局証明書を設定する\] \(P.421\)](#) で相手装置から発行された証明書関連情報の設定が行われている必要があります。

### ● 前提条件

#### [支社 (PPPoE 常時接続)]

- ローカルネットワーク IPv4 アドレス : 192.168.1.1/24
- ローカルネットワークポート : ETHER グループ 2 ポート 1~4
- ローカルネットワークポート VLAN : 2
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.1.66/24
- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザパスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHER グループ 1 ポート 1
- PPPoE ポート VLAN : 1

#### [本社]

- ローカルネットワーク IPv4 アドレス : 192.168.2.1/24
- インターネットプロバイダから割り当てられた固定 IPv4 アドレス : 202.168.2.66/24
- インターネットプロバイダから指定されたデフォルトルートの IPv4 アドレス : 202.168.2.65

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● 設定コマンド

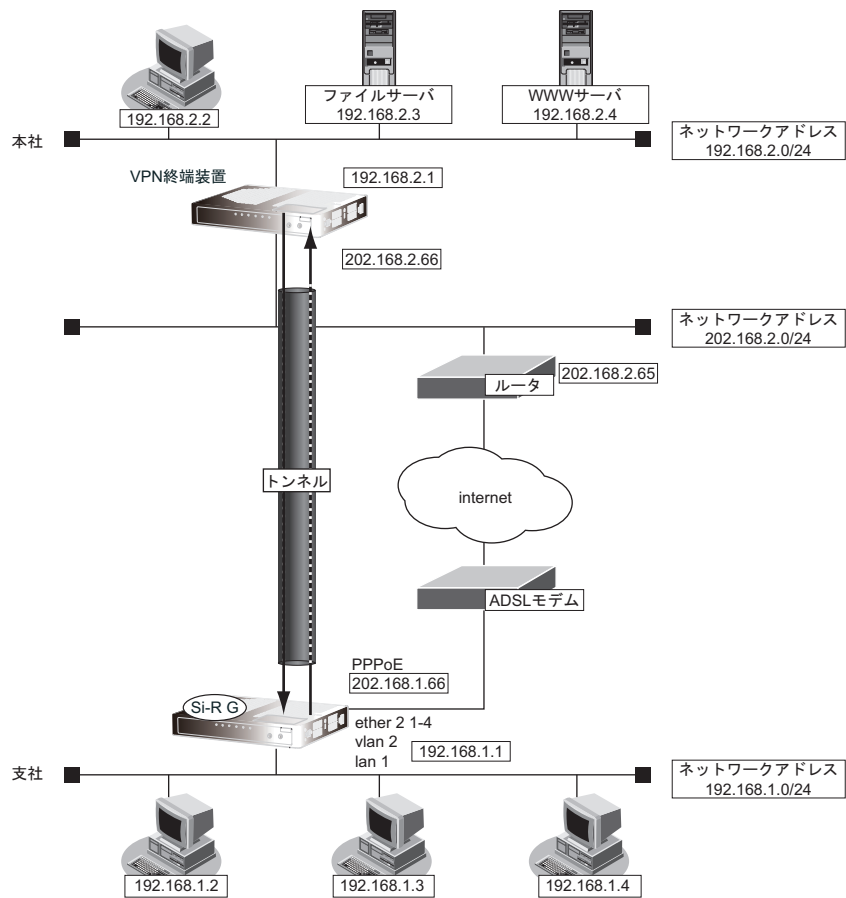
```
支社 (PPPoE 常時接続) を設定する
# delete ether 1
# delete ether 2
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip address local 202.168.1.66
```

```
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```



● 設定条件

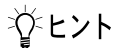
[支社]

- ・ ネットワーク名 : vpn-hon
- ・ 接続先名 : honsya
- ・ IPsec/IKE 区間 : 202.168.1.66-202.168.2.66
- ・ IPsec 対象範囲 : IPsec相手情報を使用するすべてのパケット
- ・ 相手装置証明書識別番号 : なし
- ・ 自装置証明書識別番号 : 0
- ・ 秘密識別番号 : 0
- ・ IKE Version : ikev2
- ・ 証明書要求 : 送信する
- ・ 認証局識別番号 : 0
- ・ 有効期限切れ証明書 : 使用する
- ・ IPsec プロトコル : esp
- ・ IPsec 暗号アルゴリズム : des-cbc
- ・ IPsec 認証アルゴリズム : hmac-md5
- ・ IPsec DHグループ : なし
- ・ IKE 支社 IDタイプ : FQDN
- ・ IKE 本社 ID/IDタイプ : honsya (自装置識別情報) /FQDN

- IKE 認証方法 : shared-key (事前共有鍵方式)
- IKE 暗号アルゴリズム : des-cbc
- IKE 認証アルゴリズム : hmac-md5
- IKE DHグループ : modp768
- IKE PRFアルゴリズム : hmac-md5
- IKE EAP 認証ID/PASSWORD : shisya/shisyapass

### こんな事に気をつけて

- EAP 認証機能を利用するときは、以下の点に注意してください。
  - IKE Version2 でのみ動作します。
  - 初回 IKE ネゴシエーションは Initiator でのみ動作します。
  - EAP 認証機能のユーザIDとパスワードは対向装置と同一の設定となるよう設定してください。  
互いの装置で一致しないユーザIDとパスワードが設定されていた場合、IKE ネゴシエーションで接続に失敗します。
  - EAP 認証機能を使用する場合、IDtype の設定は FQDN および USER\_FQDN のみ有効となります。  
それ以外の設定の場合は、IKE ネゴシエーションで接続に失敗します。



ヒント

#### ◆ DHグループとは？

鍵を作るための素数です。大きな数を指定することにより、処理に時間がかかりますが、セキュリティを強固にすることができます。

#### ◆ IKEとは？

自動鍵交換を行うためのプロトコルです。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 支社 (Initiator) を設定する

### ● コマンド

```
VPNを設定する
# remote 1 name vpn-hon
# remote 1 ap 0 name honsya
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ikev2
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike local-idtype fqdn
# remote 1 ap 0 ike remote-idtype fqdn
# remote 1 ap 0 ike name remote honsya
# remote 1 ap 0 ike proposal 0 auth-method shared-key
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike proposal 0 prf hmac-md5
# remote 1 ap 0 ike certificate request enable 0
# remote 1 ap 0 ike eap auth send shisya shisyapass
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ip route 0 192.168.2.0/24 1 1

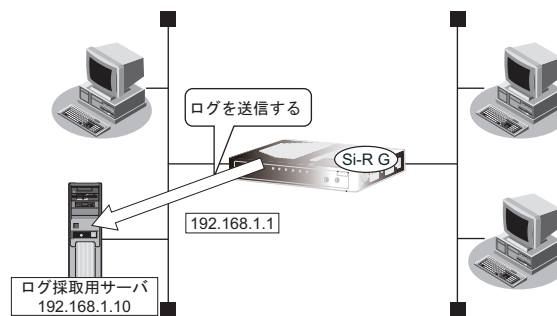
設定終了
# save
# reset
```

## 2.14 システムログを採取する

本装置では、各種システムログ（回線の接続／切断など）をネットワーク上の syslog サーバに送信することができます。また、セキュリティログとして以下のログを採取することができます。

- PPP（着信拒否）
- IPフィルタ（遮断したパケット）
- URLフィルタ（遮断したパケット）
- NAT（遮断したパケット、変換テーブル作成）
- DHCP（配布したIPv4アドレス、IPv6プレフィックス）
- IDS（検出されたパケット）

ここでは、システムログを採取する場合の設定方法を説明します。



### ● 設定条件

- 以下のプライオリティを設定する
  - プライオリティ LOG\_ERROR
  - プライオリティ LOG\_WARNING
  - プライオリティ LOG\_NOTICE
  - プライオリティ LOG\_INFO
- 以下のセキュリティログを採取する
  - IPフィルタ
  - NAT
  - PPP
  - DHCP
  - Proxy DNS
  - IDS
- ログ受信用サーバのIPアドレス : 192.168.1.10

上記の設定条件に従ってシステムログを採取する場合のコマンド例を示します。

### ● コマンド

```
# syslog server 0 address 192.168.1.10
```

システムログを設定する

```
# syslog pri error,warn,notice,info
```

```
# syslog security ipfilter,nat,ppp,dhcp,proxydns,ids
```

設定終了

```
# save
```

```
# commit
```

## 採取したシステムログを確認する

---

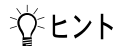
採取したシステムログの確認方法は、お使いのサーバによって異なります。

## 2.15 マルチ NAT 機能（アドレス変換機能）を使う

本装置のマルチ NAT 機能を使用すると、通信発生のたびにあってはいるグローバルアドレスを割り当てるので、限られた数のグローバルアドレスでそれ以上のパソコンを接続できます。

ここでは、静的 NAT を使って、サーバを公開する場合を例に説明します。静的 NAT は、特定のパソコンやアプリケーションに同じ IP アドレス、ポート番号を割り当てます。そのために Web を公開するような場合に適しています。

☛ 参照 マニュアル「機能説明書」



### ◆ 同時に接続できる台数

機能	セッション数	備考
基本 NAT	グローバルアドレス数 セッション数制限なし	割り当て時間内は外部からの通信もできる 基本 NAT と静的 NAT で同一グローバルアドレスを使用しないでください
動的 NAT	最大 20000 セッション	外部からの通信はできない
静的 NAT	最大 200 個	プライベートアドレスとポートをグローバルアドレスとポートに割り当てできる 割り当てたアドレスとポートに関しては外部からの通信もできる
あて先変換	最大 200 個	グローバルアドレスをプライベートアドレスに割り当てできる

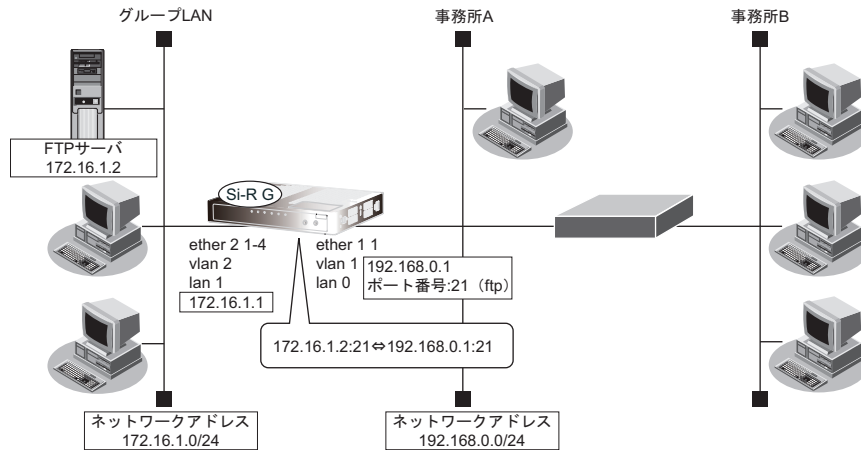
### こんな事に気をつけて

コマンド入力時は、半角文字（0～9、A～Z、a～z、および記号）だけを使用してください。ただし、空白文字、「|」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザーズガイド」

## 2.15.1 プライベートLAN接続でサーバを公開する

ここでは、静的NATを使って、FTPサーバを公開する場合の設定方法を説明します。



### ● 設定条件

#### 【事務所A側】

- ETHERグループ1ポート1を使用する
- 静的NATを使用する

#### 【グループLAN側】

- IPアドレス : 172.16.1.1
- ネットワークアドレス/ネットマスク : 172.16.1.0/24
- FTPサーバのIPアドレス : 172.16.1.2

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```

本装置のIPアドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
    
```

### こんな事に気をつけて

NATでは、FTPやDNSが要求した相手からの応答かどうかをチェックします。相手サーバがNAT機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```

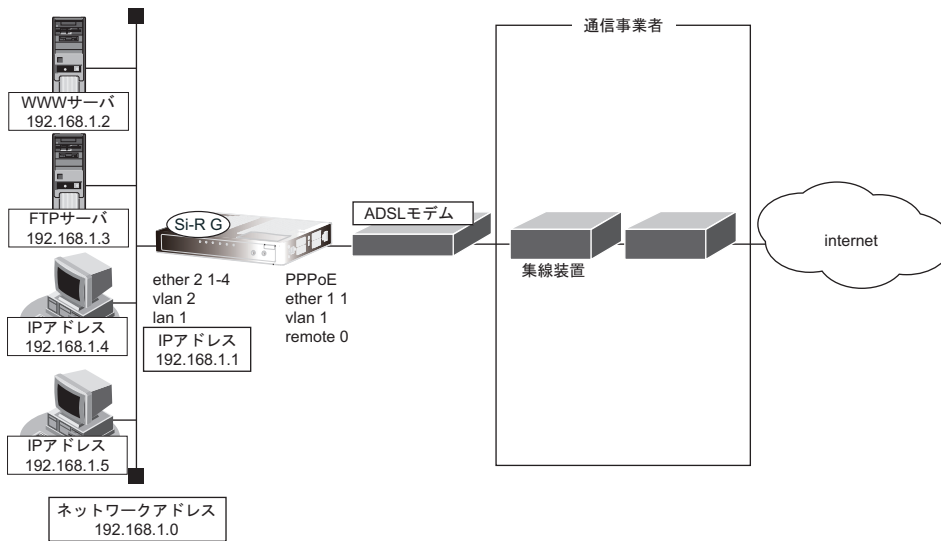
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
    
```



## 2.15.2 PPPoE 接続でサーバを公開する

PPPoE を使ってインターネットへ接続している場合の例です。

ここでは、PPPoE 接続時に静的 NAT を使ってサーバを公開する場合の設定方法を説明します。



### ● 設定条件

- 既存の LAN を使用する
- ユーザ認証 ID : userid
- ユーザ認証パスワード : userpass
- ネットワークアドレス/ネットマスク : 192.168.1.0/24
- ブロードキャストアドレス : 192.168.1.255

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

PPPoE でインターネットへ接続する環境を設定する

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# delete lan

# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info dns 192.168.1.1
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 vlan 2

# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414

# proxydns domain 0 any * any to 0
# proxydns address 0 any to 0
```

NAT 情報を設定する

```
# remote 0 ip nat static 0 192.168.1.2 80 any 80 any
# remote 0 ip nat static 1 192.168.1.3 21 any 21 any
```

設定終了

```
# save
```

再起動

```
# reset
```

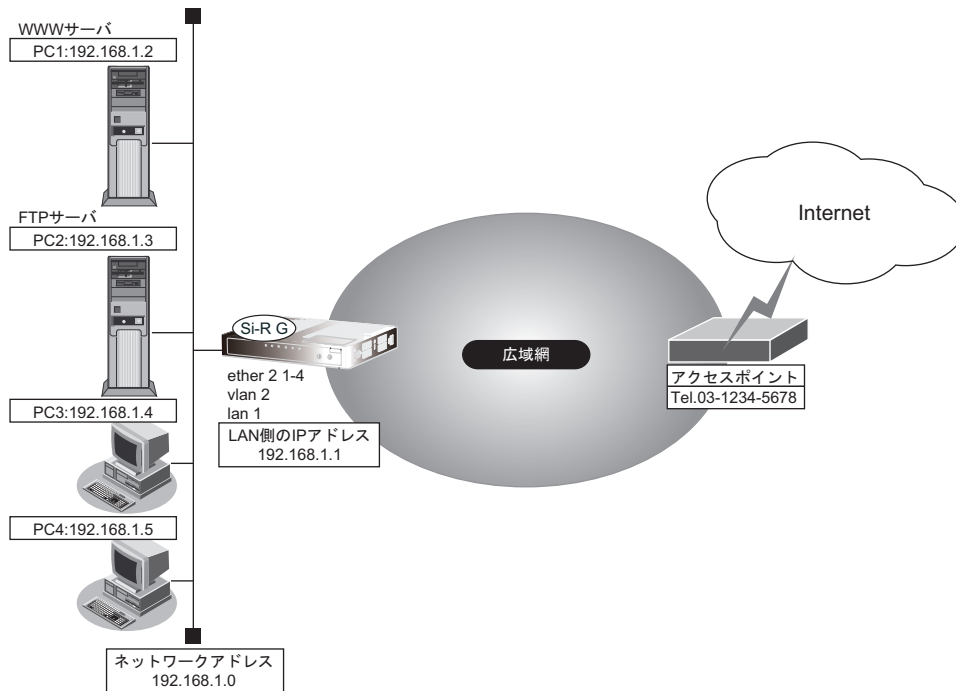
### こんな事に気をつけて

- ネットワーク型接続でマルチ NAT を使用する際、グローバルアドレスの設定が必須となります。なお、端末型接続では、接続時にグローバルアドレスが割り当てられるため、設定は不要です。
- 動的 NAT と静的 NAT が混在する場合、動的 NAT で使用する IP アドレスと静的 NAT で使用する IP アドレスは重複しないようにしてください。
- NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# remote 0 ip nat rule 0 ftp any 21 off
# remote 0 ip nat rule 1 dns global 53 off
```

## 2.15.3 ネットワーク型接続でサーバを公開する

ここでは、静的NATを使ってサーバを公開する場合の設定方法を説明します。



### ● 設定条件

- ネットワーク型接続を行う
- 広域網接続ETHERポート : ETHERグループ1ポート1
- 広域網接続ETHERポートVLAN : 1
- 広域網接続lanインタフェース : lan 0
- 割り当てネットワークアドレス : 10.10.10.96/29
- wwwに割り当てるIPアドレス : 10.10.10.98
- ftpに割り当てるIPアドレス : 10.10.10.99
- 動的NATで使用するIPアドレス : 10.10.10.100 ~ 102
- 既存のLANを接続するETHERポート : ETHERグループ2ポート1~4
- 既存のLANを接続するETHERポートVLAN : 2
- ネットワークアドレス/ネットマスク : 192.168.1.0/24
- ブロードキャストアドレス : 192.168.1.255

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

広域網接続を設定する

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# lan 0 ip address 10.10.10.96/29 3
```

本装置の IP アドレスを設定する

```
# ether 2 1-4 use on
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2
```

NAT 情報を設定する

```
# lan 0 ip nat mode multi 10.10.10.100 3 5m
# lan 0 ip nat static 0 192.168.1.2 80 10.10.10.98 80 any
# lan 0 ip nat static 1 192.168.1.3 21 10.10.10.99 21 any
```

設定終了

```
# save
```

再起動

```
# reset
```

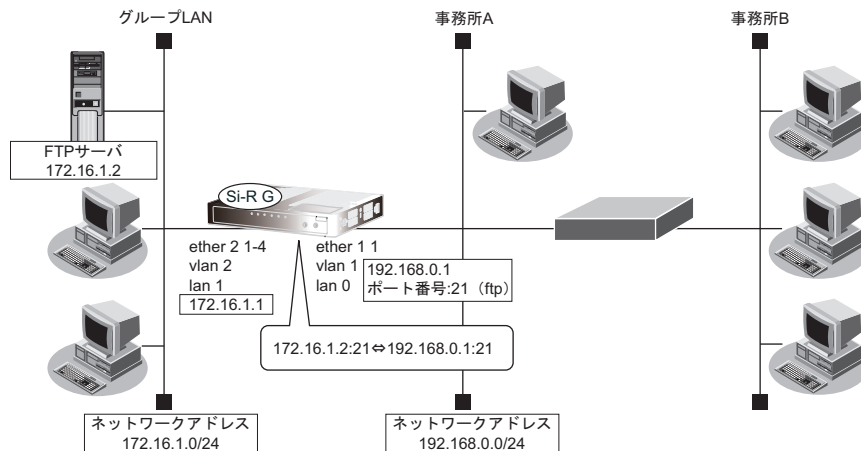
### こんな事に気をつけて

NAT では、FTP や DNS が要求した相手からの応答かどうかをチェックします。相手サーバが NAT 機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# remote 0 ip nat rule 0 ftp any 21 off
# remote 0 ip nat rule 1 dns global 53 off
```

## 2.15.4 サーバ以外のアドレス変換をしないで、プライベートLAN接続でサーバを公開する

ここでは、静的NATだけを使って、サーバ以外のアドレス変換をしないで、FTPサーバを公開する場合の設定方法を説明します。



### ● 設定条件

#### [事務所A側]

- ETHERグループ1ポート1を使用する
- 静的NATだけを使用する

#### [グループLAN側]

- IPアドレス : 172.16.1.1
- ネットワークアドレス/ネットマスク : 172.16.1.0/24
- FTPサーバのIPアドレス : 172.16.1.2

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```

本装置のIPアドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3

NAT情報を設定する
# lan 0 ip nat mode static any 1 5m
# lan 0 ip nat static 0 172.16.1.2 21 192.168.0.1 21 6

設定終了
# save
# commit
    
```

### こんな事に気をつけて

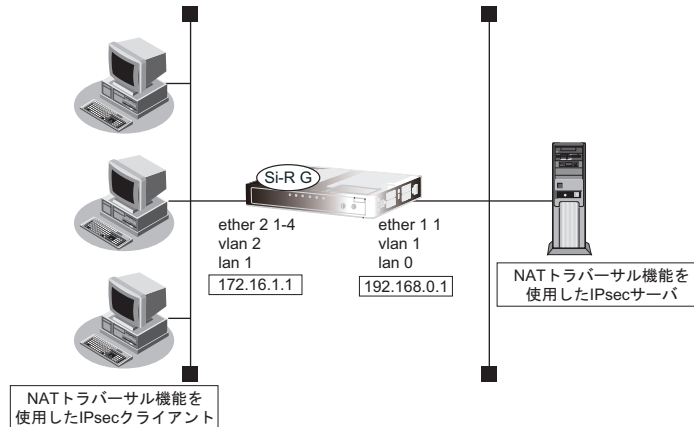
NATでは、FTPやDNSが要求した相手からの応答かどうかをチェックします。相手サーバがNAT機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```

# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
    
```

## 2.15.5 複数のNATトラバーサル機能を使用したIPsecクライアントを同じIPsecサーバに接続する

ここでは、静的NATを使って、複数のNATトラバーサル機能を使用したIPsecクライアントを同じIPsecサーバに接続する場合の設定方法を説明します。



### ● 設定条件

#### [IPsecサーバ側]

- ETHERグループ1ポート1を使用する
- マルチNATを使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
本装置のIPアドレスを設定する
# lan 0 ip address 192.168.0.1/24 3
# lan 1 ip address 172.16.1.1/24 3
```

```
NAT情報を設定する
# lan 0 ip nat mode multi any 1 5m
# lan 0 ip nat wellknown 0 500 off
```

```
設定終了
# save
# commit
```

#### こんな事に気をつけて

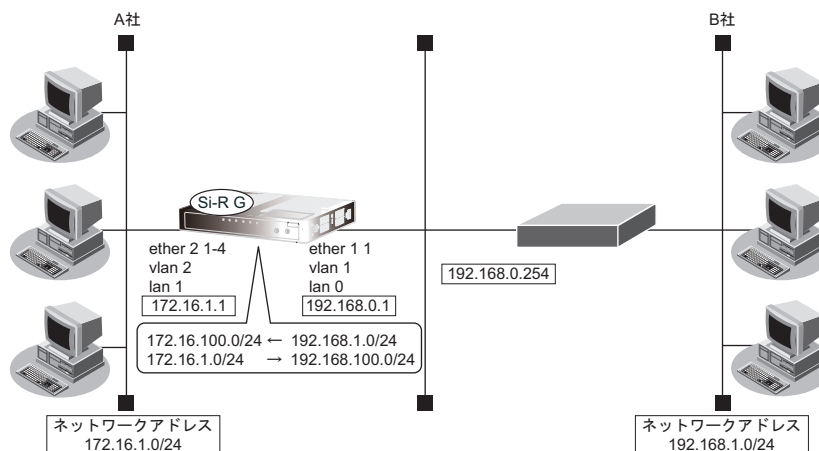
NATでは、FTPやDNSが要求した相手からの応答かどうかをチェックします。相手サーバがNAT機能を使用している場合など、要求先とは別のアドレスから応答する場合は、以下の設定を追加してください。

```
# lan 0 ip nat rule 0 ftp any 21 off
# lan 0 ip nat rule 1 dns global 53 off
```

## 2.15.6 NAT あて先変換で双方向のアドレスを変換する

ここでは、NAT あて先変換を使って、双方向のIPアドレスを変換する場合の設定方法を説明します。

この機能を使用して異なるアドレス体系を持つA社とB社を接続した場合、同じアドレス体系であるかのように見せることができます。



### ● 設定条件

#### [A社]

- IPアドレス : 172.16.1.1
- ネットワークアドレス/ネットマスク : 172.16.1.0/24

#### [B社]

- ETHERグループ1ポート1を使用する
- マルチNATを使用する
- NAT あて先変換を使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

本装置のIPアドレスを設定する

```
# lan 0 ip address 192.168.0.1/24 3
```

```
# lan 1 ip address 172.16.1.1/24 3
```

B社 への経路を設定する

```
# lan 0 ip route 0 172.16.100.0/24 192.168.0.254
```

NAT 情報を設定する

```
# lan 0 ip nat mode multi any 1 5m
```

```
# lan 0 ip nat static 0 172.16.1.2 any 192.168.100.2-192.168.100.254 any any
```

```
# lan 0 ip nat destination 0 172.16.100.2 192.168.1.2-192.168.1.254
```

設定終了

```
# save
```

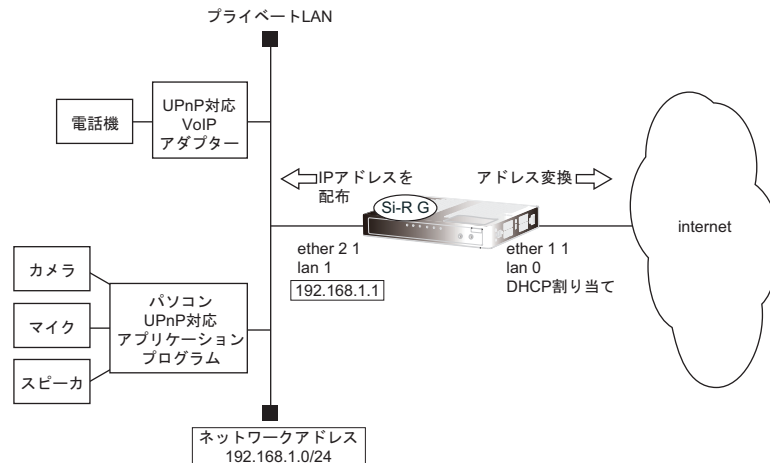
```
# commit
```

## 2.16 VoIP NAT トラバーサル機能を使う

マルチ NAT 機能を使用すると動作しない VoIP アダプターが UPnP に対応している場合、本装置の VoIP NAT トラバーサル機能を使用することによって動作できるようになることがあります。同様に、UPnP に対応した装置やアプリケーションプログラムもマルチ NAT 機能を使用しても動作できるようになることがあります。

☛ 参照 マニュアル「機能説明書」

ここでは、UPnP 対応 VoIP アダプターや UPnP 対応アプリケーションプログラムを使用する設定方法を説明します。



### ● 設定条件

#### [インターネット側 LAN]

- ETHERグループ 1 ポート 1 を使用する
- 使用する VLAN ID : 1
- LAN0 ポートを使用する
- 転送レート : 自動認識
- IP アドレス : DHCP サーバから自動的に取得
- マルチ NAT を使用する
  - グローバルアドレス : インターネットプロバイダから割り当てられた IP アドレスを使用する
  - アドレス個数 : 1
  - アドレス割り当てタイマ : 5分
- NAT での SIP アプリ対応を無効にする

#### [UPnP 対応装置 (プライベート LAN) 側]

- ETHERグループ 2 ポート 1 を使用する
- 使用する VLAN ID : 2
- LAN1 ポートを使用する
- 転送レート : 自動認識
- IP アドレス : 192.168.1.1/24
- DHCP サーバ機能を使用する
  - 割り当て先頭アドレス : 192.168.1.2
  - 割り当てアドレス数 : 253



リース期間 : 1日  
デフォルトルータ広報 : 192.168.1.1

### こんな事に気をつけて

コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「'」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

インターネット側のLAN情報を設定する
# lan 0 vlan 1
# lan 0 ip dhcp service client
# lan 0 ip rip use off v1 0 off
# lan 0 ip nat mode multi any 1
# lan 0 ip nat appli sip off

UPnP 対応装置側のLAN情報を設定する
# lan 1 vlan 2
# lan 1 ip address 192.168.1.1/24 3
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.1.2/24 253
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.1.1
# lan 1 ip rip use v1 v1 0 off

UPnP 機能を設定する
# upnp use on

設定終了
# save

再起動
# reset
```

本装置の設定が終了したら、設定を有効にするためにパソコンのシステムを終了し、パソコンおよび本装置の電源を切断します。各装置をLANケーブルで正しく接続したあと、本装置、UPnP対応装置やパソコンの順に電源を投入します。

## 2.17 TOS/Traffic Class 値書き換え機能を使う

本装置を経由してネットワークに送信される、またはネットワークから受信したパケットをIPアドレスとポート番号の組み合わせでTOS/Traffic Class 値を変更することにより、ポリシーベースネットワークのポリシーに合わせるすることができます。

☛ 参照 マニュアル「機能説明書」

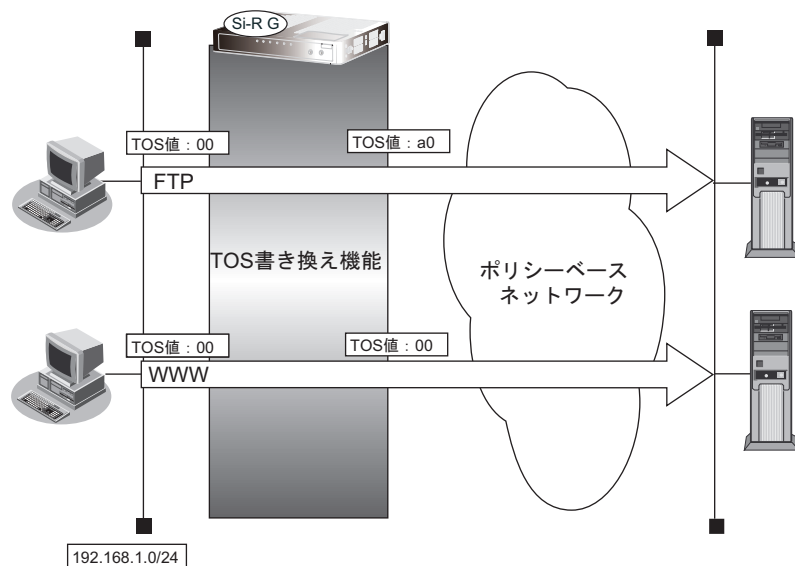
### TOS/Traffic Class 値書き換え機能の条件

本装置では、コマンドで以下の条件を指定することによって、ポリシーベースネットワークのポリシーに合ったTOS/Traffic Class 値に書き換えることができます。

- プロトコル
- 送信元情報 (IPアドレス/アドレスマスク/ポート番号)
- あて先情報 (IPアドレス/アドレスマスク/ポート番号)
- IPパケットのTOS値またはIPv6パケットのTraffic Class 値
- 新TOSまたはTraffic Class

ここではネットワークが以下のポリシーを持つ場合の設定方法を説明します。

- FTP (TOS 値 a0) を最優先とする
- その他はなし



**● 設定条件**

- 送信元IPアドレス/アドレスマスク : 192.168.1.0/24
- 送信元ポート番号 : 指定しない
- あて先IPアドレス/アドレスマスク : 指定しない
- あて先ポート番号 : 20 (ftp-dataのポート番号)、21 (ftpのポート番号)
- プロトコル : TCP
- TOS値 : 00
- 新TOS値 : a0

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド**

```
FTPサーバのアクセスでTOS値を00からa0に書き換える
# acl 0 ip 192.168.1.0/24 any 6 tos 0
# acl 0 tcp any 20,21 yes
# remote 0 ip tos 0 acl 0 a0
```

```
設定終了
# save
# commit
```

## 2.18 VLANプライオリティマッピング機能を使う

VLANプライオリティマッピング機能を使用して、レイヤ2スイッチなどでQoS制御を行うことができます。本装置から送信されるVLANパケットのVLANのプライオリティ値を、VLAN ID、IPパケットのTOSフィールドおよびIPv6パケットのトラフィッククラスフィールドの値から設定します。

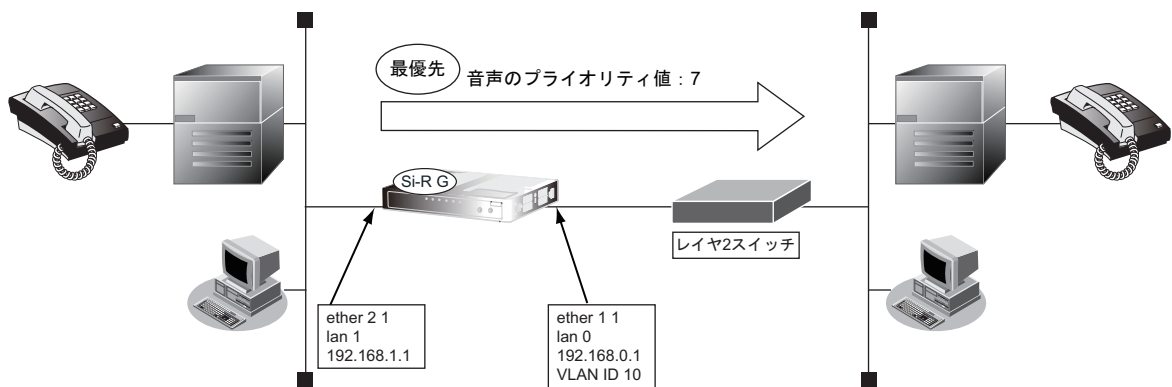
☞ 参照 マニュアル「機能説明書」

本装置では、コマンドで以下の条件を指定することによって、VLANのプライオリティフィールドを設定することができます。

- VLAN ID
- プロトコル
- TOS/Traffic Class
- プライオリティ

ここでは、本装置が以下の音声データを転送する場合の設定方法を説明します。

- 音声 (IPでTOS値がa0) を最優先とする (プライオリティ値が7)



### ● 設定条件

- VLAN ID : 10
- プロトコル : IPv4
- TOS値 : a0
- プライオリティ値 : 7

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド**

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan tag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

VLAN ID 10、TOS 値 a0 のパケットのプライオリティ値を 7 に設定する
# ether 1 1 vlan primap mode enable
# ether 1 1 vlan primap rule 0 10 ip a0 7

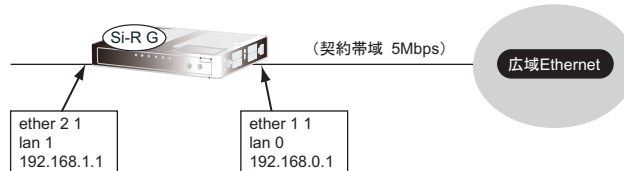
設定終了
# save
# commit
```

## 2.19 シェーピング機能を使う

シェーピング機能を使用すると、インタフェースから送出するデータ量を制限することができます。

### 2.19.1 特定のインタフェースでシェーピング機能を使う

ここでは、lan インタフェースに送出するデータ量を制限する場合の設定方法を説明します。



#### ● 設定条件

- 広域 Ethernet 側への送信データを、最大 5Mbps に制限する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

#### ● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

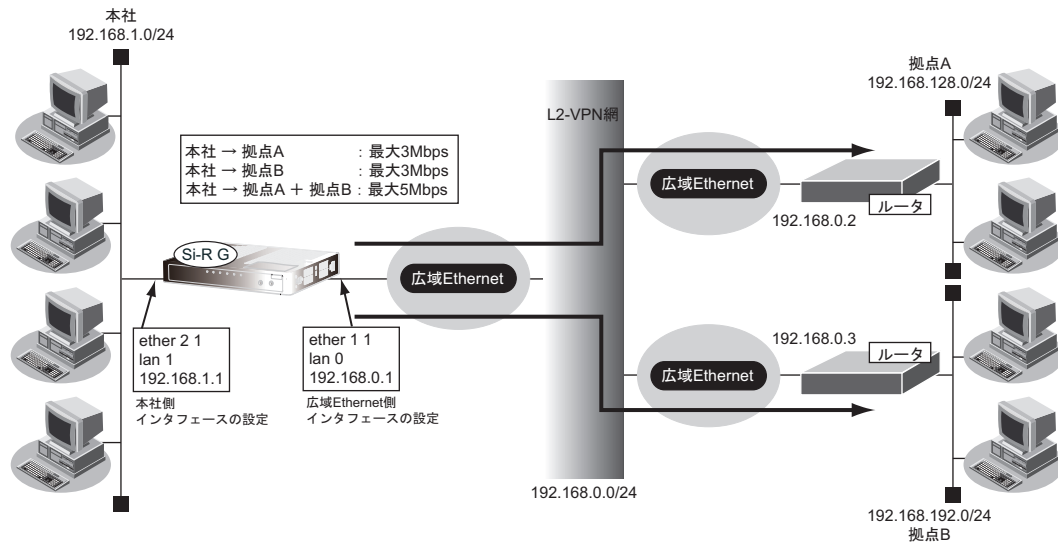
lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

lan 0 から送出するデータ量を 5Mbps に制限する
# lan 0 shaping on 5m

設定終了
# save
# commit
```

## 2.19.2 送信先ごとにシェーピング機能を使う

ここでは、各拠点に送出するデータ量を制限する場合の設定方法を説明します。



### ● 設定条件

- 広域 Ethernet をアクセスラインとする。L2-VPN 網を利用して本社と各拠点を接続する
- 本社から拠点 A への送信データは、最大 3Mbps に制限する
- 本社から拠点 B への送信データは、最大 3Mbps に制限する
- 本社から拠点 A と拠点 B への送信データの合計は、最大 5Mbps に制限する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

lan 0 から送出するデータ量を 5Mbps に制限する
# lan 0 shaping on 5m

拠点 A の情報を設定する
# remote 0 name kyotenA
# remote 0 ip route 0 192.168.128.0/24 1 1
# remote 0 ap 0 name OV-A
# remote 0 ap 0 datalink type overlap
# remote 0 ap 0 overlap to lan 0
# remote 0 ap 0 overlap nexthop 192.168.0.2

拠点 B の情報を設定する
# remote 1 name kyotenB
```

```
# remote 1 ip route 0 192.168.192.0/24 1 1
# remote 1 ap 0 name OV-B
# remote 1 ap 0 datalink type overlap
# remote 1 ap 0 overlap to lan 0
# remote 1 ap 0 overlap nexthop 192.168.0.3

remote 0 から送出するデータ量を 3Mbps に制限する
# remote 0 shaping on 3m

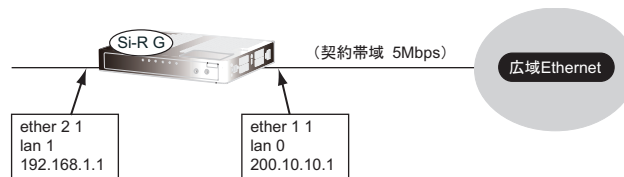
remote 1 から送出するデータ量を 3Mbps に制限する
# remote 1 shaping on 3m

設定終了
# save
# commit
```



## 2.19.3 特定のポートでシェーピング機能を使う

ここでは、Ethernetポートに送出するデータ量を制限する場合の設定方法を説明します。



### ● 設定条件

- 広域 Ethernet 側への送信データを、最大 5Mbps に制限する

#### [広域 Ethernet 側]

- ポート : ether 1 1 を使う
- VLAN : untag 10
- lan : lan 0
- IP アドレス : 200.10.10.1/29

#### [LAN 側]

- ポート : ether 2 1 を使う
- VLAN : untag 20
- lan : lan 1
- IP アドレス : 192.168.1.1/24

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 200.10.10.1/29 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

ether 1 1 から送出するデータ量を 5Mbps に制限する
# ether 1 1 shaping on 5m

設定終了
# save
# commit
```

## 2.20 ヘッダ圧縮機能を使う

PPPを使った相手装置との接続時に、ヘッダ圧縮機能によって回線の利用効率を高めることができます。

ヘッダ圧縮機能を利用する場合、接続する相手装置側でも同じ圧縮機能をサポートしている必要があります。以下に、サポートしている圧縮機能を示します。

- ヘッダ圧縮
  - VJ : VJヘッダ圧縮 (RFC1144 に準拠) の利用
  - IPHC : IPヘッダ圧縮 (圧縮方法: RFC2507/RFC2508、ネゴシエーション方法: RFC2509 に準拠) の利用

### ヘッダ圧縮の場合

ここでは、PPPoE 接続をネットワーク 0 (remote 0) で定義している環境に対して、ヘッダ圧縮を行う場合の設定方法を説明します。

#### ● 設定条件

- ネットワーク 0 (remote 0) で PPPoE による通信環境が設定済み
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってヘッダ圧縮を行う場合のコマンド例を示します。

#### ● コマンド

```
ヘッダ圧縮機能を設定する
# remote 0 ppp ipcp vjcomp enable
# remote 0 ppp ipcp iphc enable
```

```
設定終了
# save
# commit
```

#### こんな事に気をつけて

ヘッダ圧縮機能は、シェーピングによって通信速度が低速の場合に効果があります。高速回線で使用した場合は、処理のオーバーヘッドによって回線の利用効率が低くなる場合があります。

## 2.21 帯域制御 (WFQ) 機能を使う

本装置の帯域制御 (WFQ) 機能では、IPアドレスやポート番号の組み合わせで帯域を割り当てることによって、特定のデータを優先的に通すことができます。

☛ 参照 マニュアル「機能説明書」

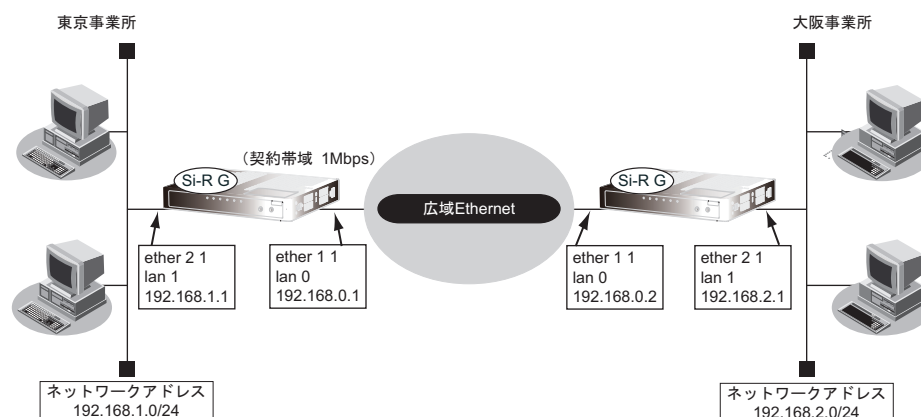
### 帯域制御 (WFQ) 機能の条件

本装置では、以下の条件を指定することによって、優先的にデータを通すように帯域を割り当てることができます。

- プロトコル
- IPアドレス
- ポート番号
- IPパケットのTOS値またはIPv6パケットのTraffic Class値

#### 2.21.1 特定のインタフェースで帯域制御 (WFQ) 機能を使う

ここでは、lanインタフェースから送出する音声データを最優先で透過させる場合の設定方法を説明します。



#### ● 設定条件

- 広域 Ethernet 側への送信データを、最大 1Mbps に制限する
- 音声データ (TOS 値 : a0) を最優先で透過させる

上記の設定条件に従って帯域制御する場合のコマンド例を示します。

## ● コマンド

### 東京事業所の設定

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 0 ip route 0 192.168.2.0/24 192.168.0.2 1
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

lan 0 から送出するデータ量を 1Mbps に制限する
# lan 0 shaping on 1m

音声データを最優先で透過させる
# acl 0 ip any any any tos a0
# lan 0 ip priority 0 acl 0 express

設定終了
# save
# commit
```

### 大阪事業所の設定

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.2/24 3
# lan 0 ip route 0 192.168.1.0/24 192.168.0.1 1
# lan 1 vlan 20
# lan 1 ip address 192.168.2.1/24 3

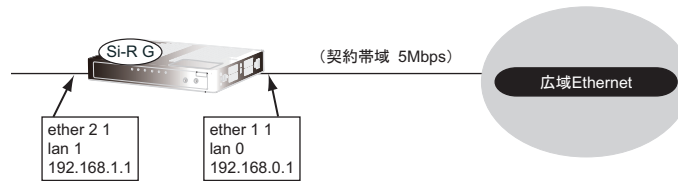
lan 0 から送出するデータ量を 1Mbps に制限する
# lan 0 shaping on 1m

音声データを最優先で透過させる
# acl 0 ip any any any tos a0
# lan 0 ip priority 0 acl 0 express

設定終了
# save
# commit
```

## 2.21.2 特定のポートで帯域制御 (WFQ) 機能を使う

ここでは、ether ポートから送出する音声データを最優先で透過させる場合の設定方法を説明します。



### ● 設定条件

- 広域 Ethernet 側への送信データを、最大 5Mbps に制限する
- 音声データ (TOS 値 : a0) を最優先で透過させる

上記の設定条件に従って帯域制御する場合のコマンド例を示します。

### ● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.0.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

ether 1 1 から送出するデータ量を 5Mbps に制限する
# ether 1 1 shaping on 5m

音声データを最優先で透過させる
# acl 0 ip any any tos a0
# ether 1 1 priority ip 0 acl 0 express

設定終了
# save
# commit
```

## 2.22 DHCP 機能を使う

本装置のIPv4 DHCPには、以下の機能があります。

- DHCP サーバ機能
- DHCP スタティック機能
- DHCP クライアント機能
- DHCP リレーエージェント機能

☞ 参照 マニュアル「機能説明書」

本装置では、それぞれのインタフェースでDHCP機能が使用できます。

こんな事に気をつけて

- 1つのインタフェースでは、1つの機能だけ動作します。同時に複数の機能を動作することはできません。
- 本装置のDHCPサーバは、リレーエージェントを経由して運用することはできません。

本装置のIPv6 DHCPには、以下の機能があります。

- IPv6 DHCP サーバ機能
- IPv6 DHCP クライアント機能
- IPv6 DHCP リレーエージェント機能

☞ 参照 マニュアル「機能説明書」

## 2.22.1 DHCP サーバ機能を使う

DHCPサーバ機能は、ネットワークに接続されているパソコンに対して、IPアドレスの自動割り当てを行う機能です。管理者はパソコンが増えるたびにIPアドレスが重複しないように設定する必要があります。

この機能を利用すると、DHCPクライアント機能を持つパソコンはIPアドレスの設定が不要になり、管理者の手間を大幅に省くことができます。

本装置のDHCPサーバ機能は、以下の情報を広報することができます。

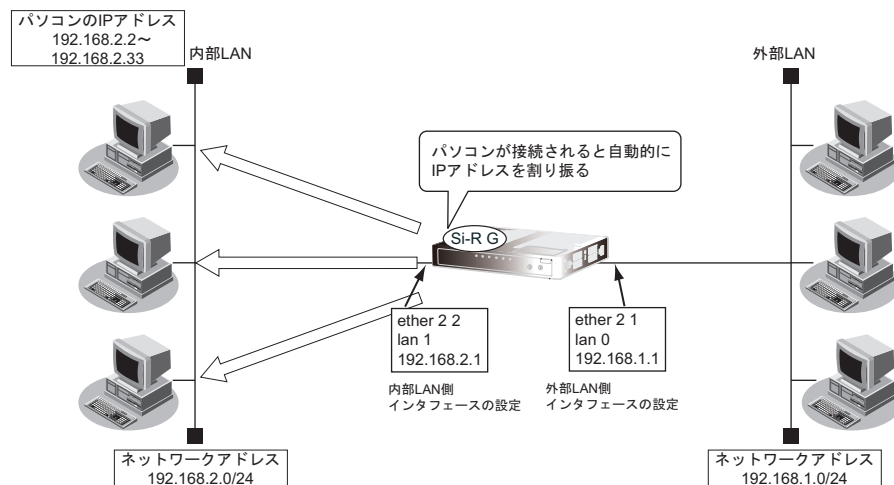
- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- ドメイン名
- NTPサーバのIPアドレス
- TIMEサーバのIPアドレス
- WINSサーバのIPアドレス
- SIPサーバのドメイン名またはIPアドレス

### こんな事に気をつけて

本装置のDHCPサーバ機能は、DHCPリレーエージェントのサーバにはなれません。

ここでは、DHCPサーバ機能を使用する場合の設定方法を説明します。

**補足** DHCPサーバ機能で割り当てることができるIPアドレスの最大数は253個です。



## ● 設定条件

### [外部LAN側]

- IPアドレス : 192.168.1.1
- ネットワークアドレス/ネットマスク : 192.168.1.0/24

### [内部LAN側]

- IPアドレス : 192.168.2.1
- ブロードキャストアドレス : 3 (ネットワークアドレス+オール1)
- パソコンに割り当てるIPアドレス : 192.168.2.2～192.168.2.33
- パソコンに割り当て可能IPアドレス数 : 32
- ネットワークアドレス/ネットマスク : 192.168.2.0/24
- デフォルトルータのIPアドレス : 192.168.2.1
- リース期間 : 1日
- NTPサーバのIPアドレス : 192.168.2.1
- DHCPサーバ機能を使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

### 外部LAN側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lan インタフェースを設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10

設定終了
# save
# commit
```

### 内部側LAN インタフェースの設定

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

DHCP サーバ機能を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp info ntpserver 192.168.2.1
# lan 1 ip dhcp info address 192.168.2.2/24 32
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.2.1
# lan 1 ip dhcp service server
# lan 1 vlan 20

設定終了
# save
# commit
```



## 2.22.2 DHCP スタティック機能を使う

DHCPサーバは、使用していないIPアドレスを一定期間（またはパソコンがIPアドレスを返却するまで）割り当てます。不要になったIPアドレスは自動的に再利用されるため、パソコンのIPアドレスが変わることがあります。本装置では、IPアドレスとMACアドレスを対応付けることによって、登録されたパソコンからDHCP要求が発行されると、常に同じIPアドレスを割り当てることができます。これをDHCPスタティック機能と言います。

DHCPスタティック機能を利用する場合は、ホストデータベース情報にIPアドレスとMACアドレスを設定してください。

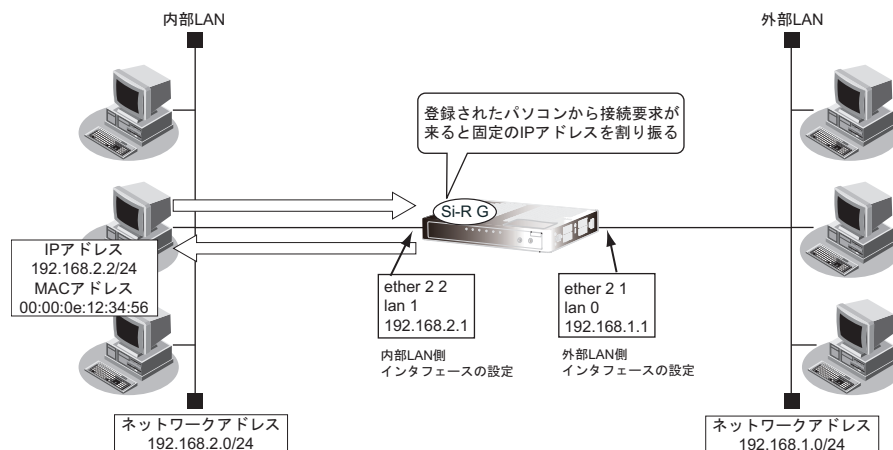


- MACアドレスとは、LAN機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
- 本装置がサポートしている「IPフィルタリング機能」、「マルチルーティング機能」などはパソコンのIPアドレスが固定されていないと使いにくい場合があります。これらの機能とDHCPサーバ機能の併用を実現するために、本装置では「DHCPスタティック機能」をサポートしています。

ここでは、DHCPスタティック機能を使用する場合の設定方法を説明します。



- ホストデータベース情報は「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だけを設定します。
- DHCPスタティック機能で設定できるホストの最大数は64個です。



### ● 設定条件

#### [外部LAN側]

- IPアドレス／ネットマスク : 192.168.1.1/24
- ネットワークアドレス／ネットマスク : 192.168.1.0/24

#### [内部LAN側]

- IPアドレス／ネットマスク : 192.168.2.1/24
- パソコンに割り当てるIPアドレス : 192.168.2.2～192.168.2.33
- パソコンに割り当て可能IPアドレス数 : 32
- ネットワークアドレス／ネットマスク : 192.168.2.0/24
- デフォルトルータのIPアドレス : 192.168.2.1
- リース期間 : 1日
- NTPサーバのIPアドレス : 192.168.2.1
- IPアドレスを固定するパソコンのMACアドレス : 00:00:0e:12:34:56
- 割り当てIPアドレス : 192.168.2.2

- DHCP サーバ機能を使用する

### こんな事に気をつけて

DHCP サーバ機能を使用するコマンドを実行していない場合、DHCP スタティック機能の設定は無効となります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

### 外部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lan インタフェースを設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10

設定終了
# save
# commit
```

### 内部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

DHCP サーバ機能を設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 ip dhcp info ntpserver 192.168.2.1
# lan 1 ip dhcp info address 192.168.2.2/24 32
# lan 1 ip dhcp info time 1d
# lan 1 ip dhcp info gateway 192.168.2.1
# lan 1 ip dhcp service server
# lan 1 vlan 20

DHCP スタティック機能を設定する
# host 0 ip address 192.168.2.2
# host 0 mac 00:00:0e:12:34:56

設定終了
# save
# commit
```

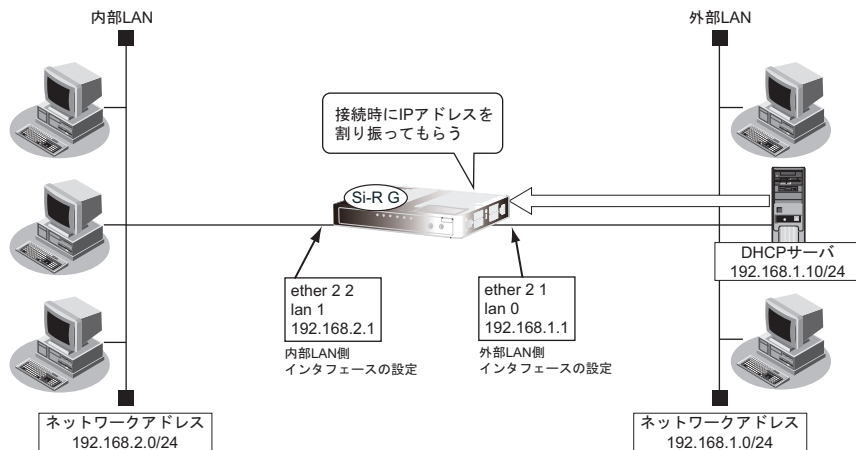
## 2.22.3 DHCPクライアント機能を使う

DHCPクライアント機能は、DHCPサーバからIPアドレスなどの情報を取得する機能です。使用する場合は、DHCPサーバが動作しているLANに接続する必要があります。利用者は、IPアドレスを意識することなくネットワークを利用できます。

本装置のDHCPクライアント機能は、以下の情報を受け取って動作します。

- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- TIMEサーバのIPアドレス
- NTPサーバのIPアドレス
- ドメイン名
- リース更新時間

ここでは、DHCPクライアント機能を使用する場合の設定方法を説明します。



### ● 設定条件

#### [外部LAN側]

- IPアドレス : DHCPサーバから取得する

#### [内部LAN側]

- IPアドレス : 192.168.2.1

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド****外部 LAN 側インタフェースの設定**

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

DHCP クライアント機能を設定する
# lan 0 ip dhcp service client
# lan 0 vlan 10

マルチ NAT 機能を設定する
# lan 0 ip nat mode multi any 1

設定終了
# save
# commit
```

**内部 LAN 側インタフェースの設定**

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

lan インタフェースを設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 20

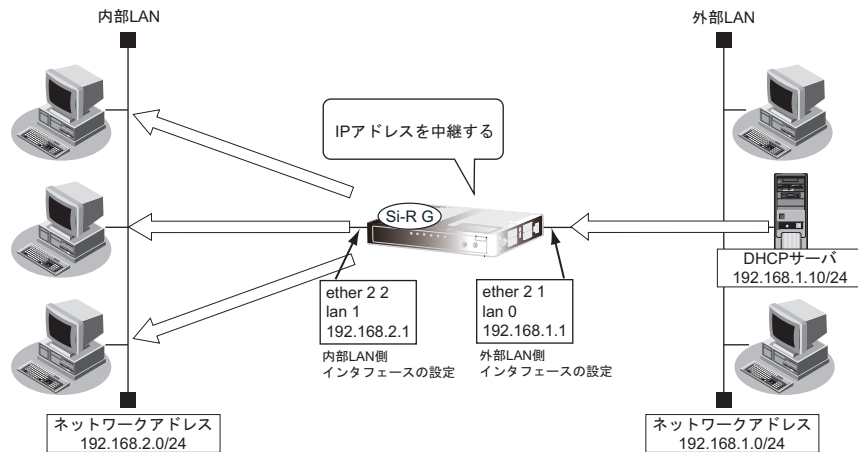
設定終了
# save
# commit
```

## 2.22.4 DHCP リレーエージェント機能を使う

DHCPクライアントは、同じネットワーク上にあるサーバから、IPアドレスなどの情報を獲得することができます。DHCPリレーエージェントは、遠隔地にあるDHCPクライアントの要求をDHCPサーバが配布する情報を中継する機能です。この機能を利用することで、遠隔地の別のネットワークにDHCPサーバが存在する場合も同様に情報を獲得することができます。

ここでは、DHCPリレーエージェント機能を使用する場合の設定方法を説明します。

### LAN 接続の場合



#### ● 設定条件

##### [外部LAN側]

- ・ IPアドレス : 192.168.1.1
- ・ DHCPサーバ : 192.168.1.10

##### [内部LAN側]

- ・ IPアドレス : 192.168.2.1
- ・ DHCPリレーエージェント機能を使用する



DHCPリレーエージェント機能を使用するときは、NAT機能を使用できません。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド****外部LAN側インタフェースの設定**

```
etherポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lanインタフェースを設定する
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 10

設定終了
# save
# commit
```

**内部LAN側インタフェースの設定**

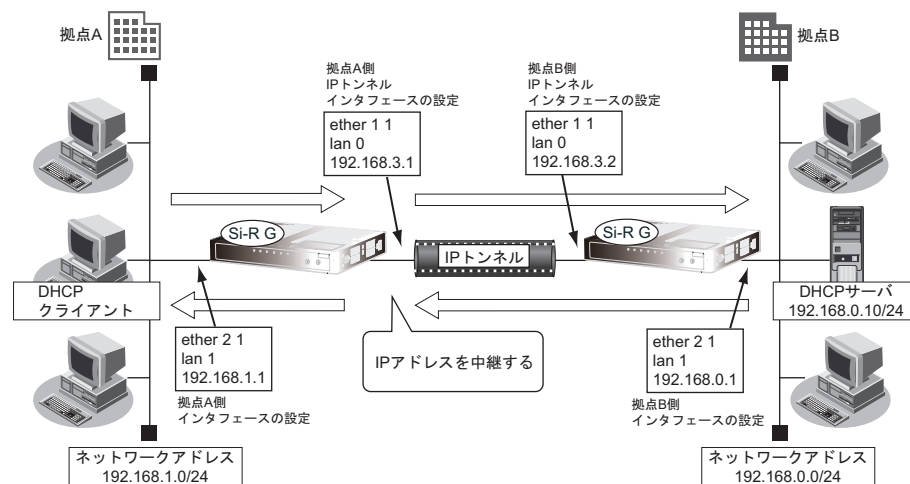
```
etherポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

lanインタフェースを設定する
# lan 1 ip address 192.168.2.1/24 3
# lan 1 vlan 20

DHCPリレーエージェント機能を設定する
# lan 1 ip dhcp service relay 192.168.1.10

設定終了
# save
# commit
```

## リモート接続の場合



### ● 設定条件

- DHCPリレーエージェント機能を使用する
- 拠点AにDHCPクライアントが存在する
- 拠点BにDHCPサーバが存在する

#### [拠点A]

- 装置のIPアドレス : 192.168.1.1
- IPトンネル用インタフェースIPアドレス : 192.168.3.1
- ネットワークアドレス/ネットマスク : 192.168.1.0/24

#### [拠点B]

- 装置のIPアドレス : 192.168.0.1
- IPトンネル用インタフェースIPアドレス : 192.168.3.2
- ネットワークアドレス/ネットマスク : 192.168.0.0/24
- DHCPサーバのIPアドレス : 192.168.0.10

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

### 拠点A側装置の設定

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.3.1/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.1.1/24 3

接続先の情報を設定する
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 192.168.3.1
# remote 0 ap 0 tunnel remote 192.168.3.2
# remote 0 ip route 0 default 1 1

リレーエージェントを設定する
# lan 1 ip dhcp service relay 192.168.0.10

設定終了
# save
# commit
```

### 拠点B側装置の設定

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

lan インタフェースを設定する
# lan 0 vlan 10
# lan 0 ip address 192.168.3.2/24 3
# lan 1 vlan 20
# lan 1 ip address 192.168.0.1/24 3

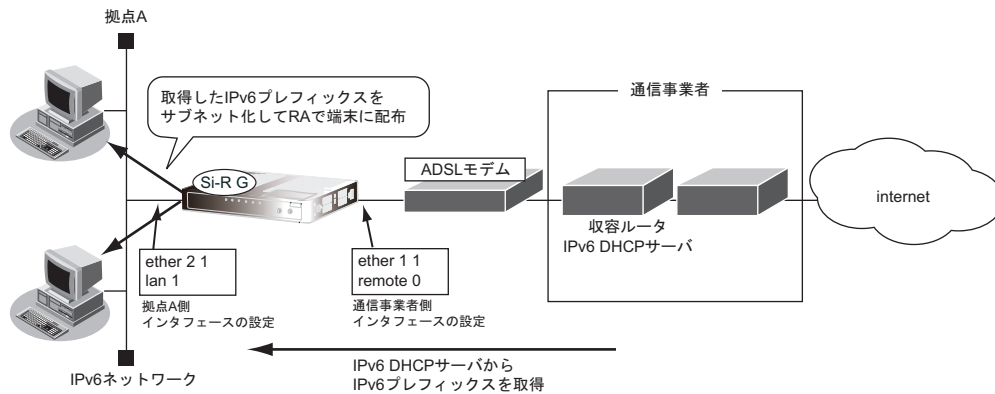
接続先の情報を設定する
# remote 0 ap 0 datalink type ip
# remote 0 ap 0 tunnel local 192.168.3.2
# remote 0 ap 0 tunnel remote 192.168.3.1
# remote 0 ip route 0 default 1 1

設定終了
# save
# commit
```



## 2.22.5 IPv6 DHCP クライアント機能を使う

IPv6 DHCPクライアント機能は、プロバイダのIPv6 DHCPサーバからIPv6プレフィックスなどの情報を取得する機能です。この機能を利用すると、プロバイダから取得したIPv6プレフィックスをサブネット化して、Router Advertisement Message (RA) で下流ネットワークに64ビットのIPv6プレフィックスを配布することができます。ここでは、PPPoEでインターネットに接続して、IPv6 DHCPクライアント機能を使用する場合の設定方法を説明します。



### ● 設定条件

- PPPoE で使用するポート : ETHERグループ 1 ポート 1
- ユーザ認証 ID : userid
- ユーザ認証パスワード : userpass
- IPv6 DHCPクライアントを有効にするインタフェース : remote 0
- IPv6 DHCPサーバから取得するIPv6プレフィックス長 : 48ビット
- IPv6プレフィックスを配布するインタフェース : lan 1
- RAで配布するIPv6プレフィックスのサブネットID : 0001

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド**

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 datalink type physical
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 default 1 1

IPv6 DHCP クライアントを設定する
# remote 0 ipv6 dhcp service client
# remote 0 ipv6 dhcp client option na off
# remote 0 ipv6 dhcp client option pd on

ProxyDNS を設定する
# proxydns domain 0 any * any on 0
# proxydns address 0 any on 0

lan 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@rmt0:1::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra prefix 0 dhcp@rmt0:1::/64 infinity infinity
# lan 1 vlan 20

設定終了
# save
# commit
```

## 2.22.6 IPv6 DHCP サーバ機能を使う

本装置のIPv6 DHCP サーバ機能は、以下の情報を広報することができます。

- IPv6 アドレス
- IPv6 プレフィックス
- DNS サーバのIPv6 アドレス
- DNS ドメイン名
- SIP サーバのIPv6 アドレス
- SIP ドメイン名
- SNTP サーバのIPv6 アドレス

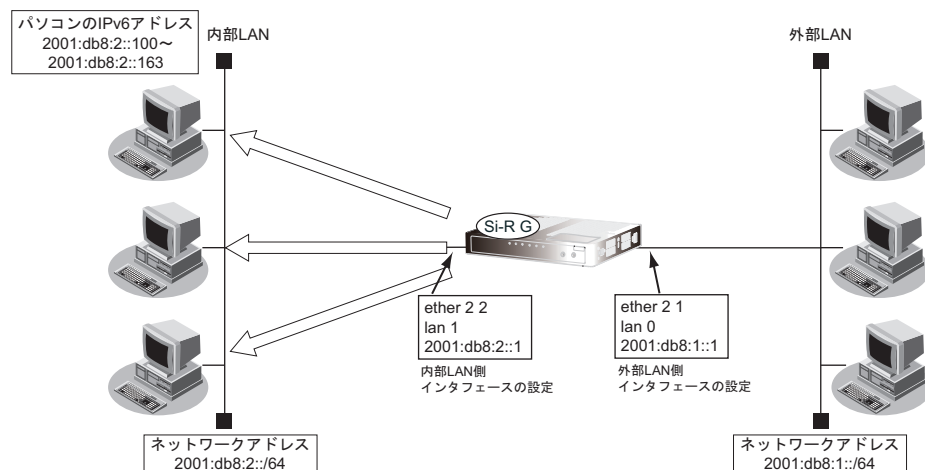
### こんな事に気をつけて

本装置のIPv6 DHCP サーバ機能は、IPv6 DHCP リレーエージェントのサーバにはなれません。

ここでは、IPv6 DHCP サーバ機能を使用する場合の設定方法を説明します。



IPv6 DHCP サーバ機能で割り当てることができるIPアドレスの最大数は300個です。



### ● 設定条件

#### [外部LAN側]

- 本装置のIPアドレス : 2001:db8:1::1
- ネットワークアドレス/プレフィックス長 : 2001:db8:1::/64

#### [内部LAN側]

- 本装置のIPアドレス : 2001:db8:2::1
- パソコンに割り当てるIPv6アドレス : 2001:db8:2::100~2001:db8:2::163
- パソコンに割り当て可能IPv6アドレス数 : 100
- ネットワークアドレス/プレフィックス長 : 2001:db8:2::/64
- Valid Lifetime : 30日
- Preferred Lifetime : 7日
- DNSサーバのIPv6アドレス : 2001:db8:2::1
- SNTPサーバのIPv6アドレス : 2001:db8:2::1
- IPv6 DHCP サーバ機能を使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

### 外部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lan インタフェースを設定する
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1::1/64
# lan 0 vlan 10

設定終了
# save
# commit
```

### 内部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

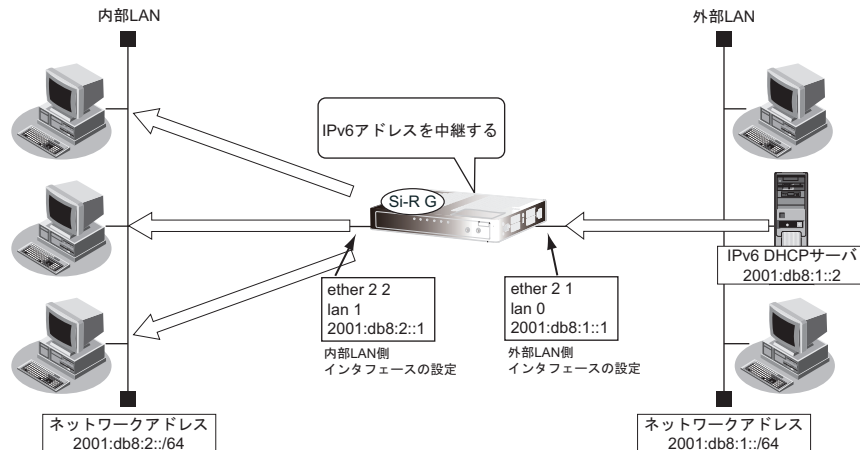
IPv6 DHCP サーバの動作するインタフェースを設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:2::1/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 2001:db8:2::/64 infinity infinity c0
# lan 1 vlan 20

IPv6 DHCP サーバ機能を設定する
# lan 1 ipv6 dhcp service server
# lan 1 ipv6 dhcp server info address 2001:db8:2::100 100 30d 7d
# lan 1 ipv6 dhcp server info dns 2001:db8:2::1
# lan 1 ipv6 dhcp server info sntpserver 2001:db8:2::1

設定終了
# save
# commit
```

## 2.22.7 IPv6 DHCP リレーエージェント機能を使う

ここでは、IPv6 DHCP リレーエージェント機能を使用する場合の設定方法を説明します。



### ● 設定条件

#### [外部 LAN 側]

- 本装置の IPv6 アドレス : 2001:db8:1::1
- IPv6 DHCP サーバアドレス : 2001:db8:1::2

#### [内部 LAN 側]

- 本装置の IPv6 アドレス : 2001:db8:2::1
- IPv6 DHCP リレーエージェント機能を使用する

#### こんな事に気をつけて

IPv6 DHCP リレーエージェント機能を使用するインタフェースには、ユニークローカルユニキャストアドレスのプレフィックス「fc00::/7」、またはグローバルユニキャストアドレスのプレフィックス「2000::/3」を持つ IPv6 アドレスが設定されている必要があります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

#### 外部 LAN 側インタフェースの設定

```
ether ポートを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 10

lan インタフェースを設定する
# lan 0 ipv6 use on
# lan 0 ipv6 address 0 2001:db8:1::1/64
# lan 0 vlan 10

設定終了
# save
# commit
```

**内部LAN インタフェースの設定**

```
ether ポートを設定する
# ether 2 2 use on
# ether 2 2 vlan untag 20

lan インタフェースを設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 2001:db8:2::1/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 2001:db8:2::/64 infinity infinity c0
# lan 1 vlan 20

IPv6 DHCP リレーエージェント機能を設定する
# lan 1 ipv6 dhcp service relay
# lan 1 ipv6 dhcp relay interface lan0

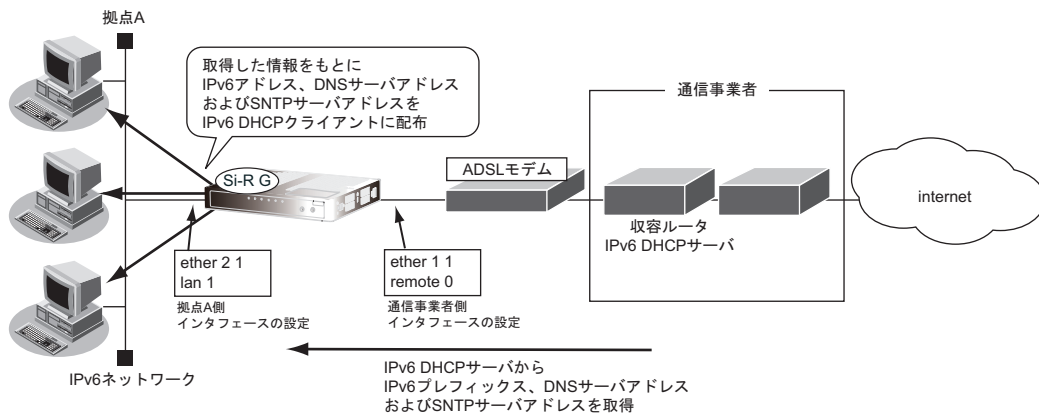
設定終了
# save
# commit
```

## 2.22.8 IPv6 DHCP クライアント機能で取得した情報を IPv6 DHCP サーバ機能で配布する

ここでは、IPv6 DHCP クライアント機能と IPv6 DHCP サーバ機能を併用し、クライアントが取得した情報をサーバが配布する場合の設定方法を説明します。

### こんな事に気をつけて

クライアントが取得した情報のうち、IPv6 プレフィックス、DNS サーバアドレス以外の取得情報を自装置で使うことはできません。



### ● 設定条件

- PPPoE で使用するポート : ETHER グループ 1 ポート 1
- ユーザ認証 ID : userid
- ユーザ認証パスワード : userpass
- IPv6 DHCP サーバから取得する IPv6 プレフィックス長 : 48 ビット
- IPv6 アドレスを配布する lan ポート : lan 1 ポート
- パソコンに割り当てる IPv6 アドレスのサブネット ID : 0001
- パソコンに割り当てる IPv6 アドレスのインターフェース ID : ::100 ~ ::163
- パソコンに割り当て可能 IPv6 アドレス数 : 100
- パソコンに配布する DNS サーバの IPv6 アドレス : IPv6 DHCP クライアントが取得した DNS サーバアドレス
- パソコンに配布する SNTP サーバの IPv6 アドレス : IPv6 DHCP クライアントが取得した SNTP サーバアドレス

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド**

ETHER ポートを設定する

```
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20
```

接続先の情報を設定する

```
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ipv6 use on
# remote 0 ipv6 route 0 default 1 1
```

IPv6 DHCP クライアントを設定する

```
# remote 0 ipv6 dhcp service client
# remote 0 ipv6 dhcp client option na off
# remote 0 ipv6 dhcp client option pd on
```

LAN 情報を設定する

```
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@rmt0:1::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 dhcp@rmt0:1::/64 infinity infinity
# lan 1 vlan 20
```

IPv6 DHCP サーバを設定する

```
# lan 1 ipv6 dhcp service server
# lan 1 ipv6 dhcp server info address dhcp@rmt0:1::100 100 30d 7d
# lan 1 ipv6 dhcp server info dns dhcp@rmt0
# lan 1 ipv6 dhcp server info sntpserver dhcp@rmt0
```

設定終了

```
# save
# commit
```



## 2.22.9 通信事業者からのRA情報と連携してIPv6 DHCPクライアント機能を使用する

通信事業者の収容ルータが広報するRA (Router Advertisement) と連携して、IPv6 DHCPクライアント機能を使用することができます。

受信したRAと連携できるIPv6 DHCPクライアントの機能は以下のとおりです。

- IPv6 DHCPサーバへの問い合わせ  
MまたはOフラグが設定されたRAを受信した場合に、問い合わせを開始することができます。
- IPv6アドレスの要求  
Mフラグが設定されたRAを受信した場合に、IPv6 DHCPサーバにIPv6アドレスを要求することができます。
- IPv6プレフィックスの要求  
Mフラグが設定されたRAを受信した場合に、IPv6 DHCPサーバにIPv6プレフィックスを要求することができます。
- IPv6アドレス、IPv6プレフィックス以外の要求  
Oフラグだけが設定されたRAを受信した場合に、IPv6アドレス、IPv6プレフィックス以外のIPv6 DHCPサーバアドレスといったパラメタ情報だけを要求します。  
Mフラグが設定されたRAを受信した場合は、Oフラグの設定に関係なく、IPv6アドレス、IPv6プレフィックスに加え、DNSサーバアドレスなどのパラメタ情報の要求を行います。

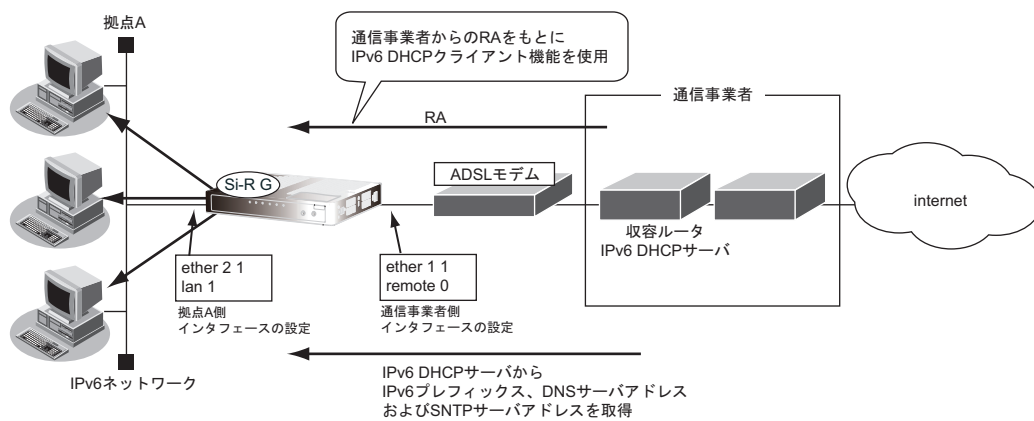
RAをもとにIPv6 DHCPクライアントが取得した情報は、以下の場合無効となります。

- RAのルータ有効期限 (Router Lifetime) がタイムアウトした場合
- MおよびOフラグが設定されていないRAを受信した場合

### こんな事に気をつけて

複数の通信事業者からRAを受信し、それぞれのRAでMフラグ、Oフラグの設定が異なっている場合は、すべてのRAのフラグの論理和の結果で判断します。たとえば、Mフラグを設定する収容ルータが1台だけであっても、IPv6 DHCPクライアントは、Mフラグが設定されている場合の動作となります。

ここでは、受信したRAをもとにIPv6 DHCPクライアント機能で通信事業者から情報を取得し、取得した情報をIPv6 DHCPサーバ機能で配布する方法について説明します。



● **設定条件**

- PPPoE で使用するポート : ETHERグループ 1 ポート 1
- ユーザ認証 ID : userid
- ユーザ認証パスワード : userpass
- 通信事業者からの RA : 受信
- IPv6 DHCP サーバへの問い合わせ : M または O フラグが指定された RA を受信した場合に問い合わせを開始
- IPv6 DHCP サーバへの IPv6 アドレスの要求 : M フラグが指定された RA を受信した場合に要求
- IPv6 DHCP サーバへの IPv6 プレフィックスの要求 : M フラグが指定された RA を受信した場合に要求
- IPv6 DHCP サーバから取得する IPv6 プレフィックス長 : 48 ビット
- IPv6 アドレスを配布する lan ポート : lan 1 ポート
- パソコンに割り当てる IPv6 アドレスのサブネット ID : 0001
- パソコンに割り当てる IPv6 アドレスのインタフェース ID : ::100 ~ ::163
- パソコンに割り当て可能 IPv6 アドレス数 : 100
- パソコンに配布する DNS サーバの IPv6 アドレス : IPv6 DHCP クライアントが取得した DNS サーバアドレス
- パソコンに配布する SNTP サーバの IPv6 アドレス : IPv6 DHCP クライアントが取得した SNTP サーバアドレス

上記の設定条件に従って設定を行う場合のコマンド例を示します。

● **コマンド**

```
ETHER ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 10
# ether 2 1 use on
# ether 2 1 vlan untag 20

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 keep connect
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ipv6 use on
# remote 0 ipv6 ra mode recv
# remote 0 ipv6 route 0 default 1 1

IPv6 DHCP クライアントを設定する
# remote 0 ipv6 dhcp service client auto
# remote 0 ipv6 dhcp client option na on
# remote 0 ipv6 dhcp client option pd on

LAN 情報を設定する
# lan 1 ipv6 use on
# lan 1 ipv6 address 0 dhcp@rmt0:1::/64
# lan 1 ipv6 ra mode send
# lan 1 ipv6 ra flags c0
# lan 1 ipv6 ra prefix 0 dhcp@rmt0:1::/64 infinity infinity
```

```
# lan 1 vlan 20
```

```
IPv6 DHCP サーバを設定する
```

```
# lan 1 ipv6 dhcp service server
```

```
# lan 1 ipv6 dhcp server info address dhcp@rmt0:1::100 100 30d 7d
```

```
# lan 1 ipv6 dhcp server info dns dhcp@rmt0
```

```
# lan 1 ipv6 dhcp server info sntpserver dhcp@rmt0
```

```
設定終了
```

```
# save
```

```
# commit
```

## 2.23 DNS サーバ機能を使う (ProxyDNS)

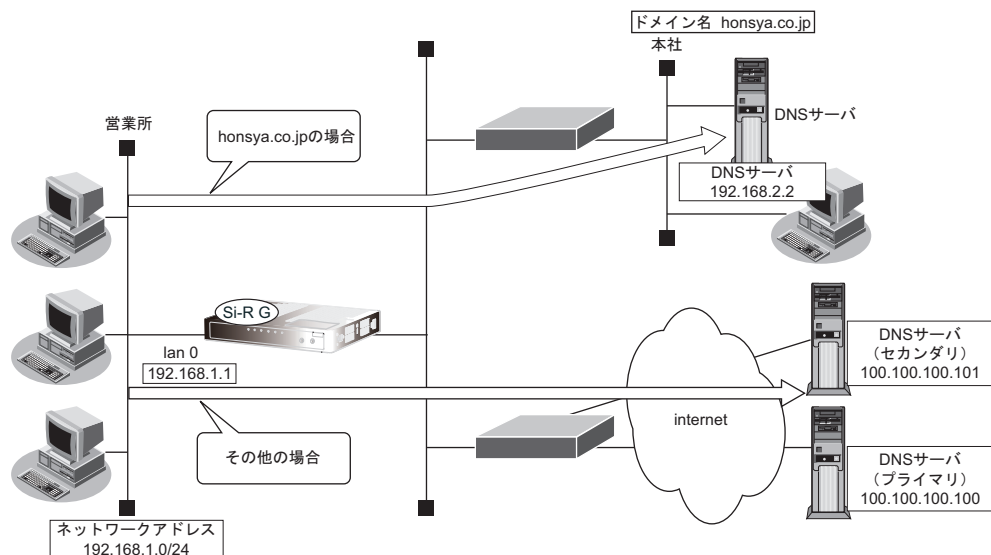
本装置のProxyDNSには、以下の機能があります。

- DNS サーバの自動切り替え機能
- DNS サーバアドレスの自動取得機能
- DNS 問い合わせタイプフィルタ機能
- DNS サーバ機能

☞ 参照 マニュアル「機能説明書」

### 2.23.1 DNS サーバの自動切り替え機能 (順引き) を使う

ProxyDNSは、パソコン側で本装置のIPアドレスをDNSサーバのIPアドレスとして登録するだけで、ドメインごとに使用するDNSサーバを切り替えて中継できます。ここでは、順引きの場合の設定方法を説明します。



#### ● 設定条件

- 会社のDNSサーバを使用する場合
 

使用するドメイン	: honsya.co.jp
DNSサーバのIPアドレス	: 192.168.2.2
- インターネット上のDNSサーバを使用する場合
 

使用するドメイン	: honsya.co.jp 以外
DNSサーバのIPアドレス	: 100.100.100.100、100.100.100.101

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

```
DNS サーバ自動切り替え機能 (順引き) を設定する
# proxydns domain 0 any *.honsya.co.jp any static 192.168.2.2
# proxydns domain 1 any * any static 100.100.100.100 100.100.100.101

設定終了
# save
# commit
```

## パソコン側の設定を確認する

1. パソコン側が DHCP クライアントかどうか確認します。

DHCP クライアントでない場合は設定します。

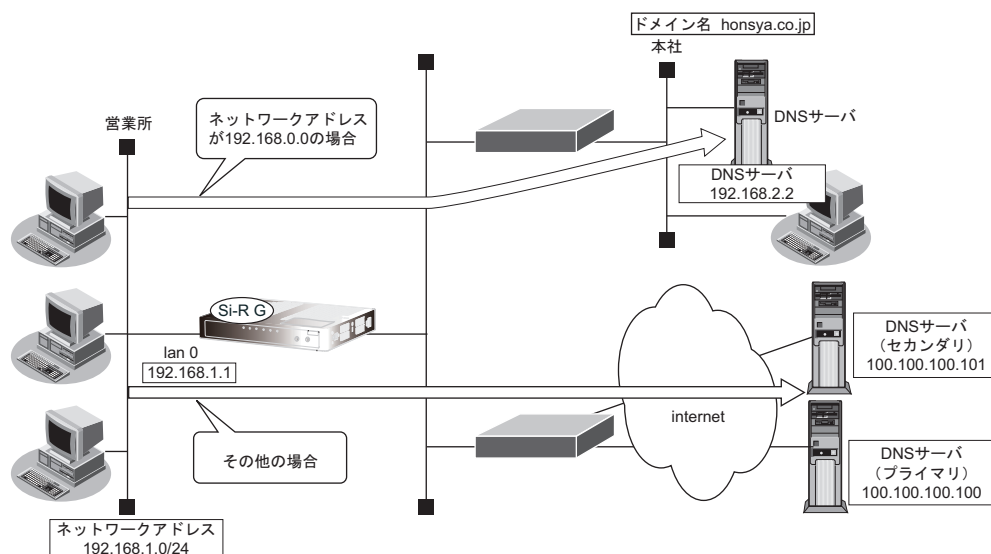
### こんな事に気をつけて

コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザーズガイド」

## 2.23.2 DNS サーバの自動切り替え機能（逆引き）を使う

ProxyDNSは、先に説明した順引きとは逆に、IP アドレスごとに使用する DNS サーバを切り替えて中継できます。ここでは、逆引きの場合の設定方法を説明します。



### ● 設定条件

- 会社の DNS サーバを使用する場合  
 逆引き対象のネットワークアドレス : 192.168.0.0  
 DNS サーバの IP アドレス : 192.168.2.2
- インターネット上の DNS サーバを使用する場合  
 逆引き対象のネットワークアドレス : 192.168.0.0 以外  
 DNS サーバの IP アドレス : 100.100.100.100、100.100.100.101

### こんな事に気をつけて

コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「[」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
DNS サーバ自動切り替え機能（逆引き）を設定する
# proxydns address 0 192.168.0.0/24 static 192.168.2.2
# proxydns address 1 any static 100.100.100.100 100.100.100.101

設定終了
# save
# commit
```

## パソコン側の設定を確認する

1. パソコン側が DHCP クライアントかどうか確認します。  
 DHCP クライアントでない場合は設定します。

## 2.23.3 DNS サーバアドレスの自動取得機能を使う

この機能を利用すると、ProxyDNSがDNSサーバのアドレスを、回線接続時に接続先から自動的に取得します。そのため、DNSサーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、接続先がPPP IPCP (RFC1877)、DHCP (RFC2131)、IPv6 DHCP (RFC3361) のどれかによるDNSサーバアドレスの配布機能に対応している場合に利用できます。

### ● 設定条件

- ドメイン名 : \*
- 動作 : 接続先のDNSサーバへ指定ネットワークを経由して問い合わせる

### こんな事に気をつけて

コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「[」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置側を設定する

### ● コマンド

```
DNS サーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any on 0 off

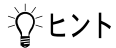
設定終了
# save
# commit
```

## パソコン側の設定を行う

---

ここでは、Windows 7の場合を例に説明します。

1. [スタート] - [コントロールパネル] をクリックします。
2. [ネットワークとインターネット] をクリックします。
3. [ネットワークと共有センター] をクリックします。
4. [アダプターの設定の変更] をクリックします。
5. [ローカルエリア接続] アイコンを右クリックし、[プロパティ] ボタンをクリックします。  
[ローカルエリア接続のプロパティ] ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4 (TCP/IPv4)」を選択します。
7. [プロパティ] ボタンをクリックします。  
[インターネットプロトコルバージョン4 (TCP/IPv4) のプロパティ] ダイアログボックスが表示されます。
8. 「次のDNSサーバーのアドレスを使う」を選択します。
9. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
10. [OK] ボタンをクリックします。  
[ローカルエリア接続のプロパティ] ダイアログボックスに戻ります。
11. [閉じる] ボタンをクリックします。  
設定した内容が有効になります。



### ◆ 本装置の「DHCP サーバ機能」を使わない場合の設定は？

パソコン側の「DNS 設定」で本装置のIPアドレスを指定すると、ProxyDNS 機能だけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを指定するとProxyDNS 機能を使用できます。

### ◆ DNS 解決したホストへのホスト経路を自動で作成する設定は？

以下のコマンドを設定することにより、DNS 解決したホストへのホスト経路を自動で作成することができます。

```
# proxydns domain 0 any * any on 0 on
```

### ◆ 「接続先のDNSサーバへ問い合わせる」と「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」の違いは？

「接続先のDNSサーバへ問い合わせる」は、経路情報に従って、接続先から取得したDNSサーバへ問い合わせるのに対して、「接続先のDNSサーバへ指定ネットワークを経由して問い合わせる」は、経路情報を無視して指定ネットワークを経由して、接続先から取得したDNSサーバへ問い合わせます。ただし、TCPによる問い合わせ時は「接続先のDNSサーバへ問い合わせる」と同様に経路情報に従います。

---



## 2.23.4 DNS サーバアドレスを DHCP サーバから取得して使う

この機能を利用すると、ProxyDNSがDNSサーバのアドレスを、DHCPサーバから自動的に取得します。そのため、DNSサーバのアドレスを、あらかじめ設定しておく必要はありません。

なお、この機能は、DHCPサーバがDNSサーバのアドレスを広報している場合にだけ利用できます。

### ● 設定条件

- ドメイン名 : \*
- 動作 : lan0のDNSサーバへ問い合わせる

### こんな事に気をつけて

コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「[」、<、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置側を設定する

### ● コマンド

```
DNSサーバアドレスの自動取得機能を設定する
# proxydns domain 0 any * any dhcp lan0
```

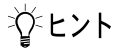
```
設定終了
# save
# commit
```

## パソコン側の設定を行う

---

ここでは、Windows 7の場合を例に説明します。

1. [スタート] - [コントロールパネル] をクリックします。
2. [ネットワークとインターネット] をクリックします。
3. [ネットワークと共有センター] をクリックします。
4. [アダプターの設定の変更] をクリックします。
5. [ローカルエリア接続] アイコンを右クリックし、[プロパティ] ボタンをクリックします。  
[ローカルエリア接続のプロパティ] ダイアログボックスが表示されます。
6. 一覧から「インターネットプロトコルバージョン4 (TCP/IPv4)」を選択します。
7. [プロパティ] ボタンをクリックします。  
[インターネットプロトコルバージョン4 (TCP/IPv4) のプロパティ] ダイアログボックスが表示されます。
8. 「次のDNSサーバーのアドレスを使う」を選択します。
9. 「優先DNSサーバー」に、本装置のIPアドレスを入力します。
10. [OK] ボタンをクリックします。  
[ローカルエリア接続のプロパティ] ダイアログボックスに戻ります。
11. [閉じる] ボタンをクリックします。  
設定した内容が有効になります。



### ヒント

#### ◆ 本装置の「DHCP サーバ機能」を使わない場合の設定は？

パソコン側の「DNS 設定」で本装置のIPアドレスを指定すると、ProxyDNS 機能だけ使用できます。また、本装置以外のDHCPサーバを使用している場合でも、DHCPサーバで広報するDNSサーバのIPアドレスとして本装置のIPアドレスを指定するとProxyDNS 機能を使用できます。

---

## 2.23.5 DNS 問い合わせタイプフィルタ機能を使う

端末が送信するDNSパケットのうち、特定の問い合わせタイプ (QTYPE) のパケットを破棄することができます。たとえば、パソコンからの予期しないDNSパケット送信によって、自動発信の問題を回避するために、かんたん設定のかんたんフィルタを「使用する」に設定します。このとき、問い合わせタイプがSOA (6) とSRV (33) のパケットを破棄する場合の設定方法を説明します。

### こんな事に気をつけて

ProxyDNS機能を使用する場合、問い合わせタイプがA (1) のDNS問い合わせパケットを破棄するように指定すると、正常な通信が行えなくなります。

### ● 設定条件

- ドメイン名 : \*
- 問い合わせタイプ : SOA (6)
- 動作 : 破棄する

### こんな事に気をつけて

コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「|」、「<」、「>」、「&」、「%」は入力しないでください。

☛ 参照 マニュアル「コマンドユーザーズガイド」

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置側を設定する

### ● コマンド

```
DNS 問い合わせパケット破棄を設定する
# proxydns domain 0 6 * any reject

設定終了
# save
# commit
```

## パソコン側の設定を行う

パソコン側の設定を行います。

設定方法は、[\[2.23.3 DNS サーバアドレスの自動取得機能を使う\]](#) (P.355) の「[パソコン側の設定を行う](#)」(P.356)を参照してください。

## 2.23.6 DNS サーバ機能を使う


本装置のホストデータベースにホスト名とIPアドレスを登録します。登録したホストに対してDNS要求があった場合は、ProxyDNSがDNSサーバの代わりに応答します。LAN内の情報をホストデータベースにあらかじめ登録しておくと、LAN内のホストのDNS要求によって回線が接続されるといったトラブルを防止できます。

### ● 設定条件

- ホスト名 : host.com
- IPv4 アドレス : 192.168.1.2
- IPv6 アドレス : 2001:db8::2

### こんな事に気をつけて

コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「[」、<、「>」、「&」、「%」は入力しないでください。

 参照 マニュアル「コマンドユーザーズガイド」


上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置側を設定する

### ● コマンド

```
ホストデータベース情報を設定する
# host 0 name host.com
# host 0 ip address 192.168.1.2
# host 0 ipv6 address 2001:db8::2

設定終了
# save
# commit
```

 補足 ホストデータベース情報は「DHCPスタティック機能」、「DNSサーバ機能」で使われており、それぞれ必要な項目だけを設定します。

## パソコン側の設定を行う

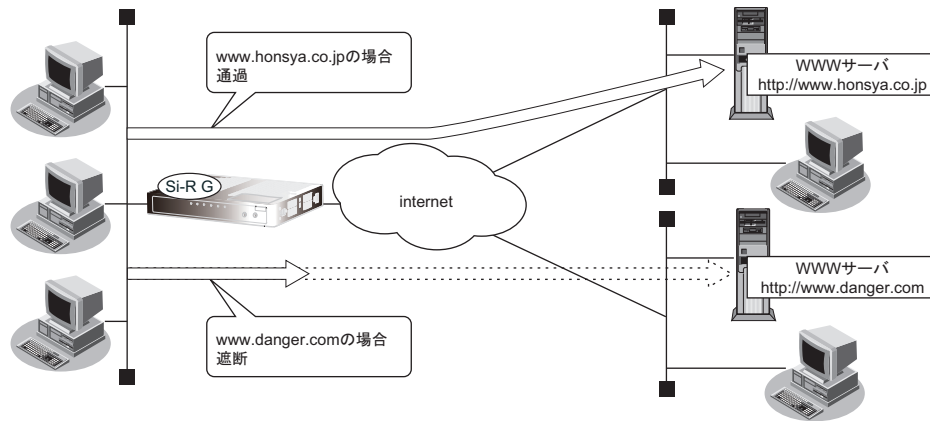
パソコン側の設定を行います。

設定方法は、[\[2.23.3 DNSサーバアドレスの自動取得機能を使う\] \(P.355\)](#) の「[パソコン側の設定を行う](#)」(P.356)を参照してください。

## 2.24 特定のURLへのアクセスを禁止する (URLフィルタ機能)

URLフィルタ機能は、特定のURLへのアクセスを禁止することができます。本機能を使用する場合は、ProxyDNS情報で設定します。

以下にURLフィルタを行う場合の設定方法を説明します。



☞ 参照 マニュアル「機能説明書」

ここでは、会社のネットワークとプロバイダがすでに接続されていることを前提とします。また、ProxyDNS情報は何も設定されていないものとします。

### ● 設定条件

- アクセスを禁止するドメイン名 : www.danger.com

### こんな事に気をつけて

- URLフィルタ機能を使用する場合は、LAN内のパソコンが本装置のIPアドレスをDNSサーバのIPアドレスとして登録する必要があります。
- コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、「」、「<」、「>」、「&」、「%」は入力しないでください。

☞ 参照 マニュアル「コマンドユーザーズガイド」

### 💡 ヒント

#### ◆ 「\*」は使えるの？

たとえば「www.danger.com」と「XXX.danger.com」の両方をURLフィルタの対象とする場合は「\*.danger.com」と指定することで両方を対象にできます。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

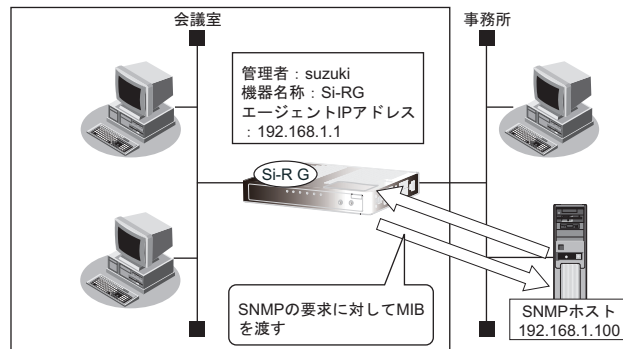
**● コマンド**

```
URL の情報を設定する  
# proxydns domain 0 any www.danger.com any reject  
# proxydns domain 1 any * any on 0
```

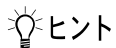
```
設定終了  
# save  
# commit
```

## 2.25 SNMP エージェント機能を使う

本装置は、SNMP (Simple Network Management Protocol) エージェント機能をサポートしています。ここでは、SNMP ホストに対して MIB 情報を通知する場合の設定方法を説明します。



☞ 参照 マニュアル「機能説明書」



### ◆ SNMP とは？

SNMP (Simple Network Management Protocol) は、ネットワーク管理用のプロトコルです。SNMP ホストは、ネットワーク上の端末の稼動状態や障害状況を一元管理します。SNMP エージェントは、SNMP ホストの要求に対して MIB (Management Information Base) という管理情報を返します。

また、特定の情報についてはトラップという機能を用いて、SNMP エージェントから SNMP ホストに対して非同期通知を行うことができます。

☞ 参照 マニュアル「仕様一覧」

### こんな事に気をつけて

- エージェントアドレスには、本装置に設定されたどれかのインタフェースの IP アドレスを設定します。誤った IP アドレスを設定した場合は、SNMP ホストとの通信ができなくなります。
- 認証プロトコルとパスワード、暗号プロトコルとパスワードは、SNMP ホストの設定と同じにしてください。誤ったプロトコルとパスワードを設定した場合は、SNMP ホストとの通信ができなくなります。
- SNMPv3 で認証/暗号プロトコルを使用する場合、snmp 設定反映時の認証/暗号鍵生成に時間がかかります。このとき、セッション監視タイムアウトが発生するなど、ほかの処理に影響する可能性があります。
- SNMPv3 で使用される snmpEngineBoots 値は、装置再起動時に初期化 (初期値: 1) されます。そのため、MIB 情報取得中に装置が再起動されると、SNMP ホストによっては継続した MIB 情報の取得ができないことがあります。

## SNMPv1 または SNMPv2c でアクセスする場合の情報を設定する

SNMPv1 または SNMPv2c でアクセスする場合は、以下の情報を設定します。

### ● 設定条件

- SNMP エージェント機能を使用する
- 管理者 : suzuki
- 機器名称 : Si-RG
- 機器設置場所 : 1F (1階)
- エージェントアドレス : 192.168.1.1 (自装置 IP アドレス)
- SNMP ホストアドレス : 192.168.1.100
- コミュニティ名 : public00

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname Si-RG
# snmp agent location 1F
# snmp agent ip address 192.168.1.1

SNMP ホスト情報を設定する
# snmp manager 0 192.168.1.100 public00 off disable

SNMP エージェント機能を使用する
# snmp service enable

設定終了
# save
# commit
```



## SNMPv3 でアクセスする場合の情報を設定する

SNMPv3 でアクセスする場合は、以下の情報を設定します。

### ● 設定条件

- SNMP エージェント機能を使用する
- 管理者 : suzuki
- 機器名称 : Si-RG
- 機器設置場所 : 1F (1階)
- エージェントアドレス : 192.168.1.1 (自装置 IP アドレス)
- SNMP ホストアドレス : 192.168.1.100
- トラップ通知ホストアドレス : 192.168.1.100
- ユーザ名 : user00
- 認証プロトコル : MD5
- 認証パスワード : auth\_password
- 暗号プロトコル : DES
- 暗号パスワード : priv\_password
- MIB ビュー : MIB 読み出しは system、interfaces グループのみ許可。  
トラップ通知は linkDown、linkUp トラップのみ許可。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
SNMP エージェント情報を設定する
# snmp agent contact suzuki
# snmp agent sysname Si-RG
# snmp agent location 1F
# snmp agent ip address 192.168.1.1

SNMPv3 情報を設定する
# snmp user 0 name user00
# snmp user 0 address 0 192.168.1.100
# snmp user 0 notification 0 192.168.1.100

認証・暗号プロトコルを設定する
# snmp user 0 auth md5 auth_password
# snmp user 0 priv des priv_password

MIB ビュー情報を設定する
# snmp user 0 read view 0
# snmp user 0 notify view 0
# snmp view 0 subtree 0 include system
# snmp view 0 subtree 1 include interfaces
# snmp view 0 subtree 2 include linkdown
# snmp view 0 subtree 3 include linkup

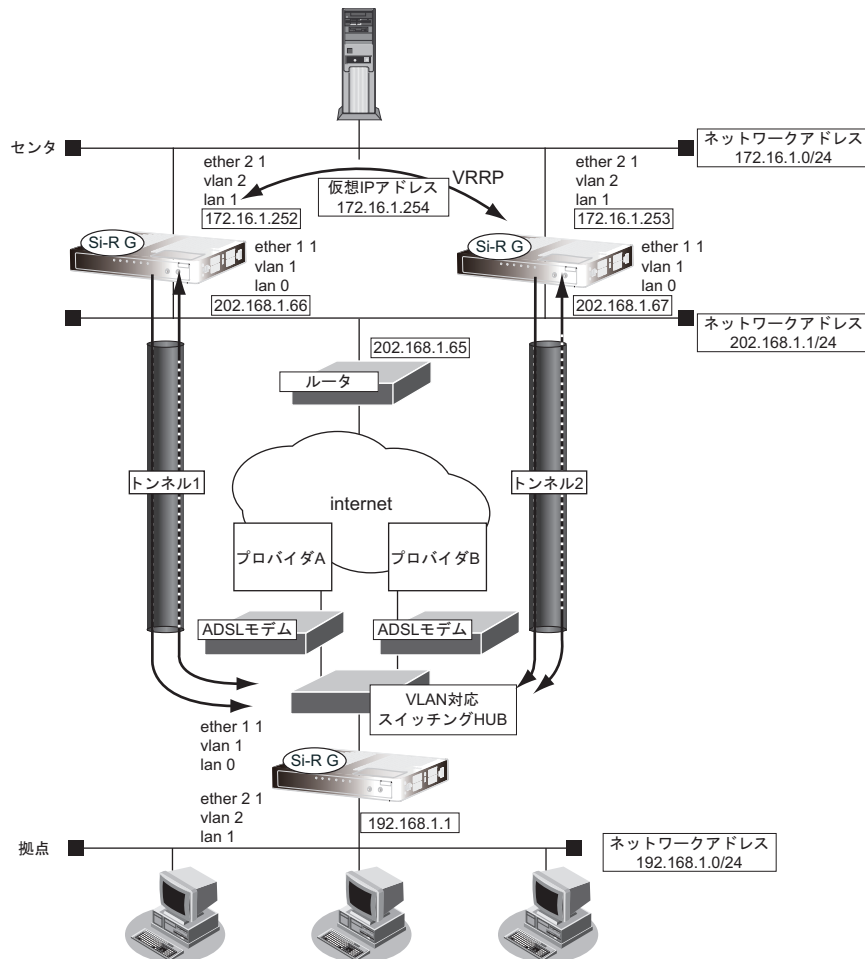
SNMP エージェント機能を使用する
# snmp service enable

設定終了
# save
# commit
```

## 2.26 ECMP 機能を使う

ここでは、ECMP 機能を利用した負荷分散通信を行う場合の設定方法を説明します。

ADSL では、受信速度は高速ですが、送信速度はそれほど高速ではありません。この例では、ADSL を2本利用して負荷を分散することで、送信速度の向上をはかります。さらに、片方のトンネルに障害が発生した場合に、通信可能なトンネルを利用して通信のバックアップを実現します。



☞ 参照 マニュアル「機能説明書」

### ● 設定条件

- 拠点では、センターへの通信は、トンネル1とトンネル2を利用して負荷分散して送信します。どちらかのトンネルで通信障害が発生した場合は、通信可能なトンネルだけを利用して送信します。
- センタでは、拠点への通信は、トンネル1だけを利用して送信します。トンネル1で通信障害が発生した場合は、トンネル2を利用して送信します。
- トンネル1の通信障害は、両端の本装置が接続先監視で検出します。  
この監視は、ISP Aの通信障害およびセンタ側本装置（左）の故障を検出します。
- トンネル2の通信障害は、両端の本装置が接続先監視で検出します。  
この監視は、ISP Bの通信障害およびセンタ側本装置（右）の故障を検出します。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

## [センタ側本装置 (左)]

```
lan 定義を削除する
# delete lan

Ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

lan 0 側を設定する
# lan 0 ip address 202.168.1.66/24 3
# lan 0 ip route 0 default 202.168.1.65 1 1
# lan 0 ip filter 0 pass acl 0 reverse
# lan 0 ip filter 1 pass acl 1 reverse
# lan 0 ip filter default reject
# lan 0 vlan 1

lan 1 側を設定する
# lan 1 ip address 172.16.1.252/24 3
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 172.16.1.254
# lan 1 vrrp group 0 trigger 0 ifdown rmt0
# lan 1 vlan 2

IPsec に関する ACL を設定する
# acl 0 ip 202.168.1.66/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.66/32 any 50 any

トンネルを設定する
# remote 0 name RMTbyA
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyA
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.66
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyA
# remote 0 ap 0 ike shared key text 12345678-A
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.252 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

**[センタ側本装置 (右)]**

```
lan 定義を削除する
# delete lan

Ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

lan 0 側を設定する
# lan 0 ip address 202.168.1.67/24 3
# lan 0 ip route 0 default 202.168.1.65 1 1
# lan 0 ip filter 0 pass acl 0 reverse
# lan 0 ip filter 1 pass acl 1 reverse
# lan 0 ip filter default reject
# lan 0 vlan 1

lan 1 側を設定する
# lan 1 ip address 172.16.1.253/24 3
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 100 172.16.1.254
# lan 1 vrrp group 0 trigger 0 ifdown rmt0
# lan 1 vlan 2

IPsec に関する ACL を設定する
# acl 0 ip 202.168.1.67/32 any 17 any
# acl 0 udp 500 500
# acl 1 ip 202.168.1.67/32 any 50 any

トンネルを設定する
# remote 0 name RMTbyB
# remote 0 ip route 0 192.168.1.0/24 1 1
# remote 0 ip msschange 1360
# remote 0 mtu 1400
# remote 0 ap 0 name IPsecbyB
# remote 0 ap 0 datalink type ipsec
# remote 0 ap 0 tunnel local 202.168.1.67
# remote 0 ap 0 ipsec type ike
# remote 0 ap 0 ipsec ike protocol esp
# remote 0 ap 0 ipsec ike range any4 any4
# remote 0 ap 0 ipsec ike encrypt des-cbc
# remote 0 ap 0 ipsec ike auth hmac-md5
# remote 0 ap 0 ipsec ike pfs modp768
# remote 0 ap 0 ike name remote RMTbyB
# remote 0 ap 0 ike shared key text 12345678-B
# remote 0 ap 0 ike proposal 0 encrypt des-cbc
# remote 0 ap 0 sessionwatch address 172.16.1.253 192.168.1.1
# remote 0 ap 0 sessionwatch interval 5s 1m 5s

設定終了
# save
# commit
```

**[拠点側本装置]**

```
lan 定義を削除する
# delete lan

PPPoE で利用する Ether ポート LAN を設定する
# ether 1 1 use on
# ether 1 1 vlan tag 10,20

lan で使用する Ether ポートとアドレスを設定する
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2
# lan 0 ip address 192.168.1.1/24 3
# lan 0 vlan 2

IPsec に関する ACL を設定する
# acl 0 ip any 202.168.1.66/32 17 any
# acl 0 udp 500 500
# acl 1 ip any 202.168.1.66/32 50 any
# acl 2 ip any 202.168.1.67/32 17 any
# acl 2 udp 500 500
# acl 3 ip any 202.168.1.67/32 50 any

プロバイダ A を利用する PPPoE 接続を設定する
# remote 0 name INTER-A
# remote 0 ip route 0 202.168.1.66/32 1 1
# remote 0 ip filter 0 pass acl 0 reverse
# remote 0 ip filter 1 pass acl 1 reverse
# remote 0 ip filter default reject
# remote 0 ip msschange 1414
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-A
# remote 0 ap 0 datalink bind vlan 10
# remote 0 ap 0 ppp auth send UIDtoA PASStoA
# remote 0 ap 0 keep connect
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.1.1 500 any 500 17
# remote 0 ip nat static 1 192.168.1.1 any any any 50

プロバイダ B を利用する PPPoE 接続を設定する
# remote 1 name INTER-B
# remote 1 ip route 0 202.168.1.67/32 1 1
# remote 1 ip filter 0 pass acl 2 reverse
# remote 1 ip filter 1 pass acl 3 reverse
# remote 1 ip filter default reject
# remote 1 ip msschange 1414
# remote 1 mtu 1454
# remote 1 ap 0 name ISP-B
# remote 1 ap 0 datalink bind vlan 20
# remote 1 ap 0 ppp auth send UIDtoB PASStoB
# remote 1 ap 0 keep connect
# remote 1 ip nat mode multi any 1 5m
# remote 1 ip nat static 0 192.168.1.1 500 any 500 17
# remote 1 ip nat static 1 192.168.1.1 any any any 50
```

```
センタ側本装置（左）とのトンネルを設定する
# remote 2 name CENTER-A
# remote 2 ip route 0 172.16.1.0/24 1 2
# remote 2 ip msschange 1360
# remote 2 mtu 1400
# remote 2 ap 0 name IPsecbyA
# remote 2 ap 0 datalink type ipsec
# remote 2 ap 0 tunnel remote 202.168.1.66
# remote 2 ap 0 ipsec type ike
# remote 2 ap 0 ipsec ike protocol esp
# remote 2 ap 0 ipsec ike range any4 any4
# remote 2 ap 0 ipsec ike encrypt des-cbc
# remote 2 ap 0 ipsec ike auth hmac-md5
# remote 2 ap 0 ipsec ike pfs modp768
# remote 2 ap 0 ike name local RMTbyA
# remote 2 ap 0 ike shared key text 12345678-A
# remote 2 ap 0 ike proposal 0 encrypt des-cbc
# remote 2 ap 0 sessionwatch address 192.168.1.1 172.16.1.252
# remote 2 ap 0 sessionwatch interval 5s 1m 5s

センタ側本装置（右）とのトンネルを設定する
# remote 3 name CENTER-B
# remote 3 ip route 0 172.16.1.0/24 1 2
# remote 3 ip msschange 1360
# remote 3 mtu 1400
# remote 3 ap 0 name IPsecbyB
# remote 3 ap 0 datalink type ipsec
# remote 3 ap 0 tunnel remote 202.168.1.67
# remote 3 ap 0 ipsec type ike
# remote 3 ap 0 ipsec ike protocol esp
# remote 3 ap 0 ipsec ike range any4 any4
# remote 3 ap 0 ipsec ike encrypt des-cbc
# remote 3 ap 0 ipsec ike auth hmac-md5
# remote 3 ap 0 ipsec ike pfs modp768
# remote 3 ap 0 ike name local RMTbyB
# remote 3 ap 0 ike shared key text 12345678-B
# remote 3 ap 0 ike proposal 0 encrypt des-cbc
# remote 3 ap 0 sessionwatch address 192.168.1.1 172.16.1.253
# remote 3 ap 0 sessionwatch interval 5s 1m 5s

ECMPを設定する
# routemanage ip ecmp mode hash

設定終了
# save
# commit
```

## 2.27 VRRP 機能を使う

VRRP 機能は2つ以上のルータがグループを形成し、1台のルータ（仮想ルータ）のように動作します。グループ内の各ルータには優先度が設定されており、その優先度に従ってマスタールータ（実際に経路情報を処理する装置）とバックアップルータ（マスタールータで異常を検出したときに経路情報の処理を引き継ぐ装置）を決定します。

本装置には、以下のVRRP 機能があります。

- 簡易ホットスタンバイ機能  
動的に経路制御（RIP など）できない端末から、別のネットワークへの通信に使用しているルータがなんらかの理由で中継できなくなった場合、自動でほかのルータが通信をバックアップします。
- クラスタリング機能  
VRRP のグループを複数設定することで、通信の負荷分散と冗長構成を実現します。本装置では、2台のルータを組み合わせることで簡易ホットスタンバイによる信頼性の高い通信を実現できます。

☛ 参照 マニュアル「機能説明書」

### こんな事に気をつけて

- 本装置の電源の投入、マスタールータでの設定反映、または装置リセットを実行した場合、バックアップルータがマスタールータとなることがあります。プリエンプトモードが on の場合は自動で切り戻りますが、プリエンプトモードが off の場合は、`vrrp preempt-permit` コマンドで切り戻しを行う必要があります。
- 優先度の値が大きい方が優先的にマスタールータとなります。
- LAN に接続される装置はデフォルトルートとして仮想 IP アドレスを設定してください。
- ルータに設定する IP アドレスと仮想 IP アドレスには、異なる IP アドレスを設定することをお勧めします。同じ IP アドレスを設定した場合、その IP アドレスで装置にアクセスすることはできなくなります。同じにした場合、必ず、VRRP グループの VRRP ルータの優先度を `“master ip|ipv6”` に設定してください（VRRP ルータの優先度として `“master ip|ipv6”` を設定した場合、仮想 IP アドレスは設定できません）。
- VRRP 機能では、VRRP-AD メッセージに以下のパケットを使用します。IP フィルタ設定時には、このパケットを遮断しないように設定する必要があります。

#### IPv4-VRRP

あて先 IP アドレス : 224.0.0.18

プロトコル番号 : 112

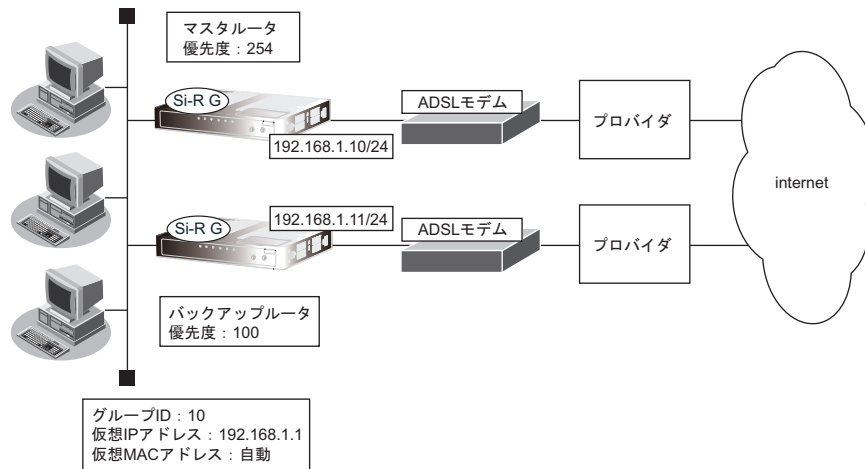
#### IPv6-VRRP

あて先 IP アドレス : ff02::12

IPv6 Next Header : 112

## 2.27.1 簡易ホットスタンバイ機能を使う

本装置では、2台のルータを組み合わせることで簡易ホットスタンバイ機能による信頼性の高い通信を実現できます。2台のルータをPPPoEでインターネットに接続して、ホットスタンバイを構成する場合の設定方法を説明します。



### ● 設定条件

- ・ 故障発生後の切り戻しは手動で行う
- ・ マスタルータはWAN側経路をノードダウントリガによって監視する

#### [マスタルータ]

- ・ PPPoEで使用するポート : ETHERグループ1ポート1
- ・ 本装置のIPアドレス/ネットマスク : 192.168.1.10/24
- ・ ユーザ認証ID : userid
- ・ ユーザ認証パスワード : userpass
- ・ ノードダウントリガの監視IPアドレス : 202.168.2.1 (プロバイダ側のDNSサーバアドレスなど)

#### [バックアップルータ]

- ・ PPPoEで使用するポート : ETHERグループ1ポート1
- ・ 本装置のIPアドレス/ネットマスク : 192.168.1.11/24
- ・ ユーザ認証ID : userid2
- ・ ユーザ認証パスワード : userpass2

上記の設定条件に従って設定を行う場合のコマンド例を示します。



**● コマンド****[マスタルータの設定]**

ADSL モデムに接続するインタフェースを設定する  
# ether 1 1 vlan untag 1

# delete lan 0

本装置の IP アドレスを設定する

# ether 2 1-4 vlan untag 2

# delete lan 1

# lan 1 ip address 192.168.1.10/24 3

# lan 1 vlan 2

接続先の情報を設定する

# remote 0 name internet

# remote 0 mtu 1454

# remote 0 ip route 0 default 1 1

# remote 0 ip nat mode multi any 1 5m

# remote 0 ip msschange 1414

# remote 0 ap 0 name ISP-1

# remote 0 ap 0 datalink bind vlan 1

# remote 0 ap 0 ppp auth send userid userpass

VRRP を設定する (ノードダウントリガを使用する)

# lan 1 vrrp use on

# lan 1 vrrp group 0 id 10 254 192.168.1.1

# lan 1 vrrp group 0 preempt off

# lan 1 vrrp group 0 trigger 0 node 202.168.2.1 any

設定終了

# save

再起動

# reset

**[バックアップルータの設定]**

ADSL モデムに接続するインタフェースを設定する

```
# ether 1 1 vlan untag 1
```

```
# delete lan 0
```

本装置の IP アドレスを設定する

```
# ether 2 1-4 vlan untag 2
```

```
# delete lan 1
```

```
# lan 1 ip address 192.168.1.11/24 3
```

```
# lan 1 vlan 2
```

接続先の情報を設定する

```
# remote 0 name internet
```

```
# remote 0 mtu 1454
```

```
# remote 0 ip route 0 default 1 1
```

```
# remote 0 ip nat mode multi any 1 5m
```

```
# remote 0 ip msschange 1414
```

```
# remote 0 ap 0 name ISP-1
```

```
# remote 0 ap 0 datalink bind vlan 1
```

```
# remote 0 ap 0 ppp auth send userid2 userpass2
```

VRRP を設定する

```
# lan 1 vrrp use on
```

```
# lan 1 vrrp group 0 id 10 100 192.168.1.1
```

```
# lan 1 vrrp group 0 preempt on
```

設定終了

```
# save
```

再起動

```
# reset
```

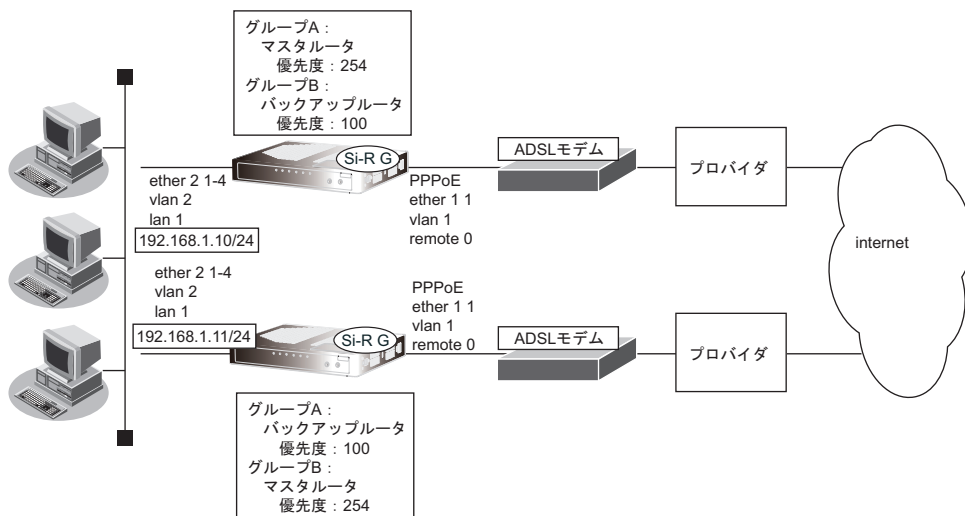
上の設定例で、インタフェースダウントリガを使用してWAN側（PPPoE）インタフェース状態を監視する場合は、以下の設定を追加します。

**● コマンド****[マスタルータの設定]**

```
# lan 1 vrrp group 0 trigger 0 ifdown rmt0
```

## 2.27.2 クラスタリング機能を使う

本装置では、2台のルータに複数のグループIDを設定することで、信頼性を高めると同時に通信の負荷分散を実現できます。2台のルータを PPPoE でインターネットに接続する場合の設定方法を説明します。



### ● 設定条件

- ・ 故障発生後の切り戻しは手動で行う
- ・ マスタルータは PPPoE 側のインタフェースをインタフェースダウントリガにより監視する

#### [グループA]

- ・ グループID : 10
- ・ 仮想IPアドレス : 192.168.1.1

#### [グループB]

- ・ グループID : 11
- ・ 仮想IPアドレス : 192.168.1.2

#### [マスタルータ]

- ・ PPPoE で使用するポート : ETHERグループ1ポート1
- ・ 本装置のIPアドレス/ネットマスク : 192.168.1.10/24
- ・ ユーザ認証ID : userid
- ・ ユーザ認証パスワード : userpass

#### [バックアップルータ]

- ・ PPPoE で使用するLANポート : ETHERグループ1ポート1
- ・ 本装置のIPアドレス/ネットマスク : 192.168.1.11/24
- ・ ユーザ認証ID : userid2
- ・ ユーザ認証パスワード : userpass2

### こんな事に気をつけて

クラスタリング機能を有効に利用するには、PCからのトラフィック量に応じて、PC側で設定するデフォルトルートの定義を適切に分散する必要があります。

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド****[マスタールータの設定]**

```
ADSL モデムに接続するインタフェースを設定する
# delete lan

# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

本装置の IP アドレスを設定する
# lan 1 ip address 192.168.1.10/24 3
# lan 1 vlan 2

接続先の情報を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ip route 0 default 1 1
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip msschange 1414
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass

VRRP を設定する (インタフェースダウントリガを使用する)
# lan 1 vrrp use on
# lan 1 vrrp group 0 id 10 254 192.168.1.1
# lan 1 vrrp group 0 preempt off
# lan 1 vrrp group 0 trigger 0 ifdown rmt0 254
# lan 1 vrrp group 1 id 11 100 192.168.1.2

設定終了
# save

再起動
# reset
```

**[バックアップルータの設定]**

ADSL モデムに接続するインタフェースを設定する

```
# delete lan
```

```
# ether 1 1 vlan untag 1
```

```
# ether 2 1-4 vlan untag 2
```

本装置のIPアドレスを設定する

```
# lan 1 ip address 192.168.1.11/24 3
```

```
# lan 1 vlan 2
```

接続先の情報を設定する

```
# remote 0 name internet
```

```
# remote 0 mtu 1454
```

```
# remote 0 ip route 0 default 1 1
```

```
# remote 0 ip nat mode multi any 1 5m
```

```
# remote 0 ip msschange 1414
```

```
# remote 0 ap 0 name ISP-1
```

```
# remote 0 ap 0 datalink bind vlan 1
```

```
# remote 0 ap 0 ppp auth send userid2 userpass2
```

VRRPを設定する

```
# lan 1 vrrp use on
```

```
# lan 1 vrrp group 0 id 10 100 192.168.1.1
```

```
# lan 1 vrrp group 1 id 11 254 192.168.1.2
```

```
# lan 1 vrrp group 1 preempt off
```

```
# lan 1 vrrp group 1 trigger 0 ifdown rmt0 254
```

設定終了

```
# save
```

再起動

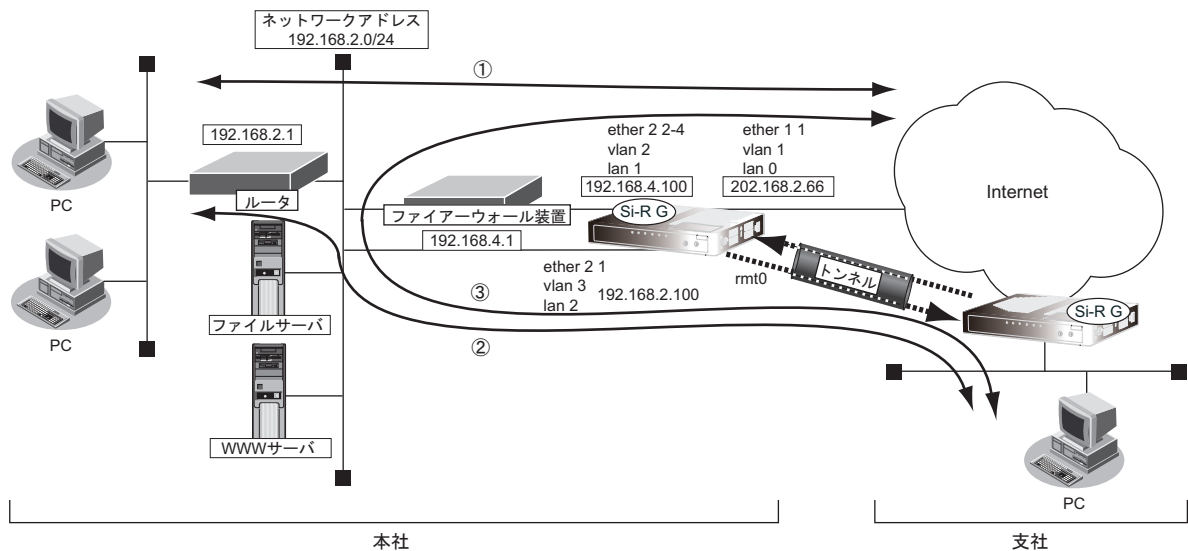
```
# reset
```

## 2.28 ポリシールーティング機能を使う

本装置では、入力側でポリシールーティングを行う Ingress ポリシールーティングと、出力側でポリシールーティングを行うマルチルーティングの2つを設定することができます。

### 2.28.1 Ingress ポリシールーティング機能を使う

Ingress ポリシールーティング機能とは、ルーティングによる経路情報の参照前に、入力パケットのあて先 IP アドレスだけではなく、送信元 IP アドレスやポート番号などの情報も利用して、設定した送出先へパケットを転送する機能です。この機能を利用することによって、受信インタフェースごとに経路情報に従わないパケット転送を行うことができます。ここでは、支社↔️本社は本社ネットワークのファイアウォールを通さずに通信し、支社↔️インターネットは本社ネットワークのファイアウォールを通して通信する場合の設定方法を説明します。



#### ● 前提条件

- 通信インタフェース
  - 本社の本装置の通信インタフェースが設定済み (ether、vlan、lan)
- 本社↔️インターネットの通信パス (①の通信パス)
  - 本社の本装置にインターネットへの通信が設定済み (lan 0)
- 支社↔️本社の通信パス (②の通信パス)
  - 本社の本装置に IPsec を利用した VPN 通信が設定済み (remote 0 ap 0)

#### ● 設定条件

- 支社↔️インターネットの通信は、本社のファイアウォールを経由する (③の通信パス)
  - lan 0 インタフェースに、本装置あてパケット以外を lan1 の 192.168.4.1 (ファイアウォール) に転送する Ingress ポリシールーティングを設定する
  - remote 0 インタフェースに、本装置あてパケット以外を lan2 の 192.168.2.1 に転送する Ingress ポリシールーティングを設定する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

本装置あて IPv4 パケットに一致する ACL 定義を設定する

```
# acl 0 ip any 202.168.2.66/32 any
```

すべての IPv4 パケットに一致する ACL 定義を設定する

```
# acl 1 ip any any any
```

本装置あてパケット以外を lan1 の 192.168.4.1 に転送するポリシーグループを設定する

```
# policy-group 0 pattern 0 unmatched acl 0
```

```
# policy-group 0 pattern 1 match acl 1
```

```
# policy-group 0 interface lan1
```

```
# policy-group 0 nexthop 192.168.4.1
```

本装置あてパケット以外を lan2 の 192.168.2.1 に転送するポリシーグループを設定する

```
# policy-group 1 pattern 0 unmatched acl 0
```

```
# policy-group 1 pattern 1 match acl 1
```

```
# policy-group 1 interface lan2
```

```
# policy-group 1 nexthop 192.168.2.1
```

lan 0 インタフェースに Ingress ポリシールーティングを設定する

```
# lan 0 ip in-policy 0 policy-group 0
```

remote 0 インタフェースに Ingress ポリシールーティングを設定する

```
# remote 0 ip in-policy 0 policy-group 1
```

設定終了

```
# save
```

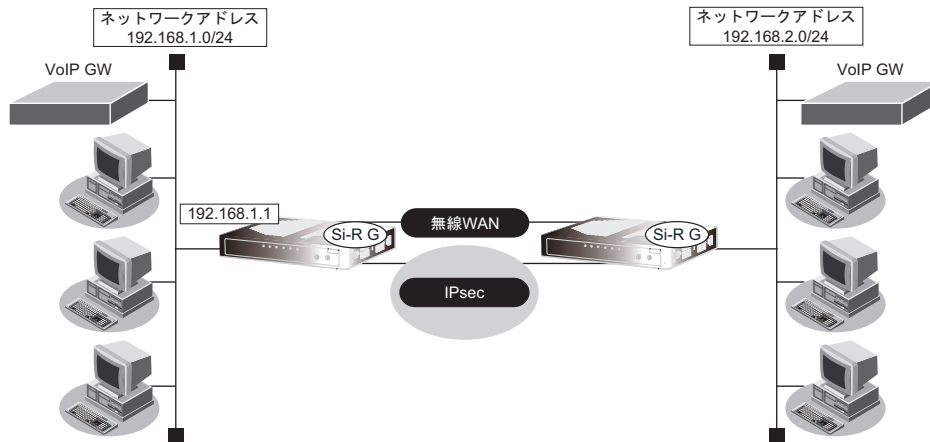
```
# commit
```

### こんな事に気をつけて

Ingress ポリシールーティング機能は、パケット選択ルールに一致した場合、ブロードキャストパケットやマルチキャストパケット、本装置あてパケットも転送します。

## 2.28.2 マルチルーティング機能を使う

マルチルーティング機能を使用すると、同じあて先ネットワークへの送信データを、別の通信パスを利用して送信することができます。



### ● 設定条件

- IPsec を利用した VPN 通信が設定済み (remote 0 ap 0)
  - 参照 [\[2.13.1 IPv4 over IPv4 で固定 IP アドレスでの VPN \(手動鍵交換\)\] \(P.159\)](#)
- 新規に音声データ用の無線 WAN (データ通信モジュール) を追加する
- 通常、音声データ (TOS 値 : a0) は無線 WAN を利用する
- 通常、その他のデータは IP-VPN を利用する
- 無線 WAN (音声用) がダウンした場合は、音声データも IP-VPN を使用する
- IP-VPN (データ用) がダウンした場合は、その他のデータも無線 WAN を使用する

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
無線 WAN 設定する
# wan 1 use on
# wan 1 bind usb
# wan 1 line modemmodule

通常は IP-VPN を音声データで使用しないように設定する
# remote 0 ap 0 multiroute pattern 0 backup any any any any 0 a0
# remote 0 ap 0 multiroute pattern 1 use any any any any 0 any

無線 WAN の接続先を設定する
# remote 0 ap 1 name WWAN
# remote 0 ap 1 datalink bind wan 1
# remote 0 ap 1 ppp auth send mopera mopara
# remote 0 ap 1 dial 0 number *99***1#
# remote 0 ppp ipcp vjcomp disable

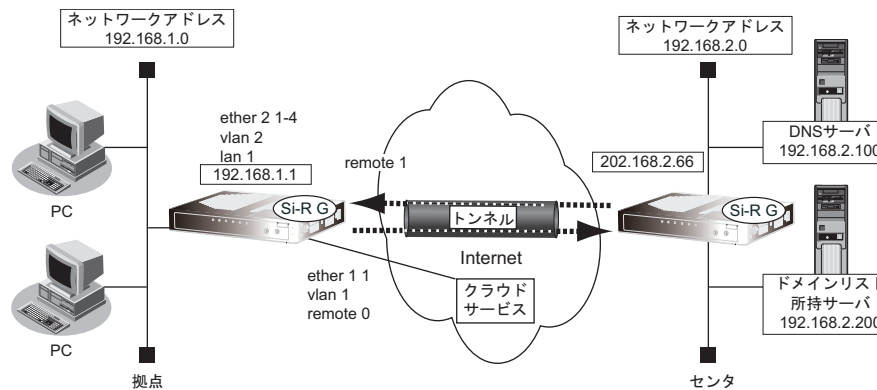
設定終了
# save
# commit
```



## 2.29 クラウドサービスゲートウェイ機能を使う

クラウドサービスゲートウェイ機能とは、通常の経路とは異なる経路を利用し、アクセス制御を行う機能です。アクセス制御はドメイン名によって行います。ドメイン名は、ドメインリストで設定する方法と構成定義に設定する方法があります。

この例では、拠点とセンタ間をインターネットVPNのデフォルト経路として設定し、Windows Updateに関する通信は直接インターネットへむかう設定について説明します。



### ● 前提条件

#### PPPoE 接続

- PPPoE ユーザ認証 ID : userid (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass (プロバイダから提示された内容)
- PPPoE ポート : ETHERグループポート1

#### 拠点内ローカルネットワーク

- ローカルネットワーク IP アドレス : 192.168.1.0/24

#### VPN 接続

- ネットワーク名 : v-center
- 接続先名 : center
- IPsec/IKE 区間 : 拠点-202.168.2.66
- IPsec 対象範囲 : any4-any4
- 鍵交換タイプ : Aggressive Mode
- IPsec プロトコル : esp
- IPsec 暗号アルゴリズム : aes-cbc-128
- IPsec 認証アルゴリズム : hmac-sha1
- IPsecDHグループ : modp768
- IKE 拠点 ID/ID タイプ : kyoten (自装置識別情報) /FQDN
- IKE 認証鍵 : abcdefghijklmnopqrst
- IKE 認証方法 : pre-shared (事前共有鍵方式)
- IKE 暗号アルゴリズム : aes-cbc-128
- IKE 認証アルゴリズム : hmac-sha1
- IKE DHグループ : modp768

## ● コマンド (共通部)

```
# ether 1 1 vlan untag 1
# ether 2 1-4 vlan untag 2

拠点内ローカルネットワークを設定する
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

PPPoE 接続を設定する
# remote 0 name internet
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 keep connect
# remote 0 ip nat mode multi any 1 5m

VPN 接続を設定する
# remote 1 name v-center
# remote 1 ip route 0 default 1 1
# remote 1 ap 0 name center
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike range any4 any4
# remote 1 ap 0 ipsec ike encrypt aes-cbc-128
# remote 1 ap 0 ipsec ike auth hmac-sha1
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike mode aggressive
# remote 1 ap 0 ike bind self
# remote 1 ap 0 ike idtype fqdn
# remote 1 ap 0 ike name local kyoten
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrst
# remote 1 ap 0 ike proposal 0 encrypt aes-cbc-128
# remote 1 ap 0 ike proposal 0 hash hmac-sha1
# remote 1 ap 0 ike proposal 0 pfs modp768
```

## パソコンの設定を確認する

DNS サーバのアドレスが本装置になっていることを確認してください。

## 2.29.1 ドメイン名をドメインリストで設定する

ドメイン名をセンタ側からドメインリストとして取得し、経路を制御します。経路制御方法としてProxyDNS機能およびIngress ポリシールーティング機能を併用します。

### ● 設定条件

- ・ ドメインリスト所持サーバのIPアドレス : 192.168.2.200
- ・ ドメインリスト所持サーバのユーザ名 : user
- ・ ドメインリスト所持サーバのパスワード : password
- ・ ドメインリストのパス名 : /list/domainlist
- ・ ドメインリストで使用するドメインID番号 : 0
- ・ 動的IPアドレスを使用するACL定義番号 : 0
- ・ 動的IPアドレス保持時間 : 1時間
- ・ センタ内のDNSサーバアドレス : 192.168.2.100
- ・ インターネット接続インタフェース : remote 0
- ・ 拠点内ローカルネットワークインタフェース : lan 1

### 💡 ヒント

#### ◆ ドメインID番号とは？

本機能では経路ごとにドメインID番号を定義することができます。  
ドメインID番号はドメインリストに記載し、対応したドメインだけが設定されます。

#### ◆ 動的IPアドレスを使用するACLとは？

本機能ではドメインリストのドメインで得られたIPアドレスをACLに動的に反映させます。  
使用する定義番号のACLのあて先IPアドレスに"dynamic"を記述し、ProxyDNS機能で設定するACL定義番号と対応させます。"dynamic"指定をしたACLはポリシーグループ設定以外に使用しないでください。

上記の設定条件に従って、クラウドサービスゲートウェイ設定を行う場合のコマンド例を示します。

### ● コマンド

```
ProxyDNS を設定する
# proxydns domain 0 domainlist 0 acl 0
# proxydns domain 0 any * any on 0 off
# proxydns domain 1 any * any static 192.168.2.100
# proxydns agetime 1h

ACL を設定する
# acl 0 ip any dynamic any

Ingress ポリシールーティングを設定する
# policy-group 0 pattern 0 match acl 0
# policy-group 0 interface rmt0
# lan 1 ip in-policy 0 policy-group 0


ドメインリスト情報を設定する
# domainlistinfo 192.168.2.200 user password /list/domainlist

設定終了
# save
# commit
```

---

### こんな事に気をつけて

- ドメインリストは、以下の方法で取得できます。
    - getdomainlist コマンド (domainlistinfo 設定必須)
    - スケジュール機能を使用する
  - ドメインリストおよびそのリスト内ドメインのIPアドレスは本装置がリセットするとクリアされます。そのため装置再起動後、ドメインリストのドメインに対して通信ができなくなってしまうことがあります。
  - ProxyDNS 機能で domainlist を指定する場合、proxysql domain コマンドで設定する <qname> は無視されます。
  - 拠点で使用する端末 (OS、インターネットブラウザなど) が設定した保持時間以上IPアドレスを保持する場合は、通信ができなくなってしまうことがあります。
  - ドメインリストの内容が変更された場合、ACLに含まれる動的IPアドレスは、継続して使用するドメインのIPアドレスを含めてすべてクリアされます。  
ただし、ドメインリストにドメインを追記する場合に限り、それまでのIPアドレスは保持されて継続して通信を行うことができます。
  - "dynamic" 指定をしたACLはポリシーグループ設定以外に使用しないでください。
  - proxysql domain コマンドの構成定義の変更を反映させると、ドメインリストおよび動的あて先IPアドレスはクリアされます。
- 

-  **参照** マニュアル「機能説明書」  
マニュアル「コマンドユーザーズガイド」  
「コマンドリファレンス」の「スケジュール情報」

## 2.29.2 ドメイン名を構成定義に設定する方法

ドメインリストを使用しないで、あらかじめドメイン名を設定しておき、そのドメイン名に対して経路を制御します。

経路制御方法としては ProxyDNS 機能を使用します。

### ● 設定条件

- Windows Update の際に通信を行うドメイン名

以下のドメインは 2012 年 4 月現在のもので、最新は Microsoft® のホームページでご確認ください。

ドメイン 1	: windowsupdate.microsoft.com
ドメイン 2	: *.windowsupdate.microsoft.com
ドメイン 3	: *.update.microsoft.com
ドメイン 4	: *.windowsupdate.com
ドメイン 5	: download.windowsupdate.com
ドメイン 6	: download.microsoft.com
ドメイン 7	: *.download.windowsupdate.com
ドメイン 8	: wustat.windows.com
ドメイン 9	: ntservicepack.microsoft.com

(\* は 0 文字以上複数文字列)

- 経路保持時間 : 1 時間

上記の設定条件に従って、クラウドサービスゲートウェイ設定を行う場合のコマンド例を示します。

### ● コマンド

```
ProxyDNS を設定する
# proxydns domain 0 any windowsupdate.microsoft.com any on 0 on
# proxydns domain 1 any *.windowsupdate.microsoft.com any on 0 on
# proxydns domain 2 any *.update.microsoft.com any on 0 on
# proxydns domain 3 any *.windowsupdate.com any on 0 on
# proxydns domain 4 any download.windowsupdate.com any on 0 on
# proxydns domain 5 any download.microsoft.com any on 0 on
# proxydns domain 6 any *.download.windowsupdate.com any on 0 on
# proxydns domain 7 any wustat.windows.com any on 0 on
# proxydns domain 8 any ntservicepack.microsoft.com any on 0 on
# proxydns domain 9 any * any static 192.168.2.100
# proxydns agetime 1h

設定終了
# save
# commit
```

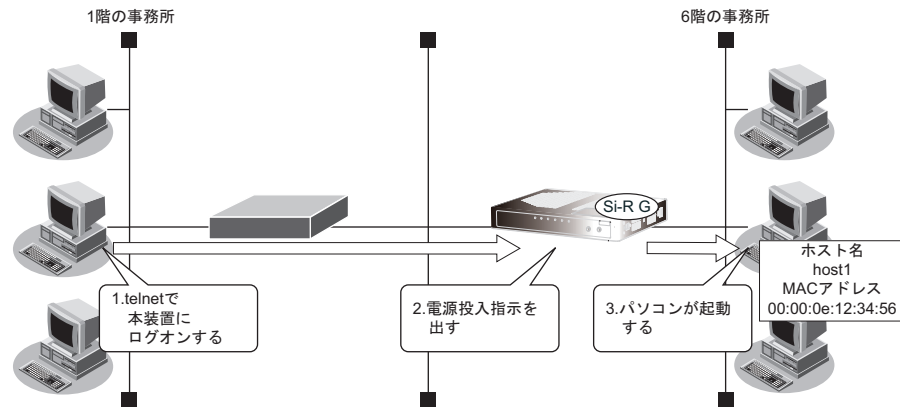
### こんな事に気をつけて

- 経路保持時間を設定しない場合、保持時間は DNS 回答パケットに含まれる TTL 時間になります。
- 拠点で使用する端末 (OS、インターネットブラウザなど) が設定した保持時間以上 IP アドレスを保持する場合は、通信ができなくなってしまうことがあります。

## 2.30 遠隔地のパソコンを起動させる (リモートパワーオン機能)

リモートパワーオン機能は、本装置につながっている離れた所にあるパソコンを、本装置から Wakeup on LAN 機能を使用して起動させることができます。

ここでは、1階の事務所のパソコンから6階の事務所のパソコンを起動する場合の設定方法を説明します。



### ● 設定条件

#### [本社側]

- ・ 起動するパソコンのホスト名 : host1
- ・ 起動するパソコンのMACアドレス : 00:00:0e:12:34:56

### 💡 ヒント

#### ◆ Wakeup on LAN機能とは？

AMD社が開発したネットワーク上の電源OFF状態のパソコンを遠隔操作で起動する機能です。起動は Magic Packet と呼ばれるパケットを送付して行います。なお、Wakeup on LAN 機能はパソコンを起動するだけで電源OFFは行いません。

電源OFFする場合は、別途、電源制御用ソフトウェアが必要になります。

#### こんな事に気をつけて

- ・ 本機能は、Wakeup on LAN に対応したパソコンだけで利用できます。Wakeup on LAN 対応機種については、パソコンのメーカーにお問い合わせください。
- ・ コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、[ ]、[ < ]、[ > ]、[ & ]、[ % ] は入力しないでください。

☞ 参照 マニュアル「コマンドユーザズガイド」



ホストデータベース情報は「リモートパワーオン機能」、「DHCP スタティック機能」、「DNS サーバ機能」で使われており、それぞれ必要な項目だけを設定します。

## 2.30.1 リモートパワーオン情報を設定する

### ● 設定コマンド

```
ホストデータベースへ登録する  
# host 0 name host1  
# host 0 mac 00:00:0e:12:34:56
```

```
設定終了  
# save  
# commit
```

## 2.30.2 リモートパワーオン機能を使う

1. パソコン上の telnet クライアントから本装置にログインします。
2. 本装置からコマンドによって、Wake up on LAN 機能を使用します。

### ● コマンド

```
# rpon all
```



パソコンが Magic Packet を受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種や OS によって異なります）。

## 2.31 スケジュール機能を使う

本装置のスケジュール機能には、以下のとおりです。

- **スケジュール予約**  
特定の動作とそれを行う時間をスケジュール予約情報として登録できます。スケジュール予約情報を登録しておくと、特定時間帯のデータの発着信を制限したり、定期的に課金情報をクリアしたりする作業を、本装置が自動的に行います。スケジュール予約情報は、最大20件まで登録できます。
- **電話番号変更予約**  
指定した日時に構成定義情報の電話番号を一括して変更することができます。電話番号変更予約情報は、最大4件まで登録できます。電話番号は、予約情報1件に対して4つまで登録することができます。
- **構成定義情報切り替え予約**  
本装置は、内部に2つ構成定義情報を持つことができます。運用構成の変更に備え、あらかじめ構成定義情報を用意し、指定した日時に新しい構成定義に切り替えることができます。

こんな事に気をつけて

設定前に本装置の内部時刻を正しくセットしてください。

☛ 参照 マニュアル「コマンドユーザズガイド」

### 2.31.1 スケジュールを予約する

#### 発信抑止を予約する

ここでは、毎日午後11時から午前8時までの発信を抑止する場合の設定方法を説明します。

##### ● 設定条件

- |        |         |
|--------|---------|
| • 動作   | : 発信抑止  |
| • 日/曜日 | : 毎日    |
| • 開始時刻 | : 23:00 |
| • 終了時刻 | : 08:00 |

上記の設定条件に従ってスケジュールを予約する場合のコマンド例を示します。

##### ● コマンド

```
スケジュールを予約する
# schedule 0 in any 2300-0800 diallock
```

```
設定終了
# save
# commit
```

こんな事に気をつけて

回線接続中に、発信抑止または着信抑止が実行されても、回線は切断されません。



## リモートパワーオンを予約する

---

ここでは、毎朝8時に特定のパソコンを起動する場合の設定方法を説明します。

### ● 設定条件

- ・ 動作 : リモートパワーオン
- ・ 予約時刻 : 08:00  
: 毎日

上記の設定条件に従ってリモートパワーオンを予約する場合のコマンド例を示します。

### ● コマンド

```
スケジュールを予約する  
# schedule 0 at any 0800 rpon all
```

```
設定終了  
# save  
# commit
```

### こんな事に気をつけて

リモートパワーオン機能を利用する場合は、あらかじめ対象とするパソコンの情報を本装置のホストデータベース情報に登録しておく必要があります。スケジュール機能を使ってリモートパワーオンを行うと、host rpon コマンドで off が指定されていないすべてのパソコンが起動します。

☛ 参照 [「2.30 遠隔地のパソコンを起動させる \(リモートパワーオン機能\)」 \(P.386\)](#)

---

## 2.31.2 電話番号変更を予約する

ここでは、2015年10月1日午前2時に電話番号を「\*99\*\*\*1#」から「\*99\*\*\*5#」に変更する場合の設定方法を説明します。

### ● 設定条件

- ・ 実行日時 : 2015年10月1日 2時00分
- ・ 電話番号変更前情報 : \*99\*\*\*1#
- ・ 電話番号変更後情報 : \*99\*\*\*5#

上記の設定条件に従って電話番号変更を予約する場合のコマンド例を示します。

### ● コマンド

```
電話番号変更を予約する
# dnconvinfo 0 date 1510010200
# dnconvinfo 0 dial 0 *99***1# *99***5#

設定終了
# save
# commit
```

### こんな事に気をつけて

指定時刻になると自動的に本装置が再起動され、電話番号が更新されます。その際、データ通信中の場合は、回線が切断されます。

## 2.31.3 構成定義情報の切り替えを予約する

本装置は、構成定義情報を内部に2つ持つことができます。

ここでは、2015年2月1日6時30分に構成定義情報を1から2に切り替える場合の設定方法を説明します。

### ● 設定条件

- ・ 実行日時 : 2015年2月1日 6時30分
- ・ 構成定義情報切り替え : 構成定義情報1→構成定義情報2

上記の設定条件に従って構成定義情報を切り替える場合のコマンド例を示します。

### ● コマンド

```
構成定義を切り替える
# addact 0 1502010630 reset config2

設定終了
# save
# commit
```

## 2.32 ブリッジグループ機能を使う

ブリッジグループ機能とは、各VLANインタフェースおよび相手接続情報にグループ識別子を設定し、ブリッジ転送が、そのグループ内に閉じた形で行われるようにする機能です。グループを分けることで、ブリッジ通信を各グループに分離することができます。

### こんな事に気をつけて

- ブリッジグループ学習テーブル生存時間は、mac age で設定した値がすべてのグループで使用されます。
- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数のVLAN インタフェースを同じグループに含めてIPブリッジをする場合は、同じグループ内でVLAN IDがもっとも小さいVLAN インタフェースに関連付けられたlanインタフェースでだけ以下の機能を利用できます。
  - FTP (ソフトウェア更新など)
  - telnet
  - syslog の送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング
- IP フレームをブリッジする場合に、転送ポリシーを loose に設定したときだけ、ブリッジグループ外とブリッジ転送が行われます。また、ブリッジドメイン内は唯一のIPセグメントであることに注意してダイナミックルーティングを使用してください。
- IP をブリッジする場合、WAN 側にはブリッジで中継されるフレームだけが転送され、直接 WAN 側に Ethernet フレームではないIPパケットを送受信することはできません。IP をブリッジする運用形態では、IP に関するすべての設定はLANインタフェース側で定義します。リモートインタフェースではIPに関する設定は定義しないでください。
- WAN 経由でIPをブリッジし、ブリッジ転送を許す場合 (転送ポリシーが Loose)、たとえ WAN の先に存在するネットワークに対する経路であっても、すべての静的経路の設定はLANインタフェース側で定義してください。ブリッジによって相手装置のLANと本装置のLANがWAN経由で接続されているため、LAN側に経路設定を定義すれば問題なくWANの先に存在するあて先ネットワークにブリッジで転送されます。
- コマンド入力時は、半角文字 (0~9、A~Z、a~z、および記号) だけを使用してください。ただし、空白文字、[ ]、[ < ]、[ > ]、[ & ]、[ % ] は入力しないでください。

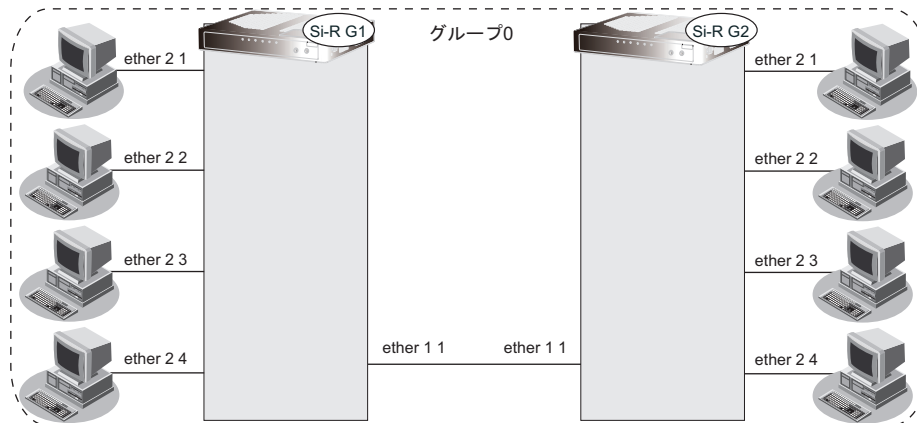
■ 参照 マニュアル「コマンドユーザズガイド」

## 2.32.1 異なる VLAN をグループ化する

ここでは、ブリッジグループ機能を使用して、異なる VLAN を 1 つのブリッジセグメントとして運用する場合の設定方法を説明します。

### こんな事に気をつけて

- 異なる VLAN 同士をグループ化する場合、ブリッジ転送されると送出フレームには送出先の VLAN 識別子が付与されます。
- 異なる VLAN 同士をグループ化する場合、IP セグメントは同一になるように構成する必要があります。



### ● 前提条件

- ETHERグループ 1 ポート 1 と ETHERグループ 2 ポート 1～4 を同一ブリッジグループ 0 にする

#### [グループ 0]

- ETHER ポート  
ether 1 1 : VLAN 番号=1  
ether 2 1～4 : VLAN 番号=3

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

#### [本装置 1][本装置 2]

グループ 0 の ETHER ポート設定

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 3
```

VLAN の設定

```
# vlan 1 bridgegroup use on
# vlan 1 bridgegroup group 0
# vlan 3 bridgegroup use on
# vlan 3 bridgegroup group 0
```

グループ 0 の設定

```
# bridgegroup 0 ip routing off
# bridgegroup 0 ipv6 routing off
# bridgegroup 0 ip policy strict
# bridgegroup 0 ipv6 policy strict
```

設定終了

```
# save
# commit
```

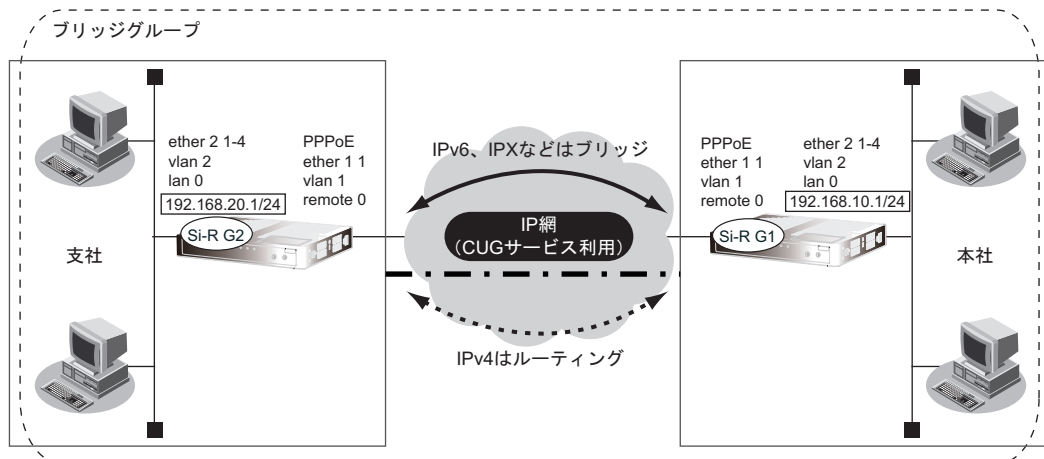
## 2.32.2 IP トンネルで事業所間をブリッジ接続する (Ethernet over IP ブリッジ)

IP トンネル上でブリッジグループ機能を使用することにより、IP 通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。

### こんな事に気をつけて

- IP フレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IP フレームをブリッジするインタフェース上では利用できません。また、複数の VLAN インタフェースを同じグループに含めて IP ブリッジをする場合は、同じグループ内で VLAN ID がもっとも小さい VLAN インタフェースに関連付けられた lan インタフェースでだけ以下の機能を利用できます。
  - FTP (ソフトウェア更新など)
  - telnet
  - syslog の送信
  - SNMP エージェント、Trap 送信
  - ダイナミックルーティング
- IP フレームをブリッジする場合に、転送ポリシーを loose に設定したときだけ、ブリッジグループ外とブリッジ転送が行われます。また、ブリッジドメイン内は唯一の IP セグメントであることに注意してダイナミックルーティングを使用してください。
- ブリッジグループ学習テーブル生存時間は、mac age に設定した値がすべてのグループで使用されます。
- IP をブリッジする場合、WAN 側にはブリッジで中継されるフレームだけが転送され、直接 WAN 側に Ethernet フレームではない IP パケットを送受信することはできません。IP をブリッジする運用形態では、IP に関するすべての設定は LAN インタフェース側で定義します。リモートインタフェースでは IP に関する設定は定義しないでください。
- WAN 経由で IP をブリッジし、ブリッジ転送を許す場合 (転送ポリシーが Loose)、たとえ WAN の先に存在するネットワークに対する経路であっても、すべての静的経路の設定は LAN インタフェース側で定義してください。ブリッジによって相手装置の LAN と本装置の LAN が WAN 経由で接続されているため、LAN 側に経路設定を定義すれば、問題なく WAN の先に存在するあて先ネットワークにブリッジで転送されます。
- Ethernet over IP ブリッジの接続先に対して接続先監視を行うことができません。接続先監視の設定は行わないでください。
- IPsec トンネル内で Ethernet over IP ブリッジ接続を行う際などで、パケットの複数回フラグメントを避けるため、送出先インタフェースの MTU をもとに、Ethernet over IP でカプセル化されたパケットのフラグメントサイズを調整しています。しかし、PPPoE によってインターネット接続されるなどで、PPPoE で利用する相手情報の MTU 値が送出先インタフェースの MTU 値より著しく下回った場合は、複数回フラグメントされる場合があります。

ここでは、本社と特定の支社との間で、IP 網を経由し、IPv4 以外のフレームに対してブリッジ通信を行う場合の設定方法を説明します。



● 前提条件

- IP 網は、PPPoE 接続で LAN 型払い出しによりアドレス割り当てを行う CUG (Closed Users Group) サービスを利用する

**[本社 (PPPoE 常時接続)]**

**PPPoE 接続条件**

- PPPoE ETHER ポート : ETHER グループ 1 ポート 1
- PPPoE ETHER ポート VLAN 番号 : 1
- PPPoE ユーザ認証 ID : userid1@groupname
- PPPoE ユーザ認証パスワード : userpass1
- NAT 機能を使用しない
- 常時接続機能を使用する

**社内 LAN 接続条件**

- ETHER ポート : ETHER グループ 2 ポート 1～4
- VLAN 番号 : 2
- lan 定義番号 : 0
- 払い出される IPv4 アドレス (lan 0 インタフェースに設定) : 192.168.10.1/24

**[支社 (PPPoE 常時接続)]**

**PPPoE 接続条件**

- PPPoE ETHER ポート : ETHER グループ 1 ポート 1
- PPPoE ETHER ポート VLAN 番号 : 1
- PPPoE ユーザ認証 ID : userid2@groupname
- PPPoE ユーザ認証パスワード : userpass2
- NAT 機能を使用しない
- 常時接続機能を使用する

**社内LAN接続条件**

- ETHER ポート : ETHERグループ2ポート1~4
- VLAN 番号 : 2
- lan 定義番号 : 0
- 払い出されるIPv4 アドレス (lan 0 インタフェースに設定)  
: 192.168.20.1/24

**● 設定条件****[本社]**

- 自側エンドポイントアドレス : 192.168.10.1
- 相手側エンドポイントアドレス : 192.168.20.1

**[支社]**

- 自側エンドポイントアドレス : 192.168.20.1
- 相手側エンドポイントアドレス : 192.168.10.1

**[本社、支社共通]**

- ブリッジ対象インタフェース : VLAN 番号1のVLANとIP トンネル
- IPv4の転送方式 : ルーティングで転送
- IPv6の転送方式 : ブリッジで転送

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド****[本装置1 (本社側)]**

```
# delete ether 1
# delete ether 2

# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1

# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1@groupname userpass1
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414

lan 0 の IP アドレスを設定する
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 2
```

```
IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.10.1
# remote 1 ap 0 tunnel remote 192.168.20.1

ブリッジを行うインタフェースを設定する
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# vlan 2 bridgegroup use on
# vlan 2 bridgegroup group 0

ブリッジグループを設定する
# bridgegroup 0 ip routing on
# bridgegroup 0 ipv6 routing off

設定終了
# save
# commit
```

**[本装置 2 (支社側)]**

```
# delete ether 1
# delete ether 2

# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1

# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2@groupname userpass2
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414

lan 0 の IP アドレスを設定する
# ether 2 1-4 use on
# ether 2 1-4 vlan untag 2

# lan 0 ip address 192.168.20.1/24 3
# lan 0 vlan 2

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.20.1
# remote 1 ap 0 tunnel remote 192.168.10.1

ブリッジを行うインタフェースを設定する
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# vlan 2 bridgegroup use on
# vlan 2 bridgegroup group 0
```



```
ブリッジグループを設定する  
# bridgegroup 0 ip routing on  
# bridgegroup 0 ipv6 routing off
```

```
設定終了  
# save  
# commit
```

## 2.33 透過モードを使う

透過モードとは、タグ付きVLANフレームおよびタグなしフレームをVLAN設定なしに転送可能とするモードです。本装置ではVLAN設定を行い、設定に従った転送と、VLAN設定なしに全フレームを透過するモードをサポートします。

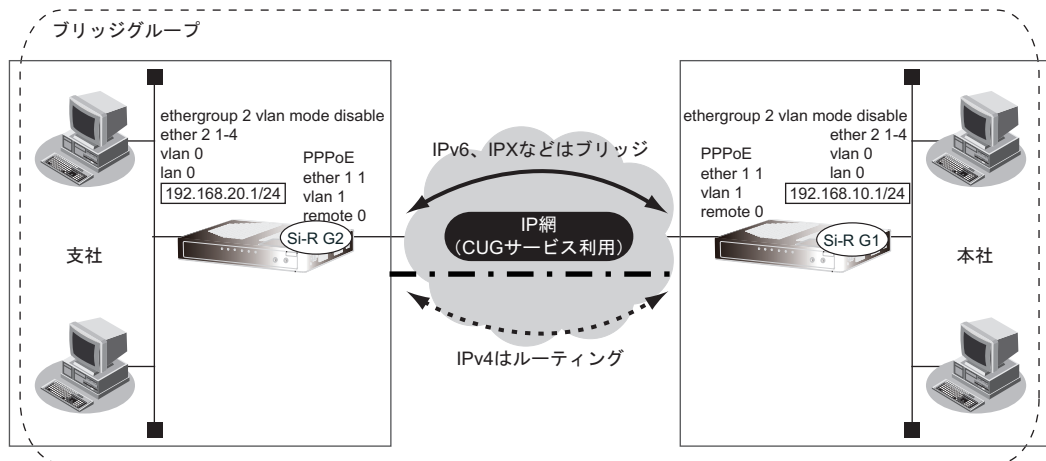
### 2.33.1 ブリッジグループ機能と併用する

ETHERグループ2を透過モードで使用し、IPトンネル上でブリッジグループ機能を使用することにより、IP通信だけが可能な網でも、拠点間でブリッジ通信を行うことができます。また、透過モードを使用することで、ETHERグループ2配下に存在するすべてのVLANを相手拠点に転送することができます。

#### こんな事に気をつけて

- 透過モード設定時に、ブリッジグループを有効にすると、ETHERグループ2は各ポート単位でのブリッジグループ分けができません。全ポートが1つのブリッジグループにだけ属することができます。
- 透過モードとブリッジグループを併用する場合、VLANタグ透過モードを設定してください。
- 透過モード設定時は、タグなしフレームをlanインタフェースと括り付ける場合、VIDとして"0"を指定してください。
- 透過モード設定時は、ETHERグループ1に設定されていないVIDを、lanインタフェースで指定することができます。その場合、該当lanインタフェースはETHERグループ2の全ポートがリンクダウンまたは未使用状態になるまでup状態となります。
- IPフレームをブリッジする場合、そのブリッジグループに属するインタフェース上では、以下の機能を利用することができます。それ以外の機能は、IPフレームをブリッジするインタフェース上では利用できません。また、複数のVLANインタフェースを同じグループに含めてIPブリッジをする場合は、同じグループ内でVLAN IDがもっとも小さいVLANインタフェースに関連付けられたlanインタフェースでだけ以下の機能を利用できます。
  - FTP (ソフトウェア更新など)
  - telnet
  - syslogの送信
  - SNMPエージェント、Trap送信
  - ダイナミックルーティングIPフレームをブリッジする場合に、転送ポリシーをlooseに設定したときだけ、ブリッジグループ外とブリッジ転送が行われます。また、ブリッジドメイン内は唯一のIPセグメントであることに注意してダイナミックルーティングを使用してください。
- ブリッジグループ学習テーブル生存時間は、mac ageに設定した値が、すべてのグループで使用されます。
- IPをブリッジする場合、WAN側にはブリッジで中継されるフレームだけが転送され、直接WAN側にEthernetフレームではないIPパケットを送受信することはできません。IPをブリッジする運用形態では、IPに関するすべての設定はLANインタフェース側で定義します。リモートインタフェースではIPに関する設定は定義しないでください。
- WAN経由でIPをブリッジし、ブリッジ転送を許す場合(転送ポリシーがLoose)、たとえWANの先に存在するネットワークに対する経路であっても、すべての静的経路の設定はLANインタフェース側で定義してください。ブリッジによって相手装置のLANと本装置のLANがWAN経由で接続されているため、LAN側に経路設定を定義すれば、問題なくWANの先に存在するあて先ネットワークにブリッジで転送されます。
- Ethernet over IPブリッジの接続先に対して接続先監視を行うことができません。接続先監視の設定は行わないでください。
- Ethernet over IPと透過モードを併用する場合、タグ透過モード(bridgegroup vlan tag transmit on)を必ず設定してください。

ここでは、本社と特定の支社との間で、IP網を経由し、IPv4以外のフレームに対してブリッジ通信を行う場合の設定方法を説明します。



● 前提条件

- IP網は、PPPoE接続でLAN型払い出しによりアドレス割り当てを行う、CUG (Closed Users Group) サービスを利用する

[本社 (PPPoE常時接続)]

PPPoE接続条件

- PPPoE ETHERポート : ETHERグループ1ポート1
- PPPoE ETHERポートVLAN番号 : 1
- PPPoE ユーザ認証ID : userid1@groupname
- PPPoE ユーザ認証パスワード : userpass1
- NAT機能を使用しない
- 常時接続機能を使用する

社内LAN接続条件

- ETHERグループ2 : 透過モード
- ETHERポート : ETHERグループ2ポート1~4
- VLAN番号 : 0 (タグなしフレーム)
- lan定義番号 : 0
- 払い出されるIPv4アドレス (lan 0 インタフェースに設定) : 192.168.10.1/24

[支社 (PPPoE常時接続)]

PPPoE接続条件

- PPPoE ETHERポート : ETHERグループ1ポート1
- PPPoE ETHERポートVLAN番号 : 1
- PPPoE ユーザ認証ID : userid2@groupname
- PPPoE ユーザ認証パスワード : userpass2
- NAT機能を使用しない
- 常時接続機能を使用する

**社内LAN接続条件**

- ETHERグループ2 : 透過モード
- ETHERポート : ETHERグループ2ポート1~4
- VLAN番号 : 0 (タグなしフレーム)
- lan定義番号 : 0
- 払い出されるIPv4アドレス (lan 0 インタフェースに設定) : 192.168.20.1/24

**● 設定条件****[本社]**

- 自側エンドポイントアドレス : 192.168.10.1
- 相手側エンドポイントアドレス : 192.168.20.1

**[支社]**

- 自側エンドポイントアドレス : 192.168.20.1
- 相手側エンドポイントアドレス : 192.168.10.1

**[本社、支社共通]**

- ブリッジ対象インタフェース : VLAN番号1のVLANとIPトンネル
- IPv4の転送方式 : ルーティングで転送
- IPv6の転送方式 : ブリッジで転送

上記の設定条件に従って設定を行う場合のコマンド例を示します。

**● コマンド****[本装置1 (本社側)]**

```
# ether 1 1 use off
# ether 2 1-4 use off
# delete lan

CUG サービスに接続する PPPoE の接続情報を設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid1@groupname userpass1
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414

lan 0 の IP アドレスを設定する
# ethergroup 2 vlan mode disable
# ether 2 1-4 use on
# lan 0 ip address 192.168.10.1/24 3
# lan 0 vlan 0

IPv4 トンネルを設定する
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.10.1
```

```
# remote 1 ap 0 tunnel remote 192.168.20.1
```

ブリッジを行うインタフェースを設定する

```
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# ethergroup 2 bridgegroup use on
# ethergroup 2 bridgegroup group 0
```

ブリッジグループを設定する

```
# bridgegroup 0 ip routing on
# bridgegroup 0 ipv6 routing off
# bridgegroup 0 vlan tag transmit on
```

設定終了

```
# save
# reset
```

### [本装置2 (支社側)]

```
# ether 1 1 use off
# ether 2 1-4 use off
# delete lan
```

CUG サービスに接続する PPPoE の接続情報を設定する

```
# ether 1 1 use on
# ether 1 1 vlan untag 1
# remote 0 name CUG
# remote 0 mtu 1454
# remote 0 ap 0 name user1
# remote 0 ap 0 datalink bind vlan 1
# remote 0 ap 0 ppp auth send userid2@groupname userpass2
# remote 0 ap 0 keep connect
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip route 0 default 1 1
# remote 0 ip msschange 1414
```

lan 0 の IP アドレスを設定する

```
# ethergroup 2 vlan mode disable
# ether 2 1-4 use on
# lan 0 ip address 192.168.20.1/24 3
# lan 0 vlan 0
```

IPv4 トンネルを設定する

```
# remote 1 name EtherIP
# remote 1 ap 0 name EtherIP
# remote 1 ap 0 datalink type ip
# remote 1 ap 0 tunnel local 192.168.20.1
# remote 1 ap 0 tunnel remote 192.168.10.1
```

ブリッジを行うインタフェースを設定する

```
# remote 1 bridgegroup use on
# remote 1 bridgegroup group 0
# ethergroup 2 bridgegroup use on
# ethergroup 2 bridgegroup group 0
```

ブリッジグループを設定する

```
# bridgegroup 0 ip routing on
# bridgegroup 0 ipv6 routing off
# bridgegroup 0 vlan tag transmit on
```

設定終了

```
# save
# reset
```

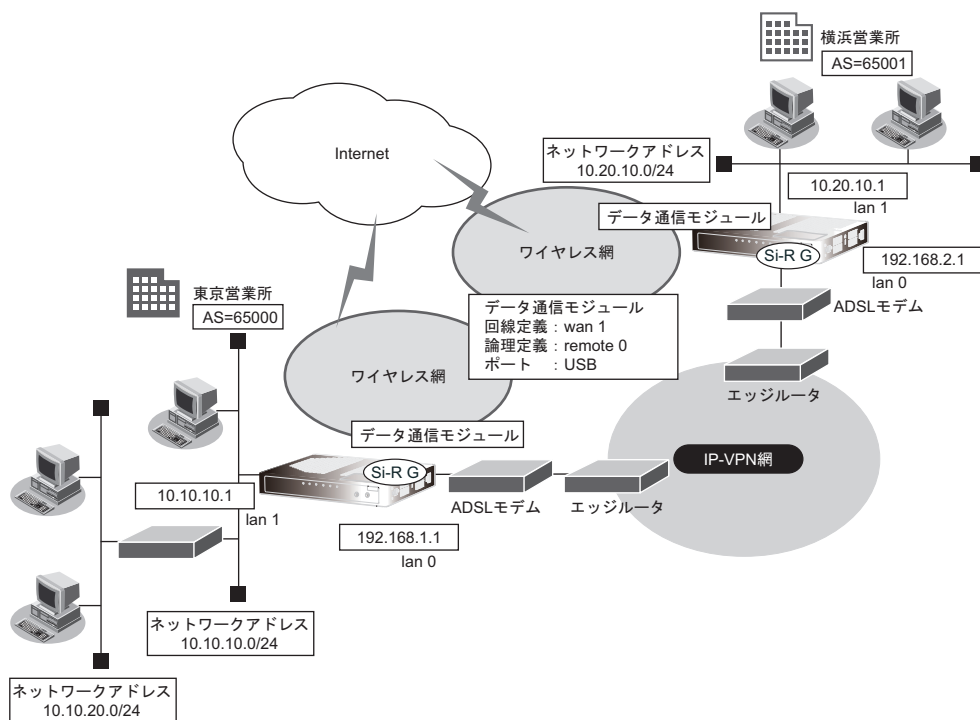
## 2.34 データ通信モジュールで通信バックアップをする

本装置にデータ通信モジュールを装着することで、ワイヤレス網を使用して通信することができます。

ここでは、営業所間を IP-VPN 網で接続し、IP-VPN 網側の通信が通信不能になった場合にワイヤレス網側で通信バックアップする場合を例に説明します。

☛ 参照 対応データ通信モジュール (富士通ホームページ)  
<http://fenics.fujitsu.com/products/sir/sirg110/#supportcard>

この例では、BGP 経路によって優先度の低いスタティックルートをバックアップ回線側に設定します。メインの IP-VPN 側が通信不能になり BGP セッションが切断され、相手拠点の BGP 経路が消えた際に、バックアップ回線側に定義したスタティックルートが有効になり、通信がバックアップ回線側に切り替わる方法を用います。



### こんな事に気をつけて

- データ通信モジュールの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからデータ通信モジュールを装着してください。
- データ通信モジュールは、回線の切断に時間がかかるため、課金単位時間を超えて切断される場合があります。
- データ通信モジュール接続では、常時接続機能は動作しません。
- データ通信モジュールで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- データ通信モジュールによる発信は従量課金が発生するため、データ通信モジュール接続のアカウント情報を監視して不要な接続が行われていないか、こまめに確認してください。また、異常課金を防止する場合は、強制切断を行う累計接続時間、累計パケット数を設定してください。
- 課金制御機能（強制切断）による回線切断が発生した場合、以下のシステムログが出力されます。  
 protocol: [USB] forced disconnection <target> <reason>
- データ通信モジュールの通信速度は64Kbpsとみなして動作します。

ここでは、以下を参照して、IP-VPN 網接続が設定されていることを前提とします。

☛ 参照 「1.7 複数の事業所 LAN を IP-VPN 網を利用して接続する」 (P.27)

## ● 設定条件

### [東京営業所]

- ・ インターネットプロバイダから割り当てられた固定 IP アドレス  
: 202.168.1.66
- ・ 認証 ID  
: userid (通信事業者から提示された内容)
- ・ 認証パスワード  
: userpass (通信事業者から提示された内容)
- ・ 電話番号  
: \*99\*\*\*1# (通信事業者から提示された内容)
- ・ 無通信監視タイマ  
: 無通信監視時間を 1 分とする
- ・ 強制切断  
: 100000 パケット (128 バイト単位) を超えた場合に回線を切断し、以降自動発信を行わない
- ・ バックアップ用のスタティックルート  
: 10.20.0.0/16 (優先度 30)

### [横浜営業所]

- ・ インターネットプロバイダから割り当てられた固定 IP アドレス  
: 202.168.2.66
- ・ 認証 ID  
: userid (通信事業者から提示された内容)
- ・ 認証パスワード  
: userpass (通信事業者から提示された内容)
- ・ 電話番号  
: \*99\*\*\*1# (通信事業者から提示された内容)
- ・ 無通信監視タイマ  
: 無通信監視時間を 1 分とする
- ・ 強制切断  
: 100000 パケット (128 バイト単位) を超えた場合に回線を切断し、以降自動発信を行わない
- ・ バックアップ用のスタティックルート  
: 10.10.0.0/16 (優先度 30)

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 東京営業所のバックアップ回線を設定する

### ● コマンド

```

回線情報を設定する
# wan 1 use on
# wan 1 bind usb
# wan 1 line modemmodule
# wan 1 description L-03F

接続先の情報を設定する
# remote 0 description internet
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip route 0 default 1 1
# remote 0 ap 0 description ISP-1
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 dial 0 number *99***1#
# remote 0 ap 0 idle 1m

強制切断を行う累計パケット数を設定する
# remote 0 ap 0 disconnect packet 100000 per128

VPNを設定する
# remote 1 name tokyo
# remote 1 ip route 0 10.20.10.0/24 1 30

```

```
# remote 1 ap 0 name yokohama
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.1.66
# remote 1 ap 0 tunnel remote 202.168.2.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
```

インターネットからIPsec/IKE パケットを受信する設定をする

```
# remote 0 ip nat static 0 10.10.10.1 500 any 500 17
# remote 0 ip nat static 1 10.10.10.1 any any any 50
```

設定終了

```
# save
# commit
```

## 横浜営業所のバックアップ回線を設定する

### ● コマンド

回線情報を設定する

```
# wan 1 use on
# wan 1 bind usb
# wan 1 line modemmodule
# wan 1 description L-03A
```

接続先の情報を設定する

```
# remote 0 description internet
# remote 0 ppp ipcp vjcomp disable
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip route 0 default 1 1
# remote 0 ap 0 description ISP-1
# remote 0 ap 0 datalink bind wan 1
# remote 0 ap 0 ppp auth send userid userpass
# remote 0 ap 0 dial 0 number *99***1#
# remote 0 ap 0 idle 1m
```

強制切断を行う累計パケット数を設定する

```
# remote 0 ap 0 disconnect packet 100000 per128
```

VPNを設定する

```
# remote 1 name yokohama
# remote 1 ip route 0 10.10.10.0/24 1 30
# remote 1 ap 0 name tokyo
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 tunnel local 202.168.2.66
# remote 1 ap 0 tunnel remote 202.168.1.66
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text abcdefghijklmnopqrstuvwxyz1234567890
# remote 1 ap 0 ike proposal encrypt des-cbc
```

インターネットからIPsec/IKE パケットを受信する設定をする

```
# remote 0 ip nat static 0 10.20.10.1 500 any 500 17
```



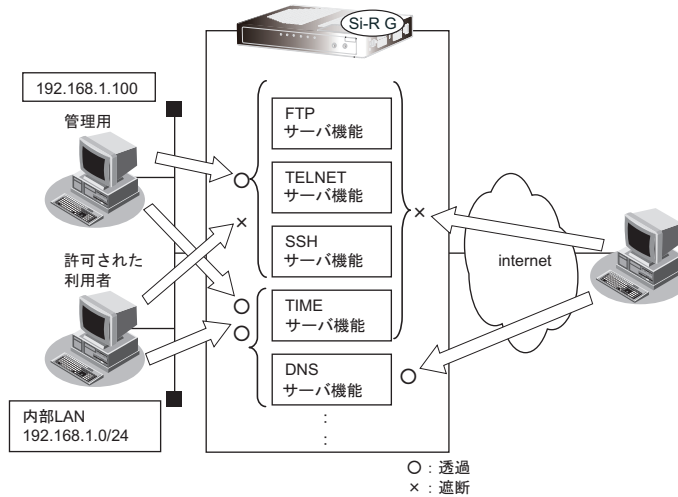
```
# remote 0 ip nat static 1 10.20.10.1 any any any 50
```

```
設定終了  
# save  
# commit
```

## 2.35 アプリケーションフィルタ機能を使う

本装置上で動作する各サーバ機能に対してアクセス制限を行うことができます。

これにより、装置をメンテナンスまたは装置のサーバ機能を使用する端末を限定し、セキュリティを向上させることができます。



ここでは、アプリケーションフィルタを利用して各サーバ機能へのアクセスを制限する場合の設定方法を説明します。

### ● 設定条件

- 管理用のホスト（192.168.1.100）からのみ TELNET/FTP/SSH サーバ機能へのアクセスを許可する
- 内部 LAN のホスト（192.168.1.0/24）からのみ TIME サーバ機能へのアクセスを許可する
- その他のサーバ機能は制限しない

### こんな事に気をつけて

IP フィルタリングにより自装置へのパケットを遮断している場合、アプリケーションフィルタで許可する設定を行ってもアクセスはできません。

上記の設定条件に従ってアプリケーションフィルタを設定する場合のコマンド例を示します。

**● コマンド**

制限するサーバ機能に対し、デフォルトのアクセスを遮断する

```
# serverinfo ftp filter default reject  
# serverinfo telnet filter default reject  
# serverinfo ssh filter default reject  
# serverinfo time filter default reject
```

管理用のホストからのFTP/TELNET/SSHサーバ機能へのアクセスを許可する

```
# acl 0 ip 192.168.1.100/32 any any any  
# serverinfo ftp filter 0 accept acl 0  
# serverinfo telnet filter 0 accept acl 0  
# serverinfo ssh filter 0 accept acl 0
```

内部LANのホストからのTIMEサーバ機能へのアクセスを許可する

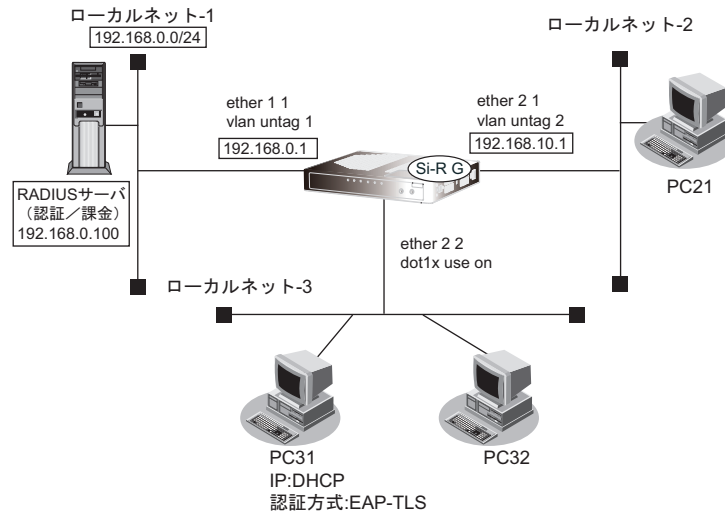
```
# acl 1 ip 192.168.1.0/24 any any any  
# serverinfo time filter 0 accept acl 1
```

設定終了

```
# save  
# commit
```

## 2.36 IEEE802.1X 認証機能を使う

ここでは、ether ポートで IEEE802.1X 認証を行う場合の設定方法を説明します。



### こんな事に気をつけて

- 認証端末に割り当てる VLAN ID は、本装置のほかの ether ポートまたは認証 VLAN 用予約 VLAN に設定されている必要があります。
- 本認証使用時は、ether ポートの種別を通常ポート (ether type normal) 設定にしてください。
- IEEE802.1X 認証を使用する ETHER ポートで STP を有効にした場合、ブロッキングからフォワーディングに復帰しても、再認証間隔の設定時間の間は通信が回復しないことがあります。
- MAC アドレス認証と併用時に認証状態初期化操作を行う場合は、dot1xctl initialize port ether を実施してください。

### ● 設定条件

#### 有線 LAN を使ってローカルサーバに接続する

- 利用する ether ポート : ether 1 1
- 利用する lan インタフェース : lan0
- IP アドレス : 192.168.0.1/24

#### 有線 LAN で IEEE802.1X 認証を行って端末を収容する

- 利用する ether ポート : ether 2 2
- 利用する lan インタフェース : lan1
- IP アドレス : 192.168.10.1/24
- IEEE802.1X 認証 : 有効
- IEEE802.1X 認証 (認証サーバ) : aaa1
- その他 : 接続端末のアドレスは DHCP 機能を利用する

#### 認証/課金サーバを AAA 定義で指定する

- aaa 定義番号 : aaa1
- 認証サーバ IP アドレス : 192.168.0.100
- 認証サーバシークレットキー : passwd

- 課金サーバIP アドレス : 192.168.0.100
- 課金サーバシークレットキー : passwd

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置を設定する

### ● コマンド

```
ether ポートと lan インタフェースを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# lan 0 ip address 192.168.0.1/24 3
# lan 0 vlan 1

有線LAN で IEEE802.1X 認証を行って端末を収容する
IEEE802.1X 機能を有効にする
# dot1x use on

ether ポートと lan インタフェースを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 2
# lan 1 ip address 192.168.10.1/24 3
# lan 1 vlan 2

lan インタフェースに DHCP サーバを設定する
# lan 1 ip dhcp service server
# lan 1 ip dhcp info address 192.168.10.10/24 10
# lan 1 ip dhcp info gateway 192.168.10.1

ether ポートで IEEE802.1X 認証を有効にする
# ether 2 2 dot1x use on

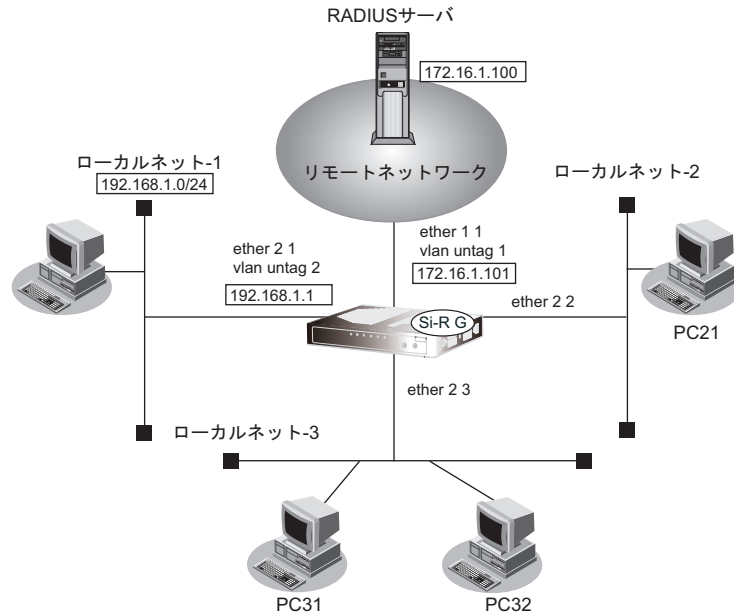
認証に利用する RADIUS サーバを AAA 定義番号で指定する
# ether 2 2 dot1x aaa 1

認証/課金サーバを AAA 定義で指定する
# aaa 1 name aaasvr
# aaa 1 radius service client both
# aaa 1 radius client server-info auth 0 secret passwd
# aaa 1 radius client server-info auth 0 address 192.168.0.100
# aaa 1 radius client server-info auth 0 source 192.168.0.1
# aaa 1 radius client server-info accounting 0 secret passwd
# aaa 1 radius client server-info accounting 0 address 192.168.0.100
# aaa 1 radius client server-info accounting 0 source 192.168.0.1

設定終了
# save
# commit
```

## 2.37 不正端末アクセス防止機能 (MAC アドレス認証) を使う

不正端末アクセス防止機能 (MAC アドレス認証) を使用すると、本装置のローカル LAN に接続する端末がリモートネットワークへのアクセス権を持っているかを認証することができます。



### こんな事に気をつけて

- MAC アドレス認証で利用する AAA のグループ ID を正しく設定してください。
- 認証端末に割り当てる VLAN ID は、本装置のほかの ether ポートまたは認証 VLAN 用予約 VLAN に設定されている必要があります。
- 本認証使用時は、ether ポートの種別を通常ポート (ether type normal) 設定にしてください。
- IEEE802.1X 認証と併用時に認証状態初期化操作を行う場合は、dot1xctl initialize port ether を実施してください。

ここでは、リモートネットワークへの接続がすでに設定されている場合を例に MAC アドレス認証機能を利用する設定方法を説明します。

### ● 設定条件

- ether 1 1 で WAN 接続
- ether 2 1 は固定 VALN ローカルネット
- ether 2 2、ether 2 3 で MAC アドレス認証機能を使う
- ether 2 2、ether 2 3 で使用する認証データベース
 

ether 2 2	: RADIUS サーバ
ether 2 3	: ローカルで設定した認証情報
- AAA グループ ID
 

ether 2 2	: 0
ether 2 3	: 1

- ローカルネット-3 で利用可能なユーザは以下のとおり

ユーザ	MACアドレス
PC31	00:11:11:00:00:01
PC32	00:22:22:00:00:02

- リモートネットワークへの接続定義は設定済み
- RADIUS サーバはリモートネットワークに接続
- RADIUS サーバのIPアドレス : 172.16.1.100
- RADIUS サーバのシークレット : radius-secret
- 認証成功時に割り当てるVID : 2

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 本装置を設定する

### ● コマンド

```

MACアドレス認証を有効にする
# macauth use on

MACアドレス認証で使用するパスワードを設定する
# macauth password macauth-pass

固定VLAN ローカルネットを設定する
# ether 2 1 use on
# ether 2 1 vlan untag 2
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

有線ポートでMACアドレス認証を使用する
# ether 2 2 use on
# ether 2 2 macauth use on
# ether 2 2 macauth aaa 0
# ether 2 3 use on
# ether 2 3 macauth use on
# ether 2 3 macauth aaa 1

RADIUSサーバを利用するAAAグループ情報を設定する
# aaa 0 name radiusAuth
# aaa 0 radius service client auth
# aaa 0 radius auth source 172.16.1.101
# aaa 0 radius client server-info auth secret radius-secret
# aaa 0 radius client server-info auth address 172.16.1.100

ローカル認証情報を利用するAAAグループ情報を設定する
# aaa 1 name localAuth
# aaa 1 user 0 id 001111000001
# aaa 1 user 0 password macauth-pass
# aaa 1 user 0 supplicant vid 2
# aaa 1 user 1 id 002222000002
# aaa 1 user 1 password macauth-pass
# aaa 1 user 1 supplicant vid 2

設定終了
# save
# commit

```

## 2.38 ARP 認証機能を使う

ここでは、既存のネットワークに本装置を追加して、ARP 認証を行う場合の設定方法を説明します。  
Si-R G110 の場合を例にします。

### ● 設定条件

- 認証用パスワード : abcd
- VLAN10 で ARP 認証を使用する
- ARP 認証で利用する認証データベース : RADIUS サーバ
- AAA グループの ID : 0
- RADIUS サーバの IP アドレス : 172.16.1.100
- RADIUS サーバは VLAN20 に接続されている
- RADIUS サーバのシークレット : radius-secret
- 認証失敗時の通信妨害を行う
- 通信妨害のための ARP パケット送信間隔 : 10 秒

上記の設定条件に従って設定を行う場合のコマンド例を示します。

### ● コマンド

```
ARP 認証基本情報の設定
# arpauth use on
# arpauth password abcd

RADIUS サーバの VLAN を設定する
# ether 1 1 vlan untag 20
# lan 0 vlan 20
# lan 0 ip address 172.16.1.200/16 3

ARP 認証が動作する VLAN を設定する
# ether 2 1 vlan untag 10
# lan 1 vlan 10
# lan 1 ip address 172.17.1.100/16 3

ARP 認証を設定する
# vlan 10 arpauth use on
# vlan 10 arpauth aaa 0
# vlan 10 arpauth obstruction enable 10s

RADIUS サーバを利用する AAA グループ情報を設定する
# aaa 0 name RADIUS
# aaa 0 radius service client auth
# aaa 0 radius auth source 172.16.1.200
# aaa 0 radius client server-info auth 0 secret radius-secret
# aaa 0 radius client server-info auth 0 address 172.16.1.100

設定終了
# save
# commit
```



## 2.39 PKI機能を使う

PKI機能とは、デジタル証明書の作成、登録、削除を行います。

証明書とは、ITU-T 勧告の X.509 に定義されており、本人情報、公開鍵、有効期限、シリアル番号、シグネチャなどが含まれています。

本装置はアプリケーションが、デジタル証明書を利用するために使用されます。

本装置のPKI機能では、以下の設定が利用できます。

- RSA 鍵ペアの作成（証明書要求の作成）
- 自装置証明書の設定（認証局での証明書の発行）
- 自装置証明書の自己発行
- 相手装置証明書の設定
- 認証局証明書の設定

こんな事に気をつけて

- 本装置のPKI機能では、証明書について認証局（CA）に問い合わせることはできません。
- 認証局証明書は証明書の検証に利用されるため、設定した認証局証明書から発行されていない証明書の場合、検証に失敗することがあります。  
詳しくは、各アプリケーションの説明を参照してください。
- 自装置証明書の有効期限失効日付には、過去の日付や現在の日付を指定することはできません。

### 2.39.1 装置に証明書を登録する（自装置証明書を認証局（CA）で発行する）

RSA 鍵ペア（証明書要求）を作成し、認証局（CA）で自装置証明書を Base64 形式で受け取り（注）、登録する方法を説明します。また、相手装置証明書について登録する方法も説明します。

注）本装置では、認証局（CA）に問い合わせで証明書を取得することはできません。端末（パソコンなど）を使用して認証局（CA）に問い合わせで取得してください。

ここでは以下の条件によって、本装置のRSA鍵ペア（証明書要求）の作成、および自装置証明書と相手装置証明書を登録します。

#### ● 設定条件

- |                         |                      |
|-------------------------|----------------------|
| • 鍵ペア識別番号               | : 0                  |
| • 鍵長                    | : 1024bit            |
| • 証明書要求で使用するハッシュアルゴリズム  | : md5                |
| • 自装置証明書識別番号            | : 0                  |
| • 自装置証明書識別名             | : my-cert0.pem       |
| • 自装置証明書で使用するハッシュアルゴリズム | : md5                |
| • 国名 (C)                | : JP                 |
| • 都道府県 (ST)             | : Kanagawa           |
| • 市区町村 (L)              | : Kawasaki           |
| • 組織または会社名 (O)          | : Fujitsu Limited    |
| • 組織ユニットまたは部門 (OU)      | : Tech Div.          |
| • ホスト名 (CN)             | : shisya.fujitsu.com |

- メールアドレス : shisya@fujitsu.com
- サブジェクト代替名称 (IP アドレス) : 192.168.1.1
- サブジェクト代替名称 (DNS 名) : shisya-A.fujitsu.com
- 相手装置証明書識別名 : rmt-cert0.pem

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 自装置証明書要求の作成 (鍵ペアの作成)

### ● コマンド

```
自装置証明書要求 (鍵ペア) の作成を行う
# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :y
Local certificate number[0-4] :
key bit(361-2048) :1024
certificate request hash(sha1 or md5) :md5
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.
Common Name :shisya.fujitsu.com
Email Address :shisya@fujitsu.com
subjectAltName IP :192.168.1.1
subjectAltName DNS :shisya-A.fujitsu.com
```

以下のようなコマンドが表示され、自装置証明書要求 (鍵ペア) の設定が行われます。

Please wait to create RSA private key and Certificate request.

```
certificate private 0 line 0 riUB@No/FTnpCpEt5EFOcCIRdgTiDnB5n4DLemM5Lr1D8@zQQAL90cFFlCgzCY7P@W3ddbEokoMnHTc@6SP7VOy/isD2
certificate private 0 line 1 qC0dBFKQC1TpoWDZtpiUkK5cU1YilubYxhA5V2dudYWb0xAcjfiFvsNRzF/xcoi5FnKiOdZjzWxv75NjYMY@nzuVnL6
certificate private 0 line 2 w27xcCjoF1paovVWw1aA4rXXY2L4DGW30rs04sDWCnERcL855Mqw0@Xz0raGv@g8MfKGX3bnEaDIrmiyAIFflbxRVFsQU
certificate private 0 line 3 xM5/V6omhXp2WaRn6Xi/04wipg357HvboVnJKAiQpY6AbeAftphz47KFPKnMDaMuxlPY2w@15Obr1KUM1VknouU/tyP
certificate private 0 line 4 cfsRgjZ8kEbsUEsNzfntKATIbtDSBqIZ5Bo46RwRiBkpkJ9dlVv30dJ7cdfnJi9hX@fajbP3@F3NZP4yKAE3CWtqf
certificate private 0 line 5 jk31xZd75OHuAGNPWsWEVVMa6Kt@YpKpV9zwWGDImOKBs8XgTA8Y5hg8Ut@THKIRI0TgdM4avfQaYwwXWwCFxvUHz
certificate private 0 line 6 KsrHISB2rYuTnCYcm2sYndVXaVrMv6VqkNfYrNOfwueu0OqczYUZEDNOYsKp2tLDqBoO47nNWmJWObE2BOex1ujZktW/
certificate private 0 line 7 59UMtzcra44eZToKjXqU2JH3ukoKH4FETyElj2ZMRMoz0DAflVspeddmCjmA0F7SvHh1egTyF0u9GfXW6kTmBy6/lgc
certificate private 0 line 8 7Vjmf4AQXaAW4MROzjMMmT2kM0phwZ35MNeg977kXr2E2vzjnOh9Wlk4JmBYplxkw@OHo54sC9@HTYy8PNIJcP1nSs
certificate private 0 line 9 pn21UtTKuk7eVV7WHuxeEZnr0V7Wom0FA8Y0u0yQTX5Ebeft7DZMgNGrCxpH@jilCmgstpyehofYQuC3KFvNmx2ujLJQ
certificate private 0 line 10 uitrerlb9m0JxHmle91wPzGZqMwCy5HFL2IUIn/cuv0y1sh8qC20unS26tO0iv87dpWwCeqAlwt3PGZHM339YV7Cp
certificate private 0 line 11 i0q8WeYLk4sSb9vcsnicFdINaYl9wrWBaZjQIV09vSleN26oTDNBxvmCbJmQyJlUxcDntSirylyIUPthzziagC@Slet
certificate private 0 line 12 WbqjnfBFwGhY6RxCav38qx6@04Eb1bfVaubC/zDH9rLwgr10N/10Rzli0ZqzJ63oL
certificate request 0 line 0 MIICMDCCAZkCAQAwgZ8xCzAJBgNVBAYTAKpQMRERwDwYDVQQIEWhLYW5hZ2F3YTER
certificate request 0 line 1 MA8GA1UEBxMIS2F3YXNha2kxGDAWBG9vBAoTD0Z1aml0c3UgTGItaXRIZDESMBAG
certificate request 0 line 2 A1UECXMJVGVjaCBEaXUuMRswGQYDVQQDEXJzaGlzeWEuZnVqaXRzdS5jb20xHZAAd
certificate request 0 line 3 BgkqjnfBFwGhY6RxCav38qx6@04Eb1bfVaubC/zDH9rLwgr10N/10Rzli0ZqzJ63oL
certificate request 0 line 4 gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEj3UwGPb/19yaAuR9ZB/TTIglLUw7nHj
certificate request 0 line 5 Eu+i2RSudi7YhH70YOGMdBG81CtelqV2zP+x/9507lqs5YyJkHYzqyS4E4+KOAQG
certificate request 0 line 6 fs/o1JlcpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwUUNAXX13CyHQ/x0LagMBAAgG
certificate request 0 line 7 UDBOBGqkqhkIG9w0BCQ4xQTA/MAsGA1UdDwQEAwChDAPBgNVHREEDCAGhwTAqAEB
certificate request 0 line 8 MB8GA1UdEQQYMBaCFHNoaXN5S1hLmZ1aml0c3UuY29tMA0GCSqSIsb3DQEBAUA
certificate request 0 line 9 A4GBADod3PXDfWBJOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqO
certificate request 0 line 10 Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6lkDXcl5xw0JKU79r1syllGboCJa
certificate request 0 line 11 CzIBS/zl+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
Created RSA private key and Certificate request.
#
```

```
自装置証明書要求 (鍵ペア) の作成終了
# save
```

```
自装置証明書要求 (鍵ペア) の表示
# show crypto certificate base64 candidate
[Certificate Request]
```

```
[1] Number : 0
-----BEGIN CERTIFICATE REQUEST-----
MIICMDCCAzCAQAwZ8xCzAJBgNVBAYTAkpQMREwDwYDVQQIEWhLYW5hZ2F3YTER
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGItXRIZDESMBAG
A1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTIgLuw7nHj
Eu+i2RSudi7YhH70YOGmDbG81CtelqV2zP+x/9507lqs5YyJkHYzqyS4E4+KOAQG
fs/o1JlcpEPD2iAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXI3CyHQ/x0LAgMBAAGg
UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAgHwTAqAEB
MB8GA1UdEQQYMBaCFHNoaXN5S1hLmZ1aml0c3UuY29tMA0GCSqGSIb3DQEBBAUA
A4GBADod3PXDfWBJOmrUNdeODdrlKakzNtmEx6py42t92reStv3Lx903TJ503QqO
Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6lkDXcl5xw0JKU79rIsyllGboCJa
CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
-----END CERTIFICATE REQUEST-----
#
```

表示された自装置証明書要求の証明書部分「-----BEGIN CERTIFICATE REQUEST-----」から「-----END CERTIFICATE REQUEST-----」の最後の改行までをカット＆ペーストで端末（パソコンなど）に保存します。

保存した自装置証明書要求は端末で、FTPなどで認証局（CA）と交換します。

次に認証局で発行された自装置証明書をFTPなどで認証局から端末（パソコンなど）に保存します。

## 自装置証明書の取り込み

### ● コマンド

```
# crypto certificate local 0 name my-cert0.pem
Please input.
端末（パソコンなど）に保存した自装置証明書を貼り付けます。
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQEWdQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGItXRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA1MDIyMjE1WWhcNMDcwMTAxMDIyMjE1WjCBnzELMAkGA1UEBhMCSIAXETAP
BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPPRnVq
aXRzdSBMaW1pdGVkMRlWEAYDVQQLEWlUZWN0IERpdj4xGzAZBgNVBAMTEnNoaXN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwGgYkCgYEAocGCIVZtO1Tool3eIltbmsOxhK3
KIOqwZhDM11sOGIQUvT6ImpyL25NcoQIJbN9mT31MWWpp1nfirBB3LenaT3X/MEo
vveD9FJ1VbnENjbuEmmjhvxnj7/MHDvQ1D3163BpslkOIVs1dauO+uOZ6R11iM4G
Kypoad0ukW05f9ECAwEAATANBgkqhkiG9w0BAQFAAQBBgQBHokgsMEIT5CJbozH7
rX4u+dLwb0Y48rkfuTmlTRfx+eVniPVCdaUxV0lh361RaWtta/8116OxHylmHCnt
LOLEsckXxnU0ArYBNjyYlrXwurBJYtIVZPOPqRDq7gSez4zp1IPkt14DrTRSGoH
3rQwOpmTcYT9UuDuD4iddD9CmUrA==
-----END CERTIFICATE-----
以下のようなコマンドが表示され、自装置証明書の設定が行われます。
certificate local 0 name my-cert0.pem
certificate local 0 line 0 MIICITCCAf4CAQAwDQYJKoZIhvcNAQEEBQAwwZlxCzAJBgNVBAYTAkpQMREwDwYD
certificate local 0 line 1 VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMla2F3YXNha2kxEDAObgNVBAoTB3NjYyBM
certificate local 0 line 2 dGQxDtALBgNVBAAsTBGRhaTlxGDAWBgNVBAMTD0hpcm9mdW1pIEthc3VnYTEiMCAg
certificate local 0 line 3 CSqGSIb3DQEJARYTa2FzdWdAc2NjLWluYy5jby5qcDAeFw0wNjA1MDIyMjE1WWhcN
certificate local 0 line 4 Fw0wNjA1MDIyMjE1WWhcNMDcwMTAxMDIyMjE1WjCBnzELMAkGA1UEBhMCSIAXETAP
certificate local 0 line 5 d2ExETAPBgNVBAcTCGthd2FzYWwTMRADgYDVQQKEWdzY2MgTHRkMQ0wCwYDVQQLE
certificate local 0 line 6 EwRkYWkyMRGwFgYDVQQDEw9laXJvZnVtaSBLYXN1Z2ExIjAgBgkqhkiG9w0BCQEW
certificate local 0 line 7 E2thc3VnQHnjYy1pbmMuY28uanAwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGB
certificate local 0 line 8 AM5sXoNnzM4FQrpYnF/ekLWYfH3w0yz11qtGUpoWRZIGWiAs4rx/1RgGtnQnjNBc
certificate local 0 line 9 8tD9tG2Uo2ngiNsKNvRB39j7EGFgdpJwwfAaKqA7rgRzQo7jyH7rE5CATVBAnYI
certificate local 0 line 10 HUOIhUAOzDy851u5p4ZjADdlcsPu+5FUqgMgVZ7/B/sdAgMBAEwDQYJKoZIhvcN
certificate local 0 line 11 AQEEBQADgYEAwpvly/Ak6d1vMgdctIYY5S14jQkD2tnB9CtHz+byG4l75lqgh2uF
certificate local 0 line 12 xZlPbYuSGvVOS+zll1yilexM5p7QPUs/BAWU1ePUmrLrasetEbgIFX0pXyIWF8C
```

```
certificate local 0 line 13 bW08H9SMIDfkd6dindxpka3VmVIPQKSwCkaAF2ka+LAao0lasskjm04=
#
```

自装置証明書の設定終了

```
# save
# reset
```

認証局や相手装置で発行された相手装置証明書をFTPなどで認証局から端末（パソコンなど）に保存します。

## 相手装置証明書の取り込み

### ● コマンド

```
# crypto certificate remote 0 name rmt-cert0.pem
```

Please input.

端末（パソコンなど）に保存した相手装置証明書を貼り付けます。

```
-----BEGIN CERTIFICATE-----
```

```
MIIICrZCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGItaXRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAXETAP
BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPrnVq
aXRzdSBMaW1pdGVkMRlwEAYDVQQLEwIUZWNolERpdj4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMBlg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrijACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrgSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GikoN+tXc4Q==
```

```
-----END CERTIFICATE-----
```

以下のようなコマンドが表示され、相手装置証明書の設定が行われます。

```
certificate remote 0 name rmt-cert0.pem
```

```
certificate remote 0 line 0 MIIICrZCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
```

```
certificate remote 0 line 1 VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
```

```
certificate remote 0 line 2 c3UgTGItaXRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
```

```
certificate remote 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
```

```
certificate remote 0 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAXETAP
```

```
certificate remote 0 line 5 BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPrnVq
```

```
certificate remote 0 line 6 aXRzdSBMaW1pdGVkMRlwEAYDVQQLEwIUZWNolERpdj4xGzAZBgNVBAMTEmhvbnN5
```

```
certificate remote 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
```

```
certificate remote 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
```

```
certificate remote 0 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
```

```
certificate remote 0 line 10 mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
```

```
certificate remote 0 line 11 zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
```

```
certificate remote 0 line 12 /9AqZo3mV7b/uXDdljRMBlg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
```

```
certificate remote 0 line 13 Wiv3s5KaqrijACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrgSNM5zzg4AgIX+uE8XY5fE
```

```
certificate remote 0 line 14 VAupZ2q7za3Slq6GikoN+tXc4Q==
```

相手装置証明書の設定終了

```
# save
# reset
```

## 2.39.2 装置に証明書を登録する（自装置証明書を自己発行する）

RSA 鍵ペア（証明書要求）および自装置証明書を本装置で作成し登録する方法を説明します。  
また、相手装置証明書について登録する方法も説明します。

ここでは以下の条件によって、本装置の RSA 鍵ペア（証明書要求）、自装置証明書の作成および相手装置証明書を登録します。

### ● 設定条件

- 鍵ペア識別番号 : 0
- 鍵長 : 1024bit
- 証明書要求で使用するハッシュアルゴリズム : md5
- 自装置証明書識別名 : my-cert0.pem
- 自装置証明書で使用するハッシュアルゴリズム : md5
- 自装置証明書の有効期限  
失効日付 : 2018年1月1日
- 国名 (C) : JP
- 都道府県 (ST) : Kanagawa
- 市区町村 (L) : Kawasaki
- 組織または会社名 (O) : Fujitsu Limited
- 組織ユニットまたは部門 (OU) : Tech Div.
- ホスト名 (CN) : shisya.fujitsu.com
- メールアドレス : shisya@fujitsu.com
- サブジェクト代替名称 (IP アドレス) : 192.168.1.1
- サブジェクト代替名称 (DNS 名) : shisya-A.fujitsu.com
- 相手装置証明書識別名 : rmt-cert0.pem

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 自装置証明書の作成

### ● コマンド

```

自装置証明書の作成を行う
# crypto certificate generate
RSA key pair number[0-4] :0
generate RSA key pair.
Are you sure?[y/n] :y
Local certificate number[0-4] :0
key bit(361-2048) :1024
certificate request hash(sha1 or md5) :md5
local certificate name :my-cert0.pem
local certificate hash(sha1 or md5) :md5
expire date(YYYYMMDD) :20180101
Country Name(2 letter code) :JP
State or Province Name :Kanagawa
Locality Name :Kawasaki
Organization Name :Fujitsu Limited
Organizational Unit Name :Tech Div.

```

```

Common Name :shisyafujitsu.com
Email Address :shisyafujitsu.com
subjectAltName IP :192.168.1.1
subjectAltName DNS :shisyafujitsu.com
以下の様なコマンドが表示され、鍵ペアと自装置証明書の設定が行われます。
Please wait to create RSA private key and Certificate request.
certificate private 0 line 0 riUB@No/FTnpCpEt5EFOcClRdgTIDnB5n4DLemM5Lr1D8@zQQAL90cFFlczCY7P@W3ddbEokoMnHTc@6SP7VOy/isD2
certificate private 0 line 1 qC0dBFQC1TpoWDZtpUkK5cU1YilubYxhA5V2duYwB0xAqjlfVsNRzF/xcoi5FnKiOdZjzWxv75NjMYM@nzuVnL6
certificate private 0 line 2 w27xcCjoF1paovWVw1aA4rXXY2L4DGW30rs04sDWCnErCL855Mqw0@Xz0raGv@g8MfKGX3bnEaDImiyAIFflbxRVFsQU
certificate private 0 line 3 xM5V6omhXp2WaRn6Xi/04wipg357HvboVnJKAIQpY6AbeAftpphz47KFPKnmDMaMuxiPY2w@150br1KUM1VknouUfYTP
certificate private 0 line 4 cfsRgjZ8kEbsUESNzftKATlbtDSBqLZ5B046RwRIBkpkakJ9dlVv30dJ7cdfnJi9hX@faJbpP3@F3NZP4yKAE3CWtqF
certificate private 0 line 5 jk31xz750HuAGNPWsWEVMA6Kt@YpKpV9zvWwGdlmOKBs8XgTA8Y5hg8Ut@THKIRI0TgdM4avfQaYwwXWWCFxvUHZ
certificate private 0 line 6 KsrHISB2rYuTnCYcm2sYNdVXaVrMv6VqkNfYnrOwfwu0OqczYUZEDNOYSKp2tLDqBo047nNVmJWOb2BOex1ujZktW/
certificate private 0 line 7 59UMtzc44eZToKjXqU2JH3ukoKH4FEtYelJ2ZMRMoz0DAfVspeddmCjmA0F7SvHh1egTyF0u9GfXW6kTImBy6lgc
certificate private 0 line 8 7Vjmfca4QXaAW4MR0zjMMmT2kM0phwZ35MNeg977kXr2E2vzjnOh9Wlk4JmByplxkw@OHo54sC9@HTYy8PNIJcP1nSs
certificate private 0 line 9 pn21UitKuk7eV7WHuxeEznr0V7Wom0FA8Y0u0yQTX5Ebefr7DZMgNGrCxph@jClmgstpyehofYQUC3kFvNmx2ujLJQ
certificate private 0 line 10 uittrerl9m0JxHmle91wPzGZqMwCy5HFL2UIIn/cuv0y1sh8qC20unS26t00iv87dpWwocEqAlw3PGZHm339V7Cp
certificate private 0 line 11 i0q8WeYLk4sSb9vcsnicFdINaYl9wrVBAzQJlV09vSleN26oTDNBxvmCbJmJqJUlXcDntSirylyUPthzziagC@Slet
certificate private 0 line 12 WbjmBFwGhY6RxCav38qx6@04Eb1bfVaubC/zDH9Lwgr10N/10RzI0ZqzJ63oL
certificate request 0 line 4 gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTlgkLUw7nHj
certificate request 0 line 1 MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGItaXRIZDESMBAG
certificate request 0 line 2 A1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
certificate request 0 line 3 BgkqhkiG9w0BCQEWEghvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
certificate request 0 line 4 gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTlgkLUw7nHj
certificate request 0 line 5 Eu+i2RSudi7YhH70YOGmDBG81CtelqV2zP+x/95O7lqs5YyJkHYzqyS4E4+KOAQG
certificate request 0 line 6 fs/o1JlcpEPD2IAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXI3CyHQ/x0LAGMBAAGg
certificate request 0 line 7 UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAghwTAqAEB
certificate request 0 line 8 MB8GA1UdEQQYMBaCFHNoaXN5S1hLmZ1aml0c3UuY29tMA0GCsGqSIb3DQEBAUA
certificate request 0 line 9 A4GBADod3PXFDFWBJOmRUnDeODrIkKakzNtmEx6py42t92reStv3Lx903TJ503QqO
certificate request 0 line 10 Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6lkDXcl.5xw0JKU79rlylGboCJa
certificate request 0 line 11 CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAN4tqbCv6EnNHAAn3L
Created RSA private key and Certificate request.

```

Please wait to create Local certificate.

```

certificate local 0 name my-cert0.pem
certificate local 0 line 0 MIIDBJCCAm8CAQEwDQYJKoZIhvcNAQEEBQAwZ8xZzAJBgNVBAYTAkQREwDwYD
certificate local 0 line 1 VQIIEwhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate local 0 line 2 c3UgTGItaXRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
certificate local 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEghvZ2VAZnVqaXRzdS5jb20wHhcN
certificate local 0 line 4 MDYxMDEwMDE1MDI5WjcBnzELMAkGA1UEBhMCSiAxETAP
certificate local 0 line 5 BgNVBAGTCEthbnFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPrnVq
certificate local 0 line 6 aXRzdSBMaW1pdGVkMRlweAYDVQQLWEwUZWNoIERpdj4xGzAZBgNVBAMTEEnoXN5
certificate local 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCsGqSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTcB
certificate local 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAAnmXhgzmp9MDVjifGcSOLdTAy9v8
certificate local 0 line 9 j3Joc5H1kH9NMiCQtTDuceMS76LZFK52LtiEfvRg6Ax0EbZUK16WpXbM/7H/3k7u
certificate local 0 line 10 WqzJlImQdjOrJLgTj4o4BAZ+z+jUkhykQ8PalCpbSuRcZWhxGM27E3sV2F8OLCxR
certificate local 0 line 11 Q0BdeXclLdD/HQsCAwEAaANVMFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAAaHBMCo
certificate local 0 line 12 AQEwHwYDVR0RBGwFolUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAGw
certificate local 0 line 13 BgEBwIBATANBgkqhkiG9w0BAQQFAAOBGAQAAZLDJ3a38HgT3el7FkXLWcfEaK
certificate local 0 line 14 ulZnNv7/cj9KimdSianZWdgEvDKQOx41KtrWxxrHgrzRSbg4KpkjgUgthadJvq
certificate local 0 line 15 hKK1zelemN7RnpFuuBODkxx4hM1vuzJRTVUWH+UJciFoMAQOnrjB8hoNygFqVji
certificate local 0 line 16 9OyuMYZvejGO5A==
Created Local certificate.
#

```

自装置証明書の作成終了

# save

自装置証明書の表示

# show crypto certificate base64 candidate

[Certificate Request]

[1] Number : 0

-----BEGIN CERTIFICATE REQUEST-----

```

MIICMDCCAZkCAQAwZ8xZzAJBgNVBAYTAkQREwDwYD
MA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0c3UgTGItaXRIZDESMBAG
A1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEuZnVqaXRzdS5jb20xHzAd
BgkqhkiG9w0BCQEWEghvZ2VAZnVqaXRzdS5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBAJ6514c4JqfTA1Y43xnEji3UwGPb/I9yaAuR9ZB/TTlgkLUw7nHj
Eu+i2RSudi7YhH70YOGmDBG81CtelqV2zP+x/95O7lqs5YyJkHYzqyS4E4+KOAQG
fs/o1JlcpEPD2IAqW0rkXGVocRjNuxN7FdhfDiwsUUNAXXI3CyHQ/x0LAGMBAAGg
UDBOBgkqhkiG9w0BCQ4xQTA/MAsGA1UdDwQEAwIChDAPBgNVHREECDAghwTAqAEB
MB8GA1UdEQQYMBaCFHNoaXN5S1hLmZ1aml0c3UuY29tMA0GCsGqSIb3DQEBAUA

```

```
A4GBADod3PXDFWBJOmrUNdeODdrIKakzNtmEx6py42t92reStv3Lx903TJ503QqO
Zzs7YoyRK2BZCkdRuzrs7eAmMPO41/tRNalR6IkDXcL5xw0JKU79rlsYllGboCJa
CzIBS/z/+Rkq72KHOWQa/lqZZRMEJAAN4tqbCv6EnNHAAn3L
-----END CERTIFICATE REQUEST-----
```

[Local Certificate]

```
[1] Number : 0, Name : my-cert0.pem
```

```
-----BEGIN CERTIFICATE-----
```

```
MIIDBjCCAm8CAQEwDQYJKoZIhvcNAQEEBQAwwGZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaxRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJzaGlzeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYxMDEwMDE1MDI5WWhcNMDcwMTAxMDE1MDI5WjCBnzELMAkGA1UEBhMCSiAxETAP
BgNVBAgTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEWhUZWNolERpdi4xGzAZBgNVBAMTEEnoAXN5
YS5mdWppdHN1LmNvbTEfMB0GCsqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwGyKCGYEAAnrnXhzgmp9MDVjffGcSOLdTAY9v8
j3JoC5H1kH9NMicQtTDuceMS76LZFK52LtiEfvRg6Ax0EbZUK16WpXbM/7H/3k7u
WqzljmQdjOrJLgTj4o4BAZ+z+jUkhykQ8PalCpbSuRcZWWhxGM27E3sV2F8OLCxR
Q0BdeXcLldD/HQsCAwEAAaNVFMwCwYDVR0PBAQDAgKEMA8GA1UdEQQIMAaHBMCo
AQEwHwYDVR0RBBGwFoUc2hpc3lhLWEuZnVqaXRzdS5jb20wEgYDVR0TAQH/BAGw
BgEB/wIBATANBgkqhkiG9w0BAQQFAAOBgQAAZ2LDxJ3a38HgT3el7FkXLWcfEEaK
ulZnNv7/cjj9KimdSianZWdgEvDKQQOx41KtrWxxrHgrzRSbg4KpkjgUgthadJvq
hKK1zelemN7RnpFuuBODkxx4hM1vuzJRTVUWH+UJciFoMAQOnrjB8hoNyGfiQVji
9OyuMYZvejGO5A==
-----END CERTIFICATE-----
```

表示された証明書要求と自装置証明書の証明書部分「-----BEGIN CERTIFICATE-----」から「-----END CERTIFICATE-----」の最後の改行までをカット&ペーストで端末（パソコンなど）に保存します。

保存した自装置証明書は端末で、FTPなどで相手装置と交換します。

設定終了

```
# reset
```

認証局や相手装置で発行された相手装置証明書をFTPなどで認証局から端末（パソコンなど）に保存します。

## 相手装置証明書の取り込み

### ● コマンド

```
# crypto certificate remote 0 name rmt-cert0.pem
Please input.
端末 (パソコンなど) に保存した相手装置証明書を貼り付けます。
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQLIWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltXRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWjcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAXETAP
BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwIUZWNolERpdj4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSzmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
zeFdGj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMBlg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrgSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GikoN+tXc4Q==
-----END CERTIFICATE-----
以下のようなコマンドが表示され、相手装置証明書の設定が行われます。
certificate remote 0 name rmt-cert0.pem
certificate remote 0 line 0 MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate remote 0 line 1 VQQLIWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate remote 0 line 2 c3UgTGltXRIZDESMBAGA1UECXMJVGVjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
certificate remote 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate remote 0 line 4 MDYwNjA2MDczNTIzWjcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAXETAP
certificate remote 0 line 5 BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate remote 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwIUZWNolERpdj4xGzAZBgNVBAMTEmhvbnN5
certificate remote 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate remote 0 line 8 nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAua6liSE7sVwzRHhfUnUrwnQay45L
certificate remote 0 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSzmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
certificate remote 0 line 10 mVOTGe1ovNGcpj6T73v5MJHivp69Vhc8a25KE7BSaTbsAkvTOPAJt83QE4aXJIZx
certificate remote 0 line 11 zeFdGj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
certificate remote 0 line 12 /9AqZo3mV7b/uXDdljRMBlg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMpUuU
certificate remote 0 line 13 Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrgSNM5zzg4AgIX+uE8XY5fE
certificate remote 0 line 14 VAupZ2q7za3Slq6GikoN+tXc4Q==

相手装置証明書の設定終了
# save
# reset
```



## 2.39.3 認証局証明書を設定する

認証局証明書を使用する場合に認証局証明書を設定する方法を説明します。

[2.39.1 装置に証明書を登録する (自装置証明書を認証局 (CA) で発行する)] (P.413) または [2.39.2 装置に証明書を登録する (自装置証明書を自己発行する)] (P.417) のどちらかで自装置証明書および相手装置証明書を登録してください。

ここでは以下の条件によって、本装置の認証局証明書を作成することを前提とします。

### ● 設定条件

- 認証局証明書識別名 : ca-cert0.pem

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## 認証局証明書を交換し設定する

認証局で発行された認証局証明書を FTP など認証局から端末 (パソコンなど) に保存します。

端末 (パソコンなど) に保存した認証局証明書を貼り付けます。

### ● コマンド

```
# crypto certificate ca 0 name ca-cert0.pem
-----BEGIN CERTIFICATE-----
MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
c3UgTGltaxRIZDESMBAGA1UECXMJVGvjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAXETAP
BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwIUZWNoIERpdj4xGzAZBgNVBAMTEmhvbnN5
YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
nzANBkgqhkiG9w0BAQEFAAOBjQAwGyKCyYEAua6liSE7sVwzRHhfUnUrwnQay45L
3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
/9AqZo3mV7b/uXDdljRMBlg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMPuUu
Wiv3s5KaqrijACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrqSNM5zzg4AgIX+uE8XY5fE
VAupZ2q7za3Slq6GikoN+tXc4Q==
-----END CERTIFICATE-----
```

以下のようなコマンドが表示され、認証局証明書の設定が行われます。

```
certificate ca 0 name ca-cert0.pem
certificate ca 0 line 0 MIICrzCCAhgCAQIwDQYJKoZIhvcNAQEEBQAwwZ8xCzAJBgNVBAYTAkpQMREwDwYD
certificate ca 0 line 1 VQQIEWhLYW5hZ2F3YTERMA8GA1UEBxMIS2F3YXNha2kxGDAWBgNVBAoTD0Z1aml0
certificate ca 0 line 2 c3UgTGltaxRIZDESMBAGA1UECXMJVGvjaCBEaXYuMRswGQYDVQQDEExJob25zeWEu
certificate ca 0 line 3 ZnVqaXRzdS5jb20xHzAdBgkqhkiG9w0BCQEWEGhvZ2VAZnVqaXRzdS5jb20wHhcN
certificate ca 0 line 4 MDYwNjA2MDczNTIzWhcNMDcwMTAxMDczNTIzWjCBnzELMAkGA1UEBhMCSIAXETAP
certificate ca 0 line 5 BgNVBAGTCEthbmFnYXdhMREwDwYDVQQHEWhLYXdhc2FraTEYMBYGA1UEChMPRnVq
certificate ca 0 line 6 aXRzdSBMaW1pdGVkMRIwEAYDVQQLEwIUZWNoIERpdj4xGzAZBgNVBAMTEmhvbnN5
certificate ca 0 line 7 YS5mdWppdHN1LmNvbTEfMB0GCSqGSIb3DQEJARYQaG9nZUBmdWppdHN1LmNvbTCB
certificate ca 0 line 8 nzANBkgqhkiG9w0BAQEFAAOBjQAwGyKCyYEAua6liSE7sVwzRHhfUnUrwnQay45L
certificate ca 0 line 9 3nQ4/7zfeAk5uEcXM69NqL+XoSSZmRr0fKA3qCrZ0t5R5v9KpwgjbG/ogzQePq1m
certificate ca 0 line 10 mVOTGe1ovNGcjp6T73v5MJHivp69Vhc8a25KE7BSaTbsAkVTOPAJt83QE4aXJIZx
certificate ca 0 line 11 zeFdgj7jLuAHMAcCAwEAATANBgkqhkiG9w0BAQQFAAOBgQABZiYiPujmlasvYvUw
certificate ca 0 line 12 /9AqZo3mV7b/uXDdljRMBlg6aEc3Xj1YStFtdb34O8j8koSO/+wmM3Tm6uCMPuUu
```

```
certificate ca 0 line 13 Wiv3s5KaqrjjACYTVnCHU7RKqQjpnJ6TNwSKUIAxDrgSNM5zzg4AglX+uE8XY5fE
certificate ca 0 line 14 VAupZ2q7za3Slq6GlkoN+tXc4Q==
```

認証局証明書の設定終了

```
# save
```

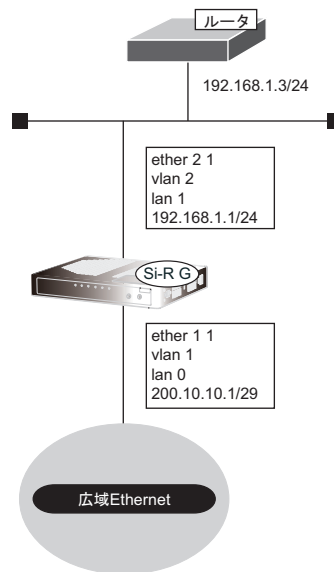
```
# reset
```

## 2.40 トラッキング機能を使う

トラッキング機能を使用すると、トリガの状態が遷移した際にアクション（コマンド）を適用できます。ここでは、トラッキング機能を使用する場合の設定方法を説明します。

### こんな事に気をつけて

- 適用するアクション（コマンド）として、カウンタ・ログ・統計・状態などの表示コマンド、および、トラッキング機能自身の設定・削除や統計情報表示・クリア操作コマンドを指定した場合、コマンドは実行されません。
- ノードトリガでの監視を行う場合、相手ノードにICMP ECHO パケットを定期的送信します。そのため、定額制ではない回線を使用している場合は、超過課金の原因になることがあります。このような環境ではノードトリガを使わないでください。



### ● 設定条件

#### [広域Ethernet側]

- ポート : ether 1 1 を使う
- VLAN : untag 1
- lan : lan 0
- IPアドレス : 200.10.10.1/29

#### [lan側]

- ポート : ether 2 1 を使う
- VLAN : untag 2
- lan : lan 1
- IPアドレス : 192.168.1.1/24

#### [トラッキング]

- 監視先IPアドレス : 192.168.1.3
- 障害発生時のアクション : ether 1 1 を offline にする
- 復旧時のアクション : ether 1 1 を online にする

上記の設定条件に従って設定を行う場合のコマンド例を示します。

## ● コマンド

```
ether ポートを設定する
# ether 1 1 use on
# ether 1 1 vlan untag 1
# ether 2 1 use on
# ether 2 1 vlan untag 2

lan インタフェースを設定する
# lan 0 ip address 200.10.10.1/29 3
# lan 0 vlan 1
# lan 1 ip address 192.168.1.1/24 3
# lan 1 vlan 2

トラッキング情報を設定する
# tracking 0 trigger 0 node 0
# tracking 0 action 0 down "offline ether group 1 port 1"
# tracking 0 action 1 up "online ether group 1 port 1"
# node-trigger 0 address 192.168.1.1 192.168.1.3

設定終了
# save
# commit
```

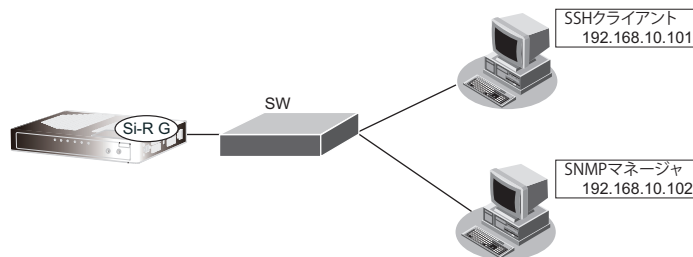
## 2.41 装置を保護する

本装置に対するセキュリティ対策として、以下の設定を行います。

- 管理者 (admin) 用パスワードの設定
- オートログアウトの設定
- Telnet/SSH および SNMP 接続に対するアクセス制限
- 不要なサービスの停止

### 2.41.1 設定例

以下にそれぞれの設定を行う場合の例を示します。



#### ● 設定条件

- 管理者 (admin) パスワード : sirg\_admin-2022
- IP アドレス : 192.168.10.100/24
- オートログアウトの設定 (ログインしたままの状態指定時間無操作だった際に自動切断を行う)  
 コンソールのオートログアウト時間 : 5分  
 SSHのオートログアウト時間 : 5分  
 ※SSH のオートログアウト時間は "telnetinfo autologout" と共通
- SNMP 設定  
 アクセス許可する SNMP マネージャ : 192.168.10.102  
 コミュニティ名 : private  
 マネージャからの書き込み : 許可しない
- SSH接続を許可するホストのIPアドレス : 192.168.10.101
- Telnet 接続 : 禁止
- 不要なサーバ機能はすべて停止  
 # serverinfo <サーバ機能名> ip off
- IPv6 アドレスを Si-R G に付与した際には、IPv6 に関する不要なサーバ機能はすべて停止  
 # serverinfo <サーバ機能名> ipv6 off

```

adminパスワードをsirg_admin-2022に設定
# password admin set sirg_admin-2022
  
```

```

コンソール接続のオートログアウト時間を5分に設定
# consoleinfo autologout 5m
  
```

```

Telnet/SSHのオートログアウトまでの無操作時間を5分に設定
# telnetinfo autologout 5m
  
```

## 自装置IPアドレスとVLANの設定

```
# lan 0 ip address 192.168.10.100/24 3  
# lan 0 vlan 1
```

## SNMPを有効、コミュニティ名をprivate、書き込み許可しない

```
# snmp service enable  
# snmp manager 0 192.168.10.102 private v1 disable
```

## 許可するホストからのSSH接続のみ許可する

```
# acl 0 ip 192.168.10.101/32 any any  
# serverinfo ssh filter 0 accept acl 0  
# serverinfo ssh filter default reject
```

## Telnetサーバ機能を停止

```
# serverinfo telnet ip off
```

## 不要なサーバ機能はすべて停止

```
# serverinfo ftp ip off  
# serverinfo sftp ip off  
# serverinfo http ip off  
# serverinfo dns ip off  
# serverinfo snmp ip off  
# serverinfo time ip tcp off  
# serverinfo time ip udp off
```

## 設定終了

```
# save  
# commit
```

# 索引

## A

AAA 認証	153, 188
ADSL モデム	28
ARP 認証機能	412
AS 外部経路	87
AS 境界ルータ	87

## B

BGP4	27
BGP 機能 (IPv6)	101
BGP 経路の制御 (IPv4)	95
BSR (ブートストラップルータ)	112

## C

CATV インターネット接続	13
----------------	----

## D

DHCP 機能	330
DHCP クライアント機能	335
DHCP サーバ機能	331
DHCP スタティック機能	333
DHCP リレーエージェント機能	337
DH グループ	37, 43, 304
DNS サーバ	131
DNS サーバアドレスの自動取得機能	355
DNS サーバ機能	360
DNS サーバの自動切り替え機能 (逆引き)	354
DNS サーバの自動切り替え機能 (順引き)	352
DNS 問い合わせタイプフィルタ機能	359

## E

ECMP 機能	366
---------	-----

## I

ID タイプ	49, 275
IEEE802.1X 認証機能	408
IKE	37, 43, 304
Ingress ポリシールーティング機能	378
IPsec Version3	157
IPsec 機能	152
IPsec クライアント	314
IPsec サーバ	314
IPv6	52
IPv6 DHCP クライアント機能	341, 347
IPv6 DHCP サーバ機能	343
IPv6 DHCP リレーエージェント機能	345

IPv6 over IPv4 トンネル	55
IPv6 トンネル	52
IPv6 ネットワークの追加	19
IPv6 フィルタリング	141
IP-VPN 接続	27
IP アドレス	60, 126, 327
IP アドレスの自動割り当て	331
IP フィルタリング機能	125, 183
IP フィルタリングの条件	125
IP フィルタリングの設計方針	128

## L

LAN のネットワーク間接続	16
LSA	85, 90

## M

MAC アドレス	333
MAC アドレス認証	410
MED メトリック値	99, 106
MIB	363
MSS 書き換え機能	185
MTU 分割機能	185

## N

NAT	55
NAT トラバースル機能	314
NetBIOS サーバ	147

## O

OSPFv2 (IPv4)	78
OSPF 機能 (IPv6)	90
OSPF 経路の制御 (IPv4)	85

## P

PIM-DM	108
PIM-SM	112
PING	149
PPPoE 接続	20
ProxyDNS	352

## R

RADIUS 認証	153, 197
RA 情報	349
RFC1877	355
RFC2131	355
RFC3361	355
RIP 経路の制御 (IPv4)	60

RIP 経路の制御 (IPv6) ..... 69  
 RP (ランデブーポイント) ..... 112

**S**

SNMP ..... 363  
 SNMP エージェント機能 ..... 363  
 SNTP ..... 17  
 SPI ..... 137, 161  
 SPT (最短経路) ..... 112  
 STP ..... 124

**T**

TCP 接続要求 ..... 125, 126, 128  
 TIME プロトコル ..... 17  
 TOS ..... 318, 327  
 TOS/Traffic Class ..... 320  
 TOS/Traffic Class 値書き換え機能 ..... 318  
 TOS 値 ..... 125  
 TOS 値書き換え機能 ..... 183  
 Traffic Class 値 ..... 318, 327

**U**

URL フィルタ機能 ..... 361

**V**

VLAN ID ..... 320  
 VLAN 機能 ..... 121  
 VLAN パケット ..... 320  
 VLAN プライオリティマッピング機能 ..... 320  
 VoIP NAT トラバーサル機能 ..... 316  
 VPN ..... 152, 157  
 VRRP 機能 ..... 371

**W**

Wakeup on LAN 機能 ..... 386  
 WFQ 機能 ..... 327

**あ**

あて先情報 ..... 125, 318  
 あて先変換 ..... 307  
 アドレス変換機能 ..... 307  
 アドレスマスク ..... 60, 126  
 アプリケーションフィルタ機能 ..... 406  
 暗号情報 ..... 152

**え**

エリア ID ..... 78  
 エリア境界ルータ ..... 85

**か**

可変 IP アドレス ..... 46  
 簡易ホットスタンバイ機能 ..... 371, 372

**き**

基本 NAT ..... 307  
 逆引き ..... 354

**く**

クラウドサービスゲートウェイ機能 ..... 381  
 クラスタリング機能 ..... 371, 375  
 グループ ID ..... 375

**け**

ケーブルモデム ..... 13  
 ケーブルモデム接続 ..... 13

**こ**

構成定義情報切り替え予約 ..... 388, 390  
 固定 IP アドレス ..... 33, 40, 159  
 コネクション確立要求 ..... 126

**さ**

サーバの公開 (PPPoE 接続) ..... 309  
 サーバの公開 (ネットワーク型接続) ..... 311  
 サーバの公開 (プライベート LAN 接続) ..... 313, 308

**し**

シェーピング機能 ..... 184, 322  
 システムログ ..... 305  
 システムログの確認 ..... 306  
 自動鍵交換 ..... 33, 40, 152, 157  
 自動鍵交換 IKE Version2 ..... 270, 274, 278, 281, 284, 287, 290, 293, 296, 299  
 手動鍵交換 ..... 152, 159  
 準スタブエリア ..... 82  
 順引き ..... 352  
 冗長化ネットワーク ..... 98  
 冗長構成の通信経路 ..... 99, 106  
 新 TOS ..... 318

**す**

スイッチング HUB ..... 121  
 スケジュール機能 ..... 388  
 スケジュール予約 ..... 388  
 スタティックルーティング ..... 118



スタブエリア ..... 82

## せ

制御 ..... 125  
 静的 NAT ..... 307  
 セキュリティ ..... 125  
 接続先監視機能 ..... 186

## そ

送信元情報 ..... 125, 318

## た

帯域制御機能 ..... 184, 327  
 ダイアルアップ接続 ..... 13  
 タグ VLAN 機能 ..... 122

## ち

超過課金 ..... 125

## つ

通信の負荷分散 ..... 99, 106  
 通信バックアップ ..... 402

## て

データ圧縮機能 ..... 326  
 データ通信モジュール接続 ..... 22  
 テンプレート着信機能 ..... 188  
 電話番号変更予約 ..... 388, 390

## と

動画・音声 ..... 108  
 透過モード ..... 398  
 動的 IP アドレスの ACL ..... 383  
 動的 NAT ..... 307  
 動的 VPN ..... 153, 208, 217, 220  
 動的経路 (RIP) 機能 ..... 186  
 ドメイン ..... 352  
 ドメイン ID 番号 ..... 383  
 ドメイン名の設定 ..... 383, 385  
 トラッキング機能 ..... 423  
 トラフィックの制御 ..... 95, 101  
 トランジット ..... 104  
 トンネリング ..... 52

## に

認証情報 ..... 152

## は

バックアップポート機能 ..... 123  
 バックアップルータ ..... 371  
 バックボーンエリア ..... 78, 85  
 発信抑止予約 ..... 388

## ふ

フィルタリング条件 (ルーティング) ..... 60  
 フィルタリングの設計方針 (ルーティング) ..... 61, 70  
 負荷分散通信 ..... 366  
 不正端末アクセス防止機能 ..... 410  
 プライオリティ ..... 320  
 プライベート LAN 構築 ..... 11  
 プライベートアドレス ..... 127  
 ブリッジ ..... 391  
 ブリッジグループ機能 ..... 393  
 フレッツ・ADSL ..... 20  
 プロトコル ..... 125, 318, 320, 327

## へ

ヘッダ圧縮機能 ..... 326

## ほ

ポート VLAN 機能 ..... 121  
 ポート番号 ..... 327  
 方向 ..... 60, 69, 125  
 ホストデータベース ..... 360  
 ホストデータベース情報 ..... 333  
 ポリシーベースネットワーク ..... 318  
 ポリシールーティング機能 ..... 378

## ま

マスタールータ ..... 371  
 マニュアル構成 ..... 9  
 マルチ NAT 機能 ..... 183, 307  
 マルチキャスト機能 ..... 108  
 マルチキャスト・パケット ..... 112  
 マルチルーティング機能 ..... 380

## め

メトリック値 ..... 60, 69

## ゆ

優先順位 ..... 128  
 ユニキャスト ..... 108

## り

---

リモートパワーオン機能 .....	386
リモートパワーオン予約 .....	389

---

## Si-R G シリーズ コマンド設定事例集

P3NK-5312-03Z0

発行日 2023年5月

発行責任 富士通株式会社

---

- 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- 本書は、改善のために予告なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、弊社はその責を負いません。