GIGABIT GATE

L2TPv3対応 GigabitGate

FutureNet XR-1200

ユーザーズガイド

Ver3.5.0対応版

Release 2

CENTURY SYSTEMS

目次

はじめに

◆ご注意

1 本装置の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸したために生じた損害などの純粋経済損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承下さい。

2 通信情報が漏洩した事による経済的、精神的損害につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承下さい。

3 本書の内容の一部または全部を無断で転載、複写することを禁じます。

4 本書およびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。

5 本書の内容については万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきの点がありましたらご連絡下さい。

◆商標の表示

□「GIGABIT GATE」はセンチュリー・システムズ株式会社の登録商標です。

□「FutureNet」はセンチュリー・システムズ株式会社の商標です。

□下記製品名等は米国Microsoft Corporationの登録商標です。
Microsoft、Windows、Windows XP、Windows Vista

□下記製品名等は米国Apple Inc.の登録商標です。
Macintosh、Mac OS X

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

ご使用にあたって

安全にお使いいただくために

この取扱説明書では、FutureNet XR-1200（以下「本製品」）をお使いになる方、および周囲の人への危害や財産への損害を未然に防ぎ、製品を安全に正しくお使いいただくための注意事項を記載しています。
安全にご使用いただくために、必ず下記をお読みいただき、記載事項をお守りください。
また、お読みになった後は、いつでも読める場所へ大切に保管してください。

以下の注意事項は、これを無視して誤った取り扱いで想定される「損傷や損害」を示しています。

「使用者、および周囲の人が多大な損傷を負う可能性が想定される内容」

「使用者、および周囲の人が損傷を負う可能性が想定される内容、または物的損害のみの発生が想定される内容」

また、機器の取り扱いを始める前に、電気回線の危険性、および一般的な事故防止対策に十分注意してください。

絵表示の意味

危険 使用者が死亡または重傷を負う可能性が想定される内容	**注意** 人が障害を負う可能性および物的損害の発生が想定される内容

◆重要な警告

注意	ご使用の際は取扱説明書に従って正しい取り扱いをしてください。
危険	万一、煙が出ている、異常な発熱をしている、変なにおいがする、変な音がする、といった場合は、すぐに使用を中止してください。 そのまま使用すると、火災、感電、故障の原因になります。 すぐに、本製品に接続するACアダプタ、もしくはAC電源、その他のケーブル類を取り外してください。 煙などが出なくなるのを確認してからお買い上げの販売店、または弊社サポートデスクに連絡してください。
危険	装置内部へ異物（金属片・水・液体）を入れないでください。 万一、異物が製品の内部に入った場合は、まず電源を外し、お買い上げの販売店にご連絡ください。 そのまま使用すると、火災の原因になります。
注意	万一の異常時にすぐに電源プラグを抜けるように、コンセントの周りには物を置かないでください。

ご使用にあたって

◆使用環境や設置に関する事項

	本体を下記のような場所で使用したり放置しないでください。 故障や火災、感電、変形、変色、誤動作の原因になります。 ・直射日光の当たる場所 ・ストーブのそばなど、高温の場所 ・調理場や風呂場、加湿器のそばなど、湿気の多い場所 ・ホコリの多い場所 ・振動や衝撃の加わる場所 ・ヒーター、クーラーの吹き出し口など、温度変化の激しい場所 ・強い電波や磁界、静電気、電気ノイズが発生する場所
	人の通行を妨げる場所には、設置しないでください。 本製品に接触したり、落下したりして、けがの原因になります。
	製品、および電源コード、接続ケーブルは、赤ちゃんや小さなお子さまの手の届かないところに設置してください。 感電、けがなどの原因になります。
	屋外に設置しないでください。 屋外で使用できる構造にはなっていないので、故障の原因になります。
	ぐらついた台の上や、傾いたところなど、不安定な場所に置かないでください。 落下したりして、火災、けが、故障の原因になります。
	製品の仕様で定められた使用温度範囲以外では使用しないでください。
	通気孔をふさがないでください。 通気孔は本体内部の温度上昇を防ぐものです。本体を重ねたり、物を置いたり、立てかけたりして通気孔をふさがないでください。 内部の発熱などにより、火災、感電、故障の原因になります。
	本製品をぬらしたり、水気の多い場所で使用しないでください。 お風呂場、雨天、降雪中、海岸、水辺での使用は、火災、感電、故障の原因になります。
	結露するような場所で使用しないでください。 温度差の激しい環境を急に移動した場合、結露する恐れがありますのでご注意ください。 変形、変色、火災、故障の原因になります。 結露した場合は、乾燥させるか、ご使用になる場所で電源を入れずに数時間放置した後、ご使用ください。
	本製品は日本国内仕様です。 国外で使用した場合、弊社は一切責任を負いかねます。

ご使用にあたって

◆製品の取り扱いに関する事項

注意	本製品の取り付けや、取り外しは、必ず電源を切ってからおこなってください。
注意	本製品のコネクタ部にホコリが付着していないことを確認してからコネクタ部を差し込んでください。 ホコリは、火災、感電の原因になります。
危険	本製品を使用中は、ぬれた手で本製品に触れないでください。 感電の原因になります。
注意	素手で機器のコネクタの接点などに触れないでください。 部品が静電破壊する場合があり、故障の原因になります。
注意	説明と異なる接続をしないでください。 また、本製品への接続を間違えないように十分注意してください。 故障の原因となります。
危険	本製品の分解、改造は、絶対にしないでください。 また、ご自分で修理しないでください。 火災、感電、やけど、動作不良の原因になります。 修理は弊社サポートデスクにご依頼ください。 分解したり、改造した場合、保証期間内であっても有料修理となる場合があります。
注意	製品にディップスイッチがある場合､ディップスイッチの操作は電源を切った状態でおこなってください。 また、針などの鋭利なものや通電性のあるもので操作しないでください。 故障や感電の原因になります。
注意	本製品に乗ったり、重い物を載せたり、挟んだりしないでください。 本体が壊れて、けがの原因となります。また、故障の原因になります。
危険	近くに雷が発生したときは、機器の取り扱い、およびケーブルの接続や取り外しをしないでください。 製品の導入や保守の作業もおこなわないでください。 また、AC アダプタ、もしくは AC 電源を接続しているコンセントから抜いて、ご使用をお控えください。 雷によって、火災、感電、故障の原因になります。
注意	ベンジン、シンナー、アルコール等の引火性溶剤で拭かないでください。 本製品の変色や変形、変質の原因となることがあります。また、引火する恐れがあります。 普段はやわらかい布で、汚れのひどいときは水で薄めた中性洗剤を少し含ませて汚れを拭き取り、やわらかい布でから拭きしてください。

◆接続ケーブルに関する事項

注意	接続ケーブルは、足などに引っかけないように配線してください。 足を引っかけると、けがや接続機器の故障の原因となります。
危険	接続ケーブルの上に重量物を載せないでください。また、熱器具のそばに配線しないでください。 ケーブル被覆が破れ、接触不良などの原因となります。

ご使用にあたって

◆電源コードに関する事項

	電源コードの扱いに注意ください。 電源コードは付属のものを使用し、次のことに注意して取り扱ってください。取り扱いを誤ると、ケーブルが痛み、火災や感電、動作不良の原因になります。 ・物を乗せない ・引っ張らない ・ねじらない ・折り曲げない ・押しつけない ・加工しない ・熱器具のそばで使わない
	電源コードを AC コンセントから抜くときは、必ずプラグ部分を持って抜いてください。 コードを引っ張るとコードに傷がつき、火災、感電、故障の原因になります。
	電源コードが傷ついたり、コンセントの差し込みがゆるいときは使用しないでください。 火災、感電、故障、データの消失、または破損の原因になりますので、お買い上げの販売店、または弊社サポートデスクに連絡してください。
	本装置に電源ケーブルが付属している場合は、必ず付属の電源ケーブルをご使用ください。 不適切なケーブルをご使用になると、本装置の故障や火災、感電の恐れがあります。 また、付属の電源ケーブルは本装置専用品です。他の装置には使用しないでください。普段はやわらかい布で、汚れのひどいときは水で薄めた中性洗剤を少し含ませて汚れを拭き取り、やわらかい布でから拭きしてください。

◆電源に関する事項

	本装置では、AC 100V ± 10V（50/60Hz）の電源以外は絶対に使用しないでください。 異なる電圧などで使用すると、火災、感電の原因になります。
	ぬれた手で電源プラグに絶対触れないでください。 感電の原因になります。
	電源プラグは、コンセントの奥まで確実に差し込んでください。 差し込みが不十分な場合、接触不良で火災、感電の原因になります。
	本装置の電源ケーブルの接続は、テーブルタップ、分岐コンセント、分岐ソケットを使用したタコ足配線にしないでください。 AC コンセントが加熱し、火災、感電の原因になります。
	電源プラグにドライバなどの金属が触れないようにしてください。 火災、感電、故障の原因になります。
	電源プラグの金属部分、およびその周辺にホコリが付着している場合は、乾いた布でよく拭き取ってください。 そのまま使うと接触不良で火災の原因になります。

ご使用にあたって

◆AC アダプタに関する事項

AC アダプタが添付されている製品の場合は、以下のことにご注意ください。

	AC アダプタは、AC 100V 以外の電圧で使用しないでください。 本製品に添付の AC アダプタは AC 100V 専用です。指定以外の電源電圧で使用しないでください。 火災、感電、故障の原因になります。
	AC アダプタを本製品以外の機器で使用しないでください。 火災、感電、故障の原因になります。
	ぬれた手で AC アダプタに絶対触れないでください。 感電の原因になります。
	AC アダプタを水などでぬれやすい場所で使用しないでください。 火災、感電、故障の原因になります。
	AC アダプタを保温・保湿性の高いもの（じゅうたん、カーペット、スポンジ、緩衝材、段ボール箱、発泡スチロールなど）の上では使用しないでください。 火災、感電、故障の原因になります。
	AC アダプタは、タコ足配線しないでください。 火災、感電、故障の原因になります。
	AC アダプタの金属部分、およびその周辺にホコリが付着している場合は、乾いた布でよく拭き取ってください。 そのまま使うと接触不良で火災の原因になります。
	DC プラグの抜き差しにご注意ください。 DC ジャック以外の端子に電源を接続しないでください。 火災、感電、故障の原因になります。 また、抜き差しするときは、必ず DC プラグや AC アダプタ本体を持っておこなってください。

◆保管に関する事項

	製品を保管する際は、製品の仕様で定められた保存温度、湿度範囲を守ってください。 湿気やホコリの多いところ、または高温となるところには保管しないでください。 故障の原因になります。
	長時間、使用しないときは、安全のため本製品に接続する電源コードもしくは AC アダプタを取り外してください。 発熱、発火、故障の原因になります。
	火の中に投入したり、加熱したりしないでください。

◆廃棄について

	本製品の廃棄にあたっては、地方自治体の条例、または規則に従ってください。

パッケージの内容物の確認

本製品のパッケージには以下の品が同梱されております。本製品をお使いいただく前に、内容物が全て揃っているかご確認ください。
万が一、不足がありましたら、お買い上げいただいた店舗、または、弊社サポートデスクまでご連絡くださいますようお願いいたします。

同梱品一覧

XR-1200本体	１台
はじめにお読みください	１部
安全にお使いいただくために	１部
電源コード	１本
海外使用禁止シート	１部
保証書	１部
ラックマウント用レール	１式
ラックマウントガイド	１部

第1章

本装置の概要

Ⅰ．本装置の特長

XR-1200(以下、本装置)は、次のような特長を持っています。

◆ギガビット対応
本装置は、ギガビット対応のインタフェースを 4 ポート保有しており、最大 1Gpbs の高速ルーティングを提供します。

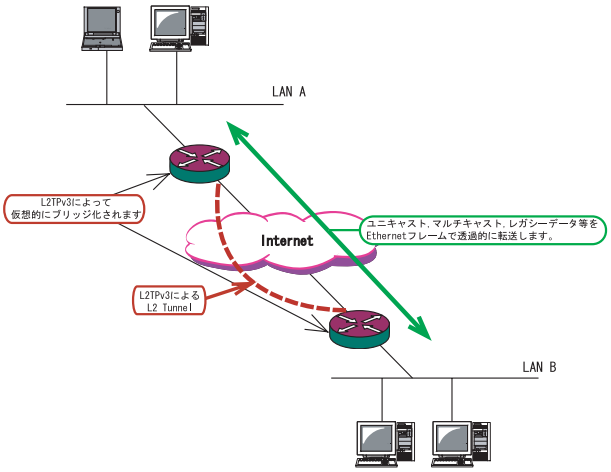
◆ Century Systems 独自 MIB に対応
本製品は標準 MIB-II の他、当社独自の MIB/Trap をサポートしています。
独自 MIB/Trap ではシステムや各種サービス、L2TPv3 サービスに関する情報が取得でき、保守性やメンテナンス性に優れた運用が可能になります。

◆ L2TPv3 機能を搭載
本製品は次世代ネットワークのトンネリング及び VPN における主要技術になりつつある L2TPv3 機能を搭載しています。

L2TPv3 機能は、IP ネットワーク上のルータ間で L2TP トンネルを構築します。
これにより本製品が仮想的なブリッジとなり、遠隔のネットワーク間でレイヤ 2 通信が可能となります。

レイヤ 2 でトンネリングするため、2 つのネットワークは HUB で繋がった１つの Ethernet ネットワークとして使うことができます。また、上位プロトコルに依存せずにネットワーク通信ができ、TCP/IP だけでなく、任意の上位プロトコル(IPX、AppleTalk、SNA 等)を透過的に転送することができます。

また、L2TPv3 機能は、従来の専用線やフレームリレー網ではなく IP 網で利用できますので、低コストな運用が可能です。



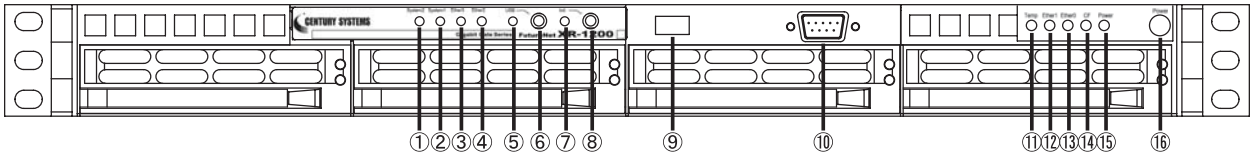
L2TPv3 機能につきましては、
「第 15 章 L2TPv3 機能」をご参照ください。

◆ IPsec 機能を搭載
本製品の IPsec 機能を使うことで、インターネット上で複数の拠点をつなぐ IP 仮想専用線(インターネット VPN)の構築に利用できます。

◆ 802.1q VLAN に対応
本製品の各 Ethernet ポートで VLAN ID が最大 1024 個までの 802.1q マルチプル VLAN を構築できます。
インタフェース毎に複数の VLAN セグメントを設定し、LAN 内でのセキュリティを強化することができます。

Ⅱ．各部の名称と機能

◆製品前面



① System 2 LED(緑)
本装置の動作状況を表示します。
　動作状態 ： 

② System 1 LED(緑)
本装置では使用しません。

③ Ether 3 LED(緑)　④ Ether 2 LED(緑)
⑫ Ether 1 LED(緑)　⑬ Ether 0 LED(緑)
本装置の各 Ether ポートの状態を示します。
　Link DOWN　：
　Link UP　：
　データ通信時 ： 

⑤ USB Status LED(橙)
オプション USB フラッシュディスクの接続状態を表示します。
　接続時　： 
　動作状態 ：
　「USB スイッチ」で取り外し操作時 ： 

⑥ USB スイッチ
本装置に接続しているオプション USB フラッシュディスクを取り外すときに押します。
詳細は「第37章 運用管理設定」をご参照ください。

⑦ Init Status LED(橙)
本装置の起動状態を表示します。
　起動中　： 
　「Init スイッチ」で初期設定にて起動中 ：
　起動完了時 ：

⑧ Init スイッチ
このスイッチを長押しすることで、本装置を工場出荷状態に戻します。
詳細は「第37章 運用管理設定」をご参照ください。

⑨ USB インタフェース
オプションの USB フラッシュデバイスを接続します。
オプション USB フラッシュデバイス以外の機器を接続することはできません。

⑩ RS-232 ポート(D-Sub 9 ピン)
このポートは、使用できません。

⑪ Temp LED(赤)
本装置の温度状態を表示します。
　システムの内部温度が一定以上になった時 ：

⑭ CF LED(橙)
本装置内部に搭載している CF カードの使用状態を表示します。
　CF へのアクセス時 ：

⑮ Power LED(緑)
本装置の電源の状態を表示します。
　電源が投入されている状態 ：

⑯ Power スイッチ
本装置を起動させるには、スイッチを押します。

また、稼働中にスイッチを押すと、動作が停止して待機状態になります。

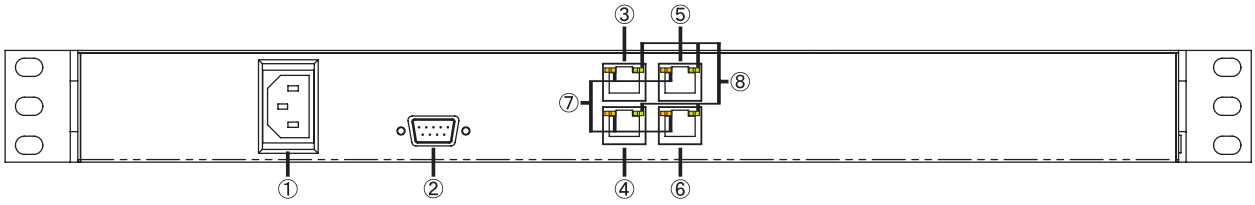
※待機状態とは、電源オフ状態と同じですが、本装置には通電している状態です。

ただし、通常は設定画面の「システム設定」→「本体停止」画面で待機状態にしてください。
待機状態にするのは、本装置がハングアップした時などの、非常時のみにしてください。

完全に電源をオフにする場合は、電源スイッチを短押（１秒程度）してください。

Ⅱ．各部の名称と機能

◆製品背面



① 電源ケーブル差し込み口

② RS-232 ポート(D-Sub 9 ピン)
モデム /TA を接続します。
ダイヤルアップやアクセスサーバ機能を使用するときに使用します。

③ Ether0 ポート(RJ-45)
④ Ether1 ポート(RJ-45)
⑤ Ether2 ポート(RJ-45)
⑥ Ether3 ポート(RJ-45)
Ethernet 規格の LAN ケーブルを接続します。
ポートは Auto-MDIX 対応です。

搭載されているインタフェース / ポートは、上記のもの以外は使用できません。

⑦ 速度表示ランプ（緑 / 橙）
Ethernet の接続速度を示します。
ランプは以下のようなパターンで点灯/消灯します。

10Base-T モード ：
100Base-TX モード ：
1000Base-T モード ：

⑧ LINK ランプ（緑）
Ethernet ケーブルのリンク状態を示します。
ランプは以下のようなパターンで点灯/消灯します。

Link DOWN ：
Link UP ：
データ送受信時 ：

III．動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

・本製品に接続するコンピュータの全てに、10Base-T または 100Base-TX の LAN ボード / カードがインストールされていること。

・ADSL モデムまたは CATV モデムに、10Base-T または 100Base-TX のインタフェースが搭載されていること。

・本製品と全てのコンピュータを接続するためのハブやスイッチングハブが用意されていること。

・本製品と全てのコンピュータを接続するために必要な種類のネットワークケーブルが用意されていること。

・シリアルポートを使う場合は、接続に必要なシリアルケーブルが用意されていること。

◆ソフトウェア環境

・TCP/IP を利用できる OS がインストールされていること。

・接続されている全てのコンピュータの中で少なくとも 1 台に、InternetExplorer5.0 以降か NetscapeNavigator6.0 以降がインストールされていること。

なおサポートにつきましては、本製品固有の設定項目と本製品の設定に関係する OS 上の設定に限らせていただきます。
OS 上の一般的な設定やパソコンにインストールされた LAN ボード / カードの設定、各種アプリケーションの固有の設定等のお問い合わせについてはサポート対象外とさせていただきますので、あらかじめご了承ください。

第2章

本装置の設置

本装置の設置

本装置と ADSL/ ケーブルモデムやコンピュータは、以下の手順で接続してください。

1 本装置と ADSL/ ケーブルモデムやパソコン・HUB など、接続する全ての機器の電源が OFF になっていることを確認してください。

2 本装置の背面にある Ether1 ポートと ADSL/ ケーブルモデムや ONU を、LAN ケーブルで接続してください。
本装置の Ethernet ポートは Auto-MDIX 対応です。

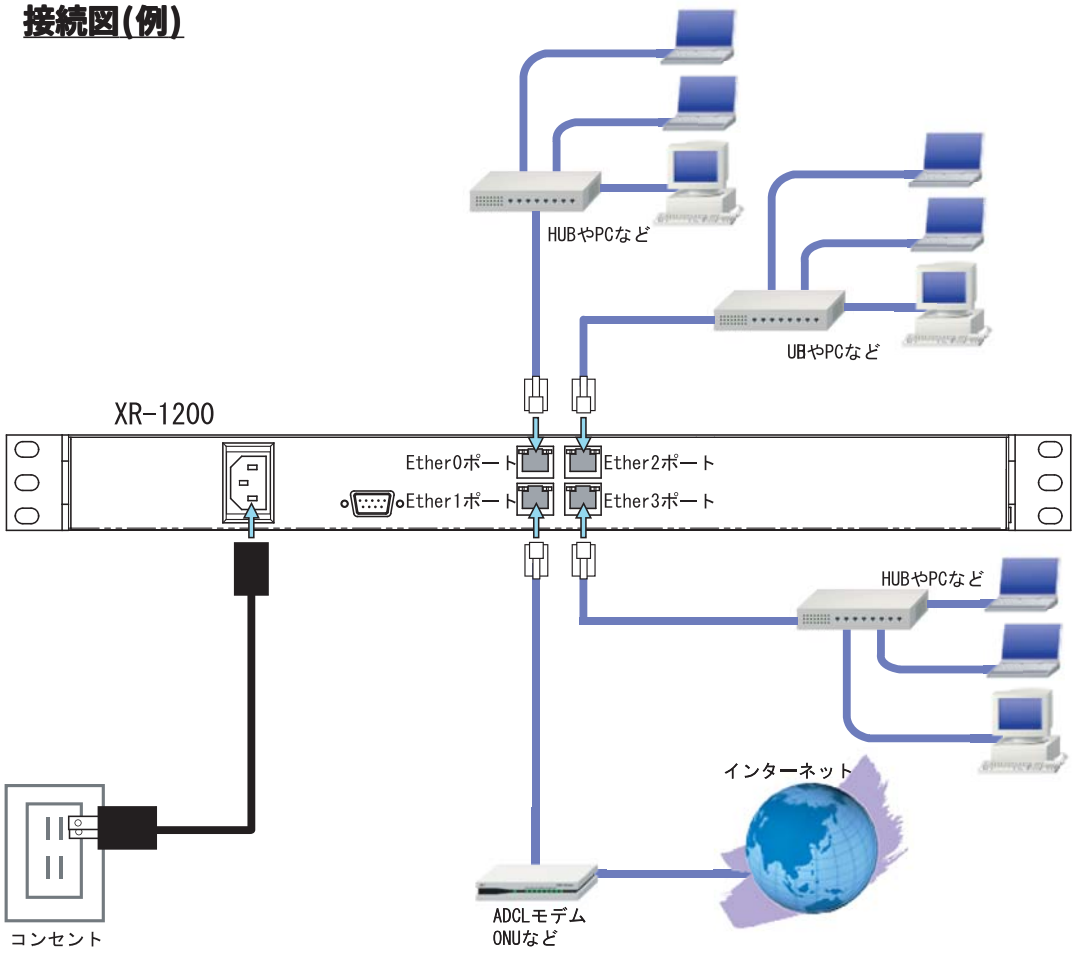
3 本装置の背面にある Ether0 ポートと HUB や PC を LAN ケーブルで接続してください。
本装置の Ethernet ポートは Auto-MDIX 対応です。

4 本装置と電源コード、電源コードとコンセントを接続してください。

5 全ての接続が完了しましたら、本装置と各機器の電源を投入してください。

本装置は、全ての Ethernet ポート(Ether0～Ether3)において認定制度に基づく設計認証を受けていますので、通信事業者が設置した ADSL モデムおよび ONU 等を直接接続することが可能です。

接続図(例)



第3章

コンピュータのネットワーク設定

第３章 コンピュータのネットワーク設定

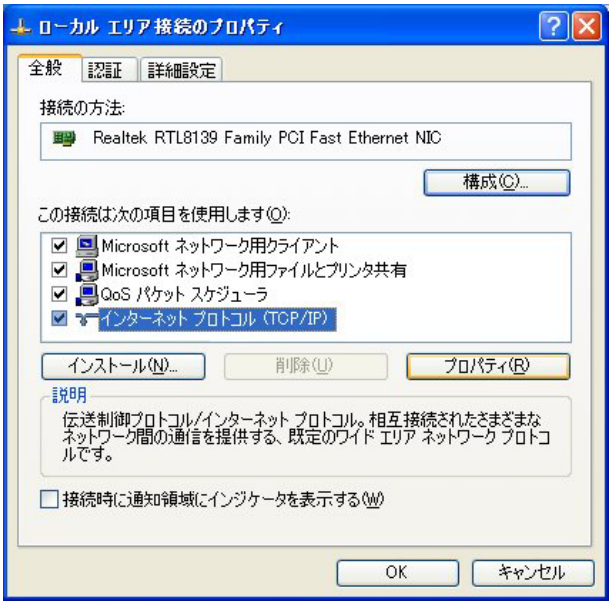
Ⅰ．Windows XP のネットワーク設定

ここではWindowsXPが搭載されたコンピュータのネットワーク設定について説明します。

1 「コントロールパネル」→「ネットワーク接続」から、「ローカル接続」を開きます。

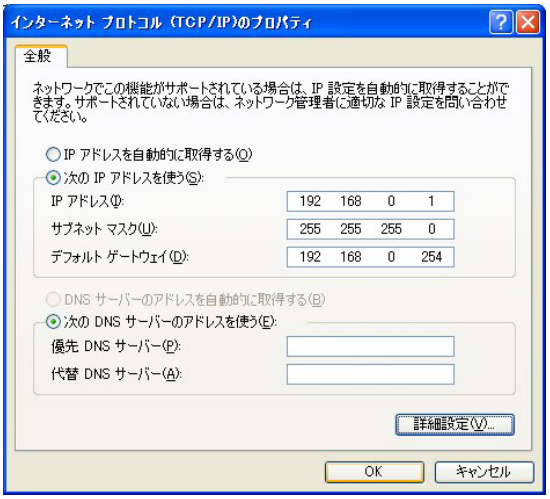
2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコル(TCP/IP)」を選択して「プロパティ」ボタンをクリックします。



4 「インターネットプロトコル(TCP/IP)」の画面では、「次の IP アドレスを使う」にチェックを入れて以下のように入力します。

IP アドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



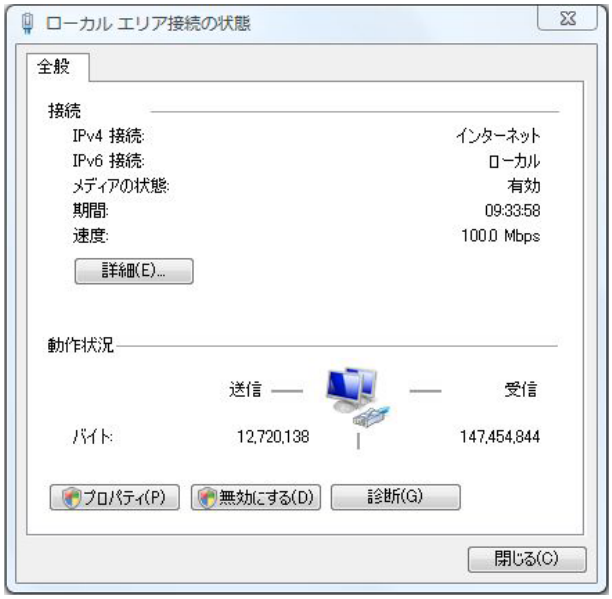
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

II．Windows Vistaのネットワーク設定

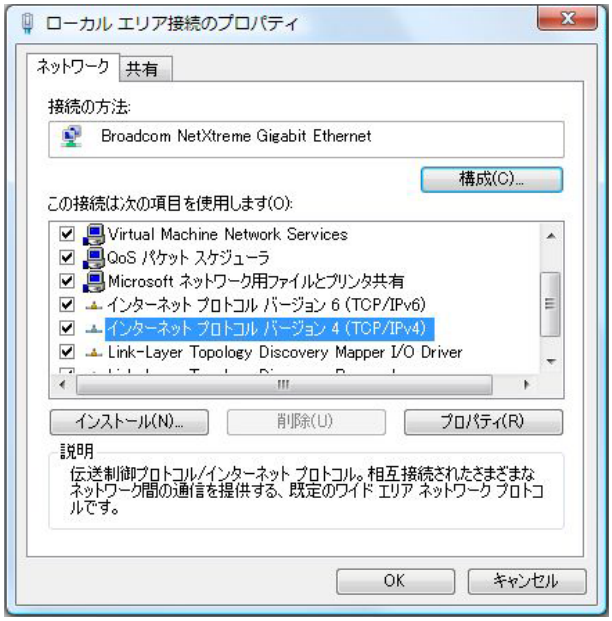
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

1 「コントロールパネル」→「ネットワークと共有センター」→「ネットワーク接続の管理」から、「ローカル接続」を開きます。

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

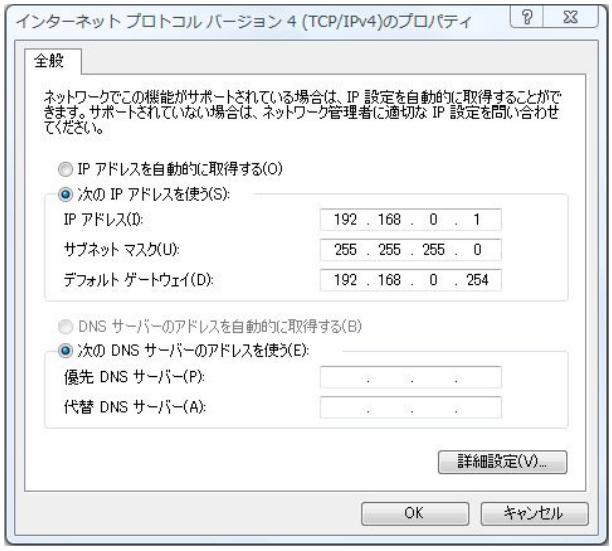


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



4 「インターネットプロトコルバージョン4(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



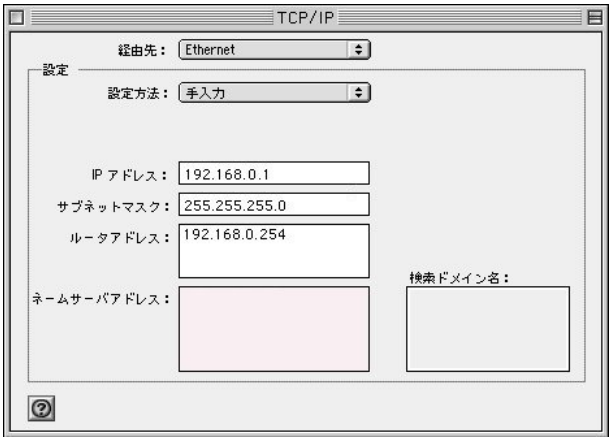
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

III. Macintoshのネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

1 「アップルメニュー」から「コントロールパネル」→「TCP/IP」を開きます。

2 経由先を「Ethernet」、設定方法を「手入力」にして、以下のように入力してください。
IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
ルータアドレス「192.168.0.254」

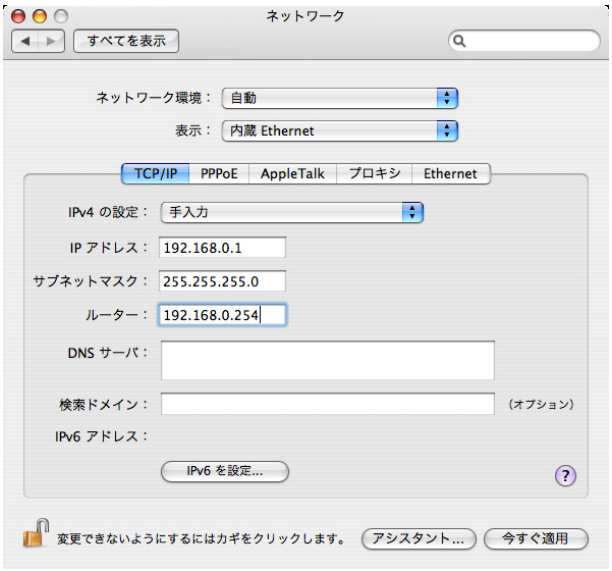


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これで本装置へログインする準備が整いました。

ここでは、Mac OS Xのネットワーク設定について説明します。

1 「システム環境設定」から「ネットワーク」を開きます。

2 ネットワーク環境を「自動」、表示を「内蔵Ethernet」、IPv4の設定を「手入力」にして、以下のように入力してください。
IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
ルーター「192.168.0.254」



3 ウィンドウを閉じて設定の変更を適用します。これで、本装置へログインする準備が整いました。

Ⅳ．IPアドレスの確認と再取得

◆Windows XP/Vistaの場合

1 「スタート」→「プログラム」→「アクセサリ」→「コマンドプロンプト」を開きます。

2 以下のコマンドを入力すると、現在のIP設定がウィンドウ内に表示されます。

```
c:\>ipconfig /all
```

3 IP設定のクリアと再取得をするには以下のコマンドを入力してください。

```
c:\>ipconfig /release   (IP設定のクリア)
c:\>ipconfig /renew     (IP設定の再取得)
```

本装置のIPアドレス・DHCPサーバ設定を変更したときは、必ずIP設定の再取得をするようにしてください。

◆Macintoshの場合

IP設定のクリア/再取得をコマンド等でおこなうことはできませんので、Macintosh本体を再起動してください。

本装置のIPアドレス・DHCPサーバ設定を変更したときは、必ずIP設定の再取得をするようにしてください。

第4章

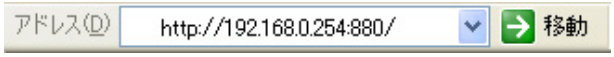
設定画面へのログイン

設定画面へのログイン方法

1 各種ブラウザを開きます。

2 ブラウザから設定画面にアクセスします。

ブラウザのアドレス欄に、以下の IP アドレスとポート番号を入力してください。



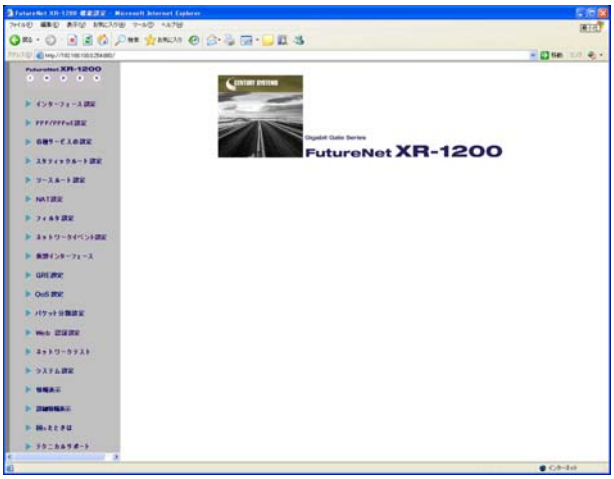
「192.168.0.254」は、Ether0 ポートの工場出荷時のアドレスです。
アドレスを変更した場合は、そのアドレスを指定してください。
設定画面のポート番号 880 は変更することができません。

3 次のような認証ダイアログが表示されます。

4 ダイアログ画面にパスワードを入力します。

工場出荷設定のユーザー名とパスワードはともに「admin」です。
ユーザー名・パスワードを変更している場合は、それにあわせてユーザー名・パスワードを入力します。

5 ブラウザ設定画面が表示されます。



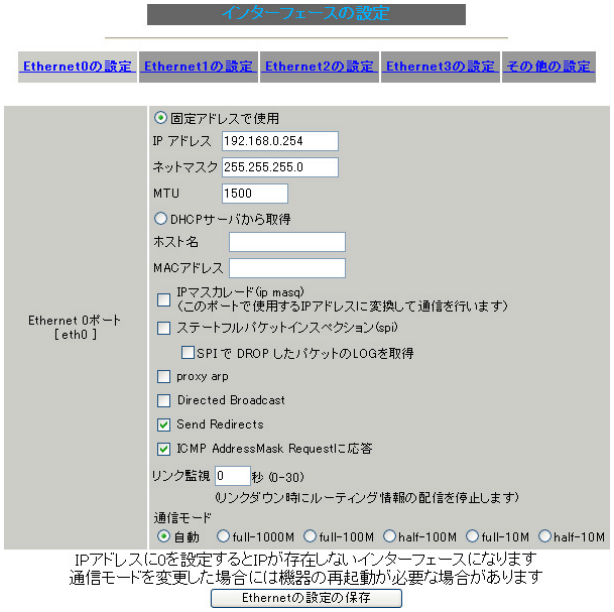
第5章

インタフェース設定

Ⅰ．Ethernet ポートの設定

◆各 Ethernet ポートの設定

ここでは本装置の各 Ethernet ポートの設定をおこないます。
Web設定画面「インターフェース設定」→「Ethernet0 (または 1、2、3)の設定」をクリックして画面を開き、各インタフェースについてそれぞれ必要な情報を入力、設定します。



(画面は Ethernet0 での表示例です)

[固定アドレスで使用]

○ IP アドレス
○ネットマスク
IP アドレス固定割り当ての場合にチェックし、IP アドレスとネットマスクを入力します。
IPアドレスに“０”を設定すると、そのインタフェースは IP アドレス等が設定されず、ルーティング・テーブルに載らなくなります。
OSPFなどで使用していないインタフェースの情報を配信したくないときなどに“０”を設定してください。

○ MTU
「Path-MTU-Black-HOLE」現象が発生した場合等は、ここの値を変更することで回避できます。通常は初期設定の 1500byte のままでかまいません。

[DHCP サーバから取得]

○ホスト名
○ MAC アドレス
IP アドレスを DHCP で割り当てる場合にチェックして、必要であればホスト名と MAC アドレスを設定します。

○ IP マスカレード（ip masq）
チェックを入れると、その Ethernet ポートで IP マスカレードされます。

○ステートフルパケットインスペクション(spi)
チェックを入れると、その Ethernet ポートでステートフルパケットインスペクション(SPI)が適用されます。

○ SPI で DROP したパケットの LOG を取得
チェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 26 章 補足：フィルタのログ出力内容について」をご覧ください。

○ proxy arp
Proxy ARP を使う場合にチェックを入れます。

○ Directed Broadcast
チェックを入れると、そのインタフェースにおいて Directed Broadcast の転送を許可します。

Directed Broadcast
IP アドレスのホスト部がすべて 1 のアドレスのことです。
ex> 192.168.0.0/24 の Directed Broadcast は 192.168.0.255 です。

○ Send Redirects
チェックを入れると、そのインタフェースにおいて ICMP Redirects を送出します。

ICMP Redirects
他に適切な経路があることを通知する ICMP パケットのことです。

Ⅰ．Ethernetポートの設定

本装置のインタフェースのアドレス変更は、直ちに設定が反映されます。
設定画面にアクセスしているホストやその他クライアントのIPアドレス等も本装置の設定に合わせて変更し、変更後のIPアドレスで設定画面に再ログインしてください。

○ICMP AddressMask Requestに応答
NW監視装置によっては、LAN内装置の監視をICMP Address Maskの送受信によっておこなう場合があります。
チェックを入れると、そのインタフェースにて受信したICMP AddressMask Request(type=17)に対して、 Reply(type=18)を返送し、インタフェースのサブネットマスク値を通知します。
チェックをしない場合は、Requestに対して応答しません。

○リンク監視
Ethernetポートのリンク状態の監視を定期的におこないます。
監視間隔は、1-30秒の間で設定できます。
また、0秒で設定するとリンク監視をおこないません。
OSPFの使用時にリンクのダウンを検知した場合、そのインタフェースに関連付けられたルーティング情報の配信を停止します。再度リンク状態がアップした場合には、そのインタフェースに関連付けられたルーティング情報の配信を再開します。

○通信モード
本装置のEthernetポートの通信速度・方式を選択します。工場出荷設定では「自動」(オートネゴシエーション)となっていますが、必要に応じて通信速度・方式を選択してください。
選択モードは「自動」、「full-1000M」、「full-100M」、「half-100M」、「full-10M」、「half-10M」です。

入力が終わりましたら「Ethernetの設定の保存」をクリックして設定完了です。
設定はすぐに反映されます。

II．Ethernetポートの設定について

[ステートフルパケットインスペクション]
ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能とも言えるものです。
通常はWANからのアクセスを全て遮断し、WAN方向へのパケットに対応するLAN方向へのパケット(WANからの戻りパケット)に対してのみポートを開放します。
これにより、自動的にWANからの不要なアクセスを制御でき、簡単な設定でより高度な安全性を保つことができます。

ステートフルパケットインスペクション機能を有効にすると、そのインタフェースへのアクセスは一切不可能となります。
ステートフルパケットインスペクション機能とバーチャルサーバ機能を同時に使う場合等は、パケットフィルタリングの設定をおこなって、外部からアクセスできるように設定する必要があります。
「第26章 パケットフィルタリング機能」を参照してください。

[PPPoE接続時のEthernetポート設定]
PPPoE回線に接続するEthernetポートの設定については、実際には使用しない、ダミーのプライベートIPアドレスを設定しておきます。

本装置がPPPoEで接続する場合には”ppp”という論理インタフェースを自動的に生成し、このppp論理インタフェースを使ってPPPoE接続をおこなうためです。

物理的なEthernetポートとは独立して動作していますので、「DHCPサーバから取得」の設定やグローバルIPアドレスの設定はしません。
PPPoEに接続しているインタフェースでこれらの設定をおこなうと、正常に動作しなくなる場合があります。

[IPsec通信時のEthernetポート設定]
本装置をIPsecゲートウェイとして使う場合は、Ethernetポートの設定に注意してください。
IPsec通信をおこなう相手側のネットワークと同じネットワークのアドレスが本装置のEthernetポートに設定されていると、正常にIPsec通信がおこなえません。

たとえば、IPsec通信をおこなう相手側のネットワークが192.168.1.0/24で、且つ、本装置のEther1ポートに192.168.1.254が設定されていると、正常にIPsec通信がおこなえません。

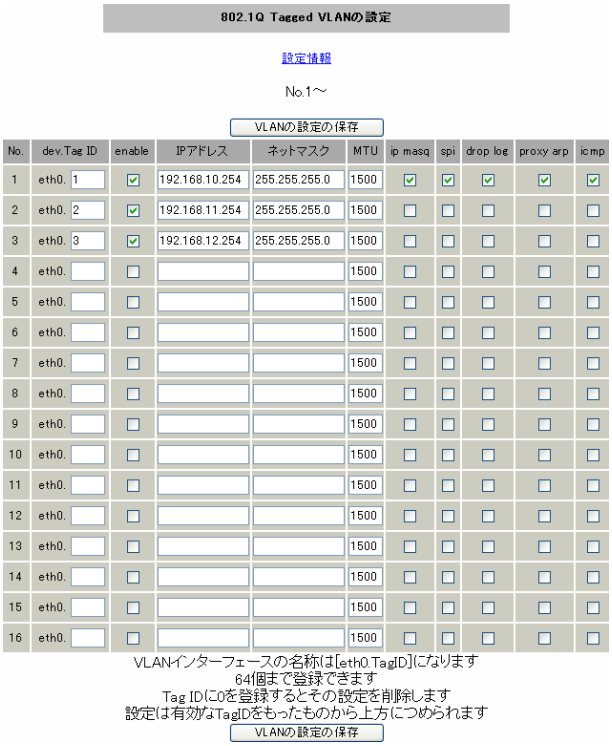
このような場合は本装置のEthernetポートのIPアドレスを、別のネットワークに属するIPアドレスに設定し直してください。

III. VLAN タギングの設定

◆各 802.1Q Tagged VLAN の設定

本装置の各 Ethernet ポートで、VLAN タギング(IEEE802.1Q 準拠)設定ができます。

Web設定画面「インターフェース設定」→「Ethernet0(または 1、2、3)の設定」をクリックして、以下の画面で設定します。



(Ether0 ポートの表示例です)

○ dev.Tag ID

VLAN のタグ ID を設定します。1 から 4094 の間で設定します。各 Ethernet ポートごとに 1024 個までの設定ができます。

設定後の VLAN インタフェース名は「eth0.<ID>」「eth1.<ID>」「eth2.<ID>」「eth3.<ID>」となります。

○ enable

チェックを入れることで設定を有効にします。

○ IP アドレス

○ネットマスク

VLAN インタフェースの IP アドレスとサブネットマスクを設定します。

○ MTU

VLAN インタフェースの MTU 値を設定します。

○ ip masq

チェックを入れることで、VLAN インタフェースでの IP マスカレードが有効となります。

○ spi

チェックを入れることで、VLAN インタフェースでステートフルパケットインスペクションが有効となります。

○ drop log

チェックを入れると、SPI により破棄(DROP)したパケットの情報を syslog に出力します。
SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 26 章 パケットフィルタリング機能　補足：フィルタのログ出力内容について」をご覧ください。

○ proxy arp

チェックを入れることで、VLAN インタフェースで proxy arp が有効となります。

○ icmp

チェックを入れると、そのインタフェースにて受信した ICMP AddressMask Request(type=17)に対して、サブネットマスク値を設定した ICMP AddressMask Reply(type=18)を返送します。

入力が終わりましたら「VLAN の設定の保存」をクリックして設定完了です。
設定はすぐに反映されます。
また、VLAN 設定を削除する場合は、dev.Tag ID 欄に「0」を入力して「VLAN の設定の保存」をクリックしてください。

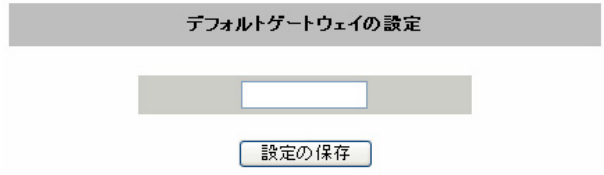
設定情報の表示

「802.1Q Tagged VLAN の設定」の「設定情報」リンクをクリックすると、現在の VLAN 設定情報が表示されます。

Ⅳ．その他の設定

◆デフォルトゲートウェイの設定

Web 設定画面「インターフェース設定」→「その他の設定」にある以下の画面で設定します。



本装置のデフォルトルートとなる IP アドレスを入力してください。
(PPPoE 接続時は設定の必要はありません。)

入力が終わりましたら、「設定の保存」をクリックして設定完了です。
設定はすぐに反映されます。

◆Dummy Interface の設定

Web 設定画面「インターフェース設定」→「その他の設定」の以下の画面で設定します。

Dummy Interface は、「BGP 設定における peer アドレス」に相当するものです。
「IP アドレス / マスク値」の形式で設定してください。

入力が終わりましたら「設定の保存」をクリックして設定完了です。設定はすぐに反映されます。

Ⅳ．その他の設定

◆ARP テーブル

「その他の設定」画面中央にある「ARP テーブル」をクリックすると、「ARP テーブル設定」画面が開きます。

（画面は表示例です）

[現在の ARP テーブル]
本装置に登録されている ARP テーブルの内容を表示します。初期状態では動的な ARP エントリが表示されています。

○ARP エントリの固定化
ARP エントリをクリックしてボタンをクリックすると、そのエントリは固定エントリとして登録されます。

○ARP エントリの削除
ARP エントリをクリックしてボタンをクリックすると、そのエントリがテーブルから削除されます。

[新しい ARP エントリ]
ARP エントリを手動で登録するときは、ここから登録します。

○ARP エントリの追加
入力欄に IP アドレスと MAC アドレスを入力後、ボタンをクリックして登録します。

＜エントリの入力例＞
192.168.0.1 00:11:22:33:44:55

[固定の ARP エントリ]
ARP エントリを固定するときは、ここから登録します。

○固定 ARP エントリの編集
入力欄に IP アドレスと MAC アドレスを入力後、ボタンをクリックして登録します。
エントリの入力方法は「新しい ARP エントリ」と同様です。

ARP テーブルの確認

「その他の設定」画面中央で、現在の ARP テーブルの内容を確認できます。

（画面は表示例です）

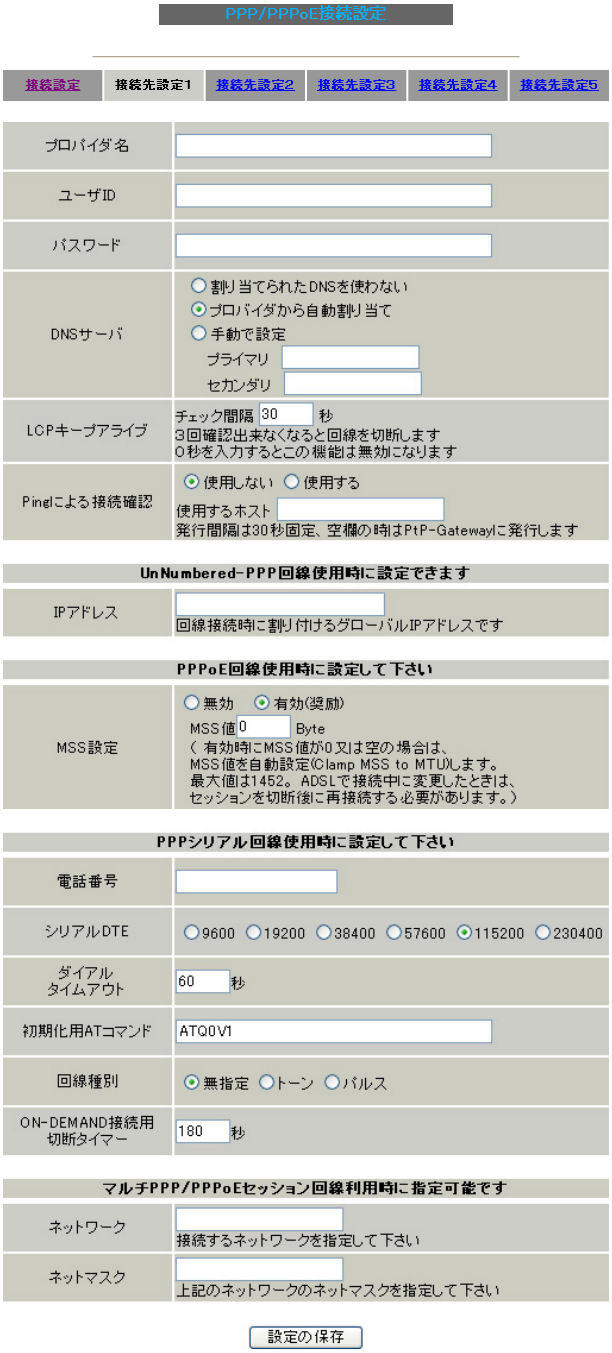
第 6 章

PPPoE 設定

Ⅰ．PPPoE の接続先設定

接続先設定

はじめに、接続先の設定（ISP のアカウント設定）をおこないます。
Web 設定画面「PPP/PPPoE 設定」→「接続先設定 1～5」のいずれかをクリックします。
設定は 5 つまで保存しておくことがきます。



（画面は「接続先設定１」）

○プロバイダ名
接続するプロバイダ名を入力します。
任意に入力できますが、「 ’」「(」「)」「｜」「\」等の特殊記号については使用できません。

○ユーザー ID
プロバイダから指定されたユーザー ID を入力してください。1～63 文字まで入力可能です。

○ パスワード
プロバイダから指定された接続パスワードを入力してください。1～63 文字まで入力可能です。
原則として「 ’」「(」「)」「｜」「\」等の特殊記号については使用できませんが、入力が必要な場合は該当文字の直前に「\」を付けて入力してください。

＜例＞
abc(def)g ’ h → abc\(def\)g\ ’ h

○ DNS サーバ
特に指定のない場合は「プロバイダから自動割り当て」をチェックします。
指定されている場合は「手動で設定」をチェックして、DNS サーバのアドレスを入力します。
プロバイダから DNS アドレスを自動割り当てされてもそのアドレスを使わない場合は「割り当てられた DNS を使わない」をチェックします。この場合は、LAN 側の各ホストに DNS サーバのアドレスをそれぞれ設定しておく必要があります。

○ LCP キープアライブ
キープアライブのための LCP echo パケットを送出する間隔を指定します。設定した間隔で LCP echo パケットを 3 回送出して reply を検出しなかったときに、本装置が PPPoE セッションをクローズします。「0」を指定すると、LCP キープアライブ機能は無効となります。

Ⅰ．PPPoE の接続先設定

○Ping による接続確認
回線によっては、LCP echo を使ったキープアライブを使うことができないことがあります。その場合は、Ping を使ったキープアライブを使用します。「使用するホスト」欄には、Ping の宛先ホストを指定します。空欄にした場合は P-t-P Gateway 宛に Ping を送出します。
通常は空欄にしておきます。

○ IP アドレス
固定 IP アドレスを割り当てられる接続の場合(unnumbered 接続を含む)、ここにプロバイダから割り当てられた IP アドレスを設定します。IP アドレスを自動的に割り当てられる形態での接続の場合は、ここにはなにも入力しないでください。

○ MSS 設定
「有効」を選択すると、本装置が MSS 値を自動的に調整します。「MSS 値」は任意に設定できます。
最大値は 1452 バイトです。
「0」にすると最大 1414byte に自動調整します。
特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします
(それ以外では正常にアクセスできなくなる場合があります)。

○電話番号
○シリアル DTE
○ダイアルタイムアウト
○初期化用 AT コマンド
○回線種別
○ ON-DEMAND 接続用切断タイマー

上記項目は、PPPoE 接続の場合、設定の必要はありません。

○ネットワーク
○ネットマスク
<例>
　ネットワーク「172.26.0.0」
　ネットマスク「255.255.0.0」
と指定すると、172.26.0.0/16 のネットワークにアクセスするときはマルチ接続を使ってアクセスするようになります。

別途「スタティックルート設定」でマルチ接続を使う経路を登録することもできます。

<u>このどちらも設定しない場合はすべてのアクセスが、主接続を使うことになります。</u>

最後に「設定」ボタンをクリックして、設定完了です。設定はすぐに反映されます。

II．PPPoE の接続設定と回線の接続 / 切断

Web 設定画面「PPP/PPPoE 接続設定」→「接続設定」をクリックして、以下の画面から設定します。

接続設定

○回線状態
現在の回線状態を表示します。

○接続先の選択
どの接続先設定を使って接続するかを選択します。

○接続ポート
どのポートを使って接続するかを選択します。
PPPoE 接続では、いずれかの「Ethernet」ポートを選択します。

○接続形態
「手動接続」は、PPPoE(PPP)の接続 / 切断を手動で切り替えます。
「常時接続」では、本装置が起動すると自動的に PPPoE 接続を開始します。

○ RS232C 接続タイプ
PPPoE 接続では「通常」を選択します。

○ IP マスカレード
PPPoE 接続時に IP マスカレードを有効にするかどうかを選択します。

○ステートフルパケットインスペクション
PPPoE 接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。
SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 26 章 パケットフィルタリング機能　補足：フィルタのログ出力内容について」をご覧ください。

○デフォルトルートの設定
「有効」を選択すると、PPPoE 接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。「インタフェース設定」でデフォルトルートが設定されていても、PPPoE 接続で通知されるものに置き換えられます。
「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。
通常は「有効」設定にしておきます。

○ ICMP AddressMask Request
「応答する」にチェックを入れると、そのインタフェースにて受信した ICMP AddressMask Request (type=17)に対して、サブネットマスク値を設定した ICMP AddressMask Reply(type=18)を返送します。

最後に「設定の保存」ボタンをクリックして、設定完了です。

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。
「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

II．PPPoE の接続設定と回線の接続 / 切断

接続 IP 変更お知らせメール機能

IP アドレスを自動的に割り当てられる方式で PPPoE 接続する場合、接続のたびに割り当てられる IP アドレスが変わってしまうことがあります。
この機能を使うと、IP アドレスが変わったときに、その IP アドレスを任意のメールアドレスにメールで通知することができるようになります。

本機能を設定する場合は、Web 設定画面「システム設定」→「メール送信機能の設定」をクリックして以下の画面で設定します。

＜ PPPoE お知らせメール送信＞

設定方法については「**第33章 各種システム設定**」の「**◆メール送信機能の設定**」を参照してください。

III．バックアップ回線

PPPoE 接続では、「バックアップ回線接続」設定ができます。

[バックアップ回線接続]

主回線がダウンしたときに、自動的に回線を切り替えて接続を維持しようとします。

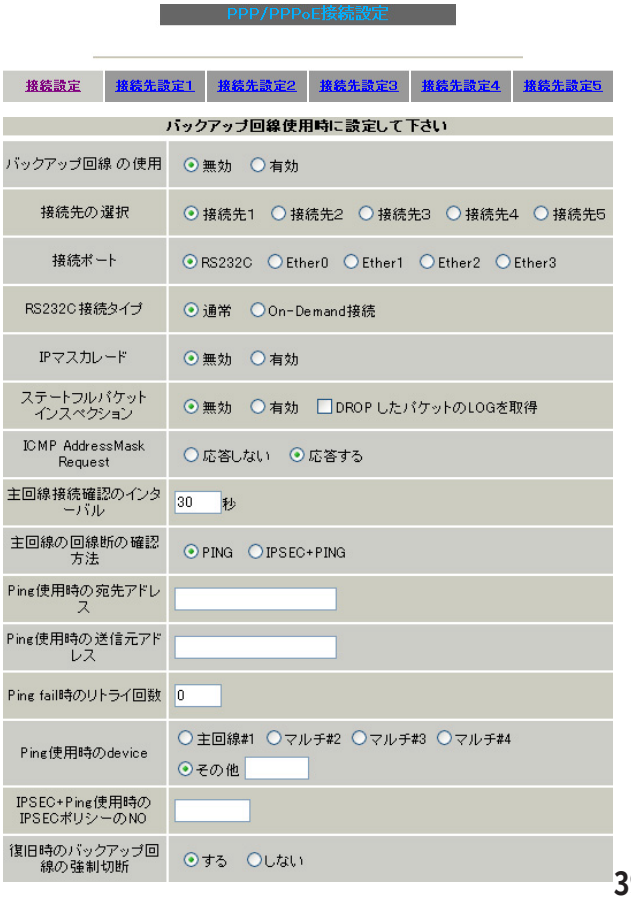
ただし、NAT 設定やパケットフィルタ設定等は、主回線用の設定とは別に設定しなければなりません。

これにより、主回線接続時とバックアップ回線接続時とでセキュリティレベルを変更したり、回線品質にあった帯域制御などを個別に設定する、といったことができるようになります。

回線状態の確認は、ping を用います。

バックアップ回線設定

PPPoE 接続設定画面の「バックアップ回線使用時に設定して下さい」欄で設定します。



○バックアップ回線 の使用
バックアップ回線を利用する場合は「有効」を選択します。

○接続先の選択
バックアップ回線接続で利用する接続先設定を選択します。

○接続ポート
バックアップ回線を接続しているインタフェースを選択します。

○ RS232C 接続タイプ
RS232C インタフェースを使ってバックアップ回線接続するときの接続タイプを選択します。
「通常」を選択すると常時接続となります。
「On-Demand 接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

○ IP マスカレード
バックアップ回線接続時の IP マスカレードの動作を選択します。

○ステートフルパケットインスペクション
バックアップ回線接続時のステートフルパケットインスペクションの動作を選択します。
SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 26 章 補足：フィルタのログ出力内容について」をご覧ください。

○ ICMP AddressMask Request
「応答する」にチェックを入れると、そのインタフェースにて受信した ICMP AddressMask Request (type=17)に対して、サブネットマスク値を設定した ICMP AddressMask Reply(type=18)を返送します。

○主回線接続確認のインターバル
主回線接続の確認ためにパケットを送出する間隔を設定します。

III. バックアップ回線

○主回線の回線断の確認方法
主回線の回線断を確認する方法を選択します。
「PING」は ping パケットにより、「IPSEC+PING」は IPSEC上でのpingにより、回線の切断を確認します。

○ Ping 使用時の宛先アドレス
回線断の確認方法で「PING」「IPSEC+PING」を選択したときの、ping パケットのあて先 IP アドレスを設定します。ここから ping の Reply が返ってこなかった場合に、バックアップ回線接続に切り替わります。

○ Ping 使用時の送信元アドレス
回線断の確認方法で「IPSEC+PING」を選択したときの、ping パケットの送信元 IP アドレスを設定できます。

○ Ping fail 時のリトライ回数
pingのリプライがないときに何回リトライするかを指定します。

○ Ping 使用時の device
ping を使用する際の、ping を発行する回線(インタフェース)を選択します。「その他」を選択して、インタフェース名を直接指定もできます。

＜例＞主回線上の IPsec インタフェースは
“ ipsec0 ”です。

○ IPSEC+Ping 使用時の IPSEC ポリシーの NO
IPSEC+PING で回線断を確認するときは必ず、使用する IPsec ポリシーの設定番号を指定します。
IPsec 設定については「第 12 章 IPsec 機能」や IPsec 設定ガイドをご覧ください。

○復旧時のバックアップ回線の強制切断
主回線の接続が復帰したときに、バックアップ回線を強制切断させるときに「する」を選択します。「しない」を選択すると、主回線の接続が復帰しても、バックアップ回線接続の設定に従ってバックアップ回線の接続を維持します。

最後に「設定の保存」ボタンをクリックして、設定完了です。

このほか、NAT 設定・パケットフィルタ設定・ルーティング設定など、バックアップ回線接続時のための各種設定を別途行なってください。

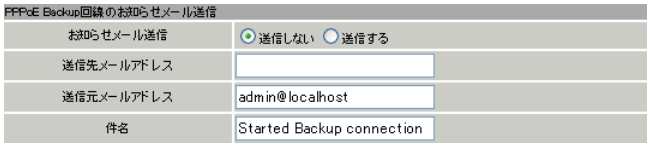
バックアップ回線接続機能は、「接続接定」で「常時接続」に設定してある場合のみ有効です。また「接続設定」を変更した場合には、回線を一度切断して再接続した際に変更が反映されます。

接続お知らせメール機能

バックアップ回線で接続したときに、それを電子メールによって通知させることができます。

本機能を設定する場合は、Web 設定画面「システム設定」→「メール送信機能の設定」をクリックして以下の画面で設定します。

＜ PPPoE Backup 回線のお知らせメール送信＞



設定方法については「**第33章 各種システム設定**」の「**◆メール送信機能の設定**」を参照してください。

Ⅳ．PPPoE 特殊オプション設定

地域 IP 網での工事や不具合・ADSL 回線の不安定な状態によって、正常に PPPoE 接続がおこなえなくなることがあります。

これはユーザー側が PPPoE セッションが確立していないことを検知していても地域 IP 網側はそれを検知していないために、ユーザー側からの新規接続要求を受け入れることができない状態になっていることが原因です。

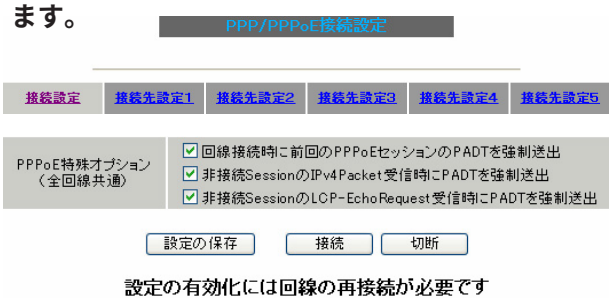
ここで PPPoE 特殊オプション機能を使うことにより、本装置が PPPoE セッションを確立していないことを検知し、強制的に PADT パケットを地域 IP 網側へ送信して、地域 IP 網側に PPPoE セッションの終了を通知します。

本装置から PADT パケットを送信することで地域 IP 網側の PPPoE セッション情報がクリアされ、PPPoE の再接続性を高めることができます。

PADT ＝ PPPoE Active Discovery Terminate の略。
PPPoE セッションが終了したことを示すパケットです。これにより、PADT を受信した側で該当する PPPoE セッションを終了させます。

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。



①回線接続時に前回の PPPoE セッションの PADT を強制送出する。

②非接続 Session の IPv4Packet 受信時に PADT を強制送出する。

③非接続 Session の LCP-EchoReqest 受信時に PADT を強制送出する。

①の動作について
本装置側が回線断と判断していても網側が回線断と判断していない状況下において、本装置側から強制的に PADT を送出してセッションの終了を網側に認識させます。その後、本装置側から再接続をおこないます。

②、③の動作について
本装置が LCP キープアライブにより断を検知しても網側が断と判断していない状況下において、網側から
・IPv4 パケット
・LCP エコーリクエスト
のいずれかを本装置が受信すると、本装置が PADT を送出してセッションの終了を網側に認識させます。その後、本装置側から再接続をおこないます。

使用したい特殊オプションごとに、チェックボックスにチェックを付けてください。PPPoE 回線接続中に設定を変更したときは、PPPoE を再接続する必要があります。

地域 IP 網の工事後に PPPoE 接続ができなってしまう事象を回避するためにも、PPPoE 特殊オプション機能を有効にした上で PPPoE 接続をしていただくことを推奨します。

第7章

RS-232ポートを使った接続
(ダイヤルアップ機能)

第 7 章　RS-232 ポートを使った接続(ダイヤルアップ機能)

Ⅰ．本装置とアナログモデム /TA の接続

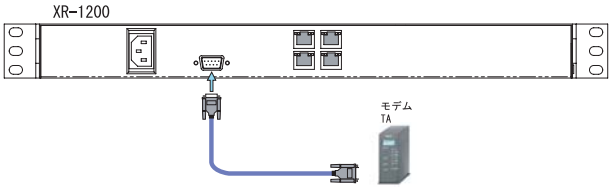
本装置は、RS-232 ポートを搭載しています。
この各ポートにアナログモデムやターミナルアダプタを接続し、本装置の PPP 接続機能を使うことでダイヤルアップが可能となります。

◆アナログモデム /TA のシリアル接続

1　本装置本体背面の「RS-232」ポートとアナログモデム /TA のシリアルポートをシリアルケーブルで接続してください。シリアルケーブルは別途ご用意ください。

2　全ての接続が完了しましたら、本装置とモデム /TA の電源を投入してください。

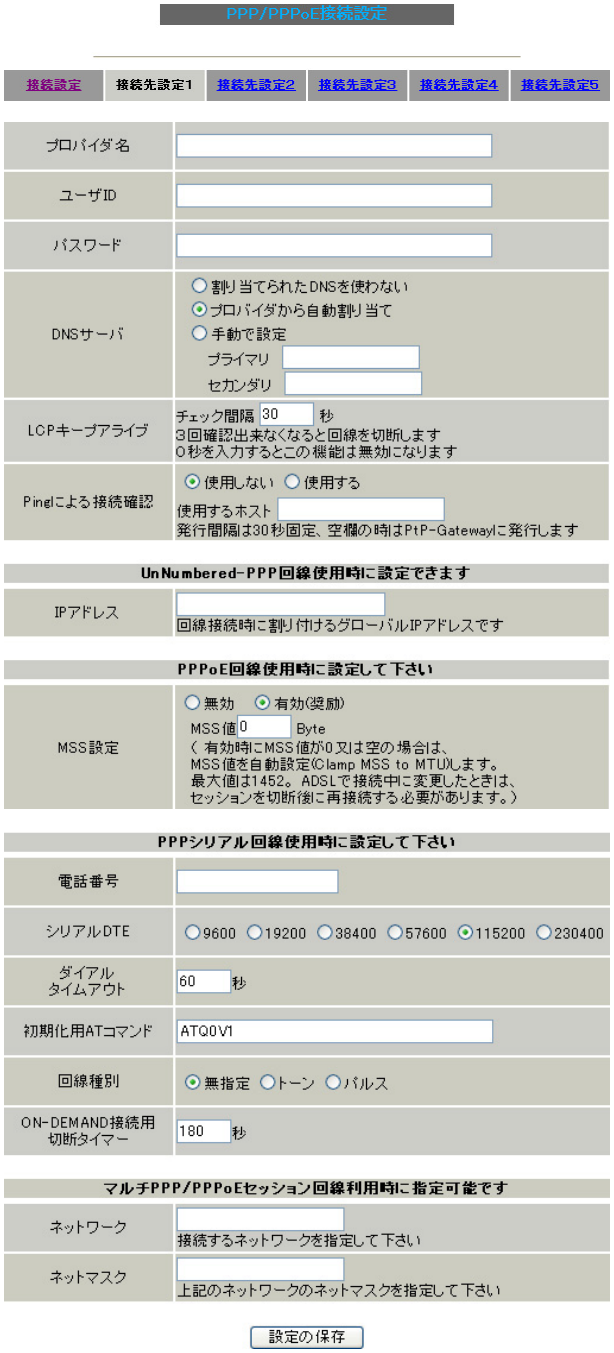
接続図



Ⅱ．ダイヤルアップ回線の接続先設定

PPP(ダイヤルアップ)接続の接続先設定をおこないます。

Web 設定画面「PPP/PPPoE 設定」の画面上部にある「接続先設定１～5」のいずれかをクリックして接続先の設定をおこないます。
設定は５つまで保存しておくことができます。



（画面は「接続先設定１」）

○プロバイダ名
接続するプロバイダ名を入力します任意に入力できますが、「’」「(」「)」「｜」「\」等の特殊文字については使用できません。

○ユーザ ID
プロバイダから指定されたユーザ ID を入力してください。1～63 文字まで入力可能です。

○パスワード
プロバイダから指定された接続パスワードを入力してください。1～63 文字まで入力可能です。

原則として「’」「(」「)」「｜」「\」等の特殊文字については使用できませんが、入力が必要な場合は該当文字の直前に「\」を付けて入力してください。

＜例＞　abc(def)g’h → abc\(def\)g\’h

○ DNS サーバ
特に指定のない場合は「プロバイダから自動割り当て」をチェックします。指定されている場合は「手動で設定」をチェックして、DNS サーバのアドレスを入力します。
プロバイダから DNS アドレスを自動割り当てされてもそのアドレスを使わない場合は「割り当てられた DNS を使わない」をチェックします。この場合は、LAN 側の各ホストに DNS サーバのアドレスをそれぞれ設定しておく必要があります。

○ LCP キープアライブ
○ ping による接続確認
○ IP アドレス
○ MSS 設定
上記項目は、ダイヤルアップ接続の場合は設定のしません。

○電話番号
アクセス先の電話番号を入力します。
市外局番から入力してください。

II．ダイヤルアップ回線の接続先設定

○ダイアルタイムアウト
アクセス先にログインするときのタイムアウト時間を設定します。単位は秒です。

○シリアル DTE
本装置とモデム /TA 間の DTE 速度を選択します。
工場出荷値は 115200bps です。

○初期化用 AT コマンド
モデム /TA によっては、発信するときに初期化が必要なものもあります。その際のコマンドをここに入力します。

○回線種別
回線のダイアル方法を選択します。

○ ON-DEMAND 接続用切断タイマー
PPP 接続設定の RS232C 接続タイプを On-Demand 接続にした場合の、自動切断タイマーを設定します。ここで設定した時間を過ぎて無通信状態のときに、PPP 接続を切断します。

○ネットワーク
○ネットマスク
< 例 >
　　ネットワーク「172.26.0.0」
　　ネットマスク「255.255.0.0」
と指定すると、172.26.0.0/16 のネットワークにアクセスするときはマルチ接続を使ってアクセスするようになります。

別途「スタティックルート設定」でマルチ接続を使う経路を登録することもできます。

<u>このどちらも設定しない場合はすべてのアクセスが、主接続を使うことになります。</u>

最後に「設定の保存」ボタンをクリックして、設定完了です。設定はすぐに反映されます。

続いて、PPP の接続設定をおこないます。

III．ダイヤルアップ回線の接続と切断

接続先設定に続いて、ダイヤルアップ接続のために接続設定をおこないます。

Web 設定画面「PPP/PPPoE 接続設定」を開き「接続設定」をクリックして、以下の画面から設定します。

接続設定

PPP/PPPoE接続設定

接続設定 | 接続先設定1 | 接続先設定2 | 接続先設定3 | 接続先設定4 | 接続先設定5

回線状態	回線は接続されていません
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	◉RS232C ○Ether0 ○Ether1 ○Ether2 ○Ether3
接続形態	◉手動接続 ○常時接続
RS232C接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケットインスペクション	○無効 ◉有効 ☐DROPしたパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効
ICMP AddressMask Request	○応答しない ◉応答する

○回線状態
現在の回線状態を表示します。

○接続先の選択
どの接続先設定を使って接続するかを選択します。

○接続ポート
どのポートを使って接続するかを選択します。
ダイヤルアップ接続では「RS232C」ポートを選択します。

○接続形態
「手動接続」ダイヤルアップの接続 / 切断を手動で切り替えます。
「常時接続」本装置が起動すると自動的にダイヤルアップ接続を開始します。

○ RS232C 接続タイプ
「通常」は接続形態設定にあわせて接続します。
「On-Demand 接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

○ IP マスカレード
ダイヤルアップ接続時に IP マスカレードを有効にするかどうかを選択します。
unnumbered 接続時以外は、「有効」を選択してください。

○ステートフルパケットインスペクション
ダイヤルアップ接続時に、ステートフルパケットインスペクションを有効にするかどうかを選択します。
SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 27 章 補足：フィルタのログ出力内容について」をご覧ください。

○デフォルトルートの設定
「有効」を選択すると、ダイヤルアップ接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。「インタフェース設定」でデフォルトルートが設定されていても、ダイヤルアップ接続で通知されるものに置き換えられます。
「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。
通常は「有効」設定にしておきます。

○ ICMP AddressMask Request
「応答する」にチェックを入れると、そのインタフェースにて受信した ICMP AddressMask Request (type=17)に対して、サブネットマスク値を設定した ICMP AddressMask Reply(type=18)を返送します。

最後に「設定の保存」ボタンをクリックして、設定完了です。

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。
「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

Ⅳ．バックアップ回線接続

ダイヤルアップ接続についても、PPPoE 接続と同様に、
　・PPPoE お知らせメール送信
および
　・バックアップ回線接続設定
が可能です。

設定方法については、
「第 6 章 PPPoE 設定」の各ページをご参照ください。
　「II .PPPoE の接続設定と回線の遮断 / 切断」
　「III . バックアップ回線接続設定」

Ｖ．回線への自動発信の防止について

Windows OS は NetBIOS で利用する名前からアドレス情報を得るために、自動的に DNS サーバへ問い合わせをかけるようになっています。

そのため「On-Demand 接続」機能を使っている場合には、ダイヤルアップ回線に自動接続してしまう問題が起こります。

この意図しない発信を防止するために、本装置ではあらかじめ以下のフィルタリングを設定しています。

(入力フィルタ)

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth0	パケット受信時	破棄	tcp				137:139
2	eth0	パケット受信時	破棄	udp				137:139
3	eth0	パケット受信時	破棄	tcp		137		
4	eth0	パケット受信時	破棄	udp		137		

(転送フィルタ)

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth0	パケット受信時	破棄	tcp				137:139
2	eth0	パケット受信時	破棄	udp				137:139
3	eth0	パケット受信時	破棄	tcp		137		
4	eth0	パケット受信時	破棄	udp		137		

第8章

複数アカウント同時接続設定

複数アカウント同時接続の設定

本装置シリーズは、同時に複数の PPPoE 接続をおこなうことができます。

以下のような運用が可能です。

・NTT 東西が提供している B フレッツサービスで、インターネットとフレッツ・スクエアに同時に接続する(注)
・フレッツ ADSL での接続と、ISDN 接続(ダイヤルアップ)を同時におこなう

(注)NTT 西日本の提供するフレッツスクエアは NTT 東日本提供のものとはネットワーク構造がことなるため、B フレッツとの同時接続運用はできません。

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。
本装置のマルチ PPPoE セッション機能は、主回線 1 セッションと、マルチ接続 3 セッションの合計 4 セッションまでの同時接続をサポートしています。
なお、以下の項目については主回線では設定できますが、マルチ接続（#2 ～ #4）では設定できませんので、ご注意ください。

・デフォルトルートとして指定する
・接続 IP アドレス変更のお知らせメールを送る
・接続確認として、IPsec + PING を設定する

マルチ PPPoE セッションを利用する場合のルーティングは、宛先ネットワークアドレスによって切り替えます。
したがって、フレッツ・スクウェアやフレッツ・オフィスのように特定の IP アドレス体系で提供されるサービスをインターネット接続と同時に利用する場合でも、アクセスする PC 側の設定を変更する必要はありません。

ただし、マルチリンクには対応していませんので、帯域を広げる目的で利用することはできません。
また、本装置のマルチ PPPoE セッション機能は、PPPoE で接続しているすべてのインタフェースがルーティングの対象となります。
したがいまして、それぞれのインタフェースにステートフルパケットインスペクション、またはフィルタリング設定をしてください。

また、マルチ接続側（主回線ではない側）は**フレッツスクエアのように閉じた空間を想定している**ので、工場出荷設定ではステートフルパケットインスペクションは無効となっています。
必要に応じてステートフルパケットインスペクション等の設定をして使用してください。

この機能を利用する場合は以降のステップに従って設定してください。

複数アカウント同時接続の設定

STEP 1 主接続の接続先設定

１つ目のプロバイダの接続設定をおこないます。
ここで設定した接続を主接続とします。

最初に Web 設定画面「PPP/PPPoE 設定」をクリックし、「接続先設定１～5」のいずれかをクリックして設定します。

詳しい設定方法は、「第 6 章 PPPoE 設定」または「第 7 章 RS-232 ポートを使った接続（ダイヤルアップ機能）」をご覧ください。

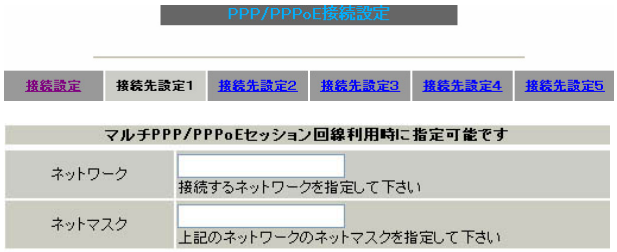
STEP 2 マルチ接続用の接続先設定

マルチ接続(同時接続)用の接続先設定をおこないます。

Web 設定画面「PPP/PPPoE 設定」の、「接続先設定１～5」のいずれかをクリックして設定します。

設定方法については、「第 6 章 PPPoE 設定」をご参照ください。

さらに、設定画面最下部にある下図の部分で、マルチ接続を使ってアクセスしたい先のネットワークアドレスとネットマスクを指定します。



○ネットワーク
○ネットマスク
＜例＞
　ネットワーク「172.26.0.0」
　ネットマスク「255.255.0.0」
と指定すると、172.26.0.0/16 のネットワークにアクセスするときはマルチ接続を使ってアクセスするようになります。

別途「スタティックルート設定」でマルチ接続を使う経路を登録することもできます。

このどちらも設定しない場合はすべてのアクセスが、主接続を使うことになります。

最後に「設定の保存」をクリックして接続先設定は完了です。

複数アカウント同時接続の設定

STEP 3 PPPoE 接続の設定

複数同時接続のための接続設定をおこないます。
主接続とマルチ接続それぞれについて接続設定をおこないます。

「PPP/PPPoE 設定」→「接続設定」を開きます。

[主接続用の接続設定]
以下の部分で設定します。

○回線状態
現在の回線状態を表示します。

○接続先の選択
主接続用の設定を選択します。

○接続先ポート
主接続で使用する、本装置のインタフェースを選択します。

○接続形態
常時接続の回線を利用する場合は通常、「常時接続」を選択します。
手動接続を選択した場合は、同画面最下部のボタンで接続・切断の操作をおこなってください。

○ RS232C 接続タイプ
「通常」では接続形態設定にあわせて接続します。
「On-Demand 接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

○ IP マスカレード
通常は「有効」を選択します。
LAN 側をグローバル IP で運用している場合は「無効」を選択します。

○ステートフルパケットインスペクション
任意で選択します。
SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 26 章 補足：フィルタのログ出力内容について」をご覧ください。

○デフォルトルートの設定
「有効」を選択します。

○ ICMP AddressMask Request
任意で選択します。

○ PPPoE お知らせメール送信
「システム設定」→「メール送信機能の設定」にある＜PPPoE お知らせメール送信＞を任意で設定します。
設定方法については「第 33 章 各種システム設定」をご覧ください。

続いて、マルチ接続用の接続設定をおこないます。

複数アカウント同時接続の設定

[マルチ接続用の設定]

以下の部分で設定します。

PPP/PPPoE接続設定

接続設定 | 接続先設定1 | 接続先設定2 | 接続先設定3 | 接続先設定4 | 接続先設定5

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい

マルチ接続 #2	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1 ○Ether2 ○Ether3
RS232C接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 ☐DROPしたパケットのLOGを取得
ICMP AddressMask Request	○応答しない ◉応答する
マルチ接続 #3	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1 ○Ether2 ○Ether3
RS232C接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 ☐DROPしたパケットのLOGを取得
ICMP AddressMask Request	○応答しない ◉応答する
マルチ接続 #4	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1 ○Ether2 ○Ether3
RS232C接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 ☐DROPしたパケットのLOGを取得
ICMP AddressMask Request	○応答しない ◉応答する

○マルチ接続 #2 ～ #4

マルチ PPPoE セッション用の回線として使うものに「有効」を選択します。

○接続先の選択

マルチ接続用の接続先設定を選択します。

○接続ポート

マルチ接続で使用する、本装置のインタフェースを選択します。

B フレッツ回線で複数の同時接続をおこなう場合は、主接続の設定と同じインタフェースを選択します。

○ RS232C 接続タイプ

RS232C を使って複数アカウント同時接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

「On-Demand 接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

○ IP マスカレード

任意で選択します。通常は「有効」にします。

LAN 側をグローバル IP で運用している場合は「無効」を選択します。

○ステートフルパケットインスペクション

任意で選択します。

SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。

ログの出力内容については、「第 26 章 補足：フィルタのログ出力内容について」をご覧ください。

○ ICMP AddressMask Request

任意で選択します。

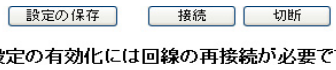
マルチ接続設定は 3 つまで設定可能です。

最大 4 セッションの同時接続が可能です。

複数アカウント同時接続の設定

STEP 4　PPPoE 接続の開始

すべて設定した後、「接続」をクリックして PPPoE 接続を開始します。



PPPoE の接続状態は、接続設定画面上部の「回線状態」に赤文字で表示されます。

接続に成功した場合:

主回線で接続しています。
マルチセッション回線 1 で接続しています。

接続できていない場合:

主回線で接続を試みています。
マルチセッション回線 1 で接続を試みています。

などと表示されます。

PPPoE 接続に成功したあとは、STEP 2 の設定、「スタティックルート設定」、もしくは「ソースルート設定」にしたがって接続を振り分けられてアクセスできます。

複数アカウント同時接続時の注意点

通常の ISP とフレッツスクエアへの同時接続をするには、本装置の「DNS キャッシュ機能」を「有効」にし、各 PC の DNS サーバ設定を本装置の IP アドレスに設定してください。

本装置に名前解決要求をリレーさせないと、同時接続ができません。

第9章

各種サービスの設定

各種サービス設定

本装置の設定画面「各種サービスの起動・停止・設定」をクリックすると、以下の画面が表示されます。

ここで

・各種サービスの設定
・各種サービスの起動と停止
・サービスの稼働状況の確認

をおこないます。

サービスの設定

それぞれのサービスの設定をおこなうには、画面中の各サービス名をクリックしてください。そのサービスの設定画面が表示されます。
それぞれの設定方法については、以下のページを参照してください。

- DNS リレー / キャッシュ機能
- DHCP サーバ / リレー機能
- IPsec 機能
- UPnP 機能
- ダイナミックルーティング
- L2TPv3 機能
- SYSLOG 機能
- 攻撃検出機能
- SNMP エージェント機能
- NTP サービス
- VRRP サービス
- アクセスサーバ機能

サービスの起動と停止

それぞれのサービスを起動・停止するときは、それぞれのサービス項目で、「停止」か「起動」を選択して画面最下部にある「動作変更」ボタンをクリックすることで、サービスの稼働状態が変更されます。
また、サービスの稼働状態は、各項目の右側に表示されます。

第 10 章

DNS リレー / キャッシュ機能

DNS リレー / キャッシュ機能の設定

◆DNS リレー機能

本装置ではLAN内の各ホストのDNSサーバを本装置に指定して、ISPから指定されたDNSサーバや任意のDNSサーバへリレーすることができます。

DNSリレー機能を使う場合は、各種サービス設定画面の「DNS キャッシュ」を起動させてください。

任意のDNSを指定する場合は、Web設定画面「各種サービスの設定」→「DNS キャッシュ」をクリックして以下の画面で設定します。

○プライマリ DNS IP アドレス
○セカンダリ DNS IP アドレス
任意のDNSサーバのIPアドレスを入力してください。
PPPoE接続時、ISPから指定されたDNSサーバへリレーする場合は本設定の必要はありません。

○ root server
上記プライマリ DNS IP アドレス、セカンダリ DNS IP アドレスで設定したDNSサーバへの問い合わせに失敗した場合や、DNS サーバの指定が無い場合に、ルートサーバへの問い合わせをおこなうかどうかを指定します。

○タイムアウト
DNSサーバへの問い合わせが無応答の場合のタイムアウトを設定します。
5-30 秒で設定できます。初期設定は 30 秒です。
使用環境によっては、DNSキャッシュのタイムアウトよりもブラウザなどのアプリケーションのタイムアウトが早く発生する場合があります。
この場合は、DNSキャッシュのタイムアウトを調整してください。

○送信元ポート
DNSリクエストの送信元ポート番号を範囲指定することができます。
指定可能な範囲：10000-65535 です。ポート番号は、指定した範囲内からランダムに選択されます。

ただし、「フィルタ設定」で以下の設定を実行している場合には注意が必要です。

DNSのポート番号を指定してフィルタしている場合

<「出力フィルタ」設定例>

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット送信時	許可	udp		1024		53
2	eth1	パケット送信時	破棄	udp				

↓

DNS リクエストの送信元ポート番号の範囲設定
“ 10000 ” ～ “ 19999 ”

<「出力フィルタ」設定例>

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット送信時	許可	udp		10000:1999		53
2	eth1	パケット送信時	破棄	udp				

または、

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット送信時	許可	udp				53
2	eth1	パケット送信時	破棄	udp				

UDP のポート番号 10000-65535 をフィルタしている場合

<「出力フィルタ」設定例>

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット送信時	破棄	udp		10000:655		

↓

DNS リクエストの送信元ポート番号の範囲設定
“ 10000 ” ～ “ 65535 ”

<「出力フィルタ」設定例>

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット送信時	許可	udp		10000:655		53
2	eth1	パケット送信時	破棄	udp		10000:655		

設定後に「設定の保存」をクリックして設定完了です。
設定はすぐに反映されます。

◆DNS キャッシュ機能

また、「DNSキャッシュ」を起動した場合、本装置がリレーして名前解決された情報は、自動的にキャッシュされます。

第 11 章

DHCP サーバ / リレー機能

第 11 章 DHCP サーバ / リレー機能

Ⅰ．本装置の DHCP 関連機能について

本装置は、以下の 4 つの DHCP 関連機能を搭載しています。

◆ DHCP クライアント機能
本装置のインターネット /WAN 側ポートは DHCP クライアントとなることができますので、IP アドレスの自動割り当てをおこなう CATV インターネット接続サービスで利用できます。
また既存 LAN に仮設 LAN を接続したい場合などに、本装置の IP アドレスを決めなくても既存 LAN から IP アドレスを自動的に取得でき、LAN 同士の接続が容易に可能となります。
DHCP クライアント機能の設定は「第 5 章 インタフェース設定」を参照してください。

◆ DHCP サーバ機能
本装置のインタフェースは DHCP サーバとなることができますので、LAN 側のコンピュータに自動的に IP アドレス等の設定をおこなえます。

◆ IP アドレスの固定割り当て
DHCP サーバ機能では通常、使用されていない IP アドレスを順に割り当てる仕組みになっていますので、DHCP クライアントの IP アドレスは変動することがあります。
しかし、固定割り当ての設定をすることで、DHCP クライアントの MAC アドレス毎に常に同じ IP アドレスを割り当てることができます。

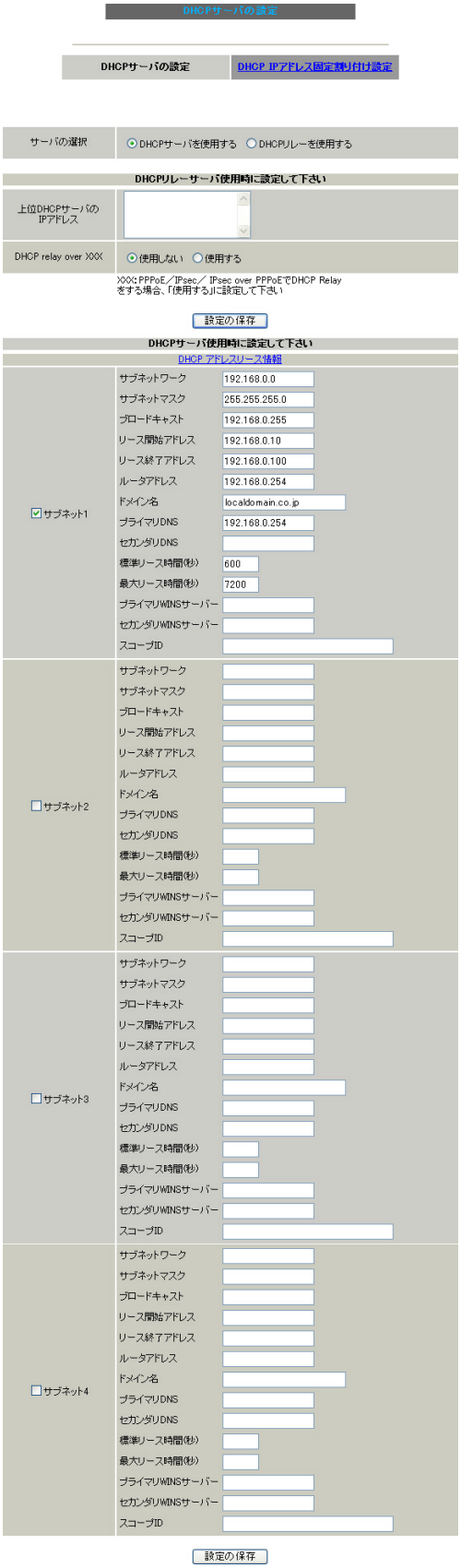
◆ DHCP リレー機能
DHCP サーバと DHCP クライアントは通常、同じネットワークにないと通信できません。
しかし、本装置の DHCP リレー機能を使うことで、異なるネットワークにある DHCP サーバを利用できるようになります(本装置が DHCP クライアントからの要求と DHCP サーバからの応答を中継します)。

NAT 機能を利用している場合、DHCP リレー機能は利用できません。

II．DHCP サーバ機能の設定

◆DHCP サーバの設定

Web 設定画面「各種サービスの設定」→「DHCP (Relay)サーバ」を開き、画面上部「DHCP サーバの設定」をクリックして、以下の画面で設定します。



○サーバの選択

DHCPサーバ機能/リレー機能のどちらを使用するかを選択します。

サーバ機能とリレー機能を同時に使うことはできません。

[DHCPリレーサーバ使用時に設定して下さい]

「サーバの選択」で「DHCP リレーを使用する」を選択した場合に設定します。

○上位 DHCP サーバの IP アドレス

上位の DHCP サーバの IP アドレスを指定します。

複数のサーバを登録するときは、IP アドレスごとに改行して設定します。

○ DHCP relay over XXX

PPPoE・IPsec・PPPoE接続時のIPsec上でDHCPリレー機能を利用する場合に「使用する」に設定してください。

[DHCPサーバ使用時に設定して下さい]

「サーバの選択」で「DHCP サーバを使用する」を選択した場合に設定をおこないます。

○サブネット 1～4

DHCP サーバ機能の動作設定をおこないます。

- **複数のサブネットを設定することができます。**
- **どのサブネットを使うかは、本装置のインタフェースに設定されたIPアドレスを参照の上、自動的に決定されます。**
- **ラジオボックスにチェックを入れたサブネット設定が、参照・動作の対象となります。**

各サブネットごとの詳細設定は以下の通りです。

○サブネットワーク

DHCPサーバ機能を有効にするサブネットワーク空間のアドレスを指定します。

○サブネットマスク

DHCPサーバ機能を有効にするサブネットワーク空間のサブネットマスクを指定します。

II．DHCP サーバ機能の設定

○ブロードキャスト
DHCPサーバ機能を有効にするサブネットワーク空間のブロードキャストアドレスを指定します。

○リース開始アドレス
○リース終了アドレス
DHCP クライアントに割り当てる最初と最後の IP アドレスを指定します(割り当て範囲となります)。

○ルータアドレス
DHCP クライアントのデフォルトゲートウェイとなるアドレスを入力してください。
通常は、本装置のインタフェースの IP アドレスを指定します。

○ドメイン名
DHCP クライアントに割り当てるドメイン名を入力します。必要であれば指定してください。

○プライマリ DNS
○セカンダリ DNS
DHCP クライアントに割り当てる DNS サーバアドレスを指定します。必要であれば指定してください。

○標準リース時間(秒)
DHCP クライアントに IP アドレスを割り当てる時間を指定します。
単位は秒です。初期設定では600秒になっています。

○最大リース時間(秒)
DHCP クライアント側が割り当て時間を要求してきたときの、最大限の割り当て時間を指定します。
単位は秒です。初期設定では 7200 秒になっています。(7200秒以上のリース時間要求を受けても、7200 秒がリース時間になります)

○プライマリ WINS サーバー
○セカンダリ WINS サーバー
DHCP クライアントに割り当てる WINS サーバアドレスを指定します。必要であれば指定してください。

○スコープ ID
DHCP クライアントに通知する NetBIOS スコープ ID を指定します。WINS サーバー設定時に有効になります。

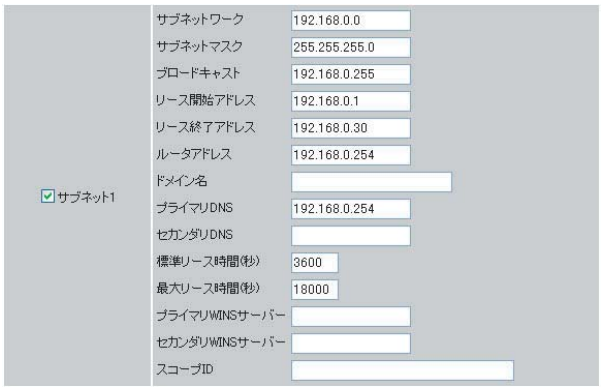
入力が終わりましたら「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。

DHCP サーバ機能の設定例

- LAN は 192.168.0.0/24 のネットワーク
- 192.168.0.1 から 30 のアドレスをリース
- ルータアドレスは 192.168.0.254
- ルータは DNS リレー機能が有効
- 標準リース時間は 1 時間
- 最大リース時間は 5 時間

上記条件の場合の設定例です。



III. IP アドレス固定割り当て設定

DHCP サーバ機能を利用して、特定のクライアントに特定の IP アドレスを固定で割り当てる場合は、以下の手順で設定します。

設定方法

Web 設定画面「各種サービスの設定」→「DHCP (Relay)サーバ」→画面上部の「DHCP IP アドレス固定割り付け設定」をクリックして、以下の画面で設定をおこないます。
設定は 256 まで可能です。画面下部にある「IP アドレス固定割り当て設定インデックス」のリンクをクリックすると画面が切り替わります。

○ MAC アドレス
コンピュータに装着されている LAN ボードなどの MAC アドレスを入力します。
＜入力例＞　**00:80:6d:49:ff:ff**

○ IP アドレス
その MAC アドレスに固定で割り当てる IP アドレスを入力します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
固定割り当て機能は、DHCP サーバ機能を再起動してから有効になります。

DHCP IP アドレス固定割り付け設定の削除

設定画面一覧の右側にある「削除」項目にチェックを入れて「設定 / 削除の実行」をクリックすると、そのエントリが削除されます。

第 12 章

IPsec 機能

Ⅰ．本装置の IPsec 機能について

◆鍵交換について
IKE を使用しています。
IKEフェーズ1ではメインモード、アグレッシブモードの両方をサポートしています。
フェーズ2ではクイックモードをサポートしています。
固定 IP アドレス同士の接続はメインモード、固定 IP アドレスと動的 IP アドレスの接続はアグレッシブモードで設定してください。

◆認証方式について
本装置では「共通鍵方式」「RSA 公開鍵方式」「X.509」による認証に対応しています。
ただし、アグレッシブモードは「共通鍵方式」にのみ対応、「X.509」はメインモードにのみ対応しています。

◆暗号化アルゴリズム
シングル DES とトリプル DES、AES128bit をサポートしています。
暗号化はソフトウェア処理でおこないます。

◆ハッシュアルゴリズム
SHA1 と MD-5 を使用しています。

◆認証ヘッダ
本装置は ESP の認証機能を利用していますので、AH での認証はおこなっていません。

◆DH 鍵共有アルゴリズムで使用するグループ
group1、group2、group5 をサポートしています。

◆ IPsec 使用時の通信可能対地数
1024 拠点まで IPsec 接続が可能です。

◆ IPsec とインターネット接続
IPsec 通信をおこなっている場合でも、その設定以外のネットワークへは、通常通りインターネットアクセスが可能です。

◆NAT トラバーサルに対応
XR 同士の場合、NAT 内のプライベートアドレス環境においても IPsec 接続をおこなうことができます。

他の機器との接続実績について

以下のルータとの接続を確認しています。

- FutureNet XR シリーズ
- FutureNet XR VPN Clinet(SSH Sentinel)
- Linux サーバ(FreeS/WAN)

II．IPsec 設定の流れ

◆PreShared(共通鍵)方式での IPsec 通信

STEP 1　共通鍵の決定

IPsec 通信をおこなうホスト同士の認証と、データの暗号化・復号化で使う共通秘密鍵の生成に必要な鍵を任意で決定します。
IPsec通信をおこなう双方で共通の鍵を使います。
半角英数字であればどんな文字列でもかまいません。

STEP 2　共通鍵の交換

決定した共通鍵は、第三者に知られないように十分注意して交換してください。
共通鍵が第三者に渡ると、その鍵を利用して不正な IPsec接続が確立されるおそれがあります。

STEP 3　本装置側の設定

自分側の本装置の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

データの暗号化と復号に必要な共通の秘密鍵を交換するための IKE/ISAKMP ポリシー設定をおこないます。
ここで共通鍵の設定、IKE の動作設定、相手側の IPsec ゲートウェイの設定や IKE の有効期間の設定をおこないます。

STEP 5　IPsec ポリシー設定

IPsec 通信をおこなう相手側セグメントの設定をおこないます。
このとき、どのIKE設定を使用するかを指定します。

STEP 6　IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7　IPsec 接続の確認

IPsec 起動後に、正常に IPsec 通信ができるかどうかを確認します。
「情報表示」画面でのインタフェースとルーティングテーブル、ログで確認します。

◆RSA(公開鍵)方式での IPsec 通信

STEP 1　公開鍵・暗号鍵の生成

IPsec 通信をおこなうホスト同士の認証とデータの暗号化に必要な公開鍵と、復号化に必要な秘密鍵を生成します。
公開鍵は IPsec の通信相手に渡しておきます。
鍵の長さを指定するだけで、自動的に生成されます。

STEP 2　公開鍵の交換

鍵を生成すると、設定画面上では公開鍵が表示されます。この鍵を IPsec 通信をおこなう相手側に通知してください。また、同様に、相手側が生成した公開鍵を入手してください。
公開鍵は第三者に知られても問題ありません。

STEP 3　本装置側の設定

自分側の本装置の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

データの暗号化と復号に必要な共通の秘密鍵を交換するためのIKE/ISAKMPポリシーの設定をおこないます。
ここで公開鍵の設定、IKE の動作設定、相手側の IPsec ゲートウェイの設定や IKE の有効期間の設定をおこないます。

STEP 5　IPsec ポリシー設定

IPsec 通信をおこなう相手側セグメントの設定をおこないます。このとき、どの IKE 設定を使用するかを指定します。

STEP 6　IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7　IPsec 接続の確認

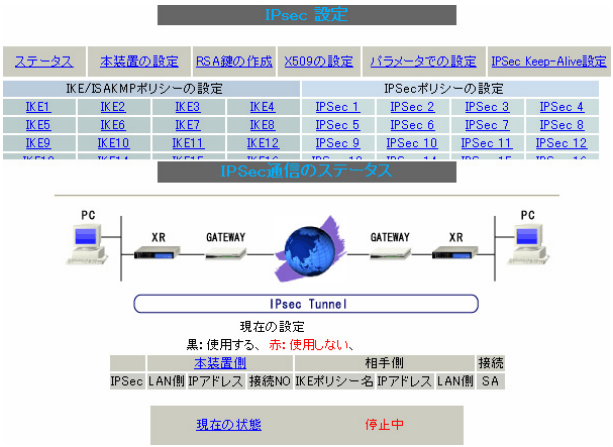
IPsec 起動後に、正常に IPsec 通信ができるかどうかを確認します。
「情報表示」画面でのインタフェースとルーティングテーブル、ログで確認します。

III. IPsec 設定

STEP 0　設定画面を開く

1　Web 設定画面にログインします。

2　「各種サービスの設定」→「IPsec サーバ」をクリックして、以下の画面から設定します。



- **ステータスの確認**
- **本装置の設定**
- **RSA 鍵の作成**
- **X.509 の設定**
- **パラメータでの設定**
- **IPsec Keep-Alive 設定**
- **IKE/ISAKMP ポリシーの設定**
- **IPsec ポリシーの設定**

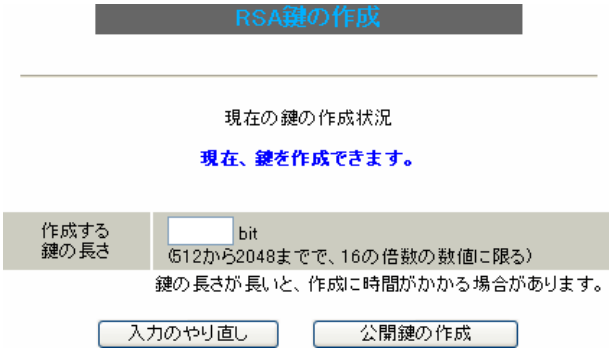
IPsec に関する設定・確認は、全てこの設定画面からおこなえます。

STEP 1,2　鍵の作成・交換

RSA 公開鍵方式を用いて IPsec 通信をおこなう場合は、最初に鍵を自動生成します。

PSK 共通鍵方式を用いて IPsec 通信をおこなう場合は、「鍵の作成」は不要です。相手側と任意で共通鍵を決定し、交換しておきます。

1　IPsec 設定画面上部の「RSA 鍵の作成」をクリックして、以下の画面を開きます。



2　作成する鍵の長さを指定して「公開鍵の作成」をクリックします。
鍵の長さは 512bit から 2048bit までで、16 の倍数となる数値が指定可能です。
現在の鍵の作成状況が「鍵を作成できます」の表示の時に限り、作成可能です。

3　鍵を生成します。**「鍵を作成しました。」**のメッセージが表示されると、鍵の生成が完了です。

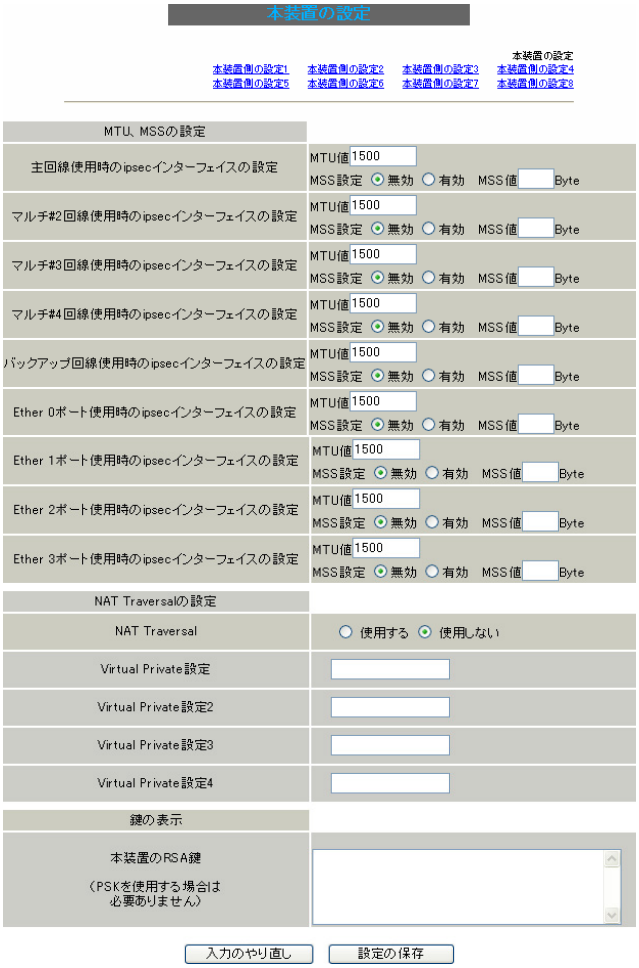
生成した鍵は、後述する「本装置側の設定」に自動的に反映されます。
またこの鍵は公開鍵となりますので、相手側にも通知してください。

STEP 3　本装置側の設定をおこなう

IPsec 設定画面上部の「本装置の設定」をクリックして設定します。

[本装置の設定]

「本装置の設定」をクリックします。



[MTU、MSS の設定]

◯ MTU 値

◯ MSS 設定

◯ MSS 値

IPsec 接続時の MTU/MSS 値を設定します。

各インタフェースごとに設定できます。

（指定可能範囲 MTU:68-1500,MSS:1-1460）

[NAT Traversal の設定]

NAT トラバーサル機能を使うことで、NAT 内のネットワークでも IPsec 通信をおこなえるようになります。

◯ NAT Traversal

NAT トラバーサル機能を使うかどうかを選択します。

◯ Virtual Private 設定～4

接続相手のNAT内クライアントが属しているネットワークと同じネットワークアドレスを入力します。以下のような書式で入力してください。

<入力形式> %v4:<ネットワーク>/<マスクビット値>

<設定例> %v4:192.168.0.0/24

本装置がNATの外側のIPsecサーバとして動作する場合に設定します。

最大４箇所までのNAT環境の接続先ネットワークを設定できます。

本装置がNAT背後のIPsecクライアントとして動作する場合は空欄のままにします。

「鍵の表示」

◯本装置の RSA 鍵

RSA 鍵の作成をおこなった場合ここに、作成した本装置の RSA 鍵の公開鍵が表示されます。

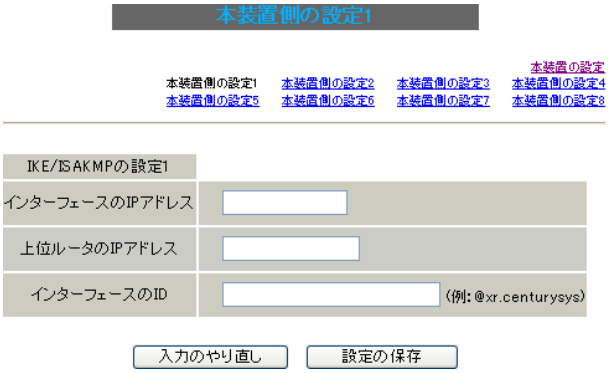
PSK 方式や X.509 電子証明を使う場合はなにも表示されません。

最後に「設定の保存」をクリックして設定完了です。

III. IPsec 設定

[本装置側の設定]

「本装置側の設定 1～8」のいずれかをクリックします。
ここで本装置自身の IP アドレスやインタフェース ID を設定します。



[IKE/ISAKMP の設定 1～8]

○インターフェースの IP アドレス

・**固定アドレスの場合**
本装置に設定されている IP アドレスをそのまま入力します。

・**動的アドレスの場合**
PPP/PPPoE 主回線接続の場合は「%ppp0」と入力します。
Ether0(Ether1,Ether2,Ether3)ポートで接続している場合は「%eth0(%eth1、または %eth2,%eth3)」と入力します。

○上位ルータの IP アドレス
空欄にしておきます。

○インタフェースの ID
本装置への IP アドレスの割り当てが動的割り当ての場合(aggressive モードで接続する場合)は、インタフェースの ID を設定します（必須)。
また、NAT 内のクライアントとして接続する場合も必ず設定してください。

＜入力形式＞ **@＜任意の文字列＞**
＜入力例＞ @centurysystems
(@の後は、任意の文字列でかまいません。)

固定アドレスの場合は、設定を省略できます。
省略した場合は、自動的に「インタフェースの IP アドレス」を ID として使用します。

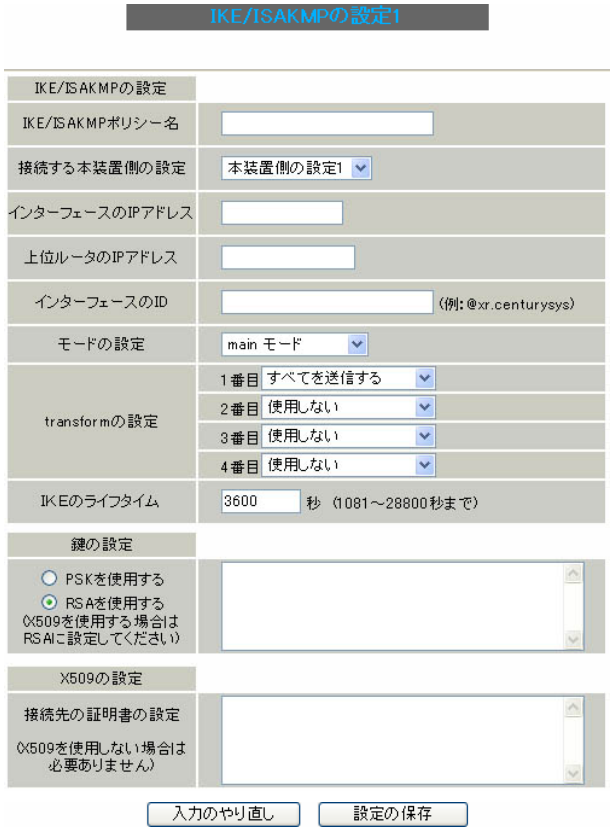
最後に「設定の保存」をクリックして設定完了です。

続いて IKE/ISAKMP ポリシーの設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

IPsec 設定画面上部の「IKE/ISAKMP ポリシーの設定」の「IKE1」～「IKE1024」のいずれかをクリックして、以下の画面から設定します。
32 個以上設定する場合は「IKE/ISAKMP ポリシーの設定画面インデックス」で切り替えてください。

（画面は「IKE20」までの表示例です）



（画面は「IKE/ISAKMP の設定 1」です）

[IKE/ISAKMP の設定]
○ IKE/ISAKMP ポリシー名
設定名を任意で設定します。(省略可)

○接続する本装置側の設定
接続で使用する「本装置側の設定 1～8」を選択します。

○インターフェースの IP アドレス
相手側 IPsec 装置の IP アドレスを設定します。
相手側装置への IP アドレスの割り当てが固定か動的かで、入力が異なります。

[**相手側装置が固定アドレスの場合**]
IP アドレスをそのまま入力します。

[**相手側装置が動的アドレスの場合**]
「0.0.0.0」を入力します。

○上位ルータの IP アドレス
空欄にしておきます。

○インターフェースの ID
対向側装置への IP アドレスの割り当てが動的割り当ての場合に限り、IP アドレスの代わりに ID を設定します。

＜入力形式＞　**@＜任意の文字列＞**
＜入力例＞　@centurysystems
(@ の後は、任意の文字列でかまいません。)

対向側装置への割り当てが固定アドレスの場合は設定の必要はありません。

○モードの設定
IKE のフェーズ 1 モードを「main モード」と「aggressive モード」のどちらかから選択します。

III. IPsec 設定

○ transform の選択
ISAKMP SAの折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。
本装置は､以下のものの組み合わせが選択できます。

- DH group 値 (group1、group2、group5)
- 暗号化アルゴリズム (des、3des、aes)
- 認証アルゴリズム (md5、sha1)

「aggressive モード」の場合、接続相手の機器に合わせて transform を選択する必要があります。
aggressive モードでは transform を 1 つだけ選択してください(2 番目～4 番目は「使用しない」を選択しておきます)。

「main モード」の場合も transform を選択できますが、基本的には「すべてを送信する」の設定で構いません。

○ IKE のライフタイム
ISAKMP SA のライフタイムを設定します。
ISAKMP SA のライフタイムとは、双方のホスト認証と秘密鍵を交換するトンネルの有効期間のことです。
1081～28800 秒の間で設定します。

[鍵の設定]
○ PSK を使用する
PSK 方式の場合に、「PSK を使用する」にチェックして、相手側と任意に決定した共通鍵を入力してください。
半角英数字のみ使用可能です。

○ RSA を使用する
RSA 公開鍵方式の場合には、「RSA を使用する」にチェックして、相手側から通知された公開鍵を入力してください。
「X.509」設定の場合も「RSA を使用する」にチェックします。

[X509 の設定]
○接続先の証明書の設定
「X.509」設定で IPsec 通信をおこなう場合は、相手側のデジタル証明書をテキストボックス内に貼り付けます。

最後に「設定の保存」をクリックして設定完了です。

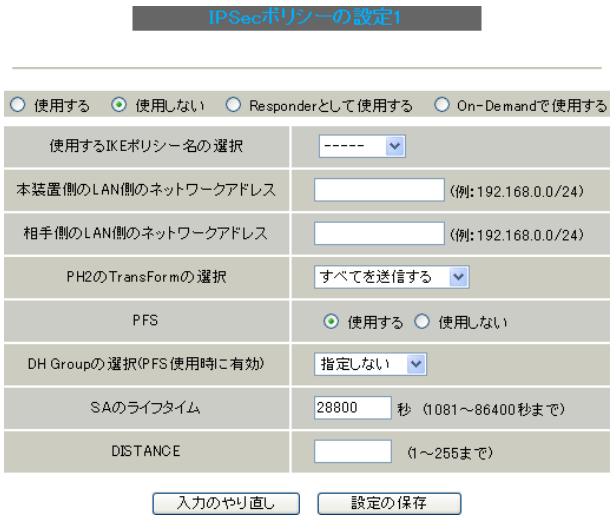
続いて、**IPsec ポリシーの設定**をおこないます。

III．IPsec 設定

STEP 5　IPsec ポリシーの設定

IPsec 設定画面上部の「IPsec ポリシーの設定」の「IPsec 1」～「IPsec 1024」いずれかをクリックして、以下の画面から設定します。
32 個以上設定する場合は「IPSec ポリシーの設定画面インデックス」で切り替えてください。

（画面は「IPSec 20」までの表示例です）



(画面は「IPSec ポリシーの設定 1」です)

○最初に IPsec の起動状態を選択します。

「使用する」
initiator にも responder にもなります。

「使用しない」
その IPsec ポリシーを使用しません。

「Responder として使用する」
サービス起動時や起動中の IPsec ポリシー追加時に、responder として IPsec 接続を待ちます。
本装置が固定 IP アドレス設定で接続相手が動的 IP アドレス設定の場合は、本値を選択してください。
また、後述する IPsec　KeepAlive 機能において、backupSA として使用する場合もこの選択にしてください。メイン側の IPsecSA で障害を検知した場合に、Initiator として接続を開始します。

「On-Demand で使用する」
IPsec をオンデマンド接続します。
切断タイマーは SA のライフタイムとなります。

○使用する IKE ポリシー名の選択
STEP 4 で設定した IKE/ISAKMP ポリシーのうち、どのポリシーを使うかを選択します。

○本装置側の LAN 側のネットワークアドレス
本装置が接続している LAN のネットワークアドレスを入力します。
ネットワークアドレス / マスクビット値の形式で入力します。
＜入力例＞　**192.168.0.0/24**

○相手側の LAN 側のネットワークアドレス
対向の IPsec 装置が接続している LAN 側ネットワークアドレスを入力します。
ネットワークアドレス / マスクビット値の形式で入力します。設定の要領は「本装置側の LAN 側のネットワークアドレス」と同様です。
ただし、NAT Traversal 機能を使用し、接続相手が NAT 内にある場合に限っては、“**vhost:%priv**”と設定します

○ PH2 の TransForm の選択
IPsec SA の折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。
- すべてを送信する
- 暗号化アルゴリズム　(des、3des、aes)
- 認証アルゴリズム　(md5、sha1)

通常は「すべてを送信する」の選択で構いません。

○ PFS
PFS(PerfectForwardSecrecy)を「使用する」か「使用しない」かを選択します。
PFS とは、パケットを暗号化している秘密鍵が解読されても、その鍵ではその後に生成された鍵を解読できないようにするものです。装置への負荷が増加しますが、より高いセキュリティを保つためには PFS を使用することを推奨します。

III. IPsec 設定

○DH Group の選択(PFS 使用時に有効)
「PFS を使用する」場合に使用する DH group を選択します。
ただし「指定しない」を選択しても構いません。
その場合は、PH1 の結果、選択された DH Group 条件と同じ DH Group を接続相手に送ります。

○SA のライフタイム
IPsec SA の有効期間を設定します。
IPsecSA とはデータを暗号化して通信するためのトラフィックのことです。1081～86400 秒の間で設定します。

○DISTANCE
IPsec ルートの DISTANCE 値を設定します。
同じ内容でかつ DISTANCE 値の小さい IPsec ポリシーが起動したときには、DISTANCE 値の大きいポリシーは自動的に切断されます。
なお、本設定は省略可能です。省略した場合は“1”として扱います。

IPsec ルートを OSPF で再配信する場合は、「OSPF 機能設定」の「static ルートの再配信」を「有効」にする必要があります。

最後に「設定の保存」をクリックして設定完了です。
続いて、**IPsec 機能の起動**をおこないます。

[IPsec 通信時の Ethernet ポート設定について]
IPsec 設定をおこなう場合は、Ethernet ポートの設定に注意してください。

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが本装置の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。
たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 の設定で、かつ、本装置の Ether1 ポートに 192.168.1.254 が設定されていると、正常に IPsec 通信がおこなえません。

このような場合は本装置の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

STEP 6 IPsec 機能を起動する

「各種サービスの設定」をクリックして、以下の画面を開きます。

○動作状態の制御
IPsec サーバ項目、「起動」にチェックして「動作変更」をクリックすると、IPsec 機能が起動します。以降は、本装置を起動するたびに IPsec 機能が自動起動します。
IPsec 機能を止める場合は「停止」にチェックして「動作変更」をクリックしてください。

IPsec 機能を起動した後は、現在のサービス稼働状況が「動作中」と表示されます。

起動する IKE/ISAKMP ポリシー、IPsec ポリシーが増えるほど、IPsec の起動に時間がかかります。起動が完了するまで数十分かかる場合もあります。

III. IPsec 設定

STEP 7 IPsec 接続を確認する

IPsec が正常に接続したかどうかは、「システム設定」の「ログの表示」でログを確認します。

ログの中で、以下のメッセージが含まれているかを確認してください。

<以下のログメッセージは「メインモード」で通信した場合の表示例です>

```
Aug  1 12:00:20 localhost ipsec__plutorun:
004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP SA
established  ・・・(1)
```

および

```
Aug  1 12:00:20 localhost ipsec__plutorun:
004 "xripsec1" #2: STATE_QUICK_I2: sent QI2,
IPsec SA established  ・・・(2)
```

上記 2 つのメッセージが表示されていれば、IPsec が正常に接続されています。

(1)のメッセージ
IKE 鍵交換が正常に完了し、ISAKMP SA が確立したことを示しています。

(2)のメッセージ
IPsec SA が正常に確立したことを示しています。

STEP 8 IPsec ステータス確認の確認

IPsec の簡単なステータスを確認できます。
「各種サービスの設定」→「IPsec サーバ」→「ステータス」をクリックして、画面を開きます。

(画面は表示例です)

それぞれの対向側設定でおこなった内容から、本装置・相手側の LAN アドレス・IP アドレス・上位ルータアドレスの一覧や、現在の動作状況が表示されます。

「現在の状態」リンクをクリックすると、現在の IPsec の状況が表示されます。

また、それぞれの設定番号をクリックすると、設定画面に移ることができます。

Ⅳ. IPsec Keep-Alive 機能

IPsec Keep-Alive 機能は、IPsec トンネルの障害を検出する機能です。

指定した宛先へ IPsec トンネル経由で ping パケットを発行して、応答がない場合に IPsec トンネルに障害が発生したと判断し、その IPsec トンネルを自動的に削除します。
不要な IPsec トンネルを自動的に削除し、IPsecSA の再起動またはバックアップ SA を起動することで、IPsec の再接続性を高めます。

[IPsec Keep-Alive 設定]
IPsec 設定画面上部の「IPsec Keep-Alive 設定」をクリックして設定します。
設定は 1024 まで可能です。画面下部にある「ページインデックス」のリンクをクリックしてください。

IPSec Keep-Alive設定

No.1～16まで

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1 *	動作option 2 *	interface	backup SA	remove?
1	☐			30	3	60	☑	☐	ipsec0		☐
2	☐			30	3	60	☑	☐	ipsec0		☐
3	☐			30	3	60	☑	☐	ipsec0		☐
4	☐			30	3	60	☑	☐	ipsec0		☐
5	☐			30	3	60	☑	☐	ipsec0		☐
6	☐			30	3	60	☑	☐	ipsec0		☐
7	☐			30	3	60	☑	☐	ipsec0		☐
8	☐			30	3	60	☑	☐	ipsec0		☐
9	☐			30	3	60	☑	☐	ipsec0		☐
10	☐			30	3	60	☑	☐	ipsec0		☐
11	☐			30	3	60	☑	☐	ipsec0		☐
12	☐			30	3	60	☑	☐	ipsec0		☐
13	☐			30	3	60	☑	☐	ipsec0		☐
14	☐			30	3	60	☑	☐	ipsec0		☐
15	☐			30	3	60	☑	☐	ipsec0		☐
16	☐			30	3	60	☑	☐	ipsec0		☐

設定/削除の実行

ページインデックス

1 - 16 17 - 32 33 - 48 49 - 64 65 - 80 81 - 96 97 -112 113-128
129-144 145-160 161-176 177-192 193-208 209-224 225-240 241-256
257-272 273-288 289-304 305-320 321-336 337-352 353-368 369-384
385-400 401-416 417-432 433-448 449-464 465-480 481-496 497-512
513-528 529-544 545-560 561-576 577-592 593-608 609-624 625-640
641-656 657-672 673-688 689-704 705-720 721-736 737-752 753-768
769-784 785-800 801-816 817-832 833-848 849-864 865-880 881-896
897-912 913-928 929-944 945-960 961-976 977-992 993-1008 1009-1024

動作optionの説明
動作option 1 check on
IPsecのネゴシエーション動作と連動して動作します。timeout/delayはicmp echo reply timeout値として認識します。
timeout値>(interval/count)の場合は実行時にtimeout値は(interval/count)秒となります。
動作option 2は無視します。
動作option 1 check off
IPsecのネゴシエーション動作とは非連動、動作option 2の設定に従って動作します。timeout/delayはdelay値として認識します。
動作option 2 check on
IPsec SAの状態に依存せず指定したパラメータでkeepalive動作をします。
動作option 2 check off
IPsec SAがestablishした後の最初のicmp echo replyが確認出来た時点からkeepalive動作を始めます。

○ enable
設定を有効にする時にチェックします。
IPsec Keep-Alive 機能を使いたい IPsec ポリシーと同じ番号にチェックを入れます。

○ source address
IPsec通信をおこなう際の、XRのLAN側インタフェースの IP アドレスを入力します。

IV. IPsec Keep-Alive 機能

○ destination address
IPsec 通信をおこなう際の、本装置の対向側装置の LAN 側のインタフェースの IP アドレスを入力します。

○ interval(sec)
○ watch count
ping を発行する間隔を設定します。
「『interval(sec)』間に『watch count』回 ping を発行する」という設定になります。

○ timeout/delay(sec)
後述の「動作 option 1」の設定に応じて、入力値の意味が異なります。

・動作 option 1 が有効の場合
入力値は timeout(秒)として扱います。
timeout とは ping 送出時の reply 待ち時間です。
ただし、timeout 値が(interval/watch count)より大きい場合は、reply 待ち時間は(interval/watch count)となります。

・動作 option 1 が無効の場合
入力値は delay(秒)として扱います。
delay とは IPsec が起動してから ping 送信を開始するまでの待ち時間です。IPsec が確立するまでの時間を考慮して設定します。
また、ping の reply 待ち時間は、(interval/watch count)秒となります。

○動作 option 1
IPsec ネゴシエーションと同期して Keep-Alive をおこなう場合は、チェックを入れます。
チェックを入れない場合は、IPsec ネゴシエーションと非同期に Keep-Alive をおこないます。

注) 本オプションにチェックを入れない場合、IPsec ネゴシエーションと Keep-Alive が非同期におこなわれるため、タイミングによっては IPsecSA の確立と ping の応答待ちタイムアウトが重なってしまい、確立直後の IPsecSA を切断してしまう場合があります。

■ IPsec ネゴシエーションとの同期について
IPsec ポリシーのネゴシエーションは下記のフェーズを遷移しながらおこないます。
動作 option 1 を有効にした場合、各フェーズと同期した Keep-Alive 動作をおこないます。

・フェーズ 1 (イニシエーションフェーズ)
ネゴシエーションを開始し、IPSec ポリシー確立中の状態です。
この後、正常に IPSec ポリシーが確立できた場合はフェーズ 3 へ移行します。
また、要求に対して対向装置からの応答がない場合はタイムアウトによりフェーズ 2 へ移行します。
※ フェーズ 3 に移行するまで ping の送出はおこないません。

・フェーズ 2 (ネゴシエーション T.O. フェーズ)
フェーズ 1 におけるネゴシエーションが失敗、またはタイムアウトした状態です。
この時、バックアップ SA を起動し、フェーズ 1 に戻ります。

・フェーズ 3 (ポリシー確立フェーズ)
IPSec ポリシーが正常に確立した状態です。
確立した IPSec ポリシー上を通過できる ping を使用して IPSec ポリシーの疎通確認を始めます。
この時、マスター SA として確立した場合は、バックアップ SA のダウンをおこないます。
また、同じ IKE を使う他の IPSec ポリシーがある場合は、それらのネゴシエーションを開始します。
この後、ping の応答がタイムアウトした場合は、フェーズ 4 に移行します。

・フェーズ 4 (ポリシーダウンフェーズ)
フェーズ 3 において ping の応答がタイムアウトした時や対向機器より delete SA を受け取った時には、ping の送出を停止して、監視対象の IPSec ポリシーをダウンさせます。
さらに、バックアップ SA を起動させた後、フェーズ 1 に戻ります。

IV. IPsec Keep-Alive 機能

○動作 option 2
本オプションは「動作 option 1」が無効の場合のみ、有効になります。
チェックを入れると、delay 後に ping を発行して、ping が失敗したら即座に指定された IPsec トンネルの削除、再折衝を開始します。
また、Keep-Alive による SA 削除後は、毎回 delay 秒待ってから Keep-Alive が開始されます。
チェックはずすと、delay 後に最初に ping が成功(IPsec が確立)し、その後に ping が失敗してはじめて指定された IPsec トンネルの削除、再折衝を開始します。
IPsec が最初に確立する前に ping が失敗してもなにもしません。
また、delay は初回のみ発生します。

○ interface
Keep-Alive 機能を使う、本装置の IPsec インタフェース名を選択します。
本装置のインタフェース名については、本マニュアルの「付録 A インタフェース名一覧」をご参照ください。

○ backup SA
ここに IPsec ポリシーの設定番号を指定しておくと、IPsec Keep-Alive 機能で IPsec トンネルを削除した時に、ここで指定した IPsec ポリシー設定を backup SA として起動させます。

注) backup SA として使用する IPsec ポリシーの起動状態は必ず「Responder として使用する」を選択してください。

複数の IPsec ポリシーを設定することも可能です。その場合は、”_”でポリシー番号を区切って設定します。これにより、指定した複数の IPsec ポリシーがネゴシエーションを開始します。

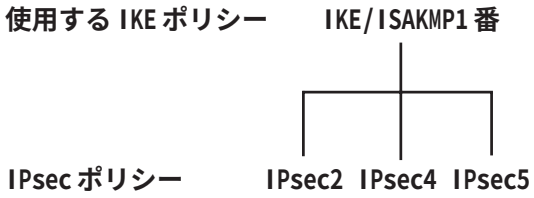
＜入力例＞ 1_2_3

またここに、以下のような設定もできます。

ike<n> ※ <n> は 1 ～ 128 の整数

この設定の場合、バックアップ SA 動作時には、「IPsec ポリシー設定の<n>番」が使用しているものと同じ IKE/ISAKMP ポリシーを使う他の IPsec ポリシーが、同時にネゴシエーションをおこないます。

＜例＞



上図の設定で backupSA に「ike2」と設定すると、「IPsec2」が使用している IKE/ISAKMP ポリシー設定 1 番を使う、他の IPsec ポリシー(IPsec4 と IPsec5)も同時にネゴシエーションを開始します。

○ remove?
設定を削除したいときにチェックします。

IV. IPsec Keep-Alive 機能

最後に「設定 / 削除の実行」をクリックしてください。
設定は即時に反映され、enable を設定したものは Keep-Alive 動作を開始します。

remove 項目にチェックが入っているものについては、その設定が削除されます。

設定番号について

IPsec Keep-Alive 機能を使う際は、監視する IPsec のポリシー No. と Keep-Alive の Pocily No. は一致させてください。

IPsec トンネルの障害を検知する条件

IPsec Keep-Alive 機能によって障害を検知するのは、「interval/watch count」に従って ping を発行して、一度も応答がなかったときです。
このとき本装置は、ping の応答がなかった IPsec トンネルを自動的に削除します。
反対に一度でも応答があったときは、本装置は IPsec トンネルを保持します。

動的アドレスの場合の本機能の利用について

拠点側に動的 IP アドレスを用いた構成で、センター側からの通信があるようなケースについては SA の不一致が起こりうるため、拠点側で IPsec Keep-Alive 機能を動作させることを推奨します。

Ⅴ.「X.509 デジタル証明書」を用いた電子認証

本装置は X.509 デジタル証明書を用いた電子認証方式に対応しています。

ただし、本装置は証明書署名要求の発行や証明書の発行ができません。
あらかじめ CA 局から証明書の発行を受けておく必要があります。

電子証明の仕組みや証明書発行の詳しい手順につきましては、関連書籍等をご参考ください。

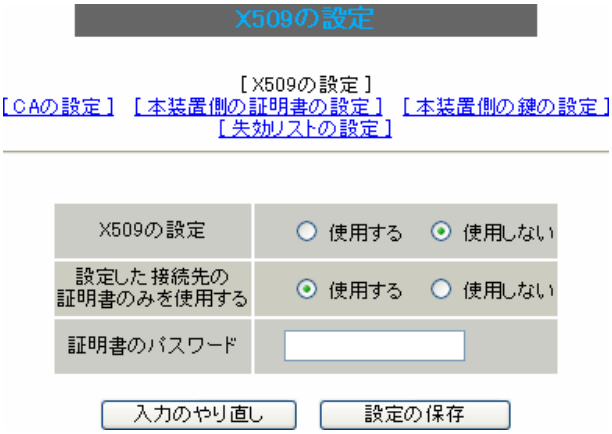
情報処理振興事業協会セキュリティセンター
http://www.ipa.go.jp/security/pki/

設定は、IPsec 設定画面内の「X.509 の設定」からおこなえます。

設定方法

IPsec 設定画面上部の「X509 の設定」→「X509 の設定」を開きます。

[X.509 の設定]



○X509 の設定
X.509 の使用 / 不使用を選択します。

○設定した接続先の証明書のみを使用する
設定した接続先の証明書のみの使用 / 不使用を選択します。

○証明書のパスワード
証明書のパスワードを入力します。

入力後「設定の保存」をクリックします。

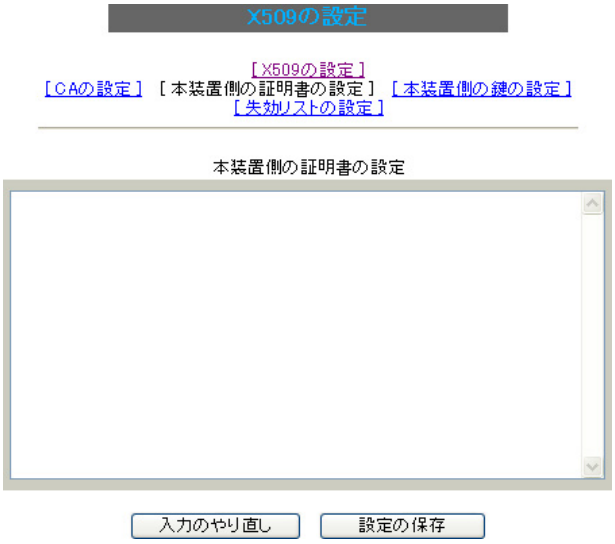
[CA の設定]

ここには、CA 局自身のデジタル証明書の内容をコピーして貼り付けます。(「cacert.pem」ファイル等。)

コピーを貼り付けましたら、「設定の保存」をクリックします。

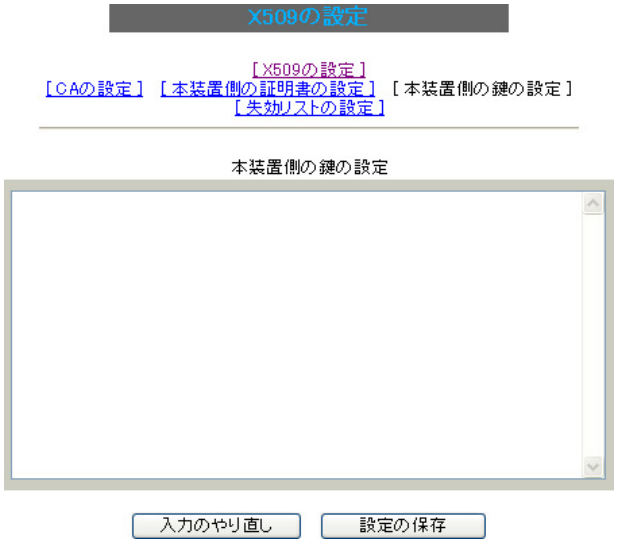
V．「X.509 デジタル証明書」を用いた電子認証

[本装置側の証明書の設定]
ここには、本装置に対して発行されたデジタル証明書の内容をコピーして貼り付けます。



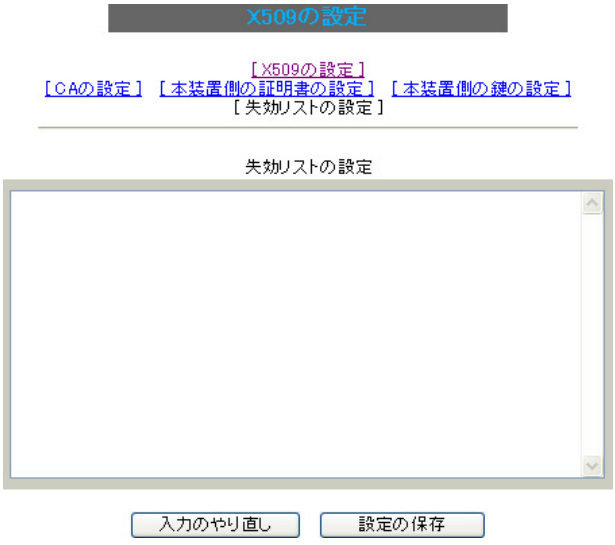
コピーを貼り付けましたら、「設定の保存」をクリックします。

[本装置側の鍵の設定]
ここにはデジタル証明書と同時に発行された、本装置の秘密鍵の内容をコピーして貼り付けます。
(「cakey.pem」ファイル等。)



コピーを貼り付けましたら、「設定の保存」をクリックします。

[失効リストの設定]
失効リストを作成している場合は、その内容をコピーして貼り付けます。(「crl.pem」ファイル等。)



コピーを貼り付けましたら、「設定の保存」をクリックします。

[接続先の証明書の設定]
「IKE/ISAKMP ポリシーの設定」画面内の[鍵の設定]は下記のように設定してください。
- 「RSA を使用する」　チェック
- 設定欄　空欄

(「本装置の設定」画面の[鍵の表示]欄も空欄にしておきます。)

「IKE/ISAKMP ポリシーの設定」画面内[X509 の設定]の「接続先の証明書の設定」は下記のように設定してください。
- 設定欄　相手側のデジタル証明書の貼付

以上で X.509 の設定は完了です。

[その他の IPsec 設定]
上記以外の設定については、通常の IPsec 設定と同様です。

VI．IPsec 通信時のパケットフィルタ設定

ステートフルパケットインスペクション機能を使っていたり、パケットフィルタの設定によっては、IPsec通信ができない場合があります。
このような場合は IPsec 通信でのデータをやりとりできるように、パケットフィルタの設定を追加する必要があります。

IPsec では、以下の 2 種類のプロトコル・ポートを使用します。

- **プロトコル「UDP」のポート「500」番**
  → IKE(IPsec の鍵交換)のトラフィックに必要です。

- **プロトコル「ESP」**
  →ESP(暗号化ペイロード)のトラフィックに必要です。

これらのパケットを通せるように、**「入力フィルタ」**に設定を追加してください。なお、「ESP」については、ポート番号の指定はしません。

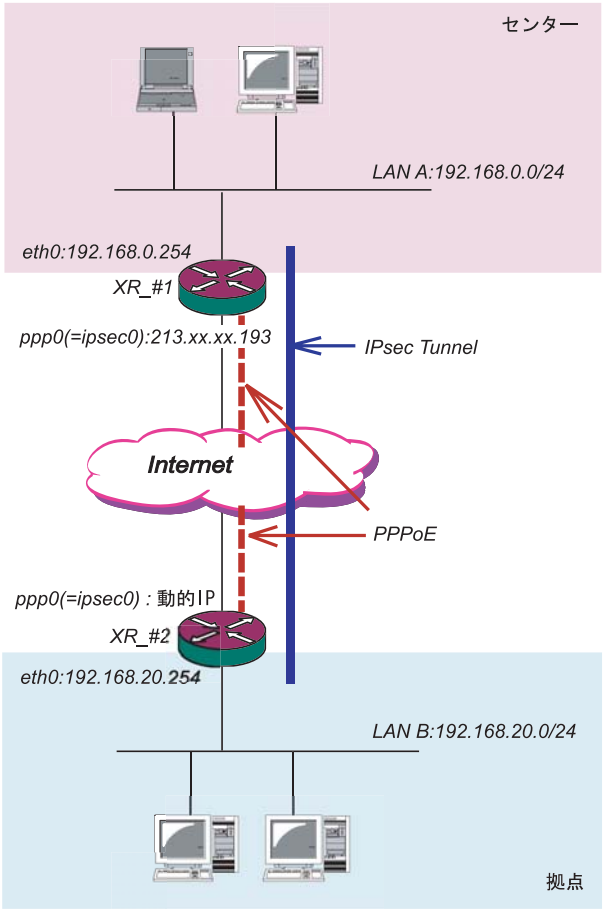
＜設定例＞

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	udp				500
2	ppp0	パケット受信時	許可	esp				

Ⅶ. IPsec 設定例 1（センター／拠点間の 1 対 1 接続）

センター／拠点間で IPsec トンネルを 1 対 1 で構築する場合の設定例です。

＜設定例 1＞



＜接続条件＞

- センター側／拠点側ともに PPPoE 接続とします。
- 但し、センター側は固定アドレス、拠点側は動的アドレスとします。
- IPsec 接続の再接続性を高めるため、IPsec Keep-Alive を用います。
- IP アドレス、ネットワークアドレス、インタフェース名は図中の表記を使用するものとします。
- 拠点側を Initiator、センター側を Responder とします。
- 拠点側が動的アドレスのため、aggressive モードで接続します。
- PSK 共通鍵を用い、鍵は「test_key」とします。

■ XR_#1(センター側 XR)の設定
各設定画面で下記のように設定します。

「本装置の設定」
「本装置側の設定 1」を選択します。

IKE/ISAKMPの設定1	
インターフェースのIPアドレス	213.xxx.xxx.193
上位ルータのIPアドレス	%ppp0
インターフェースのID	（例：@xr.centurysys）

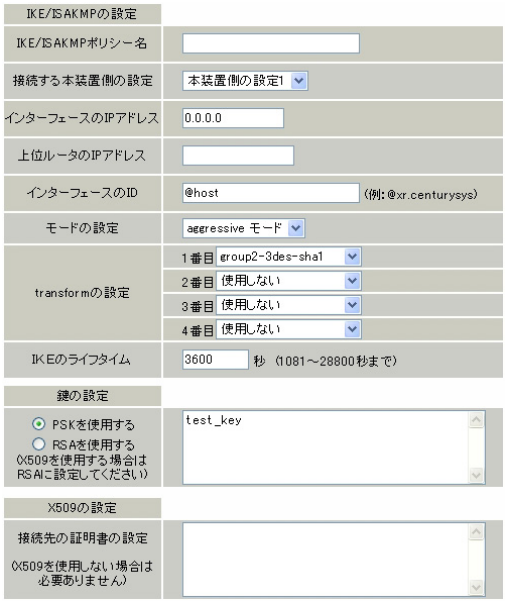
○インターフェースの IP アドレス
「213.xxx.xxx.193」

○上位ルータの IP アドレス
「%ppp0」
※ PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

○インターフェースの ID
「空欄」
※ 固定アドレスの場合は、「インターフェースの ID」は省略できます。省略した場合は、自動的に「インターフェースの IP アドレス」を ID として使用します。

Ⅶ. IPsec 設定例 1（センター／拠点間の 1 対 1 接続）

「IKE/ISAKMP ポリシーの設定」
「IKE1」を選択します。



○ IKE/ISAKMP ポリシー名 「(任意で設定します)」

○接続する本装置側の設定 「本装置側の設定 1」

○インターフェースの IP アドレス 「0.0.0.0」
※対向装置が動的アドレスの場合は必ずこの設定にしてください。

○上位ルータの IP アドレス 「空欄」

○インターフェースの ID 「@host」
(@以降は任意の文字列)
※上記の 2 項目は、対向装置の「本装置の設定」と同じものを設定します。

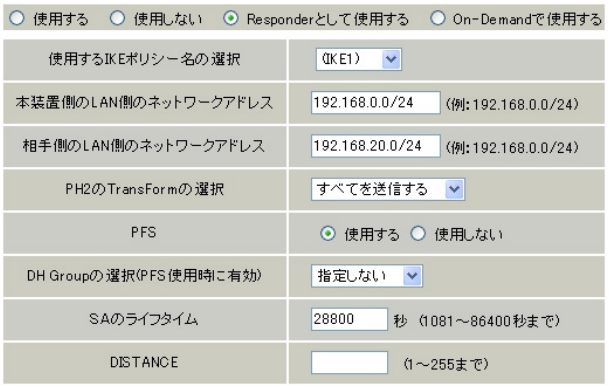
○モードの設定 「aggressive モード」

○ transform の設定 「group2-3des-sha1」
(任意の設定を選択)

○ IKE のライフタイム 「3600」
(任意の設定値)

○鍵の設定
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

「IPSec ポリシーの設定」
「IPSec1」を選択します。



○「Responder として使用する」を選択します。
※対向が動的アドレスの場合は、固定アドレス側は Initiator にはなれません。

○使用する IKE ポリシー名の選択 「IKE1」

○本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」

○相手側の LAN 側のネットワークアドレス
「192.168.20.0/24」

○ PH2 の TransForm の選択 「すべてを送信する」

○ PFS 「使用する」(推奨)

○ DH Group の選択 「指定しない」

○ SA のライフタイム 「28800」(任意の設定値)

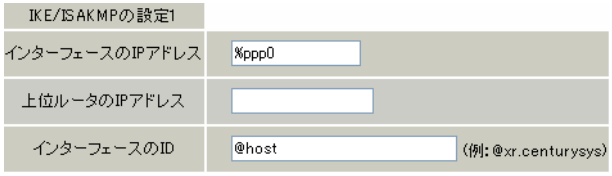
○ DISTANCE 「空欄」
※省略した場合は、自動的にディスタンス値を「1」として扱います。

「IPsec Keep-Alive の設定」
対向装置が動的アドレスの場合は、固定アドレス側からの再接続ができないため、通常、IPsec Keep-Alive は動的アドレス側(Initiator 側)で設定します。
よって、本装置では設定しません。

Ⅶ. IPsec 設定例 1（センター／拠点間の 1 対 1 接続）

■ XR_#2(拠点側 XR)の設定
各設定画面で下記のように設定します。

「本装置の設定」
「本装置側の設定１」を選択します。



○インタフェースの IP アドレス 「%ppp0」
※ PPPoE 接続かつ動的アドレスの場合は、必ずこの設定にします。

○上位ルータの IP アドレス [空欄]
※ PPPoE 接続かつ動的アドレスの場合は、空欄にして下さい。

○インタフェースの ID
「@host」(@以降は任意の文字列)
※ 動的アドレスの場合は、必ず任意の ID を設定します。

「IKE/ISAKMP ポリシーの設定」
「IKE1」を選択します。

○ IKE/ISAKMP ポリシー名 「(任意で設定します)」

○接続する本装置側の設定 「本装置側の設定 1」

○インターフェースの IP アドレス 「213.xx.xx.193」
※対向装置の IP アドレスを設定します。

○上位ルータの IP アドレス 「空欄」
※対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

○インターフェースの ID 「空欄」
※対向装置が固定アドレスなので、設定不要です。

○モードの設定 「aggressive モード」

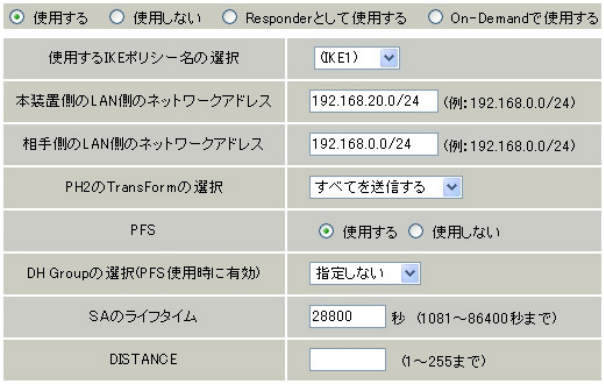
○ transform の設定 「group2-3des-sha1」
(任意の設定を選択)

○ IKE のライフタイム 「3600」(任意の設定値)

○鍵の設定
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

Ⅶ. IPsec 設定例 1（センター／拠点間の 1 対 1 接続）

「IPSec ポリシーの設定」
「IPSec1」を選択します。



○「使用する」を選択します。
※動的アドレスの場合は、必ず initiator として動作させます。

○使用する IKE ポリシー名の選択　「IKE1」

○本装置側の LAN 側のネットワークアドレス
「192.168.20.0/24」

○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」

○PH2 の TransForm の選択　「すべてを送信する」

○PFS　「使用する」（推奨）

○DH Group の選択　「指定しない」

○SA のライフタイム　「28800」（任意の設定値）

○DISTANCE　「空欄」
※省略した場合は、自動的にディスタンス値を「1」として扱います。

○enable にチェックを入れます。

○source address　「192.168.20.254」

○destination address　「192.168.0.254」
※source address には本装置側 LAN のインタフェースアドレスを、destination address には相手側 LAN のインタフェースアドレスを設定することを推奨します。

○ interval　「30」（任意の設定値）

○watch count　「3」（任意の設定値）

○timeout/delay　「60」（任意の設定値）
※動作 option 1 を無効にするため、本値は delay(ping 送出開始待ち時間)=60 秒を意味します。

○動作 option 1　「空欄」

○動作 option 2　「チェック」

○ interface　「ipsec0」
※ ppp0 上のデフォルトの IPsec インタフェース名は“ ipsec0 ”です。

○backup SA　「空欄」

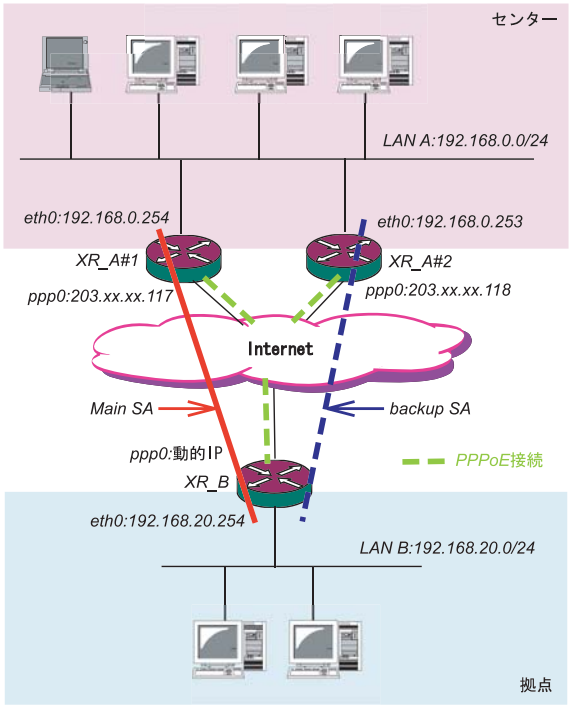
「IPsec Keep-Alive の設定」
PolicyNo.1 の行に設定します。

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1※	動作option 2※	interface	backup SA	remove?
1	☑	192.168.20.254	192.168.0.254	30	3	60	☐	☑	ipsec0		☐

Ⅷ. IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

センター側を 2 台の冗長構成とし、センター側の装置障害やネットワーク障害に備えて、センター／拠点間の IPsec トンネルを二重化する場合の設定例です。

＜設定例 2＞



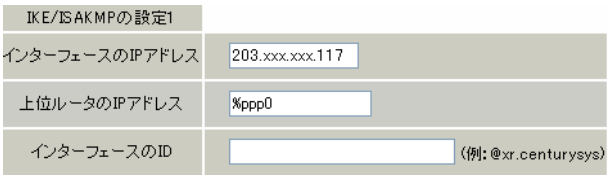
＜接続条件＞

- センター側は XR2 台の冗長構成とします。メインの IPsec トンネルは XR_A#1 側で、バックアップの IPsec トンネルは XR_A#2 側で接続するものとします。
- センター側／拠点側ともに PPPoE 接続とします。
- 但し、センター側は固定アドレス、拠点側は動的アドレスとします。
- 障害の検出および IPsec トンネルの切り替えは、拠点側の IPsec Keep-Alive を用いて行います。
- IP アドレス、ネットワークアドレス、インタフェース名は図中の表記を使用するものとします。
- 拠点側を Initiator、センター側を Responder とします。
- 拠点側が動的アドレスのため、aggressive モードで接続します。
- PSK 共通鍵を用い、鍵は「test_key」とします。
- センター側 LAN では、拠点方向のルートをアクティブの SA にフローティングさせるため、スタティックルートを用います。

「本装置の設定」

■ XR_A#1(センター側 XR#1)の設定

「本装置側の設定１」を選択します。



○インターフェースの IP アドレス

「203.xxx.xxx.117」

○上位ルータの IP アドレス　「%ppp0」

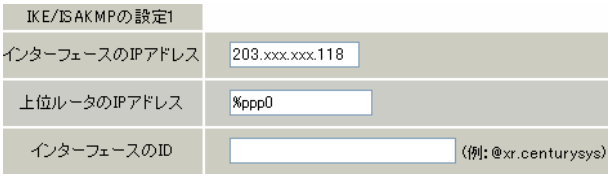
※ PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

○インターフェースの ID　「空欄」

※固定アドレスの場合は、「インターフェースの ID」は省略できます。省略した場合は、自動的に「インターフェースの IP アドレス」を ID として使用します。

■ XR_A#2(センター側 XR#2)の設定

「本装置側の設定１」を選択します。



○インターフェースの IP アドレス

「203.xxx.xxx.118」

○上位ルータの IP アドレス　「%ppp0」

※ PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

○インターフェースの ID　「空欄」

※固定アドレスの場合は、「インターフェースの ID」は省略できます。省略した場合は、自動的に「インターフェースの IP アドレス」を ID として使用します。

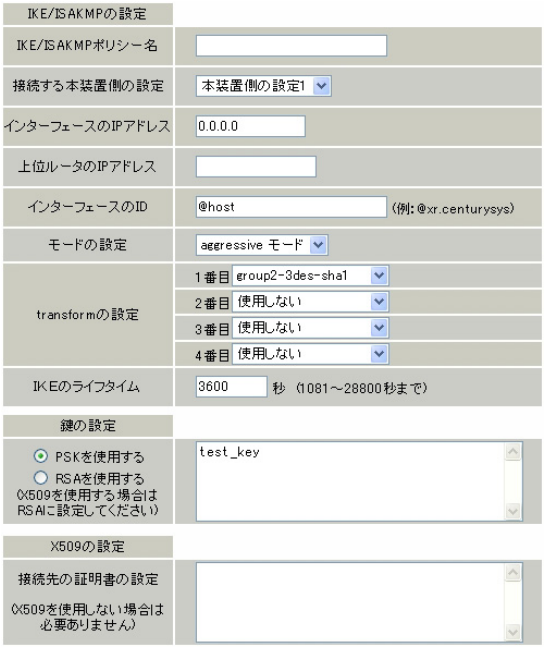
Ⅷ．IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

「IKE/ISAKMP ポリシーの設定」

■ XR_A#1,XR_A#2 の IKE/ISAKMP ポリシーの設定

IKE/ISAKMP ポリシーの設定は、鍵の設定を除いて、センター側 XR#1,XR#2 共に同じ設定で構いません。

「IKE1」を選択します。



○ IKE/ISAKMP ポリシー名 「(任意で設定します)」

○接続する本装置側の設定 「本装置側の設定 1」

○インターフェースの IP アドレス 「0.0.0.0」
※対向装置が動的アドレスの場合は必ずこの設定にします。

○上位ルータの IP アドレス 「空欄」

○インターフェースの ID 「@host」
(@以降は任意の文字列)
※上記の 2 項目は、対向装置の「本装置の設定」と同じものを設定します。

○モードの設定 「aggressive モード」

○ transform の設定 「group2-3des-sha1」
(任意の設定を選択)

○ IKE のライフタイム 「3600」(任意の設定値)

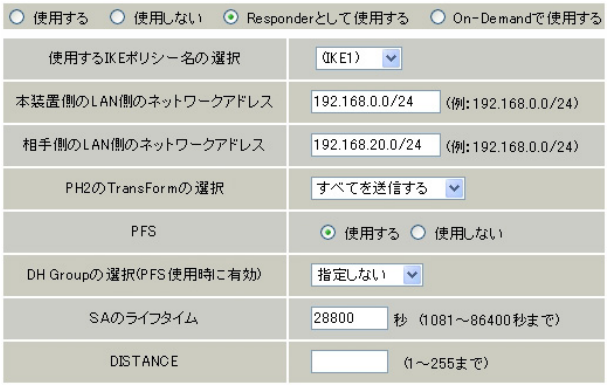
○鍵の設定
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

「IPSec ポリシーの設定」

■ XR_A#1,XR_A#2 の IPsec ポリシーの設定

IPsec ポリシーの設定は、センター側 XR#1,XR#2 共に同じ設定で構いません。

「IPSec1」を選択します。



○「Responder として使用する」を選択します。

○使用する IKE ポリシー名の選択 「IKE1」

○本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」

○相手側の LAN 側のネットワークアドレス
「192.168.20.0/24」

○ PH2 の TransForm の選択 「すべてを送信する」

○ PFS 「使用する」(推奨)

○ DH Group の選択 「指定しない」

○ SA のライフタイム 「28800」(任意の設定値)

○ DISTANCE 「空欄」

Ⅷ. IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

「転送フィルタ」の設定

メイン側 XR と WAN とのネットワーク断により、バックアップ SA へ切り替えた際、メイン SA への KeepAlive 要求がバックアップ XR からセンター側 LAN を経由してメイン側 XR に届いてしまいます。これにより、IPsec 接続が復旧したと誤認し、再びメイン SA へ切り戻ししようとするため、バックアップ接続が不安定な状態になります。

これを防ぐために、**バックアップ側 XR(XR_A#2)**に下記のような転送フィルタを設定してください。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.254	

○インターフェース　「ipsec0」
※ ppp0 のデフォルトの IPsec インタフェースの“ ipsec0 ”を設定します。

○動作　「破棄」

○送信元アドレス　「192.168.20.254」
※拠点側メイン SA の KeepAlive の送信元アドレスを設定します。

○あて先アドレス　「192.168.0.254」
※拠点側メイン SA の KeepAlive の送信先アドレスを設定します。

また同じ理由から、メイン SA で接続中に IPsec 接続が不安定になるのを防ぐために、**メイン側 XR (XR_A#1)**にも下記のような転送フィルタを設定してください。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.253	

○インターフェース　「ipsec0」
※ ppp0 のデフォルトの IPsec インタフェースの“ ipsec0 ”を設定します。

○動作　「破棄」

○送信元アドレス　「192.168.20.254」
※拠点側バックアップ SA の KeepAlive の送信元アドレスを設定します。

○あて先アドレス　「192.168.0.253」
※拠点側バックアップ SA の KeepAlive の送信先アドレスを設定します。

「スタティックルート」の設定

センター側の XR では自分が IPsec 接続していないときに、拠点方向のルートを IPsec 接続中の XR へフローティングさせるために、スタティックルートの設定をおこないます。
自分が IPsec 接続しているときは、IPsec ルートのディスタンス値(=1)の方が小さいため、このスタティックルートは無効の状態となっています。

■ XR_A#1 のスタティックルート設定

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.20.0	255.255.255.0		192.168.0.253	20

○アドレス　「192.168.20.0」

○ネットマスク　「255.255.255.0」

○ゲートウェイ　「192.168.0.253」
※ XR_A#2 のアドレスを設定します。

○ディスタンス　「20」
※ IPsec ルートのディスタンス(=1)より大きい任意の値を設定します。

■ XR_A#2 のスタティックルート設定

アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス <1-255>
192.168.20.0	255.255.255.0		192.168.0.254	20

○アドレス　「192.168.20.0」

○ネットマスク　「255.255.255.0」

○ゲートウェイ　「192.168.0.254」
※ XR_A#1 のアドレスを設定します。

○ディスタンス　「20」
※ IPsec ルートのディスタンス(=1)より大きい任意の値を設定します。

Ⅷ. IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

「IPSec Keep-Alive 設定」
さらに、障害時にすぐにフローティングスタティックルートへ切り替えるために、IPsec Keep-Alive を設定します。
(KeepAlive 機能を使用しない場合は、Rekey のタイミングまでフローティングできない場合があります。)

■ XR_A#1 の IPsec Keep-Alive 設定

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1※	動作option 2※	interface	backup SA	remove?
1	☑	192.168.0.254	192.168.20.254	30	3	60	☐	☑	ipsec0		☐

○enable にチェックを入れます。
○source address 「192.168.0.254」
○destination address 「192.168.20.254」
○interval 「30」(任意の設定値) **※注)**
○watch count 「3」(任意の設定値)
○timeout/delay 「60」(任意の設定値)
※ 動作 option 1 を無効にするため、本値は delay(ping 送出 delay 時間)=60 秒を意味します。
○動作 option 1 「空欄」
○動作 option 2 「チェック」
○interface 「ipsec0」
○backup SA 「空欄」

■ XR_A#2 の IPsec Keep-Alive 設定

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1※	動作option 2※	interface	backup SA	remove?
1	☑	192.168.0.253	192.168.20.254	30	3	60	☐	☑	ipsec0		☐

○enable にチェックを入れます。
○source address 「192.168.0.253」
○destination address 「192.168.20.254」
○interval 「30」(任意の設定値) **※注)**
○watch count 「3」(任意の設定値)
○timeout/delay 「60」(任意の設定値)
※ 動作 option 1 を無効にするため、本値は delay(ping 送出 delay 時間)=60 秒を意味します。
○動作 option 1 「空欄」
○動作 option 2 「チェック」
○interface 「ipsec0」
○backup SA 「空欄」

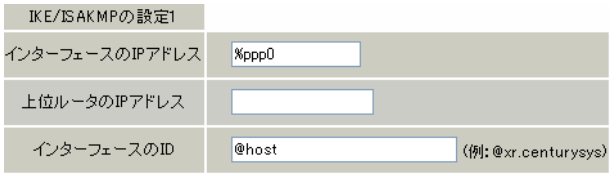
※注)
センター側と拠点側の interval が同じ値の場合、Keep-Alive の周期が同期してしまい、障害時の IPsec 切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec 通信が不安定になることがあります。
これを防ぐために、センター側の interval は拠点側のメイン SA, バックアップ SA のいずれの interval とも異なる値を設定することを推奨します。
ただし、センター内の XR 同士は同じ interval 値でも構いません。

Ⅷ．IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

■ XR_B(拠点側 XR)の設定

「本装置の設定」

「本装置側の設定１」を選択します。



○インターフェースの IP アドレス　「%ppp0」

※ PPPoE 接続かつ動的アドレスの場合は、必ずこの設定にします。

○上位ルータの IP アドレス　「空欄」

※ PPPoE 接続かつ動的アドレスの場合は、空欄にしてください。

○インターフェースの ID　「@host」

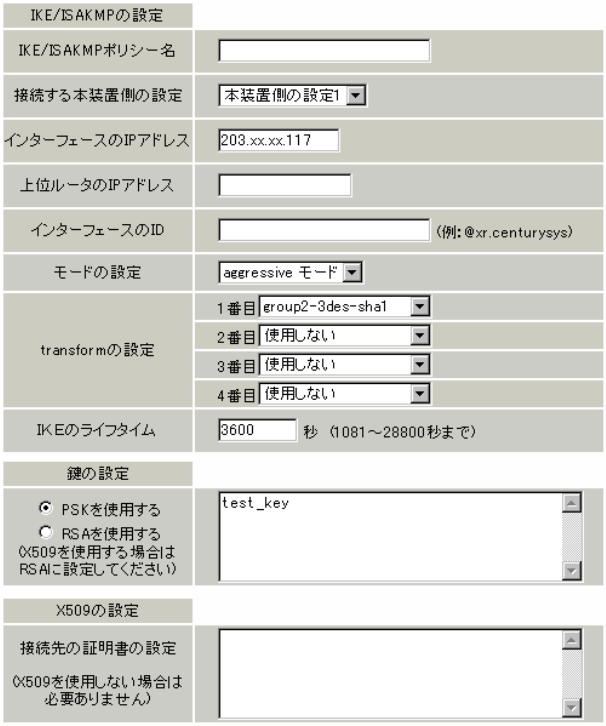
(@以降は任意の文字列)

※動的アドレスの場合は、必ず任意の ID を設定します。

メイン SA 用の IKE/ISAKMP ポリシーの設定をおこないます。

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。



○ IKE/ISAKMP ポリシー名　「(任意で設定します)」

○接続する本装置側の設定　「本装置側の設定1」

○インターフェースの IP アドレス　「203.xx.xx.117」

※対向装置が固定アドレスなので、そのIPアドレスを設定します。

○上位ルータの IP アドレス　「空欄」

※対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

○インターフェースの ID　「空欄」

※対向装置が固定アドレスなので、設定不要です。

○モードの設定　「aggressive モード」

○ transform の設定

1番目「group2-3des-sha1」（任意の設定を選択）

2～4番目「使用しない」

○ IKE のライフタイム　「3600」（任意の設定値）

○鍵の設定

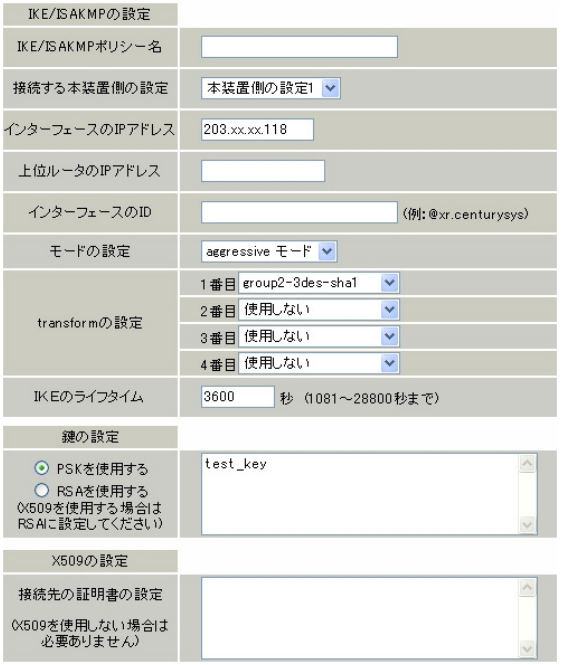
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

Ⅷ. IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

バックアップ SA 用の IKE/ISAKMP ポリシーの設定をおこないます。

「IKE/ISAKMP ポリシーの設定」

「IKE2」を選択します。



○ IKE/ISAKMP ポリシー名　「(任意で設定します)」

○接続する本装置側の設定　「本装置側の設定 1」

○インターフェースの IP アドレス　「203.xx.xx.118」
※対向装置が固定アドレスなので、そのIPアドレスを設定します。

○上位ルータの IP アドレス　「空欄」
※対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

○インターフェースの ID　「空欄」
※対向装置が固定アドレスなので、設定不要です。

○モードの設定　「aggressive モード」

○ transform の設定
1番目「group2-3des-sha1」（任意の設定を選択）
2～4 番目「使用しない」

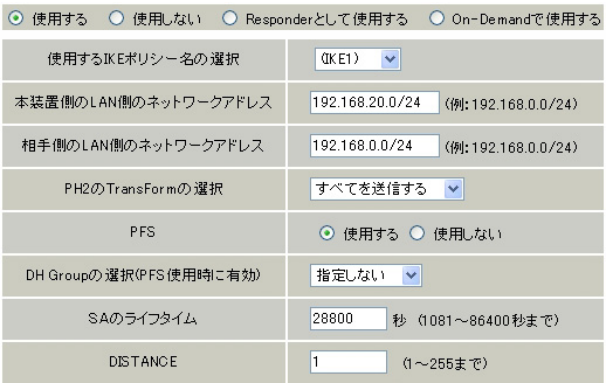
○ IKE のライフタイム　「3600」（任意の設定値）

○鍵の設定
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

メイン SA 用の IPsec ポリシーの設定をおこないます。

「IPSec ポリシーの設定」

「IPSec1」を選択します。



○「使用する」を選択します。
※本装置は Initiator として動作し、かつメイン SA 用の IPsec ポリシーであるため、「使用する」を選択します。

○使用する IKE ポリシー名の選択　「IKE1」

○本装置側の LAN 側のネットワークアドレス
「192.168.20.0/24」

○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」

○ PH2 の TransForm の選択　「すべてを送信する」

○ PFS　「使用する」（推奨）

○ DH Group の選択　「指定しない」

○ SA のライフタイム　「28800」（任意の設定値）

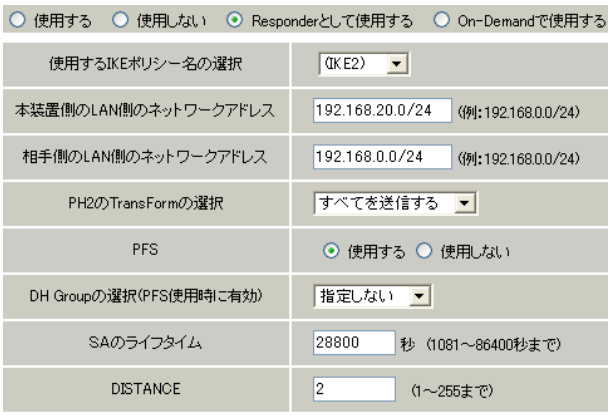
○ DISTANCE　「1」
※メイン側のディスタンス値は最小値(=1)を設定します。

Ⅷ．IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

バックアップ SA 用の IPsec ポリシーの設定をおこないます。

「IPSec ポリシーの設定」

「IPSec2」を選択します。



○「Responder として使用する」を選択します。
※バックアップ SA 用の IPsec ポリシーであるため、「Responder として使用する」を選択してください。

○使用する IKE ポリシー名の選択　「IKE2」

○本装置側の LAN 側のネットワークアドレス
「192.168.20.0/24」

○相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」

○ PH2 の TransForm の選択　「すべてを送信する」

○ PFS　「使用する」（推奨）

○ DH Group の選択　「指定しない」

○ SA のライフタイム　「28800」（任意の設定値）

○ DISTANCE　「2」
※バックアップ側のディスタンス値は、メイン側のディスタンス値より大きな値を設定します。

「IPsec Keep-Alive の設定」

拠点側が動的 IP アドレスを用いた構成で、センター側からの通信があるようなケースでは SA の不一致が起こりうるため、メイン側、バックアップ側の両方で Keep-Alive を動作させることを推奨します。

■メイン SA 用の KeepAlive の設定

PolicyNo.1 の行に設定します。

○ enable にチェックを入れます。
○ source address　「192.168.20.254」
○ destination address　「192.168.0.254」
○ interval　「45」（任意の設定値）
○ watch count　「3」（任意の設定値）
○ timeout/delay　「60」（任意の設定値）
○動作 option 1　「空欄」
○動作 option 2　「チェック」
○ interface　「ipsec0」
○ backupSA　「2」
※ Keep-Alive により障害検知した場合に、IPSec2 のポリシーに切り替えるため、“2”を設定します。

■バックアップ SA 用の KeepAlive の設定

PolicyNo.2 の行に設定します。

○ enable にチェックを入れます。
○ source address　「192.168.20.254」
○ destination address　「192.168.0.253」
○ interval　「60」（任意の設定値）　**※注)**
○ watch count　「3」（任意の設定値）
○ timeout/delay　「60」（任意の設定値）
○動作 option 1　「空欄」
○動作 option 2　「チェック」
○ interface　「ipsec0」
○ backupSA　「空欄」

※注)
メイン SA とバックアップ SA、または拠点側とセンター側の interval が同じ値の場合、Keep-Alive の周期が同期してしまい、障害時の IPsec 切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec 通信が不安定になることがあります。
これを防ぐために、拠点側の XR 同士の interval は、それぞれ異なる値を設定することを推奨します。さらにそれぞれの値はセンター側とも異なる値を設定してください。

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作option 1※	動作option 2※	interface	backup SA
1	☑	192.168.20.254	192.168.0.254	45	3	60	☐	☑	ipsec0	2
2	☑	192.168.20.254	192.168.0.253	60	3	60	☐	☑	ipsec0	

IX. IPsec がつながらないとき

IPsec で正常に通信できないときは本体ログを確認することで、どの段階で接続に失敗しているかを把握することができます。

本体ログは、Web 設定画面「システム設定」内の「ログ表示」で確認します。

[正常に IPsec 接続できたときのログメッセージ]

メインモードの場合

```
Aug  3 12:00:14 localhost ipsec_setup:
  ...FreeS/WAN IPsec started

Aug  3 12:00:20 localhost ipsec__plutorun:
 104 "xripsec1" #1: STATE_MAIN_I1: initiate

Aug  3 12:00:20 localhost ipsec__plutorun:
 106 "xripsec1" #1: STATE_MAIN_I2: from
 STATE_MAIN_I1; sent MI2, expecting MR2

Aug  3 12:00:20 localhost ipsec__plutorun:
 108 "xripsec1" #1: STATE_MAIN_I3: from
 STATE_MAIN_I2; sent MI3, expecting MR3

Aug  3 12:00:20 localhost ipsec__plutorun:
 004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP
SAestablished

Aug  3 12:00:20 localhost ipsec__plutorun:
 112 "xripsec1" #2: STATE_QUICK_I1: initiate

Aug  3 12:00:20 localhost ipsec__plutorun:
 004 "xripsec1" #2: STATE_QUICK_I2: sent QI2,
IPsec SA established
```

アグレッシブモードの場合

```
Apr 25 11:14:27 localhost ipsec_setup:
...FreeS/WAN IPsec started

Aug 3 11:14:34 localhost ipsec__plutorun:
whack:ph1_mode=aggressive whack:CD_ID=@home
whack:ID_FQDN=@home 112 "xripsec1" #1:
STATE_AGGR_I1: initiate

Aug 3 11:14:34 localhost ipsec__plutorun: 004
"xripsec1" #1: SAEST(e)=STATE_AGGR_I2: sent
AI2, ISAKMP SA established

Aug 3 12:14:34 localhost ipsec__plutorun: 117
"xripsec1" #2: STATE_QUICK_I1: initiate

Aug 3 12:14:34 localhost ipsec__plutorun: 004
"xripsec1" #2: SAEST(13)=STATE_QUICK_I2: sent
QI2, IPsec SA established
```

IX. IPsec がつながらないとき

「現在の状態」は IPsec 設定画面の「ステータス」から、画面中央下の「現在の状態」をクリックして表示します。

[正常に IPsec が確立したときの表示例]

```
000 interface ipsec0/eth1 218.xxx.xxx.xxx

000

000 "xripsec1": 192.168.xxx.xxx/24
===218.xxx.xxx.xxx[@<id>]---218.xxx.xxx.xxx...

000 "xripsec1": ...219.xxx.xxx.xxx
===192.168.xxx.xxx/24

000 "xripsec1":   ike_life: 3600s; ipsec_life:
28800s; rekey_margin: 540s; rekey_fuzz: 100%;
keyingtries: 0

000 "xripsec1":   policy: PSK+ENCRYPT+TUNNEL+PFS;
interface: eth1; erouted

000 "xripsec1":   newest ISAKMP SA: #1; newest
IPsec SA: #2; eroute owner: #2

000

000 #2: "xripsec1" STATE_QUICK_I2 (sent QI2, IPsec
SA established); EVENT_SA_REPLACE in 27931s;
newest IPSEC; eroute owner

000 #2: "xripsec1" esp.32a406c4@219.xxx.xxx.xxx
esp.1be9611c@218.xxx.xxx.xxx
tun.1002@219.xxx.xxx.xxx tun.1001@218.xxx.xxx.xxx

000 #1: "xripsec1" STATE_MAIN_I4 (ISAKMP SA
established); EVENT_SA_REPLACE in 2489s; newest
ISAKMP
```

これらのログやメッセージ内に

- **ISAKMP SA established**
- **IPsec SA established**

のメッセージがない場合は IPsec が確立していません。
設定を再確認してください。

IX．IPsec がつながらないとき

○「 ...FreeS/WAN IPsec started」でメッセージが止まっています。

この場合は、接続相手との IKE 鍵交換が正常におこなえていません。
IPsec 設定の「IKE/ISAKMP ポリシーの設定」項目で相手側機器についての設定を確認してください。

また、ステートフルパケットインスペクションを有効にしている場合、IPsec 通信のパケットを受信できるようにフィルタ設定を施す必要があります。IPsec のパケットを通すフィルタ設定は、「VI .IPsec 通信時のパケットフィルタ設定」をご覧ください。

○「ISAKMP SA established」メッセージは表示されていますが「IPsec SA established」メッセージが表示されていません。

この場合は、IPsec SA が正常に確立できていません。
IPsec 設定の「IPsec ポリシー設定」項目で、自分側と相手側のネットワークアドレスが正しいか、設定を確認してください。

○新規に設定を追加したのですが、追加した設定については IPsec がつながりません。

設定を追加し、その設定を有効にする場合には IPsec 機能を再起動(本体の再起動)をおこなってください。
設定を追加しただけでは設定が有効になりません。

○ IPSec は確立していますが、Windows でファイル共有ができません。

XR シリーズは工場出荷設定において、NetBIOS を通さないフィルタリングが設定されています。Windows ファイル共有をする場合はこのフィルタ設定を削除もしくは変更してください。

○ IPsec 通信中に回線が一時的に切断してしまうと、回線が回復しても IPsec 接続がなかなか復帰しません。

固定 IP アドレスと動的 IP アドレス間の IPsec 通信で、固定 IP アドレス側装置の IPsec 通信が意図しない切断をしてしまったときに起こりえる現象です。

相手が動的 IP アドレスの場合は相手側の IP アドレスが分からないために、固定 IP アドレス側からは IPsec 通信を開始することが出来ず、動的 IP アドレス側から IPsec 通信の再要求を受けるまでは IPsec 通信が復帰しなくなります。また動的側 IP アドレス側が IPsec 通信の再要求を出すのは IPsec SA のライフタイムが過ぎてからとなります。

これらの理由によって、IPsec 通信がなかなか復帰しない現象となります。

すぐに IPsec 通信を復帰させたいときは、動的 IP アドレス側の IPsec サービスも再起動してください。

動的 IP アドレス側の IPsec サービスの再起動が困難な環境でお使いの場合は、IPsec SA のライフタイムを短くして運用してください。

○相手の本装置には IPsec のログが出ているのに、こちらの本装置にはログが出ていません。IPsec は確立しているようなのですが、確認方法はありませんか？

固定 IP - 動的 IP 間での IPsec 接続をおこなう場合、固定 IP 側(受信者側)の本装置ではログが表示されないことがあります。その場合は「各種サービスの設定」→「IPsec サーバ」→「ステータス」を開き、「現在の状態」をクリックして下さい。ここに現在の IPsec の状況が表示されます。

第 13 章

UPnP 機能

第 13 章 UPnP 機能

Ⅰ．UPnP 機能 の設定

本装置は UPnP(Universal Plug and Play)に対応していますので、UPnP に対応したアプリケーションを使うことができます。

対応している Windows OS とアプリケーション

Windows OS

- Windows XP
- Windows Me

アプリケーション

- Windows Messenger
- MSN Messenger

利用できる Messenger の機能について

以下の機能について動作を確認しています。

- インスタントメッセージ
- 音声チャット
- ビデオチャット
- ダイヤルアップ
- ホワイトボード

「ファイルまたは写真の送受信」および「アプリケーションの共有」については現在使用できません。

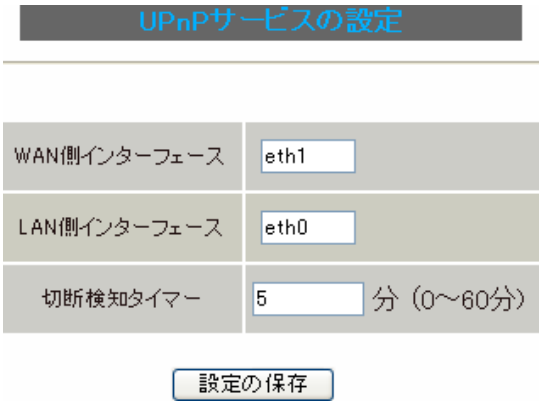
Windows OS の UPnP サービス

Windows XP/Windows Me で UPnP 機能を使う場合は、オプションネットワークコンポーネントとして、ユニバーサルプラグアンドプレイサービスがインストールされている必要があります。
UPnP サービスのインストール方法の詳細については Windows のマニュアル、ヘルプ等をご参照ください。

◆UPnP 機能の設定

本装置の UPnP 機能の設定は以下の手順でおこなってください。

Web 設定画面「各種サービスの設定」→「UPnP サービス」をクリックして設定します。



○WAN 側インターフェース
WAN側に接続しているインタフェース名を指定します。

○LAN 側インターフェース
LAN側に接続しているインタフェース名を指定します。

本装置のインタフェース名については、本マニュアルの「付録 A」をご参照ください。

○切断検知タイマー
UPnP 機能使用時の無通信切断タイマーを設定します。
ここで設定した時間だけ無通信時間が経過すると、本装置が保持する Windows Messenger のセッションが強制終了されます。
切断タイマーを無効にするときは「0」を指定してください。

入力が終わりましたら「設定の保存」をクリックして設定完了です。
機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。

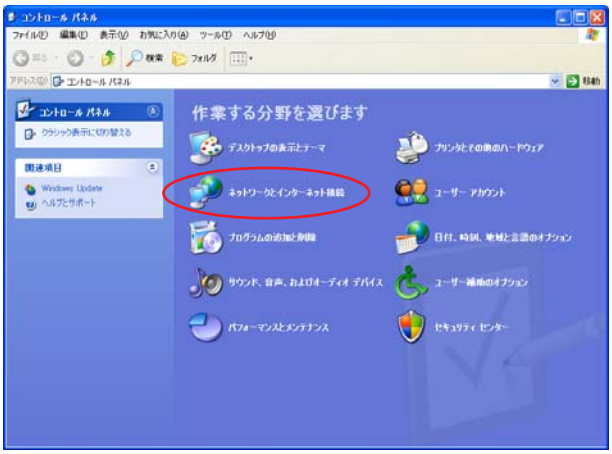
Ⅰ．UPnP 機能 の設定

◆UPnP の接続状態の確認

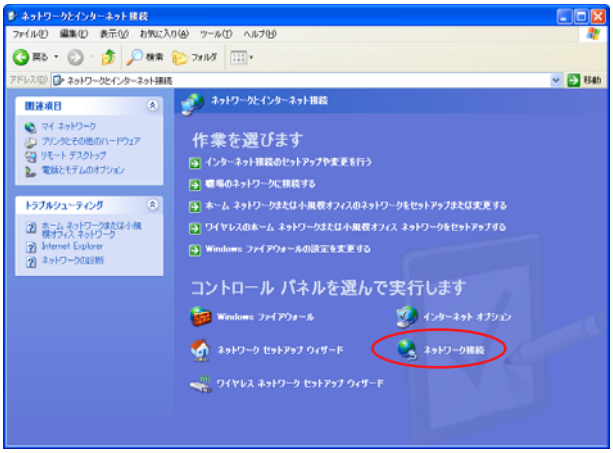
各コンピュータが本装置と正常に UPnP で接続されているかどうかを確認します。

1 「スタート」→「コントロール パネル」を開きます。

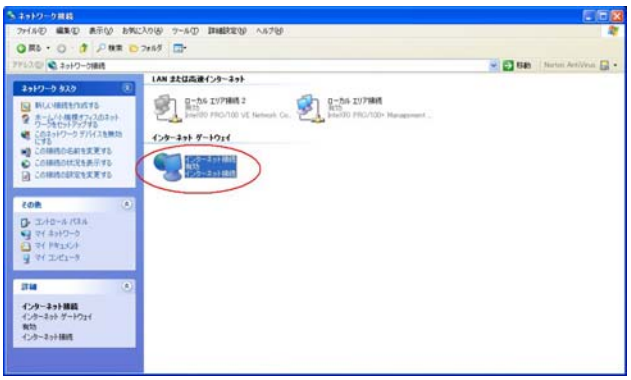
2 「ネットワークとインターネット接続」を開きます。



3 「ネットワーク接続」を開きます。



4 「ネットワーク接続」画面内に、「インターネットゲートウェイ」として**「インターネット接続 有効」**と表示されていれば、正常に UPnP 接続できています。



(画面は Windows XP での表示例です)

Windows OS や Windows Messenger の詳細につきましては、Windows のマニュアル / ヘルプをご参照ください。
弊社では Windows や各アプリケーションの操作法や仕様等についてはお答えできかねますので、ご了承ください。

II．UPnP とパケットフィルタ設定

◆UPnP 機能使用時の注意

UPnP機能を使用するときは原則として、**WAN側インタフェースでの「ステートフルパケットインスペクション機能」を無効にしてください。**

ステートフルパケットインスペクション機能を有効にしている場合は、ご利用になるUPnPアプリケーション側で使用する特定のポートをフィルタ設定で開放してください。

参考：NTT 東日本の VoIP-TA の利用ポートは、UDP・5060、UDP・5090、UDP・5091 です。
(詳細は NTT 東日本にお問い合せください)

各 UPnP アプリケーションが使用するポートにつきましては、アプリケーション提供事業者にお問い合わせください。

◆UPnP 機能使用時の推奨フィルタ設定

Microsoft Windows 上の UPnP サービスのバッファオーバフローを狙った DoS(サービス妨害)攻撃からの危険性を緩和する為の措置として、本装置は工場出荷設定で以下のようなフィルタをあらかじめ設定しています。

(入力フィルタ)

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	ICMP type/code
5	eth1	パケット受信時	破棄	udp					1900	
6	ppp0	パケット受信時	破棄	udp					1900	
7	eth1	パケット受信時	破棄	tcp					5000	
8	ppp0	パケット受信時	破棄	tcp					5000	
9	eth1	パケット受信時	破棄	tcp					2869	
10	ppp0	パケット受信時	破棄	tcp					2869	

(転送フィルタ)

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	ICMP type/code
5	eth1	パケット受信時	破棄	udp					1900	
6	ppp0	パケット受信時	破棄	udp					1900	
7	eth1	パケット受信時	破棄	tcp					5000	
8	ppp0	パケット受信時	破棄	tcp					5000	
9	eth1	パケット受信時	破棄	tcp					2869	
10	ppp0	パケット受信時	破棄	tcp					2869	

UPnP 使用時は特に、上記フィルタ設定を作動させておくことを推奨いたします。

第 14 章

ダイナミックルーティング

第 14 章 ダイナミックルーティング機能

Ⅰ．ダイナミックルーティング機能

本装置のダイナミックルーティング機能は下記のプロトコルをサポートしています。

- RIP
- OSPF
- BGP4

RIP 機能のみで運用することはもちろん、RIP で学習した経路情報を OSPF で配布することなどもできます。

設定の開始

1 Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング」をクリックして以下の画面を開きます。

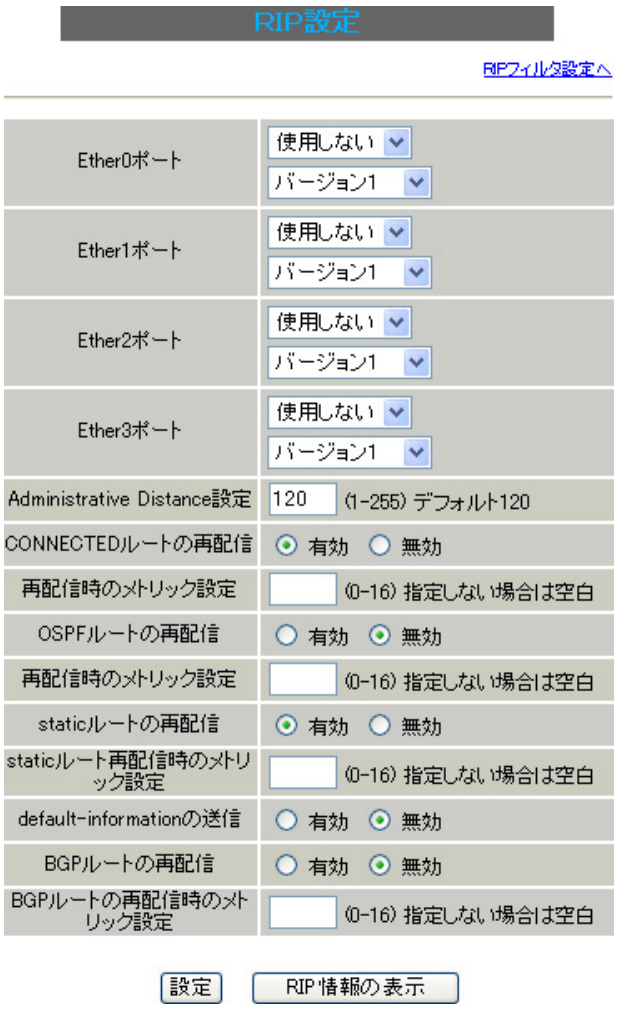
2 「RIP」、「OSPF」、「BGP4」のいずれかをクリックして、それぞれの機能の設定画面で設定をおこないます。

II．RIP の設定

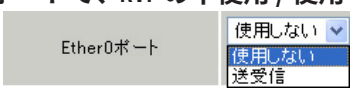
RIP の設定

Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング」→「RIP」をクリックして、以下の画面から設定します。

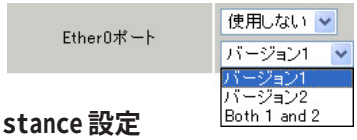
◆RIP 設定



○ Ether0、Ether1、Ether2、Ether3 ポート
本装置の各 Ethernet ポートで、RIP の不使用 / 使用を選択します。



また、使用する場合はRIPバージョンを選択します。



○ Administrative Distance 設定
RIP と OSPF を併用していて全く同じ経路を学習する場合がありますが、その際はこの値の小さい方を経路として採用します。

○ CONNECTED ルートの再配信
connected ルート(インタフェースに関連付けされたルート)を RIP で配信したいときに「有効」にしてください。
RIP のみを使う場合は「無効」にします。

○再配信時のメトリック設定
connected ルートを RIP で配信するときのメトリック値を設定します。

○ OSPF ルートの再配信
RIP と OSPF を併用していて、OSPF で学習したルーティング情報を RIP で配信したいときに「有効」にしてください。
RIP のみを使う場合は「無効」にします。

○再配信時のメトリック設定
OSPF ルートを RIP で配信するときのメトリック値を設定します。

○ static ルートの再配信
static ルーティング情報も RIP で配信したいときに「有効」にしてください。
RIP のみを使う場合は「無効」にします。

○再配信時のメトリック設定
static ルートを RIP で配信するときのメトリック値を設定します。

○ default-information の送信
デフォルトルート情報を RIP で配信したいときに「有効」にしてください。

○ BGP ルートの再配信
RIP と BGP を併用していて、BGP で学習したルーティング情報を RIP で配信したいときに「有効」にしてください。
RIP のみを使う場合は「無効」にします。

○ BGP ルートの再配信時のメトリック設定
BGP ルートを RIP で配信するときのメトリック値を設定します。

II．RIP の設定

選択、入力後は「設定」をクリックして設定完了です。

設定後は「ダイナミックルーティング設定」画面に戻り、「起動」を選択して「動作変更」をクリックしてください。
また、設定を変更した場合には、「再起動」をクリックしてください。

なお、RIP の動作状況およびルーティング情報は、「RIP 情報の表示」をクリックすることで確認できます。

◆RIP フィルタの設定

RIP による route 情報の送信または受信をしたくないときに設定します。

Web 設定画面「各種サービスの設定」→「ダイナミックルーティング」→「RIP」→画面右の「RIP フィルタ設定へ」のリンクをクリックして、以下の画面から設定します。

○NO.
設定番号を指定します。1-64 の間で指定します。

○インタフェース
RIP フィルタを実行するインタフェースをプルダウンから選択します。

○方向
・in-coming
本装置が RIP 情報を受信する際に RIP フィルタリングします(受信しない)。

・out-going
本装置から RIP 情報を送信する際に RIP フィルタリングします(送信しない)。

○ネットワーク
RIP フィルタリングの対象となるネットワークアドレスを指定します。
＜入力形式＞
ネットワークアドレス / サブネットマスク値

入力後は「追加」をクリックしてください。
「取消」をクリックすると、入力内容がクリアされます。

RIP フィルタ設定後は、ただちに設定が有効となります。

設定後は、画面上部に設定内容が一覧表示されます。

(画面は表示例です)

[編集 削除]欄

○削除
クリックすると、設定が削除されます。

○編集
クリックすると、その設定について内容を編集できます。

III．OSPF の設定

OSPF の設定

OSPF はリンクステート型経路制御プロトコルです。

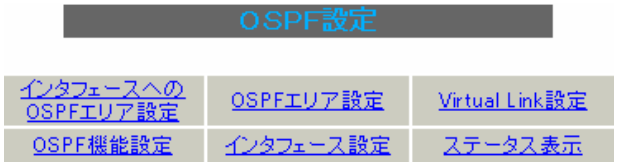
OSPF では各ルータがリンクステートを交換しあい、そのリンクステートをもとに、他のルータがどこに存在するか、どのように接続されているか、というデータベースを生成し、ネットワークトポロジを学習します。

また OSPF は主に帯域幅からコストを求め、コストがもっとも低いものを最適な経路として採用します。
これにより、トラフィックのロードバランシングが可能となっています。

その他、ホップ数に制限がない、リンクステートの更新に IP マルチキャストを利用する、RIP より収束が早いなど、大規模なネットワークでの利用に向いています。

**OSPF の具体的な設定方法に関しましては、弊社サポートデスクでは対応しておりません。
専門のコンサルティング部門にて対応いたしますので、その際は弊社までご連絡ください。**

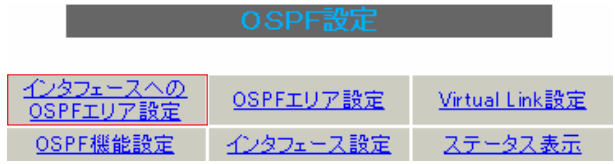
OSPF 設定は、Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング」→「OSPF」をクリックします。
ここで各種設定をおこないます。



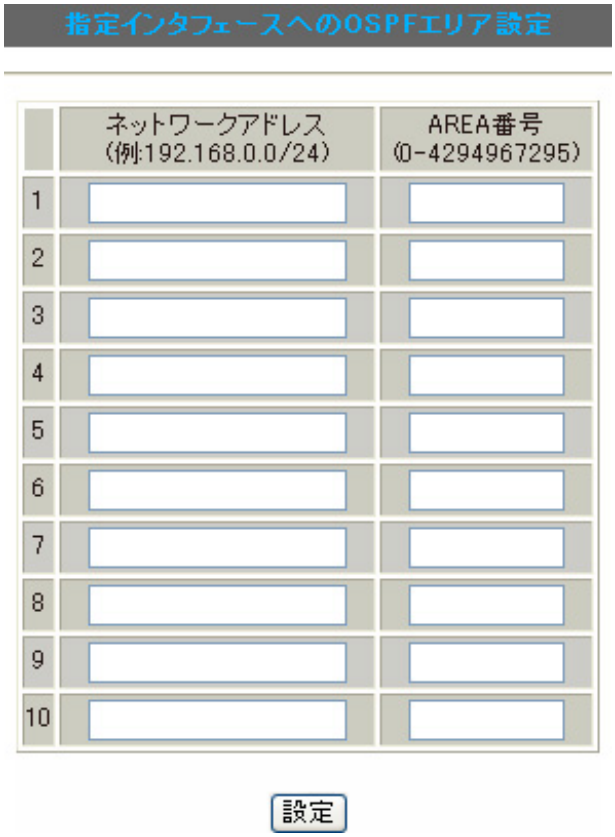
◆インタフェースへの OSPF エリア設定
◆OSPF エリア設定
◆Virtual Link 設定
◆OSPF 機能設定
◆インタフェース設定
◆ステータス表示

◆インタフェースへの OSPF エリア設定

どのインタフェースで OSPF 機能を動作させるかを設定します。256 まで設定可能です。



設定画面上部の「インタフェースへの OSPF エリア設定」をクリックします。



◯ネットワークアドレス
本装置に接続しているネットワークのネットワークアドレスを指定します。
ネットワークアドレス / マスクビット値の形式で入力します。

◯ AREA 番号
そのネットワークのエリア番号を指定します。

※ AREA：リンクステートアップデートを送信する範囲を制限するための論理的な範囲。

入力後は「設定」をクリックして設定完了です。

III．OSPF の設定

◆OSPF エリア設定

各AREA(エリア)ごとの機能設定をおこないます。
設定画面の「OSPF エリア設定」をクリックします。

初めて設定するとき、もしくは設定を追加する場合は「New Entry」をクリックします。

○AREA 番号
機能設定をおこなうエリアの番号を指定します。

○スタブ設定
外部に通じる経路がひとつしかない場合や最適な経路を通る必要がない場合にはスタブエリアに指定します。スタブエリアに指定するときは「有効」を選択します。スタブエリアには LSA type5 を送信しません。

○トータリースタブ設定
LSA type5 に加え、type3、4 も送信しないエリアに指定するときに「有効」にします。

○default-cost 設定
スタブエリアに対してデフォルトルート情報を送信する際のコスト値を指定します。
指定しない場合、設定内容一覧では空欄で表示されますが、実際は 1 で機能します。

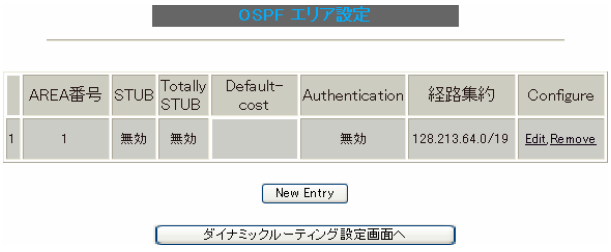
○認証設定
該当エリアでパスワード認証か MD5 認証をおこなうかどうかを選択します。初期設定は「使用しない」です。

○エリア間ルートの経路集約設定
経路情報を集約して送信したいときに設定します。

<設定例>
128.213.64.0～128.213.95.0 のレンジのサブネットを渡すときに 1 つずつ渡すのではなく、128.213.64.0/19 に集約して渡す、といったときに使用します。ただし、連続したサブネットでなければなりません(レンジ内に存在しないサブネットがあってはなりません)。

入力後は「設定」をクリックしてください。

設定後は「OSPF エリア設定」画面に、設定内容が一覧で表示されます。



(画面は表示例です)

[Configure]欄

○Edit
クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○Remove
クリックすると設定の「削除」をおこなえます。

III．OSPF の設定

◆Virtual Link 設定

OSPF において、すべてのエリアはバックボーンエリア(エリア 0)に接続している必要があります。もし接続していなければ、他のエリアの経路情報は伝達されません。

しかし、物理的にバックボーンエリアに接続できない場合には Virtual Link を設定して、論理的にバックボーンエリアに接続させます。

設定画面上部の「Virtual Link 設定」をクリックして設定します。

初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。

○ Transit AREA 番号
Virtual Link を設定する際に、バックボーンと設定するルータのエリアが接続している共通のエリアの番号を指定します。
このエリアが「Transit AREA」となります。

○ Remote-ABR Router-ID 設定
Virtual Link を設定する際のバックボーン側のルータ ID を設定します。

○ Hello インターバル設定
Hello パケットの送出間隔を設定します。

○ Dead インターバル設定
Dead タイムを設定します。

○ Retransmit インターバル設定
LSA を送出する間隔を設定します。

○ transmit delay 設定
LSU を送出する際の遅延間隔(delay)を設定します。

○認証パスワード設定
Virtual Link 上で simple パスワード認証を使用する際のパスワードを設定します。

○ MD5 KEY-ID 設定(1)
MD5 認証使用時の KEY ID を設定します。

○ MD5 パスワード設定(1)
エリア内で MD5 認証を使用する際の MD5 パスワードを設定します。

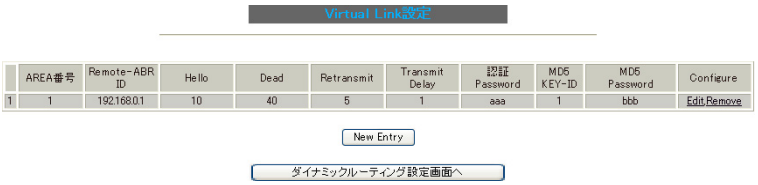
○ MD5 KEY-ID 設定(2)
○ MD5 パスワード設定(2)
MD5 KEY-ID とパスワードは2つ同時に設定可能です。その場合は(2)に設定します。

Virtual Link 設定では、スタブエリアおよびバックボーンエリアを Transit AREA として設定することはできません。

入力後は「設定」をクリックしてください。

III．OSPF の設定

設定後は「Virtual Link 設定」画面に、設定内容が一覧で表示されます。



(画面は表示例です)

[Configure]欄

○ Edit

クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○ Remove

クリックすると設定の「削除」をおこなえます。

◆ OSPF 機能設定

OSPF の動作について設定します。

○ Router-ID 設定

neighbor を確立した際に、ルータの ID として使用されたり、DR、BDR の選定の際にも使用されます。指定しない場合は、ルータが持っている IP アドレスの中でもっとも大きい IP アドレスを Router-ID として採用します。

○ Connected 再配信

connectedルートをOSPFで配信するかどうかを選択します。

「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

III．OSPF の設定

○ static ルートの再配信
static ルートを OSPF で配信するかどうかを選択します。
IPsec ルートを再配信する場合も、この設定を「有効」にする必要があります。
「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ
配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
配信する際のメトリック値を設定します。
入力しない場合はメトリック値 20 となります。

○ RIP ルートの再配信
RIPが学習したルート情報をOSPFで配信するかどうかを選択します。
「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ
配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
配信する際のメトリック値を設定します。
入力しない場合はメトリック値 20 となります。

○ BGP ルートの再配信
BGPが学習したルート情報をOSPFで配信するかどうかを選択します。
「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ
配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
配信する際のメトリック値を設定します。
入力しない場合はメトリック値 20 となります。

○ Administrative Distance 設定
ディスタンス値を設定します。
OSPFと他のダイナミックルーティングを併用していて同じサブネットを学習した際に、この値の小さい方のダイナミックルートを経路として採用します。

○ External ルート Distance 設定
OSPF以外のプロトコルで学習した経路のディスタンス値を設定します。

○ Inter-area ルート Distance 設定
エリア間の経路のディスタンス値を設定します。

○ Intra-area ルート Distance 設定
エリア内の経路のディスタンス値を設定します。

○ Default-information
デフォルトルート(0.0.0.0/0)をOSPFで配信するかどうかを選択します。

・送信しない

・送信する
ルータがデフォルトルートを持っていれば送信されますが、たとえば PPPoE セッションが切断してデフォルトルート情報がなくなってしまったときは配信されなくなります。

・常に送信
デフォルトルートの有無にかかわらず、自分にデフォルトルートを向けるように、OSPF で配信します。

「送信する」「常に送信する」の場合は、以下の 2 項目についても設定します。

a. メトリックタイプ
配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値
配信する際のメトリック値を設定します。
入力しない場合はメトリック値 20 となります。

○ SPF 計算 Delay 設定
LSU を受け取ってから SPF 計算をする際の遅延(delay)時間を設定します。

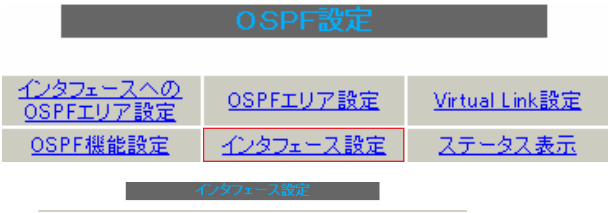
○ 2 つの SPF 計算の最小間隔設定
連続してSPF計算をおこなう際の間隔を設定します。

入力後は「設定」をクリックしてください。

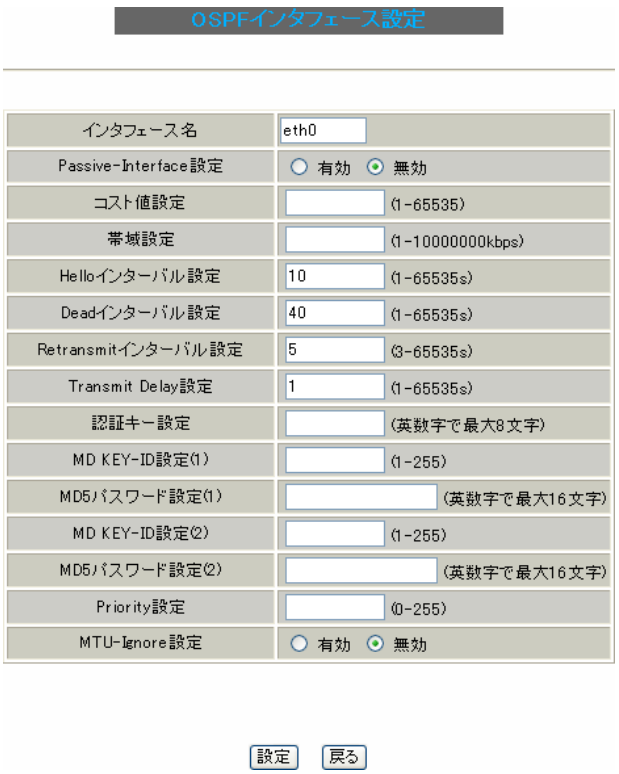
III．OSPF の設定

◆インタフェース設定

各インタフェースごとの OSPF 設定をおこないます。
設定画面上部の「インタフェース設定」をクリックして設定します。



初めて設定するとき、もしくは設定を追加するときは「New Entry」をクリックします。



○インタフェース名
設定するインタフェース名を入力します。
本装置のインタフェース名については、**「付録 A インタフェース名一覧」**をご参照ください。

○ Passive-Interface 設定
インタフェースが該当するサブネット情報を OSPF で配信し、かつ、このサブネットには OSPF 情報を配信したくないという場合に「有効」を選択します。

○コスト値設定
コスト値を設定します。

○帯域設定
帯域設定をおこないます。この値をもとにコスト値を計算します。コスト値＝ 100Mbps/ 帯域 kbps です。
コスト値と両方設定した場合は、コスト値設定が優先されます。

○ Hello インターバル設定
Hello パケットを送出する間隔を設定します。

○ Dead インターバル設定
Dead タイムを設定します。

○ Retransmit インターバル設定
LSA の送出間隔を設定します。

○ Transmit Delay 設定
LSU を送出する際の遅延間隔を設定します。

○認証キー設定
simple パスワード認証を使用する際のパスワードを設定します。
半角英数字で最大 8 文字まで使用できます。

○ MD KEY-ID 設定(1)
MD5 認証使用時の KEY ID を設定します。

○ MD5 パスワード設定(1)
エリア内で MD5 認証を使用する際の MD5 パスワードを設定します。
半角英数字で最大 16 文字まで使用できます。

III．OSPF の設定

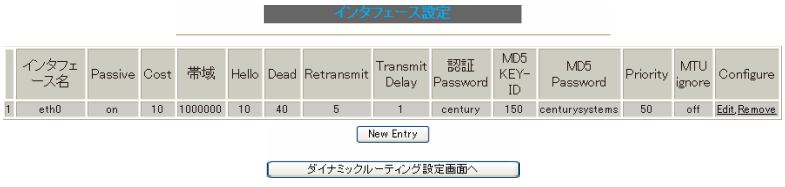
○ MD KEY-ID 設定(2)
○ MD5 パスワード設定(2)
MD5 KEY-IDとパスワードは2つ同時に設定可能です。
その場合は(2)に設定します。

○ Priority 設定
DR、BDR の設定の際に使用する priority を設定します。
priority 値が高いものが DR に、次に高いものが BDR に選ばれます。“ 0 ”を設定した場合は DR、BDR の選定には関係しなくなります。
DR、BDR の選定は、priority が同じであれば、IP アドレスの大きいものが DR、BDR になります。

○ MTU-Ignore 設定
DBD 内の MTU 値が異なる場合、Full の状態になることはできません(Exstart になります)。
どうしてもMTUを合わせることができないときには、このMTU値の不一致を無視してNeighbor(Full)を確立させるためのMTU-Ignoreを「有効」にしてください。

入力後は「設定」をクリックしてください。

設定後は「インタフェース設定」画面に、設定内容が一覧で表示されます。



(画面は表示例です)

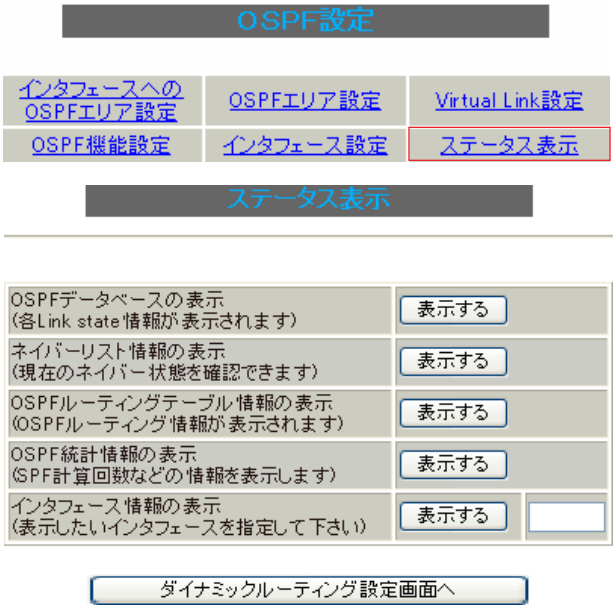
[Configure]欄

○ Edit
クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○ Remove
クリックすると設定の「削除」をおこなえます。

◆ステータス表示

OSPF の各種ステータスを表示します。
設定画面上部の「ステータス表示」をクリックして設定します。



○ OSPF データベースの表示
各 LinkState 情報が表示されます。

○ネイバーリスト情報の表示
現在のネイバー状態が表示されます。

○ OSPF ルーティングテーブル情報の表示
OSPF ルーティング情報が表示されます。

○ OSPF 統計情報の表示
SPF の計算回数や Router ID などが表示されます。

○インタフェース情報の表示
現在のインタフェースの状態が表示されます。表示したいインタフェース名を指定してください。

表示したい情報の項目にある「表示する」をクリックしてください。

Ⅳ．BGP4 の設定

BGP の設定

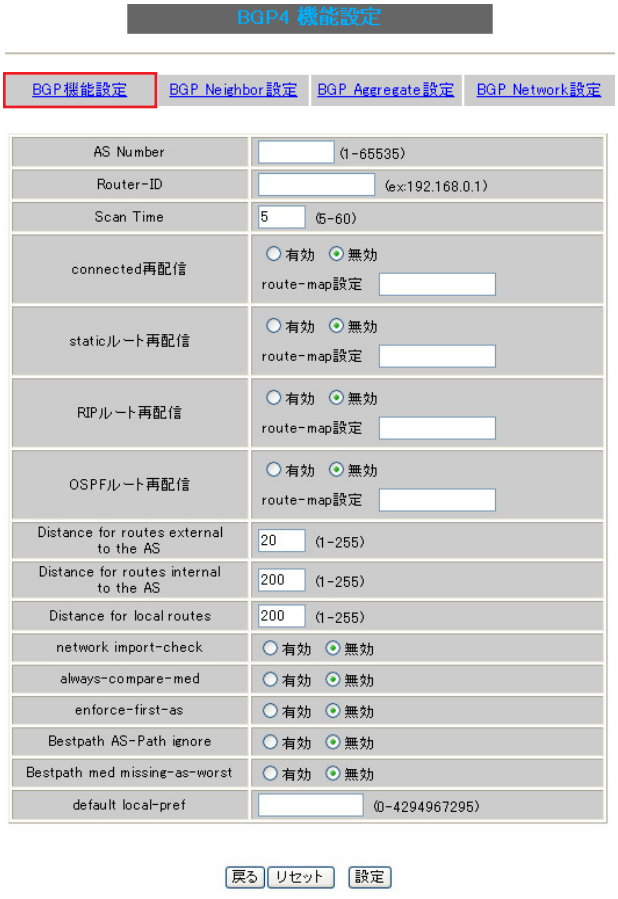
ダイナミックルーティングの「BGP4」をクリックすると、以下の画面が表示されます。
ここで各種設定をおこないます。

◆BGP 機能設定
◆BGP Route-MAP 設定
◆BGP ACL 設定
◆BGP 情報表示

◆BGP4 機能設定

BGP 機能設定

Router-IDやルート情報再配信などの設定をおこないます。
BGP 機能設定をクリックして、以下の画面で設定します。



○AS Number
AS 番号を設定します。
入力可能な範囲：1-65535 です。

○Router-ID
Router-ID を IP アドレス形式で設定します。

○Scan Time
Scan Time を設定します。
指定可能な範囲：5-60 秒です。

IV．BGP4 の設定

○ connected 再配信
Connected ルートを BGP4 で再配信したい場合には「有効」を選択します。
また route-map を適用するときは、「route-map」欄に route-map 名を設定してください。

○ static ルート再配信
Static ルートを BGP4 で再配信したい場合には「有効」を選択します。
また route-map を適用するときは、「route-map」欄に route-map 名を設定してください。

○ RIP ルート再配信
RIP ルートで学習したルートを BGP4 で再配信したい場合には「有効」を選択します。
また route-map を適用するときは、「route-map」欄に route-map 名を設定してください。

○ OSPF ルート再配信
OSPF で学習したルートを BGP4 で再配信したい場合には「有効」を選択します。
また route-map を適用するときは、「route-map」欄に route-map 名を設定してください。

○ Distance for routes external to the AS
eBGP ルートの administrative ディスタンス値を設定します。入力可能な範囲：1-255 です。

○ Distance for routes internal to the AS
iBGP ルートの administrative ディスタンス値を設定します。入力可能な範囲：1-255 です。

○ Distance for local routes
local route(aggregate 設定によって BGP が学習したルート情報)の administrative Distance 値を設定します。入力可能な範囲：1-255 です。

○ network import-check
「有効」を選択すると、「BGP network Setup」で設定したルートを BGP で配信するときに、IGP で学習していないときは BGP で配信しません。
「無効」を選択すると、IGP で学習していない場合でも BGP で配信します。

○ always-compare-med
「有効」を選択すると、異なる AS を生成元とするルートの MED 値の比較をおこないます。
「無効」を選択すると比較しません。

○ enforce-first-as
「有効」を選択すると、UPDATE に含まれる AS Sequence の中の最初の AS がネイバーの AS ではないときに、Notification メッセージを送信してネイバーとのセッションをクローズします。

○ Bestpath AS-Path ignore
「有効」を選択すると、BGP の最適パス決定プロセスにおいて、AS PATH が最短であるルートを優先するというプロセスを省略します。

○ Bestpath med missing-as-worst
「有効」を選択すると、MED 値のない prefix を受信したとき、その prefix に「4294967294」が割り当てられます。
「無効」のときは「0」を割り当てます。

○ default local-pref
local preference 値のデフォルト値を変更します。入力可能な範囲：0-4294967295 です。デフォルト値は「100」です。

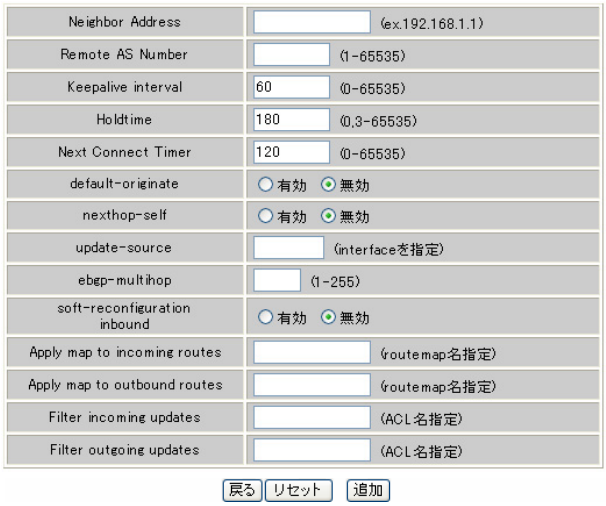
入力後「設定」ボタンをクリックし、設定を保存します。

Ⅳ．BGP4 の設定

BGP4 Neighbor 設定

Neighbor Address の設定をおこないます。
BGP 機能設定の「BGP Neighbor 設定」をクリックすると、BGP4 Neighbor 設定が一覧表示されます。

新規に設定をおこなう場合は、「追加」ボタンをクリックします。



○ Neighbor Address
BGP Neighbor の IP アドレスを設定します。

○ Remote AS Number
対向装置の AS 番号を設定します。
入力可能な範囲：1-65535 です。

○ Keepalive Interval
Keepalive の送信間隔を設定します。
入力可能な範囲：0-65535 秒です。

○ Holdtime
Holdtime を設定します。
入力可能な範囲：0,3-65535 秒です。

○ Next Connect Timer
Next Connect Timer を設定します。
入力可能な範囲：0-65535 秒です。

○ default-originate
デフォルトルートを配信する場合は、「有効」を選択します。

○ nexthop-self
「有効」を選択すると、iBGP peer に送信する Nexthop 情報を、peer のルータとの通信に使用するインタフェースの IP アドレスに変更します。

○ update-source
BGP パケットのソースアドレスを、指定したインタフェースの IP アドレスに変更します。
インタフェース名を指定してください。

本装置のインタフェース名については、本マニュアルの**「付録 A インタフェース名一覧」**をご参照ください。

○ ebgp-multihop
入力欄に数値を指定すると、eBGP の Neighbor ルータが直接接続されていない場合に、到達可能なホップ数を設定します。入力可能な範囲：1-255 です。

○ soft-reconfiguration inbound
「有効」を選択すると BGP Session をクリアせずに、ポリシーの変更をおこないます。

○ Apply map to incoming routes
○ Apply map to outbound routes
incoming route/outbound route に適用する routemap 名を指定します。

○Filter incoming updates
○Filter outgoing updates
incoming updates/outgoing updates をフィルタリングしたいときに、該当する ACL 名を指定します。

入力後「追加」ボタンをクリックし、設定を保存します。
設定内容の変更をおこなう場合は、BGP4 Neighbor設定一覧表示画面で「Edit」をクリックしてください。

設定を削除する場合は、一覧表示画面「Remove」下の空欄にチェックを入れて「削除」ボタンをクリックしてください。

BGP4 Aggregate 設定

Aggregate Address の設定をおこないます。
BGP 機能設定の「BGP Aggregate 設定」をクリックすると、BGP4 Aggregate 設定が一覧表示されます。

新規に設定をおこなう場合は、「追加」ボタンをクリックします。

○Aggregate Address
集約したいルートを設定します。

○summary only
集約ルートのみを配信したい場合は、「有効」を選択してください。

入力後「追加」ボタンをクリックし、設定を保存します。

設定内容の変更をおこなう場合は、BGP4 Aggregate 設定一覧表示画面で「Edit」をクリックしてください。

設定を削除する場合は、一覧表示画面「Remove」下の空欄にチェックを入れて「削除」ボタンをクリックしてください。

BGP4 Network 設定

Network Address の設定をおこないます。
BGP 機能設定の「BGP Network 設定」をクリックすると、BGP4 Network 設定が一覧表示されます。

新規に設定をおこなう場合は、「追加」ボタンをクリックします。

○Specify a network to announce via BGP
BGPにより配信したいネットワークを設定します。

○backdoor
backdoor 機能を使用したい場合は、「有効」を選択してください。

入力後「追加」ボタンをクリックします。

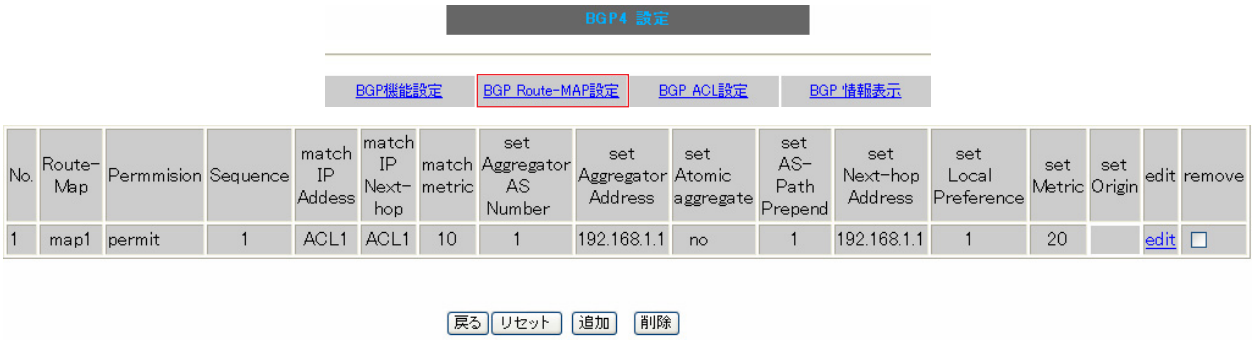
設定内容の変更をおこなう場合は、BGP4 Network 設定一覧表示画面で「Edit」をクリックしてください。

設定を削除する場合は、一覧表示画面「Remove」下の空欄にチェックを入れて「削除」ボタンをクリックしてください。

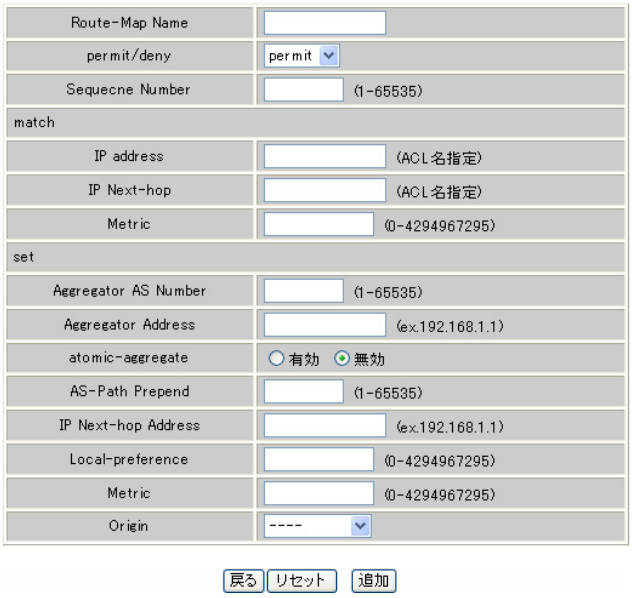
Ⅳ．BGP4 の設定

◆BGP4 Route-MAP 設定

Route-MAP の設定をおこないます。
BGP4 設定画面の「BGP Route－MAP 設定」をクリックすると、以下の Route-Map 設定が一覧表示されます。



新規に設定をおこなう場合は「追加」ボタンをクリックします。



○ Route-Map name
Route-MAP の名前を設定します。
使用可能な文字は半角、英数、“ _ ”(アンダースコア)です。1-32 文字で設定可能です。

○ permit/deny
Route-MAP で“ match ”条件に合致したルートの制御方法を設定します。「permit」を選択すると、ルートは“ set ”で指定されている通りに制御されます。
「deny」を選択すると、ルートは制御されません。

○ Sequence Number
すでに設定されている Route-MAP のリストの中で、新しい Route-MAP リストの位置を示す番号です。小さい番号のリストが上位に置かれます。入力可能な範囲：1-65535 です。

○ match
・IP address
アクセスリストで指定した IP アドレスを match 条件とします。match 条件となる ACL 名を設定します。

・IP Next-hop
next-hop の IP アドレスがアクセスリストで指定した IP アドレスと同じものを match 条件とします。match 条件となる ACL 名を設定します。

・Metric
ここで指定した metric 値を match 条件とします。入力可能な範囲：0-4294967295 です。

○ set
match 条件と一致したときの属性値を設定します。
以下のものが設定できます。

・Aggregator AS Number
アグリゲータ属性を付加します。
アグリゲータ属性は、集約経路を生成した AS や BGP ルータを示します。
入力欄に AS 番号を設定します。入力可能な範囲：1-65535 です。

・Aggregator Address
アグリゲータ属性を付加します。
アグリゲータ属性は、集約経路を生成した AS や BGP ルータを示します。
入力欄に IP アドレスを設定します。

・atomic-aggregate
「有効」を選択すると、atomic-aggrigate 属性を付加します。
atomi-aggrigate は、経路集約の際に細かい経路に付加されていた情報が欠落したことを示すものです。

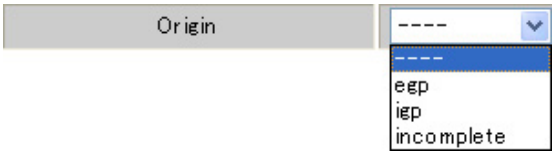
・As-Path Prepend
AS 番号を付加します。
入力欄に AS 番号を設定してください。入力可能な範囲：1-65535 です。

・IP Next-hop Address
ネクストホップの IP アドレスを付加します。
入力欄に IP アドレスを設定します。

・Local-preference
Local Preference 属性を付加します。
これは、同一 AS 内部で複数経路の優先度を表すために用いられる値で、大きいほど優先されます。入力可能な範囲：0-4294967295 です。

・Metric
metric 属性を付加します。
入力可能な範囲：0-4294967295 です。

・Origin
origin 属性を付加します。
origin 属性は、経路の生成元を示す属性です。
付加する場合は以下の３つから選択します。



igp：経路情報を AS 内から学習したことを示します。

egp：経路情報を EGP から学習したことを示します。

incomplete：経路情報を上記以外から学習したことを示します。

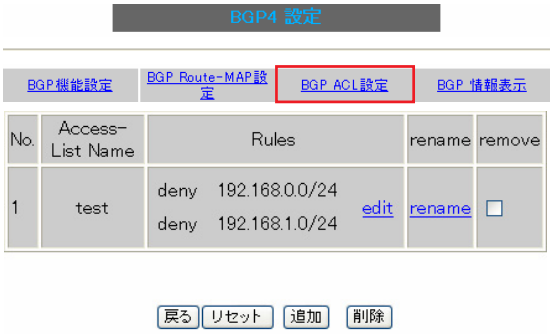
入力後「追加」ボタンをクリックし、設定を保存します。
設定内容の変更をおこなう場合は、Route-Map 一覧表示画面の「Edit」をクリックしてください。

設定を削除する場合は、「Remove」下の空欄にチェックを入れて「削除」ボタンをクリックしてください。

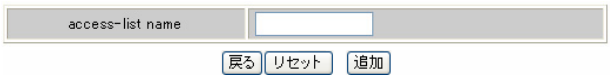
Ⅳ．BGP4 の設定

◆BGP4 ACL 設定

BGP4 の ACL(ACCESS-LIST)設定をおこないます。
BGP4 設定画面の「BGP ACL 設定」をクリックすると、BGP4 ACL 設定が一覧表示されます。



新規に設定をおこなう場合は「追加」ボタンをクリックします。



access-list name 欄に任意の ACL 名を設定します。
使用可能な文字は半角、英数、“ _ ”(アンダースコア）です。数字だけでの設定は出来ません。
入力可能な範囲：1-32 文字です。

入力後「追加」ボタンをクリックしてください。

一覧表示画面の Rules の「Edit」をクリックすると、選択した ACL に設定されているルールが一覧表示されます。

ルールを追加する場合は、「追加」ボタンをクリックします。

○ permit/deny
パケットの permit(許可)/deny(拒否)を選択します。

○ prefix to match
マッチング対象とするネットワークアドレスを設定します。「IP アドレス / マスクビット値」の形式で入力してください。

入力後「追加」ボタンをクリックし、設定を保存します。

設定済みのルールを削除する場合は、ルールの一覧表示画面で「remove」下の空欄にチェックを入れ、「削除」ボタンをクリックしてください。

ACL を削除する場合は、BGP4 ACL 設定の一覧表示画面で「Remove」下の空欄にチェックを入れ、「削除」ボタンをクリックしてください。

IV．BGP4 の設定

◆BGP 情報表示

BGP4 の各種情報表示をおこないます。
BGP4 設定画面の「BGP 情報表示」をクリックすると、以下の画面が表示されます。

◯ BGP Table
BGP のルーティングテーブル情報を表示します。
入力欄でネットワークを指定すると、指定されたネットワークだけが表示されます。

◯ Detailed information BGP Neighbor
BGP Neighbor の詳細情報を表示します。

・advertised-routes
選択すると、BGP Neighbor ルータへ配信しているルート情報を表示します。

・received-routes
選択すると、BGP Neighbor ルータから受け取ったルート情報を表示します。

・route
選択すると、BGP Neighbor から学習したロート情報を表示します。

Neighbor Address を指定すると、指定された Neighbor に関係した情報のみ表示されます。

◯ Summary of BGP neighbor status
BGP Neighbor のステータスを表示します。

◯ Clear BGP peers
設定の変更をおこなった場合などに BGP peer 情報をクリアします。特定の peer をクリアするときは、Neighbor アドレスか AS 番号を指定してください。

また BGP soft reconfig により BGP セッションを終了することなく、変更した設定を有効にすることができます。Soft reconfig をおこなう場合は、「Soft in」(inbound)または「Soft out」(outbound)をチェックしてください。

第 15 章

L2TPv3 機能

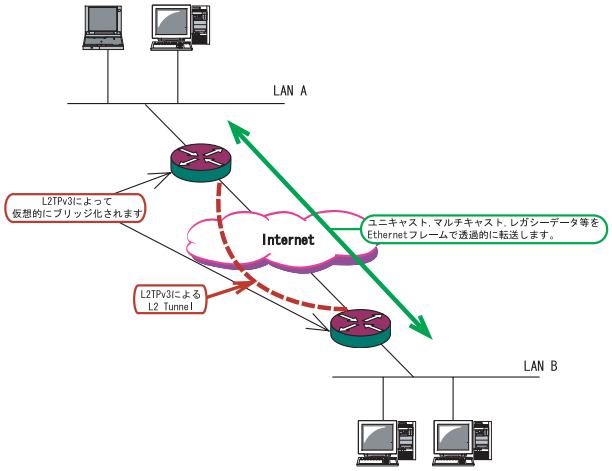
第 15 章 L2TPv3 機能

Ⅰ．L2TPv3 機能概要

L2TPv3 機能は、IP ネットワーク上のルータ間で L2TPv3 トンネルを構築します。
これにより本製品が仮想的なブリッジとなり、遠隔のネットワーク間でレイヤ2通信が可能となります。

レイヤ2レベルでトンネリングするため、2つのネットワークは HUB で繋がった１つの Ethernet ネットワークのように使うことができます。
また、上位プロトコルに依存せずにネットワーク通信ができ、TCP/IP だけでなく、任意の上位プロトコル(IPX、AppleTalk、SNA 等)を透過的に転送することができます。

さらに、L2TPv3 機能は、従来の専用線やフレームリレー網ではなく IP網で利用できますので、低コストな運用が可能です。



- **End to End で Ethernet フレームを転送したい**
- **FNA や SNA などのレガシーデータを転送したい**
- **ブロードキャスト / マルチキャストパケットを転送したい**
- **IPX や AppleTalk 等のデータを転送したい**

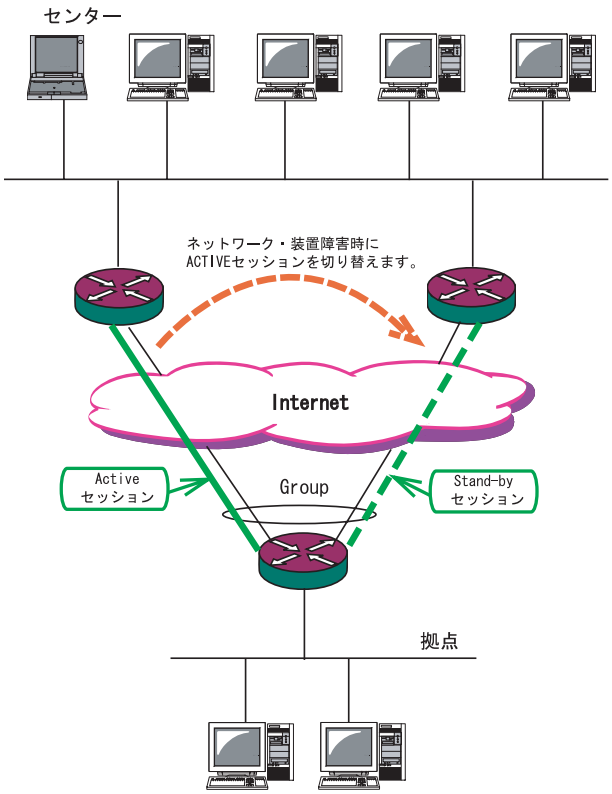
このような、従来の IP-VPN やインターネット VPN では通信させることができなかったものも、L2TPv3 を使うことで通信ができるようになります。

また Point to Multi-Point に対応しており、１つの Xconnect Interface に対して複数の L2TP session を関連づけすることが可能です。

◆ L2TPv3 セッションの二重化機能

本装置では、L2TPv3 Group 機能(L2TPv3 セッションの二重化機能)を具備しています。
ネットワーク障害や対向機器の障害時に二重化された L2TPv3 セッションの Active セッションを切り替えることによって、レイヤ 2 通信の冗長性を高めることができます。

<L2TPv3 セッション二重化の例>
センター側を 2 台の冗長構成にし、拠点側の XR で、センター側への L2TPv3 セッションを二重化します。

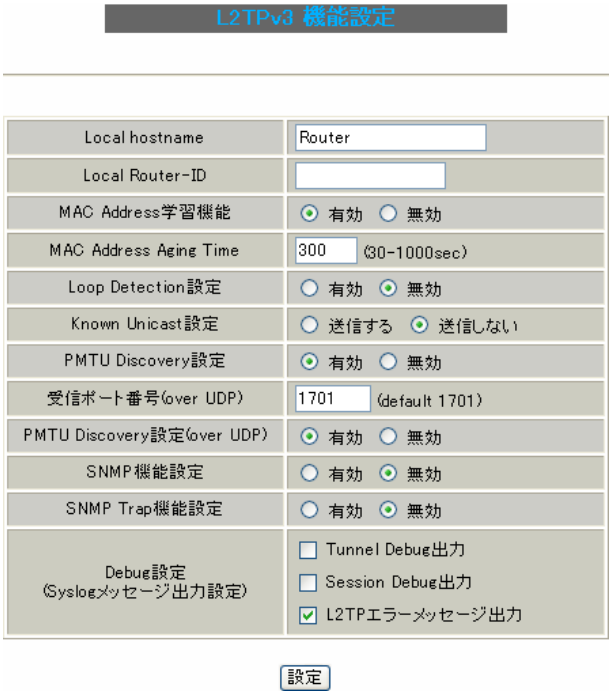


II．L2TPv3 機能設定

本装置の IDやホスト名、MACアドレスに関する設定をおこないます。

設定方法

「各種サービスの設定」→「L2TPv3」の
「L2TPv3 機能設定」をクリックします。



○ Localhostname
本装置のホスト名を設定します。
使用可能な文字は半角英数字です。
対向LCCE(※)の“ リモートホスト名 ”設定と同じ文字列を指定してください。
設定は必須ですが、後述の「L2TPv3 Tunnel設定」で設定した場合はそちらが優先されます。

※ LCCE(L2TP Control Connection Endpoint)
L2TP コネクションの末端にある装置を指す言葉。

○ Local Router-ID
本装置のルータ ID を、IP アドレス形式で設定します。
<例> 192.168.0.1 など
LCCE のルータ ID の識別に使用します。
対向LCCEの“ リモートルータ ID ”設定と同じ文字列を指定してください。
設定は必須ですが、後述の「L2TPv3 Tunnel設定」で設定した場合はそちらが優先されます。

○ MAC Address 学習機能(※)
MACアドレス学習機能を有効にするかを選択します。

※ MAC Address 学習機能
本装置が受信したフレームのMACアドレスを学習し、不要なトラフィックの転送を抑制する機能です。
ブロードキャスト、マルチキャストについては MAC アドレスに関係なく、すべて転送されます。

Xconnect インタフェースで受信した MAC アドレスはローカル側 MAC テーブル(以下、Local MAC テーブル)に、L2TP セッション側で受信した MAC アドレスはセッション側 MAC テーブル(以下、FDB)にてそれぞれ保存されます。

さらに、本装置は Xconnect インタフェース毎に Local MAC テーブル /FDB を持ち、それぞれの Local MAC テーブル /FDB につき、最大 65535 個の MAC アドレスを学習することができます。
学習した MAC テーブルは手動でクリアすることができます。

○ MAC Address Aging Time
本装置が学習した MAC アドレスの保持時間を設定します。
指定可能な範囲は、30-1000 秒です。

II．L2TPv3 機能設定

○ Loop Detection 設定(※)
LoopDetect 機能を有効にするかを選択します。

※ Loop Detection 機能
フレームの転送がループしてしまうことを防ぐ機能です。
この機能が「有効」になっているときは、以下の２つの場合にフレームの転送をおこないません。
・Xconnect インタフェースより受信したフレームの送信元 MAC アドレスが FDB に存在するとき
・L2TP セッションより受信したフレームの送信元 MAC アドレスが Local MAC テーブルに存在するとき

○ Known Unicast 設定(※)
Known Unicast 送信機能を有効にするかを選択します。

※ Known Unicast 送信機能
Known Unicast とは、既に MAC アドレス学習済みの Unicast フレームのことを言います。
この機能を「無効」にしたときは、以下の場合に Unicast フレームの転送をおこないません。
・Xconnect インタフェースより受信した Unicast フレームの送信先 MAC アドレスが Local MAC テーブルに存在するとき

○ Path MTU Discovery
L2TPv3 over IP 使用時に Path MTU Discovery 機能を有効にするかを選択します。
本機能を「有効」にした場合は、送信する L2TPv3 パケットの DF(Don't Fragment)ビットを 1 にします。「無効」にした場合は、DF ビットを常に 0 にして送信します。ただし、カプセリングしたフレーム長が送信インタフェースの MTU 値を超過する場合は、ここの設定に関係なく、フラグメントされ、DF ビットを 0 にして送信します。

○受信ポート番号（over UDP）
L2TPv3 over UDP 使用時の L2TP パケットの受信ポートを指定します。

○ PMTU Discovery 設定（over UDP）
L2TPv3 over UDP 使用時に Path MTU Discovery 機能を有効にするかを選択します。

○ SNMP 機能設定
L2TPv3 用の SNMP エージェント機能を有効にするかを選択します。
L2TPv3 に関する MIB の取得が可能になります。

○ SNMP Trap 機能設定
L2TPv3 用の SNMP Trap 機能を有効にするかを選択します。
L2TPv3 に関する Trap 通知が可能になります。

これらの SNMP 機能を使用する場合は、SNMP サービスを起動させてください。
また、MIB や Trap に関する詳細は、「第 17 章 SNMP エージェント機能」を参照してください。

○ Debug 設定
syslog に出力するデバッグ情報の種類を選択します。
トンネルのデバッグ情報、セッションのデバッグ情報、L2TP エラーメッセージの 3 種類を選択できます。

入力、選択後「設定」ボタンをクリックしてください。

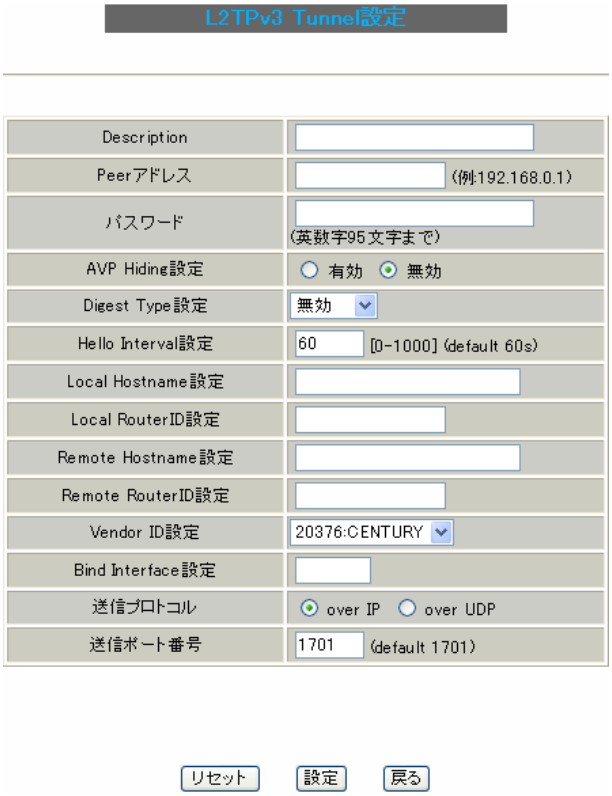
III. L2TPv3 Tunnel 設定

L2TPv3のトンネル(制御コネクション)のための設定をおこないます。

設定方法

「各種サービスの設定」→「L2TPv3」の
「L2TPv3 Tunnel 設定」をクリックします。

新規に設定をおこなうときは「New Entry」をクリックして、以下の画面で設定します。



○Description
このトンネル設定についてのコメントや説明を付記します。
この設定はL2TPv3の動作には影響しません。

○Peer アドレス
対向LCCEの IP アドレスを設定します。
ただし、対向LCCEが動的 IP アドレスの場合には空欄にしてください。

○パスワード
CHAP認証やメッセージダイジェスト、AVP Hidingで利用する共有鍵を設定します。
パスワードは、制御コネクションの確立時における対向 LCCE の識別、認証に使われます。
パスワードは設定しなくてもかまいません。

○ AVP Hiding 設定(※)
AVP Hiding を有効にするかを選択します。

※ AVP Hiding
L2TPv3 では、AVP(Attribute Value Pair)と呼ばれる、属性と値のペアでトンネルの確立や解放、維持などの制御メッセージをやりとりします。
AVPは通常、平文で送受信されますが、AVP Hiding機能を使うことでAVPの中のデータを暗号化します。

○ Digest Type 設定
メッセージダイジェストを使用する場合に設定します。

○ Hello Interval 設定
Helloパケットの送信間隔を設定します。
指定可能な範囲は0-1100秒です。
「0」を設定するとHelloパケットを送信しません。

Helloパケットは、L2TPv3の制御コネクションの状態を確認するために送信されます。
L2TPv3二重化機能で、ネットワークや機器障害を自動的に検出したい場合は必ず設定してください。

○ Local Hostname 設定
本装置のホスト名を設定します。LCCEの識別に使用します。設定しない場合は「L2TPv3機能設定」での設定が有効になります。

○ Local Router ID 設定
対向LCCEのルータIDを設定します。LCCEのルータIDの識別に使用します。設定しない場合は「L2TPv3機能設定」での設定が有効になります。

III. L2TPv3 Tunnel 設定

○ Remote Hostname 設定
対向 LCCE のホスト名を設定します。
LCCE の識別に使用します。設定は必須となります。

○ Remote Router ID 設定
対向 LCCE のルータ ID を設定します。
LCCE のルータ ID の識別に使用します。設定は必須となります。

○ Vender ID 設定
対向 LCCE のベンダー ID を設定します。
「0」は RFC3931 対応機器、「9」は Cisco Router、「20376」は XR シリーズとなります。

○ Bind Interface 設定
バインドさせる本装置のインタフェースを設定します。指定可能なインタフェースは「PPP インタフェース」のみです。

この設定により、PPP/PPPoE の接続 / 切断に伴って、L2TP トンネルとセッションの自動確立 / 解放がおこなわれます。

○送信プロトコル
L2TP パケット送信時のプロトコルを「over IP」「over UDP」から選択します。
接続する対向装置と同じプロトコルを指定する必要があります。

○送信ポート番号
L2TPv3 over UDP 使用時（上記「送信プロトコル」で「over UDP」を選択した場合）に、対向装置のポート番号を指定します。

入力、選択後「設定」ボタンをクリックしてください。

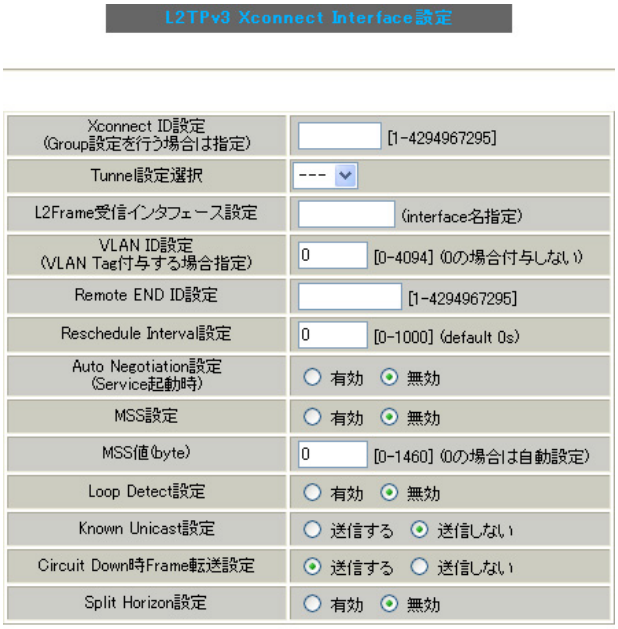
Ⅳ．L2TPv3　Xconnect(クロスコネクト)設定

主に L2TP セッションを確立するときに使用する、パラメータの設定をおこないます。

設定方法

「各種サービスの設定」→「L2TPv3」の「L2TPv3 Xconnect 設定」をクリックします。

新規に設定をおこなうときは「New Entry」をクリックして、以下の画面で設定します。



○ Xconnect ID 設定(Group 設定を行う場合は指定)
「L2TPv3 Group 設定」で使用する ID を任意で設定します。

○ Tunnel 設定選択
「L2TPv3 Tunnel 設定」で設定したトンネル設定を選択して、トンネルの設定とセッションの設定を関連づけます。

プルダウンメニューには、「L2TPv3 Tunnel 設定」の「Remote Router ID」で設定された値が表示されます。

○ L2Frame 受信インタフェース設定
レイヤー 2 フレーム(Ethernet フレーム)を受信するインタフェース名を設定します。
設定可能なインタフェースは、本装置の Ethernet ポートと VLAN インタフェースのみです。

Point to Multi-point 接続をおこなう場合は、１つのインタフェースに対し、複数の L2TPv3 セッションの関連付けが可能です。
ただし、本装置の Ethernet インタフェースと VLAN インタフェースを同時に設定することはできません。

<2 つ(以上)の Xconnect 設定をおこなうときの例>
「eth0.10」と「eth0.20」・・・設定可能
「eth0.10」と「eth0.10」・・・設定可能(※)
「eth0」と「eth0.10」・・・・ 設定不可

※ Point to Multi-point 接続、もしくは L2TPv3 二重化の場合のみ設定可能。

○ VLAN ID 設定(VLAN Tag 付与する場合指定)
本装置で VLAN タギング機能を使用する場合に設定します。
本装置の配下に VLAN に対応していない L2 スイッチが存在するときに使用できます。
0-4094 まで設定でき、「0」のときは VLAN タグを付与しません。

○ Remote END ID 設定
対向 LCCE の END ID を設定します。
END ID は、1-4294967295 の任意の整数値です。
対向 LCCE の END ID 設定と同じものにします。
ただし、L2TPv3 セッション毎に異なる値を設定してください。

○ Reschedule Interval 設定
L2TP トンネル / セッションが切断したときに reschedule(自動再接続)することができます。
自動再接続するときはここで、自動再接続を開始するまでの間隔を、0-1000(秒)で設定します。
「0」を設定したときは自動再接続はおこなわれません。
このときは手動による接続か対向 LCCE からのネゴシエーションによって再接続します。
L2TPv3 二重化機能で、ネットワークや機器の復旧時に自動的にセッション再接続させたい場合は必ず設定してください。

Ⅳ．L2TPv3　Xconnect(クロスコネクト)設定

○ Auto Negotiation 設定(Service 起動時)
この設定が有効になっているときは、L2TPv3 機能が起動後に自動的に L2TPv3 トンネルの接続が開始されます。
この設定は Ethernet 接続時に有効です。
PPP/PPPoE 環境での自動接続は、「L2TPv3 Tunnel 設定」の「Bind Interface 設定」で ppp インタフェースを設定してください。

○ MSS 設定
MSS値の調整機能を有効にするかどうかを選択します。

○ MSS 値（byte）
MSS 設定を「有効」に選択した場合、MSS 値を指定することができます。
指定可能範囲：0-1460 です。
“0”を指定すると、自動的に計算された値を設定します。

特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします（それ以外では正常にアクセスできなくなる場合があります)。

○ Loop Detection 設定
この Xconnect において、Loop Detection 機能を有効にするかを選択します。

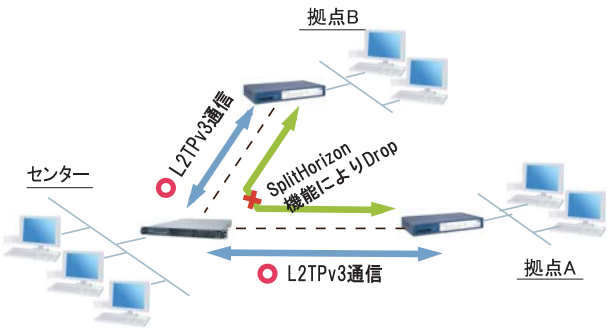
○ Known Unicast 設定
この Xconnect において、Known Unicast 送信機能を有効にするかを選択します。

注）LoopDetect 設定、Known Unicast 設定は、「L2TPv3 機能設定」でそれぞれ有効にしていない場合、ここでの設定は無効となります。

○ Circuit Down 時 Frame 転送設定
Circuit Status が Down 状態の時に、対向 LCCE に対して Non-Unicast Frame を送信するかを選択します。

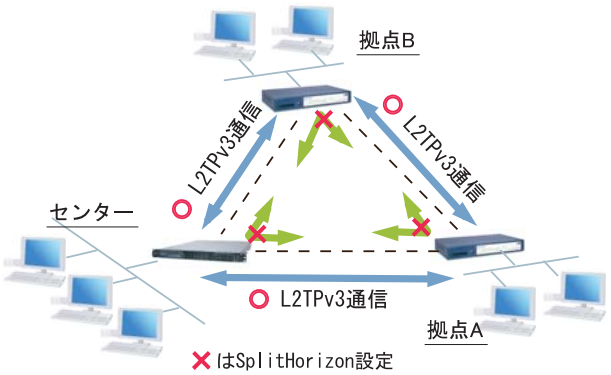
○ Split Horizon 設定
Point-to-Multi-Point 機能によって、センターと２拠点間を接続しているような構成において、センターと拠点間のL2TPv3通信はおこなうが、拠点同士間の通信は必要ない場合に、センター側でこの機能を「有効」にします。
センター側では、Split Horizon 機能が「有効」の場合、一方の拠点から受信したフレームをもう一方のセッションへは転送せず、Local Interfaceに対してのみ転送します。

※ Split Horizon の使用例 1



また、この機能は、拠点間でフルメッシュの構成をとる様な場合に、フレームの Loop の発生を防ぐための設定としても有効です。
この場合、全ての拠点において Split Horizon 機能を「有効」に設定します。
LoopDetect 機能を有効にする必要はありません。

※ Split Horizon の使用例 2



入力、選択後「設定」ボタンをクリックしてください。

V．L2TPv3　Group 設定

L2TPv3 セッション二重化機能を使用する場合に、二重化グループのための設定をおこないます。

二重化機能を使用しない場合は、設定する必要はありません。

設定方法

「各種サービスの設定」→「L2TPv3」の「L2TPv3 Group 設定」をクリックします。

新規のグループ設定をおこなうときは、「New Entry」をクリックします。

○ Group ID 設定

Group を識別する番号を設定します。
指定可能な範囲は 1-4095 です。
他の Group と重複しない値を設定してください。

○ Primary Xconnect 設定選択

○ Secondary Xconnect 設定選択

Primary/Secondary として使用したい Xconnect をプルダウンから選択します。
プルダウンには「L2TPv3 Xconnect 設定」の「Xconnect ID 設定」で設定した値が表示されます。
既に他の Group で使用されている Xconnect を指定することはできません。

○ Preenmpt 設定

Group の Preempt モード(※)を有効にするかどうかを設定します。

※ Preempt モード

Secondary セッションが Active となっている状態で、Primary セッションが確立したときに、通常 Secondary セッションが Active な状態を維持し続けますが、Preempt モードが「有効」の場合は、Primary セッションが Active になり、Secondary セッションは Stand-by となります。

○Primary active 時の Secondary Session 強制切断設定

この設定が「有効」となっている場合、Primary セッションが Active に移行した際に、Secondary セッションを強制的に切断します。
本機能を「有効」にする場合、「Preempt 設定」も「有効」に設定してください。

Secondary セッションを ISDN などの従量回線で接続する場合には「有効」にすることを推奨します。

○ Active Hold 設定

Group の Active Hold 機能(※)を有効にするかどうかを設定します。

※ Active Hold 機能

対向の LCCE から Link Down を受信した際に、Secondary セッションへの切り替えをおこなわず、Primary セッションを Active のまま維持する機能のことを言います。

1vs1 の二重化構成の場合、対向 LCCE で Link Down が発生した際に、Primary から Secondary へ Active セッションを切り替えたとしても、通信できない状態は変わりません。よってこの構成においては、不要なセッションの切り替えを抑止するために本機能を有効に設定することを推奨します。

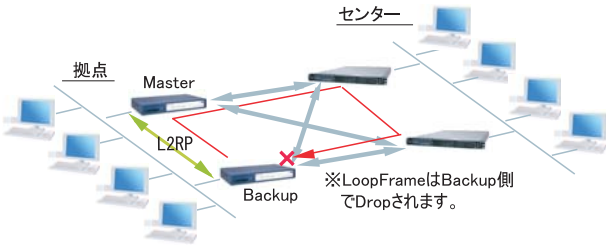
入力、選択後「設定」ボタンをクリックしてください。

VI．Layer2 Redundancy 設定

Layer2 Redundancy Protocol 機能（以下、L2TP 機能)とは、装置の冗長化をおこない、Frameの Loop を抑止するための機能です。
L2RP 機能では、2 台の LCCE で Master/Backup 構成を取り、Backup側は受信Frameを全てDropさせることによって、Loop の発生を防ぐことができます。
また、機器や回線の障害発生時には、Master/Backup を切り替えることによって拠点間の接続を維持することができます。

下図のようなネットワーク構成では、フレームの Loopが発生し得るため、本機能を有効にしてください。

※ L2RP 機能の使用例



設定方法

「各種サービスの設定」→「L2TPv3」の
「L2TPv3 Layer2 Redundancy 設定」をクリックします。

「New Entry」をクリックすると次の設定画面が開きます。

◯ L2RP ID
L2RP の ID です。
対になる LCCE の L2RP と同じ値を設定します。
1～255 の間で設定します。

◯ Type 設定
Master/Backup を決定する判定方法を選択します。
「Priority」は Priority 値の高い方が Master となります。
「Active Session」は Active Session 数の多い方が Master となります。

◯ Priority 設定
Masterの選定に使用するPriority値を設定します。
1～255 の間で設定します。

◯ Advertisement Interval 設定
Advertise Frame(※)を送信する間隔を設定します。
1～60(秒)の間で設定します。

※ Advertise Frame
Master側が定期的に送出する情報フレームです。
Backup 側ではこれを監視し、一定時間受信しない場合に Master 側の障害と判断し、自身が Master へ遷移します。

Ⅵ．Layer2 Redundancy 設定

○ Preempt 設定
Priority 値が低いものが Master で高いものが Backup となることを許可するかどうかの設定です。

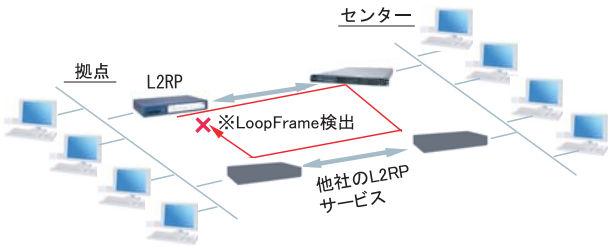
○ Xconnect インタフェース設定
Xconnect インタフェース名を指定してください。
Advertise Frame は Xconnect 上で送受信されます。

○ Forward Delay 設定
Forward Delay とは、L2TP セッション確立後、指定された Delay Time の間、Frame の転送をおこなわない機能のことです。

例えば、他の L2 サービスと併用し、L2RP の対向が存在しないような構成において、L2RP 機能では自身が送出した Advertise フレームを受信することで Loop を検出しますが、Advertise フレームを受信するまでは一時的に Loop が発生する可能性があります。
このような場合に Forward Delay を有効にすることによって、Loop の発生を抑止することができます。

delay Time の設定値は Advertisement Interval より長い時間を設定することを推奨します。

※他の L2RP サービスとの併用例



○ Port Down Time 設定
L2RP 機能によって、Active セッションの切り替えが発生した際、配下のスイッチにおける MAC アドレスのエントリが、以前 Master だった機器の Port を向いているために最大約 5 分間通信ができなくなる場合があります。
これを回避するために、Master から Backup の切り替え時に自身の Port のリンク状態を一時的にダウンさせることによって配下のスイッチの MAC テーブルをフラッシュさせることができます。

設定値は、切り替え時に Port をダウンさせる時間です。
“ 0 ”を指定すると本機能は無効になります。

L2RP Group Blocking 状態について
他の L2 サービスと併用している場合に、自身が送出した Advertise Frame を受信したことによって、Frame の転送を停止している状態を Group Blocking 状態と言います。
この Group Blocking 状態に変化があった場合にも、以下の設定で、機器の MAC テーブルをフラッシュすることができます。

○ Block Reset 設定
自身の Port のリンク状態を一時的に Down させ、配下のスイッチの MAC テーブルをフラッシュします。
Group Blocking状態に遷移した場合のみ動作します。

入力、選択後「設定」ボタンをクリックしてください。

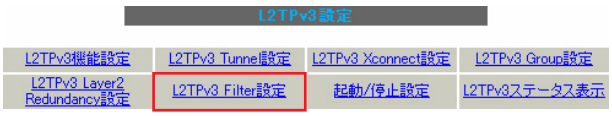
L2RP 機能使用時の注意

L2RP 機能を使用する場合は、Xconnect 設定において以下のオプション設定をおこなってください。

- Loop Detect 機能 「無効」
- known-unicast 機能 「送信する」
- Circuit Down 時 Frame 転送設定「送信する」

Ⅶ. L2TPv3 Filter 設定

L2TPv3 Filter 設定については、次章
「第 16 章 L2TPv3 フィルタ機能」で説明します。

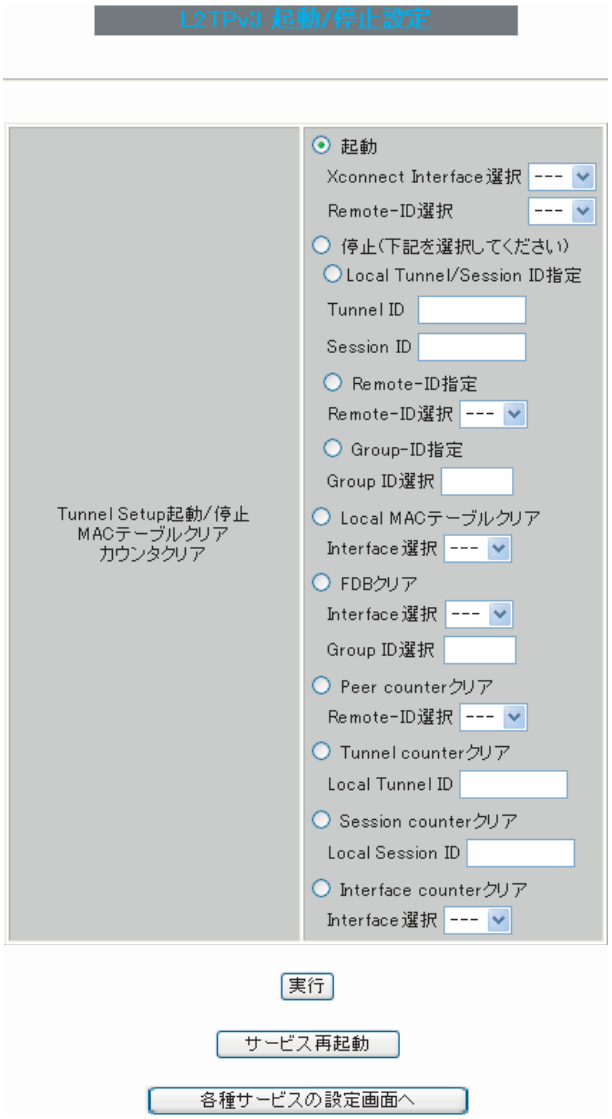


Ⅷ. 起動 / 停止設定

L2TPv3 トンネル / セッションの起動や停止、MAC テーブルのクリア等をおこないます。

実行方法

「各種サービスの設定」→「L2TPv3」の「起動 / 停止設定」をクリックします。



○起動

・Xconnect Interface 選択
トンネル / セッション接続を実行したい Xconnect インタフェースを選択します。
プルダウンには、「L2TPv3 Xconnect 設定」で設定したインタフェースが表示されます。

・Remote-ID 選択
Point to Multi-point 接続や L2TPv3 二重化の場合に、1 セッションずつ接続したい場合は、接続したい Remote-ID をプルダウンから選択してください。

画面下部の「実行」ボタンを押下すると、接続を開始します。

Ⅷ. 起動 / 停止設定

○停止
トンネル / セッションの停止をおこないます。停止したい方法を以下から選択してください。

○ Local Tunnel/Session ID 指定
１セッションのみ切断したい場合は、切断するセッションの Tunnel ID/Session ID を指定してください。

○ Remote-ID 指定
ある LCCE に対するセッションを全て切断したい場合は、対向 LCCE の Remote-ID を選択してください。

○ Group-ID 指定
グループ内のセッションを全て停止したい場合は、停止する Group ID を指定してください。

○ Local MAC テーブルクリア
L2TPv3 機能で保持しているローカル側の MAC テーブル(Local MAC テーブル)をクリアします。
クリアしたい Xconnect Interface をプルダウンから選択してください。

○ FDB クリア
L2TPv3 機能で保持している L2TP セッション側の MAC テーブル(FDB)をクリアします。
Group ID を選択した場合は、そのグループで持つ FDB のみクリアします。
Xconnect Interface をプルダウンから選択した場合は、その Interface で持つ全てのセッション ID の FDB をクリアします。

なお、「Local MAC テーブル」、「FDB」における MAC テーブルは、本装置の「情報表示」で表示される ARP テーブルとは別です。

○ Peer counter クリア
「L2TPv3 ステータス表示」で表示される「Peer ステータス表示」のカウンタをクリアします。
プルダウンからクリアしたい Remote-ID を選択してください。
プルダウンには、「L2TPv3 Xconnect 設定」で設定した Peer ID が表示されます。

○ Tunnel Counter クリア
「L2TPv3 ステータス表示」で表示される「Tunnel ステータス表示」のカウンタをクリアします。
クリアしたい Local Tunnel ID を指定してください。

○ Session counter クリア
「L2TPv3 ステータス表示」で表示される「Session ステータス」のカウンタをクリアします。
クリアしたい Local Session ID を指定してください。

○ Interface counter クリア
「L2TPv3 ステータス表示」で表示される「Xconnect Interface 情報表示」のカウンタをクリアします。
プルダウンからクリアしたい Interface を選択してください。
プルダウンには、「L2TPv3 Xconnect 設定」で設定したインタフェースが表示されます。

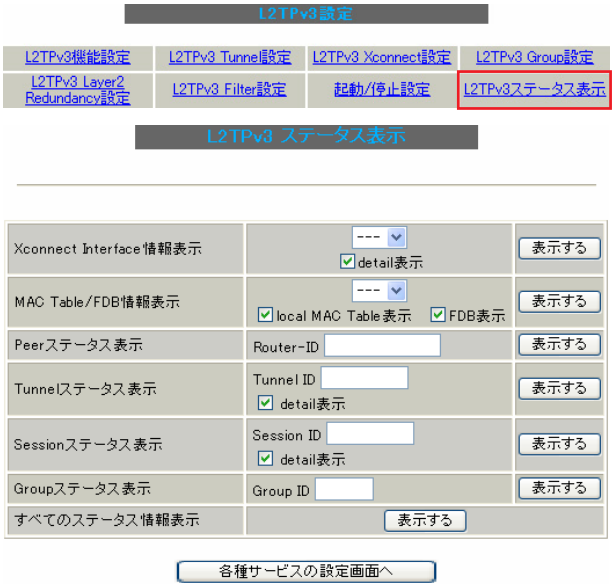
画面下部の「実行」ボタンを押下すると、接続を停止します。

IX．L2TPv3　ステータス表示

L2TPv3の各種ステータスを表示します。

実行方法

「各種サービスの設定」→「L2TPv3」の
「L2TPv3 ステータス表示」をクリックします。



○ Xconnect Interface 情報表示
Xconnect Interfaceのカウンタ情報を表示します。
プルダウンから表示したいInterfaceを選択してください。

・detail 表示
チェックを入れると詳細情報を表示することができます。

○ MAC Table/FDB 情報表示
L2TPv3機能が保持しているMACアドレステーブルの内容を表示します。
プルダウンから表示したいXconnectインタフェースを選択してください。

・local MAC Table 表示
ローカル側で保持するMACテーブルを表示したい場合はチェックを入れてください。

・FDB 表示
L2TPセッション側で保持するMACテーブルを表示したい場合はチェックを入れてください。

「local MAC Table 表示」と「FDB 表示」の両方にチェックを入れることもできます。

○ Peer ステータス表示
Peer ステータス情報を表示します。
表示したい Router-ID を指定してください。

○ Tunnel ステータス表示
L2TPv3 トンネルの情報のみを表示します。
表示したい Tunnel ID を指定してください。

・detail 表示
チェックを入れると詳細情報を表示することができます。

○ Session ステータス表示
L2TPv3セッションの情報とカウンタ情報を表示します。
表示したい Session ID を指定してください。
指定しない場合は全てのセッションの情報を表示します。

・detail 表示
チェックを入れると詳細情報を表示することができます。

○ Group ステータス表示
L2TPv3グループの情報を表示します。
プライマリ・セカンダリの Xconnect/ セッション情報と現在 Active のセッション ID が表示されます。
表示したい Group ID を指定してください。
指定しない場合は全てのグループの情報を表示します。

○すべてのステータス情報表示
上記 5 つの情報を一覧表示します。

「表示する」ボタンをクリックすると、新しいウィンドウが開いて、L2TPv3 のステータス情報が表示されます。

X．制御メッセージ一覧

L2TPのログには各種制御メッセージが表示されます。
メッセージの内容については、下記を参照してください。

[制御コネクション関連メッセージ]

SCCRQ：Start-Control-Connection-Request
制御コネクション(トンネル)の確立を要求するメッセージ。

SCCRP：Start-Control-Connection-Reply
SCCRQ に対する応答メッセージ。トンネルの確立に同意したことを示します。

SCCCN：Start-Control-Connection-Connected
SCCRP に対する応答メッセージ。このメッセージにより、トンネルが確立したことを示します。

StopCCN：Stop-Control-Connection-Notification
トンネルを切断するメッセージ。これにより、トンネル内のセッションも切断されます。

HELLO：Hello
トンネルの状態を確認するために使われるメッセージ。

[呼管理関連メッセージ]

ICRQ：Incoming-Call-Request
リモートクライアントから送られる着呼要求メッセージ。

ICRP：Incoming-Call-Reply
ICRQ に対する応答メッセージ。

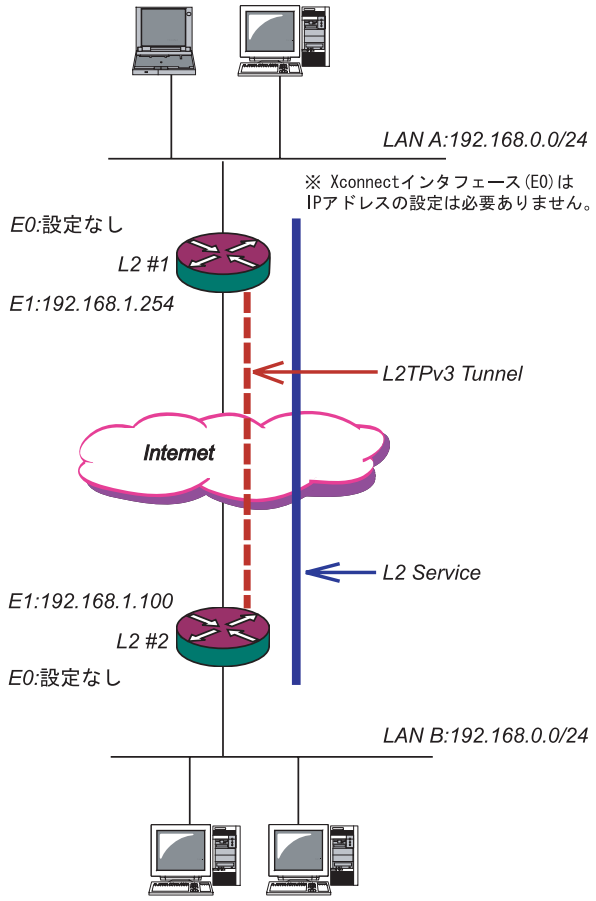
ICCN：Incoming-Call-Connected
ICRP に対する応答メッセージ。このメッセージにより、L2TP セッションが確立した状態になったことを示します。

CDN：Call-Disconnect-Notify
L2TPセッションの切断を要求するメッセージ。

XⅠ．L2TPv3　設定例 1(2 拠点間の L2TP トンネル)

2 拠点間で L2TP トンネルを構築し、End to End で Ethernet フレームを透過的に転送する設定例です。

構成図（例）



L2TPv3 サービスの起動

L2TPv3 機能を設定するときは、はじめに「各種サービス」の「L2TPv3」を起動してください。

ＸＩ．L2TPv3　設定例 1(2 拠点間の L2TP トンネル)

L2 #1 ルータの設定

L2TPv3 機能設定をおこないます。

・Local Router-ID は IP アドレス形式で設定します(この設定例では Ether1 ポートの IP アドレスとしています)。

Local hostname	L2-1
Local Router-ID	192.168.1.254
MAC Address学習機能	◉ 有効 ○ 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
PMTU Discovery設定	◉ 有効 ○ 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	◉ 有効 ○ 無効
SNMP機能設定	○ 有効 ◉ 無効
SNMP Trap機能設定	○ 有効 ◉ 無効
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☑ L2TPエラーメッセージ出力

L2TPv3 Tunnel 設定をおこないます。

・「AVP Hinding」「Digest type」を使用するときは、「パスワード」を設定する必要があります。

・PPPoE 接続と L2TPv3 接続を連動させるときは、「Bind Interface」に PPP インタフェース名を設定します。

Description	sample
Peerアドレス	192.168.1.100 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	○ 有効 ◉ 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-2
Remote RouterID設定	192.168.1.100
Vendor ID設定	20376:CENTURY
Bind Interface設定	
送信プロトコル	◉ over IP ○ over UDP
送信ポート番号	1701 (default 1701)

L2TPv3 Xconnect Interface 設定をおこないます。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.100
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	◉ 有効 ○ 無効
MSS設定	◉ 有効 ○ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
Circuit Down時Frame転送設定	◉ 送信する ○ 送信しない
Split Horizon設定	○ 有効 ◉ 無効

XⅠ．L2TPv3　設定例 1(2 拠点間の L2TP トンネル)

L2 #2 ルータの設定

L2#1 ルータと同様に設定します。

L2TPv3 機能設定をおこないます。

Local hostname	L2-2
Local Router-ID	192.168.1.100
MAC Address学習機能	◉ 有効 ○ 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
PMTU Discovery設定	◉ 有効 ○ 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	◉ 有効 ○ 無効
SNMP機能設定	○ 有効 ◉ 無効
SNMP Trap機能設定	○ 有効 ◉ 無効
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☑ L2TPエラーメッセージ出力

L2TPv3 Tunnel 設定をおこないます。

Description	
Peerアドレス	192.168.1.254 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	○ 有効 ◉ 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-1
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376:CENTURY
Bind Interface設定	
送信プロトコル	◉ over IP ○ over UDP
送信ポート番号	1701 (default 1701)

L2TPv3 Xconnect Interface設定をおこないます。

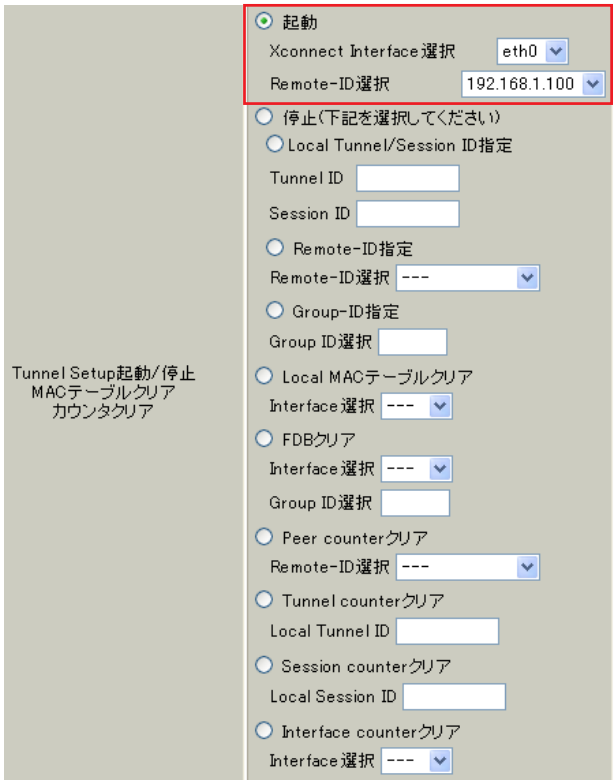
Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.254
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	◉ 有効 ○ 無効
MSS設定	◉ 有効 ○ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
Circuit Down時Frame転送設定	◉ 送信する ○ 送信しない
Split Horizon設定	○ 有効 ◉ 無効

XI.L2TPv3　設定例 1（2 拠点間の L2TP トンネル）

L2TPv3TunnelSetup の起動

ルータの設定後、「起動 / 停止設定」画面で L2TPv3 接続を開始させます。

下の画面で「起動」にチェックを入れ、Xconnect Interface と Remote-ID を選択します。
画面下の「実行」ボタンをクリックすると L2TPv3 接続を開始します。

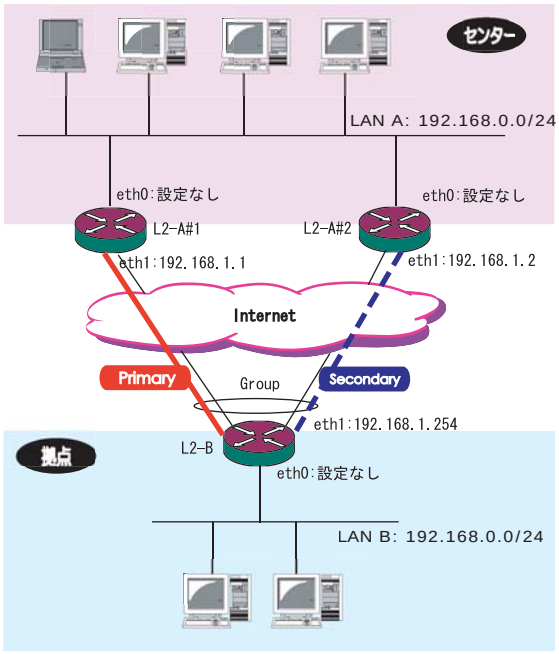


L2TPv3 接続を停止するときは、「起動 / 停止設定」画面で停止するか、各種サービス設定画面で L2TPv3 を停止します。

X II．L2TPv3　設定例 2（L2TP トンネル二重化）

次に、センター側を 2 台の冗長構成にし、拠点 / センター間のL2TPトンネルを二重化する場合の設定例です。
本例では、センター側の 2 台の XR のそれぞれに対し、拠点側 XR から L2TPv3 セッションを張り、Secondary 側セッションは STAND-BY セッションとして待機させるような設定をおこないます。

構成図（例）



XII．L2TPv3　設定例 2（L2TP トンネル二重化）

L2-A#1/L2-A#2(センター側)ルータの設定

L2-A#1（Primary）ルータ

L2TPv3 機能設定をおこないます。

- 「LocalHostName」には任意のホスト名を設定します。
- 「Local Router-ID」には WAN 側の IP アドレスを設定します。

Local hostname	L2-A1
Local Router-ID	192.168.1.1
MAC Address学習機能	◉ 有効 ○ 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
PMTU Discovery設定	◉ 有効 ○ 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	◉ 有効 ○ 無効
SNMP機能設定	○ 有効 ◉ 無効
SNMP Trap機能設定	○ 有効 ◉ 無効
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☑ L2TPエラーメッセージ出力

L2-A#2（Secondary）ルータ

L2TPv3 機能設定をおこないます。

- Primaryルータと同じ要領で設定してください。

Local hostname	L2-A2
Local Router-ID	192.168.1.2
MAC Address学習機能	◉ 有効 ○ 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
PMTU Discovery設定	◉ 有効 ○ 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	◉ 有効 ○ 無効
SNMP機能設定	○ 有効 ◉ 無効
SNMP Trap機能設定	○ 有効 ◉ 無効
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☑ L2TPエラーメッセージ出力

X II．L2TPv3　設定例 2（L2TP トンネル二重化）

L2-A#1（Primary）ルータ

L2TPv3 Tunnel 設定をおこないます。

- 「Peer アドレス」には拠点側ルータの WAN 側の IP アドレスを設定します。
- 「LocalHostName」「Local Router-ID」が未設定の場合は、機能設定で設定した値が使用されます。
- 「Local Router-ID」には WAN 側の IP アドレスを設定します。
- 「RemoteHostName」「Remote Router-ID」は、それぞれ拠点側ルータで設定します。「LocalHostName」「Local Router-ID」と同じものを設定します。

Description	primary
Peerアドレス	192.168.1.254 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	○ 有効 ◉ 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-B
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376:CENTURY
Bind Interface設定	
送信プロトコル	◉ over IP ○ over UDP
送信ポート番号	1701 (default 1701)

L2-A#2（Secondary）ルータ

L2TPv3 Tunnel 設定をおこないます。

- Primary ルータと同じ要領で設定してください。本例の場合、Primary ルータと同じ設定になります。

Description	secondary
Peerアドレス	192.168.1.254 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	○ 有効 ◉ 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-B
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376:CENTURY
Bind Interface設定	
送信プロトコル	◉ over IP ○ over UDP
送信ポート番号	1701 (default 1701)

XII．L2TPv3　設定例 2（L2TP トンネル二重化）

L2-A#1（Primary）ルータ

L2TPv3 Xconnect Interface 設定をおこないます。

- 「Xconnect ID 設定」は Group 設定をおこなわないので設定不要です。
- 「Tunnel 設定選択」はプルダウンから拠点側ルータの Peer アドレスを選択します。
- 「L2Frame 受信インタフェース」は LAN 側のインタフェースを指定します。
  LAN 側インタフェースには IP アドレスを設定する必要はありません。
- 「Remote End ID 設定」は任意の END ID を設定します。必ず拠点側ルータの Primary セッションと同じ値を設定してください。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.254
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	◉ 有効 ○ 無効
MSS設定	◉ 有効 ○ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
Circuit Down時Frame転送設定	◉ 送信する ○ 送信しない
Split Horizon設定	○ 有効 ◉ 無効

L2-A#2（Secondary）ルータ

L2TPv3 Xconnect Interface 設定をおこないます。

- Primary ルータと同じ要領で設定してください。
- 「Remote End ID 設定」は、拠点側ルータの Secondary セッションと同じ値を設定します。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.254
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	2 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	◉ 有効 ○ 無効
MSS設定	◉ 有効 ○ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
Circuit Down時Frame転送設定	◉ 送信する ○ 送信しない
Split Horizon設定	○ 有効 ◉ 無効

XII．L2TPv3　設定例 2（L2TP トンネル二重化）

L2TPv3 Group 設定について

・Primary、Secondary ルータともに、L2TP セッションの Group 化はおこなわないので、設定の必要はありません。

L2-B(拠点側ルータ)の設定

L2TPv3 機能設定をおこないます。

・「LocalHostName」には任意のホスト名を設定します。

・「Local Router-ID」には WAN 側の IP アドレスを設定します。

Local hostname	L2-B
Local Router-ID	192.168.1.254
MAC Address学習機能	◉ 有効 ○ 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
PMTU Discovery設定	◉ 有効 ○ 無効
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	◉ 有効 ○ 無効
SNMP機能設定	○ 有効 ◉ 無効
SNMP Trap機能設定	○ 有効 ◉ 無効
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☑ L2TPエラーメッセージ出力

X II．L2TPv3　設定例 2（L2TP トンネル二重化）

Primary セッション側

L2TPv3 Tunnel 設定をおこないます。

- 「Peer アドレス」にはセンター側 Primary ルータの WAN 側の IP アドレスを設定します。
- 「Hello Interval 設定」を設定した場合、L2TP セッションの Keep-Alive をおこないます。回線または対向 LCCE の障害を検出し、ACTIVE セッションを Secondary 側へ自動的に切り替えることができます。
- 「LocalHostName」「Local Router-ID」が未設定の場合は、機能設定で設定した値が使用されます。
- 「Local Router-ID」には WAN 側の IP アドレスを設定します。
- 「RemoteHostName」「Remote Router-ID」は、それぞれセンター側 Primary ルータで設定する「LocalHostName」「Local Router-ID」と同じものを設定します。

Description	primary
Peerアドレス	192.168.1.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	○ 有効 ◉ 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-A1
Remote RouterID設定	192.168.1.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	
送信プロトコル	◉ over IP ○ over UDP
送信ポート番号	1701 (default 1701)

Secondary セッション側

L2TPv3 Tunnel 設定をおこないます。

- Primary セッションと同じ要領で設定してください。

Description	secondary
Peerアドレス	192.168.1.2 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	○ 有効 ◉ 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-A2
Remote RouterID設定	192.168.1.2
Vendor ID設定	20376:CENTURY
Bind Interface設定	
送信プロトコル	◉ over IP ○ over UDP
送信ポート番号	1701 (default 1701)

X II．L2TPv3　設定例 2（L2TP トンネル二重化）

Primary セッション側

L2TPv3 Xconnect 設定をおこないます。

- 「Xconnect ID 設定」は任意の XconnectID を設定します。必ず Secondary 側と異なる値を設定してください。
- 「Tunnel 設定選択」はプルダウンから Primary セッションの Peer アドレスを選択します。
- 「L2Frame 受信インタフェース」は LAN 側のインタフェースを指定します。
  LAN 側インタフェースには IP アドレスを設定する必要はありません。
- 「Remote End ID 設定」は任意の END ID を設定します。必ずセンター側 Primary ルータで設定する End ID と同じ値を設定します。ただし、Secondary 側と同じ値は設定できません。
- 「Reschedule Interval 設定」に任意の Interval 時間を設定してください。この場合、L2TP セッションの切断検出時に自動的に再接続をおこないます。

Xconnect ID設定 (Group設定を行う場合は指定)	1 [1-4294967295]
Tunnel設定選択	192.168.1.1
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	◉ 有効 ○ 無効
MSS設定	◉ 有効 ○ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
Circuit Down時Frame転送設定	◉ 送信する ○ 送信しない
Split Horizon設定	○ 有効 ◉ 無効

Secondary セッション側

L2TPv3 Xconnect 設定をおこないます。

- Primary セッションと同じ要領で設定してください。

Xconnect ID設定 (Group設定を行う場合は指定)	2 [1-4294967295]
Tunnel設定選択	192.168.1.2
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	2 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	◉ 有効 ○ 無効
MSS設定	◉ 有効 ○ 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	○ 有効 ◉ 無効
Known Unicast設定	○ 送信する ◉ 送信しない
Circuit Down時Frame転送設定	◉ 送信する ○ 送信しない
Split Horizon設定	○ 有効 ◉ 無効

X II．L2TPv3　設定例 2（L2TP トンネル二重化）

L2TPv3 Group 設定をおこないます。

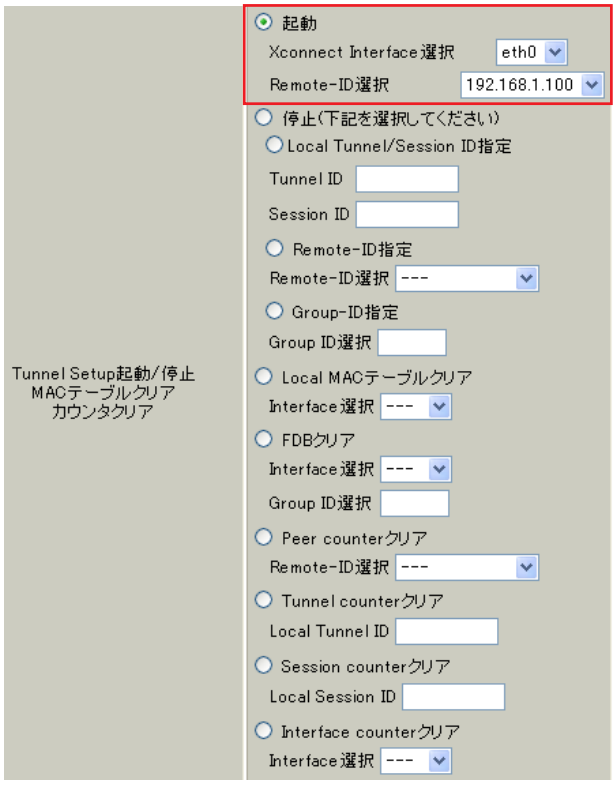
- 「Group ID」は任意のグループ ID を設定します。
- 「Primary Xconnect 設定選択」はプルダウンから Primary セッションの Xconnect ID を選択します。
- 「Secondary Xconnect 設定選択」はプルダウンから Secondary セッションの Xconnect ID を選択します。
- 本例では「Preempt 設定」「Primary active 時の Secondary Session 強制切断設定」をそれぞれ「無効」に設定しています。常に Primary/Secondary セッションの両方が接続された状態となり、Secondary セッション側は Stand-by 状態として待機しています。Primary セッションの障害時には、Secondary セッションを即時に Active 化します。

Group ID	1 [1-4095]
Primary Xconnect設定選択	1
Secondary Xconnect設定選択	2
Preempt設定	○ 有効 ◉ 無効
Primary active時の Secondary Session強制切断設定	○ 有効 ◉ 無効
Active Hold設定	○ 有効 ◉ 無効

L2TPv3TunnelSetup の起動

設定後が終わりましたら L2TPv3 機能の起動 / 停止設定をおこないます。

「起動 / 停止」画面で Xconnect Interface と Remote-ID を選択し、画面下の「実行」ボタンをクリックすると L2TPv3 接続を開始します。



本例では、拠点側から Primary/Secondary の両方の L2TPv3 接続を開始し、Primary 側が ACTIVE セッション、Secondary 側は STAND-BY セッションとして確立します。

L2TPv3 接続を停止するときは、「起動 / 停止設定」画面で停止するか、各種サービス設定画面で L2TPv3 を停止します。

第 16 章

L2TPv3 フィルタ機能

第 16 章 L2TPv3 フィルタ機能

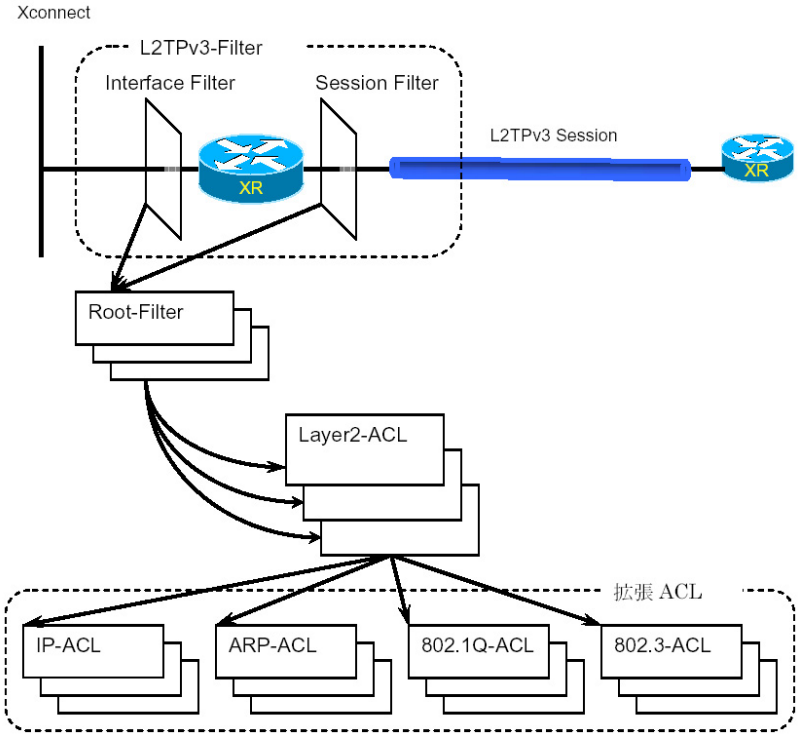
Ⅰ．L2TPv3 フィルタ 機能概要

L2TPv3 フィルタ概要

XR の L2TPv3 フィルタ機能は、ユーザが設定したフィルタリングルールに従い、Xconnect Interface 上もしくは Session 上でアクセス制御をおこないます。
アクセス制御は、MAC アドレスや IPv4 、ARP、802.1Q、TCP/UDP など L2-L4 での詳細な指定が可能です。

L2TPv3 フィルタ設定概要

L2TPv3 フィルタは以下の要素で構成されています。



(1)Access Control List (ACL)
Layer2 レベルでルールを記述する「Layer2 ACL」およびプロトコル毎に詳細なルールを記述する拡張 ACL として IP-ACL、ARP-ACL、802.1Q-ACL、802.3-ACL があります。

(2)Root-Filter
Root-FilterではLayer2 ACLを検索する順にリストします。
各Root Filterにはユーザによりシステムでユニークな名前を付与し、識別します。
Root Filter では、配下に設定された全ての Layer2 ACL に一致しなかった場合の動作を Default ポリシーとします。
Defaultポリシーとして定義可能な動作は、deny（破棄）/permit（許可）です。

(3)L2TPv3-Filter
Xconnect Interface、Session それぞれに適用する Root-Filter を設定します。
Xconnect Interfaceに関してはInterface Filter、Session に関しては Session Filter で設定します。

第 16 章 L2TPv3 フィルタ機能

Ⅰ．L2TPv3 フィルタ 機能概要

L2TPv3 フィルタの動作（ポリシー）

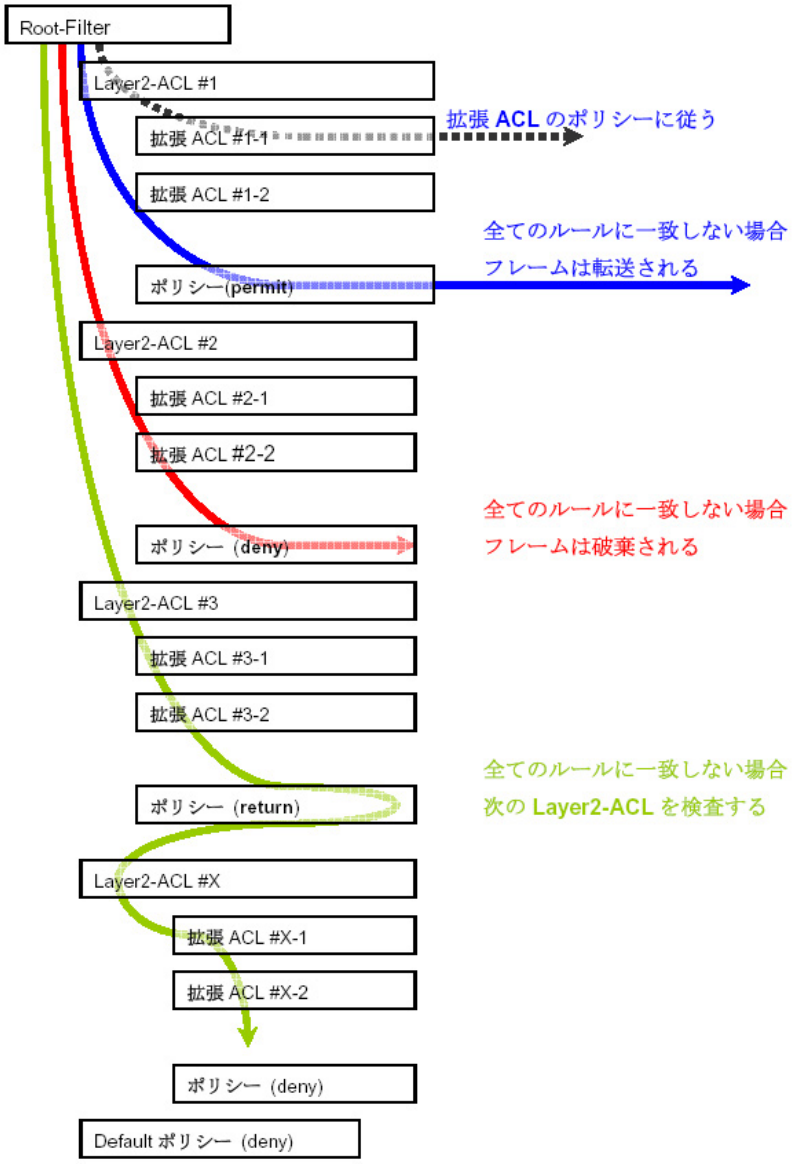
設定条件に一致した場合、L2TPv3 フィルタは以下の動作をおこないます。

1)許可(permit)
フィルタルールに一致した場合、検索を中止してフレームを転送します。

2)破棄(deny)
フィルタルールに一致した場合、検索を中止してフレームを破棄します。

3)復帰(return)
Layer2 ACL でのみ指定可能です。フィルタルールに一致しない場合、該当 Layer2 ACL での検索を中止して呼び出し元の次の Layer2 ACL から検索を再開します。

フィルタ評価のモデル図



第 16 章 L2TPv3 フィルタ機能

Ⅰ．L2TPv3 フィルタ 機能概要

フィルタの評価

Root-Filter の配下に設定された Layer2 ACL の検索は、定義された上位から順番におこない、最初に条件に一致したもの（1st match）に対して以下の評価をおこないます。

・拡張 ACL がない場合

該当 Layer2 ACL のポリシーに従い、deny/permit/return をおこないます。

・拡張 ACL がある場合

Layer2 ACL の配下に設定された拡張 ACL の検索は、1st match にて検索をおこない、以下の評価をおこないます。

1) 拡張 ACL に一致する場合、拡張 ACL の policy に従い deny/permit をおこないます。
2) 全ての拡張 ACL に一致しない場合、該当 Layer2 ACL のポリシーに従い、 deny/permit/return をおこないます。

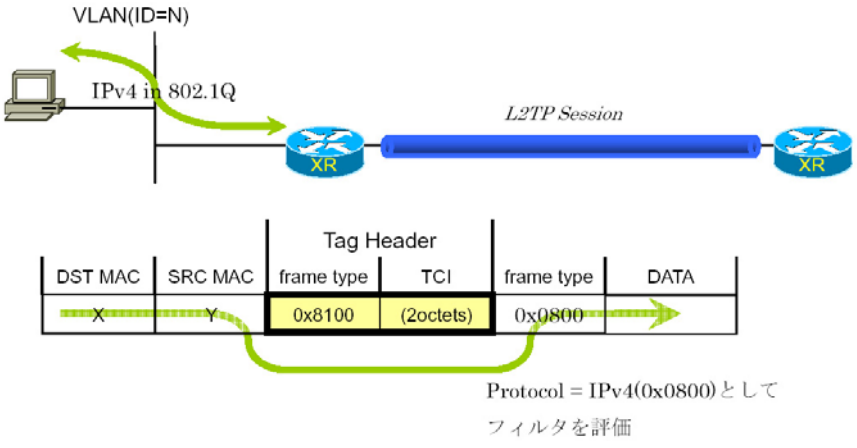
フレームが配下に設定された全ての Layer2 ACL に一致しなかった場合は、Default ポリシーによりフレームを deny または permit します。

フィルタ処理順序

L2TPv3 フィルタにおける処理順序は、IN 側フィルタでは送信元 / あて先 MAC アドレスのチェックをおこなったあとになります。
「Known Unicast 設定」や「Circuit Down 時の Frame 転送」によりフレームの転送が禁止されている状態で permit 条件に一致するフレームを受信しても、フレームの転送はおこなわれませんのでご注意ください。

802.1Q タグヘッダ

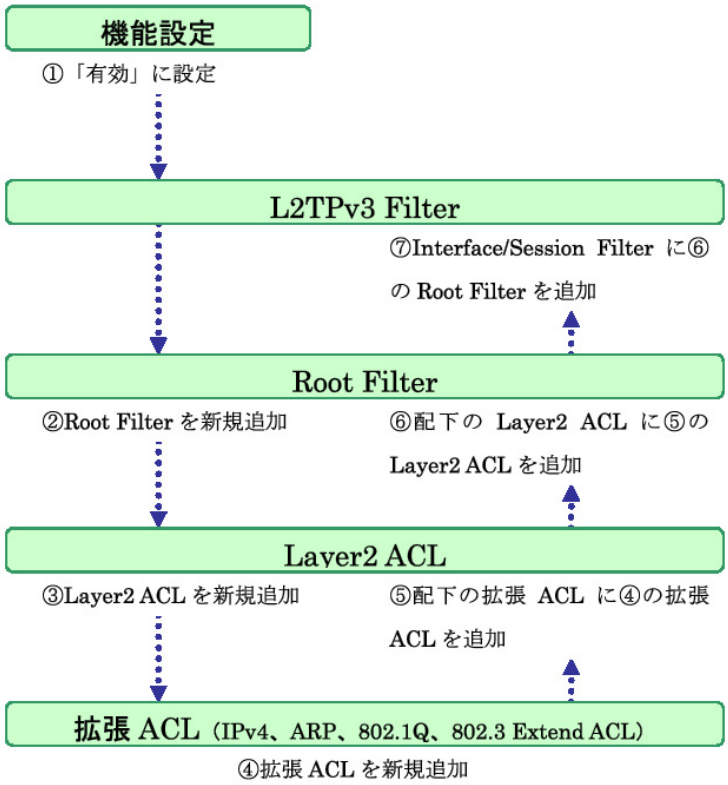
Xconnect Interface が VLAN(802.1Q)であるフレームをフィルタリングする場合、タグヘッダについては、フィルタの評価対象から除外し、タグヘッダに続くフィールドから再開します(下図参照)。



Ⅱ．設定順序について

L2TPv3 Filter の設定順序は、下の表を参考にしてください。

【L2TPv3 Filter の設定順序】



III．機能設定

設定方法

Web 設定画面「各種サービスの設定」→「L2TPv3」をクリックして、画面上部の「L2TPv3 Filter 設定」をクリックします。

L2TPv3 フィルタは以下の画面で設定をおこないます。

◆機能設定
◆L2TPv3 Filter 設定
◆Root Filter 設定
◆Layer2 ACL 設定
◆IPv4 Extend ACL 設定
◆ARP Extend ACL 設定
◆802.1Q Extend ACL 設定
◆802.3 Extend ACL 設定
◆情報表示

◆機能設定

L2TPv3 フィルタ設定画面の「機能設定」をクリックします。

設定

○本機能
L2TPv3 Fitler 機能の有効 / 無効を選択し、設定ボタンを押します。

IV. L2TPv3 Filter 設定

◆L2TPv3 Filter 設定

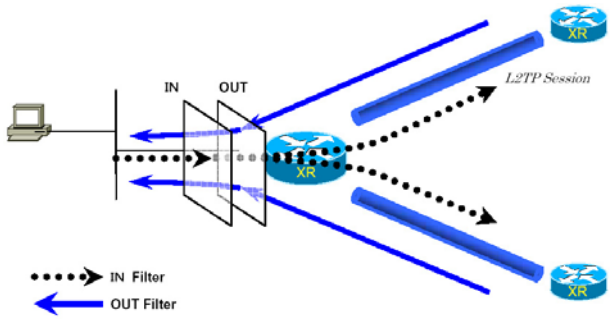
L2TPv3 Filter 設定画面の「L2TPv3 Filter 設定」をクリックします。
現在設定されている Interface Filter と Session Filter が一覧表示されます。

Interface Filter

Interface Filter

Index	Interface	IN Filter	OUT Filter	edit
1	eth0	Root-1	Root-2	edit

Interface Filter は、Root Filter を Xconnect Interface に対応づけてフィルタリングをおこないます。
IN Filter は外側のネットワークから Xconnect Interface を通して XR が受信するフレームをフィルタリングします。OUT Filter は XR が Xconnect Interface を通して送信するフレームをフィルタリングします。



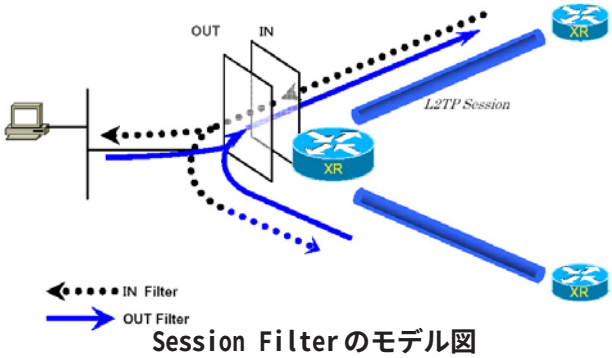
Interface Filter のモデル図

Session Filter

Session Filter

Index	Peer ID	RemoteEND ID	IN Filter	OUT Filter	edit
1	192.168.0.1	1	Root-2	Root-3	edit
2	192.168.0.2	2	Root-3	Root-4	edit

Session Filter は、Root Filter を Session に関連づけてフィルタリングをおこないますので、Session から Session への通信を制御することが出来ます。
下の図で、IN Filter は XR が L2TP Session A から受信するフレームをフィルタリングしています。
OUT Filter は XR が L2TP Session A へ送信するフレームをフィルタリングしています。



Session Filter のモデル図

Interface Filter の編集

Interface Filter 一覧表示内の「edit」ボタンをクリックします。

L2TPv3 Filter適用設定

Interface	eth0
ACL(in)	Root-1
ACL(out)	Root-2

リセット 設定 戻る

○ Interface
Xconnect Interface に設定したインタフェース名が表示されます。

○ ACL(in)
IN 方向に設定する Root Filter 名を選択します。

○ ACL(out)
OUT 方向に設定する Root Filter 名を選択します。

Session Filter の編集

Session Filter 一覧表示内の「edit」ボタンをクリックします。

L2TPv3 Filter適用設定

PeerID : RemoteEndID	192.168.0.1:1
ACL(in)	Root-2
ACL(out)	Root-3

リセット 設定 戻る

○ PeerID : RemoteEndID
対向側の Xconnect Interface ID と Remote End ID が表示されます。

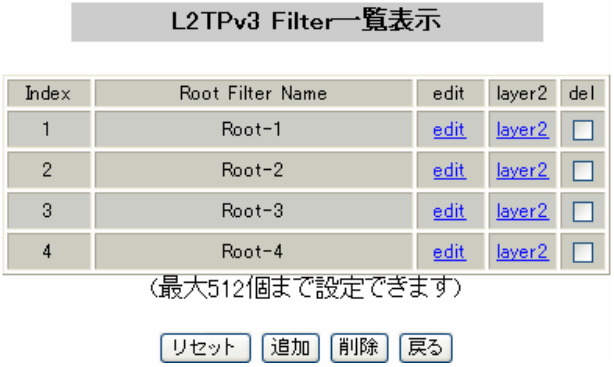
○ ACL(in)
IN 方向に設定したい Root Filter 名を選択します。

○ ACL(out)
OUT方向に設定したいRoot Filter名を選択します。

V．Root Filter 設定

◆Root Filter 設定

L2TPv3 Filter 設定画面の「Root Filter 設定」をクリックします。
現在設定されている Root Filter が一覧表示されます。



Root Filter の追加

画面下の「追加」ボタンをクリックします。

○ Root Filter Name

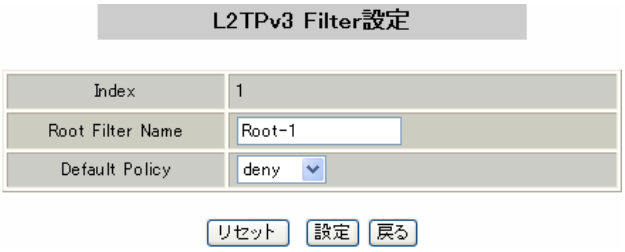
Root Filter を識別するための名前を入力します。設定可能な文字は、英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。
１ -64 文字の間で設定できます。ただし、１文字目は英数字に限ります。

○ Default Policy

受け取ったフレームが、その Root Filter の配下にある Layer2 ACL のすべてに一致しなかった場合の動作を設定します。Permit/Deny のどちらかを選択してください。

Root Filter の編集

一覧表示内の「edit」をクリックします。



追加画面と同様に設定してください。

Root Filter の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

V. Root Filter 設定

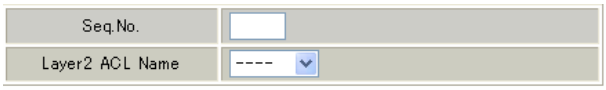
配下の Layer2 ACL を設定する

「L2TPv3 Filter 一覧表示」内の「layer2」をクリックすると、現在設定されている配下の Layer2 ACL が一覧で表示されます。

Seq.No.	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length	edit	del
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4	edit	☐
*	default	deny					

配下の Layer2 ACL の追加

画面下の「追加」ボタンをクリックします。

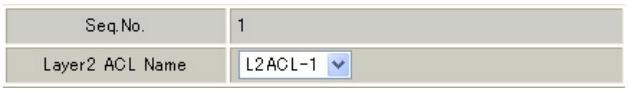


○ Seq.No.
配下の Layer2 ACL を検索する際の順番（シーケンス番号）を指定します。
無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

○ Layer2 ACL Name
その Root Filter の配下に設定したい Layer2 ACL を選択します。同一 Root Filter 内で重複する Layer2 ACL を設定することはできません。

配下の Layer2 ACL の編集

一覧表示内の「edit」をクリックします。



追加画面と同様に設定してください。

配下の Layer2 ACL の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

VI. Layer2 ACL 設定

◆Layer2 ACL 設定

L2TPv3 Filter 設定画面の「Layer2 ACL 設定」をクリックします。
現在設定されている Layer2 ACL が一覧表示されます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length	edit	extend	del
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4	edit	extend	☐

Layer2 ACL の追加

画面下の「追加」ボタンをクリックします。

Layer2 ACL Name	
Policy	----
Source MAC	
Destination MAC	
Type/Length	---- or [0x0600-0xffff]

○ Layer2 ACL Name
ACL を識別するための名前を入力します。
設定可能な文字は、英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。
１-64 文字の間で設定できます。ただし、１文字目は英数字に限ります。

○ Policy
deny（破棄）/permit（許可）/return（復帰）のいずれかを選択します。

○ Source MAC
送信元 MAC アドレスを指定します。
（マスクによるフィルタリングも可能です。）
＜フォーマット＞
XX:XX:XX:XX:XX:XX
XX:XX:XX:XX:XX:XX/MM:MM:MM:MM:MM:MM

○ Destination MAC
あて先 MAC アドレスを指定します。Source MAC 設定と同様に設定してください。

○ Type/Length
IPv4、IPv6、ARP、802.1Q、length または 16 進数指定の中から選択します（無指定でも可）。
16進数指定の場合は右側の入力欄に指定値を入力します。指定可能な範囲：0600-ffff です。
IPv4、ARP、802.1Q を指定すると配下の拡張 ACL に IPv4 Extend ACL、ARP Extend ACL、802.1Q Extend ACL を指定することが出来ます。
16 進数で length を指定すると、802.3 Extend ACL を指定することが出来ます。

Layer2 ACL の編集

一覧表示内の「edit」をクリックします。

Layer2 ACL Name	L2ACL-1
Policy	permit
Source MAC	00:11:22:33:44:55
Destination MAC	
Type/Length	IPv4 or [0x0600-0xffff]

追加画面と同様に設定してください。

Layer2 ACL の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

Ⅵ．Layer2 ACL 設定

配下に拡張 ACL を設定する

「Layer2 ACL 一覧表示」内の「extend」をクリックすると、現在設定されている配下の拡張 ACL が一覧で表示されます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4

Seq.No.	Extend ACL Name	edit	del
1	IPv4-1	edit	☐

配下の拡張 ACL の追加

画面下の「追加」ボタンをクリックします。

Seq.No.	
Name	----

○ Seq.NO.
配下の拡張 ACL を検索する際の順番（シーケンス番号）を指定します。
無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

○ Name
設定可能な拡張 ACL 名を選択します。
同一 Layer2 ACL 内で重複する拡張 ACL を設定することはできません。

配下の拡張 ACL の編集

一覧表示内の「edit」をクリックします。

Seq.No.	1
Name	IPv4acl_sample

追加画面と同様に設定してください。

配下の拡張 ACL の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

Ⅶ. IPv4 Extend ACL 設定

◆ IPv4 Extend ACL 設定

L2TPv3 Filter 設定画面の「IPv4 Extend ACL 設定」をクリックします。
現在設定されている IPv4 Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	Source IP	Destination IP	TOS	Protocol	option	edit	del
1	IPv4-1	permit	192.168.0.100	192.168.0.200		tcp		edit	☐

オプション欄表示の意味は次の通りです。

- src-port=X　送信元ポート番号が X
- dst-port=X:Y　あて先ポート番号の範囲が X～Y

IPv4 Extend ACL の追加

画面下の「追加」ボタンをクリックします。

Extend ACL Name	
Policy	----
Source IP	
Destination IP	
TOS	[0-0xff]
IP Protocol	---- or [0-255]
Source Port	[1-65535]
Destination Port	[1-65535]
ICMP Type	[0-255]
ICMP Code	[0-255]

○ Extend ACL Name
拡張 ACL を識別するための名前を入力します。
設定可能な文字は、英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。
１ -64 文字の間で設定できます。ただし、１文字目は英数字に限ります。

○ Policy
deny（破棄）/permit（許可）を選択します。

○ Source IP
送信元 IP アドレスを指定します。
（マスクによる指定も可能です。）
＜フォーマット＞
A.B.C.D
A.B.C.D/M

○ Destination IP
あて先 IP アドレスを指定します。
Source IP と同様に設定してください。

○ TOS
TOS 値を 16 進数で指定します。
指定可能な範囲：00-ff です。

○ IP Protocol
TCP/UDP/ICMP または 10 進数指定の中から選択します（無指定でも可）。
10 進数指定の場合は右側の入力欄に指定値を入力してください。
指定可能な範囲：0-255 です。

○ Source Port
送信元ポートを指定します。IP Protocol に TCP/UDP を指定した時のみ設定可能です。
範囲設定が可能です。
＜フォーマット＞
xxx（ポート番号 xx）
xxx:yyy（xxx 以上、yyy 以下のポート番号）

○ Destination Port
あて先ポートを指定します。設定方法は Source Port と同様です。

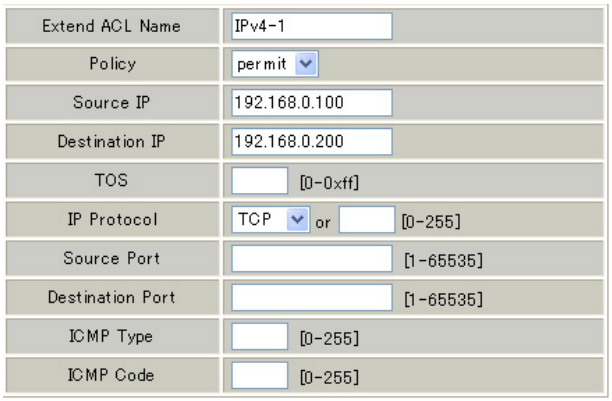
○ ICMP Type
ICMP Type の指定が可能です。IP Protocol に ICMP を指定した場合のみ設定可能です。
指定可能な範囲：0-255 です。

○ ICMP Code
ICMP Code の指定が可能です。ICMP Type が指定されていないと設定できません。
指定可能な範囲：0-255 です。

Ⅶ. IPv4 Extend ACL 設定

IPv4 Extend ACL を編集する

一覧表示内の「edit」をクリックします。



追加画面と同様に設定してください。

IPv4 Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

Ⅷ. ARP Extend ACL 設定

◆ARP Extend ACL 設定

L2TPv3 Filter 設定画面の「ARP Extend ACL 設定」をクリックします。
現在設定されている ARP Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	OPCODE	Source MAC	Destination MAC	Source IP	Destination IP	edit	del
1	ARP-1	permit		00:11:22:33:44:55			192.168.0.200	edit	☐

ARP Extend ACL の追加

画面下の「追加」ボタンをクリックします。

Extend ACL Name	
Policy	----
OPCODE	---- or [0-65535]
Source MAC	
Destination MAC	
Source IP	
Destination IP	

○ Extend ACL Name
拡張 ACL を識別するための名前を入力します。
設定可能な文字は、英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。
１ -64 文字の間で設定できます。ただし、１文字目は英数字に限ります。

○ Policy
deny（破棄）/permit（許可）を選択します。

○ OPCODE
Request、Reply、Request_Reverse、Reply_Reverse、DRARP_Request、DRARP_Reply、DRARP_Error、InARP_Request、ARP_NAK または10進数指定の中から選択します。無指定でも可能です。
10進数指定の場合は右側の入力欄に指定値を入力してください。
指定可能な範囲：0-65535 です。

○ Source MAC
送信元 MAC アドレスを指定します。
（マスクによるフィルタリングも可能です。）
＜フォーマット＞
XX:XX:XX:XX:XX:XX
XX:XX:XX:XX:XX:XX/MM:MM:MM:MM:MM:MM

○ Destination MAC
あて先 MAC アドレスを指定します。Source MAC 設定と同様に設定してください。

○ Source IP
送信元 IP アドレスを指定します。
（マスクによるフィルタリングも可能です。）
＜フォーマット＞
A.B.C.D
A.B.C.D/M

○ Destination IP
あて先 IP アドレスを指定します。Source IP 設定と同様に設定してください。

ARP Extend ACL の編集

一覧表示内の「edit」をクリックします。

Extend ACL Name	ARP-1
Policy	permit
OPCODE	---- or [0-65535]
Source MAC	00:11:22:33:44:55
Destination MAC	
Source IP	
Destination IP	192.168.0.200

追加画面と同様に設定してください。

ARP Extend ACL の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

IX. 802.1Q Extend ACL 設定

◆802.1Q Extend ACL 設定

L2TPv3 Filter 設定画面の「802.1Q Extend ACL 設定」をクリックします。
現在設定されている 802.1Q Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	VLAN ID	Priority	Ethernet Type	edit	extend	del
1	802.1Q-1	permit	10		IPv4	edit	extend	☐

802.1Q Extend ACL の追加

画面下の「追加」ボタンをクリックします。

Name	
Policy	----
VLAN ID	[0-4095]
Priority	[0-7]
Ethernet Type	---- or [0x0600-0xffff]

○ Name
拡張 ACL を識別するための名前を入力します。
設定可能な文字は、英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。
１ -64 文字の間で設定できます。ただし、１文字目は英数字に限ります。

○ Policy
deny（破棄）/permit（許可）のいずれかを選択します。

○ VLAN ID
VLAN ID を指定します。
範囲設定が可能です。指定可能な範囲：0-4095です。
＜フォーマット＞
xxx（VLAN ID：xx）
xxx:yyy（xxx 以上、yyy 以下の VLAN ID）

○ Priority
IEEE 802.1P で規定されている Priority Field を判定します。
指定可能な範囲：0-7 です。

○ Ethernet Type
カプセリングされたフレームの Ethernet Type を指定します。IPv4、IPv6、ARP または 16 進数指定の中から選択します。無指定でも設定可能です。
16進数指定の場合は右側の入力欄に指定値を入力してください。
指定可能な範囲：0600-ffff です。
IPv4、ARP を指定すると配下の拡張 ACL に IPv4 Extend ACL、ARP Extend ACL を指定することが出来ます。

802.1Q Extend ACL の編集

一覧表示内の「edit」をクリックします。

Name	802.1Q-1
Policy	permit
VLAN ID	10 [0-4095]
Priority	[0-7]
Ethernet Type	IPv4 or [0x0600-0xffff]

追加画面と同様に設定してください。

802.1Q Extend ACL の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

IX. 802.1Q Extend ACL 設定

配下に拡張 ACL を設定する

「802.1Q ACL 一覧表示」内の「extend」をクリックすると、現在設定されている配下の拡張 ACL の一覧が表示されます。

Index	Extend ACL Name	Policy	VLAN ID	Priority	Ethernet Type
1	802.1Q-1	deny	10		ARP

Seq.No.	Extend ACL Name	edit	del
1	ARP-1	edit	☐

配下の拡張 ACL の追加

画面下の「追加」ボタンをクリックします。

Seq.No.	
Name	----

○ Seq.NO.
配下の拡張 ACL を検索する際の順番（シーケンス番号）を指定します。無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

○ Name
設定可能な拡張 ACL 名を選択します。
同一 802.1Q Extend ACL 内で重複する拡張 ACL を設定することはできません。

配下の拡張 ACL の編集

一覧表示内の「edit」をクリックします。

Seq.No.	1
Name	ARP-1

追加画面と同様に設定してください。

配下の拡張 ACL の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

X . 802.3 Extend ACL 設定

◆802.3 Extend ACL 設定

L2TPv3 Filter 設定画面の「802.3 Extend ACL 設定」をクリックします。
現在設定されている 802.3 Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	DSAP/SSAP	type	edit	del
1	802.3-1	permit	0xaa		edit	☐

802.3 Extend ACL の追加

画面下の「追加」ボタンをクリックします。

Name	
Policy	----
DSAP/SSAP	0x [0x00-0xff]
Type	0x [0x0600-0xffff]

○ Name
拡張 ACL を識別するための名前を入力します。
設定可能な文字は、英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。
１ -64 文字の間で設定できます。ただし、１文字目は英数字に限ります。

○ Policy
deny（破棄）/permit（許可）のいずれかを選択します。

○ DSAP/SSAP
16 進数で DSAP/SSAP を指定します。
指定可能な範囲：00-ff です。
DSAP/SSAP は等値なので 1byte で指定します。

○ Type
16 進数で 802.3 with SNAP の type field を指定します。
指定可能な範囲：0600-ffff です。
DSAP/SSAP を指定した場合は設定できません。
この入力欄で Type を指定した場合の DSAP/SSAP は 0xaa/0xaa として判定されます。

802.3 Extend ACL の編集

一覧表示内の「edit」をクリックします。

Name	ACL-802_3-1
Policy	permit
DSAP/SSAP	0x aa [0x00-0xff]
Type	0x [0x0600-0xffff]

追加画面と同様に設定してください。

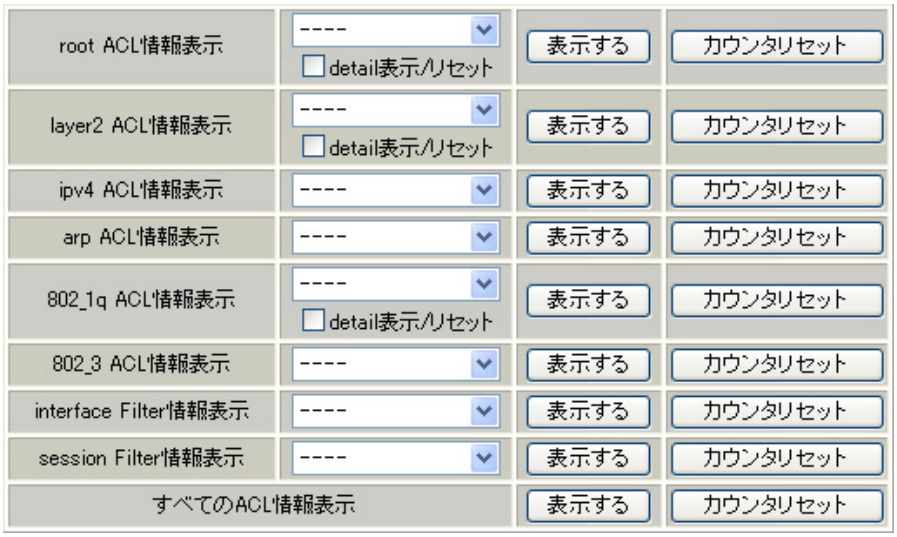
802.3 Extend ACL の削除

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

ＸＩ．情報表示

◆情報表示

L2TPv3 Filter 設定画面の「情報表示」をクリックします。



○表示する
「表示する」ボタンをクリックすると ACL 情報を表示します。
プルダウンから ACL 名を選択して個別に表示することもできます。
「detail 表示 / リセット」にチェックを入れてクリックすると、設定した全ての ACL 情報が表示されます。

○カウンタリセット
「カウンタリセット」ボタンをクリックすると ACL のカウンタをリセットします。
プルダウンから ACL 名を選択して個別にリセットすることもできます。
「detail 表示 / リセット」にチェックを入れてクリックすると、配下に設定されている ACL のカウンタも同時にリセットできます。

「表示する」ボタンで表示される情報は以下の通りです。
（※は detail 表示にチェックを入れた時に表示されます。）

○ Root ACL 情報表示
Root Filter名　総カウンタ（frame数、 byte数）
　　+Layer2 ACL 名
　　カウンタ（frame 数、byte 数）、Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
　　（+ 拡張 ACL 名）※
　　（カウンタ（frame 数、byte 数）、Policy）※
　　+Default Policy カウンタ（frame 数、byte 数） Default Policy

○ layer2 ACL 情報表示
Layer2 ACL 名
　　カウンタ（frame 数、byte 数）、Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
　　（+ 拡張 ACL 名）※
　　（カウンタ（frame 数、byte 数）、Policy）※

Ｘ Ｉ．情報表示

○ ipv4 ACL 情報表示
IPv4 ACL 名
　　カウンタ（frame 数、 byte 数）、Policy、送信元 IP アドレス、あて先 IP アドレス、TOS、Protocol、
　　オプション

○ arp ACL 情報表示
ARP ACL 名
　　カウンタ（frame 数、byte 数）、Policy、Code、送信元 MAC アドレス、あて先 MAC アドレス、
　送信元 IP アドレス、あて先 IP アドレス

○ 802_1q ACL 情報表示
802.1Q ACL 名
　　カウンタ（frame 数、byte 数）、Policy、VLAN-ID、Priority、encap-type
　　(+ 拡張 ACL 名）※
　　(カウンタ（frame 数、byte 数）、Policy）※

○ 802_3 ACL 情報表示
802.3 ACL 名
　　カウンタ（frame 数、byte 数）、Policy、DSAP/SSAP、type

○ interface Filter 情報表示
interface、in：カウンタ（frame 数、byte 数）：Root Filter 名
Root Filter 名、カウンタ（frame 数、byte 数）
　　+Layer2 ACL 名
　　 カウンタ（frame 数、byte 数）、Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
　　+Default Policy カウンタ（frame 数、byte 数） Default Policy

interface、out：カウンタ（frame 数、byte 数）：Root Filter 名
Root Filter 名、カウンタ（frame 数、byte 数）
　　+Layer2 ACL 名
　　 カウンタ（frame 数、byte 数）、Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
　　+Default Policy カウンタ（frame 数、byte 数） Default Policy

○ session Filter 情報表示
Peer ID、RemoteEND-ID、in：カウンタ（frame 数、byte 数）：Root Filter 名
Root Filter 名、カウンタ（frame 数、byte 数）
　　+Layer2 ACL 名
　　 カウンタ（frame 数、byte 数）、Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
　　+Default Policy カウンタ（frame 数、byte 数） Default Policy

Peer ID、RemoteEND-ID、out：カウンタ（frame 数、byte 数）：Root Filter 名
Root Filter 名、カウンタ（frame 数、byte 数）
　　+Layer2 ACL 名
　　 カウンタ（frame 数、byte 数）、Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
　　+Default Policy カウンタ（frame 数、byte 数） Default Policy

第 17 章

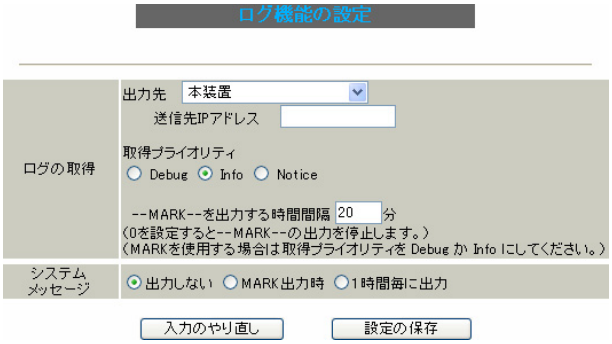
SYSLOG 機能

syslog 機能の設定

本装置は、syslogを出力・表示することが可能です。
また、他の syslog サーバに送出することもできます。
さらに、ログの内容を電子メールで送ることも可能です。電子メール設定は、「第 33 章 各種システム設定」をご参照ください。

syslog 取得機能の設定

Web 設定画面「各種サービスの設定」→「SYSLOG サービス」をクリックして、以下の画面から設定をおこないます。



<ログの取得>
○出力先
syslog の出力先を選択します。
「本装置」
本装置で syslog を取得する場合に選択します。

「SYSLOG サーバ」
syslog サーバに送信するときに選択します。

「本装置と SYSLOG サーバ」
本装置と syslog サーバの両方で syslog を管理します。

○送信先 IP アドレス
syslog サーバの IP アドレスを指定します。

○取得プライオリティ
ログ内容の出力レベルを指定します。
プライオリティの内容は以下のようになります。

- Debug：デバッグ時に有益な情報
- Info：システムからの情報
- Notice：システムからの通知

○ --MARK-- を出力する時間間隔
syslog が動作していることを表す「-- MARK --」ログを送出する間隔を指定します。
初期設定は 20 分です。

装置本体に記録しておけるログの容量には制限があります。継続的にログを取得される場合は外部の syslog サーバにログを送出するようにしてください。

<システムメッセージ>
本装置のシステム情報を定期的に出力することができます。
以下から選択してください。

○出力しない
システムメッセージを出力しません。

○ MARK 出力時
“ -- MARK -- ”の出力と同時にシステムメッセージが出力されます。

○１時間ごとに出力
１時間ごとにシステムメッセージを出力します。

最後に「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。

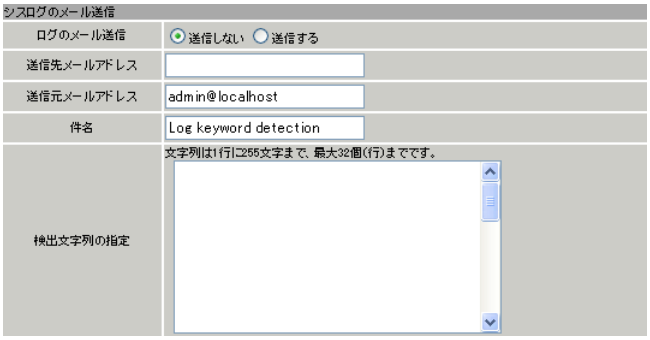
syslog 機能の設定

syslog のメール送信機能の設定

ログの内容を電子メールで送信したい場合の設定です。

Web 設定画面「システム設定」→「メール送信機能の設定」をクリックして以下の画面で設定します。

＜シスログのメール送信＞



設定方法については「**第33章 各種システム設定**」の「**◆メール送信機能の設定**」を参照してください。

ログファイルの取得

出力した syslog は、Web 設定画面「システム設定」→「ログの表示」で表示されます。

ローテーションで記録されたログは、圧縮して保存されます。
保存されるファイルは最大で 6 つです。

・USB フラッシュディスク装着時の syslog

本装置で初期化済みのオプション USB フラッシュディスクを装着している場合、ログは自動的にオプション USB フラッシュディスクに記録されます。

保存最大容量を超えると、以降は古いログファイルから順に削除されていきます。
ログファイルが作成されたときは画面上にリンクが生成され、各端末にダウンロードして利用できます。

ファシリティと監視レベルについて

本装置で設定されている syslog のファシリティ・監視レベルは以下のようになっています。

[ファシリティ：監視レベル]
***.info;mail.none;news.none;authpriv.none**

syslog 内容

出力される情報は下記の内容です。

```
Nov  7 14:57:44 localhost system: cpu:0.00
mem:28594176 session:0/2
```

・cpu:0.00
cpu のロードアベレージです。
1 に近いほど高負荷を表し、1 を超えている場合は過負荷の状態を表します。

・mem:28594176
空きメモリ量(byte)です。

・session:0/2 (XX/YY)
本装置内部で保持している NAT および IP マスカレード のセッション情報数です。

0 (XX)
現在 Establish している TCP セッションの数

2 (YY)
本装置が現在キャッシュしている全てのセッション数

第 18 章

攻撃検出機能

攻撃検出機能の設定

攻撃検出機能の概要

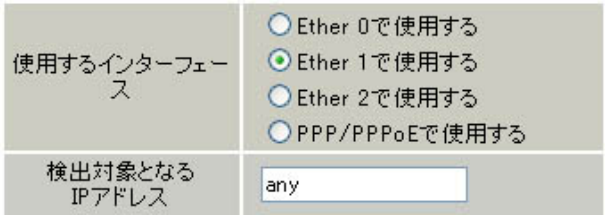
攻撃検出機能とは、外部から LAN への侵入や本装置を踏み台にした他のホスト・サーバ等への攻撃を仕掛けられた時などに、そのログを記録しておくことができる機能です。検出方法には、統計的な面から異常な状態を検出する方法やパターンマッチング方法などがあります。本装置ではあらかじめ検出ルールを定めていますので、パターンマッチングによって不正アクセスを検出します。ホスト単位の他、ネットワーク単位で監視対象を設定できます。

ログの出力

攻撃検出ログも、システムログの中に統合されて出力されますので、「システム設定」内の「ログの表示」やログメール機能で、ログを確認してください。

攻撃検出機能の設定

Web 設定画面「各種サービスの設定」→「攻撃検出サービス」をクリックして、以下の画面で設定します。



○使用するインタフェース
DoS の検出をおこなうインタフェースを選択します。PPPoE/PPP 接続しているインタフェースで検出する場合は「PPP/PPPoE で使用する」を選択してください。

○検出対象となる IP アドレス
攻撃を検出する、本装置のインタフェースの IP アドレスネットワークアドレスを指定します。

< 入力例 >
ホスト単体の場合　***192.168.0.1/32***（”/32”を付ける）
ネットワーク単位の場合　***192.168.0.0/24***（”/ネットマスク”を付ける）

「any」と入力すると、すべてのアドレスが検出対象となります。そのため通常のアクセスも攻撃として誤検知する場合があります。

入力が終わりましたら「設定の保存」をクリックして設定完了です。**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合は、サービスの再起動をおこなってください。**

第 19 章

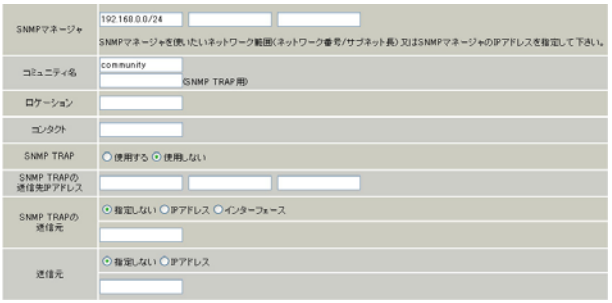
SNMP エージェント機能

第 19 章 SNMP エージェント機能

Ⅰ．SNMP エージェント機能の設定

SNMPエージェントを起動すると、SNMPマネージャから本装置のMIB Ver.2(RFC1213)および、プライベートMIBの情報を取得することができます。

Web 設定画面「各種サービス設定」→「SNMP サービス」をクリックして、以下の画面で設定します。



○ SNMP マネージャ
SNMP マネージャを使いたいネットワーク範囲（ネットワーク番号 / サブネット長）または、SNMP マネージャの IP アドレスを指定します。
最大３つまで指定することができます。

○コミュニティ名
任意のコミュニティ名を指定します。
ご使用の SNMP マネージャの設定に合わせて入力してください。
Get/Response 用と Trap 用とそれぞれ異なるコミュニティ名が設定可能です。

○ロケーション
装置の設置場所を表す標準 MIB“ sysLocation ”(oid=.1.3.6.1.2.1.1.6.0)に、任意のロケーション名を設定することができます。

○コンタクト
装置管理者の連絡先を表す標準 MIB“ sysContact ”(oid=.1.3.6.1.2.1.1.4.0)に、任意の連絡先情報を設定することができます。

○ SNMP TRAP
「使用する」を選択すると、SNMP TRAP を送信できるようになります。

○ SNMP TRAP の送信先 IP アドレス
SNMP TRAP を送信する先(SNMP マネージャ)の IP アドレスを指定します。
最大３つまで指定することができます。

○ SNMP TRAP の送信元
SNMP パケット内の ” Agent Address ” に、任意のインタフェースアドレスを指定することができます。

「指定しない」を選択した場合
SNMP TRAP の送信元アドレスが自動的に設定されます。

「IP アドレス」を選択した場合
SNMP TRAP の送信元アドレスを指定します。

「インタフェース」を選択した場合
SNMP TRAPの送信元アドレスとなるインタフェース名を指定します。
指定可能なインタフェースは、本装置のイーサネットポートと PPP インタフェースのみです。

○送信元
SNMP RESPONSE パケットの送信元アドレスを設定できます。
IPsec 接続を通して、リモート拠点のマネージャから SNMP を取得したい場合は、ここに IPsecSA の LAN 側アドレスを指定してください。
通常の LAN 内でマネージャを使用する場合には設定の必要はありません。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動させてください。
なお、設定を変更した場合は、即時設定が反映されますが、「SNMP TRAP の送信元」および「送信元」を変更した場合には、「動作変更」をクリックしてください。

第 19 章 SNMP エージェント機能

Ⅰ．SNMP エージェント機能の設定

MIB 項目について

以下の MIB に対応しております。

- MIB II(RFC 1213)
- UCD-SNMP MIB
- RFC2011(IP-MIB)
- RFC2012(TCP-MIB)
- RFC2013(UDP-MIB)
- RFC2863(IF-MIB)

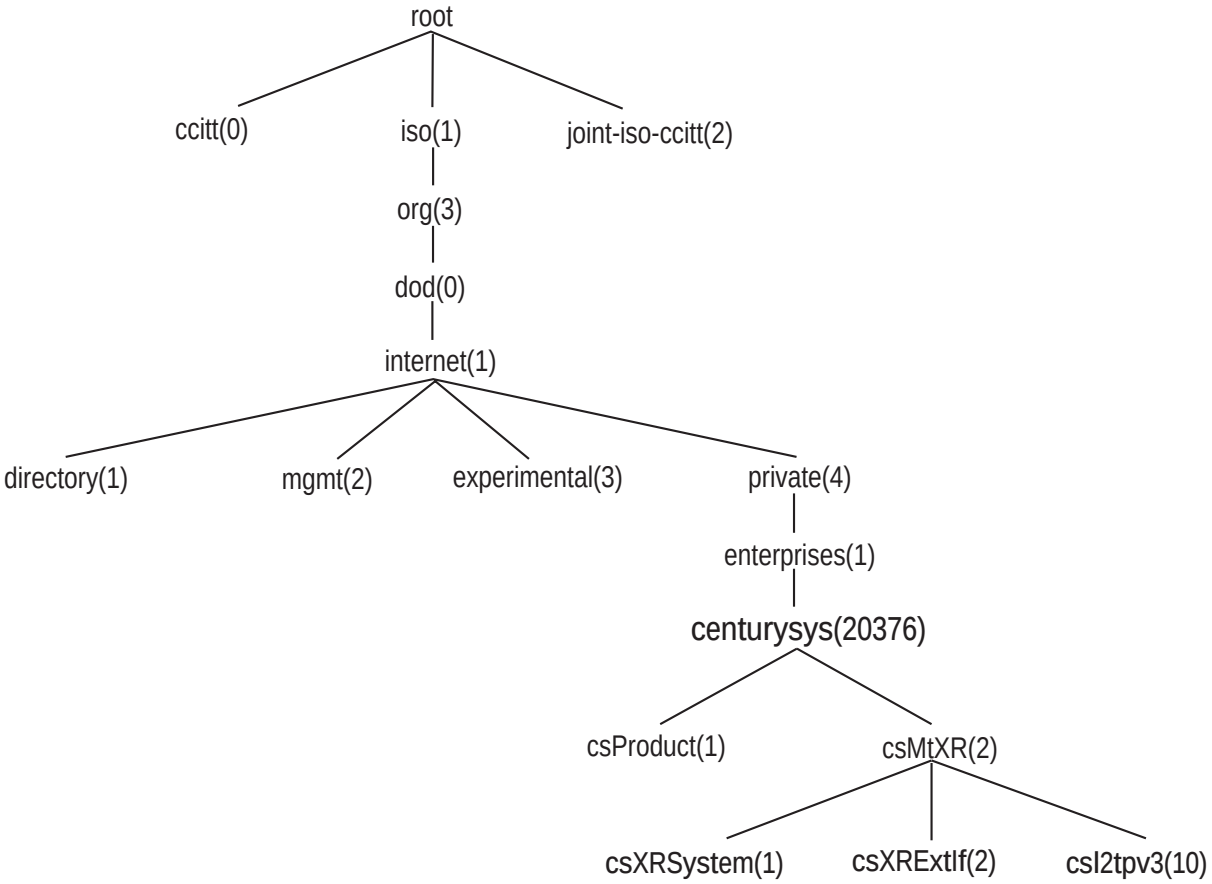
SNMP TRAP を送信するトリガーについて

以下のものに関して、SNMP TRAP を送信します。

- Ethernet インタフェースの up、down
- PPP インタフェースの up、down
- 下記の各機能の up、down
  - DNS
  - DHCP サーバー
  - DHCP リレー
  - PLUTO(IPSec の鍵交換を行う IKE 機能)
  - UPnP
  - RIP
  - OSPF
  - BGP4
  - L2TPv3
  - SYSLOG
  - 攻撃検出
  - NTP
  - VRRP
- SNMP TRAP 自身の起動、停止

II．Century Systems プライベート MIB について

本装置では保守性を高めるために以下のようなプライベートMIB(centurysys)を実装しています。
この MIB 定義の階層下には、XR システム用 MIB(csXRSystem)、XR インタフェース用 MIB(csXRExtIf)、L2TPv3 用 MIB(csl2tpv3)の３つがあります。



■ csXRSystem
システム情報に関する XR 独自の定義 MIB です。
CPU 使用率、空きメモリ量、コネクショントラッキング数、ファンステータスのシステム情報や、サービスの状態に関する情報を定義しています。また、これらに関する Trap 通知用の MIB 定義も含みます。
なお、主なシステム情報 Trap の通知条件は下記の通りです。

- CPU 使用率：90% 超過時
- 空きメモリ量：2MB 低下時
- コネクショントラッキング：総数の 90% 超過時

■ csXRExtIf
インタフェースに関する XR 独自の定義 MIB です。
各インタフェースの状態や IP アドレス情報などを定義しています。
また、UP/DOWN やアドレス変更時などの Trap 通知用の MIB 定義も含みます。

■ csl2tpv3
L2TPv3 サービスに関する定義 MIB です。Tunnel/Session の状態や、送受信フレームのカウンタ情報などを定義しています。
また、Tunnel/Session の Establish や Down 時などの Trap 通知用の MIB 定義も含みます。

これらの MIB 定義の詳細については、MIB 定義ファイルを参照して下さい。

注) システム、インタフェース、サービスに関する情報は標準 MIB-II でも取得できますが、Trap については全て独自 MIB によって通知されます。

第 20 章

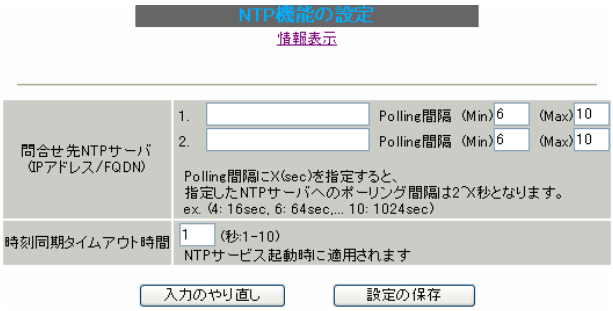
NTP サービス

NTP サービスの設定方法

本装置は、NTP クライアント / サーバ機能を持っています。
インターネットを使った時刻同期の手法の一つである NTP(Network Time Protocol)を用いて NTP サーバと通信をおこない、時刻を同期させることができます。

設定方法

Web 設定画面「各種サービスの設定」→「NTP サービス」をクリックして、以下の画面で NTP 機能の設定をします。



[問合せ先 NTP サーバ（IP アドレス /FQDN)]
○ 1.
○ 2.
NTP サーバの IP アドレスまたは FQDN を、設定「1.」もしくは「2.」に入力します。
NTP サーバの場所は 2 箇所設定できます。
これにより、本装置が NTP クライアント / サーバとして動作できます。

NTP サーバの IP アドレスもしくは FQDN を入力しない場合は、本装置は NTP サーバとしてのみ動作します。

○ Polling 間隔　(Min)/(Max)
NTP サーバと通信をおこなう間隔を設定します。
サーバとの接続状態により、指定した最小値(「Min」)と最大値(「Max」)の範囲でポーリングの間隔を調整します。

Polling 間隔 X(sec)を指定した場合、秒単位での間隔は 2 の X 乗(秒)となります。

＜例 4：16 秒、 6：64 秒、... 10：1024 秒＞

数字は、4～17(16-131072 秒)の間で設定出来ます。

Polling 間隔の初期設定は「Min」6（64 秒)、「Max」10（1024 秒）です。
初期設定のまま NTP サービスを起動させると、はじめは 64 秒間隔で NTP サーバとポーリングをおこない、その後は 64 秒から 1024 秒の間で NTP サーバとポーリングをおこない、時刻のずれを徐々に補正していきます。

[時刻同期タイムアウト時間]
サーバ応答の最大待ち時間を 1-10 秒の間で設定できます。

注）時刻同期の際、内部的には NTP サーバに対する時刻情報のサンプリングを 4 回おこなっています。
本装置から NTP サーバへの同期がおこなえない状態では、サービス起動時に NTP サーバの 1 設定に対し「(指定したタイムアウト時間)×4」秒程度の同期処理時間が掛かる場合があります。

入力が終わりましたら「設定の保存」をクリックして設定完了です。
機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動してください。
また設定を変更した場合は、サービスの再起動をおこなってください。

○情報表示
クリックすると、現在の NTP サービスの動作状況を確認できます。

NTP サービスの設定方法

基準 NTP サーバについて

基準となる NTP サーバには次のようなものがあります。

- ntp1.jst.mfeed.ad.jp (210.173.160.27)
- ntp2.jst.mfeed.ad.jp (210.173.160.57)
- ntp3.jst.mfeed.ad.jp (210.173.160.87)

(注) サーバを FQDN で指定するときは、各種サービス設定の「DNS サーバ」を起動しておきます。

NTP クライアントの設定方法

各ホスト / サーバーを NTP クライアントとして本装置と時刻同期させる方法は、OS により異なります。

○ Windows 9x/Me/NT の場合

これらの OS では NTP プロトコルを直接扱うことができません。フリーウェアの NTP クライアント・アプリケーション等を入手してご利用下さい。

○ Windows 2000 の場合

「net time」コマンドを実行することにより時刻の同期を取ることができます。コマンドの詳細については Microsoft 社にお問い合わせ下さい。

○ Windows XP の場合

Windows 2000 と同様のコマンドによるか、「日付と時刻のプロパティ」で NTP クライアントの設定ができます。詳細については Microsoft 社にお問い合わせください。

○ Macintosh の場合

コントロールパネル内の NTP クライアント機能で設定してください。詳細は Apple 社にお問い合わせください。

○ Linux の場合

Linux 用 NTP サーバをインストールして設定してください。詳細は NTP サーバの関連ドキュメント等をご覧下さい。

第 21 章

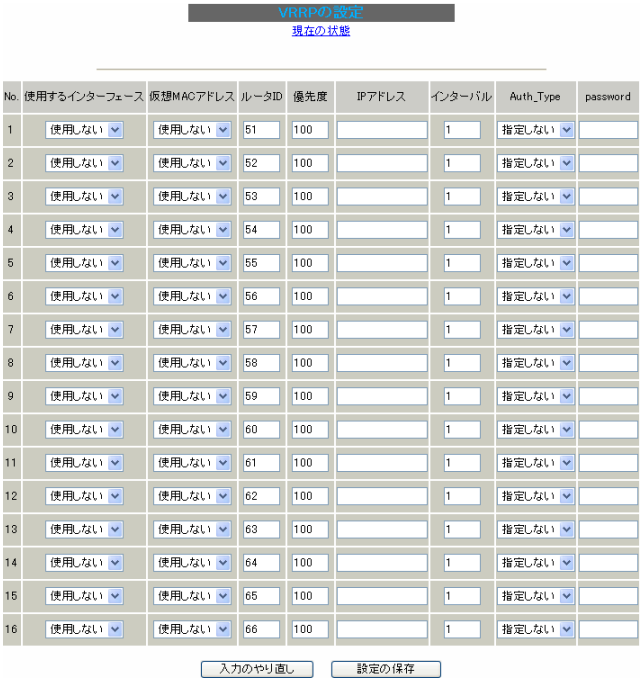
VRRP 機能

VRRP の設定方法

VRRP は動的な経路制御ができないネットワーク環境において、複数のルータのバックアップ(ルータの多重化)をおこなうためのプロトコルです。

設定方法

「各種サービスの設定」→「VRRP サービス」をクリックして以下の画面で VRRP サービスの設定をします。



○使用するインターフェース
VRRP を作動させるインタフェースを選択します。

○仮想 MAC アドレス
VRRP 機能を運用するときに、仮想 MAC アドレスを使用する場合は「使用する」を選択します。
１つのインタフェースにつき、設定可能な仮想 MAC アドレスは１つです。
「使用しない」設定の場合は、本装置の実 MAC アドレスを使って VRRP が動作します。

○ルータ ID
VRRP グループの ID を入力します。
他の設定 No. と同一のルータ ID を設定すると、同一の VRRP グループに属することになります。
ID が異なると、違うグループと見なされます。

○優先度
VRRP グループ内での優先度を 1～255 の間で設定します。数字が大きい方が優先度が高くなります。
優先度の値が最も大きいものが、VRRP グループ内での「マスタールータ」となり、他のルータは「バックアップルータ」となります。

○ IP アドレス
VRRP ルータとして作動するときの仮想 IP アドレスを設定します。
VRRP を作動させている環境では、各ホストはこの仮想 IP アドレスをデフォルトゲートウェイとして指定してください。

○インターバル
VRRP パケットを送出する間隔を設定します。
単位は秒です。1～255 の間で設定します。
VRRP パケットの送受信によって、VRRP ルータの状態を確認します。
※ 仮想 MAC アドレスを使用する場合、インターバルは５秒に設定してください。

○ Auth_Type
「指定しない」か、「PASS」認証を使用するかを選択します。

○ password
認証をおこなう場合のパスワードを設定します。
設定できる文字数は半角英数字で 1～8 文字です。
Auth_Type を「指定しない」にした場合は、パスワードは設定しません。

入力が終わりましたら「設定の保存」をクリックして設定完了です。
機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動させてください。
また設定を変更した場合には、サービスの再起動をおこなってください。

ステータスの表示

VRRP 機能設定画面上部にある「現在の状態」をクリックすると、VRRP 機能の動作状況を表示するウィンドウがポップアップします。

第 22 章

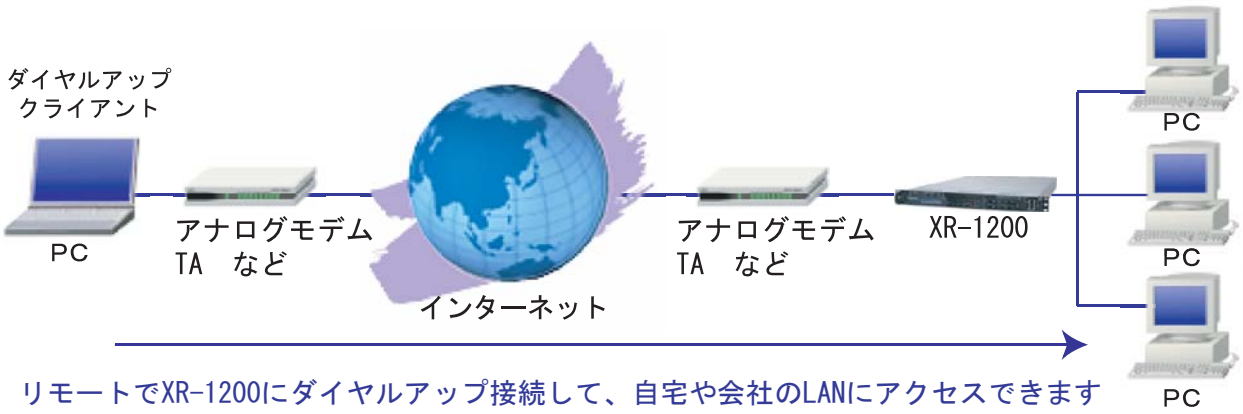
アクセスサーバ機能

第 22 章 アクセスサーバ機能

Ⅰ．アクセスサーバ機能について

アクセスサーバとは、電話回線などを使った外部からの接続要求を受けて、LAN に接続する機能です。例えば、アクセスサーバとして設定した本装置を会社に設置すると、モデムを接続した外出先のコンピュータから会社の LAN に接続できます。これは、モバイルコンピューティングや在宅勤務を可能にします。クライアントはモデムによる PPP 接続を利用できるものであれば、どのような PC でもかまいません。この機能を使って接続したクライアントは、接続先のネットワークにハブで接続した場合と同じようにネットワークを利用できます。

セキュリティは、ユーザー ID・パスワード認証によって確保します。ユーザー ID・パスワードは、最大 5 アカウント分を登録できます。



II．本装置とアナログモデム /TA の接続

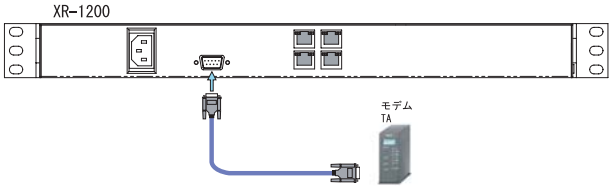
アクセスサーバ機能を設定する前に、本装置とアナログモデムや TA を接続します。以下のように接続してください。

◆アナログモデム /TA の接続

1 本装置本体背面の「RS-232」ポートとアナログモデム /TA のシリアルポートをシリアルケーブルで接続してください。シリアルケーブルは別途ご用意ください。

2 全ての接続が完了しましたら、モデム /TA の電源を投入してください。

接続図



III．アクセスサーバ機能の設定

Web 設定画面「各種サービスの設定」→「アクセスサーバ」をクリックして設定します。

○着信
シリアル回線で着信したい場合は「許可する」を選択します。

○アクセスサーバ(本装置)の IP アドレス
ダイヤルアップされた時の本装置自身の IP アドレスを入力します。各 Ethernet ポートのアドレスとは異なるプライベートアドレスを設定してください。***なお、サブネットマスクビット値は 24 ビット(255.255.255.0)に設定されています。***

○クライアントの IP アドレス
本装置にダイヤルアップしてきたホストに割り当てる IP アドレスを入力します。上記の「アクセスサーバの IP アドレス」で設定したものと同じネットワークとなるアドレスを設定してください。

○モデムの速度
本装置とモデムの間の通信速度を選択します。

○着信のための AT コマンド
モデムが外部から着信する場合、AT コマンドが必要な場合があります。その場合は、ここで AT コマンドを入力してください。コマンドについては、各モデムの説明書をご確認ください。多くの場合、コマンドの入力は必要有りません。

続けてユーザーアカウントの設定をおこないます。

ユーザーアカウントの設定

設定画面の下側でユーザーアカウントの設定をおこないます。

No.	アカウント	パスワード	アカウント毎に別IPを割り当てる場合		削除
			本装置のIP	クライアントのIP	
1					☐
2					☐
3					☐
4					☐
5					☐

外部からダイヤルアップする場合の、ユーザーアカウントとパスワードを登録してください。そのまま、ダイヤルアップ時のユーザーアカウント・パスワードとなります。5 アカウントまで登録しておけます。

入力後、「設定の保存」をクリックしてください。設定が反映されます。
アカウント設定覧の「削除」ラジオボックスにチェックして「設定 / 削除の実行」をクリックすると、その設定が削除されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

III．アクセスサーバ機能の設定

◆スタティックルートを設定する場合

通常のスタティックルート設定では「インタフェース / ゲートウェイ」のどちらかひとつの項目のみ設定可能ですが、アクセスサーバ機能で着信するインタフェース向けにスタティックルート設定を行う場合は、以下の両項目ともに設定が必要になりますのでご注意下さい。

インタフェース：ppp6（固定）
ゲートウェイ：アクセスサーバ設定画面にて指定した着信時のクライアントの IP アドレス

設定例

前ページ「シリアル回線」設定画面のスタティックルート設定例です。

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ		ディスタンス<1-255>
1	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	ppp6	192.168.253.170	1

第 23 章

スタティックルート設定

第 23 章 スタティックルート設定

スタティックルート設定方法

Web 設定画面「スタティックルート設定」をクリックして、以下の画面から設定します。

入力方法

○ホスト / ネットワーク
ルーティング先が、単一ホストかネットワークかを選択します。

○アドレス
あて先ホストのアドレス、またはネットワークアドレスを入力します。

○ネットマスク
あて先ネットワークのサブネットマスクを入力します。IP アドレス形式で入力してください。

入力例 ： ***255.255.255.248*** (29 ビットマスク)

また、あて先アドレスを単一ホストで指定した場合には、「255.255.255.255」と入力します。

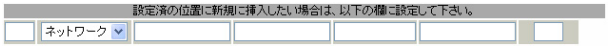
○インタフェース / ゲートウェイ
ルーティングをおこなうインタフェース名、もしくは上位ルータの IP アドレスのどちらかを設定します。
本装置のインタフェース名については、本マニュアルの**「付録 A インタフェース名一覧」**をご参照ください。

○ディスタンス
経路選択の優先順位を指定します。1 ～ 255 の間で指定します。値が低いほど優先度が高くなります。
スタティックルートのデフォルトディスタンス値は 1 です。
ディスタンス値を変更することで、フローティングスタティックルート設定とすることも可能です。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

設定を挿入する

ルーティング設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。



最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

スタティックルート設定方法

設定を削除する

ルーティング設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

デフォルトルートを設定する

スタティックルート設定でデフォルトルートを設定するときは、「アドレス」と「ネットマスク」項目をいずれも ”0.0.0.0 ” として設定してください。

ルーティング情報を確認する

現在のルーティング情報を確認するには、設定画面上部にある「経路情報表示」をクリックします。ウィンドウがポップアップし、経路情報が確認できます。
” inactive ” と表示されている経路は、その時点では有効な経路ではなく、無視されます。

表示されていないものに関しては、正しい設定ではありません。設定をご確認のうえ、再度設定してください。

第 24 章

ソースルート機能

第 24 章　ソースルート機能

ソースルート設定

通常のダイナミックルーティングおよびスタティックルーティングでは、パケットのあて先アドレスごとにルーティングを行ないますが、ソースルーティングはパケットの送信元アドレスをもとにルーティングをおこないます。

このソースルート機能を使うことで、外部へアクセスするホスト / ネットワークごとにアクセス回線を選択することができますので、複数のインターネット接続をおこなって負荷分散が可能となります。

ソースルート設定は、設定画面「ソースルート設定」でおこないます。

1　はじめに、ソースルートのテーブル設定をおこないます。「ソースルートのテーブル設定へ」をクリックしてください。

テーブルNO	IP	DEVICE
1		
2		
3		
4		
5		
6		
7		
8		

○ IP
デフォルトゲートウェイ(上位ルータ)の IP アドレスを設定します。必ず明示的に設定しなければなりません。

○ DEVICE
デフォルトゲートウェイが存在する回線に接続しているインタフェースのインタフェース名を設定します(情報表示で確認できます。”eth0 ”や ”ppp0 ”などの表記のものです)。省略することもできます。

設定後は「設定の保存」をクリックします。

2　画面右上の「ソースルートのルール設定へ」をクリックします。

ルールNO	送信元ネットワークアドレス	送信先ネットワークアドレス	ソースルートのテーブルNO
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

○送信元ネットワークアドレス
送信元のネットワークアドレスもしくはホストの IP アドレスを設定します。ネットワークアドレスで設定する場合は、
　ネットワークアドレス / マスクビット値
の形式で設定してください。

○送信先ネットワークアドレス
送信先のネットワークアドレスもしくはホストの IP アドレスを設定します。ネットワークアドレスで設定する場合は、
　ネットワークアドレス / マスクビット値
の形式で設定してください。

○ソースルートのテーブル No.
使用するソースルートテーブルの番号(1 ～ 8)を設定します。

最後に「設定の保存」をクリックして設定完了です。

※送信元ネットワークアドレスをネットワークアドレスで指定した場合、そのネットワークに本装置のインタフェースが含まれていると、設定後は本装置の設定画面にアクセスできなくなります。

<例 >Ether0 ポートの IP アドレスが 192.168.0.254 で、送信元ネットワークアドレスを 192.168.0.0/24 と設定すると、192.168.0.0/24 内のホストは本装置の設定画面にアクセスできなくなります。

第 25 章

NAT 機能

第 25 章　NAT 機能

Ⅰ．本装置の NAT 機能について

NAT(Network Address Translation)は、プライベートアドレスをグローバルアドレスに変換してインターネットにアクセスできるようにする機能です。また 1 つのプライベートアドレス・ポートと、1 つのグローバルアドレス・ポートを対応させて、インターネット側から LAN のサーバへアクセスさせることもできます。

本装置は以下の 3 つの NAT 機能をサポートしています。

◆ IP マスカレード機能
複数のプライベートアドレスを、ある 1 つのグローバルアドレスに変換する機能です。グローバルアドレスは本装置のインターネット側ポートに設定されたものを使います。また LAN のプライベートアドレス全てが変換されることになります。この機能を使うと、グローバルアドレスを 1 つしか持っていなくても複数のコンピュータからインターネットにアクセスすることができるようになります。

なお IP マスカレード(NAT 機能)では、プライベートアドレスからグローバルアドレスだけではなく、プライベートアドレスからプライベートアドレス、グローバルアドレスからグローバルアドレスの変換も可能です。IP マスカレード機能については、「インタフェース設定」もしくは「PPP/PPPoE 接続」の接続設定画面で設定します。

◆送信元 NAT 機能
IP マスカレードとは異なり、プライベートアドレスをどのグローバル IP アドレスに変換するかをそれぞれ設定できるのが送信元 NAT 機能です。例えば、プライベートアドレスＡをグローバルアドレスＸに、プライベートアドレスＢをグローバルアドレスＹに、プライベートアドレスＣからＦをグローバルアドレスＺに変換する、といった設定が可能になります。IP マスカレード機能を設定せずに送信元 NAT 機能だけを設定した場合は、送信元 NAT 機能で設定されたアドレスを持つコンピュータしかインターネットにアクセスできません。

◆バーチャルサーバ機能
インターネット上から LAN 上のサーバ等にアクセスさせることができる機能です。通常はインターネット側から LAN へアクセスする事はできませんが、送信先グローバルアドレスをプライベートアドレスへ変換する設定をおこなうことで、見かけ上はインターネット上のサーバへアクセスできているかのようにすることができます。設定上で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 で関連づけます。また同時に、プロトコルと TCP/UDP ポート番号も指定しておきます。ここで指定したプロトコル・TCP/UDP ポート番号でアクセスされた時にグローバルアドレスからプライベートアドレスへ変換され、LAN 上のサーバに転送されます。

これらの NAT 機能は同時に設定・運用が可能です。

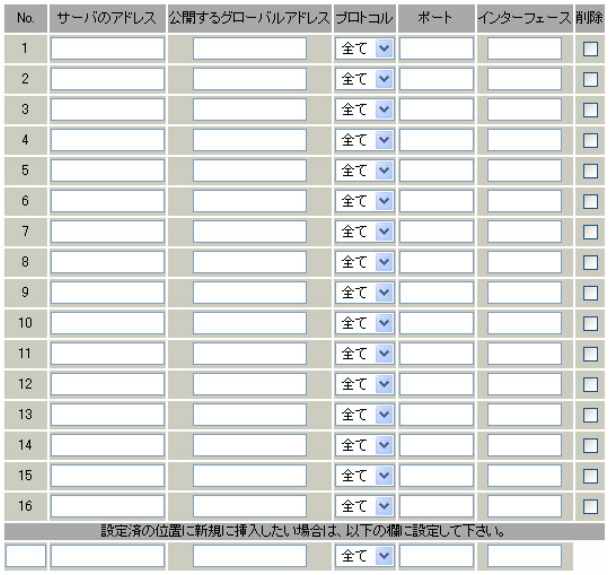
NetMeeting や各種 IM、ネットワークゲームなど、独自のプロトコル・ポートを使用しているアプリケーションについては、NAT 機能を使用すると正常に動作しない場合があります。原則として、NAT を介しての個々のアプリケーションの動作についてはサポート対象外とさせていただきます。

II．バーチャルサーバ設定

NAT 環境下において、LAN からサーバを公開するときなどの設定をおこないます。

設定方法

Web 設定画面「NAT 設定」→「バーチャルサーバ」をクリックして、以下の画面から設定します。



○サーバのアドレス
インターネットに公開するサーバの、プライベート IP アドレスを入力します。

○公開するグローバルアドレス
サーバのプライベート IP アドレスに対応させるグローバル IP アドレスを入力します。インターネットからはここで入力したグローバル IP アドレスでアクセスします。
プロバイダから割り当てられている IP アドレスが一つだけの場合は、ここは空欄にします。

○プロトコル
サーバのプロトコルを選択します。

○ポート
サーバが公開するポート番号を入力します。範囲で指定することも可能です。範囲で指定するときは、ポート番号を ":" で結びます。

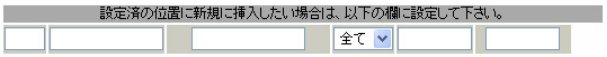
<例> ポート 20 番から 21 番を指定する → ***20:21***

○インタフェース
インターネットからのアクセスを受信するインタフェース名を指定します。本装置のインタフェース名については、本マニュアルの**「付録 A インタフェース名一覧」**をご参照下さい。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
"No." 項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。



最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

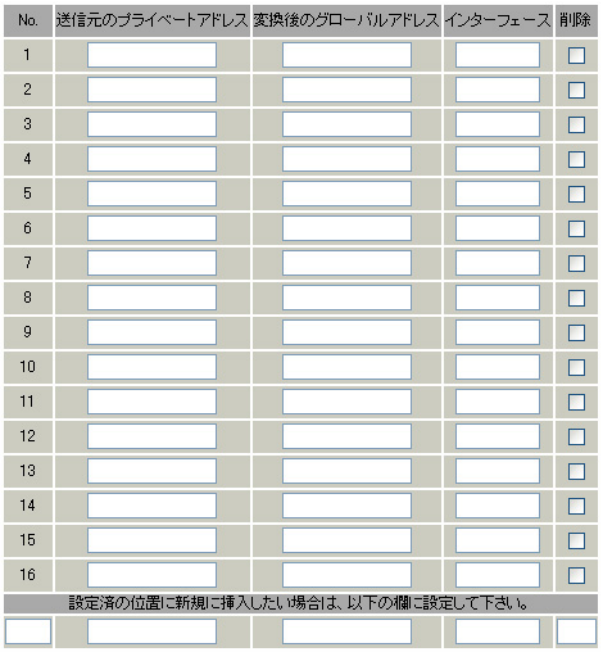
設定を削除する

バーチャルサーバ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

III．送信元 NAT 設定

設定方法

Web 設定画面「NAT 設定」→「送信元 NAT」をクリックして、以下の画面から設定します。



○送信元のプライベートアドレス
NAT の対象となる LAN 側コンピュータのプライベート IP アドレスを入力します。ネットワーク単位での指定も可能です。

○変換後のグローバルアドレス
プライベート IP アドレスの変換後のグローバル IP アドレスを入力します。送信元アドレスをここで入力したアドレスに書き換えてインターネット(WAN)へアクセスします。

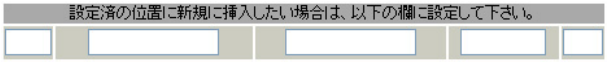
○インタフェース
どのインタフェースからインターネット(WAN)へアクセスするか、インタフェース名を指定します。インターネット(WAN)につながっているインタフェースを設定してください。本装置のインタフェース名については、本マニュアルの**「付録 A インタフェース名一覧」**をご参照下さい。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

”No.”項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

設定を挿入する

送信元 NAT 設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。



最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

設定を削除する

送信元 NAT 設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

Ⅳ．バーチャルサーバの設定例

◆WWW サーバを公開する際の NAT 設定例

NAT の条件

・WAN 側のグローバルアドレスに TCP のポート 80 番(http)でのアクセスを通す。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続。

LAN 構成

・LAN 側ポートの IP アドレス「192.168.0.254」
・WWW サーバのアドレス「192.168.0.1」
・グローバルアドレスは「211.xxx.xxx.102」のみ

設定画面での入力方法

・あらかじめ IP マスカレードを有効にします。
・「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.1	211.xxx.xxx.102	tcp	80	eth1

設定の解説

No.1 ：
WAN 側から、211.xxx.xxx.102 へポート 80 番(http)でアクセスがあれば、LAN 内のサーバ 192.168.0.1 へ通す。(WAN 側から TCP のポート 80 番以外でアクセスがあっても破棄される)

◆FTP サーバを公開する際の NAT 設定例

NAT の条件

・WAN 側のグローバルアドレスに TCP のポート 20 番(ftpdata)、21 番(ftp)でのアクセスを通す。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続する。
・Ether1 ポートは PPPoE で ADSL 接続する。

LAN 構成

・LAN 側ポートの IP アドレス「192.168.0.254」
・FTP サーバのアドレス「192.168.0.2」
・グローバルアドレスは「211.xxx.xxx.103」のみ

設定画面での入力方法

・あらかじめ IP マスカレードを有効にします。
・「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.2	211.xxx.xxx.103	tcp	20	ppp0
192.168.0.2	211.xxx.xxx.103	tcp	21	ppp0

設定の解説

No.1 ：
WAN 側から、211.xxx.xxx.103 へポート 21 番(ftp)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。

No.2 ：
WAN 側から、211.xxx.xxx.103 へポート 20 番(ftpdata)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。

Ⅳ．バーチャルサーバの設定例

◆PPTP サーバを公開する際の NAT 設定例

NAT の条件

・WAN 側のグローバルアドレスにプロトコル「gre」と TCP のポート番号 1723 を通す。
・WAN は Ether1、LAN は Ether0 ポートに接続する。
・WAN 側ポートは PPPoE で ADSL 接続する。

LAN 構成

・LAN 側ポートの IP アドレス「192.168.0.254」
・PPTP サーバのアドレス「192.168.0.3」
・割り当てられるグローバルアドレスは 1 つのみ。

設定画面での入力方法

・あらかじめ IP マスカレードを有効にします。
・「バーチャルサーバ設定」で以下の様に設定します。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	削除
192.168.0.3		tcp	1723	ppp0	☐
192.168.0.3		gre		ppp0	☐

Ⅳ．バーチャルサーバの設定例

◆DNS、メール、WWW、FTP サーバを公開する際の NAT 設定例(複数グローバルアドレスを利用)

NAT の条件

- WAN 側からは、LAN 側のメール、WWW,FTP サーバへアクセスできるようにする。
- LAN 内の DNS サーバが WAN と通信できるようにする。
- LAN から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続。
- グローバルアドレスは複数使用する。

LAN 構成

- LAN 側ポートの IP アドレス「192.168.0.254」
- WWW サーバのアドレス「192.168.0.1」
- 送受信メールサーバのアドレス「192.168.0.2」
- FTP サーバのアドレス「192.168.0.3」
- DNS サーバのアドレス「192.168.0.4」
- WWW サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.104」
- 送受信メールサーバに対応させるグローバル IP アドレスは「211.xxx.xxx.105」
- FTP サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.106」
- DNS サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.107」

設定画面での入力方法

1 まず最初に、使用する複数のグローバルアドレスを、仮想インタフェースとして登録します。メニューにある「仮想インタフェース設定」を開き、以下のように設定しておきます。

インターフェース	仮想I/F番号	IPアドレス	ネットマスク
eth1	1	211.xxx.xxx.104	255.255.255.248
eth1	2	211.xxx.xxx.105	255.255.255.248
eth1	3	211.xxx.xxx.106	255.255.255.248
eth1	4	211.xxx.xxx.107	255.255.255.248

2 IP マスカレードを有効にします。

(第 5 章「インタフェース設定」参照)

3 「バーチャルサーバ設定」で以下の様に設定してください。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.1	211.xxx.xxx.104	tcp	80	eth1
192.168.0.2	211.xxx.xxx.105	tcp	25	eth1
192.168.0.2	211.xxx.xxx.105	tcp	110	eth1
192.168.0.3	211.xxx.xxx.106	tcp	20	eth1
192.168.0.3	211.xxx.xxx.106	tcp	21	eth1
192.168.0.4	211.xxx.xxx.107	tcp	53	eth1
192.168.0.4	211.xxx.xxx.107	udp	53	eth1

設定の解説

No.1
WAN 側から 211.xxx.xxx.104 へポート 80 番(http)でアクセスがあれば、LAN 内のサーバ 192.168.0.1 へ通す。

No.2、3
WAN 側から 211.xxx.xxx.105 へポート 25 番(smtp)か 110 番(pop3)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。

No.4、5
WAN 側から 211.xxx.xxx.106 へポート 20 番(ftpdata)か 21 番(ftp)でアクセスがあれば、LAN 内のサーバ 192.168.0.3 へ通す。

No.6、7
WAN 側から 211.xxx.xxx.107 へ、tcp ポート 53 番(domain)か udp ポート 53 番(domain)でアクセスがあれば LAN 内のサーバ 192.168.0.4 へ通す。

複数のグローバルアドレスを使ってバーチャルサーバ設定をおこなうときは、必ず「仮想インタフェース機能」において使用するグローバルアドレスを設定しておく必要があります。

Ⅴ．送信元 NAT の設定例

送信元 NAT 設定では、LAN 側のコンピュータのアドレスをどのグローバルアドレスに変換するかを個々に設定することができます。

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.0.1	61.xxx.xxx.101	ppp0
192.168.0.2	61.xxx.xxx.102	ppp0
192.168.10.0/24	61.xxx.xxx.103	ppp0

例えば上記のような送信元 NAT 設定をおこなうと、

・送信元アドレス 192.168.0.1 を 61.xxx.xxx.101 に変換して WAN へアクセスする

・送信元アドレス 192.168.0.2 を 61.xxx.xxx.102 に変換して WAN へアクセスする

・送信元アドレスとして 192.168.10.0/24 からのアクセスを 61.xxx.xxx.103 に変換して WAN へアクセスする

という設定になります。

送信元のアドレスは、ホスト単位かネットワーク単位で指定できます。範囲指定はできません。ネットワークで指定するときは、以下のように設定して下さい。

＜設定例＞　***192.168.254.0/24***

> 複数のグローバルアドレスを使って送信元NAT設定をおこなうときは、必ず「仮想インタフェース機能」で設定しておく必要がありますので、ご注意下さい。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

第 26 章

パケットフィルタリング機能

第 26 章 パケットフィルタリング機能

Ⅰ．機能の概要

本装置はパケットフィルタリング機能を搭載しています。
パケットフィルタリング機能を使うと、以下のようなことができます。

- 外部から LAN に入ってくるパケットを制限する。
- LAN から外部に出ていくパケットを制限する。
- 本装置自身が受信するパケットを制限する。
- 本装置自身から送信するパケットを制限する。
- Web 認証機能を使用しているときにアクセス可能にする。

またフィルタリングは以下の情報に基づいて条件を設定することができます。

- インタフェース
- 入出力方向(入力 / 転送 / 出力)
- プロトコル(TCP/UDP/ICMP など), プロトコル番号
- 送信元 / あて先 IP アドレス
- 送信元 / あて先ポート番号

パケットフィルタリング機能を有効にすると、パケットを単にルーティングするだけでなく、パケットのヘッダ情報を調べて、送信元やあて先の IP アドレス、プロトコルの種類(TCP/UDP/ICMP など、またはプロトコル番号)、ポート番号に基づいてパケットを通過させたり破棄させることができます。

このようなパケットフィルタリング機能は、コンピュータやアプリケーション側の設定を変更する必要がないために、個々のコンピュータでパケットフィルタの存在を意識することなく、簡単に利用できます。

※ Xconnect Interface に指定されたインタフェースは、フィルタ設定を適用することができません。L2TP セッション間でのフィルタリングを設定するには、「第 16 章 L2TPv3 フィルタ機能」を参考にしてください。

II．本装置のフィルタリング機能について

本装置は、以下の 4 つの基本ルールについてフィルタリングの設定をおこないます。

- 入力(input)
- 転送(forward)
- 出力(output)
- Web 認証(authgw)

◆入力(input)フィルタ
外部から本装置自身に入ってくるパケットに対して制御します。
インターネットや LAN から本装置へのアクセスについて制御したい場合には、この入力ルールにフィルタ設定をおこないます。

◆転送(forward)フィルタ
LAN からインターネットへのアクセスや、インターネットから LAN 内サーバへのアクセス、LAN から LAN へのアクセスなど、本装置で内部転送する(本装置がルーティングする)アクセスを制御するという場合には、この転送ルールにフィルタ設定をおこないます。

◆出力(output)フィルタ
本装置内部からインターネットや LAN などへのアクセスを制御したい場合には、この出力ルールにフィルタ設定をおこないます。
パケットが「転送されるもの」か「本装置自身へのアクセス」か「本装置自身からのアクセス」かをチェックしてそれぞれのルールにあるフィルタ設定を実行します。

◆Web 認証(authgw)フィルタ
「Web 認証機能」を使用しているときに設定するフィルタです。
Web 認証を必要とせずに外部と通信可能にするフィルタ設定をおこないます。
Web 認証機能については「第 31 章 Web 認証機能」をご覧ください。

各ルール内のフィルタ設定は先頭から順番にマッチングされ、最初にマッチした設定がフィルタとして動作することになります。逆に、マッチするフィルタ設定が見つからなければそのパケットはフィルタリングされません。

フィルタの初期設定について
本装置の工場出荷設定では、「入力フィルタ」と「転送フィルタ」において、以下のフィルタ設定がセットされています。

- NetBIOS を外部に送出しないフィルタ設定
- 外部から UPnP で接続されないようにするフィルタ設定

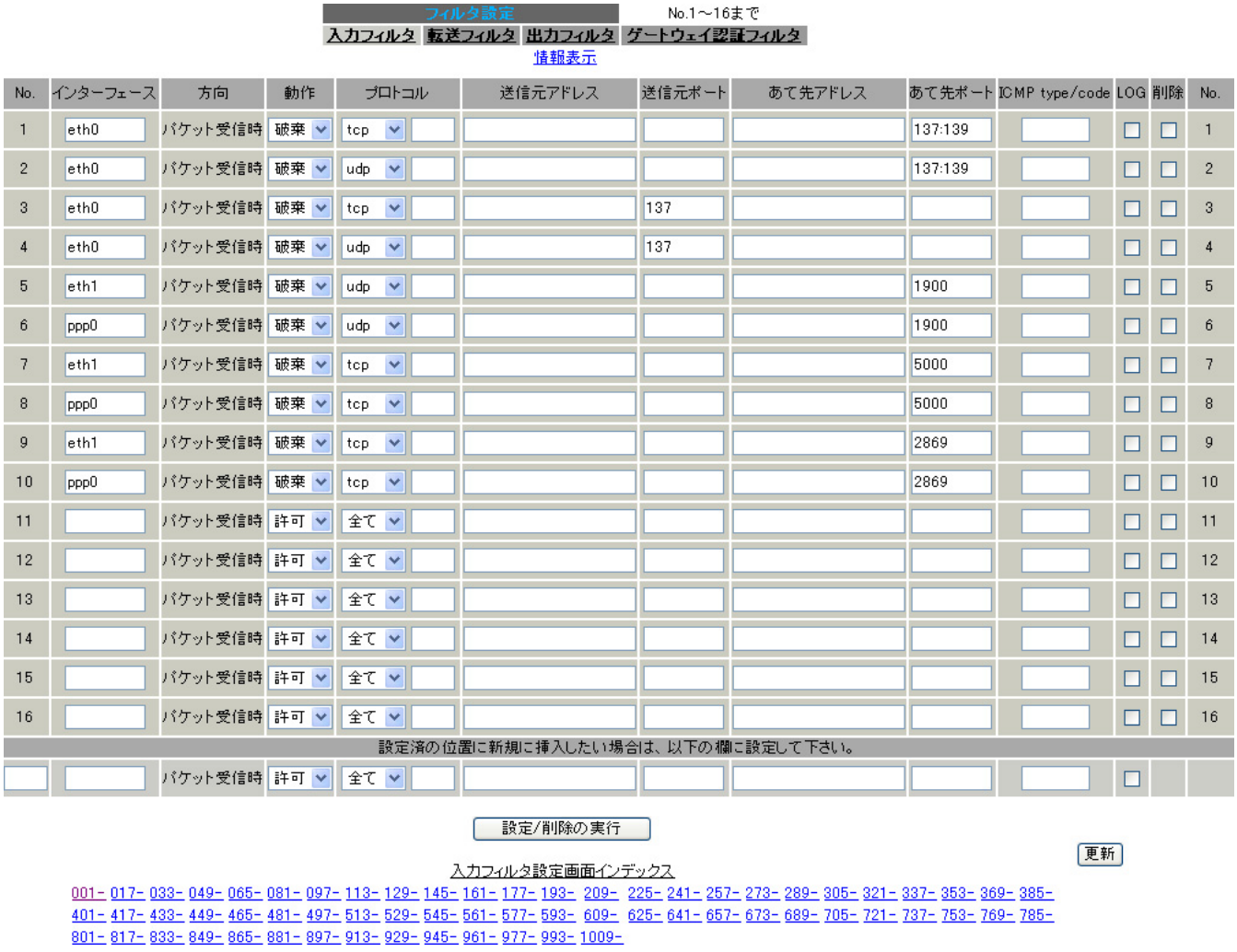
Windows ファイル共有をする場合は、NetBIOS 用のフィルタを削除してお使いください。

III．パケットフィルタリングの設定

フィルタは、入力・転送・出力・Web 認証の 4 種類ありますが、設定方法はすべて同様となります。
設定可能な各フィルタの最大数は 1024 です。
各フィルタ設定画面の最下部にある「フィルタ設定画面インデックス」のリンクをクリックしてください。

設定方法

Web 設定画面「フィルタ設定」→「入力フィルタ」・「転送フィルタ」・「出力フィルタ」・「Web 認証フィルタ」のいずれかをクリックして、以下の画面から設定します。



(画面は「入力フィルタ」です)

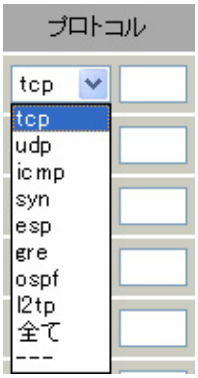
○インターフェース
フィルタリングをおこなうインタフェース名を指定します。本装置のインタフェース名については、本マニュアルの「付録 A」をご参照ください。

○方向
ポートがパケットを受信するときにフィルタリングするか、送信するときにフィルタリングするかを選択します。
入力フィルタでは「パケット受信時」、出力フィルタでは「パケット送信時」のみとなります。

III．パケットフィルタリングの設定

○動作
フィルタリング設定にマッチしたときにパケットを破棄するか通過させるかを選択します。

○プロトコル
フィルタリング対象とするプロトコルを選択します。
右側の空欄でプロトコル番号による指定もできます。
ポート番号も指定する場合は、ここで必ずプロトコルを選択しておいてください。



○送信元アドレス
フィルタリング対象とする、送信元の IP アドレスを入力します。
ホストアドレスのほか、ネットワークアドレス、FQDN での指定が可能です。

< 入力例 >
単一の IP アドレスを指定する：
192.168.253.19
192.168.253.19/32
(“ アドレス /32 ” の書式 “ /32 ” は省略可能です。)

ネットワーク単位で指定する：
192.168.253.0/24
(“ ネットワークアドレス / マスクビット値 ” の書式)

○送信元ポート
フィルタリング対象とする、送信元のポート番号を入力します。
範囲での指定も可能です。範囲で指定するときは “ : ” でポート番号を結びます。

< 入力例 >
ポート 1024 番から 65535 番を指定する場合。
1024:65535

ポート番号を指定するときは、プロトコルも合わせて選択しておかなければなりません。
(「全て」のプロトコルを選択して、ポート番号を指定することはできません。)

○あて先アドレス
フィルタリング対象とする、あて先の IP アドレスを入力します。
ホストアドレスのほか、ネットワークアドレス、FQDN での指定が可能です。
入力方法は、送信元 IP アドレスと同様です。

○あて先ポート
フィルタリング対象とする、あて先のポート番号を入力します。
範囲での指定も可能です。
指定方法は送信元ポート同様です。

○ ICMP type/code
プロトコルで「icmp」を選択した場合に、ICMP の type/code を指定することができます。
プロトコルで「icmp」以外を選択した場合は指定できません。

○ LOG
チェックを入れると、そのフィルタ設定に合致したパケットがあったとき、そのパケットの情報を syslog に出力します。
許可 / 破棄いずれの場合も出力します。

○削除
フィルタ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れてください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

” No. ” 項目が赤字で表示されている行は入力内容が正しくありません。
再度入力をやり直してください。

III. パケットフィルタリングの設定

○更新ボタン
IP アドレスを FQDN で指定したフィルタの名前解決を手動でおこないます。
通常は、DNS の TTL の値が“ 0 ”になるタイミングで名前解決がおこなわれますが、更新タイミング以外で名前解決をおこないたい場合にクリックしてください。

送信元アドレス、または、あて先アドレスとして FQDN 形式を指定する場合、各フィルタ設定（入力、転送、出力、Web 認証）を含めた指定数の合計は 64 個まで可能とします。
（１行の設定で送信元アドレスとあて先アドレスの両方を FQDN 指定した場合の指定数は 2 です。）

設定を挿入する

フィルタ設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。

（画面は「入力フィルタ」）

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

設定情報の確認

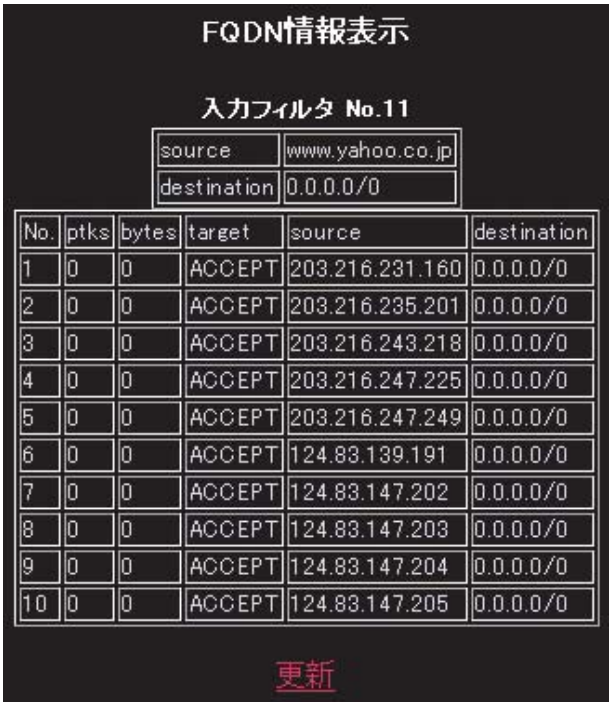
「情報表示」をクリックすると、現在のフィルタ設定の情報が一覧表示されます。

入力フィルタ 情報表示

No.	type	ptks	bytes	target	log	prot	in	out	source	destination		
1	IP	0	0	DROP	-	tcp	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp	dpts:137:139
2	IP	6	468	DROP	-	udp	eth0	*	0.0.0.0/0	0.0.0.0/0	udp	dpts:137:139
3	IP	0	0	DROP	-	tcp	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp	spt:137
4	IP	0	0	DROP	-	udp	eth0	*	0.0.0.0/0	0.0.0.0/0	udp	spt:137
5	IP	0	0	DROP	-	udp	eth1	*	0.0.0.0/0	0.0.0.0/0	udp	dpt:1900
6	IP	0	0	DROP	-	udp	ppp0	*	0.0.0.0/0	0.0.0.0/0	udp	dpt:1900
7	IP	0	0	DROP	-	tcp	eth1	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:5000
8	IP	0	0	DROP	-	tcp	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:5000
9	IP	0	0	DROP	-	tcp	eth1	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:2869
10	IP	0	0	DROP	-	tcp	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:2869
11	FQDN	---	---	ACCEPT	-	tcp	eth1	*	www.yahoo.co.jp	0.0.0.0/0	tcp	dpt:80

更新

IP アドレス指定を FQDN でおこなった場合は、「type」欄の「FQDN」リンクをクリックするとクリックしたフィルタ設定の名前解決した IP アドレス一覧が表示されます。



FQDN情報表示

入力フィルタ No.11

source	www.yahoo.co.jp
destination	0.0.0.0/0

No.	ptks	bytes	target	source	destination
1	0	0	ACCEPT	203.216.231.160	0.0.0.0/0
2	0	0	ACCEPT	203.216.235.201	0.0.0.0/0
3	0	0	ACCEPT	203.216.243.218	0.0.0.0/0
4	0	0	ACCEPT	203.216.247.225	0.0.0.0/0
5	0	0	ACCEPT	203.216.247.249	0.0.0.0/0
6	0	0	ACCEPT	124.83.139.191	0.0.0.0/0
7	0	0	ACCEPT	124.83.147.202	0.0.0.0/0
8	0	0	ACCEPT	124.83.147.203	0.0.0.0/0
9	0	0	ACCEPT	124.83.147.204	0.0.0.0/0
10	0	0	ACCEPT	124.83.147.205	0.0.0.0/0

更新

Ⅳ．パケットフィルタリングの設定例

◆インターネットからLANへのアクセスを破棄する設定

本製品の工場出荷設定では、インターネット側から LAN へのアクセスは全て通過させる設定となっていますので、以下の設定をおこない、外部からのアクセスを禁止するようにします。

フィルタの条件

・WAN 側からは LAN 側へアクセス不可にする。
・LAN から WAN へのアクセスは自由にできる。
・本装置から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続する。
・LAN から WAN へ IP マスカレードをおこなう。
・ステートフルパケットインスペクションは有効。

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス「192.168.0.1」

設定画面での入力方法

「入力フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp					1024:65535
2	eth1	パケット受信時	許可	udp					1024:65535
3	eth1	パケット受信時	許可	---	1				
4	eth1	パケット受信時	破棄	全て					

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp					1024:65535
2	eth1	パケット受信時	許可	udp					1024:65535
3	eth1	パケット受信時	許可	---	1				
4	eth1	パケット受信時	破棄	全て					

フィルタの解説

「入力フィルタ」「転送フィルタ」

No.1、2：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.3：
WAN から来る、ICMP（プロトコル番号“1”）パケットを通す。

No.4：
上記の条件に合致しないパケットを全て破棄する。

Ⅳ．パケットフィルタリングの設定例

◆WWW サーバを公開する際のフィルタ設定例

フィルタの条件

・WAN 側からは LAN 側の WWW サーバにだけアクセス可能にする。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続。
・ステートフルパケットインスペクションは有効。

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス 「192.168.0.254」
・WWW サーバのアドレス 「192.168.0.1」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp				192.168.0.1	80
2	eth1	パケット受信時	許可	tcp					1024:65535
3	eth1	パケット受信時	許可	udp					1024:65535
4	eth1	パケット受信時	破棄	全て					

フィルタの解説

No.1：
192.168.0.1 のサーバに HTTP のパケットを通す。
No.2、3：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。
No.4：
上記の条件に合致しないパケットを全て破棄する。

◆FTP サーバを公開する際のフィルタ設定例

フィルタの条件

・WAN 側からは LAN 側の FTP サーバにだけアクセスが可能にする。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続する。
・NAT は有効。
・Ether1 ポートは PPPoE 回線に接続する。
・ステートフルパケットインスペクションは有効。

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス 「192.168.0.254」
・FTP サーバのアドレス 「192.168.0.2」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp				192.168.0.2	21
2	ppp0	パケット受信時	許可	tcp				192.168.0.2	20
3	ppp0	パケット受信時	許可	tcp					1024:65535
4	ppp0	パケット受信時	許可	udp					1024:65535
5	ppp0	パケット受信時	破棄	全て					

フィルタの解説

No.1：
192.168.0.2 のサーバに ftp のパケットを通す。
No.2：
192.168.0.2 のサーバに ftpdata のパケットを通す。
No.3、4：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。
No.5：
上記の条件に合致しないパケットを全て破棄する。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

Ⅳ．パケットフィルタリングの設定例

◆WWW、FTP、メール、DNS サーバを公開する際のフィルタ設定例

フィルタの条件

- WAN 側からは LAN 側の WWW、FTP、メールサーバにだけアクセスが可能にする。
- DNS サーバが WAN と通信できるようにする。
- LAN から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- PPPoE で ADSL に接続する。
- NAT は有効。
- ステートフルパケットインスペクションは有効。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス 「192.168.0.254」
- WWW サーバのアドレス 「192.168.0.1」
- メールサーバのアドレス 「192.168.0.2」
- FTP サーバのアドレス 「192.168.0.3」
- DNS サーバのアドレス 「192.168.0.4」

フィルタの解説

No.1：
192.168.0.1 のサーバに HTTP のパケットを通す。
No.2：
192.168.0.2 のサーバに SMTP のパケットを通す。
No.3：
192.168.0.2 のサーバに POP3 のパケットを通す。
No.4：
192.168.0.3 のサーバに ftp のパケットを通す。
No.5：
192.168.0.3 のサーバに ftpdata のパケットを通す。
No.6、7：
192.168.0.4 のサーバに、domain のパケット(tcp,udp)を通す。
No.8、9：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。
No.10：
上記の条件に合致しないパケットを全て破棄する。

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp				192.168.0.1	80
2	ppp0	パケット受信時	許可	tcp				192.168.0.2	25
3	ppp0	パケット受信時	許可	tcp				192.168.0.2	110
4	ppp0	パケット受信時	許可	tcp				192.168.0.3	21
5	ppp0	パケット受信時	許可	tcp				192.168.0.3	20
6	ppp0	パケット受信時	許可	tcp				192.168.0.4	53
7	ppp0	パケット受信時	許可	udp				192.168.0.4	53
8	ppp0	パケット受信時	許可	tcp					1024:65535
9	ppp0	パケット受信時	許可	udp					1024:65535
10	ppp0	パケット受信時	破棄	全て					

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

Ⅳ．パケットフィルタリングの設定例

◆NetBIOS パケットが外部へ出るのを防止するフィルタ設定

フィルタの条件

・LAN 側から送出された NetBIOS パケットを WAN へ出さない。(Windows での自動接続を防止する)

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス 「192.168.0.254」

設定画面での入力方法

「入力フィルタ」

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth0	パケット受信時	破棄	tcp					137:139
2	eth0	パケット受信時	破棄	udp					137:139
3	eth0	パケット受信時	破棄	tcp			137		
4	eth0	パケット受信時	破棄	udp			137		

「転送フィルタ」

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth0	パケット受信時	破棄	tcp					137:139
2	eth0	パケット受信時	破棄	udp					137:139
3	eth0	パケット受信時	破棄	tcp			137		
4	eth0	パケット受信時	破棄	udp			137		

フィルタの解説

「入力フィルタ」「転送フィルタ」
No.1：
　あて先ポートが tcp の 137 から 139 のパケットを Ether0 ポートで破棄する。
No.2：
　あて先ポートが udp の 137 から 139 のパケットを Ether0 ポートで破棄する。
No.3：
　送信先ポートが tcp の 137 のパケットを Ether0 ポートで破棄する。
No.4：
　送信先ポートが udp の 137 のパケットを Ether0 ポートで破棄する。

◆WAN からのブロードキャストパケットを破棄するフィルタ設定(smurf 攻撃の防御)

フィルタの条件

・WAN 側からのブロードキャストパケットを受け取らないようにする。→ smurf 攻撃を防御する

LAN 構成

・プロバイダから割り当てられたネットワーク空間「210.xxx.xxx.32/28」
・WAN 側は PPPoE 回線に接続する。
・WAN 側ポートの IP アドレス「210.xxx.xxx.33」

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	全て				210.xxx.xxx.32/32	
2	ppp0	パケット受信時	破棄	全て				210.xxx.xxx.47/32	

フィルタの解説

No.1：
　210.xxx.xxx.32/32（210.xxx.xxx.32/28 のネットワークのネットワークアドレス）宛てのパケットを受け取らない。
No.2：
　210.xxx.xxx.47/32（210.xxx.xxx.32/28 のネットワークのブロードキャストアドレス）宛てのパケットを受け取らない。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

Ⅳ．パケットフィルタリングの設定例

◆WAN からのパケットを破棄するフィルタ設定 (IP spoofing 攻撃の防御)

フィルタの条件

・WAN 側からの不正な送信元 IP アドレスを持つパケットを受け取らないようにする。
→ IP spoofing 攻撃を受けないようにする。

LAN 構成

・LAN 側のネットワークアドレス「192.168.0.0/24」
・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			

フィルタの解説

No.1、2、3：
WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。
→ WAN 上にプライベートアドレスは存在しない。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

◆外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

・WAN 側からの不正な送信元・送信先 IP アドレスを持つパケットを受け取らないようにする。
→ WAN からの攻撃を受けない・攻撃の踏み台にされないようにする。

LAN 構成

・プロバイダから割り当てられたアドレス空間「202.xxx.xxx.112/28」
・LAN 側のネットワークアドレス「192.168.0.0/24」
・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			
4	ppp0	パケット受信時	破棄	全て			202.xxx.xxx.127/3	

「出力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット送信時	許可	全て	10.0.0.0/8			
2	ppp0	パケット送信時	許可	全て	172.16.0.0/16			
3	ppp0	パケット送信時	許可	全て	192.168.0.0/16			

フィルタの解説

「入力フィルタ」
No.1、2、3：
WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。
→ WAN 上にプライベートアドレスは存在しない。
No.4：
WAN からのブロードキャストパケットを受け取らない。
→ smurf 攻撃の防御

「出力フィルタ」
No.1、2、3：
送信元 IP アドレスが不正なパケットを送出しない。
→ WAN 上にプライベートアドレスは存在しない。

Ⅳ．パケットフィルタリングの設定例

◆PPTP を通すためのフィルタ設定

フィルタの条件

・WAN 側からの PPTP アクセスを許可する。

LAN 構成

・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「転送フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp				1723
2	ppp0	パケット受信時	許可	gre				

フィルタの解説

PPTP では以下のプロトコル・ポートを使って通信します。

- プロトコル「GRE」
- プロトコル「tcp」のポート「1723」

したがいまして、フィルタ設定では上記 2 つの条件に合致するパケットを通す設定をおこなっています。

Ｖ．外部から設定画面にアクセスさせる設定

以下は、PPPoE で接続した場合の設定方法です。

1 まず設定画面にログインし、パケットフィルタ設定の「入力フィルタ」画面を開きます。

2 「入力フィルタ」設定の中で、以下のような設定を追加してください。

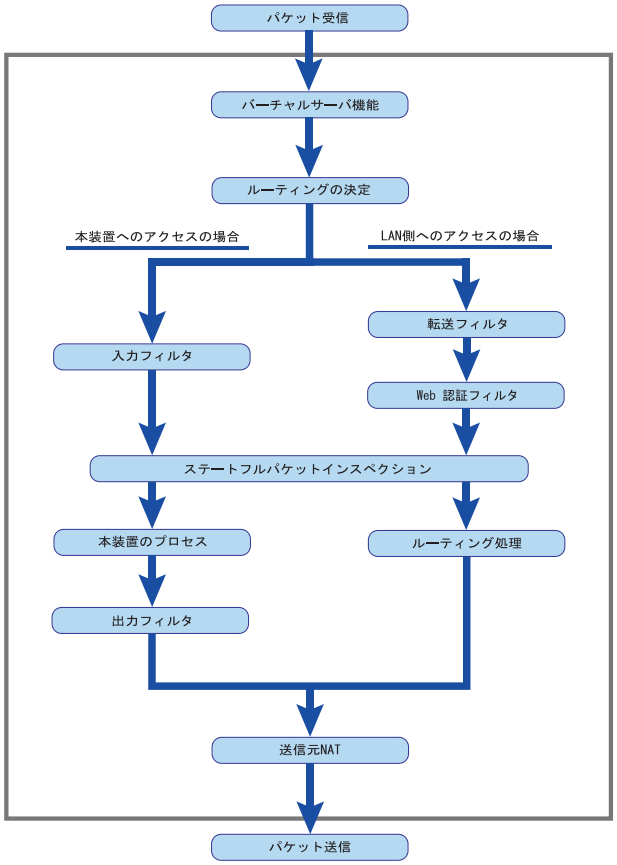
No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp	221.xxx.xxx.105			880

上記設定では、221.xxx.xxx.105 の IP アドレスを持つホストだけが、外部から本装置の設定画面へのアクセスが可能になります。

また「送信元アドレス」を空欄にすると、すべてのインターネット上のホストから、本装置にアクセス可能になります。
(**セキュリティ上たいへん危険ですので、この設定は推奨いたしません。**)

補足：NAT とフィルタの処理順序について

本装置における、NAT とフィルタリングの処理方法は以下のようになっています。



(図の上部を WAN 側、下部を LAN 側とします。
また LAN → WAN へ NAT をおこなうとします。)

- WAN 側からパケットを受信したとき、最初に「バーチャルサーバ設定」が参照されます。
- 「バーチャルサーバ設定」で静的 NAT 変換したあとに、パケットがルーティングされます。
- 本装置自身へのアクセスをフィルタするときは「入力フィルタ」、本装置自身からのアクセスをフィルタするときは「出力フィルタ」で設定します。
- WAN 側から LAN 側へのアクセスをフィルタするときは「転送フィルタ」で設定します。その場合のあて先アドレスは「(LAN 側の)プライベートアドレス」になります(NAT の後の処理となるため)。
- ステートフルパケットインスペクションだけを有効にしている場合、WAN から LAN、また本装置自身へのアクセスはすべて破棄されます。
- ステートフルパケットインスペクションと同時に「転送フィルタ」「入力フィルタ」を設定している場合は、先に「転送フィルタ」「入力フィルタ」にある設定が優先して処理されます。
- 「送信元 NAT 設定」は、一番最後に参照されます。
- LAN 側から WAN 側へのアクセスの場合も、処理の順序は同様です(最初にバーチャルサーバ設定が参照される)。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。
詳細はRFC1700(Oct. 1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

補足：フィルタのログ出力内容について

フィルタ設定画面で「LOG」にチェックを入れると、その設定に合致したパケットの情報を syslog に出力します。
出力内容は以下のようになります。

<入力パケットを破棄したときのログ出力例>

```
Jan 25 14:14:07 localhost XR-Filter:  FILTER_INPUT_1 IN=eth0 OUT=
MAC=00:80:6d:xx:xx:xx:00:20:ed:yy:yy:yy:80:00  SRC=192.168.xxx.xxx DST=xxx.xxx.xxx.xxx
LEN=40 TOS=00 PREC=0x00 TTL=128 ID=43951 CE DF PROTO=TCP SPT=2526 DPT=880 SEQ=4098235374
ACK=1758964579 WINDOW=48000 ACK URGP=0
```

Jan 25 14:14:07	syslog がログを取得した日時です。
XR-Filter:	フィルタのログであることを表します。
FILTER_INPUT_1	入力フィルタの１番目のフィルタで取得されたものです。 「FILTER_FORWARD」は転送フィルタを意味します。 「FILTER_OUTPUT」は出力フィルタを意味します。 「FILTER_AUTHGW」はWeb 認証フィルタを意味します。
IN=	パケットを受信したインタフェースが記されます。
OUT=	パケットを送出したインタフェースが記されます。 何も記載されていないときは、XRのどのインタフェースからもパケットを送出していないことを表わしています。
MAC=	送信元・あて先のMACアドレスが記されます。
SRC=	送信元IPアドレスが記されます。
DST=	送信先IPアドレスが記されます。
LEN=	パケット長が記されます。
TOS=	TOS bitの状態が記されます。
TTL=	TTLの値が記されます。
ID=	IPのIDが記されます。
PROTO=	プロトコルが記されます。

プロトコルが ICMP の時は、以下のような ICMP 用のメッセージも記されます。

TYPE=0	ICMPのタイプが記されます。
CODE=0	ICMPのコードが記されます。
ID=3961	ICMPのIDが記されます。
SEQ=6656	ICMPのシーケンス番号が記されます。

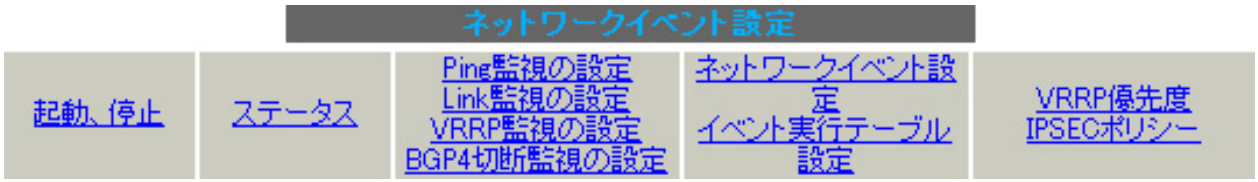
第 27 章

ネットワークイベント機能

第 27 章 ネットワークイベント機能

Ⅰ．機能の概要

ネットワークイベントは、回線障害などのネットワーク状態の変化を検知し、それをトリガとして特定のイベントを実行する機能です。



本装置では、以下のネットワーク状態の変化をトリガとして検知することができます。

- Ping 監視の状態
- Link 監視の状態
- VRRP 監視の状態
- BGP4 切断監視の状態

◆Ping 監視
本装置から任意の宛先へ ping を送信し、その応答の有無を監視します。
一定時間応答がなかった時にトリガーとして検知します。
また再び応答を受信した時は、復旧トリガーとして検知します。

◆Link 監視
Ethernet インタフェースや ppp インタフェースのリンク状態を監視します。
監視するインタフェースのリンクがダウンした時にトリガーとして検知します。
また再びリンクがアップした時は、復旧トリガーとして検知します。

◆VRRP 監視
本装置の VRRP ルータ状態を監視します。
指定したルータ ID の VRRP ルータがバックアップルータへ切り替わった時にトリガーとして検知します。
また再びマスタルータへ切り替わった時は、復旧トリガーとして検知します。

◆BGP4 切断監視
BGP4 neighbor state の状態を監視して、VRRP の優先度を変更させます。
Neighbor state が Established 変化した時に、トリガーとして検知します。
VRRP の優先度は「ネットワークイベント設定」→「BGP4 切断監視」→「VRRP 優先度」にて設定された優先度へ変更されます。
また、Neighbor state が Established から他の state へ変化した時に、復旧トリガーとして検知します。

VRRPの優先度は「各種サービスの設定」→「VRRPサービス」にて設定された優先度へと戻ります。

Ⅰ．機能の概要

また、これらのトリガを検知した際に実行可能なイベントとして、以下の 2 つがあります。

- VRRP 優先度変更
- IPsec 接続切断

◆ VRRP 優先度変更
トリガ検知時に、指定した VRRP ルータの優先度を変更します。
またトリガ復旧時には、元の VRRP 優先度に変更します。

例えば、Ping 監視と連動して、PPPoE 接続先がダウンした時に、自身は VRRP バックアップルータに移行し、新マスタールータ側の接続へ切り替える、といった使い方ができます。

◆ IPsec 接続 / 切断
トリガ検知時に、指定した IPsec ポリシーを切断します。
またトリガ復旧時には、IPsec ポリシーを再び接続します。

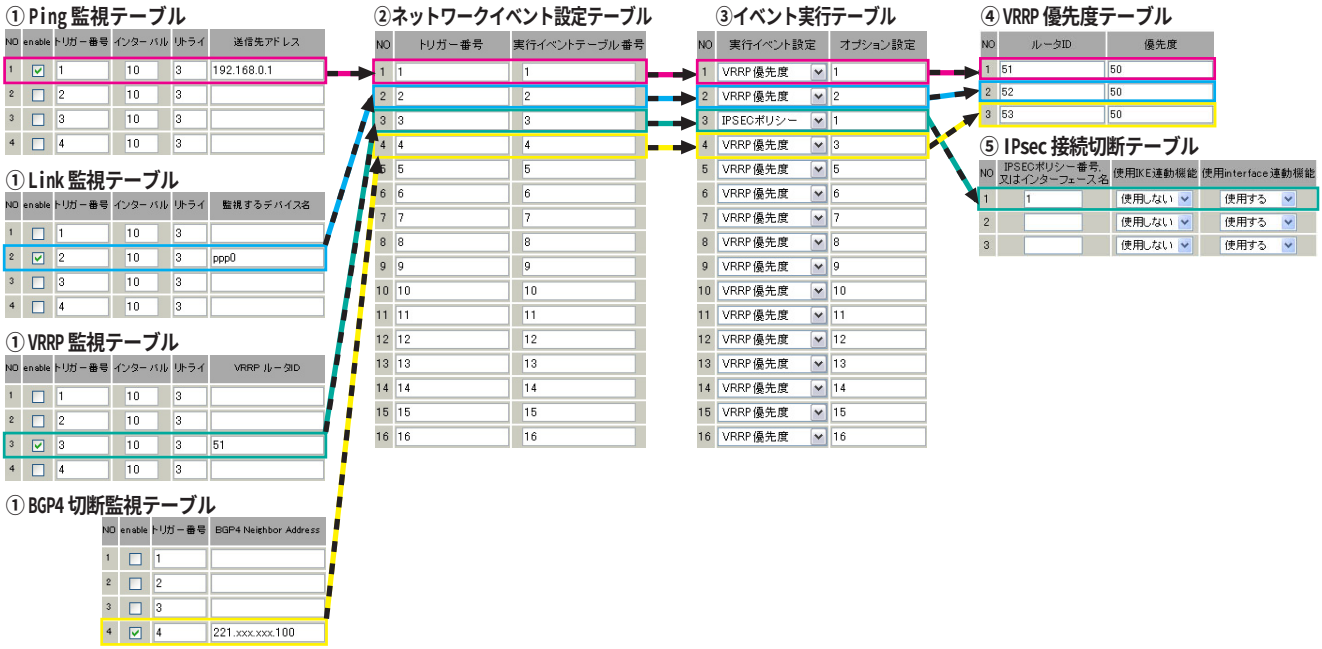
例えば、VRRP 監視と連動して、2 台の VRRP ルータのマスタルータの切り替わりに応じて、IPsec 接続を繋ぎかえる、といった使い方ができます。

第 27 章 ネットワークイベント機能

Ⅰ．機能の概要

本機能で使用する各種テーブルについて

本機能は複数のテーブル定義を連携させることによって実現しています。



①Ping 監視テーブル /Link 監視テーブル /VRRP 監視テーブル /BGP4 切断監視テーブル

これらのテーブルでは、監視対象、監視周期、障害検出した場合のトリガー番号を設定します。
ここで設定を有効(enable)にしたトリガー番号は、次の「②ネットワークイベント設定テーブル」のインデックス番号になります。

②ネットワークイベント設定テーブル

このテーブルでは、トリガー番号とイベント番号の関連付けを定義します。
ここで設定したイベント番号は、次の「③イベント実行テーブル」のインデックス番号になります。

③イベント実行テーブル

このテーブルでは、イベント番号と実行イベント種別 / オプション番号の関連付けを定義します。

イベントの実行種別を「VRRP 優先度」に設定した場合は、次に「④VRRP 優先度テーブル」を索引します。
設定したオプション番号は、テーブル④のインデックス番号になります。

また、イベントの実行種別を「IPSEC ポリシー」に設定した場合は、次に「⑤ IPsec 接続切断テーブル」を索引します。
設定したオプション番号は、テーブル⑤のインデックス番号になります。

④ VRRP 優先度テーブル

このテーブルでは、VRRP 優先度を変更するルータ ID とその優先度を定義します。

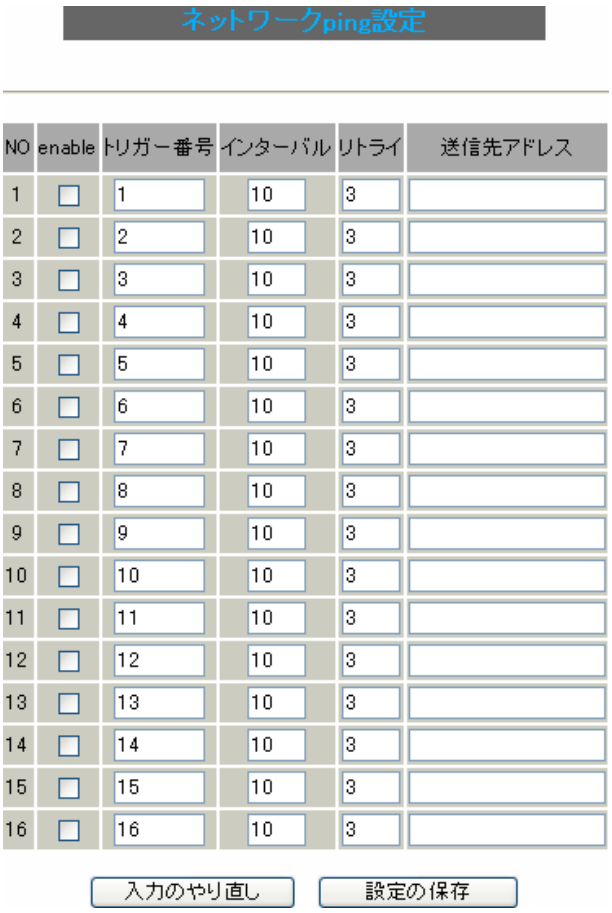
⑤ IPsec 接続切断テーブル

このテーブルでは、IPsec 接続 / 切断をおこなう IPsec ポリシー番号、または IPsec インタフェース名を定義します。

Ⅱ．各トリガテーブルの設定

Ping監視の設定方法

設定画面上部の「Ping監視の設定」をクリックして、以下の画面から設定します。



○enable
チェックを入れることで設定を有効にします。

○トリガー番号
ping送信先から応答が無かった場合に、検知するトリガーの番号(1～16)を指定します。
本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

○インターバル(秒)
○リトライ
pingを発行する間隔を設定します。
「『インターバル』秒間に、『リトライ』回pingを発行する」という設定になります。
この間、一度も応答が無かった場合にトリガーとして検知されます。

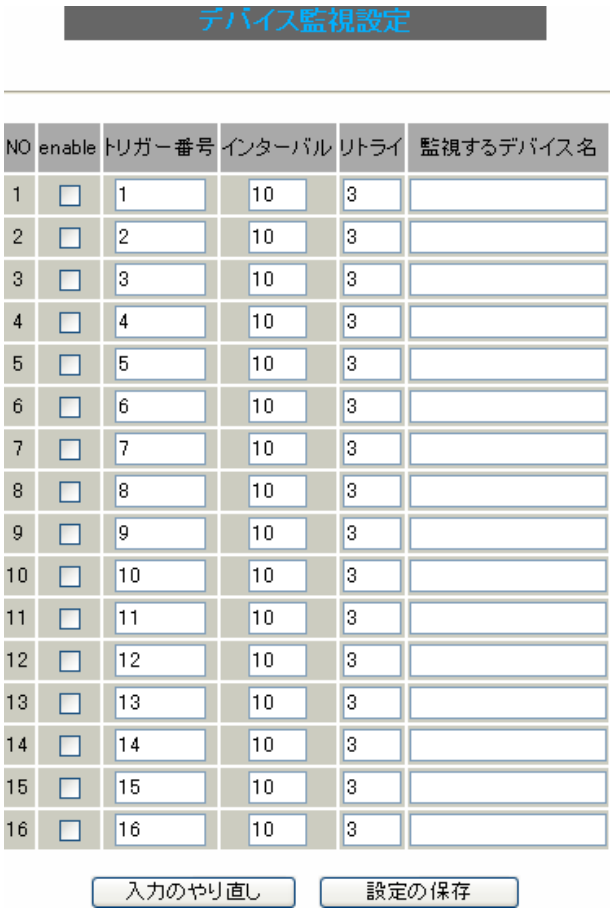
○送信先アドレス
pingを送信する先のIPアドレスを指定します。

最後に「設定の保存」をクリックして設定完了です。

II．各トリガテーブルの設定

Link 監視の設定方法

設定画面上部の「Link 監視の設定」をクリックして、以下の画面から設定します。



○ enable
チェックを入れることで設定を有効にします。

○トリガー番号
監視するインターフェースのリンクがダウンした場合に、検知するトリガーの番号(1～16)を指定します。
本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

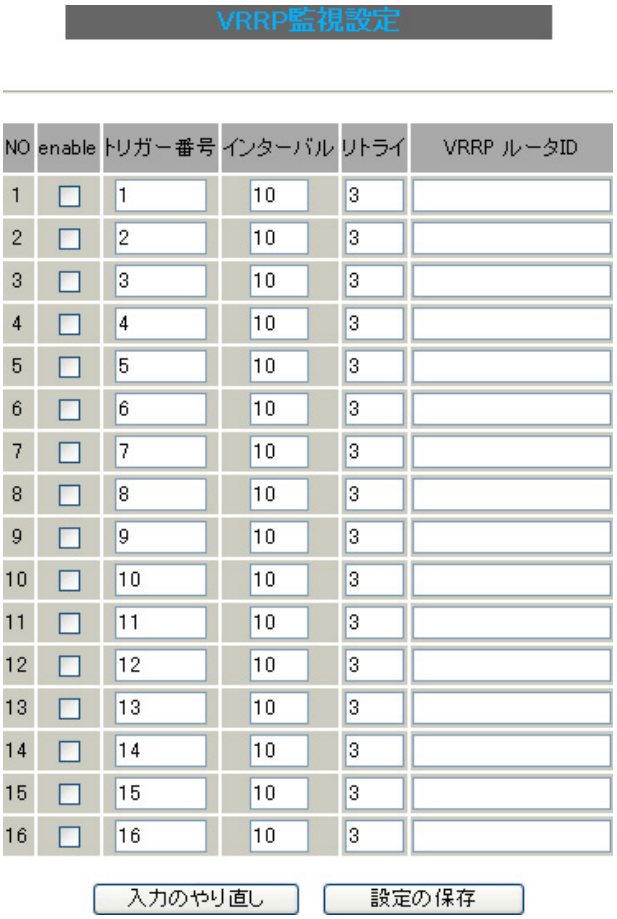
○インターバル(秒)
○リトライ
インターフェースのリンク状態を監視する間隔を設定します。
「『インターバル』秒間に、『リトライ』回、インターフェースのリンク状態をチェックする」という設定になります。
この間、リンク状態が全てダウンだった場合にトリガーとして検知されます。

○監視するデバイス名
リンク状態を監視するデバイスのインタフェース名を指定します。
Ethernet インタフェース名、または PPP インタフェース名を入力してください。

最後に「設定の保存」をクリックして設定完了です。

VRRP 監視の設定方法

設定画面上部の「VRRP 監視の設定」をクリックして、以下の画面から設定します。



○ enable
チェックを入れることで設定を有効にします。

○トリガー番号
監視する VRRP ルータがバックアップへ切り替わった場合に、検知するトリガーの番号(1～16)を指定します。
本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

○インターバル(秒)
○リトライ
VRRP ルータの状態を監視する間隔を設定します。
「『インターバル』秒間に、『リトライ』回、VRRP のルータ状態を監視する」という設定になります。
この間、監視した状態が全てバックアップ状態であった場合にトリガーとして検知されます。

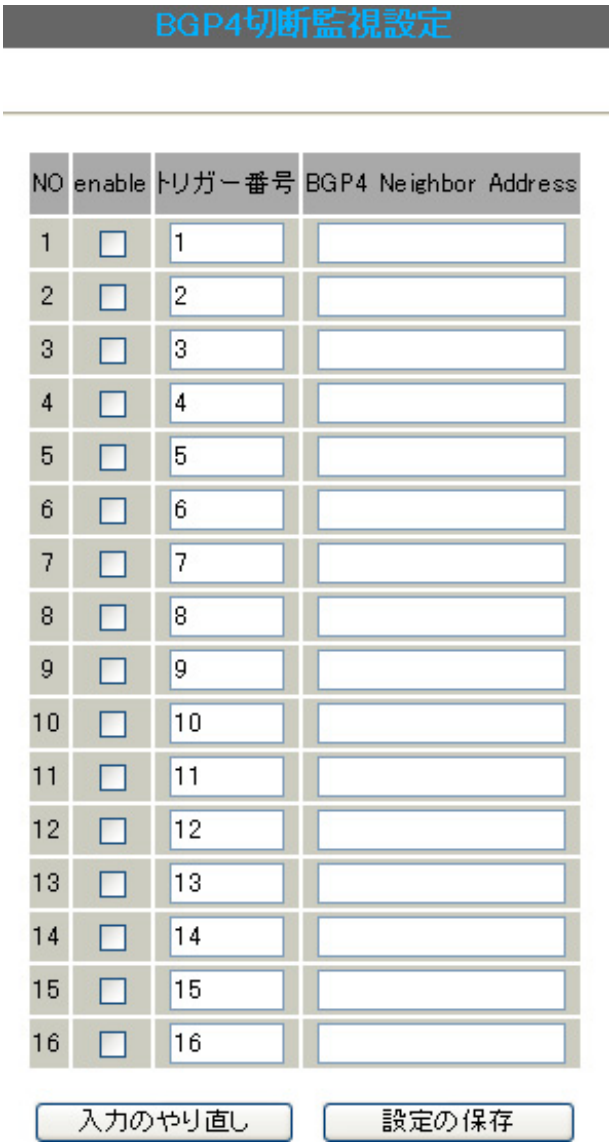
○ VRRP ルータ ID
VRRP ルータ状態を監視するルータ ID を指定します。

最後に「設定の保存」をクリックして設定完了です。

II．各トリガテーブルの設定

BGP4 切断監視の設定方法

設定画面上部の「BGP4 切断監視の設定」をクリックして、以下の画面から設定します。



○ enable
チェックを入れることで設定を有効にします。

○トリガー番号
監視する BGP4 peer の neighbor 状態が変化した場合に、検知するトリガーの番号(1～16)を指定します。
本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

○ BGP4 Neighbor Address
BGP4 peer の IP アドレスを指定します。

最後に「設定の保存」をクリックして設定完了です。

II．各トリガテーブルの設定

各種監視設定の起動と停止方法

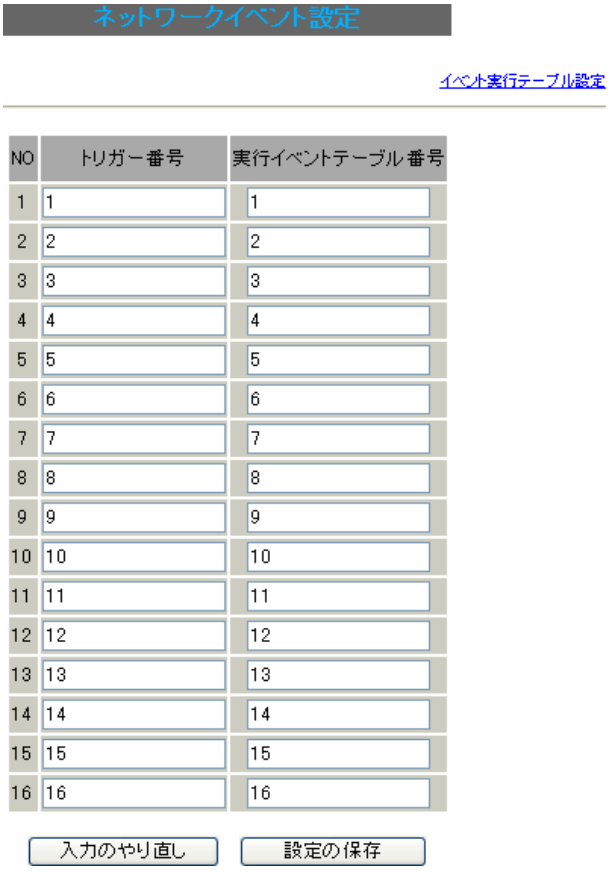
各監視機能（Ping 監視、Link 監視、VRRP 監視、BGP4 切断監視）を有効にするには、Web 画面「ネットワークイベント設定」画面→「起動、停止」の以下のネットワークサービス設定画面で、「起動」ボタンにチェックを入れ、「動作変更」をクリックしてサービスを起動してください。
また設定の変更、追加、削除をおこなった場合は、サービスの再起動をおこなってください。

注) 各監視設定で指定したトリガー番号は、「ネットワークイベント設定」テーブルでのインデックス番号となるため、それぞれの監視設定の間で同じトリガー番号が有効にならないように設定してください。

III. 実行イベントテーブルの設定

ネットワークイベント設定テーブルの設定

設定画面上部の「ネットワークイベント設定」をクリックして、以下の画面から設定します。
(「イベント実行テーブル設定」画面のリンクをクリックしても以下の画面を開くことができます。)



○トリガー番号
「Ping 監視の設定」、「Link 監視の設定」、「VRRP 監視の設定」「BGP4 切断監視の設定」で設定したトリガー番号を指定します。
なお、複数のトリガー検知の組み合わせによって、イベントを実行させることも可能です。

＜例＞
・トリガー番号 1 とトリガー番号 2 のどちらかを検知した時にイベントを実行させる場合
　1&2

・トリガー番号 1 とトリガー番号 2 の両方を検知した時、またはトリガー番号 3 を検知した時にイベントを実行させる場合
　[1|2]&3

○実行イベントテーブル番号
そのトリガー番号を検知した時に実行されるイベント番号(1～16)を指定します。
本値は、イベント実行テーブルでのインデックス番号となります。
なお、複数のイベントを同時に実行させることも可能です。その場合は ”_” でイベント番号を繋ぎます。

＜例＞ イベント番号 1,2,3 を同時に実行させる場合
　1_2_3

最後に「設定の保存」をクリックして設定完了です。

III. 実行イベントテーブルの設定

イベント実行テーブルの設定

設定画面上部の「イベント実行テーブル設定」をクリックして、以下の画面から設定します。
(「ネットワークイベント設定」画面のリンクをクリックしても以下の画面を開くことができます。)

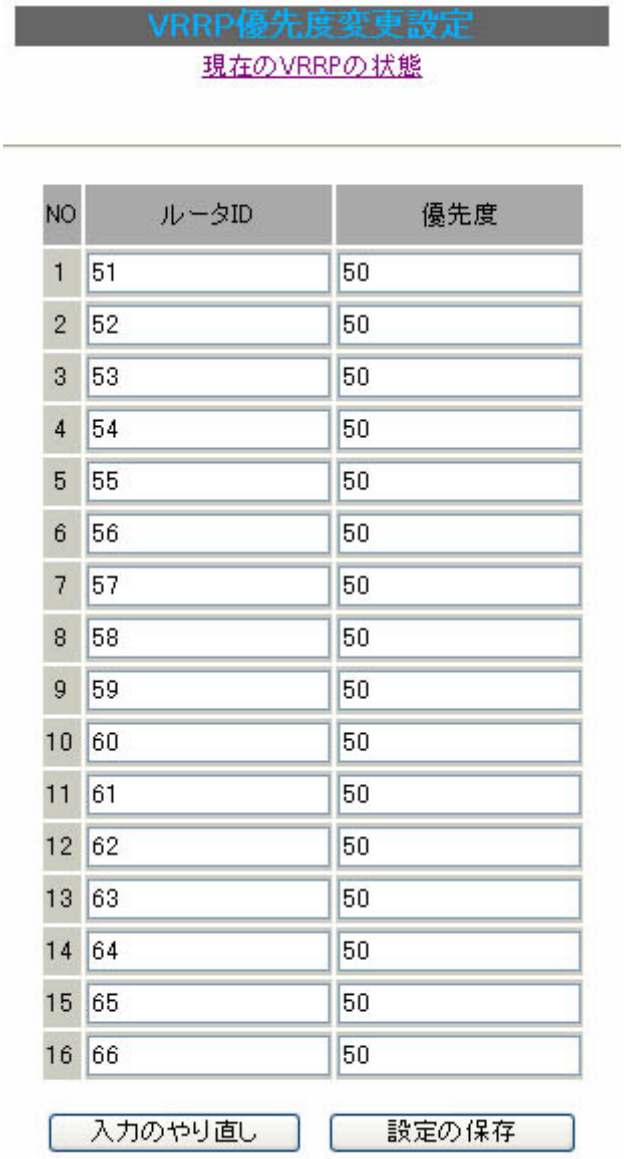
○実行イベント設定
実行されるイベントの種類を選択します。
「IPsec ポリシー」は、IPsec ポリシーの切断をおこないます。
「VRRP 優先度」は、VRRP ルータの優先度を変更します。

○オプション設定
実行イベントのオプション番号です。
本値は、「VRRP 優先度変更設定」テーブル、または「IPSEC 接続切断設定」テーブルでのインデックス番号となります。

最後に「設定の保存」をクリックして設定完了です。

VRRP 優先度変更設定テーブルの設定

設定画面上部の「VRRP 優先度」をクリックして、以下の画面から設定します。



○ルータ ID
トリガー検知時に VRRP 優先度を変更する VRRP ルータ ID を指定します。

○優先度
トリガー検知時に変更する VRRP 優先度を指定します。1～255 の間で設定してください。
なお、トリガー復旧時には「VRRP サービス」で設定されている元の値に戻ります。

最後に「設定の保存」をクリックして設定完了です。

現在の設定状態の確認

VRRP 優先度変更設定画面の上部の、
「現在の VRRP の状態」リンクをクリックすると、
「VRRP の情報」を表示するウィンドウがポップアップします。

Ⅳ．実行イベントのオプション設定

IPSEC 接続切断設定 テーブルの設定

設定画面上部の「IPSEC ポリシー」をクリックして、次の画面から設定します。

○ IPSEC ポリシー番号、又はインターフェース名
トリガー検知時に切断する IPsec ポリシーの番号、または IPsec インタフェース名を指定します。
ポリシー番号は、範囲で指定することもできます。

<例> IPsec ポリシー 1 から 20 を切断する → **1:20**

インタフェース名を指定した場合は、そのインタフェースで接続する IPsec は全て切断されます。
トリガー復旧時には再度 IPsec 接続されます。

○使用 IKE 連動機能
切断する IPsec ポリシーが使用する IKE と同じ IKE を使用する IPsec ポリシーが設定されている場合において、トリガー検知時にその IKE を使用する全ての IPsec ポリシーを切断する場合は、「使用する」を選択します。
ここで設定した IPsec ポリシーのみを切断する場合は「使用しない」を選択します。

○使用 interface 連動機能
本装置では、PPPoE 上で IPsec 接続している場合、PPPoE 接続時に自動的に IPsec 接続も開始されます。
ネットワークイベント機能を使った IPsec 二重化において、バックアップ側の PPPoE 接続時に IPsec を自動接続させたくない場合には「使用しない」を選択します。

最後に「設定の保存」をクリックして設定完了です。

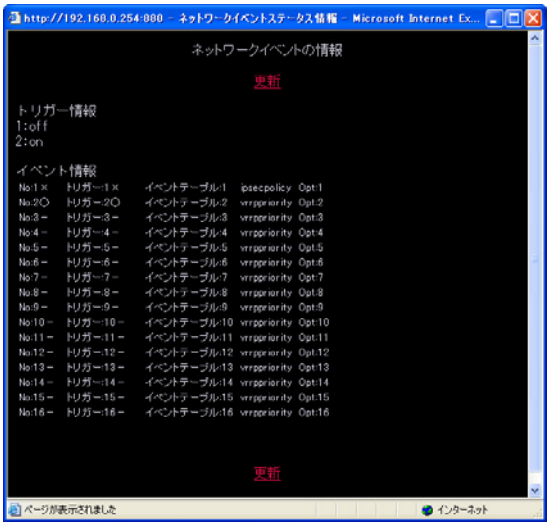
現在の設定状態の確認

IPSEC 接続切断設定画面の上部の、
「現在の IPSEC の状態」リンクをクリックすると、
「IPSEC の情報」を表示するウィンドウがポップアップします。

Ⅴ．ステータスの表示

ステータスの表示

設定画面上部の「ステータス」をクリックして表示します。



○トリガー情報
設定が有効なトリガー番号とその状態を表示します。

“ ON ”と表示されている場合は、トリガを検知していない、またはトリガが復旧している状態を表します。

“ OFF ”と表示されている場合は、トリガ検知している状態を表します。

○イベント情報

・No.
イベント番号とその状態を表します。

“ × ”の表示は、トリガ検知し、イベントを実行している状態を表します。

“ ○ ”の表示は、トリガ検知がなく、イベントが実行されていない状態を表します。

“ - ”の表示は、無効なイベントです。

・トリガー
イベント実行の条件となるトリガ番号とその状態を表します。

・イベントテーブル
左からイベント実行テーブルのインデックス番号、実行イベント種別、オプションテーブル番号を表します。

第 28 章

仮想インタフェース機能

仮想インタフェース機能の設定

主にバーチャルサーバ機能を利用する場合に、仮想インタフェースを設定します。
1024 まで設定できます。
「仮想インターフェース設定画面インデックス」のリンクをクリックしてください。

設定方法

Web 設定画面「仮想インターフェース」をクリックして、以下の画面から設定します。

No.	インターフェース	仮想I/F番号	IPアドレス	ネットマスク	削除
1					☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐
9					☐
10					☐
11					☐
12					☐
13					☐
14					☐
15					☐
16					☐

○インターフェース
仮想インタフェースを作成するインタフェース名を指定します。
本装置のインタフェース名については、本マニュアルの**「付録A インタフェース名一覧」**をご参照ください。

○仮想 I/F 番号
作成するインタフェースの番号を指定します。
0 ～ 1023 の間で設定します。

○ IP アドレス
作成するインタフェースの IP アドレスを指定します。

○ネットマスク
作成するインタフェースのネットマスクを指定します。

○削除
仮想インタフェース設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

”No.”項目が赤字で表示されている行は入力内容が正しくありません。
再度入力をやり直してください。

第 29 章

GRE 設定

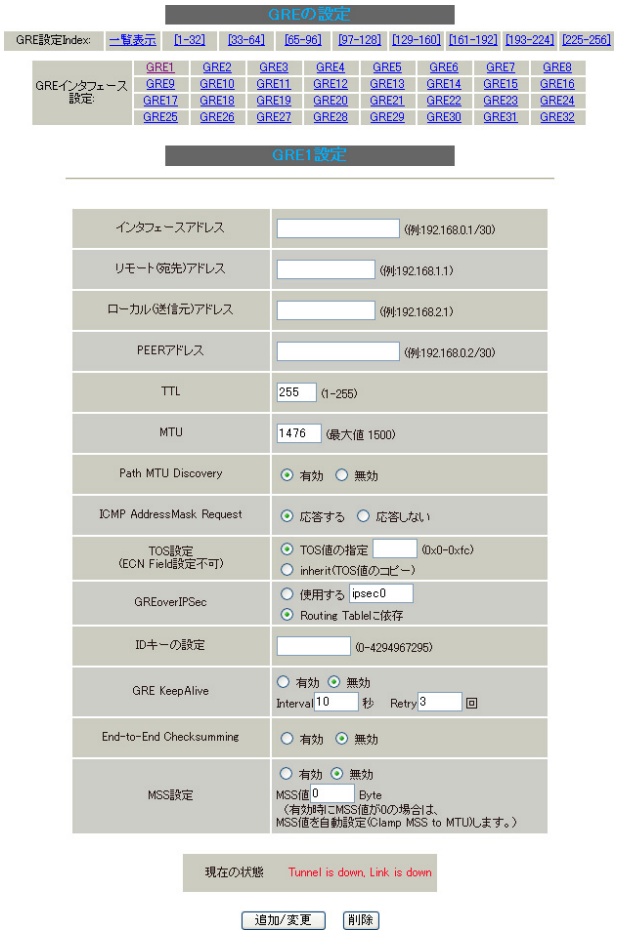
第 29 章 GRE 設定

GRE の設定

GRE は Generic Routing Encapsulation の略で、リモート側にあるルータまで仮想的なポイントツーポイント リンクを張って、多種プロトコルのパケットを IP トンネルにカプセル化するプロトコルです。また IPsec トンネル内に GRE トンネルを生成することもできますので、GRE を使用する場合でもセキュアな通信を確立することができます。

GRE の設定

設定画面「GRE 設定」→[GRE インタフェース設定:]のインタフェース名「GRE1」～「GRE256」をクリックして設定します。



○インタフェースアドレス
GRE トンネルを生成するインタフェースの仮想アドレスを設定します。任意で指定します。
＜例＞ 192.168.90.1/30

○リモート(宛先)アドレス
GRE トンネルのエンドポイントの IP アドレス(対向側装置の WAN 側 IP アドレス)を設定します。

○ローカル(送信元)アドレス
本装置の WAN 側 IP アドレスを設定します。

○ PEER アドレス
GRE トンネルを生成する対向側装置のインタフェースの仮想アドレスを設定します。「インタフェースアドレス」と同じネットワークに属するアドレスを指定してください。
例) 192.168.90.2/30

○ TTL
GRE パケットの TTL 値を設定します。

○ MTU
MTU 値を設定します。最大値は 1500byte です。

○ Path MTU Discovery
Path MTU Discovery 機能を有効にするかを選択します。
機能を「有効」にした場合は、常に IP ヘッダの DF ビットを ON にして転送します。転送パケットの DF ビットが 1 でパケットサイズが MTU を超えている場合は、送信元に ICMP Fragment Needed を返送します。
PathMTU Discovery を「無効」にした場合、TTL は常にカプセル化されたパケットの TTL 値がコピーされます。従って、GRE 上で OSPF を動かす場合には、TTL が 1 に設定されてしまうため、PathMTU Discovery を「有効」にしてください。

○ ICMP AddressMask Request
「応答する」にチェックを入れると、その GRE インタフェースにて受信した ICMP AddressMask Request (type=17)に対して、サブネットマスク値を設定した ICMP AddressMask Reply(type=18)を返送します。

○ ToS
GRE パケットの ToS 値を設定します。

GRE の設定

○ GREoverIPsec
IPsec を使用して GRE パケットを暗号化する場合に「使用する」を選択します。
またこの場合には別途、IPsec の設定が必要です。
Routing Table に合わせて暗号化したい場合には「Routing Table に依存」を選択します。
ルートが IPsec の時は暗号化、IPsec でない時は暗号化しません。

GRE トンネルを暗号化するときの IPsec 設定は次のように設定してください。

- 本装置側設定　　**通常通り**
- IKE/ISAKMP ポリシー設定　　**通常通り**
- IPsec ポリシー設定
  本装置側の LAN 側のネットワークアドレス：
  GRE 設定のローカルアドレス /32
  相手側の LAN 側のネットワークアドレス：
  GRE 設定のリモートアドレス /32

○ ID キーの設定
この機能を有効にすると、KEY Field の 4byte が GRE ヘッダに付与されます。

○ GRE KeepAlive
GREトンネルのキープアライブの設定をおこないます。
「有効」「無効」のどちらかを選択します。
対向装置が GRE キープアライブを実装していない場合は「無効」を選択してください。

・Interval
GREキープアライブパケットの送信間隔を設定します。
指定可能な範囲：1-32767 秒です。

・Retry
replyパケットを受信できなかった場合のリトライ回数を指定します。
ここで指定した回数内に一度も reply パケットが受信できない場合、GRE トンネルは Down 状態へと遷移します。指定可能な範囲：1-255 です。

GRE トンネルが Down 状態でも GRE キープアライブパケットの送信はおこなわれます。その間１度でも reply パケットを受信すると GRE トンネルは Up 状態へと遷移します。

○ End-to-End Checksumming
チェックサム機能の有効 / 無効を選択します。
この機能を有効にすると、
checksum field (2byte) + offset (2byte)
の計 4byte が GRE パケットに追加されます。

○ MSS 設定
GRE トンネルに対して、clamp to MSS 機能を有効にしたり、MSS 値の設定が可能です。

入力後は「追加 / 変更」ボタンをクリックします。
直ちに設定が反映され、GRE トンネルが生成されます。

GRE の設定

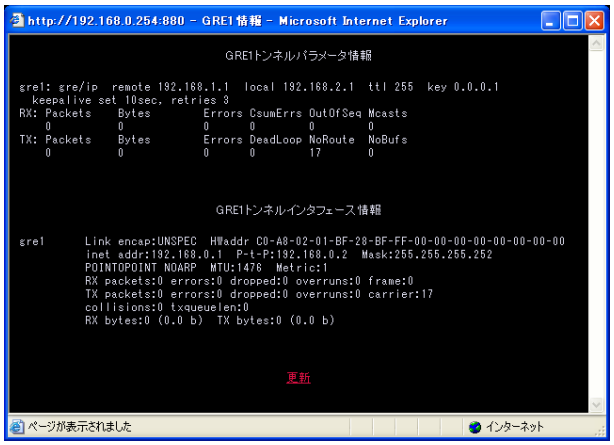
GRE の削除

「GRE インタフェース設定:GRE1」～「GRE64」の画面の「削除」ボタンをクリックすると、その設定に該当する GRE トンネルが無効化されます(設定自体は保存されています)。
再度有効とするときは「追加 / 変更」ボタンをクリックしてください。

GRE の状態表示

「GRE インタフェース設定:GRE1」～「GRE64」の画面下部にある「現在の状態」では GRE の動作状況が表示されます。

また、実行しているインタフェースでは、「現在の状態」リンクをクリックするとウィンドウポップアップして、「GRE1トンネルパラメータ情報」と「GRE1 トンネルインタフェース情報」が表示されます。



GRE の再設定

GRE 設定をおこなうと、設定内容が一覧表示されます。

GRE一覧表示

Interface名	Interface Address	Remote Address	Local Address	Peer Address	MTU	ID Key	Check sum	PMTUD	ICMP	KeepAlive	Link State
gre1	192.168.0.1/30	192.168.1.1	192.168.2.1	192.168.0.2/30	1476	1	無効	有効	有効	有効	down

○編集
設定の編集は「Interface 名」をクリックしてください。

○リンク状態
GRE トンネルのリンク状態は「Link State」に表示されます。
「up」が GRE トンネルがリンクアップしている状態です。

第 30 章

QoS 設定

第 30 章 QoS 機能

Ⅰ．QoS について

本装置の優先制御・帯域制御機能(以下、QoS 機能)は以下の 5 つのキューイング方式で、トラフィック制御をおこないます。

1. SFQ
2. PFIFO
3. TBF
4. CBQ
5. PQ

クラスフル / クラスレスなキューイング

キューイングには、クラスフルなものとクラスレスなものがあります。

クラスレス キューイング

クラスレスなキューイングは、内部に設定可能なトラフィック分割用のバンド(クラス)を持たず、到着するすべてのトラフィックを同等に取り扱います。

PFIFO、TBF、SFQ がクラスレスなキューイングです。

クラスフル キューイング

クラスフルなキューイングでは、内部に複数のクラスを持ち、選別器(クラス分けフィルタ)によって、パケットを送り込むクラスを決定します。各クラスはそれぞれに帯域を持つため、クラス分けすることで帯域制御ができるようになります。またキューイング方式によっては、あるクラスがさらに自分の配下にクラスを持つこともできます。さらに、各クラス内でそれぞれキューイング方式を決めることもできます。

PQ と CBQ がクラスフルなキューイングです。

Ⅰ．QoS について

1.SFQ

SFQはパケットの流れ(トラフィック)を整形しません。パケットを送り出す順番を決めるだけです。

SFQでは、トラフィックを多数の内部キューに分割して収納します。そして各キューをラウンドロビンで回り、各キューからパケットをFIFOで順番に送信していきます。

ラウンドロビンで順番にトラフィックが送信されることから、ある特定のトラフィックが他のトラフィックを圧迫してしまうことがなくなり、どのトラフィックも公平に送信されるようになります(複数のトラフィックを平均化できる)。

※整形とは、トラフィック量が一定以上にならないように転送速度を調節することを指します。
「シェーピング」とも呼ばれます。

2.PFIFO

もっとも単純なキューイング方式です。
あらかじめキューのサイズを決定しておき、どのパケットも区別なくキューに収納していきます。
キューからパケットを送信するとき、送信するパケットはFIFOにしたがって選別されます。

キューのサイズを超えてパケットが到着したとき、超えた分のパケットは全て破棄されてしまいます。

キューのサイズが大きすぎると、キューイングによる遅延が発生する可能性があります。

※キューとは、データの入り口と出口を一つだけ持つバッファのことを指します。

※FIFOとは「First In First Out」の略で、「最初に入ったものが最初に出る」、つまり最も古いものが最初に取り出されることを指します。

Ⅰ．QoS について

3.TBF

帯域制御方法の 1 つです。
トークンバケツにトークンを、ある一定の速度(トークン速度)で収納していきます。このトークン 1 個ずつがパケットを 1 個ずつつかみ、トークン速度を超えない範囲でパケットを送信していきます(送信後はトークンは削除されます)。

またバケツにに溜まっている余分なトークンは、突発的なバースト状態(パケットが大量に届く状態)でパケットが到着しているときに使われます。バーストが起きているときはすでにバケツに溜まっている分のトークンを使ってパケットを送信しますので、溜まった分のトークンを使い切らないような短期的なバーストであれば、トークン速度(制限 Rate)を超えたパケット送信が可能です。

バースト状態が続くとバケツのトークンがすぐになくなってしまうため遅延が発生していき、最終的にはパケットが破棄されてしまうことになります。

4.CBQ

CBQ は帯域制御の 1 つです。複数のクラスを作成しクラスごとに帯域幅を設定することで、パケットの種類に応じて使用できる帯域を割り当てる方式です。

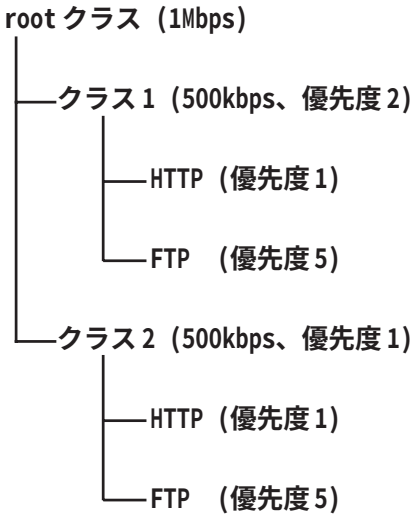
CBQ におけるクラスは、階層的に管理されます。最上位には root クラスが置かれ、利用できる総帯域幅を定義しておきます。root クラスの下に子クラスが置かれ、それぞれの子クラスには root で定義した総帯域幅の一部を利用可能帯域として割り当てます。子クラスの下には、さらにクラスを置くこともできます。

各クラスへのパケットの振り分けは、フィルタ(クラス分けフィルタ)の定義に従っておこなわれます。

各クラスには帯域幅を割り当てます。兄弟クラス間で割り当てている帯域幅の合計が、上位クラスで定義している帯域幅を超えないように設計しなければなりません。

また、それぞれのクラスには優先度を割り振り、優先度に従ってパケットを送信していきます。

<クラス構成図　例>



(次ページに続きます)

Ⅰ．QoS について

子クラスからはFIFOでパケットが送信されますが、子クラスの下にキューイングを定義し、クラス内でのキューイングをおこなうこともできます(クラスキューイング)。

CBQの特徴として、各クラス内において、あるクラスが兄弟クラスから帯域幅を借りることができます。たとえば図のクラス1において、トラフィックが500kbpsを超えていて、且つ、クラス2の使用帯域幅が500kbps以下の場合に、クラス1はクラス2で余っている帯域幅を借りてパケットを送信することができます。

5.PQ

PQは優先制御の1つです。トラフィックのシェーピングはおこないません。

PQでは、パケットを分類して送り込むクラスに優先順位をつけておきます。そしてフィルタによってパケットをそれぞれのクラスに分類したあと、優先度の高いクラスから優先的にパケットを送信します。なお、クラス内のパケットはFIFOで取り出されます。

優先度の高いクラスに常にパケットがキューイングされているときには、より優先度の低いクラスからはパケットが送信されなくなります。

II．QoS 機能の各設定画面について

本装置では下記の各種設定画面で設定をおこないます。
設定方法については各設定の説明ページをご参照ください。

QoS 機能設定
QoS 機能の有効・無効が指定できます。

QoS 簡易設定
必要最低限の設定項目を指定するだけで、優先制御および、帯域制御がおこなえます。

QoS 詳細設定
QoS 機能について、各種詳細設定をおこないます。

Interface Queuing 設定
本装置の各インタフェースでおこなうキューイング方式を定義します。
すべてのキューイング方式で設定が必要です。

CLASS 設定
CBQ をおこなう場合の、各クラスについて設定します。

CLASS Queuing 設定
各クラスにおけるキューイング方式を定義します。
CBQ 以外のキューイング方式について定義できます。

CLASS 分けフィルタ設定
パケットを各クラスに振り分けるためのフィルタ設定を定義します。
PQ、CBQ をおこなう場合に設定が必要です。

パケット分類設定
各パケットに TOS 値や MARK 値を付加するための設定です。
PQ をおこなう場合に設定します。PQ では IP ヘッダによる CLASS 分けフィルタリングができないため、TOS 値または MARK 値によってフィルタリングをおこないます。

ステータス表示
QoS 機能の各種ステータスが表示されます。

III. 各キューイング方式の設定手順について

各キューイング方式の基本的な設定手順は以下の通りです。

◆SFQ の設定手順
「Interface Queueing 設定」で設定します。

◆pfifo の設定手順
「Interface Queueing 設定」でキューのサイズを設定します。

◆TBF の設定手順
「Interface Queueing設定」で、トークンのレート、バケツサイズ、キューのサイズを設定します。

◆CBQ の設定手順
1. ルートクラスの設定
「Interface Queueing 設定」で、ルートクラスの設定をおこないます。

2. 各クラスの設定
・「CLASS 設定」で、全てのクラスの親となる親クラスについて設定します。

・「CLASS 設定」で、親クラスの下に置く子クラスについて設定します。

・「CLASS 設定」で、子クラスの下に置くリーフクラスを設定します。

3. クラス分けの設定
「CLASS 分けフィルタ設定」で、CLASS 分けのマッチ条件を設定します。

4. クラスキューイングの設定
クラス内でさらにキューイングをおこなうときには「CLASS Queueing 設定」でキューイング設定をおこないます。

◆PQ の設定手順
1. インタフェースの設定
「Interface Queueing 設定」で、Band 数、Priority-map、Marking Filter を設定します。

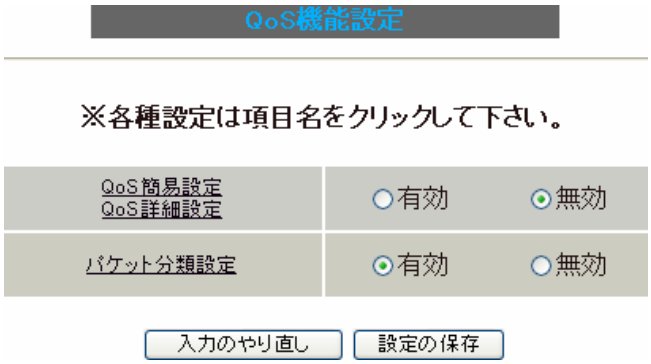
2. CLASS 分けのためのフィルタ設定
「CLASS 分けフィルタ設定」で、Mark 値によるフィルタを設定します。

3. パケット分類のための設定
「パケット分類設定」で、TOS 値または MARK 値の付与設定をおこないます。

Ⅳ．QoS 機能設定について

[QoS 機能設定]

下記の画面にてQoSの設定と制御をおこなうことができます。



この画面から以下の項目をクリックして、各種設定画面にて設定をおこなってください。

- **QoS 簡易設定**
  必要最低限の設置項目を指定するだけで、優先制御および帯域制御がおこなわれます。

- **QoS 詳細設定**
  QoS の詳細について各種設定します。

- **パケット分類設定**
  各パケットに TOS 値や MARK 値を付加するための設定です。

◯有効
◯無効
QoS 機能に関する以下の機能の有効・無効を指定します。
- QoS 機能（パケット分類設定を除く、QoS 設定の反映）
- パケット分類設定機能

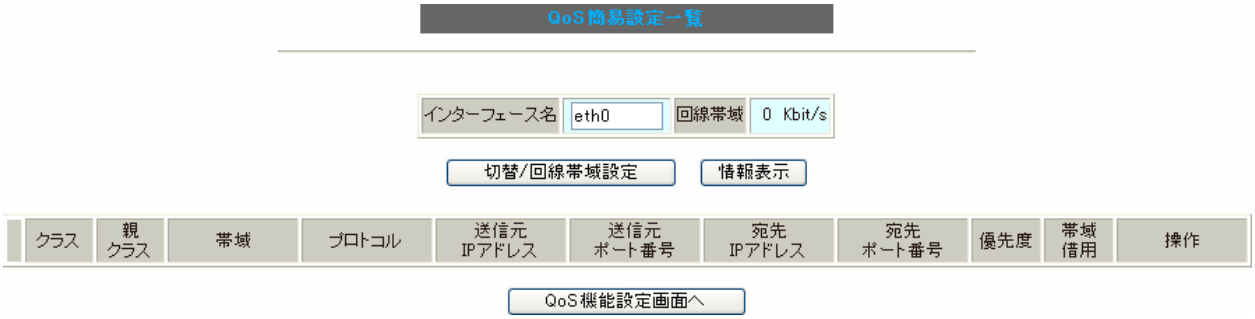
QoSサービスの制御をおこなうには、「有効」または「無効」を選択してください。

「設定の保存」をクリックしてください。

V．QoS 簡易設定について

[QoS 簡易設定]

「QoS 機能設定」→「簡易設定」をクリックして、以下の画面を開きます。



「QoS 簡易設定」では、最小限の設定項目数で QoS を設定することができます。
設定可能な項目は下記のとおりです。

○インターフェース名
Interface Queueing 設定画面の「Interface 名」に対応します。

○回線帯域
Interface Queueing 設定画面の CBQ Parameter 設定「制限 Rate」に対応します。

○クラス
CLASS 設定画面の「Class ID」に対応します。
簡易設定画面からの設定時に、未使用の ClassID が自動的に設定されます。

○親クラス
CLASS 設定画面の「親 class ID」に対応します。
簡易設定画面からの設定では、自動的に設定されます。(親 classID:1)

○帯域
CLASS 設定画面の「Rate 設定」に対応します。

○プロトコル
○送信元 IP アドレス
○送信元ポート番号
○宛先 IP アドレス
○宛先ポート番号
CLASS 分けフィルタ設定画面の各設定項目に対応しています。
パケットヘッダ情報によるフィルタ条件に相当します。TOS 値、DSCP 値、Marking によるフィルタ設定は未サポートのため未設定状態として設定されます。

○優先度
CLASS 設定画面の「Priority」に対応します。

○帯域借用
CLASS 設定画面の「Bounded 設定」に対応します。

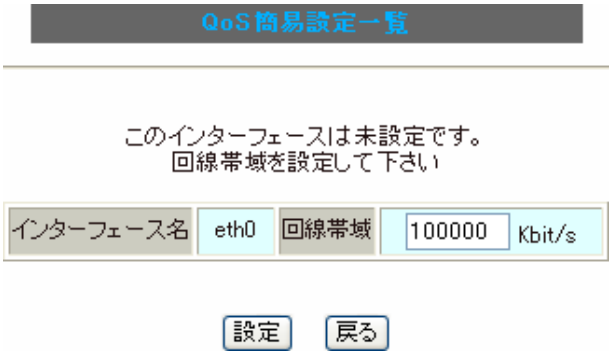
○操作
編集：該当する設定の編集画面に遷移します。
削除：該当する設定の削除をおこないます。

Ⅴ．QoS 簡易設定について

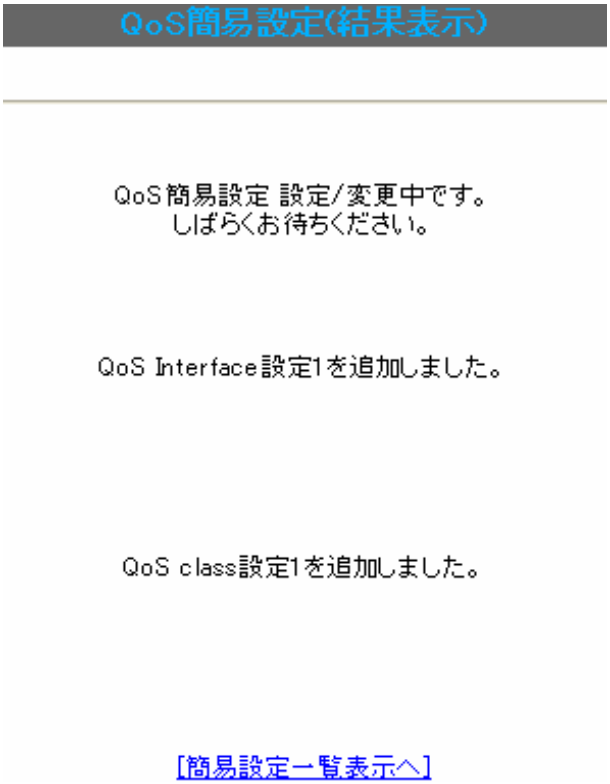
設定方法

インタフェース名の入力欄に表示もしくは編集対象のインタフェース名を入力して、「切替/回線帯域設定」ボタンをクリックしてください。

未設定のインタフェースの場合、回線帯域設定の画面に遷移します（既に設定されている場合は、画面は遷移しません）。
ここで、対象となるインタフェースの回線帯域を入力します。単位は Kbit/s です。
設定可能な範囲：1-102400Kbit/s です。

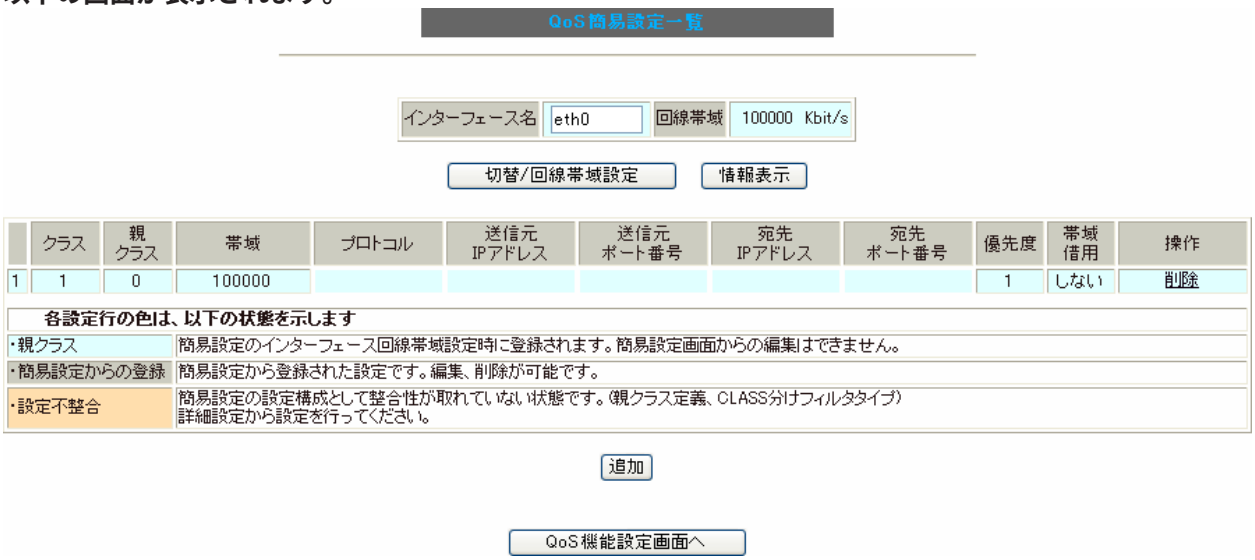


入力が終わりましたら「設定」ボタンをクリックしてください。
クリックした時点で「QoS 詳細設定」の「Interface Queueing 設定」「CLASS 設定」に追加されます。



V．QoS 簡易設定について

[簡易設定一覧表示へ]のリンクをクリックすると、
以下の画面が表示されます。



QoS 簡易設定一覧画面では、あるインタフェースについて設定済みである場合、設定状態により以下の３種類の表示形式で表示されます。

１．親クラス

インタフェース回線帯域設定時に作成される root クラスを示します。クラス ID は”1”、親クラス ID は“０”になります。
簡易設定からの設定の編集は不可、削除のみ可能です。

２．簡易設定からの登録

簡易設定画面からの登録形式である設定（親クラス ID が“１”）を示します。
簡易設定からの設定の編集と削除が可能です。

３．設定不整合

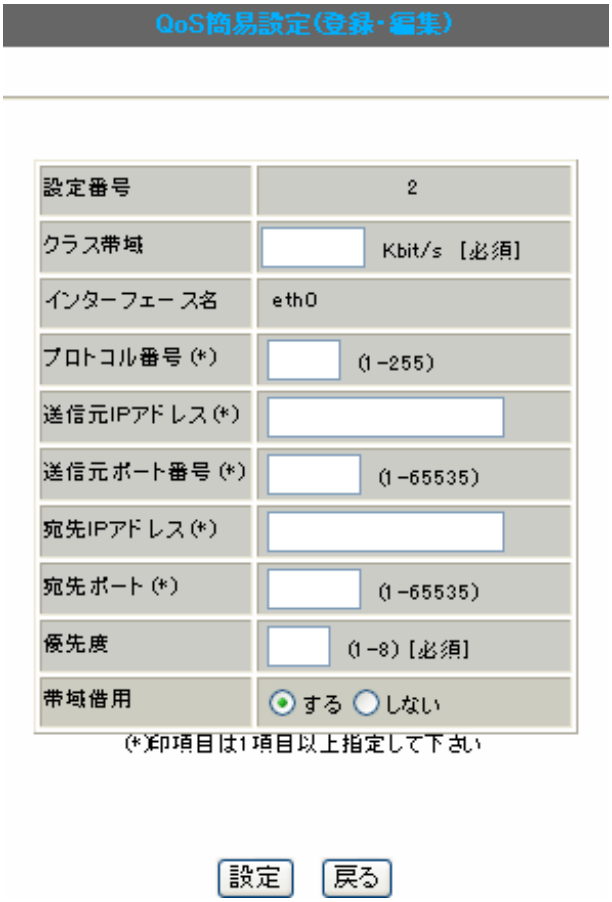
簡易設定画面からの登録形式になっていない設定を示します。

【該当する条件】

- 親クラス ID が“１”以外
- フィルタタイプが Marking である（詳細設定からの指定）
- 「QoS 詳細設定」の「CLASS 設定」画面でフィルタ指定されていない（「CLASS 分けフィルタ設定」と関連付けられていない）

簡易設定からの設定の編集、削除とも不可です。詳細設定からの設定をおこなってください。

新たに設定を追加する場合は「追加」ボタンをクリックしてください。



V．QoS 簡易設定について

○設定番号
簡易設定画面からの設定時に、未使用の設定番号が自動的に設定されます。一覧表示の左に表示される各設定の番号に対応します。

○クラス帯域
簡易簡易設定（登録・編集）画面より設定する条件にマッチするトラフィックを管理するクラスの帯域を指定します。

○インターフェース名
インタフェース毎に切り替えて表示される簡易設定一覧のインタフェース名が表示されます。

○プロトコル番号　(*)
プロトコルを指定します。プロトコル番号で指定してください。

○送信元 IP アドレス　(*)
送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。範囲での指定はできません。

○送信元ポート番号　(*)
送信元ポート番号を指定します。

○宛先 IP アドレス　(*)
宛先IPアドレスを指定します。指定方法は送信元IPアドレスと同様です。

○宛先ポート　(*)
宛先ポート番号を指定します。

○優先度
優先度は各条件で重複可能です。
指定可能範囲：1-8 です。数字の小さいものから順に優先されます。

○帯域借用
兄弟クラスの空き帯域を借りる「する」、借りない「しない」のどちらかを選択します。

(*) 印がある項目は必須設定項目になります。設定項目のうちいずれか１項目以上を設定してください。

入力が終わりましたら「設定」ボタンをクリックしてください。

自動設定項目について

「QoS 簡易設定」から設定をおこなう場合は、「QoS 詳細設定」の「Interface Queueing 設定」や「CLASS 設定」画面でも設定可能な以下の項目について、自動的に設定値を指定します。
「QoS 詳細設定」で設定した内容は上書きされます。

・平均パケットサイズ
　1000

・Class ID
　設定済みクラスの Class ID 最大値 +1

・親 class ID
　1

・Class 内 Average Packet Size 設定
　1000

・Maximum Burst 設定
　100

・Filter 設定
　設定済みクラス分けフィルタ設定のフィルタ番号最大値 +1

　注)
詳細設定で複数のフィルタ番号を設定していた場合、2 番目以降の設定は無い状態で更新されます。

V．QoS 簡易設定について

「操作」欄にある「削除」「編集」について

○削除

リンクをクリックすると、即座に設定が削除されます。

○編集

リンクをクリックすると「QoS 簡易設定（登録・編集)」画面が開きます。

QoS 簡易設定情報表示について

「QoS 簡易設定一覧」画面にある「情報表示」をクリックすると、簡易設定画面で設定されたインタフェース単位の QoS 設定情報が表示されます。

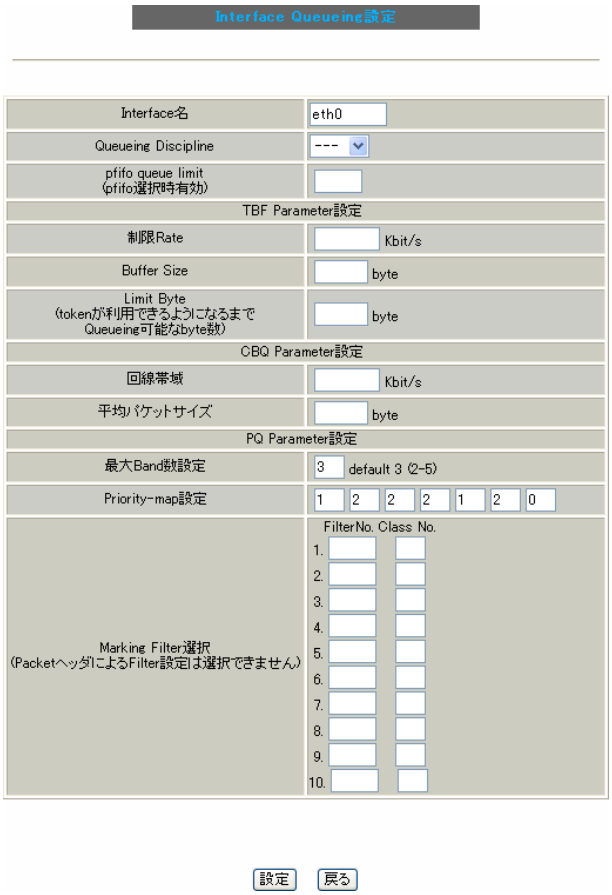
表示内容については「XIII．ステータス情報の表示例」をご参照ください。

VI. Interface Queueing 設定について

Web 画面の「QoS 設定」の「QoS 機能設定」画面から「QoS 詳細設定」を開いてください。

Interface Queueing 設定

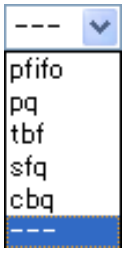
すべてのキューイング方式において設定が必要です。設定を追加するときは「New Entry」をクリックします。



○ Interface 名
キューイングをおこなうインタフェース名を入力します。
インタフェース名は「付録A インタフェース名一覧」を参照してください。

○ Queueing Discipline
プルダウンからキューイング方式を選択します。

- sfq
- pfifo
- tbf
- cbq
- pq



◆SFQ の設定
Queueing Discipline で「sfq」を選択するだけです。

◆PFIFO の設定
○ pfifo queue limit （pfifo 選択時有効）
パケットをキューイングするキューの長さを設定します。**パケットの数**で指定します。
1-10000 の範囲で設定してください。

◆TBF の設定
[TBF Paramater 設定]について設定します。

○制限 Rate
バケツにトークンを入れていく速度を設定します。
回線の実効速度を上限に設定してください。

○ Buffer Size
バケツのサイズを設定します。これは瞬間的に利用できるトークンの最大値となります。帯域の制限幅を大きくするときは、Buffer Size を大きく設定しておきます。

○ Limit Byte
トークンを待っている状態でキューイングするときの、キューのサイズを設定します。

◆CBQ の設定
[CBQ Parameter 設定]について設定します。

○回線帯域
root クラスの帯域幅を設定します。接続回線の物理的な帯域幅を設定します(10BASE-TX で接続しているときは 10000kbits/s)。

VI. Interface Queueing 設定について

○平均パケットサイズ
パケットの平均サイズを設定します。バイト単位で設定します。

◆PQ の設定
[PQ Parameter 設定]について設定します。

○最大 Band 数設定
生成するバンド数を設定します。ここでいう band 数はクラス数のことです。
本装置で設定されるクラス ID は 1001:、1002:、1003:、1004:、1005:となります。
初期設定は 3 です(クラス ID 1001:～1003:)。最大数は 5(クラス ID 1001:～1005:)です。初期設定外の数値に設定した場合は、Priority-map 設定を変更します。

○ Priority-map 設定
Priority-map には 7 つの入れ物が用意されています(左から 0、1、2、3、4、5、6 という番号が付けられています)。そしてそれぞれに Band を設定します。最大 Band 数で設定した範囲で、それぞれに Band を設定できます。

○ Marking Filter 選択
パケットの Marking 情報によって振り分けを決定するときに設定します。

・Filter No.
Class分けフィルタの設定番号を指定します。

・Class No.
パケットをおくるクラス番号を指定します。
(1001:が Class No.1、1002:が Class No.2、1003：が Class No.3、1004：が Class No.4、1005：が Class No.5 となります。)

○ Priority-map の箱に付けられている番号は、TOS 値の「Linux における扱い番号(パケットの優先度)」とリンクしています。本章の「XV.TOS について」をご参照ください。

○インタフェースに届いたパケットは、2 つの方法でクラス分けされます。

・TOS フィールドの「Linux における扱い番号(パケットの優先度)」を参照し、同じ番号の Priority-ma の箱にパケットを送ります。

・Marking Filter 設定に従って、各クラスにパケットを送る

○ Prioritymap の箱に付けられる Band はクラスのことです。箱に設定されている値のクラスに属することを意味します。より Band 数が小さい方が優先度が高くなります。

○クラス分けされたあとのパケットは、優先度の高いクラスから FIFO で送信されていきます。
各クラスの優先度は 1001: > 1002: > 1003: > 1004: > 1005:となります。

○より優先度の高いクラスにパケットがあると、その間は優先度の低いクラスからはパケットが送信されなくなります。

設定後は「設定」ボタンをクリックします。

Ⅶ. CLASS 設定について

CLASS 設定

設定を追加するときは「New Entry」をクリックします。

◯Description
設定名を付けることができます。半角英数字のみ使用可能です。

◯ Interface 名
キューイングをおこなうインタフェース名を入力します。
インタフェース名は「付録A インタフェース名一覧」を参照してください。

◯Class ID
クラス ID を設定します。クラスの階層構造における <minor 番号> となります。

◯親 class ID
親クラスの ID を指定します。クラスの階層構造における <major 番号> となります。

◯ Priority
複数の CLASS 設定での優先度を設定します。値が小さいものほど優先度が高くなります。
1-8 の間で設定します。

◯ Rate 設定
クラスの帯域幅を設定します。設定は kbit/s 単位となります。

◯ Class 内 Average Packet Size 設定
クラス内のパケットの平均サイズを指定します。
設定はバイト単位となります。

◯ Maximum Burst 設定
一度に送信できる最大パケット数を指定します。

◯ Bounded 設定
「有効」を選択すると、兄弟クラスから余っている帯域幅を借りようとはしなくなります(Rate 設定値を超えて通信しません)。
「無効」を選択すると、その逆の動作となります。

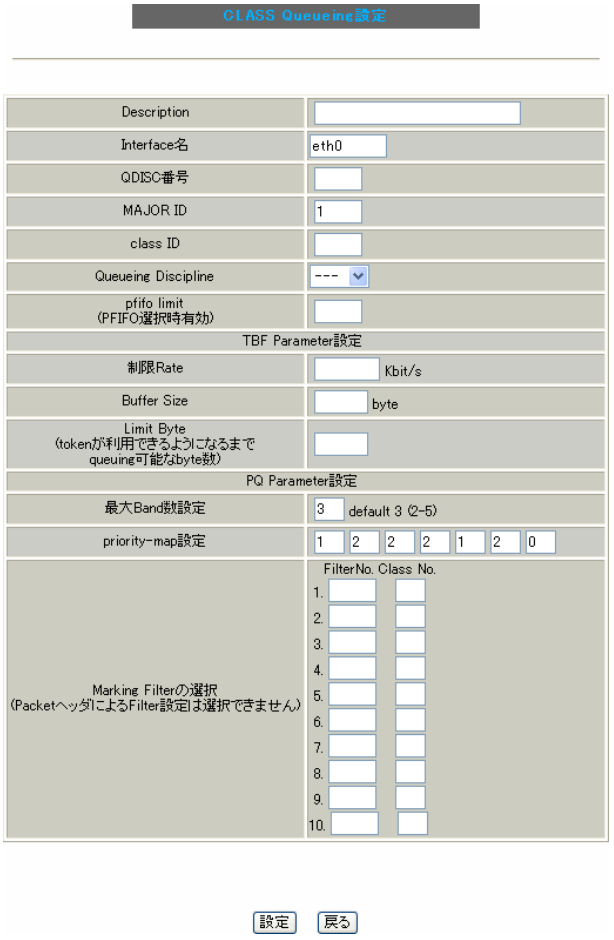
◯ Filter 設定
CLASS 分けフィルタの設定番号を指定します。ここで指定したフィルタにマッチングしたパケットが、このクラスに送られてきます。

設定後は「設定」ボタンをクリックします。

Ⅷ. CLASS Queueing 設定について

CLASS Queueing 設定

設定を追加するときは「New Entry」をクリックします。



○ Description
設定名を付けることができます。半角英数字のみ使用可能です。

○ Interface 名
キューイングをおこなうインタフェース名を選択します。
インタフェース名は「付録A インタフェース名一覧」を参照してください。

○ QDISC 番号
このクラスが属している QDISC 番号を指定します。

○ MAJOR ID
親のクラス ID を指定します。クラスの階層構造における <major 番号> となります。

○ class ID
親クラスの ID を指定します。クラスの階層構造における <minor 番号> となります。

以下は、「**Interface Queueing 設定**」と同様に設定します。
○ Queueing Discipline
「CLASS Queueing 設定」では「cbq」方式の選択はできません。

○ pfifo limit (PFIFO 選択時有効)

[TBF Parameter 設定]
○制限 Rate

○ Buffer Size

○ Limit Byte

[PQ Parameter 設定]
○最大 Band 数設定

○ priority-map 設定

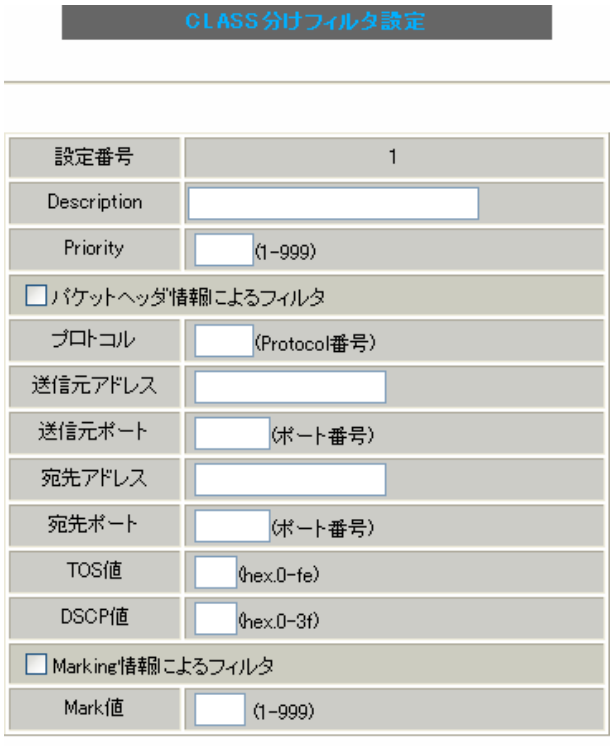
○ Marking Filter の選択

設定後は「設定」ボタンをクリックします。

IX．CLASS 分けフィルタ設定について

CLASS 分けフィルタ設定

設定を追加するときは「New Entry」をクリックします。



○設定番号
自動で未使用の設定番号が振られます。

○ Description
設定名を付けることができます。半角英数字のみ使用可能です。

○ Priority
複数の CLASS 分けフィルタ間での優先度を設定します。値が小さいものほど優先度が高くなります。1-999 の間で設定します。

○パケットヘッダ情報によるフィルタ
パケットヘッダ情報で CLASS 分けをおこなうときにチェックします。以下、マッチ条件を設定していきます。ただし PQ をおこなうときは、パケットヘッダによるフィルタはできません。

○プロトコル
プロトコルを指定します。プロトコル番号で指定してください。

○送信元アドレス
送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。範囲での指定はできません。

○送信元ポート
送信元ポート番号を指定します。
範囲で指定するときは、**始点ポート：終点ポート**の形式で指定します。

○宛先アドレス
宛先 IP アドレスを指定します。指定方法は送信元 IP アドレスと同様です。

○宛先ポート
宛先ポート番号を指定します。
指定方法は送信元ポートと同様です。

○ TOS 値
TOS 値を指定します。16 進数で指定します。

○ DSCP 値
DSCP 値を設定します。16 進数で指定します。

○ Marking 情報によるフィルタ
MARK 値によって CLASS 分けをおこなうときにチェックします。

○ Mark 値
マッチ条件となる Mark 値を、1-999 の間で指定します。PQ でフィルタをおこなうときは Marking 情報によるもののみ有効です。

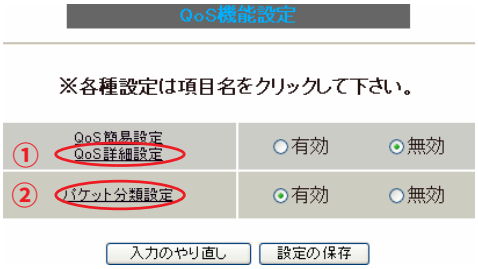
設定後は「設定」ボタンをクリックします。

X．パケット分類設定について

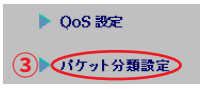
「パケット分類設定」の設定画面を開くには、「QoS 設定」からは以下の２通りと、「パケット分類設定」から直接開く方法があります。

① Web 画面「QoS 設定」→「QoS 詳細設定」
→「パケット分類設定」

② Web 画面「QoS 設定」→「パケット分類設定」



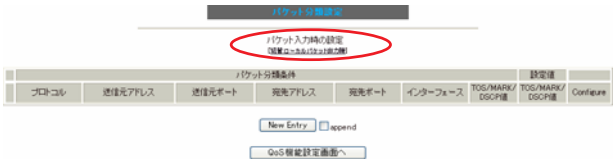
③ Web 画面「パケット分類設定」



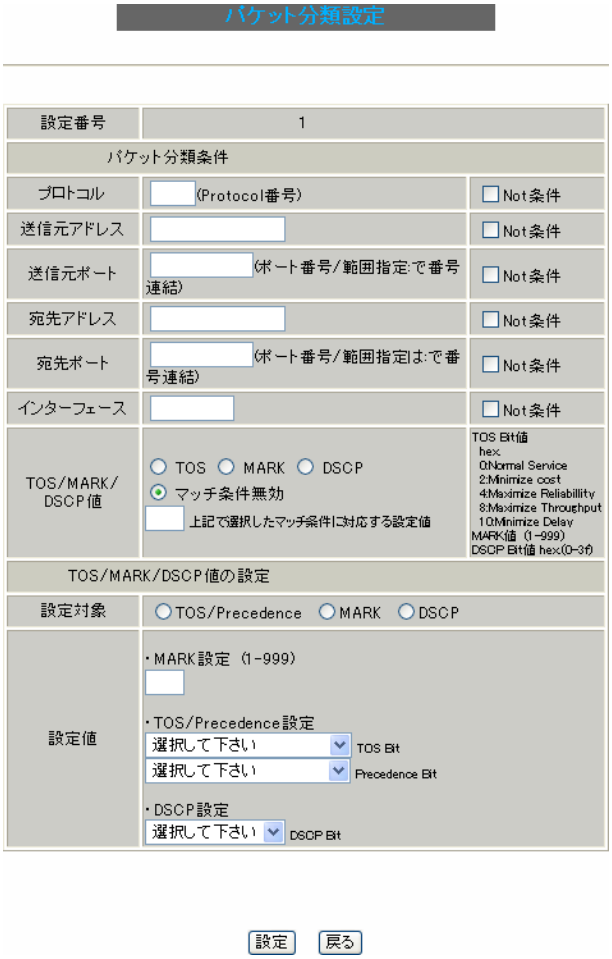
上記３通りいずれの方法でも、同じ「パケット分類設定」画面が表示されます。

パケット分類設定

「パケット入力時の設定」か「ローカルパケット出力時の設定」かを、[切替：]をクリックして選択します。



設定を追加するときは「New Entry」をクリックします。



○設定番号
自動で未使用の設定番号が振られます。

[パケット分類条件]
パケット選別のマッチ条件を定義します。

○プロトコル
プロトコルを指定します。プロトコル番号で指定してください。

○送信元アドレス
送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。範囲での指定はできません。

○送信元ポート
送信元ポート番号を指定します。
範囲で指定するときは、**始点ポート：終点ポート**の形式で指定します。

X．パケット分類設定について

○宛先アドレス
宛先 IP アドレスを指定します。指定方法は送信元 IP アドレスと同様です。

○宛先ポート
宛先ポート番号を指定します。
指定方法は送信元ポートと同様です。

○インターフェース
インタフェースを選択します。
インタフェース名は「付録A インタフェース名一覧」を参照してください。

各項目について「Not 条件」にチェックを付けると、**その項目で指定した値以外のもの**がマッチ条件となります。

○ TOS/MARK/DSCP 値
マッチングする TOS/MARK/DSCP 値を指定します。
TOS、MARK、DSCP のいずれかを選択し、その値を指定します。これらをマッチ条件としないときは「マッチ条件無効」を選択します。

[TOS/MARK/DSCP の値]
パケット分類条件で選別したパケットに、あらたに TOS 値、MARK 値または DSCP 値を設定します。

○設定対象
TOS/Precedence、MARK、DSCP のいずれかを選択します。

○設定値
設定対象で選択したものについて、設定値を指定します。

設定後は「設定」ボタンをクリックします。

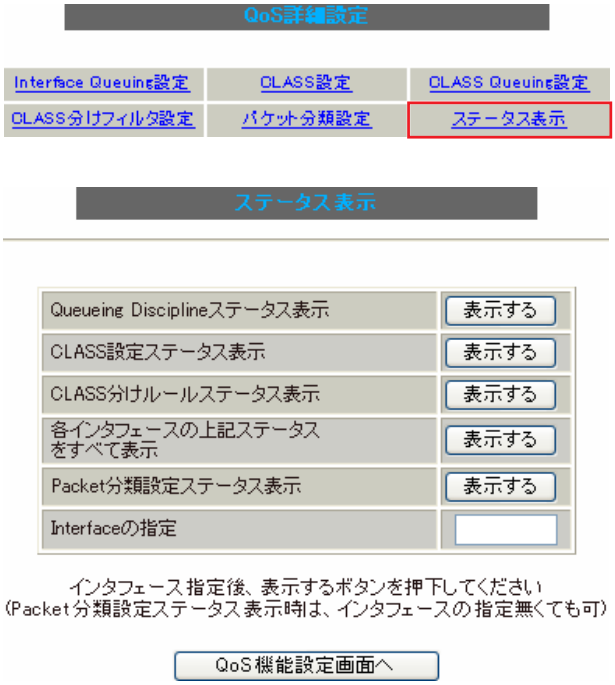
TOS/Precedence および DSCP については章末をご参照ください。

ＸＩ．ステータス表示について

ステータス表示

本機能の設定画面は以下の方法で表示されます。

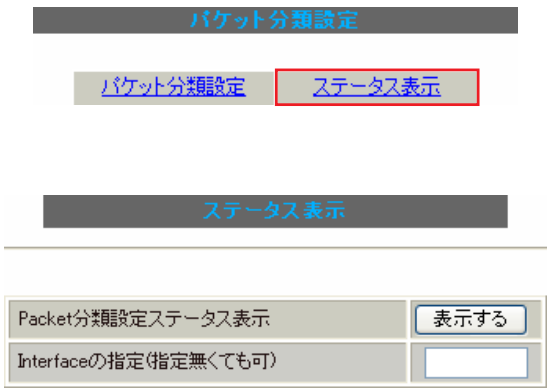
・Web 画面「QoS 設定」→「QoS 詳細設定」→「ステータス表示」



QoS機能の各種ステータスを表示します。
表示したい項目について「表示する」ボタンをクリックしてください。

「Packet 分類設定ステータス表示」以外では、必ず Interface 名を「Interface の指定」に入力してから「表示する」ボタンをクリックしてください。

・Web画面「パケット分類設定」→「ステータス表示」



パケット分類設定のステータス表示では、「Packet 分類設定ステータス表示」のみになります。

「Interface の指定」は必要な場合に入力してください。指定がなくてもステータスは表示されます。

XII．設定の編集・削除方法

各 QoS 設定をおこなうと、設定内容が一覧で表示されます。

(「CLASS 設定」画面の表示例)

○設定の編集をおこなう場合
Configure 欄の「Edit」をクリックすると設定画面に遷移し、その設定を修正できます。

○設定の削除をおこなう場合
Configure 欄の「Remove」をクリックすると、その設定が即座に削除されます。

XIII. ステータス情報の表示例

[Queueing設定情報]表示例

各クラスで設定したキューイング方式や設定パラメータの他、送信したパケット数・送信データサイズ等の情報を表示します。

```
qdisc pfifo 1: limit 300p
 Sent 9386 bytes 82 pkts (dropped 0, overlimits 0)
```

qdisc	キューイング方式
1:	キューイングを設定しているクラスID
limit	キューイングできる最大パケット数
Sent (nnn) byte (mmm) pkts	送信したデータ量とパケット数
dropped	破棄したパケット数
overlimits	過負荷の状態で届いたパケット数

```
qdisc sfq 20: limit 128p quantum 1500b flows 128/1024 perturb 10sec
 Sent 140878 bytes 206 pkts (dropped 0, overlimits 0)
```

limit (nnn)p	キューに待機できるパケット数
quantum	パケットのサイズ
flows (nnn)/(mmm)	mmm個のバケツが用意され、同時にアクティブになるのはnnn個まで
perturb (n)sec	ハッシュの更新間隔

```
qdisc tbf 1: rate 500Kbit burst 1499b/8 mpu 0b lat 4295.0s
 Sent 73050 bytes 568 pkts (dropped 2, overlimits 17)
```

rate	設定している帯域幅
burst	バケツのサイズ
mpu	最小パケットサイズ
lat	パケットがtbfに留まっていられる時間

```
qdisc cbq 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8 weight
1000Kbit allot 1514b
level 2 ewma 5 avpkt 1000b maxidle 242us
 Sent 2420755 bytes 3945 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 6399 undertime 0
```

bounded,isolated	bounded,isolated設定がされている (boundedは帯域を借りない、isolatedは帯域を貸さない)
prio	優先度(上記ではrootクラスなので、prio値はありません)
weight	ラウンドロビンプロセスの重み
allot	送信できるデータサイズ
ewma	指数重み付け移動平均
avpkt	平均パケットサイズ
maxidle	パケット送信時の最大アイドル時間
borrowed	帯域幅を借りて送信したパケット数
avgidle	EMWAで測定した値から、計算したアイドル時間を差し引いた数値 通常は数字がカウントされていますが、負荷で一杯の接続の状態では"0"、 過負荷の状態ではマイナスの値になります

XIII. ステータス情報の表示例

[CLASS 設定情報]表示例
設定している各クラスの情報を表示します。

その 1 <CBQ での表示例>

```
class cbq 1: root rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8
weight 1000Kbit allot 1514b
level 2 ewma 5 avpkt 1000b maxidle 242us
 Sent 33382 bytes 108 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 6399 undertime 0
class cbq 1:10 parent 1:1 rate 500Kbit cell 8b mpu 64b prio 1/1 weight 50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
 Sent 0 bytes 0 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 181651 undertime 0
class cbq 1:1 parent 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio 3/3 weight
100Kbit allot 1500b
level 1 ewma 5 avpkt 1000b maxidle 242us
 Sent 2388712 bytes 3843 pkts (dropped 0, overlimits 0)
  borrowed 2004 overactions 0 avgidle 6399 undertime 0
class cbq 1:20 parent 1:1 leaf 20: rate 500Kbit cell 8b mpu 64b (bounded) prio 2/2 weight
50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
 Sent 142217 bytes 212 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 174789 undertime 0
```

parent	親クラスID

その 2 <PQ での表示例>

```
class prio 1: parent 1: leaf 1001:
class prio 1: parent 1: leaf 1002:
class prio 1: parent 1: leaf 1003:
```

prio	優先度
parent	親クラスID
leaf	leafクラスID

XIII. ステータス情報の表示例

[CLASS分けフィルタ設定情報]表示例

クラス分けフィルタの設定情報を表示します。

その 1 <CBQ での表示例>

```
[ PARENT 1: ]
filter protocol ip pref 1 u32
filter protocol ip pref 1 u32 fh 805: ht divisor 1
filter protocol ip pref 1 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 1 u32 fh 804: ht divisor 1
filter protocol ip pref 1 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32
filter protocol ip pref 3 u32 fh 805: ht divisor 1
filter protocol ip pref 3 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32 fh 804: ht divisor 1
filter protocol ip pref 3 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
```

protocol	マッチするプロトコル
pref	優先度
u32	パケット内部のフィールド(発信元IPアドレスなど)に基づいて処理すべきクラスの決定をおこないます。
at 8、at16	マッチの開始は、指定した数値分のオフセットからであることを示します。 at 8であれば、ヘッダの9バイトめからマッチします。
flowid	マッチしたパケットを送るクラス

その 2 <PQ での表示例>

```
[ PARENT 1: ]
filter protocol ip pref 1 fw
filter protocol ip pref 1 fw handle 0x1 classid 1:3
filter protocol ip pref 2 fw
filter protocol ip pref 2 fw handle 0x2 classid 1:2
filter protocol ip pref 3 fw
filter protocol ip pref 3 fw handle 0x3 classid 1:1
```

pref	優先度
handle	TOSまたはMARK値
classid	マッチパケットを送るクラスID クラスID 1:(n) のとき、100(n):に送られます。

XIII. ステータス情報の表示例

[Packet 分類設定情報]表示例

パケット分類設定の情報を表示します。

```
 pkts bytes target     prot opt in     out     source               destination
  272 39111 MARK       all  --  eth0   any     192.168.120.111      anywhere            MARK set 0x1
   83  5439 MARK       all  --  eth0   any     192.168.120.113      anywhere            MARK set 0x2
  447 48695 MARK       all  --  eth0   any     192.168.0.0/24       anywhere            MARK set 0x3
    0     0  FTOS       tcp  --  eth0   any      192.168.0.1          111.111.111.111    tcp spts:1024:
65535 dpt:450 Type of Service set 0x62
```

pkts	入力(出力)されたパケット数
bytes	入力(出力)されたバイト数
target	分類の対象(MARKかTOSか)
prot	プロトコル
in	パケット入力インタフェース
out	パケット出力インタフェース
source	送信元IPアドレス
destination	あて先IPアドレス
MARK set	セットするMARK値
spts	送信元ポート番号
dpt	あて先ポート番号
Type of Service set	セットするTOSビット値

XIV．クラスの階層構造について

CBQにおけるクラスの階層構造は以下のようになります。

◆root クラス
ネットワークデバイス上のキューイングです。
本装置のシステムが直接的に対話するのはこのクラスです。

◆親クラス
すべてのクラスのベースとなるクラスです。帯域幅を 100%として定義します。

◆子クラス
親クラスから分岐するクラスです。親クラスの持つ帯域幅を分割して、それぞれの子クラスの帯域幅として持ちます。

◆leaf(葉)クラス
leaf クラスは自分から分岐するクラスがないクラスです。

◆qdisc
キューイングです。ここでキューを管理・制御します。

[クラス ID について]
各クラスはクラス ID を持ちます。クラス ID は MAJOR 番号と MINOR 番号の 2 つからなります。表記は以下のようになります。

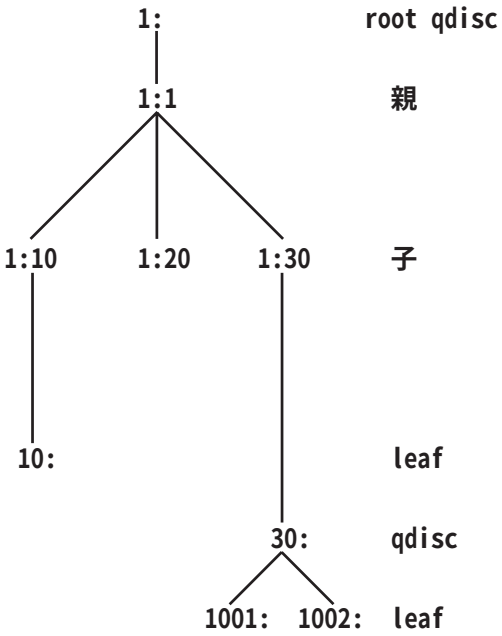
<MAJOR 番号>：<MINOR 番号>

・root クラスは「1:0」というクラス ID を持ちます。

・子クラスは、親と同じ MAJOR 番号を持つ必要があります。

・MINOR 番号は、他のクラスと qdisc 内で重複しないように定義する必要があります。

<クラス構成図　例>



XV. TOS について

IP パケットヘッダには TOS フィールドが設けられています。ここにパケットの優先度情報を付与しておくことで、優先度にあわせて機器がパケットを適切に扱えることを期待します。

IP ヘッダ内の TOS フィールドの各ビットは、以下のように定義されています。<表 1>

バイナリ	10 進数	意味
1000	8	Minimize delay (md)
0100	4	Maximize throughput (mt)
0010	2	Maximize reliability (mr)
0001	1	Minimize monetary cost (mmc)
0000	0	Normal Service

md は最小の遅延、mt は最高のスループット、mr は高い信頼性、mmc は低い通信コスト、を期待するパケットであることを示します。

各ビットの組み合わせによる TOS 値は以下のように定義されます。<表 2>

TOS	ビット	意味	Linux での扱い	バンド
0x0	0	Normal Service	0 Best Effort	1
0x2	1	Minimize Monetary Cost	1 Filler	2
0x4	2	Maximize Reliability	0 Best Effort	1
0x6	3	mmc+mr	0 Best Effort	1
0x8	4	Maximize Throughput	2 Bulk	2
0xa	5	mmc+mt	2 Bulk	2
0xc	6	mr+mt	2 Bulk	2
0xe	7	mmc+mr+mt	2 Bulk	2
0x10	8	Minimize Delay	6 Interactive	0
0x12	9	mmc+md	6 Interactive	0
0x14	10	mr+md	6 Interactive	0
0x16	11	mmc+mr+md	6 Interactive	0
0x18	12	mt+md	4 Int. Bulk	1
0x1a	13	mmc+mt+md	4 Int. Bulk	1
0x1c	14	mr+mt+md	4 Int. Bulk	1
0x1e	15	mmc+mr+mt+md	4 Int. Bulk	1

バンドは優先度です。0 が最も優先度が高いものです。初期値ではバンド数は 3(優先度は 3 段階)です。本装置では、PQ Paramater 設定の「最大 Band 数設定」でバンド数を変更できます(0 ～ 4)。

Linux での扱いの数値は、Linux での TOS ビット列の解釈です。これは PQ Paramater 設定の「Priority-map 設定」の箱にリンクしており、対応する Priority-map の箱に送られます。

XV．TOS について

またアプリケーションごとのパケットの取り扱い方法も定義されています(RFC1349)。
アプリケーションの TOS 値は以下のようになっています。<表 3>

アプリケーション	TOS ビット値	定義
TELNET	1000	(minimize delay)
FTP		
Control	1000	(minimize delay)
Data	0100	(maximize throughput)
TFTP	1000	(minimize delay)
SMTP		
Command phase	1000	(minimize delay)
DATA phase	0100	(maximize throughput)
Domain Name Service		
UDP Query	1000	(minimize delay)
TCP Query	0000	
Zone Transfer	0100	(maximize throughput)
NNTP	0001	(minimize monetary cost)
ICMP		
Errors	0000	
Requests	0000 (mostly)	
Responses	<same as request>	(mostly)

※表中の TOS ビット値(2 進数表記)が、<表 2>のビットに対応しています。

TOS 値は定義があいまいで相互運用できない、正しい値が設定されている保証がない、悪用される可能性があるなどの要因により、現在までほとんど使われていません。

XVI．DSCP について

本装置では DS(DiffServ)フィールドの設定・書き換えも可能です。DS フィールドとは、IP パケット内の TOS の再定義フィールドであり、DiffServ に対応したネットワークにおいて QoS 制御動作の基準となる値が設定されます。DiffServ 対応機器では、DS フィールド内の DSCP 値だけを参照して QoS 制御をおこなうことができます。

○ TOS と DS フィールドのビット定義

【TOS フィールド構造】

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
|Precedence |Type of Service|CU |
+---+---+---+---+---+---+---+---+
```

【DSCP フィールド構造】

```
  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+---+
|           DSCP        |   CU  |
+---+---+---+---+---+---+---+---+
```

DSCP: differentiated services code point

CU: currently unused（現在未使用）

DSCPビットのとりうる値とその制御方法の定義は以下のようになっています。

定義名	DSCP値	制御方法
EF(Expedited Forwarding)	0x2e	パケットを最優先で転送(RFC3246)
AF(Assured Forwarding) AF11/AF12/AF13 AF21/AF22/AF23 AF31/AF32/AF33 AF41/AF42/AF43	 0x0a / 0x0c / 0x0e 0x12 / 0x14 / 0x16 0x1a / 0x1c / 0x1e 0x22 / 0x24 / 0x26	4つの送出優先度と3つの廃棄優先度を持ち、数字の上位桁は送出優先度(クラス)、下位桁は廃棄優先度を表します。(RFC2597) ・送出優先度　(高) 1 > 2 > 3 > 4 (低) ・廃棄優先度　(高) 1 > 2 > 3 (低)
CS(Class Selector) CS1 CS2 CS3 CS4 CS5 CS6 CS7	 0x08 0x10 0x18 0x20 0x28 0x30 0x38	既存のTOS互換による優先制御をおこないます。 Precedence1(Priority) Precedence2(Immediate) Precedence3(Flash) Precedence4(Flash Override) Precedence5(Critic/ESP) Precedence6(Internetwork Control) Precedence7(Network Control)
BE (Best Effort)	0x00	ベストエフォート(優先制御なし)

第 31 章

Web 認証機能

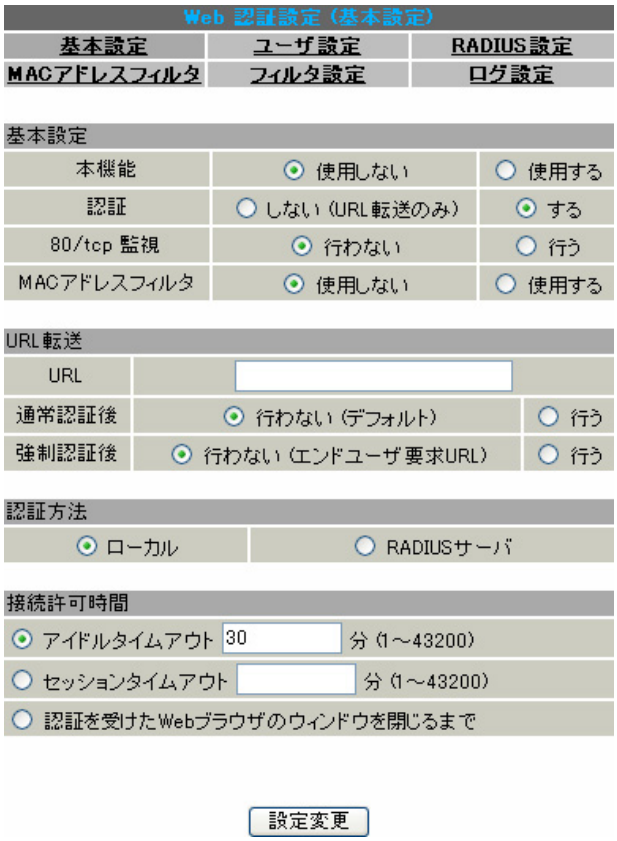
Ⅰ．Web 認証機能の設定

「Web 認証機能」は、本装置を経由して外部にアクセスをする場合に、本装置での認証を必要とする機能です。
この機能を使うことで、外部へアクセスできるユーザーを管理できるようになります。

実行方法

Web 設定画面で「Web 認証設定」をクリックして、各設定をおこないます。

◆基本設定



[基本設定]

○本機能

Web 認証機能を使う場合は「使用する」を選択します。

○認証

当機能を使用していて、かつ認証をおこなうときは「する」を選択します(初期設定)。
認証をおこなわないときは「しない(URL 転送のみ)」を選択します。このときは、外部へのアクセスをリダイレクトするだけの動作となります。

○80/tcp 監視

認証を受けていない IP アドレスからの TCP ポート 80 番のコネクションを監視し、**このコネクションがあったときに、強制的に Web 認証をおこないます。**
初期設定は監視を「行わない」設定となります。

○MAC アドレスフィルタ

MAC アドレスフィルタを有効にする場合は「使用する」を選択します。

[URL 転送]

○URL

転送先の URL を設定します。

○通常認証後

「行う」を選択すると、Web 認証後に「URL」で指定したサイトに転送させることができます。
初期設定では URL 転送をおこないません。

○強制認証後

「行う」を選択すると、強制認証後に「URL」で指定したサイトに転送させることができます。
初期設定では URL 転送をおこないません。この機能を使う場合は「80/tcp 監視」を有効にしてください。

[認証方法]

○ローカル

本装置でアカウントを管理 / 認証します。

○RADIUS サーバ

外部の RADIUS サーバでアカウントを管理 / 認証します。

Ⅰ．Web 認証機能の設定

[接続許可時間]

○接続許可時間

認証したあとの、ユーザーの接続形態を選択できます。

○アイドルタイムアウト

認証で許可された通信が無通信状態となってから切断するまでの時間を設定します。

○セッションタイムアウト

認証で許可された通信を強制的に切断するまでの時間を設定します。

認証してからこの時間が経過すると、通信状態にかかわらず通信を切断します。

○認証を受けた Web ブラウザのウィンドウを閉じるまで

認証を受けた後にブラウザに表示された画面を閉じたときに、通信を切断します。

通信可能な状態を保つには、認証後の画面を開いたままにしなければなりません。Web ブラウジングをする場合は、別のブラウザを開く必要があります。

上記設定にしたがって通信が切断した場合は、各ユーザーは再度Web 認証を実行する必要があります。

最後に「設定変更」をクリックしてください。

Web 認証機能を「使用する」にした場合はただちに機能が有効となりますので、ユーザー設定等から設定をおこなってください。

◆ユーザー設定

設定可能なユーザの最大数は 64 です。

画面最下部にある「ユーザ設定画面インデックス」のリンクをクリックしてください。

Web 認証設定 (ユーザ設定)

基本設定	ユーザ設定	RADIUS設定
MACアドレスフィルタ	フィルタ設定	ログ設定

No.1～16まで

No.	ユーザID	パスワード	削除
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

設定/削除の実行

ユーザ設定画面インデックス

001- 017- 033- 049-

○ユーザ ID

○パスワード

ユーザアカウントを登録します。

ユーザ ID・パスワードには半角英数字で設定してください。空白やコロン(:)は含めることができません。

○削除

チェックすると、その設定が削除対象となります。

最後に「設定 / 削除の実行」をクリックしてください。

Ⅰ．Web 認証機能の設定

◆RADIUS 設定

「基本設定」において、認証方法を「RADIUS サーバ」に設定した場合にのみ設定します。

[プライマリサーバ設定]

プライマリサーバ項目の設定は必須です。

○ IP アドレス

○ポート番号

○ secret

RADIUS サーバの IP アドレス、ポート番号、secret を設定します。

[セカンダリサーバ設定]

セカンダリ項目の設定はなくてもかまいません。

○ IP アドレス

○ポート番号

○ secret

設定はプライマリサーバ設定と同様です。

[サーバ共通設定]

RADIUS サーバへ問い合わせをする際に送信する NAS の情報を設定します。RADUIS サーバが、どの NAS かを識別するために使います。どちらかの設定が必須です。

○ NAS-IP-Address

通常は本装置の IP アドレスを設定します。

○ NAS-Identifier

任意の文字列を設定します。

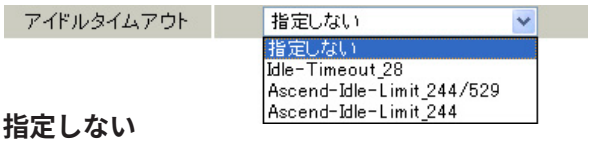
半角英数字が使用できます。

[接続許可時間（RADIUS サーバから送信されるアトリビュートの指定)]

それぞれ、基本設定で選択されているものが有効となります。

○アイドルタイムアウト

プルダウンの以下の項目から選択してください。



・指定しない

RADIUS サーバからの認証応答に該当のアトリビュートがあればその値を使います。

該当のアトリビュートがなければ「基本設定」で設定した値を使用します。

・Idle-Timeout_28

Idle-Timeout (Type=28)をアイドルタイムアウト値として使用します。

・Ascend-Idle-Limit_244/529

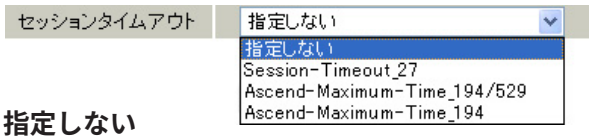
Ascend-Idle-Limit (Vendor-Specific Attribute Type=26, Vendor-Id=529, Attribute Type=244) をアイドルタイムアウト値として使用します。

・Ascend-Idle-Limit_244

Ascend-Idle-Limit (Type=244) をアイドルタイムアウト値として使用します。

Ⅰ．Web 認証機能の設定

○セッションタイムアウト
プルダウンの以下の項目から選択してください。



・指定しない
RADIUSサーバからの認証応答に該当のアトリビュートがあればその値を使います。
該当のアトリビュートがなければ「基本設定」で設定した値を使用します。

・Session-Timeout_27
Session-Timeout (Type=27)をセッションタイムアウト値として使用します。

・Ascend-Maximum-Time_194/529
Ascend-Maximum-Time (Vendor-Specific Attribute Type=26, Vendor-Id=529, Attribute Type=194)をセッションタイムアウト値として使用します。

・Ascend-Maximum-Time_194
Ascend-Maximum-Time (Type=194)をセッションタイムアウト値として使用します。

※ アトリビュートとは、RADIUSで設定されるパラメータのことを指します。

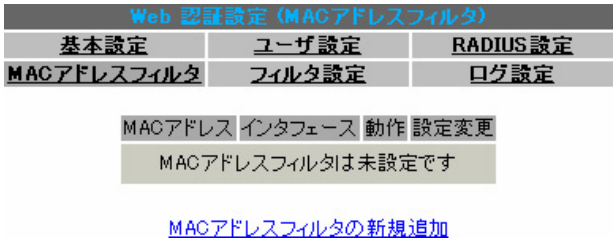
最後に「設定変更」をクリックしてください。

Ⅰ．Web 認証機能の設定

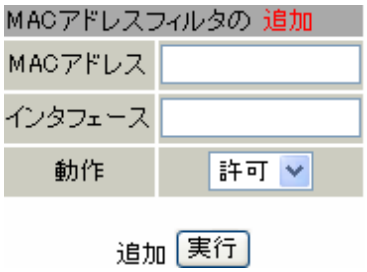
◆MAC アドレスフィルタ

Web 認証機能を有効にすると、外部との通信は認証が必要となりますが、MAC アドレスフィルタを設定することによって認証を必要とせずに通信が可能になります。

本機能で設定した MAC アドレスを送信元 MAC アドレスとする IP パケットの転送がおこなわれると、それ以降はその IP アドレスを送信元 / 送信先とする IP パケットの転送を許可します。
ここで設定する MAC アドレスは、転送許可を最初に決定する場合に用いられます。



「基本設定」で MAC アドレスフィルタを「使用する」に選択して、「MAC アドレスフィルタ」設定画面「MAC アドレスフィルタの新規追加」をクリックします。



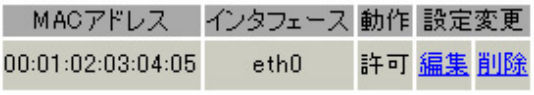
[MAC アドレスフィルタの 追加]

○ MAC アドレス
フィルタリング対象とする、送信元 MAC アドレスを入力します。

○インタフェース
フィルタリングをおこなうインタフェース名を入力します（任意で指定）。
本装置のインタフェース名については、本マニュアルの「付録 A」をご参照ください。

○動作
フィルタリング設定にマッチしたときにパケットを破棄するか通過させるかを選択します。

入力が終わりましたら、「実行」をクリックして設定完了です。
設定をおこなうと設定内容が一覧表示されます。



一覧表示からは、設定の編集・削除をおこなう事ができます。

○編集
編集したい設定の行にある「編集」ボタンをクリックしてください。
「インタフェース」と「動作」の設定が変更できます。

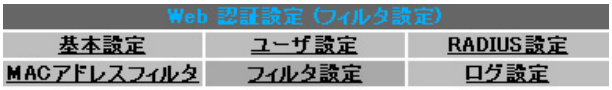
○削除
削除したい設定の行にある「削除」ボタンをクリックしてください。
削除確認画面が表示されます。「実行」ボタンをクリックすると設定の削除がおこなわれます。

Ⅰ．Web 認証機能の設定

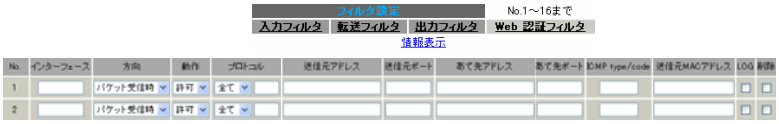
◆フィルタ設定

Web 認証機能を有効にすると外部との通信は認証が必要となりますが、フィルタ設定によって認証を必要とせずに通信可能にできます。
「特定のポートだけは常に通信できるようにしたい」といった場合に設定します。

設定画面「フィルタ設定」をクリックします。



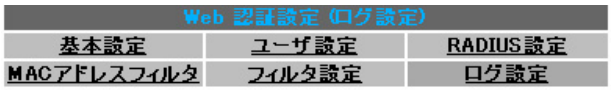
上記のメッセージが表示されたらリンクをクリックしてください。
「Web 認証フィルタ」設定画面に移ります。

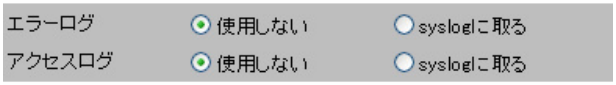


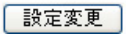
ここで設定した IP アドレスやポートについては、Web 認証機能によらず、通信可能になります。
設定方法については「第 26 章 パケットフィルタリング機能」をご参照ください。

◆ログ設定

Web 認証機能のログを本装置のシステムログに出力できます。







ログを取得するかどうかを選択します。

○エラーログ
Web 認証時のログインエラーを出力します。

<エラーログの表示例>

```
Apr  7 17:04:45 localhost httpd[21529]:
[error] [client 192.168.0.1] user abc: au-
thentication failure for "/": password mis-
match
```

○アクセスログ
Web 認証時のアクセスログを出力します。

<アクセスログの表示例>

```
Apr  7 17:04:49 localhost authgw: 192.168.0.1
- abc [07/Apr/2003:17:04:49 +0900] "GET /
HTTP/1.1" 200 353
```

II . Web 認証下のアクセス方法

ホストからのアクセス方法

1 ホストから本装置にアクセスします。
以下の形式でアドレスを指定してアクセスします。

http://<本装置の IP アドレス>/login.cgi

2 認証画面がポップアップしますので、通知されているユーザー ID とパスワードを入力します。

3 認証に成功すると以下のメッセージが表示され、本装置を経由して外部にアクセスできるようになります。

<認証成功時の表示例>
You can connect to the External Network (abc@192.168.0.1).

Date: Mon Apr 7 10:06:51 2003

設定画面へのアクセスについて

Web 認証機能を使用していて認証をおこなっていなくても、本装置の設定画面にはアクセスすることができます。
アクセス方法は、通常と同じです。

RADIUS 設定について

認証方法を「RADIUS サーバ」に選択した場合、本装置は RADIUS サーバに対して認証要求のみを送信します。

RADIUS サーバへの要求はタイムアウトが 5 秒、リトライが最大 3 回です。
プライマリサーバから応答がない場合は、セカンダリサーバに要求を送信します。

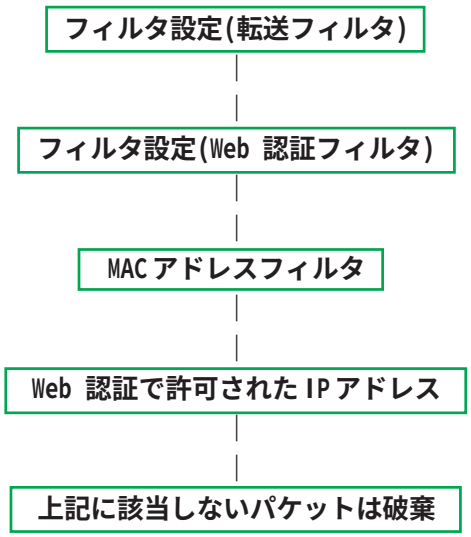
認証について

認証方法が「ローカル」、「RADIUS サーバ」のどちらの場合でも、クライアント - 本装置間の認証には、HTTP Basic 認証が用いられます。
また、「RADIUS サーバ」を使用する場合、本装置 - RADIUS サーバ間は User-Password を用いた認証 (PAP) がおこなわれます。

III. Web 認証の制御方法について

Web 認証機能はパケットフィルタの一種で、認証で許可されたユーザー(ホスト)の IP アドレスを送信元 / あて先に持つ転送パケットのみを通過させます。制御は、転送フィルタ設定の最後でおこなわれます。

フィルタリング制御の順番は以下の通りです。



Web 認証機能を使わない場合は、通常の「転送フィルタ」のみ有効となります。

「転送フィルタ」に設定をしてしまうと、Web 認証よりも優先してそのフィルタが参照されてしまい、Web 認証が有効に機能しなくなる恐れがあります。

Web 認証機能を使用する場合は、「転送フィルタ」には何も設定せずに運用してください。

第 32 章

ネットワークテスト

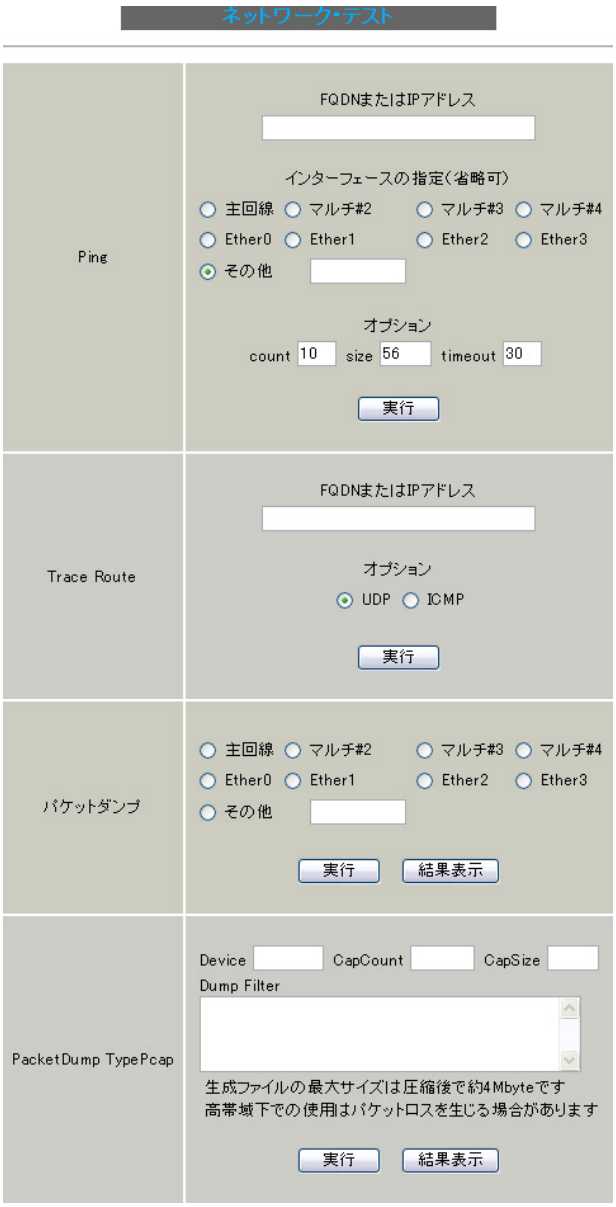
ネットワークテスト

本装置の運用時において、ネットワークテストをおこなうことができます。ネットワークのトラブルシューティングに有効です。以下の 3 つのテストができます。

- **Ping テスト**
- **Trace Route テスト**
- **パケットダンプの取得**

実行方法

Web 設定画面「ネットワークテスト」をクリックして、以下の画面でテストを実行します。



[Ping テスト]

指定した相手に本装置から Ping を発信します。

○ FQDN または IP アドレス
FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

○インターフェースの指定（省略可）
ping パケットを送信するインタフェースを選択できます。省略することもできます。

○オプション

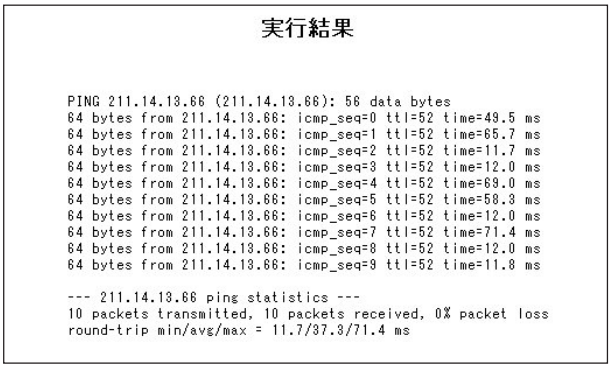
・count
送信する ping パケット数を指定します。
入力可能な範囲：1-10 です。 初期値は 10 です。

・size
送信するデータサイズ(byte)を指定します。
入力可能な範囲：56-1500 です。初期値は 56 です(8 バイトの ICMP ヘッダが追加されるため、64 バイトの ICMP データが送信されます)。

・timeout
ping コマンドの起動時間を指定します。
入力可能な範囲：1-30 です。初期値は 30 です。

入力が終わりましたら「実行」をクリックします。

実行結果例



ネットワークテスト

[Trace Route テスト]
指定した宛先までに経由するルータの情報を表示します。

○ FQDN または IP アドレス
FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

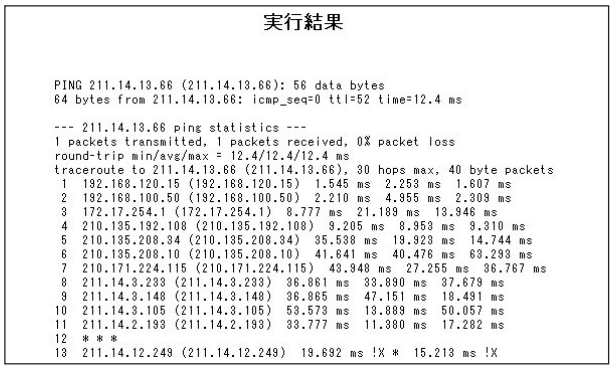
○オプション

・UDP
UDP パケットを使用する場合に指定します。
初期設定は UDP です。

・ICMP
ICMP パケットを使用する場合に指定します。

入力が終わりましたら「実行」をクリックします。

実行結果例



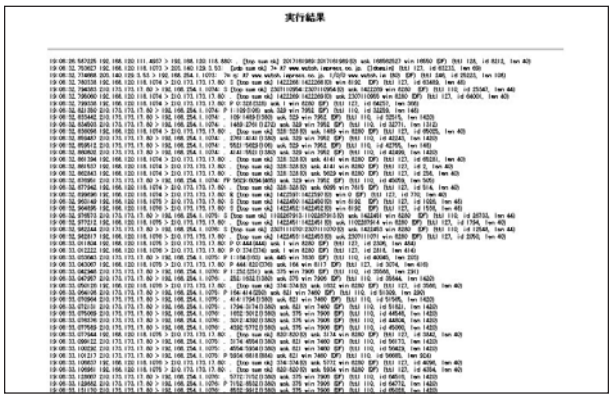
Ping・Trace Route テストで応答メッセージが表示されない場合は、DNS で名前解決ができていない可能性があります。その場合はまず、IP アドレスを直接指定してご確認ください。

[パケットダンプテスト]
パケットのダンプを取得できます。
ダンプを取得したいインタフェースを選択して「実行」をクリックします。

インタフェースについては「その他」を選択し、直接インタフェースを指定することもできます。
その場合はインタフェース名(「gre1」や「ipsec0」など)を指定してください。

その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例



「結果表示」をクリックするたびに、表示結果が更新されます。
パケットダンプの表示は、最大で 100 パケット分までです。100 パケット分を超えると、古いものから順に表示されなくなります。

ネットワークテスト

[PacketDump TypePcap テスト]
拡張版パケットダンプ取得機能です。
指定したインタフェースで、指定した数のパケットダンプを取得できます。

○ Device
パケットダンプを実行する、本装置のインタフェース名を設定します。インタフェース名は本書「付録 A インタフェース名一覧」をご参照ください。

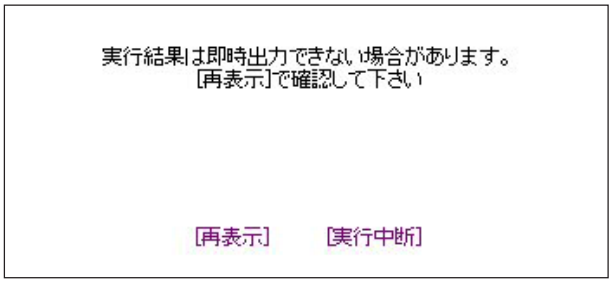
○ CapCount
パケットダンプの取得数を指定します。
1-999999 の間で指定します。

○ CapSize
1 パケットごとのダンプデータの最大サイズを指定できます。単位は " byte " です。
たとえば 128 と設定すると、128 バイト以上の長さのパケットでも 128 バイト分だけをダンプします。大きなサイズでダンプするときは、本装置への負荷が増加することがあります。また記録できるダンプ数も減少します。

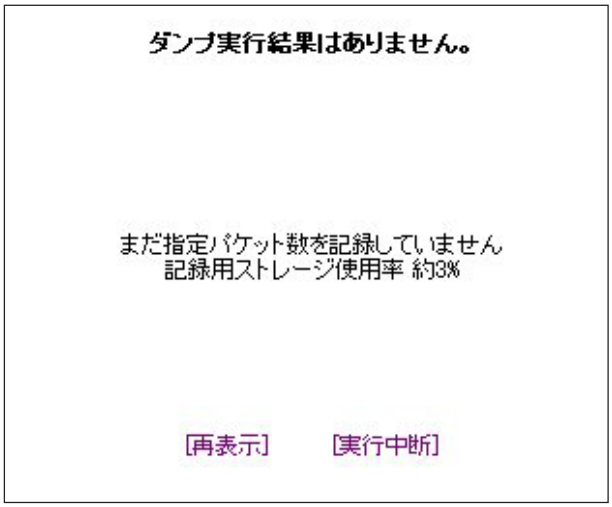
○ Dump Filter
ここに文字列を指定して、それに合致するダンプ内容のみを取得できます。空白・大小文字も判別します。一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したパケットダンプ内容のみ抽出して記録します。

入力後、「実行」ボタンでパケットダンプを開始します。

パケットダンプを開始したときの画面表示

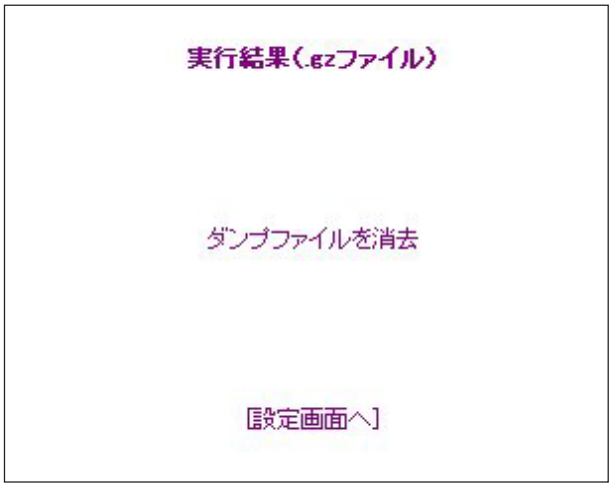


また、パケットダンプ実行中に「再表示」ボタンをクリックすると、下記のような画面が表示されます。



ネットワークテスト

パケットダンプが実行終了したときの画面



「Count」で指定した数のパケットダンプを取得したとき、「実行中断」ボタンをクリックしたとき、またはパケットダンプ取得終了後に「結果表示」をクリックしたとき、上記の画面が表示されます。

「実行結果(.gz ファイル)」リンクから、パケットダンプ結果を圧縮したファイルをローカルホストに保存してください。

ローカルホスト上で解凍してできたファイルは、Ethereal で閲覧することができます。

「ダンプファイルを消去」をクリックすると、本装置に記録されているダンプファイルを消去します。

[PacketDump TypePcap の注意点]

- 取得したパケットダンプ結果は、libcap 形式で gzip 圧縮して保存されます。
- 取得できるデータサイズは、gzip 圧縮された状態で最大約 4MB です。
- 本装置上にはパケットダンプ結果を 1 つだけ記録しておけます。パケットダンプ結果を消去せずに PacketDump TypePcap を再実行して実行結果ファイルを作成したときは、それまでに記録されていたパケットダンプ結果に上書きされます。

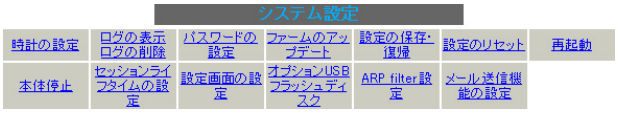
本装置のインタフェース名については本書の**「付録 A インタフェース名一覧」**をご参照ください。

第 33 章

システム設定

システム設定

「システム設定」メニューでは、本装置の運用に関する制御をおこないます。
下記の項目に関して設定・制御が可能です。



- 時計の設定
- ログの表示 / 削除
- パスワードの設定
- ファームウェアアップデート
- 設定の保存・復帰
- 設定のリセット
- 再起動
- 本体停止
- セッションライフタイムの設定
- 設定画面の設定
- オプション USB フラッシュディスクの操作
- ARP filter 設定
- メール送信機能の設定

実行方法

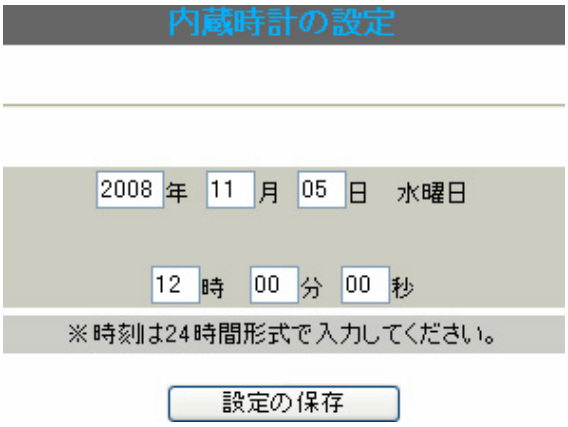
Web 設定画面「システム設定」をクリックします。
各項目のページへは、設定画面上部のリンクをクリックして移動します。

◆時計の設定

本装置内蔵時計の設定をおこないます。

設定方法

「時計の設定」をクリックして設定画面を開きます。



24 時間単位で時刻を設定してください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

システム設定

◆ログの表示

本装置のログが全てここで表示されます。

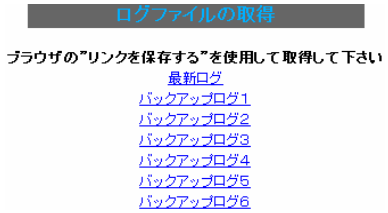
実行方法

「ログの表示」をクリックして表示画面を開きます。

「表示の更新」ボタンをクリックすると表示が更新されます。

本装置自身に保存されるログファイルは、最大で６つです。
本装置で初期化済みのオプション USB ディスク装着時は、USB ディスクに最大で５つのログファイルを保存します。

ログファイルが作成されたときは画面上にリンクが生成されます。
古いログファイルから順に削除されていきます。



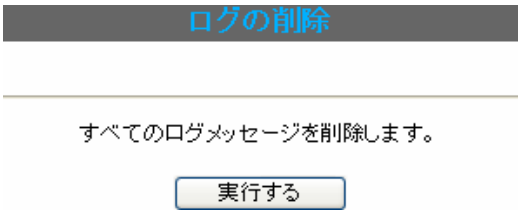
（本装置内部へのログ保存時のリンク）

◆ログの削除

ログ情報は最大 2MB までのサイズで保存されます。また再起動時にログ情報は削除されます。手動で削除する場合は次のようにしてください。

実行方法

「ログの削除」をクリックして画面を開きます。



「実行する」ボタンをクリックすると、保存されているログが**全て削除**されます。

本体の再起動をおこなった場合も、それまでのログは全てクリアされます。

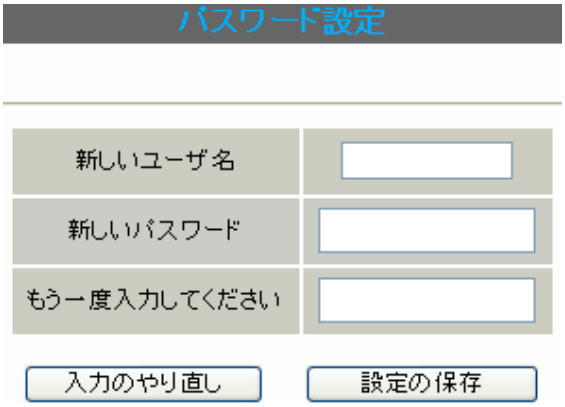
システム設定

◆パスワードの設定

本装置の設定画面にログインする際のユーザ名、パスワードを変更します。
ルータ自身のセキュリティのためにパスワードを変更されることを推奨します。

設定方法

「パスワードの設定」をクリックして設定画面を開きます。



ユーザー名とパスワードの設定ができます。

○新しいユーザ名
半角英数字で 1 から 15 文字まで設定可能です。

○新しいパスワード
半角英数字で 1 から 8 文字まで設定可能です。
大文字・小文字も判別しますのでご注意ください。

○もう一度入力してください
確認のため再度「新しいパスワード」を入力してください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。

本装置の操作を続行すると、ログイン用のダイアログ画面がポップしますので、新たに設定したユーザ名とパスワードで再度ログインしてください。

システム設定

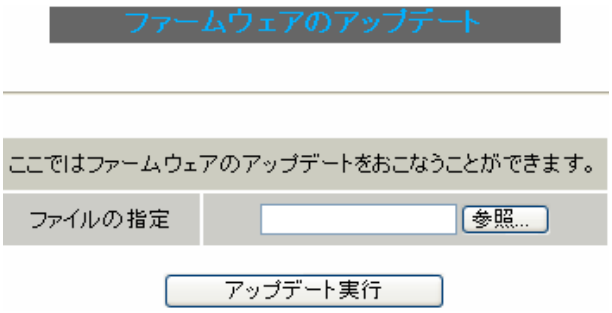
◆ファームウェアのアップデート

本装置は、ブラウザ上からファームウェアのアップデートをおこないます。
ファームウェアは弊社ホームページよりダウンロードできます。

弊社サポートサイト
http://www.centurysys.co.jp/support/xr1200.html

実行方法

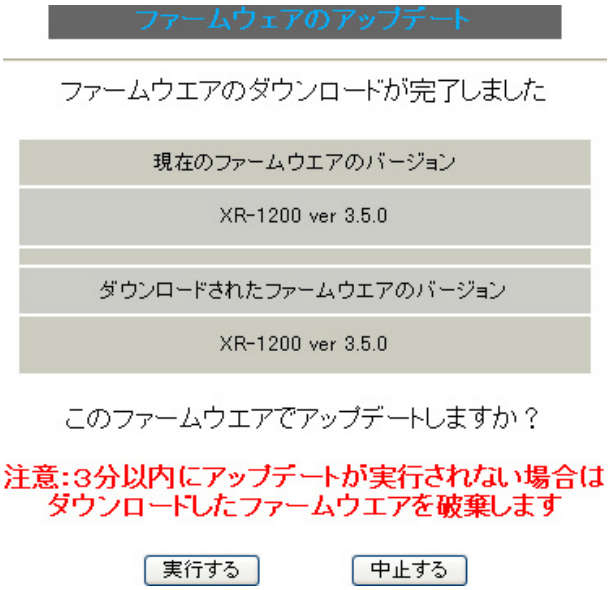
1 「ファームウェアのアップデート」をクリックして画面を開きます。



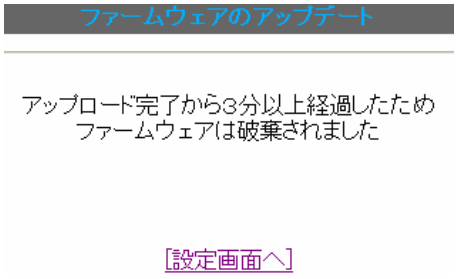
2 「参照」ボタンを押して、弊社ホームページからダウンロードしてきたファームウェアファイルを選択し、「アップデート実行」ボタンを押してください。

3 その後、ファームウェアを本装置に転送します。
転送が終わるまではしばらく時間がかかります。

転送完了後に、以下のようなアップデートの確認画面が表示されます。
バージョン等が正しければ「実行する」をクリックしてください。

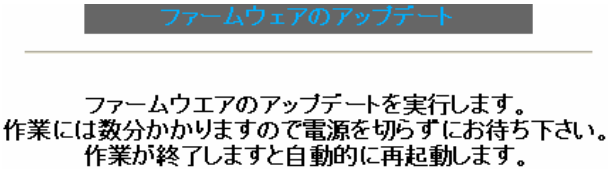


上記画面が表示されたままで3分間以上経過してから、「実行する」ボタンをクリックすると、以下の画面が表示され、アップデートは実行されません。



アップデートを実行するには再度、2の操作からおこなってください。

4 アップデートを実行した場合は以下の画面が表示され、ファームウェアの書き換えが始まります。



アップデート中は、本装置の LED が時計回りに回転します。
LED が動作中は、アクセスをおこなわずに、そのままお待ちください。
ファームウェアの書き換えが終了すると、本装置は自動的に再起動して、アップデートの完了となります。

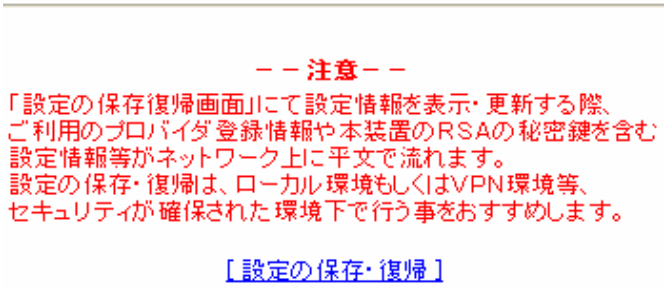
システム設定

◆設定の保存と復帰

本装置の設定の保存および、保存した設定の復帰をおこないます。

実行方法

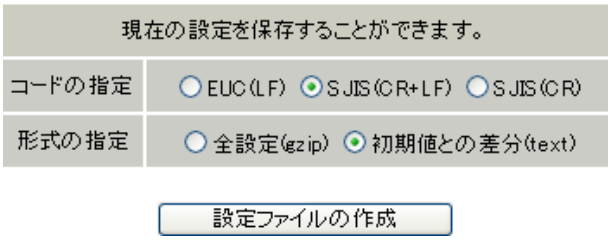
「設定の保存・復帰」をクリックして画面を開きます。



上記のメッセージが表示されます。
ご確認いただいた上で、[設定の保存・復帰]のリンクをクリックしてください。

[設定の保存]

設定を保存するときは、テキストのエンコード方式と保存形式を選択ます。



○コードの指定

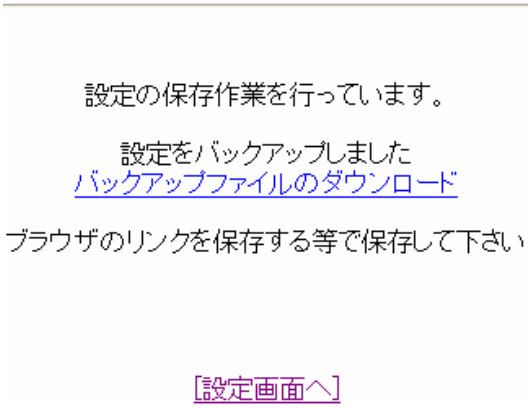
「EUC(LF)」「SJIS(CR+LF)」「SJIS(CR)」のいずれかを選択します。

○形式の指定

・全設定(gzip)
　本装置のすべての設定を gzip 形式で圧縮して保存します。

・初期値との差分(text)
　初期設定と異なる設定のみを抽出して、テキスト形式で保存します。
　このテキストファイルの内容を直接書き換えて設定を変更することもできます。

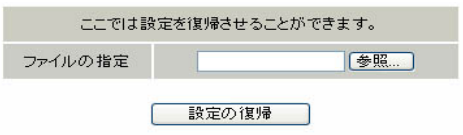
選択後は「設定ファイルの作成」をクリックします。
クリックすると以下のメッセージが表示されます。



「バックアップファイルのダウンロード」リンクから、設定をテキストファイルで保存しておきます。
設定ファイル名は「backup.txt」です。

[設定の復帰]

「参照」をクリックして、保存しておいた設定ファイル（「backup.txt」）を選択します。
全設定の保存ファイルは gzip 圧縮形式のまま、復帰させることができます。



設定の復帰が正しく行われると本機器は自動的に再起動します

その後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、本装置が自動的に再起動されます。

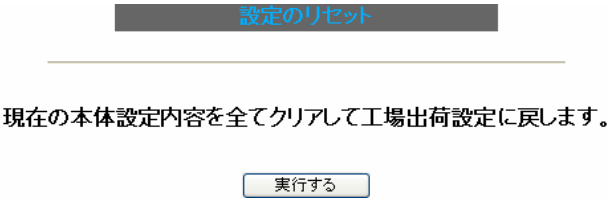
システム設定

◆設定のリセット

本装置の設定を全てリセットし、工場出荷時の設定に戻します。

実行方法

「設定のリセット」をクリックして画面を開きます。



「実行する」ボタンをクリックするとリセットが実行され、本体の全設定が工場出荷設定に戻ります。

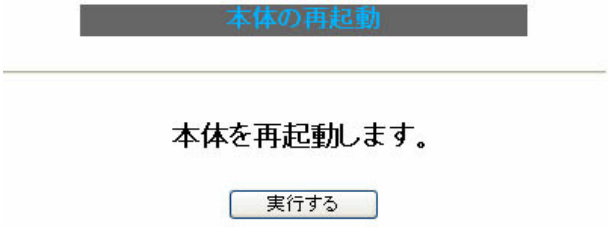
設定のリセットにより全ての設定が失われますので、念のために「設定のバックアップ」を実行しておくようにしてください。

◆再起動

本装置を再起動します。設定内容は変更されません。

実行方法

「再起動」をクリックして画面を開きます。



「実行する」ボタンをクリックすると、リセットが実行されます。

本体の再起動をおこなった場合、それまでのログは全てクリアされます。

システム設定

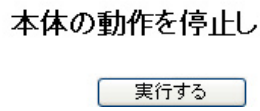
◆本体停止

本装置を停止状態にします。

停止状態とは、電源オフの状態とほぼ同じですが、本体前面の「Power」スイッチで操作することなく、本体の動作を停止します。

実行方法

「本体停止」をクリックして画面を開きます。



「実行する」ボタンをクリックすると、本装置は停止状態となります。

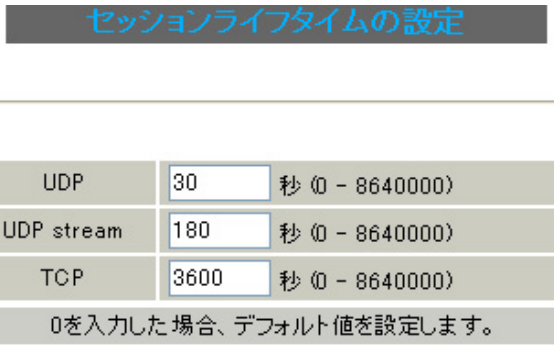
停止状態から稼働状態に復帰する場合は、本装置本体前面にある「Power」スイッチを押してください。

◆セッションライフタイムの設定

本装置内部では、NAT/IP マスカレードの通信を高速化するために、セッション生成時に NAT/IP マスカレードのセッション情報を記憶し、一定時間保存しています。
ここでは、そのライフタイムを設定します。

設定方法

「セッションライフタイムの設定」をクリックして画面を開きます。



◯ UDP

UDP セッションのライフタイムを設定します。
単位は秒です。0-8640000 の間で設定します。
初期設定は 30 秒です。

◯ UDP stream

UDP stream セッションのライフタイムを設定します。
単位は秒です。0-8640000 の間で設定します。
初期設定は 180 秒です。

◯ TCP

TCP セッションのライフタイムを設定します。単位は秒です。0-8640000 の間で設定します。
初期設定は 3600 秒です。

それぞれの項目で“0”を設定すると、初期値で動作します。

「設定の保存」ボタンをクリックすると、設定が保存されます。設定内容はすぐに反映されます。

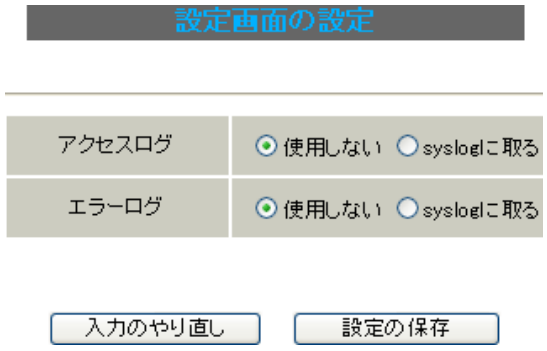
システム設定

◆設定画面の設定

WEB設定画面へのアクセスログについての設定をします。

設定方法

「設定画面の設定」をクリックして画面を開きます。



○アクセスログ
○(アクセス時の)エラーログ
取得するかどうかを指定します。

「設定の保存」をクリックします。

アクセスログ・エラーログは、「syslog」サービスの設定にしたがって出力されます。

システム設定

◆オプション USB フラッシュディスク

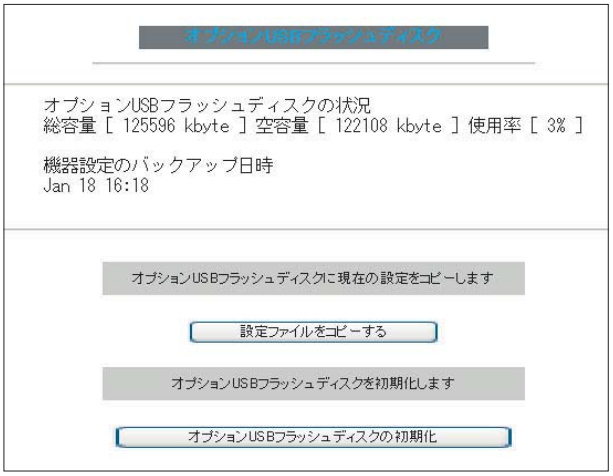
オプションで用意されている USB フラッシュディスク「FutureNet Memory Media USB-128」を装着している場合の、USB フラッシュディスクの操作をおこないます。

ここでは以下の操作をおこなうことができます。

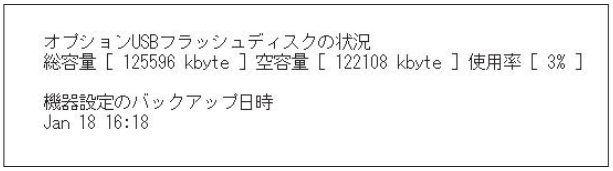
- USB フラッシュディスクの初期化
- USB フラッシュディスクへの設定のバックアップ

実行方法

USB フラッシュディスクを装着してから、「オプション USB フラッシュディスク」をクリックして画面を開きます。
画面には、装着したフラッシュディスクの情報が表示されます。

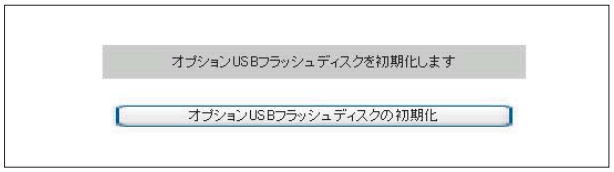


設定のバックアップがある場合は、画面上部に、装着した USB フラッシュディスクの状況とバックアップ情報が表示されます。



○USB フラッシュディスクの初期化

初めて USB フラッシュディスクを装着したときは、必ず USB フラッシュディスクを初期化する必要があります。
初期化をおこなわないと USB フラッシュディスクを使用できません。
USB フラッシュディスクを初期化するときは「オプション USB フラッシュディスクの初期化」をクリックします。



○USB フラッシュディスクへの設定のバックアップ

設定のバックアップを USB フラッシュディスクにコピーするときは「設定ファイルをコピーする」をクリックしてコピーを実行します。

[USB フラッシュディスクの取り扱いについて]

USB フラッシュディスクは、本装置前面パネルの USB インタフェースに装着してください。

- フラッシュディスクが装着可能なポートは１ポートのみです。
- 「USB Status LED」(橙)が、消灯→点滅→点灯後、USB フラッシュディスクが使用可能状態となります。

USB フラッシュディスクを本装置から取り外すときは、必ず、「システム設定」メニューの「本体停止」を実行するか、本体前面の「USB」スイッチを使用してください。
「本体停止」操作、もしくは「USB」スイッチを使わずに USB フラッシュディスクを取り外すと、本装置および USB フラッシュディスクが破損する場合があります。

詳しい USB フラッシュディスクの取り外し方法は「第 37 章 運用管理設定」をご参照ください。

システム設定

◆ARP filter 設定

ARP filter 設定をおこないます。

設定方法

「ARP filter 設定」をクリックして画面を開きます。

ARP filter を「無効」にするか、「有効」にするかを選択します。

有効にすると ARP filter が動作して、同一 IP アドレスの ARP を複数のインタフェースで受信したときに、当該 MAC アドレス以外のインタフェースから ARP 応答を出さないようにできます。

選択しましたら「設定の保存」をクリックしてください。設定が完了します。
設定はすぐに反映されます。

システム設定

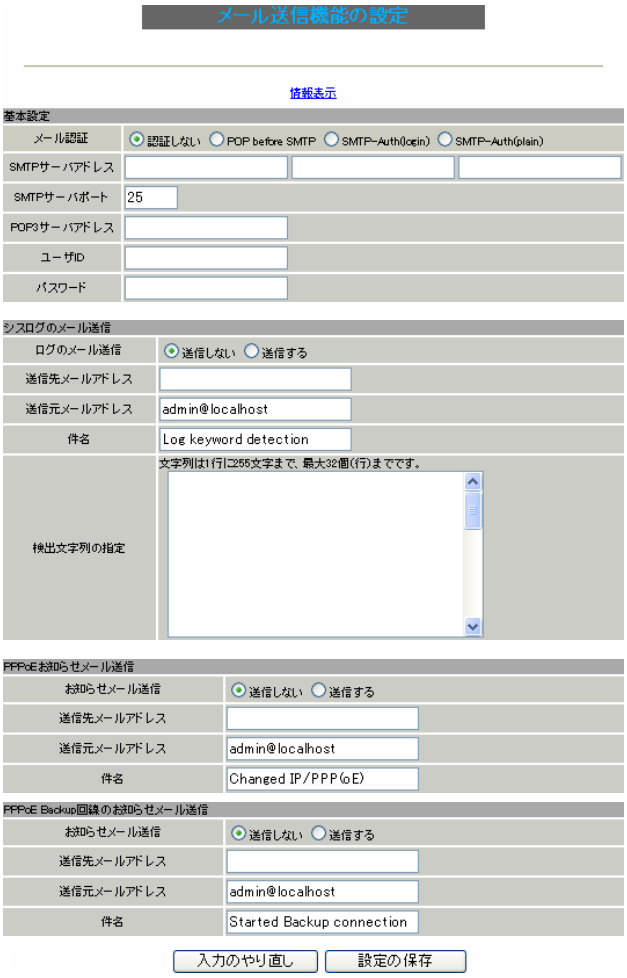
◆メール送信機能の設定

各種メール送信機能の設定をおこないます。
ここでは以下の場合にメール送信を設定出来ます。

- SYSLOG サービスのログメール送信
- PPP/PPPoE 接続設定の主回線 接続 IP 変更 お知らせメール
- PPP/PPPoE 接続設定のバックアップ回線 接続 お知らせメール

設定方法

「メール送信機能の設定」をクリックして画面を開きます。



<基本設定>

◯メール認証

下記よりいずれかを選択します。

「認証しない」

メールサーバとの認証をおこなわずに、本装置が自律的にメールを送信します。

「POP before SMTP」

指定した POP3 サーバにあらかじめアクセスさせることによって、SMTP によるメールの送信を許可する方式です。

「SMTP-Auth(login)」

メール送信時にユーザ認証をおこない、メールの送信を許可する方法です。平文によるユーザ認証方式です。

「SMTP-Auth(plain)」

メール送信時にユーザ認証をおこない、メールの送信を許可する方法です。LOGIN も PLAIN 同様、平文を用いた認証形式です。

◯ SMTP サーバアドレス

SMTP サーバアドレスは３箇所まで設定できます。
それぞれの設定箇所において１つの IPv4 アドレス、または FQDN が設定可能です。
FQDN は最大 64 文字で、ドメイン形式とホスト形式のどちらでも設定できます。

ドメイン形式で指定する場合
＜入力例＞ @centurysys.co.jp

ホスト形式で指定する場合
＜入力例＞ smtp.centurysys.co.jp

本設定は、メール認証設定で「認証しない」場合は任意ですが、認証ありの場合は必ず設定してください。

◯ SMTP サーバポート

設定されたポートを使用してメールを送信します。
設定可能な範囲：1-65535 です。
初期設定は“ 25 ”です。

システム設定

○ POP3 サーバアドレス
IPv4 アドレス、または FQDN で設定します。
FQDN は最大 64 文字で、ホスト形式のみ設定できます。
認証方式で「POP before SMTP」を指定した場合は必ず設定してください。

○ユーザ ID
ユーザ ID を設定します。
最大文字数は 64 文字です。
認証方式を「認証しない」以外で選択した場合は必ず設定してください。

○パスワード
パスワードを設定します。
半角英数字で 64 文字まで設定可能です。大文字・小文字も判別しますのでご注意ください。
認証方式を「認証しない」以外で選択した場合は必ず設定してください。

＜シスログのメール送信＞
ログの内容を電子メールで送信したいときの設定です。

○ログのメール送信
ログメール機能を使用する場合は「送信する」を選択します。

○送信先メールアドレス
ログメッセージの送信先メールアドレスを指定します。
最大文字数は 64 文字です。

○送信元メールアドレス
送信元のメールアドレスは任意で指定できます。
最大文字数は 64 文字です。
初期設定は「admin@localhost」です。

○件名
任意で指定できます。
使用可能な文字は半角英数字で、最大 64 文字です。
初期設定は「Log Keyword detection」です。

○検出文字列の指定
ここで指定した文字列が含まれるログをメールで送信します。検出文字列には、pppd、IP、DNS など、ログ表示に使用される文字列を指定してください。なお、文字列の記述に正規表現は使用できません。**文字列を指定しない場合はログメールは送信されません。**

文字列の指定は、半角英数字で一行につき 255 文字まで、かつ最大 32 行までです。
空白・大小文字も判別します。
一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したログのみ抽出して送信します。
なお「検出文字列の指定」項目は、「シスログのメール送信」機能のみ有効です。

システム設定

＜PPPoE お知らせメール送信＞
IP アドレスを自動的に割り当てられる方式で PPPoE 接続する場合、接続のたびに割り当てられる IP アドレスが変わってしまうことがあります。この機能を使うと、IP アドレスが変わったときに、その IP アドレスを任意のメールアドレスにメールで通知することができるようになります。

○お知らせメール送信
お知らせメール機能を使用する場合は「送信する」を選択します。

○送信先メールアドレス
お知らせメールの送り先メールアドレスを１箇所入力します。
最大文字数は 64 文字です。

○送信元メールアドレス
お知らせメールの送り元メールアドレスを１箇所入力します。
最大文字数は 64 文字です。
初期設定は「admin@localhost」です。

○件名
送信されるメールの件名を任意で設定できます。
使用可能な文字は半角英数字で、最大 64 文字です。
初期設定は「Changed IP/PPP(oE)」です。

＜PPPoE Backup 回線のお知らせメール送信＞
バックアップ回線で接続したときに、それを電子メールによって通知させることができます。

設定内容は＜PPPoE お知らせメール送信＞と同様です。
○お知らせメール送信
○送信先メールアドレス
○送信元メールアドレス
○件名
初期設定は「Started Backup connection」です。

必要項目への入力が終わりましたら「設定の保存」をクリックしてください。

○情報表示
リンクをクリックすると、メール送信の成功 / 失敗に関する情報が表示されます。

第 34 章

情報表示

本体情報の表示

本体の機器情報を表示します。
以下の項目を表示します。

- **ファームウェアバージョン情報**
  現在のファームウェアバージョンを確認できます。

- **インタフェース情報**
  各インタフェースの IP アドレスや MAC アドレスなどです。
  PPP/PPPoE や IPsec 論理インタフェースもここに表示されます。

- **リンク情報**
  本装置の各 Ethernet ポートのリンク状態、リンク速度が表示されます。

- **ルーティング情報**
  インタフェースルート、スタティックルート、ダイナミックルートに関するルーティング情報です。

- **Default Gateway 情報**
  デフォルトルート情報です。

- **ARP テーブル情報**
  XR が保持している ARP テーブルです。

- **DHCP クライアント取得情報**
  DHCP クライアントとして設定しているインタフェースがサーバから取得した IP アドレス等の情報を表示します。

実行方法

Web 設定画面の「情報表示」をクリックすると、新しいウィンドウが開いて本体情報表示されます。

画面中の「更新」をクリックすると、表示内容が更新されます。

第 35 章

詳細情報表示

各種情報の表示

システム設定の「詳細情報表示」をクリックすると、以下の画面が表示されます。

実行方法

左列の機能名をクリックすると、新しいウィンドウが開いて、その機能に関する情報がまとめて表示されます。
右列の小項目名をクリックした場合は、その小項目のみの情報が表示されます。

「OSPF」の「インターフェース情報」または、「QoS」の各情報については、ボックス内に表示したいインタフェース名を入力してください。

画面下の「全ての詳細情報を表示する」をクリックすると、全ての機能の全項目についての情報が一括表示されます。

表示される内容は以下のとおりです。

- **ルーティング情報**
  XR のルーティングテーブル、ルーティングテーブルの内部情報、ルートキャッシュの情報、デフォルトゲートウェイ情報が表示できます。
  このうち、ルーティングテーブルの内部情報とルートキャッシュの情報はここでのみ表示できます。
- **OSPF 情報**
- **RIP 情報**
- **IPsec サーバ情報**
- **DHCP サーバ情報**
- **NTP サービス情報**
- **VRRP サービス情報**
- **QoS 情報**

第 36 章

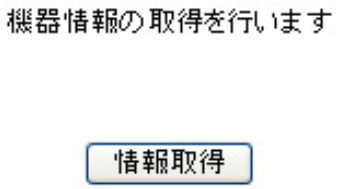
テクニカルサポート

テクニカルサポート

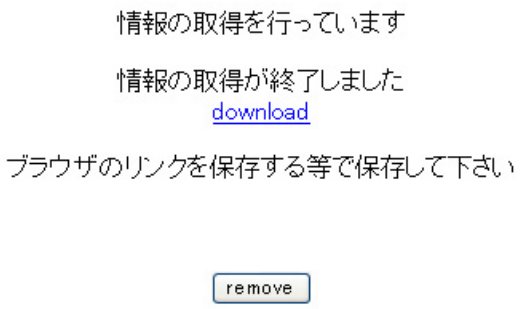
テクニカルサポートを利用することによって、本体の情報を一括して取得することが出来ます。

実行方法

Web 設定画面の「テクニカルサポート」をクリックすると以下の画面が表示されます。



「情報取得」をクリックします。



「download」のリンクをクリックして、本装置の機器情報ファイルをダウンロードしてください。
「remove」をクリックすると、取得した情報ファイルは消去されます。

取得情報の内容

ここでは、下記の３つの情報を一括して取得することが出来ます。

○ログ
詳細は、「第 33 章 各種システム設定　◆ログの表示 / ◆ログの削除」をご覧ください。

○設定ファイル
詳細は、「第 33 章 各種システム設定　◆設定の保存と復帰」をご覧ください。

○本体の機器情報
詳細は、「第 34 章 情報表示」をご覧ください。

第 37 章

運用管理設定

Ⅰ．各種ボタンの操作

本装置の前面にある各種ボタンを使用して、以下の操作をおこないます。

＜ Init スイッチ＞
- 本装置の設定を初期化する
- オプション USB フラッシュディスクに保存された設定で起動する

＜ Power スイッチ＞
- 本装置を起動させる
- 本装置をシャットダウンする

＜ USB スイッチ＞
- 装着状態のオプション USB フラッシュディスクを取り外す

◆本装置の設定を初期化する

1 本装置が停止状態になっていることを確認します。

2 本体前面にある「Init」スイッチを押します。

3 「Init」スイッチを押したままの状態で、「Power」スイッチをオンにします。
本体前面にある「Init Status LED」ランプ（橙）が点灯します。
「Init」スイッチは押したままにしておきます。

4 本体前面の「Init Status LED」ランプが消灯したら「Init」スイッチを放します。
本装置が工場出荷設定で起動します。

5 本装置が起動すると「System 2 LED」ランプ(緑)が点滅します。

Ⅰ．各種ボタンの操作

◆オプション USB フラッシュディスクの設定で起動する

1 本装置が停止状態になっていることを確認します。

2 本装置に、オプション USB フラッシュディスク
FutureNet Memory Media USB-128
が装着されていることを確認します。

3 本体前面にある「Init」スイッチを押します。

4 「Init」スイッチを押したままの状態で、「Power」スイッチをオンにします。
本体前面にある「Init Status LED」ランプ（橙）が点灯します。
「Init」スイッチは押したままにしておきます。

5 本体前面の「Init Status LED」ランプが消灯したら「Init」スイッチを放します。
その後、本装置がオプション USB メモリに保存されている設定内容で起動します。

6 本装置が起動すると「System 2 LED」ランプ(緑)が点滅します。

◆本装置をシャットダウンする

本装置のシャットダウンは、「システム設定」画面の「本体停止」からおこなうか、本体前面の「Power」スイッチを押してください。

シャットダウン
完全に電源をオフにする場合は、本体前面の「Power」スイッチを、短押（１秒程度）してください。

待機状態
待機状態とは、電源オフ状態と同じですが、本装置には通電している状態です。
待機状態にするのは、本装置がハングアップしたときなどの非常時のみにしてください。

・「システム設定」→「本体停止」で実行
Web 設定画面の「システム設定」→「本体停止」画面の「本体の動作を停止します。」を実行すると、動作が停止して待機状態になります。
※ 通常は、上記の操作で待機状態にしてください。

・「Power」スイッチで実行
本体前面の「Power」スイッチを押すと、動作が停止して待機状態になります。

II．オプション USB フラッシュディスクの操作

◆オプション USB フラッシュディスクを接続する

1 オプション USB フラッシュディスク

FutureNet Memory Media USB-128

を本体前面の USB インタフェースに差し込みます。
インタフェースは１ポートのみ使用可能です。
図柄の印刷されている面が上面です。

2 「USB Status LED」ランプ(橙)の状態が、消灯→点滅→点灯の順序で遷移します。

3 「USB STATUS LED」ランプが点灯した後、オプション USB フラッシュディスクが使用できる状態となります。

◆オプション USB フラッシュディスクを取り外す

本装置から USB フラッシュディスクを取り外すときは、必ず、以下の手順で操作してください。

1 本体前面の「USB」スイッチを押します。

2 「USB Status LED」ランプ(橙)の状態が、点灯→点滅→消灯の順序で遷移します。

3 「USB STATUS LED」ランプが消灯したのを確認後、オプション USB フラッシュディスクを取り外すことができます。

付録 A

インタフェース名一覧

付録 A

インタフェース名一覧

本装置は以下の設定において、インタフェース名を直接指定する場合があります。

- OSPF 機能
- IPsec 機能
- L2TPv3 機能
- SNMP エージェント機能
- UPnP 機能
- スタティックルート設定
- ソースルート設定
- NAT 機能
- パケットフィルタリング機能
- ネットワークイベント機能
- 仮想インタフェース機能
- QoS 機能
- ネットワークテスト

本装置のインタフェース名と実際の接続インタフェースの対応付けは次の表の通りとなります。

表左：インタフェース名
表右：実際の接続デバイス

eth0	Ether0ポート
eth1	Ether1ポート
eth2	Ether2ポート
eth3	Ether3ポート
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
ipsec7	eth2上のipsec
ipsec8	eth3上のipsec
gre<n>	gre(<n>は設定番号)
eth0.<n>	eth0上のVLANインタフェース(<n>はVLAN ID)
eth1.<n>	eth1上のVLANインタフェース(<n>はVLAN ID)
eth2.<n>	eth2上のVLANインタフェース(<n>はVLAN ID)
eth3.<n>	eth3上のVLANインタフェース(<n>はVLAN ID)
eth0:<n>	eth0上の仮想インタフェース(<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インタフェース(<n>は仮想IF番号)
eth2:<n>	eth2上の仮想インタフェース(<n>は仮想IF番号)
eth3:<n>	eth3上の仮想インタフェース(<n>は仮想IF番号)

付録 B

工場出荷設定一覧

付録 B

工場出荷設定一覧

IPアドレス設定	IPアドレス/サブネットマスク値
Ether0ポート	192.168.0.254/255.255.255.0
Ether1ポート	192.168.1.254/255.255.255.0
Ether2ポート	192.168.2.254/255.255.255.0
Ether3ポート	192.168.3.254/255.255.255.0

DHCPクライアント機能	無効
IPマスカレード機能	無効
ステートフルパケットインスペクション機能	無効
デフォルトゲートウェイ設定	設定なし
ダイヤルアップ接続	無効
DNSリレー/キャッシュ機能	無効
DHCPサーバ/リレー機能	有効
IPsec機能	無効
UPnP機能	無効
ダイナミックルーティング機能	設定なし
L2TPv3機能	無効
SYSLOG機能	有効
攻撃検出機能	無効
SNMPエージェント機能	無効
NTP機能	無効
VRRP機能	無効
アクセスサーバ機能	無効
スタティックルート設定	設定なし
ソースルーティング設定	設定なし
NAT機能	設定なし
パケットフィルタリング機能	NetBIOSからの漏洩を防止するフィルタ設定 （入力・転送フィルタ設定） 外部からのUPnPパケットを遮断する設定 （入力・転送フィルタ設定）
ネットワークイベント機能	無効
仮想インターフェース機能	設定なし
GRE機能	無効
QoS機能	設定なし
パケット分類機能	設定なし
Web 認証機能	無効

設定画面ログインID	admin
設定画面ログインパスワード	admin

付録 C

サポートについて

付録 C

サポートについて

◆本製品に関してのサポートは、ユーザー登録をされたお客様に限らせていただきます。
必ずユーザー登録していただきますよう、お願いいたします。

◆サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。
・サポートデスク
e-mail ： support@centurysys.co.jp
電話 ： 0422-37-8926
FAX ： 0422-55-3373
受付時間 ： 10:00～17:00 (土日祝祭日、および弊社の定める休日を除きます)
・ホームページ http://www.centurysys.co.jp/

◆故障と思われる場合は
製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。
事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

◆ご連絡をいただく前に
スムーズなユーザーサポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。

・ファームウェアのバージョンと MAC アドレス
(バージョンの確認方法は設定画面「情報表示」でご確認いただけます)
・ネットワークの構成(図)
どのようなネットワークで運用されているかを、差し支えのない範囲でお知らせ下さい。
・不具合の内容または、不具合の再現手順
何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせ下さい。
・エラーメッセージ
エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
・本装置の設定内容、およびコンピュータの IP 設定
・**可能であれば、「設定のバックアップファイル」をお送りください。**

◆サポート情報
弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。
また製品の FAQ も掲載しておりますので、是非ご覧下さい。

FutureNet XR シリーズ 製品サポートページ
http://www.centurysys.co.jp/support/
※ インデックスページから本装置の製品名をクリックしてください。

◆製品の保証について
本製品の保証期間は、お買い上げ日より 1 年間です。
保証期間を過ぎたもの、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承下さい。保証規定については、同梱の保証書をご覧ください。

XR-1200 ユーザーズガイド 3.5.0対応版
2011年8月版
発行 センチュリー・システムズ株式会社