

MR1000

取扱説明書

# Web設定事例集

OMRON

# 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。

2005年1月初版

2005年3月第2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。  
© OMRON Corporation 2004-2005 All Rights Reserved.

# 目次

はじめに .....	2
本書の構成と使いかた .....	6
本書の読者と前提知識 .....	6
本書の構成 .....	6
本書における商標の表記について .....	7
<b>第 1 章 導入例 .....</b>	<b>8</b>
1.1 「かんたん設定メニュー」で設定する .....	9
1.1.1 プライベート LAN を構築する .....	9
1.1.2 セグメント接続／分割する .....	13
1.1.3 PPPoE 接続する .....	17
1.1.4 CATV インターネットに接続する .....	21
1.1.5 インターネットへ ISDN 接続する .....	24
1.1.6 インターネットへ専用線接続する .....	29
1.1.7 オフィスへ ISDN 接続する .....	33
1.1.8 オフィスへ専用線接続する .....	38
1.2 LAN をネットワーク間接続する .....	41
1.3 IPv4 のネットワークに IPv6 ネットワークを追加する .....	48
1.4 プライベート LAN を構築する .....	53
1.5 インターネットへ専用線で接続する .....	59
1.6 インターネットへ PPPoE で接続する .....	64
1.7 事業所 LAN を ISDN で接続する .....	73
1.8 事業所 LAN を専用線で接続する .....	79
1.9 複数の事業所 LAN をフレームリレーで接続する .....	85
1.10 IPv6 の事業所 LAN を ISDN で接続する .....	91
1.11 IPv6 の事業所 LAN を IPv6 トンネルで接続する .....	99
1.12 複数の事業所 LAN を IP-VPN 網を利用して接続する .....	109
1.12.1 ADSL モデムを使用して IP-VPN 網と接続する .....	110
1.12.2 高速デジタル専用線を使用して IP-VPN 網と接続する .....	118
1.13 NAT を併用しない固定 IP アドレスでの VPN (自動鍵交換) .....	127
1.14 NAT と併用した固定 IP アドレスでの VPN (自動鍵交換) .....	138
1.15 NAT と併用した可変 IP アドレスでの VPN (自動鍵交換) .....	150
<b>第 2 章 活用例 .....</b>	<b>163</b>
2.1 RIP の経路を制御する (IPv4) .....	166
2.1.1 特定の経路情報の送信を許可する .....	167
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 .....	169
2.1.3 特定の経路情報の受信を許可する .....	171
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 .....	173
2.1.5 特定の経路情報の送信を禁止する .....	176
2.1.6 特定の経路情報の受信を禁止する .....	178
2.2 RIP の経路を制御する (IPv6) .....	180
2.2.1 特定の経路情報の送信を許可する .....	182
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 .....	184
2.2.3 特定の経路情報の受信を許可する .....	186
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 .....	188
2.2.5 特定の経路情報の送信を禁止する .....	191

2.2.6	特定の経路情報の受信を禁止する	193
2.3	OSPFv2 を使用したネットワークを構築する (IPv4)	195
2.3.1	バーチャルリンクを使う	202
2.3.2	スタブエリアを使う	210
2.4	OSPF の経路を制御する (IPv4)	222
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	222
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	225
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	229
2.5	BGP の経路を制御する (IPv4)	233
2.5.1	特定の経路情報の受信を透過させる	233
2.5.2	特定の AS からの経路情報の受信を遮断する	235
2.5.3	IP-VPN 網からの受信情報の他 IP-VPN 網への送信を遮断する	237
2.5.4	冗長構成の通信経路を使用する	239
2.6	事業所間を MPLS 接続サービスを利用して接続する	243
2.6.1	トンネルエンドポイントをインタフェースアドレスにして MPLS LSP を使用する	244
2.6.2	トンネルエンドポイントをインタフェースアドレスとは別のアドレスにして MPLS LSP を使用する	253
2.7	MPLS を使用したレイヤ 2VPN (EoMPLS) を構築する	263
2.8	MPLS を使用したレイヤ 3VPN (BGP/MPLS VPN) を構築する	271
2.8.1	MPLS 網と LAN を使用して接続する	272
2.8.2	MPLS 網と専用線を使用して接続する	283
2.9	マルチリンク機能を使う	294
2.10	マルチキャスト機能を使う	296
2.10.1	マルチキャスト機能 (PIM-DM) を使う	296
2.10.2	マルチキャスト機能 (PIM-SM) を使う	300
2.11	VLAN 機能を使う	305
2.12	IP フィルタリング機能を使う	309
2.12.1	外部の特定サービスへのアクセスだけ許可する	313
2.12.2	外部から特定サーバへのアクセスだけ許可する	325
2.12.3	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	338
2.12.4	外部の特定サービスへのアクセスだけ許可する (IPv6 フィルタリング)	348
2.12.5	外部の特定サーバへのアクセスだけを禁止する	358
2.12.6	利用者が意図しない発信を防ぐ	362
2.12.7	回線が接続しているときだけ許可する	365
2.12.8	外部から特定サーバへの ping だけを禁止する	367
2.13	IPsec 機能を使う	373
2.13.1	IPv4 over IPv4 で固定 IP アドレスでの VPN (手動鍵交換)	376
2.13.2	IPv4 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)	384
2.13.3	IPv4 over IPv6 で可変 IP アドレスでの VPN (自動鍵交換)	392
2.13.4	IPv6 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)	400
2.13.5	IPv6 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換)	410
2.13.6	IPv6 over IPv6 で固定 IP アドレスでの VPN (自動鍵交換)	421
2.13.7	IPv6 over IPv6 で可変 IP アドレスでの VPN (自動鍵交換)	430
2.13.8	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)	440
2.13.9	IPsec 機能と他機能との併用	452
2.14	システムログを採取する	471
2.15	マルチ NAT 機能 (アドレス変換機能) を使う	473
2.15.1	プライベート LAN 接続でサーバを公開する	474
2.15.2	PPPoE 接続でサーバを公開する	476
2.15.3	ネットワーク型接続でサーバを公開する	479
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	482
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	484
2.16	VoIP NAT トラバーサル機能を使う	486

2.17	TOS/Traffic Class 値書き換え機能を使う	488
2.18	VLAN プライオリティマッピング機能を使う	491
2.19	シェーピング機能を使う	493
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	493
2.19.2	送信先ごとにシェーピング機能を使う	494
2.20	データ圧縮／ヘッダ圧縮機能を使う	498
2.21	帯域制御 (WFQ) 機能を使う	500
2.22	DHCP 機能を使う	504
2.22.1	DHCP サーバ機能を使う	505
2.22.2	DHCP スタティック機能を使う	508
2.22.3	DHCP クライアント機能を使う	510
2.22.4	DHCP リレーエージェント機能を使う	512
2.22.5	IPv6 DHCP クライアント機能を使う	516
2.23	DNS サーバ機能を使う (ProxyDNS)	520
2.23.1	DNS サーバの自動切り替え機能 (順引き) を使う	520
2.23.2	DNS サーバの自動切り替え機能 (逆引き) を使う	522
2.23.3	DNS サーバアドレスの自動取得機能を使う	524
2.23.4	DNS 問い合わせタイプフィルタ機能を使う	526
2.23.5	DNS サーバ機能を使う	528
2.24	特定の URL へのアクセスを禁止する (URL フィルタ機能)	530
2.25	SNMP エージェント機能を使う	532
2.26	ECMP 機能を使う	534
2.27	VRRP 機能を使う	573
2.27.1	簡易ホットスタンバイ機能を使う	574
2.27.2	クラスタリング機能を使う	578
2.28	マルチルーティング機能を使う	583
2.29	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)	586
2.29.1	リモートパワーオン情報を設定する	587
2.29.2	リモートパワーオン機能を使う	587
2.30	スケジュール機能を使う	588
2.30.1	スケジュールを予約する	588
2.30.2	電話番号変更を予約する	590
2.30.3	構成定義情報の切り替えを予約する	591
2.31	通信料金を節約する (課金制御機能)	593
2.31.1	課金単位時間を設定する	593
2.31.2	課金制御機能を設定する	595
2.32	ブリッジ／STP 機能を使う	597
2.32.1	ブリッジで FNA をつないで STP 機能を使う	597
2.32.2	ブリッジルーピング機能を使う	604
2.32.3	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)	611
2.33	複数の LAN ポートをスイッチング HUB のように使う	617
2.34	ISDN 接続を契機とした通信バックアップを使う	620
2.35	外部のパソコンから PIAFS 接続する	627
2.36	アナログモデムで通信バックアップをする	633
2.37	外部のパソコンから着信接続する (リモートアクセスサーバ)	639

<b>索引</b>	<b>644</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。

また、CD-ROMの中の README ファイルには大切な情報が記載されていますので、併せてお読みください。

## 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。

## 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

本装置をご使用になる際に、注意していただきたいことを説明しています。



**補足** 操作手順で説明しているものの他に、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。

## 本書における商標の表記について

Microsoft、Windows および Windows NT 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。

Microsoft® Windows® XP Professional operating system、または Microsoft® Windows® XP Home Edition operating system は、Windows® XP と表記します。

Microsoft® Windows® Millennium Edition operating system は、Windows® Me と表記します。

Microsoft® Windows® 98 operating system は、Windows® 98 と表記します。

Microsoft® Windows® 95 operating system は、Windows® 95 と表記します。

Microsoft® Windows® 2000 Server Network operating system、または Microsoft® Windows® 2000 Professional operating system は、Windows® 2000 と表記します。

Microsoft® Windows NT® Server network operating system Version 4.0、または Microsoft® Windows NT® Workstation operating system Version 4.0 は、Windows NT® 4.0 と表記します。

フレッツは、NTT 東日本・NTT 西日本のサービス名であり、登録商標です。

フレッツ・ADSL は、NTT 東日本・NTT 西日本の登録商標です。

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。

# 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	「かんたん設定メニュー」で設定する	9
1.1.1	プライベートLANを構築する	9
1.1.2	セグメント接続／分割する	13
1.1.3	PPPoE接続する	17
1.1.4	CATV インターネットに接続する	21
1.1.5	インターネットへISDN接続する	24
1.1.6	インターネットへ専用線接続する	29
1.1.7	オフィスへISDN接続する	33
1.1.8	オフィスへ専用線接続する	38
1.2	LANをネットワーク間接続する	41
1.3	IPv4のネットワークにIPv6ネットワークを追加する	48
1.4	プライベートLANを構築する	53
1.5	インターネットへ専用線で接続する	59
1.6	インターネットへPPPoEで接続する	64
1.7	事業所LANをISDNで接続する	73
1.8	事業所LANを専用線で接続する	79
1.9	複数の事業所LANをフレームリレーで接続する	85
1.10	IPv6の事業所LANをISDNで接続する	91
1.11	IPv6の事業所LANをIPv6トンネルで接続する	99
1.12	複数の事業所LANをIP-VPN網を利用して接続する	109
1.12.1	ADSLモデムを使用してIP-VPN網と接続する	110
1.12.2	高速デジタル専用線を使用してIP-VPN網と接続する	118
1.13	NATを併用しない固定IPアドレスでのVPN（自動鍵交換）	127
1.14	NATと併用した固定IPアドレスでのVPN（自動鍵交換）	138
1.15	NATと併用した可変IPアドレスでのVPN（自動鍵交換）	150



## 1.1 「かんたん設定メニュー」で設定する

[設定] タブをクリックすると、[かんたん設定メニュー] ボタンと [詳細設定メニュー] ボタンの2つが表示されます。

通常のご利用では、「かんたん設定メニュー」で十分に設定することができます。「かんたん設定メニュー」で設定したあとに、その他の必要な設定に関しては、「詳細設定メニュー」で設定を追加する方法をお勧めします。

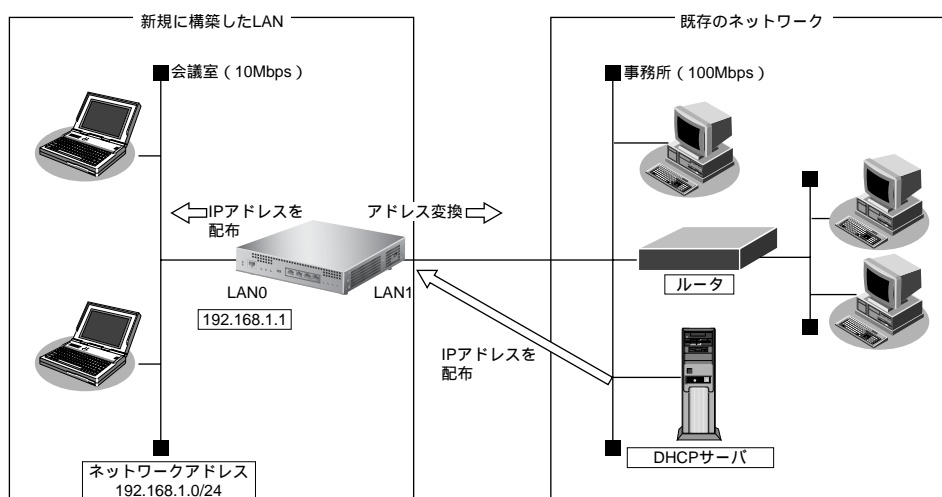
「かんたん設定」は、LAN0およびLAN1インタフェースの構成定義を行います。

### 1.1.1 プライベートLANを構築する

プライベートLAN側では、マルチ NAT 機能を利用しているため、割り当てられた1つのグローバルアドレスを使って、複数台のパソコンからネットワークにアクセスできます。また、DHCPサーバ機能が動作しているため、パソコンのIPアドレスの管理が必要ないので簡単にLANを構築できます。ここでは、以下の条件で一時的に会議室にLANを構築し、事務所のネットワークと接続する場合を例に説明します。

#### 本装置のIPアドレスを変更しない場合

本装置がご購入時の状態の場合、「かんたん設定」では以下の省略値が表示されます。[設定終了] ボタンをクリックして、設定を有効にすると通信することができます。



#### ● 設定条件

##### 【事務所側】

- ・ 転送レートは自動認識
- ・ IPアドレスはDHCPサーバから自動的に取得する

##### 【会議室側】

- ・ 転送レートは自動認識
- ・ 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

### 【その他の条件】

- パスワードを設定する  
パスワード : himitu

☛ 参照 MR1000 Webユーザズガイド「パスワードを設定する」(P.12)

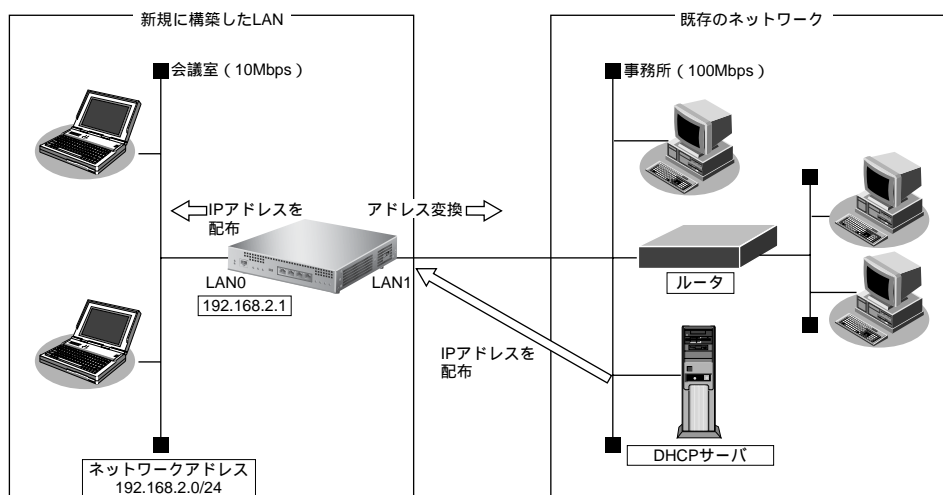
### こんな事に気をつけて

- パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。
- 「プライベートLAN構築」でDHCPサーバを使用すると設定した場合は、DHCPサーバが広報する情報（デフォルトルータ、DNSサーバ、ドメイン名）には、DHCPサーバが動作するインタフェース側のネットワーク構成に応じた情報を設定してください。

## 本装置のIPアドレスを変更する場合

「プライベートLAN構築」では、プライベートLAN側のネットワークアドレスを変更することができます。

以下に、プライベートLAN側（LAN0側）のネットワークアドレスを192.168.2.0/24に変更する設定方法を説明します。



### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Webユーザズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

- 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。

### 1. かんたん設定メニューでLAN間接続の「プライベートLAN構築」をクリックします。

「プライベートLAN構築かんたん設定」ページが表示されます。

この例では、グローバルLAN側（LAN1側）はDHCPサーバから情報を自動的に取得するので、プライベートLAN側（LAN0側）の設定を変更します。

## 2. 「必須設定」で以下の項目を指定します。

- グローバル側IPアドレス → DHCPで自動的に取得する
- プライベート側IPアドレス
  - IPアドレス → 192.168.2.1
  - ネットマスク → 24 (255.255.255.0)

■必須設定	
グローバル側IPアドレス	<input checked="" type="radio"/> DHCPで自動的に取得する <input type="radio"/> 指定する IPアドレス <input type="text"/> ネットマスク 2 (192.0.0.0)
プライベート側IPアドレス	IPアドレス <input type="text" value="192.168.2.1"/> ネットマスク <input type="text" value="24 (255.255.255.0)"/>

## 3. 「オプション設定」で以下の項目を指定します。

- DHCPサーバ → 使用する
  - デフォルトルータ広報 → 192.168.2.1
  - DNSサーバ広報 → 192.168.2.1
- UPnP機能 → UPnP対応装置やUPnP対応アプリケーションプログラムを使用する場合は“使用する”を選択します。

☛ 参照 「VoIP NATトラバーサル機能を使う」(P.486)

■オプション設定	
デフォルトルータ	<input type="text"/>
DNSサーバアドレス	<input type="text"/>
DHCPサーバ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	デフォルトルータ広報 <input type="text" value="192.168.2.1"/>
	DNSサーバ広報 <input type="text" value="192.168.2.1"/>
	ドメイン名広報 <input type="text"/>
UPnP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
LAN0転送レート	自動認識
LAN1転送レート	自動認識

## 4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に通信できる状態になります。

こんな事に気をつけて

- 本装置のIPアドレスを変更した場合、以下に示す2つの操作が必要です。
  - 本装置に接続しているパソコンのIPアドレスも変わります。再度、DHCPサーバから割り当ててもらう必要があります。
  - 再起動後に本装置にアクセスするためには、URLで指定するIPアドレスに変更後のIPアドレスを指定する必要があります。
- 本装置に接続するネットワーク上のパソコンは、IPアドレスを自動的に取得する設定にしてください。IPアドレスを固定的に設定していると、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。なお、常時同じIPアドレスを取得する場合は、設定の「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。
- ご購入時は、LAN0ポートからだけ設定できます。
- グローバル側インタフェースをLAN0側に変更した場合、LAN1ポートからだけ設定できるように変更されます。



### ◆ 省略値について

プライベートLAN 構築かんたん設定に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目		適用される省略値	かんたん設定での設定変更
グローバル側	IP アドレス	DHCP クライアント機能により自動的に取得する	○
	ネットマスク	DHCP クライアント機能により自動的に取得する	○
	セカンダリ IP アドレス	なし	×
	デフォルトルータ	DHCP クライアント機能により自動的に取得する	○
	DNS サーバアドレス	DHCP クライアント機能により自動的に取得する	○
	DHCP サーバ機能	使用しない	×
	NAT 機能	マルチ NAT を使用する ・アドレス個数：1個 ・アドレス割り当てタイム：5分	×
	RIP 機能 ・RIP 送信 ・RIP 受信	ルーティングプロトコルを使用しない RIP-V1 を使用する	×
	インタフェース	LAN1	○
	転送レート	自動認識	○
プライベート側	IP アドレス	192.168.1.1	○
	ネットマスク	24 (255.255.255.0)	○
	セカンダリ IP アドレス	なし	×
	DHCP サーバ機能 ・割り当て先頭 IP アドレス ・割り当てアドレス数	使用する 本装置のプライベートLAN 側の IP アドレス、ネットマスクから求めたネットワークアドレス + 2 253	○ × ×
	デフォルトルータ広報	192.168.1.1	○
	DNS サーバ広報	192.168.1.1	○
	ドメイン名広報	なし	○
	RIP 機能 ・RIP 送信 ・RIP 受信	RIP-V1 を使用する RIP-V1 を使用する	×
	転送レート	自動認識	○
	IPv6 経路	使用しない	×
ブリッジ	使用しない	×	
UPnP 機能	使用しない	○	

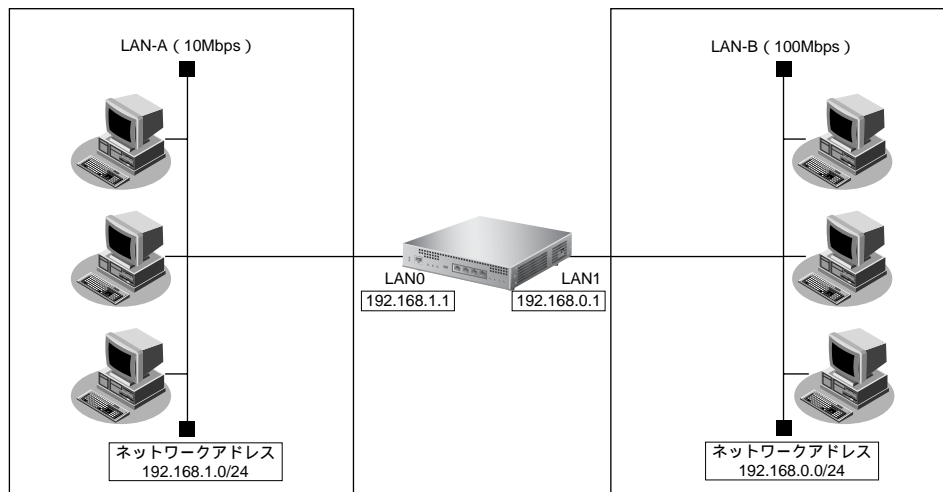
## 1.1.2 セグメント接続／分割する

ネットワークへの接続台数が増加したり、同じネットワーク上に大量データを送受信するホストがあると、トラフィックが増加し、通信性能が劣化する場合があります。このような場合、ネットワークを分割することで、トラフィックを分散することができます。本装置は、2つのネットワークインターフェースを持っているので、簡単にネットワークを接続したり分割したりすることができます。

ここでは、以下の条件で LAN-A と LAN-B をネットワーク間接続する場合を例に説明します。

### 本装置の IP アドレスを変更しない場合

本装置をご購入時の状態の場合、「かんたん設定」では以下の省略値が表示されます。[設定終了] ボタンをクリックして、設定を有効にすると通信することができます。



#### ● 設定条件

##### 【LAN-A 側】

- 転送レートは自動認識
- 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

##### 【LAN-B 側】

- 転送レートは自動認識
- IPアドレス : 192.168.0.1
- ネットワークアドレス/ネットマスク : 192.168.0.0/24

##### 【その他の条件】

- パスワードを設定する  
パスワード : himitu

☞ 参照 MR1000 Web ユーザーズガイド「パスワードを設定する」(P.12)

#### こんな事に気をつけて

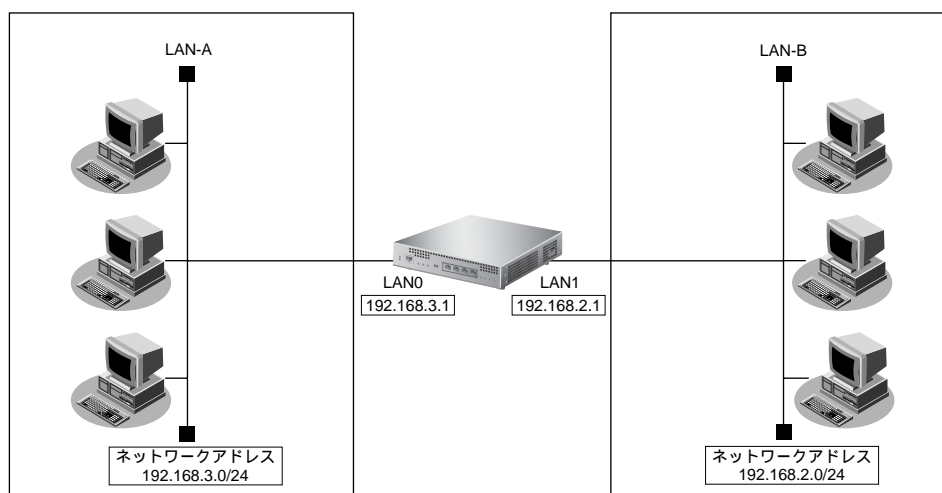
パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。

1. **かんたん設定メニュー**でLAN間接続の「セグメント接続／分割」をクリックします。  
「セグメント接続／分割かんたん設定」ページが表示されます。
2. **【設定終了】** ボタンをクリックします。  
再起動後に通信できる状態となります。

## 本装置のIPアドレスを変更する場合

既存のネットワークどうしを接続／分割する場合は、それぞれのネットワーク環境に合わせた設定が必要です。「セグメント接続／分割」では、それぞれのネットワークのアドレスを設定できます。

以下に、LAN0側のネットワークアドレスが192.168.3.0/24、LAN1側のネットワークアドレスが192.168.2.0/24を接続する設定方法を説明します。



### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

- 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。

**1. かんたん設定メニューで LAN 間接続の「セグメント接続／分割」をクリックします。**

「セグメント接続／分割かんたん設定」ページが表示されます。

**2. 「LAN0」で以下の項目を指定します。**

- IPアドレス → 192.168.3.1
- ネットマスク → 24 (255.255.255.0)

LAN0	
IPアドレス	<input type="text" value="192.168.3.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>

**3. 「LAN1」で以下の項目を指定します。**

- IPアドレス → 192.168.2.1
- ネットマスク → 24 (255.255.255.0)

LAN1	
IPアドレス	<input type="text" value="192.168.2.1"/>
ネットマスク	<input type="text" value="24 (255.255.255.0)"/>

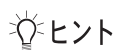
**4. 設定が終了したら、[設定終了] ボタンをクリックします。**

再起動後に通信できる状態になります。

**こんな事に気をつけて**

本装置の IP アドレスを変更した場合、以下に示す 2 つの操作が必要です。

- 本装置に接続しているパソコンの IP アドレスも合わせて変更する必要があります。
- 再起動後に本装置にアクセスするためには、URL で指定する IP アドレスに変更後の IP アドレスを指定する必要があります。



## ヒント

### ◆ 省略値について

セグメント接続/分割かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目		適用される省略値	かんたん設定での設定変更
LAN0	IPアドレス	192.168.1.1	○
	ネットマスク	24 (255.255.255.0)	○
	セカンダリIPアドレス	なし	×
	DHCPサーバ機能	使用しない	×
	NAT機能	使用しない	×
	RIP機能 ・RIP送信 ・RIP受信	RIP-V1を使用する RIP-V1を使用する	×
	転送レート	自動認識	○
LAN1	IPアドレス	192.168.0.1	○
	ネットマスク	24 (255.255.255.0)	○
	セカンダリIPアドレス	なし	×
	DHCPサーバ機能	使用しない	×
	NAT機能	使用しない	×
	RIP機能 ・RIP送信 ・RIP受信	RIP-V1を使用する RIP-V1を使用する	×
	転送レート	自動認識	○

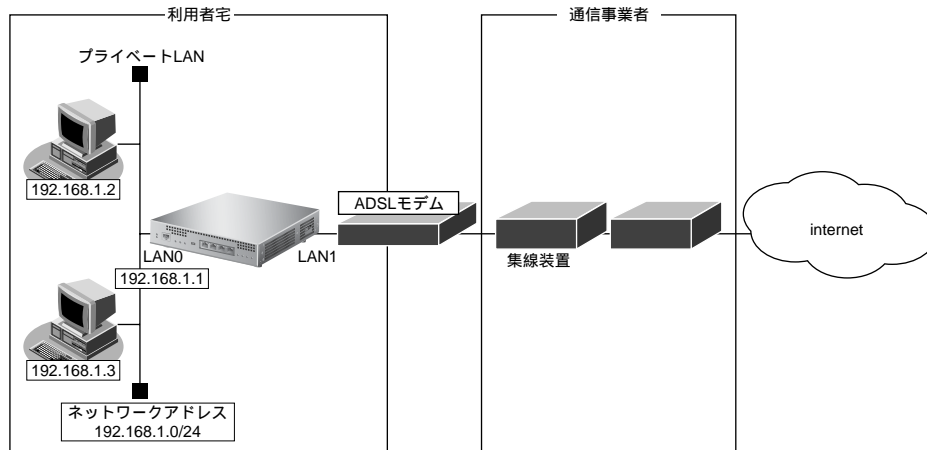


## 1.1.3 PPPoE 接続する

本装置は、通信事業者が提供する ADSL 回線で、PPPoE プロトコルを利用した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できます。

PPPoE プロトコルは、ダイヤルアップ接続で使用する PPP プロトコルを Ethernet 上で使用するものです。

PPPoE 接続を使ってフレッツ・ADSL などのサービスを利用できます。具体的には、本装置の PPPoE で使用するインタフェースと ADSL モデムを接続し、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します。



### ● 設定条件

#### 【通信事業者側】

- 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)
- LAN0 ポートを使用する

#### 【プライベートLAN側】

- 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

#### 【その他の条件】

- パスワードを設定する  
パスワード : himitu

この例の場合、本装置がご購入時の状態の場合、まず、**かんたん設定**でインターネットへの「PPPoE 接続」をクリックし、「PPPoE かんたん設定」画面でユーザ認証 ID とユーザ認証パスワードを入力します。次に、[設定終了] ボタンをクリックすると、通信できます。

以下に、PPPoE 接続の設定方法を説明します。ただし、パスワードだけは、基本設定で設定する必要があります。

☛ 参照 MR1000 Web ユーザーズガイド [「パスワードを設定する」](#) (P.12)

### こんな事に気をつけて

- パスワードを設定することを強く推奨します。設定しない場合、ネットワーク上のだれからでもアクセスできるため非常に危険です。
- 文字入力フィールドでは半角文字（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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

- 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。

## 1. かんたん設定メニューでインターネットへの「PPPoE 接続」をクリックします。

「PPPoE かんたん設定」ページが表示されます。

## 2. 「必須設定」で以下の項目を指定します。

- 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)

■ 必須設定	
ユーザ認証 ID	userid
ユーザ認証パスワード	*****

## 3. 必要に応じて、「オプション設定」で以下の項目を指定します。

- IP アドレス → 192.168.1.1
- ネットマスク → 24 (255.255.255.0)
- DNS サーバ → DNS サーバの IP アドレスが公開されていない場合、または DNS サーバアドレスの自動取得機能を利用する場合は“自動取得”をチェックします。ただし、自動取得はプロバイダが DNS 自動取得に対応している場合だけ使用できます。
- 接続ネットワーク名 → internet (接続するネットワークの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。)
- 接続先名 → ISP-1 (プロバイダの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。)
- PPPoE で使用するインタフェース → PPPoE で使用するインタフェースを選択します。
- 常時接続機能 → 常時接続を行う場合は、“使用する”を選択します。
- アドレス変換 → 1 つのグローバル IP アドレスを使って、複数台のパソコンからネットワークにアクセスする場合は、“マルチ NAT”を選択します。
- UPnP 機能 → アドレス変換で“マルチ NAT”を選択した場合だけ設定します。UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合に“使用する”を選択します。
- LAN0 / 1 転送レート → LAN インタフェースに接続するネットワークの転送レートを選択します。“自動認識”を選択した場合、HUB とのネゴシエーションによって速度と全二重 / 半二重を自動決定します。

■オプション設定	
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
DNSサーバ	<input checked="" type="checkbox"/> 自動取得
接続ネットワーク名	internet
接続先名	ISP-1
PPPoEで使用するインタフェース	<input checked="" type="radio"/> LAN0 <input type="radio"/> LAN1
常時接続機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 無通信監視タイム <input type="text" value="0"/> 秒
アドレス変換	<input type="radio"/> 使用しない <input checked="" type="radio"/> マルチNAT UPnP機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
LAN0転送レート	自動認識
LAN1転送レート	自動認識

#### 4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に、通信できる状態になります。

#### こんな事に気をつけて

- フレッツ・ADSL とは、NTTが提供するサービスです。定額料金でインターネットが使えます。フレッツ・ADSL を使用する場合は、NTTとの契約とフレッツ・ADSLに対応しているプロバイダとの契約が必要です。また、ユーザ認証IDは「xxx@xxx.ne.jp」や「xxx@xxx.com」などの形式を使用しています。詳しくは、契約しているプロバイダに確認してください。
- プライベートLAN上のパソコンに通信事業者が配布したPPPoE接続ソフト（フレッツ・ADSLの場合フレッツ接続ツール）をインストールする必要はありません。
- ADSL回線でのインターネット接続では、PPPoEだけでなく、DHCPや固定でIPアドレスを割り当てるものもあります。その場合は、「[CATVインターネットに接続する](#)」(P.21)を参照してください。また、通信事業者の指示に従ってください。
- 通信事業者によってはルータを用いた接続形態を認めていない事業者もあります。通信事業者の指示に従ってください。
- ご購入時は、LAN0ポートからだけ設定できます。
- 本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするには、パソコンのIPアドレスの変更（再起動）およびURLを変更する必要があります。
- 本装置を既存のLANに接続する場合は、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。
- PPPoEで使用するインタフェースをLAN0側に変更した場合、LAN1側の10/100BASE-TXポートからだけ設定できるように変更されます。



## ◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	かんたん設定での設定変更
プライベート側 IP アドレス	192.168.1.1	○
ネットマスク	24 (255.255.255.0)	○
DNS サーバアドレス	なし (自動取得)	○
自動接続	する	×
常時接続	使用する	○
無通信監視	しない	○
接続ネットワーク名	internet	○
接続先名	ISP-1	○
DHCP サーバ機能 ・ 割り当て先頭 IP アドレス ・ 割り当てアドレス数 ・ DNS サーバの IP アドレス	使用する 本装置のプライベート側 IP アドレス、ネットマスクから求めたネットワークアドレス +2 253 「自動取得 (※ 1)」指定時は、本装置のプライベート側 IP アドレス	×
アドレス変換	マルチ NAT を使用 アドレス割り当てタイマ：5分	○
UPnP 機能	使用しない	○
RIP 機能 ・ RIP 送信 (LAN 側) ・ RIP 受信 (LAN 側) ・ RIP 送信 (PPPoE 側) ・ RIP 受信 (PPPoE 側)	送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・ LAN 側 ・ PPPoE 側	なし デフォルトルートを設定する (メトリック値：1)	×
LAN0 転送レート	自動認識	○
LAN1 転送レート	自動認識	○
インタフェース	LAN1	○
ヘッダ圧縮	VJ-Compression：使用しない	×
MTU サイズ	1454	×
MSS 書き換え	使用する (1414 バイト)	×

※ 1) DNS サーバの IP アドレスを「自動取得」にした場合は、ProxyDNS 情報が以下のように設定されます。

## 「順引き情報一覧」

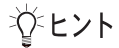
- ・ 優先順位 : 1
- ・ ドメイン : \*
- タイプ : すべて
- 送信元 IP アドレス/マスク : any
- ・ 動作 : 接続先の DNS サーバへ問い合わせる
- ・ ネットワーク名 : internet

## 「逆引き情報一覧」

- ・ 優先順位 : 1
- ・ ネットワークアドレス : any
- ・ 動作 : 接続先の DNS サーバへ問い合わせる
- ・ ネットワーク名 : internet

## 1.1.4 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。



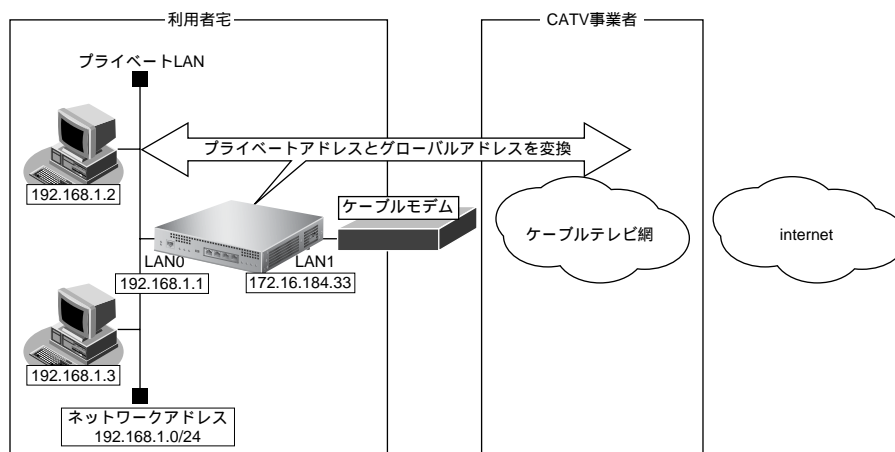
### ◆ ケーブルモデムとは？

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。

CATVインターネット接続は「プライベートLAN構築かんたん設定」で設定します。



### ● 設定条件

#### 【CATV事業者側】

- LAN1ポートを使用する
- 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】

- 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。
  - 文字入力フィールドでは半角文字（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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)
- 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。

## 1. かんたん設定メニューでLAN間接続の「プライベートLAN構築」をクリックします。

「プライベートLAN構築かんたん設定」ページが表示されます。

## 2. 「必須設定」で以下の項目を指定します。

- グローバル側IPアドレス → 指定する  
IPアドレス → 172.16.184.33  
ネットマスク → 24 (255.255.255.0)
- プライベート側IPアドレス  
IPアドレス → 192.168.1.1  
ネットマスク → 24 (255.255.255.0)
- グローバル側インタフェース → LAN0

■ 必須設定	
グローバル側IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する IPアドレス <input type="text" value="172.16.184.33"/> ネットマスク <input type="text" value="24 (255.255.255.0)"/>
プライベート側IPアドレス	IPアドレス <input type="text" value="192.168.1.1"/> ネットマスク <input type="text" value="24 (255.255.255.0)"/>
グローバル側インタフェース	<input checked="" type="radio"/> LAN0 <input type="radio"/> LAN1

**3. 「オプション設定」で以下の項目を指定します。**

- デフォルトルータ → 172.16.184.100
- DNSサーバアドレス → 192.10.10.10
- DHCPサーバ → 使用する  
デフォルトルータ広報 → 192.168.1.1  
DNSサーバ広報 → 192.10.10.10

■オプション設定	
デフォルトルータ	<input type="text" value="172.16.184.100"/>
DNSサーバアドレス	<input type="text" value="192.10.10.10"/>
DHCPサーバ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	デフォルトルータ広報 <input type="text" value="192.168.1.1"/>
	DNSサーバ広報 <input type="text" value="192.10.10.10"/>
	ドメイン名広報 <input type="text"/>
UPnP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
LAN0転送レート	<input type="text" value="自動認識"/>
LAN1転送レート	<input type="text" value="自動認識"/>

**4. 設定が終了したら、[設定終了] ボタンをクリックします。**

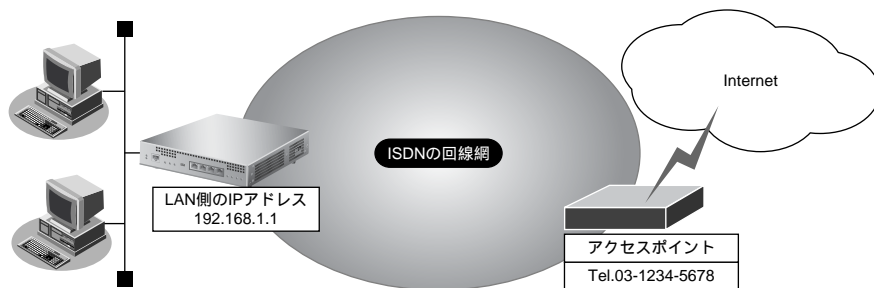
再起動後に、通信できる状態になります。

## 1.1.5 インターネットへISDN接続する

インターネットへISDN接続するときは、「かんたん設定」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- 本装置のIPアドレスとLAN側のネットマスクの変更
- DNSサーバの設定
- 同一プロバイダのアクセスポイントを複数指定（マルチダイヤル）
- ISDN回線を自動切断するまでの時間の変更（無通信監視タイマ）
- 回線の切断タイミングの調整（課金単位時間）
- 接続ネットワーク名と接続先名の設定
- データの転送速度を早くする（MP-Multilink PPP）
- むだな通信料金の抑止（かんたんフィルタ）

ここでは、以下の条件でインターネットへISDN接続する場合を例に説明します。



### ● 設定条件

- 端末型ダイヤルアップ接続を行う
- 新規にLANを構築する
- 接続先の電話番号 : 03-1234-5678
- ユーザ認証ID : userid
- ユーザ認証パスワード : userpass

### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Webユーザズガイド「文字入力フィールドで入力できる文字一覧」(P.13)
- 本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンのIPアドレスの変更（再起動）およびURLを変更する必要があります。
- 本装置を既存のLANに接続する場合は、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置ご購入時のIPアドレスは「192.168.1.1」が設定されています。

## 1. かんたん設定メニューでインターネットへの「ISDN接続」をクリックします。

「インターネットへISDN接続かんたん設定」ページが表示されます。



かんたんメニューは、本装置のトップページで画面上部の「トップ」アイコンをクリックして表示させることができます。



## 2. 「必須設定」で以下の項目を指定します。

- 接続先の電話番号 → 03-1234-5678 (プロバイダから提示された内容)
- 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)

■ 必須設定	
接続先の電話番号	03-1234-5678
ユーザ認証ID	userid
ユーザ認証パスワード	*****

## 3. 必要に応じて、「オプション設定」で以下の項目を指定します。

- IPアドレス → 192.168.1.1
- ネットマスク → 24 (255.255.255.0)
- DNS サーバ → DNS サーバの IP アドレスが公開されていない場合、または DNS サーバアドレスの自動取得機能を利用する場合は“自動取得”をチェックします。ただし、自動取得はプロバイダが DNS 自動取得に対応している場合だけ使用できます。
- 接続先の電話番号2 → プロバイダのほかのアクセスポイントの電話番号 2
- 接続先の電話番号3 → プロバイダのほかのアクセスポイントの電話番号 3



「接続先の電話番号2」、「接続先の電話番号3」は、マルチダイヤル機能を利用する場合に設定します。

- 常時接続機能 → 初期値は“使用しない”。
- 無通信監視タイマ → 初期値は 60 秒。必要に応じて変更します (0 ~ 3600 秒)。



0 を指定した場合、回線の自動切断は行いません。

- 課金単位時間 → 初期値は 0 秒。必要に応じて変更します (0 ~ 3600 秒)。



接続先までの課金単位に合わせて指定します。なお、0 を設定した場合、課金単位の調整は行いません。たとえば、接続先までの電話料金が 3 分 10 円の場合、180 秒をお勧めします。

- 接続ネットワーク名 → internet (接続するネットワークの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。)
- 接続先名 → ISP-1 (プロバイダの名称を半角英数字 8 文字以内で入力します。接続先を区別するための任意の名称を指定します。)
- アドレス変換 → 1 つのグローバル IP アドレスを使って、複数台のパソコンからネットワークにアクセスする場合は、“マルチ NAT” を選択します。  
UPnP 機能 → アドレス変換で“マルチ NAT”を選択した場合だけ設定します。UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合に“使用する”を選択します。
- MP → 初期値は“使用しない”。プロバイダが MP をサポートしていて、MP を使用する場合は“使用する”を選択します。通信量が多くなった場合に自動的に MP を使用します。

### こんな事に気をつけて

接続先のプロバイダがMPに対応していない場合は、MPでは通信できません。

- かんたんフィルタ →初期値は“使用しない”。



Windows®環境でネットワークを構成している場合は、むだな課金が発生する可能性があるため、「かんたんフィルタ」で“使用する”を選択することをお勧めします。

■オプション設定	
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
DNSサーバ	<input checked="" type="checkbox"/> 自動取得
接続先の電話番号2	
接続先の電話番号3	
常時接続機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない 無通信監視タイム 60 秒 課金単位時間 0
接続先ネットワーク名	Internet
接続先名	ISP-1
アドレス変換	<input type="radio"/> 使用しない <input checked="" type="radio"/> マルチNAT UPnP機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
MP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
かんたんフィルタ	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

#### 4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に、通信できる状態になります。

#### ⚠注意

本装置は、10BASE-Tポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、またはLANの利用条件によって、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。

## インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

#### 1. WWWブラウザでURL「http://www.omron.co.jp/」を入力します。

インターネットに接続できた場合は、弊社のページが表示されます。



## ◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	オプション設定での設定変更
自動ダイヤル	使用する	×
すべてのデータ通信の着信	許可しない	×
常時接続機能	使用しない	○
無通信監視タイマ	60秒	○
課金単位時間	なし	○
接続ネットワーク名	internet	○
接続先名	ISP-1	○
接続先のサブアドレス	なし	×
DHCPサーバ機能 ・ 割り当て先頭IPアドレス ・ 割り当てアドレス数 ・ DNSサーバのIPアドレス	使用する 本装置のIPアドレス、ネットマスクから求めたネットワークアドレス+2 64 「自動取得（※1）」指定時は、本装置のIPアドレス	×
アドレス変換	マルチNATを使用 アドレス割り当てタイマ：5分	○
UPnP機能	使用しない	○
MP機能（※2）	使用しない	○
かんたんフィルタ（※3）	使用する	○
RIP機能 ・ RIP送信（LAN側） ・ RIP受信（LAN側） ・ RIP送信（WAN側） ・ RIP受信（WAN側）	送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・ LAN側 ・ WAN側	なし デフォルトルートを設定する（メトリック値：1）	×
データ圧縮	LZS：なし	×
ヘッダ圧縮	VJ-Compression：使用する IPヘッダ圧縮：使用しない	×
IPv6経路	使用しない	×
ブリッジ	使用しない	×
課金制御	上限 3,000円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

※1) DNS サーバのIPアドレスを「自動取得」にした場合は、ProxyDNS情報が以下のように設定されます。

「順引き情報一覧」

- 優先順位 : 1
- ドメイン : \*
- タイプ : すべて
- 送信元IPアドレス/マスク : any
- 動作 : 接続先のDNSサーバへ問い合わせる
- ネットワーク名 : internet

「逆引き情報一覧」

- 優先順位 : 1
- ネットワークアドレス : any
- 動作 : 接続先のDNSサーバへ問い合わせる
- ネットワーク名 : internet

※2) MP機能を「使用する(自動)」にした場合は、以下のように設定されます。

- トラフィックによる増減 : する
- 回線増加条件 : 回線使用率(90%)、猶予時間(10秒)
- 回線削除条件 : 回線使用率(40%)、猶予時間(60秒)

※3) かんたんフィルタを「使用する」にした場合は、以下のように設定されます。

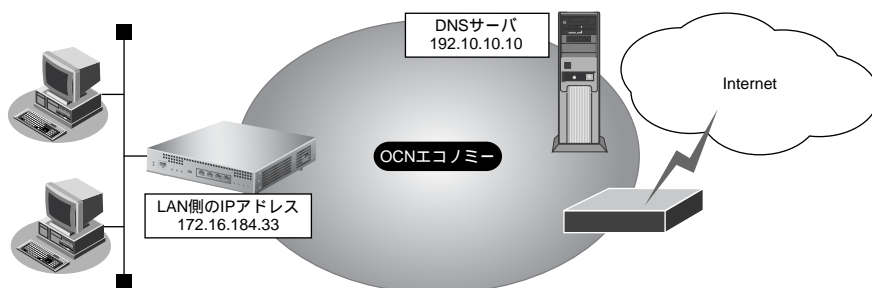
- トラフィックによる増減 : する
- Windows<sup>®</sup> 95 / 98 / Me / 2000、Windows NT<sup>®</sup> でMicrosoft Networkを使用する場合に、NetBIOS over TCPが使用するTCPおよびUDPのサービスポート137から139を遮断するフィルタを設定します。
- ping (ICMP echo) やsyslog、time、SNTPで使用するプロトコルを抑止するフィルタを設定します。なお、回線が接続状態の場合はそれぞれのパケットを通過させます。
- Windows<sup>®</sup> 2000から本装置を経由してインターネットへ接続する場合、Windows<sup>®</sup> 2000が送信する予期しないDNSパケットによって自動発信してしまう場合があります。この問題を回避するために、ProxyDNS情報に問い合わせタイプがSOA(6)、SRV(33)のDNSパケットを破棄するフィルタ、およびホストデータベース情報にIPアドレス「127.0.0.1」でホスト名「localhost」の情報を設定します。

## 1.1.6 インターネットへ専用線接続する

インターネットへ専用線接続するときは、「かんたん設定」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- 接続ネットワーク名称の設定
- 契約時に指示されたドメイン名の設定
- アドレス変換の設定

ここでは、以下の条件で OCN エコノミーを利用する場合を例に説明します。



### ● 設定条件

- OCN エコノミー専用線（128Kbps）を使用する
- 新規にLANを構築する
- OCN 側の DNS サーバを使用 : 192.10.10.10
- OCN より提示されたドメイン名 : domain.ocn.ne.jp
- 接続するパソコンの台数は OCN より割り当てられた IP アドレスよりも少ない
- 割当て IP アドレス
 

ネットワークアドレス	: 172.16.184.32/29
本装置の IP アドレス	: 172.16.184.33
ホストアドレス	: 172.16.184.34 ~ 172.16.184.38
ブロードキャストアドレス	: 172.16.184.39

### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)
- 本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。
- 本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。
- 本装置の IP アドレスに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。

## 1. かんたん設定メニューでインターネットへの「専用線接続」をクリックします。

「インターネットへ専用線接続かんたん設定」ページが表示されます。

## 2. 「必須設定」で以下の項目を指定します。

- IPアドレス → 172.16.184.33 (割り当てられたホストアドレスの先頭)
- ネットマスク → 29 (255.255.255.248)
- 使用する回線速度 → 128Kbps
- DNSサーバ → 192.10.10.10 (OCNから提示されたIPアドレス)

■必須設定	
IPアドレス	172.16.184.33
ネットマスク	29 (255.255.255.248)
使用する回線速度	<input type="radio"/> 64Kbps <input checked="" type="radio"/> 128Kbps
DNSサーバ	192.10.10.10

## 3. 必要に応じて、「オプション設定」で以下の項目を指定します。

- 接続ネットワーク名 → internet (接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するため任意の名称を指定します。)
- ドメイン名 → domain.ocn.ne.jp (OCNより提示されたドメイン名)
- アドレス変換  
アドレス個数 → 初期値は“使用しない”。  
→アドレス変換で“マルチNAT”を指定した場合は、グローバルアドレスの個数を指定します。



この例のように割り当てられたIPアドレスよりも接続するパソコンの台数が同数または少ない場合、“使用しない”を選択します。割り当てられたIPアドレスより接続するパソコンの台数が多い場合は、“マルチNAT”を選択すると、すべてのパソコンがインターネットを利用できます。その際は、「グローバルアドレス」と「アドレス個数」を設定します。

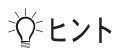
UPnP 機能

→ UPnP 対応装置や UPnP 対応アプリケーションプログラムを使用する場合は“使用する”を選択します。

■オプション設定	
接続ネットワーク名	internet
接続先名	ISP-1
ドメイン名	domain.ocn.ne.jp
アドレス変換	<input checked="" type="radio"/> 使用しない <input type="radio"/> マルチNAT
	グローバルアドレス <input type="text"/>
	アドレス個数 <input type="text"/> 個
	UPnP機能 <input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する

## 4. 設定が終了したら、[設定終了] ボタンをクリックします。

再起動後に、通信できる状態になります。



### ◆ OCN エコノミーなら「マルチ NAT」機能が便利

OCN エコノミーの契約時に割り当てられた IP アドレスの個数より、パソコンの台数が多い場合は、本装置の「マルチ NAT 機能」が便利です。「マルチ NAT 機能」によって、実際に割り当てられた IP アドレスの数を上回る台数の LAN 上のパソコンでインターネットを利用できるようになります。

### ◆ マルチ NAT

本装置では、インターネットを利用する際に、プロバイダより割り当てられた IP アドレス（グローバルアドレス）と、ネットワーク上で設定した IP アドレス（プライベートアドレス）を対応付けることによって、従来のネットワークの設定を変更することなくインターネット接続ができるアドレス変換（NAT）機能をサポートしています。

NAT 機能は、プライベートアドレスとグローバルアドレスを 1 対 1 に対応付けるもので、NAT 機能を介して通信できるパソコンの台数は割り当てられる IP アドレスと同じになります。このため、プロバイダと端末型ダイヤルアップ契約の場合、1 つしか IP アドレスが割り当てられないので、同時接続台数が 1 台に制限されます。

マルチ NAT は、この問題を解決するために 1 対 1 の対応付けから、多対 1 の対応付けを実現した機能です。IP アドレスとポート番号を組み合わせた IP 情報の割り当てを行うことによって、プライベートアドレスとグローバルアドレスとを多対 1 に対応付け、同時に複数のパソコンからの利用が可能となります。

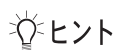
☞ 参照 「マルチ NAT 機能（アドレス変換機能）を使う」（P.473）

## インターネットに接続できることを確認する

設定が終わったら、インターネットに接続できるかどうかを確認します。

### 1. WWW ブラウザで URL 「<http://www.omron.co.jp/>」を入力します。

インターネットに接続できた場合は、弊社のページが表示されます。



## ◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	オプション設定での設定変更
ブロードキャストアドレス	ネットワークドレス+オール1	×
接続ネットワーク名	internet	○
DHCPサーバ機能 ・ 割り当て先頭IP アドレス ・ 割り当てアドレス数	使用する 本装置のIPアドレス、ネットマスクから求めたネットワークアドレス+2 64	×
NAT 機能	使用しない (※ 1)	○
UPnP機能	使用しない	○
かんたんフィルタ	使用しない	×
RIP 機能 ・ RIP 送信 (LAN 側) ・ RIP 受信 (LAN 側) ・ RIP 送信 (WAN 側) ・ RIP 受信 (WAN 側)	送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・ LAN 側 ・ WAN 側	なし デフォルトルートを設定する (メトリック値：1)	×
データ圧縮	LZS：なし	×
ヘッダ圧縮	VJ-Compression : 使用する IPヘッダ圧縮 : 使用しない	×
IPv6経路	使用しない	×
ブリッジ	使用しない	×

※ 1) マルチ NAT 使用時のアドレス割り当てタイムは 5 分を設定します。



## 1.1.7 オフィスへISDN接続する

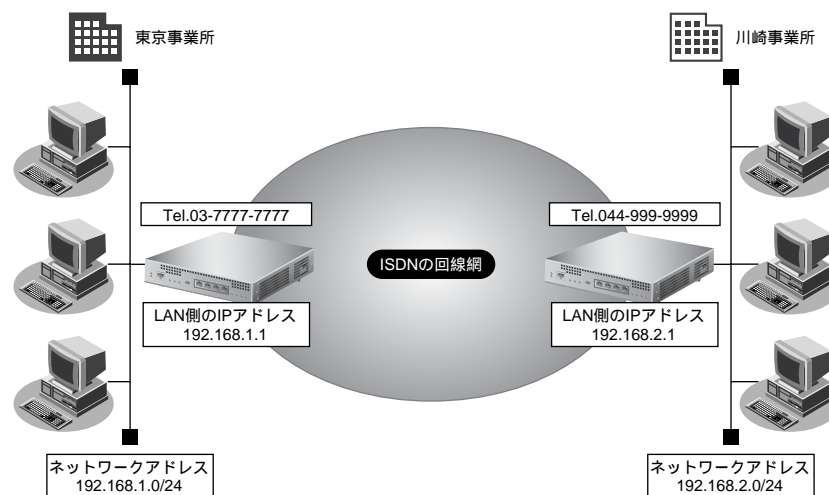
事業所 LAN どうしを ISDN で接続するときは、「かんたん設定メニュー」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- DHCP サーバ機能の設定
- ISDN 回線を自動切断するまでの時間の変更（無通信監視タイマ）
- 回線の切断タイミングの調整（課金単位時間）
- 接続ネットワーク名と接続先名の設定
- データの転送速度を早くする（MP-Multilink PPP）
- 送受信するヘッダの圧縮

ここでは、ISDN 回線を介して 2 つの事業所（東京、川崎）のネットワークを接続する場合を例に説明します。



「詳細設定」で設定する場合や基幹ネットワーク（大規模ネットワーク）に接続する場合は、「[事業所 LAN を ISDN で接続する](#)」(P.73) を参照してください。



### ● 設定条件

- DHCP サーバ機能は使用しない

#### 【東京事業所】

- 電話番号 : 03-7777-7777
- ユーザ認証IDとユーザ認証パスワード
  - 発信 : tokyo, tokyopass
  - 着信 : kawasaki, kawapass
- LAN 側のネットワークアドレス/ネットマスク : 192.168.1.0/24（本装置のIPアドレス : 192.168.1.1）

#### 【川崎事業所】

- 電話番号 : 044-999-9999
- ユーザ認証IDとユーザ認証パスワード
  - 発信 : kawasaki, kawapass
  - 着信 : tokyo, tokyopass
- LAN 側のネットワークアドレス/ネットマスク : 192.168.2.0/24（本装置のIPアドレス : 192.168.2.1）

### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Webユーザズガイド「文字入力フィールドで入力できる文字一覧」(P.13)
- 本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンのIPアドレスの変更（再起動）およびURLを変更する必要があります。
- 本装置を既存のLANに接続する場合は、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。

## 東京事業所の本装置を設定する

### 1. かんたん設定でオフィスへの「ISDN接続」をクリックします。

「オフィスへISDN接続かんたん設定」ページが表示されます。

### 2. 「必須設定」で以下の項目を指定します。

- 接続先の電話番号 → 044-999-9999
- ユーザ認証ID（発信） → tokyo
- ユーザ認証パスワード（発信） → tokyopass
- ユーザ認証ID（着信） → kawasaki
- ユーザ認証パスワード（着信） → kawapass
- IPアドレス → 192.168.1.1（既存のLANにつなぐときは適宜変更）
- ネットマスク → 24（255.255.255.0）（既存のLANにつなぐときは適宜変更）
- 相手ルータのIPアドレス → 192.168.2.1（接続先となる本装置のネットワークアドレス）
- 相手ルータのネットマスク → 24（255.255.255.0）（接続先となる本装置のネットマスク）

■必須設定	
接続先の電話番号	044-999-9999
ユーザ認証ID(発信)	tokyo
ユーザ認証パスワード(発信)	*****
ユーザ認証ID(着信)	kawasaki
ユーザ認証パスワード(着信)	*****
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
相手ルータのIPアドレス	192.168.2.1
相手ルータのネットマスク	24 (255.255.255.0)

### 3. 「オプション設定」で以下の項目を指定します。

- DHCPサーバ → 使用しない
- 接続ネットワーク名 → kaisya (接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するため任意の名称を指定します。)
- 接続先名 → kawasaki (接続先の名称を半角英数字8文字以内で入力します。接続先を区別するための任意の名称を指定します。)


■ オプション設定	
DHCPサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する DNSサーバ広報 <input type="text"/>
常時接続機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない 無通信監視タイム <input type="text"/> 秒 課金単位時間 <input type="text"/> .0
接続ネットワーク名	<input type="text" value="kaisya"/>
接続先名	<input type="text" value="kawasaki"/>
MP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
ヘッダ圧縮	<input checked="" type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
データ圧縮	<input type="checkbox"/> LZS

### 4. 設定が終了したら、「設定終了」ボタンをクリックします。

再起動後に、通信できる状態になります。

## 川崎事業所の本装置を設定する

「東京事業所の本装置を設定する」を参考に、川崎事業所の本装置を設定します。その際、特に指定のないものは、東京事業所と同じ設定にします。

 設定が終わったら、「設定終了」ボタンをクリックします。

#### 「必須設定」

- 接続先の電話番号 → 03-7777-7777
- ユーザ認証ID (発信) → kawasaki
- ユーザ認証パスワード (発信) → kawapass
- ユーザ認証ID (着信) → tokyo
- ユーザ認証パスワード (着信) → tokyopass
- IPアドレス → 192.168.2.1 (本装置のLAN側のIPアドレス)
- ネットマスク → 24 (255.255.255.0)
- 相手ルータのIPアドレス → 192.168.1.1 (接続先となる本装置のネットワークアドレス)
- 相手ルータのネットマスク → 24 (255.255.255.0) (接続先となる本装置のネットマスク)

#### 「オプション設定」

- 接続ネットワーク名 → kaisya (接続するネットワークの名称)
- 接続先名 → tokyo

## 通信する

---

WWW ブラウザや電子メールソフトなどの通信用アプリケーションを起動しておきます。通信が必要な状態になると、本装置が自動的に回線を接続します。

### 注意

**本装置は、10BASE-Tポートに接続したパソコンからの要求によって、自動的にダイヤル発信を行い、回線を接続します。そのため、お客様がお使いになる機器、ソフトウェア、またはLANの利用条件により、不要なダイヤル発信が行われ、回線が接続されてしまう場合があります。本装置の表示メニューで、課金情報を定期的にチェックしてください。**

---



「かんたん設定」で設定した初期設定の状態では、約60秒間データの送受信が行われない場合、自動的に回線を切断します。



## ◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可


項目	適用される省略値	オプション設定での設定変更
自動ダイヤル	使用する	×
サブアドレス	なし	×
不特定相手着信	許可しない	×
常時接続機能	使用しない	○
無通信監視タイマ	60秒	○
課金単位時間	なし	○
接続ネットワーク名	localnet	○
接続先名	OFFICE-1	○
該当接続先への着信許可	許可する	×
DHCPサーバ機能 ・ 割り当て先頭IPアドレス ・ 割り当てアドレス数	使用する 本装置のIPアドレス、ネットマスクから求めたネットワークアドレス+2 64	○
NAT 機能	使用しない	×
MP 機能	使用しない	○
かんたんフィルタ	使用しない	×
RIP 機能 ・ RIP 送信 (LAN 側) ・ RIP 受信 (LAN 側) ・ RIP 送信 (WAN 側) ・ RIP 受信 (WAN 側)	送信しない 受信しない 送信しない 受信しない	×
スタティック経路 ・ LAN 側 ・ WAN 側	なし 相手ルータのIPアドレス、ネットマスクを元にスタティックルートを設定する	×
データ圧縮	LZS：なし	○
ヘッダ圧縮	VJ-Compression：使用する IPヘッダ圧縮：使用しない	○
IPv6経路	使用しない	×
ブリッジ	使用しない	×
課金制御	上限 3,000円	×
スケジュール	毎週金曜日 00:00 に課金情報クリア	×

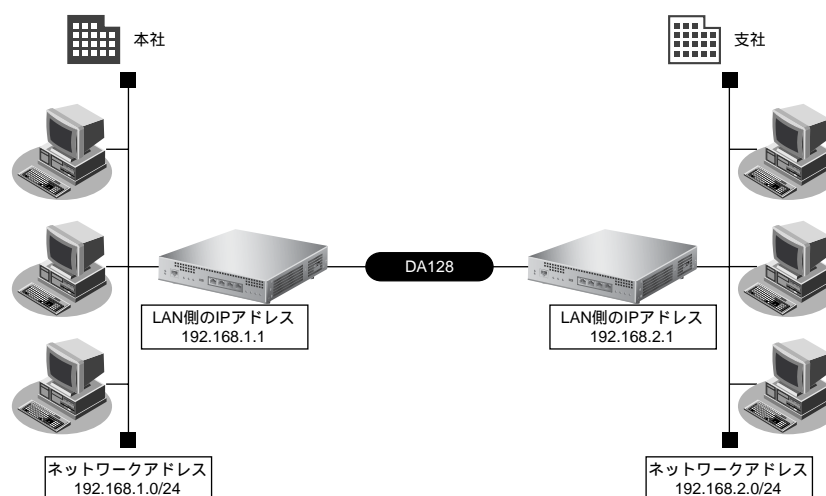
## 1.1.8 オフィスへ専用線接続する

事業所 LAN どうしを専用線で接続するときは、「かんたん設定メニュー」で「必須設定」の情報を設定するだけで接続できます。また、「オプション設定」の情報を設定すると、以下のことができます。

- 接続ネットワーク名の設定
- DHCPサーバ機能の設定
- 送受信するヘッダの圧縮

ここでは、専用線（HSD128Kbps）を介して2つの事業所（本社、支社）のネットワークを接続する場合を例に説明します。

 「詳細設定」で設定する場合や基幹ネットワーク（大規模ネットワーク）に接続する場合は、「[事業所 LAN を専用線で接続する](#)」(P.79) を参照してください。



### ● 設定条件

#### 【本社】

- 専用線（128Kbps）を使用する
- DHCPサーバ機能は使用しない
- アドレス変換は使用しない
- LAN側のネットワークアドレス／ネットマスク : 192.168.1.0/24
- 本装置のIPアドレス : 192.168.1.1

#### 【支社】

- LAN側のネットワークアドレス／ネットマスク : 192.168.2.0/24
- 本装置のIPアドレス : 192.168.2.1

### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)
- 本装置の IP アドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンの IP アドレスの変更（再起動）および URL を変更する必要があります。
- 本装置を既存の LAN に接続する場合は、LAN 上のほかのホストと IP アドレスが重複しないように適切な IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」が設定されています。

## 本社の本装置を設定する

### 1. かんたん設定でオフィスへの「専用線接続」をクリックします。

「オフィスへ専用線接続かんたん設定」ページが表示されます。

### 2. 「必須設定」で以下の項目を指定します。

- IP アドレス → 192.168.1.1（既存の LAN につなぐときは適宜変更）
- ネットマスク → 24 (255.255.255.0)（既存の LAN につなぐときは適宜変更）
- 相手ルータの IP アドレス → 192.168.2.1（接続先となる本装置の IP アドレス）
- 相手ルータのネットマスク → 24 (255.255.255.0)（接続先となる本装置のネットマスク）
- 使用する回線速度 → 128Kbps

■必須設定	
IPアドレス	192.168.1.1
ネットマスク	24 (255.255.255.0)
相手ルータのIPアドレス	192.168.2.1
相手ルータのネットマスク	24 (255.255.255.0)
使用する回線速度	<input type="radio"/> 64Kbps <input checked="" type="radio"/> 128Kbps

### 3. 「オプション設定」で以下の項目を指定します。

- 接続ネットワーク名 → kaisya（接続するネットワークの名称を半角英数字8文字以内で入力します。接続先を区別するため任意の名称を指定します。）
- DHCPサーバ → 使用しない

■オプション設定	
接続ネットワーク名	kaisya
接続先名	kawasaki
DHCPサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する DNSサーバ広報 <input type="text"/>
ヘッダ圧縮	<input checked="" type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
データ圧縮	<input type="checkbox"/> LZS

### 4. 設定が終了したら、「設定終了」ボタンをクリックします。

再起動後に、通信できる状態になります。

## 支社の本装置を設定する

「本社の本装置を設定する」を参考に、支社の本装置を設定します。その際、特に指定のないものは、本社と同じ設定にします。



設定が終わったら、「設定終了」ボタンをクリックします。

### 「必須設定」

- IPアドレス → 192.168.2.1 (本装置のLAN側のIPアドレス)
- ネットマスク → 24 (255.255.255.0)
- 相手ルータのIPアドレス → 192.168.1.1 (接続先となる本装置のIPアドレス)
- 相手ルータのネットマスク → 24 (255.255.255.0) (接続先となる本装置のネットマスク)
- 使用する回線速度 → 128Kbps

### 「オプション設定」

- 接続ネットワーク名 → kaisya (接続するネットワークの名称)
- DHCPサーバ → 使用しない



### ヒント

#### ◆ 省略値について

かんたん設定時に適用される主な省略値を示します。

○：変更可能、×：変更不可

項目	適用される省略値	オプション設定での設定変更
接続ネットワーク名	localnet	○
DHCPサーバ機能	使用する	○
・割り当て先頭アドレス	本装置のIPアドレス、ネットマスクから求めたネットワークアドレス+2	
・割り当てアドレス数	64	
NAT機能	使用しない	×
かんたんフィルタ	使用しない	×
RIP機能		×
・RIP送信 (LAN側)	送信しない	
・RIP受信 (LAN側)	受信しない	
・RIP送信 (WAN側)	送信しない	
・RIP受信 (WAN側)	受信しない	
スタティック経路		×
・LAN側	なし	
・WAN側	相手ルータのIPアドレス、ネットマスクを元にスタティックルートを設定する	
データ圧縮	LZS：なし	○
ヘッダ圧縮	VJ-Compression : 使用する IPヘッダ圧縮 : 使用しない	○
IPv6経路	使用しない	×
ブリッジ	使用しない	×



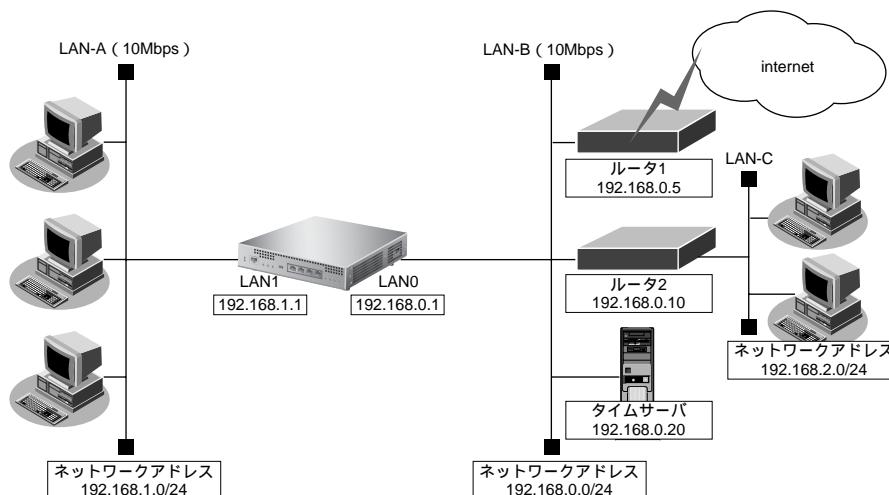
## 1.2 LAN をネットワーク間接続する

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 MR1000 トラブルシューティング「ご購入時の状態に戻すには」(P.42)



### ● 設定条件

#### [LAN-A 側]

- 転送レートは自動認識
- 本装置の LAN1 側の 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
- DHCP 機能を使用する
- NAT を使用しない

#### [LAN-B 側]

- 転送レートは自動認識
- 本装置の LAN0 側の IP アドレス : 192.168.0.1
- ネットワークアドレス/ネットマスク : 192.168.0.0/24
- DHCP 機能を使用しない
- ルーティングプロトコルとして RIP-V1 を使用する
- インターネットにつながるルータ 1 と、事業所内のその他のネットワークにつながるルータ 2 が存在し、静的に経路情報を登録する
  - ルータ 1 の IP アドレス : 192.168.0.5
  - 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/ネットマスク : 192.168.2.0/24
- NAT は使用しない

**【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付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。「LAN1 情報を設定する」場合は、あらかじめ物理 LAN1 定義を追加する必要があります。

**LAN0 情報を設定する**

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. 以下の項目を指定します。
 

• IPv4	→ 使用する
• IP アドレス	→ 指定する
IP アドレス	→ 192.168.0.1
ネットマスク	→ 24 (255.255.255.0)
ブロードキャストアドレス	→ ネットワークアドレス + オール 1

5. [保存] ボタンをクリックします。
6. IP 関連の設定項目の「RIP 情報」をクリックします。  
「RIP 情報」が表示されます。

## 7. 以下の項目を指定します。

- RIP送信 → V1で送信する
- RIP受信 → V1で受信する
- メトリック値 → 0

■RIP情報	
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	0

## 8. [保存] ボタンをクリックします。

## 9. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

## 10. 以下の項目を指定します。

- ネットワーク → デフォルトルート  
中継ルータアドレス → 192.168.0.5
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input checked="" type="radio"/> デフォルトルート 中継ルータアドレス <input type="text" value="192.168.0.5"/>
	<input type="radio"/> ネットワーク指定 あて先IPアドレス <input type="text"/>
	あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
	中継ルータアドレス <input type="text"/>
メトリック値	1
優先度	0

## 11. [追加] ボタンをクリックします。

## 12. 以下の項目を指定します。

- ネットワーク → ネットワーク指定  
   あて先IPアドレス → 192.168.2.0  
   あて先アドレスマスク → 24 (255.255.255.0)  
   中継ルータアドレス → 192.168.0.10
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート 中継ルータアドレス <input type="text"/>
	<input checked="" type="radio"/> ネットワーク指定 あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/> 中継ルータアドレス <input type="text" value="192.168.0.10"/>
	メトリック値 <input type="text" value="1"/>
	優先度 <input type="text" value="0"/>

## 13. [追加] ボタンをクリックします。

## 14. IP関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

## 15. 以下の項目を指定します。

- DHCP 機能 → 使用しない

■ DHCP情報		
DHCP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> リレー機能を使用する DHCPサーバIPアドレス1 <input type="text"/> DHCPサーバIPアドレス2 <input type="text"/>	
	<input type="radio"/> サーバ機能を使用する 割当て先頭IPアドレス <input type="text"/> 割当てアドレス数 <input type="text" value="32"/> リース期間 <input type="text" value="1"/> 日 デフォルトルータ広報 <input type="text"/> DNSサーバ広報 <input type="text"/> セカンダリDNSサーバ広報 <input type="text"/> ドメイン名広報 <input type="text"/>	
	※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。	

## 16. [保存] ボタンをクリックします。

## LAN1 情報を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN1 の【修正】 ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 4. 以下の項目を指定します。

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス → 192.168.1.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス + オール1

■IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IPアドレス	192.168.1.1
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス + オール1

### 5. 【保存】 ボタンをクリックします。

### 6. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

### 7. 以下の項目を指定します。

- RIP 送信 → V1 で送信する
- RIP 受信 → V1 で受信する
- メトリック値 → 0

■RIP情報	
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	0

### 8. 【保存】 ボタンをクリックします。

**9. IP関連の設定項目の「DHCP情報」をクリックします。**

「DHCP情報」が表示されます。

**10. 以下の項目を指定します。**

- DHCP機能 →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
- DNSサーバ広報 →192.168.1.1
- セカンダリDNSサーバ広報 →指定しない
- ドメイン名広報 →指定しない

■DHCP情報	
DHCP機能	<input type="radio"/> 使用しない
	<input type="radio"/> リレー機能を使用する
	DHCPサーバIPアドレス1 <input type="text"/>
	DHCPサーバIPアドレス2 <input type="text"/>
	<input checked="" type="radio"/> サーバ機能を使用する
	割当て先頭IPアドレス <input type="text" value="192.168.1.2"/>
	割当てアドレス数 <input type="text" value="253"/>
	リース期間 <input type="text" value="1"/> 日
	デフォルトルータ広報 <input type="text" value="192.168.1.1"/>
	DNSサーバ広報 <input type="text" value="192.168.1.1"/>
セカンダリDNSサーバ広報 <input type="text"/>	
ドメイン名広報 <input type="text"/>	
※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。	

**11. [保存] ボタンをクリックします。**

## 自動時刻を設定する

1. 設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

2. 「タイムサーバ情報」をクリックします。

「タイムサーバ情報」が表示されます。

3. 以下の項目を指定します。

- タイムサーバ機能 → 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IPアドレス → 192.168.0.20

■タイムサーバ情報	
タイムサーバ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
サーバ設定	<input type="radio"/> DHCPで取得する ※IPv4のDHCPクライアントの設定が必要です。
	<input checked="" type="radio"/> 設定する
	プロトコル <input checked="" type="radio"/> TIMEプロトコル <input type="radio"/> SNTPプロトコル
タイムサーバIPアドレス	192.168.0.20
自動時刻設定 間隔	<input type="text"/> 日

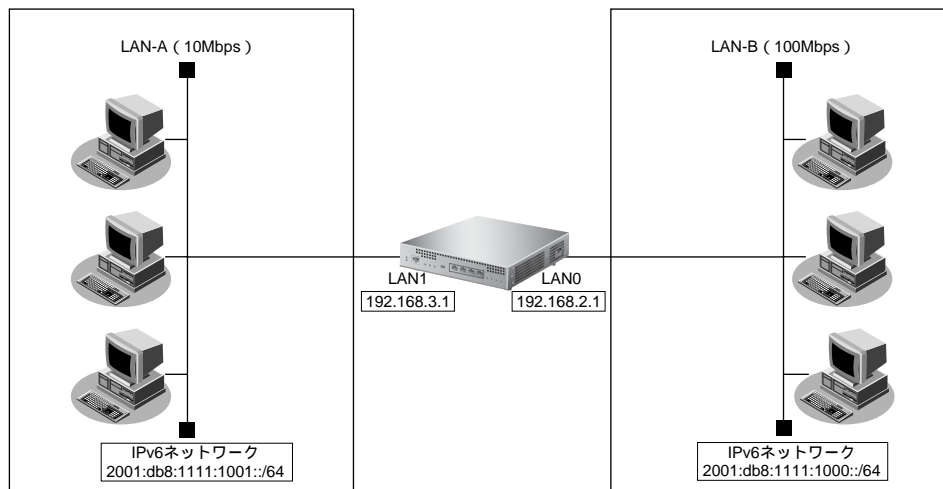
4. [保存] ボタンをクリックします。

5. 画面左側の [設定反映] 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。

## 1.3 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]

- プレフィックス/プレフィックス長 : 2001:db8:1111:1001::/64

#### [LAN-B 側]

- プレフィックス/プレフィックス長 : 2001:db8:1111:1000::/64

#### こんな事に気をつけて

文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

## LAN0 情報を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

### 3. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。



#### 4. 以下の項目を指定します。

- IPv6 →使用する
- インタフェースID →自動
- IPv6 アドレス  
アドレスまたはプレフィックス →2001:db8:1111:1000::
- ルータ広報 →送信する

IPv6基本情報				
IPv6	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する			
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>			
	アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限	Pref. Lifetime 期限有 無期限	フラグ
IPv6 アド レス	<input type="text" value="2001:db8:1111:1000::"/>	<input type="text" value="30"/> 日 <input type="checkbox"/>	<input type="text" value="7"/> 日 <input type="checkbox"/>	<input type="text" value="00"/>
	<input type="text"/>	<input type="text" value="30"/> 日 <input type="checkbox"/>	<input type="text" value="7"/> 日 <input type="checkbox"/>	<input type="text" value="00"/>
	<input type="text"/>	<input type="text" value="30"/> 日 <input type="checkbox"/>	<input type="text" value="7"/> 日 <input type="checkbox"/>	<input type="text" value="00"/>
	<input type="text"/>	<input type="text" value="30"/> 日 <input type="checkbox"/>	<input type="text" value="7"/> 日 <input type="checkbox"/>	<input type="text" value="00"/>
ルー タ 広 報	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する			
	最大送信間隔	<input type="text" value="600"/> 秒		
	最小送信間隔	<input type="text" value="200"/> 秒		
	Router Lifetime	<input type="text" value="1800"/> 秒		
	MTU	<input type="text"/>		
	Reachable Time	<input type="text" value="0"/> ミリ秒		
	Retrans Timer	<input type="text" value="0"/> ミリ秒		
	Cur Hop Limit	<input type="text" value="64"/>		
	フラグ	<input type="text" value="00"/>		

#### 5. [保存] ボタンをクリックします。

#### 6. IPv6 関連の設定項目の「IPv6 RIP 情報」をクリックします。

「IPv6 RIP情報」が表示されます。

## 7. 以下の項目を指定します。

- RIP送信 →送信する
- RIP受信 →受信する
- サイトローカルプレフィックス →交換する

IPv6 RIP情報											
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する メトリック値 <input type="text" value="0"/>										
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> 受信する										
集約経路送信	<table border="1"> <thead> <tr> <th>集約経路</th> <th>破棄経路設定</th> </tr> </thead> <tbody> <tr> <td> <input type="radio"/> デフォルトルート  <input checked="" type="radio"/> ネットワーク指定  <input type="text"/> </td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> </tbody> </table>	集約経路	破棄経路設定	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する
	集約経路	破棄経路設定									
	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する									
	<input type="text"/>	<input checked="" type="checkbox"/> 設定する									
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
サイトローカルプレフィックス	<input type="radio"/> 交換しない <input checked="" type="radio"/> 交換する										

## 8. [保存] ボタンをクリックします。

## LAN1 情報を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースがLAN1の [修正] ボタンをクリックします。

「LAN1情報 (物理 LAN)」ページが表示されます。

### 3. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

#### 4. 以下の項目を指定します。

- IPv6 →使用する
- インタフェースID →自動
- IPv6 アドレス  
アドレスまたはプレフィックス →2001:db8:1111:1001::
- ルータ広報 →送信する

IPv6基本情報						
IPv6	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する					
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>					
IPv6 アド レス	アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限		Pref. Lifetime 期限有 無期限	フラ グ	
	2001:db8:1111:1001::	30	日	7	日	e0
	<input type="text"/>	30	日	7	日	e0
	<input type="text"/>	30	日	7	日	e0
ルー タ 広 報	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する					
	最大送信間隔	600	秒			
	最小送信間隔	200	秒			
	Router Lifetime	1800	秒			
	MTU	<input type="text"/>				
	Reachable Time	0	ミリ秒			
	Retrans Timer	0	ミリ秒			
	Cur Hop Limit	64				
フラグ	00					

#### 5. [保存] ボタンをクリックします。

#### 6. IPv6 関連の設定項目の「IPv6 RIP 情報」をクリックします。

「IPv6 RIP情報」が表示されます。

## 7. 以下の項目を指定します。

- RIP送信 →送信する
- RIP受信 →受信する
- サイトローカルプレフィックス →交換する

IPv6 RIP情報											
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する メトリック値 <input type="text" value="0"/>										
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> 受信する										
集約経路送信	<table border="1"> <thead> <tr> <th>集約経路</th> <th>破棄経路設定</th> </tr> </thead> <tbody> <tr> <td> <input type="radio"/> デフォルトルート  <input checked="" type="radio"/> ネットワーク指定  <input type="text"/> </td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> <tr> <td><input type="text"/></td> <td><input checked="" type="checkbox"/> 設定する</td> </tr> </tbody> </table>	集約経路	破棄経路設定	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する	<input type="text"/>	<input checked="" type="checkbox"/> 設定する
	集約経路	破棄経路設定									
	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定 <input type="text"/>	<input checked="" type="checkbox"/> 設定する									
	<input type="text"/>	<input checked="" type="checkbox"/> 設定する									
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
<input type="text"/>	<input checked="" type="checkbox"/> 設定する										
サイトローカルプレフィックス	<input type="radio"/> 交換しない <input checked="" type="radio"/> 交換する										

## 8. [保存] ボタンをクリックします。

## 9. 画面左側の [設定反映] 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。

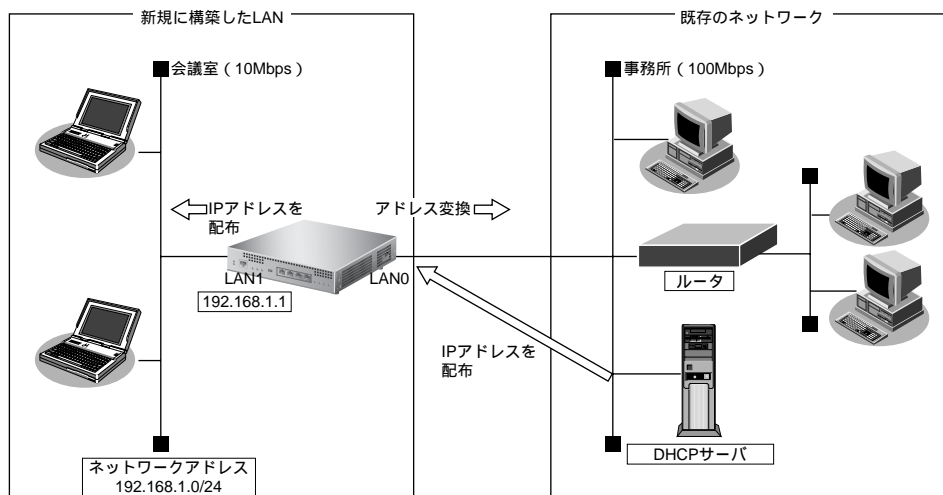
## 1.4 プライベートLANを構築する

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 MR1000 トラブルシューティング 「ご購入時の状態に戻すには」 (P.42)



### ● 設定条件

#### 【事務所側 LAN】

- 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 : 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
  - アドレス個数 : 1
  - アドレス割当てタイム : 5 分

#### 【会議室側 LAN】

- LAN1 ポートを使用する
- 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
  - DNS サーバ広報 : 192.168.1.1

**こんな事に気をつけて**

- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

- 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。

**LAN0 情報を設定する****1. 設定メニューのルータ設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。**

「LAN0 情報（物理 LAN）」ページが表示されます。

**3. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**4. 以下の項目を指定します。**

- IPv4 → 使用する
- IP アドレス → DHCP で自動的に取得する

■ IPアドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPアドレス	<input checked="" type="radio"/> DHCPで自動的に取得する
	<input type="radio"/> 指定する
	IPアドレス <input type="text"/>
ネットマスク	2 (192.0.0.0)
ブロードキャストアドレス	0.0.0.0

**5. 【保存】 ボタンをクリックします。****6. IP 関連の設定項目の「RIP 情報」をクリックします。**

「RIP 情報」が表示されます。

## 7. 以下の項目を指定します。

- RIP送信 →送信しない
- RIP受信 →V1 で受信する
- メトリック値 →0

■RIP情報	
RIP送信	<input checked="" type="radio"/> 送信しない <input type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	0

## 8. [保存] ボタンをクリックします。

## 9. IP関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

## 10. 以下の項目を指定します。

- NATの使用 →マルチ NAT
- グローバルアドレス →指定しない
- アドレス個数 →1
- アドレス割当てタイム →5分
- NATセキュリティ →高い

■NAT情報	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ ※NATの使用とDHCPリレーサービスの併用はできません
グローバルアドレス	
アドレス個数	1 個
アドレス割当てタイム	5 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsecパススルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

## 11. [保存] ボタンをクリックします。

## LAN1 情報を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 以下の項目を指定します。

- インタフェース →物理 LAN

<LAN情報追加フィールド>	
インタフェース	物理LAN ▼

### 3. [追加] ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。

### 4. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 5. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →192.168.1.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

<b>■ IPアドレス情報</b>		
<b>IPv4</b>	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
<b>IPアドレス</b>	<input type="radio"/> DHCPで自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IPアドレス	192.168.1.1
	ネットマスク	24 (255.255.255.0) ▼
	ブロードキャストアドレス	ネットワークアドレス+オール1 ▼

### 6. [保存] ボタンをクリックします。

### 7. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。



## 8. 以下の項目を指定します。

- DHCP機能 →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
- DNSサーバ広報 → 192.168.1.1
- セカンダリDNSサーバ広報 → 指定しない
- ドメイン名広報 → 指定しない

DHCP情報	
DHCP 機能	<input type="radio"/> 使用しない
	<input checked="" type="radio"/> リレー機能を使用する
	DHCPサーバIPアドレス1 <input type="text"/>
	DHCPサーバIPアドレス2 <input type="text"/>
	<input checked="" type="radio"/> サーバ機能を使用する
	割当て先頭IPアドレス <input type="text" value="192.168.1.2"/>
	割当てアドレス数 <input type="text" value="253"/>
	リース期間 <input type="text" value="1"/> 日
	デフォルトルータ広報 <input type="text" value="192.168.1.1"/>
	DNSサーバ広報 <input type="text" value="192.168.1.1"/>
セカンダリDNSサーバ広報 <input type="text"/>	
ドメイン名広報 <input type="text"/>	
※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。	

## 9. [保存] ボタンをクリックします。

## 10. IP関連の設定項目の「RIP情報」をクリックします。

「RIP情報」が表示されます。

## 11. 以下の項目を指定します。

- RIP送信 → V1で送信する
- RIP受信 → V1で受信する
- メトリック値 → 0

RIP情報	
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	<input type="text" value="0"/>

## 12. [保存] ボタンをクリックします。

### 13. 画面左側の【設定反映】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、「[DHCP スタティック機能を使う](#)」(P.508) を参考にして、IP アドレスと MAC アドレスを設定してください。
-

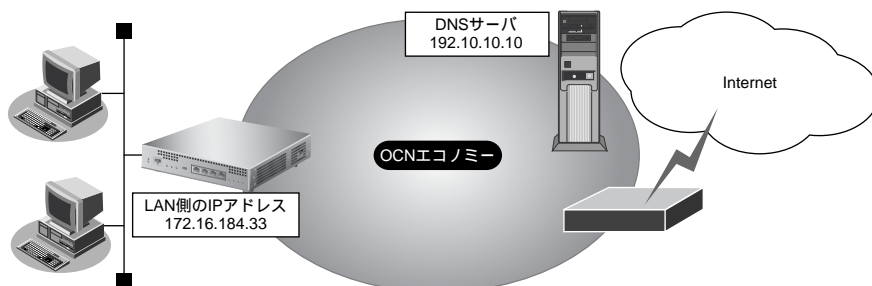
## 1.5 インターネットへ専用線で接続する

ここでは、以下の設定条件で専用線を利用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 MR1000 トラブルシューティング 「ご購入時の状態に戻すには」 (P.42)



### ● 設定条件

- ISDN ポートでOCNエコノミー専用線（128Kbps）を使用する
- LAN0を使用して、新規にLANを構築する
- OCN側のDNSサーバを使用 : 192.10.10.10
- OCNより提示されたドメイン名 : domain.ocn.ne.jp
- 接続するパソコンの台数はOCNから割り当てられたIPアドレスよりも少ない
- 割当てIPアドレス
 

ネットワークアドレス/ネットマスク	: 172.16.184.32/29
ホストアドレス	: 172.16.184.33～172.16.184.38
ブロードキャストアドレス	: 172.16.184.39
本装置のLAN側のIPアドレス	: 172.16.184.33
- 接続ネットワーク名 : internet

### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Webユーザズガイド 「文字入力フィールドで入力できる文字一覧」 (P.13)

- 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。

## WAN0 情報を設定する

1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2. 以下の項目を指定します。

- 回線インタフェース → 専用線

<WAN情報追加フィールド>	
回線インタフェース	専用線

3. [追加] ボタンをクリックします。

「WAN0 情報 (専用線)」ページが表示されます。

4. 「基本情報」をクリックします。

「基本情報」が表示されます。

5. 以下の項目を指定します。

- 回線速度 → 128Kbps

■基本情報	
ポート	基本 0
回線速度	128Kbps

6. [保存] ボタンをクリックします。

## LAN0 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

#### 4. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →172.16.184.33
  - ネットマスク →29 (255.255.255.248)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IPアドレス	172.16.184.33
	ネットマスク	29 (255.255.255.248)
	ブロードキャストアドレス	ネットワークアドレス+オール1

#### 5. [保存] ボタンをクリックします。

#### 6. IP関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

#### 7. 以下の項目を指定します。

- DHCP機能 →サーバ機能を使用する
- 割当て先頭IPアドレス →172.16.184.34
- 割当てアドレス数 →6
- リース期間 →1日
- デフォルトルータ広報 →172.16.184.33
- DNSサーバ広報 →192.10.10.10
- セカンダリDNSサーバ広報 →指定しない
- ドメイン名広報 →domain.ocn.ne.jp

■DHCP情報		
DHCP機能	<input type="radio"/> 使用しない	
	<input checked="" type="radio"/> リレー機能を使用する	
	DHCPサーバIPアドレス1	
	DHCPサーバIPアドレス2	
	<input checked="" type="radio"/> サーバ機能を使用する	
	割当て先頭IPアドレス	172.16.184.34
	割当てアドレス数	6
	リース期間	1 日
	デフォルトルータ広報	172.16.184.33
	DNSサーバ広報	192.10.10.10
セカンダリDNSサーバ広報		
ドメイン名広報	domain.ocn.ne.jp	
※「割当て先頭アドレス」が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。		

#### 8. [保存] ボタンをクリックします。

## 相手情報を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3. 以下の項目を指定します。

- ネットワーク名 → internet

<ネットワーク情報追加フィールド>	
ネットワーク名	internet

4. [追加] ボタンをクリックします。

「ネットワーク情報 (internet)」ページが表示されます。

5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7. 以下の項目を指定します。

- ネットワーク → デフォルトルート
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input checked="" type="radio"/> デフォルトルート
	<input type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text"/>
	あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

8. [追加] ボタンをクリックします。

9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → ISP-1
- 接続先種別 → 専用線接続

<接続先情報追加フィールド>

接続先名	ISP-1		
接続先種別	<input checked="" type="radio"/> 専用線接続		
	<input type="radio"/> ISDN接続		
	ダイヤル1	電話番号	<input type="text"/>
		サブアドレス	<input type="text"/>
	<input type="radio"/> フレームリレー接続		
	DLCI	<input type="text"/>	
	<input type="radio"/> PPPoE接続		
	<input type="radio"/> IPTunnel接続		
	<input type="radio"/> IPsec/IKE接続		
	<input type="radio"/> 別インタフェースから送出		
	<input type="radio"/> MPLSTunnel接続		
	<input type="radio"/> パケット破棄		

## 11. [追加] ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 使用インタフェース → WAN0
- DNSサーバ → 192.10.10.10

■基本情報

接続先名	ISP-1
使用インタフェース	WAN0
DNSサーバ	192.10.10.10

## 13. [保存] ボタンをクリックします。

## 14. 画面左側の [再起動] 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。

こんな事に気をつけて

- 本装置のIPアドレスを変更した場合、再起動後に本装置にアクセスするためには、パソコンのIPアドレスを変更する必要があります。パソコンを再起動してください。
- 本装置を既存のLANに接続する場合は、LAN上のほかのホストとIPアドレスが重複しないように適切なIPアドレスを設定してください。本装置のご購入時のIPアドレスは「192.168.1.1」が設定されています。

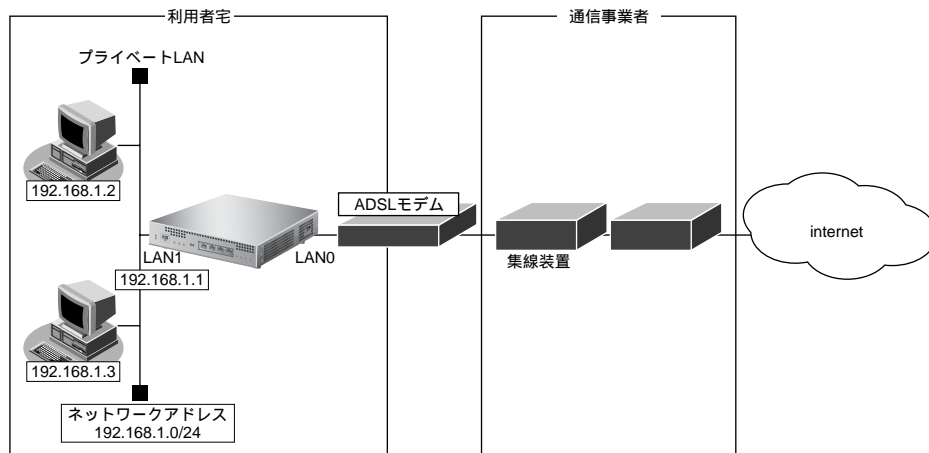
## 1.6 インターネットへPPPoEで接続する

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 MR1000 トラブルシューティング「ご購入時の状態に戻すには」(P.42)



### ● 設定条件

#### 【通信事業者側】

- 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)
- LAN0ポートを使用する

#### 【プライベートLAN側】

- 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

- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)
- 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。
- PPPoE を利用する物理 LAN インタフェースの情報として、以下の手順で「ポート番号」と「転送レート」を必ず設定してください。「LAN 情報 (物理 LAN)」を設定しない場合、通信できなくなります。以下に手順を示します。
  - 設定メニューのルータ設定で「LAN 情報」をクリックします。
  - インタフェースに“物理インタフェース”を指定して、[追加] ボタンをクリックします。
  - 「共通情報」－「基本情報」で、ポート番号と転送レートを選択して、[保存] ボタンをクリックします。
- 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。

## LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
  - 「LAN 情報」でインタフェースが LAN0 の [削除] ボタンをクリックします。  
メッセージボックスに「削除していいですか?」というメッセージが表示されます。
  - [OK] ボタンをクリックします。  
インタフェースが LAN0 の定義が削除されます。
  - 以下の項目を指定します。
    - インタフェース → 物理 LAN
- 
- [追加] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
  - 「共通情報」をクリックします。  
共通情報の設定項目と「基本情報」が表示されます。

## 7. 以下の項目を指定します。

- ポート番号  
 master →基本 0  
 backup →バックアップなし
- 転送レート →自動認識

■基本情報	
ポート番号	master 基本 0
	backup バックアップなし
優先使用ポート	<input checked="" type="radio"/> master <input type="radio"/> 先にリンクアップしたポート
転送レート	自動認識

## 8. [保存] ボタンをクリックします。

## LAN1 情報を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 以下の項目を指定します。

- インタフェース →物理 LAN

<LAN情報追加フィールド>	
インタフェース	物理LAN

### 3. [追加] ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

### 4. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

## 5. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →192.168.1.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する	
	IPアドレス	192.168.1.1
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス+オール1

## 6. [保存] ボタンをクリックします。

## 7. IP関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

## 8. 以下の項目を指定します。

- DHCP機能 →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
- DNSサーバ広報 →192.168.1.1
- セカンダリDNSサーバ広報 →指定しない
- ドメイン名広報 →指定しない

■DHCP情報		
DHCP機能	<input type="radio"/> 使用しない <input type="radio"/> リレー機能を使用する <input checked="" type="radio"/> サーバ機能を使用する	
	DHCPサーバIPアドレス1	
	DHCPサーバIPアドレス2	
	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
	DNSサーバ広報	192.168.1.1
	セカンダリDNSサーバ広報	
	ドメイン名広報	

※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。

## 9. [保存] ボタンをクリックします。

## 相手情報を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3. 以下の項目を指定します。

- ネットワーク名 → internet

<ネットワーク情報追加フィールド>	
ネットワーク名	internet

4. [追加] ボタンをクリックします。

「ネットワーク情報 (internet)」ページが表示されます。

5. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

6. 以下の項目を指定します。

- MTU サイズ → 1454
- 自動接続 → する

■基本情報	
ネットワーク名	internet
MTUサイズ	1454 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps

7. [保存] ボタンをクリックします。

8. 「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

9. 以下の項目を指定します。

- ヘッダ圧縮 (IPCP) → チェックしない
- ヘッダ圧縮 (IPV6CP) → チェックしない

■圧縮情報	
ヘッダ圧縮 (IPCP)	<input type="checkbox"/> VJ <input type="checkbox"/> IPヘッダ圧縮
ヘッダ圧縮 (IPV6CP)	<input type="checkbox"/> IPヘッダ圧縮
データ圧縮 (CCP)	<input type="checkbox"/> LZS

10. [保存] ボタンをクリックします。

**11. 「IP 関連」 をクリックします。**

IP 関連の設定項目と「IP 基本情報」が表示されます。

**12. IP 関連の設定項目の「スタティック経路情報」 をクリックします。**

「スタティック経路情報」が表示されます。

**13. 以下の項目を指定します。**

- ネットワーク →デフォルトルート
- メトリック値 →1
- 優先度 →0

<スタティック経路情報入力フィールド>	
ネットワーク	<input checked="" type="radio"/> デフォルトルート <input type="radio"/> ネットワーク指定
	宛先IPアドレス <input type="text"/> 宛先アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**14. [追加] ボタンをクリックします。****15. IP 関連の設定項目の「NAT 情報」 をクリックします。**

「NAT 情報」が表示されます。

**16. 以下の項目を指定します。**

- NATの使用 →マルチ NAT
- グローバルアドレス →指定しない
- アドレス個数 →1
- アドレス割当てタイマ →5分
- NATセキュリティ →高い

■ NAT 情報	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ
グローバルアドレス	<input type="text"/>
アドレス個数	<input type="text" value="1"/> 個
アドレス割当てタイマ	<input type="text" value="5"/> 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsecパススルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

**17. [保存] ボタンをクリックします。****18. IP 関連の設定項目の「IP 基本情報」 をクリックします。**

「IP 基本情報」が表示されます。

## 19. 以下の項目を指定します。

- MSS書き換え →使用する  
書き換えサイズ →1414

■IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する 相手側IPアドレス <input type="text"/> 自側IPアドレス <input type="text"/>
MSS書き換え	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する 書き換えサイズ <input type="text" value="1414"/> バイト

## 20. [保存] ボタンをクリックします。

## 21. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 22. 以下の項目を指定します。

- 接続先名 →ISP-1
- 接続先種別 →PPPoE 接続

<接続先情報追加フィールド>	
接続先名	<input type="text" value="ISP-1"/>
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 ダイヤル1 <input type="text"/> 電話番号 <input type="text"/> サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続 DLCI <input type="text"/>
	<input checked="" type="radio"/> PPPoE接続 <input type="radio"/> IPTトンネル接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄

## 23. [追加] ボタンをクリックします。

PPPoE 接続の設定項目と「基本情報」が表示されます。

## 24. 以下の項目を指定します。

- 使用インタフェース →LAN0
- DNSサーバ →指定しない

■基本情報	
接続先名	<input type="text" value="ISP-1"/>
使用インタフェース	<input type="text" value="LAN0"/>
DNSサーバ	<input type="text"/>

25. [保存] ボタンをクリックします。
26. PPPoE 接続の設定項目の「PPP 情報」をクリックします。  
「PPP 情報」が表示されます。
27. 以下の項目を指定します。
- 送信認証情報
    - 認証 ID → userid
    - 認証パスワード → userpass

28. [保存] ボタンをクリックします。

## ProxyDNS 情報、URL フィルタ情報を設定する

29. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。  
「ProxyDNS 情報 / URL フィルタ情報」ページが表示されます。
30. 「順引き情報」をクリックします。  
「順引き情報」が表示されます。
31. 以下の項目を指定します。
- ドメイン名 → \*
  - タイプ → すべて
  - 送信元 IP アドレス → 指定しない
  - 動作 → 接続先の DNS サーバへ問い合わせる
  - ネットワーク名 → internet

32. [追加] ボタンをクリックします。

**33. 「逆引き情報」をクリックします。**

「逆引き情報」が表示されます。

**34. 以下の項目を指定します。**

- ネットワークアドレス → すべて
- 動作 → 接続先の DNS サーバへ問い合わせる
- ネットワーク名 → internet

<逆引き情報入力フィールド>

ネットワークアドレス	<div style="border: 1px solid gray; padding: 2px;">           すべて  <small>(“指定する”を選択時のみ有効です。)</small> </div> <div style="border: 1px solid gray; height: 20px; margin-top: 2px;"></div> <small>※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。</small>
動作	<input type="radio"/> 廃棄する <input checked="" type="radio"/> 接続先のDNSサーバへ問い合わせる <div style="border: 1px solid gray; padding: 2px; margin: 2px 0;">           ネットワーク名 <span style="border: 1px solid gray; padding: 0 5px;">internet</span> </div> <input type="radio"/> 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 <div style="border: 1px solid gray; padding: 2px; margin: 2px 0;">           ネットワーク名 <span style="border: 1px solid gray; padding: 0 5px;">rmt0</span> </div> <input type="checkbox"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する <input type="radio"/> 設定したDNSサーバへ問い合わせる <div style="border: 1px solid gray; padding: 2px; margin: 2px 0;">           DNSサーバアドレス <span style="border: 1px solid gray; padding: 0 20px;"></span> </div>

**35. [追加] ボタンをクリックします。****36. 画面左側の [設定反映] 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。



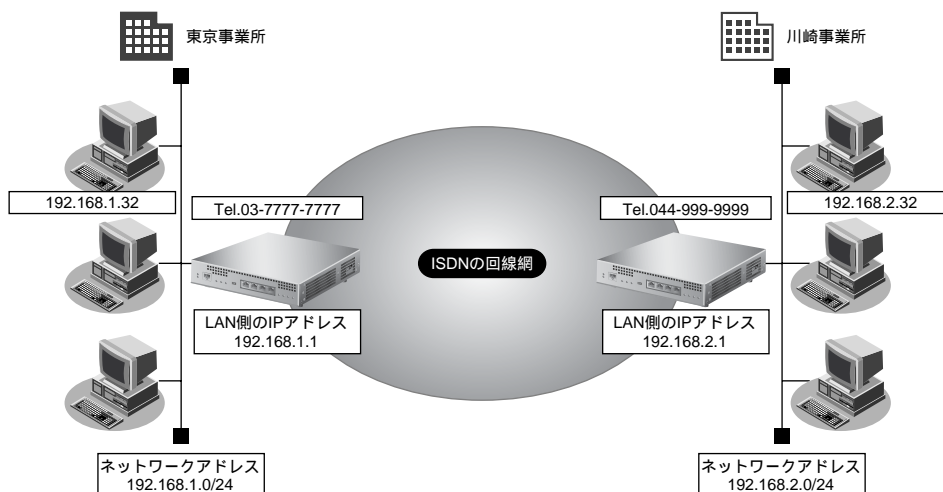
## 1.7 事業所 LAN を ISDN で接続する

ここでは、ISDN回線を介して2つの事業所（東京、川崎）のネットワークを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 MR1000 トラブルシューティング 「ご購入時の状態に戻すには」 (P.42)



### ● 設定条件

- ISDN ポートでISDN回線（64Kbps）を使用する
- スタティック経路機能を使用する
- 接続ネットワーク名 : intranet
- 無通信監視時間を1分とする

#### 【東京事業所】

- 本装置のIPアドレス/ネットマスク : 192.168.1.1/24
- 電話番号 : 03-7777-7777
- ユーザ認証IDとユーザ認証パスワード
  - 発信 : tokyo、tokyopass
  - 着信 : kawasaki、kawapass

#### 【川崎事業所】

- 本装置のIPアドレス/ネットマスク : 192.168.2.1/24
- 電話番号 : 044-999-9999
- ユーザ認証IDとユーザ認証パスワード
  - 発信 : kawasaki、kawapass
  - 着信 : tokyo、tokyopass

### 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。

## 東京事業所を設定する

### WAN0 情報を設定する

1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2. 以下の項目を指定します。

- 回線インタフェース → ISDN

<WAN情報追加フィールド>	
回線インタフェース	ISDN

3. [追加] ボタンをクリックします。

「WAN0 情報 (ISDN)」ページが表示されます。

### LAN0 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. 以下の項目を指定します。

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 192.168.1.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール1

■ IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する	
	IPアドレス	192.168.1.1
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス + オール1

5. [保存] ボタンをクリックします。

## 相手情報を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → intranet

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="intranet"/>

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (intranet)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
ネットワーク	<input type="text" value=""/> <input type="text" value=""/> <input type="text" value=""/>
	<input type="text" value="192.168.2.0"/> <input type="text" value="24 (255.255.255.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → kawasaki
- 接続先種別 → ISDN 接続
  - ダイヤル1
  - 電話番号 → 044-999-9999
  - サブアドレス → 指定しない

<接続先情報追加フィールド>						
接続先名	<input type="text" value="kawasaki"/>					
接続先種別	<input type="radio"/> 専用線接続 <input checked="" type="radio"/> ISDN接続					
	<table border="1"> <tr> <td>ダイヤル1</td> <td>電話番号</td> <td><input type="text" value="044-999-9999"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> </table>	ダイヤル1	電話番号	<input type="text" value="044-999-9999"/>		サブアドレス
ダイヤル1	電話番号	<input type="text" value="044-999-9999"/>				
	サブアドレス	<input type="text"/>				
	<input type="radio"/> フレームリレー接続 <input type="radio"/> PPPoE接続 <input type="radio"/> IPTトンネル接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄					
	DLCI <input type="text"/>					

## 11. [追加] ボタンをクリックします。


ISDN 接続の設定項目と「基本情報」が表示されます。

## 12. ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

## 13. 以下の項目を指定します。

- 認証方式 → PAP、CHAP
- 送信認証情報
  - 認証 ID → tokyo
  - 認証パスワード → tokyopass
- 受諾認証情報
  - 認証 ID → kawasaki
  - 認証パスワード → kawapass

■ PPP 情報 	
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
送信認証情報	認証 ID <input type="text" value="tokyo"/>
	認証パスワード <input type="password" value="*****"/>
受諾認証情報	認証 ID <input type="text" value="kawasaki"/>
	認証パスワード <input type="password" value="*****"/>
MP 接続	<input checked="" type="radio"/> しない <input type="radio"/> する
	BAP/BACP 利用 <input checked="" type="radio"/> しない <input type="radio"/> する <small>※ 発信者番号による識別で番号をチェックしない場合は着信相手識別情報の設定が有効</small>

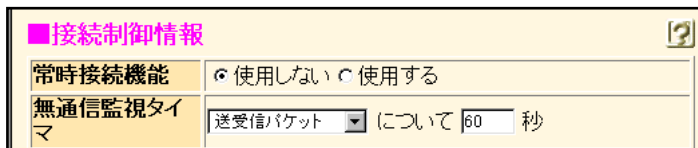
14. [保存] ボタンをクリックします。

15. ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

16. 以下の項目を指定します。

- 常時接続情報 → 使用しない
- 無通信監視タイマ → 送受信パケットについて 60 秒



■ 接続制御情報	
常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
無通信監視タイマ	送受信パケット について 60 秒

17. [保存] ボタンをクリックします。

18. 画面左側の [再起動] 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。

## 川崎事業所を設定する

「東京事業所を設定する」を参考に、川崎事業所を設定します。

### 「WAN0 情報」

- 回線インタフェース → ISDN

### 「LAN0 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 192.168.2.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → intranet

### 「ネットワーク情報」 - 「IP 関連」

#### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
  - あて先 IP アドレス → 192.168.1.0
  - あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

### 「接続先情報」

- 接続先名 → tokyo
- 接続先種別 → ISDN 接続
  - ダイヤル 1
  - 電話番号 → 03-7777-7777
  - サブアドレス → 指定しない

### 「接続先情報」 - 「ISDN 接続」

#### 「PPP 情報」

- 認証方式 → PAP、CHAP
- 送信認証情報
  - 認証 ID → kawasaki
  - 認証パスワード → kawapass
- 受諾認証情報
  - 認証 ID → tokyo
  - 認証パスワード → tokyopass

### 「接続制御情報」

- 常時接続情報 → 使用しない
- 無通信監視タイマ → 送受信パケットについて 60 秒

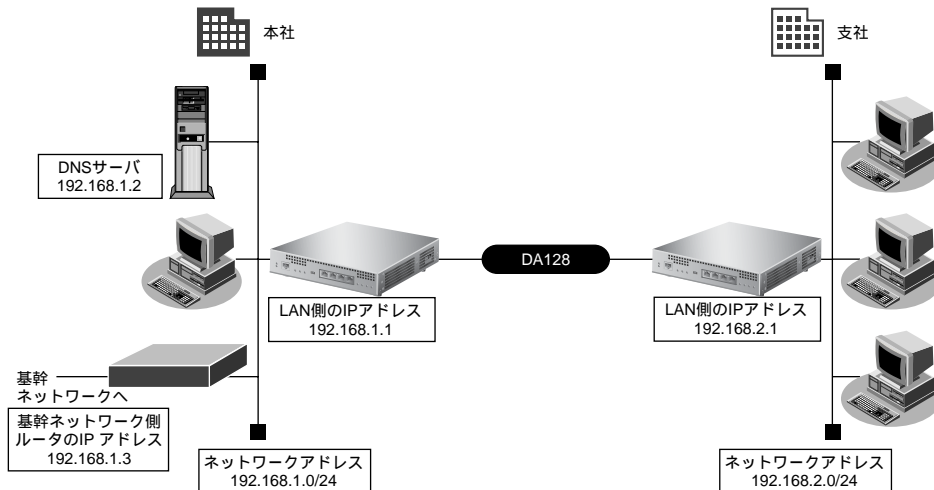
## 1.8 事業所 LAN を専用線で接続する

ここでは、高速デジタル専用線を介して 2 つの事業所（本社、支社）のネットワークを接続する場合について説明します。

### 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 MR1000 トラブルシューティング「ご購入時の状態に戻すには」(P.42)



### ● 設定条件

- ISDN ポートで専用線（BRI：128Mbps）を使用する
- DHCP サーバ機能は使用しない

#### 【本社】

- 接続ネットワーク名 : honsya
- 接続先名 : honsya-1
- ネットワークアドレス/ネットマスク : 192.168.1.0/24
- 本装置の LAN 側の IP アドレス : 192.168.1.1
- DNS サーバ : 192.168.1.2
- 基幹ネットワーク側ルータ IP アドレス : 192.168.1.3

#### 【支社】

- 接続ネットワーク名 : shisya1
- 接続先名 : shisya-1
- ネットワークアドレス/ネットマスク : 192.168.2.0/24
- 本装置の LAN 側の IP アドレス : 192.168.2.1



この例では、本社に DNS サーバが存在し、IP アドレスを固定にする必要があります。そのため、本社側では DHCP サーバ機能は使用しない条件にします。

### こんな事に気をつけて

- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

- 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。

## 本機を設定する

### WAN0 情報を設定する

- 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

- 以下の項目を指定します。

- 回線インタフェース → 専用線

<WAN情報追加フィールド>	
回線インタフェース	専用線

- 「追加」ボタンをクリックします。

「WAN0 情報（専用線）」ページが表示されます。

- 「基本情報」をクリックします。

「基本情報」が表示されます。

- 以下の項目を指定します。

- 回線速度 → 128Kbps

■基本情報	
ポート	基本 0
回線速度	128Kbps

- 「保存」ボタンをクリックします。

### LAN0 情報を設定する

- 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

- 「LAN 情報」でインタフェースが LAN0 の「修正」ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

- 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。



#### 4. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →192.168.1.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■ IPアドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPアドレス	<input type="radio"/> DHCPで自動的に取得する
	<input checked="" type="radio"/> 指定する
	IPアドレス <input type="text" value="192.168.1.1"/>
	ネットマスク <input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス <input type="text" value="ネットワークアドレス+オール1"/>

#### 5. [保存] ボタンをクリックします。

#### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

#### 7. 以下の項目を指定します。

- ネットワーク →デフォルトルート
  - 中継ルータアドレス →192.168.1.3
- メトリック値 →1
- 優先度 →0

<スタティック経路情報入力フィールド>	
ネットワーク	<input checked="" type="radio"/> デフォルトルート
	中継ルータアドレス <input type="text" value="192.168.1.3"/>
	<input type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text"/> あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/> 中継ルータアドレス <input type="text"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

#### 8. [追加] ボタンをクリックします。

#### 相手情報を設定する

##### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

##### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → shisya1

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="shisya1"/>

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (shisya1)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.1
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.1"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → shisya-1
- 接続先種別 → 専用線接続

<接続先情報追加フィールド>	
接続先名	shisya-1
接続先種別	<input checked="" type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インターフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

## 11. [追加] ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 使用インターフェース → WAN0
- DNSサーバ → 192.10.10.10

■基本情報	
接続先名	shisya-1
使用インターフェース	WAN0
DNSサーバ	192.10.10.10

## 13. [保存] ボタンをクリックします。

## 14. 画面左側の [再起動] 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。

## 支社を設定する

---

「本社を設定する」を参考に、支社を設定します。

### 「WAN0 情報」

- 回線インタフェース →専用線

### 「専用線」 - 「基本情報」

- 回線速度 →128Mbps

### 「LAN0 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス →192.168.2.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス + オール 1

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 →honsya

### 「ネットワーク情報」 - 「IP 関連」

#### 「スタティック経路情報」

- ネットワーク →デフォルトルート
- メトリック値 →1
- 優先度 →0

### 「接続先情報」

- 接続先名 →honsya-1
- 接続先種別 →専用線接続

## 1.9 複数の事業所 LAN をフレームリレーで接続する

ここでは、フレームリレーで複数の事業所を接続する場合を例に説明します。

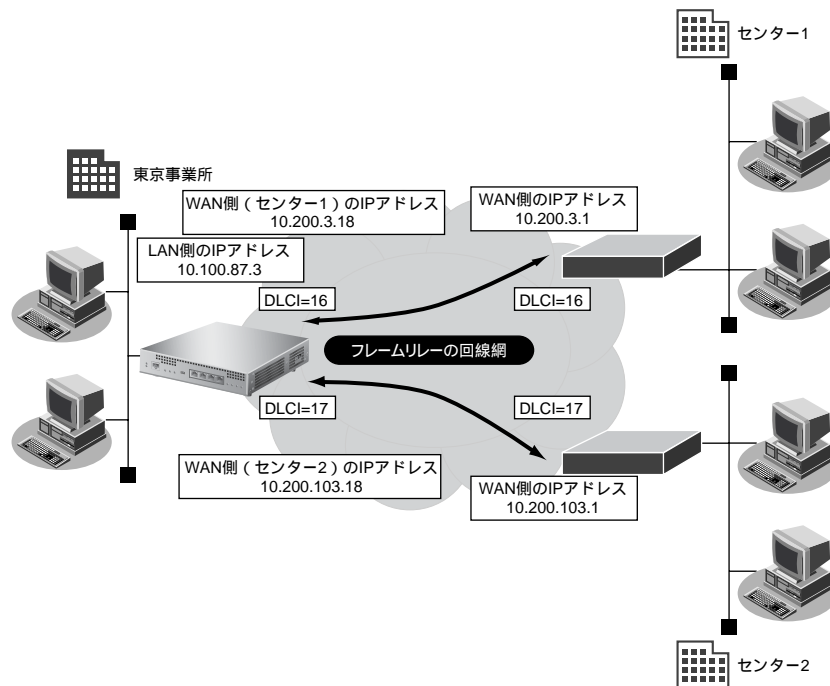
フレームリレーを利用すると複数の事業所の LAN と接続できるため、データを高速に転送することができます。

また、相手ごとに固定的な回線を接続するので、公衆網であるフレームリレー網に閉域ネットワークを構築することができ、セキュリティの確保にも適しています。

### 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 MR1000 トラブルシューティング 「ご購入時の状態に戻すには」 (P.42)



### ● 設定条件

- ISDN ポートでフレームリレー (128Kbps) を使用する
- RIPv1 を使用する
- 本装置の LAN 側の IP アドレス / ネットマスク : 10.100.87.3/24

#### 【センター 1 と接続する条件】

- ネットワーク名 : center1
- 接続先名 : ap1
- WAN の自側 IP アドレス : 10.200.3.18
- WAN の相手側 IP アドレス : 10.200.3.1
- DLCI : 16
- CIR : 64Kbps

#### 【センター 2 と接続する条件】

- ネットワーク名 : center2
- 接続先名 : ap2

- WAN の自側IP アドレス : 10.200.103.18
- WAN の相手側IP アドレス : 10.200.103.1
- DLCI : 17
- CIR : 64Kbps

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。

## WAN0 情報を設定する

### 1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

### 2. 以下の項目を指定します。

- 回線インタフェース → フレームリレー

<WAN情報追加フィールド>	
回線インタフェース	フレームリレー

### 3. [追加] ボタンをクリックします。

「WAN0 情報 (フレームリレー)」ページが表示されます。

### 4. 「基本情報」をクリックします。

「基本情報」が表示されます。

### 5. 以下の項目を指定します。

- 回線速度 → 128Kbps
- PVC 状態確認手順 → 使用する
- CLLM メッセージ → 使用する
- 輻輳通知ビット → FECN、BECN

■基本情報	
ポート	基本 0
回線速度	128Kbps
PVC 状態確認手順	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
CLLM メッセージ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
輻輳通知ビット	<input checked="" type="checkbox"/> FECN <input checked="" type="checkbox"/> BECN

### 6. [保存] ボタンをクリックします。

## LAN0 情報を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 4. 以下の項目を指定します。

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.100.87.3
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

■ IP アドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IP アドレス	<input type="radio"/> DHCP で自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IP アドレス	<input type="text" value="10.100.87.3"/>
	ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス	<input type="text" value="ネットワークアドレス + オール 1"/>

### 5. 【保存】 ボタンをクリックします。

### 6. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

### 7. 以下の項目を指定します。

- RIP 送信 → V1 で送信する
- RIP 受信 → V1 で受信する
- メトリック値 → 0

■ RIP 情報	
RIP 送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1 で送信する <input type="radio"/> V2 で送信する <input type="radio"/> V2 (Multicast) で送信する
RIP 受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1 で受信する <input type="radio"/> V2、V2 (Multicast) で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	<input type="text" value="0"/>

### 8. 【保存】 ボタンをクリックします。

## 接続先（センター 1）の情報を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3. 以下の項目を指定します。

- ネットワーク名 → center1

<ネットワーク情報追加フィールド>	
ネットワーク名	center1

4. [追加] ボタンをクリックします。

「ネットワーク情報（center1）」ページが表示されます。

5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. 以下の項目を指定します。

- IPアドレス → 設定する
- 相手側IPアドレス → 10.200.3.1
- 自側IPアドレス → 10.200.3.18

■ IP基本情報	
IPアドレス	<input type="radio"/> 設定しない
	<input checked="" type="radio"/> 設定する
	相手側IPアドレス <input type="text" value="10.200.3.1"/>
自側IPアドレス <input type="text" value="10.200.3.18"/>	
MSS書き換え	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> 使用する
	書き換えサイズ <input type="text" value="0"/> バイト

7. [保存] ボタンをクリックします。

8. IP関連の設定項目の「RIP情報」をクリックします。

「RIP情報」が表示されます。



## 9. 以下の項目を指定します。

- RIP送信 → V1で送信する
- RIP受信 → V1で受信する
- メトリック値 → 0

**■ RIP情報** ?

RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する

《 RIP 送信時は加算するメトリック値を設定してください。》

メトリック値

## 10. [保存] ボタンをクリックします。

## 11. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 12. 以下の項目を指定します。

- 接続先名 → ap1
- 接続先種別 → フレームリレー接続  
DLCI → 16

<接続先情報追加フィールド>

接続先名	<input style="width: 80%;" type="text" value="ap1"/>
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 <div style="margin-left: 20px;"> <input type="text" value="ダイヤル1"/> <input type="text" value="電話番号"/> <input style="width: 50px;" type="text"/>  <input type="text" value="サブアドレス"/> <input style="width: 50px;" type="text"/> </div> <input checked="" type="radio"/> フレームリレー接続 <input style="width: 50px;" type="text" value="DLCI 16"/> <input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

## 13. [追加] ボタンをクリックします。

フレームリレー接続の設定項目と「基本情報」が表示されます。

**14. 以下の項目を指定します。**

- 使用インタフェース → WAN0
- DLCI → 16
- CIR → 64Kbps

■基本情報	
接続先名	ap1
使用インタフェース	WAN0
DLCI	16
CIR	64Kbps

**15. [保存] ボタンをクリックします。****接続先 (センター 2) の情報を設定する**

「接続先 (センター 1) の情報を設定する」を参考に、接続先 (センター 2) を設定します。

**「相手情報」 - 「ネットワーク情報」**

- ネットワーク名 → center2

**「ネットワーク情報」 - 「IP 関連」****「IP 基本情報」**

- IP アドレス → 設定する
- 相手側 IP アドレス → 10.200.103.1
- 自側 IP アドレス → 10.200.103.18

**「RIP 情報」**

- RIP 送信 → V1 で送信する
- RIP 受信 → V1 で受信する
- メトリック値 → 0

**「接続先情報」**

- 接続先名 → ap2
- 接続先種別 → フレームリレー接続
- DLCI → 17

**「接続先情報」 - 「フレームリレー接続」****「基本情報」**

- 使用インタフェース → WAN0
- DLCI → 17
- CIR → 64Kbps

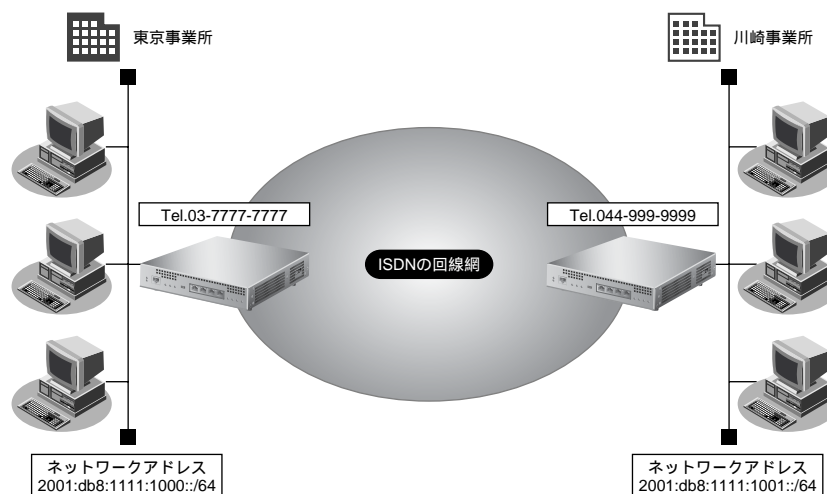
## 1.10 IPv6の事業所LANをISDNで接続する

ここでは、ISDN回線を介して2つの事業所（東京、川崎）のIPv6ネットワークを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 MR1000 トラブルシューティング 「ご購入時の状態に戻すには」 (P.42)



### ● 設定条件

- ISDNポートでISDN（64Kbps）を使用する
- IPv6を使用する
- スタティック経路機能を使用する
- 接続ネットワーク名 : kaisya
- 無通信監視時間を1分とする

#### 【東京事業所】

- ネットワークアドレス/プレフィックス長 : 2001:db8:1111:1000::/64
- 接続先名 : tokyo
- 電話番号 : 03-7777-7777
- ユーザ認証IDとユーザ認証パスワード
  - 発信 : tokyo、tokyopass
  - 着信 : kawasaki、kawapass

#### 【川崎事業所】

- ネットワークアドレス/プレフィックス長 : 2001:db8:1111:1001::/64
- 接続先名 : kawasaki
- 電話番号 : 044-999-9999
- ユーザ認証IDとユーザ認証パスワード
  - 発信 : kawasaki、kawapass
  - 着信 : tokyo、tokyopass

### こんな事に気をつけて

文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

## 東京事業所を設定する

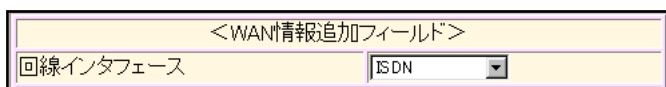
### WAN0 情報を設定する

1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2. 以下の項目を指定します。

- 回線インタフェース → ISDN



<WAN情報追加フィールド>	
回線インタフェース	ISDN

3. [追加] ボタンをクリックします。

「WAN0 情報 (ISDN)」ページが表示されます。

### LAN0 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

#### 4. 以下の項目を指定します。

- IPv6 →使用する
- インタフェースID →自動
- IPv6 アドレス  
アドレスまたはプレフィックス →2001:db8:1111:1000::  
Valid Lifetime →30日  
Pref. Lifetime →7日  
フラグ →c0
- ルータ広報 →送信する

IPv6基本情報				
IPv6	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する			
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>			
IPv6 アド レス	アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限	Pref. Lifetime 期限有 無期限	フラ グ
	2001:db8:1111:1000::	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0
	<input type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0
	<input type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0
ルー タ 広 報	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する			
	最大送信間隔	600 秒		
	最小送信間隔	200 秒		
	Router Lifetime	1800 秒		
	MTU	<input type="text"/>		
	Reachable Time	0 ミリ秒		
	Retrans Timer	0 ミリ秒		
	Cur Hop Limit	64		
フラグ	00			

#### 5. [保存] ボタンをクリックします。

#### 相手情報を設定する

##### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

##### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

##### 3. 以下の項目を指定します。

- ネットワーク名 →kaisya

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="kaisya"/>

##### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (kaisya)」ページが表示されます。

## 5. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 6. 以下の項目を指定します。

- 接続先名 → kawasaki
- 接続先種別 → ISDN 接続
  - ダイヤル1
  - 電話番号 → 044-999-9999
  - サブアドレス → 指定しない

<接続先情報追加フィールド>

接続先名	<input type="text" value="kawasaki"/>		
接続先種別	<input type="radio"/> 専用線接続 <input checked="" type="radio"/> ISDN接続		
	ダイヤル1	電話番号	<input type="text" value="044-999-9999"/>
		サブアドレス	<input type="text"/>
	<input type="radio"/> フレームリレー接続 <input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄		
	DLCI	<input type="text"/>	

## 7. [追加] ボタンをクリックします。

ISDN接続の設定項目と「基本情報」が表示されます。

## 8. ISDN 接続の設定項目の「PPP 情報」をクリックします。

「PPP情報」が表示されます。

## 9. 以下の項目を指定します。

- 認証方式 → PAP、CHAP
- 送信認証情報
  - 認証ID → tokyo
  - 認証パスワード → tokyopass
- 受諾認証情報
  - 認証ID → kawasaki
  - 認証パスワード → kawapass

■ PPP情報	
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
送信認証情報	認証ID <input type="text" value="tokyo"/>
	認証パスワード <input type="password" value="*****"/>
受諾認証情報	認証ID <input type="text" value="kawasaki"/>
	認証パスワード <input type="password" value="*****"/>
MP接続	<input checked="" type="radio"/> しない <input type="radio"/> する
	<input type="checkbox"/> BAP/BACP利用 <input checked="" type="radio"/> しない <input type="radio"/> する <small>※ 発信者番号による識別で番号をチェックしない場合は着信相手識別情報の設定が有効</small>

## 10. [保存] ボタンをクリックします。

## 11. ISDN 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

## 12. 以下の項目を指定します。

- 常時接続機能 → 使用しない
- 無通信監視タイマ → 送受信パケットについて 60 秒

■ 接続制御情報	
常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
無通信監視タイマ	送受信パケット (について) <input type="text" value="60"/> 秒

## 13. [保存] ボタンをクリックします。

## 14. 画面上部の「ネットワーク情報 (kaisya)」をクリックします。

「ネットワーク情報 (kaisya)」ページが表示されます。

## 15. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

## 16. 以下の項目を指定します。

- IPv6 →使用する
- インタフェースID →自動
- IPv6アドレス →指定しない
- ルータ広報 →送信しない

IPv6基本情報				
IPv6	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する			
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>			
IPv6アドレス	アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限	Pref. Lifetime 期限有 無期限	フラグ
	<input type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0
	<input type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0
	<input type="text"/>	30 日 <input type="checkbox"/>	7 日 <input type="checkbox"/>	c0
ルータ広報	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する			
	最大送信間隔	600 秒		
	最小送信間隔	200 秒		
	Router Lifetime	1800 秒		
	MTU	<input type="text"/>		
	Reachable Time	0 ミリ秒		
	Retrans Timer	0 ミリ秒		
	Cur Hop Limit	64		
フラグ	00			

## 17. [保存] ボタンをクリックします。

## 18. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

## 19. 以下の項目を指定します。

- ネットワーク →ネットワーク指定  
あて先ネットワーク/プレフィックス長 →2001:db8:1111:1001::/64
- メトリック値 →1
- 優先度 →0

<IPv6スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先プレフィックス/プレフィックス長 <input type="text" value="2001:db8:1111:1001::"/> / <input type="text" value="64"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

## 20. [追加] ボタンをクリックします。



## 21. 画面左側の [再起動] 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。



**注意** ISDNまたはフレームリレーの場合、RIP (IPv6) を送信しないでください。RIP (IPv6) を送信すると、**思わぬ課金 (定期発信または長時間接続) が発生します。**

## 川崎事業所を設定する

「東京事業所を設定する」を参考に、川崎事業所を設定します。

### 「WAN0 情報」

- 回線インタフェース → ISDN

### 「LAN0 情報」 - 「IPv6 関連」

#### 「IPv6 基本情報」

- IPv6 → 使用する
- インタフェース ID → 自動
- IPv6 アドレス  
アドレスまたはプレフィックス → 2001:db8:1111:1001::  
Valid Lifetime → 30 日  
Pref. Lifetime → 7 日  
フラグ → c0
- ルータ広報 → 送信する

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → tokyo

#### 「接続先情報」

- 接続先名 → tokyo
- 接続先種別 → ISDN 接続  
ダイヤル1  
電話番号 → 03-7777-7777  
サブアドレス → 指定しない

### 「接続先情報」 - 「ISDN 接続」

#### 「PPP 情報」

- 認証方式 → PAP、CHAP
- 送信認証情報  
認証 ID → kawasaki  
認証パスワード → kawapass
- 受諾認証情報  
認証 ID → tokyo  
認証パスワード → tokyopass

#### 「接続制御情報」

- 常時接続情報 → 使用しない
- 無通信監視タイマ → 送受信パケットについて 60 秒

**「相手情報」 - 「IPv6 関連」**

## 「IPv6基本情報」

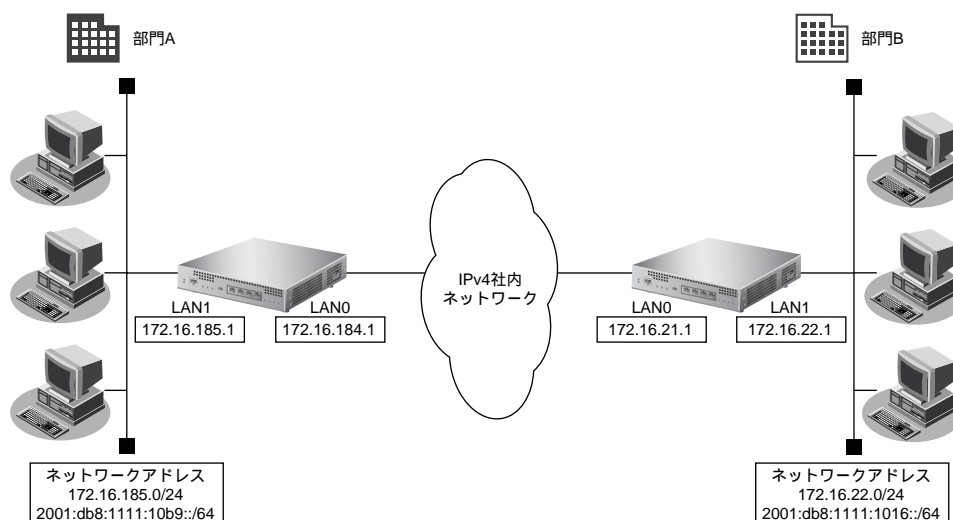
- IPv6 →使用する
- インタフェースID →自動
- IPv6 アドレス →指定しない
- ルータ広報 →送信しない

## 「IPv6スタティック経路情報」

- ネットワーク →ネットワーク指定
- あて先ネットワーク/プレフィックス長 →2001:db8:1111:1000::/64
- メトリック値 →1
- 優先度 →0

## 1.11 IPv6の事業所LANをIPv6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]

- ダイナミック経路を使用する
- LAN0側のIPv4アドレス : 172.16.184.1
- LAN1側のIPv4アドレス : 172.16.185.1
- LAN1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]

- ダイナミック経路を使用する
- LAN0側のIPv4アドレス : 172.16.21.1
- LAN1側のIPv4アドレス : 172.16.22.1
- LAN1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

- 文字入力フィールドでは、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 MR1000 Webユーザズガイド「文字入力フィールドで入力できる文字一覧」(P.13)

- 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。

## 東京事業所の本装置を設定する

### LAN0 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。  
「LAN0 情報（物理 LAN）」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. 以下の項目を指定します。
  - IPv4 → 使用する
  - IP アドレス → 指定する  
IP アドレス → 172.16.184.1  
ネットマスク → 24 (255.255.255.0)  
ブロードキャストアドレス → ネットワークアドレス+オール1

■ IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IPアドレス	<input type="text" value="172.16.184.1"/>
	ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス	<input type="text" value="ネットワークアドレス+オール1"/>

5. 【保存】 ボタンをクリックします。
6. IP 関連の設定項目の「RIP 情報」をクリックします。  
「RIP 情報」が表示されます。
7. 以下の項目を指定します。
  - RIP 送信 → V1 で送信する
  - RIP 受信 → V1 で受信する

■ RIP情報	
RIP送信	<input type="radio"/> 送信しない
	<input checked="" type="radio"/> V1で送信する
	<input type="radio"/> V2で送信する
	<input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない
	<input checked="" type="radio"/> V1で受信する
	<input type="radio"/> V2、V2(Multicast)で受信する

8. 【保存】 ボタンをクリックします。
9. IP 関連の設定項目の「DHCP 情報」をクリックします。  
「DHCP 情報」が表示されます。

## 10. 以下の項目を指定します。

- DHCP 機能 →使用しない

■DHCP情報	
DHCP 機能	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> リレー機能を使用する
	DHCPサーバIPアドレス1 <input type="text"/>
	DHCPサーバIPアドレス2 <input type="text"/>
	<input type="radio"/> サーバ機能を使用する
	割当て先頭IPアドレス <input type="text"/>
	割当てアドレス数 <input type="text" value="32"/>
	リース期間 <input type="text" value="1"/> 日 <input type="text"/>
	デフォルトルータ広報 <input type="text"/>
	DNSサーバ広報 <input type="text"/>
セカンダリDNSサーバ広報 <input type="text"/>	
ドメイン名広報 <input type="text"/>	
※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。	

## 11. [保存] ボタンをクリックします。

## 12. IP関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

## 13. 以下の項目を指定します。

- NATの使用 →使用しない

■NAT情報	
NATの使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ ※NATの使用とDHCPリレーサービスの併用はできません

## 14. [保存] ボタンをクリックします。

## LAN1情報を設定する

こんな事に気をつけて

「LAN1情報を設定する」場合は、あらかじめ物理LAN1定義を追加する必要があります。

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースがLAN1の [修正] ボタンをクリックします。

「LAN1情報 (物理 LAN)」ページが表示されます。

### 3. 「IP 関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

#### 4. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →172.16.185.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する	
	IPアドレス	172.16.185.1
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス+オール1

#### 5. [保存] ボタンをクリックします。

#### 6. IP関連の設定項目の「RIP情報」をクリックします。

「RIP情報」が表示されます。

#### 7. 以下の項目を指定します。

- RIP送信 →V1で送信する
- RIP受信 →V1で受信する

■RIP情報	
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する

#### 8. [保存] ボタンをクリックします。

#### 9. IP関連の設定項目の「DHCP情報」をクリックします。

「DHCP情報」が表示されます。

## 10. 以下の項目を指定します。

- DHCP 機能 →使用しない

■DHCP情報	
DHCP 機能	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> リレー機能を使用する
	DHCPサーバIPアドレス1 <input type="text"/>
	DHCPサーバIPアドレス2 <input type="text"/>
	<input type="radio"/> サーバ機能を使用する
	割当て先頭IPアドレス <input type="text"/>
	割当てアドレス数 <input type="text" value="32"/>
	リース期間 <input type="text" value="1"/> 日 <input type="text"/>
	デフォルトルータ広報 <input type="text"/>
	DNSサーバ広報 <input type="text"/>
セカンダリDNSサーバ広報 <input type="text"/>	
ドメイン名広報 <input type="text"/>	
※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。	

## 11. [保存] ボタンをクリックします。

## 12. IP関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

## 13. 以下の項目を指定します。

- NATの使用 →使用しない

■NAT情報	
NATの使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ ※NATの使用とDHCPリレーサービスの併用はできません

## 14. [保存] ボタンをクリックします。

## LAN 情報（東京事業所）を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。

### 3. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

#### 4. 以下の項目を指定します。

- IPv6 →使用する
- インタフェースID →自動
- IPv6 アドレス  
アドレスまたはプレフィックス →2001:db8:1111:10b9::
- ルータ広報 →送信する

IPv6基本情報				
IPv6	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する			
インタフェースID	<input checked="" type="radio"/> 自動 <input type="radio"/> 指定する <input type="text"/>			
IPv6 アドレス	アドレスまたはプレフィックス	Valid Lifetime 期限有 無期限	Pref. Lifetime 期限有 無期限	フラグ
	2001:db8:1111:10b9::	30 日	7 日	c0
		30 日	7 日	c0
		30 日	7 日	c0
ルータ 広報	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する			
	最大送信間隔	600 秒		
	最小送信間隔	200 秒		
	Router Lifetime	1800 秒		
	MTU			
	Reachable Time	0 ミリ秒		
	Retrans Timer	0 ミリ秒		
	Cur Hop Limit	64		
フラグ	00			

#### 5. [保存] ボタンをクリックします。

#### IPトンネル接続の情報 (川崎事業所) を設定する

##### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「ネットワーク情報」が表示されます。

##### 2. 以下を指定します。

- ネットワーク名 →v6kawasa (接続するネットワークの名称)

<ネットワーク情報追加フィールド>	
ネットワーク名	v6kawasa

##### 3. [追加] ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

##### 4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。



## 5. 以下の項目を指定します。

- MTU サイズ → 1280

■基本情報	
ネットワーク名	lv6kawasa
MTUサイズ	1280 バイト

## 6. [保存] ボタンをクリックします。

## 7. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 8. 以下を指定します。

- 接続先名 → tun-kawa
- 接続先種別 → IP トンネル接続

<接続先情報追加フィールド>	
接続先名	tun-kawa
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 <div style="display: flex; align-items: center;"> <input type="text" value="ダイヤル1"/> <input type="text" value="電話番号"/>  <input type="text" value="サブアドレス"/> </div> <input type="radio"/> フレームリレー接続 <input type="text" value="DLCI"/>
	<input type="radio"/> PPPoE接続 <input checked="" type="radio"/> IPトンネル接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄

## 9. [追加] ボタンをクリックします。

IP トンネル接続の設定項目と「基本情報」が表示されます。

## 10. 以下の項目を指定します。

- 自側エンドポイント → 172.16.184.1
- 相手側エンドポイント → 172.16.21.1

■基本情報	
接続先名	tun-kawa
自側エンドポイント	172.16.184.1
相手側エンドポイント	172.16.21.1

## 11. [保存] ボタンをクリックします。

## 12. 画面上部の「ネットワーク情報」をクリックします。

「ネットワーク情報」ページが表示されます。

## 13. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

**14. 以下の項目を指定します。**

- IPv6 →使用する

**15. [保存] ボタンをクリックします。****16. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。**

「IPv6 スタティック経路情報」が表示されます。

**17. 以下の項目を指定します。**

- ネットワーク →ネットワーク指定  
あて先ネットワーク/プレフィックス長 →2001:db8:1111:1016::/64
- メトリック値 →1

**18. [追加] ボタンをクリックします。****19. 画面左側の [設定反映] 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。

## 川崎事業所の本装置を設定する

「東京事業所の本装置を設定する」を参考に、川崎事業所の本装置を設定します。  
その際、特に指定のないものは、東京事業所と同じ設定にします。

### LAN 情報（川崎事業所）を設定する

#### 「LAN0 情報」 - 「IP 関連」

##### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する  
IP アドレス →172.16.21.1  
ネットマスク →24 (255.255.255.0)  
ブロードキャストアドレス →ネットワークアドレス+オール1

**「LAN1 情報」 - 「IP 関連」**

## 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス → 172.16.22.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

**「LAN1 情報」 - 「IPv6 関連」**

## 「IPv6 基本情報」

- IPv6 →使用する
- インタフェースID →自動
- IPv6 アドレス
  - アドレスまたはプレフィックス → 2001:db8:1111:1016::
- ルータ広報 →送信する

**IP トンネル接続の情報（東京事業所）を設定する****「相手情報」 - 「ネットワーク情報」**

- ネットワーク名 →v6tokyo（接続するネットワークの名称）

**「ネットワーク情報」 - 「共通情報」**

## 「基本情報」

- MTU サイズ → 1280

**「ネットワーク情報」 - 「IPv6 関連」**

## 「IPv6 基本情報」

- IPv6 →使用する

**「IPv6 スタティック経路情報」**

- ネットワーク →ネットワーク指定
  - あて先ネットワーク/プレフィックス長 → 2001:db8:1111:10b9::/64
- メトリック値 → 1

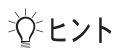
**「接続先情報」**

- 接続先名 → tun-tkyo
- 接続先種別 → IP トンネル接続

**「接続先情報」 - 「IP トンネル接続」**

## 「基本情報」

- 自側エンドポイント → 172.16.21.1
- 相手側エンドポイント → 172.16.184.1



### ◆ 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>「相手情報」－「ネットワーク情報」－「IP 関連」－「IP 基本情報」の自側 IP アドレスで設定された 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               <ul style="list-style-type: none"> <li>IP アドレス 自側エンドポイントに設定したアドレス</li> <li>ポート番号 すべて</li> </ul> </li> <li>グローバル IP 情報               <ul style="list-style-type: none"> <li>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</li> <li>ポート番号 すべて</li> </ul> </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。
  - 自側エンドポイント 192.168.1.1
  - 相手側エンドポイント 172.31.0.1

静的 NAT 設定：

- プライベート IP 情報
  - IP アドレス 192.168.1.1
  - ポート番号 すべて
- グローバル IP 情報
  - IP アドレス 172.16.0.1
  - ポート番号 すべて
- プロトコル IPv6 over IPv4

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 に本装置（NAT 未使用）を利用する場合は、相手側の本装置に以下を設定します。

自側エンドポイント 172.31.0.1  
相手側エンドポイント 172.16.0.1

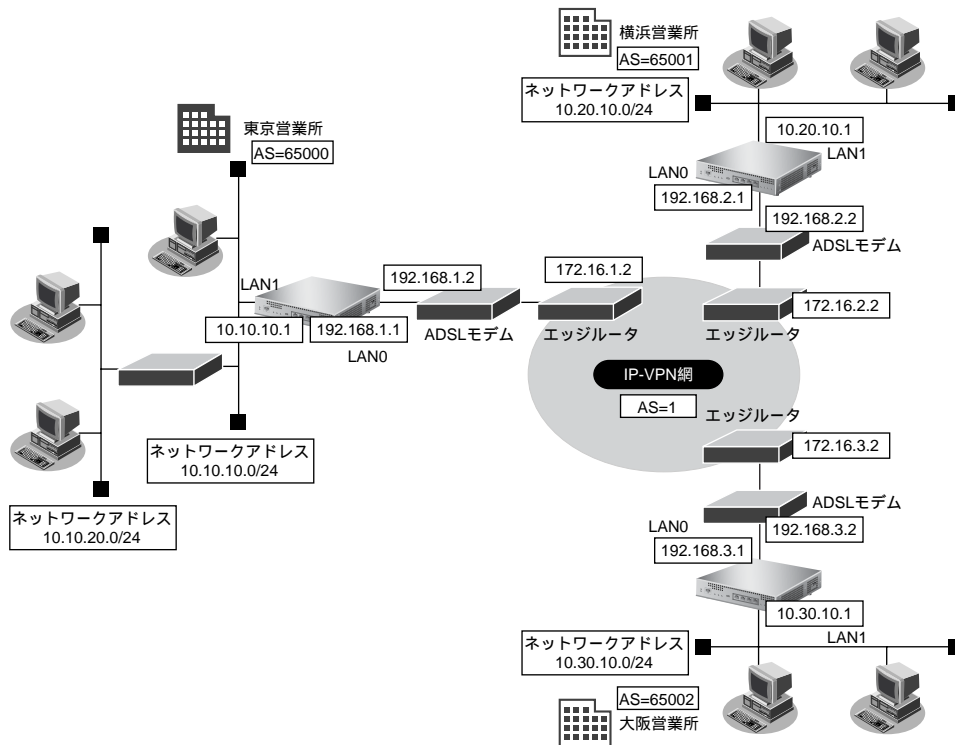
## 1.12 複数の事業所LANをIP-VPN網を利用して接続する

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 MR1000 トラブルシューティング「[ご購入時の状態に戻すには](#)」(P.42)
- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「[文字入力フィールドで入力できる文字一覧](#)」(P.13)
- 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。
- BGP の認証機能はサポートしていません。
- BGP で利用できるセッション数は使用する装置ごとに異なります。
  - ☛ 参照 MR1000 仕様一覧「[システム最大値一覧](#)」(P.19)
- 相手情報でBGPを使用する場合は、IPアドレスを設定してください。
- BGP集約経路を設定した場合、設定した集約経路アドレス/アドレスマスクよりも長いサブネットマスクの経路は受信しません。
- 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「[設定反映](#)」ボタンをクリックした場合、接続中のセッションが一度切断されることがあります。
- 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。

## 1.12.1 ADSL モデムを使用して IP-VPN 網と接続する



### ● 設定条件

- LAN0 ポートを ADSL モデムに接続する

#### 【IP-VPN 網】

- 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 : 1

#### 【東京営業所】

- IP-VPN 網側ポート : LAN0
- LAN0 側 IP アドレス : 192.168.1.1
- LAN0 側ネットワークアドレス/ネットマスク : 192.168.1.0/24
- LAN1 側 IP アドレス : 10.10.10.1
- LAN1 側ネットワークアドレス/ネットマスク : 10.10.10.0/24
- AS 番号 : 65000
- 営業所内のルーティングプロトコル : RIPv2

#### 【横浜営業所】

- IP-VPN 網側ポート : LAN0
- LAN0 側 IP アドレス : 192.168.2.1
- LAN0 側ネットワークアドレス/ネットマスク : 192.168.2.0/24
- LAN1 側 IP アドレス : 10.20.10.1
- LAN1 側ネットワークアドレス/ネットマスク : 10.20.10.0/24
- AS 番号 : 65001

**【大阪営業所】**

- IP-VPN 網側ポート : LAN0
- LAN0 側 IP アドレス : 192.168.3.1
- LAN0 側ネットワークアドレス/ネットマスク : 192.168.3.0/24
- LAN1 側 IP アドレス : 10.30.10.1
- LAN1 側ネットワークアドレス/ネットマスク : 10.30.10.0/24
- AS 番号 : 65002

**東京営業所を設定する****LAN0 情報を設定する****1. 設定メニューのルータ設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。**

「LAN0 情報 (物理 LAN)」ページが表示されます。

**3. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**4. 以下の項目を指定します。**

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 192.168.1.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

■ IP アドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IP アドレス	<input type="radio"/> DHCP で自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IP アドレス	<input type="text" value="192.168.1.1"/>
	ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス	<input type="text" value="ネットワークアドレス + オール 1"/>

**5. 【保存】 ボタンをクリックします。****6. IP 関連の設定項目の「NAT 情報」をクリックします。**

「NAT 情報」が表示されます。

**7. 以下の項目を指定します。**

- NAT の使用 → 使用しない

■ NAT 情報	
NAT の使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチ NAT <input type="radio"/> 静的 NAT のみ ※ NAT の使用と DHCP リレーサービスの併用はできません

8. [保存] ボタンをクリックします。
9. IP関連の設定項目の「スタティック経路情報」をクリックします。  
「スタティック経路情報」が表示されます。
10. 以下の項目を指定します。
  - ネットワーク → ネットワーク指定  
   あて先IPアドレス → 172.16.1.0  
   あて先アドレスマスク → 24 (255.255.255.0)  
   中継ルータアドレス → 192.168.1.2
  - メトリック値 → 1
  - 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート 中継ルータアドレス <input type="text"/>
	<input checked="" type="radio"/> ネットワーク指定 あて先IPアドレス <input type="text" value="172.16.1.0"/>
	あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	中継ルータアドレス <input type="text" value="192.168.1.2"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

11. [追加] ボタンをクリックします。

## LAN1 情報を設定する

こんな事に気をつけて

「LAN1 情報を設定する」場合は、あらかじめ物理 LAN1 定義を追加する必要があります。

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN1 の【修正】 ボタンをクリックします。  
「LAN1 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。



#### 4. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス → 10.10.10.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■ IPアドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPアドレス	<input type="radio"/> DHCPで自動的に取得する
	<input checked="" type="radio"/> 指定する
	IPアドレス <input type="text" value="10.10.10.1"/>
	ネットマスク <input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス <input type="text" value="ネットワークアドレス+オール1"/>

#### 5. [保存] ボタンをクリックします。

#### 6. IP関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

#### 7. 以下の項目を指定します。

- RIP送信 →V2 (Multicast) で送信する
- RIP受信 →V2、V2 (Multicast) で受信する

■ RIP情報	
RIP送信	<input type="radio"/> 送信しない
	<input type="radio"/> V1で送信する
	<input type="radio"/> V2で送信する
	<input checked="" type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない
	<input type="radio"/> V1で受信する
	<input checked="" type="radio"/> V2、V2(Multicast)で受信する

#### 8. [保存] ボタンをクリックします。

### ルーティングプロトコル情報を設定する

#### 1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

#### 2. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

### 3. 以下の項目を指定します。

- RIP  
BGP 経路情報 →再配布する
- BGP  
RIP 経路情報 →再配布する

■再配布情報		?
RIP	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する メトリック値: 0
	OSPF経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する メトリック値: 0
	DNS経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する メトリック値: 0
BGP	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	RIP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	OSPF経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	DNS経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する

### 4. [保存] ボタンをクリックします。

### 5. 「BGP 関連」 をクリックします。

BGP 関連の設定項目と「BGP 情報」が表示されます。

### 6. 以下の項目を指定します。

- BGP 機能 →使用する
- 自 AS 番号 → 65000

■BGP情報		?
BGP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する	
自AS番号	65000	

### 7. [保存] ボタンをクリックします。

### 8. BGP 関連の設定項目の「BGP ネットワーク情報」 をクリックします。

「BGP ネットワーク情報」が表示されます。

### 9. 以下の項目を指定します。

- あて先IPアドレス → 10.10.10.0
- あて先アドレスマスク → 24 (255.255.255.0)

<BGPネットワーク情報入力フィールド>	
あて先IPアドレス	10.10.10.0
あて先アドレスマスク	24 (255.255.255.0)

### 10. [追加] ボタンをクリックします。

### 11. BGP 関連の設定項目の「BGP 相手情報」 をクリックします。

「BGP 相手情報」が表示されます。

**12. [追加] ボタンをクリックします。**

BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。

**13. 以下の項目を指定します。**

- 相手側IPアドレス → 172.16.1.2
- 相手AS番号 → 1
- EBGP MULTIHOP → 2

■BGP相手基本情報	
相手側IPアドレス	<input type="text" value="172.16.1.2"/>
相手AS番号	<input type="text" value="1"/>
自側IPアドレス	<input type="text"/>
KeepAliveタイマ	<input type="text" value="30"/> 秒
Holdタイマ	<input type="text" value="90"/> 秒
MEDメトリック値	<input type="text" value="0"/>
ASパスプリベンド	<input type="text" value="0"/>
EBGP MULTIHOP	<input type="text" value="2"/>

必要に応じて上記以外の項目を指定します。

**14. [保存] ボタンをクリックします。****15. 画面左側の [設定反映] 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。

## 横浜営業所を設定する

---

「東京営業所を設定する」を参考に、横浜営業所を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス →192.168.2.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

#### 「NAT 情報」

- NAT の使用 →使用しない

#### 「スタティック経路情報」

- ネットワーク →ネットワーク指定
  - あて先IP アドレス →172.16.2.0
  - あて先アドレスマスク →24 (255.255.255.0)
  - 中継ルータアドレス →192.168.2.2
- メトリック値 →1
- 優先度 →0

### 「LAN1 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス →10.20.10.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「BGP 情報」

- BGP 機能 →使用する
- 自AS 番号 →65001

#### 「BGP ネットワーク情報」

- あて先IP アドレス →10.20.10.0
- あて先アドレスマスク →24 (255.255.255.0)

#### 「BGP 相手情報」 - 「BGP 相手基本情報」

- 相手側IP アドレス →172.16.2.2
- 相手AS 番号 →1
- EBGMP MULTIHOP →2

## 大阪営業所を設定する

---

「東京営業所を設定する」を参考に、大阪営業所を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス →192.168.3.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

#### 「NAT 情報」

- NAT の使用 →使用しない

#### 「スタティック経路情報」

- ネットワーク →ネットワーク指定
  - あて先IP アドレス →172.16.3.0
  - あて先アドレスマスク →24 (255.255.255.0)
  - 中継ルータアドレス →192.168.3.2
- メトリック値 →1
- 優先度 →0

### 「LAN1 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス →10.30.10.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「BGP 情報」

- BGP 機能 →使用する
- 自AS 番号 →65002

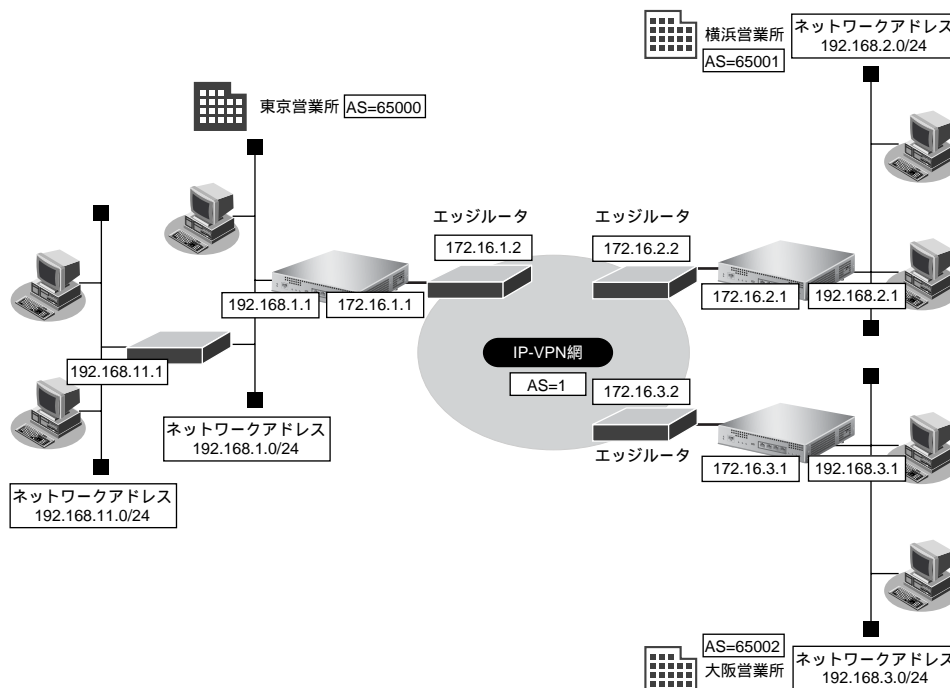
#### 「BGP ネットワーク情報」

- あて先IP アドレス →10.30.10.0
- あて先アドレスマスク →24 (255.255.255.0)

#### 「BGP 相手情報」 - 「BGP 相手基本情報」

- 相手側IP アドレス →172.16.3.2
- 相手AS 番号 →1
- EBGp MULTIHOP →2

## 1.12.2 高速デジタル専用線を使用して IP-VPN 網と接続する



### ● 設定条件

- ISDN ポートで専用線に接続する

#### 【IP-VPN 網】

- 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 : 1

#### 【東京営業所】

- LAN 側の IP アドレス : 192.168.1.1
- LAN 側のネットワークアドレス/ネットマスク : 192.168.1.0/24
- サブ LAN 側のネットワークアドレス/ネットマスク : 192.168.11.0/24
- サブ LAN 側のルーティングプロトコル : RIPv2
- WAN 側の IP アドレス : 172.16.1.1
- AS 番号 : 65000

#### 【横浜営業所】

- LAN 側の IP アドレス : 192.168.2.1
- LAN 側のネットワークアドレス/ネットマスク : 192.168.2.0/24
- WAN 側の IP アドレス : 172.16.2.1
- AS 番号 : 65001

#### 【大阪営業所】

- LAN 側の IP アドレス : 192.168.3.1
- LAN 側のネットワークアドレス/ネットマスク : 192.168.3.0/24
- WAN 側の IP アドレス : 172.16.3.1
- AS 番号 : 65002

## 東京営業所を設定する

### LAN0 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。  
「LAN0 情報（物理 LAN）」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. 以下の項目を指定します。
  - IPv4 →使用する
  - IP アドレス →指定する
    - IP アドレス → 192.168.1.1
    - ネットマスク → 24 (255.255.255.0)
    - ブロードキャストアドレス →ネットワークアドレス+オール1

■ IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IPアドレス	<input type="text" value="192.168.1.1"/>
	ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス	<input type="text" value="ネットワークアドレス+オール1"/>

5. 【保存】 ボタンをクリックします。
6. IP 関連の設定項目の「NAT 情報」をクリックします。  
「NAT 情報」が表示されます。
7. 以下の項目を指定します。
  - NAT の使用 →使用しない

■ NAT 情報	
NAT の使用	<input checked="" type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチ NAT <input type="radio"/> 静的 NAT のみ ※ NAT の使用と DHCP リレー サービス の併用 は できま せん

8. 【保存】 ボタンをクリックします。
9. IP 関連の設定項目の「RIP 情報」をクリックします。  
「RIP 情報」が表示されます。

## 10. 以下の項目を指定します。

- RIP送信 → V2 (Multicast) で送信する
- RIP受信 → V2、V2 (Multicast) で受信する

■ RIP情報	
RIP送信	<input type="radio"/> 送信しない <input type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input checked="" type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input type="radio"/> V1で受信する <input checked="" type="radio"/> V2、V2(Multicast)で受信する

## 11. [保存] ボタンをクリックします。

### IP-VPN 網と接続する相手情報を設定する

#### 1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

#### 2. 以下の項目を指定します。

- 回線インタフェース → 専用線

<WAN情報追加フィールド>	
回線インタフェース	専用線

#### 3. [追加] ボタンをクリックします。

「WAN0 情報 (専用線)」ページが表示されます。

#### 4. 「基本情報」をクリックします。

「基本情報」が表示されます。

#### 5. 以下の項目を指定します。

- 回線速度 → 128Kbps

■ 基本情報	
ポート	基本 0
回線速度	128Kbps

#### 6. [保存] ボタンをクリックします。

#### 7. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

#### 8. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。



## 9. 以下の項目を指定します。

- ネットワーク名 → IP-VPN

<ネットワーク情報追加フィールド>	
ネットワーク名	IP-VPN

## 10. [追加] ボタンをクリックします。

「ネットワーク情報 (IP-VPN)」 ページが表示されます。

## 11. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 12. 以下の項目を指定します。

- 接続先名 → ip-vpn
- 接続先種別 → 専用線接続

<接続先情報追加フィールド>	
接続先名	ip-vpn
接続先種別	<input checked="" type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 <div style="display: flex; align-items: center;"> <input type="text" value="ダイヤル1"/> <input type="text" value="電話番号"/>  <input type="text" value="サブアドレス"/> </div> <input type="radio"/> フレームリレー接続 <input type="text" value="DLCI"/>
	<input type="radio"/> PPPoE接続 <input type="radio"/> IPトンネル接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄

## 13. [追加] ボタンをクリックします。

専用線接続の設定項目と「基本情報」が表示されます。

## 14. 以下の項目を指定します。

- 使用インターフェース → WAN0

■基本情報	
接続先名	ip-vpn
使用インターフェース	WAN0
DNSサーバ	

## 15. [保存] ボタンをクリックします。

## 16. 画面上部の「ネットワーク情報 (IP-VPN)」をクリックします。

「ネットワーク情報 (IP-VPN)」が表示されます。

## 17. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

**18. 以下の項目を指定します。**

- IPアドレス →設定する
  - 相手側IPアドレス → 172.16.1.2
  - 自側IPアドレス → 172.16.1.1

■ IP基本情報				
IPアドレス	<input type="radio"/> 設定しない			
	<input checked="" type="radio"/> 設定する			
	<table border="1"> <tr> <td>相手側IPアドレス</td> <td>172.16.1.2</td> </tr> <tr> <td>自側IPアドレス</td> <td>172.16.1.1</td> </tr> </table>	相手側IPアドレス	172.16.1.2	自側IPアドレス
相手側IPアドレス	172.16.1.2			
自側IPアドレス	172.16.1.1			

**19. [保存] ボタンをクリックします。****ルーティングプロトコル情報を設定する****1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**2. 「ルーティングマネージャ情報」をクリックします。**

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

**3. 以下の項目を指定します。**

- RIP
  - BGP経路情報 →再配布する
- BGP
  - RIP経路情報 →再配布する

■再配布情報		
RIP	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する メトリック値: 0
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
BGP	インタフェース経路情報	<input type="radio"/> 再配布しない <input type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する

**4. [保存] ボタンをクリックします。****5. 「BGP関連」をクリックします。**

BGP関連の設定項目と「BGP情報」が表示されます。

## 6. 以下の項目を指定します。

- BGP機能 →使用する
- 自AS番号 →65000

■BGP情報	
BGP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
自AS番号	65000

## 7. [保存] ボタンをクリックします。

## 8. BGP関連の設定項目の「BGPネットワーク情報」をクリックします。

「BGPネットワーク情報」が表示されます。

## 9. 以下の項目を指定します。

- あて先IPアドレス →192.168.1.0
- あて先アドレスマスク →24 (255.255.255.0)

<BGPネットワーク情報入力フィールド>	
あて先IPアドレス	192.168.1.0
あて先アドレスマスク	24 (255.255.255.0)

## 10. [追加] ボタンをクリックします。

## 11. BGP関連の設定項目の「BGP相手情報」をクリックします。

「BGP相手情報」が表示されます。

## 12. [追加] ボタンをクリックします。

BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。

## 13. 以下の項目を指定します。

- 相手側IPアドレス →172.16.1.2
- 相手AS番号 →1

■BGP相手基本情報	
相手側IPアドレス	172.16.1.2
相手AS番号	1

必要に応じて上記以外の項目を指定します。

## 14. [保存] ボタンをクリックします。

## 15. 画面左側の [設定反映] 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。

## 横浜営業所を設定する

---

「東京営業所を設定する」を参考に、横浜営業所を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス →192.168.2.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

#### 「NAT 情報」

- NAT の使用 →使用しない

### 「WAN0 情報」

- 回線インタフェース →専用線
- 回線速度 →128Kbps

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 →IP-VPN

#### 「接続先情報」

- 接続先名 →ip-vpn
- 接続先種別 →専用線接続

#### 「接続先情報」 - 「専用線接続」

##### 「基本情報」

- 使用インタフェース →WAN0

### 「ネットワーク情報」 - 「IP 関連」

#### 「IP 基本情報」

- IP アドレス →設定する
  - 相手側IP アドレス →172.16.2.2
  - 自側IP アドレス →172.16.2.1

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「BGP 情報」

- BGP 機能 →使用する
- 自AS 番号 →65001

#### 「BGP ネットワーク情報」

- あて先IP アドレス →192.168.2.0
- あて先アドレスマスク →24 (255.255.255.0)

#### 「BGP 相手情報」 - 「BGP 相手基本情報」

- 相手側IP アドレス →172.16.2.2
- 相手AS 番号 →1

## 大阪営業所を設定する

---

「東京営業所を設定する」を参考に、大阪営業所を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 192.168.3.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

#### 「NAT 情報」

- NAT の使用 → 使用しない

### 「WAN0 情報」

- 回線インタフェース → 専用線
- 回線速度 → 128Kbps

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → IP-VPN

#### 「接続先情報」

- 接続先名 → ip-vpn
- 接続先種別 → 専用線接続

#### 「接続先情報」 - 「専用線接続」

##### 「基本情報」

- 使用インタフェース → WAN0

### 「ネットワーク情報」 - 「IP 関連」

#### 「IP 基本情報」

- IP アドレス → 設定する
  - 相手側 IP アドレス → 172.16.3.2
  - 自側 IP アドレス → 172.16.3.1

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「BGP 情報」

- BGP 機能 → 使用する
- 自 AS 番号 → 65002

#### 「BGP ネットワーク情報」

- あて先 IP アドレス → 192.168.3.0
- あて先アドレスマスク → 24 (255.255.255.0)

#### 「BGP 相手情報」 - 「BGP 相手基本情報」

- 相手側 IP アドレス → 172.16.3.2
- 相手 AS 番号 → 1

---

**⚠注意**

- BGP4 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、BGP4 機能を使用しないでください。
  - BGP セッションで使用する WAN インタフェースのインタフェース経路（ホストルート）を BGP で広報した場合、BGP セッションの接続・切断を繰り返す場合があります。該当するインタフェース経路は BGP で広報しないように設定してください。該当しないインタフェース経路を BGP で広報する場合は、以下のどちらかを設定してください。
    - BGP にインタフェース経路を再配布しないで、広報するインタフェース経路を BGP ネットワークとして設定します。
    - BGP にインタフェース経路を再配布し、該当するインタフェース経路を BGP フィルタリングで送信を破棄するように設定します。
-

## 1.13 NAT を併用しない固定 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。

ここでは以下の条件によって、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)】

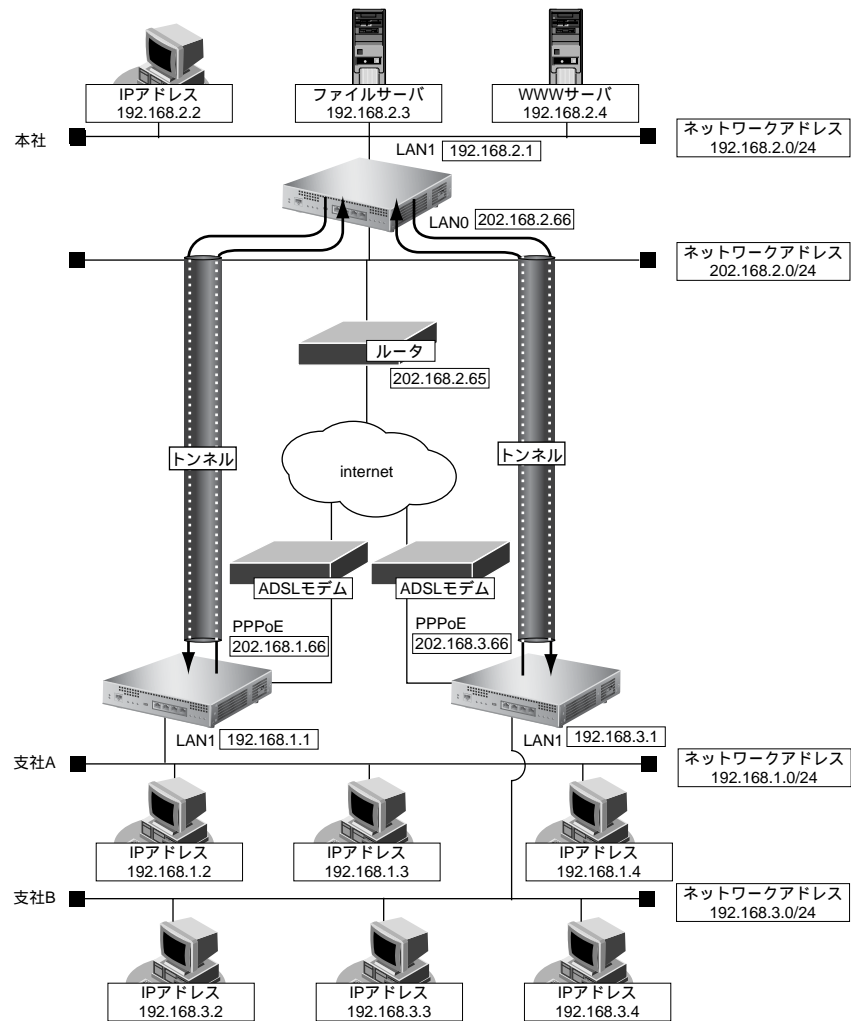
- ローカルネットワーク IP アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.1.66/24
- PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE LAN ポート : LAN0 ポート使用

#### 【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
- 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 LAN ポート : LAN0 ポート使用

#### 【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-I192.168.1.0/24
- 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 使用
- 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 : shared
- 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 使用
- 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設定例を示します。

## 支社 A の IPsec/IKE を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

### 6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先 IP アドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先 IP アドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	honsya
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インタフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**12. 以下の項目を指定します。**

- 鍵交換モード → Main Mode 使用
- 相手側エンドポイント → 202.168.2.66
- 自側エンドポイント → 202.168.1.66

鍵交換モード	<input checked="" type="radio"/> Main Mode 使用
	相手側エンドポイント <input type="text" value="202.168.2.66"/>
	自側エンドポイント <input type="text" value="202.168.1.66"/>

**13. [保存] ボタンをクリックします。****14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**15. 以下の項目を指定します。**

- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

SA の設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	<input type="text" value="使用しない"/>
	SA有効時間	<input type="text" value="8"/> 時間
	SA有効データ量	<input type="text" value="0"/> GByte

**16. [保存] ボタンをクリックします。**

**17.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

**18.** 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■ IKE情報		
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**19.** [保存] ボタンをクリックします。**20.** 画面左側の [設定反映] 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。

## 支社BのIPsec/IKEを設定する

---

「支社AのIPsec/IKEを設定する」を参考に、支社Bを設定します。

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → vpn-hon

### 「ネットワーク情報」 - 「IP関連」

#### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.3.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

### 「接続先情報」

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

### 「接続先情報」 - 「IPsec/IKE 接続」

#### 「基本情報」

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 202.168.2.66
- 自側エンドポイント → 202.168.3.66

#### 「IPsec情報」

- SAの設定
- 暗号アルゴリズム → 3des-cbc
- 認証アルゴリズム → hmac-sha1

#### 「IKE情報」

- IKE 認証鍵
- 鍵種別 → 文字列
- 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SAの設定
- 暗号アルゴリズム → 3des-cbc
- 認証 (ハッシュ) アルゴリズム → hmac-sha1
- DHグループ → modp1024

## 本社のIPsec/IKEを設定する

### 支社A向けの設定をする

**1. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**2. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**3. 以下の項目を指定します。**

- ネットワーク名 → vpn-shiA

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shiA

**4. [追加] ボタンをクリックします。**

「ネットワーク情報 (vpn-shiA)」ページが表示されます。

**5. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**6. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**7. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>				
ネットワーク	<input type="radio"/> デフォルトルート			
	<input checked="" type="radio"/> ネットワーク指定			
	<table border="1"> <tr> <td>あて先IPアドレス</td> <td>192.168.1.0</td> </tr> <tr> <td>あて先アドレスマスク</td> <td>24 (255.255.255.0)</td> </tr> </table>	あて先IPアドレス	192.168.1.0	あて先アドレスマスク
あて先IPアドレス	192.168.1.0			
あて先アドレスマスク	24 (255.255.255.0)			
メトリック値	1			
優先度	0			

**8. [追加] ボタンをクリックします。**

**9. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → shisyaA
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	shisyaA
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 <div style="border: 1px solid black; padding: 2px; margin: 5px 0;">           ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>                              <input type="text"/> サブアドレス <input type="text"/> </div> <input type="radio"/> フレームリレー接続 <input type="text"/> DLCI <input type="text"/> <input type="radio"/> PPPoE接続 <input type="radio"/> IPトンネル接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄

## 11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 202.168.1.66
- 自側エンドポイント → 202.168.2.66

鍵交換モード	<input checked="" type="radio"/> Main Mode使用	
	相手側エンドポイント	202.168.1.66
	自側エンドポイント	202.168.2.66

## 13. [保存] ボタンをクリックします。

## 14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

SA の設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

16. [保存] ボタンをクリックします。

17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

18. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DH グループ → modp768 (グループ 1)

■ IKE 情報		
IKE 認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE 認証方式		shared
ポート番号		500
SA の設定	暗号アルゴリズム	des-cbc
	認証 (ハッシュ) アルゴリズム	hmac-md5
	DH グループ	modp768 (グループ 1)
	SA 有効時間	24 時間

19. [保存] ボタンをクリックします。

20. 画面左側の [設定反映] 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。



## 支社B向けの設定をする

「支社A向けを設定する」を参考に、支社B向けを設定します。

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → vpn-shiB

### 「ネットワーク情報」 - 「IP関連」

#### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.3.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

### 「接続先情報」

- 接続先名 → shisyaB
- 接続先種別 → IPsec/IKE 接続

### 「接続先情報」 - 「IPsec/IKE 接続」

#### 「基本情報」

- 鍵交換モード → Main Mode 使用
- 相手側エンドポイント → 202.168.3.66
- 自側エンドポイント → 202.168.2.66

#### 「IPsec情報」

- SAの設定
- 暗号アルゴリズム → 3des-cbc
- 認証アルゴリズム → hmac-sha1

#### 「IKE情報」

- IKE 認証鍵
- 鍵種別 → 文字列
- 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SAの設定
- 暗号アルゴリズム → 3des-cbc
- 認証 (ハッシュ) アルゴリズム → hmac-sha1
- DHグループ → modp1024

## 1.14 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。

ここでは以下の条件によって、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】

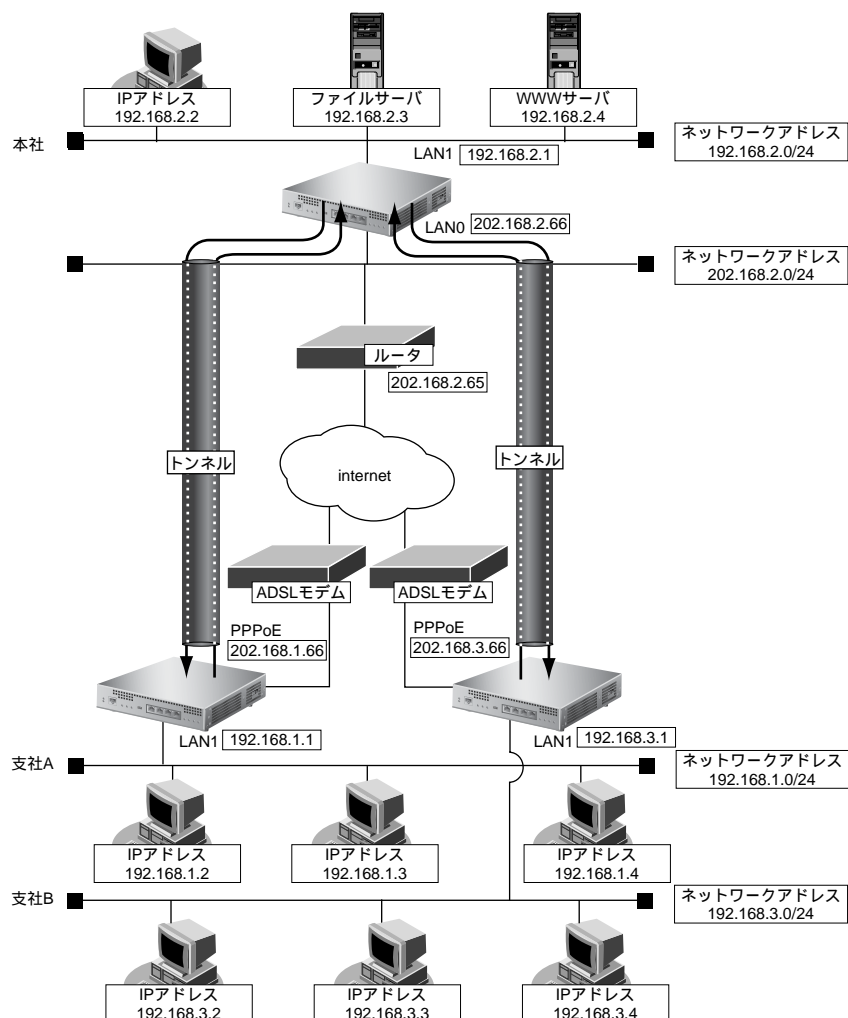
- ローカルネットワーク IP アドレス : 192.168.1.1/24
- インターネットプロバイダから割り当てられた固定 IP アドレス : 202.168.1.66/24
- グローバルネットワーク IP アドレス : 10.0.1.1/24
- PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE LAN ポート : LAN0 ポート使用

#### 【支社 B】

- 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 LAN ポート : LAN0 ポート使用

#### 【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-I192.168.1.0/24
- 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 : any4-1192.168.3.0/24

**[共通 A]**

- 鍵交換タイプ : Main Mode 使用
- 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 : shared
- 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 使用
- 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設定例を示します。

## 支社 A を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 「ネットワーク情報」でネットワーク名が internet の【修正】ボタンをクリックします。

「ネットワーク情報 (internet)」ページが表示されます。

### 4. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

### 5. IP 関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

### 6. 以下の項目を指定します。

- プライベート IP 情報
  - IP アドレス → 202.168.1.66
  - ポート番号 → isakmp
- グローバル IP 情報
  - IP アドレス → 10.0.1.1
  - ポート番号 → isakmp
- プロトコル → udp

＜静的NAT情報入力フィールド＞		
プライベート IP 情報	IP アドレス	202.168.1.66
	ポート番号	isakmp (番号指定: [ ] "その他"を選択時のみ有効です)
グローバル IP 情報	IP アドレス	10.0.1.1
	ポート番号	isakmp (番号指定: [ ] "その他"を選択時のみ有効です)
プロトコル		udp (番号指定: [ ] "その他"を選択時のみ有効です)

### 7. [追加] ボタンをクリックします。

### 8. 手順 6. ～ 7. を参考に、以下の項目を指定します。

- プライベート IP 情報
  - IP アドレス → 202.168.1.66
  - 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

**9. 画面上部の「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**10. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**11. 以下の項目を指定します。**

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

**12. [追加] ボタンをクリックします。**

「ネットワーク情報 (vpn-hon)」ページが表示されます。

**13. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP 基本情報」が表示されます。

**14. IP 関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**15. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先 IP アドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先 IP アドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**16. [追加] ボタンをクリックします。****17. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

## 18. 以下の項目を指定します。

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	honsya
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 ダイヤル1 電話番号 <input type="text"/> サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続 DLCI <input type="text"/> <input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

## 19. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 20. 以下の項目を指定します。

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 202.168.2.66
- 自側エンドポイント → 202.168.1.66

鍵交換モード	<input checked="" type="radio"/> Main Mode使用
	相手側エンドポイント <input type="text" value="202.168.2.66"/>
	自側エンドポイント <input type="text" value="202.168.1.66"/>

## 21. [保存] ボタンをクリックします。

## 22. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

## 23. 以下の項目を指定します。

- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

SA の設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	<input type="text" value="使用しない"/>
	SA有効時間	<input type="text" value="β"/> 時間
	SA有効データ量	<input type="text" value="0"/> GByte

## 24. [保存] ボタンをクリックします。

**25. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

**26. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ 1)

■ IKE情報		
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**27. [保存] ボタンをクリックします。****28. 画面左側の [設定反映] 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。



## 支社Bを設定する

「支社Aを設定する」を参考に、支社Bを設定します。

### 「相手情報」 - 「ネットワーク情報」

#### 「ネットワーク情報」 - 「IP 関連」

##### 「静的NAT 情報」

- プライベートIP 情報
  - IPアドレス → 202.168.3.66
  - ポート番号 → isakmp
- グローバル IP 情報
  - IPアドレス → 10.0.3.1
  - ポート番号 → isakmp
- プロトコル → udp
- プライベートIP 情報
  - IPアドレス → 202.168.3.66
  - 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

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → vpn-hon

#### 「ネットワーク情報」 - 「IP 関連」

##### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
- あて先 IP アドレス → 192.168.2.0
- あて先アドレスマスク → 24 ( 255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

##### 「接続先情報」

- 接続先名 → honshya
- 接続先種別 → IPsec/IKE 接続

#### 「接続先情報」 - 「IPsec/IKE 接続」

##### 「基本情報」

- 鍵交換モード → Main Mode 使用
- 相手側エンドポイント → 202.168.2.66
- 自側エンドポイント → 202.168.3.66

##### 「IPsec 情報」

- SA の設定
  - 暗号アルゴリズム → 3des-cbc
  - 認証アルゴリズム → hmac-sha1

##### 「IKE 情報」

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321

- SAの設定
  - 暗号アルゴリズム → 3des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-sha1
  - DHグループ → modp1024

## 本社のIPsec/IKEを設定する

### 支社A向けの設定をする

#### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

#### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

#### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shiA

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shiA

#### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shiA)」ページが表示されます。

#### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

#### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

#### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

#### 8. [追加] ボタンをクリックします。

#### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → shisyaA
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	shisyaA
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 <div style="display: flex; align-items: center;"> <input type="text" value="ダイヤル1"/> <input type="text" value="電話番号"/> </div> <div style="display: flex; align-items: center;"> <input type="text" value="サブアドレス"/> </div>
	<input type="radio"/> フレームリレー接続 <input type="text" value="DLCI"/>
	<input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**12. 以下の項目を指定します。**

- 鍵交換モード → Main Mode 使用
- 相手側エンドポイント → 10.0.1.1
- 自側エンドポイント → 202.168.2.66

鍵交換モード	<input checked="" type="radio"/> Main Mode 使用	
	相手側エンドポイント	10.0.1.1
	自側エンドポイント	202.168.2.66

**13. [保存] ボタンをクリックします。****14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- 対象パケット
  - 自側IPアドレス/マスク → IPv4 すべて
  - 相手側IPアドレス/マスク → 指定する
  - 192.168.1.0/24
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv4 すべて (“指定する”を選択時のみ有効です。)
	相手側IPアドレス/マスク	指定する (“指定する”を選択時のみ有効です。) 192.168.1.0 / 24 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

## 16. [保存] ボタンをクリックします。

## 17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

## 18. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ 1)

■ IKE情報		
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	abcdefghijklmnopqrstuvwxyz1234567890
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

## 19. [保存] ボタンをクリックします。

## 20. 画面左側の [設定反映] 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。

## 支社 B 向けの設定をする

「支社 A 向けを設定する」を参考に、支社 B を設定します。

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → vpn-shiB

### 「ネットワーク情報」 - 「IP 関連」

#### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
- あて先 IP アドレス → 192.168.3.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

### 「接続先情報」

- 接続先名 → shisyaB
- 接続先種別 → IPsec/IKE 接続

### 「接続先情報」 - 「IPsec/IKE 接続」

#### 「基本情報」

- 鍵交換モード → Main Mode 使用
- 相手側エンドポイント → 10.0.3.1
- 自側エンドポイント → 202.168.2.66

#### 「IPsec 情報」

- 対象パケット
  - 自側 IP アドレス/マスク → IPv4 すべて
  - 相手側 IP アドレス/マスク → 指定する  
→ 192.168.3.0/24
- SA の設定
  - 暗号アルゴリズム → 3des-cbc
  - 認証アルゴリズム → hmac-sha1

#### 「IKE 情報」

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  - 暗号アルゴリズム → 3des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-sha1
  - DH グループ → modp1024

## 1.15 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、以下の条件によって、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)】

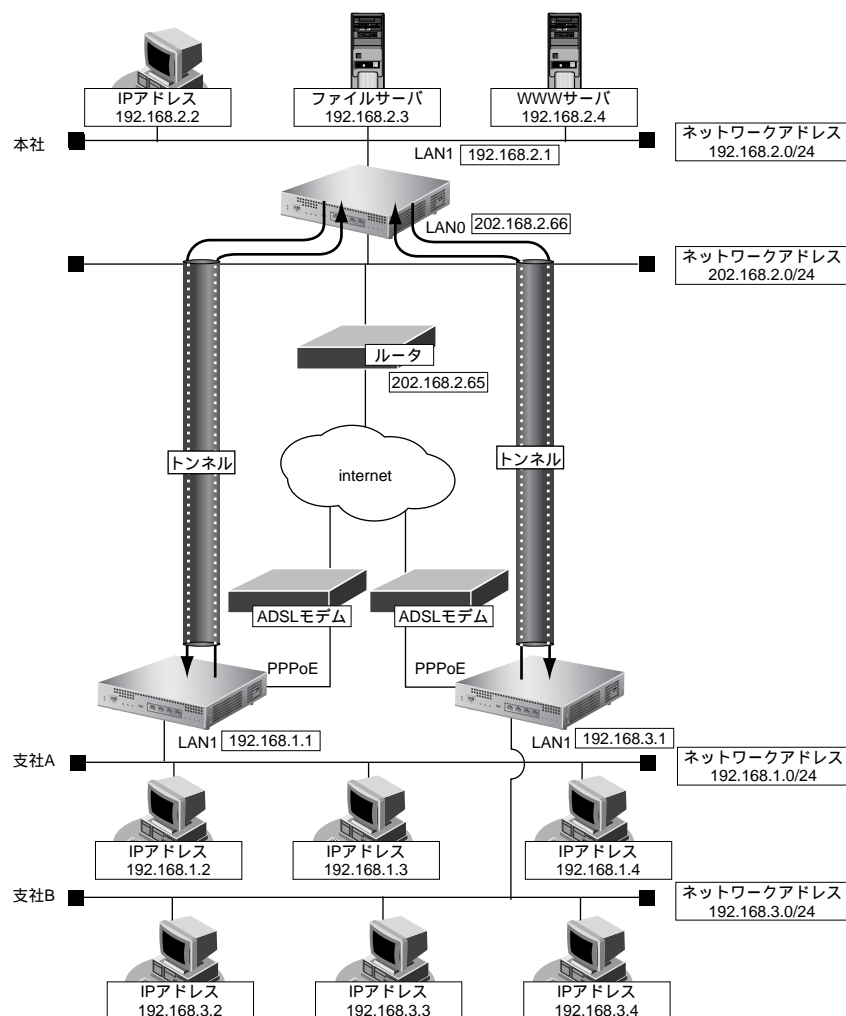
- ローカルネットワーク IP アドレス : 192.168.1.1/24
- PPPoE ユーザ認証 ID : userid1 (プロバイダから提示された内容)
- PPPoE ユーザ認証パスワード : userpass1 (プロバイダから提示された内容)
- PPPoE LAN ポート : LAN0 ポート使用

#### 【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 LAN ポート : LAN0 ポート使用

#### 【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

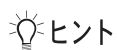
**【共通 A】**

- 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 : shared
- 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設定例を示します。

## 支社 A (Initiator) を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」でネットワーク名が internet の【修正】ボタンをクリックします。  
「ネットワーク情報 (internet)」ページが表示されます。
4. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
5. IP 関連の設定項目の「静的 NAT 情報」をクリックします。  
「静的 NAT 情報」が表示されます。

## 6. 以下の項目を指定します。

- プライベートIP 情報
  - IPアドレス → 192.168.1.1
  - ポート番号 → isakmp
- グローバルIP 情報
  - IPアドレス → 指定しない
  - ポート番号 → isakmp
- プロトコル → udp

＜静的NAT情報入力フィールド＞		
プライベートIP情報	IPアドレス	192.168.1.1
	ポート番号	isakmp (番号指定: [ ] “その他”を選択時のみ有効です)
グローバルIP情報	IPアドレス	
	ポート番号	isakmp (番号指定: [ ] “その他”を選択時のみ有効です)
プロトコル		udp (番号指定: [ ] “その他”を選択時のみ有効です)

## 7. [追加] ボタンをクリックします。

## 8. 手順 6. ～7. を参考に、以下の項目を指定します。

- プライベートIP 情報
  - IPアドレス → 192.168.1.1
  - 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

## 9. 画面上部の「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 10. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

## 11. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

＜ネットワーク情報追加フィールド＞	
ネットワーク名	vpn-hon

## 12. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

## 13. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

## 14. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

**15. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定  
あて先IPアドレス → 192.168.2.0  
あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**16. [追加] ボタンをクリックします。****17. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**18. 以下の項目を指定します。**

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	<input type="text" value="honsya"/>
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 ダイヤル1 電話番号 <input type="text"/> サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続 DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

**19. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**20. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode(Initiator) 使用
- 相手側エンドポイント → 202.168.2.66
- 自装置識別情報 → shisyaA

鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Initiator)使用	
	自側エンドポイント	<input type="text"/>
	相手側エンドポイント	202.168.2.66
	自装置識別情報	shisyaA
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**21. [保存] ボタンをクリックします。****22. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**23. 以下の項目を指定します。**

- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

SA の設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

**24. [保存] ボタンをクリックします。****25. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

## 26. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DH グループ → modp768 (グループ 1)

IKE情報		
IKE 認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE 認証方式		shared
ポート番号		500
SA の設定	暗号アルゴリズム	des-cbc
	認証 (ハッシュ) アルゴリズム	hmac-md5
	DH グループ	modp768 (グループ 1)
	SA 有効時間	24 時間

## 27. [保存] ボタンをクリックします。

## 28. 画面左側の [設定反映] 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。

こんな事に気をつけて

IKE 認証鍵には、文字列か数値 (16 進数) を使用することができます。鍵として数値を入力したつもりでも、鍵識別で文字列を指定していると、文字列として認識されてしまうために、鍵が一致しない原因になります。

## 支社 B (Initiator) を設定する

「支社 A (Initiator) を設定する」を参考に、支社 B (Initiator) を設定します。

「相手情報」 - 「ネットワーク情報」

「ネットワーク情報」 - 「IP 関連」

「静的 NAT 情報」

- プライベート IP 情報
  - IP アドレス → 192.168.3.1
  - ポート番号 → isakmp
- グローバル IP 情報
  - IP アドレス → 指定しない
  - ポート番号 → isakmp
- プロトコル → udp
- プライベート IP 情報
  - IP アドレス → 192.168.3.1
  - 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

#### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → vpn-hon

#### 「ネットワーク情報」 - 「IP 関連」

##### 「スタティック経路情報」

- ネットワーク → ネットワーク指定  
あて先 IP アドレス → 192.168.2.0  
あて先アドレスマスク → 24 ( 255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

##### 「接続先情報」

- 接続先名 → honshya
- 接続先種別 → IPsec/IKE 接続

#### 「接続先情報」 - 「IPsec/IKE 接続」

##### 「基本情報」

- 鍵交換モード → Aggressive Mode (Initiator) 使用  
相手側エンドポイント → 202.168.2.66  
自装置識別情報 → shisyaB

##### 「IPsec 情報」

- SA の設定  
暗号アルゴリズム → 3des-cbc  
認証アルゴリズム → hmac-sha1

##### 「IKE 情報」

- IKE 認証鍵  
鍵種別 → 文字列  
鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定  
暗号アルゴリズム → 3des-cbc  
認証 (ハッシュ) アルゴリズム → hmac-sha1  
DH グループ → modp1024

## 本社 (Responder) を設定する

### 支社 A 向けの設定をする

**1. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**2. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**3. 以下の項目を指定します。**

- ネットワーク名 → vpn-shiA

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shiA

**4. [追加] ボタンをクリックします。**

「ネットワーク情報 (vpn-shiA)」ページが表示されます。

**5. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**6. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**7. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先 IP アドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>					
	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定				
ネットワーク	<table border="1"> <tr> <td>あて先IPアドレス</td> <td>192.168.1.0</td> </tr> <tr> <td>あて先アドレスマスク</td> <td>24 (255.255.255.0)</td> </tr> </table>	あて先IPアドレス	192.168.1.0	あて先アドレスマスク	24 (255.255.255.0)
あて先IPアドレス	192.168.1.0				
あて先アドレスマスク	24 (255.255.255.0)				
メトリック値	1				
優先度	0				

**8. [追加] ボタンをクリックします。**

**9. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → shisyaA
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	shisyaA
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インターフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**12. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode (Responder) 使用
- 自側エンドポイント → 202.168.2.66
- 相手装置識別情報 → shisyaA

鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Responder)使用
	自側エンドポイント <input type="text"/> 202.168.2.66
	相手側エンドポイント <input type="text"/>
	相手装置識別情報 <input type="text"/> shisyaA
	IDタイプ <input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**13. [保存] ボタンをクリックします。****14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。



## 15. 以下の項目を指定します。

- 対象パケット
  - 自側IPアドレス/マスク → IPv4 すべて
  - 相手側IPアドレス/マスク → 指定する
  - 192.168.1.0/24
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		?
対象パケット	自側IPアドレス/マスク	IPv4すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	指定する (“指定する”を選択時のみ有効です。) 192.168.1.0 / 24 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	β 時間
	SA有効データ量	0 GByte

## 16. [保存] ボタンをクリックします。

## 17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

## 18. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ 1)

■ IKE情報		?
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

## 19. [保存] ボタンをクリックします。

## 20. 画面左側の [設定反映] 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。

## 支社 B 向けの設定をする

「支社 A 向けを設定する」を参考に、支社 B 向けを設定します。

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → vpn-shiB

### 「ネットワーク情報」 - 「IP 関連」

#### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
- あて先 IP アドレス → 192.168.3.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

### 「ネットワーク情報」 - 「接続先情報」

- 接続先名 → shisyaB
- 接続先種別 → IPsec/IKE 接続

### 「接続先情報」 - 「IPsec/IKE 接続」

#### 「基本情報」

- 鍵交換モード → Aggressive Mode (Responder) 使用
- 自側エンドポイント → 202.168.2.66
- 相手装置識別情報 → shisyaB

#### 「IPsec 情報」

- 対象パケット
  - 自側 IP アドレス/マスク → IPv4 すべて
  - 相手側 IP アドレス/マスク → 指定する
  - 192.168.3.0/24
- SA の設定
  - 暗号アルゴリズム → 3des-cbc
  - 認証アルゴリズム → hmac-sha1

#### 「IKE 情報」

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → ABCDEFGHIJKLMNOPQRSTUVWXYZ0987654321
- SA の設定
  - 暗号アルゴリズム → 3des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-sha1
  - DH グループ → modp1024S

## 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)	166
2.1.1	特定の経路情報の送信を許可する	167
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	169
2.1.3	特定の経路情報の受信を許可する	171
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	173
2.1.5	特定の経路情報の送信を禁止する	176
2.1.6	特定の経路情報の受信を禁止する	178
2.2	RIPの経路を制御する (IPv6)	180
2.2.1	特定の経路情報の送信を許可する	182
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	184
2.2.3	特定の経路情報の受信を許可する	186
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	188
2.2.5	特定の経路情報の送信を禁止する	191
2.2.6	特定の経路情報の受信を禁止する	193
2.3	OSPFv2を使用したネットワークを構築する (IPv4)	195
2.3.1	バーチャルリンクを使う	202
2.3.2	スタブエリアを使う	210
2.4	OSPFの経路を制御する (IPv4)	222
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	222
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	225
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	229
2.5	BGPの経路を制御する (IPv4)	233
2.5.1	特定の経路情報の受信を透過させる	233
2.5.2	特定のASからの経路情報の受信を遮断する	235
2.5.3	IP-VPN 網からの受信情報の他IP-VPN 網への送信を遮断する	237
2.5.4	冗長構成の通信経路を使用する	239
2.6	事業所間をMPLS 接続サービスを利用して接続する	243
2.6.1	トンネルエンドポイントをインタフェースアドレスにしてMPLS LSPを使用する	244
2.6.2	トンネルエンドポイントをインタフェースアドレスとは別のアドレスにしてMPLS LSPを使用する	253
2.7	MPLSを使用したレイヤ2VPN (EoMPLS) を構築する	263
2.8	MPLSを使用したレイヤ3VPN (BGP/MPLS VPN) を構築する	271

2.8.1	MPLS 網とLANを使用して接続する	272
2.8.2	MPLS 網と専用線を使用して接続する	283
2.9	マルチリンク機能を使う	294
2.10	マルチキャスト機能を使う	296
2.10.1	マルチキャスト機能 (PIM-DM) を使う	296
2.10.2	マルチキャスト機能 (PIM-SM) を使う	300
2.11	VLAN 機能を使う	305
2.12	IP フィルタリング機能を使う	309
2.12.1	外部の特定サービスへのアクセスだけ許可する	313
2.12.2	外部から特定サーバへのアクセスだけ許可する	325
2.12.3	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	338
2.12.4	外部の特定サービスへのアクセスだけ許可する (IPv6 フィルタリング)	348
2.12.5	外部の特定サーバへのアクセスだけを禁止する	358
2.12.6	利用者が意図しない発信を防ぐ	362
2.12.7	回線が接続しているときだけ許可する	365
2.12.8	外部から特定サーバへのpingだけを禁止する	367
2.13	IPsec 機能を使う	373
2.13.1	IPv4 over IPv4 で固定IPアドレスでのVPN (手動鍵交換)	376
2.13.2	IPv4 over IPv6 で固定IPアドレスでのVPN (自動鍵交換)	384
2.13.3	IPv4 over IPv6 で可変IPアドレスでのVPN (自動鍵交換)	392
2.13.4	IPv6 over IPv4 で固定IPアドレスでのVPN (自動鍵交換)	400
2.13.5	IPv6 over IPv4 で可変IPアドレスでのVPN (自動鍵交換)	410
2.13.6	IPv6 over IPv6 で固定IPアドレスでのVPN (自動鍵交換)	421
2.13.7	IPv6 over IPv6 で可変IPアドレスでのVPN (自動鍵交換)	430
2.13.8	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)	440
2.13.9	IPsec 機能と他機能との併用	452
2.14	システムログを採取する	471
2.15	マルチNAT機能 (アドレス変換機能) を使う	473
2.15.1	プライベートLAN接続でサーバを公開する	474
2.15.2	PPPoE接続でサーバを公開する	476
2.15.3	ネットワーク型接続でサーバを公開する	479
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	482
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	484
2.16	VoIP NATトラバーサル機能を使う	486
2.17	TOS/Traffic Class 値書き換え機能を使う	488
2.18	VLANプライオリティマッピング機能を使う	491
2.19	シェーピング機能を使う	493
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	493
2.19.2	送信先ごとにシェーピング機能を使う	494
2.20	データ圧縮/ヘッダ圧縮機能を使う	498
2.21	帯域制御 (WFQ) 機能を使う	500
2.22	DHCP 機能を使う	504
2.22.1	DHCPサーバ機能を使う	505
2.22.2	DHCPスタティック機能を使う	508
2.22.3	DHCPクライアント機能を使う	510
2.22.4	DHCPリレーエージェント機能を使う	512

2.22.5	IPv6 DHCPクライアント機能を使う	516
2.23	DNSサーバ機能を使う (ProxyDNS)	520
2.23.1	DNSサーバの自動切り替え機能 (順引き) を使う	520
2.23.2	DNSサーバの自動切り替え機能 (逆引き) を使う	522
2.23.3	DNSサーバアドレスの自動取得機能を使う	524
2.23.4	DNS問い合わせタイプフィルタ機能を使う	526
2.23.5	DNSサーバ機能を使う	528
2.24	特定のURLへのアクセスを禁止する (URLフィルタ機能)	530
2.25	SNMPエージェント機能を使う	532
2.26	ECMP機能を使う	534
2.27	VRRP機能を使う	573
2.27.1	簡易ホットスタンバイ機能を使う	574
2.27.2	クラスタリング機能を使う	578
2.28	マルチルーティング機能を使う	583
2.29	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)	586
2.29.1	リモートパワーオン情報を設定する	587
2.29.2	リモートパワーオン機能を使う	587
2.30	スケジュール機能を使う	588
2.30.1	スケジュールを予約する	588
2.30.2	電話番号変更を予約する	590
2.30.3	構成定義情報の切り替えを予約する	591
2.31	通信料金を節約する (課金制御機能)	593
2.31.1	課金単位時間を設定する	593
2.31.2	課金制御機能を設定する	595
2.32	ブリッジ/STP機能を使う	597
2.32.1	ブリッジでFNAをつないでSTP機能を使う	597
2.32.2	ブリッジグルーピング機能を使う	604
2.32.3	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)	611
2.33	複数のLANポートをスイッチングHUBのように使う	617
2.34	ISDN接続を契機とした通信バックアップを使う	620
2.35	外部のパソコンからPIAFS接続する	627
2.36	アナログモデムで通信バックアップをする	633
2.37	外部のパソコンから着信接続する (リモートアクセスサーバ)	639

## 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

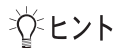
#### 指定条件

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
- フィルタリング条件 (IPアドレス/アドレスマスク)
- 方向
- 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

フィルタリング条件 : 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、経路情報の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

フィルタリング条件 : 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) 192.168.1.1/24が設定されているインタフェースで 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。

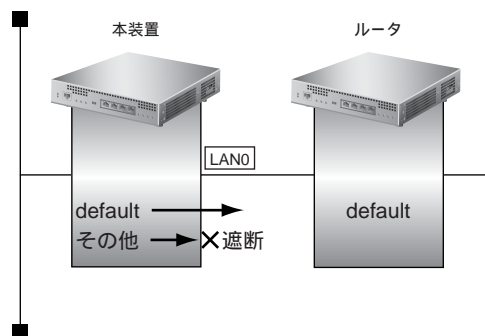
- 特定の経路情報の送信を禁止する
- 特定の経路情報の受信を禁止する

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みを送信だけを許可し、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。



#### ● 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みを送信だけを許可
- 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例を示します。

#### 1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の「修正」ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

5. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → デフォルトルート
- メトリック値 → 指定しない

<RIP フィルタリング情報入力フィールド>						
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信					
フィルタリング条件	<input type="radio"/> すべて					
	<input checked="" type="radio"/> デフォルトルート					
	<input type="radio"/> 経路情報指定					
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IP アドレス</td> <td><input type="text"/></td> </tr> <tr> <td>アドレスマスク</td> <td>0 (0.0.0.0) <input type="text"/></td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IP アドレス	<input type="text"/>	アドレスマスク
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致					
IP アドレス	<input type="text"/>					
アドレスマスク	0 (0.0.0.0) <input type="text"/>					
メトリック値	<input type="text"/>					

6. 「追加」ボタンをクリックします。

7. 手順 5. ~ 6. を参考に、以下の項目を指定します。

- 動作 → 遮断
- 方向 → 送信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

8. 画面左側の「設定反映」ボタンをクリックします。

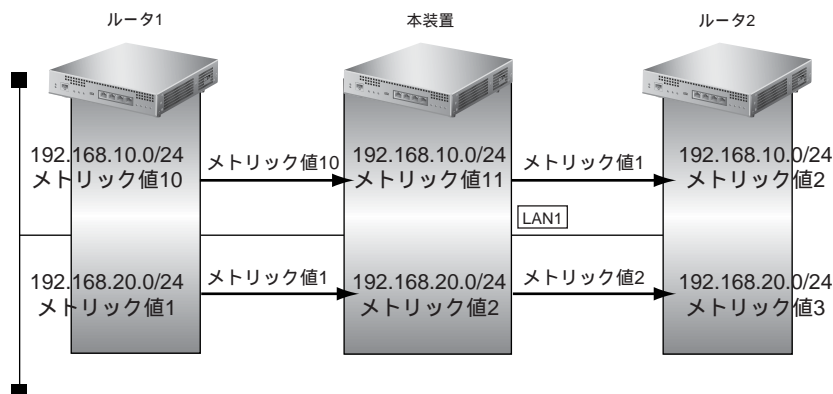
設定した内容が有効になります。



## 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。



### ● 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例を示します。

#### 1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

#### 2. 「LAN 情報」でインターフェースが LAN1 の【修正】 ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

#### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

#### 4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - IPアドレス → 192.168.10.0
  - アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1

<RIPフィルタリング情報入力フィールド>						
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信					
フィルタリング条件	<input type="radio"/> すべて					
	<input type="radio"/> デフォルトルート					
	<input checked="" type="radio"/> 経路情報指定					
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IPアドレス</td> <td>192.168.10.0</td> </tr> <tr> <td>アドレスマスク</td> <td>24 (255.255.255.0)</td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス	192.168.10.0	アドレスマスク
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致					
IPアドレス	192.168.10.0					
アドレスマスク	24 (255.255.255.0)					
メトリック値	1					

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

## 8. 画面左側の [設定反映] ボタンをクリックします。

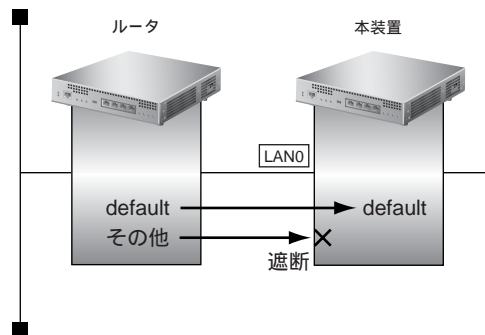
設定した内容が有効になります。

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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。  
「RIP フィルタリング情報」が表示されます。
5. 以下の項目を指定します。
  - 動作 → 透過
  - 方向 → 受信
  - フィルタリング条件 → デフォルトルート
  - メトリック値 → 指定しない

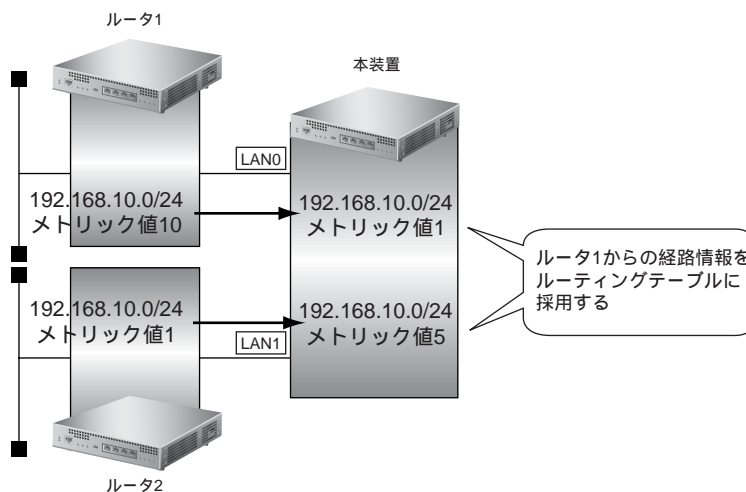
<RIPフィルタリング情報入力フィールド>						
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信					
フィルタリング条件	<input type="radio"/> すべて					
	<input checked="" type="radio"/> デフォルトルート					
	<input type="radio"/> 経路情報指定					
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IPアドレス</td> <td><input type="text"/></td> </tr> <tr> <td>アドレスマスク</td> <td>0 (0.0.0.0)</td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス	<input type="text"/>	アドレスマスク
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致					
IPアドレス	<input type="text"/>					
アドレスマスク	0 (0.0.0.0)					
メトリック値	<input type="text"/>					

6. **〔追加〕 ボタンをクリックします。**
7. **手順 5. ～ 6. を参考に、以下の項目を指定します。**
  - 動作 → 遮断
  - 方向 → 受信
  - フィルタリング条件 → すべて
  - メトリック値 → 指定しない
8. **画面左側の〔設定反映〕 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。

## 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。



### ● 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例を示します。

#### 1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

#### 2. 「LAN 情報」でインターフェースがLAN0の【修正】ボタンをクリックします。

「LAN0 情報（物理 LAN）」ページが表示されます。

#### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

#### 4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - IPアドレス → 192.168.10.0
  - アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1

<RIPフィルタリング情報入力フィールド>							
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断						
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信						
フィルタリング条件	<input type="radio"/> すべて <input type="radio"/> デフォルトルート <input checked="" type="radio"/> 経路情報指定						
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IPアドレス</td> <td>192.168.10.0</td> </tr> <tr> <td>アドレスマスク</td> <td>24 (255.255.255.0) ▼</td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス	192.168.10.0	アドレスマスク	24 (255.255.255.0) ▼
	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致					
	IPアドレス	192.168.10.0					
アドレスマスク	24 (255.255.255.0) ▼						
メトリック値	1						

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

## 8. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

## 9. 「LAN 情報」でインタフェースが LAN1 の [修正] ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

## 10. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

## 11. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。

「RIP フィルタリング情報」が表示されます。

**12. 手順 5. ～ 6. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件
  - 経路情報指定 → 経路情報指定
  - 検索条件 → 完全に一致
  - IP アドレス → 192.168.10.0
  - アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 5

**13. 手順 5. ～ 6. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

**14. 画面左側の [設定反映] ボタンをクリックします。**

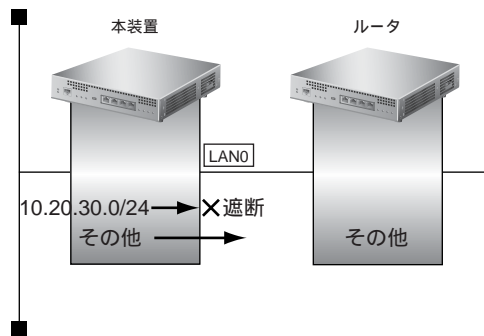
設定した内容が有効になります。

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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。  
「RIP フィルタリング情報」が表示されます。



## 5. 以下の項目を指定します。

- 動作 →遮断
- 方向 →送信
- フィルタリング条件 →経路情報指定
  - 検索条件 →完全に一致
  - IPアドレス →10.20.30.0
  - アドレスマスク →24 (255.255.255.0)
- メトリック値 →指定しない

<RIPフィルタリング情報入力フィールド>						
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断					
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信					
フィルタリング条件	<input type="radio"/> すべて					
	<input type="radio"/> デフォルトルート					
	<input checked="" type="radio"/> 経路情報指定					
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IPアドレス</td> <td><input type="text" value="10.20.30.0"/></td> </tr> <tr> <td>アドレスマスク</td> <td><input type="text" value="24 (255.255.255.0)"/></td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス	<input type="text" value="10.20.30.0"/>	アドレスマスク
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致					
IPアドレス	<input type="text" value="10.20.30.0"/>					
アドレスマスク	<input type="text" value="24 (255.255.255.0)"/>					
メトリック値	<input type="text"/>					

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

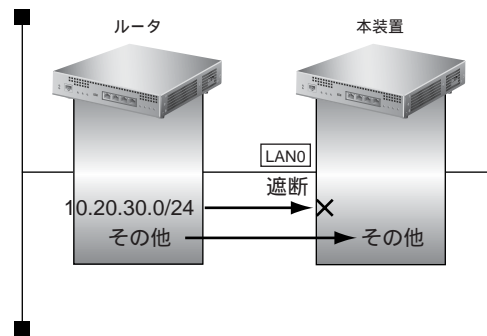
- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて
- メトリック値 →指定しない

## 8. 画面左側の [設定反映] 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。

## 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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。  
「LAN0 情報（物理 LAN）」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「RIP フィルタリング情報」をクリックします。  
「RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 →遮断
- 方向 →受信
- フィルタリング条件 →経路情報指定
  - 検索条件 →完全に一致
  - IPアドレス →10.20.30.0
  - アドレスマスク →24 (255.255.255.0)
- メトリック値 →指定しない

<RIPフィルタリング情報入力フィールド>						
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断					
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信					
フィルタリング条件	<input type="radio"/> すべて					
	<input type="radio"/> デフォルトルート					
	<input checked="" type="radio"/> 経路情報指定					
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IPアドレス</td> <td><input type="text" value="10.20.30.0"/></td> </tr> <tr> <td>アドレスマスク</td> <td><input type="text" value="24 (255.255.255.0)"/></td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス	<input type="text" value="10.20.30.0"/>	アドレスマスク
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致					
IPアドレス	<input type="text" value="10.20.30.0"/>					
アドレスマスク	<input type="text" value="24 (255.255.255.0)"/>					
メトリック値	<input type="text"/>					

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作 →透過
- 方向 →受信
- フィルタリング条件 →すべて
- メトリック値 →指定しない

## 8. 画面左側の [設定反映] 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。

## 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
- 経路情報 (プレフィックス/プレフィックス長)
- 方向
- 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。



#### ヒント

##### ◆ 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。

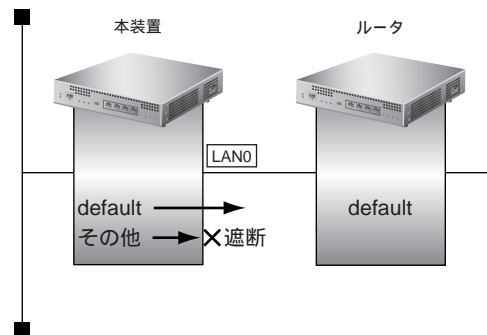
RIP 受信時には、優先順位の高い定義から順に受信方向の条件を参照し、一致した条件があった時点で定義された動作を行います。一致した以降の条件は参照されません。また、受信方向のすべての条件に一致しない RIP 経路情報は遮断されます。

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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の「修正」ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。  
「IPv6 RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → デフォルトルート
- メトリック値 → 指定しない

<IPv6 RIPフィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信				
フィルタリング条件	<input type="radio"/> すべて				
	<input checked="" type="radio"/> デフォルトルート				
	<input type="radio"/> 経路情報指定				
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>プレフィックス /プレフィックス長</td> <td><input type="text"/></td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	プレフィックス /プレフィックス長	<input type="text"/>
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致				
プレフィックス /プレフィックス長	<input type="text"/>				
メトリック値	<input type="text"/>				

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作 → 遮断
- 方向 → 送信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

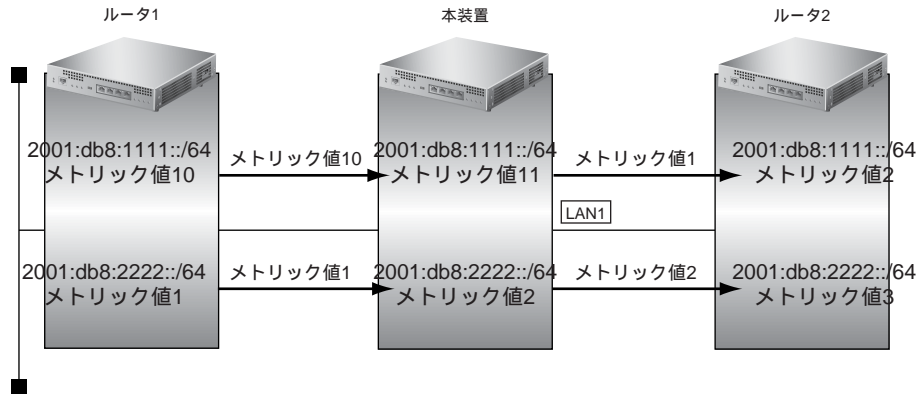
## 8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

## 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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインターフェースがLAN0の【修正】ボタンをクリックします。  
「LAN0情報（物理 LAN）」ページが表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。  
「IPv6 RIP フィルタリング情報」が表示されます。



## 5. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - プレフィックス/プレフィックス長 → 2001:db8:1111::/64
- メトリック値 → 1

<IPv6 RIPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信
フィルタリング条件	<input type="radio"/> すべて <input type="radio"/> デフォルトルート <input checked="" type="radio"/> 経路情報指定
	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
	プレフィックス/プレフィックス長 <input type="text" value="2001:db8:1111::"/> / <input type="text" value="64"/>
メトリック値	<input type="text" value="1"/>

## 6. [追加] ボタンをクリックします。

## 7. 手順5.～6.を参考に、以下の項目を指定します。

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

## 8. 画面左側の [設定反映] ボタンをクリックします。

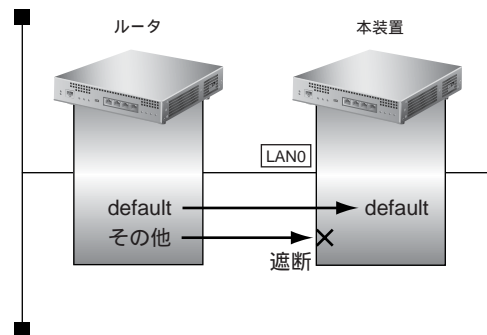
設定した内容が有効になります。

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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。  
「IPv6 RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → デフォルトルート
- メトリック値 → 指定しない

<IPv6 RIPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信
フィルタリング条件	<input type="radio"/> すべて
	<input checked="" type="radio"/> デフォルトルート
	<input type="radio"/> 経路情報指定
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
プレフィックス /プレフィックス長	<input type="text"/> / <input type="text"/>
メトリック値	<input type="text"/>

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

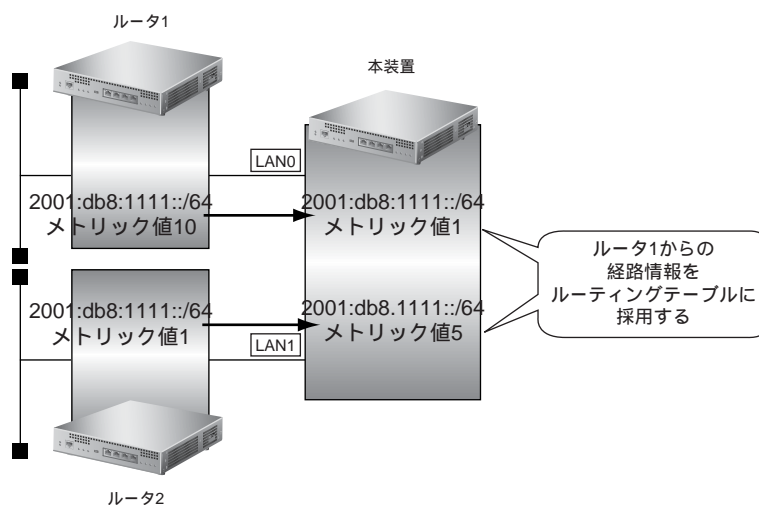
- 動作 → 遮断
- 方向 → 受信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

## 8. 画面左側の [設定反映] 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。

## 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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。  
「IPv6 RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - プレフィックス/プレフィックス長 → 2001:db8:1111::/64
- メトリック値 → 1

<IPv6 RIPフィルタリング情報入力フィールド>					
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断				
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信				
フィルタリング条件	<input type="radio"/> すべて				
	<input type="radio"/> デフォルトルート				
	<input checked="" type="radio"/> 経路情報指定				
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>プレフィックス/プレフィックス長</td> <td>2001:db8:1111:: / 64</td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	プレフィックス/プレフィックス長	2001:db8:1111:: / 64
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致				
プレフィックス/プレフィックス長	2001:db8:1111:: / 64				
メトリック値	1				

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

## 8. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

## 9. 「LAN 情報」でインタフェースが LAN1 の [修正] ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

## 10. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

## 11. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。

「IPv6 RIP フィルタリング情報」が表示されます。

## 12. 手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - プレフィックス/プレフィックス長 → 2001:db8:1111::/64
- メトリック値 → 5

**13. 手順 5. ～6. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

**14. 画面左側の [設定反映] ボタンをクリックします。**

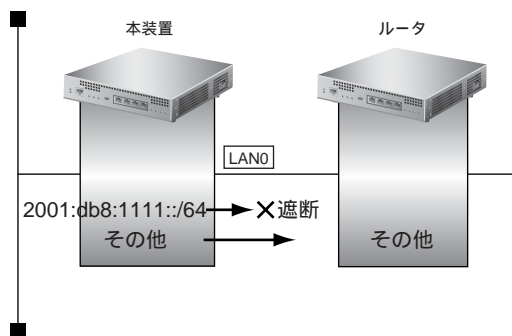
設定した内容が有効になります。

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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。  
「LAN0情報（物理 LAN）」ページが表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。  
「IPv6 RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 遮断
- 方向 → 送信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - プレフィックス/プレフィックス長 → 2001:db8:1111::/64
- メトリック値 → 指定しない

<IPv6 RIPフィルタリング情報入力フィールド>	
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信
フィルタリング条件	<input type="radio"/> すべて <input type="radio"/> デフォルトルート <input checked="" type="radio"/> 経路情報指定
	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
	プレフィックス/プレフィックス長 <input type="text" value="2001:db8:1111::"/> / <input type="text" value="64"/>
メトリック値	<input type="text"/>

## 6. [追加] ボタンをクリックします。

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

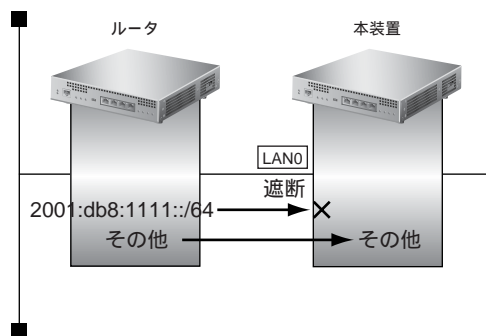
## 8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。



## 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。



### ● 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例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 RIP フィルタリング情報」をクリックします。  
「IPv6 RIP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 遮断
- 方向 → 受信
- フィルタリング条件
  - 検索条件 → 完全に一致
  - プレフィックス/プレフィックス長 → 2001:db8:1111::/64
- メトリック値 → 指定しない

<IPv6 RIPフィルタリング情報入力フィールド>	
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信
フィルタリング条件	<input type="radio"/> すべて <input type="radio"/> デフォルトルート <input checked="" type="radio"/> 経路情報指定
	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
	プレフィックス/プレフィックス長 <input type="text" value="2001:db8:1111::"/> / <input type="text" value="64"/>
メトリック値	<input type="text"/>

## 6. [追加] ボタンをクリックします。

## 7. 手順 5.～6. を参考に、以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → すべて
- メトリック値 → 指定しない

## 8. 画面左側の [設定反映] 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。

## 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。

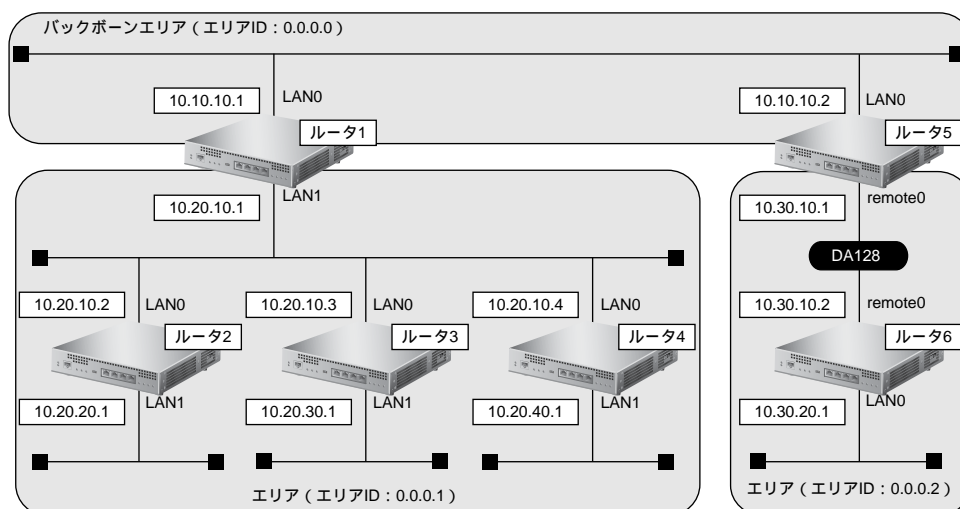
☞ 参照 MR1000 機能説明書 [2.5 OSPF 機能] (P.33)

### 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。
- 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ルータ同士は、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オーバーフロー)。
 

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、本装置の電源を再投入したり、または【設定反映】ボタンや【再起動】ボタンをクリックしても、正常に通信ができるまでに最大60分かかります。
- OSPF使用中に【設定反映】ボタンをクリックした場合、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で使用するインタフェースは、以下の条件で使用してください。

項目	条件
インタフェース数	(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。



ここでは、ルータ5とルータ6が専用線 (remote定義) で接続され、以下のとおりに設定されていることを前提とします。

**● 前提条件**

- ルータ1からルータ6のすべてのインタフェースにIPアドレスを設定する
- ルータ1からルータ6のすべてのインタフェースでNAT機能およびDHCPクライアント機能を使用しない

**● 設定条件**

- ルータ5およびルータ6は、ISDNポートで専用線に接続する

**[ルータ1でのルーティングプロトコル情報]**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN1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]**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN0でのルータ優先度 : 1
- LAN1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]**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN0でのルータ優先度 : 255
- LAN1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]**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1
- LAN1でのpassive-interface設定 : 設定する
- LAN0でのルータ優先度 : 1

**[ルータ5でのルーティングプロトコル情報]**

- LAN0でのルーティングプロトコル : OSPF
- remote定義でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- remote定義でのOSPFエリアID : 0.0.0.2
- エリア0.0.0.2への集約経路設定 : 10.30.0.0/16

**[ルータ6でのルーティングプロトコル情報]**

- LAN0でのルーティングプロトコル : OSPF

- remote 定義でのルーティングプロトコル : OSPF
- LAN0でのOSPF エリアID : 0.0.0.2
- remote 定義でのOSPF エリアID : 0.0.0.2
- LAN0でのpassive-interface設定 : 設定する

上記の設定条件に従って設定を行う場合の設定例を示します。

## ルータ 1 を設定する

### LAN 情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。  
「LAN0情報（物理 LAN）」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
5. 以下の項目を指定します。
  - OSPF 機能 →使用する
  - エリア定義番号 →0

OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. [保存] ボタンをクリックします。
7. 手順 2.～6. を参考に、「LAN1 情報（物理 LAN）」で以下の項目を指定します。

「LAN1 情報（物理 LAN）」 - 「IP 関連」

「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →1
- 指定ルータ優先度 →0

### OSPF 関連を設定する

8. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」ページが表示されます。
9. 「OSPF 関連」をクリックします。  
OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

**10. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。**

「OSPF エリア情報」が表示されます。

**11. [追加] ボタンをクリックします。**

OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。

**12. 以下の項目を指定します。**

- エリアID → 0.0.0.0

■OSPFエリア基本情報	
エリアID	0.0.0.0

**13. [保存] ボタンをクリックします。****14. 画面上部のルーティングプロトコル情報をクリックします。**

OSPF 関連項目と「OSPF エリア情報」が表示されます。

**15. 手順 11. ~ 13. を参考に、以下の項目を指定します。**

「OSPF エリア情報 (1)」 - 「OSPF エリア基本情報」

- エリアID → 0.0.0.1

**16. OSPF エリア情報 (1) の「経路集約情報」をクリックします。**

「経路集約情報」が表示されます。

**17. 以下の項目を指定します。**

- ネットワークアドレス → 10.20.0.0
- ネットマスク → 16 (255.255.0.0)

<経路集約情報入力フィールド>	
ネットワークアドレス	10.20.0.0
ネットマスク	16 (255.255.0.0)

**18. [追加] ボタンをクリックします。****19. 画面左側の [設定反映] 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。

## ルータ2を設定する

---

「ルータ1を設定する」を参考に、ルータ2を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0
- 指定ルータ優先度 →1

### 「LAN1 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0
- パケット送信 →抑止する

### 「ルーティングプロトコル情報」 - 「OSPF 関連」

#### 「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.1

## ルータ3を設定する

---

「ルータ1を設定する」を参考に、ルータ3を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0
- 指定ルータ優先度 →255

### 「LAN1 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0
- パケット送信 →抑止する

### 「ルーティングプロトコル情報」 - 「OSPF 関連」

#### 「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.1

## ルータ4を設定する

---

「ルータ1を設定する」を参考に、ルータ4を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0
- 指定ルータ優先度 →1

### 「LAN1 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0
- パケット送信 →抑止する

### 「ルーティングプロトコル情報」 - 「OSPF 関連」

#### 「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.1

## ルータ5を設定する

---

「ルータ1を設定する」を参考に、ルータ5を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0

### 「ルーティングプロトコル情報」 - 「OSPF 関連」

#### 「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.0

#### 「OSPF エリア情報 (1)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.2
- 経路集約情報
  - ネットワークアドレス →10.30.0.0
  - ネットマスク →16 (255.0.0.0)

## ルータ6と接続する remote 定義に OSPF 機能を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. OSPF 機能を設定するネットワーク欄の [修正] ボタンをクリックします。  
「ネットワーク情報」ページが表示されます。



4. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
5. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
6. 以下の項目を指定します。
  - OSPF 機能 →使用する
  - エリア定義番号 →1

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	1

7. 「保存」ボタンをクリックします。
8. 画面左側の「設定反映」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。

## ルータ 6 を設定する

「ルータ 1 を設定する」および「ルータ 5 を設定する」を参考に、ルータ 6 を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0
- パケット送信 →抑止する

### 「ルーティングプロトコル情報」 - 「OSPF 関連」

#### 「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.2

### 「相手情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0

こんな事に気をつけて

remote 定義で使用する場合は、IP アドレスを必ず設定してください。

#### ⚠注意

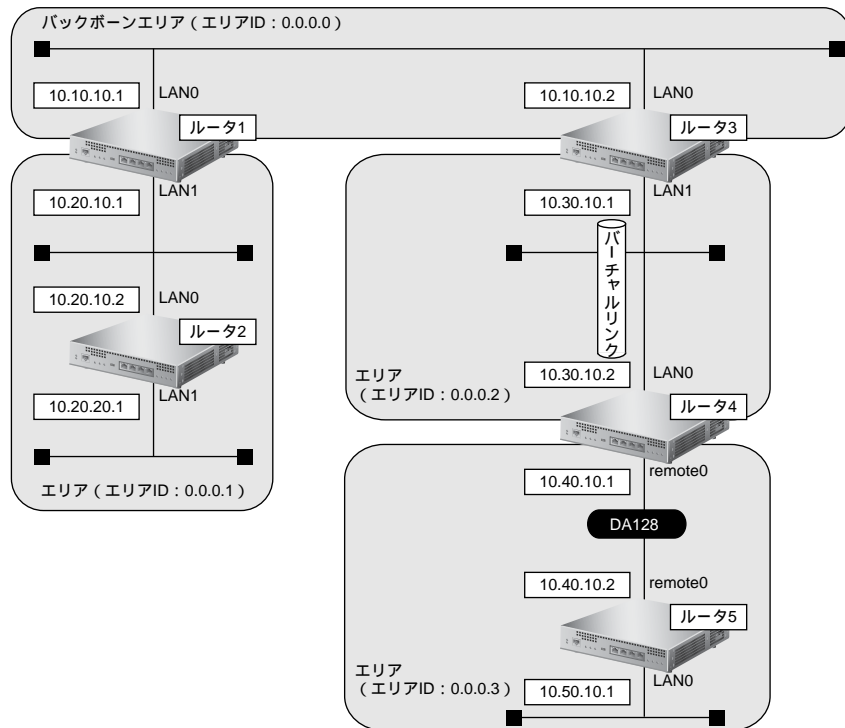
OSPF 機能を使用する場合、定期的にパケットを送信します。このため、定額制でない回線を使用している場合は、超過課金の原因となることがあります。このような環境では、OSPF 機能は使用しないでください。

## 2.3.1 バーチャルリンクを使う

バックボーンエリアと直接接続できないエリアを、バーチャルリンクを使用して接続する設定方法について説明します。

こんな事に気をつけて

- バーチャルリンクは、スタブエリア、準スタブエリアを経由して使用することはできません。
- バーチャルリンクを使用する場合は、OSPF ルータ ID を設定する必要があります。設定する際は、OSPF ルータ ID が重複しないように設定してください。



ここでは、ルータ4とルータ5が専用線（remote定義）で接続され、以下のとおりに設定されていることを前提とします。

### ● 前提条件

- ルータ1からルータ5のすべてのインタフェースにIPアドレスを設定する
- ルータ1からルータ5のすべてのインタフェースでNAT機能およびDHCPクライアント機能を使用しない

**● 設定条件**

- ルータ4およびルータ5は、ISDNポートで専用線に接続する

**【ルータ1でのルーティングプロトコル情報】**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.1

**【ルータ2でのルーティングプロトコル情報】**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1でのOSPFエリアID : 0.0.0.1

**【ルータ3でのルーティングプロトコル情報】**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1でのOSPFエリアID : 0.0.0.2
- OSPFルータID : 10.30.10.1
- バーチャルリンク接続先OSPFルータID : 10.40.10.1

**【ルータ4でのルーティングプロトコル情報】**

- LAN0でのルーティングプロトコル : OSPF
- remote定義でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.2
- remote定義でのOSPFエリアID : 0.0.0.3
- OSPFルータID : 10.40.10.1
- バーチャルリンク接続先OSPFルータID : 10.30.10.1

**【ルータ5でのルーティングプロトコル情報】**

- LAN0でのルーティングプロトコル : OSPF
- remote定義でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.3
- remote定義でのOSPFエリアID : 0.0.0.3

上記の設定条件に従って設定を行う場合の設定例を示します。

## ルータ1を設定する

### LAN0 情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
5. 以下の項目を指定します。
  - OSPF 機能 → 使用する
  - エリア定義番号 → 0

OSPF 情報	
OSPF 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. 【保存】 ボタンをクリックします。
7. 手順 2. ~ 6. を参考に、「LAN1 情報 (物理 LAN)」で以下の項目を指定します。

「LAN1 情報 (物理 LAN)」 - 「IP 関連」

「OSPF 情報」

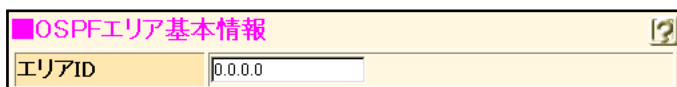
- OSPF 機能 → 使用する
- エリア定義番号 → 1

### OSPF 関連を設定する

8. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」ページが表示されます。
9. 「OSPF 関連」をクリックします。  
OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
10. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。  
「OSPF エリア情報」が表示されます。
11. 【追加】 ボタンをクリックします。  
OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。

**12. 以下の項目を指定します。**

- エリアID → 0.0.0.0

**13. [保存] ボタンをクリックします。****14. 画面上部のルーティングプロトコル情報をクリックします。**

OSPF関連の設定項目と「OSPF エリア情報」が表示されます。

**15. 手順 11. ～ 13. を参考に、以下の項目を指定します。**

「OSPF エリア情報 (1)」 - 「OSPF エリア基本情報」

- エリアID → 0.0.0.1

**16. 画面左側の [設定反映] 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。

## ルータ2を設定する

---

「ルータ1を設定する」を参考に、ルータ2を設定します。

「LAN0 情報」 - 「IP 関連」

「OSPF 情報」

- OSPF 機能 → 使用する
- エリア定義番号 → 0

「LAN1 情報」 - 「IP 関連」

「OSPF 情報」

- OSPF 機能 → 使用する
- エリア定義番号 → 0

「ルーティングプロトコル情報」 - 「OSPF 関連」

「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID → 0.0.0.1

## ルータ3を設定する

---

### LAN0 情報を設定する

**1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。**

「LAN0 情報 (物理 LAN)」ページが表示されます。

**3. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP関連の設定項目の「OSPF情報」をクリックします。

「OSPF情報」が表示されます。

5. 以下の項目を指定します。

- OSPF機能 →使用する
- エリア定義番号 →0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. [保存] ボタンをクリックします。

7. 手順2.～6.を参考に、以下の項目を指定します。

「LAN1情報」 - 「IP関連」

「OSPF情報」

- OSPF機能 →使用する
- エリア定義番号 →1

### OSPF関連を設定する

8. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

9. 「OSPF関連」をクリックします。

OSPF関連の設定項目と「ルータID情報」が表示されます。

10. 以下の項目を指定します。

- ルータID →10.30.10.1

■ルータID情報	
ルータID	<input type="text" value="10.30.10.1"/>

11. [保存] ボタンをクリックします。

12. OSPF関連の設定項目の「OSPFエリア情報」をクリックします。

「OSPFエリア情報」が表示されます。

13. [追加] ボタンをクリックします。

OSPFエリア情報 (0) の「OSPFエリア基本情報」が表示されます。

14. 以下の項目を指定します。

- エリアID →0.0.0.0

■OSPFエリア基本情報	
エリアID	<input type="text" value="0.0.0.0"/>

15. [保存] ボタンをクリックします。
16. 画面上部のルーティングプロトコル情報をクリックします。  
OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。
17. 手順 13. ～ 15. を参考に、以下の項目を指定します。  
「OSPF エリア情報 (1)」 - 「OSPF エリア基本情報」
  - エリアID → 0.0.0.2
18. OSPF エリア情報 (1) の設定項目の「バーチャルリンク情報」をクリックします。  
「バーチャルリンク情報」が表示されます。
19. 以下の項目を指定します。
  - 接続先ルータID → 10.40.10.1

<バーチャルリンク情報入力フィールド>	
接続先ルータID	<input type="text" value="10.40.10.1"/>

20. [追加] ボタンをクリックします。
21. 画面左側の [設定反映] 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。

## ルータ 4 を設定する

### LAN0 情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
5. 以下の項目を指定します。
  - OSPF 機能 → 使用する
  - エリア定義番号 → 0

■ OSPF 情報 <span style="float: right;">?</span>	
OSPF 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. [保存] ボタンをクリックします。

## ルータ5と接続する remote 定義に OSPF 機能を設定する

7. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
8. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
9. OSPF 機能を設定するネットワーク欄の【修正】ボタンをクリックします。  
「ネットワーク情報」ページが表示されます。
10. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
11. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
12. 以下の項目を指定します。
  - OSPF 機能 → 使用する
  - エリア定義番号 → 1

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="1"/>

13. 【保存】ボタンをクリックします。

## OSPF 関連を設定する

14. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」ページが表示されます。
15. 「OSPF 関連」をクリックします。  
OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
16. 以下の項目を指定します。
  - ルータID → 10.40.10.1

■ルータID情報	
ルータID	<input type="text" value="10.40.10.1"/>

17. 【保存】ボタンをクリックします。
18. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。  
「OSPF エリア情報」が表示されます。
19. 【追加】ボタンをクリックします。  
OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。



**20. 以下の項目を指定します。**

- エリアID → 0.0.0.2

**21. [保存] ボタンをクリックします。****22. OSPF エリア情報 (0) の「バーチャルリンク情報」をクリックします。**

「バーチャルリンク情報」が表示されます。

**23. 以下の項目を指定します。**

- 接続先ルータID → 10.30.10.1

**24. [追加] ボタンをクリックします。****25. 画面上部の「ルーティングプロトコル情報」をクリックします。**

OSPF 関連の設定項目と「OSPF エリア基本情報」が表示されます。

**26. 手順 19. ～ 21. を参考に、以下の項目を指定します。**

「OSPF エリア情報 (1)」 - 「OSPF エリア基本情報」

- エリアID → 0.0.0.3

**27. 画面左側の [設定反映] 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。

## ルータ5を設定する

---

「ルータ4を設定する」を参考に、ルータ5を設定します。

「LAN0 情報」 - 「IP 関連」

「OSPF 情報」

- OSPF 機能 → 使用する
- エリア定義番号 → 0

「相手情報」 - 「IP 関連」

「OSPF 情報」

- OSPF 機能 → 使用する
- エリア定義番号 → 0

「ルーティングプロトコル情報」 - 「OSPF 関連」

「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID → 0.0.0.3

## 2.3.2 スタブエリアを使う

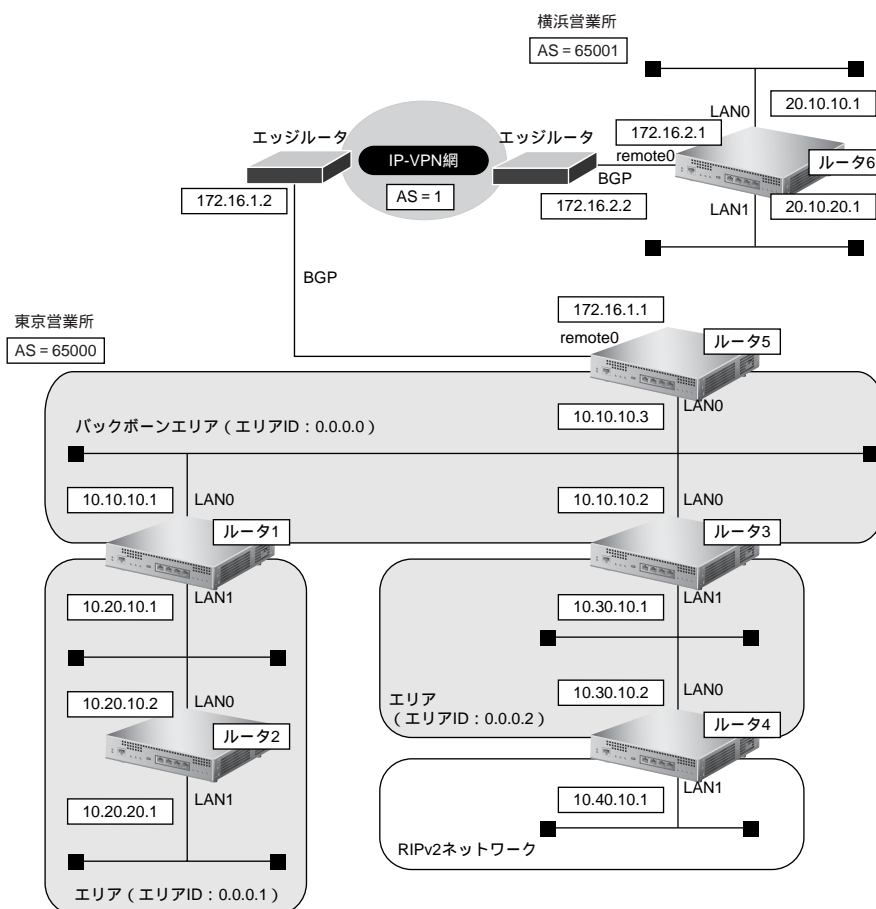
OSPF以外のルーティングプロトコルを使用したネットワークとの接続の設定について説明します。

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。



ここでは、ルータ5とルータ6が専用線（remote定義）でIP-VPN網に接続され、以下のとおりに設定されていることを前提とします。

### ● 前提条件

- ルータ1からルータ6のすべてのインタフェースにIPアドレスを設定する
- ルータ1からルータ6のすべてのインタフェースでNAT機能およびDHCPクライアント機能を使用しない

### ● 設定条件

- ルータ5およびルータ6は、ISDNポートで専用線に接続する

**【東京営業所】****【ルータ1でのルーティングプロトコル情報】**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1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】**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.1
- LAN1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】**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのOSPFエリアID : 0.0.0.0
- LAN1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】**

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : RIP V2,OSPF
- LAN0でのOSPFエリアID : 0.0.0.2
- LAN1でのpassive-interface設定 : 設定する
- エリアID0.0.0.2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

**【ルータ5でのルーティングプロトコル情報】**

- LAN0でのルーティングプロトコル : OSPF
- remote定義でのルーティングプロトコル : BGP
- LAN0でのOSPFエリアID : 0.0.0.0
- BGP経路のOSPFでの広報 : 再配布する
- BGP AS番号 : 65000
- BGPネットワークのIGPとの同期 : 同期させる
- BGPネットワーク : 10.10.10.0/24
- BGP集約経路 : 10.0.0.0/8
- AS外部経路の集約 : 20.10.0.0/16

**【横浜営業所】****【ルータ6でのルーティングプロトコル情報】**

- BGP AS番号 : 65001
- BGPネットワークのIGPとの同期 : 同期させる
- BGPネットワーク : 20.10.10.0/24、20.10.20.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

## 東京営業所を設定する

### ルータ 1 を設定する

#### LAN0 情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
5. 以下の項目を指定します。
  - OSPF 機能 → 使用する
  - エリア定義番号 → 0

OSPF 情報	
OSPF 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. [保存] ボタンをクリックします。
7. 手順 2. ~ 6. を参考に、以下の項目を指定します。

#### 「LAN1 情報」 - 「IP 関連」

#### 「OSPF 情報」

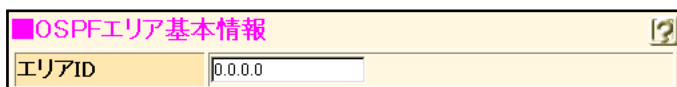
- OSPF 機能 → 使用する
- エリア定義番号 → 1

#### OSPF 関連を設定する

8. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」ページが表示されます。
9. 「OSPF 関連」をクリックします。  
OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
10. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。  
「OSPF エリア情報」が表示されます。
11. [追加] ボタンをクリックします。  
OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。

**12. 以下の項目を指定します。**

- エリアID →0.0.0.0



■OSPFエリア基本情報	
エリアID	0.0.0.0

**13. [保存] ボタンをクリックします。****14. 画面上部のルーティングプロトコル情報をクリックします。**

OSPF関連の設定項目と「OSPF エリア情報」が表示されます。

**15. 手順 11. ～ 13. を参考に、以下の項目を指定します。**

OSPFエリア情報 (1) の「OSPF エリア基本情報」

- エリアID →0.0.0.1
- エリア種別 →スタブエリア

**16. 画面左側の [設定反映] 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。

**ルータ2を設定する**

「ルータ1を設定する」を参考に、ルータ2を設定します。

**「LAN0 情報」 - 「IP 関連」****「OSPF 情報」**

- OSPF 機能 →使用する
- エリア定義番号 →0

**「LAN1 情報」 - 「IP 関連」****「OSPF 情報」**

- OSPF 機能 →使用する
- エリア定義番号 →0

**「ルーティングプロトコル情報」 - 「OSPF 関連」****「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」**

- エリアID →0.0.0.1
- エリア種別 →スタブエリア

## ルータ3を設定する

「ルータ1を設定する」を参考に、ルータ3を設定します。

### 「LAN0 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →0

### 「LAN1 情報」 - 「IP 関連」

#### 「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →1

### 「ルーティングプロトコル情報」 - 「OSPF 関連」

#### 「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.0

#### 「OSPF エリア情報 (1)」 - 「OSPF エリア基本情報」

- エリアID →0.0.0.2
- エリア種別 →準スタブエリア

## ルータ4を設定する

### LAN0 情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースがLAN0の「修正」ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

5. 以下の項目を指定します。

- OSPF 機能 →使用する
- エリア定義番号 →0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. 「保存」ボタンをクリックします。

### LAN1 情報を設定する

7. 設定メニューのルータ設定で、「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

8. 「LAN 情報」でインタフェースが LAN1 の「修正」ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

9. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

10. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

11. 以下の項目を指定します。

- RIP 送信 → V2(Multicast) で送信する
- RIP 受信 → V2、V2(Multicast) で受信する

RIP 情報	
RIP 送信	<input type="radio"/> 送信しない <input type="radio"/> V1 で送信する <input type="radio"/> V2 で送信する <input checked="" type="radio"/> V2(Multicast) で送信する
RIP 受信	<input type="radio"/> 受信しない <input type="radio"/> V1 で受信する <input checked="" type="radio"/> V2、V2(Multicast) で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》 メトリック値 <input type="text" value="0"/>	

12. 「保存」ボタンをクリックします。

13. IP 関連の設定項目の「OSPF 情報」をクリックします。

「OSPF 情報」が表示されます。

14. 以下の項目を指定します。

- OSPF 機能 → 使用する
- エリア定義番号 → 0
- パケット送信 → 抑止する

OSPF 情報	
OSPF 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>
出力コスト	<input type="text" value="10"/>
指定ルータ優先度	<input type="text" value="1"/>
Hello パケット送信間隔	<input type="text" value="10"/> 秒
隣接ルータ停止確認間隔	<input type="text" value="40"/> 秒
パケット再送間隔	<input type="text" value="5"/> 秒
LSU パケット送信遅延時間	<input type="text" value="1"/> 秒
認証方式	<input checked="" type="radio"/> 認証を行わない <input type="radio"/> テキスト認証 鍵種別 <input checked="" type="radio"/> 文字列 <input type="radio"/> 16進数 認証鍵 <input type="text"/> <input type="radio"/> MD5 認証 MD5 認証鍵ID <input type="text"/> MD5 認証鍵 <input type="text"/>
パケット送信	<input checked="" type="radio"/> 抑止する <input type="radio"/> 抑止しない

**15. [保存] ボタンをクリックします。**

OSPF 関連を設定する

**16. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**17. 「OSPF 関連」をクリックします。**

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

**18. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。**

「OSPF エリア情報」が表示されます。

**19. [追加] ボタンをクリックします。**

OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。

**20. 以下の項目を指定します。**

- エリアID → 0.0.0.2
- エリア種別 → 準スタブエリア

■OSPFエリア基本情報	
エリアID	<input type="text" value="0.0.0.2"/>
エリア種別	<input type="radio"/> 通常エリア <input type="radio"/> スタブエリア <input checked="" type="radio"/> 準スタブエリア

**21. [保存] ボタンをクリックします。**

ルーティングマネージャ情報を設定する

**22. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**23. 「ルーティングマネージャ情報」をクリックします。**

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。



## 24. 以下の項目を指定します。

- RIP
  - OSPF 経路情報 →再配布する
- OSPF
  - RIP 経路情報 →再配布する

再配布情報	
RIP	インタフェース経路情報 <input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	スタティック経路情報 <input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	BGP経路情報 <input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
	OSPF経路情報 <input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する メトリック値: 0
	DNS経路情報 <input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値: 0
BGP	インタフェース経路情報 <input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	スタティック経路情報 <input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報 <input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報 <input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	DNS経路情報 <input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
OSPF	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="text" value="type2"/>
	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="text" value="type2"/>
	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="text" value="type2"/>

## 25. [保存] ボタンをクリックします。

## 26. 画面左側の [設定反映] 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。

## ルータ5を設定する

### LAN0情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。  
「LAN0情報（物理 LAN）」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
5. 以下の項目を指定します。
  - OSPF 機能 →使用する
  - エリア定義番号 →0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. 【保存】ボタンをクリックします。
- ### ルーティングマネージャ情報を設定する
7. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」ページが表示されます。
  8. 「ルーティングマネージャ情報」をクリックします。  
ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。
  9. 以下の項目を指定します。
    - OSPF  
BGP経路情報 →再配布する

OSPF	BGP経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
		メトリック値 <input type="text" value="20"/> メトリックタイプ <input type="text" value="type2"/>

10. 【保存】ボタンをクリックします。
- ### BGP 関連を設定する
11. ルーティングプロトコル情報の設定項目の「BGP 関連」をクリックします。  
BGP 関連の設定項目と「BGP 情報」が表示されます。

## 12. 以下の項目を指定します。

- BGP機能 →使用する
- 自AS番号 →65000
- BGPネットワーク →チェックしない

■BGP情報	
BGP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
自AS番号	65000
自ID番号	0.0.0.0
BGPネットワーク	<input type="checkbox"/> 常に広報する

## 13. [保存] ボタンをクリックします。

## 14. BGP関連の設定項目の「BGP ネットワーク情報」をクリックします。

「BGP ネットワーク情報」が表示されます。

## 15. 以下の項目を指定します。

- あて先IPアドレス →10.10.10.0
- あて先アドレスマスク →24 (255.255.255.0)

<BGPネットワーク情報入力フィールド>	
あて先IPアドレス	10.10.10.0
あて先アドレスマスク	24 (255.255.255.0)

## 16. [追加] ボタンをクリックします。

## 17. BGP関連の設定項目の「BGP 集約経路情報」をクリックします。

「BGP 集約経路情報」が表示されます。

## 18. 以下の項目を指定します。

- 集約IPアドレス →10.0.0.0
- 集約アドレスマスク →8 (255.0.0.0)
- 集約対象経路 →広報しない

<BGP集約経路情報入力フィールド>	
集約IPアドレス	10.0.0.0
集約アドレスマスク	8 (255.0.0.0)
集約対象経路	<input type="radio"/> 広報する <input checked="" type="radio"/> 広報しない

## 19. [追加] ボタンをクリックします。

## 20. BGP関連の設定項目の「BGP 相手情報」をクリックします。

「BGP 相手情報」が表示されます。

## 21. [追加] ボタンをクリックします。

BGP相手情報 (0) の設定項目と「BGP相手基本情報」が表示されます。

**22. 以下の項目を指定します。**

- 相手側IPアドレス → 172.16.1.2
- 相手AS番号 → 1

■BGP相手基本情報	
相手側IPアドレス	172.16.1.2
相手AS番号	1

必要に応じて上記以外の項目を指定します。

**23. [保存] ボタンをクリックします。**

OSPF 関連を設定する

**24. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**25. 「OSPF 関連」をクリックします。**

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

**26. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。**

「OSPF エリア情報」が表示されます。

**27. [追加] ボタンをクリックします。**

OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。

**28. 以下の項目を指定します。**

- エリアID → 0.0.0.0
- エリア種別 → 通常エリア

■OSPFエリア基本情報	
エリアID	0.0.0.0
エリア種別	<input checked="" type="radio"/> 通常エリア <input type="radio"/> スタブエリア <input type="radio"/> 準スタブエリア

**29. [保存] ボタンをクリックします。****30. 画面上部のルーティングプロトコル情報をクリックします。**

OSPF 関連の設定項目と「OSPF エリア情報」が表示されます。

**31. 「AS 外部経路集約情報」をクリックします。**

「AS 外部経路集約情報」が表示されます。

**32. 以下の項目を指定します。**

- ネットワークアドレス → 20.10.0.0
- ネットマスク → 16 (255.255.0.0)

<AS外部経路集約情報入力フィールド>	
ネットワークアドレス	20.10.0.0
ネットマスク	16 (255.255.0.0)

33. [追加] ボタンをクリックします。

34. 画面左側の [設定反映] 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。

## 横浜営業所を設定する

---

### ルータ6を設定する

「ルータ5を設定する」を参考に、ルータ6を設定します。

#### 「ルーティングプロトコル情報」 - 「BGP 関連」

##### 「BGP 情報」

- BGP機能 →使用する
- 自AS番号 →65001
- BGPネットワーク →チェックしない

##### 「BGP ネットワーク情報」

- あて先IPアドレス →20.10.10.0
- あて先アドレスマスク →24 (255.255.255.0)
- あて先IPアドレス →20.10.20.0
- あて先アドレスマスク →24 (255.255.255.0)

##### 「BGP 相手情報」 - 「BGP相手基本情報」

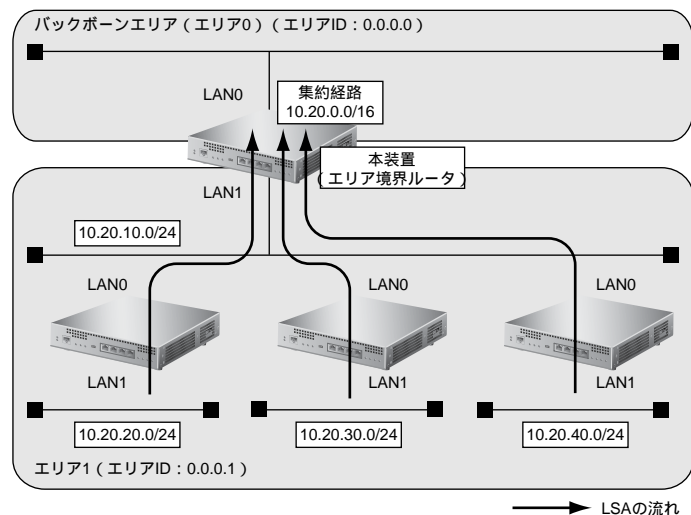
- 相手側IPアドレス →172.16.2.2
- 相手AS番号 →1

## 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。



#### ● 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

- LAN0でのルーティングプロトコル : OSPF
- LAN1でのルーティングプロトコル : OSPF
- LAN0でのエリア ID : 0.0.0.0
- LAN1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設定例を示します。

#### LAN 情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。

5. 以下の項目を指定します。

- OSPF 機能 →使用する
- エリア定義番号 →0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

6. [保存] ボタンをクリックします。

7. 手順 2.～6.を参考に、「LAN1 情報（物理 LAN）」で以下の項目を指定します。

「OSPF 情報」

- OSPF 機能 →使用する
- エリア定義番号 →1

### OSPF 関連を設定する

8. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

9. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

10. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

「OSPF エリア情報」が表示されます。

11. [追加] ボタンをクリックします。

OSPF エリア情報（0）の「OSPF エリア基本情報」が表示されます。

12. 以下の項目を指定します。

- エリアID →0.0.0.0

■OSPFエリア基本情報	
エリアID	<input type="text" value="0.0.0.0"/>

13. [保存] ボタンをクリックします。

14. 画面上部のルーティングプロトコル情報をクリックします。

OSPF 関連項目と「OSPF エリア情報」が表示されます。

15. 手順 11.～13.を参考に、以下の項目を指定します。

OSPF エリア情報（1）の「OSPF エリア基本情報」

- エリアID →0.0.0.1

16. OSPF エリア情報（1）の「経路集約情報」をクリックします。

「経路集約情報」が表示されます。

**17. 以下の項目を指定します。**

- ネットワークアドレス → 10.20.0.0
- ネットマスク → 16 (255.255.0.0)

<経路集約情報入力フィールド>	
ネットワークアドレス	<input type="text" value="10.20.0.0"/>
ネットマスク	<input type="text" value="16 (255.255.0.0)"/>

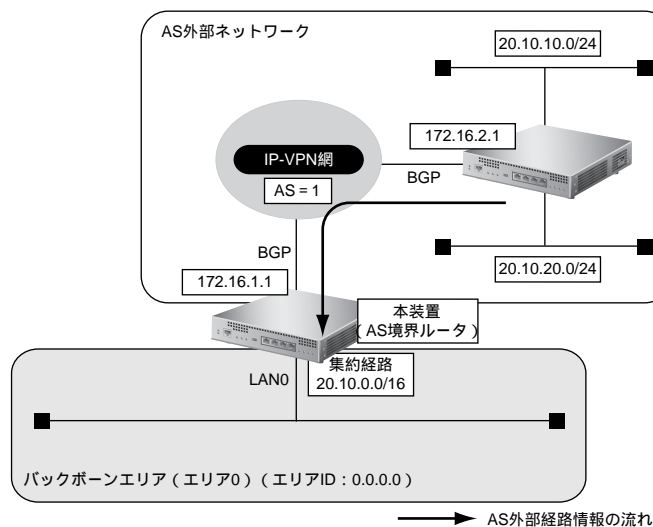
**18. [追加] ボタンをクリックします。****19. 画面左側の [設定反映] ボタンをクリックします。**

設定した内容が有効になります。



## 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。



### ● 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
- その他の AS 外部経路情報はすべて遮断する

### ● 設定条件

- LAN0 でのルーティングプロトコル : OSPF
- remote0 でのルーティングプロトコル : BGP
- LAN0 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

上記の経路情報に従って設定する場合の設定例を示します。

### LAN 情報を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。

## 5. 以下の項目を指定します。

- OSPF 機能 →使用する
- エリア定義番号 →0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

## 6. [保存] ボタンをクリックします。

## OSPF 関連を設定する

## 7. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

## 8. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

## 9. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

「OSPF エリア情報」が表示されます。

## 10. [追加] ボタンをクリックします。

OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。

## 11. 以下の項目を指定します。

- エリアID →0.0.0.0

■OSPFエリア基本情報	
エリアID	<input type="text" value="0.0.0.0"/>

## 12. [保存] ボタンをクリックします。

## ルーティングマネージャ情報を設定する

## 13. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

## 14. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

**15. 以下の項目を指定します。**

- OSPF  
BGP 経路情報 →再配布する

OSPF	BGP経路情報	<input type="radio"/> 再配布しない
		<input checked="" type="radio"/> 再配布する
		メトリック値 <input type="text" value="20"/>
		メトリックタイプ <input type="text" value="type2"/>

**16. [保存] ボタンをクリックします。**

OSPF 関連を設定する

**17. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**18. 「OSPF 関連」をクリックします。**

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

**19. 「AS 外部経路集約情報」をクリックします。**

「AS 外部経路集約情報」が表示されます。

**20. 以下の項目を指定します。**

- ネットワークアドレス → 20.10.0.0
- ネットマスク → 16 (255.255.0.0)

<AS外部経路集約情報入力フィールド>	
ネットワークアドレス	<input type="text" value="20.10.0.0"/>
ネットマスク	<input type="text" value="16 (255.255.0.0)"/>

**21. [追加] ボタンをクリックします。****22. OSPF 関連項目の「OSPF 再配布フィルタリング情報」をクリックします。**

「OSPF 再配布フィルタリング情報」が表示されます。

**23. 以下の項目を指定します。**

- 動作 → 透過
- フィルタリング条件 → 経路情報指定
  - 検索条件 → マスクした結果が一致
  - IPアドレス → 20.10.0.0
  - アドレスマスク → 16 (255.255.0.0)
- メトリック → 指定しない

<OSPF再配布フィルタリング情報入力フィールド>								
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断							
フィルタリング条件	<input type="radio"/> すべて							
	<input type="radio"/> デフォルトルート							
	<input checked="" type="radio"/> 経路情報指定							
	<table border="1"> <tr> <td>検索条件</td> <td><input type="radio"/> 完全に一致</td> </tr> <tr> <td></td> <td><input checked="" type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IPアドレス</td> <td><input type="text" value="20.10.0.0"/></td> </tr> <tr> <td>アドレスマスク</td> <td><input type="text" value="16 (255.255.0.0)"/></td> </tr> </table>	検索条件	<input type="radio"/> 完全に一致		<input checked="" type="radio"/> マスクした結果が一致	IPアドレス	<input type="text" value="20.10.0.0"/>	アドレスマスク
検索条件	<input type="radio"/> 完全に一致							
	<input checked="" type="radio"/> マスクした結果が一致							
IPアドレス	<input type="text" value="20.10.0.0"/>							
アドレスマスク	<input type="text" value="16 (255.255.0.0)"/>							
メトリック	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する <table border="1"> <tr> <td>メトリック値</td> <td><input type="text"/></td> </tr> <tr> <td>メトリックタイプ</td> <td><input type="text" value="type2"/></td> </tr> </table>	メトリック値	<input type="text"/>	メトリックタイプ	<input type="text" value="type2"/>			
メトリック値	<input type="text"/>							
メトリックタイプ	<input type="text" value="type2"/>							

**24. [追加] ボタンをクリックします。****25. 手順 23. ~ 24. を参考に、以下の項目を指定します。**

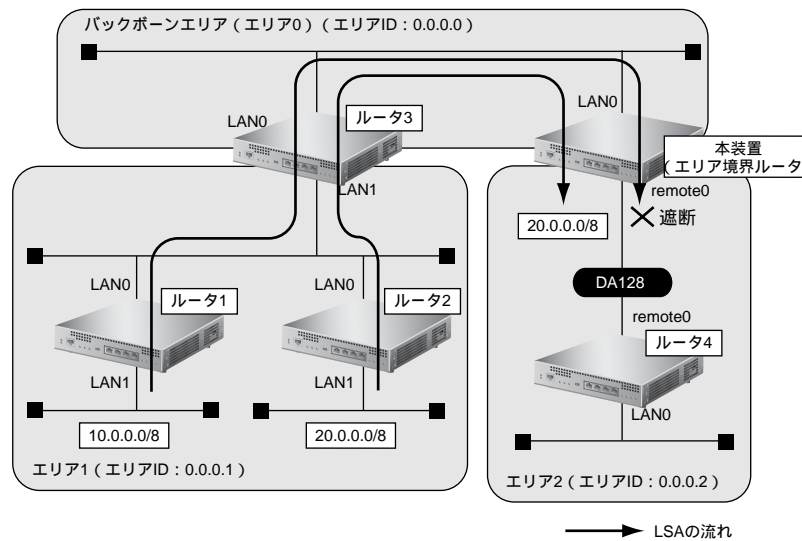
- 動作 → 遮断
- フィルタリング条件 → すべて
- メトリック → 指定しない

**26. 画面左側の [設定反映] 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。

## 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

ここでは、本装置とルータ4が、専用線 (remote 定義) で接続され、以下のとおりに設定されていることを前提とします。

- 本装置およびルータ1～4までのすべての装置で、使用するすべてのインタフェースにIPアドレスが設定されている

### ● 設定条件

- LAN0でのルーティングプロトコル : OSPF
- remote0でのルーティングプロトコル : OSPF
- LAN0でのエリアID : 0.0.0.0
- remote0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設定例を示します。

### LAN 情報を設定する

#### 1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

#### 2. 「LAN 情報」でインタフェースがLAN0の【修正】ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

#### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**4. IP関連の設定項目の「OSPF情報」をクリックします。**

「OSPF情報」が表示されます。

**5. 以下の項目を指定します。**

- OSPF機能 →使用する
- エリア定義番号 →0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="0"/>

**6. [保存] ボタンをクリックします。****相手情報を設定する****7. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**8. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**9. 「相手情報」でネットワーク名が rmt0 の [修正] ボタンをクリックします。**

「ネットワーク情報 (rmt0)」ページが表示されます。

**10. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**11. IP関連の設定項目の「OSPF情報」をクリックします。**

「OSPF情報」が表示されます。

**12. 以下の項目を指定します。**

- OSPF機能 →使用する
- エリア定義番号 →1

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	<input type="text" value="1"/>

**13. [保存] ボタンをクリックします。****OSPF関連を設定する****14. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**15. 「OSPF関連」をクリックします。**

OSPF関連の設定項目と「ルータID情報」が表示されます。

**16. OSPF関連の設定項目の「OSPFエリア情報」をクリックします。**

「OSPFエリア情報」が表示されます。

**17. [追加] ボタンをクリックします。**

OSPFエリア情報 (0) の「OSPF エリア基本情報」が表示されます。

**18. 以下の項目を指定します。**

- エリアID → 0.0.0.0

■OSPFエリア基本情報	
エリアID	0.0.0.0

**19. [保存] ボタンをクリックします。****20. 画面上部のルーティングプロトコル情報をクリックします。**

OSPF 関連項目と「OSPF エリア情報」が表示されます。

**21. 手順 17. ~ 19. を参考に、以下の項目を指定します。**

OSPFエリア情報 (1) の「OSPF エリア基本情報」

- エリアID → 0.0.0.2

**22. 画面上部のルーティングプロトコル情報をクリックします。**

OSPF 関連項目と「OSPF エリア情報」が表示されます。

**23. エリア定義番号 (1) の [修正] ボタンをクリックします。**

OSPF エリア情報 (1) 関連項目と「OSPF エリア基本情報」が表示されます。

**24. OSPF エリア情報 (1) 関連項目の「サマリLSA入出力可否情報」をクリックします。**

「サマリLSA入出力可否情報」が表示されます。

**25. 以下の項目を指定します。**

- 動作 → 遮断
- 方向 → 入力
- 対象経路情報 → 経路情報指定
  - 検索条件 → 完全に一致
  - IPアドレス → 10.0.0.0
  - アドレスマスク → 8 (255.0.0.0)

<サマリLSA入出力可否情報入力フィールド>	
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断
方向	<input checked="" type="radio"/> 入力 <input type="radio"/> 出力
対象経路情報	<input type="radio"/> すべて <input checked="" type="radio"/> 経路情報指定
	検索条件 <input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
	IPアドレス <input type="text" value="10.0.0.0"/>
	アドレスマスク <input type="text" value="8 (255.0.0.0)"/>

**26. [追加] ボタンをクリックします。**

**27. 手順 25. ～ 26. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 方向 → 入力
- 対象経路情報 → すべて

**28. 画面左側の [設定反映] 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。



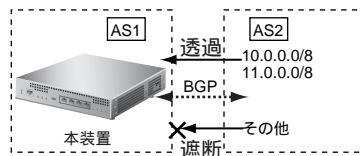
## 2.5 BGP の経路を制御する (IPv4)

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 MR1000 機能説明書「2.4 BGP4 機能」(P.30)

### 2.5.1 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設定例を示します。

1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」のページが表示されます。
2. 「BGP関連」をクリックします。  
BGP関連の設定項目と「BGP情報」が表示されます。
3. BGP関連の設定項目の「BGP相手情報」をクリックします。  
「BGP相手情報」が表示されます。
4. フィルタリング設定を行う BGP 相手情報の [修正] ボタンまたは [追加] ボタンをクリックします。  
BGP 相手情報の設定項目と「BGP相手基本情報」が表示されます。
5. BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。  
「BGP フィルタリング情報」が表示されます。

## 6. 以下の項目を指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - IPアドレス → 10.0.0.0
  - アドレスマスク → 8 (255.0.0.0)

<BGPフィルタリング情報入力フィールド>						
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断					
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信					
フィルタリング条件	<input type="radio"/> AS番号指定 AS番号 <input type="text"/>					
	<input type="radio"/> すべて					
	<input type="radio"/> デフォルトルート					
	<input checked="" type="radio"/> 経路情報指定					
	<table border="1"> <tr> <td>検索条件</td> <td><input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致</td> </tr> <tr> <td>IPアドレス</td> <td><input type="text" value="10.0.0.0"/></td> </tr> <tr> <td>アドレスマスク</td> <td><input type="text" value="8 (255.0.0.0)"/> ▼</td> </tr> </table>	検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致	IPアドレス	<input type="text" value="10.0.0.0"/>	アドレスマスク
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致					
IPアドレス	<input type="text" value="10.0.0.0"/>					
アドレスマスク	<input type="text" value="8 (255.0.0.0)"/> ▼					

## 7. [追加] ボタンをクリックします。

優先順位 1 の定義が追加されます。

## 8. 手順 6. ~ 7. を参考に、以下の項目を優先順位 2 の定義として指定します。

- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → 経路情報指定
  - 検索条件 → 完全に一致
  - IPアドレス → 11.0.0.0
  - アドレスマスク → 8 (255.0.0.0)

## 9. 手順 6. ~ 7. を参考に、以下の項目を優先順位 3 の定義として指定します。

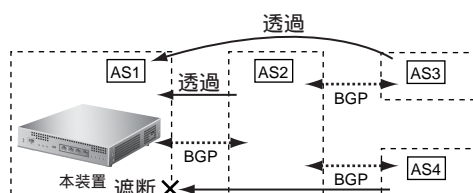
- 動作 → 遮断
- 方向 → 受信
- フィルタリング条件 → すべて

## 10. 画面左側の [設定反映] 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。

## 2.5.2 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

- AS4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設定例を示します。

1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」のページが表示されます。
2. 「BGP関連」をクリックします。  
BGP関連の設定項目と「BGP情報」が表示されます。
3. BGP関連の設定項目の「BGP相手情報」をクリックします。  
「BGP相手情報」が表示されます。
4. フィルタリング設定を行うBGP相手情報の「修正」ボタンまたは「追加」ボタンをクリックします。  
BGP相手情報の設定項目と「BGP相手基本情報」が表示されます。
5. BGP相手情報の設定項目の「BGPフィルタリング情報」をクリックします。  
「BGPフィルタリング情報」が表示されます。

## 6. 以下の項目を指定します。

- 動作 → 遮断
- 方向 → 受信
- フィルタリング条件 → AS 番号指定  
AS 番号 → 4

<BGPフィルタリング情報入力フィールド>	
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断
方向	<input checked="" type="radio"/> 受信 <input type="radio"/> 送信
フィルタリング条件	<input checked="" type="radio"/> AS番号指定
	AS番号 <input type="text" value="4"/>
	<input type="radio"/> すべて
	<input type="radio"/> デフォルトルート
	<input type="radio"/> 経路情報指定
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
IPアドレス	<input type="text"/>
アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>

## 7. [追加] ボタンをクリックします。

優先順位 1 の定義が追加されます。

## 8. 手順 6. ～ 7. を参考に、以下の項目を優先順位 2 の定義として指定します。

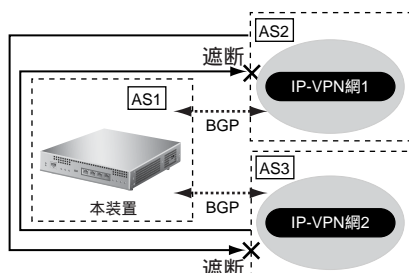
- 動作 → 透過
- 方向 → 受信
- フィルタリング条件 → すべて

## 9. 画面左側の [設定反映] 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。

## 2.5.3 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

- AS2 から AS3 への経路情報を遮断
- AS3 から AS2 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設定例を示します。

## AS2 への広報時の BGP フィルタリングを設定する

1. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」のページが表示されます。
2. 「BGP 関連」をクリックします。  
BGP 関連の設定項目と「BGP 情報」が表示されます。
3. BGP 関連の設定項目の「BGP 相手情報」をクリックします。  
「BGP 相手情報」が表示されます。
4. フィルタリング設定を行う BGP 相手情報の「修正」ボタンまたは「追加」ボタンをクリックします。  
BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。
5. BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。  
「BGP フィルタリング情報」が表示されます。

## 6. 以下の項目を指定します。

- 動作 → 遮断
- 方向 → 送信
- フィルタリング条件 → AS 番号指定  
AS 番号 → 3

<BGPフィルタリング情報入力フィールド>	
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信
フィルタリング条件	<input checked="" type="radio"/> AS番号指定
	AS番号 <input type="text" value="3"/>
	<input type="radio"/> すべて
	<input type="radio"/> デフォルトルート
	<input type="radio"/> 経路情報指定
検索条件	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
IPアドレス	<input type="text"/>
アドレスマスク	<input type="text" value="0.0.0.0"/>

## 7. [追加] ボタンをクリックします。

優先順位 1 の定義が追加されます。

## 8. 手順 6. ～ 7. を参考に、以下の項目を指定します。

BGP 相手情報 (0) の優先順位 2 の定義

- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → すべて

## AS3 への広報時の BGP フィルタリングを設定する

### 9. 「AS2 への広報時の BGP フィルタリングを設定する」を参考に、以下の項目を指定します。

BGP 相手情報 (1) の優先順位 1 の定義

- 動作 → 遮断
- 方向 → 送信
- フィルタリング条件 → AS 番号指定  
AS 番号 → 2

BGP 相手情報 (1) の優先順位 2 の定義

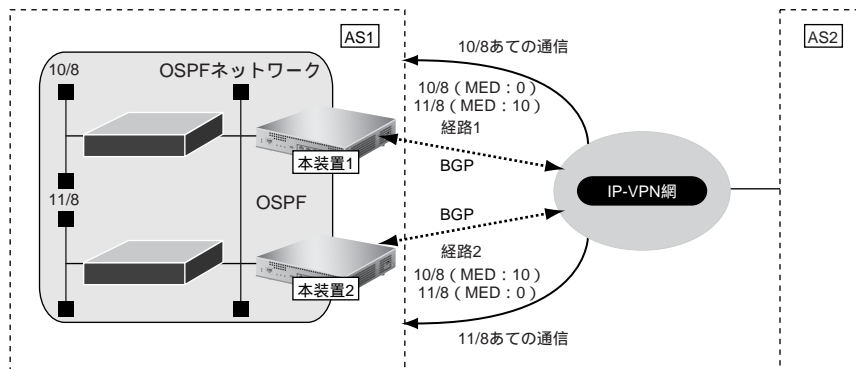
- 動作 → 透過
- 方向 → 送信
- フィルタリング条件 → すべて

### 10. 画面左側の [設定反映] 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。

## 2.5.4 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 AS1 で IP-VPN 網を経由した AS2 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
- AS1 内の OSPF ネットワークでの経路変更は BGP で AS2 に広報する

上記の経路情報に従って設定する場合の設定例を示します。

## 本装置 1 を設定する

### ルーティングプロトコル情報を設定する

- 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」のページが表示されます。
- 「BGP 関連」をクリックします。  
BGP 関連の設定項目と「BGP 情報」が表示されます。
- BGP 関連の設定項目の「BGP 相手情報」をクリックします。  
「BGP 相手情報」が表示されます。
- フィルタリング設定を行う BGP 相手情報の【修正】ボタンまたは【追加】ボタンをクリックします。  
BGP 相手情報の設定項目と「BGP 相手基本情報」が表示されます。
- BGP 相手情報の設定項目の「BGP フィルタリング情報」をクリックします。  
「BGP フィルタリング情報」が表示されます。

## 6. 以下の項目を指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →経路情報指定
  - 検索条件 →完全に一致
  - IPアドレス →10.0.0.0
  - アドレスマスク →8 (255.0.0.0)
- MEDメトリック値 →0

<BGPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
方向	<input type="radio"/> 受信 <input checked="" type="radio"/> 送信
フィルタリング条件	<input type="radio"/> AS番号指定 <input type="text" value="AS番号"/>
	<input type="radio"/> すべて <input type="radio"/> デフォルトルート
	<input checked="" type="radio"/> 経路情報指定 <input type="text" value="検索条件"/>
	<input checked="" type="radio"/> 完全に一致 <input type="radio"/> マスクした結果が一致
	<input type="text" value="IPアドレス"/> 10.0.0.0 <input type="text" value="アドレスマスク"/> 8 (255.0.0.0)
MEDメトリック値	<input type="text" value="0"/>

## 7. [追加] ボタンをクリックします。

優先順位1の定義が追加されます。

## 8. 手順6.～7.を参考に、以下の項目を優先順位2の定義として指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →経路情報指定
  - 検索条件 →完全に一致
  - IPアドレス →11.0.0.0
  - アドレスマスク →8 (255.0.0.0)
- MEDメトリック値 →10

## 9. 手順6.～7.を参考に、以下の項目を優先順位3の定義として指定します。

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて

## 10. 画面上部の「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

## 11. 「ルーティングマネージャ情報」をクリックします。

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。



**12. 以下の項目を指定します。**

- BGP  
OSPF 経路情報 →再配布する

BGP	インタフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	DNS経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する

**13. [保存] ボタンをクリックします。****14. 画面左側の [設定反映] 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2を設定する**

「本装置1を設定する」を参考に、本装置2を設定します。

**「ルーティングプロトコル情報」 - 「BGP 関連」****「BGP フィルタリング情報」**

BGP相手情報 (0) の優先順位 1 の定義

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →経路情報指定  
検索条件 →完全に一致  
IPアドレス →10.0.0.0  
アドレスマスク →8 (255.0.0.0)
- MEDメトリック値 →10

BGP相手情報 (0) の優先順位 2 の定義

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →経路情報指定  
検索条件 →完全に一致  
IPアドレス →11.0.0.0  
アドレスマスク →8 (255.0.0.0)
- MEDメトリック値 →0

BGP相手情報 (0) の優先順位 3 の定義

- 動作 →透過
- 方向 →送信
- フィルタリング条件 →すべて

**「ルーティングプロトコル情報」 - 「ルーティングマネージャ情報」****「再配布情報」**

- BGP  
OSPF 経路情報 →再配布する

---

### 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。
  - BGP/MPLS VPN 機能では、BGP フィルタリング情報は無効となります。
  - 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 [設定反映] をクリックした場合、接続中のセッションが一度切断されることがあります。
-

## 2.6 事業所間をMPLS接続サービスを利用して接続する

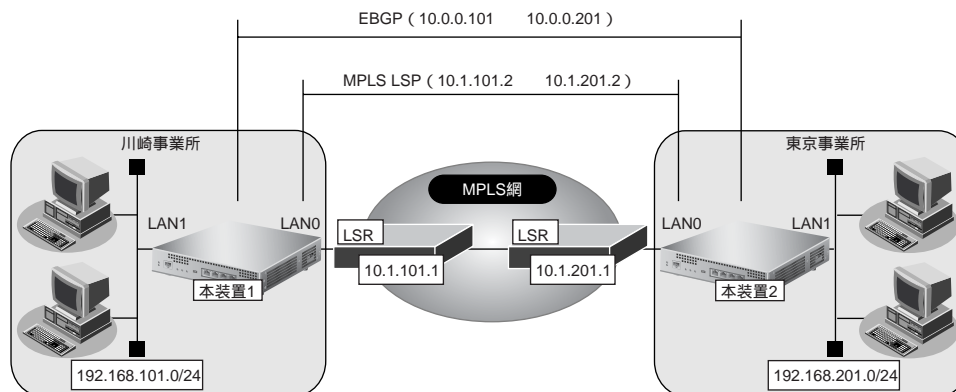
本装置では MPLS の LSP (label Switching Path : トンネルラベルスイッチングパス) をトンネルとしてインタフェースに対応させるため、シェーピングや帯域制御などの機能を LSP ごとに使用することができます (MPLS LSP トンネル)。

ここでは、MPLS 接続サービス (キャリアなどから提供される MPLS をユーザインタフェースとするデータ伝送サービスを想定しています) と本装置の MPLS LSP トンネルを使用して、事業所の間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

- 隣接 LSR は、ダイナミックルーティングを用いて最適経路から決定することはできません。MPLS LSP の送出先の設定と MPLS LSP での次ホップのラベルスイッチルータの設定で静的に指定する必要があります。
- MPLS LSP トンネルでは、IPv4、IPv6 のプロトコルだけをサポートしています。ブリッジは使用できません。MPLS LSP トンネル上にさらにラベルをスタックできるのは、BGP/MPLS VPN 機能だけです。LDP over LDP の形態はサポートしていません。MPLS LSP トンネルを使用するインタフェースでは、MPLS を利用しないように設定してください。
- MPLS LSP トンネルで IPv6 通信を行う場合は、2 層目のラベルスタックに IPv6 Explicit NULL ラベルを用いた多重スタックとなります。また、MPLS TTL 伝達の設定で指定した値に関係なく、TTL の継承は行われません。
- 複数の MPLS LSP トンネルを使用する場合は、それぞれ別の自側トンネルエンドポイントアドレスと相手側トンネルエンドポイントアドレスを設定してください。同じ自側トンネルエンドポイントアドレスが複数設定されている場合は、それぞれの LSP で受信したパケットが期待した LSP のインタフェースとは別のインタフェースで受信されてしまうため、受信インタフェースに依存して動作する IP フィルタリング機能、TOS 値書き換え機能、NAT 機能、マルチキャスト機能、ダイナミックルーティング (RIP、OSPF) 機能などは正しく動作しません。
- 複数の MPLS LSP トンネルで相手側トンネルエンドポイントアドレスの設定が同じアドレスであった場合は、MPLS LSP の送出先の設定と MPLS LSP での次ホップのラベルスイッチルータは同じ値を設定してください。違う値を設定した場合、どれかの値だけが使用されます。
- MPLS 通信で、優先制御機能、EXP 値書き換え機能、およびシェーピング機能を利用する場合は、MPLS LSP トンネルを使用してください。

## 2.6.1 トンネルエンドポイントをインタフェースアドレスにして MPLS LSP を使用する



### ● 前提条件

#### 【本装置 1】

- LAN0がMPLS網、LAN1が事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、インタフェースアドレスで接続を確立する
- MPLS網とのラベル交換はインタフェースアドレスに対して行う
- 本装置1と本装置2の間は、EBGPでループバックインタフェースどうしで経路情報を交換する

#### 【本装置 2】

- LAN0がMPLS網、LAN1が事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、インタフェースアドレスで接続を確立する
- MPLS網とのラベル交換は、インタフェースアドレスに対して行う
- 本装置2と本装置1の間は、EBGPでループバックインタフェースどうしで経路情報を交換する

### ● 設定条件

#### 【本装置 1】

- LAN0 (MPLS網側) のIPアドレス : 10.1.101.2
- 接続するMPLS網の次ホップLSRのIPアドレス : 10.1.101.1
- LAN1 (事業所内側) のIPアドレス : 192.168.101.1
- ループバックインタフェースのIPアドレス : 10.0.0.101
- 本装置1の属するAS番号 : 101
- 本装置2の属するAS番号 : 201

#### 【本装置 2】

- LAN0 (MPLS網側) のIPアドレス : 10.1.201.2
- 接続するMPLS網の次ホップLSRのIPアドレス : 10.1.201.1
- LAN1 (事業所内側) のIPアドレス : 192.168.201.1
- ループバックインタフェースのIPアドレス : 10.0.0.201
- 本装置2の属するAS番号 : 201
- 本装置1の属するAS番号 : 101

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置 1 を設定する

### MPLS 網との接続情報を設定する

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の「修正」ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. 以下の項目を指定します。

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.1.101.2
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

■ IP アドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IP アドレス	<input type="radio"/> DHCP で自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IP アドレス	10.1.101.2
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス + オール 1

5. 「保存」ボタンをクリックします。

6. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

7. 以下の項目を指定します。

- MPLS 機能 → 使用する
- ラベル配布プロトコル → LDP

■ MPLS 基本情報	
MPLS 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
ラベル配布プロトコル	LDP

8. 「保存」ボタンをクリックします。

9. 設定メニューのルータ設定で、「MPLS 情報」をクリックします。

「MPLS 情報」ページが表示されます。

**10. 「基本情報」をクリックします。**

「基本情報」が表示されます。

**11. 以下の項目を指定します。**

- MPLS TTL 伝達 → しない
- LDP
  - router ID → 10.1.101.2
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.1.101.2

■基本情報	
MPLS TTL伝達	<input checked="" type="radio"/> しない <input type="radio"/> する
LDP router ID	<input type="text" value="10.1.101.2"/>
LDP 制御方式	<input checked="" type="radio"/> independent <input type="radio"/> ordered
IPv4 Transport アドレス	<input type="text" value="10.1.101.2"/>

**12. [保存] ボタンをクリックします。****13. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**14. 「ルーティングマネージャ情報」をクリックします。**

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

**15. 以下の項目を指定します。**

- LDP
  - インタフェース経路情報 → 再配布しない
  - RIP 経路情報 → 再配布しない
  - OSPF 経路情報 → 再配布しない

LDP	インタフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する

**16. [保存] ボタンをクリックします。****MPLS トンネルを設定する****17. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**18. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**19. 以下の項目を指定します。**

- ネットワーク名 → tokyo

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="tokyo"/>

**20. [追加] ボタンをクリックします。**

「ネットワーク情報 (tokyo)」 ページが表示されます。

**21. 「接続先情報」 をクリックします。**

「接続先情報」 が表示されます。

**22. 以下の項目を指定します。**

- 接続先名 → lsp1
- 接続先種別 → MPLS トンネル接続

<接続先情報追加フィールド>

接続先名	lsp1		
接続先種別	<input type="radio"/> 専用線接続		
	<input type="radio"/> ISDN接続		
		ダイヤル1	電話番号
		サブアドレス	
	<input type="radio"/> フレームリレー接続		
	DLCI		
	<input type="radio"/> PPPoE接続		
	<input type="radio"/> IPTunnel接続		
	<input type="radio"/> IPsec/IKE接続		
	<input type="radio"/> 別インタフェースから送出		
	<input checked="" type="radio"/> MPLSTunnel接続		
	<input type="radio"/> パケット破棄		

**23. [追加] ボタンをクリックします。**

MPLS トンネル接続の設定項目と「基本情報」が表示されます。

**24. 以下の項目を指定します。**

- 送出先インタフェース → LAN0
- IPv4 転送先ルータ → 10.1.101.1
- 自側エンドポイント → 10.1.101.2
- 相手側エンドポイント → 10.1.201.2

■基本情報	
接続先名	lsp1
送出先インタフェース	LAN0
IPv4転送先ルータ	10.1.101.1
自側エンドポイント	10.1.101.2
相手側エンドポイント	10.1.201.2

**25. [保存] ボタンをクリックします。****ループバックインタフェースを設定する****26. 設定メニューの基本設定で「装置情報」 をクリックします。**

「装置情報」 ページが表示されます。

**27. 「ループバック情報」 をクリックします。**

「ループバック情報」 が表示されます。

**28. 以下の項目を指定します。**

- IPアドレス → 10.0.0.101

ループバック情報	
IPアドレス	10.0.0.101
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する エリア定義番号 <input type="text" value="0"/>
PHP機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない

**29. [保存] ボタンをクリックします。****LAN1 情報を設定する****30. 設定メニューのルータ設定で、「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**31. 以下の項目を指定します。**

- インタフェース → 物理 LAN

<LAN情報追加フィールド>	
インタフェース	物理LAN

**32. [追加] ボタンをクリックします。**

「LAN1 情報 (物理 LAN)」ページが表示されます。

**33. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**34. 以下の項目を指定します。**

- IPv4 → 使用する
- IPアドレス → 指定する
  - IPアドレス → 192.168.101.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス+オール1

IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する	
	IPアドレス	192.168.101.1
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス+オール1

**35. [保存] ボタンをクリックします。****本装置 1 との間で経路交換を設定する****36. 設定メニューのルータ設定の「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。



**37. 「BGP関連」をクリックします。**

BGP関連の設定項目と「BGP情報」が表示されます。

**38. 以下の項目を指定します。**

- BGP機能 →使用する
- 自AS番号 →101
- BGPネットワーク →チェックしない

■BGP情報	
BGP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
自AS番号	101
自ID番号	0.0.0.0
BGPネットワーク	<input type="checkbox"/> 常に広報する

**39. [保存] ボタンをクリックします。****40. BGP関連の設定項目の「BGP相手情報」をクリックします。**

「BGP相手情報」が表示されます。

**41. [追加] ボタンをクリックします。**

BGP相手情報 (0) の設定項目と「BGP相手基本情報」が表示されます。

**42. 以下の項目を指定します。**

- 相手側IPアドレス →10.0.0.201
- 相手AS番号 →201
- 自側IPアドレス →10.0.0.101

こんな事に気をつけて

- ルートリフレクタのIPアドレスを相手側IPアドレスに設定してください。
- 自側IPアドレスには、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■BGP相手基本情報	
相手側IPアドレス	10.0.0.201
相手AS番号	201
自側IPアドレス	10.0.0.101

**43. [保存] ボタンをクリックします。****44. BGP関連の設定項目の「BGPネットワーク情報」をクリックします。**

「BGPネットワーク情報」が表示されます。

**45. 以下の項目を指定します。**

- あて先IPアドレス →192.168.101.0
- あて先アドレスマスク →24 (255.255.255.0)

<BGPネットワーク情報入力フィールド>	
あて先IPアドレス	192.168.101.0
あて先アドレスマスク	24 (255.255.255.0)

46. [追加] ボタンをクリックします。

47. BGP相手情報 (0) の設定項目の「BGP 拡張機能情報」をクリックします。

「BGP 拡張機能情報」が表示されます。

48. 以下の項目を指定します。

- エンフォースマルチホップ →使用する

■BGP拡張機能情報	
アドレスファミリー情報	IPv4ユニキャスト
エンフォースマルチホップ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する

49. [保存] ボタンをクリックします。

50. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

51. 「ネットワーク情報」で相手定義番号が0の[修正] ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

52. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

53. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

54. 以下の項目を指定します。

- ネットワーク →ネットワーク指定
- あて先IPアドレス →10.0.0.201
- あて先アドレスマスク →32 (255.255.255.255)

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート
	<input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="10.0.0.201"/>
	あて先アドレスマスク <input type="text" value="32 (255.255.255.255)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

55. [追加] ボタンをクリックします。

56. 画面左側の[設定反映] 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2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

### MPLS 網との接続情報を設定する

#### 「LAN0 情報 (物理LAN)」 - 「IP 関連」

##### 「IP アドレス情報」

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.1.201.2
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール1

#### 「LAN0 情報 (物理LAN)」 - 「MPLS 関連」

##### 「MPLS 基本情報」

- MPLS 機能 → 使用する
  - ラベル配布プロトコル → LDP

##### 「MPLS 情報」

##### 「基本情報」

- MPLS TTL 伝達 → しない
  - router ID → 10.1.201.2
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.1.201.2

#### 「ルーティングプロトコル情報」 - 「ルーティングマネージャ情報」

##### 「再配布情報」

- LDP
  - インタフェース経路情報 → 再配布しない
  - RIP 経路情報 → 再配布しない
  - OSPF 経路情報 → 再配布しない

### MPLS トンネルを設定する

#### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → kawasaki

#### 「ネットワーク情報」 - 「接続先情報」

- 接続先名 → lsp1
- 接続先種別 → MPLS トンネル接続

#### 「接続先情報」 - 「MPLS トンネル接続」

##### 「基本情報」

- 送出先インタフェース → LAN0
- IPv4 転送先ルータ → 10.1.201.1
- 自側エンドポイント → 10.1.201.2
- 相手側エンドポイント → 10.1.101.2

## ループバックインタフェースを設定する

### 「装置情報」 - 「ループバック情報」

- IPアドレス → 10.0.0.201

## LAN1 情報を設定する

### 「LAN1 情報 (物理LAN)」 - 「IP 関連」

#### 「IPアドレス情報」

- IPv4 → 使用する
- IPアドレス → 指定する  
IPアドレス → 192.168.201.1  
ネットマスク → 24 (255.255.255.0)  
ブロードキャストアドレス → ネットワークアドレス + オール1

### 「LAN1 情報 (物理LAN)」 - 「MPLS 関連」

#### 「MPLS 基本情報」

- MPLS 機能 → 使用する  
ラベル配布プロトコル → LDP

## 本装置 1 との間で経路交換を設定する

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「BGP 情報」

- BGP 機能 → 使用する
- 自AS番号 → 201

#### 「BGP 相手情報」

#### 「BGP 相手基本情報」

- 相手側IPアドレス → 10.0.0.101
- 相手AS番号 → 101
- 自側IPアドレス → 10.0.0.201

#### 「BGP 拡張機能情報」

- エンフォースマルチホップ → 使用する

### 「ルーティングプロトコル情報」 - 「ルーティングマネージャ情報」

#### 「再配布情報」

- BGP  
インタフェース経路情報 → 再配布する

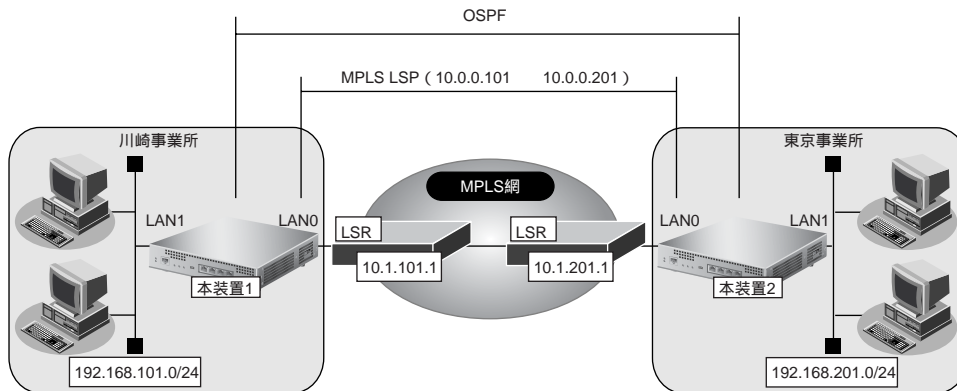
### 「相手情報」 - 「ネットワーク情報」

#### 「ネットワーク情報」 - 「IP 関連」

#### 「スタティック経路情報」

- ネットワーク指定  
あて先IPアドレス → 10.0.0.101  
あて先アドレスマスク → 32 (255.255.255.255)

## 2.6.2 トンネルエンドポイントをインタフェースアドレスとは別のアドレスにしてMPLS LSPを使用する



### ● 前提条件

#### 【本装置1】

- LAN0がMPLS網、LAN1が事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、インタフェースアドレスで接続を確立する
- MPLS網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置1と本装置2の間は、LSP上でOSPFを用いて経路情報を交換する
- MPLS網を使用したLSP上の通信は5Mbpsに帯域を制限する
- LSPでセッション監視を行い、セッションの切断を検知する

#### 【本装置2】

- LAN0がMPLS網、LAN1が事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、インタフェースアドレスで接続を確立する
- MPLS網とのラベル交換はインタフェースアドレスを使用しないで別のアドレスを使用する
- 本装置1と本装置2の間は、LSP上でOSPFを用いて経路情報を交換する
- MPLS網を使用したLSP上の通信は5Mbpsに帯域を制限する
- LSPでセッション監視を行い、セッションの切断を検知する

### ● 設定条件

#### 【本装置1】

- LAN0 (MPLS網側) のIPアドレス : 10.1.101.2
- 接続するMPLS網の次ホップLSRのIPアドレス : 10.1.101.1
- LAN1 (事業所内側) のIPアドレス : 192.168.101.1
- MPLSトンネルの自側IPアドレス : 10.0.0.101
- MPLSトンネルの相手側IPアドレス : 10.0.0.201

#### 【本装置2】

- LAN0 (MPLS網側) のIPアドレス : 10.1.201.2
- 接続するMPLS網の次ホップLSRのIPアドレス : 10.1.201.1
- LAN1 (事業所内側) のIPアドレス : 192.168.201.1
- MPLSトンネルの自側IPアドレス : 10.0.0.101
- MPLSトンネルの相手側IPアドレス : 10.0.0.201

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置 1 を設定する

### MPLS 網との接続情報を設定する

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. 以下の項目を指定します。

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.1.101.2
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

■ IP アドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IP アドレス	<input type="radio"/> DHCP で自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IP アドレス	10.1.101.2
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス + オール 1

5. 【保存】 ボタンをクリックします。

6. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

7. 以下の項目を指定します。

- MPLS 機能 → 使用する
- ラベル配布プロトコル → LDP

■ MPLS 基本情報	
MPLS 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
ラベル配布プロトコル	LDP

8. 【保存】 ボタンをクリックします。

9. 設定メニューのルータ設定で、「MPLS 情報」をクリックします。

「MPLS 情報」ページが表示されます。

**10. 「基本情報」をクリックします。**

「基本情報」が表示されます。

**11. 以下の項目を指定します。**

- MPLS TTL 伝達 → しない
- LDP
  - router ID → 10.1.101.2
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.1.101.2

■基本情報	
MPLS TTL伝達	<input checked="" type="radio"/> しない <input type="radio"/> する
LDP router ID	<input type="text" value="10.1.101.2"/>
LDP 制御方式	<input checked="" type="radio"/> independent <input type="radio"/> ordered
IPv4 Transport アドレス	<input type="text" value="10.1.101.2"/>

**12. [保存] ボタンをクリックします。****13. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**14. 「ルーティングマネージャ情報」をクリックします。**

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

**15. 以下の項目を指定します。**

- LDP
  - インタフェース経路情報 → 再配布しない
  - RIP 経路情報 → 再配布しない
  - OSPF 経路情報 → 再配布しない

LDP	インタフェース経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	スタティック経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	RIP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	BGP経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する
	OSPF経路情報	<input checked="" type="radio"/> 再配布しない <input type="radio"/> 再配布する

**16. [保存] ボタンをクリックします。****MPLS トンネルを設定する****17. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**18. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**19. 以下の項目を指定します。**

- ネットワーク名 → tokyo

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="tokyo"/>

**20. [追加] ボタンをクリックします。**

「ネットワーク情報 (tokyo)」ページが表示されます。

**21. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**22. 以下の項目を指定します。**

- 接続先名 → lsp1
- 接続先種別 → MPLS トンネル接続

<接続先情報追加フィールド>							
接続先名	<input type="text" value="lsp1"/>						
接続先種別	<input type="radio"/> 専用線接続						
	<input type="radio"/> ISDN接続						
	<table border="1"> <tr> <td>ダイヤル1</td> <td>電話番号</td> <td><input type="text"/></td> </tr> <tr> <td></td> <td>サブアドレス</td> <td><input type="text"/></td> </tr> </table>	ダイヤル1	電話番号	<input type="text"/>		サブアドレス	<input type="text"/>
	ダイヤル1	電話番号	<input type="text"/>				
		サブアドレス	<input type="text"/>				
<input type="radio"/> フレームリレー接続							
<input type="text" value="DLCI"/> <input type="text"/>							
<input type="radio"/> PPPoE接続							
<input type="radio"/> IPトンネル接続							
<input type="radio"/> IPsec/IKE接続							
<input type="radio"/> 別インタフェースから送出							
<input checked="" type="radio"/> MPLSトンネル接続							
<input type="radio"/> パケット破棄							

**23. [追加] ボタンをクリックします。**

MPLS トンネル接続の設定項目と「基本情報」が表示されます。

**24. 以下の項目を指定します。**

- 送出先インタフェース → LAN0
- IPv4 転送先ルータ → 10.1.101.1
- 自側エンドポイント → 10.0.0.101
- 相手側エンドポイント → 10.0.0.201

■基本情報	
接続先名	<input type="text" value="lsp1"/>
送出先インタフェース	<input type="text" value="LAN0"/>
IPv4転送先ルータ	<input type="text" value="10.1.101.1"/>
自側エンドポイント	<input type="text" value="10.0.0.101"/>
相手側エンドポイント	<input type="text" value="10.0.0.201"/>

**25. [保存] ボタンをクリックします。****26. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**27. 「ネットワーク情報」で相手定義番号が0の【修正】ボタンをクリックします。**

「ネットワーク情報」ページが表示されます。



**28. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**29. 以下の項目を指定します。**

- IPアドレス → 設定する
- 相手側IPアドレス → 10.0.0.201
- 自側IPアドレス → 10.0.0.101

**30. 「保存」ボタンをクリックします。****MPLS トンネルでシェーピングを設定する****31. 「共通情報」をクリックします。**

共通情報の設定項目と「基本情報」が表示されます。

**32. 以下の項目を指定します。**

- シェーピング → 使用する
- 最大送信レート → 5Mbps

**33. 「保存」ボタンをクリックします。****MPLS トンネルでセッション監視を設定する****34. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**35. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**36. 「ネットワーク情報」で相手定義番号が0の【修正】ボタンをクリックします。**

「ネットワーク情報」ページが表示されます。

**37. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**38. 「接続先情報」で接続先定義番号が0の【修正】ボタンをクリックします。**

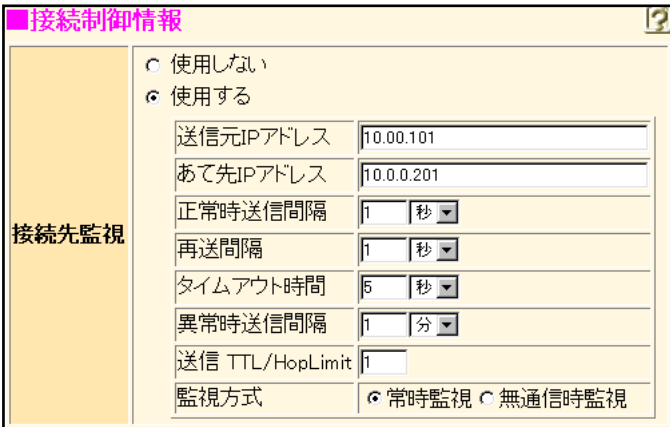
MPLS トンネル接続の設定項目と「基本情報」が表示されます。

**39. MPLS トンネル接続の設定項目の「接続制御情報」をクリックします。**

「接続制御情報」が表示されます。

**40. 以下の項目を指定します。**

- 接続先監視 → 使用する
- 送信元IPアドレス → 10.0.0.101
- あて先IPアドレス → 10.0.0.201
- 正常時送信間隔 → 1 秒
- 再送間隔 → 1 秒
- タイムアウト時間 → 5 秒
- 異常時送信間隔 → 1 分
- 送信TTL/HopLimit → 1



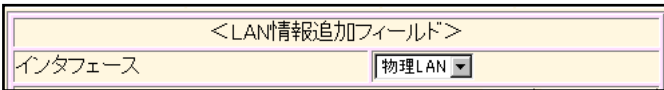
■ 接続制御情報		
接続先監視	<input type="radio"/> 使用しない	
	<input checked="" type="radio"/> 使用する	
	送信元IPアドレス	10.0.0.101
	あて先IPアドレス	10.0.0.201
	正常時送信間隔	1 秒
	再送間隔	1 秒
	タイムアウト時間	5 秒
	異常時送信間隔	1 分
	送信 TTL/HopLimit	1
	監視方式	<input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視

**41. [保存] ボタンをクリックします。****LAN1 情報を設定する****42. 設定メニューのルータ設定で、「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**43. 以下の項目を指定します。**

- インタフェース → 物理 LAN



<LAN情報追加フィールド>	
インタフェース	物理LAN

**44. [追加] ボタンをクリックします。**

「LAN1 情報 (物理 LAN)」ページが表示されます。

**45. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

#### 46. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →192.168.101.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPアドレス	<input type="radio"/> DHCPで自動的に取得する
	<input checked="" type="radio"/> 指定する
	IPアドレス <input type="text" value="192.168.101.1"/>
	ネットマスク <input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス <input type="text" value="ネットワークアドレス+オール1"/>

#### 47. [保存] ボタンをクリックします。

#### 本装置2との間で経路交換を設定する

#### 48. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

#### 49. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

#### 50. 「ネットワーク情報」で相手定義番号が0の【修正】ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

#### 51. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

#### 52. IP関連の設定項目の「OSPF情報」をクリックします。

「OSPF情報」が表示されます。

#### 53. 以下の項目を指定します。

- OSPF機能 →使用する

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する

#### 54. [保存] ボタンをクリックします。

#### 55. 設定メニューのルータ設定で、「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

#### 56. 「LAN情報」でインタフェースがLAN1の【修正】ボタンをクリックします。

「LAN1情報 (物理LAN)」ページが表示されます。

#### 57. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

**58. IP関連の設定項目の「OSPF情報」をクリックします。**

「OSPF情報」が表示されます。

**59. 以下の項目を指定します。**

- OSPF機能 →使用する
- パケット送信 →抑止する

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	0
出力コスト	10
指定ルータ優先度	1
Hello/パケット送信間隔	10 秒
隣接ルータ停止確認間隔	40 秒
パケット再送間隔	5 秒
LSU/パケット送信遅延時間	1 秒
認証方式	<input checked="" type="radio"/> 認証を行わない <input type="radio"/> テキスト認証 鍵種別 <input checked="" type="radio"/> 文字列 <input type="radio"/> 16進数 認証鍵 <input type="text"/> <input type="radio"/> MD5認証 MD5認証鍵ID <input type="text"/> MD5認証鍵 <input type="text"/>
パケット送信	<input checked="" type="radio"/> 抑止する <input type="radio"/> 抑止しない

**60. [保存] ボタンをクリックします。****61. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」ページが表示されます。

**62. 「ルーティングマネージャ情報」をクリックします。**

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

**63. 「OSPF関連」をクリックします。**

OSPF関連の設定項目と「ルータID情報」が表示されます。

**64. OSPF関連の設定項目の「OSPFエリア情報」をクリックします。**

「OSPFエリア情報」が表示されます。

**65. [追加] ボタンをクリックします。**

OSPFエリア情報 (0) の「OSPFエリア基本情報」が表示されます。

**66. 以下の項目を指定します。**

- エリアID →0.0.0.0

■OSPFエリア基本情報	
エリアID	0.0.0.0

**67. [保存] ボタンをクリックします。**

**68. 画面左側の [設定反映] 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 2 を設定する**

「本装置 1 を設定する」を参考に、本装置 2 を設定します。

**MPLS 網との接続情報を設定する****「LAN0 情報 (物理 LAN)」 - 「IP 関連」****「IP アドレス情報」**

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.1.201.2
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

**「LAN0 情報 (物理 LAN)」 - 「MPLS 関連」****「MPLS 基本情報」**

- MPLS 機能 → 使用する
  - ラベル配布プロトコル → LDP

**「MPLS 情報」****「基本情報」**

- MPLS TTL 伝達 → しない
- router ID → 10.1.201.2
- 制御方式 → independent
- IPv4 Transport アドレス → 10.1.201.2

**「ルーティングプロトコル情報」 - 「ルーティングマネージャ情報」****「再配布情報」**

- LDP
  - インタフェース経路情報 → 再配布しない
  - RIP 経路情報 → 再配布しない
  - OSPF 経路情報 → 再配布しない

**MPLS トンネルを設定する****「相手情報」 - 「ネットワーク情報」**

- ネットワーク名 → kawasaki

**「ネットワーク情報」 - 「接続先情報」**

- 接続先名 → lsp1
- 接続先種別 → MPLS トンネル接続

**「接続先情報」 - 「MPLS トンネル接続」****「基本情報」**

- 送出先インタフェース → LAN0
- IPv4 転送先ルータ → 10.1.201.1
- 自側エンドポイント → 10.0.0.201
- 相手側エンドポイント → 10.0.0.101

### 「ネットワーク情報」 - 「IP 関連」

- IPアドレス → 設定する
- 相手側IPアドレス → 10.0.0.101
- 自側IPアドレス → 10.0.0.201

## MPLS トンネルでシェーピングを設定する

### 「相手情報」 - 「ネットワーク情報」

#### 「ネットワーク情報」 - 「共通情報」

- シェーピング → 使用する
- 最大送信レート → 5Mbps

## MPLS トンネルでセッション監視を設定する

### 「相手情報」 - 「ネットワーク情報」

#### 「接続先情報」 - 「MPLS トンネル接続」

##### 「接続制御情報」

- 接続先監視 → 使用する
- 送信元IPアドレス → 10.0.0.201
- あて先IPアドレス → 10.0.0.101
- 正常時送信間隔 → 1秒
- 再送間隔 → 1秒
- タイムアウト時間 → 5秒
- 異常時送信間隔 → 1分
- 送信TTL/Hoplimit → 1

## LAN1 情報を設定する

### 「LAN1 情報 (物理LAN)」 - 「IP 関連」

#### 「IPアドレス情報」

- IPv4 → 使用する
- IPアドレス → 指定する
- IPアドレス → 192.168.201.1
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス → ネットワークアドレス + オール1

## 本装置 1 との間で経路交換を設定する

### 「相手情報」 - 「ネットワーク情報」

#### 「ネットワーク情報」 - 「IP 関連」

##### 「OSPF 情報」

- OSPF 機能 → 使用する

### 「LAN1 情報 (物理LAN)」 - 「IP 関連」

##### 「OSPF 情報」

- OSPF 機能 → 使用する
- パケット送信 → 抑止する

### 「ルーティングプロトコル情報」 - 「OSPF 関連」

#### 「OSPF エリア情報」

- エリアID → 0.0.0.0

## 2.7 MPLSを使用したレイヤ2VPN (EoMPLS) を構築する

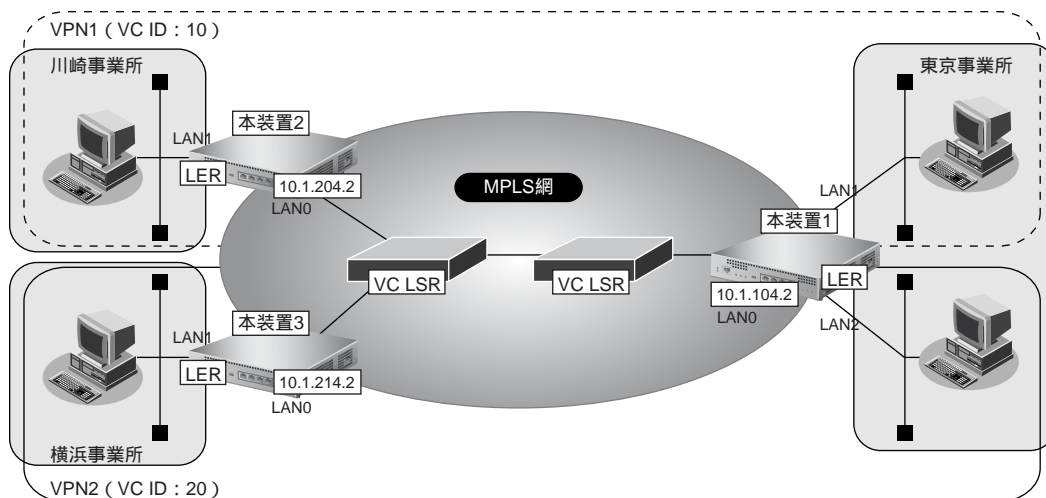
本装置では、MPLS 網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用することができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

☞ 参照 MR1000 機能説明書「2.7.1 MPLSを使用したレイヤ2VPN (EoMPLS)」(P.39)

ここでは、MPLS 接続サービス（キャリアなどから提供される MPLS をユーザインタフェースとするデータ伝送サービスを想定しています）と、MPLS LSP トンネルを使用して事業所でレイヤ2VPN を EoMPLS で構築する事例を紹介します。

こんな事に気をつけて

- 複数のインタフェースを同一の VC に含めることはできません。
- トンネル LSP を使用するインタフェースでは、MPLS を利用する設定にしてください。
- VC インタフェースでは、シェーピング機能、LAN ポートバックアップ機能および VLAN 機能を併用して動作させることができます。IP 機能、IPv6 機能、ブリッジ機能（MAC フィルタ機能を含む）、VRRP 機能は動作できません。
- EoMPLS 通信を行う場合は、MAC 学習や STP のサポートを行わないため、パケットのループが発生しないように構成してください。Ethernet フレームがループし続けて通信できなくなります。また、EoMPLS 通信を用いて冗長構成を行う場合も、LAN インタフェース側に、STP などを使用できるスイッチ装置を設置し、Ethernet フレームがループしないように設定してください。
- VLAN Tag が異なる VLAN インタフェースどうしで VC を構成し、LAN 側で STP を使用する場合は、VLAN Tag の値をそろえてください。



**● 前提条件****【本装置 1】**

- LAN0はMPLS網とし、LAN1、LAN2は事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、ループバックアドレスで接続を確立する
- MPLS網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

**【本装置 2】**

- LAN0はMPLS網とし、LAN1は事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、ループバックアドレスで接続を確立する
- MPLS網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

**【本装置 3】**

- LAN0はMPLS網とし、LAN1は事業所内LANとする
- 接続するMPLS網の次ホップLSRとは、ループバックアドレスで接続を確立する
- MPLS網とのラベル交換はループバックに対して行う
- 拠点間はスタティックルートで通信を行う

**● 設定条件****【本装置 1】**

- LAN0 (MPLS網側) のIPアドレス: 10.1.104.2
- ループバックのIPアドレス : 10.0.0.104
- LAN1のVC番号 : 10
- LAN2のVC番号 : 20

**【本装置 2】**

- LAN0 (MPLS網側) のIPアドレス: 10.1.204.2
- ループバックのIPアドレス : 10.0.0.204
- LAN1のVC番号 : 10

**【本装置 3】**

- LAN0 (MPLS網側) のIPアドレス: 10.1.214.2
- ループバックのIPアドレス : 10.0.0.214
- LAN1のVC番号 : 20

上記の設定条件に従って設定を行う場合の設定例を示します。



## 本装置 1 を設定する

### MPLS 網との接続情報を設定する

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の「修正」ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. 以下の項目を指定します。

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.1.104.2
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

IP アドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IP アドレス	<input type="radio"/> DHCP で自動的に取得する
	<input checked="" type="radio"/> 指定する
	IP アドレス: 10.1.104.2
	ネットマスク: 24 (255.255.255.0)
	ブロードキャストアドレス: ネットワークアドレス + オール 1

5. 「保存」ボタンをクリックします。

6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」ページが表示されます。

7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
  - あて先 IP アドレス → 10.0.0.204
  - あて先アドレスマスク → 32 (255.255.255.255)
  - 中継ルータアドレス → 10.1.104.1
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート
	<input checked="" type="radio"/> ネットワーク指定
	中継ルータアドレス: [ ]
	あて先 IP アドレス: 10.0.0.204
	あて先アドレスマスク: 32 (255.255.255.255)
	中継ルータアドレス: 10.1.104.1
メトリック値	1
優先度	0

8. [追加] ボタンをクリックします。

9. 手順 7.～8. を参考に、以下の項目を指定します。

- ネットワーク → ネットワーク指定  
あて先IPアドレス → 10.0.0.214  
あて先アドレスマスク → 32 (255.255.255.255)  
中継ルータアドレス → 10.1.104.1
- メトリック値 → 1
- 優先度 → 0

10. [追加] ボタンをクリックします。

11. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

12. 以下の項目を指定します。

- MPLS 機能 → 使用する
- ラベル配布プロトコル → LDP

■ MPLS 基本情報	
MPLS 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
ラベル配布プロトコル	LDP

13. [保存] ボタンをクリックします。

14. 設定メニューのルータ設定で「MPLS 情報」をクリックします。

「MPLS 情報」ページが表示されます。

15. 「基本情報」をクリックします。

「基本情報」が表示されます。

16. 以下の項目を指定します。

- MPLS TTL 伝達 → する
- LDP  
router ID → 10.0.0.104  
制御方式 → independent  
IPv4 Transport アドレス → 10.0.0.104

こんな事に気をつけて

router ID と IPv4 Transport アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

■ 基本情報		
MPLS TTL 伝達	<input type="radio"/> しない <input checked="" type="radio"/> する	
LDP	router ID	10.0.0.104
	制御方式	<input checked="" type="radio"/> independent <input type="radio"/> ordered
	IPv4 Transport アドレス	10.0.0.104

17. [保存] ボタンをクリックします。
18. 設定メニューの基本設定で「装置情報」をクリックします。  
「装置情報」ページが表示されます。
19. 「ループバック情報」をクリックします。  
「ループバック情報」が表示されます。
20. 以下の項目を指定します。
  - IPアドレス → 10.0.0.104
  - OSPF 機能 → 使用しない
  - PHP 機能 → 使用しない

■ ループバック情報	
IPアドレス	<input type="text" value="10.0.0.104"/>
OSPF機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する エリア定義番号 <input type="text" value="0"/>
PHP機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

21. [保存] ボタンをクリックします。

### 各拠点へのVCを設定する

22. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
23. 以下の項目を指定します。
  - インタフェース → 物理 LAN

<LAN情報追加フィールド>	
インタフェース	<input type="text" value="物理LAN"/>

24. [追加] ボタンをクリックします。  
「LAN1 情報 (物理 LAN)」ページが表示されます。
25. 「MPLS 関連」をクリックします。  
MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。
26. MPLS 関連の設定項目の「EoMPLS 情報」をクリックします。  
「EoMPLS 情報」が表示されます。

**27. 以下の項目を指定します。**

- EoMPLS 機能 →使用する
- VC ID →10
- 相手装置のIPv4アドレス →10.0.0.204
- VCタイプ →auto
- EXP 値書き換え →固定値0

■EoMPLS情報	
EoMPLS機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
VC ID	<input type="text" value="10"/>
相手装置のIPv4アドレス	<input type="text" value="10.0.0.204"/>
VCタイプ	<input type="text" value="auto"/>
EXP値書き換え	<input checked="" type="radio"/> 固定値 <input type="text" value="0"/> <input type="radio"/> VLANタグのプライオリティを使用する

**28. [保存] ボタンをクリックします。****29. 手順 22. ～28. を参考に、以下の項目を設定します。**

「LAN2情報 (物理 LAN)」

- EoMPLS 機能 →使用する
- VC ID →20
- 相手装置のIPv4アドレス →10.0.0.214
- VCタイプ →auto
- EXP 値書き換え →固定値0

**30. 画面左側の [設定反映] 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2を設定する

「本装置1を設定する」を参考に、本装置2を設定します。

### MPLS 網との接続情報を設定する

#### 「LAN0 情報 (物理LAN)」 - 「IP 関連」

##### 「IP アドレス情報」

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.1.204.2
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール1

##### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
  - あて先IP アドレス → 10.0.0.104
  - あて先アドレスマスク → 32 (255.255.255.0)
  - 中継ルータアドレス → 10.1.204.1
- メトリック値 → 1
- 優先度 → 0

#### 「LAN0 情報」 - 「MPLS 関連」

##### 「MPLS 基本情報」

- MPLS 機能 → 使用する
- ラベル配布プロトコル → LDP

#### 「MPLS 情報」 - 「MPLS 関連」

##### 「基本情報」

- MPLS TTL 伝達 → する
- LDP
  - router ID → 10.0.0.204
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.0.0.204

##### 「装置情報」

##### 「ループバック情報」

- IP アドレス → 10.0.0.204
- OSPF 機能 → 使用しない
- PHP 機能 → 使用しない

### 各拠点への VC を設定する

#### 「LAN 情報」 - 「MPLS 関連」

##### 「MPLS 基本情報」 - 「EoMPLS 情報」

- EoMPLS 機能 → 使用する
- VC ID → 10
- 相手装置のIPv4 アドレス → 10.0.0.104
- VC タイプ → auto
- EXP 値書き換え → 固定値0

## 本装置3を設定する

「本装置2を設定する」を参考に、本装置3を設定します。

### MPLS 網との接続情報を設定する

#### 「LAN0 情報 (物理LAN)」 - 「IP 関連」

##### 「IP アドレス情報」

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス → 10.1.214.2
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール1

##### 「スタティック経路情報」

- ネットワーク → ネットワーク指定
  - あて先IP アドレス → 10.0.0.104
  - あて先アドレスマスク → 32 (255.255.255.0)
  - 中継ルータアドレス → 10.1.214.1
- メトリック値 → 1
- 優先度 → 0

#### 「LAN0 情報」 - 「MPLS 関連」

##### 「MPLS 基本情報」

- MPLS 機能 →使用する
- ラベル配布プロトコル → LDP

#### 「MPLS 情報」 - 「MPLS 関連」

##### 「基本情報」

- MPLS TTL 伝達 →する
- LDP
  - router ID → 10.0.0.214
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.0.0.214

##### 「装置情報」

##### 「ループバック情報」

- IP アドレス → 10.0.0.214
- OSPF 機能 →使用しない
- PHP 機能 →使用しない

### 各拠点へのVCを設定する

#### 「LAN 情報」 - 「MPLS 関連」

##### 「MPLS 基本情報」 - 「EoMPLS 情報」

- EoMPLS 機能 →使用する
- VC ID → 10
- 相手装置のIPv4 アドレス → 10.0.0.104
- VC タイプ → auto
- EXP 値書き換え →固定値0

## 2.8 MPLS を使用したレイヤ3VPN (BGP/MPLS VPN) を構築する

本装置では、MPLS 網を経由することによって、公衆ネットワーク上に仮想的なプライベートネットワーク（閉域網）を構築することができ、遠隔地のネットワークを同じオフィス内のネットワークと同じように利用することができます。また、少ない設備で、業務単位で隔離したネットワークを実現することができます。

☛ 参照 MR1000 機能説明書「[2.7.2 MPLS を使用したレイヤ3VPN \(BGP/MPLS VPN\)](#)」(P.41)

ここでは、MPLS を使用したVPN ネットワークを構築する場合の設定方法を説明します。

東京事業所と川崎事業所が MPLS 網に接続し、業務ごとに異なる VPN ネットワークを構築します。このとき、本装置 1、2 がそれぞれの前提条件を満たしていることを前提とします。

### こんな事に気をつけて

- BGP/MPLS VPN 機能は IPv4 の場合だけ利用できます。IPv6 では使用できません。
- BGP で接続できる相手は 1 セッションだけです。このため、ルータリフレクタと接続する必要があります。
- IP-VPN 接続と併用することはできません。
- BGP ネットワーク、BGP 集約経路および BGP フィルタリングの機能は使用できません。
- BGP/MPLS VPN 機能と NAT 機能を併用することはできません。
- 本装置は、LER としてだけ動作します。
- BGP/MPLS VPN で構成された VPN ネットワーク内では、EBGP、OSPF および RIP は使用できません。
- 異なる VPN を収容する場合、VPN のインタフェースに設定した IP アドレスおよび属するネットワークアドレスを他 VPN インタフェースに設定できません。必ず異なるネットワークアドレスを設定してください。
- MPLS 網と接続するインタフェースで RIP を使用する場合、VPN で使用するインタフェース経路を RIP で広報します。MPLS への広報に対してフィルタリングを行ってください。
- LER では、受信した IP パケットを IP 処理層を通さずにラベルを付加します。IP フィルタリング機能、TOS 値書き換え機能およびソートフラグメント機能は、VPN に設定したインタフェースへの入力に限り動作します。ただし、VPN からの入力を IPsec によって暗号化し、対向ルータに送信する運用や帯域制御 (WFQ) 機能、イコールコストマルチパスなどの他 IP 機能を使用した運用は行うことはできません。
- VRRP と併用する場合は、トリガとしてインタフェースダウントリガまたはルートダウントリガ (VPN 内経路は対象外) が利用できます。ノードダウントリガは利用できません。
- BGP/MPLS VPN 構成では、LER は MTU 長の設定にかかわらず、IP パケットのフラグメント処理を行いません。受信したパケットはそのままラベルを付加して送信します。このため、MTU 長を調整する必要がある運用 (VoIP 通信でのインターリーブなど) はできません。
- ループバックインタフェースで設定した IP アドレスを BGP の自側 IP アドレスとして使用しなければいけません。
- IP アドレスが設定されていないインタフェースでは MPLS は使用できません。隣接 MPLS 装置間で LDP セッションを構築する際、インタフェースのアドレスを用いる場合があります。
- BRI などの低速回線での高負荷時や装置の転送能力を超える高負荷が発生する場合、LDP セッションが切断されることがあります。LDP の Hello ホールドタイムを長め (例: 30 秒) に設定してください。
- MPLS を利用すると、Ethernet フレームに 4 バイトのシムヘッダが最大 2 つ付加されます。最大 1526 バイトの Ethernet フレームが送出されることとなります。通常の Ethernet フレームの最大サイズは 1518 バイトです。1526 バイトのフレームに対応していない機器と接続する場合は、MPLS を利用するインタフェースの MTU サイズを初期値の 1500 バイトから 1492 バイトに変更することで通信することができます。
- VPN 通信で使用するネットワークアドレスと、本装置に設定するすべてのネットワークアドレスが重複しないように設定してください。たとえば、本装置の MPLS ドメイン側 IP アドレスが 10.1.1.1/24 のとき、10.1.1.0/24 のネットワークを VPN として収容することはできません。
- VPN 以外の SNMP マネージャは VPN 内の装置を管理することはできません。
- BGP セッションの通信に使用するループバックインタフェースに設定したアドレスへの経路は集約しないでください。集約すると、トンネル LSP が正しく生成されません。





## ● 設定条件

- MPLS 網の使用条件
  - BGP AS 番号 : 10
  - RR の IP アドレス : 172.16.100.1
  - MPLS 網で使用する IPv4 ネットワーク : OSPF
  - : バックボーンエリア
- VPN-A の使用条件
  - ルート識別子 : 10:1
  - 使用するネットワーク : 10.10.10/24 川崎事業所
  - : 10.10.20/24 東京事業所
  - : 10.10.21/24 東京事業所
- VPN-B の使用条件
  - ルート識別子 : 10:2
  - 使用するネットワーク : 10.20.10/24 川崎事業所
  - : 10.20.20/24 東京事業所
  - : 10.20.21/24 東京事業所

### 【本装置 1】

- ループバックインタフェースの IP アドレス : 10.1.1.1
- ループバックインタフェースでのルーティングプロトコル : OSPF
- ループバックインタフェースでの OSPF エリア ID : 0.0.0.1
- LAN0 でのルーティングプロトコル : OSPF
- LAN0 での OSPF エリア ID : 0.0.0.1
- LAN2 で使用する VPN : VPN-A
- LAN3 で使用する VPN : VPN-B

### 【本装置 2】

- ループバックインタフェースの IP アドレス : 10.2.1.1
- ループバックインタフェースでのルーティングプロトコル : OSPF
- ループバックインタフェースでの OSPF エリア ID : 0.0.0.2
- LAN0 でのルーティングプロトコル : OSPF
- LAN0 での OSPF エリア ID : 0.0.0.2
- LAN2 で使用する VPN : VPN-A
- LAN2 で使用する BGP/MPLS VPN スタティック経路情報
  - あて先 IP アドレス : 10.10.21.0/24
  - 中継ルータアドレス : 10.10.20.2
- LAN3 で使用する VPN : VPN-B
- LAN3 で使用する BGP/MPLS VPN スタティック経路情報
  - あて先 IP アドレス : 10.20.21.0/24
  - 中継ルータアドレス : 10.20.20.2

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置2を設定する

### ループバック情報を設定する

**1. 設定メニューの基本設定で「装置情報」をクリックします。**

「装置情報」ページが表示されます。

**2. 「ループバック情報」をクリックします。**

「ループバック情報」が表示されます。

**3. 以下の項目を指定します。**

- IPアドレス → 10.2.1.1
- OSPF 機能 → 使用する  
エリア定義番号 → 0

こんな事に気をつけて

エリア定義は、ルータ設定の「ルーティングプロトコル情報」 - 「OSPF エリア情報」で設定します。

■ ループバック情報	
IPアドレス	<input type="text" value="10.2.1.1"/>
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する <input type="text" value="0"/> エリア定義番号
PHP機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない

**4. 【保存】 ボタンをクリックします。**

### MPLS 網と接続する LAN0 に OSPF 機能を設定する

**5. 設定メニューのルータ設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**6. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。**

「LAN0 情報 (物理 LAN)」ページが表示されます。

**7. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**8. IP 関連の設定項目の「OSPF 情報」をクリックします。**

「OSPF 情報」が表示されます。

## 9. 以下の項目を指定します。

- OSPF 機能 →使用する
- エリア定義番号 →0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	0

## 10. [保存] ボタンをクリックします。

### OSPF 関連を設定する

## 11. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

## 12. 「OSPF 関連」をクリックします。

OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。

## 13. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。

「OSPF エリア情報」が表示されます。

## 14. [追加] ボタンをクリックします。

OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。

## 15. 以下の項目を指定します。

- エリアID →0.0.0.2

■OSPFエリア基本情報	
エリアID	0.0.0.2

## 16. [保存] ボタンをクリックします。

### MPLS 網と接続する LAN0 に MPLS 機能を設定する

## 17. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

## 18. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

## 19. 「MPLS 関連」をクリックします。

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

## 20. 以下の項目を指定します。

- MPLS 機能 →使用する
- ラベル配布プロトコル →LDP

■MPLS基本情報	
MPLS機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
ラベル配布プロトコル	LDP

21. [保存] ボタンをクリックします。
22. 設定メニューのルータ設定で、「MPLS 情報」をクリックします。  
「MPLS 情報」ページが表示されます。
23. 「基本情報」をクリックします。  
「基本情報」が表示されます。
24. 以下の項目を指定します。
  - MPLS TTL 伝達 → する
  - LDP
    - router ID → 10.2.1.1
    - 制御方式 → independent
    - IPv4 Transport アドレス → 10.2.1.1

こんな事に気をつけて

router ID と IPv4 Transport アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

■基本情報	
MPLS TTL伝達	<input type="radio"/> しない <input checked="" type="radio"/> する
LDP router ID	<input type="text" value="10.2.1.1"/>
LDP 制御方式	<input checked="" type="radio"/> independent <input type="radio"/> ordered
IPv4 Transport アドレス	<input type="text" value="10.2.1.1"/>

25. [保存] ボタンをクリックします。

## ルートリフレクタの接続情報を設定する

26. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」のページが表示されます。
27. 「BGP 関連」をクリックします。  
BGP 関連の設定項目と「BGP 情報」が表示されます。
28. 以下の項目を指定します。
  - BGP 機能 → 使用する
  - 自 AS 番号 → 10
  - 自 ID 番号 → 10.2.1.1

こんな事に気をつけて

自 ID 番号には、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

■BGP情報	
BGP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
自AS番号	<input type="text" value="10"/>
自ID番号	<input type="text" value="10.2.1.1"/>
BGPネットワーク	<input type="checkbox"/> 常に広報する

29. [保存] ボタンをクリックします。

30. BGP関連の設定項目の「BGP相手情報」をクリックします。

「BGP相手情報」が表示されます。

31. [追加] ボタンをクリックします。

BGP相手情報 (0) の設定項目と「BGP相手基本情報」が表示されます。

32. 以下の項目を指定します。

- 相手側IPアドレス → 172.16.100.1
- 相手AS番号 → 10
- 自側IPアドレス → 10.2.1.1

こんな事に気をつけて

- ルートリフレクタのIPアドレスを相手側IPアドレスに設定してください。
- 自側IPアドレスには、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■BGP相手基本情報	
相手側IPアドレス	172.16.100.1
相手AS番号	10
自側IPアドレス	10.2.1.1

33. [保存] ボタンをクリックします。

34. BGP相手情報 (0) の設定項目の「BGP拡張機能情報」をクリックします。

「BGP拡張機能情報」が表示されます。

35. 以下の項目を指定します。

- アドレスファミリー情報 → VPN IPv4 ユニキャスト

■BGP拡張機能情報	
アドレスファミリー情報	VPN IPv4ユニキャスト
エンフォースマルチホップ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する

36. [保存] ボタンをクリックします。

VPN-A およびVPN-B 情報としてVRF情報を設定する

37. 画面上部の「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」のページが表示されます。

38. 「BGP関連」をクリックします。

BGP関連の設定項目と「BGP情報」が表示されます。

39. BGP関連の設定項目の「VRF情報」をクリックします。

「VRF情報」が表示されます。

**40. 以下の項目を指定します。**

- ルート識別子  
AS 番号 → 10  
識別番号 → 1
- BGP/MPLS VPN 広報  
スタティック経路情報 →再配布する  
インタフェース経路情報 →再配布する

<VRF情報入力フィールド>		
ルート識別子	AS番号	10
	識別番号	1
BGP/MPLS VPN 広報	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する

**41. [追加] ボタンをクリックします。****42. 手順 40.、41. を参考に、以下の項目を指定します。**

- ルート識別子  
AS 番号 → 10  
識別番号 → 2
- BGP/MPLS VPN 広報  
スタティック経路情報 →再配布する  
インタフェース経路情報 →再配布する

**LAN2 情報を設定する****43. 設定メニューのルータ設定で、「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**44. 「LAN 情報」でインタフェースが LAN2 の [修正] ボタンをクリックします。**

「LAN2 情報 (物理 LAN)」ページが表示されます。

**45. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**46. 以下の項目を指定します。**

- IPv4 →使用する
- IP アドレス →指定する  
IP アドレス → 10.10.20.1  
ネットマスク → 24 (255.255.255.0)  
ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IP アドレス	<input type="radio"/> DHCPで自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IPアドレス	10.10.20.1
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス+オール1

47. [保存] ボタンをクリックします。

48. IP関連の設定項目の「BGP/MPLS VPN情報」をクリックします。

「BGP/MPLS VPN情報」が表示されます。

49. 以下の項目を指定します。

- BGP/MPLS VPN機能 →使用する
- VRF 定義番号 →0

50. [保存] ボタンをクリックします。

51. IP関連の設定項目の「BGP/MPLS VPNスタティック経路情報」をクリックします。

「BGP/MPLS VPNスタティック経路情報」が表示されます。

52. 以下の項目を指定します。

- ネットワーク →ネットワーク指定
- あて先IPアドレス →10.10.21.0
- あて先アドレスマスク →24 (255.255.255.0)
- 中継ルータアドレス →10.10.20.2

53. [追加] ボタンをクリックします。

54. 43.～53.を参考に、「LAN3情報 (物理LAN)」で以下の項目を指定します。

### LAN3情報を設定する

#### 「LAN情報3情報 (物理LAN)」 - 「IP関連」

##### 「IPアドレス情報」

- IPv4 →使用する
- IPアドレス →指定する
- IPアドレス →10.20.20.1
- ネットマスク →24 (255.255.255.0)
- ブロードキャストアドレス →ネットワークアドレス+オール1

##### 「BGP/MPLS VPN情報」

- BGP/MPLS VPN機能 →使用する
- VRF 定義番号 →1

**「BGP/MPLS VPNスタティック経路情報」**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 10.20.21.0
- あて先アドレスマスク → 24 (255.255.255.0)
- 中継ルータアドレス → 10.20.20.2

**55. 画面左側の「設定反映」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1を設定する**

「本装置2を設定する」を参考に、本装置1を設定します。

**ループバック情報を設定する****「装置情報」 - 「ループバック情報」**

- IPアドレス → 10.1.1.1
- OSPF 機能 → 使用する
- エリア定義番号 → 0

**MPLS 網と接続する LAN0 に OSPF 機能を設定する****「LAN0 情報」 - 「IP 関連」****「OSPF 情報」**

- OSPF 機能 → 使用する
- エリア定義番号 → 0

**「ルーティングプロトコル情報」 - 「OSPF 関連」****「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」**

- エリアID → 0.0.0.1

**MPLS 網と接続する LAN0 に MPLS 機能を設定する****「LAN0 情報」 - 「MPLS 関連」****「MPLS 基本情報」**

- MPLS 機能 → 使用する
- ラベル配布プロトコル → LDP

**「MPLS 情報 - 「基本情報」**

- MPLS TTL 伝達 → する
- LDP
  - router ID → 10.1.1.1
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.1.1.1



## ルータリフレクタの接続情報を設定する

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「BGP 情報」

- BGP機能 →使用する
- 自AS番号 →10
- 自ID番号 →10.1.1.1

#### 「BGP 相手情報」 - 「BGP相手基本情報」

- 相手側IPアドレス →172.16.100.1
- 相手AS番号 →10
- 自側IPアドレス →10.1.1.1

#### 「BGP 相手情報」 - 「BGP拡張機能情報」

- アドレスファミリー情報 →VPN IPv4 ユニキャスト

## VPN-A およびVPN-B 情報としてVRF 情報を設定する

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「VRF 情報 (0)」

- ルート識別子  
AS番号 →10  
識別番号 →1
- BGP/MPLS VPN 広報  
スタティック経路情報 →再配布しない  
インタフェース経路情報 →再配布する

#### 「VRF 情報 (1)」

- ルート識別子  
AS番号 →10  
識別番号 →2
- BGP/MPLS VPN 広報  
スタティック経路情報 →再配布しない  
インタフェース経路情報 →再配布する

## LAN2 情報を設定する

### 「LAN2 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 →使用する
- IPアドレス →指定する  
IPアドレス →10.10.10.1  
ネットマスク →24 (255.255.255.0)  
ブロードキャストアドレス →ネットワークアドレス+オール1

### 「LAN2 情報」 - 「BGP 関連」

#### 「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能 →使用する
- VRF 定義番号 →0

## LAN3 情報を設定する

### 「LAN3 情報」 - 「IP 関連」

#### 「IP アドレス情報」

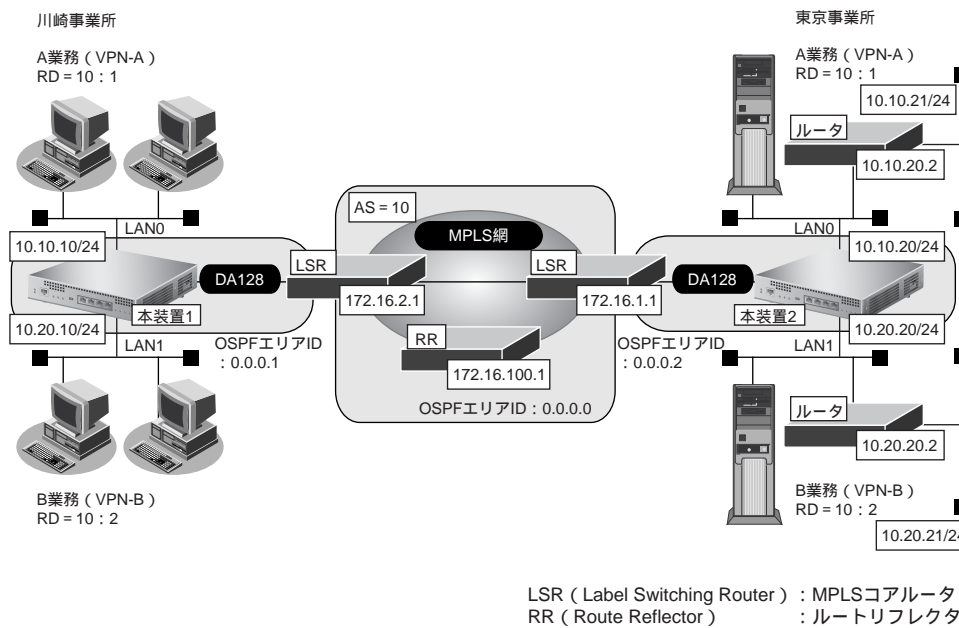
- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス → 10.20.10.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

### 「LAN3 情報」 - 「BGP 関連」

#### 「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能 →使用する
- VRF 定義番号 → 1

## 2.8.2 MPLS 網と専用線を使用して接続する



### ● 前提条件

- すべてのインタフェースにIPアドレスを設定する
- すべてのインタフェースでNAT機能およびDHCPクライアント機能を使用しない

### ● 設定条件

- MPLS網の使用条件
 

BGP AS番号	: 10
RRのIPアドレス	: 172.16.100.1
MPLS網で使用するIPv4ネットワーク	: OSPF
	: バックボーンエリア
- VPN-Aの使用条件
 

ルート識別子	: 10:1
使用するネットワーク	: 10.10.10/24 川崎事業所
	: 10.10.20/24 東京事業所
	: 10.10.21/24 東京事業所
- VPN-Bの使用条件
 

ルート識別子	: 10:2
使用するネットワーク	: 10.20.10/24 川崎事業所
	: 10.20.20/24 東京事業所
	: 10.20.21/24 東京事業所

### 【本装置1 (川崎事業所)】

- ループバックインタフェースのIPアドレス : 10.1.1.1
- ループバックインタフェースでのルーティングプロトコル : OSPF
- ループバックインタフェースでのOSPFエリアID : 0.0.0.1
- rmt0でのルーティングプロトコル : OSPF
- rmt0でのOSPFエリアID : 0.0.0.1
- LAN0で使用するVPN : VPN-A
- LAN1で使用するVPN : VPN-B

**【本装置2 (東京事業所)】**

- ループバックインタフェースのIPアドレス : 10.2.1.1
- ループバックインタフェースでのルーティングプロトコル : OSPF
- ループバックインタフェースでのOSPFエリアID : 0.0.0.2
- rmt0でのルーティングプロトコル : OSPF
- rmt0でのOSPFエリアID : 0.0.0.2
- LAN0で使用するVPN : VPN-A
- LAN0で使用するBGP/MPLS VPNスタティック経路情報  
あて先IPアドレス : 10.10.21.0/24  
中継ルータアドレス : 10.10.20.2
- LAN1で使用するVPN : VPN-B
- LAN1で使用するBGP/MPLS VPNスタティック経路情報  
あて先IPアドレス : 10.20.21.0/24  
中継ルータアドレス : 10.20.20.2

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置2を設定する

### ループバック情報を設定する

#### 1. 設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

#### 2. 「ループバック情報」をクリックします。

「ループバック情報」が表示されます。

#### 3. 以下の項目を指定します。

- IPアドレス → 10.2.1.1
- OSPF機能 → 使用する  
エリア定義番号 → 0

こんな事に気をつけて

エリア定義は、ルータ設定の「ルーティングプロトコル情報」－「OSPFエリア情報」で設定します。

■ ループバック情報	
IPアドレス	10.2.1.1
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する エリア定義番号 <input type="text" value="0"/>
PHP機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない

#### 4. [保存] ボタンをクリックします。

## MPLS 網と接続するインタフェースに OSPF 機能を設定する

5. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
6. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
7. OSPF 機能を設定するネットワーク欄の【修正】ボタンをクリックします。  
「ネットワーク情報」ページが表示されます。
8. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
9. IP 関連の設定項目の「OSPF 情報」をクリックします。  
「OSPF 情報」が表示されます。
10. 以下の項目を指定します。
  - OSPF 機能 → 使用する
  - エリア定義番号 → 0

■OSPF情報	
OSPF機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
エリア定義番号	0

11. 【保存】ボタンをクリックします。
12. 設定メニューのルータ設定で、「ルーティングプロトコル情報」をクリックします。  
「ルーティングプロトコル情報」ページが表示されます。
13. 「OSPF 関連」をクリックします。  
OSPF 関連の設定項目と「ルータ ID 情報」が表示されます。
14. OSPF 関連の設定項目の「OSPF エリア情報」をクリックします。  
「OSPF エリア情報」が表示されます。
15. 【追加】ボタンをクリックします。  
OSPF エリア情報 (0) の「OSPF エリア基本情報」が表示されます。
16. 以下の項目を指定します。
  - エリアID → 0.0.0.2

■OSPFエリア基本情報	
エリアID	0.0.0.2

17. 【保存】ボタンをクリックします。

## MPLS 網と接続するインタフェースに MPLS 機能を設定する

18. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。

**19. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**20. MPLS 機能を設定するネットワーク欄の [修正] ボタンをクリックします。**

「ネットワーク情報」ページが表示されます。

**21. 「MPLS 関連」をクリックします。**

MPLS 関連の設定項目と「MPLS 基本情報」が表示されます。

**22. 以下の項目を指定します。**

- MPLS 機能 → 使用する
- ラベル配布プロトコル → LDP

■MPLS基本情報	
MPLS機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
ラベル配布プロトコル	LDP

**23. [保存] ボタンをクリックします。****24. 設定メニューのルータ設定で、「MPLS 情報」をクリックします。**

「MPLS 情報」ページが表示されます。

**25. 「基本情報」をクリックします。**

「基本情報」が表示されます。

**26. 以下の項目を指定します。**

- MPLS TTL 伝達 → する
- LDP
  - router ID → 10.2.1.1
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.2.1.1

こんな事に気をつけて

router ID と IPv4 Transport アドレスには、装置のループバックインタフェースに設定された IPv4 アドレスを設定する必要があります。

■基本情報	
MPLS TTL伝達	<input type="radio"/> しない <input checked="" type="radio"/> する
LDP router ID	10.2.1.1
LDP 制御方式	<input checked="" type="radio"/> independent <input type="radio"/> ordered
IPv4 Transport アドレス	10.2.1.1

**27. [保存] ボタンをクリックします。****ルートルフレクタへの接続情報を設定する****28. 設定メニューのルータ設定で「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」のページが表示されます。

**29. 「BGP関連」をクリックします。**

BGP関連の設定項目と「BGP情報」が表示されます。

**30. 以下の項目を指定します。**

- BGP機能 → 使用する
- 自AS番号 → 10
- 自ID番号 → 10.2.1.1

こんな事に気をつけて

自ID番号には、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■BGP情報	
BGP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
自AS番号	<input type="text" value="10"/>
自ID番号	<input type="text" value="10.2.1.1"/>
BGPネットワーク	<input type="checkbox"/> 常に広報する

**31. [保存] ボタンをクリックします。****32. BGP関連の設定項目の「BGP相手情報」をクリックします。**

「BGP相手情報」が表示されます。

**33. [追加] ボタンをクリックします。**

BGP相手情報 (0) の設定項目と「BGP相手基本情報」が表示されます。

**34. 以下の項目を指定します。**

- 相手側IPアドレス → 172.16.100.1
- 相手AS番号 → 10
- 自側IPアドレス → 10.2.1.1

こんな事に気をつけて

- ルートリフレクタのIPアドレスを相手側IPアドレスに設定してください。
- 自側IPアドレスには、装置のループバックインタフェースに設定されたIPv4アドレスを設定する必要があります。

■BGP相手基本情報	
相手側IPアドレス	<input type="text" value="172.16.100.1"/>
相手AS番号	<input type="text" value="10"/>
自側IPアドレス	<input type="text" value="10.2.1.1"/>

**35. [保存] ボタンをクリックします。****36. BGP相手情報 (0) の設定項目の「BGP拡張機能情報」をクリックします。**

「BGP拡張機能情報」が表示されます。

**37. 以下の項目を指定します。**

- アドレスファミリー情報 → VPN IPv4 ユニキャスト

■ BGP拡張機能情報	
アドレスファミリー情報	VPN IPv4ユニキャスト
エンフォースマルチホップ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する

**38. [保存] ボタンをクリックします。****VPN-A およびVPN-B 情報としてVRF情報を設定する****39. 画面上部の「ルーティングプロトコル情報」をクリックします。**

「ルーティングプロトコル情報」のページが表示されます。

**40. 「BGP関連」をクリックします。**

BGP関連の設定項目と「BGP情報」が表示されます。

**41. BGP関連の設定項目の「VRF情報」をクリックします。**

「VRF情報」が表示されます。

**42. 以下の項目を指定します。**

- ルート識別子
  - AS番号 → 10
  - 識別番号 → 1
- BGP/MPLS VPN広報
  - スタティック経路情報 → 再配布する
  - インタフェース経路情報 → 再配布する

<VRF情報入力フィールド>		
ルート識別子	AS番号	10
	識別番号	1
BGP/MPLS VPN広報	スタティック経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する
	インタフェース経路情報	<input type="radio"/> 再配布しない <input checked="" type="radio"/> 再配布する

**43. [追加] ボタンをクリックします。****44. 手順 42. ~ 43. を参考に、以下の項目を指定します。**

- ルート識別子
  - AS番号 → 10
  - 識別番号 → 2
- BGP/MPLS VPN広報
  - スタティック経路情報 → 再配布する
  - インタフェース経路情報 → 再配布する

**LAN0 情報を設定する****45. 設定メニューのルータ設定で、「LAN情報」をクリックします。**

「LAN情報」ページが表示されます。



**46. 「LAN 情報」でインタフェースが LAN0 の「修正」ボタンをクリックします。**

「LAN0 情報 (物理 LAN)」ページが表示されます。

**47. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**48. 以下の項目を指定します。**

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.10.20.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

■ IP アドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IP アドレス	<input type="radio"/> DHCP で自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IP アドレス	<input type="text" value="10.10.20.1"/>
	ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス	<input type="text" value="ネットワークアドレス + オール 1"/>

**49. 「保存」ボタンをクリックします。****50. IP 関連の設定項目の「BGP/MPLS VPN 情報」をクリックします。**

「BGP/MPLS VPN 情報」が表示されます。

**51. 以下の項目を指定します。**

- BGP/MPLS VPN 機能 → 使用する
- VRF 定義番号 → 0

■ BGP/MPLS VPN 情報	
BGP/MPLS VPN 機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
VRF 定義番号	<input type="text" value="0"/>

**52. 「保存」ボタンをクリックします。****53. IP 関連の設定項目の「BGP/MPLS VPN スタティック経路情報」をクリックします。**

「BGP/MPLS VPN スタティック経路情報」が表示されます。

**54. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 10.10.21.0
- あて先アドレスマスク → 24 (255.255.255.0)
- 中継ルータアドレス → 10.10.20.2

<スタティック経路情報入力フィールド>

ネットワーク

デフォルトルート  
 ネットワーク指定

中継ルータアドレス

あて先IPアドレス 10.10.21.0

あて先アドレスマスク 24 (255.255.255.0)

中継ルータアドレス 10.10.20.2

**55. [追加] ボタンをクリックします。****56. 45.～55.を参考に、「LAN1 情報（物理LAN）」で以下の項目を指定します。****LAN1 情報を設定する****「LAN1 情報（物理LAN）」 - 「IP 関連」****「IP アドレス情報」**

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 10.20.20.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス+オール1

**「LAN1 情報（物理LAN）」 - 「BGP 関連」****「BGP/MPLS VPN 情報」**

- BGP/MPLS VPN 機能 → 使用する
- VRF 定義番号 → 1

**「BGP/MPLS VPN スタティック経路情報」**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 10.20.21.0
- あて先アドレスマスク → 24 (255.255.255.0)
- 中継ルータアドレス → 10.20.20.2

**57. 画面左側の [設定反映] 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 1 を設定する

---

「本装置 2 を設定する」を参考に、本装置 1 を設定します。

### ループバック情報を設定する

#### 「装置情報」 - 「ループバック情報」

- IPアドレス → 10.1.1.1
- OSPF 機能 → 使用する
- エリア定義番号 → 0

### MPLS 網と接続するインタフェースに OSPF 機能を設定する

#### 「LAN 情報」 - 「IP 関連」

##### 「OSPF 情報」

- OSPF 機能 → 使用する
- エリア定義番号 → 0

#### 「ルーティングプロトコル情報」 - 「OSPF 関連」

##### 「OSPF エリア情報 (0)」 - 「OSPF エリア基本情報」

- エリアID → 0.0.0.1

### MPLS 網と接続するインタフェースに MPLS 機能を設定する

#### 「相手情報」 - 「ネットワーク情報」

#### 「ネットワーク情報」 - 「MPLS 関連」

##### 「MPLS 基本情報」

- MPLS 機能 → 使用する
- ラベル配布プロトコル → LDP

#### 「MPLS 情報」 - 「基本情報」

- MPLS TTL 伝達 → する
- LDP
  - router ID → 10.1.1.1
  - 制御方式 → independent
  - IPv4 Transport アドレス → 10.1.1.1

### ルートリフレクタへの接続情報を設定する

#### 「ルーティングプロトコル情報」 - 「BGP 関連」

##### 「BGP 情報」

- BGP 機能 → 使用する
- 自 AS 番号 → 10
- 自 ID 番号 → 10.1.1.1

#### 「BGP 相手情報」 - 「BGP 相手基本情報」

- 相手側 IP アドレス → 172.16.100.1
- 相手 AS 番号 → 10
- 自側 IP アドレス → 10.1.1.1

### 「BGP 相手情報」 - 「BGP 拡張機能情報」

- アドレスファミリー情報 → VPN IPv4 ユニキャスト

## VPN-A および VPN-B 情報として VRF 情報を設定する

### 「ルーティングプロトコル情報」 - 「BGP 関連」

#### 「VRF 情報 (0)」

- ルート識別子
  - AS 番号 → 10
  - 識別番号 → 1
- BGP/MPLS VPN 広報
  - スタティック経路情報 → 再配布しない
  - インタフェース経路情報 → 再配布する

#### 「VRF 情報 (1)」

- ルート識別子
  - AS 番号 → 10
  - 識別番号 → 2
- BGP/MPLS VPN 広報
  - スタティック経路情報 → 再配布しない
  - インタフェース経路情報 → 再配布する

## LAN0 情報を設定する

### 「LAN0 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 → 使用する
- IP アドレス
  - IP アドレス → 10.10.10.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

#### 「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能 → 使用する
- VRF 定義番号 → 0

## LAN1 情報を設定する

### 「LAN1 情報」 - 「IP 関連」

#### 「IP アドレス情報」

- IPv4 → 使用する
- IP アドレス
  - IP アドレス → 10.20.10.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

#### 「BGP/MPLS VPN 情報」

- BGP/MPLS VPN 機能 → 使用する
- VRF 定義番号 → 1

### こんな事に気をつけて

サポートインタフェースは BRI (ISDN、HSD) と LAN です。モデムや FR には対応していません。

**⚠注意**

---

MPLS、BGP、OSPF および RIP 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、BGP/MPLS VPN 機能は使用しないでください。

---

## 2.9 マルチリンク機能を使う

ISDNによって相手装置と接続するときに、マルチリンク機能を使用することができます。マルチリンク機能では、Bチャンネル（64Kbps）を論理的に2本束ねることによって、最大128Kbpsで通信できます。また、BAP/BACP機能を利用すると動的にチャンネルを増減することができ、回線を効率良く利用することができます。

☞ 参照 MR1000 機能説明書「2.8 マルチリンク機能」(P.44)

ここでは、ISDN接続をネットワーク情報（internet）で定義してある環境に対してマルチリンクを行う場合の設定方法を説明します。

### ● 設定条件

- ネットワーク情報（internet）でISDNによる通信環境が設定済み
- 接続直後のリンク数は2チャンネル
- チャンネルの使用率90%以上が60秒以上続いたら、チャンネルを増加する
- チャンネルの使用率40%以下が10秒以上続いたら、チャンネルを減少する
- 受信順序制御機能（MP）を使用する

上記の設定条件に従ってマルチリンクを行う場合の設定例を示します。

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. ネットワーク名がinternetの【修正】ボタンをクリックします。  
「ネットワーク情報（internet）」ページが表示されます。
4. 「接続先情報」をクリックします。  
「接続先情報」が表示されます。
5. マルチリンクを設定する接続先欄の【修正】ボタンをクリックします。  
ISDN接続の設定項目と「基本情報」が表示されます。
6. ISDN接続の設定項目の「PPP情報」をクリックします。  
「PPP情報」が表示されます。
7. 以下の項目を指定します。
  - MP接続 → する
  - BAP/BACP利用 → しない

MP接続	<input type="radio"/> しない
	<input checked="" type="radio"/> する
	BAP/BACP利用 <input checked="" type="radio"/> しない <input type="radio"/> する
※ 発信者番号による識別で番号をチェックしない場合は着信相手識別情報の設定が有効	

8. 【保存】ボタンをクリックします。

**9. 画面上部の「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**10. 「PPP 関連」をクリックします。**

PPP 関連の設定項目と「圧縮情報」が表示されます。

**11. PPP 関連の設定項目の「MP 情報」をクリックします。****12. 以下の項目を指定します。**

- MP回線初期リンク数 → 2
- トラフィックによる増減 → する
  - 回線増加条件
  - 回線使用率 → 90
  - 猶予時間 → 60
  - 回線削減条件
  - 回線使用率 → 40
  - 猶予時間 → 10
- 受信パケット順序制御 → する

■MP情報													
MP回線初回リンク数	2												
トラフィックによる増減	<input type="radio"/> しない <input checked="" type="radio"/> する												
	<table border="1"> <thead> <tr> <th>回線増加条件</th> <th>回線使用率</th> <th>猶予時間</th> </tr> </thead> <tbody> <tr> <td>90 %</td> <td></td> <td>60 秒</td> </tr> <tr> <th>回線削減条件</th> <th>回線使用率</th> <th>猶予時間</th> </tr> <tr> <td>40 %</td> <td></td> <td>10 秒</td> </tr> </tbody> </table>	回線増加条件	回線使用率	猶予時間	90 %		60 秒	回線削減条件	回線使用率	猶予時間	40 %		10 秒
	回線増加条件	回線使用率	猶予時間										
	90 %		60 秒										
回線削減条件	回線使用率	猶予時間											
40 %		10 秒											
受信パケット順序制御	<input type="radio"/> しない <input checked="" type="radio"/> する												

**13. [保存] ボタンをクリックします。****14. 画面左側の [設定反映] 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。

## 2.10 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

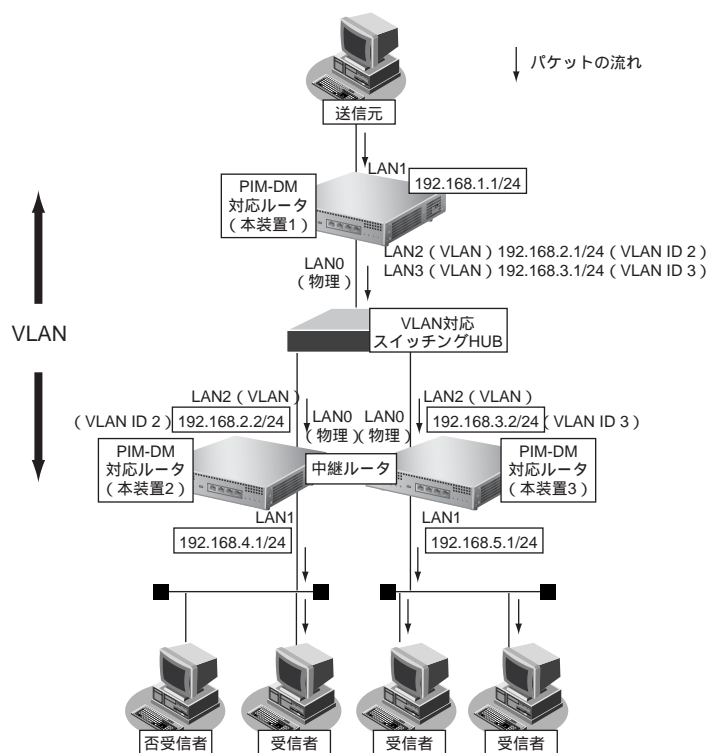
☛ 参照 MR1000 機能説明書 「2.9 マルチキャスト機能」 (P.45)

### 2.10.1 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。







上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置 1 を設定する

### LAN1 情報を設定する

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN1 の【修正】 ボタンをクリックします。  
「LAN1 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「マルチキャスト情報」をクリックします。  
「マルチキャスト情報」が表示されます。
5. 以下の項目を指定します。
  - マルチキャスト機能 → PIM-DM

■ マルチキャスト情報	
マルチキャスト機能	<input type="radio"/> 使用しない <input type="radio"/> static <input checked="" type="radio"/> PIM-DM <input type="radio"/> PIM-SM
TTLしきい値	<input type="text" value="1"/>
PIMプリファレンス値	<input type="text" value="1024"/>
上流ルータの種類	<input checked="" type="radio"/> PIMルータのみ <input type="radio"/> すべて

6. 【保存】 ボタンをクリックします。
7. 手順 1. ~ 6. を参考に、以下の項目を指定します。  
「LAN2 情報 (VLAN)」
  - マルチキャスト機能 → PIM-DM「LAN3 情報 (VLAN)」
  - マルチキャスト機能 → PIM-DM
8. 画面左側の【設定反映】 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2を設定する

---

「本装置1を設定する」を参考に、以下の項目を指定します。

### LAN1 情報を設定する

「LAN1 情報」 - 「IP 関連」

「マルチキャスト情報」

- マルチキャスト機能 → PIM-DM

### LAN2 情報を設定する

「LAN2 情報」 - 「IP 関連」

「マルチキャスト情報」

- マルチキャスト機能 → PIM-DM

## 本装置3を設定する

---

「本装置1を設定する」を参考に、以下の項目を指定します。

### LAN1 情報を設定する

「LAN1 情報」 - 「IP 関連」

「マルチキャスト情報」

- マルチキャスト機能 → PIM-DM

### LAN2 情報を設定する

「LAN2 情報」 - 「IP 関連」

「マルチキャスト情報」

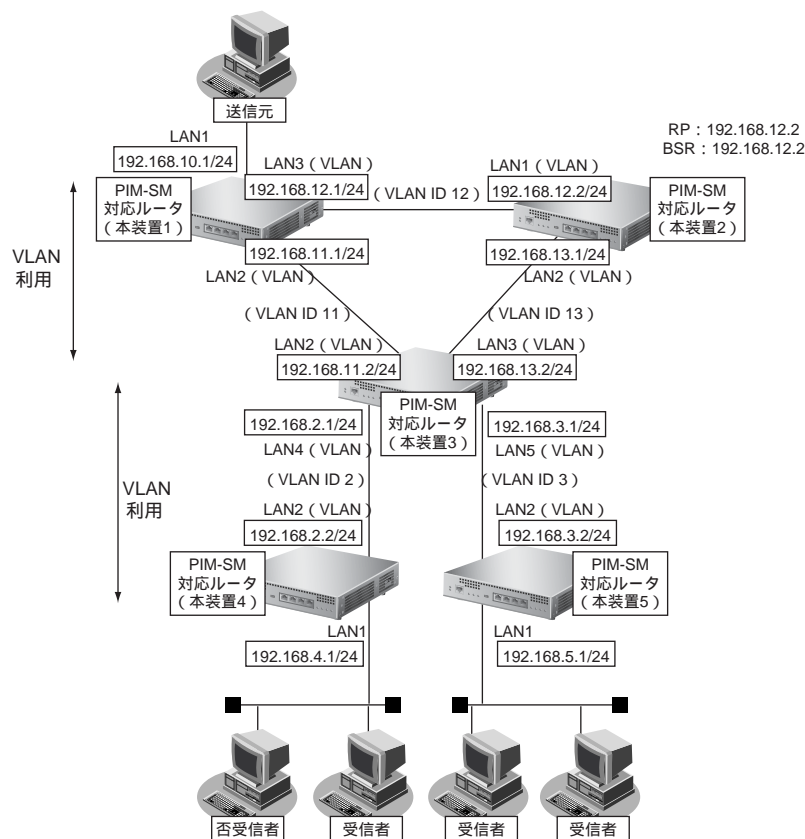
- マルチキャスト機能 → PIM-DM

## 2.10.2 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。



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。

ここでは、本装置1、本装置2、本装置3、本装置4、本装置5が以下のとおりに設定されていることを前提とします。

### ● 前提条件

- 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 : 2                                  ネットワークアドレス : 192.168.2.0/24  
VLAN ID : 3                                  ネットワークアドレス : 192.168.3.0/24  
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
- 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1】

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス                                  : 192.168.10.1/24
- LAN2のIPアドレス                                  : 192.168.11.1/24
- LAN3のIPアドレス                                  : 192.168.12.1/24

#### 【本装置2】

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN1、LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス                                  : 192.168.12.2/24
- LAN2のIPアドレス                                  : 192.168.13.1/24

#### 【本装置3】

- LAN0、LAN1はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2、LAN3はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN4、LAN5はVLANとし、出力先の物理インタフェースはLAN1とする
- LAN2のIPアドレス                                  : 192.168.11.2/24
- LAN3のIPアドレス                                  : 192.168.13.2/24
- LAN4のIPアドレス                                  : 192.168.2.1/24
- LAN5のIPアドレス                                  : 192.168.3.1/24

#### 【本装置4】

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス                                  : 192.168.4.1/24
- LAN2のIPアドレス                                  : 192.168.2.2/24

#### 【本装置5】

- LAN0はVLANの出力先としてだけ使用し、通常のLANとしては使用しない
- LAN2はVLANとし、出力先の物理インタフェースはLAN0とする
- LAN1のIPアドレス                                  : 192.168.5.1/24
- LAN2のIPアドレス                                  : 192.168.3.2/24

### ● 設定条件

- 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
- RP、BSRは本装置2が行う
- SPTへの切り替えを行う（初期値）

#### 【本装置1】

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2、LAN3を使用する

#### 【本装置2】

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する
- RP : 192.168.12.2
- BSR : 192.168.12.2

#### 【本装置3】

- マルチキャスト・パケットを転送するインタフェースとしてLAN2～5を使用する

#### 【本装置4】

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する

#### 【本装置5】

- マルチキャスト・パケットを転送するインタフェースとしてLAN1、LAN2を使用する

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置1を設定する

### 1. 設定メニューのルータ設定の「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

### 2. 「LAN情報」でインタフェースがLAN1の【修正】ボタンをクリックします。

「LAN1情報（物理LAN）」ページが表示されます。

### 3. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

### 4. IP関連の設定項目の「マルチキャスト情報」をクリックします。

「マルチキャスト情報」が表示されます。

### 5. 以下の項目を指定します。

- マルチキャスト機能 → PIM-SM

■ マルチキャスト情報	
マルチキャスト機能	<input type="radio"/> 使用しない <input type="radio"/> static <input type="radio"/> PIM-DM <input checked="" type="radio"/> PIM-SM
TTLしきい値	<input type="text" value="1"/>
PIMプリファレンス値	<input type="text" value="1024"/>
上流ルータの種類	<input checked="" type="radio"/> PIMルータのみ <input type="radio"/> すべて

### 6. 【保存】ボタンをクリックします。

## 7. 手順 1.～6. を参考に、以下の項目を指定します。

### 「LAN2 情報 (VLAN)」

- マルチキャスト機能 → PIM-SM

### 「LAN3 情報 (VLAN)」

- マルチキャスト機能 → PIM-SM

## 8. 画面左側の [設定反映] 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 2 を設定する

### 1. 「本装置 1 を設定する」を参考に、以下の項目を指定します。

#### 「LAN1 情報 (VLAN)」

- マルチキャスト機能 → PIM-SM

#### 「LAN2 情報 (VLAN)」

- マルチキャスト機能 → PIM-SM

### 2. 設定メニューのルータ設定の「マルチキャスト情報」をクリックします。

「マルチキャスト情報」ページが表示されます。

### 3. 「IP マルチキャスト情報」をクリックします。

「IP マルチキャスト情報」が表示されます。

### 4. 以下の項目を指定します。

- PIM-SM
  - RP 候補 → する
  - IP アドレス → 192.168.12.2
  - BSR 候補 → する
  - IP アドレス → 192.168.12.2

■ IP マルチキャスト情報		?
PIM-SM	RP 候補	<input type="radio"/> しない <input checked="" type="radio"/> する IP アドレス <input type="text" value="192.168.12.2"/> プライオリティ <input type="text" value="0"/>
	BSR 候補	<input type="radio"/> しない <input checked="" type="radio"/> する IP アドレス <input type="text" value="192.168.12.2"/> プライオリティ <input type="text" value="0"/>
	SPT への経路変更	<input type="radio"/> しない <input checked="" type="radio"/> 即時 <input type="radio"/> 転送速度 <input type="text"/> Kbps
register	チェックサム	<input checked="" type="radio"/> ヘッダ部 <input type="radio"/> パケット全体

### 5. [保存] ボタンをクリックします。

## 6. 画面左側の「設定反映」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3を設定する

---

「本装置1を設定する」を参考に、以下の項目を指定します。

#### 「LAN2 (VLAN) 情報」 - 「IP 関連」

##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM

#### 「LAN3 (VLAN) 情報」 - 「IP 関連」

##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM

#### 「LAN4 (VLAN) 情報」 - 「IP 関連」

##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM

#### 「LAN5 (VLAN) 情報」 - 「IP 関連」

##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM

### 本装置4を設定する

---

「本装置1を設定する」を参考に、以下の項目を指定します。

#### 「LAN1 (VLAN) 情報」 - 「IP 関連」

##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM

#### 「LAN2 (VLAN) 情報」 - 「IP 関連」

##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM

### 本装置5を設定する

---

「本装置1を設定する」を参考に、以下の項目を指定します。

#### 「LAN1 (VLAN) 情報」 - 「IP 関連」

##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM

#### 「LAN2 (VLAN) 情報」 - 「IP 関連」

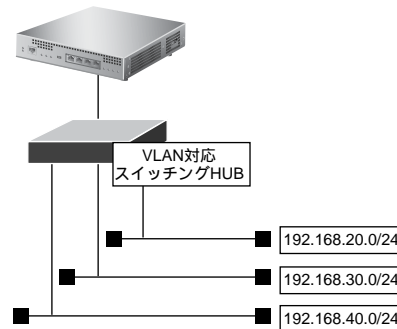
##### 「マルチキャスト情報」

- マルチキャスト機能 → PIM-SM



## 2.11 VLAN機能を使う

ここでは、VLAN機能を利用して、1つの物理ポートで3つのネットワークを組む場合を例に説明します。



参照 MR1000 機能説明書 [「2.10 VLAN機能」](#) (P.48)

### ● 設定条件

- LAN0ポートを使用する
- VLAN IDとして2、3、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 : 2                      ネットワークアドレス : 192.168.20.0/24  
VLAN ID : 3                      ネットワークアドレス : 192.168.30.0/24  
VLAN ID : 4                      ネットワークアドレス : 192.168.40.0/24

上記の設定条件に従って設定を行う場合の設定例を示します。

#### 1. 設定メニューのルータ設定の「LAN情報」をクリックします。

「LAN情報」ページが表示されます。

#### 2. 以下の項目を指定します。

- インタフェース                      → VLAN

<LAN情報追加フィールド>	
インタフェース	VLAN

#### 3. [追加] ボタンをクリックします。

「LAN1情報 (VLAN)」ページが表示されます。

#### 4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

## 5. 以下の項目を指定します。

- 出力先 → LAN0
- VLAN ID → 2
- プライオリティ → 0

■基本情報	
出力先	LAN0
VLAN ID	2
プライオリティ	0
VRRP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する パスワード <input type="text"/>
MTUサイズ	1500 バイト

## 6. [保存] ボタンをクリックします。

## 7. 「IP関連」をクリックします。

IP関連の設定項目と「IPアドレス情報」が表示されます。

## 8. 以下の項目を指定します。

- IPv4 → 使用する
- IPアドレス → 指定する
  - IPアドレス → 192.168.20.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス+オール1

■IPアドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない <input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する
IPアドレス	IPアドレス <input type="text" value="192.168.20.1"/>
	ネットマスク <input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス <input type="text" value="ネットワークアドレス+オール1"/>

## 9. [保存] ボタンをクリックします。

## 10. IP関連の設定項目の「RIP情報」をクリックします。

「RIP情報」が表示されます。

**11. 以下の項目を指定します。**

- RIP送信 → V1 で送信する
- RIP受信 → V1 で受信する
- メトリック値 → 0

RIP情報	
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	<input type="text" value="0"/>

**12. [保存] ボタンをクリックします。****13. 手順 1. ～ 12. を参考に、以下の項目を指定します。**

[192.168.30.0/24のネットワーク]

- インタフェース情報 → VLAN  
出力先 → lan0  
VLAN ID → 3  
プライオリティ → 0
- IPアドレス → 指定する  
IPアドレス → 192.168.30.1  
ネットマスク → 24 (255.255.255.0)  
ブロードキャストアドレス → ネットワークアドレス+オール1
- RIP送信 → V1 で送信する
- RIP受信 → V1 で受信する
- メトリック値 → 0

**14. 手順 1. ～ 12. を参考に、以下の項目を指定します。**

[192.168.40.0/24のネットワーク]

- インタフェース情報 → VLAN  
出力先 → lan0  
VLAN ID → 4  
プライオリティ → 0
- IPアドレス → 指定する  
IPアドレス → 192.168.40.1  
ネットマスク → 24 (255.255.255.0)  
ブロードキャストアドレス → ネットワークアドレス+オール1
- RIP送信 → V1 で送信する
- RIP受信 → V1 で受信する
- メトリック値 → 0

**15. 画面左側の [設定反映] 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。

---

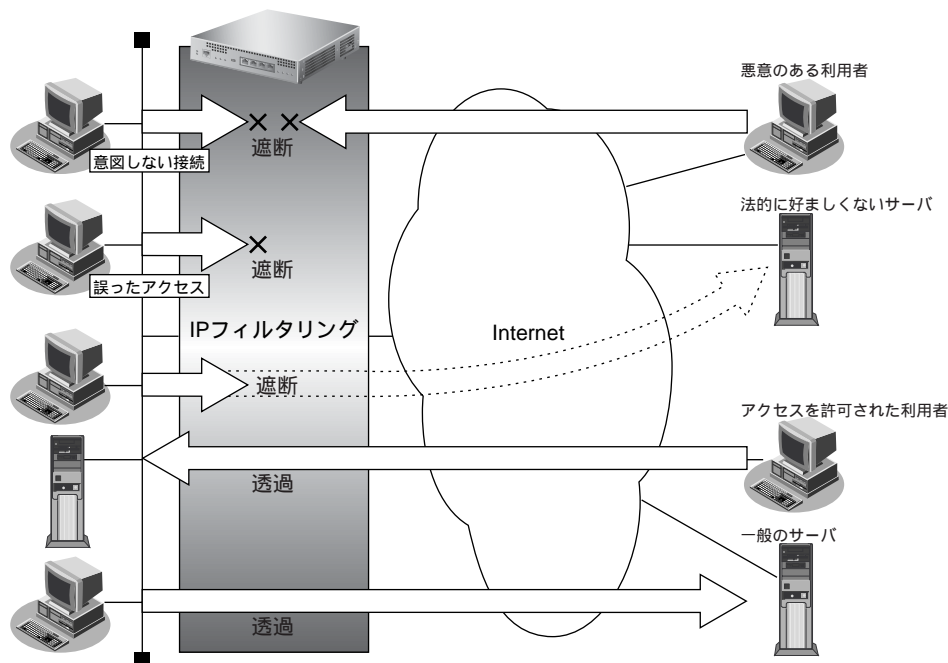
### こんな事に気をつけて

- VLAN 機能を利用すると、Ethernet フレームに 4 バイトの VLAN タグが付加され、最大 1522 バイトの Ethernet フレームが送出されることとなります。通常の Ethernet フレームの最大サイズは 1518 バイトです。そのため、その状態では 1522 バイトのフレームに対応していない機器とは接続することはできません。1522 バイトのフレームに対応していない機器と接続する場合は、VLAN インタフェースの MTU サイズを 1496 に変更してください。
  - VLAN インタフェース上では、シェーピング、帯域制御 (WFQ)、ホットスタンバイの機能を利用することはできません。
  - VLAN の物理インタフェースに、VLAN インタフェースを使用することはできません。
  - 同じ物理インタフェースを使用する複数の VLAN インタフェース上で、重複する VLAN ID を使用することはできません。
  - VLAN 対応スイッチング HUB やルータ製品の中には、VLAN が設定されていない LAN ポートで、VLAN タグ付きフレームを受信してしまう装置があります。  
このような装置と接続する際には、スイッチング HUB (またはルータ) の設定を「VLAN あり」から「VLAN なし」に設定を変更してください。  
また、フレームを送信する PC の arp エントリが本装置に残っていると、arp エントリの生存時間中だけ通信するという現象が発生する場合があります。これを防ぐために、設定後に本装置の [設定反映] ボタンをクリックしてください。
  - VLAN を利用する物理 LAN インタフェースの情報として、以下の手順で「ポート番号」と「転送レート」を必ず設定してください。「LAN 情報 (物理 LAN)」を設定しない場合、VLAN を利用する LAN 情報は設定できません。  
以下に手順を示します。
    1. 設定メニューのルータ設定で「LAN 情報」をクリックします。
    2. インタフェースに“物理インタフェース”を指定して、[追加] ボタンをクリックします。
    3. 「共通情報」 - 「基本情報」で、ポート番号と転送レートを選択して、[保存] ボタンをクリックします。
  - VLAN インタフェースを追加する場合は、先に物理 LAN インタフェースを設定してください。
-

## 2.12 IPフィルタリング機能を使う

☞ 参照 MR1000 機能説明書「2.11 IPフィルタリング機能」(P.49)

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。



### 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



### ◆ 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。

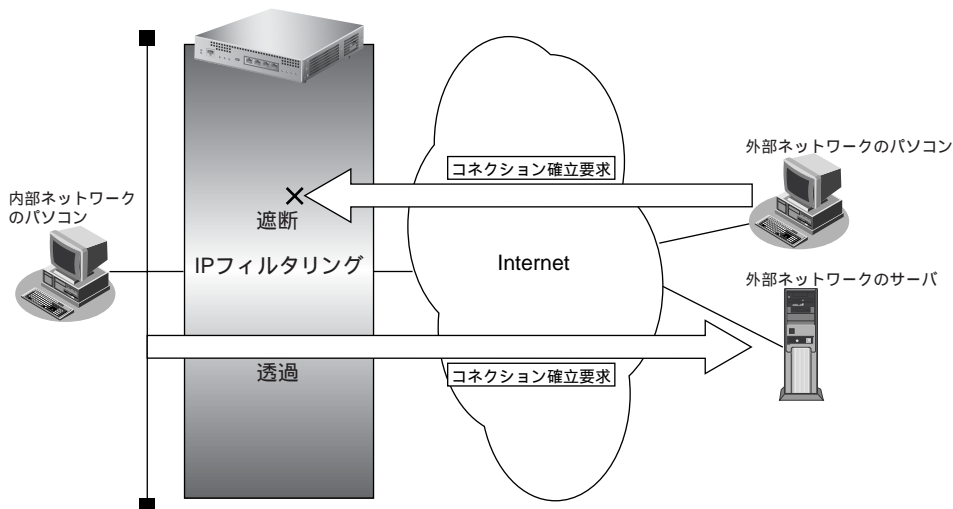
次に、TCP パケットとフラグ設定について説明します。TCPパケット内にはSYN フラグとACK フラグの2つの制御フラグがあります。このフラグの組み合わせによって、TCP パケットの内容が分かります。以下に、対応表を示します。

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です。

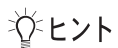
### ◆ IPフィルタリングの方向

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



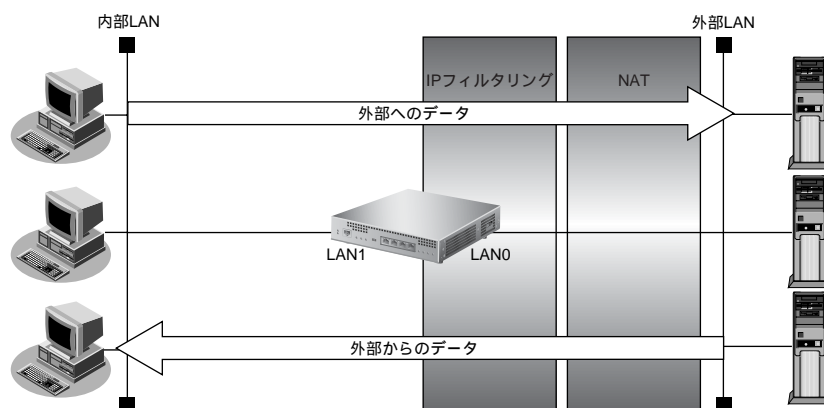
IPフィルタリング機能とNAT機能を併用する場合、回線切断時にNAT機能の情報が消えてしまうため、回線切断後に再度接続しても、サーバからの応答が正しくアドレス変換されず、IPフィルタリング機能によってパケットは破棄されてしまいます。



### ◆ 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 ブラウザから設定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
-



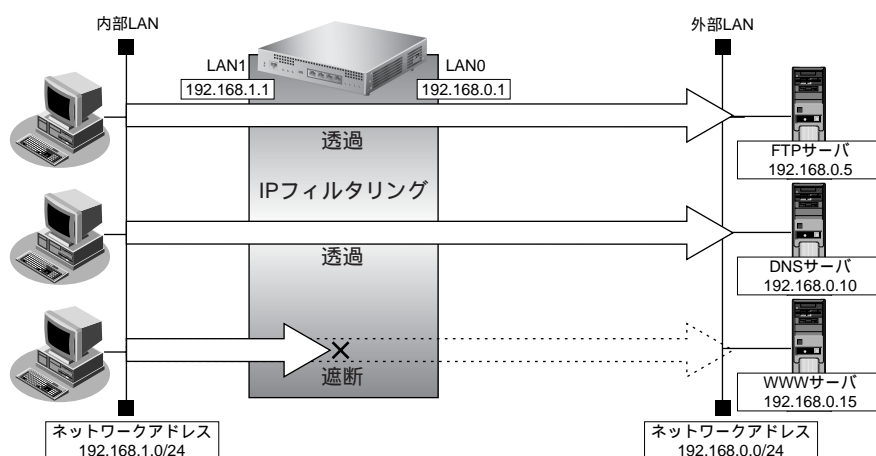
## 2.12.1 外部の特定サービスへのアクセスだけ許可する

### 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



このルールでは、ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

### 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 (内部 LAN → 外部 LAN)

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。  
「IP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 21 (ftpのポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
プロトコル	tcp <input type="text"/> (番号指定: <input type="text"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス <input type="text" value="192.168.1.0"/>
	アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ポート番号 <input type="text"/>
あて先情報	IPアドレス <input type="text"/>
	アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
	ポート番号 <input type="text" value="21"/>
ICMP	タイプ <input type="text"/>
	コード <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	<input type="text"/>
方向	<input type="text" value="入出力"/>

## 6. [追加] ボタンをクリックします。

## FTPサーバからの応答パケットを透過させる (外部 LAN → 内部 LAN)

### 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 21 (ftp のポート番号)
- あて先情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象外
- TOS → 指定しない
- 方向 → 入出力

## DNSサーバのポート 53 への UDP パケットを透過させる (内部 LAN → 外部 LAN)

### 8. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.0.10
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 53 (domain のポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## DNSサーバからの応答パケットを透過させる (外部 LAN → 内部 LAN)

### 9. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 192.168.0.10
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 53 (domainのポート番号)
- あて先情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## ICMPのパケットを透過させる

### 10. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → icmp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## 残りのパケットをすべて遮断する

### 11. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

### 12. 画面左側の「設定反映」ボタンをクリックします。

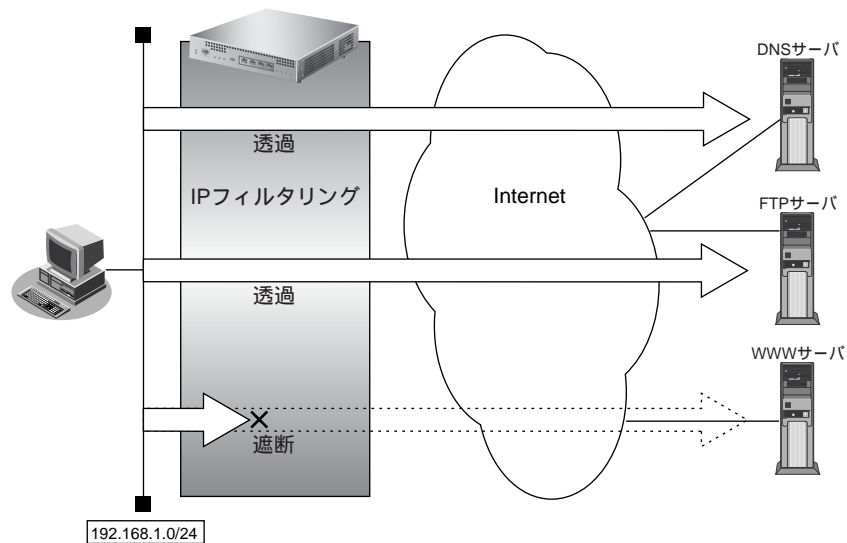
設定した内容が有効になります。

## 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



このルールでは ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

### 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 (LAN → インターネット)

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. フィルタリングを行うネットワーク情報の「修正」ボタンをクリックします。  
「ネットワーク情報」が表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。  
「IP フィルタリング情報」が表示されます。



## 5. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 21 (ftpのポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断
プロトコル	tcp <input type="button" value="▼"/> (番号指定: <input type="text"/> "その他"を選択時のみ有効です)
送信元情報	IPアドレス <input type="text" value="192.168.1.0"/>
	アドレスマスク <input type="text" value="24 (255.255.255.0)"/> <input type="button" value="▼"/>
	ポート番号 <input type="text"/>
あて先情報	IPアドレス <input type="text"/>
	アドレスマスク <input type="text" value="0 (0.0.0.0)"/> <input type="button" value="▼"/>
	ポート番号 <input type="text" value="21"/>
ICMP	タイプ <input type="text"/>
	コード <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	<input type="text"/>
方向	<input type="text" value="入出力"/> <input type="button" value="▼"/>

## 6. [追加] ボタンをクリックします。

## FTPサーバからの応答パケットを透過させる（インターネット→LAN）

### 7. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →tcp
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →21 (ftpのポート番号)
- あて先情報
  - IPアドレス →192.168.1.0
  - アドレスマスク →24 (255.255.255.0)
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象外
- TOS →指定しない
- 方向 →入出力

## DNSサーバのポート53へのUDPパケットを透過させる（LAN→インターネット）

### 8. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →udp
- 送信元情報
  - IPアドレス →192.168.1.0
  - アドレスマスク →24 (255.255.255.0)
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →192.168.0.10
  - アドレスマスク →32 (255.255.255.255)
  - ポート番号 →53 (domainのポート番号)
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

## DNSサーバからの応答パケットを透過させる (インターネット→LAN)

### 9. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →udp
- 送信元情報
  - IPアドレス →192.168.0.10
  - アドレスマスク →32 (255.255.255.255)
  - ポート番号 →53 (domainのポート番号)
- あて先情報
  - IPアドレス →192.168.1.0
  - アドレスマスク →24 (255.255.255.0)
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

## ICMPのパケットを透過させる

### 10. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →icmp
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

## 残りのパケットをすべて遮断する

### 11. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IP フィルタリング情報」

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IP アドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IP アドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

### 12. 画面左側の「設定反映」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。

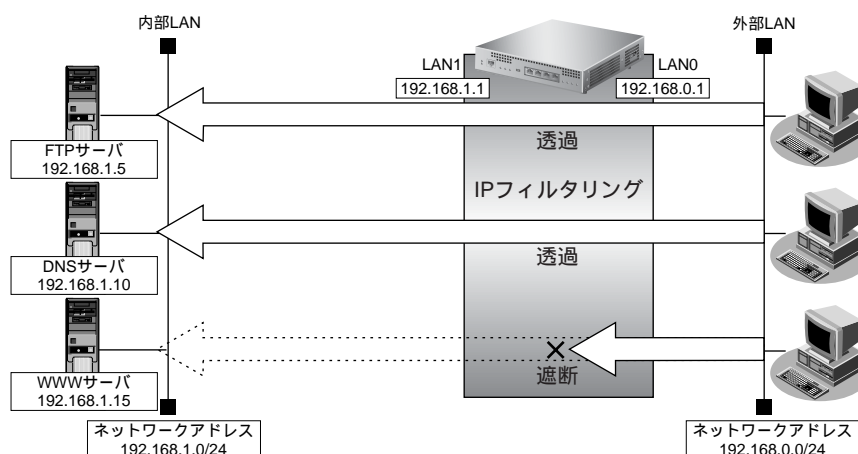
## 2.12.2 外部から特定サーバへのアクセスだけ許可する

### 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
- 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



このルールでは、ftp passive モードによるデータ転送はできません。

上記のフィルタリングルールの設定を行う場合の設定例を示します。

### 内部 LAN のホストのポート 21 への TCP パケットを透過させる (外部 LAN → 内部 LAN)

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。  
「IP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.5
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 21 (ftpのポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
プロトコル	tcp <input type="button" value="▼"/> (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)
送信元情報	IPアドレス 192.168.0.0
	アドレスマスク 24 (255.255.255.0) <input type="button" value="▼"/>
	ポート番号 <input type="text"/>
あて先情報	IPアドレス 192.168.1.5
	アドレスマスク 32 (255.255.255.255) <input type="button" value="▼"/>
	ポート番号 21
ICMP	タイプ <input type="text"/>
	コード <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	<input type="text"/>
方向	入出力 <input type="button" value="▼"/>

## 6. [追加] ボタンをクリックします。

## 内部 LAN のホストからの応答パケットを透過させる (内部 LAN → 外部 LAN)

### 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.5
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 21 (ftp のポート番号)
- あて先情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → なにも指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象外
- TOS → 指定しない
- 方向 → 入出力

## DNS サーバのポート 53 への UDP パケットを透過させる (外部 LAN → 内部 LAN)

### 8. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.10
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 53 (domain のポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力



## DNSサーバからの応答パケットを透過させる (内部 LAN → 外部 LAN)

### 9. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 192.168.1.10
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 53 (domainのポート番号)
- あて先情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

### ICMPのパケットを透過させる

### 10. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → icmp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## 残りのパケットをすべて遮断する

### 11. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

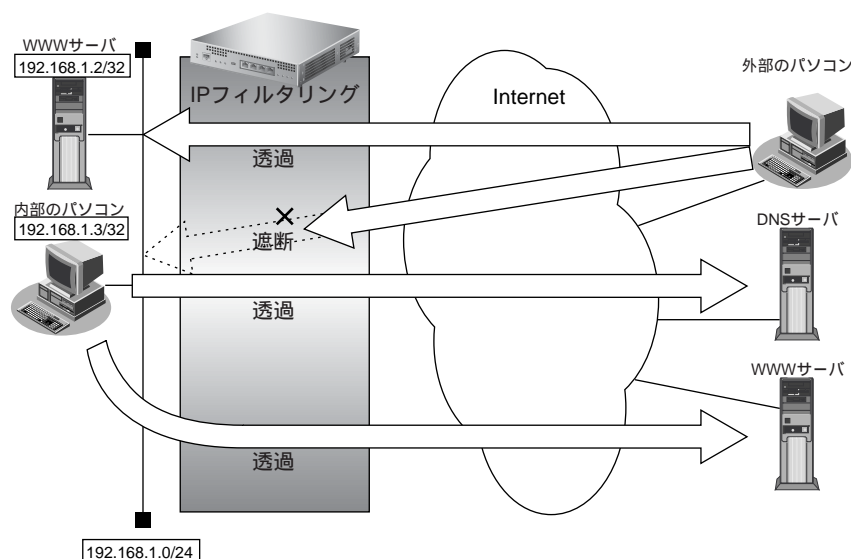
- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

### 12. 画面左側の「設定反映」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。

## 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付けません。



### ● 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の設定を行う場合の設定例を示します。

### LAN上のホストのポート80へのパケットを透過させる (インターネット→LAN)

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. フィルタリングを行うネットワーク情報の「修正」ボタンをクリックします。  
「ネットワーク情報」が表示されます。
3. 「IP関連」をクリックします。  
IP関連の設定項目と「IPアドレス情報」が表示されます。
4. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.2
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 80 (www-httpのポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断
プロトコル	tcp <input type="button" value="▼"/> <番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です>
送信元情報	IPアドレス <input type="text"/>
	アドレスマスク <input type="text" value="0 (0.0.0.0)"/> <input type="button" value="▼"/>
	ポート番号 <input type="text"/>
あて先情報	IPアドレス <input type="text" value="192.168.1.2"/>
	アドレスマスク <input type="text" value="32 (255.255.255.255)"/> <input type="button" value="▼"/>
	ポート番号 <input type="text" value="80"/>
ICMP	タイプ <input type="text"/>
	コード <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	<input type="text"/>
方向	<input type="text" value="入出力"/> <input type="button" value="▼"/>

## 6. [追加] ボタンをクリックします。

## LAN上のホストからの応答パケットを透過させる (LAN→インターネット)

### 7. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →tcp
- 送信元情報
  - IPアドレス →192.168.1.2
  - アドレスマスク →32
  - ポート番号 →80 (WWW-httpのポート番号)
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

## 任意のWWWサーバのポート80へのパケットを透過させる (LAN→インターネット)

### 8. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →tcp
- 送信元情報
  - IPアドレス →192.168.1.3
  - アドレスマスク →32
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →80 (WWW-httpのポート番号)
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

## 任意の WWW サーバからの応答パケットを透過させる (インターネット→LAN)

### 9. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 80 (www-http のポート番号)
- あて先情報
  - IPアドレス → 192.168.1.3
  - アドレスマスク → 32
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## DNS サーバのポート 53 への UDP パケットを透過させる (LAN→インターネット)

### 10. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 53 (domain のポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## DNSサーバからの応答パケットを透過させる (インターネット→LAN)

### 11. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →udp
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →53 (domainのポート番号)
- あて先情報
  - IPアドレス →192.168.1.0
  - アドレスマスク →24
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

### ICMPのパケットを透過させる

### 12. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →icmp
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力



## 残りのパケットをすべて遮断する

### 13. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

### 14. 画面左側の「設定反映」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。

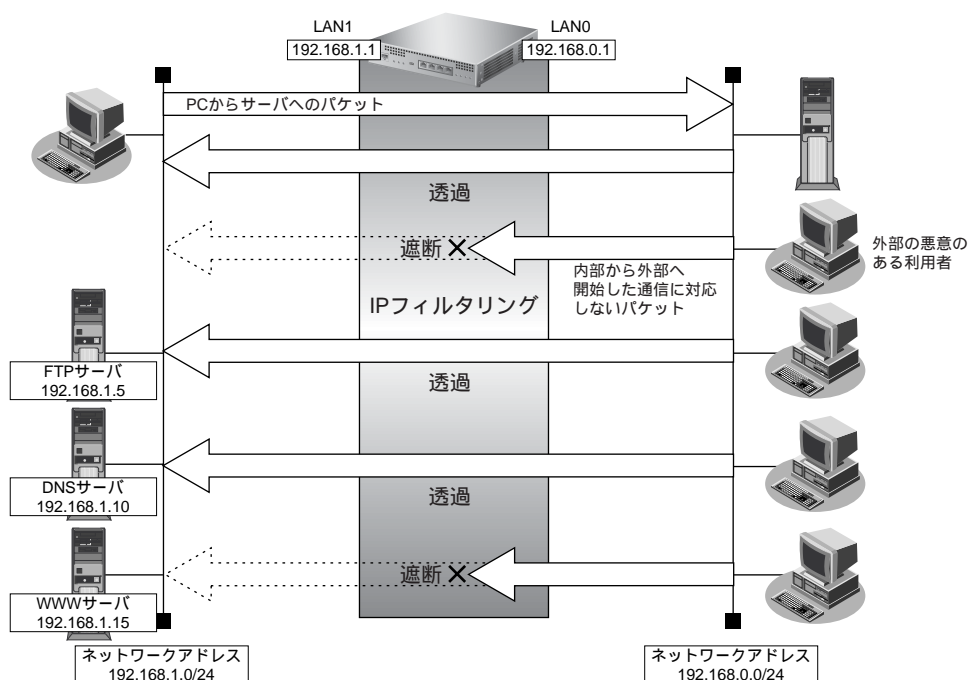
## 2.12.3 外部から特定サーバへのアクセスだけ許可してSPIを併用する

### 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
- 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の設定を行う場合の設定例を示します。

### 内部LANのホストのポート21へのTCPパケットを透過させる（外部LAN→内部LAN）

1. 設定メニューのルータ設定で「LAN情報」をクリックします。  
「LAN情報」ページが表示されます。
2. 「LAN情報」でインタフェースがLAN0の「修正」ボタンをクリックします。  
「LAN0情報（物理LAN）」ページが表示されます。
3. 「IP関連」をクリックします。  
IP関連の設定項目と「IPアドレス情報」が表示されます。
4. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.5
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 21 (ftpのポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
プロトコル	tcp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス: 192.168.0.0
	アドレスマスク: 24 (255.255.255.0)
	ポート番号:
あて先情報	IPアドレス: 192.168.1.5
	アドレスマスク: 32 (255.255.255.255)
	ポート番号: 21
ICMP	タイプ:
	コード:
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	
方向	入出力

## 6. [追加] ボタンをクリックします。

## 内部 LAN のホストからの応答パケットを透過させる (内部 LAN → 外部 LAN)

### 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.5
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 21 (ftp のポート番号)
- あて先情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → なにも指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象外
- TOS → 指定しない
- 方向 → 入出力

## DNS サーバのポート 53 への UDP パケットを透過させる (外部 LAN → 内部 LAN)

### 8. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.10
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 53 (domain のポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## DNSサーバからの応答パケットを透過させる (内部 LAN → 外部 LAN)

### 9. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 192.168.1.10
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 53 (domainのポート番号)
- あて先情報
  - IPアドレス → 192.168.0.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## ICMPのパケットを透過させる

### 10. 手順 5. ～ 6. を参考に、以下の項目を指定します。

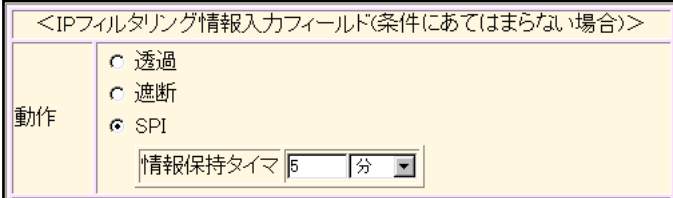
「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → icmp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## 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

11. 条件にあてはまらない場合の [修正] ボタンをクリックします。  
「IPフィルタリング情報」(条件にあてはまらない場合)が表示されます。
12. 以下の項目を指定します。

- 動作 → SPI

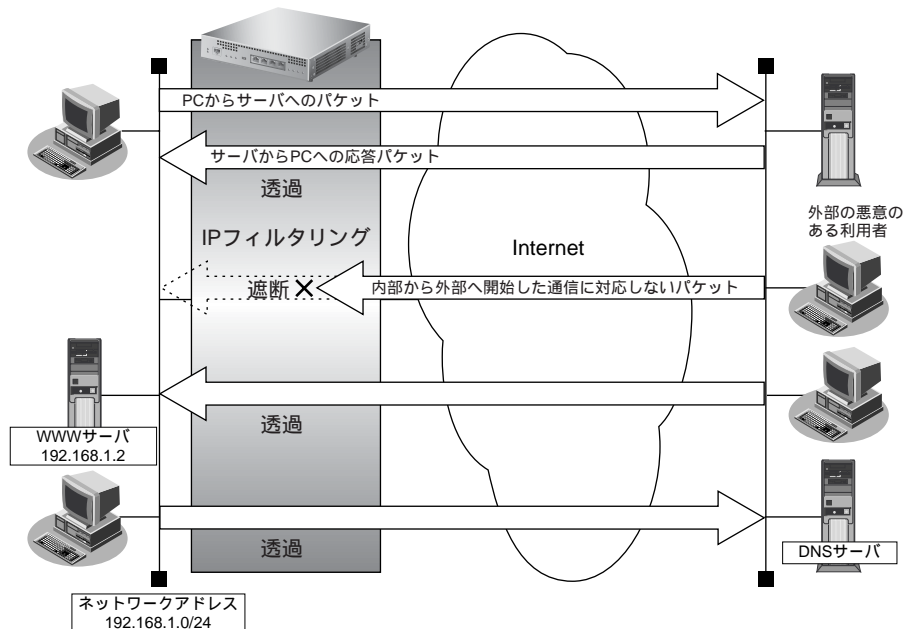


The screenshot shows a configuration window titled "<IPフィルタリング情報入力フィールド(条件にあてはまらない場合)>". It contains a section labeled "動作" (Action) with three radio button options: "透過" (Pass), "遮断" (Block), and "SPI" (Selected). Below the radio buttons is a field for "情報保持タイム" (Information Retention Time) set to "5" minutes.

13. [保存] ボタンをクリックします。
14. 画面左側の [設定反映] 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。

## 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の設定を行う場合の設定例を示します。

## LAN上のホストのポート80へのパケットを透過させる（インターネット→LAN）

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。



**2. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**3. フィルタリングを設定するネットワークの欄の【修正】ボタンをクリックします。**

「ネットワーク情報」ページが表示されます。

**4. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**5. IP関連の設定項目の「IPフィルタリング情報」をクリックします。**

「IPフィルタリング情報」が表示されます。

**6. 以下の項目を指定します。**

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.2
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 80 (www-httpのポート番号)
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

＜IPフィルタリング情報入力フィールド＞		
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断	
プロトコル	tcp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	<input type="text"/>
	アドレスマスク	0 (0.0.0.0)
	ポート番号	<input type="text"/>
あて先情報	IPアドレス	192.168.1.2
	アドレスマスク	32 (255.255.255.255)
	ポート番号	80
ICMP	タイプ	<input type="text"/>
	コード	<input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	
TOS	<input type="text"/>	
方向	入出力	

**7. 【追加】ボタンをクリックします。**

## LAN上のホストからの応答パケットを透過させる (LAN→インターネット)

### 8. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →tcp
- 送信元情報
  - IPアドレス →192.168.1.2
  - アドレスマスク →32 (255.255.255.255)
  - ポート番号 →80 (www-httpのポート番号)
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象外
- TOS →指定しない
- 方向 →入出力

### ICMPのパケットを透過させる

### 9. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →透過
- プロトコル →icmp
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

## 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

10. 条件にあてはまらない場合の [修正] ボタンをクリックします。  
「IPフィルタリング情報」(条件にあてはまらない場合)が表示されます。
11. 以下の項目を指定します。

- 動作 → SPI

<IPフィルタリング情報入力フィールド(条件にあてはまらない場合)>

動作

- 透過
- 透過(接続中のみ)
- 遮断
- SPI

情報保持タイム 5 分

12. [保存] ボタンをクリックします。
13. 画面左側の [設定反映] 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。

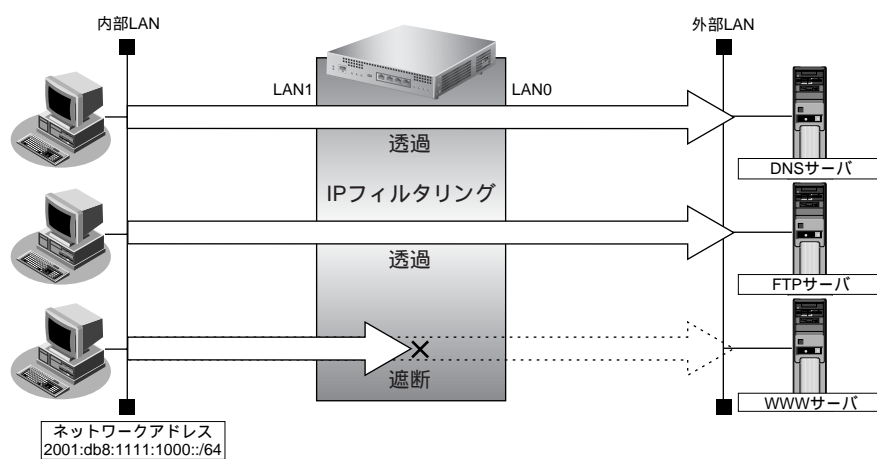
## 2.12.4 外部の特定サービスへのアクセスだけ許可する (IPv6 フィルタリング)

### 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の設定を行う場合の設定例を示します。

### FTP サーバのポート 21 (ftp) への TCP パケットを透過させる (内部 LAN → 外部 LAN)

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の【修正】 ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 フィルタリング情報」をクリックします。  
「IPv6 フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPv6 アドレス/プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- あて先情報
  - IPv6 アドレス/プレフィックス長 → 指定しない
  - ポート番号 → 21 (ftp のポート番号)
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象

＜IPv6フィルタリング情報入力フィールド＞	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
プロトコル	tcp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)
送信元情報	IPv6 アドレス / プレフィックス長: 2001:db8:1111:1000:: / 64
	ポート番号: <input type="text"/>
あて先情報	IPv6 アドレス / プレフィックス長: <input type="text"/> / <input type="text"/>
	ポート番号: 21
ICMPv6	タイプ: <input type="text"/>
	コード: <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
Traffic Class	<input type="text"/>
方向	入力のみ

## 6. [追加] ボタンをクリックします。

FTPサーバからの応答パケットを透過させる (外部 LAN → 内部 LAN)

## 7. 手順 5. ~ 6. を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPv6 アドレス/プレフィックス長 → 指定しない
  - ポート番号 → 21
- あて先情報
  - IPv6 アドレス/プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象外

## DNSサーバのポート53へのUDPパケットを透過させる (内部 LAN → 外部 LAN)

### 8. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPv6 アドレス/プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- あて先情報
  - IPv6 アドレス/プレフィックス長 → 指定しない
  - ポート番号 → 53
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象

## DNSサーバからの応答パケットを透過させる (外部 LAN → 内部 LAN)

### 9. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPv6 アドレス/プレフィックス長 → 指定しない
  - ポート番号 → 53
- あて先情報
  - IPv6 アドレス/プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象

## ICMPv6のパケットを透過させる

### 10. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 →透過
- プロトコル → icmpv6
- 送信元情報
  - IPv6 アドレス/プレフィックス長 →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPv6 アドレス/プレフィックス長 →指定しない
  - ポート番号 →指定しない
- ICMPv6
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象

### 残りのパケットをすべて遮断する

### 11. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPv6 アドレス/プレフィックス長 →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPv6 アドレス/プレフィックス長 →指定しない
  - ポート番号 →指定しない
- ICMPv6
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象

### 12. 画面左側の【設定反映】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。

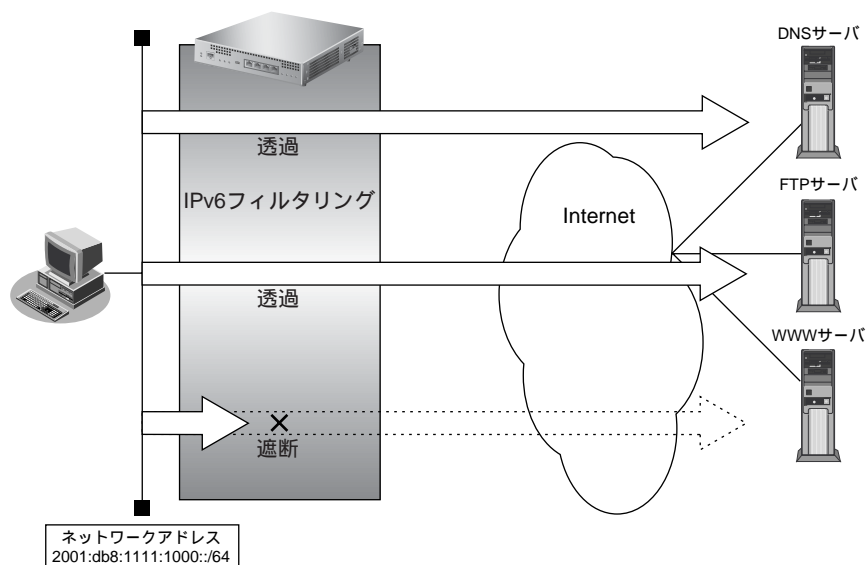


## リモート定義の場合

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の設定を行う場合の設定例を示します。

### 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 (LAN→イントラネット)

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. フィルタリングを行うネットワーク情報の「修正」ボタンをクリックします。  
「ネットワーク情報」が表示されます。
3. 「IPv6 関連」をクリックします。  
IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。
4. IPv6 関連の設定項目の「IPv6 フィルタリング情報」をクリックします。  
「IPv6 フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPv6 アドレス／プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- あて先情報
  - IPv6 アドレス／プレフィックス長 → 指定しない
  - ポート番号 → 21 (ftp のポート番号)
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象

＜IPv6フィルタリング情報入力フィールド＞	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断
プロトコル	tcp (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)
送信元情報	IPv6アドレス／プレフィックス長: 2001:db8:1111:1000:: / 64
	ポート番号: <input type="text"/>
あて先情報	IPv6アドレス／プレフィックス長: <input type="text"/> / <input type="checkbox"/>
	ポート番号: 21
ICMPv6	タイプ: <input type="text"/>
	コード: <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
Traffic Class	<input type="text"/>
方向	入力のみ

## 6. [追加] ボタンをクリックします。

### FTPサーバからの応答パケットを透過させる (イントラネット→LAN)

## 7. 手順 5. ～ 6. を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPv6 アドレス／プレフィックス長 → 指定しない
  - ポート番号 → 21 (ftp のポート番号)
- あて先情報
  - IPv6 アドレス／プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象

## DNSサーバのポート53へのUDPパケットを透過させる (LAN→イントラネット)

### 8. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPv6 アドレス／プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- あて先情報
  - IPv6 アドレス／プレフィックス長 → 指定しない
  - ポート番号 → 53 (domain のポート番号)
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象

## DNSサーバからの応答パケットを透過させる (イントラネット→LAN)

### 9. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPv6 アドレス／プレフィックス長 → 指定しない
  - ポート番号 → 53 (domain のポート番号)
- あて先情報
  - IPv6 アドレス／プレフィックス長 → 2001:db8:1111:1000::/64
  - ポート番号 → 指定しない
- ICMPv6
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象

## ICMPv6のパケットを透過させる

### 10. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 →透過
- プロトコル → icmpv6
- 送信元情報
  - IPv6 アドレス／プレフィックス長 →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPv6 アドレス／プレフィックス長 →指定しない
  - ポート番号 →指定しない
- ICMPv6
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象

### 残りのパケットをすべて遮断する

### 11. 手順5.～6.を参考に、以下の項目を指定します。

「IPv6フィルタリング情報」

- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPv6 アドレス／プレフィックス長 →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPv6 アドレス／プレフィックス長 →指定しない
  - ポート番号 →指定しない
- ICMPv6
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象

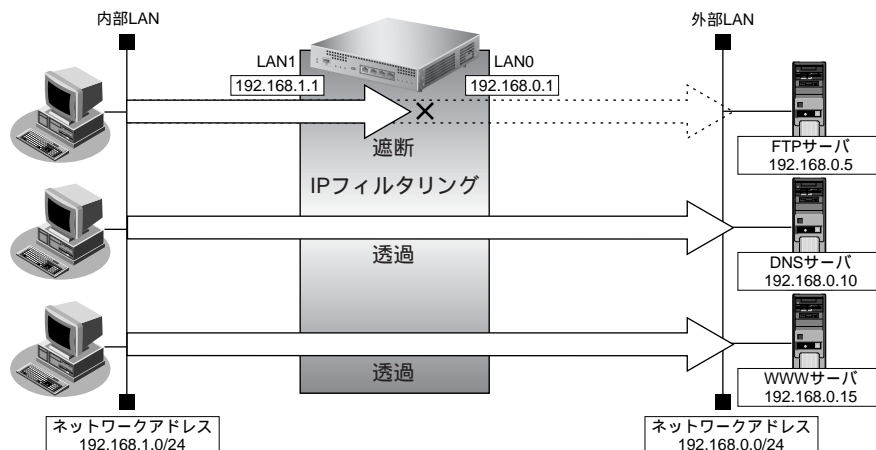
### 12. 画面左側の【設定反映】ボタンをクリックします。

設定した内容が有効になります。

## 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。



#### ● フィルタリング設定

- 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の設定を行う場合の設定例を示します。

### FTP サーバ (192.168.0.5) への TCP パケットを遮断する (内部 LAN → 外部 LAN)

#### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

#### 2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

#### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

#### 4. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。

「IP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 遮断
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.0.5
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 21
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
プロトコル	tcp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス 192.168.1.0
	アドレスマスク 24 (255.255.255.0)
	ポート番号
あて先情報	IPアドレス 192.168.0.5
	アドレスマスク 32 (255.255.255.255)
	ポート番号 21
ICMP	タイプ
	コード
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	
方向	入出力

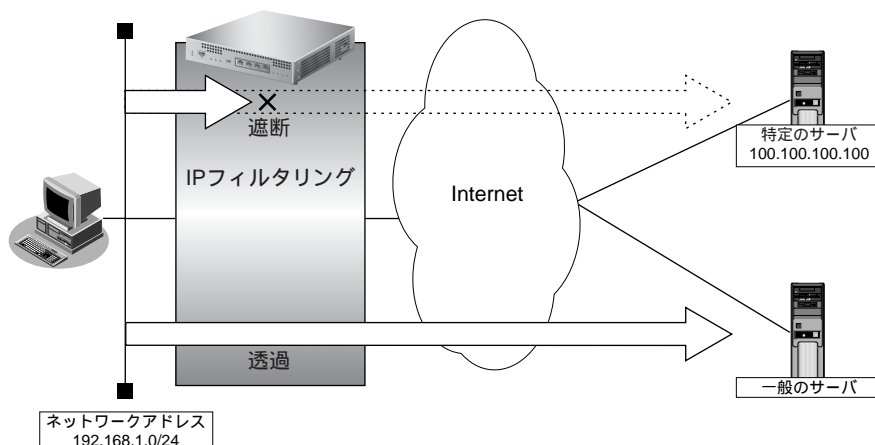
## 6. [追加] ボタンをクリックします。

## 7. 画面左側の [設定反映] 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。

## 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の設定を行う場合の設定例を示します。

### アドレス（100.100.100.100）へのすべてのパケットを遮断する（LAN→インターネット）

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. フィルタリングを設定するネットワークの欄の【修正】ボタンをクリックします。  
「ネットワーク情報」ページが表示されます。
4. 「IP関連」をクリックします。  
IP関連の設定項目と「IP基本情報」が表示されます。
5. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。



## 6. 以下の項目を指定します。

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 100.100.100.100
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input checked="" type="radio"/> 遮断
プロトコル	すべて <input type="button" value="▼"/> (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)
送信元情報	IPアドレス 192.168.1.0
	アドレスマスク 24 (255.255.255.0) <input type="button" value="▼"/>
	ポート番号 <input type="text"/>
あて先情報	IPアドレス 100.100.100.100
	アドレスマスク 32 (255.255.255.255) <input type="button" value="▼"/>
	ポート番号 <input type="text"/>
ICMP	タイプ <input type="text"/>
	コード <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	<input type="text"/>
方向	入出力 <input type="button" value="▼"/>

## 7. [追加] ボタンをクリックします。

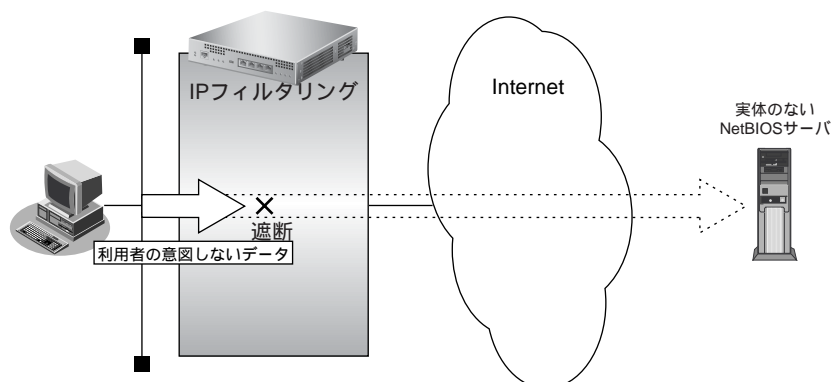
## 8. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

## 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<sup>®</sup>（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の設定を行う場合の設定例を示します。

### ポート137～139へのすべてのパケットを遮断する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. フィルタリングを行うネットワーク情報の【修正】ボタンをクリックします。  
「ネットワーク情報」が表示されます。
3. 「IP関連」をクリックします。  
IP関連の設定項目と「IPアドレス情報」が表示されます。
4. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 137-139
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input checked="" type="radio"/> 遮断
プロトコル	すべて <input type="button" value="▼"/> (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス <input type="text"/>
	アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
	ポート番号 <input type="text"/>
あて先情報	IPアドレス <input type="text"/>
	アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
	ポート番号 <input type="text" value="137-139"/>
ICMP	タイプ <input type="text"/>
	コード <input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	<input type="text"/>
方向	<input type="button" value="▼"/> 入出力

## 6. [追加] ボタンをクリックします。

## ポート 137～139 からのすべてのパケットを遮断する

### 7. 手順 5.～6. を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →137-139
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

### 8. 画面左側の [設定反映] ボタンをクリックします。

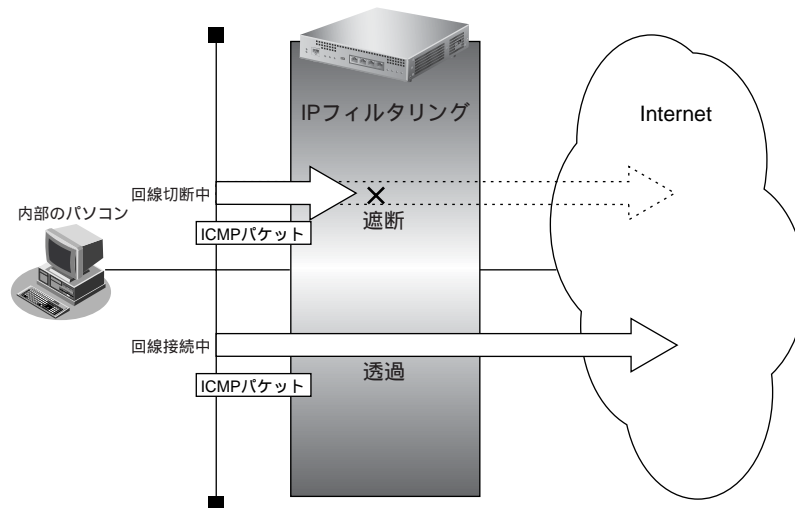
設定した内容が有効になります。

## 2.12.7 回線が接続しているときだけ許可する

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またはISDN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の設定を行う場合の設定例を示します。

### 回線が接続しているときだけICMPパケットを透過させる

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. フィルタリングを行うネットワーク情報の「修正」ボタンをクリックします。  
「ネットワーク情報」が表示されます。
3. 「IP関連」をクリックします。  
IP関連の設定項目と「IPアドレス情報」が表示されます。
4. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 透過 (接続中のみ)
- プロトコル → icmp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>		
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断	
プロトコル	icmp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	
あて先情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	
ICMP	タイプ	
	コード	
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	
TOS		
方向	入出力	

## 6. [追加] ボタンをクリックします。

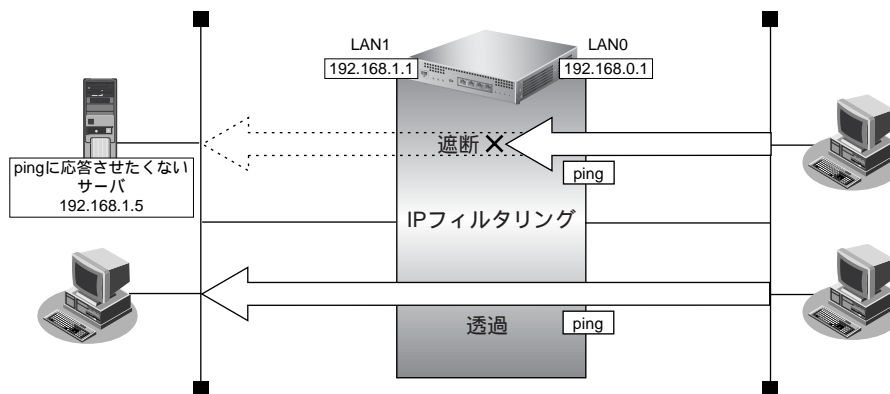
## 7. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

## 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。



#### ● フィルタリング設定

- 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の設定を行う場合の設定例を示します。

### 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(外部LAN→内部LAN)

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「IP フィルタリング情報」をクリックします。  
「IP フィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 遮断
- プロトコル → ICMP
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.5
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 8
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>		
動作	<input type="radio"/> 透過 <input checked="" type="radio"/> 遮断	
プロトコル	icmp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	
あて先情報	IPアドレス	192.168.1.5
	アドレスマスク	32 (255.255.255.255)
	ポート番号	
ICMP	タイプ	8
	コード	
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	
TOS		
方向	入出力	

## 6. [追加] ボタンをクリックします。



## 残りのパケットをすべて透過させる

### 7. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

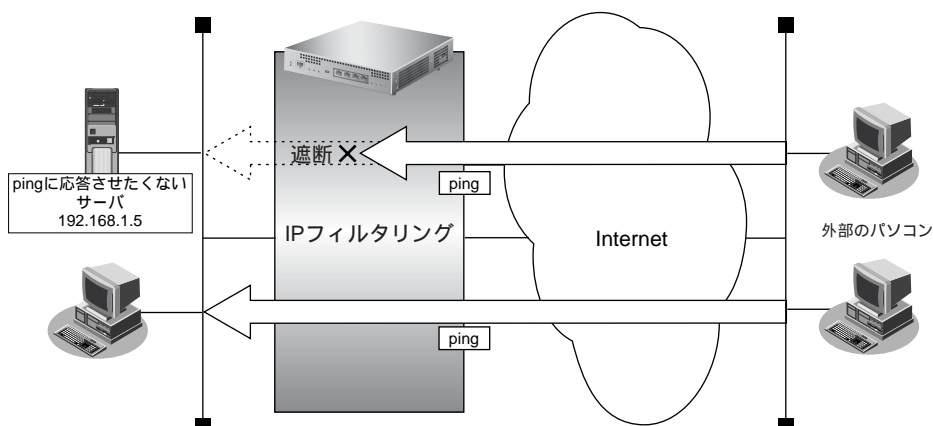
- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

### 8. 画面左側の【設定反映】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。

## 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

### 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(インターネット→LAN)

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. フィルタリングを行うネットワーク情報の【修正】ボタンをクリックします。  
「ネットワーク情報」が表示されます。
3. 「IP関連」をクリックします。  
IP関連の設定項目と「IPアドレス情報」が表示されます。
4. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。

## 5. 以下の項目を指定します。

- 動作 → 遮断
- プロトコル → icmp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.1.5
  - アドレスマスク → 32
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 8
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>		
動作	<input type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input checked="" type="radio"/> 遮断	
プロトコル	icmp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	<input type="text"/>
	アドレスマスク	0 (0.0.0.0)
	ポート番号	<input type="text"/>
あて先情報	IPアドレス	192.168.1.5
	アドレスマスク	32 (255.255.255.255)
	ポート番号	<input type="text"/>
ICMP	タイプ	8
	コード	<input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	
TOS	<input type="text"/>	
方向	入出力	

## 6. [追加] ボタンをクリックします。

## 残りのパケットをすべて透過させる

### 7. 手順5.～6.を参考に、以下の項目を指定します。

「IPフィルタリング情報」

- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

### 8. 画面左側の【設定反映】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。

## 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。

- 固定 IP アドレスでの VPN (手動鍵交換)  
固定 IP アドレスで送信元、送信先の IP アドレス範囲を指定して 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。
- 固定 IP アドレスでの VPN (自動鍵交換)  
固定 IP アドレスで送信元、送信先の IP アドレス範囲を指定して VPN 通信を行います。  
認証情報、暗号情報の鍵は自動で交換します。
- 可変 IP アドレスでの VPN (自動鍵交換)  
自側の IP アドレスが動的に割り当てられる環境で、経路情報 (送信先の IP アドレス) に従って VPN 通信を行います。認証情報、暗号情報の鍵は自動で交換します。
- 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)  
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で交換します。
- 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説明します。

☞ 参照 MR1000 機能説明書 [2.13 IPsec機能] (P.58)

### こんな事に気をつけて

- IPsec 機能は 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「ネットワーク情報」で設定します。IPsec 後に変換する場合は、回線接続用の「ネットワーク情報」または「LAN 情報」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 機能では、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 機能と 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 機能とマルチ NAT を併用する場合は、静的 NAT の設定が必要となる場合があります。
- ルーティングを設定する場合、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。
- AES 暗号アルゴリズムは、128 ビット鍵長だけをサポートしています。他機種と接続する際には、128 ビット鍵長を選択してください。



### ◆ 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。

### ◆ 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、「LAN 情報」または「ネットワーク情報」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)	<p>ESP パケットの受信を設定します。</p> <ul style="list-style-type: none"> <li>・プライベートIP 情報               <ul style="list-style-type: none"> <li>IP アドレス 自側エンドポイントに設定したアドレス</li> <li>ポート番号 すべて</li> </ul> </li> <li>・グローバルIP 情報               <ul style="list-style-type: none"> <li>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</li> <li>ポート番号 すべて</li> </ul> </li> <li>・プロトコル ESP</li> </ul>
固定IPアドレスでのVPN (自動鍵交換)	<p>IKE パケットの受信を設定します。</p> <ul style="list-style-type: none"> <li>・プライベートIP 情報               <ul style="list-style-type: none"> <li>IP アドレス 自側エンドポイントに設定したアドレス</li> <li>ポート番号 500</li> </ul> </li> <li>・グローバルIP 情報               <ul style="list-style-type: none"> <li>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</li> <li>ポート番号 500</li> </ul> </li> <li>・プロトコル UDP</li> </ul> <p>ESP パケットの受信を設定します。</p> <ul style="list-style-type: none"> <li>・プライベートIP 情報               <ul style="list-style-type: none"> <li>IP アドレス 自側エンドポイントに設定したアドレス</li> <li>ポート番号 すべて</li> </ul> </li> <li>・グローバルIP 情報               <ul style="list-style-type: none"> <li>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</li> <li>ポート番号 すべて</li> </ul> </li> <li>・プロトコル ESP</li> </ul> <p>例)</p> <p>本装置の WAN (ネットワーク情報) の自側 IP アドレスが 202.168.1.66 (固定) であり、と 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 IP アドレスおよびグローバル IP アドレスには、202.16.1.66 を設定します。</p>
可変IPアドレスでのVPN (Initiator)	<p>IKE パケットの受信を設定します。</p> <ul style="list-style-type: none"> <li>・プライベートIP 情報               <ul style="list-style-type: none"> <li>IP アドレス 本装置の LAN 側 IP アドレス</li> <li>ポート番号 500</li> </ul> </li> <li>・グローバルIP 情報               <ul style="list-style-type: none"> <li>IP アドレス 指定しない</li> <li>ポート番号 500</li> </ul> </li> <li>・プロトコル UDP</li> </ul>

利用形態	設定内容
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。 <ul style="list-style-type: none"><li>• プライベートIP情報<ul style="list-style-type: none"><li>IPアドレス 本装置のLAN側IPアドレス</li><li>ポート番号 すべて</li></ul></li><li>• グローバルIP情報<ul style="list-style-type: none"><li>IPアドレス 指定しない</li><li>ポート番号 すべて</li></ul></li><li>• プロトコル ESP</li></ul>

## 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。

ここでは以下の条件によって、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 LANポート : LAN0 ポート使用

#### 【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

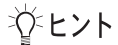
#### 【支社】

- 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。

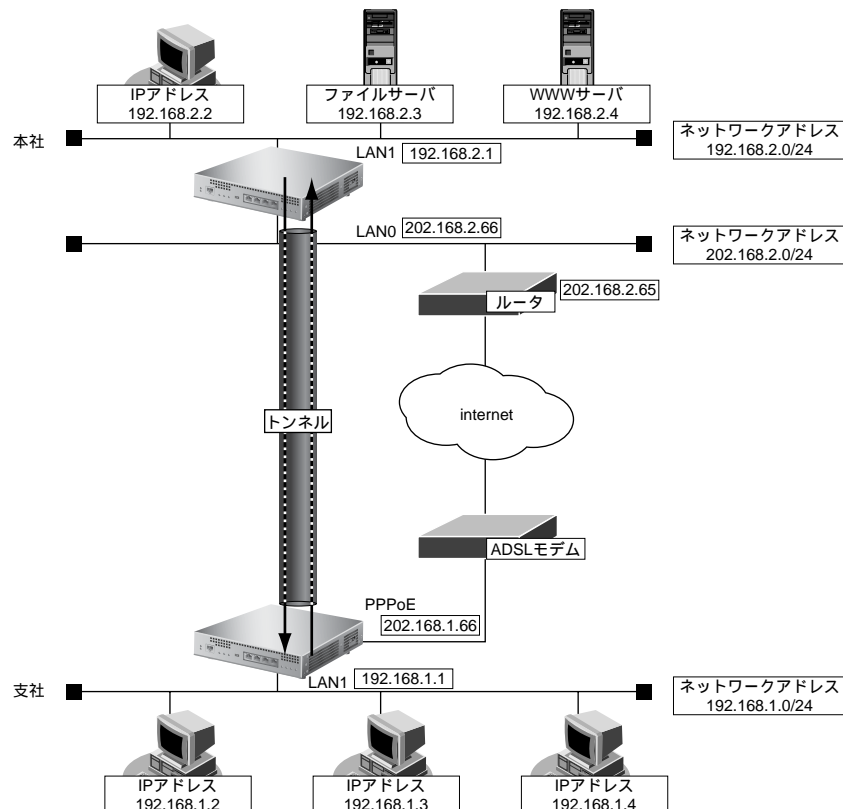
0101 0101 0101 0101、1F1F 1F1F E0E0 E0E0、E0E0 E0E0 1F1F 1F1F、FEFE FEFE FEFE FEFE  
01FE 01FE 01FE 01FE、1FE0 1FE0 0EF1 0EF1、01E0 01E0 01F1 01F1、FE01 FE01 FE01 FE01、  
E01F E01F F10E F10E、E001 E001 F101 F101、1FFE 1FFE 0EFE 0EFE、011F 011F 010E 010E、  
E0FE E0FE F1FE F1FE、FE1F FE1F FE0E FE0E、1F01 1F01 0E01 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設定例を示します。

## 支社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	<input type="text" value="honsya"/>
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インタフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**12. 以下の項目を指定します。**

- 鍵交換モード → 手動鍵使用
- 相手側エンドポイント → 202.168.2.66
- 自側エンドポイント → 202.168.1.66

鍵交換モード	<input checked="" type="radio"/> 手動鍵使用
	相手側エンドポイント <input type="text" value="202.168.2.66"/>
	自側エンドポイント <input type="text" value="202.168.1.66"/>

**13. [保存] ボタンをクリックします。****14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- SAの設定 (送信用)
  - SPI値 → 100
  - 暗号アルゴリズム → des-cbc
  - 暗号鍵
  - 鍵識別 → 16進数
  - 鍵 → 0123456789
  - 認証アルゴリズム → hmac-md5
  - 認証鍵
  - 鍵識別 → 16進数
  - 鍵 → 123456789a
- SAの設定 (受信用)
  - SPI値 → 101
  - 暗号アルゴリズム → des-cbc
  - 暗号鍵
  - 鍵識別 → 16進数
  - 鍵 → 23456789ab
  - 認証アルゴリズム → hmac-md5
  - 認証鍵
  - 鍵識別 → 16進数
  - 鍵 → 3456789abc

■ IPsec情報(手動鍵)			
対象バケット (送信用)	自側IPアドレス	<input type="text"/>	
	自側アドレスマスク	0 (0.0.0.0)	
	相手側IPアドレス	<input type="text"/>	
	相手側アドレスマスク	0 (0.0.0.0)	
SAの設定 (送信用)	SPI値	100 (16進数)	
	暗号アルゴリズム	des-cbc	
	暗号鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	*****
	認証アルゴリズム	hmac-md5	
	認証鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
鍵		*****	
対象バケット (受信用)	相手側IPアドレス	<input type="text"/>	
	相手側アドレスマスク	0 (0.0.0.0)	
	自側IPアドレス	<input type="text"/>	
	自側アドレスマスク	0 (0.0.0.0)	
SAの設定 (受信用)	SPI値	101 (16進数)	
	暗号アルゴリズム	des-cbc	
	暗号鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	*****
	認証アルゴリズム	hmac-md5	
	認証鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
鍵		*****	

## 16. [保存] ボタンをクリックします。

## 17. 画面左側の [設定反映] 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。

## 本社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	shisya
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 <div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 2px;">ダイヤル1</div> <div style="border: 1px solid black; padding: 2px;">電話番号</div> </div> <div style="display: flex; justify-content: space-between;"> <div style="border: 1px solid black; padding: 2px;"></div> <div style="border: 1px solid black; padding: 2px;">サブアドレス</div> </div>
	<input type="radio"/> フレームリレー接続 <input type="radio"/> PPPoE接続 <input type="radio"/> IPトンネル接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄
	DLCI <input type="text"/>

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**12. 以下の項目を指定します。**

- 鍵交換モード → 手動鍵使用
- 相手側エンドポイント → 202.168.1.66
- 自側エンドポイント → 202.168.2.66

鍵交換モード	<input checked="" type="radio"/> 手動鍵使用	
	相手側エンドポイント	202.168.1.66
	自側エンドポイント	202.168.2.66

**13. [保存] ボタンをクリックします。****14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- SAの設定 (送信用)
  - SPI値 → 101
  - 暗号アルゴリズム → des-cbc
  - 暗号鍵
  - 鍵識別 → 16進数
  - 鍵 → 23456789ab
  - 認証アルゴリズム → hmac-md5
  - 認証鍵
  - 鍵識別 → 16進数
  - 鍵 → 3456789abc
- SAの設定 (受信用)
  - SPI値 → 100
  - 暗号アルゴリズム → des-cbc
  - 暗号鍵
  - 鍵識別 → 16進数
  - 鍵 → 0123456789
  - 認証アルゴリズム → hmac-md5
  - 認証鍵
  - 鍵識別 → 16進数
  - 鍵 → 123456789a

■ IPsec情報(手動鍵)			
対象パケット (送信用)	自側IPアドレス	<input type="text"/>	
	自側アドレスマスク	0 (0.0.0.0)	
	相手側IPアドレス	<input type="text"/>	
	相手側アドレスマスク	0 (0.0.0.0)	
SAの設定 (送信用)	SPI値	101 (16進数)	
	暗号アルゴリズム	des-cbc	
	暗号鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	*****
	認証アルゴリズム	hmac-md5	
	認証鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
鍵		*****	
対象パケット (受信用)	相手側IPアドレス	<input type="text"/>	
	相手側アドレスマスク	0 (0.0.0.0)	
	自側IPアドレス	<input type="text"/>	
	自側アドレスマスク	0 (0.0.0.0)	
SAの設定 (受信用)	SPI値	100 (16進数)	
	暗号アルゴリズム	des-cbc	
	暗号鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
		鍵	*****
	認証アルゴリズム	hmac-md5	
	認証鍵	鍵識別	<input checked="" type="radio"/> 16進数 <input type="radio"/> 文字列
鍵		*****	

## 16. [保存] ボタンをクリックします。

## 17. 画面左側の [設定反映] 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。

## 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。

ここでは以下の条件によって、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。

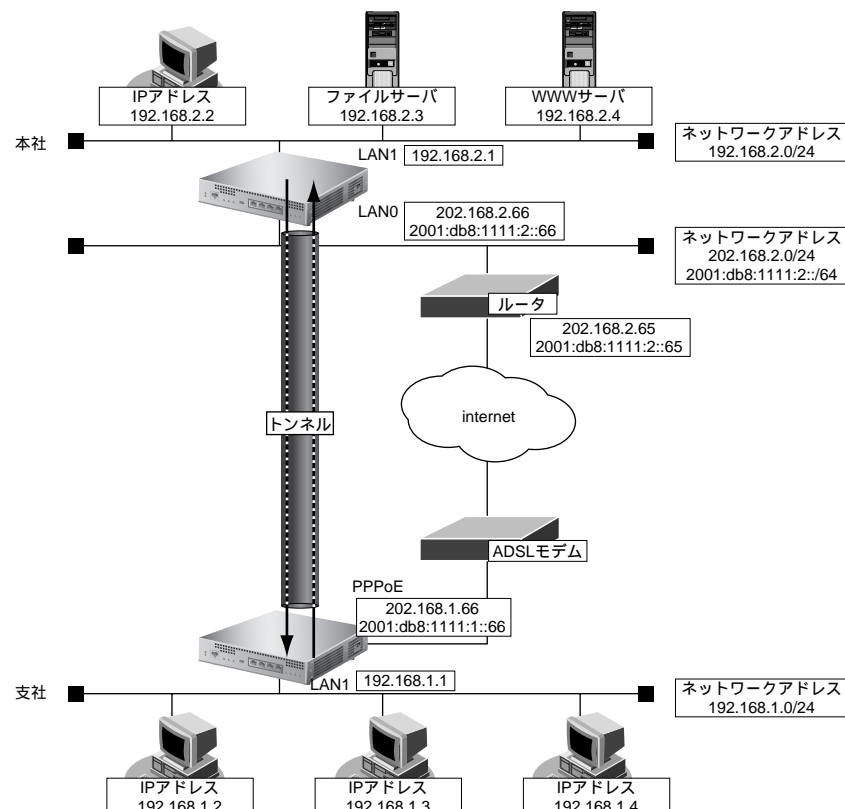
### ● 前提条件

#### 【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 LANポート：LAN0ポート使用

#### 【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 使用
- 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 : shared
- 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設定例を示します。

## 支社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	honsya
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インタフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

## 11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 2001:db8:1111:2::66
- 自側エンドポイント → 2001:db8:1111:1::66

鍵交換モード	<input checked="" type="radio"/> Main Mode使用
	相手側エンドポイント <input type="text"/> 2001:db8:1111:2::66
	自側エンドポイント <input type="text"/> 2001:db8:1111:1::66

## 13. [保存] ボタンをクリックします。

## 14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

SA の設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

## 16. [保存] ボタンをクリックします。

**17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

**18. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■ IKE情報		
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**19. [保存] ボタンをクリックします。****20. 画面左側の [設定反映] 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。

## 本社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	shisya
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インターフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

## 11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 鍵交換モード → Main Mode 使用
- 相手側エンドポイント → 2001:db8:1111:1::66
- 自側エンドポイント → 2001:db8:1111:2::66

鍵交換モード	<input checked="" type="radio"/> Main Mode 使用
	相手側エンドポイント <input type="text" value="2001:db8:1111:1::66"/>
	自側エンドポイント <input type="text" value="2001:db8:1111:2::66"/>

## 13. [保存] ボタンをクリックします。

## 14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- SA の設定
- 暗号アルゴリズム → des-cbc
- 認証アルゴリズム → hmac-md5

SA の設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	<input type="text" value="使用しない"/>
	SA有効時間	<input type="text" value="8"/> 時間
	SA有効データ量	<input type="text" value="0"/> GByte

## 16. [保存] ボタンをクリックします。

**17.** IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

**18.** 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DH グループ → modp768 (グループ1)

■ IKE 情報		
IKE 認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE 認証方式		shared
ポート番号		500
SA の設定	暗号アルゴリズム	des-cbc
	認証 (ハッシュ) アルゴリズム	hmac-md5
	DH グループ	modp768 (グループ1)
	SA 有効時間	24 時間

**19.** [保存] ボタンをクリックします。**20.** 画面左側の [設定反映] 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。

## 2.13.3 IPv4 over IPv6 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。

IPv4 ローカルネットワーク間を IPv6 インターネットで結んで IPsec を行います。

ここでは以下の条件によって、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。

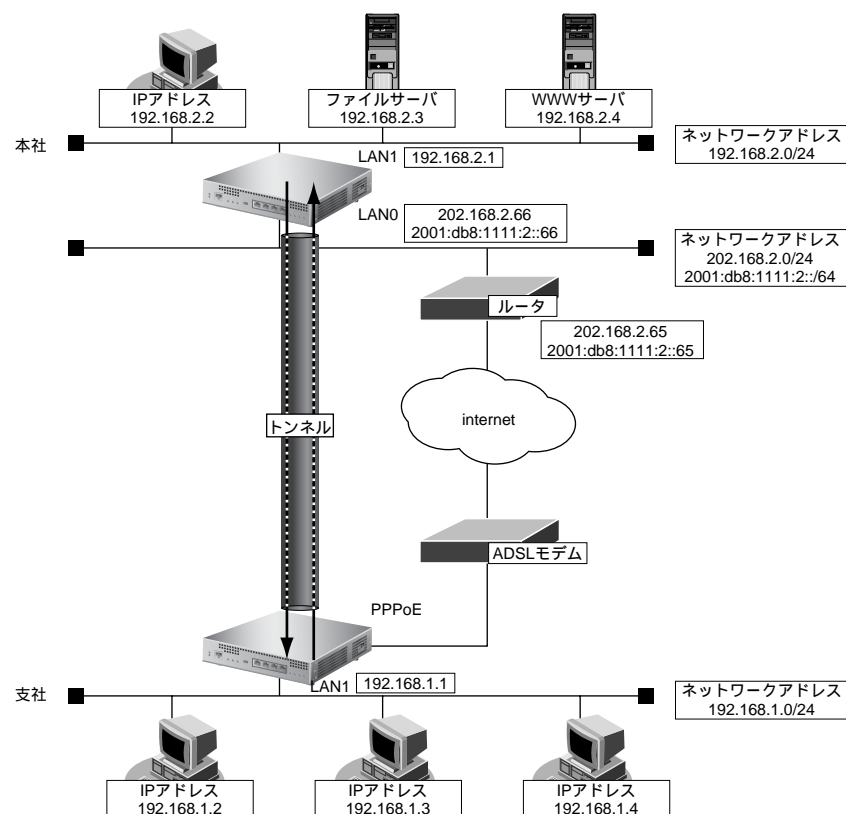
### ● 前提条件

#### 【支社 (PPPoE 常時接続)】

- ローカルネットワーク 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 LAN ポート : LAN0 ポート使用

#### 【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-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
- IKE (UDP:500 番ポート) のプライベートアドレス : 2001:db8:1111:1::66  
(インターネットプロバイダから割り当てられた IPv6 アドレス)
- ESP のプライベートアドレス : 2001:db8:1111:1::66  
(インターネットプロバイダから割り当てられた IPv6 アドレス)

### 【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-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 : shared
- 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設定例を示します。

## 支社 (Initiator) を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	<input type="text" value="honsya"/>
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インターフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

## 11. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 鍵交換モード → Aggressive Mode (Initiator) 使用
- 相手側エンドポイント → 2001:db8:1111:2::66
- 自装置識別情報 → shisya

鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Initiator)使用
	自側エンドポイント <input type="text"/>
	相手側エンドポイント <input type="text" value="2001:db8:1111:2::66"/>
	自装置識別情報 <input type="text" value="shisya"/>
	IDタイプ <input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

## 13. [保存] ボタンをクリックします。

## 14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

### 15. 以下の項目を指定します。

- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

### 16. [保存] ボタンをクリックします。

### 17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

### 18. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■ IKE情報		
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

### 19. [保存] ボタンをクリックします。

### 20. 画面左側の [設定反映] 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。

## 本社 (Responder) を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 5. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

### 6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	shisya
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インターフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**12. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode (Responder) 使用
- 自側エンドポイント → 2001:db8:1111:2::66
- 相手装置識別情報 → shisya

鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Responder)使用
	自側エンドポイント <input type="text" value="2001:db8:1111:2::66"/>
	相手側エンドポイント <input type="text"/>
	相手装置識別情報 <input type="text" value="shisya"/>
	IDタイプ <input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**13. [保存] ボタンをクリックします。****14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

### 15. 以下の項目を指定します。

- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

### 16. [保存] ボタンをクリックします。

### 17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

### 18. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■ IKE情報		
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

### 19. [保存] ボタンをクリックします。

### 20. 画面左側の [設定反映] 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。

## 2.13.4 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。

ここでは以下の条件によって、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。

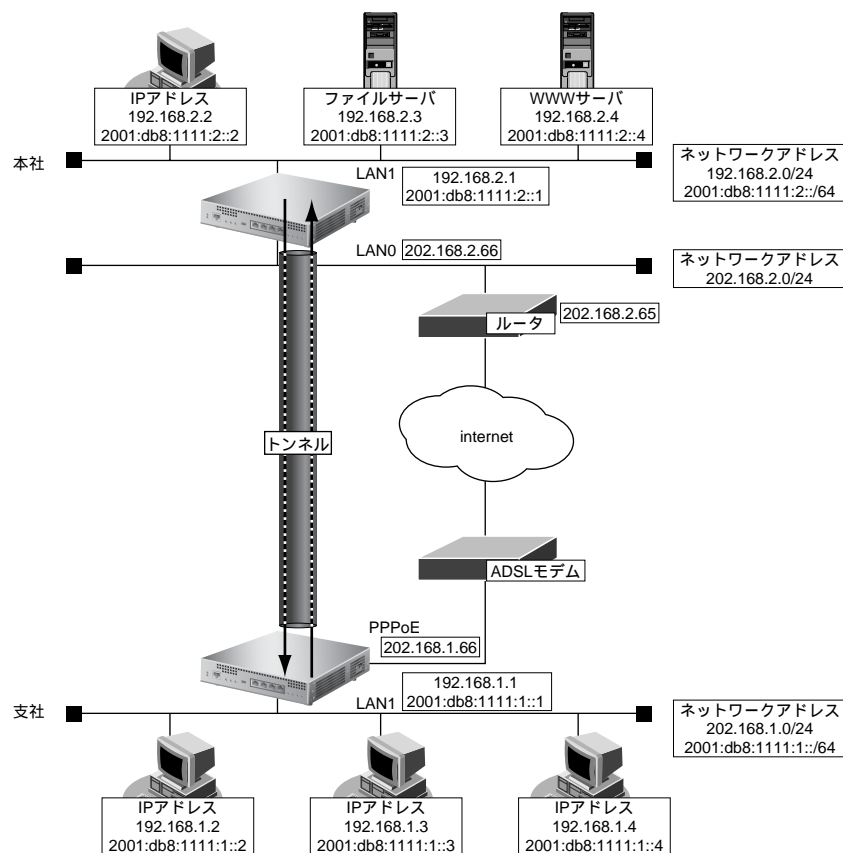
### ● 前提条件

#### 【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 LANポート : LAN0ポート使用

#### 【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 使用
- 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 : shared
- 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設定例を示します。

## 支社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「IPv6関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

## 10. 以下の項目を指定します。

- IPv6 →使用する

## 11. [保存] ボタンをクリックします。

## 12. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6スタティック経路情報」が表示されます。

## 13. 以下の項目を指定します。

- ネットワーク →ネットワーク指定  
あて先プレフィックス/プレフィックス長 →2001:db8:1111:2::/64
- メトリック値 →1

## 14. [追加] ボタンをクリックします。

## 15. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 16. 以下の項目を指定します。

- 接続先名 →honsya
- 接続先種別 →IPsec/IKE接続

**17. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**18. 以下の項目を指定します。**

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 202.168.2.66
- 自側エンドポイント → 202.168.1.66

鍵交換モード	Main Mode使用	
	相手側エンドポイント	202.168.2.66
	自側エンドポイント	202.168.1.66

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**21. 以下の項目を指定します。**

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv6すべて (「指定する」を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv6すべて (「指定する」を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

**22. [保存] ボタンをクリックします。****23. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

## 24. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

## 25. [保存] ボタンをクリックします。

## 26. 画面左側の [設定反映] 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。

## 本社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「IPv6関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

## 10. 以下の項目を指定します。

- IPv6 →使用する

## 11. [保存] ボタンをクリックします。

## 12. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

## 13. 以下の項目を指定します。

- ネットワーク →ネットワーク指定  
あて先プレフィックス/プレフィックス長 →2001:db8:1111:1::/64
- メトリック値 →1

## 14. [追加] ボタンをクリックします。

## 15. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 16. 以下の項目を指定します。

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

**17. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**18. 以下の項目を指定します。**

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 202.168.1.66
- 自側エンドポイント → 202.168.2.66

鍵交換モード	Main Mode使用	
	相手側エンドポイント	202.168.1.66
	自側エンドポイント	202.168.2.66

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**21. 以下の項目を指定します。**

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

**22. [保存] ボタンをクリックします。****23. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。



## 24. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

## 25. [保存] ボタンをクリックします。

## 26. 画面左側の [設定反映] 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。

## 2.13.5 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。

ここでは以下の条件によって、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。

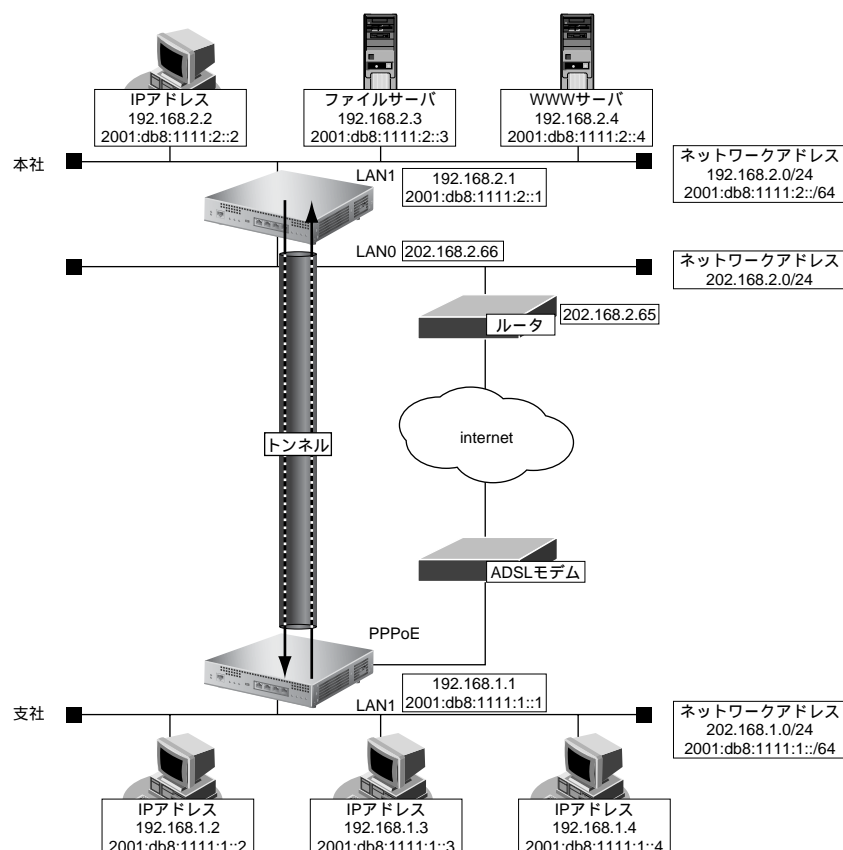
### ● 前提条件

#### 【支社 (PPPoE 常時接続)】

- ローカルネットワーク 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
- 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 LAN ポート : LAN0 ポート使用

#### 【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 : shared
- 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設定例を示します。

## 支社 (Initiator) を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」でネットワーク名が internet の【修正】ボタンをクリックします。  
「ネットワーク情報 (internet)」ページが表示されます。
4. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
5. IP 関連の設定項目の「静的 NAT 情報」をクリックします。  
「静的 NAT 情報」が表示されます。
6. 以下の項目を指定します。
  - プライベート IP 情報
 

IP アドレス	→ 192.168.1.1
ポート番号	→ isakmp
  - グローバル IP 情報
 

IP アドレス	→ 指定しない
ポート番号	→ isakmp
  - プロトコル
 

	→ udp
--	-------

<静的NAT情報入力フィールド>					
プライベート IP 情報	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">IP アドレス</td> <td><input type="text" value="192.168.1.1"/></td> </tr> <tr> <td>ポート番号</td> <td>isakmp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)</td> </tr> </table>	IP アドレス	<input type="text" value="192.168.1.1"/>	ポート番号	isakmp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)
IP アドレス	<input type="text" value="192.168.1.1"/>				
ポート番号	isakmp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)				
グローバル IP 情報	<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%;">IP アドレス</td> <td><input type="text"/></td> </tr> <tr> <td>ポート番号</td> <td>isakmp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)</td> </tr> </table>	IP アドレス	<input type="text"/>	ポート番号	isakmp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)
IP アドレス	<input type="text"/>				
ポート番号	isakmp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)				
プロトコル	udp (番号指定: <input type="text"/> "その他"を選択時のみ有効です)				

7. [追加] ボタンをクリックします。
8. 手順 6. ~ 7. を参考に、以下の項目を指定します。
  - プライベート IP 情報
 

IP アドレス	→ 192.168.1.1
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
--	-------
9. 画面上部の「相手情報」をクリックします。  
「相手情報」ページが表示されます。

**10. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**11. 以下の項目を指定します。**

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

**12. [追加] ボタンをクリックします。**

「ネットワーク情報 (vpn-hon)」ページが表示されます。

**13. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**14. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**15. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**16. [追加] ボタンをクリックします。****17. 「IPv6関連」をクリックします。**

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

## 18. 以下の項目を指定します。

- IPv6 →使用する

## 19. [保存] ボタンをクリックします。

## 20. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6スタティック経路情報」が表示されます。

## 21. 以下の項目を指定します。

- ネットワーク →ネットワーク指定  
あて先プレフィックス/プレフィックス長 →2001:db8:1111:2::/64
- メトリック値 →1

## 22. [追加] ボタンをクリックします。

## 23. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 24. 以下の項目を指定します。

- 接続先名 →honsya
- 接続先種別 →IPsec/IKE 接続

**25. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**26. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode (Initiator) 使用
- 相手側エンドポイント → 202.168.2.66
- 自装置識別情報 → shisyu

鍵交換モード	Aggressive Mode(Initiator)使用	
	自側エンドポイント	<input type="text"/>
	相手側エンドポイント	202.168.2.66
	自装置識別情報	shisyu
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**27. [保存] ボタンをクリックします。****28. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**29. 以下の項目を指定します。**

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv6すべて (「指定する」を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv6すべて (「指定する」を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

**30. [保存] ボタンをクリックします。****31. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

**32. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**33. [保存] ボタンをクリックします。****34. 画面左側の [設定反映] 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。



## 本社 (Responder) を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 5. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

### 6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6基本情報」が表示されます。

## 10. 以下の項目を指定します。

- IPv6 →使用する

## 11. [保存] ボタンをクリックします。

## 12. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

## 13. 以下の項目を指定します。

- ネットワーク →ネットワーク指定  
あて先プレフィックス/プレフィックス長 →2001:db8:1111:1::/64
- メトリック値 →1

## 14. [追加] ボタンをクリックします。

## 15. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 16. 以下の項目を指定します。

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

**17. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**18. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode (Responder) 使用
- 自側エンドポイント → 202.168.2.66
- 相手装置識別情報 → shisya

鍵交換モード	Aggressive Mode(Responder)使用	
	自側エンドポイント	202.168.2.66
	相手側エンドポイント	
	相手装置識別情報	shisya
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**21. 以下の項目を指定します。**

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		[?]
対象パケット	自側IPアドレス/マスク	IPv6すべて ("指定する"を選択時のみ有効です。) <input type="text"/>
	相手側IPアドレス/マスク	IPv6すべて ("指定する"を選択時のみ有効です。) <input type="text"/>
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	<input type="text" value="使用しない"/>
	SA有効時間	<input type="text" value="8"/> 時間
	SA有効データ量	<input type="text" value="0"/> GByte

**22. [保存] ボタンをクリックします。****23. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

**24. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**25. [保存] ボタンをクリックします。****26. 画面左側の [設定反映] 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。

## 2.13.6 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。

ここでは以下の条件によって、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。

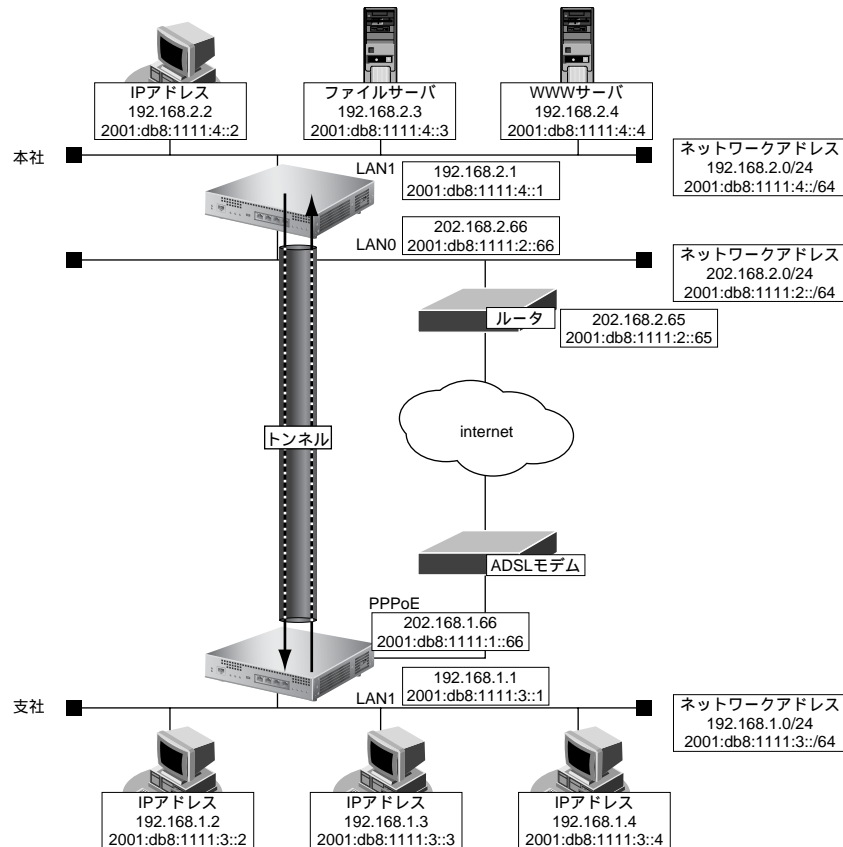
### ● 前提条件

#### 【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 LANポート : LAN0ポート使用

#### 【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 使用
- 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 : shared
- 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設定例を示します。

## 支社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

### 6. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

### 10. 以下の項目を指定します。

- IPv6 → 使用する

■ IPv6 基本情報	
IPv6	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する

### 11. [保存] ボタンをクリックします。

### 12. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6 スタティック経路情報」が表示されます。

**13. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定  
あて先プレフィックス/プレフィックス長 → 2001:db8:1111:4::/64
- メトリック値 → 1

<IPv6スタティック経路情報入力フィールド>	
ネット ワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先プレフィックス/プレフィックス長 <input type="text" value="2001:db8:1111:4::"/> / <input type="text" value="64"/>
メトリック 値	<input type="text" value="1"/>
優先 度	<input type="text" value="0"/>

**14. [追加] ボタンをクリックします。****15. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**16. 以下の項目を指定します。**

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	<input type="text" value="honsya"/>
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 ダイヤル1 電話番号 <input type="text"/> サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続 DLCI <input type="text"/> <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄

**17. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。



**18. 以下の項目を指定します。**

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 2001:db8:1111:2::66
- 自側エンドポイント → 2001:db8:1111:1::66

鍵交換モード	Main Mode使用	
	相手側エンドポイント	2001:db8:1111:2::66
	自側エンドポイント	2001:db8:1111:1::66

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**21. 以下の項目を指定します。**

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec 情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

**22. [保存] ボタンをクリックします。****23. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

**24. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	C 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**25. [保存] ボタンをクリックします。****26. 画面左側の [設定反映] 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。

## 本社を設定する

---

**1. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**2. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**3. 以下の項目を指定します。**

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

**4. [追加] ボタンをクリックします。**

「ネットワーク情報 (vpn-shi)」ページが表示されます。

**5. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**6. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

## 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定  
あて先IPアドレス → 192.168.1.0  
あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

## 8. [追加] ボタンをクリックします。

## 9. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6基本情報」が表示されます。

## 10. 以下の項目を指定します。

- IPv6 → 使用する

■ IPv6基本情報	
IPv6	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する

## 11. [保存] ボタンをクリックします。

## 12. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6スタティック経路情報」が表示されます。

## 13. 以下の項目を指定します。

- ネットワーク → ネットワーク指定  
あて先プレフィックス/プレフィックス長 → 2001:db8:1111:3::/64
- メトリック値 → 1

<IPv6スタティック経路情報入力フィールド>	
ネット ワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先プレフィックス/プレフィックス長 <input type="text" value="2001:db8:1111:3::"/> / <input type="text" value="64"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

## 14. [追加] ボタンをクリックします。

## 15. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

**16. 以下の項目を指定します。**

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	shisya
接続先種別	<input type="radio"/> 専用線接続
	<input type="radio"/> ISDN接続
	ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>
	サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続
	DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続
	<input type="radio"/> IPTunnel接続
	<input checked="" type="radio"/> IPsec/IKE接続
	<input type="radio"/> 別インタフェースから送出
<input type="radio"/> MPLSTunnel接続	
<input type="radio"/> パケット破棄	

**17. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**18. 以下の項目を指定します。**

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 2001:db8:1111:1::66
- 自側エンドポイント → 2001:db8:1111:2::66

鍵交換モード	<input checked="" type="radio"/> Main Mode使用	
	相手側エンドポイント	<input type="text" value="2001:db8:1111:1::66"/>
	自側エンドポイント	<input type="text" value="2001:db8:1111:2::66"/>

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

## 21. 以下の項目を指定します。

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		?
対象パケット	自側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

## 22. [保存] ボタンをクリックします。

## 23. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

## 24. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証(ハッシュ)アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■ IKE情報		?
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

## 25. [保存] ボタンをクリックします。

## 26. 画面左側の「設定反映」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。

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

接続するたびに IPv6 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。

ここでは以下の条件によって、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。

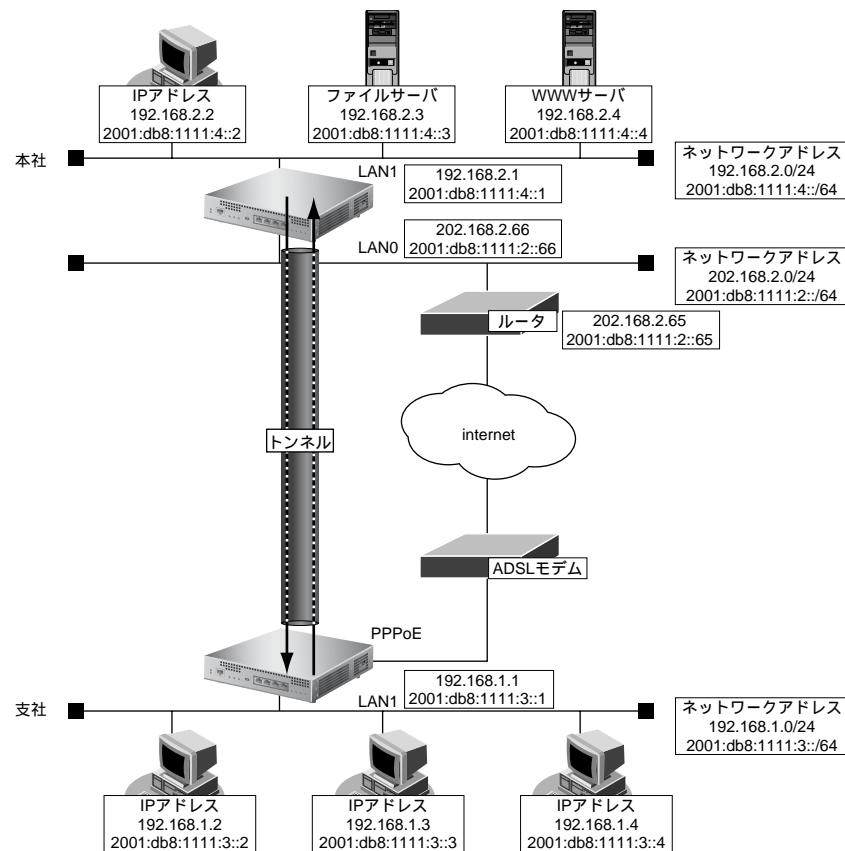
### ● 前提条件

#### 【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
- 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 LAN ポート : LAN0 ポート使用

#### 【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-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
- IKE (UDP:500 番ポート) のプライベートアドレス : 2001:db8:1111:1::66 (インターネットプロバイダから割り当てられた IPv6 アドレス)
- ESP のプライベートアドレス : 2001:db8:1111:1::66 (インターネットプロバイダから割り当てられた IPv6 アドレス)

### 【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-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 : shared
- 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設定例を示します。

## 支社 (Initiator) を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.2.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「IPv6関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。



## 10. 以下の項目を指定します。

- IPv6 →使用する

## 11. [保存] ボタンをクリックします。

## 12. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。

「IPv6スタティック経路情報」が表示されます。

## 13. 以下の項目を指定します。

- ネットワーク →ネットワーク指定  
あて先プレフィックス/プレフィックス長 →2001:db8:1111:4::/64
- メトリック値 →1

## 14. [追加] ボタンをクリックします。

## 15. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 16. 以下の項目を指定します。

- 接続先名 →honsya
- 接続先種別 →IPsec/IKE 接続

**17. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**18. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode (Initiator) 使用
- 相手側エンドポイント → 2001:db8:1111:2::66
- 自装置識別情報 → shisya

鍵交換モード	Aggressive Mode(Initiator)使用	
	自側エンドポイント	
	相手側エンドポイント	2001:db8:1111:2::66
	自装置識別情報	shisya
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**21. 以下の項目を指定します。**

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv6すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

**22. [保存] ボタンをクリックします。****23. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

## 24. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

## 25. [保存] ボタンをクリックします。

## 26. 画面左側の [設定反映] 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。

## 本社 (Responder) を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 7. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

### 8. [追加] ボタンをクリックします。

### 9. 「IPv6関連」をクリックします。

IPv6関連の設定項目と「IPv6基本情報」が表示されます。

**10. 以下の項目を指定します。**

- IPv6 →使用する

**11. [保存] ボタンをクリックします。****12. IPv6 関連の設定項目の「IPv6 スタティック経路情報」をクリックします。**

「IPv6 スタティック経路情報」が表示されます。

**13. 以下の項目を指定します。**

- ネットワーク →ネットワーク指定  
あて先プレフィックス/プレフィックス長 →2001:db8:1111:3::/64
- メトリック値 →1

**14. [追加] ボタンをクリックします。****15. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**16. 以下の項目を指定します。**

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

**17. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**18. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode (Responder) 使用
- 自側エンドポイント → 2001:db8:1111:2::66
- 相手装置識別情報 → shisya

鍵交換モード	Aggressive Mode(Responder)使用	
	自側エンドポイント	2001:db8:1111:2::66
	相手側エンドポイント	
	相手装置識別情報	shisya
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

**21. 以下の項目を指定します。**

- 対象パケット
  - 自側IPアドレス/マスク → IPv6 すべて
  - 相手側IPアドレス/マスク → IPv6 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		[?]
対象パケット	自側IPアドレス/マスク	IPv6すべて (<"指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv6すべて (<"指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	0 時間
	SA有効データ量	0 GByte

**22. [保存] ボタンをクリックします。****23. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。**

「IKE 情報」が表示されます。

## 24. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

## 25. [保存] ボタンをクリックします。

## 26. 画面左側の [設定反映] 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。

## 2.13.8 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）。

ここでは以下の条件により、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。

### ● 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 LANポート : LAN0ポート使用

#### 【本社】

- ローカルネットワークIPアドレス1 : LAN0ポート使用
- 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

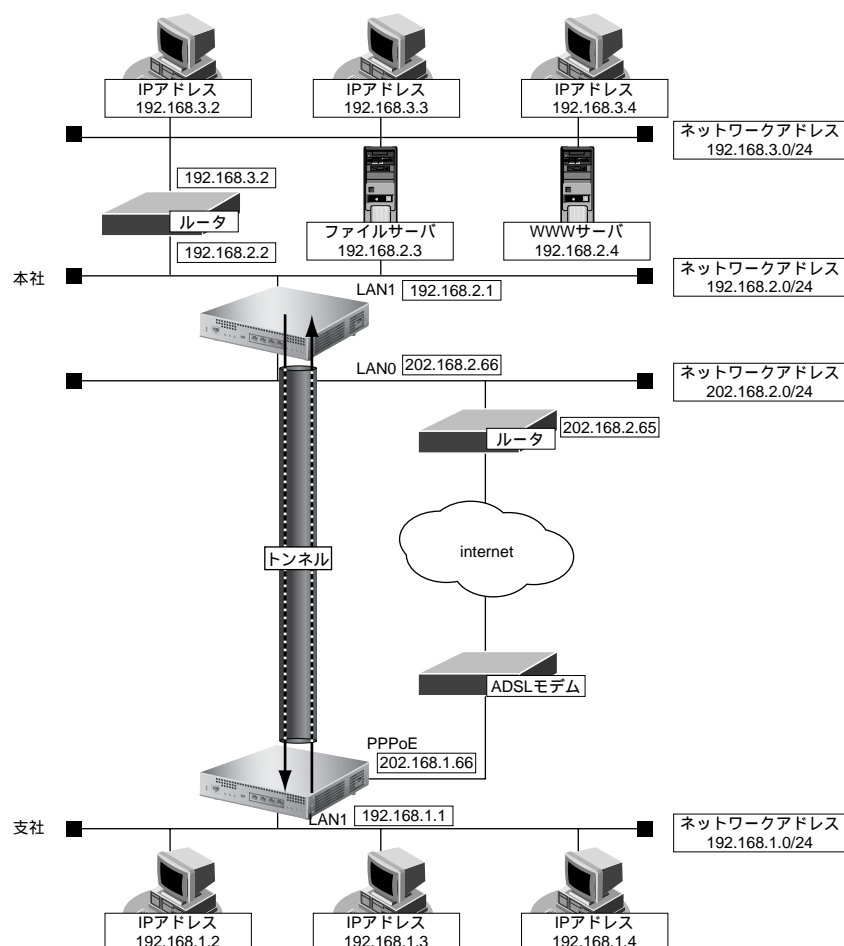
#### 【本社】

- 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 使用
- 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 : 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設定例を示します。

## 支社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-hon

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-hon

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

**6. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**7. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定  
   あて先IPアドレス → 192.168.2.0  
   あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.2.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**8. [追加] ボタンをクリックします。****9. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → honsya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	<input type="text" value="honsya"/>
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続
	ダイアル1 <input type="text"/> 電話番号 <input type="text"/> サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続 DLCI <input type="text"/>
	<input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 202.168.2.66
- 自側エンドポイント → 202.168.1.66

鍵交換モード	Main Mode使用	
	相手側エンドポイント	202.168.2.66
	自側エンドポイント	202.168.1.66

## 13. [保存] ボタンをクリックします。

## 14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- 対象パケット
  - 相手側IPアドレス/マスク → 指定する
  - 192.168.2.0/24
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv4すべて (“指定する”を選択時のみ有効です。)
	相手側IPアドレス/マスク	指定する (“指定する”を選択時のみ有効です。) 192.168.2.0 / 24 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

## 16. [保存] ボタンをクリックします。

## 17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

**18. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	C 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。**

「マルチルーティング情報」が表示されます。

**21. 以下の項目を指定します。**

- あて先情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)

<マルチルーティング情報入力フィールド>		
動作	この接続先を <input type="checkbox"/> 使用する <input checked="" type="checkbox"/>	
プロトコル	すべて <input checked="" type="checkbox"/> (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)	
送信元情報	IPアドレス	<input type="text"/>
	アドレスマスク	0 (0.0.0.0)
	ポート番号	<input type="text"/>
あて先情報	IPアドレス	192.168.2.0
	アドレスマスク	24 (255.255.255.0)
	ポート番号	<input type="text"/>
TOS	<input type="text"/>	

**22. 画面左側の [設定反映] 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。

**23. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**24. 以下の項目を指定します。**

- 接続先名 → honsya2
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>

接続先名

接続先種別

- 専用線接続
- ISDN接続
- ダイヤル1  電話番号
- サブアドレス
- フレームリレー接続
- DLCI
- IPsec/IKE接続
- PPPoE接続
- IPトンネル接続
- 別インタフェースから送出
- MPLSトンネル接続
- パケット破棄

**25. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**26. 以下の項目を指定します。**

- 鍵交換モード → IKE は他の接続先情報を使用
- 接続先名 → honsya

鍵交換モード

- IKEは他の接続先情報を使用

接続先名

**27. [保存] ボタンをクリックします。****28. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

## 29. 以下の項目を指定します。

- 対象パケット  
相手側IPアドレス/マスク → 指定する  
→ 192.168.3.0/24
- SAの設定  
暗号アルゴリズム → des-cbc  
認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv4すべて (“指定する”を選択時のみ有効です。)
	相手側IPアドレス/マスク	指定する (“指定する”を選択時のみ有効です。)
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

## 30. [保存] ボタンをクリックします。

## 31. 画面左側の [設定反映] 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。

## 本社のIPsec/IKEを設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワーク名 → vpn-shi

<ネットワーク情報追加フィールド>	
ネットワーク名	vpn-shi

### 4. [追加] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

**6. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**7. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定  
   あて先IPアドレス → 192.168.1.0  
   あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**8. [追加] ボタンをクリックします。****9. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**10. 以下の項目を指定します。**

- 接続先名 → shisya
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>	
接続先名	<input type="text" value="shisya"/>
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続
	ダイヤル1 <input type="text" value=""/> 電話番号 <input type="text" value=""/> サブアドレス <input type="text" value=""/>
	<input type="radio"/> フレームリレー接続 DLCI <input type="text" value=""/>
	<input checked="" type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

**11. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 12. 以下の項目を指定します。

- 鍵交換モード → Main Mode使用
- 相手側エンドポイント → 202.168.1.66
- 自側エンドポイント → 202.168.2.66

鍵交換モード	Main Mode使用	
	相手側エンドポイント	202.168.1.66
	自側エンドポイント	202.168.2.66

## 13. [保存] ボタンをクリックします。

## 14. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

## 15. 以下の項目を指定します。

- 対象パケット
  - 自側IPアドレス/マスク → 指定する
  - 192.168.2.0/24
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	指定する (“指定する”を選択時のみ有効です。) 192.168.2.0 / 24 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv4すべて (“指定する”を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	使用しない
	SA有効時間	8 時間
	SA有効データ量	0 GByte

## 16. [保存] ボタンをクリックします。

## 17. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。



**18. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → abcdefghijklmnopqrstuvwxyz1234567890
- SA の設定
  - 暗号アルゴリズム → des-cbc
  - 認証 (ハッシュ) アルゴリズム → hmac-md5
  - DHグループ → modp768 (グループ1)

■IKE情報		?
IKE認証鍵	鍵種別	C 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****
IKE認証方式		shared
ポート番号		500
SAの設定	暗号アルゴリズム	des-cbc
	認証(ハッシュ)アルゴリズム	hmac-md5
	DHグループ	modp768(グループ1)
	SA有効時間	24 時間

**19. [保存] ボタンをクリックします。****20. IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。**

「マルチルーティング情報」が表示されます。

**21. 以下の項目を指定します。**

- 送信元情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)

<マルチルーティング情報入力フィールド>		
動作	この接続先を <input type="checkbox"/> 使用する <input checked="" type="checkbox"/>	
プロトコル	すべて <input checked="" type="checkbox"/> (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)	
送信元情報	IPアドレス	192.168.2.0
	アドレスマスク	24 (255.255.255.0)
	ポート番号	
あて先情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	
TOS		

**22. [追加] ボタンをクリックします。****23. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**24. 以下の項目を指定します。**

- 接続先名 → shisya2
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>

接続先名 shisya2

専用線接続  
 ISDN接続  
 フレームリレー接続  
 IPsec/IKE接続  
 別インタフェースから送出  
 MPLSトンネル接続  
 パケット破棄

ダイヤル1 電話番号 [ ]  
サブアドレス [ ]

接続先種別 DLCI [ ]

**25. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**26. 以下の項目を指定します。**

- 鍵交換モード → IKE は他の接続先情報を使用
- 接続先名 → shisya

鍵交換モード

- IKE(は他の接続先情報を使用)

接続先名 shisya

**27. [保存] ボタンをクリックします。****28. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

## 29. 以下の項目を指定します。

- 対象パケット
  - 自側IPアドレス/マスク → 指定する  
→ 192.168.3.0/24
  - 相手側IPアドレス/マスク → 指定する  
→ 192.168.3.0/24
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5

IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	指定する (<"指定する"を選択時のみ有効です。)            192.168.3.0 / 24            ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv4すべて (<"指定する"を選択時のみ有効です。)            / /             ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	<input type="checkbox"/> 使用しない
	SA有効時間	0 時間
	SA有効データ量	0 GByte

## 30. [保存] ボタンをクリックします。

## 31. 画面左側の [設定反映] 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。

## 2.13.9 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、「IPv4 over IPv4 で固定 IP アドレスでの VPN (自動鍵交換)」または「IPv4 over IPv4 で可変 IP アドレスでの VPN (自動鍵交換)」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
- IKE セッション監視機能
- 動的経路 (RIP) 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
- IKE セッション監視機能

### 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設定例を示します。

## 支社を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名がvpn-honの【修正】ボタンをクリックします。  
「ネットワーク情報 (vpn-hon)」ページが表示されます。
4. 「IP関連」をクリックします。  
IP関連の設定項目と「IP基本情報」が表示されます。
5. IP関連の設定項目の「NAT情報」をクリックします。  
「NAT情報」が表示されます。
6. 以下の項目を指定します。
  - NATの使用 → マルチ NAT
  - グローバルアドレス → 192.168.1.1
  - アドレス個数 → 1

■ NAT情報	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチ NAT <input type="radio"/> 静的NATのみ
グローバルアドレス	<input type="text" value="192.168.1.1"/>
アドレス個数	<input type="text" value="1"/> 個
アドレス割当てタイマ	<input type="text" value="5"/> 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsecパススルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

7. 【保存】ボタンをクリックします。
8. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。

## 9. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 21,23
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断
プロトコル	tcp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス 192.168.1.0
	アドレスマスク 24 (255.255.255.0)
	ポート番号 
あて先情報	IPアドレス 192.168.2.0
	アドレスマスク 24 (255.255.255.0)
	ポート番号 21,23
ICMP	タイプ 
	コード 
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	
方向	入出力

## 10. [追加] ボタンをクリックします。

**11. 手順9.～10.を参考に、以下の項目を指定します。**

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 21,23
- あて先情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象外
- TOS → 指定しない
- 方向 → 入出力

**12. 手順9.～10.を参考に、以下の項目を指定します。**

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**13. IP関連の設定項目の「TOS 値書き換え情報」をクリックします。**

「TOS 値書き換え情報」が表示されます。

**14. 以下の項目を指定します。**

- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 20,21
- TOS → 指定しない
- 新TOS → a0

<TOS値書き換え情報入力フィールド>	
プロトコル	tcp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス: 192.168.1.0
	アドレスマスク: 24 (255.255.255.0)
	ポート番号:
あて先情報	IPアドレス: 192.168.2.0
	アドレスマスク: 24 (255.255.255.0)
	ポート番号: 20,21
TOS	
新TOS	a0

**15. [追加] ボタンをクリックします。****16. 画面左側の [設定反映] 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。

**本社を設定する**

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名がvpn-shiの [修正] ボタンをクリックします。  
「ネットワーク情報 (vpn-shi)」ページが表示されます。
4. 「IP関連」をクリックします。  
IP関連の設定項目と「IP基本情報」が表示されます。
5. IP関連の設定項目の「IPフィルタリング情報」をクリックします。  
「IPフィルタリング情報」が表示されます。



## 6. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 21,23
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断
プロトコル	tcp (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)
送信元情報	IPアドレス: 192.168.1.0
	アドレスマスク: 24 (255.255.255.0)
	ポート番号:
あて先情報	IPアドレス: 192.168.2.0
	アドレスマスク: 24 (255.255.255.0)
	ポート番号: 21,23
ICMP	タイプ:
	コード:
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外
TOS	
方向	入出力

## 7. [追加] ボタンをクリックします。

**8. 手順 6.～7.を参考に、以下の項目を指定します。**

- 動作 →透過
- プロトコル →tcp
- 送信元情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 21,23
- あて先情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象外
- TOS →指定しない
- 方向 →入出力

**9. 手順 6.～7.を参考に、以下の項目を指定します。**

- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →指定しない
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

**10. IP関連の設定項目の「TOS 値書き換え情報」をクリックします。**

「TOS 値書き換え情報」が表示されます。

**11. 以下の項目を指定します。**

- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 20,21
- あて先情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- TOS → 指定しない
- 新TOS → a0

＜TOS値書き換え情報入力フィールド＞	
プロトコル	tcp <input type="checkbox"/> 番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です
送信元情報	IPアドレス 192.168.2.0
	アドレスマスク 24 (255.255.255.0)
	ポート番号 20,21
あて先情報	IPアドレス 192.168.1.0
	アドレスマスク 24 (255.255.255.0)
	ポート番号 
TOS	
新TOS	a0

**12. [追加] ボタンをクリックします。****13. 画面左側の [設定反映] 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。

## 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設定例を示します。

### 本社を設定する

#### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

#### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

#### 3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名がvpn-shiの【修正】ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

#### 4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

#### 5. 以下の項目を指定します。

- シェーピング → 使用する
- 最大送信レート → 2Mbps

■基本情報	
ネットワーク名	vpn-shi
MTUサイズ	1500 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	最大送信レート 2 Mbps

#### 6. 【保存】ボタンをクリックします。

#### 7. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

#### 8. IP関連の設定項目の「帯域制御 (WFQ) 情報」をクリックします。

「帯域制御 (WFQ) 情報」が表示されます。

## 9. 以下の項目を指定します。

- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.2.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → any
- あて先情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → any
- 対象TOSフィールド値 → any
- 帯域 → 最優先

＜帯域制御(WFQ)情報入力フィールド＞	
プロトコル	tcp (番号指定: <input type="checkbox"/> "その他"を選択時のみ有効です)
送信元情報	IPアドレス: 192.168.2.0
	アドレスマスク: 24 (255.255.255.0)
	ポート番号: any
あて先情報	IPアドレス: 192.168.1.0
	アドレスマスク: 24 (255.255.255.0)
	ポート番号: any
対象TOSフィールド値	any
帯域	<input checked="" type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 <input type="text"/> 共有できる定義が存在しません

## 10. [追加] ボタンをクリックします。

## 11. 画面左側の [設定反映] 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。

### 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「相手情報」 - 「ネットワーク情報」で設定します。この場合、IPsec用の「ネットワーク情報」でシェーピングを行うか、または、実回線の「ネットワーク情報」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設定例を示します。

### 支社を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の【修正】ボタンをクリックします。  
「ネットワーク情報 (vpn-hon)」ページが表示されます。
4. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
5. 以下の項目を指定します。
  - MSS 書き換え →使用する  
書き換えサイズ →1414

■ IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない
	<input type="radio"/> 設定する
	相手側IPアドレス <input type="text"/>
	自側IPアドレス <input type="text"/>
MSS書き換え	<input type="radio"/> 使用しない
	<input checked="" type="radio"/> 使用する
	書き換えサイズ <input type="text" value="1414"/> バイト

6. 【保存】ボタンをクリックします。
7. 画面左側の【設定反映】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。

### 本社を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。

3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の [修正] ボタンをクリックします。  
「ネットワーク情報 (vpn-shi)」ページが表示されます。
4. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
5. 以下の項目を指定します。
  - MSS 書き換え → 使用する  
書き換えサイズ → 1414

6. [保存] ボタンをクリックします。
7. 画面左側の [設定反映] 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。

## 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設定例を示します。

### 支社を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-hon の [修正] ボタンをクリックします。  
「ネットワーク情報 (vpn-hon)」ページが表示されます。
4. 「共通情報」をクリックします。  
共通情報の設定項目と「基本情報」が表示されます。

## 5. 以下の項目を指定します。

- MTU サイズ → 1460

■基本情報	
ネットワーク名	vpn-hon
MTUサイズ	1460 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps

## 6. [保存] ボタンをクリックします。

## 7. 画面左側の [設定反映] 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。

## 本社を設定する

## 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

## 3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名が vpn-shi の [修正] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

## 4. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

## 5. 以下の項目を指定します。

- MTU サイズ → 1460

■基本情報	
ネットワーク名	vpn-shi
MTUサイズ	1460 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps

## 6. [保存] ボタンをクリックします。

## 7. 画面左側の [設定反映] 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。



## 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設定例を示します。

### 支社を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名がvpn-honの【修正】ボタンをクリックします。  
「ネットワーク情報 (vpn-hon)」ページが表示されます。
4. 「接続先情報」をクリックします。  
「接続先情報」が表示されます。
5. 「接続先情報」でIPsec/IKE 接続で接続先名がhonsyaの【修正】ボタンをクリックします。  
IPsec/IKE 接続の設定項目と「基本情報」が表示されます。
6. IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。  
「接続制御情報」が表示されます。

## 7. 以下の項目を指定します。

- 接続先監視 → 使用する
- 送信元IPアドレス → 192.168.1.1
- あて先IPアドレス → 192.168.2.1
- 正常時送信間隔 → 10秒
- 再送間隔 → 1秒
- タイムアウト時間 → 5秒
- 異常時送信間隔 → 1分

■ 接続制御情報		
接続先監視	<input type="radio"/> 使用しない	
	<input checked="" type="radio"/> 使用する	
	送信元IPアドレス	192.168.1.1
	あて先IPアドレス	192.168.2.1
	正常時送信間隔	10 秒
	再送間隔	1 秒
	タイムアウト時間	5 秒
	異常時送信間隔	1 分
	送信 TTL/HopLimit	255
監視方式	<input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視	

## 8. [保存] ボタンをクリックします。

## 9. 画面左側の [設定反映] 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。

## IKE セッション監視機能との併用例

### ● 設定条件

#### [支社]

- 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設定例を示します。

### 支社を設定する

#### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

#### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名がvpn-honの [修正] ボタンをクリックします。

「ネットワーク情報 (vpn-hon)」ページが表示されます。

4. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

5. 「接続先情報」でIPsec/IKE 接続で接続先名がhonsyaの [修正] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

6. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

7. 以下の項目を指定します。

- IKEセッション監視
  - 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

IKEセッション監視	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

8. [保存] ボタンをクリックします。

9. 画面左側の [設定反映] 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。

こんな事に気をつけて

- IKEセッション監視のあて先IPアドレスは、「IPsec 情報」の“対象パケット”に含まれるIPアドレスを指定してください。
- IKEセッション監視のあて先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なることがあります。

## 動的経路 (RIP) 機能と併用する場合

---

### ● 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設定例を示します。

### 支社を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」でIPsec/IKE 接続を行うネットワーク名がvpn-honの【修正】ボタンをクリックします。  
「ネットワーク情報 (vpn-hon)」ページが表示されます。
4. 「IP関連」をクリックします。  
IP関連の設定項目と「IP基本情報」が表示されます。
5. IP関連の設定項目の「スタティック経路情報」をクリックします。  
「スタティック経路情報」が表示されます。
6. 【全削除】ボタンをクリックします。  
「削除していいですか？」の確認画面が表示されます。
7. 【OK】ボタンをクリックします。  
「スタティック経路情報」が削除されます。
8. IP関連の設定項目の「RIP情報」をクリックします。  
「RIP情報」が表示されます。

## 9. 以下の項目を指定します。

- RIP送信 → V1で送信する
- RIP受信 → V1で受信する
- メトリック値 → 0

■ RIP情報	
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	0

## 10. [保存] ボタンをクリックします。

## 11. 画面左側の [設定反映] 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。

## 本社を設定する

### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 3. 「ネットワーク情報」で IPsec/IKE 接続を行うネットワーク名がvpn-shiの [修正] ボタンをクリックします。

「ネットワーク情報 (vpn-shi)」ページが表示されます。

### 4. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

### 5. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 6. [全削除] ボタンをクリックします。

「削除していいですか？」の確認画面が表示されます。

### 7. [OK] ボタンをクリックします。

「スタティック経路情報」が削除されます。

### 8. IP関連の設定項目の「RIP情報」をクリックします。

「RIP情報」が表示されます。

**9. 以下の項目を指定します。**

- RIP送信 → V1で送信する
- RIP受信 → V1で受信する
- メトリック値 → 0

■RIP情報	
RIP送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input checked="" type="radio"/> V1で受信する <input type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	0

**10. [保存] ボタンをクリックします。****11. 画面左側の [設定反映] ボタンをクリックします。**

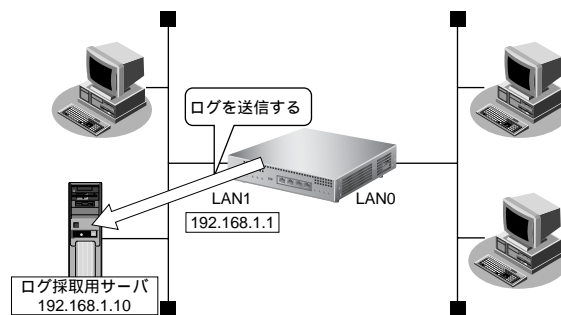
設定した内容が有効になります。

## 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システムログ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）

ここでは、採取したログをサーバに送信する場合の設定方法を説明します。



### ● 設定条件

- 以下のセキュリティログを採取する
  - PPP
  - IPフィルタ
  - URLフィルタ
  - NAT
  - DHCP
- 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設定を行う場合の設定例を示します。

## システムログ情報を設定する

### 1. 設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

### 2. 「システムログ情報」をクリックします。

「システムログ情報」が表示されます。

### 3. 以下の項目を指定します。

- システムログ送信 → 送信する  
送信先ホスト → 192.168.1.10
- セキュリティログ → PPP、IPフィルタ、URLフィルタ、NAT、DHCP

■システムログ情報	
システムログ送信	<input type="radio"/> 送信しない <input checked="" type="radio"/> 送信する 送信先ホスト <input type="text" value="192.168.1.10"/>
セキュリティログ	<input checked="" type="checkbox"/> PPP <input checked="" type="checkbox"/> IPフィルタ <input checked="" type="checkbox"/> URLフィルタ <input checked="" type="checkbox"/> NAT <input checked="" type="checkbox"/> DHCP
重複メッセージの出力	<input checked="" type="radio"/> する <input type="radio"/> しない

### 4. [保存] ボタンをクリックします。

### 5. 画面左側の [設定反映] 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。

## 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。

ここでは、本装置で確認する方法を説明します。

### 1. 表示メニューで「システムログ」をクリックします。

「システムログ」ページが表示されます。

【システムログ】
Sep 19 18:03:14 init: system startup now.

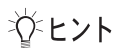


## 2.15 マルチ NAT 機能（アドレス変換機能）を使う

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いて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 MR1000 機能説明書「[2.14 マルチ NAT 機能](#)」(P.63)



ヒント

### ◆ 同時に接続できる台数

機能	同時接続台数およびセッション数	備考
基本 NAT	グローバル IP 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 IP アドレスを使用しないでください
動的 NAT	最大 1024 セッションまで	外部からの通信はできない
静的 NAT	最大 64 個まで割り当て可能	プライベート IP アドレスとポートをグローバル IP 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

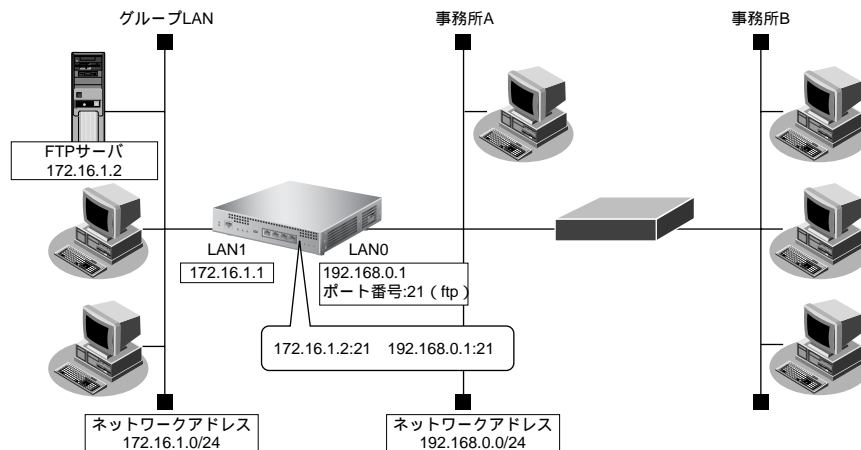
### こんな事に気をつけて

文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「[1.5 文字入力フィールドで入力できる文字一覧](#)」(P.13)

## 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】

- LAN0ポートを使用する
- 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設定例を示します。

## 静的NAT情報を設定する

1. 設定メニューのルータ設定で「LAN情報」をクリックします。  
「LAN情報」ページが表示されます。
2. 「LAN情報」でインタフェースがLAN0の【修正】ボタンをクリックします。  
「LAN0情報 (物理LAN)」ページが表示されます。
3. 「IP関連」をクリックします。  
IP関連の設定項目と「IPアドレス情報」が表示されます。
4. IP関連の設定項目の「NAT情報」をクリックします。  
「NAT情報」が表示されます。

## 5. 以下の項目を指定します。

- NATの使用 →マルチ NAT

■NAT情報	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ ※NATの使用とDHCPリレーサービスの併用はできません

## 6. [保存] ボタンをクリックします。

## 7. IP関連の設定項目の「静的NAT情報」をクリックします。

「静的NAT情報」が表示されます。

こんな事に気をつけて

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設定してください。

## 8. 以下の項目を指定します。

- プライベートIP情報
  - IPアドレス → 172.16.1.2
  - ポート番号 → ftp
- グローバルIP情報
  - IPアドレス → 192.168.0.1
  - ポート番号 → ftp
- プロトコル → tcp

<静的NAT情報入力フィールド>		
プライベートIP情報	IPアドレス	172.16.1.2
	ポート番号	ftp (番号指定: [ ] “その他”を選択時のみ有効です)
グローバルIP情報	IPアドレス	192.168.0.1
	ポート番号	ftp (番号指定: [ ] “その他”を選択時のみ有効です)
プロトコル	tcp (番号指定: [ ] “その他”を選択時のみ有効です)	

## 9. [追加] ボタンをクリックします。

## 10. 画面左側の [設定反映] 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。

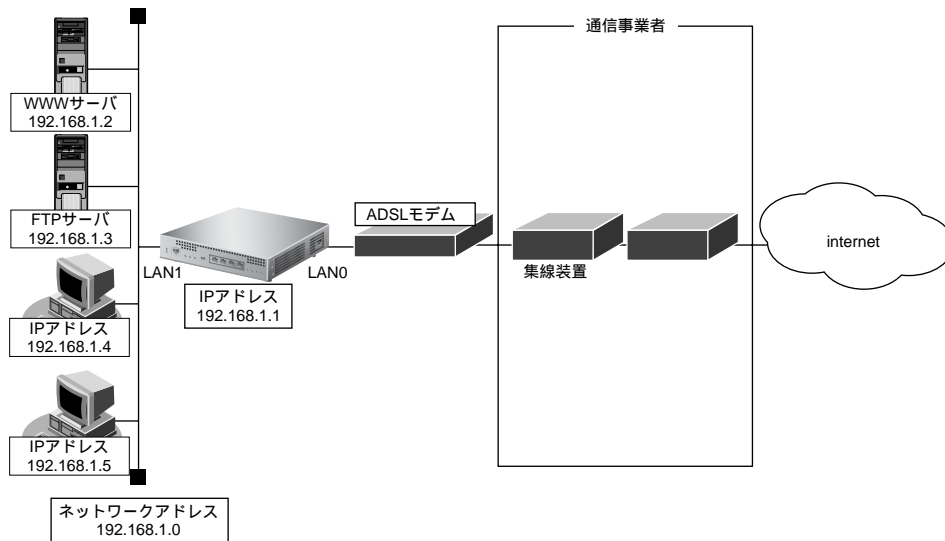
こんな事に気をつけて

NATセキュリティは、“高い”が初期値として選択されています。ftpやdnsの要求した相手からの応答時には“高い”を選択します。相手サーバがNATを使用している場合など、要求先とは別のアドレスからの応答時には“通常”を選択してください。

## 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

上記の設定条件に従って設定を行う場合の設定例を示します。

## かんたん設定で PPPoE 接続の情報を設定する

### 1. かんたん設定メニューで「PPPoE 接続」をクリックします。

「PPPoE かんたん設定」ページが表示されます。

### 2. [必須設定] で以下の項目を指定します。

- 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)

■ 必須設定	
ユーザ認証ID	userid
ユーザ認証パスワード	*****

### 3. [設定終了] ボタンをクリックします。

再起動後に、通信できる状態になります。

## アドレス変換情報を設定する

1. 詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3. 「ネットワーク情報」で登録したネットワークの欄の【修正】ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

4. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

5. IP関連の設定項目の「NAT情報」をクリックします。

「NAT情報」が表示されます。

6. 以下の項目を指定します。


- NATの使用 →マルチ NAT



NATセキュリティで“高い”を選択した場合、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、“通常”を選択してください。

### 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。

■ NAT情報 	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチ NAT <input type="radio"/> 静的 NATのみ

7. 【保存】ボタンをクリックします。

8. IP関連の設定項目の「静的 NAT情報」をクリックします。

「静的 NAT情報」が表示されます。

**9. 以下の項目を指定します。**

- プライベートIP 情報
  - IPアドレス → 192.168.1.2
  - ポート番号 → www,http
- グローバルIP 情報
  - IPアドレス → 指定しない
  - ポート番号 → www,http

**こんな事に気をつけて**

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。

<静的NAT情報入力フィールド>		
プライベート IP情報	IPアドレス	192.168.1.2
	ポート 番号	www,http (番号指定: [ ] “その他”を選択時のみ有効です)
グローバル IP情報	IPアドレス	
	ポート 番号	www,http (番号指定: [ ] “その他”を選択時のみ有効です)
プロトコル		すべて (番号指定: [ ] “その他”を選択時のみ有効です)

**10. [追加] ボタンをクリックします。****11. 手順9.～10.を参考に、以下の項目を指定します。**

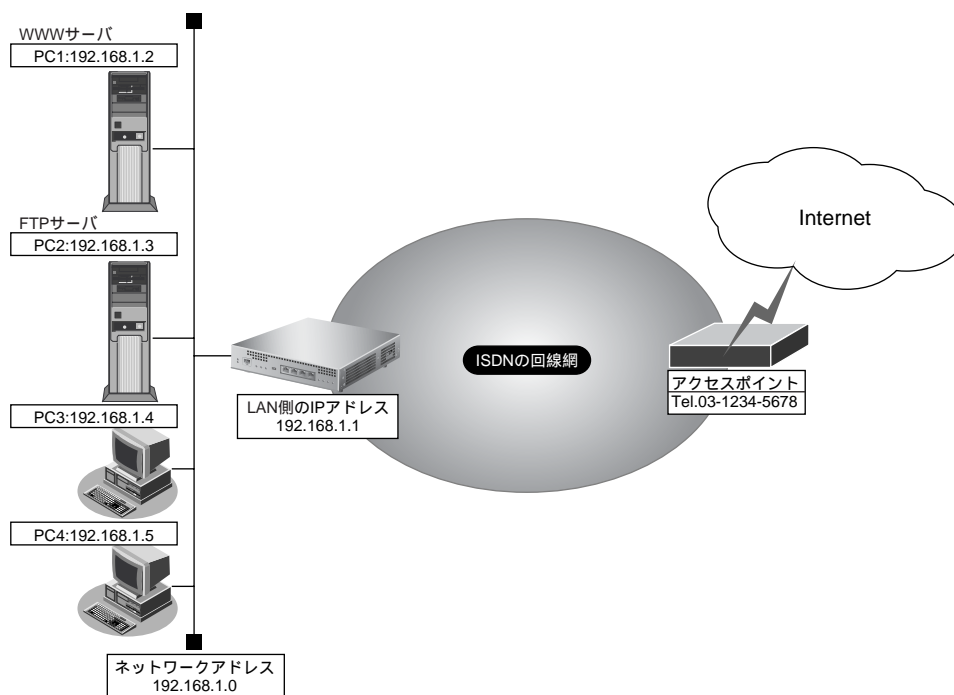
- プライベートIP 情報
  - IPアドレス → 192.168.1.3
  - ポート番号 → ftp
- グローバルIP 情報
  - IPアドレス → 指定しない
  - ポート番号 → ftp

**12. 画面左側の [設定反映] 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。

## 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

- ISDN ポートでISDN でインターネットに接続する
- ISDN に接続する
- ユーザ認証ID : userid
- ユーザ認証パスワード : userpass
- ネットワーク型接続を行う
- 既存のLANを使用する
- 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
- 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

ここでは、設定条件に従って、ISDN接続する設定が行われていることを前提として、設定例を示します。

## NAT 情報を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. NAT 情報を行うネットワーク情報の【修正】ボタンをクリックします。  
「ネットワーク情報 (internet)」ページが表示されます。
4. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP 基本情報」が表示されます。
5. IP 関連の設定項目の「NAT 情報」をクリックします。  
「NAT 情報」が表示されます。
6. 以下の項目を指定します。
  - NATの使用 → マルチ NAT
  - グローバルアドレス → 10.10.10.100
  - アドレス個数 → 3
  - アドレス割当てタイマ → 5分
  - NATセキュリティ → 高い

■ NAT 情報	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチ NAT <input type="radio"/> 静的NATのみ
グローバルアドレス	<input type="text" value="10.10.10.100"/>
アドレス個数	<input type="text" value="3"/> 個
アドレス割当てタイマ	<input type="text" value="5"/> 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsecパススルー	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

7. 【保存】ボタンをクリックします。
8. IP 関連の設定項目の「静的 NAT 情報」をクリックします。  
「静的 NAT 情報」が表示されます。



## 9. 以下の項目を指定します。

- プライベートIP 情報
  - IPアドレス → 192.168.1.2
  - ポート番号 → www,http
- グローバルIP 情報
  - IPアドレス → 10.10.10.98
  - ポート番号 → www,http
- プロトコル → すべて

<静的NAT情報入力フィールド>		
プライベート IP情報	IPアドレス	192.168.1.2
	ポート 番号	www,http (番号指定: [ ] "その他"を選択時のみ有効です)
グローバル IP情報	IPアドレス	10.10.10.98
	ポート 番号	www,http (番号指定: [ ] "その他"を選択時のみ有効です)
プロトコル		すべて (番号指定: [ ] "その他"を選択時のみ有効です)

## 10. [追加] ボタンをクリックします。

## 11. 手順 10. ~ 11. を参考に、以下の項目を指定します。

- プライベートIP 情報
  - IPアドレス → 192.168.1.3
  - ポート番号 → ftp (21)
- グローバルIP 情報
  - IPアドレス → 10.10.10.99
  - ポート番号 → ftp (21)
- プロトコル → すべて

## 12. 画面左側の [設定反映] ボタンをクリックします。

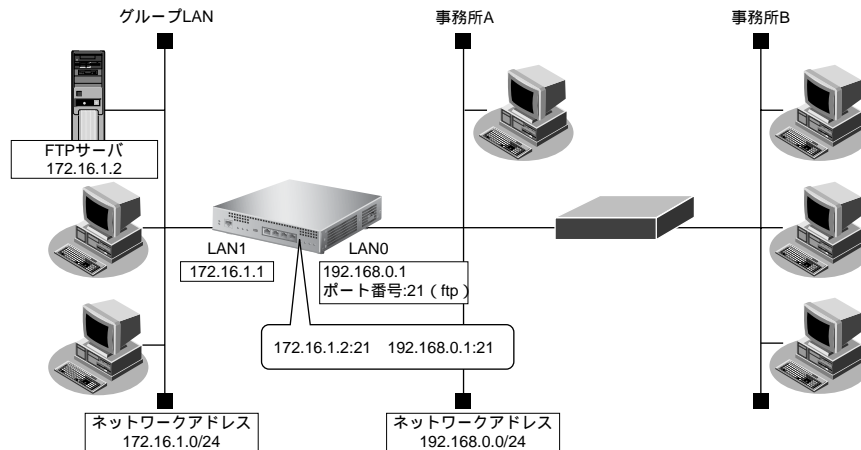
設定した内容が有効になります。

### 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ときには、「相手情報」 - 「ネットワーク情報」 - 「IP関連」 - 「NAT情報」で、「NATセキュリティ」を“通常”に設定してください。

## 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】

- LAN0 ポートを使用する
- 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設定例を示します。

### 静的 NAT 情報を設定する

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインターフェースが LAN0 の【修正】ボタンをクリックします。  
「LAN0 情報 (物理 LAN)」ページが表示されます。
3. 「IP 関連」をクリックします。  
IP 関連の設定項目と「IP アドレス情報」が表示されます。
4. IP 関連の設定項目の「NAT 情報」をクリックします。  
「NAT 情報」が表示されます。

## 5. 以下の項目を指定します。

- NATの使用 → 静的 NATのみ

■ NAT 情報	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input type="radio"/> マルチNAT <input checked="" type="radio"/> 静的NATのみ ※NATの使用とDHCP/ルーターサービスの併用はできません

## 6. [保存] ボタンをクリックします。

## 7. IP関連の設定項目の「静的 NAT 情報」をクリックします。

「静的 NAT 情報」が表示されます。

## 8. 以下の項目を指定します。

- プライベート IP 情報
  - IPアドレス → 172.16.1.2
  - ポート番号 → ftp
- グローバル IP 情報
  - IPアドレス → 192.168.0.1
  - ポート番号 → ftp
- プロトコル → tcp

<静的NAT情報入力フィールド>		
プライベート IP 情報	IPアドレス	<input type="text" value="172.16.1.2"/>
	ポート番号	ftp (番号指定: <input type="text"/> “その他”を選択時のみ有効です)
グローバル IP 情報	IPアドレス	<input type="text" value="192.168.0.1"/>
	ポート番号	ftp (番号指定: <input type="text"/> “その他”を選択時のみ有効です)
プロトコル		tcp (番号指定: <input type="text"/> “その他”を選択時のみ有効です)

## 9. [追加] ボタンをクリックします。

## 10. 画面左側の [設定反映] ボタンをクリックします。

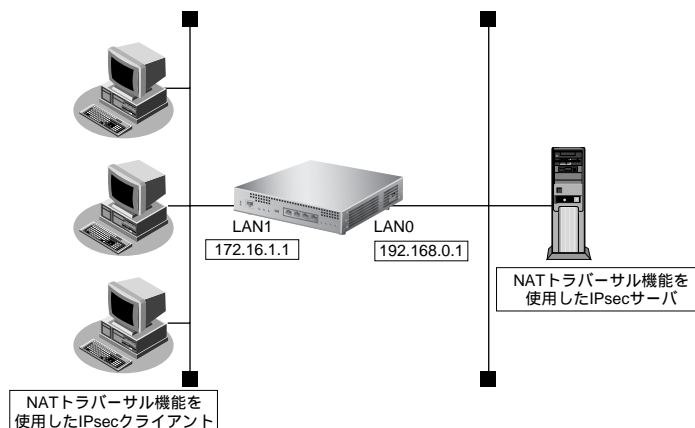
設定した内容が有効になります。

#### こんな事に気をつけて

NAT セキュリティは、“高い” が初期値として選択されています。ftp や dns の要求した相手からの応答時には“高い”を選択します。相手サーバが NAT を使用している場合など、要求先とは別のアドレスからの応答時には“通常”を選択してください。

## 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】

- LAN0ポートを使用する
- 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設定例を示します。

## NAT情報を設定する

1. 設定メニューのルータ設定で「LAN情報」をクリックします。  
「LAN情報」ページが表示されます。
2. 「LAN情報」でインタフェースがLAN0の【修正】ボタンをクリックします。  
「LAN0情報（物理LAN）」ページが表示されます。
3. 「IP関連」をクリックします。  
IP関連の設定項目と「IPアドレス情報」が表示されます。
4. IP関連の設定項目の「NAT情報」をクリックします。  
「NAT情報」が表示されます。

## 5. 以下の項目を指定します。

- NATの使用 →マルチ NAT
- IPsec パススルー →無効

■NAT情報	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチNAT <input type="radio"/> 静的NATのみ ※NATの使用とDHCPリレーサービスの併用はできません
グローバルアドレス	<input type="text"/>
アドレス個数	<input type="text" value="1"/> 個
アドレス割当てタイム	<input type="text" value="5"/> 分
NATセキュリティ	<input type="radio"/> 通常 <input checked="" type="radio"/> 高い
IPsec パススルー	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

## 6. [保存] ボタンをクリックします。

## 7. 画面左側の [設定反映] 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。

こんな事に気をつけて

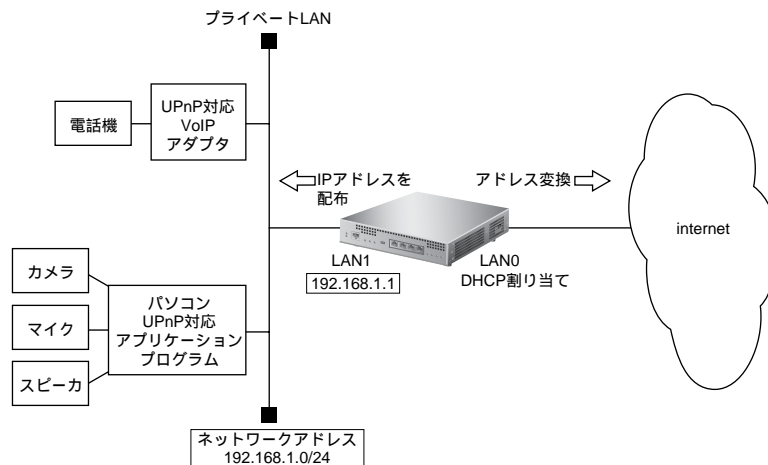
- NATセキュリティは、“高い” が初期値として選択されています。ftpや dnsの要求した相手からの応答時には“高い”を選択します。相手サーバがNATを使用している場合など、要求先とは別のアドレスからの応答時には“通常”を選択してください。
- IPsec クライアントがNATトラバーサル機能を使用する場合は、IPsec パススルーを“無効”に設定します。IPsec パススルーを“有効”に設定すると、相手ごとに1つのIPsecパスしか接続することができません。

## 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 MR1000 機能説明書「2.15 VoIP NAT トラバーサル機能」(P.66)

ここでは、UPnP 対応 VoIP アダプタや 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】

- 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

#### 【UPnP 対応装置 (プライベート LAN) 側】

- 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
  - DNS サーバ広報 → 192.168.1.1

こんな事に気をつけて

文字入力フィールドでは半角文字（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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

ここでは、設定条件に従って、LAN の設定が行われていることを前提とします。

上記の設定条件に従って設定を行う場合の設定例を示します。

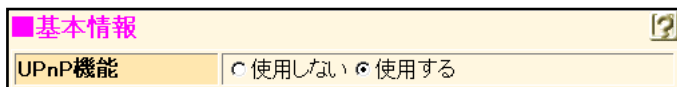
## UPnP 情報を設定する

1. 設定メニューのルータ設定で「UPnP 情報」をクリックします。

「UPnP 情報」ページが表示されます。

2. 以下の項目を指定します。

- UPnP 機能 →使用する



■基本情報	
UPnP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する

3. [保存] ボタンをクリックします。
4. 画面左側の [設定反映] 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。

## 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ことができます。

☛ 参照 MR1000 機能説明書 [2.16 TOS/Traffic Class 値書き換え機能] (P.69)

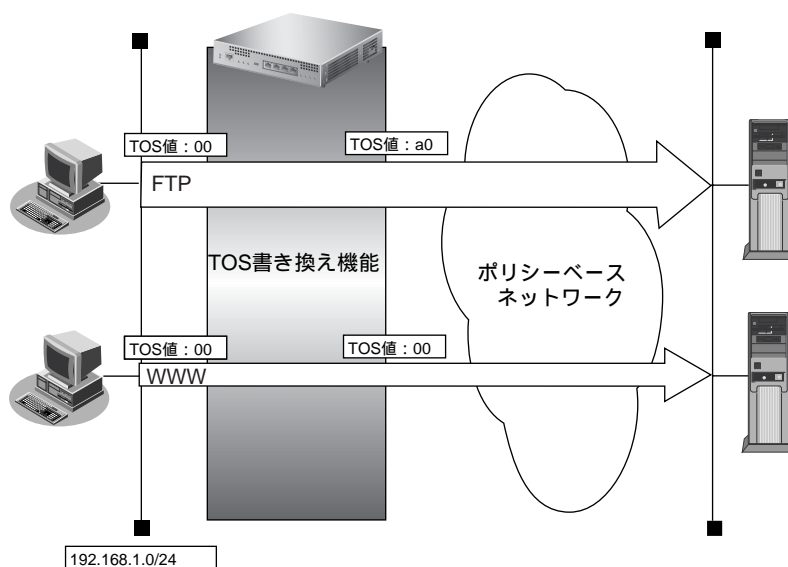
### TOS/Traffic Class 値書き換え機能の条件

本装置では、以下の条件を指定することによって、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も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設定例を示します。

**FTP サーバのアクセスで TOS 値を 00 から a0 に変更する**

---

1. **設定メニューのルータ設定で「相手情報」をクリックします。**  
「相手情報」ページが表示されます。
2. **「ネットワーク情報」をクリックします。**  
「ネットワーク情報」が表示されます。
3. **「ネットワーク情報」で TOS 値書き換えの設定を行うネットワーク名の【修正】ボタンをクリックします。**  
「ネットワーク情報」が表示されます。
4. **「IP関連」をクリックします。**  
IP関連の設定項目と「IPアドレス情報」が表示されます。
5. **「TOS 値書き換え情報」をクリックします。**  
「TOS 値書き換え情報」が表示されます。

## 6. 以下の項目を指定します。

- プロトコル → tcp
- 送信元情報
  - IPアドレス → 192.168.1.0
  - アドレスマスク → 24 (255.255.255.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 指定しない
  - ポート番号 → 20 (ftp-data のポート番号)、21 (ftp のポート番号)
- TOS → 00
- 新TOS → a0

<TOS値書き換え情報入力フィールド>	
プロトコル	tcp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス 192.168.1.0
	アドレスマスク 24 (255.255.255.0)
	ポート番号
あて先情報	IPアドレス
	アドレスマスク 0 (0.0.0.0)
	ポート番号 20,21
TOS	00
新TOS	a0

## 7. [追加] ボタンをクリックします。

## 8. 画面左側の [設定反映] 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。

## 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、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。

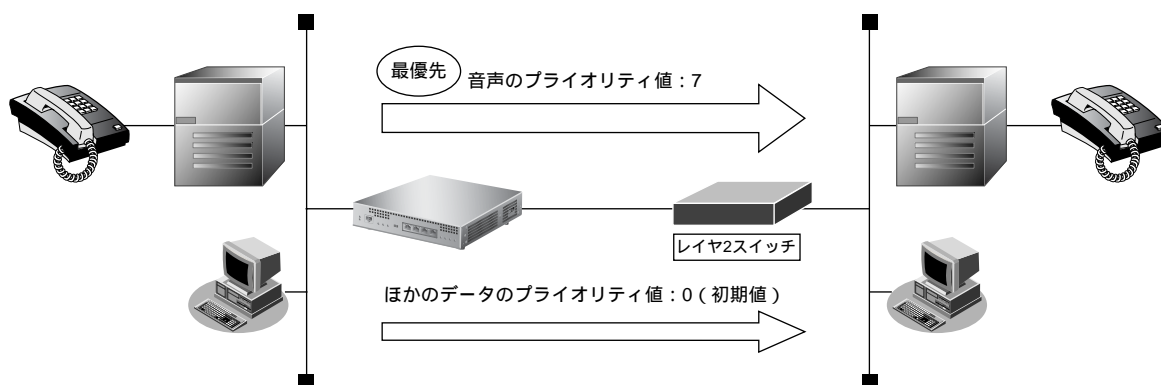
☞ 参照 MR1000 機能説明書「2.17 VLANプライオリティマッピング機能」(P.71)

本装置では、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。

- 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)
- その他は初期値 (プライオリティ値が0)



### ● 設定条件

- 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設定例を示します。

1. **設定メニューのルータ設定の「LAN 情報」をクリックします。**  
「LAN 情報」ページが表示されます。
2. **「LAN 情報」で VLAN プライオリティマッピングの設定を行う LAN の[修正] ボタンをクリックします。**  
「LAN 情報 (VLAN)」ページが表示されます。
3. **「共通情報」をクリックします。**  
共通情報の設定項目と「基本情報」が表示されます。
4. **共通情報の設定項目の「VLAN プライオリティマッピング情報」をクリックします。**  
「VLAN プライオリティマッピング情報」が表示されます。
5. **以下の項目を指定します。**
  - プロトコル → IPv4
  - TOS/Traffic Class → a0
  - プライオリティ → 7

<VLANプライオリティマッピング情報入力フィールド>	
プロトコル	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
TOS/Traffic Class	<input type="text" value="a0"/>
プライオリティ	<input type="text" value="7"/>

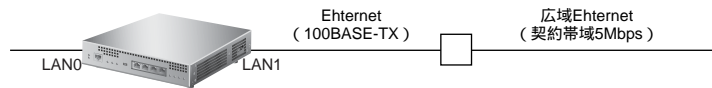
6. **[追加] ボタンをクリックします。**
7. **画面左側の [設定反映] ボタンをクリックします。**  
設定した内容が有効になります。

## 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、LAN および WAN 回線に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、Ethernet回線の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 を利用する通信環境が設定済み
- 広域 Ethernet の契約帯域は 5Mbps

上記の設定条件に設定を行う場合の設定例を示します。

#### 1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

#### 2. 「LAN 情報」でインタフェースが LAN1 の [修正] ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

#### 3. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

#### 4. 以下の項目を指定します。

- シェーピング → 使用する
- 最大送信レート → 5Mbps

■ 基本情報	
ポート番号	master 基本 1 backup バックアップなし
優先使用ポート	<input checked="" type="radio"/> master <input type="radio"/> 先にリンクアップしたポート
転送レート	自動認識
シェーピング	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する 最大送信レート 5 Mbps

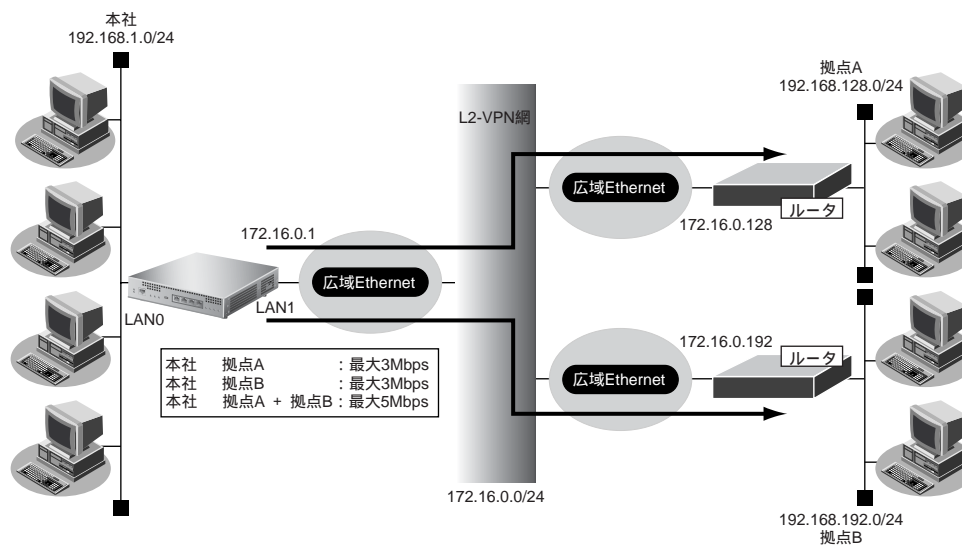
#### 5. [保存] ボタンをクリックします。

#### 6. 画面左側の [設定反映] 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。

## 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
- 本社の本装置はLANポートのアドレス設定ができた状態から設定を始める

上記の設定条件に設定を行う場合の設定例を示します。

1. 設定メニューのルータ設定の「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
2. 「LAN 情報」でインタフェースがLAN1の「修正」ボタンをクリックします。  
「LAN1 情報 (物理 LAN)」ページが表示されます。
3. 「共通情報」をクリックします。  
共通情報に関する設定項目と「基本情報」が表示されます。

## 4. 以下の項目を指定します。

- シェーピング →使用する  
最大送信レート →5Mbps

■基本情報	
ポート番号	master 基本1 backup バックアップなし
優先使用ポート	<input checked="" type="radio"/> master <input type="radio"/> 先にリンクアップしたポート
転送レート	自動認識
シェーピング	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する 最大送信レート 5 Mbps

## 5. [保存] ボタンをクリックします。

## 6. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 7. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

## 8. 以下の項目を指定します。

- ネットワーク名 →kyotenA

<ネットワーク情報追加フィールド>	
ネットワーク名	kyotenA

## 9. [追加] ボタンをクリックします。

「ネットワーク情報 (kyotenA)」が表示されます。

## 10. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

## 11. 以下の項目を指定します。

- シェーピング →使用する  
最大送信レート →3Mbps

■基本情報	
ネットワーク名	kyotenA
MTUサイズ	1500 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する 最大送信レート 3 Mbps

## 12. [保存] ボタンをクリックします。

## 13. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

**14. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**15. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.128.0
- あて先アドレスマスク → 24 (255.255.255.0)

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.128.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**16. [追加] ボタンをクリックします。****17. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**18. 以下の項目を指定します。**

- 接続先名 → OV-A
- 接続先種別 → 別インタフェースから送出

<接続先情報追加フィールド>	
接続先名	<input type="text" value="OV-A"/>
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続
	ダイヤル1 <input type="text"/> 電話番号 <input type="text"/> サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続 <input type="text" value="DLCI"/>
	<input type="radio"/> PPPoE接続 <input type="radio"/> IPトンネル接続 <input type="radio"/> IPsec/IKE接続 <input checked="" type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄

**19. [追加] ボタンをクリックします。**

別インタフェースから送出の設定項目と「基本情報」が表示されます。



**20. 以下の項目を指定します。**

- 送出先インタフェース → LAN1
- 転送先ルータ  
IPv4 ルータ → 172.16.0.128

■基本情報		
接続先名	OV-A	
送出先インタフェース	LAN1	
転送先ルータ	IPv4ルータ	172.16.0.128
	IPv6ルータ	

**21. [保存] ボタンをクリックします。****22. 手順 6. ～ 21. を参考にして、拠点 B を設定します。**

## 「ネットワーク情報」

- ネットワーク名 → kyotenB

## 「共通情報」

- シェーピング → 使用する
- 最大送信レート → 3Mbps

## 「スタティック経路情報」

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.192.0
- あて先アドレスマスク → 24 (255.255.255.0)

## 「接続先情報」

- 接続先名 → OV-B
- 接続先種別 → 別インタフェースから送出

## 「基本情報」

- 送出先インタフェース → LAN1
- 転送先ルータ  
IPv4 ルータ → 172.16.0.192

**23. 画面左側の [設定反映] 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。

## 2.20 データ圧縮／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、データ圧縮および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。

データ圧縮は、ISDN 接続、専用線接続、およびモデム接続をサポートしています。

データ圧縮および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。

- データ圧縮
  - LZS
- 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 (rmt0) 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

- ネットワーク情報 (rmt0) 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設定例を示します。

#### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

#### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

#### 3. 「PPP 関連」をクリックします。

PPP 関連に関する項目と「圧縮情報」が表示されます。

#### 4. 以下の項目を指定します。

- ヘッダ圧縮 (IPCP) → VJ、IPヘッダ圧縮

■ 圧縮情報 <span style="float: right;">?</span>	
ヘッダ圧縮 (IPCP)	<input checked="" type="checkbox"/> VJ <input checked="" type="checkbox"/> IPヘッダ圧縮
ヘッダ圧縮 (IPv6CP)	<input type="checkbox"/> IPヘッダ圧縮
データ圧縮 (CCP)	<input type="checkbox"/> LZS

#### 5. [保存] ボタンをクリックします。

#### 6. 画面左側の [設定反映] 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。

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。

## ISDN、専用線、モデム接続の場合

ここでは、ISDN接続、専用線接続、およびモデム接続をネットワーク0（remote0）で定義している環境に対してデータ圧縮およびヘッダ圧縮を併用する場合の設定方法を説明します。

### ● 設定条件

- ネットワーク情報（rmt0）でISDNによる通信環境が設定済み
- データ圧縮機能を使用する
- ヘッダ圧縮機能を使用する

上記の設定条件に従ってデータ圧縮およびヘッダ圧縮を行う場合の設定例を示します。

#### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

#### 2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

#### 3. ネットワーク名がrmt0の【修正】ボタンをクリックします。

「ネットワーク情報（rmt0）」ページが表示されます。

#### 4. 「PPP 関連」をクリックします。

PPP 関連の設定項目と「圧縮情報」が表示されます。

#### 5. 以下の項目を指定します。

- ヘッダ圧縮（IPCP） → VJ、IPヘッダ圧縮
- データ圧縮（CCP） → LZS

■圧縮情報	
ヘッダ圧縮 (IPCP)	<input checked="" type="checkbox"/> VJ <input checked="" type="checkbox"/> IPヘッダ圧縮
ヘッダ圧縮 (IPv6CP)	<input type="checkbox"/> IPヘッダ圧縮
データ圧縮 (CCP)	<input checked="" type="checkbox"/> LZS

#### 6. 【保存】ボタンをクリックします。

#### 7. 画面左側の【設定反映】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。

こんな事に気をつけて

MPと併用する場合は、「相手情報」－「ネットワーク情報」－「PPP 関連」－「MP 情報」－「受信パケット順序制御」を“する”に設定してください。

## 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。

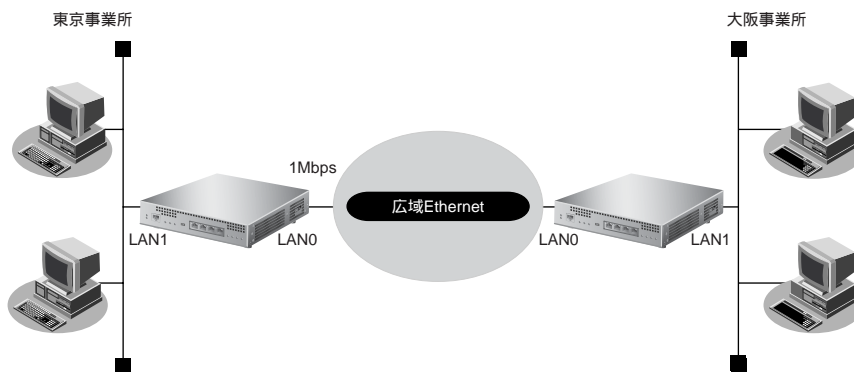
☛ 参照 MR1000 機能説明書 「2.19 帯域制御 (WFQ) 機能」 (P.73)

### 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

ここでは、広域 Ethernet サービスによる拠点間の接続がすでに設定されている場合を例に帯域制御を利用する設定方法を説明します。



#### ● 設定条件

- LAN0 インタフェースで広域 Ethernet サービスでの通信環境が設定済み
- 広域 Ethernet サービスの契約速度は 1Mbps
- 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設定例を示します。

## 東京事業所を設定する

### 1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

### 3. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

### 4. 以下の項目を指定します。

- シェーピング → 使用する  
最大送信レート → 1Mbps

■基本情報	
ポート番号	master 基本0
	backup バックアップなし
優先使用ポート	<input checked="" type="radio"/> master <input type="radio"/> 先にリンクアップしたポート
転送レート	自動認識
シェーピング	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	最大送信レート 1 Mbps

### 5. [保存] ボタンをクリックします。

### 6. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 7. IP 関連の設定項目の「帯域制御 (WFQ) 情報」をクリックします。

「帯域制御 (WFQ) 情報」が表示されます。

## 8. 以下の項目を指定します。

- プロトコル →すべて
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →0 (0.0.0.0)
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →0 (0.0.0.0)
  - ポート番号 →指定しない
- 対象TOSフィールド値 →a0
- 帯域 →最優先

＜帯域制御(WFQ)情報入力フィールド＞	
プロトコル	すべて (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)
送信元情報	IPアドレス <input type="text"/>
	アドレスマスク 0 (0.0.0.0)
	ポート番号 <input type="text"/>
あて先情報	IPアドレス <input type="text"/>
	アドレスマスク 0 (0.0.0.0)
	ポート番号 <input type="text"/>
対象TOSフィールド値	a0
帯域	<input checked="" type="radio"/> 最優先 <input type="radio"/> ベストエフォート <input type="radio"/> 使用率 <input type="text"/> % <input type="radio"/> 使用帯域 <input type="text"/> Kbps <input type="radio"/> 帯域を他と共有 共有できる定義が存在しません

## 9. [追加] ボタンをクリックします。

## 10. 画面左側の [設定反映] 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。

## 大阪事業所を設定する

---

「東京事業所を設定する」を参考に、大阪事業所を設定します。

### LAN0 情報を設定する

#### 「LAN0 情報」 - 「共通情報」

##### 「基本情報」

- インタフェース情報 →物理インタフェース  
シェーピング →使用する  
最大送信レート →1Mbps

#### 「LAN0 情報」 - 「IP 関連」

##### 「帯域制御 (WFQ) 情報」

- プロトコル →すべて
- 送信元情報  
IPアドレス →指定しない  
アドレスマスク →0 (0.0.0.0)  
ポート番号 →指定しない
- あて先情報  
IPアドレス →指定しない  
アドレスマスク →0 (0.0.0.0)  
ポート番号 →指定しない
- 対象TOSフィールド値 →a0
- 帯域 →最優先

## 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 MR1000 機能説明書 [「2.20.1 IPv4 DHCP 機能」](#) (P.76)

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。ここでは、IPv6 DHCP クライアント機能を使用する場合について説明しています。

- IPv6 DHCP サーバ機能
- IPv6 DHCP クライアント機能

☛ 参照 MR1000 機能説明書 [「2.20.2 IPv6 DHCP 機能」](#) (P.78)



## 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

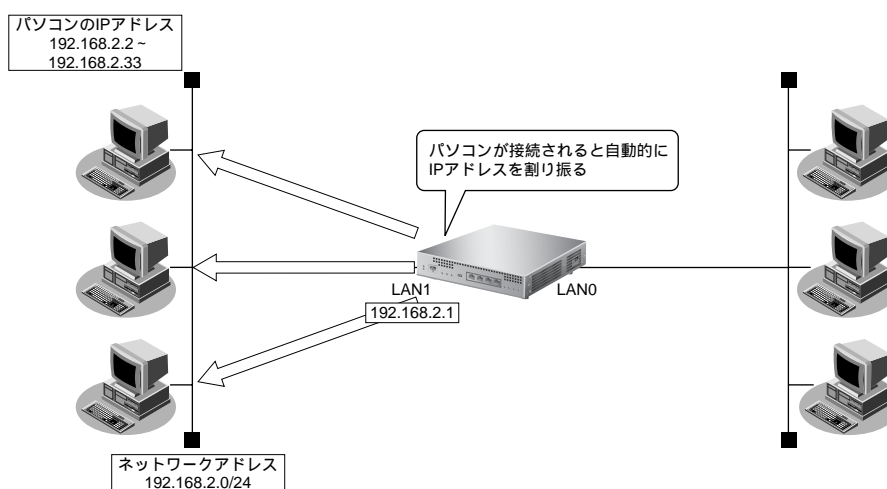
こんな事に気をつけて

- 文字入力フィールドでは半角文字（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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

- 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説明します。



### ● 設定条件

- 本装置のIP アドレス : 192.168.2.1
- 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
- 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設定例を示します。

## DHCPサーバ機能を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。

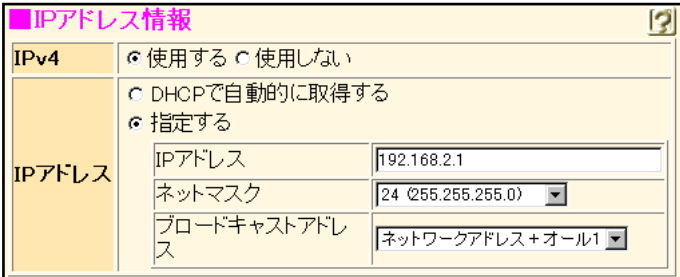
「LAN1 情報（物理 LAN）」ページが表示されます。

### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 4. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →192.168.2.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1



The screenshot shows a configuration window titled "IPアドレス情報" (IP Address Information). It has a yellow background and a question mark icon in the top right corner. The window is divided into two main sections: "IPv4" and "IPアドレス" (IP Address). In the "IPv4" section, the "使用する" (Use) radio button is selected. In the "IPアドレス" section, the "指定する" (Specify) radio button is selected. Below this, there are three input fields: "IPアドレス" with the value "192.168.2.1", "ネットマスク" (Netmask) with a dropdown menu showing "24 (255.255.255.0)", and "ブロードキャストアドレス" (Broadcast Address) with a dropdown menu showing "ネットワークアドレス+オール1".

### 5. 【保存】ボタンをクリックします。

### 6. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

## 7. 以下の項目を指定します。

- DHCP機能 →サーバ機能を使用する
- 割当て先頭IPアドレス → 192.168.2.2
- 割当てアドレス数 → 32



DHCPサーバ機能で割り当てることのできる最大数は253です。

**DHCP情報**
?

DHCP機能

使用しない

リレー機能を使用する

サーバ機能を使用する

割当て先頭IPアドレス	<input type="text" value="192.168.2.2"/>
割当てアドレス数	<input type="text" value="32"/>
リース期間	<input type="text" value="1"/> 日
デフォルトルータ広報	<input type="text"/>
DNSサーバ広報	<input type="text"/>
セカンダリDNSサーバ広報	<input type="text"/>
ドメイン名広報	<input type="text"/>

※“割当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。

必要に応じて上記以外の項目を指定します。

8. [保存] ボタンをクリックします。
9. 画面左側の [設定反映] 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。

## 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。



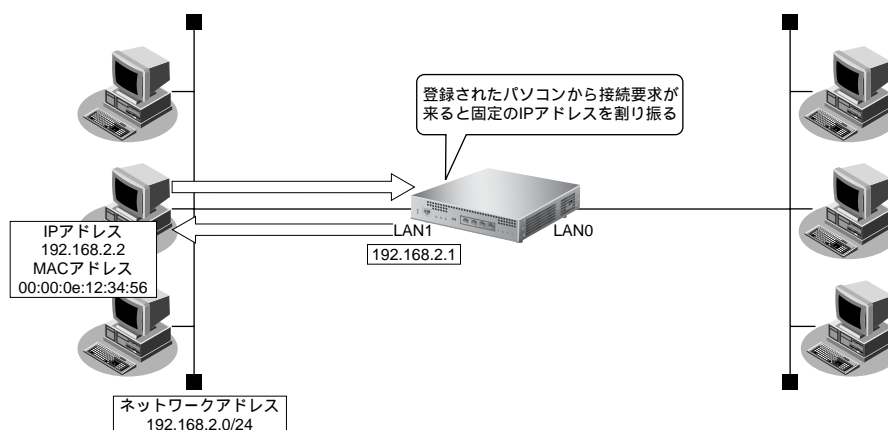
- MAC アドレスとは、LAN 機器に設定されていて世界中で重複されないように管理されている固有のアドレスです。
- 本装置がサポートしている「IP フィルタリング機能」、「マルチルーティング機能」などはパソコンの IP アドレスが固定されていないと使いにくい場合があります。これらの機能と DHCP サーバ機能の併用を実現するために、本装置では「DHCP スタティック機能」をサポートしています。

### こんな事に気をつけて

文字入力フィールドでは半角文字（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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

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。



### ● 設定条件

- ネットワークアドレス/ネットマスク : 192.168.2.0/24
- 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

設定の「LAN0 情報」、「LAN1 情報」で DHCP サーバ機能を使用する設定をしていない場合は、DHCP スタティック機能の設定は有効になりません。

上記の設定条件に従って設定を行う場合の設定例を示します。

## DHCP スタティック機能を設定する

### 1. 設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

### 2. 未設定の欄の【修正】ボタンをクリックします。

「ホストデータベース情報」が表示されます。

### 3. 以下の項目を指定します。

- IPv4 アドレス → 192.168.2.2
- MAC アドレス → 00:00:0e:12:34:56



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。

■ホストデータベース情報					
ホスト名	IPv4アドレス	MACアドレス	電源制御	操作	
	IPv6アドレス				
1	ホスト名				
	IPv4アドレス	192.168.2.2			
	IPv6アドレス				
	MACアドレス	00:00:0e:12:34:56			
	リモート電源制御	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外			

必要に応じて上記以外の項目を指定します。

### 4. 【保存】ボタンをクリックします。

### 5. 画面左側の【設定反映】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。



DHCP スタティック機能で設定できるホストの最大数は 64 です。

## 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。

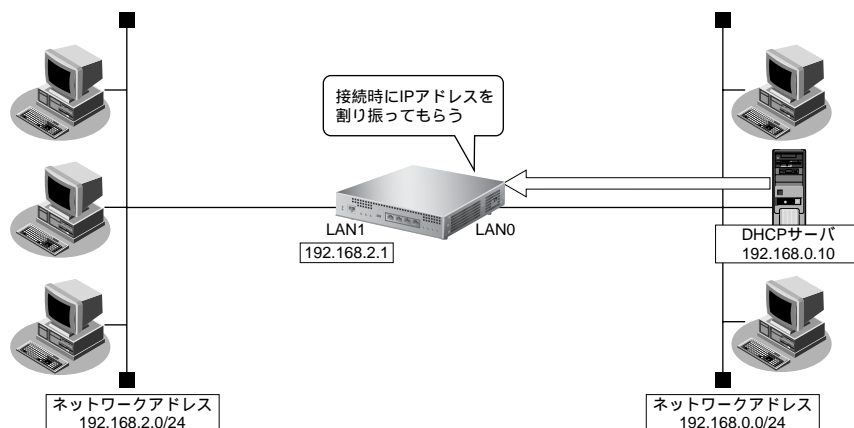
- IPアドレス
- ネットマスク
- リース期間
- デフォルトルータのIPアドレス
- DNSサーバのIPアドレス
- TIMEサーバのIPアドレス
- NTPサーバのIPアドレス

### こんな事に気をつけて

文字入力フィールドでは半角文字 (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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

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

- 本装置のIPアドレス : DHCPサーバから取得する

上記の設定条件に従って設定を行う場合の設定例を示します。

## DHCPクライアント機能を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 4. 以下の項目を指定します。

- IPv4 →使用する
- IP アドレス →DHCPで自動的に取得する

■IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input checked="" type="radio"/> DHCPで自動的に取得する <input type="radio"/> 指定する	
	IPアドレス	<input type="text"/>
	ネットマスク	2 (192.0.0.0)
	ブロードキャストアドレス	0.0.0.0

### 5. [保存] ボタンをクリックします。

### 6. IP 関連の設定項目の「NAT 情報」をクリックします。

「NAT 情報」が表示されます。

### 7. 以下の項目を指定します。

- NAT の使用 →マルチ NAT

■NAT 情報	
NAT の使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチ NAT <input type="radio"/> 静的 NAT のみ ※NATの使用とDHCPリレーサービスの併用はできません

### 8. [保存] ボタンをクリックします。

### 9. 画面左側の [設定反映] 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。

## 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。

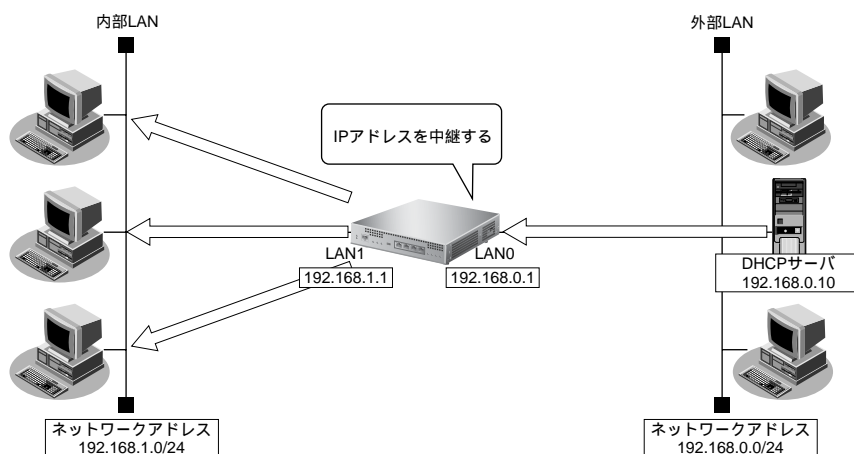
こんな事に気をつけて

文字入力フィールドでは半角文字 (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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

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

##### [内部 LAN 側]

- 本装置の IP アドレス : 192.168.1.1
- DHCP リレーエージェント機能を使用する

##### [外部 LAN 側]

- 本装置の IP アドレス : 192.168.0.1
- DHCP サーバ : 192.168.0.10



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設定例を示します。

## DHCP リレーエージェント機能を設定する

ここでは、LAN1 を使用した場合を例に説明します。LAN0 の場合も同様の手順で設定できます。

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN1 の「修正」ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。

### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 4. IP 関連の設定項目の「DHCP 情報」をクリックします。

「DHCP 情報」が表示されます。

### 5. 以下の項目を指定します。

- DHCP 機能 → リレー機能を使用する
- DHCP サーバ IP アドレス 1 → 192.168.0.10

**DHCP 情報**

使用しない  
 リレー機能を使用する

DHCPサーバIPアドレス1   
 DHCPサーバIPアドレス2

サーバ機能を使用する

割り当て先頭IPアドレス   
 割り当てアドレス数   
 リース期間  日  
 デフォルトルータ広報   
 DNSサーバ広報   
 セカンダリDNSサーバ広報   
 ドメイン名広報

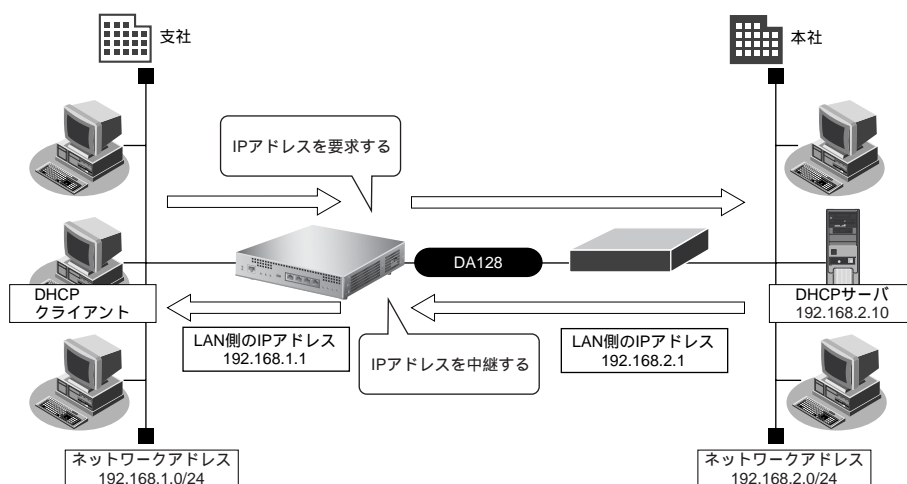
※“割り当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。

### 6. 「保存」ボタンをクリックします。

### 7. 画面左側の「設定反映」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。

## 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
- 支社にDHCPクライアントが存在する
- 本社にDHCPサーバが存在する

#### 【本社】

- ルータの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
- DHCPサーバのIPアドレス : 192.168.2.10

#### 【支社】

- 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

ここでは、本社、支社のネットワークがすでに専用線接続されていることを前提としています。

☞ 参照 「1.8 事業所LANを専用線で接続する」(P.79)

上記の設定条件に従って設定を行う場合の設定例を示します。

## 支社を設定する

### DHCPリレーエージェント機能を設定する

ここでは、LAN0を使用した場合を例に説明します。LAN1の場合も同様の手順で設定できます。

**1. 設定メニューのルータ設定で「LAN情報」をクリックします。**

「LAN情報」ページが表示されます。

**2. 「LAN情報」でインタフェースがLAN0の「修正」ボタンをクリックします。**

「LAN0情報（物理LAN）」ページが表示されます。

**3. 「IP関連」をクリックします。**

IP関連の設定項目と「IPアドレス情報」が表示されます。

**4. IP関連の設定項目の「DHCP情報」をクリックします。**

「DHCP情報」が表示されます。

**5. 以下の項目を指定します。**

- DHCP機能 → リレー機能を使用する
- DHCPサーバIPアドレス1 → 192.168.0.10

**DHCP情報**

使用しない  
 リレー機能を使用する  
 サーバ機能を使用する

DHCPサーバIPアドレス1: 192.168.0.10  
 DHCPサーバIPアドレス2:

サーバ機能を使用する

割り当て先頭IPアドレス:   
 割り当てアドレス数: 32  
 リース期間: 1 日  
 デフォルトルータ広報:   
 DNSサーバ広報:   
 セカンダリDNSサーバ広報:   
 ドメイン名広報:

※“割り当て先頭アドレス”が本装置のIPアドレスと同じネットワークアドレス内であることを確認してください。

**6. 「保存」ボタンをクリックします。**

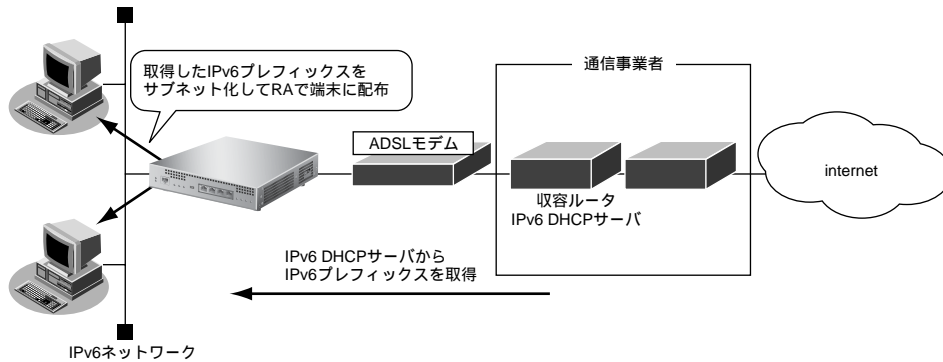
**7. 画面左側の「設定反映」ボタンをクリックします。**

設定した内容が有効になります。

## 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 LAN ポート : LAN0 ポート
- 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 プレフィックスを配布する LAN ポート : LAN1 ポート
- 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設定例を示します。

## IPv6 DHCPクライアントを設定する

1. 「1.6 インターネットへPPPoEで接続する」(P.64) を参考に、PPPoEでの接続を設定します。
2. 設定メニューのルータ設定で「相手情報」をクリックします。  
「相手情報」ページが表示されます。
3. クライアントの設定を行うネットワーク情報の「修正」ボタンをクリックします。  
「ネットワーク情報」が表示されます。
4. 「IPv6関連」をクリックします。  
IPv6関連の設定項目と「IPv6基本情報」が表示されます。

## 5. 以下の項目を指定します。

- IPv6 →使用する

## 6. [保存] ボタンをクリックします。

## 7. IPv6 関連の設定項目の「IPv6 DHCP 情報」をクリックします。

「IPv6 DHCP 情報」が表示されます。

## 8. 以下の項目を指定します。

- DHCP 機能 →クライアント機能を使用する

## 9. [保存] ボタンをクリックします。

## LAN 情報を設定する

## 1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

## 2. 以下の項目を指定します。

- インタフェース →物理 LAN

## 3. [追加] ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

## 4. 「IPv6 関連」をクリックします。

IPv6 関連の設定項目と「IPv6 基本情報」が表示されます。

## 5. 以下の項目を指定します。

- IPv6 →使用する
- IPv6 アドレス  
アドレスまたはプレフィックス → dhcp@rmt0:1::
- ルータ広報 →送信する

**IPv6基本情報** ?

**IPv6**  使用しない  使用する

**インタフェースID**  自動  指定する

	アドレスまたはプレフィックス	Valid Lifetime		Pref. Lifetime		フラグ
		期限有	無期限	期限有	無期限	
<b>IPv6 アドレス</b>	dhcp@rmt0:1::	30	日	7	日	c0
	<input type="text"/>	30	日	7	日	c0
	<input type="text"/>	30	日	7	日	c0
	<input type="text"/>	30	日	7	日	c0

**ルータ広報**  送信しない  送信する

最大送信間隔	<input type="text" value="600"/>	秒
最小送信間隔	<input type="text" value="200"/>	秒
Router Lifetime	<input type="text" value="1800"/>	秒
MTU	<input type="text"/>	
Reachable Time	<input type="text" value="0"/>	ミリ秒
Retrans Timer	<input type="text" value="0"/>	ミリ秒
Cur Hop Limit	<input type="text" value="64"/>	
フラグ	<input type="text" value="00"/>	

## 6. [保存] ボタンをクリックします。

## ProxyDNS を設定する

1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。  
「ProxyDNS 情報 / URL フィルタ情報」ページが表示されます。
2. 「順引き情報」をクリックします。  
「順引き情報」が表示されます。

### 3. 以下の項目を指定します。

- 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

<順引き情報入力フィールド>	
ドメイン名	* <input type="text"/>
タイプ	すべて <input type="checkbox"/> 番号指定 <input type="checkbox"/> “その他”を選択時のみ有効です。)
送信元 IP アドレス	<input type="text"/> / <input type="text"/> ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	<input type="radio"/> 廃棄する <input type="radio"/> 接続先のDNSサーバへ問い合わせる <input type="text" value="ネットワーク名"/> <input type="text" value="rmt0"/>
	<input checked="" type="radio"/> 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 <input type="text" value="ネットワーク名"/> <input type="text" value="rmt0"/>
	<input type="checkbox"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する
	<input type="radio"/> 設定したDNSサーバへ問い合わせる <input type="text" value="DNSサーバアドレス"/>

### 4. [追加] ボタンをクリックします。

### 5. 「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

### 6. 以下の項目を指定します。

- 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

### 7. [追加] ボタンをクリックします。

### 8. 画面左側の [設定反映] 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。

## 2.23 DNS サーバ機能を使う (ProxyDNS)

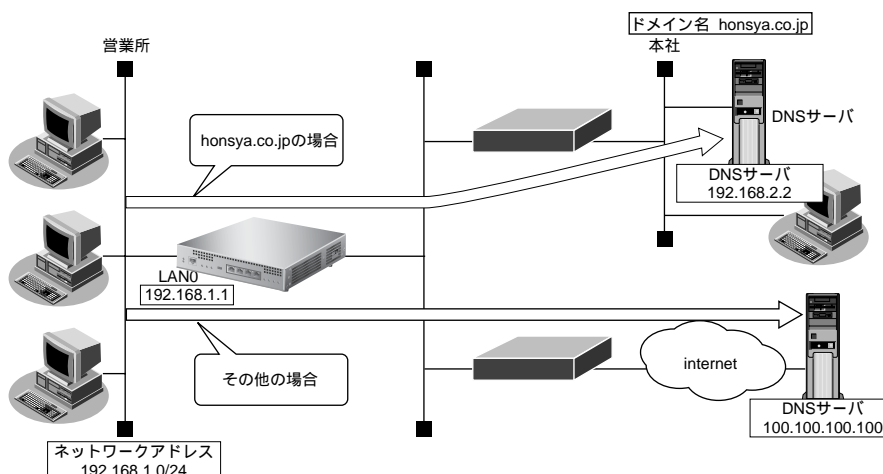
本装置の ProxyDNS には、以下の機能があります。

- 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 MR1000 機能説明書「2.21 DNS サーバ機能」(P.80)

### 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



## 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

文字入力フィールドでは半角文字 (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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

上記の設定条件に従って設定を行う場合の設定例を示します。

## ProxyDNS 情報を設定する

### 1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

「ProxyDNS 情報 / URL フィルタ情報」ページが表示されます。

### 2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

### 3. 以下の項目を指定します。

- ドメイン名 → \* .honsya.co.jp
- 動作 → 設定した DNS サーバへ問い合わせる  
DNS サーバアドレス → 192.168.2.2

<順引き情報入力フィールド>	
ドメイン名	*.honsya.co.jp
タイプ	すべて (番号指定 ( "その他" を選択時のみ有効です。))
送信元 IP アドレス	※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	<input type="radio"/> 廃棄する <input type="radio"/> 接続先のDNSサーバへ問い合わせる ネットワーク名 rmt0
	<input type="radio"/> 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 ネットワーク名 rmt0
	<input type="radio"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する
	<input checked="" type="radio"/> 設定したDNSサーバへ問い合わせる DNSサーバアドレス 192.168.2.2

### 4. [追加] ボタンをクリックします。

### 5. 手順 3. ～ 4. を参考に、以下の項目を指定します。

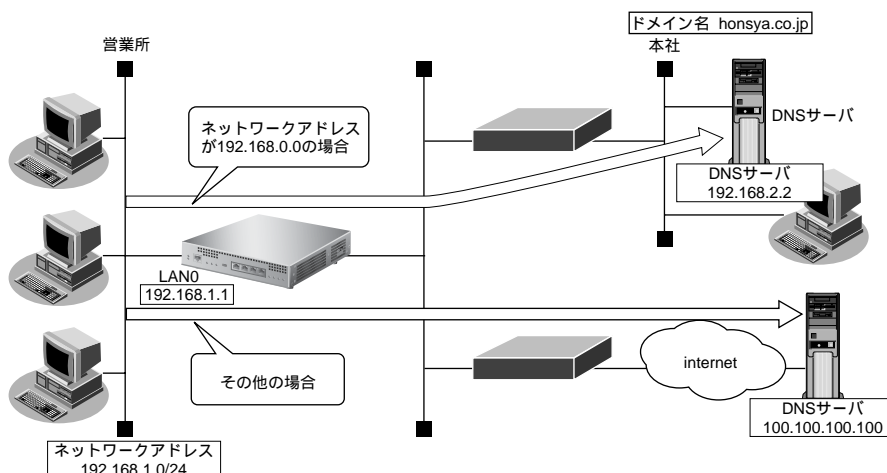
- ドメイン名 → \*
- 動作 → 設定した DNS サーバへ問い合わせる  
DNS サーバアドレス → 100.100.100.100

### 6. 画面左側の [設定反映] 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。

## 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
  - 使用する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
  - 使用する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

## 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

文字入力フィールドでは半角文字 (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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

上記の設定条件に従って設定を行う場合の設定例を示します。

## ProxyDNS 情報を設定する

### 1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

「ProxyDNS 情報 / URL フィルタ情報」ページが表示されます。

### 2. 「逆引き情報」をクリックします。

「逆引き情報」が表示されます。

### 3. 以下の項目を指定します。

- ネットワークアドレス → 指定する  
→ 192.168.0.0/24
- 動作 → 設定した DNS サーバへ問い合わせる  
DNS サーバアドレス → 192.168.2.2

<逆引き情報入力フィールド>	
ネットワークアドレス	指定する (“指定する”を選択時のみ有効です。)
	192.168.0.0 / 24 ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	<input type="radio"/> 廃棄する <input type="radio"/> 接続先のDNSサーバへ問い合わせる ネットワーク名 <input type="text" value="rmt0"/>
	<input type="radio"/> 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 ネットワーク名 <input type="text" value="rmt0"/>
	<input type="radio"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する
	<input checked="" type="radio"/> 設定したDNSサーバへ問い合わせる DNSサーバアドレス <input type="text" value="192.168.2.2"/>

### 4. [追加] ボタンをクリックします。

### 5. 手順3.～4.を参考に、以下の項目を指定します。

- ネットワークアドレス → すべて
- 動作 → 設定した DNS サーバへ問い合わせる  
DNS サーバアドレス → 100.100.100.100

### 6. 画面左側の [設定反映] 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。

## 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DNSサーバアドレスの配布機能（RFC1877）に対応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 : 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

文字入力フィールドでは半角文字（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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置側を設定する

### 1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

「ProxyDNS 情報 / URL フィルタ情報」ページが表示されます。

### 2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

### 3. 以下の項目を指定します。

- 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  
ネットワーク名 → internet (DNSサーバを使用するネットワーク名)

<順引き情報入力フィールド>	
ドメイン名	* <input type="text"/>
タイプ	すべて (番号指定 <input type="text"/> “その他”を選択時のみ有効です。)
送信元IPアドレス	<input type="text"/> / <input type="text"/> ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	<input type="radio"/> 廃棄する
	<input type="radio"/> 接続先のDNSサーバへ問い合わせる ネットワーク名 <input type="text" value="internet"/>
	<input checked="" type="radio"/> 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 ネットワーク名 <input type="text" value="internet"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する
	<input type="radio"/> 設定したDNSサーバへ問い合わせる DNSサーバアドレス <input type="text"/>

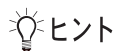
4. [追加] ボタンをクリックします。
5. 画面左側の [設定反映] ボタンをクリックします。  
設定した内容が有効になります。

## パソコン側の設定を行う

---

ここでは、Windows® 2000 の場合を例に説明します。

1. [コントロールパネル] ウィンドウで [ネットワークとダイヤルアップ接続] アイコンをダブルクリックします。
2. [ローカルエリア接続] アイコンを右クリックし、プロパティを選択します。  
[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。
3. 一覧から「インターネットプロトコル (TCP/IP)」をクリックして選択します。
4. [プロパティ] ボタンをクリックします。
5. 「次の DNS サーバーのアドレスを使う」を選択します。
6. 「優先 DNS サーバー」に、本装置の IP アドレスを入力します。
7. [OK] ボタンをクリックします。
8. [はい] ボタンをクリックし、パソコンを再起動します。  
再起動後に、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。

#### ◆ 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？

「ProxyDNS 情報 URL フィルタ情報」－「順引き情報」の動作に“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”を指定した場合は、「解決したホストへのホスト経路自動作成」に“する”を指定することにより、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。

#### ◆ 「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。

## 2.23.4 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、Windows® 2000 が送信する予期しない DNS パケットによって、自動発信する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にすると、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

文字入力フィールドでは半角文字 (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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置側を設定する

### 1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

「ProxyDNS 情報 / URL フィルタ情報」ページが表示されます。

### 2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

### 3. 以下の項目を指定します。

- ドメイン名 → \*
- タイプ → SOA
- 動作 → 廃棄する

<順引き情報入力フィールド>	
ドメイン名	* <input type="text"/>
タイプ	SOA (番号指定 <input type="text"/> “その他”を選択時のみ有効です。)
送信元 IP アドレス	<input type="text"/> / <input type="text"/> ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	<input checked="" type="radio"/> 廃棄する <input type="radio"/> 接続先のDNSサーバへ問い合わせる ネットワーク名 <input type="text" value="rmt0"/> <input type="radio"/> 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 ネットワーク名 <input type="text" value="rmt0"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する <input type="radio"/> 設定したDNSサーバへ問い合わせる DNSサーバアドレス <input type="text"/>

### 4. [追加] ボタンをクリックします。

### 5. 画面左側の [設定反映] 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。

## 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、「DNS サーバアドレスの自動取得機能」の「[パソコン側の設定を行う](#)」(P.525) を参照してください。

## 2.23.5 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

文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

上記の設定条件に従って設定を行う場合の設定例を示します。

## 本装置側を設定する

1. 設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

■ホストデータベース情報					
\	ホスト名	IPv4アドレス	MACアドレス	電源制御	操作
		IPv6アドレス			
1	-	-	-	-	修正 削除
2	-	-	-	-	修正 削除

2. 未設定の欄の【修正】ボタンをクリックします。

「ホストデータベース情報」ページが表示されます。



### 3. 以下の項目を指定します。

- ホスト名 → host.com (パソコンの名前)
- IPv4 アドレス → 192.168.1.2 (パソコンのIP アドレス)
- リモート電源制御 → 対象外



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。

■ホストデータベース情報				
ホスト名	IPv4アドレス	MACアドレス	電源制御	操作
	IPv6アドレス			
1	ホスト名	host.com		
	IPv4アドレス	192.168.1.2		
	IPv6アドレス	2001:db8::2		
	MACアドレス			
	リモート電源制御	<input type="radio"/> 対象 <input checked="" type="radio"/> 対象外		
保存    キャンセル    一覧へ戻る				

### 4. [保存] ボタンをクリックします。

### 5. 画面左側の [設定反映] 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。

## パソコン側の設定を行う

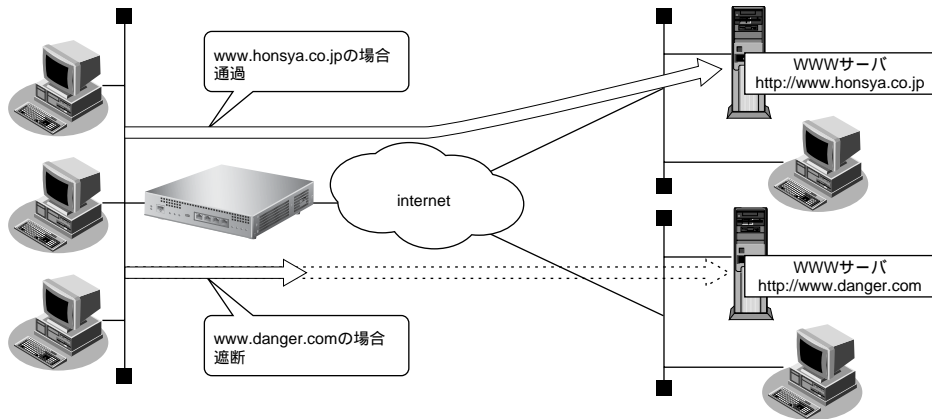
パソコン側の設定を行います。

設定方法は、「DNS サーバアドレスの自動取得機能」の「[パソコン側の設定を行う](#)」(P.525) 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 MR1000 機能説明書「2.21 DNSサーバ機能」(P.80)

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。
- 文字入力フィールドでは、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 MR1000 Webユーザズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

### 💡 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設定例を示します。

## URL フィルタの情報を設定する

### 1. 設定メニューのルータ設定で「ProxyDNS 情報 URL フィルタ情報」をクリックします。

「ProxyDNS 情報 / URL フィルタ情報」ページが表示されます。

### 2. 「順引き情報」をクリックします。

「順引き情報」が表示されます。

### 3. 以下の項目を指定します

- ドメイン名 → www.danger.com
- 動作 → 廃棄する

<順引き情報入力フィールド>	
ドメイン名	<input type="text" value="www.danger.com"/>
タイプ	すべて <input type="checkbox"/> (番号指定 <input type="checkbox"/> “その他”を選択時のみ有効です。)
送信元 IP アドレス	<input type="text"/> ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
動作	<input checked="" type="radio"/> 廃棄する <input type="radio"/> 接続先のDNSサーバへ問い合わせる ネットワーク名 <input type="text" value="rmt0"/> <input type="radio"/> 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 ネットワーク名 <input type="text" value="rmt0"/> 解決したホストへのホスト経路自動作成 <input checked="" type="radio"/> しない <input type="radio"/> する <input type="radio"/> 設定したDNSサーバへ問い合わせる DNSサーバアドレス <input type="text"/>

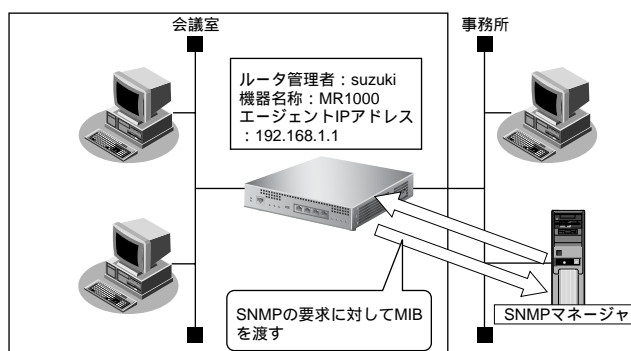
### 4. [追加] ボタンをクリックします。

### 5. 画面左側の [設定反映] ボタンをクリックします。

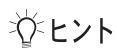
設定した内容が有効になります。

## 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。本装置が SNMP マネージャに対して MIB 情報を通知する場合の設定方法を説明します。



☞ 参照 MR1000 機能説明書「2.22 SNMP 機能」(P.82)



### ヒント

#### ◆ 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 マネージャは、ネットワーク上の端末の稼働状態や障害状況を一元管理します。SNMP エージェントは、マネージャの要求に対して 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 trap という機能を用いて、エージェントからマネージャに対して非同期通知を行うことができます。エージェントは、エージェントが起動されたときに Trap を送信します。

☞ 参照 MR1000 仕様一覧「3.1 標準 MIB 定義」(P.23)、「3.2 Trap 一覧」(P.35)

### こんな事に気をつけて

文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

#### ● 設定条件

- SNMP エージェント機能を使用する
- ルータ管理者 : suzuki
- 機器名称 : MR1000
- 機器設置場所 : 1 階 (1F)
- エージェントアドレス : 192.168.1.1 (自装置 IP アドレス)
- SNMP ホスト名 : public とする (任意のホストを対象とする)

上記の設定条件に従って設定を行う場合の設定例を示します。

## SNMP 情報を設定する

### 1. 設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

### 2. 「SNMP 情報」をクリックします。

「SNMP 情報」が表示されます。

### 3. 以下の項目を指定します。

- SNMP エージェント機能 → 使用する
- ルータ管理者 → suzuki
- 機器名称 → 指定する  
機器名称 → MR1000
- 機器設置場所 → 1F
- エージェントアドレス → 192.168.1.1
- SNMP ホスト1 → public とする（任意のホストを対象とする）
- SNMP ホスト2 → 指定しない

■ SNMP 情報	
SNMP エージェント機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
ルータ管理者	<input type="text" value="suzuki"/>
機器名称	ルータ名称を使用する (ルータ名称情報が設定されていないため選択できません) <input checked="" type="radio"/> 指定する <input type="text" value="機器名称 MR1000"/>
機器設置場所	<input type="text" value="1F"/>
エージェントアドレス	<input type="text" value="192.168.1.1"/>
SNMP ホスト1	<input checked="" type="radio"/> public とする (任意のホストを対象とする) <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IP アドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する
SNMP ホスト2	<input checked="" type="radio"/> 指定しない <input type="radio"/> 指定する コミュニティ名 <input type="text"/> IP アドレス <input type="text"/> トラップ <input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する 書き込み要求 <input checked="" type="radio"/> 許可しない <input type="radio"/> 許可する

### 4. [保存] ボタンをクリックします。

### 5. 画面左側の [設定反映] 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。

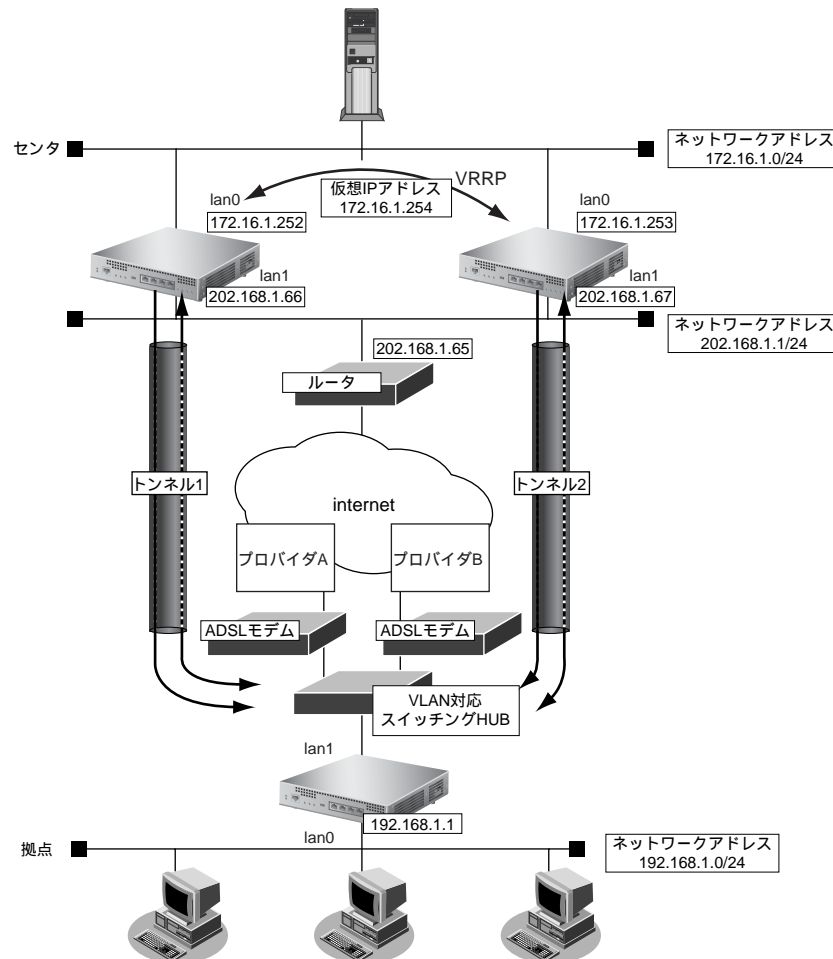
#### こんな事に気をつけて

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 マネージャとの通信ができなくなります。

## 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 MR1000 機能説明書「2.23 ECMP 機能」(P.83)

### ● 設定条件

- 拠点では、センタへの通信は、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設定例を示します。

## センタ側本装置（左）を設定する

### LAN1 側を設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 以下の項目を指定します。

- インタフェース →物理 LAN

3. [追加] ボタンをクリックします。

「LAN1 情報（物理 LAN）」ページが表示されます。

4. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

5. 以下の項目を指定します。

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス → 202.168.1.66
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

6. [保存] ボタンをクリックします。

7. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

**8. 以下の項目を指定します。**

- ネットワーク → デフォルトルート  
中継ルータアドレス → 202.168.1.65
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input checked="" type="radio"/> デフォルトルート
	中継ルータアドレス <input type="text" value="202.168.1.65"/>
	<input type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text"/>
	あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
	中継ルータアドレス <input type="text"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**9. [追加] ボタンをクリックします。****10. IP関連の設定項目の「IPフィルタリング情報」をクリックします。**

「IPフィルタリング情報」が表示されます。



## 11. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 500
- あて先情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 500
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>		
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	
プロトコル	udp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	<input type="text"/>
	アドレスマスク	0 (0.0.0.0)
	ポート番号	500
あて先情報	IPアドレス	202.168.1.66
	アドレスマスク	32 (255.255.255.255)
	ポート番号	500
ICMP	タイプ	<input type="text"/>
	コード	<input type="text"/>
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	
TOS	<input type="text"/>	
方向	入出力	

## 12. [追加] ボタンをクリックします。

**13. 手順 11. ~ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 500
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 500
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**14. 手順 11. ~ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → その他 (50)
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**15. 手順 11. ～ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → その他 (50)
- 送信元情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**16. 手順 11. ～ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## トンネルを設定する

### 17. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 18. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 19. 以下の項目を指定します。

- ネットワーク名 → RMTbyA

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="RMTbyA"/>

### 20. [追加] ボタンをクリックします。


「ネットワーク情報 (RMTbyA)」が表示されます。

### 21. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

### 22. 以下の項目を指定します。

- MTU サイズ → 1400

<b>■基本情報</b> 	
ネットワーク名	<input type="text" value="RMTbyA"/>
MTUサイズ	<input type="text" value="1400"/> バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps

### 23. [保存] ボタンをクリックします。

### 24. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

**25. 以下の項目を指定します。**

- MSS書き換え →使用する  
書き換えサイズ →1360

■ IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する
	相手側IPアドレス <input type="text"/> 自側IPアドレス <input type="text"/>
MSS書き換え	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	書き換えサイズ <input type="text" value="1360"/> バイト

**26. [保存] ボタンをクリックします。****27. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**28. 以下の項目を指定します。**

- ネットワーク →ネットワーク指定  
あて先IPアドレス →192.168.1.0  
あて先アドレスマスク →24 (255.255.255.0)
- メトリック値 →1
- 優先度 →0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**29. [追加] ボタンをクリックします。****30. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

### 31. 以下の項目を指定します。

- 接続先名 → IPsecbyA
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>

接続先名	IPsecbyA
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 <div style="display: flex; align-items: center;"> <input type="text" value="ダイヤル1"/> <input type="text" value="電話番号"/> </div> <div style="display: flex; align-items: center;"> <input type="text" value="サブアドレス"/> </div> <input type="radio"/> フレームリレー接続 <input type="text" value="DLCI"/> <input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input checked="" type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

### 32. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

### 33. 以下の項目を指定します。

- 鍵交換モード → Aggressive Mode(Responder) 使用
- 自側エンドポイント → 202.168.1.66
- 相手装置識別情報 → RMTbyA
- IDタイプ → FQDN

鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Responder)使用	
	自側エンドポイント	202.138.1.66
	相手側エンドポイント	
	相手装置識別情報	RMTbyA
IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN	

### 34. [保存] ボタンをクリックします。

### 35. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

### 36. 以下の項目を指定します。

- 対象パケット
  - 自側IP アドレス/マスク → IPv4 すべて
  - 相手側IP アドレス/マスク → IPv4 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5
  - PFS時のDH グループ → modp1536 (グループ5)
  - SA有効時間 → 8時間
- SA更新
  - Responder 時 → 更新する
  - 時間 → 30

■ IPsec情報(自動鍵)		?
対象パケット	自側IPアドレス/マスク	IPv4すべて (<"指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくは(IPv6アドレス/プレフィックス長形式で入力してください。)
	相手側IPアドレス/マスク	IPv4すべて (<"指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくは(IPv6アドレス/プレフィックス長形式で入力してください。)
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	modp1536(グループ5)
	SA有効時間	8 時間
	SA有効データ量	0 GByte
SA更新	Initiator 時間	90 秒
	Initiator データ量	0 MByte
	Responder時	<input type="radio"/> 更新しない <input checked="" type="radio"/> 更新する 時間 30 秒 データ量 0 MByte

### 37. [保存] ボタンをクリックします。

### 38. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

### 39. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → 12345678-A

■ IKE情報		?
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****

40. [保存] ボタンをクリックします。

41. IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

42. 以下の項目を指定します。

- 接続先監視 → 使用する
- 送信元IPアドレス → 172.16.1.252
- あて先IPアドレス → 192.168.1.1
- 正常時送信間隔 → 5 秒
- 再送間隔 → 1 秒
- タイムアウト時間 → 5 秒
- 異常時送信間隔 → 1 分

43. [保存] ボタンをクリックします。

### LAN0 側を設定する

44. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

45. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

46. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

47. 以下の項目を指定します。

- VRRP 機能 → 使用する

48. [保存] ボタンをクリックします。

49. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

「VRRP グループ情報」が表示されます。



**50. 「VRRPグループ情報」でグループ番号が0の「修正」ボタンをクリックします。**

VRRPグループ情報の設定項目と「基本情報」が表示されます。

**51. 以下の項目を指定します。**

- グループID → 10
- プライオリティ → バックアップ
  - 優先度 → 254
  - 仮想IPアドレス → 172.16.1.254

**52. 「保存」ボタンをクリックします。****53. VRRPグループ情報の設定項目の「VRRPトリガ情報」をクリックします。**

「VRRPトリガ情報」が表示されます。

**54. 以下の項目を指定します。**

- 減算プライオリティ → 254
- トリガ種別 → インタフェースダウントリガ (ifdown)
  - インタフェース → RMTbyA

**55. 「追加」ボタンをクリックします。****56. 画面上部の「LAN0情報」をクリックします。**

「LAN0情報（物理LAN）」ページが表示されます。

**57. 「IP関連」をクリックします。**

IP関連の設定項目と「IPアドレス情報」が表示されます。

**58. 以下の項目を指定します。**

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス → 172.16.1.252
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス+オール1

■ IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する	
	IPアドレス	172.16.1.252
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス+オール1

**59. [保存] ボタンをクリックします。****60. 画面左側の [設定反映] 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。

## センタ側本装置（右）を設定する

### LAN1側を設定する

**1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**2. 以下の項目を指定します。**

- インタフェース →物理 LAN

<LAN情報追加フィールド>	
インタフェース	物理LAN

**3. [追加] ボタンをクリックします。**

「LAN1 情報 (物理 LAN)」ページが表示されます。

**4. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

## 5. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →202.168.1.67
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■ IPアドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPアドレス	<input type="radio"/> DHCPで自動的に取得する
	<input checked="" type="radio"/> 指定する
	IPアドレス <input type="text" value="202.168.1.67"/>
	ネットマスク <input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス <input type="text" value="ネットワークアドレス+オール1"/>

## 6. [保存] ボタンをクリックします。

## 7. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

## 8. 以下の項目を指定します。

- ネットワーク →デフォルトルート
  - 中継ルータアドレス →202.168.1.65
- メトリック値 →1
- 優先度 →0

<スタティック経路情報入力フィールド>	
ネットワーク	<input checked="" type="radio"/> デフォルトルート
	中継ルータアドレス <input type="text" value="202.168.1.65"/>
	<input type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text"/>
	あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
	中継ルータアドレス <input type="text"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

## 9. [追加] ボタンをクリックします。

## 10. IP関連の設定項目の「IPフィルタリング情報」をクリックします。

「IPフィルタリング情報」が表示されます。

## 11. 以下の項目を指定します。

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 500
- あて先情報
  - IPアドレス → 202.168.1.67
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 500
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

＜IPフィルタリング情報入力フィールド＞		
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断	
プロトコル	udp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	500
あて先情報	IPアドレス	202.168.1.67
	アドレスマスク	32 (255.255.255.255)
	ポート番号	500
ICMP	タイプ	
	コード	
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	
TOS		
方向	入出力	

## 12. [追加] ボタンをクリックします。

**13. 手順 11. ～ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 202.168.1.67
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 500
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 500
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**14. 手順 11. ～ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → その他 (50)
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 202.168.1.67
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**15. 手順 11. ～ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → その他 (50)
- 送信元情報
  - IPアドレス → 202.168.1.67
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**16. 手順 11. ～ 12. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

## トンネルを設定する

### 17. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 18. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 19. 以下の項目を指定します。

- ネットワーク名 → RMTbyB

<ネットワーク情報追加フィールド>	
ネットワーク名	RMTbyB

### 20. [追加] ボタンをクリックします。

「ネットワーク情報 (RMTbyB)」が表示されます。

### 21. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

### 22. 以下の項目を指定します。

- MTU サイズ → 1400

<b>■基本情報</b>	
ネットワーク名	RMTbyB
MTUサイズ	1400 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps

### 23. [保存] ボタンをクリックします。

### 24. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

**25. 以下の項目を指定します。**

- MSS 書き換え →使用する  
書き換えサイズ → 1360

■IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する
	相手側IPアドレス <input type="text"/> 自側IPアドレス <input type="text"/>
MSS書き換え	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	書き換えサイズ <input type="text" value="1360"/> バイト

**26. [保存] ボタンをクリックします。****27. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**28. 以下の項目を指定します。**

- ネットワーク →ネットワーク指定  
あて先IP アドレス → 192.168.1.0  
あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**29. [追加] ボタンをクリックします。****30. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。



### 31. 以下の項目を指定します。

- 接続先名 → IPsecbyB
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>

接続先名: IPsecbyB

接続先種別:

- 専用線接続
- ISDN接続
- ダイヤル1:  電話番号:
- サブアドレス:
- フレームリレー接続
- DLCI:
- PPPoE接続
- IPTunnel接続
- IPsec/IKE接続
- 別インタフェースから送出
- MPLSTunnel接続
- パケット破棄

### 32. [追加] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

### 33. 以下の項目を指定します。

- 鍵交換モード → Aggressive Mode(Responder) 使用
- 自側エンドポイント → 202.168.1.67
- 相手装置識別情報 → RMTbyB
- IDタイプ → FQDN

鍵交換モード

- Aggressive Mode(Responder)使用
- 自側エンドポイント: 202.168.1.67
- 相手側エンドポイント:
- 相手装置識別情報: RMTbyB
- IDタイプ:  FQDN  User-FQDN

### 34. [保存] ボタンをクリックします。

### 35. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。

「IPsec 情報」が表示されます。

## 36. 以下の項目を指定します。

- 対象パケット
  - 自側IPアドレス/マスク → IPv4 すべて
  - 相手側IPアドレス/マスク → IPv4 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5
  - PFS時のDHグループ → modp1536 (グループ5)
  - SA有効時間 → 8時間
- SA更新
  - Responder時 → 更新する
  - 時間 → 30

■ IPsec情報(自動鍵)		?
対象パケット	自側IPアドレス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	modp1536(グループ5)
	SA有効時間	8 時間
	SA有効データ量	0 GByte
SA更新	Initiator時	時間: 90 秒 データ量: 0 MByte
	Responder時	<input type="radio"/> 更新しない <input checked="" type="radio"/> 更新する 時間: 30 秒 データ量: 0 MByte

## 37. [保存] ボタンをクリックします。

## 38. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

**39. 以下の項目を指定します。**

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → 12345678-B

■ IKE情報		
IKE認証鍵	鍵種別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****

**40. [保存] ボタンをクリックします。****41. IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。**

「接続制御情報」が表示されます。

**42. 以下の項目を指定します。**

- 接続先監視 → 使用する
- 送信元IPアドレス → 172.16.1.253
- あて先IPアドレス → 192.168.1.1
- 正常時送信間隔 → 5秒
- 再送間隔 → 1秒
- タイムアウト時間 → 5秒
- 異常時送信間隔 → 1分

■ 接続制御情報		
接続先監視	<input type="radio"/> 使用しない	
	<input checked="" type="radio"/> 使用する	
	送信元IPアドレス	172.16.1.253
	あて先IPアドレス	192.168.1.1
	正常時送信間隔	5 秒
	再送間隔	1 秒
	タイムアウト時間	5 秒
	異常時送信間隔	1 分
	送信 TTL/HopLimit	255
監視方式	<input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視	

**43. [保存] ボタンをクリックします。****LAN0側を設定する****44. 設定メニューのルータ設定の「LAN情報」をクリックします。**

「LAN情報」ページが表示されます。

**45. 「LAN情報」でインターフェースがLAN0の【修正】ボタンをクリックします。**

「LAN0情報 (物理LAN)」ページが表示されます。

**46. 「共通情報」をクリックします。**

共通情報に関する設定項目と「基本情報」が表示されます。

## 47. 以下の項目を指定します。

- VRRP 機能 →使用する

VRRP機能	<input type="radio"/> 使用しない
	<input checked="" type="radio"/> 使用する
	パスワード <input type="text"/>

## 48. [保存] ボタンをクリックします。

## 49. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

「VRRP グループ情報」が表示されます。

## 50. 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

## 51. 以下の項目を指定します。

- グループID →10
- プライオリティ →バックアップ
  - 優先度 →100
  - 仮想IPアドレス →172.16.1.254

■基本情報	
グループID	<input type="text" value="10"/>
プライオリティ	<input type="radio"/> マスタ(255)
	<input checked="" type="radio"/> バックアップ
	優先度 <input type="text" value="100"/>
	仮想IPアドレス <input type="text" value="172.16.1.254"/>

## 52. [保存] ボタンをクリックします。

## 53. VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

## 54. 以下の項目を指定します。

- 減算プライオリティ →254
- トリガ種別 →インタフェースダウントリガ (ifdown)
  - インタフェース →RMTbyB

<VRRPトリガ情報入力フィールド>	
減算プライオリティ	<input type="text" value="254"/>
トリガ種別	<input checked="" type="radio"/> インタフェースダウントリガ (ifdown)
	インタフェース <input type="text" value="RMTbyB"/>

## 55. [追加] ボタンをクリックします。

## 56. 画面上部の「LAN0 情報」をクリックします。

「LAN0情報 (物理 LAN)」ページが表示されます。

**57. 「IP関連」をクリックします。**

IP関連の設定項目と「IPアドレス情報」が表示されます。

**58. 以下の項目を指定します。**

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →172.16.1.253
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■ IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する	
	IPアドレス	172.16.1.253
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス+オール1

**59. [保存] ボタンをクリックします。****60. 画面左側の [設定反映] 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。

## 拠点側本装置を設定する

---

### PPPoEで利用するLANを設定する

**1. 設定メニューのルータ設定で、「LAN情報」をクリックします。**

「LAN情報」ページが表示されます。

**2. 以下の項目を指定します。**

- インタフェース →物理LAN

<LAN情報追加フィールド>	
インタフェース	物理LAN

**3. [追加] ボタンをクリックします。**

「LAN1情報 (物理LAN)」ページが表示されます。

**4. 設定メニューのルータ設定で、「LAN情報」をクリックします。**

「LAN情報」ページが表示されます。

## 5. 以下の項目を指定します。

- インタフェース → VLAN

<LAN情報追加フィールド>	
インタフェース	VLAN

## 6. [追加] ボタンをクリックします。

「LAN2情報 (VLAN)」ページが表示されます。

## 7. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

## 8. 以下の項目を指定します。

- 出力先 → LAN1
- VLAN ID → 10

■基本情報	
出力先	LAN1
VLAN ID	10
プライオリティ	0
VRRP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する パスワード <input type="text"/>
MTUサイズ	1500 バイト

## 9. [保存] ボタンをクリックします。

## 10. 手順 4. ～ 9. を参考に、以下の項目を指定します。

「LAN3情報 (VLAN)」 — 「共通情報」

- 出力先 → LAN1
- VLAN ID → 20

## プロバイダ A を利用する PPPoE 接続を設定する

## 11. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 12. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

## 13. 以下の項目を指定します。

- ネットワーク名 → INTER-A

<ネットワーク情報追加フィールド>	
ネットワーク名	INTER-A

## 14. [追加] ボタンをクリックします。

「ネットワーク情報 (INTER-A)」が表示されます。

**15. 「共通情報」をクリックします。**

共通情報の設定項目と「基本情報」が表示されます。

**16. 以下の項目を指定します。**

- MTU サイズ → 1454

■基本情報	
ネットワーク名	INTER-A
MTUサイズ	1454 バイト

**17. [保存] ボタンをクリックします。****18. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**19. 以下の項目を指定します。**

- MSS 書き換え → 使用する
- 書き換えサイズ → 1414

■IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する
	相手側IPアドレス <input type="text"/> 自側IPアドレス <input type="text"/>
	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
MSS書き換え	書き換えサイズ <input type="text" value="1414"/> バイト

**20. [保存] ボタンをクリックします。****21. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**22. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 202.168.1.66
- あて先アドレスマスク → 32 (255.255.255.255)
- メトリック値 → 1
- 優先度 → 0

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="202.168.1.66"/> あて先アドレスマスク <input type="text" value="32 (255.255.255.255)"/>
	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**23. [追加] ボタンをクリックします。**

**24. IP関連の設定項目の「IPフィルタリング情報」をクリックします。**

「IPフィルタリング情報」が表示されます。

**25. 以下の項目を指定します。**

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 500
- あて先情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 500
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

<IPフィルタリング情報入力フィールド>		
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断	
プロトコル	udp (番号指定: <input type="checkbox"/> “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	500
あて先情報	IPアドレス	202.168.1.66
	アドレスマスク	32 (255.255.255.255)
	ポート番号	500
ICMP	タイプ	
	コード	
TCP接続要求	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外	
TOS		
方向	入出力	

**26. [追加] ボタンをクリックします。**



**27. 手順 25. ~ 26. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → udp
- 送信元情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 500
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 500
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**28. 手順 25. ~ 26. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → その他 (50)
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**29. 手順 25. ～ 26. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」

- 動作 → 透過
- プロトコル → その他 (50)
- 送信元情報
  - IPアドレス → 202.168.1.66
  - アドレスマスク → 32 (255.255.255.255)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**30. 手順 25. ～ 26. を参考に、以下の項目を指定します。**

「IPフィルタリング情報」


- 動作 → 遮断
- プロトコル → すべて
- 送信元情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- あて先情報
  - IPアドレス → 指定しない
  - アドレスマスク → 0 (0.0.0.0)
  - ポート番号 → 指定しない
- ICMP
  - タイプ → 指定しない
  - コード → 指定しない
- TCP 接続要求 → 対象
- TOS → 指定しない
- 方向 → 入出力

**31. IP関連の設定項目の「NAT 情報」をクリックします。**

「NAT 情報」が表示されます。

**32. 以下の項目を指定します。**

- NATの使用 → マルチ NAT

■ NAT 情報 	
NATの使用	<input type="radio"/> 使用しない <input type="radio"/> NAT <input checked="" type="radio"/> マルチ NAT <input type="radio"/> 静的 NATのみ

33. [保存] ボタンをクリックします。

34. IP関連の設定項目の「静的NAT情報」をクリックします。

「静的NAT情報」が表示されます。

35. 以下の項目を指定します。

- プライベートIP情報
  - IPアドレス → 192.168.1.1
  - ポート番号 → isakmp
- グローバルIP情報
  - IPアドレス → 指定しない
  - ポート番号 → isakmp
- プロトコル → udp

<静的NAT情報入力フィールド>		
プライベートIP情報	IPアドレス	192.168.1.1
	ポート番号	isakmp (番号指定: [ ] "その他"を選択時のみ有効です)
グローバルIP情報	IPアドレス	[ ]
	ポート番号	isakmp (番号指定: [ ] "その他"を選択時のみ有効です)
プロトコル		udp (番号指定: [ ] "その他"を選択時のみ有効です)

36. [追加] ボタンをクリックします。

37. 手順 35. ~ 36. を参考に、以下の項目を指定します。

- プライベートIP情報
  - IPアドレス → 192.168.1.1
  - 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

38. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 39. 以下の項目を指定します。

- 接続先名 → ISP-A
- 接続先種別 → PPPoE 接続

<接続先情報追加フィールド>

接続先名: ISP-A

接続先種別:

- 専用線接続
- ISDN接続
- ダイヤル1:  電話番号:
- サブアドレス:
- フレームリレー接続
- DLCI:
- PPPoE接続
- IPトンネル接続
- IPsec/IKE接続
- 別インタフェースから送出
- MPLSトンネル接続
- パケット破棄

## 40. [追加] ボタンをクリックします。

PPPoE 接続の設定項目と「基本情報」が表示されます。

## 41. 以下の項目を指定します。

- 使用インタフェース → LAN2

■基本情報

接続先名: ISP-A

使用インタフェース: LAN2

DNSサーバ:

## 42. [保存] ボタンをクリックします。

## 43. PPPoE 接続の設定項目の「PPP 情報」をクリックします。

「PPP 情報」が表示されます。

## 44. 以下の項目を指定します。

- 送信認証情報
  - 認証 ID → UIDtoA
  - 認証パスワード → PASStoA

■PPP情報

送信認証情報:

- 認証ID: UIDtoA
- 認証パスワード: \*\*\*\*\*

## 45. [保存] ボタンをクリックします。

## プロバイダ B を利用する PPPoE 接続を設定する

**46. 手順 11. ~45. を参考に、以下の項目を指定します。****「相手情報」 - 「ネットワーク情報」**

- ネットワーク名 → INTER-B

**「ネットワーク情報」 - 「IP 関連」****「スタティック経路情報」**

- ネットワーク → ネットワーク指定
- あて先 IP アドレス → 202.168.1.67
- あて先アドレスマスク → 32 (255.255.255.255)
- メトリック値 → 1
- 優先度 → 0

**「IP フィルタリング情報」**

- 動作 → 透過
  - プロトコル → udp
  - 送信元情報
    - IP アドレス → 指定しない
    - アドレスマスク → 0 (0.0.0.0)
    - ポート番号 → 500
  - あて先情報
    - IP アドレス → 202.168.1.67
    - アドレスマスク → 32 (255.255.255.255)
    - ポート番号 → 500
  - ICMP
    - タイプ → 指定しない
    - コード → 指定しない
  - TCP 接続要求 → 対象
  - TOS → 指定しない
  - 方向 → 入出力
- 
- 動作 → 透過
  - プロトコル → udp
  - 送信元情報
    - IP アドレス → 202.168.1.67
    - アドレスマスク → 32 (255.255.255.255)
    - ポート番号 → 500
  - あて先情報
    - IP アドレス → 指定しない
    - アドレスマスク → 0 (0.0.0.0)
    - ポート番号 → 500
  - ICMP
    - タイプ → 指定しない
    - コード → 指定しない
  - TCP 接続要求 → 対象
  - TOS → 指定しない
  - 方向 → 入出力

- 動作 →透過
  - プロトコル →その他 (50)
  - 送信元情報
    - IPアドレス →指定しない
    - アドレスマスク →0 (0.0.0.0)
    - ポート番号 →指定しない
  - あて先情報
    - IPアドレス →202.168.1.67
    - アドレスマスク →32 (255.255.255.255)
    - ポート番号 →指定しない
  - ICMP
    - タイプ →指定しない
    - コード →指定しない
  - TCP 接続要求 →対象
  - TOS →指定しない
  - 方向 →入出力
- 
- 動作 →透過
  - プロトコル →その他 (50)
  - 送信元情報
    - IPアドレス →202.168.1.67
    - アドレスマスク →32 (255.255.255.255)
    - ポート番号 →指定しない
  - あて先情報
    - IPアドレス →指定しない
    - アドレスマスク →0 (0.0.0.0)
    - ポート番号 →指定しない
  - ICMP
    - タイプ →指定しない
    - コード →指定しない
  - TCP 接続要求 →対象
  - TOS →指定しない
  - 方向 →入出力

- 動作 →遮断
- プロトコル →すべて
- 送信元情報
  - IPアドレス →指定しない
  - アドレスマスク →0 (0.0.0.0)
  - ポート番号 →指定しない
- あて先情報
  - IPアドレス →指定しない
  - アドレスマスク →0 (0.0.0.0)
  - ポート番号 →指定しない
- ICMP
  - タイプ →指定しない
  - コード →指定しない
- TCP 接続要求 →対象
- TOS →指定しない
- 方向 →入出力

#### 「ネットワーク情報」 - 「接続先情報」

- 接続先名 →ISP-B

#### 「基本情報」

- 使用インタフェース →LAN3

#### 「PPP情報」

- 送信認証情報
  - 認証ID →UIDtoB
  - 認証パスワード →PASStoB

## センタ側本装置 (左) とのトンネルを設定する

### 47. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 48. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 49. 以下の項目を指定します。

- ネットワーク名 →CENTER-A

<ネットワーク情報追加フィールド>	
ネットワーク名	CENTER-A

### 50. [追加] ボタンをクリックします。

「ネットワーク情報 (CENTER-A)」が表示されます。

### 51. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

## 52. 以下の項目を指定します。

- MTU サイズ → 1400

■基本情報	
ネットワーク名	CENTER-A
MTUサイズ	1400 バイト
自動接続	<input checked="" type="radio"/> する <input type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps

## 53. [保存] ボタンをクリックします。

## 54. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

## 55. 以下の項目を指定します。

- MSS 書き換え → 使用する  
書き換えサイズ → 1360

■IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する
	相手側IPアドレス <input type="text"/> 自側IPアドレス <input type="text"/>
MSS書き換え	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する 書き換えサイズ 1360 バイト

## 56. [保存] ボタンをクリックします。

## 57. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

## 58. 以下の項目を指定します。

- ネットワーク → ネットワーク指定  
あて先IPアドレス → 172.16.1.0  
あて先アドレスマスク → 24 (255.255.255.0)
- メトリック値 → 1
- 優先度 → 1

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text"/> 172.16.1.0 あて先アドレスマスク <input type="text"/> 24 (255.255.255.0)
メトリック値	<input type="text"/> 1
優先度	<input type="text"/> 1

## 59. [追加] ボタンをクリックします。



**60. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**61. 以下の項目を指定します。**

- 接続先名 → IPsecbyA
- 接続先種別 → IPsec/IKE 接続

<接続先情報追加フィールド>

接続先名	IPsecbyA	
接続先種別	<input type="radio"/> 専用線接続	
	<input type="radio"/> ISDN接続	
	ダイヤル1	電話番号 <input type="text"/>
		サブアドレス <input type="text"/>
接続先種別	<input type="radio"/> フレームリレー接続	
	DLCI	<input type="text"/>
接続先種別	<input type="radio"/> PPPoE接続	
	<input type="radio"/> IPTunnel接続	
	<input checked="" type="radio"/> IPsec/IKE接続	
	<input type="radio"/> 別インターフェースから送出	
	<input type="radio"/> MPLSTunnel接続	
	<input type="radio"/> パケット破棄	

**62. [追加] ボタンをクリックします。**

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

**63. 以下の項目を指定します。**

- 鍵交換モード → Aggressive Mode(Initiator) 使用
- 相手側エンドポイント → 202.168.1.66
- 自装置識別情報 → RMTbyA
- IDタイプ → FQDN

鍵交換モード	<input checked="" type="radio"/> Aggressive Mode(Initiator)使用	
	自側エンドポイント	<input type="text"/>
	相手側エンドポイント	202.168.1.66
	自装置識別情報	RMTbyA
	IDタイプ	<input checked="" type="radio"/> FQDN <input type="radio"/> User-FQDN

**64. [保存] ボタンをクリックします。****65. IPsec/IKE 接続の設定項目の「IPsec 情報」をクリックします。**

「IPsec 情報」が表示されます。

## 66. 以下の項目を指定します。

- 対象パケット
  - 自側IPアドレス/マスク → IPv4 すべて
  - 相手側IPアドレス/マスク → IPv4 すべて
- SAの設定
  - 暗号アルゴリズム → des-cbc
  - 認証アルゴリズム → hmac-md5
  - PFS時のDHグループ → modp1536 (グループ5)
  - SA有効時間 → 8時間
- SA更新
  - Initiator時
    - 時間 → 90
  - Responder時
    - 更新する
    - 時間 → 90

■ IPsec情報(自動鍵)		
対象パケット	自側IPアドレス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
	相手側IPアドレス/マスク	IPv4すべて ("指定する"を選択時のみ有効です。) ※IPv4アドレス/マスクビット形式もしくはIPv6アドレス/プレフィックス長形式で入力してください。
SAの設定	暗号アルゴリズム	<input checked="" type="checkbox"/> des-cbc <input type="checkbox"/> 3des-cbc <input type="checkbox"/> aes-cbc <input type="checkbox"/> null
	認証アルゴリズム	<input checked="" type="checkbox"/> hmac-md5 <input type="checkbox"/> hmac-sha1 <input type="checkbox"/> 認証なし
	PFS時のDHグループ	modp1536(グループ5)
	SA有効時間	8 時間
	SA有効データ量	0 GByte
SA更新	Initiator時	時間 90 秒 データ量 0 MByte
	Responder時	<input type="radio"/> 更新しない <input checked="" type="radio"/> 更新する 時間 90 秒 データ量 0 MByte

## 67. [保存] ボタンをクリックします。

## 68. IPsec/IKE 接続の設定項目の「IKE 情報」をクリックします。

「IKE 情報」が表示されます。

## 69. 以下の項目を指定します。

- IKE 認証鍵
  - 鍵種別 → 文字列
  - 鍵 → 12345678-A

■IKE情報		
IKE認証鍵	鍵識別	<input type="radio"/> 16進数 <input checked="" type="radio"/> 文字列
	鍵	*****

## 70. [保存] ボタンをクリックします。

## 71. IPsec/IKE 接続の設定項目の「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

## 72. 以下の項目を指定します。

- 接続先監視 → 使用する
- 送信元IPアドレス → 192.168.1.1
- あて先IPアドレス → 172.16.1.252
- 正常時送信間隔 → 5 秒
- 再送間隔 → 1 秒
- タイムアウト時間 → 5 秒
- 異常時送信間隔 → 1 分

■接続制御情報		
接続先監視	<input type="radio"/> 使用しない	
	<input checked="" type="radio"/> 使用する	
	送信元IPアドレス	192.168.1.1
	あて先IPアドレス	172.16.1.252
	正常時送信間隔	5 秒
	再送間隔	1 秒
	タイムアウト時間	5 秒
	異常時送信間隔	1 分
	送信 TTL/HopLimit	255
監視方式	<input checked="" type="radio"/> 常時監視 <input type="radio"/> 無通信時監視	

## 73. [保存] ボタンをクリックします。

## センタ側本装置（右）とのトンネルを設定する

74. 手順 47.～73.を参考に、以下の項目を指定します。

### 「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → CENTER-B

### 「ネットワーク情報」 - 「接続先情報」

- 接続先名 → IPsecbyB

### 「接続先情報」 - 「IPsec/IKE 接続」

#### 「基本情報」

- 相手側エンドポイント → 202.168.1.67
- 自装置識別情報 → RMTbyB

#### 「IKE 情報」

- 鍵 → 12345678-B

#### 「接続制御情報」

- あて先IP アドレス → 172.16.1.253

## ECMPを設定する

75. 設定メニューのルータ設定の「ルーティングプロトコル情報」をクリックします。

「ルーティングプロトコル情報」ページが表示されます。

76. 「ルーティングマネージャ情報」をクリックします

ルーティングマネージャ情報の設定項目と「再配布情報」が表示されます。

77. ルーティングマネージャ情報の設定項目の「ECMP 情報」をクリックします。

「ECMP 情報」が表示されます。

78. 以下の項目を指定します。

- ECMP 機能 → ハッシュ方式

■ ECMP情報	
ECMP機能	<input type="radio"/> 使用しない <input type="radio"/> ラウンドロビン方式 <input checked="" type="radio"/> ハッシュ方式
OSPF使用ECMP数	<input type="text" value="1"/>

79. [保存] ボタンをクリックします。

80. 画面左側の [設定反映] 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。

## 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（実際にルーティングを行う装置）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ルーティング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。

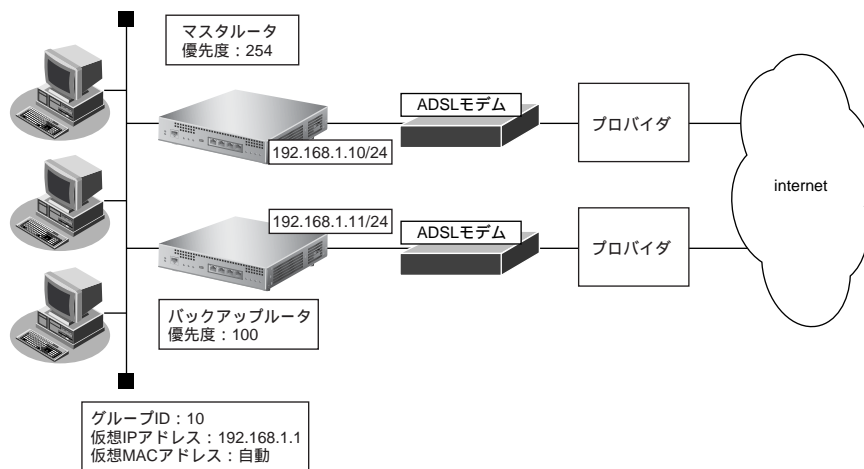
☛ 参照 MR1000 機能説明書 [2.24 VRRP 機能] (P.86)

### 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動的定義変更、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、操作メニューの「VRRP 手動切り戻し」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。
- ルータに設定される IP アドレスと仮想 IP アドレスを同じにした場合、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ることがありますので、異なる IP アドレスを設定することをお勧めします。なお、ルータに設定される IP アドレスと仮想 IP アドレスを同じにする場合は、必ず、そのルータの優先度をマスタに設定してください（優先度としてマスタを設定した場合、仮想 IP アドレスは設定できません）。
- 優先度に“マスタ”を定義した場合は、プリエンプトモードの on/off にかかわらず、プリエンプトモードが on のときと同様に動作します。
- 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。  
あて先 IP アドレス : 224.0.0.18  
プロトコル番号 : 112
- トリガ機能を使用する場合は VRRP グループの優先度に“マスタ”を指定しないでください。

## 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
- マスタールータはWAN 側経路をノードダウントリガによって監視する

#### 【マスタールータ】

- PPPoE で使用する LAN ポート : LAN0 ポート
- 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 LAN ポート : LAN0 ポート
- 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設定例を示します。

## マスタールータを設定する

1. [「1.6 インターネットへ PPPoE で接続する」\(P.64\)](#) を参考に、PPPoE での接続を設定します。
2. 設定メニューのルータ設定で「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。
3. 「LAN 情報」で LAN1 の [修正] ボタンをクリックします。  
「LAN1 情報 (物理 LAN)」ページが表示されます。

## 4. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

## 5. 以下の項目を指定します。

- VRRP 機能 →使用する

VRRP機能	<input type="radio"/> 使用しない
	<input checked="" type="radio"/> 使用する
	パスワード <input type="text"/>

## 6. [保存] ボタンをクリックします。

## 7. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

「VRRP グループ情報」が表示されます。

## 8. 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

## 9. 以下の項目を指定します。

- グループID → 10
- プライオリティ  
優先度 → バックアップ  
→ 254
- 仮想IPアドレス → 192.168.1.1
- プリエンプトモード → OFF

■基本情報	
グループID	<input type="text" value="10"/>
プライオリティ	<input type="radio"/> マスタ(255)
	<input checked="" type="radio"/> バックアップ
	優先度 <input type="text" value="254"/>
	仮想IPアドレス <input type="text" value="192.168.1.1"/>
AD送信間隔	<input type="text" value="1"/> 秒
プリエンプトモード	<input type="radio"/> ON
	<input checked="" type="radio"/> OFF
	移行禁止時間 <input type="text" value="0"/> 秒

## 10. [保存] ボタンをクリックします。

## 11. VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

## 12. 以下の項目を指定します。

- 減算プライオリティ → 254
- トリガ種別 → ノードダウントリガ (node)
  - あて先IPアドレス → 202.168.2.1
  - 送出インタフェース → 指定なし
  - 再送間隔 → 5
  - タイムアウト時間 → 16
  - 正常時送信間隔 → 17
  - 異常時送信間隔 → 30

<VRRPトリガ情報入力フィールド>

減算プライオリティ	254			
トリガ種別	<input type="radio"/> インタフェースダウントリガ(ifdown) インタフェース <input type="text" value="すべて"/>			
	<input type="radio"/> ルートダウントリガ(route)			
	ネットワーク	<input checked="" type="radio"/> デフォルトルート <input type="radio"/> 経路を指定する		
		あて先IPアドレス	<input type="text"/>	
		あて先アドレスマスク	<input type="text" value="0 (0.0.0.0)"/>	
	インタフェース	<input type="text" value="指定なし"/>		
	<input checked="" type="radio"/> ノードダウントリガ(node)			
	あて先IPアドレス	<input type="text" value="202.168.2.1"/>		
	送出インタフェース	<input type="text" value="指定なし"/>		
	再送間隔	<input type="text" value="5"/> 秒		
タイムアウト時間	<input type="text" value="16"/> 秒			
正常時送信間隔	<input type="text" value="17"/> 秒			
異常時送信間隔	<input type="text" value="30"/> 秒			

## 13. [追加] ボタンをクリックします。

## 14. 画面左側の [設定反映] 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。



## バックアップルータを設定する

---

「マスタールータを設定する」を参考に、バックアップルータを設定します。

### LAN1 情報を設定する

#### 「LAN1 情報」 - 「共通情報」

##### 「基本情報」

- VRRP 機能 →使用する

#### 「VRRP グループ0情報」

##### 「基本情報」

- グループID →10
- プライオリティ  
優先度 →バックアップ  
→100
- 仮想IPアドレス →192.168.1.1
- プリエンプトモード →OFF

手順 12. 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、マスタールータ側に以下の設定を追加します。

### LAN1 情報を設定する

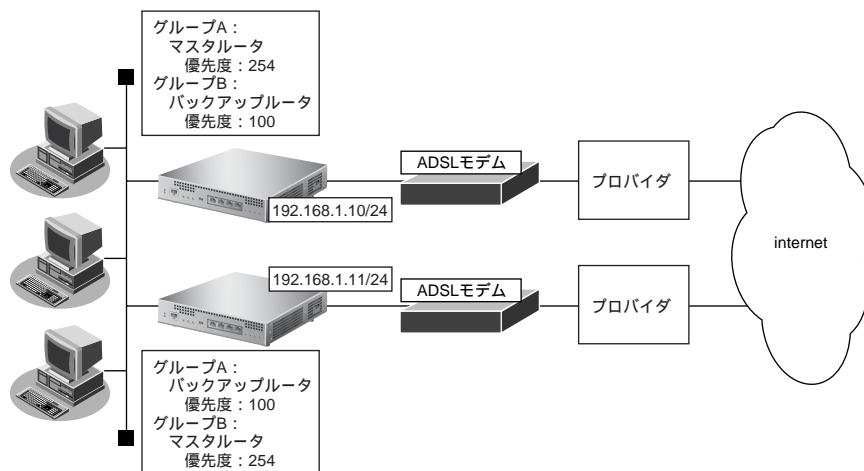
#### 「LAN1 情報」 - 「共通情報」

#### 「VRRP グループ0情報」 - 「VRRP トリガ情報」

- VRRP 機能 →使用する
- 減算プライオリティ →254
- トリガ種別 →インタフェースダウントリガ (ifdown)  
インタフェース →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LANポート : LAN0ポート
- 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 : LAN0ポート
- 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設定例を示します。

ここでは、インターネットへ PPPoE で接続されていることを前提とします。

☛ 参照 「1.6 インターネットへ PPPoE で接続する」 (P.64)

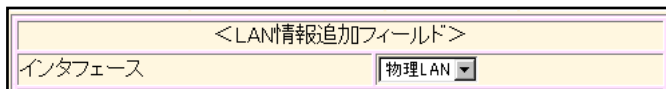
## マスタールータを設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 以下の項目を指定します。

- インタフェース →物理 LAN



### 3. [追加] ボタンをクリックします。

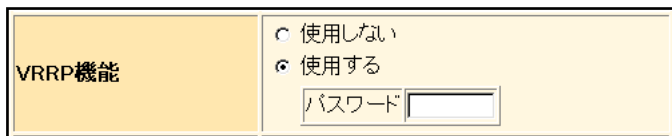
「LAN1 情報 (物理 LAN)」ページが表示されます。

### 4. 「共通情報」をクリックします。

共通情報に関する設定項目と「基本情報」が表示されます。

### 5. 以下の項目を指定します。

- VRRP 機能 →使用する



### 6. [保存] ボタンをクリックします。

### 7. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

「VRRP グループ情報」が表示されます。

### 8. 「VRRP グループ情報」でグループ番号が0の [修正] ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

## 9. 以下の項目を指定します。

- グループID → 10
- プライオリティ → バックアップ
  - 優先度 → 254
  - 仮想IPアドレス → 192.168.1.1
- プリエンプトモード → OFF

■基本情報	
グループID	10
プライオリティ	<input type="radio"/> マスタ(255) <input checked="" type="radio"/> バックアップ
	優先度 <input type="text" value="254"/>
	仮想IPアドレス <input type="text" value="192.168.1.1"/>
AD送信間隔	1 秒
プリエンプトモード	<input type="radio"/> ON <input checked="" type="radio"/> OFF
	移行禁止時間 <input type="text" value="0"/> 秒

## 10. [保存] ボタンをクリックします。

## 11. VRRP グループ情報の設定項目の「VRRP トリガ情報」をクリックします。

「VRRP トリガ情報」が表示されます。

## 12. 以下の項目を指定します。

- 減算プライオリティ → 254
- トリガ種別 → インタフェースダウントリガ (ifdown)
  - インタフェース → rmt0

<VRRPトリガ情報入力フィールド>	
減算プライオリティ	<input type="text" value="254"/>
トリガ種別	<input checked="" type="radio"/> インタフェースダウントリガ(ifdown)
	インタフェース <input type="text" value="rmt0"/>

## 13. [追加] ボタンをクリックします。

## 14. 画面上部の「LAN1 情報 (物理 LAN)」をクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

## 15. 共通情報の設定項目の「VRRP グループ情報」をクリックします。

「VRRP グループ情報」が表示されます。

## 16. 「VRRP グループ情報」でグループ番号が1の [修正] ボタンをクリックします。

VRRP グループ情報の設定項目と「基本情報」が表示されます。

**17. 以下の項目を指定します。**

- グループID → 11
- プライオリティ  
優先度 → バックアップ  
仮想IPアドレス → 100
- プリエンプトモード → 192.168.1.2  
→ ON

■基本情報	
グループID	<input type="text" value="11"/>
プライオリティ	<input type="radio"/> マスタ(255) <input checked="" type="radio"/> バックアップ 優先度 <input type="text" value="100"/> 仮想IPアドレス <input type="text" value="192.168.1.2"/>
AD送信間隔	<input type="text" value="1"/> 秒
プリエンプトモード	<input checked="" type="radio"/> ON <input type="radio"/> OFF 移行禁止時間 <input type="text" value="0"/> 秒

**18. [保存] ボタンをクリックします。****19. 画面左側の [設定反映] 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。

## バックアップルータを設定する

---

「マスタールータを設定する」を参考に、バックアップルータを設定します。

### LAN1 情報を設定する

#### 「LAN1 情報」 - 「共通情報」

##### 「基本情報」

- VRRP 機能 →使用する

#### 「VRRP グループ0情報」

##### 「基本情報」

- グループID →10
- プライオリティ  
優先度 →バックアップ  
→100  
仮想IPアドレス →192.168.1.1
- プリエンプトモード →ON

#### 「VRRP グループ1情報」

##### 「基本情報」

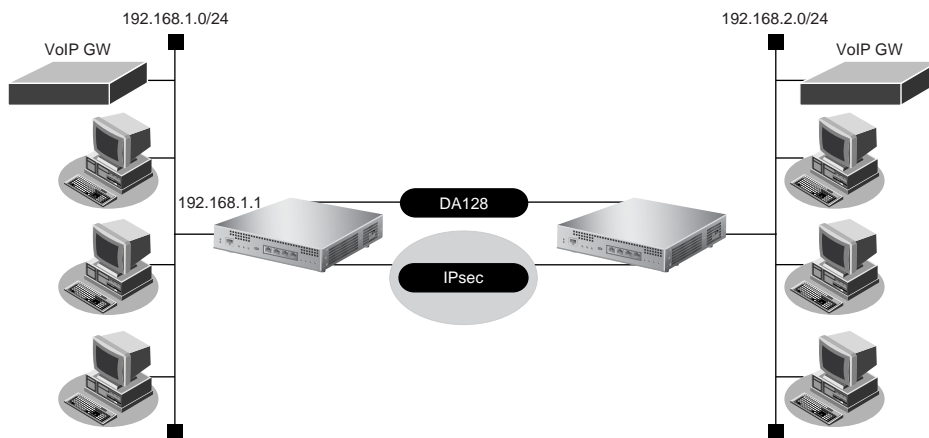
- グループID →11
- プライオリティ  
優先度 →バックアップ  
→254  
仮想IPアドレス →192.168.1.2
- プリエンプトモード →OFF

#### 「VRRP トリガ情報」

- 減算プライオリティ →254
- トリガ種別 →インタフェースダウントリガ (ifdown)  
インタフェース →rmt0

## 2.28 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 [「1.13 NAT を併用しない固定 IP アドレスでの VPN \(自動鍵交換\)」 \(P.127\)](#)、[「1.14 NAT と併用した固定 IP アドレスでの VPN \(自動鍵交換\)」 \(P.138\)](#)
  - 新規に音声データ用の専用線 (BRI:128Kbps) を追加する
  - 通常、音声データ (TOS 値 : a0) は専用線を利用する
  - 通常、その他のデータはIP-VPN を利用する
  - 専用線 (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、その他のデータも専用線を使用する
- 上記の設定条件に従って設定を行う場合の設定例を示します。

### 1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

### 2. 以下の項目を指定します。

- 回線インタフェース →専用線

<WAN情報追加フィールド>	
回線インタフェース	専用線

### 3. [追加] ボタンをクリックします。

「WAN0 情報 (専用線)」ページが表示されます。

### 4. 「基本情報」をクリックします。

「基本情報」が表示されます。

## 5. 以下の項目を指定します。

- 回線速度 → 128Kbps

■基本情報	
ポート	基本 0
回線速度	128Kbps

## 6. [保存] ボタンをクリックします。

## 7. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 8. 「ネットワーク情報」でマルチルーティングを設定するネットワーク名の [修正] ボタンをクリックします。

「ネットワーク情報」が表示されます。

## 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 「接続先情報」で IP-VPN を使用している接続先名の [修正] ボタンをクリックします。

IPsec/IKE 接続の設定項目と「基本情報」が表示されます。

## 11. IPsec/IKE 接続の設定項目の「マルチルーティング情報」をクリックします。

「マルチルーティング情報」が表示されます。

## 12. 以下の項目を指定します。

- 動作 → バックアップとして使用する
- TOS → a0

<マルチルーティング情報入力フィールド>		
動作	この接続先を [バックアップとして使用する]	
プロトコル	すべて (番号指定: [ ] “その他”を選択時のみ有効です)	
送信元情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	
あて先情報	IPアドレス	
	アドレスマスク	0 (0.0.0.0)
	ポート番号	
TOS	a0	

## 13. [追加] ボタンをクリックします。

## 14. 手順 12. ~ 13. を参考に、以下の項目を指定します。

- 動作 → 使用する

## 15. 画面上部の「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。



**16. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**17. 以下の項目を指定します。**

- 接続先名 → HSD
- 接続先種別 → 専用線接続

<接続先情報追加フィールド>

接続先名 HSD

接続先種別

- 専用線接続
- ISDN接続
- フレームリレー接続
- PPPoE接続
- IPTunnel接続
- IPsec/IKE接続
- 別インターフェースから送出
- MPLSTunnel接続
- パケット破棄

ダイヤル1 電話番号

サブアドレス

DLCI

**18. [追加] ボタンをクリックします。**

専用線接続の設定項目と「基本情報」が表示されます。

**19. 画面左側の [再起動] ボタンをクリックします。**

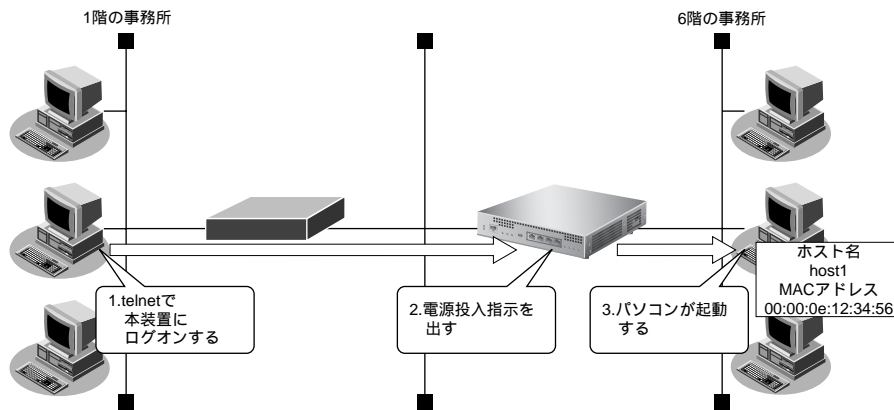
設定した内容が有効になります。

## 2.29 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、WWWブラウザから Wakeup on LAN 機能を使用して起動させることができます。

本機能は、WWW ブラウザで本装置のトップページが表示できる環境で利用できます。

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。
- 文字入力フィールドでは、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 MR1000 Web ユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)



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。

## 2.29.1 リモートパワーオン情報を設定する

1. 設定メニューのルータ設定で「ホストデータベース情報」をクリックします。

「ホストデータベース情報」ページが表示されます。

2. 未設定の欄の【修正】ボタンをクリックします。

「ホストデータベース情報」が表示されます。

3. 以下の項目を指定します。

- ホスト名 → host1
- MACアドレス → 00:00:0e:12:34:56
- リモート電源制御 → 対象



- 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。
- ホスト名は必須の設定項目ではありませんが、実際にリモートパワーオンを実行する場合にホスト情報一覧から目標とするパソコンを選択するのに有効な情報になります。

■ホストデータベース情報					
\	ホスト名	IPv4アドレス	MACアドレス	電源制御	操作
		IPv6アドレス			
1	ホスト名	host1			
	IPv4アドレス				
	IPv6アドレス				
	MACアドレス	00:00:0e:12:34:56			
	リモート電源制御	<input checked="" type="radio"/> 対象 <input type="radio"/> 対象外			

4. 【保存】ボタンをクリックします。

5. 画面左側の【設定反映】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。

## 2.29.2 リモートパワーオン機能を使う

1. パソコン上のWWWブラウザで、起動させるパソコンがつながっている本装置のトップページを表示します。

2. 操作メニューで「リモートパワーオン」をクリックします。

「リモートパワーオン」ページが表示されます。

3. 起動させるパソコンの【オン】ボタンをクリックします。

本装置が、該当するパソコンに対して「Magic Packet」を送信し、パソコンが起動します。



- 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）。

## 2.30 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ことで、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、本装置が自動的に実行します。スケジュール予約情報は、最大16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計を正しくセットしてください。

☛ 参照 MR1000 Web ユーザーズガイド「1.3 時計を設定する」(P.10)

### 2.30.1 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設定例を示します。

1. 設定メニューの基本設定で「スケジュール情報」をクリックします。  
「スケジュール情報」ページが表示されます。
2. 「月間/週間予約情報」をクリックします。  
「月間/週間予約情報」が表示されます。
3. 「月間/週間予約情報」で未設定の欄の「修正」ボタンをクリックします。

#### 4. 以下の項目を指定します。

- 動作 → 発信抑止
- 予約時刻 → 23 : 00
- 毎日
- 終了時刻 → 08:00

■月間／週間予約情報		動作	予約時刻	終了時刻	周期	操作	
1	動作	発信抑止	予約時刻	23 : 00	<input checked="" type="radio"/> 毎日 <input type="radio"/> 毎週 <input type="checkbox"/> 日曜日 <input type="checkbox"/> 月曜日 <input type="checkbox"/> 火曜日 <input type="checkbox"/> 水曜日 <input type="checkbox"/> 木曜日 <input type="checkbox"/> 金曜日 <input type="checkbox"/> 土曜日 <input type="radio"/> 毎月 <input type="checkbox"/> 日	終了時刻	08 : 00

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。

#### 5. [保存] ボタンをクリックします。

#### 6. 画面左側の [設定反映] 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。

## 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を例に説明します。

#### 1. 設定メニューの基本設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

#### 2. 「月間／週間予約情報」をクリックします。

「月間／週間予約情報」が表示されます。

#### 3. 未設定の欄の [修正] ボタンをクリックします。

#### 4. 以下の項目を指定します。

- 動作 → リモートパワーオン
- 予約時刻 → 08:00
- 毎日

■月間／週間予約情報		動作	予約時刻	終了時刻	周期	操作	
1	動作	リモートパワーオン	予約時刻	08 : 00	<input checked="" type="radio"/> 毎日 <input type="radio"/> 毎週 <input type="checkbox"/> 日曜日 <input type="checkbox"/> 月曜日 <input type="checkbox"/> 火曜日 <input type="checkbox"/> 水曜日 <input type="checkbox"/> 木曜日 <input type="checkbox"/> 金曜日 <input type="checkbox"/> 土曜日 <input type="radio"/> 毎月 <input type="checkbox"/> 日	終了時刻	

### 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には、あらかじめ利用するパソコンを「ホストデータベース情報」 - 「リモート電源制御」を「対象」として登録しておく必要があります。また、スケジュール機能を使ってリモートパワーオンする場合、「リモート電源制御」が「対象」となっているすべてのパソコンが起動します。

☛ 参照 [\[2.29 遠隔地のパソコンを起動させる \(リモートパワーオン機能\)\] \(P.586\)](#)

5. **【保存】 ボタンをクリックします。**
6. **画面左側の【設定反映】 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。

## 2.30.2 電話番号変更を予約する

ここでは、2004年7月1日午前2時に電話番号を「06-123-4567」から「06-6123-4567」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 : 2004年7月1日 2時00分
- 電話番号変更前情報 : 06-123-4567
- 電話番号変更後情報 : 06-6123-4567

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設定例を示します。

1. **設定メニューの基本設定で「スケジュール情報」をクリックします。**  
「スケジュール情報」ページが表示されます。
2. **「電話番号変更予約情報」をクリックします。**  
「電話番号変更予約情報」が表示されます。
3. **「電話番号変更予約情報」で未設定の欄の【修正】 ボタンをクリックします。**

#### 4. 以下の項目を指定します。

- 実行日時 → 2004年7月1日2時00分
- 電話番号変更情報
  - 変更前1 → 06-123-4567
  - 変更後1 → 06-6123-4567

■電話番号変更予約情報			
実行日時	電話番号変更情報		操作
実行日時	20 04 年 7 月 1 日 2 時 00 分		
1 電話番号 変更 情報	変更前1	06-123-4567	変更後1 06-6123-4567
	変更前2		変更後2
	変更前3		変更後3
	変更前4		変更後4

#### 5. [保存] ボタンをクリックします。

#### 6. 画面左側の [設定反映] 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。

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。

### 2.30.3 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、2004年7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 : 2004年7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設定例を示します。

#### 1. 設定メニューの基本設定で「スケジュール情報」をクリックします。

「スケジュール情報」ページが表示されます。

#### 2. 「構成定義切り替え予約情報」をクリックします。

「構成定義切り替え予約情報」が表示されます。

#### 3. 「構成定義切り替え予約情報」で未設定の欄の [修正] ボタンをクリックします。

**4. 以下の項目を指定します。**

- 実行日時 → 2004年7月1日6時30分
- 動作 → 構成定義情報2で再起動

■構成定義切り替え予約情報		操作
1	実行日時	20 04 年 7 月 1 日 6 時 30 分
	動作	構成定義情報2で再起動 ▼

**5. [保存] ボタンをクリックします。****6. 画面左側の [設定反映] 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。



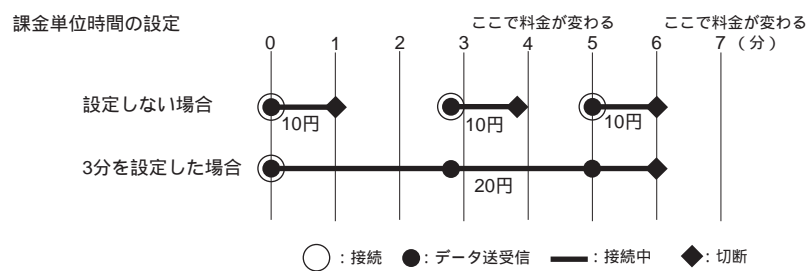
## 2.31 通信料金を節約する（課金制御機能）

本装置は通信料金を節約するための機能をサポートしています。この機能は、通信料金のむだ、使い過ぎを防ぐことができます。

ISDN回線やプロバイダの多くは、一定時間単位で料金を算定する従量課金制度を採用して料金を決めています。通信料金が3分10円で計算される場合、3分の中で何度も切断／接続を繰り返すと、料金額はその回×10円になります。

そこで課金単位時間（通信料金が計算されるとき単位時間）を設定し、無通信監視タイマ（初期値：60秒）と連動することで、単位時間内は回線を切断させないようにします。無通信監視タイマとは、設定した時間を超えてアクセスがなければ自動的に切断するという機能です。

課金単位時間に3分間を指定した場合、以下ようになります。



また、データ通信に費やした通信時間や通信料金が一定の値を超えた場合、接続を禁止したり、ログにアラームを出したりする機能（課金制御機能）もあります。無意識のうちに通信料金を使いすぎるのを防ぐことができます。

こんな事に気をつけて

- ・ 設定前に本装置の内部時計を正しくセットしてください。
- ・ 課金制御機能は、指定された料金を超えた場合に発信を制御する機能であり、運用中の回線を切断する機能ではありません。回線の接続中に指定された料金を超えても、回線を接続したままだと料金がかかり続けます。その結果、通信料金が指定した金額を超えてしまうのでご注意ください。
- ・ モデムでは、回線の切断に時間がかかるため、課金単位を超えて切断される場合があります。

☞ 参照 MR1000 Webユーザズガイド「2.2.4 課金情報で運用状況を確認する」(P.34)

### 2.31.1 課金単位時間を設定する

ここでは、相手情報として remote0、接続先情報として ap0 がすでに登録済みであることを前提としています。

#### ● 設定条件

- ・ 無通信監視タイマ : 60 秒
- ・ 課金単位時間
  - 昼間 (08:00～19:00) : 180 秒
  - 夜間 (19:00～23:00) : 180 秒
  - 深夜・早朝 (23:00～08:00) : 240 秒

上記の設定条件に従って課金単位時間を設定する場合の設定例を示します。

#### 1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2. 「ネットワーク情報」をクリックします。  
「ネットワーク情報」が表示されます。
3. 「ネットワーク情報」でネットワーク名が「rmt0」の「修正」ボタンをクリックします。  
「ネットワーク情報 (rmt0)」が表示されます。
4. 「接続先情報」をクリックします。  
「接続先情報」が表示されます。
5. 「接続先情報」で接続先名が「ap0」の「修正」ボタンをクリックします。  
ISDN接続の設定項目と「基本情報」が表示されます。
6. ISDN 接続の設定項目の「接続制御情報」をクリックします。  
「接続制御情報」が表示されます。
  - 無通信監視タイム → 送受信パケット  
60
  - 課金単位時間
    - 昼間 → 180
    - 夜間 → 180
    - 深夜・早朝 → 240

■接続制御情報	
常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
無通信監視タイム	送受信パケット (について) 60 秒
接続制限	<input type="checkbox"/> 指定した時間を超えて接続しない [ ] 時間
	<input type="checkbox"/> 指定した課金を超えて接続しない [ ] 円
課金単位時間	昼間(月～金) (08:00～19:00) 180 . 0 秒
	夜間(土日の昼間) (19:00～23:00) 180 . 0 秒
	深夜・早朝 (23:00～08:00) 240 . 0 秒

7. 「保存」ボタンをクリックします。
8. 画面左側の「設定反映」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。

## 2.31.2 課金制御機能を設定する

ここでは、接続累計時間が50時間、または通信料金の合計が10,000円になると接続要求を抑止する場合の設定方法を説明します。

### ● 設定条件

- 通信時間累計の上限時間 : 50 時間
- 通信料金の上限金額 : 10,000 円

上記の設定条件に従って設定を行う場合の設定例を示します。

#### 1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

#### 2. 回線インタフェースがISDNの【修正】ボタンをクリックします。

「WAN 情報 (ISDN)」ページが表示されます。

#### 3. 「接続制御情報」をクリックします。

「接続制御情報」が表示されます。

#### 4. 以下の項目を指定します。

- 通信時間による発信抑止 : →する  
上限時間 : →50 時間
- 課金金額による発信抑止 : →する  
上限金額 : →10000

■接続制御情報	
通信時間による発信抑止	<input type="radio"/> しない <input checked="" type="radio"/> する 上限時間: 50 時間 制御動作: <input checked="" type="radio"/> 発信抑止 <input type="radio"/> システムログ出力のみ
課金額による発信抑止	<input type="radio"/> しない <input checked="" type="radio"/> する 上限金額: 10000 円 制御動作: <input checked="" type="radio"/> 発信抑止 <input type="radio"/> システムログ出力のみ

#### 5. [保存] ボタンをクリックします。

#### 6. 画面左側の【設定反映】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。



- 現在の課金情報は、表示メニューで「課金情報」をクリックすると表示されます。
- 課金情報をクリアすることで、再度、発信ができるようになります。課金情報をクリアするには、表示メニューの「課金情報」から行います。

---


### こんな事に気をつけて

- 本書の表記で使われる通信料金とは、INS ネット 64 基本サービスの「料金情報通知」をもとに、本装置のソフトウェアが算出した値です。算出される値は、お客様の契約や回線利用状況によって異なりますので、請求金額とは必ずしも一致しません。  
たとえば以下のような場合があります。
    - INSテレホーダイサービス利用時
    - 各種料金引きサービス利用時
  - 本装置の電源を切ると、課金情報（通信時間累計、通信料金累計など）はすべてクリアされます。
-

## 2.32 ブリッジ／STP機能を使う


ここでは、ブリッジでFNAをつないでSTP機能を使用する場合、ブリッジルーピング機能を使用する場合およびIPトンネルでブリッジ通信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

- 文字入力フィールドでは半角文字（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 MR1000 Webユーザーズガイド「1.5 文字入力フィールドで入力できる文字一覧」(P.13)
- STP機能は、グループ0でだけ動作します。VLANインタフェースでは、STPを使用できません。
- WANインタフェースでブリッジを利用する場合は、1つの相手情報（remote）に対して、1つの接続先情報（ap）となるように設計してください。
- 本装置では、ファームウェアの更新やSNMPでの監視などの目的でIPv4のIPアドレスを使用します。そのため、IPv4のIPアドレスを設定しないで運用することはできません。IPv6およびブリッジだけを使用しているネットワークで運用する場合でも、どれかのLANインタフェースに必ずIPv4のIPアドレスを設定してください。
- VLANでバインドされたインタフェースでブリッジを行うことはできません。
- 本装置のブリッジMAC学習は、異なるVLAN上で同一のMACアドレスを学習することはできません。本装置は、唯一装置がもつ学習テーブルを各VLANが共有するSVL（Shared VLAN Learning）と呼ばれる方式で学習を行っています。VLANインタフェースでブリッジを行う場合は、異なるVLAN上に同一のMACアドレスを持つネットワークと接続しないでください。
- 設定を間違えてループ構成を構成し、ブロードキャストストームが発生してコンソールなどが反応しなくなった場合は、ブリッジが有効なWANやLANのケーブルを抜くとブロードキャストストームが収まります。ブロードキャストストームが収まったところで設定を修正してください。

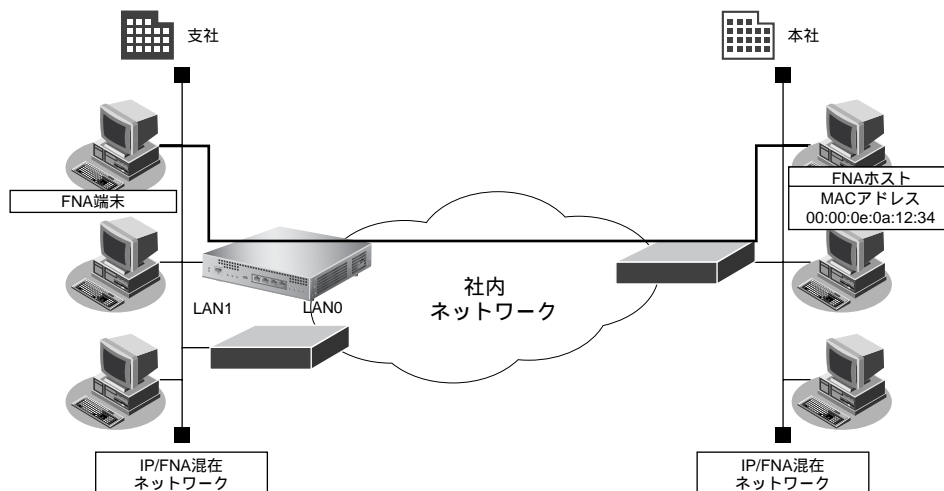
### 2.32.1 ブリッジでFNAをつないでSTP機能を使う

ブリッジ機能を使用すると、離れたLANどうしを1つのサブネットワークとして使用することができます。また、STP機能を使用すると、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 MR1000 機能説明書「2.24 VRRP機能」(P.86)

## LAN 接続の場合

ここでは、離れた LAN (FNA) をブリッジでつなぐ場合を例に説明します。



### ● 設定条件

- 本社へFNAのデータだけをブリッジする
- STP機能を使用する

こんな事に気をつけて

ブリッジ機能によりネットワークを接続する場合は、ブリッジ通信をするパケット以外をフィルタリングする設定にしてください。フィルタリングしないと不要なトラフィックが発生するだけでなく、IP通信できなくなる場合があります。

上記の設定条件に従って設定を行う場合の設定例を示します。

### ブリッジ情報を設定する (LAN1)

1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースがLAN1の【修正】ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。

3. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

#### 4. 以下の項目を指定します。

- ブリッジ機能 →使用する
- STP 機能 →使用する

■ブリッジ情報	
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
グループ識別子	0
STP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	パスコスト <input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する <input type="text"/>
	インタフェース優先度 128

#### 5. [保存] ボタンをクリックします。

#### ブリッジ情報を設定する (LAN0)

#### 6. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

#### 7. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

#### 8. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

#### 9. 以下の項目を指定します。

- ブリッジ機能 →使用する
- STP 機能 →使用する

■ブリッジ情報	
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
グループ識別子	0
STP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
	パスコスト <input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する <input type="text"/>
	インタフェース優先度 128

#### 10. [保存] ボタンをクリックします。

#### フィルタリング情報で FNA を透過させる (支社→本社)

#### 11. ブリッジ関連の設定項目の「MAC フィルタリング情報」をクリックします。

「MAC フィルタリング情報」が表示されます。

**12. 以下の項目を指定します。**

- 動作 → 透過
- 送信元MACアドレス → すべて
- あて先MACアドレス  
アドレス指定 → 指定する  
→ 00:00:0e:0a:12:34
- フォーマット種別 → LLC 形式  
LSAP → 8080

<MACフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 遮断
送信元MACアドレス	すべて アドレス指定(“指定する”を選択時のみ有効です)
あて先MACアドレス	指定する アドレス指定(“指定する”を選択時のみ有効です) 00:00:0e:0a:12:34
フォーマット種別	LLC形式 (“LLC形式”の場合はLSAP、“Ethernet形式”の場合はtype値を入力してください) 8080

**13. [追加] ボタンをクリックします。****フィルタリング情報でFNAを透過させる (本社→支社)****14. 手順 12. ～ 13. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 送信元MACアドレス  
アドレス指定 → 指定する  
→ 00:00:0e:0a:12:34
- あて先MACアドレス → すべて
- フォーマット種別 → LLC 形式  
LSAP → 8080

**フィルタリング情報でSTPを透過させる****15. 手順 12. ～ 13. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 送信元MACアドレス → すべて
- あて先MACアドレス  
アドレス指定 → 指定する  
→ 01:80:c2:00:00:00
- フォーマット種別 → LLC 形式  
LSAP → 4242

**残りの通信をすべて遮断する****16. 手順 12. ～ 13. を参考に、以下の項目を指定します。**

- 動作 → 遮断
- 送信元MACアドレス → すべて
- あて先MACアドレス → すべて
- フォーマット種別 → すべて

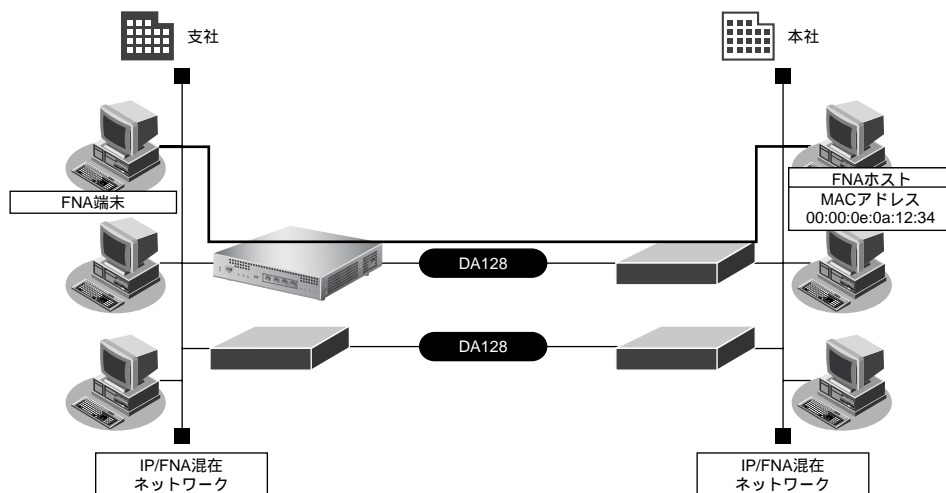


## 17. 画面左側の【設定反映】ボタンをクリックします。

設定した内容が有効になります。

## リモート接続の場合

ここでは、専用線をはさんで離れたLAN (FNA) をブリッジでつなぐ場合の設定方法を説明します。WAN インタフェースの種類によって設定が異なりますので、使用する WAN インタフェースに応じて WAN 関連定義を行ってください。



### ● 設定条件

- ISDN ポートで専用線 (128kbps) を使用する
- 本社へFNAのデータだけをブリッジする
- STP機能を使用する

### こんな事に気をつけて

ブリッジ機能を使用すると定期的に発信するため、超過課金が発生します。ISDN 回線やモデム接続で STP 機能を使用しないでください。

この例では、本社と支社がすでに専用線接続されていることを前提としています。

☛ 参照 [「1.8 事業所 LAN を専用線で接続する」](#) (P.79)

上記の設定条件に従って設定を行う場合の設定例を示します。

## ブリッジ情報を設定する

### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

### 3. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

## 4. 以下の項目を指定します。

- ブリッジ機能 →使用する
- STP 機能 →使用する

■ブリッジ情報					
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する				
グループ識別子	0				
STP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する				
	<table border="1"> <tr> <td>パスコスト</td> <td><input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する</td> </tr> <tr> <td>インタフェース優先度</td> <td>128</td> </tr> </table>	パスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する	インタフェース優先度	128
	パスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する			
インタフェース優先度	128				

## 5. [保存] ボタンをクリックします。

## 6. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 7. 「ネットワーク情報」でブリッジ設定を行うネットワーク名の [修正] ボタンをクリックします。

「ネットワーク情報」が表示されます。

## 8. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

## 9. 以下の項目を指定します。

- ブリッジ機能 →使用する
- STP 機能 →使用する

■ブリッジ情報					
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する				
グループ識別子	0				
STP機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する				
	<table border="1"> <tr> <td>パスコスト</td> <td><input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する</td> </tr> <tr> <td>インタフェース優先度</td> <td>128</td> </tr> </table>	パスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する	インタフェース優先度	128
	パスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する			
インタフェース優先度	128				

## 10. [保存] ボタンをクリックします。

## フィルタリング情報でFNAを透過させる（支社→本社）

## 11. ブリッジ関連の設定項目の「MACフィルタリング情報」をクリックします。

「MACフィルタリング情報」が表示されます。

**12. 以下の項目を指定します。**

- 動作 → 透過
- 送信元MACアドレス → すべて
- あて先MACアドレス  
アドレス指定 → 指定する  
→ 00:00:0e:0a:12:34
- フォーマット識別 → LLC 形式  
LSAP → 8080

<MACフィルタリング情報入力フィールド>	
動作	<input checked="" type="radio"/> 透過 <input type="radio"/> 透過(接続中のみ) <input type="radio"/> 遮断
送信元MACアドレス	すべて アドレス指定("指定する"を選択時のみ有効です)
あて先MACアドレス	指定する アドレス指定("指定する"を選択時のみ有効です) 00:00:0e:0a:12:34
フォーマット種別	LLC形式 ("LLC形式"の場合はLSAP, "Ethernet形式"の場合はtype値を入力してください) 8080

**13. [追加] ボタンをクリックします。****フィルタリング情報でFNAを透過させる (本社→支社)****14. 手順 12. ~ 13. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 送信元MACアドレス  
アドレス指定 → 指定する  
→ 00:00:0e:0a:12:34
- あて先MACアドレス → すべて
- フォーマット識別 → LLC 形式  
LSAP → 8080

**フィルタリング情報でSTPを透過させる****15. 手順 12. ~ 13. を参考に、以下の項目を指定します。**

- 動作 → 透過
- 送信元MACアドレス → すべて
- あて先MACアドレス  
アドレス指定 → 指定する  
→ 01:80:c2:00:00:00
- フォーマット識別 → LLC 形式  
LSAP → 4242

**残りの通信をすべて遮断する****16. 手順 12. ~ 13. を参考に、以下の項目を指定します。**

- 動作 → 遮断
- 送信元MACアドレス → すべて
- あて先MACアドレス → すべて
- フォーマット識別 → すべて

## 17. 画面左側の [設定反映] 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。

## 2.32.2 ブリッジグループピング機能を使う

ブリッジグループピング機能とは、各インタフェースにグループ識別子を設定し、それぞれのインタフェースにグループを割り当てることによって、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

- ブリッジ学習テーブル生存時間は、グループ0に設定した値がすべてのグループで使用されます。
- VLANインタフェースをブリッジグループに含める場合は、1つまたは複数のリモートインタフェースとVLANインタフェースでだけグループピングできます。
- 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LAN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、同じグループ内で定義番号がもっとも小さいLANインタフェースでだけ以下の機能を利用できます。

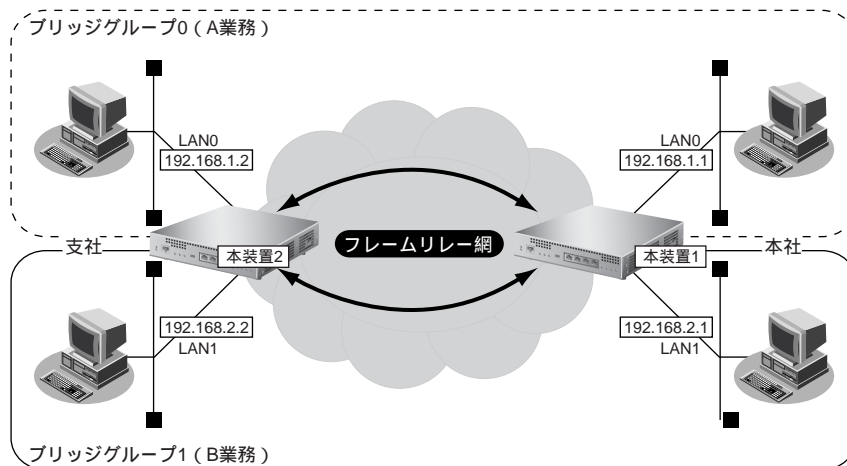
- FTP (ファームアップデートなど)
- telnet
- Web ブラウザによる設定
- syslogの送信
- SNMPエージェント、Trap送信
- ダイナミックルーティング

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ルーティングが行われます。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。

- ブリッジグループを複数定義する場合は、グループ識別子を0から順番に、間をあけないで設定してください。
- STPはグループ0でだけ動作するため、グループ0以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ0でループを構成するブリッジ構成を行う場合は、必ずSTPを有効にしてください。
- 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。よって、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経路でIPをブリッジし、ルーティングを許す場合 (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経路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て到達します。

ここでは、ブリッジグループ機能を使用して、本社と特定の支社との間で業務ごとに異なる通信を分離して実現する場合の設定方法を説明します。

本社の LAN0 と支社の LAN0 との間は A 業務関連だけを通信し、本社の LAN1 と支社の LAN1 との間は B 業務関連だけを通信します。互いの通信は IP も含めて完全に分離します。



すでにフレームリレー網を利用して、本社と支社の間で PVC を2つ接続し、以下のとおりに設定されていることを前提とします。

☛ 参照 「1.9 複数の事業所 LAN をフレームリレーで接続する」 (P.85)

## ● 前提条件

### 【本社、支社共通】

- フレームリレー網を利用して、本社と支社の間で PVC を2つ接続している

### 【本社】

- LAN0 の IPv4 アドレス : 192.168.1.1/24
- LAN1 の IPv4 アドレス : 192.168.2.1/24

### 【支社】

- LAN0 の IPv4 アドレス : 192.168.1.2/24
- LAN1 の IPv4 アドレス : 192.168.2.2/24

## ● 設定条件

### 【本社、支社共通】

- ブリッジグループ数 : 2 グループ (A 業務用と B 業務用)
- IPv4 の転送方式 : ブリッジで転送
- 転送ポリシー : strict (完全に IPv4 通信を分離)

## 本社を設定する

### ブリッジグループ0に属するインターフェースを設定する

#### 1. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

2. 「LAN 情報」でインタフェースが LAN0 の「修正」ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

4. 以下の項目を指定します。

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 192.168.1.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール1

■ IP アドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IP アドレス	<input type="radio"/> DHCP で自動的に取得する
	<input checked="" type="radio"/> 指定する
	IP アドレス <input type="text" value="192.168.1.1"/>
	ネットマスク <input type="text" value="24 (255.255.255.0)"/>
ブロードキャストアドレス	<input type="text" value="ネットワークアドレス + オール1"/>

5. 「保存」ボタンをクリックします。

6. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

7. 以下の項目を指定します。

- ブリッジ機能 → 使用する
- グループ識別子 → 0
- STP 機能 → 使用しない

■ ブリッジ情報	
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
グループ識別子	<input type="text" value="0"/>
STP 機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	パスコスト <input type="text" value="自動決定"/> <input type="text" value="指定する"/>
	インタフェース優先度 <input type="text" value="128"/>

8. 「保存」ボタンをクリックします。

9. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

10. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

11. 「ネットワーク情報」でブリッジグループ 0 に属する (A 業務用 PVC) ネットワーク名の「修正」ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

**12. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**13. 以下の項目を指定します。**

- IPアドレス → 設定しない

■ IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する 相手側IPアドレス <input type="text"/> 自側IPアドレス <input type="text"/>
MSS書き換え	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 書き換えサイズ <input type="text" value="0"/> バイト

**14. [保存] ボタンをクリックします。****15. 「ブリッジ関連」をクリックします。**

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

**16. 以下の項目を指定します。**

- ブリッジ機能 → 使用する
- グループ識別子 → 0
- STP機能 → 使用しない

■ ブリッジ情報	
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
グループ識別子	<input type="text" value="0"/>
STP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する バスコスト <input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する <input type="text"/> インタフェース優先度 <input type="text" value="128"/>

**17. [保存] ボタンをクリックします。****ブリッジグループ0を設定する****18. 設定メニューのルータ設定で「ブリッジ情報」をクリックします。**

「ブリッジ情報」ページが表示されます。

**19. 「ブリッジグループ情報」をクリックします。**

「ブリッジグループ情報」が表示されます。

**20. 「ブリッジグループ情報」でグループ識別子が0の[修正] ボタンをクリックします。**

**21. 以下の項目を指定します。**

- IPv4 ルーティング機能 → 使用しない
- 転送ポリシー → strict

0	IPv4ルーティング機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
	転送ポリシー	<input checked="" type="radio"/> strict <input type="radio"/> loose

**22. [保存] ボタンをクリックします。****ブリッジグループ 1 に属するインタフェースを設定する****23. 設定メニューのルータ設定で「LAN 情報」をクリックします。**

「LAN 情報」ページが表示されます。

**24. 以下の項目を指定します。**

- インタフェース → 物理 LAN

<LAN情報追加フィールド>	
インタフェース	物理LAN ▼

**25. [追加] ボタンをクリックします。**

「LAN1 情報 (物理 LAN)」ページが表示されます。

**26. 「IP 関連」をクリックします。**

IP 関連の設定項目と「IP アドレス情報」が表示されます。

**27. 以下の項目を指定します。**

- IPv4 → 使用する
- IP アドレス → 指定する
- IP アドレス → 192.168.2.1
- ネットマスク → 24 (255.255.255.0)
- ブロードキャストアドレス → ネットワークアドレス + オール 1

<b>IPアドレス情報</b>		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する <input checked="" type="radio"/> 指定する	
	IPアドレス	192.168.2.1
	ネットマスク	24 (255.255.255.0) ▼
	ブロードキャストアドレス	ネットワークアドレス + オール 1 ▼

**28. [保存] ボタンをクリックします。****29. 「ブリッジ関連」をクリックします。**

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。



## 30. 以下の項目を指定します。

- ブリッジ機能 →使用する
- グループ識別子 →1
- STP機能 →使用しない

■ブリッジ情報	
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
グループ識別子	1
STP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	パスコスト <input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する <input type="text"/>
	インターフェース優先度 128

## 31. [保存] ボタンをクリックします。

## 32. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 33. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

## 34. 「ネットワーク情報」でブリッジグループ1に属する (B業務用 PVC) ネットワーク名の [修正] ボタンをクリックします。

「ネットワーク情報」ページが表示されます。

## 35. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

## 36. 以下の項目を指定します。

- IPアドレス →設定しない

■IP基本情報	
IPアドレス	<input checked="" type="radio"/> 設定しない <input type="radio"/> 設定する
	相手側IPアドレス <input type="text"/>
	自側IPアドレス <input type="text"/>
MSS書き換え	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	書き換えサイズ 0 バイト

## 37. [保存] ボタンをクリックします。

## 38. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

**39. 以下の項目を指定します。**

- ブリッジ機能 →使用する
- グループ識別子 →1
- STP機能 →使用しない

■ブリッジ情報	
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
グループ識別子	1
STP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	パスコスト <input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する <input type="text"/>
	インタフェース優先度 <input type="text" value="128"/>

**40. [保存] ボタンをクリックします。****ブリッジグループ1を設定する****41. 設定メニューのルータ設定で「ブリッジ情報」をクリックします。**

「ブリッジ情報」ページが表示されます。

**42. 「ブリッジグループ情報」をクリックします。**

「ブリッジグループ情報」が表示されます。

**43. 「ブリッジグループ情報」でグループ識別子が1の【修正】ボタンをクリックします。****44. 以下の項目を指定します。**

- IPv4 ルーティング機能 →使用しない
- 転送ポリシー →strict

1	IPv4ルーティング機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
	転送ポリシー	<input checked="" type="radio"/> strict <input type="radio"/> loose

**45. [保存] ボタンをクリックします。****46. 画面左側の【設定反映】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。

**支社を設定する**

「本社を設定する」を参考に、支社を設定します。

この例では、LAN側のIPアドレス以外は、本社とすべて同じです。

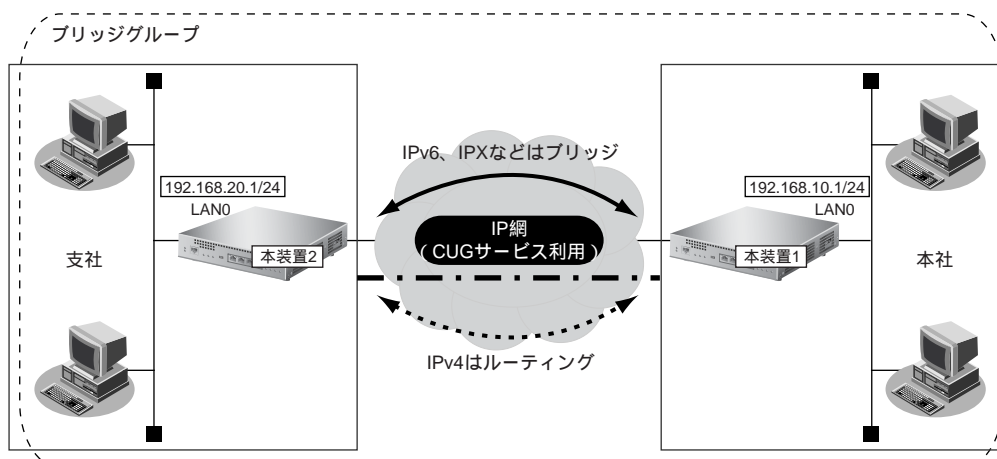
## 2.32.3 IP トンネルで事業所間をブリッジ接続する (Ethernet over IP ブリッジ)

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

- ブリッジ学習テーブル生存時間は、グループ0に設定した値がすべてのグループで使用されます。
- VLAN インタフェースをブリッジグループに含める場合は、1つまたは複数のリモートインタフェースと VLAN インタフェースでだけグルーピングできます。
- 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 LAN 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、同じグループ内で定義番号がもっとも小さい LAN インタフェースでだけ以下の機能を利用できます。
  - FTP (ファームアップデートなど)
  - telnet
  - Web ブラウザによる設定
  - 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ルーティングが行われます。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。
- ブリッジグループを複数定義する場合は、グループ識別子を 0 から順番に、間をあげないで設定してください。
- STP はグループ 0 でだけ動作するため、グループ 0 以外のグループでは冗長リンクを持つなどループを構成するブリッジ構成は行わないでください。ブロードキャストストームが発生して通信できなくなります。また、グループ 0 でループを構成するブリッジ構成を行う場合は、必ず STP を有効にしてください。
- 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。よって、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 経路で IP をブリッジし、ルーティングを許す場合 (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 経路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て到達します。
- 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。

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）】

- 払い出されるIPv4アドレス（LAN0ポートに設定） : 192.168.10.1/24
- PPPoE ユーザ認証ID : userid1@groupname
- PPPoE ユーザ認証パスワード : userpass1
- PPPoE LANポート : LAN1ポート使用
- NAT機能を使用しない
- 常時接続機能を使用する

#### 【支社（PPPoE常時接続）】

- 払い出されるIPv4アドレス（LAN0ポートに設定） : 192.168.20.1/24
- PPPoE ユーザ認証ID : userid2@groupname
- PPPoE ユーザ認証パスワード : userpass2
- PPPoE LANポート : LAN1ポート使用
- NAT機能を使用しない
- 常時接続機能を使用する

### ● 設定条件

#### 【本社】

- 接続ネットワーク名 : honsya
- 接続先名 : honsya1
- 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】

- 接続ネットワーク名 : shisya
- 接続先名 : shisya1
- 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 : LAN0 ポートと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設定例を示します。

## 本社を設定する

---

### PPPoE 接続を設定する

1. **「1.6 インターネットへPPPoEで接続する」(P.64)** を参考に、PPPoE での接続を設定します。

こんな事に気をつけて

「1.6 インターネットへPPPoEで接続する」(P.64) の設定例と本設定例は、PPPoE で使用する拠点ネットワークの LAN が逆になっています。

---

### IPv4 トンネルを設定する

2. 設定メニューのルータ設定で**「相手情報」**をクリックします。

「相手情報」ページが表示されます。

3. **「ネットワーク情報」**をクリックします。

「ネットワーク情報」が表示されます。

4. 以下の項目を指定します。

- ネットワーク名 → shisya

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="shisya"/>

5. **「追加」** ボタンをクリックします。

「ネットワーク情報 (shisya)」ページが表示されます。

6. **「接続先情報」**をクリックします。

「接続先情報」が表示されます。

## 7. 以下の項目を指定します。

- 接続先名 → shisya1
- 接続先種別 → IP トンネル接続

<接続先情報追加フィールド>

接続先名	shisya1	
接続先種別	<input type="radio"/> ATM接続	
	VCI	<input type="text"/>
	<input type="radio"/> 専用線接続	
	<input type="radio"/> ISDN接続	
	ダイヤル1	電話番号 <input type="text"/>
		サブアドレス <input type="text"/>
接続先種別	<input type="radio"/> フレームリレー接続	
	DLCI	<input type="text"/>
	<input type="radio"/> PPPoE接続	
	<input checked="" type="radio"/> IPトンネル接続	
	<input type="radio"/> IPsec/IKE接続	
	<input type="radio"/> 別インタフェースから送出	
	<input type="radio"/> MPLSトンネル接続	
	<input type="radio"/> パケット破棄	

## 8. [追加] ボタンをクリックします。

IP トンネル接続の設定項目と「基本情報」が表示されます。

## 9. 以下の項目を指定します。

- 自側エンドポイント → 192.168.10.1
- 相手側エンドポイント → 192.168.20.1

■基本情報

接続先名	shisya1
自側エンドポイント	192.168.10.1
相手側エンドポイント	192.168.20.1

## 10. [保存] ボタンをクリックします。

### ブリッジグループ0に属するインタフェースを設定する

## 11. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

## 12. 「LAN 情報」でインタフェースがLAN0の【修正】 ボタンをクリックします。

「LAN0情報（物理 LAN）」ページが表示されます。

## 13. 「ブリッジ関連」をクリックします。

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

**14. 以下の項目を指定します。**

- ブリッジ機能 →使用する
- グループ識別子 →0
- STP機能 →使用しない

■ブリッジ情報					
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する				
グループ識別子	0				
STP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する				
	<table border="1"> <tr> <td>バスコスト</td> <td><input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する </td> </tr> <tr> <td>インタフェース優先度</td> <td>128</td> </tr> </table>	バスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する	インタフェース優先度	128
	バスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する			
インタフェース優先度	128				

**15. [保存] ボタンをクリックします。****16. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**17. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**18. 「ネットワーク情報」でIPトンネルを設定したネットワーク名 (shisya) の [修正] ボタンをクリックします。**

「ネットワーク情報 (shisya)」ページが表示されます。

**19. 「ブリッジ関連」をクリックします。**

ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

**20. 以下の項目を指定します。**

- ブリッジ機能 →使用する
- グループ識別子 →0
- STP機能 →使用しない

■ブリッジ情報					
ブリッジ機能	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する				
グループ識別子	0				
STP機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する				
	<table border="1"> <tr> <td>バスコスト</td> <td><input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する </td> </tr> <tr> <td>インタフェース優先度</td> <td>128</td> </tr> </table>	バスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する	インタフェース優先度	128
	バスコスト	<input checked="" type="radio"/> 自動決定 <input type="radio"/> 指定する			
インタフェース優先度	128				

**21. [保存] ボタンをクリックします。****ブリッジグループ0を設定する****22. 設定メニューのルータ設定で「ブリッジ情報」をクリックします。**

「ブリッジ情報」ページが表示されます。

**23. 「ブリッジグループ情報」をクリックします。**

「ブリッジグループ情報」が表示されます。

**24. 「ブリッジグループ情報」でグループ識別子が0の【修正】ボタンをクリックします。****25. 以下の項目を指定します。**

- IPv4ルーティング機能                   →使用する
- IPv6ルーティング機能                   →使用しない
- 転送ポリシー                           →strict

0	IPv4ルーティング機能	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない 転送ポリシー <input checked="" type="radio"/> strict <input type="radio"/> loose
	IPv6ルーティング機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない 転送ポリシー <input checked="" type="radio"/> strict <input type="radio"/> loose

**26. 【保存】ボタンをクリックします。****27. 画面左側の【再起動】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。

## 支社を設定する

---

「本社を設定する」を参考に、支社を設定します。

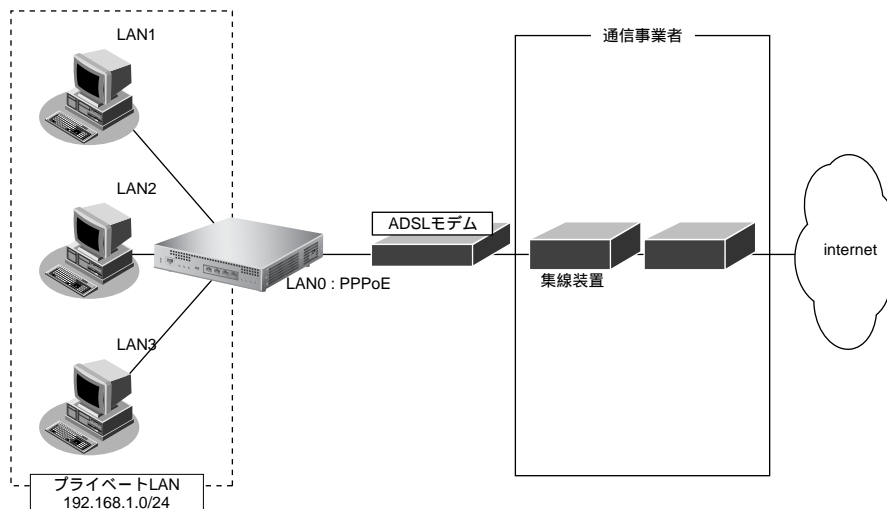
この例では、LAN側のIPアドレス、PPPoEの接続先情報（認証情報）、IPv4トンネルのエンドポイントアドレス以外は、本社とすべて同じです。



## 2.33 複数のLANポートをスイッチングHUBのように使う

ここでは、1つのLANポートをPPPoEで使用し、残りのLANポートをスイッチングHUBのように設定してプライベートLANを構築し、インターネットを利用する例を説明します。

まず、この機能を使用する前にMR1000 機能説明書「[2.25 ブリッジ機能](#)」(P.91)を参照して、ブリッジグループリングの機能と注意事項を理解してから設定してください。



### こんな事に気をつけて

- パソコンのLANインタフェースと本装置の切り替えスイッチのないLANポートを接続する場合は、クロスケーブルを使って接続してください。
- IPv4やIPv6をブリッジする場合、IP関連の定義は、ブリッジグループ内で定義番号がもっとも小さいLANインタフェース（レイヤ3代表インタフェース）を設定してください。ブリッジグループ内では、レイヤ3代表インタフェースでだけ、レイヤ3の機能が有効になります。
- LANポートのリンク状態によって動作する機能（例：OSPFやVRRPなど）は、これらの機能が定義されたレイヤ3代表インタフェースのリンク状態だけを監視して動作しています。レイヤ3代表インタフェースが同期はずれを起こし、これ機能が代表インタフェースへの出力を止めた場合、同じグループ内のほかのポートからも、この機能が出力するパケットが出なくなります。よって、リンク状態をみて動作する機能は、レイヤ3代表インタフェースのLANポートだけを使用してください。

「[1.6 インターネットへPPPoEで接続する](#)」(P.64)の設定が終了し、以下のとおりに設定されていることを前提とします。

☞ 参照 MR1000 機能説明書「[2.25 ブリッジ機能](#)」(P.91)

### ● 前提条件

- プライベートLAN側のネットワーク : 192.168.1.0/24
- レイヤ3代表インタフェース : LAN1

### ● 設定条件

- LAN1、LAN2、LAN3をグループリングして、スイッチングHUBのように利用して、プライベートLAN側に使用する
- IPv4をブリッジ対象とする
- プライベートLAN側のブリッジグループとインターネット側の間のルーティングを許可する

上記の設定条件に従って設定を行う場合の設定例を示します。

## スイッチング HUB のように利用する LAN インタフェースを設定する

1. 設定メニューのルータ設定で、「LAN 情報」をクリックします。  
「LAN 情報」ページが表示されます。

2. 以下の項目を指定します。

- インタフェース → 物理 LAN

3. [追加] ボタンをクリックします。  
「LAN1 情報 (物理 LAN)」ページが表示されます。

4. 「ブリッジ関連」をクリックします。  
ブリッジ関連の設定項目と「ブリッジ情報」が表示されます。

5. 以下の項目を指定します。

- ブリッジ機能 → 使用する
- グループ識別子 → 0
- STP 機能 → 使用しない

6. [保存] ボタンをクリックします。
7. 手順 1.～6. を参考にして、LAN2、LAN3 を設定します。

## ブリッジグループ 0 を設定する

8. 設定メニューのルータ設定で「ブリッジ情報」をクリックします。  
「ブリッジ情報」ページが表示されます。
9. 「ブリッジグループ情報」をクリックします。  
「ブリッジグループ情報」が表示されます。
10. 「ブリッジグループ情報」でグループ識別子が 0 の [修正] ボタンをクリックします。

**11. 以下の項目を指定します。**

- IPv4 ルーティング機能 →使用しない  
転送ポリシー → loose
- IPv6 ルーティング機能 →使用しない  
転送ポリシー → loose

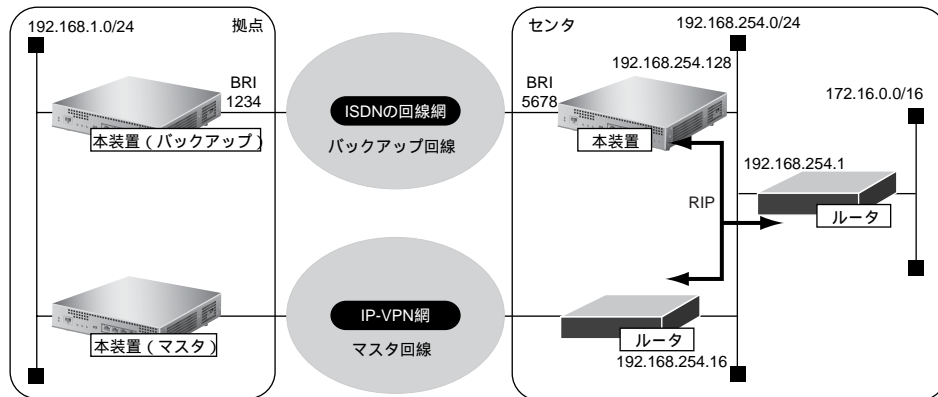
0	IPv4ルーティング機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
	転送ポリシー	<input type="radio"/> strict <input checked="" type="radio"/> loose
	IPv6ルーティング機能	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
	転送ポリシー	<input type="radio"/> strict <input checked="" type="radio"/> loose

**12. [保存] ボタンをクリックします。****13. 画面左側の [再起動] 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。

## 2.34 ISDN 接続を契機とした通信バックアップを使う

マスタ回線側で経路制御ができなくても、バックアップ回線である ISDN 回線の接続状態によって、通信をバックアップ側に切り替えることができます。



### ● 設定条件

- センタ側は、本装置以外の装置は設定が完了済み
- センタ側の 192.168.254.0/24 に接続されたそれぞれのルータは、本装置が広報する経路が選択されるように設定されている
- センタから拠点への発信は行わない
- 拠点側本装置は、ISDN 接続の設定以外は設定が完了済み

上記の設定条件に従って設定を行う場合の設定例を示します。

### センタ側本装置を設定する

#### 1. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

#### 2. 以下の項目を指定します。

- 回線インタフェース → ISDN

<WAN情報追加フィールド>	
回線インタフェース	ISDN

#### 3. [追加] ボタンをクリックします。

「WAN0 情報 (ISDN)」ページが表示されます。

#### 4. 「基本情報」をクリックします。

「基本情報」が表示されます。

## 5. 以下の項目を指定します。

- 自動接続 →すべて禁止

■基本情報	
ポート	基本 0
自動接続	<input checked="" type="radio"/> すべて禁止 <input type="radio"/> 相手毎に設定

## 6. [保存] ボタンをクリックします。

## 7. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

## 8. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

## 9. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

## 10. 以下の項目を指定します。

- IPv4 →使用する
- IP アドレス →指定する
  - IP アドレス →192.168.254.128
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス + オール1

■IPアドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IPアドレス	<input type="radio"/> DHCPで自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IPアドレス	192.168.254.128
	ネットマスク	24 (255.255.255.0)
	ブロードキャストアドレス	ネットワークアドレス + オール1

## 11. [保存] ボタンをクリックします。

## 12. IP 関連の設定項目の「RIP 情報」をクリックします。

「RIP 情報」が表示されます。

**13. 以下の項目を指定します。**

- RIP送信 → V2(Multicast) で送信する
- RIP受信 → V2、V2(Multicast) で受信する

■RIP情報	
RIP送信	<input type="radio"/> 送信しない <input type="radio"/> V1で送信する <input type="radio"/> V2で送信する <input checked="" type="radio"/> V2(Multicast)で送信する
RIP受信	<input type="radio"/> 受信しない <input type="radio"/> V1で受信する <input checked="" type="radio"/> V2、V2(Multicast)で受信する
《 RIP 送信時は加算するメトリック値を設定してください。》	
メトリック値	0

**14. [保存] ボタンをクリックします。****15. 設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**16. 「ネットワーク情報」をクリックします。**

「ネットワーク情報」が表示されます。

**17. 以下の項目を指定します。**

- ネットワーク名 → kyoten

<ネットワーク情報追加フィールド>	
ネットワーク名	kyoten

**18. [追加] ボタンをクリックします。**

「ネットワーク情報 (kyoten)」ページが表示されます。

**19. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**20. IP関連の設定項目の「スタティック経路情報」をクリックします。**

「スタティック経路情報」が表示されます。

**21. 以下の項目を指定します。**

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 192.168.1.0
- あて先アドレスマスク → 24 (255.255.255.0)

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="192.168.1.0"/> あて先アドレスマスク <input type="text" value="24 (255.255.255.0)"/>
	メトリック値 <input type="text" value="1"/>
優先度	<input type="text" value="0"/>

**22. [追加] ボタンをクリックします。**

**23. 「接続先情報」をクリックします。**

「接続先情報」が表示されます。

**24. 以下の項目を指定します。**

- 接続先名 → kyoten
- 接続先種別 → ISDN 接続
  - ダイヤル1
  - 電話番号 → 1234

<接続先情報追加フィールド>

接続先名

接続先種別

- 専用線接続
- ISDN接続
  - ダイヤル1
  - 電話番号
  - サブアドレス
- フレームリレー接続
  - DLCI
- PPPoE接続
- IPTunnel接続
- IPsec/IKE接続
- 別インターフェースから送出
- MPLSTunnel接続
- パケット破棄

**25. [追加] ボタンをクリックします。**

ISDN接続の設定項目と「基本情報」が表示されます。

**26. ISDN 接続の設定項目の「PPP 情報」をクリックします。**

「PPP 情報」が表示されます。

**27. 以下の項目を指定します。**

- 受諾認証情報
  - 認証ID → kyoten
  - 認証パスワード → kyotenpass

■ PPP情報

認証方式  PAP  CHAP

送信認証情報

認証ID

認証パスワード

受諾認証情報

認証ID

認証パスワード

**28. [保存] ボタンをクリックします。****29. 画面左側の [再起動] 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。

## 拠点側本装置を設定する

1. 設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

2. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

3. 以下の項目を指定します。

- ネットワーク名 → center

<ネットワーク情報追加フィールド>	
ネットワーク名	center

4. [追加] ボタンをクリックします。

「ネットワーク情報 (center)」ページが表示されます。

5. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

6. IP関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

7. 以下の項目を指定します。

- ネットワーク → デフォルトルート

<スタティック経路情報入力フィールド>	
ネットワーク	<input checked="" type="radio"/> デフォルトルート
	<input type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text"/>
	あて先アドレスマスク <input type="text" value="0 (0.0.0.0)"/>
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="0"/>

8. [追加] ボタンをクリックします。

9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。



**10. 以下の項目を指定します。**

- 接続先名 → center
- 接続先種別 → ISDN 接続
  - ダイヤル1
  - 電話番号 → 5678

<接続先情報追加フィールド>	
接続先名	center
接続先種別	<input type="radio"/> 専用線接続 <input checked="" type="radio"/> ISDN接続
	ダイヤル1 電話番号 5678 サブアドレス
	<input type="radio"/> フレームリレー接続 DLCI
	<input type="radio"/> PPPoE接続 <input type="radio"/> IPトンネル接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インターフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄

**11. [追加] ボタンをクリックします。**

ISDN 接続の設定項目と「基本情報」が表示されます。

**12. ISDN 接続の設定項目の「PPP 情報」をクリックします。**

「PPP 情報」が表示されます。

**13. 以下の項目を指定します。**

- 送信認証情報
  - 認証 ID → kyoten
  - 認証パスワード → kyotenpass

■ PPP情報	
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
送信認証情報	認証ID kyoten
	認証パスワード *****

**14. [保存] ボタンをクリックします。**

**15. ISDN 接続の設定項目の「接続制御情報」をクリックします。**

「接続制御情報」が表示されます。

- 無通信監視タイマ →送信パケットのみ  
60

■接続制御情報	
常時接続機能	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
無通信監視タイマ	送信パケットのみ ▾ について <input type="text" value="60"/> 秒

**16. [保存] ボタンをクリックします。****17. 画面左側の [設定反映] 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。

## 2.35 外部のパソコンから PIAFS 接続する

ここでは、PIAFS対応のPHSを使用して外部のパソコンから本装置へ着信接続する例を説明します。接続先のパソコンの設定に関する説明は省略しています。

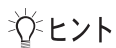
### こんな事に気をつけて

- 本装置のPIAFS接続はPIAFS 1.0/2.0/2.1に対応します。
- 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 MR1000 トラブルシューティング 「5 ご購入時の状態に戻すには」(P.42)

- 文字入力フィールドでは、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 MR1000 Webユーザズガイド 「1.5 文字入力フィールドで入力できる文字一覧」(P.13)

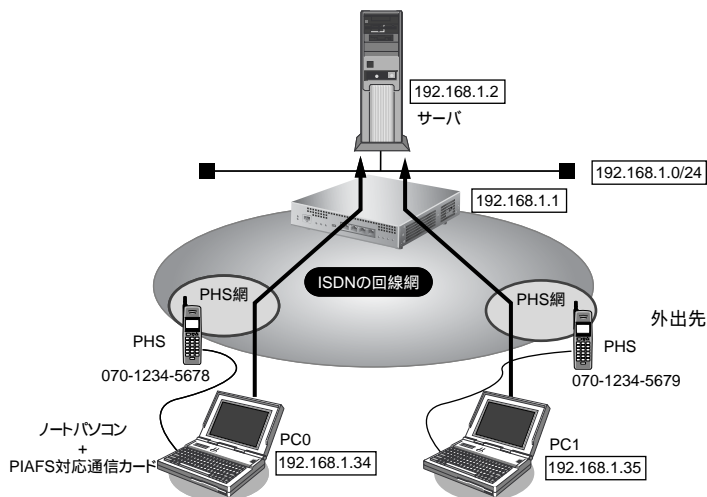


**ヒント**  
本装置のLAN側のネットワークと同じネットワークアドレスを別ネットワークのパソコンに割り当てることによって、Proxy ARPが自動的に動作し、ISDN回線経由で接続されたパソコンがLAN上に存在するように扱えます。

### ◆ Proxy ARPとは

Ethernet上で通信する場合、相手を識別するためにMACアドレスが使用されます。このとき、IPアドレスとMACアドレスの対応付けを行う手段としてARP(Address Resolution Protocol)が使用されます。ブロードキャストでARP要求を発行すると、LAN上で自分のIPアドレスに関連するARP要求であると認識したパソコンは、自分のMACアドレスを送り返します。

Proxy ARPとは、パソコンから送られてくるARP要求に対して、実際のパソコンの代わりに応答する機能です。



### ● 設定条件

- ISDN U ポートを使用して ISDN 回線に接続する
- 本装置の LAN 側のネットワークアドレス/ネットマスク : 192.168.1.0/24

#### [PC0 (ノートパソコン+ PHS) と接続する条件]

- 接続先ネットワーク名 : pc0
- 接続先名 : phs0
- 割り当て IP アドレス : 192.168.1.34
- 電話番号 : 070-1234-5678
- 受諾認証 ID : mobileid
- 受諾認証パスワード : mobilepass

#### [PC1 (ノートパソコン+ PHS) と接続する条件]

- 接続先ネットワーク名 : pc1
- 接続先名 : phs1
- 割り当て IP アドレス : 192.168.1.35
- 電話番号 : 070-1234-5679
- 受諾認証 ID : mobileid
- 受諾認証パスワード : mobilepass

上記の設定条件に従って設定を行う場合の設定例を示します。

## 回線情報を設定する

1. 詳細設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

2. 以下の項目を指定します。

- 回線インタフェース → ISDN

3. [追加] ボタンをクリックします。

「WAN0 情報 (ISDN)」ページが表示されます。

## LAN 情報を設定する

4. 詳細設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

5. 「LAN 情報」でインタフェースが LAN0 の [修正] ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

6. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

## 7. 以下の項目を指定します。

- IPv4 →使用する
- IPアドレス →指定する
  - IPアドレス →192.168.1.1
  - ネットマスク →24 (255.255.255.0)
  - ブロードキャストアドレス →ネットワークアドレス+オール1

■IPアドレス情報	
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
IPアドレス	<input type="radio"/> DHCPで自動的に取得する
	<input checked="" type="radio"/> 指定する
	IPアドレス <input type="text" value="192.168.1.1"/>
	ネットマスク <input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス <input type="text" value="ネットワークアドレス+オール1"/>

## 8. [保存] ボタンをクリックします。

## 接続先情報 (PC0) を設定する

## 9. 詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 10. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

## 11. 以下の項目を指定します。

- ネットワーク名 →pc0

<ネットワーク情報追加フィールド>	
ネットワーク名	<input type="text" value="pc0"/>

## 12. [追加] ボタンをクリックします。

「ネットワーク情報 (pc0)」ページが表示されます。

## 13. 「共通情報」をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

## 14. 以下の項目を指定します。

- 自動接続 →しない

■基本情報	
ネットワーク名	<input type="text" value="pc0"/>
MTUサイズ	<input type="text" value="1500"/> バイト
自動接続	<input type="radio"/> する <input checked="" type="radio"/> しない
シェーピング	<input checked="" type="radio"/> 使用しない
	<input type="radio"/> 使用する
	最大送信レート <input type="text"/> Mbps

必要に応じて上記以外の項目を指定します。

15. [保存] ボタンをクリックします。

16. 「IP関連」をクリックします。

IP関連の設定項目と「IP基本情報」が表示されます。

17. 以下の項目を指定します。

- IPアドレス → 設定する
  - 相手側IPアドレス → 192.168.1.34
  - 自側IPアドレス → 192.168.1.1

■ IP基本情報	
IPアドレス	<input type="radio"/> 設定しない <input checked="" type="radio"/> 設定する
	相手側IPアドレス <input type="text" value="192.168.1.34"/> 自側IPアドレス <input type="text" value="192.168.1.1"/>
MSS書き換え	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する
	書き換えサイズ <input type="text" value="0"/> バイト

18. [保存] ボタンをクリックします。

19. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

20. 以下の項目を指定します。

- 接続先名 → phs0
- 接続先種別 → ISDN 接続
  - ダイヤル1
  - 電話番号 → 070-1234-5678

<接続先情報追加フィールド>	
接続先名	<input type="text" value="phs0"/>
接続先種別	<input type="radio"/> 専用線接続 <input checked="" type="radio"/> ISDN接続
	ダイヤル1 <input type="text" value="070-1234-5678"/> 電話番号 <input type="text"/> サブアドレス <input type="text"/>
接続先種別	<input type="radio"/> フレームリレー接続 <input type="text" value=""/> DLCI
	<input type="radio"/> モデム接続 ダイヤル1 <input type="text"/> 電話番号 <input type="text"/>
<input type="radio"/> PPPoE接続 <input type="radio"/> IPトンネル接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSトンネル接続 <input type="radio"/> パケット破棄	

21. [追加] ボタンをクリックします。

ISDN接続の設定項目と「基本情報」が表示されます。

**22. ISDN 接続の設定項目の「PPP 情報」をクリックします。**

「PPP 情報」が表示されます。

**23. 以下の項目を指定します。**

- 認証方式 → PAP、CHAP
- 送信認証情報 → 設定しない
- 受諾認証情報  
  認証 ID → mobileid  
  認証パスワード → mobilepass
- MP 接続 → しない

■ PPP 情報	
認証方式	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
送信認証情報	認証 ID <input type="text"/>
	認証パスワード <input type="text"/>
受諾認証情報	認証 ID <input type="text" value="mobileid"/>
	認証パスワード <input type="text" value="*****"/>
MP 接続	<input checked="" type="radio"/> しない <input type="radio"/> する
	BAP/BACP 利用 <input checked="" type="radio"/> しない <input type="radio"/> する <small>※ 発信者番号による識別で番号をチェックしない場合は着信相手識別情報の設定が有効</small>

**24. [保存] ボタンをクリックします。**

## 接続先情報 (PC1) を設定する

---

25. 「接続先情報 (PC0) を設定する」を参考に、以下の項目を指定します。

「相手情報」 - 「ネットワーク情報」

- ネットワーク名 → pc1

「ネットワーク情報」 - 「共通情報」

「基本情報」

- 自動接続 → しない

「ネットワーク情報」 - 「IP 関連」

「IP 基本情報」

- IPアドレス → 設定する
  - 相手側IPアドレス → 192.168.1.35
  - 自側IPアドレス → 192.168.1.1
- 必要に応じて上記以外の項目を設定します。

「ネットワーク情報」 - 「接続先情報」

- 接続先名 → phs1
- 接続先種別 → ISDN 接続
- 電話番号 → 070-1234-5679
- サブアドレス → 設定しない

「接続先情報」 - 「ISDN 接続」

「PPP 情報」

- 認証方式 → PAP、CHAP
- 送信認証情報 → 設定しない
- 受諾認証情報
- 認証ID → mobileid
- 認証パスワード → mobilepass
- MP接続 → しない

26. 画面左側の [設定反映] 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。

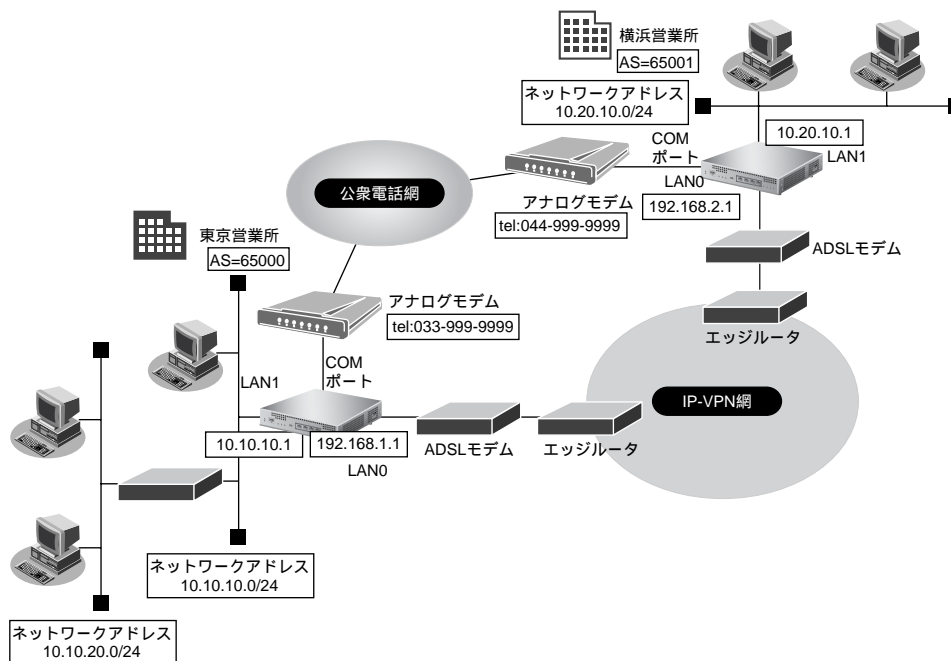


## 2.36 アナログモデムで通信バックアップをする

本装置のCOMポートに外付けのアナログモデムを接続することによって、アナログ回線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アナログ回線側で通信バックアップする場合を例に説明します。

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側が通信不能になって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。



本装置に接続できるモデムの条件は、以下のとおりです。

- COMポート側の通信速度が9600/19200/38400/57600/115200/230400bpsのどれかの速度で通信できる
- 工場出荷時の設定で、RS/CS信号によるハードフロー制御が有効になっている
- 通信中に`+++`をCOMポートから受信することによってエスケープモードになる
- 以下のATコマンドに対応している

カテゴリ	サポートコマンド
ソフトリセット	ATZ
リザルトコードを文字列にする	ATV1
エコーバックを抑止する	ATE0
CONNECTリザルトコードにDCE速度を付加する	ATW2
切断	ATH
応答	ATA
コマンド送出時先行文字	AT
電話番号送出時先行文字	ATD
パルス	P
トーン	T
ダイヤルトーン検知なし	X3
ダイヤルトーン検知あり	X4

カテゴリ	サポートコマンド
スピーカをOFFにする	M0
発呼時だけスピーカをONにする	M1
スピーカをONにする	M2
スピーカをダイヤル終了からキャリア検出までONにする	M3
音量LOW	L0
音量Midium	L2
音量High	L3

- 以下のリザルトコードを返す

カテゴリ	サポートコマンド
正常実行	OK
接続完了	CONNECT <回線速度> (※)
コマンドエラー	ERROR、+FCERROR、+FCOM、+F4、FAX、DATA、VOICE
回線接続	NO CARRIER
ダイヤルトーン未検出	NO DIALTONE、NO DIAL TONE
話し中音検出	BUSY、PHONE IN USE、HAND SET IN USE
無音未検出	NO ANSWER
呼び出し検出	RING

※) 回線速度 : 接続した回線速度

0-9の数字文字列の場合だけ回線速度として扱います。

0-9以外の文字が含まれる場合は、無視するため、回線速度を取得できません。

動作確認済みのアナログモデムは、以下のとおりです。

会社名	製品名
オムロン (株)	ME5614E2

#### こんな事に気をつけて

- アナログモデムは、COMポートに接続してください。コンソールポートは、コンソール専用ですので、モデム接続はできません。
- モデムの不揮発性メモリ（プロファイル）を工場出荷時設定にしてからモデムを接続してください。
- モデムでは、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ことがあります。
- アナログモデム接続では、以下の機能は動作しません。
  - 電話番号による相手識別機能
  - コールバック機能
  - 金額による課金制御機能
  - 常時接続機能
  - 回線接続保持タイマ機能
  - シェーピング機能
- モデムで通信できるプロトコルは、IPv4、IPv6、ブリッジだけです。
- アナログモデムによる発信は従量課金が発生するため、モデム統計情報を監視して異常課金が発生していないか、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、課金制御機能の接続時間制限を設定してください。
- アナログモデムでの通信速度は56Kbpsとみなして動作しますが、モデムの接続完了リザルトコードから速度を取得できた場合は取得した速度を採用して動作します。

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 「1.12 複数の事業所 LAN を IP-VPN 網を利用して接続する」 (P.109)

## ● 設定条件

- ADSL モデムを使用して IP-VPN 網と接続する

### 【東京営業所】

#### <横浜営業所とモデムで接続する条件>

- ネットワーク名 : backup
- 接続先名 : yokohama
- WAN の自側 IP アドレス : 172.17.1.1
- WAN の相手側 IP アドレス : 172.17.1.2
- 電話番号 : 044-999-9999
- 無通信監視 : 1分
- ユーザ認証 ID とユーザ認証パスワード  
 発信 : tokyo、tokyopass  
 着信 : kawasaki、kawapass
- ダイヤル方式 : トーン
- 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】

#### <東京営業所とモデムで接続する条件>

- ネットワーク名 : backup
- 接続先名 : tokyo
- WAN の自側 IP アドレス : 172.17.1.2
- WAN の相手側 IP アドレス : 172.17.1.1
- 電話番号 : 033-999-9999
- 無通信監視 : 1分
- ユーザ認証 ID とユーザ認証パスワード  
 発信 : kawasaki、kawapass  
 着信 : tokyo、tokyopass
- ダイヤル方式 : トーン
- 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設定例を示します。

## 東京営業所の設定する

---

### COM ポートを設定する

1. 詳細設定メニューのルータ設定で「シリアル情報」をクリックします。

「シリアル情報」ページが表示されます。

2. 「共通情報」をクリックします。

「共通情報」が表示されます。

## 3. 以下の項目を指定します。

- COMポート → 使用する
- COMポート通信速度 → 115200

■ 共通情報	
COMポート	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
COMポート通信速度	115200

## 4. [保存] ボタンをクリックします。

## バックアップ回線を設定する

## 5. 詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

## 6. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

## 7. 以下の項目を指定します。

- ネットワーク名 → backup

<ネットワーク情報追加フィールド>	
ネットワーク名	backup

## 8. [追加] ボタンをクリックします。

「ネットワーク情報 (backup)」ページが表示されます。

## 9. 「接続先情報」をクリックします。

「接続先情報」が表示されます。

## 10. 以下の項目を指定します。

- 接続先名 → yokohama
- 接続先種別 → モデム接続  
ダイヤル1 電話番号 → 044-999-9999

<接続先情報追加フィールド>	
接続先名	yokohama
接続先種別	<input type="radio"/> 専用線接続 <input type="radio"/> ISDN接続 ダイアル1 電話番号 <input type="text"/> サブアドレス <input type="text"/>
	<input type="radio"/> フレームリレー接続 DLCI <input type="text"/>
	<input checked="" type="radio"/> モデム接続 ダイアル1 電話番号 044-999-9999
	<input type="radio"/> PPPoE接続 <input type="radio"/> IPTunnel接続 <input type="radio"/> IPsec/IKE接続 <input type="radio"/> 別インタフェースから送出 <input type="radio"/> MPLSTunnel接続 <input type="radio"/> パケット破棄

**11. [追加] ボタンをクリックします。**

「接続先情報 (yokohama)」ページが表示されます。

**12. モデム接続の設定項目の「接続制御情報」をクリックします。**

「接続制御情報」が表示されます。

**13. 以下の項目を指定します。**

- 無通信監視タイマ → 送受信パケット  
60

■接続制御情報	
無通信監視タイマ	送受信パケット (について) 60 秒

**14. [保存] ボタンをクリックします。****15. モデム接続の設定項目の「PPP 情報」をクリックします。**

「PPP 情報」が表示されます。

**16. 以下の項目を指定します。**

- 送信認証情報
  - 認証 ID → yokohama
  - 認証パスワード → yokopass
- 受諾認証情報
  - 認証 ID → tokyo
  - 認証パスワード → tokyopass

■PPP情報		
送信認証情報	認証ID	yokohama
	認証パスワード	*****
受諾認証情報	認証ID	tokyo
	認証パスワード	*****

**17. [保存] ボタンをクリックします。****着信デフォルト情報を設定する****18. 詳細設定メニューのルータ設定で「相手情報」をクリックします。**

「相手情報」ページが表示されます。

**19. 「着信相手識別情報」をクリックします。**

「着信相手識別情報」が表示されます。

**20. 以下の項目を指定します。**

- 着信許可 → する

■着信相手識別情報	
着信許可	<input type="radio"/> しない <input checked="" type="radio"/> する

**21. [保存] ボタンをクリックします。**

## BGP より優先度の低いスタティックルートを設定する

### 22. 詳細設定メニューのルータ設定で「相手情報」をクリックします。

「相手情報」ページが表示されます。

### 23. 「ネットワーク情報」をクリックします。

「ネットワーク情報」が表示されます。

### 24. ネットワーク名が backup の【修正】ボタンをクリックします。

「ネットワーク情報 (backup)」ページが表示されます。

### 25. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP 基本情報」が表示されます。

### 26. IP 関連の設定項目の「スタティック経路情報」をクリックします。

「スタティック経路情報」が表示されます。

### 27. 以下の項目を指定します。

- ネットワーク → ネットワーク指定
- あて先IPアドレス → 10.20.0.0
- あて先アドレスマスク → 16 (255.255.0.0)
- メトリック値 → 1
- 優先度 → 30

<スタティック経路情報入力フィールド>	
ネットワーク	<input type="radio"/> デフォルトルート <input checked="" type="radio"/> ネットワーク指定
	あて先IPアドレス <input type="text" value="10.20.0.0"/> あて先アドレスマスク <input type="text" value="16 (255.255.0.0)"/>
	ネットワーク指定
メトリック値	<input type="text" value="1"/>
優先度	<input type="text" value="30"/>

### 28. [追加] ボタンをクリックします。

### 29. 画面左側の [設定反映] ボタンをクリックします。

## 横浜営業所を設定する

「東京営業所を設定する」を参考に、横浜営業所を設定します。

## 2.37 外部のパソコンから着信接続する (リモートアクセスサーバ)

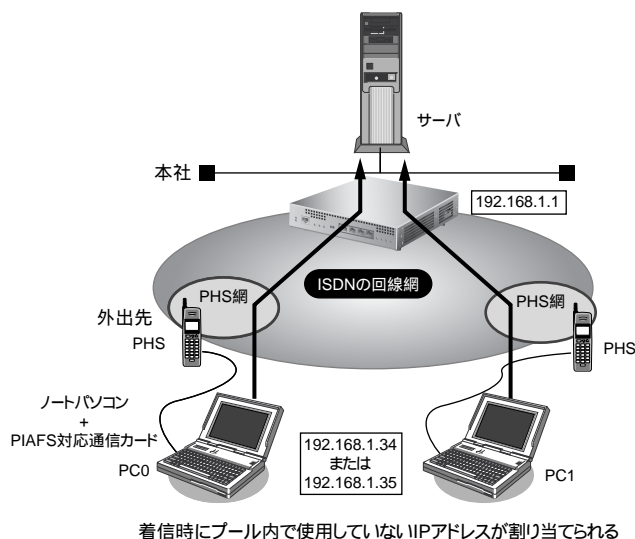
ISDN回線を使用して、外部のパソコンから本装置に着信接続する場合、本装置をリモートアクセスサーバとして使用することができます。以下の環境の場合に、リモートアクセスを行うことができます。

- デスクトップパソコン+TA → (ISDN) → 本装置
- ノート型パソコン+ISDNカード → (ISDN) → 本装置
- ノート型パソコン+PIAFS通信カード+PHS → (PHS網) → (ISDN) → 本装置
- 本装置 → (ISDN) → 本装置

本装置では、テンプレート着信機能を使用した不特定着信と、AAAによる認証を組み合わせることで、リモートアクセスサーバを実現することができます。

☛ 参照 MR1000 機能説明書「2.27 テンプレート着信機能」(P.117)

ここでは、ノートパソコンに PHS を繋いで外出先から本社のネットワークに接続する場合を例に説明します。



### ● 設定条件

- ISDN Uポートを使用してISDN回線に接続する
- テンプレートで使用するインタフェース : rmt30 から2個
- 以下からの着信を許可する

#### **[PC0<ノートパソコン+ PHS>で外出先から接続]**

- 受諾認証 ID : mobile-a
- 受諾認証パスワード : mobilepass-a
- PHSの電話番号は未登録

#### **[PC1<ノートパソコン+ PHS>で外出先から接続]**

- 受諾認証 ID : mobile-b
- 受諾認証パスワード : mobilepass-b
- PHSの電話番号は未登録

- 本社のLAN側のネットワークアドレス/ネットマスク : 192.168.1.0/24
- 外部のパソコンに割り当てるIPアドレス : 192.168.1.34、192.168.1.35

### こんな事に気をつけて

- テンプレート着信機能をサポートする回線は ISDN です (MP 接続はできません)。
- テンプレート着信で使用するインタフェースはテンプレート専用になります。テンプレート用に予約された rmt インタフェースには、remote 定義を設定しないでください。  
たとえば、rmt30～47 インタフェースをテンプレート用に予約した場合、remote 30～47 までの remote 定義を設定しないでください。
- テンプレート情報を定義する場合 (IP フィルタリングなど)、定義数は「テンプレート情報で設定した定義数×テンプレートで使用する rmt インタフェース数」で計算されるため、それを含めて装置最大定義数の範囲に収まるように定義してください。装置最大定義数を超えたときは、資源不足により該当機能が動作しない場合があります。
- 接続先情報を設定する場合、テンプレート用のインタフェースの個数分は設定しないでください。  
たとえば、接続先定義を最大 48 定義可能な装置で、10 インタフェースをテンプレート用に使用する場合、接続先定義の定義数は 38 となります。
- テンプレート情報と AAA 情報のユーザ側の設定に同じ項目がある場合は、個人情報である AAA 情報が適用されません。AAA 情報の未登録の項目に対しては、テンプレート情報の設定値が適用されます。
- 発信者番号による識別 (CLID 相手判定) を AAA 情報に設定していない場合は、発信者番号による相手判定は行いません (PPP のユーザ認証の結果だけで接続できるかどうかが決まります)。
- AAA 情報に同一ユーザ (パスワードも同一) が存在するときには、定義番号が小さい AAA ユーザ情報が優先されます。定義番号が大きいユーザ情報に発信者番号が一致する定義があり、定義番号が小さいユーザ情報に発信番号で識別を行わない定義がある場合も、定義番号の小さいユーザで着信が行われます。
- 共通 ID で複数の着信を行う場合は、AAA 情報のユーザ定義に、ID とパスワードだけを定義してください (個別情報を定義しないで、ID とパスワードだけのユーザ情報を定義すると共有 ID として扱われます)。

上記の設定条に従って設定を行う場合の設定例を示します。

## LAN0 情報を設定する

### 1. 設定メニューのルータ設定の「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

### 2. 「LAN 情報」でインタフェースが LAN0 の【修正】ボタンをクリックします。

「LAN0 情報 (物理 LAN)」ページが表示されます。

### 3. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

### 4. 以下の項目を指定します。

- IPv4 → 使用する
- IP アドレス → 指定する
  - IP アドレス → 192.168.1.1
  - ネットマスク → 24 (255.255.255.0)
  - ブロードキャストアドレス → ネットワークアドレス + オール 1

■ IP アドレス情報		
IPv4	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない	
IP アドレス	<input type="radio"/> DHCP で自動的に取得する	
	<input checked="" type="radio"/> 指定する	
	IP アドレス	<input type="text" value="192.168.1.1"/>
	ネットマスク	<input type="text" value="24 (255.255.255.0)"/>
	ブロードキャストアドレス	<input type="text" value="ネットワークアドレス + オール 1"/>



5. [保存] ボタンをクリックします。

## WAN0 情報を設定する

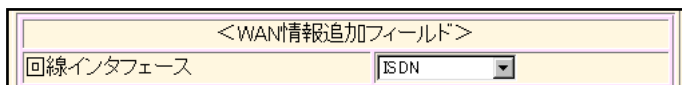
---

6. 設定メニューのルータ設定で「WAN 情報」をクリックします。

「WAN 情報」ページが表示されます。

7. 以下の項目を指定します。

- 回線インタフェース → ISDN



<WAN情報追加フィールド>	
回線インタフェース	ISDN

8. [追加] ボタンをクリックします。

「WAN1 情報 (ISDN)」ページが表示されます。

9. [保存] ボタンをクリックします。

## テンプレート情報を設定する

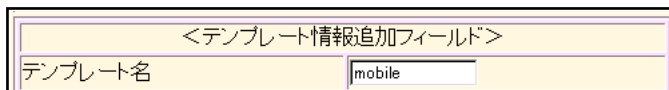
---

10. 設定メニューのルータ設定で「テンプレート情報」をクリックします。

「テンプレート情報」ページが表示されます。

11. 以下の項目を指定します。

- テンプレート名 → mobile



<テンプレート情報追加フィールド>	
テンプレート名	mobile

12. [追加] ボタンをクリックします。

「テンプレート情報 (mobile)」ページが表示されます。

13. [共通情報] をクリックします。

共通情報の設定項目と「基本情報」が表示されます。

**14. 以下の項目を指定します。**

- 使用インタフェース → WAN0
- 使用するrmtインタフェース → 30  
2
- 参照するAAA情報 → 指定する  
AAAグループID → 0

■基本情報	
テンプレート名	mobile
使用インタフェース	WAN0
使用するrmtインタフェース	rmt30 から 2 インタフェースを予約
MTUサイズ	1500 バイト
無通信監視タイマ	送受信パケット (について 0 秒)
参照するAAA情報	<input type="radio"/> 指定しない <input checked="" type="radio"/> 指定する AAAグループID 0

**15. [保存] ボタンをクリックします。****16. 「IP関連」をクリックします。**

IP関連の設定項目と「IP基本情報」が表示されます。

**17. 以下の項目を指定します。**

- 割当てIPアドレス → 設定する  
先頭IPアドレス → 192.168.1.34  
アドレス数 → 2

割当てIPアドレス	<input type="radio"/> 設定しない <input checked="" type="radio"/> 設定する
	先頭IPアドレス 192.168.1.34
	アドレス数 2

**18. [保存] ボタンをクリックします。****19. 設定メニューのルータ設定で「AAA情報」をクリックします。**

「AAA情報」が表示されます。

**20. 「グループID情報」をクリックします。**

「グループID情報」が表示されます。

**21. 以下の項目を指定します。**

- グループ名 → mobile

<グループID情報追加フィールド>	
グループ名	mobile

**22. [追加] ボタンをクリックします。**

「AAA情報 (mobile)」が表示されます。

**23. 「AAAユーザ情報」をクリックします。**

「AAAユーザ情報」が表示されます。

**24. 以下の項目を指定します。**

- ユーザID → mobile-a

<AAAユーザ情報追加フィールド>	
ユーザID	mobile-a

**25. [追加] ボタンをクリックします。**

「AAAユーザ情報 (0)」と「認証情報」が表示されます。

**26. 以下の項目を指定します。**

- 認証パスワード → mobilepass-a
- 発信者番号による識別 → 番号チェックしない

■ 認証情報		
ユーザID	mobile-a	
認証パスワード	*****	
発信者番号による識別	<input checked="" type="radio"/> 番号チェックしない <input type="radio"/> 番号チェックする	
	相手電話番号	
	相手サブアドレス	

**27. [保存] ボタンをクリックします。****28. 手順 26. ~ 27. を参考に、以下の項目を指定します。**

- ユーザID → mobile-b
- 認証パスワード → mobilepass-b

**29. 画面左側の [設定反映] 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。

# 索引

## A

ADSL 回線	19
ADSL モデム	110
arp エントリ	308
AS 外部経路	225
AS 境界ルータ	225

## B

BAP/BACP 機能	294
BGP/MPLS VPN	271
BGP4	109
BGP 経路の制御 (IPv4)	233
BSR (ブートストラップルータ)	300
B チャンネル	294

## C

CATV インターネット接続 (かんたん設定)	21
COM ポート	633
CUG (Closed Users Group)	612

## D

DHCP 機能	504
DHCP クライアント機能	510
DHCP サーバ機能	505
DHCP スタティック機能	508
DHCP リレーエージェント機能	512
DH グループ	129, 140
DNS サーバ	319
DNS サーバアドレスの自動取得機能	524
DNS サーバ機能	528
DNS サーバの自動切り替え機能 (逆引き)	522
DNS サーバの自動切り替え機能 (順引き)	520
DNS 問い合わせタイプフィルタ機能	526

## E

ECMP 機能	534
EoMPLS	263
Ethernet over IP ブリッジ	611
Ethernet フレーム	308

## F

FNA	597
-----	-----

## I

ID タイプ	153
--------	-----

IKE	129, 140
IKE セッション監視機能	466
IPsec 機能	373
IPsec クライアント	484
IPsec サーバ	484
IPv6	99
IPv6 DHCP クライアント機能	516
IPv6 over IPv4 トンネル	108
IPv6 トンネル	99
IPv6 ネットワークの追加	48
IPv6 フィルタリング	348
IP-VPN 接続	109
IP アドレス	166, 310, 500
IP アドレスの自動割り当て	505
IP トンネル	611
IP フィルタリング機能	309, 452
IP フィルタリングの条件	309
IP フィルタリングの設計方針	312
ISDN 接続 (IPv6)	91
ISDN 接続 (LAN)	73

## L

LAN のネットワーク間接続	41
LSA	222
LSP (トンネルラベルスイッチングパス)	243

## M

MAC アドレス	508
MED メトリック値	239
MIB	532
MPLS	271
MPLS LSP トンネル	243
MPLS 接続サービス	243
MPLS 網と LAN	272
MPLS 網と専用線	283
MSS 書き換え機能	462
MTU サイズ	308
MTU 分割機能	463

## N

NAT	108
NAT トラバーサル機能	484
NetBIOS サーバ	362

## O

OCN エコノミー	31
OSPFv2 (IPv4)	195
OSPF 経路の制御 (IPv4)	222

**P**

PIAFS 接続	627
PIM-DM	296
PIM-SM	300
PING	365
PPPoE 接続	64
PPPoE 接続 (かんたん設定)	17
PPPoE プロトコル	17
Proxy ARP	627
ProxyDNS	520

**R**

RFC1877	524
RIP 経路の制御 (IPv4)	166
RIP 経路の制御 (IPv6)	180
RP (ランデブーポイント)	300

**S**

SNMP	532
SNMP エージェント機能	532
SNTP	42
SPI	338, 377
SPT (最短経路)	300
STP	597

**T**

TCP 接続要求	309, 310, 312
TIME プロトコル	42
TOS	488, 500
TOS/Traffic Class	491
TOS/Traffic Class 値書き換え機能	488
TOS 値	309
TOS 値書き換え機能	452
Traffic Class 値	488, 500
Trap	532

**U**

URL フィルタ機能	530
------------	-----

**V**

VLAN ID	305
VLAN インタフェース	308
VLAN 機能	305
VLAN パケット	491
VLAN プライオリティマッピング機能	491
VoIP NAT トラバーサル機能	486
VPN	373, 374
VRRP 機能	573

**W**

Wakeup on LAN 機能	586
WAN 関連定義	601
WFQ 機能	500

**あ**

あて先情報	309, 488
アドレス変換機能	473
アドレスマスク	166, 310
アナログモデム	633
暗号情報	373

**い**

インターネットへ ISDN 接続 (かんたん設定)	24
インターネットへ専用線接続 (かんたん設定)	29

**え**

エリア ID	195
エリア境界ルータ	222

**お**

オフィスへ ISDN 接続 (かんたん設定)	33
オフィスへ専用線接続 (かんたん設定)	38

**か**

課金制御機能	593
課金制御機能設定	595
課金単位時間	593
課金単位時間設定	593
仮想的プライベートネットワーク	263, 271
可変 IP アドレス	150
簡易ホットスタンバイ機能	573, 574
かんたん設定メニュー	9
かんたんフィルタ	28

**き**

既存のネットワーク	14
基本 NAT	473
逆引き	522

**く**

クラスタリング機能	573, 578
グループ ID	578
グループ識別子	604
グローバルアドレス	31

**け**

経路制御	620
ケーブルモデム	21
ケーブルモデム接続	21

**こ**

構成定義情報切り替え予約	588, 591
高速デジタル専用線	118
固定 IP アドレス	127, 138, 376
コネクション確立要求	310

**さ**

サーバの公開 (PPPoE 接続)	476
サーバの公開 (ネットワーク型接続)	479
サーバの公開 (プライベート LAN 接続)	474, 482

**し**

シェーピング機能	460, 493
システムログ	471
システムログの確認	472
自動鍵交換	127, 138, 373, 374
手動鍵交換	373, 376
準スタブエリア	210
順引き	520
冗長化ネットワーク	237
冗長構成の通信経路	239
省略値	27
新 TOS	488

**す**

スイッチング HUB	305, 617
スケジュール機能	588
スケジュール予約	588
スタブエリア	210

**せ**

制御	309
静的 NAT	473
セキュリティ	309
セグメント接続/分割 (かんたん設定)	13
接続先監視機能	465
専用線接続	59
専用線接続 (LAN)	79

**そ**

送信元情報	309, 488
-------	----------

**た**

帯域制御機能	460, 500
ダイヤルアップ接続	21

**ち**

超過課金	309
------	-----

**つ**

通信の負荷分散	239
通信バックアップ	620, 633

**て**

データ圧縮機能	498
電話番号変更予約	588, 590

**と**

動画・音声	296
動的 NAT	473
動的経路 (RIP) 機能	468
ドメイン	520
トラフィックの制御	233
トランジット	235
トンネリング	99
トンネルエンドポイント	244, 253

**に**

認証情報	373
------	-----

**ね**

ネットワーク	73, 79
ネットワーク分割	13

**は**

バックアップルータ	573
バックボーンエリア	195, 222
発信抑止予約	588

**ふ**

フィルタリング条件 (ルーティング)	166
フィルタリングの設計方針 (ルーティング)	167
負荷分散通信	534
プライオリティ	491
プライベート LAN 構築	53
プライベート LAN 構築 (かんたん設定)	9
プライベートアドレス	31, 311
ブリッジ	597

ブリッジグループピング .....	617
ブリッジグループピング機能 .....	604
フレームリレー接続 (LAN) .....	85
フレッツ・ADSL .....	17, 19, 64
プロトコル .....	309, 488, 491, 500

---

## へ

閉域ネットワーク .....	85
ヘッダ圧縮機能 .....	498

---

## ほ

方向 .....	166, 180, 309
ポート番号 .....	500
ホストデータベース .....	528
ホストデータベース情報 .....	508
ポリシーベースネットワーク .....	488

---

## ま

マスターータ .....	573
マルチ NAT .....	31
マルチ NAT 機能 .....	452, 473
マルチキャスト機能 .....	296
マルチキャスト・パケット .....	300
マルチダイヤル .....	24
マルチリンク機能 .....	294
マルチルーティング機能 .....	583

---

## む

無通信監視タイマ .....	593
----------------	-----

---

## め

メトリック値 .....	166, 180
--------------	----------

---

## ゆ

優先順位 .....	312
ユニキャスト .....	296

---

## り

リモートアクセスサーバ .....	639
リモートパワーオン機能 .....	586
リモートパワーオン予約 .....	589

---

## れ

レイヤ 2VPN の構築 .....	263
レイヤ 3VPN の構築 .....	271

---

## **MR1000 Web 設定事例集**

発行日	2005年3月
第2版	K1N-D-04167B
発行責任	オムロン株式会社

Printed in Japan

---

- ・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。
- ・落丁、乱丁本は、お取り替えいたします。