Gigabit/Broadband GATE

L2TPv3対応　Gigabit/Broadband Gate

ユーザーズガイド

FutureNet XR-510/C

XR-540/C

XR-730/C

v3.4.0対応版

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ください。

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ください。

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ください。

◆商標の表示

□「BROADBAND 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 95、Windows 98、Windows NT3.51、Windows NT4.0
Windows 2000、Windows Me、Windows XP、Windows Vista

□Macintosh、Mac OS Xは、アップル社の登録商標です。

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

本製品を安全にお使いいただくために、まず以下の注意事項を必ずお読みください。

絵表示について	この取扱説明書では、製品を安全に正しくお使いいただき、あなたや他の人々への危害や財産への損害を未然に防止するために、いろいろな絵表示をしています。その表示と意味は次のようになっています。内容をよく理解してから本文をお読みください。

次の表示の区分は、表示内容を守らず、誤った使用をした場合に生じる「危害や損害の程度」を説明しています。

⚠ 危険	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う危険が差し迫って生じることが想定される内容を示しています。
⚠ 警告	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠ 注意	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。

次の絵表示の区分は、お守りいただく内容を説明しています。

	このような絵表示は、してはいけない「禁止」を意味するものです。 それぞれに具体的な禁止内容が書かれています。
	このような絵表示は、必ず実行していただく「強制」を指示するものです。 それぞれに具体的な指示内容が書かれています。

⚠ 危険

 必ず本体に付属している電源ケーブルをご使用ください。

 使用温度範囲は 0℃～40℃です。この温度範囲以外では使用しないでください。

 ストーブのそばなど高温の場所で使用したり、放置しないでください。

 火の中に投入したり、加熱したりしないでください。

 製品の隙間から針金などの異物を挿入しないでください。

ご使用にあたって

⚠ 警告

万一、異物(金属片・水・液体)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となります。

万一、発熱していたり、煙が出ている、変な臭いがするなどの異常状態のまま使用すると、火災の原因となります。すぐに電源を外し、お買い上げの販売店にご連絡ください。

本体を分解、改造しないでください。けがや感電などの事故の原因となります。

本体またはACアダプタを直射日光の当たる場所や 、調理場や風呂場など湿気の多い場所では絶対に使用しないでください。火災・感電・故障の原因となります。

ACアダプタの電源プラグについたほこりはふき取ってください。火災の原因になります。

濡れた手でACアダプタ、コンセントに触れないでください。感電の原因となります。

ACアダプタの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・故障の原因となります。

AC100Vの家庭用電源以外では絶対に使用しないでください。火災・感電・故障の原因となります。

ご使用にあたって

⚠ 注意

湿気やほこりの多いところ、または高温となるところには保管しないでください。故障の原因となります。

乳幼児の手の届かないところに保管してください。けがなどの原因となります。

長期間使用しないときには、ACアダプタをコンセントおよび本体から外してください。

ACアダプタの上に重いものを乗せたり、ケーブルを改造したりしないでください。また、ACアダプタを無理に曲げたりしないでください。火災・感電・故障の原因となることがあります。

ACアダプタは必ず電源プラグを持って抜いてください。ケーブルを引っ張ると、ケーブルに傷が付き、火災・感電・故障の原因となることがあります。

近くに雷が発生したときには、ACアダプタをコンセントから抜いて、ご使用をお控えください。落雷が火災・感電・故障の原因となることがあります。

ACアダプタのプラグを本体に差し込んだ後にACアダプタのケーブルを左右および上下に引っ張ったり、ねじったり、曲げたりしないでください。緩みがある状態にしてください。

本製品に乗らないでください。本体が壊れて、けがの原因となることがあります。

高出力のアンテナや高圧線などが近くにある環境下では、正常な通信ができない場合があります。

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ものが同梱されております。本製品をお使いいただく前に、内容物がすべ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。

＜XR-510/C をお買い上げの方＞

XR-510/C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
UTPケーブル（ストレート、１m）	１本
RJ-45/D-sub9ピン変換アダプタ（ストレート）	１個
ACアダプタ	１個
海外使用禁止シート	１部
保証書	１部

＜XR-540/C をお買い上げの方＞

XR-540/C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
UTPケーブル（ストレート、１m）	１本
海外使用禁止シート	１部
保証書	１部

＜XR-730/C をお買い上げの方＞

XR-730/C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
UTPケーブル（ストレート、１m）	１本
電源ケーブル	１本
海外使用禁止シート	１部
保証書	１部

第1章

本装置の概要

Ⅰ．本装置の特長

◆高速ネットワーク環境に余裕で対応

XR-730/C（以下 XR-730 または、本装置）はギガビット対応のインターフェースを２ポート保有しています。

XR-510/C・XR-540/C（以下、XR-510・XR-540 または、本装置）は、通常のルーティングスピードおよびPPPoE接続時に最大100Mbpsの通信速度を実現していますので、高速ADSLやFTTH等の高速インターネット接続やLAN環境の構成に充分な性能を備えています。

◆PPPoE クライアント機能

PPPoEクライアント機能を搭載していますので、FTTHサービスやNTT東日本/西日本などが提供するフレッツADSL・Bフレッツサービスに対応しています。また、PPPoEの自動接続機能やリンク監視機能、IP アドレス変更通知機能を搭載しています。

◆unnumbered 接続対応

unnumbered接続に対応していますので、ISP各社で提供されている固定IPサービスでの運用が可能です。

◆DHCP クライアント / サーバ機能

DHCP クライアント機能によって、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も利用できます。また、LAN 側ポートでは DHCP サーバ機能を搭載しており、LAN 側の PC に自動的に IP アドレス等の TCP/IP 設定を行なえます。

◆NAT/IP マスカレード機能

IPマスカレード機能を搭載していることにより、グローバルアドレスが1つだけしか利用できない場合でも、複数のコンピュータから同時にインターネットに接続できます。

また静的NAT設定によるバーチャルサーバ機能を使えば、プライベートLAN上のサーバをインターネットに公開することができます。

◆ステートフルパケットインスペクション機能

動的パケットフィルタリングともいえる、ステートフルパケットインスペクション機能を搭載しています。これは、WAN向きのパケットに対応するLAN向きのパケットのみを通過させるフィルタリング機能です。これ以外の要求ではパケットを通しませんので、ポートを固定的に開放してしまう静的パケットフィルタリングに比べて高い安全性を保てます。

◆静的パケットフィルタリング機能

送信元 / あて先の IP アドレス・ポート、プロトコルによって詳細なパケットフィルタの設定が可能です。入力 / 転送 / 出力それぞれに対して最大256ずつのフィルタリングポリシーを設定できます。ステートフルパケットインスペクション機能と合わせて設定することで、より高度なパケットフィルタリングを実現することができます。

◆ブリッジフィルタ機能

本装置をイーサネットインターフェースもしくはVLANのブリッジとして設定し、L2レベルのフィルタとして利用することが可能です。同一LANの特定のエリアをブリッジで分離し、ブリッジフィルタを設定することによって、LANのセキュリティをきめ細かく制御できます。

Ⅰ．本装置の特長

◆ローカルルータ / ブリッジ機能
NAT 機能を使わずに、単純なローカルルータ / ブリッジとして使うこともできます。

◆ IPsec 通信
IPsec を使いインターネット VPN(Virtual Private Network)を実現できます。WAN 上の IPsec サーバと 1 対 n で通信が可能です。最大接続数は 128 拠点です。ハードウェア回路による暗号化処理を行っています。公開鍵の作成から IPsec 用の設定、通信の開始 / 停止まで、ブラウザ上で簡単におこなうことができます。
また FutureNet XR VPN Client と組み合わせて利用することで、モバイルインターネット VPN 環境を構築できます。

◆ UPnP 機能
UPnP(ユニバーサル・プラグアンドプレイ)機能に対応しています。

◆ GRE トンネリング機能
仮想的なポイントツーポイントリンクを張って各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 GRE トンネリングに対応しています。

◆ダイナミックルーティング機能
小規模ネットワークで利用される RIP に加え、大規模ネットワーク向けのルーティングプロトコルである OSPF にも対応しています。

◆ソースルート機能
送信元アドレスによってルーティングをおこなうソースルーティングが可能です。

◆多彩な冗長化構成が実現可能
VRRP機能による機器冗長化機能だけではなく、インターフェース状態やPingによるインターネットVPNのエンド～エンドの監視を実現し、ネットワークの障害時にIブロードバンド回線を用いてバックアップする機能をを搭載しています。

◆ QoS 機能
帯域制御 / 優先制御をおこなうことができます。これにより、ストリーミングデータを利用する通信などに優先的に帯域を割り当てることが可能になります。
さらに網サービス側での QoS 制御に対応できるよう IP ヘッダの TOS、Precedence、DSCP フィールドのマーキング機能を搭載しています。

◆スケジュール機能（※ **XR-540 のみ**）
PPPoE 接続や ISDN での接続などについて、スケジュール設定をおこなうことで回線への接続 / 切断を自動制御することができます。

◆シリアルポートを搭載
本装置はRS-232ポートを備えています。常時接続のルータとして使いながら、同時にモデムやTAを接続してアクセスサーバや、リモートルータとして利用することができます。また、電話回線経由で本装置を遠隔管理することも可能です。

Ⅰ．本装置の特長

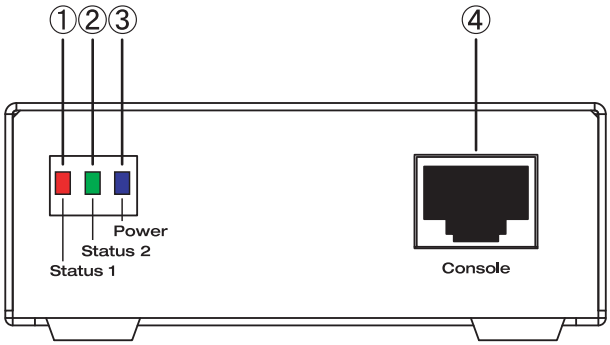
◆ログ機能
本装置のログを取得する事ができ、ブラウザ上でログを確認することが可能です。ログを電子メールで送信することも可能です。また攻撃検出設定を行なえば、インターネットからの不正アクセスのログも併せてログに記録されます。

◆バックアップ機能
本体の設定内容を一括してファイルにバックアップすることが可能です。
また設定の復元も、ブラウザ上から簡単にできます。

◆ファームウェアアップデート
ブラウザ設定画面上から簡単にファームウェアのアップデートが可能です。
特別なユーティリティを使わないので、どのOSをお使いの場合でもアップデートが可能です。

II．各部の名称と機能

◆製品前面（XR-510）



①STATUS1 LED(赤)
本装置に電源を投入した後、サービス起動中に、STATUS1(赤)は点灯します。
その後、全てのサービスが動作開始状態になると、STATUS1(赤)は消灯します。
また、ファームウェアのアップデート作業中は、STATUS1(赤)が点滅します。

これら以外の状態で、STATUS1が点滅しているときはシステム異常が起きておりますので、弊社までご連絡ください。

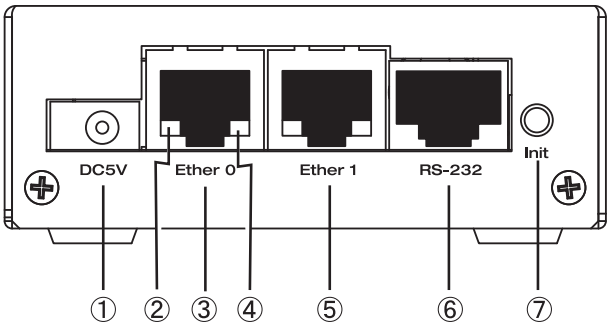
②STATUS2 LED(緑)
PPP/PPPoE主回線で接続しているときに、STATUS2(緑)は点灯します。PPP/PPPoE主回線で接続していない時は消灯しています。

③POWER LED(青)
本装置に電源が投入されているときに点灯(青)します。

④Console
弊社での保守管理用ポートです。使用できません。

※ XR-510には、Ether2ポートはありません。

◆製品背面（XR-510）



①電源コネクタ
製品付属のACアダプタを接続します。

②LINK/ACT LED(緑)
Ethernetポートの状態を表示します。
LANケーブルが正常に接続されているときに緑色LEDが点灯します。データ通信時はLEDは点滅します。

③Ether0ポート
主にLANとの接続に使用します。イーサネット規格のUTP 100Base-TXケーブルを接続します。ケーブルの極性は自動判別します。

④100M LED(黄)
100Base-TXで接続した場合に、黄色LEDが点灯します。10Base-Tで接続した場合には消灯します。

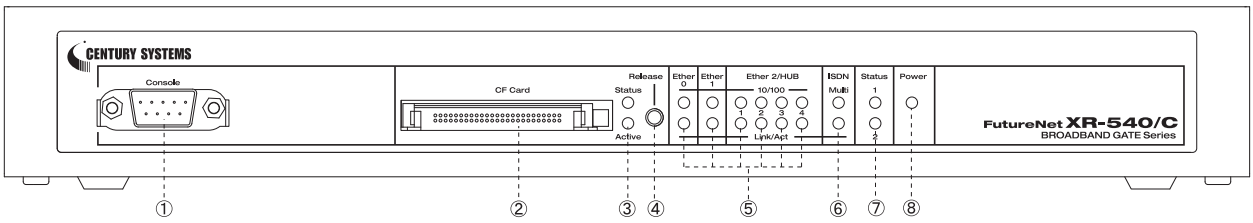
⑤Ether1ポート
WAN側ポートとして、また、Ether0ポートとは別セグメントを接続するポートとして使います。
イーサネット規格のUTP 100Base-TXケーブルを接続します。ケーブルの極性は自動判別します。

⑥RS-232ポート
リモートアクセスやアクセスサーバ機能を使用するときにモデムを接続します。ストレートタイプのLANケーブルと製品添付の変換アダプタを用いてモデムと接続してください。

⑦INITボタン
本装置を工場出荷時の設定に戻して起動するときに押します。操作方法については第41章をごらんください。

II．各部の名称と機能

◆製品前面（XR-540）



① Console
弊社での保守管理用ポートです。使用できません。

② CFカードスロット
オプションで用意されているCFカードを挿入します。

③ STATUS(橙) / ACTIVE(緑)LED
CFカードが挿入され動作しているときに、STATUS(橙)が点灯します。
CFカードをスロットに挿入してカードが使用可能状態になると、ACTIVE(緑)が点灯します。
CFカードが挿入されていないとき、また④の操作をおこないCFカードを安全に取り外せる状態になったときは、ACTIVE(緑)は消灯します。

CFカード挿入時にCFカードへのアクセス中はSTATUS(橙)が点滅します。アクセスがないときはSTATUS(橙)は消灯しています。

④ RELEASEボタン
CFカードを取り外すときに押します。RELEASEボタンを数秒押し続けると、③の「CF」LEDが消灯します。この状態になったら、CFカードを安全に取り外せます。

⑤ Ethernetポート LED
各Ethernetポートの状態を表示します。
LANケーブルが正常に接続されているときに、下段の「LINK/ACT」(緑)ランプが点灯します。上段の「100M」(橙)ランプは、10Base-Tで接続した場合に消灯、100Base-TXで接続した場合点に点灯します。
データ通信時は「LINK/ACT」(緑)ランプが点滅します。

⑥ ISDN(BRI)ポートLED
本装置のISDN(BRI)ポートを使って接続をしているときに、下段の「LINK」(緑)が点灯します。
さらに128K接続の場合は「MULTI」(橙)が同時に点灯します。

回線切断時は、ランプは消灯しています。

⑦ STATUS 1/2 LED
本装置の全てのサービスが動作開始状態になっているときに、STATUS1(赤)は消灯します。このランプが点灯しているときはシステム異常が起きておりますので、弊社までご連絡ください。

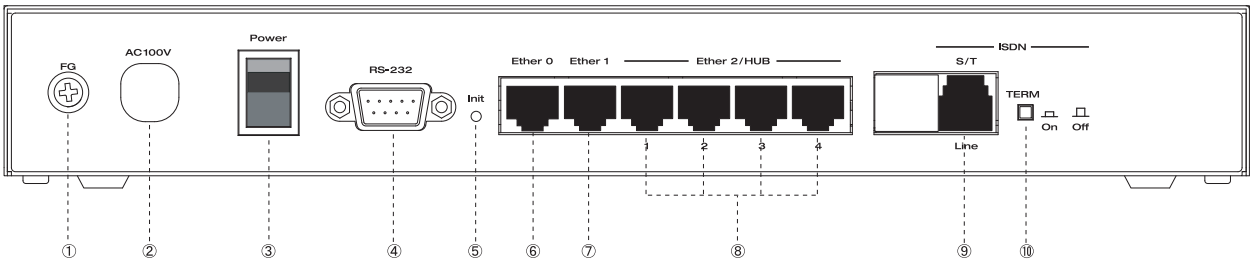
PPP/PPPoE主回線で接続しているときに、STATUS2(緑)は点灯します。PPP/PPPoE主回線で接続していない時は消灯しています。

ファームウェアのアップデート作業中は、STATUS1(赤)が点滅します。
ファームウェアのアップデートに失敗した場合など、本装置が正常に起動できない状態になったときは、STATUS1(赤)とSTATUS2(緑)のどちらも点滅します。

⑧ POWER LED
本装置に電源が投入されているときに点灯(緑)します。

II．各部の名称と機能

◆製品背面（XR-540）



① FG(アース)端子
保安用接地端子です。必ずアース線を接続してください。

② 電源ケーブル

③ 電源スイッチ
電源をオン / オフするためのスイッチです。

④ RS-232 ポート
リモートアクセスやアクセスサーバ機能を使用するときにモデムを接続します。接続には別途シリアルケーブルをご用意ください。

⑤ INIT ボタン
本装置を一時的に工場出荷時の設定に戻して起動するときに押します。

⑥ Ether0 ポート
主に DMZ ポートとして、また、Ether1、Ether2 ポートとは別セグメントを接続するポートとして使います。イーサネット規格の UTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

⑦ Ether1 ポート
主に WAN 側ポートとして、また、Ether0、Ether2 ポートとは別セグメントを接続するポートとして使います。イーサネット規格の UTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

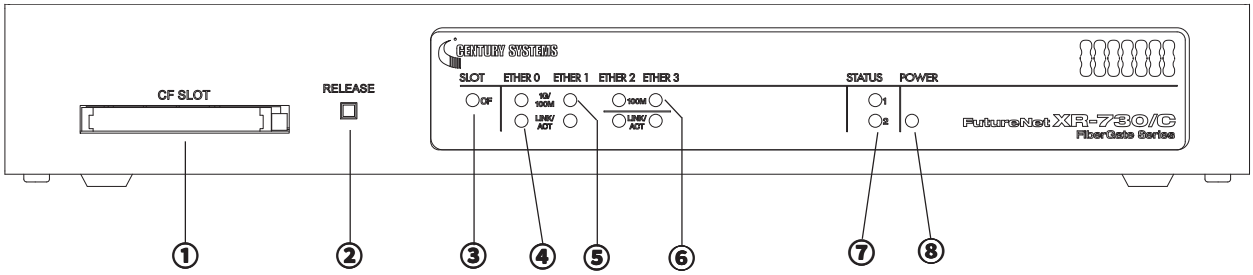
⑧ Ether2 ポート
４ポートのスイッチング HUB です。
主に LAN との接続に使用します。イーサネット規格の UTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

⑨ ISDN S/T(BRI) LINE ポート
このポートと外部 DSU を ISDN ケーブルで接続します。

⑩ TERM. スイッチ
「ISDN S/T 点ポート」接続時の終端抵抗の ON/OFF を切り替えます。外部 DSU を接続している場合は、XR-540 を含めていずれか 1 つの機器の終端抵抗を ON にしてください。

II．各部の名称と機能

◆製品前面（XR-730）



① CFカードスロット
オプションで用意されているCFカードを挿入します。

② RELEASEボタン
CFカードを取り外すときに押します。RELEASEボタンを数秒押し続けると、③のCF LEDが消灯します。この状態になったら、CFカードを安全に取り外せます。

③ CF LED（緑）
CFカードが挿入され動作しているときに、点灯します。CFカードが挿入されていないとき、また②の操作をおこないCFカードを安全に取り外せる状態になったときは、消灯します。

④ LINK/ACT LED（緑）
Ethernetポートの状態を表示します。LANケーブルが正常に接続されているときに点灯し、データ通信時は点滅します。

⑤ 1G/100M LED（橙/緑）
Ethernetポートの通信速度を表示します。
1000Base-Tで接続したときに橙色が点灯し、
100Base-TXで接続したときに緑色が点灯します。
10Base-Tで接続したときは消灯します。

⑥ 100M LED（緑）
Ethernetポートの通信速度を表示します。
100Base-TXで接続したときに点灯し、10Base-Tで接続したときに消灯します。

⑦ STATUS1/2 LED
STATUS1 LED（赤）：
本装置の全てのサービスが動作開始状態になっているときに消灯します。ファームウェアのアップデート作業中は点滅します。点灯しているときはシステム異常が起きておりますので、弊社までご連絡ください。

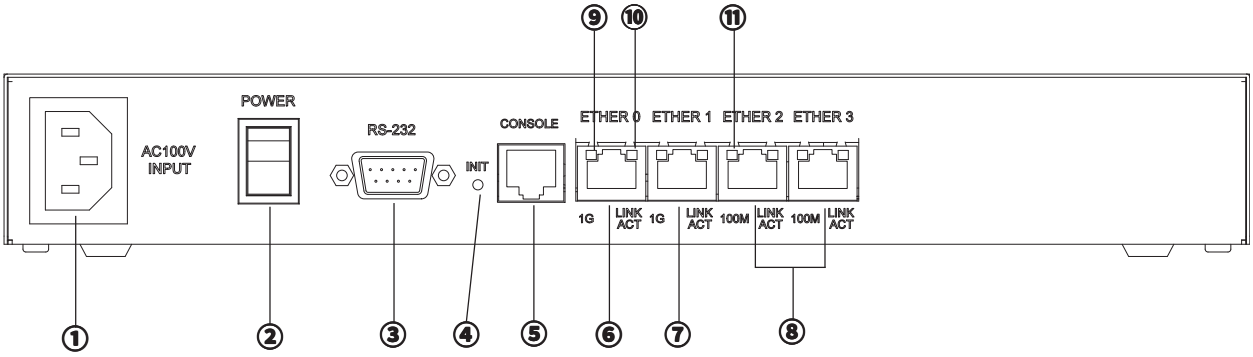
STATUS2 LED（緑）：
システムが起動し通常動作状態になると点滅します。

ファームウェアのアップデートに失敗した場合など、本装置が正常に起動できない状態になったときは、STATUS1/2 両方のLEDが点滅します。

⑧ POWER LED（緑）
本装置に電源が投入されているときに点灯します。

II．各部の名称と機能

◆製品背面（XR-730）



① 電源コネクタ
電源ケーブルを接続します。

② 電源スイッチ
電源をオン / オフするためのスイッチです。

③ RS-232 ポート
リモートアクセスやアクセスサーバ機能を使用するときにモデムを接続します。接続には別途シリアルケーブルをご用意ください。

④ INIT ボタン
本装置を一時的に工場出荷時の設定に戻して起動するときに押します。

⑤ コンソールポート
弊社での保守管理用ポートです。使用できません。

⑥ Ether0 ポート
Gigabit Ethernet 対応ポートです。主に DMZ ポートとして、また、Ether1、2、3 ポートとは別セグメントを接続するポートとして使用します。イーサネット規格の UTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

⑦ Ether1 ポート
Gigabit Ethernet 対応ポートです。主に WAN 側ポートとして、また、Ether0、2、3 ポートとは別セグメントを接続するポートとして使います。イーサネット規格の UTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

⑧ Ether2、3 ポート
Fast Ethernet 対応ポートです。主に LAN との接続に使用します。イーサネット規格の UTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

⑨ 1G LED（橙 / 緑）
Ethernet ポートの通信速度を表示します。
1000Base-T で接続したときに橙色が点灯し、
100Base-TX で接続したときに緑色が点灯します。
10Base-T で接続したときは消灯します。

⑩ LINK/ACT LED（緑）
Ethernet ポートの状態を表示します。LAN ケーブルが正常に接続されているときに点灯し、データ通信時は点滅します。

⑪ 100M LED（緑）
Ethernet ポートの通信速度を表示します。
100Base-TX で接続したときに点灯し、10Base-T で接続したときに消灯します。

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 のインター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、InternetExplorer4.0 以降か NetscapeNavigator4.0 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

装置の設置

装置の設置

本装置の各設定方法について説明します。

下記は設置に関する注意点です。
よくご確認いただきましてから設置してください。

注意！

本装置は直射日光が当たるところや、温度の高いところには設置しないようにしてください。内部温度が上がり、動作が不安定になる場合があります。

注意！

AC アダプタ、および電源ケーブルのプラグを本体に差し込んだ後にケーブルを左右及び上下に引っ張らず、緩みがある状態にしてください。
抜き差しもケーブルを引っ張らず、コネクタを持っておこなってください。
また、ケーブルを足などで引っ掛けてプラグ部に異常な力が掛からないように配線にご注意ください。

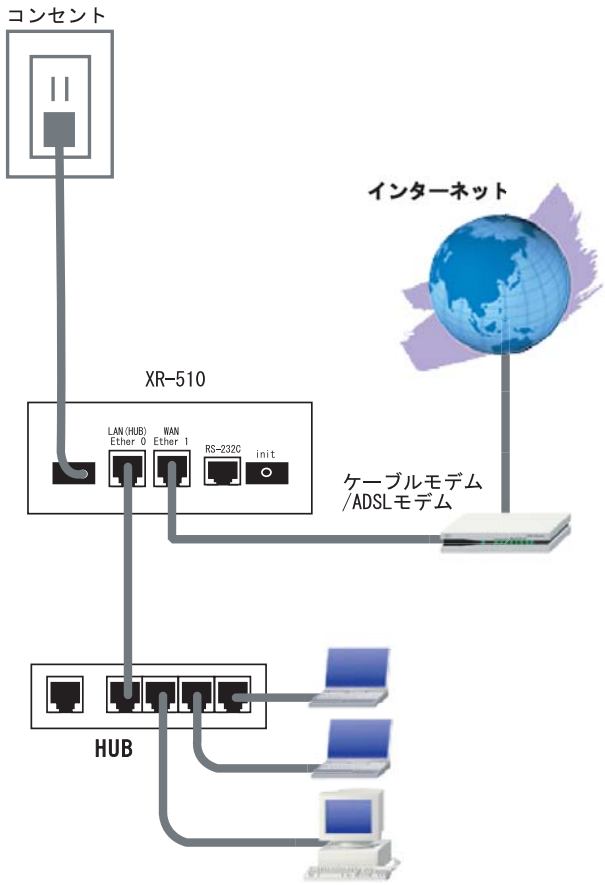
注意！

本装置側でも各ポートでARP tableを管理しているため、PC を接続しているポートを変更するとその PC から通信ができなくなる場合があります。このような場合は、本装置側のARP tableが更新されるまで(数秒～数十秒)通信できなくなりますが、故障ではありません。

Ⅰ．XR-510 の設置

XR-510 と xDSL/ 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。

接続図(例)



1 XR-510 と xDSL/ 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。

各 Ethernet ポートは LAN ケーブルの極性を自動判別します。

2 XR-510 の背面にある Ether1 ポートと xDSL/ ケーブルモデムや ONU を、LAN ケーブルで接続してください。

3 XR-510 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。

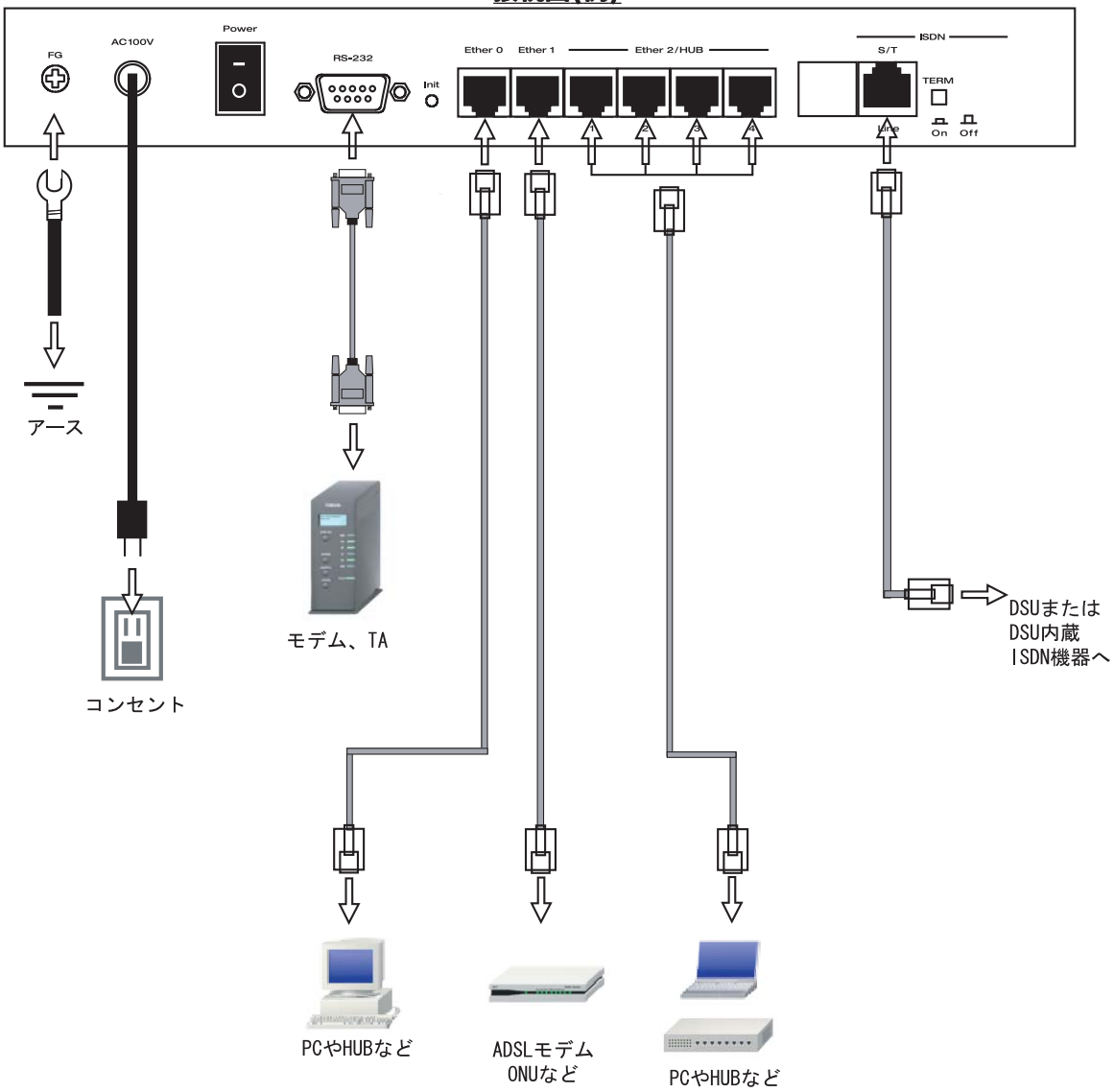
4 XR-510 と AC アダプタ、AC アダプタとコンセントを接続してください。

5 全ての接続が完了しましたら、XR-510 と各機器の電源を投入してください。

II. XR-540の設置

XR-540とxDSL/ケーブルモデムやコンピューターは、以下の手順で接続してください。

接続図(例)



1 XR-540とxDSL/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。

各Ethernetポートは LANケーブルの極性を自動判別します。

2 XR-540の背面にあるEther1ポートとxDSL/ケーブルモデムやONUを、LANケーブルで接続してください。

3 XR-540の設定が工場出荷状態の場合、Ether0ポートとPCをLANケーブルで接続してください。

4 XR-540の背面にあるEther2(HUB)ポート(1～4のいずれかのポート)とPCをLANケーブルで接続してください。

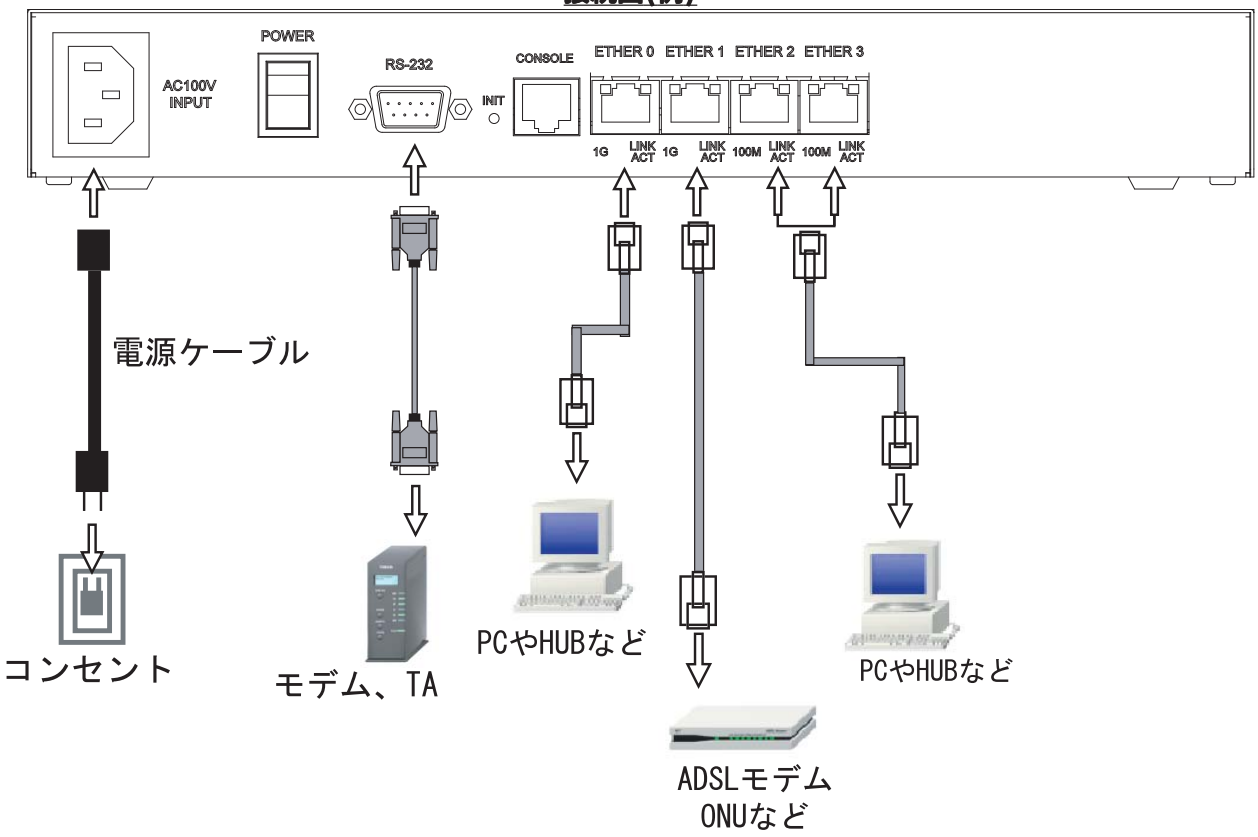
5 電源ケーブルとコンセントを接続してください。

6 全ての接続が完了しましたら、XR-540と各機器の電源を投入してください。

III. XR-730 の設置

XR-730 と xDSL/ ケーブルモデムやコンピューターは、以下の手順で接続してください。

接続図(例)



1 XR-730 と xDSL/ 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。

各 Ethernet ポートは LAN ケーブルの極性を自動判別します。

2 XR-730 の背面にある Ether1 ポートと xDSL/ ケーブルモデムや ONU を、LAN ケーブルで接続してください。

3 XR-730 の設定が工場出荷状態の場合、Ether0 ポートと PC を LAN ケーブルで接続してください。

4 XR-730 の背面にある Ether2(または 3)ポートと PC を LAN ケーブルで接続してください。

5 電源ケーブルとコンセントを接続してください。

6 全ての接続が完了しましたら、XR-730 と各機器の電源を投入してください。

第3章

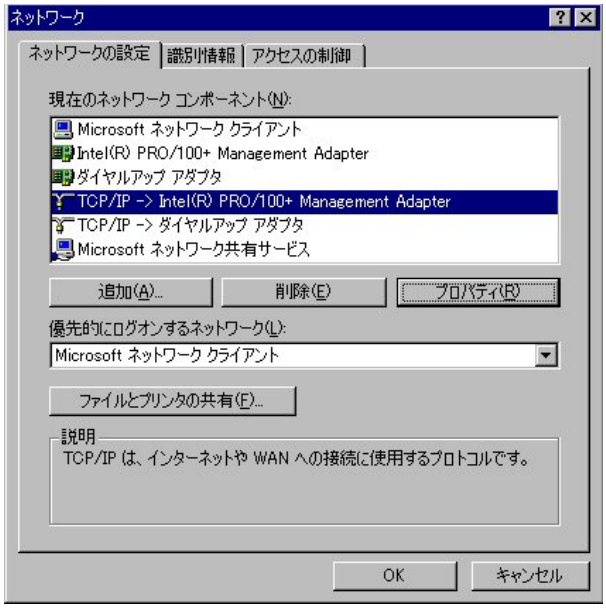
コンピュータのネットワーク設定

第3章 コンピュータのネットワーク設定

I. Windows 95/98/Me のネットワーク設定

ここではWindows95/98/Me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」の順で開き、「ネットワークの設定」タブの「現在のネットワーク構成」から、コンピュータに装着されたLANボード(カード)のプロパティを開きます。

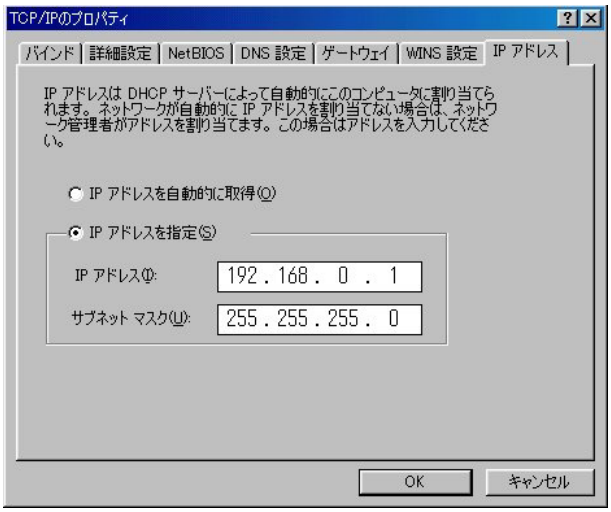


2 「TCP/IPのプロパティ」が開いたら、「IPアドレス」タブをクリックしてIP設定をおこないます。「IPアドレスを指定」にチェックを入れて、

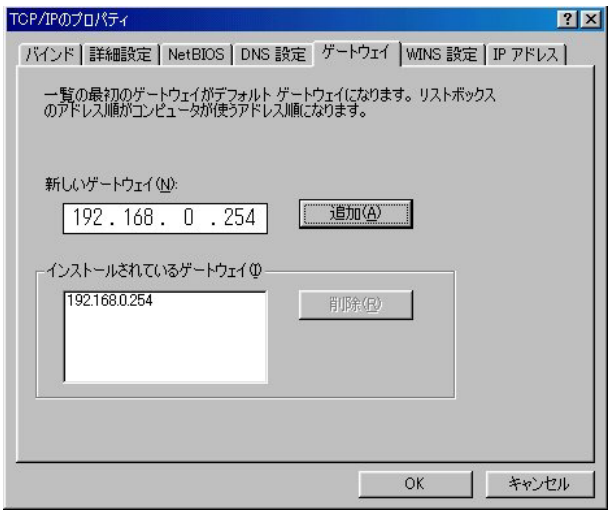
IPアドレスに「192.168.0.1」

サブネットマスクに「255.255.255.0」

と入力します。



3 続いて「ゲートウェイ」タブをクリックして、新しいゲートウェイに「192.168.0.254」と入力して追加ボタンをクリックしてください。



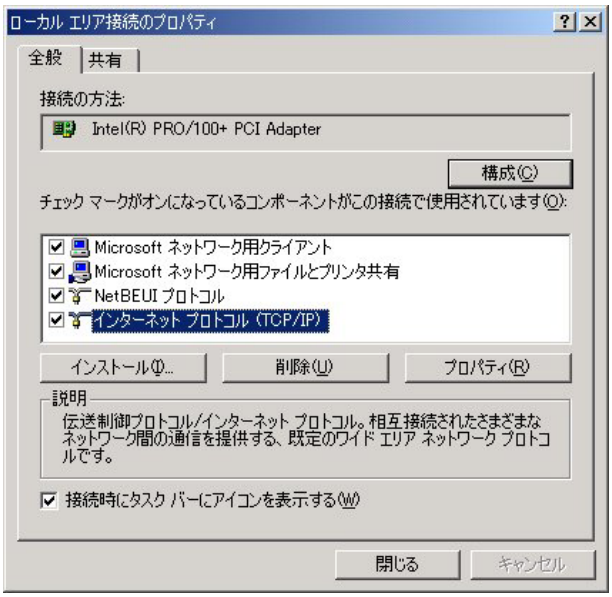
4 最後にOKボタンをクリックするとコンピュータが再起動します。再起動後に、本装置の設定画面へのログインが可能になります。

II. Windows 2000のネットワーク設定

ここではWindows2000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。

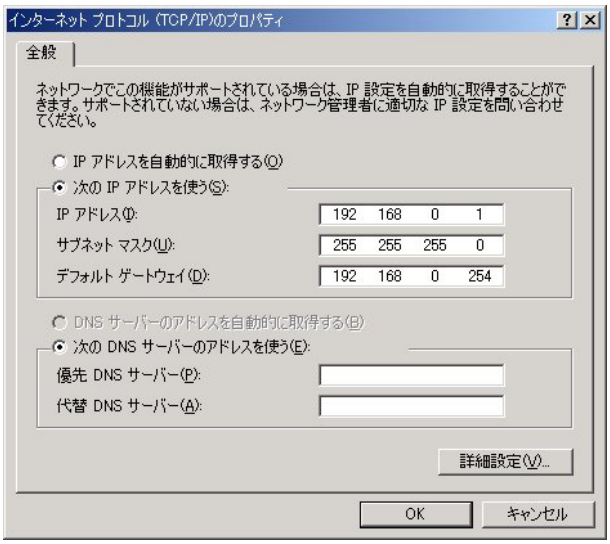
1 「コントロールパネル」→「ネットワークとダイヤルアップ接続」から、「ローカル接続」を開きます。

2 画面が開いたら、「インターネットプロトコル(TCP/IP)」のプロパティを開きます。



3 「全般」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」



4 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. 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。

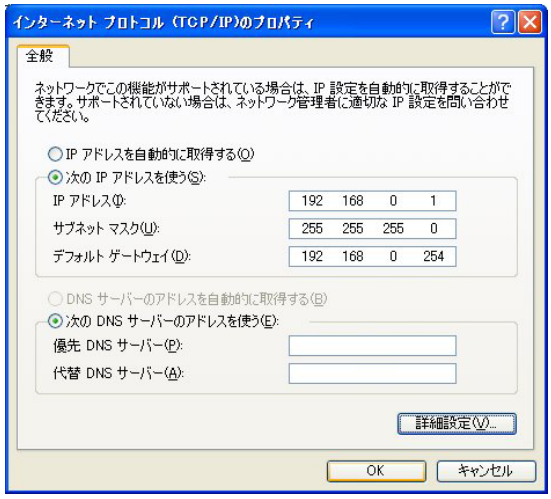
1 「コントロールパネル」→「ネットワーク接続」から、「ローカル接続」を開きます。

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」



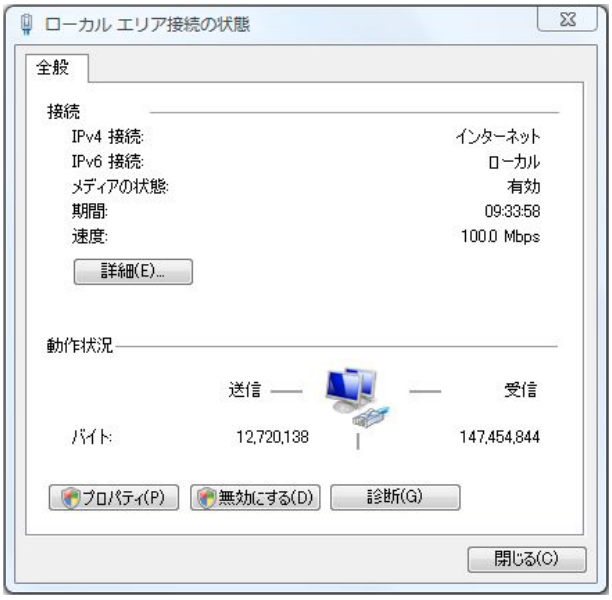
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

IV. Windows Vistaのネットワーク設定

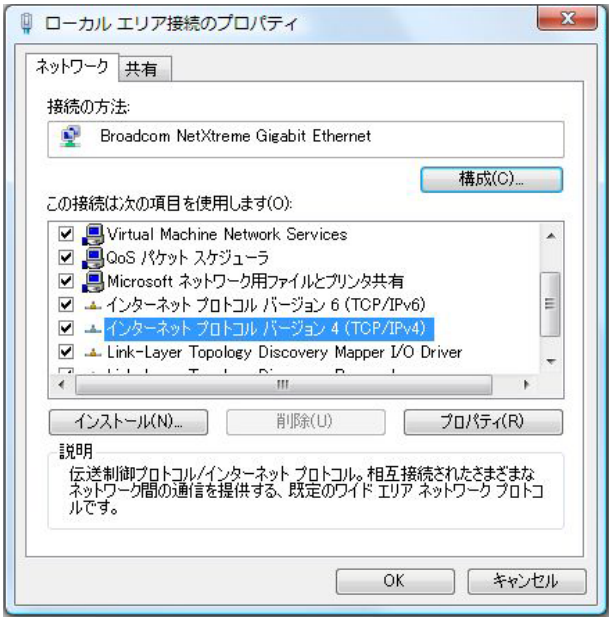
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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。

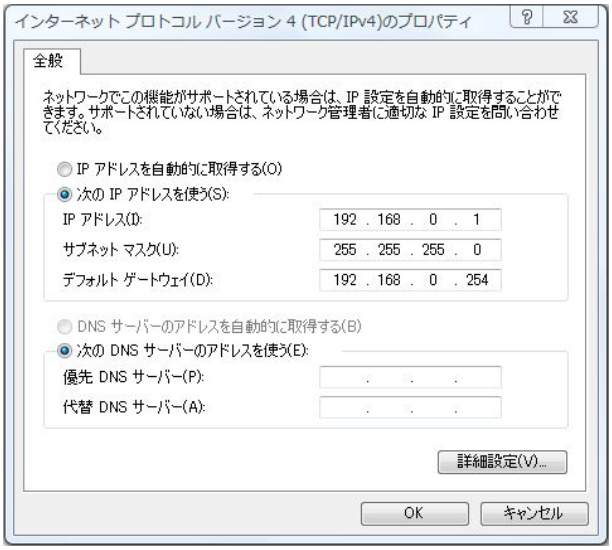


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



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」



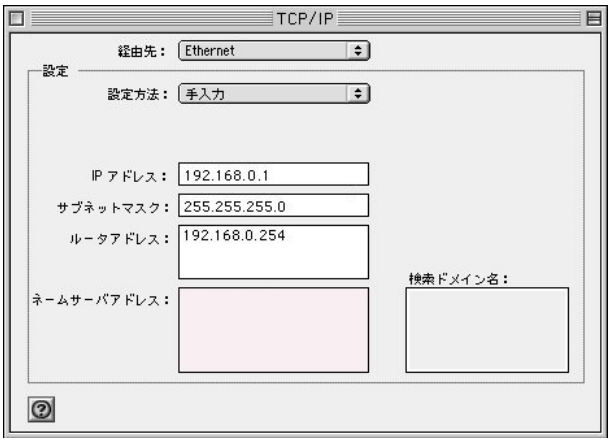
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

V. 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」

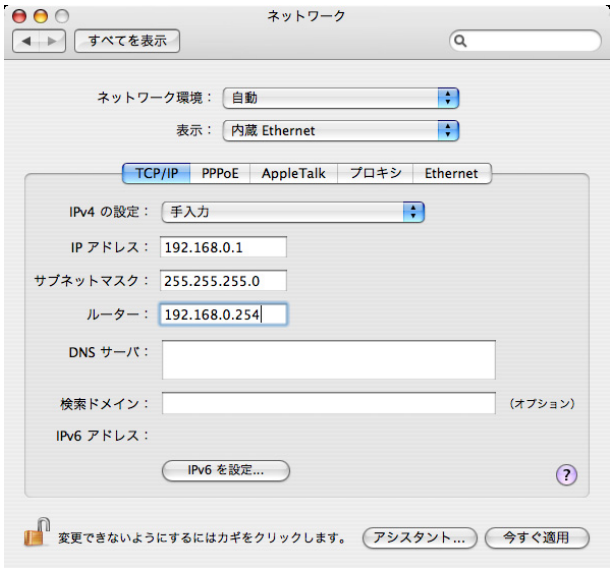


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これで本装置へログインする準備が整いました。

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。

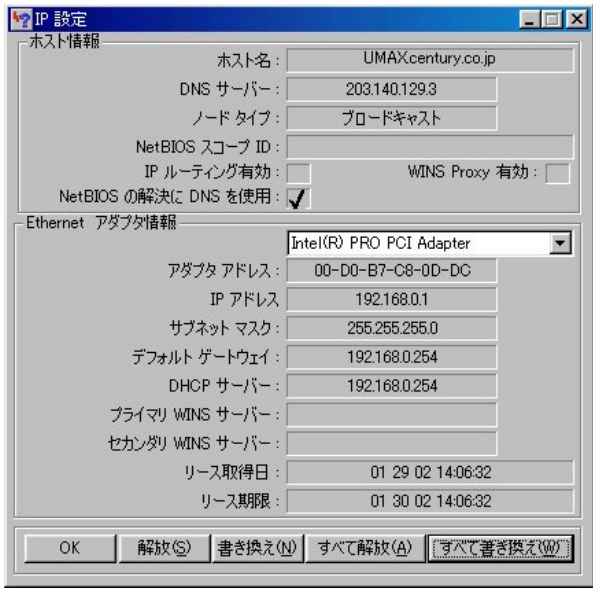
VI．IPアドレスの確認と再取得

◆Windows95/98/Meの場合

1 「スタート」→「ファイル名を指定して実行」を開きます。

2 名前欄に、”winipcfg”というコマンドを入力して「OK」をクリックしてください。

3 「IP設定」画面が開きます。リストから、パソコンに装着されているLANボード等を選び、「詳細」をクリックしてください。そのLANボードに割り当てられたIPアドレス等の情報が表示されます。



4 「IP設定」画面で「全て開放」をクリックすると、現在のIP設定がクリアされます。引き続いて「すべて書き換え」をクリックすると、IP設定を再取得します。

◆WindowsNT3.51/4.0/2000/XP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)
```

◆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。

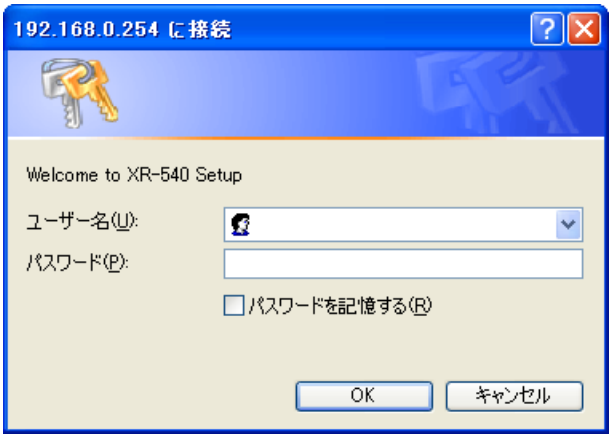
ブラウザのアドレス欄に、以下の IP アドレスとポート番号を入力してください。

http://192.168.0.254:880/

「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。

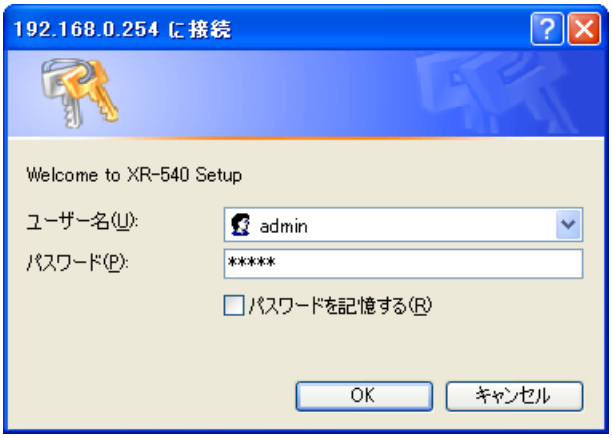
3 次のような認証ダイアログが表示されます。



（画面は XR-540）

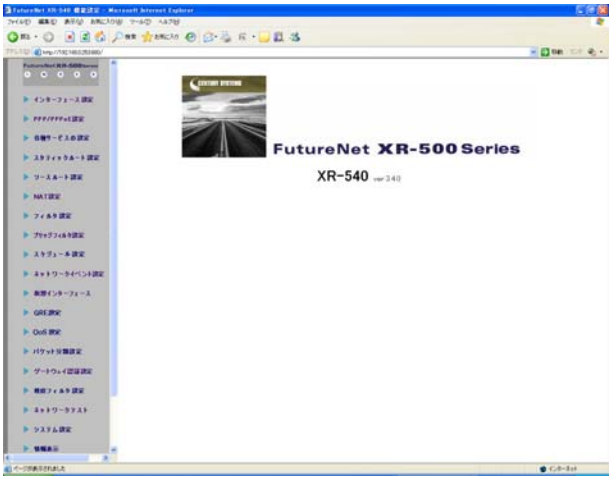
4 ダイアログ画面にパスワードを入力します。

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。



（画面は XR-540）

5 ブラウザ設定画面が表示されます。



（画面は XR-540）

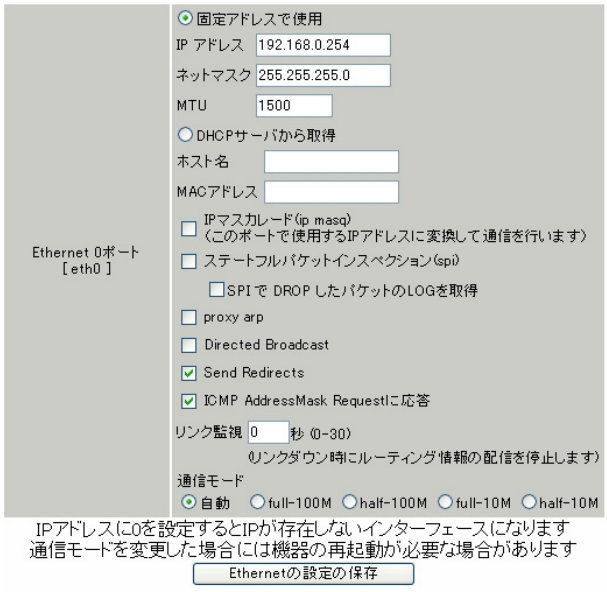
第5章

インターフェース設定

Ⅰ．Ethernet ポートの設定

◆各 Ethernet ポートの設定

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



[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はチェックし、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 から取得]

○ホスト名

○ MAC アドレス

IP アドレスが DHCP で割り当ての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。

※ XR-540 の、Ether2 ポートは対応していません。

○ IP マスカレード

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。

○ Proxy arp

ProxyARP 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 DirectedBroadcast の転送を許可します。

Directed Broeadcast

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

○ 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の送受信によって行う場合があります。
チェックを入れると、そのインター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、インター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行います。
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行いません。
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-100M」、「half-100M」、「full-10M」、「half-10M」です。
※ XR-730 の場合、「自動」を選択すると 1Gigabit に対応します。

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。

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 XR の設定にあわせて変更し、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。

11. 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、そのインターフェースへのアクセスは原則として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27章「パケットフィルタリング機能」**参照)。

[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”という論理インターフェースを自動的に生成し、このppp論理インターフェースを使って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ー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。

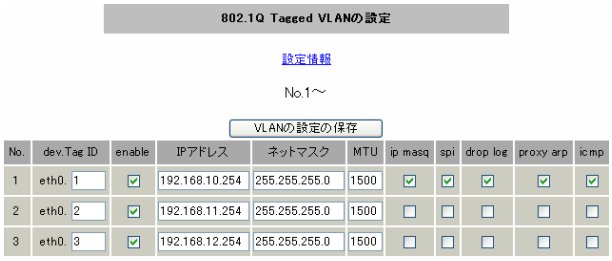
たとえば、IPsec通信をおこなう相手側のネットワークが192.168.1.0/24で、且つ、本装置のEther1ポートに192.168.1.254が設定されていると、正常にIPsec通信がおこなえません。

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

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１～３）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 64 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>」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
○サブネットマスク
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。
初期設定値は 1500byte になります。指定可能範囲は 68-1500byte です。

○ 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)されたパケットの情報を syslog に出力します。
SPI が有効の場合のみ設定可能です。

○ 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、そのインター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。

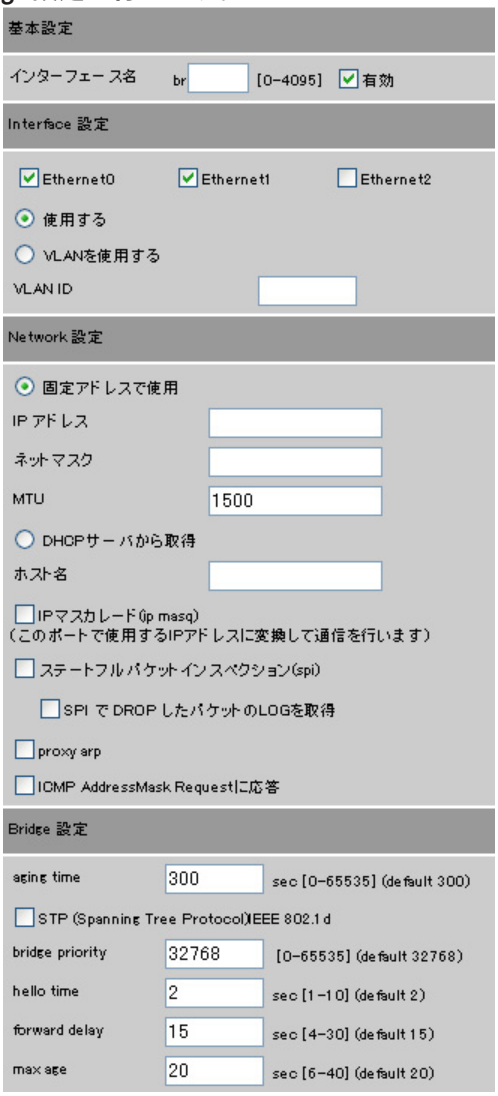
IV. Ethernet/VLAN ブリッジの設定

ここでは本装置を Bridge として運用するための設定を行います。2 つ以上の Ethernet インターフェース、または VLAN インターフェースに Bridge インターフェースを割り付けて使います。

◆Bridge の設定

まず Web 設定画面「インターフェース設定」→「Bridge の設定」をクリックすると、以下の画面が表示されます。

ここで画面下部の「追加」ボタンをクリックして、Bridge 設定を行います。



（画面は XR-540）

基本設定

○インターフェース名

作成する Bridge インターフェース名を指定します。ボックス内に 0～4095 の整数値を入力してください。また「有効」チェックボックスにチェックを入れてください。

Interface 設定

○ Ethernet0、Ethernet1、
または Ethernet2、Ethernet3

Bridge インターフェースを作成する Ethernet ポートを 2 つ選択してチェックを入れます。

○使用する

Ethernet 上の Bridge として使用する場合はチェックを入れます。

○ VLAN を使用する

○ VLAN ID

VLAN 上の Bridge として使用する場合はチェックを入れ、「VLAN ID」ボックスに VLAN タグ ID を入力してください。

VLAN 上の Bridge の場合は、指定した VLAN ID の VLAN インターフェースが、選択した Ethernet 上に作成されている必要があります。

なお、Bridge として使用しているインターフェースは、その間、元のインターフェースとしては使用できません。

IV. Ethernet/VLANブリッジの設定

Network設定

○固定アドレスで使用
○IPアドレス
○ネットマスク
Brigdeインターフェースの IPアドレスを固定で割り当てる場合は、「固定アドレスで使用」にチェックして、「IPアドレス」と「ネットマスク」を入力します。
※ IPアドレスを設定したくない場合は、IPアドレス、ネットマスクにそれぞれ「0」または「0.0.0.0」を入力してください。

○MTU
「Path-MTU-Black-HOLE」現象が発生した場合等は、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
Bridgeインターフェースの IPアドレスを DHCPで割り当てる場合は、「DHCPサーバから取得」にチェックして、必要であれば「ホスト名」を設定します。

○IPマスカレード
チェックを入れると、そのBridgeインターフェースで 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Bridgeインターフェース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が有効のときだけ設定可能です。

○Proxy ARP
Proxy ARPを使う場合はチェックします。

○ICMP AddressMask Requestに応答
チェックを入れると、そのインター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。

Bridge設定

○aging time
Bridgeインターフェースでは受信したフレームの送信元MACアドレスを学習し、一定時間保存します。aging timeはその保存時間(秒)です。
通常は初期設定(300秒)のままで構いません。

本装置では、他のブリッジとの冗長リンクを構成する場合にブリッジループによるブロードキャストストームを防ぐために Spanning Tree Protocol(IEEE 802.1D準拠 以下STP)を使用することができます。

○STP (Spanning Tree Protocol)IEEE 802.1d
STPを使用する場合はチェックを入れます。

○bridge priority
スパニングツリーアルゴリズムでは、ルートブリッジを決定するために64ビットのブリッジ IDを使用します。複数のブリッジの間で最もブリッジ IDの小さいブリッジがルートブリッジに選出されます。ブリッジ IDの上位16ビットとして用いられるのが、この bridge priorityです。
1～65535の間で設定可能です。

なお、下位48ビットは本装置の MACアドレスが用いられます。Bridgeインターフェースを設定した Ethernetポートのうち、最も若番の Ethernetポートの MACアドレスが採用されます。

○hello time
指定ポート(各セグメントにおいて最もルートブリッジに近いポート)から送られる BPDU(Bridge Protocol Data Unit)の送信間隔(秒)です。
1～10(秒)の間で設定可能です。

○forward delay
スパニングツリーのトポロジ変更により、ブロックポートが転送ポートに切り替わる際に、以下の2つの状態を経由して FORWARDING状態に遷移します。
forward delayとはそれぞれの状態における待機時間(秒)です。4～30(秒)の間で設定可能です。

- LISTENING状態
  他のブリッジからの BPDUを監視している状態
- LEARNING状態
  転送はブロックしているが MACアドレスを学習している状態

IV. Ethernet/VLAN ブリッジの設定

○ max age
指定ポート以外のポートでは、指定ポートからの BPDU を監視しており、一定時間 BPDU を受信しなくなった時にトポロジの変更が発生したと判断して STP の再構築を行います。max age とは BPDU の最大監視時間のことです。
設定可能な範囲は、6～40(秒)かつ
2×(hello_time+1)～2×(forward_delay-1)です。

注) XR-540 の Ethernet2 で STP を使用する場合、Ethernet2 の複数のポートを同じブリッジと接続すると、そこでループが発生してしまいますので注意してください。

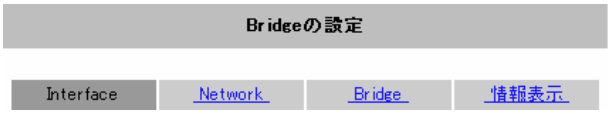
以上の入力が終わりましたら、「設定の保存」をクリックして設定完了です。

本装置では最大 64 個の Bridge インターフェースが設定できます。

注) 2 つ以上 Bridge を設定する場合の例
「eth0-eth1」と「eth1-eth2」・・・設定不可
「eth0-eth1」と「eth0.1-eth1.1」・・設定不可
「eth0.1-eth1.1」と「eth0.2-eth1.2」・・設定可
「eth0.1-eth1.1」と「eth1.1-eth1.2」・・設定不可

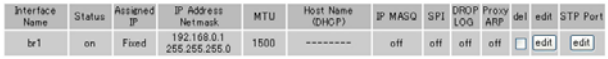
◆Bridge の設定

Bridge 設定後は「Bridge の設定」画面に設定内容が一覧で表示されます。
また画面中央の各リンクをクリックすると表示内容が切り替わります。



○ Interface
インターフェースに関する情報が表示されます。

○ Network
ネットワークに関する情報が表示されます。



○ Bridge
ブリッジ/STP に関する情報が表示されます。

○情報表示
それぞれの情報をテキストで詳細に表示します。

・インターフェース名
ボックス内に Bridge インターフェース名(ex. br1)を入力し、「表示する」をクリックします。インターフェースに関する情報を詳細に表示します。
「STP 表示」にチェックを入れた場合は、STP 情報の詳細も表示します。

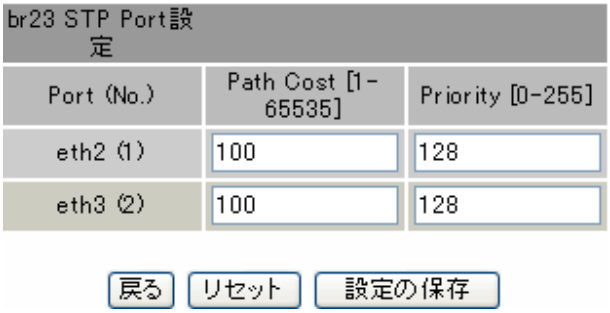
・MAC Table
ボックス内に Bridge インターフェース名を入力し、「表示する」をクリックします。Bridge インターフェースで学習した MAC アドレステーブルの詳細を表示します。

・すべての情報表示
全ての Bridge インターフェースについて、全ての詳細情報を表示します。

IV. Ethernet/VLAN ブリッジの設定

◆STP の詳細設定

本装置では STP に関してポート毎の詳細情報を設定することができます。各一覧表示の右端にある”STP Port”の「edit」をクリックします。



○Port Cost

非ルートブリッジの間でブロックポートを決定する際、お互いに BPDU を交換して、ルートブリッジまでのコスト値を比較します。コスト値の小さいブリッジのポートが優先的に転送ポートとなります。コスト値はこの Port Cost で設定します。
設定可能な範囲は 1～65535 です。

注)BPDU で配信するコスト値は、BPDU の送信ポートの Port Cost ではなく、ルートポートの Port Cost です。またルートブリッジの場合は、Port Cost の設定値に関係なく、コスト値 0 を配信します。

○Priority

本装置から同じセグメントに対して 2 つ以上のポートを接続している場合、ルートポートを決める際にこの Priority を用います。Priority の小さい方が優先的にルートポートとなります。
設定可能な範囲は 1～65535 です。

◆Bridge の変更

設定した Bridge インターフェースを変更する場合は、各一覧表示の右側にある”edit”の「edit」をクリックしてください。Bridge の設定画面が開きます。
一時的に使用しない場合は、「インターフェース名」の「有効」チェックを外してください。

◆Bridge の削除

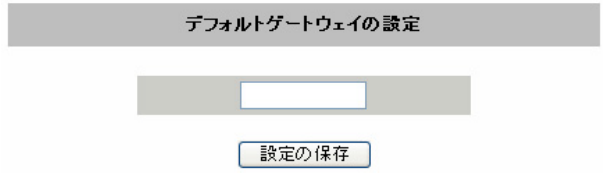
設定した Bridge インターフェースを削除する場合は、”del”のチェックボックスにチェックを入れ、「削除」をクリックします。

V. その他の設定

Web設定画面「インターフェース設定」→「その他の設定」にて設定します。

◆デフォルトゲートウェイの設定

デフォルトゲートウェイの設定は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

(※ XR-510にはありません)

XR-540、XR-730では、DummyInterfaceが設定できます。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。

V．その他の設定

◆ARP エントリの設定

「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、本装置の ARP テーブルについて設定することができます。

(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 エントリをクリックして「ARP エントリの固定化」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 エントリをクリックして「ARP エントリの削除」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。
入力欄に IP アドレスと MAC アドレスを入力し「ARP エントリの追加」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。
入力欄に IP アドレスと MAC アドレスを入力し「ARP エントリの追加」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。

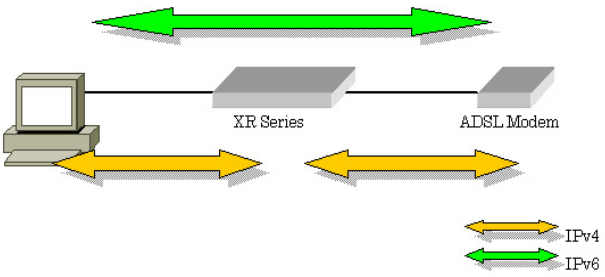
ARP テーブルの確認

「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)

V. その他の設定

本装置の IPv6 ブリッジは、NTT 東日本の FLET ’ S.Net に対応しています。
下記の図は、端末に IPv6 ブリッジ機能対応機器を使った場合のネットワーク構成です。

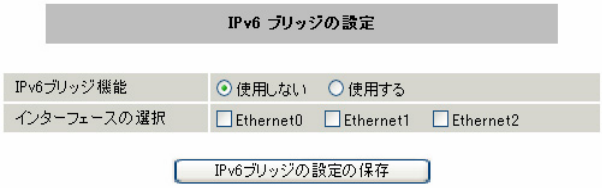


・IPv4 は、XR が PPPoE を終端します。
・IPv4 アドレスは、IPCP(Internet Protocol Control Protocol)で割り当てられます。
・IPv6 は、XR でブリッジされ、直接通信します。
・IPv6 アドレスは、FLET ’ S 側から直接払い出されます。

XR の実装においては IPv6 ブリッジ機能よりも一般のブリッジ機能のほうが優先的に処理されるますので、一般のブリッジ機能の設定がある場合には、IPv6 ブリッジ機能が設定どおりに動作しなくなる可能性があります。

◆ IPv6 ブリッジの設定

「インターフェースの設定」→「その他の設定」をクリックすると、本装置の IPv6 ブリッジについて設定することができます。



（画面は XR-540）

○ IPv6 ブリッジ機能
本機能を使用する場合は、「使用する」をチェックします。

○インターフェースの選択
（※ XR-510 にはありません）
IPv6 ブリッジを有効にするインターフェースを２つ選択します。

「IPv6 ブリッジの設定の保存」をクリックして設定完了です。

V．その他の設定

◆PPPoE ブリッジの設定

PPPoE ブリッジ機能を使用すると、本装置自身が行う PPPoE 接続の他に、本装置を経由した LAN 側のホストから外部への PPPoE 接続を行うことが可能です。その場合、本装置では PPPoE パケットを透過します。
この機能は本装置自身が PPPoE 接続している時も同時に利用できますので、PPPoE マルチセッションでの接続が可能です。

「インターフェースの設定」→「その他の設定」をクリックすると、本装置の PPPoE ブリッジについて設定することができます。

（画面は XR-540）

○PPPoE ブリッジ機能
本機能を使用する場合は、「使用する」をチェックします。

○インターフェイスの選択
（※ XR-510 にはありません）
PPPoE ブリッジを有効にするインターフェースを２つ選択します。

「PPPoE ブリッジの設定の保存」をクリックして設定完了です。

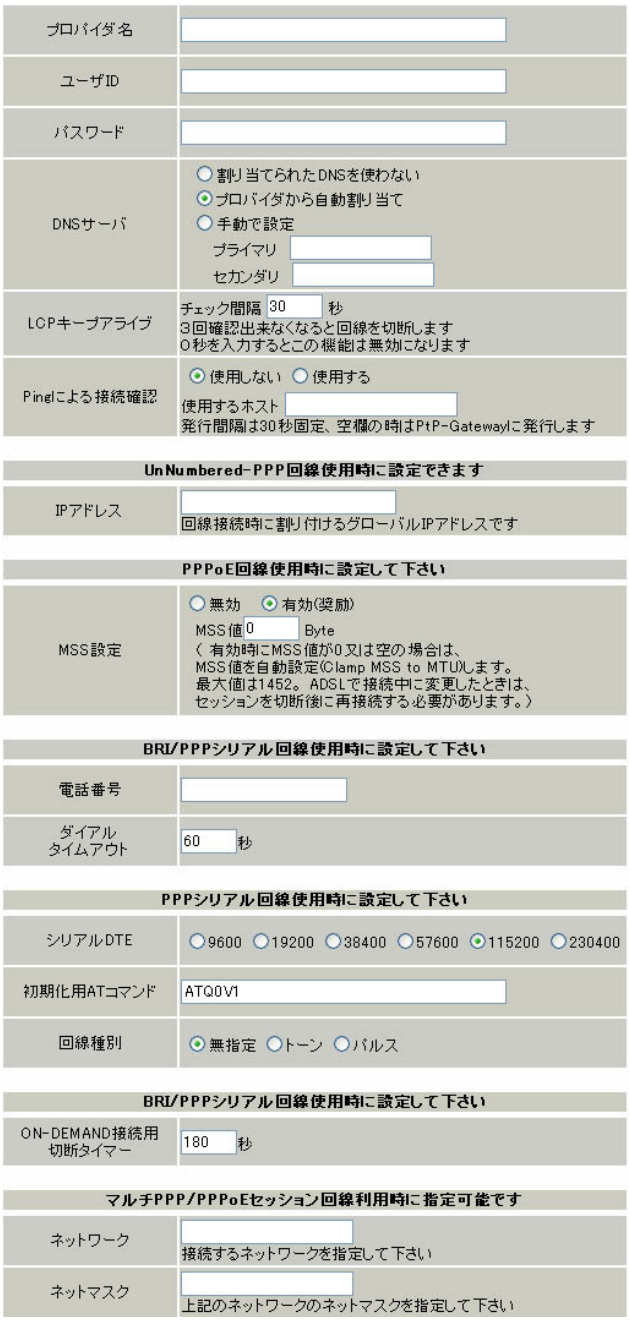
第 6 章

PPPoE 設定

第 6 章 PPPoE 設定

Ⅰ．PPPoE の接続先設定

Web 設定画面「PPP/PPPoE 設定」をクリックします。
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。「接続先設定」1～5 のいずれかをクリックします(5つまで設定を保存しておくことがきます)。



（画面は XR-540）

○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、半角英数字のみ使用できます。

○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。

○ 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。

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。

○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。

Ⅰ．PPPoE の接続先設定

○ 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)。
また ADSL で接続中に MSS 設定を変更したときは、PPPoE セッションを切断後に再接続する必要があります。

○電話番号
○ダイアルタイムアウト
○シリアル DTE
○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 接続の場合は設定の必要はありません。

○ネットワーク
○ネットマスク
例えば
　ネットワークアドレスに「172.26.0.0」
　ネットマスクに「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。

LAN 側の設定(IP アドレスや DHCP サーバ機能など)を変更する場合は、それぞれの設定ページで変更してください。

11．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」をクリックし、右画面の「接続設定」をクリックして、以下の画面から設定します。

（画面は XR-540）

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」
PPPoE(PPP)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 PPPoE 接続を開始します。

「スケジューラ接続」（※ **XR-540 のみ**）
BRI ポートでの接続をする時に選択できます。

○ RS232C 接続タイプ
（※ **XR-540 のみ**　RS232C/BRI 接続タイプ）
PPPoE 接続では「通常接続」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 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、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、そのインター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。

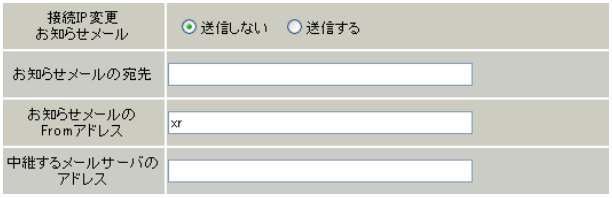
この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。
「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

III．その他の接続設定

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。

以下の箇所で設定します。



○接続 IP 変更お知らせメール
お知らせメール機能を使う場合は、「送信する」を選択します。

○お知らせメールの宛先
お知らせメールを送るメールアドレスを入力します。

○お知らせメールの From アドレス
お知らせメールのヘッダに含まれる、”From ”項目を任意で設定することができます。

○中継するメールサーバのアドレス
お知らせメールを中継する任意のメールサーバを設定できます。IP アドレス、ドメイン名のどちらでも設定できます。
ただしドメイン名で指定するときは、下記の記述で設定してください。

＜入力形式＞　**＠＜ドメイン名＞**
＜入力例＞　　@mail.xxxxxx.co.jp

IV. 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。

IV. バックアップ回線

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ください」欄で設定します。

（画面はは XR-540）

○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
バックアップ回線で使用するインタフェースを選択します。

○ RS232C 接続タイプ
（※ **XR-540 のみ**　RS232C/BRI 接続タイプ）
RS232C（/BRI）インター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
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 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。

○ ICMP AddressMask Request
「応答する」にチェックを入れると、そのインター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。

○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 が帰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。

IV. バックアップ回線

○ 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。(EX. 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 13 章 IPsec 設定**」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。

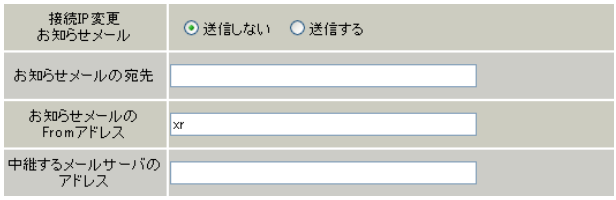
このほか、NAT 設定・パケットフィルタ設定・ルーティング設定など、バックアップ回線接続時のための各種設定を別途行なってください。

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。

接続変更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。

以下の箇所で設定します。



○接続お知らせメール
お知らせメール機能を使う場合は、「有効」を選択します。

○お知らせメールの宛先
お知らせメールを送るメールアドレスを入力します。

○お知らせメールの From アドレス
お知らせメールのヘッダに含まれる、” From ” 項目を任意で設定することができます。

○中継するメールサーバのアドレス
お知らせメールを中継する任意のメールサーバを設定できます。IP アドレス、ドメイン名のどちらでも設定できます。
ただしドメイン名で指定するときは、下記の記述で設定してください。

＜入力形式＞　**@ ＜ドメイン名＞**
＜入力例＞　　@mail.xxxxxx.co.jp

V. PPPoE 特殊オプション設定について

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 接続が行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。

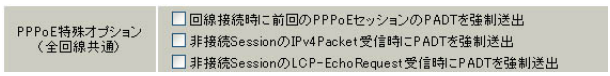
ここで PPPoE 特殊オプション機能を使うことにより、本装置が PPPoE セッションを確立していないことを検知し、強制的に PADT パケットを地域 IP 網側へ送信して、地域 IP 網側に PPPoE セッションの終了を通知します。

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行います。

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行います。

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

ダイヤルアップ接続

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接続ができます。

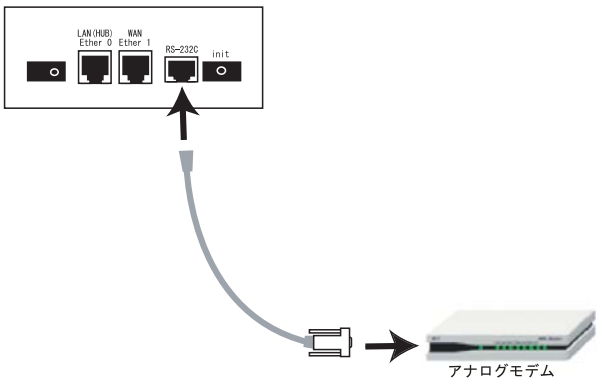
◆アナログモデム /TA の接続（XR-510 の場合）

1　XR-510 本体背面の「RS-232」ポートと製品付属の変換アダプタとを、ストレートタイプの LAN ケーブルで接続してください。

2　変換アダプタのコネクタを、アナログモデム /TA のシリアルポートに接続してください。モデム /TA のコネクタが 25 ピンタイプの場合は別途、変換コネクタをご用意ください。

3　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



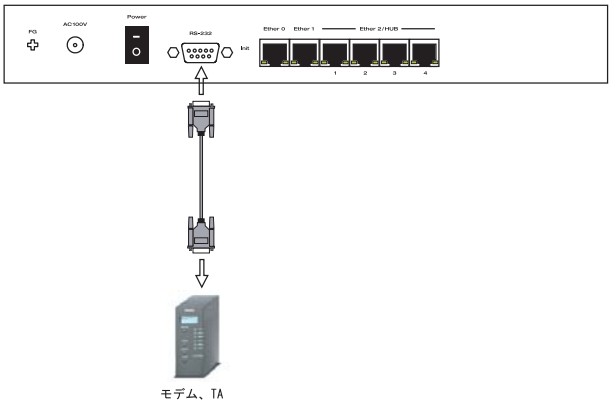
◆アナログモデム /TA のシリアル接続（XR-540、XR-730 の場合）

1　XR-540 の電源をオフにします。

2　XR-540、XR-730 の「RS-232C」ポートとモデム /TA のシリアルポートをシリアルケーブルで接続します。シリアルケーブルは別途ご用意ください。

3　全ての接続が完了しましたら、モデムの電源を投入してください。

接続図



ⅠⅠ．BRI ポートと TA/DSU の接続（※ XR-540 のみ）

◆外部の DSU を使う場合

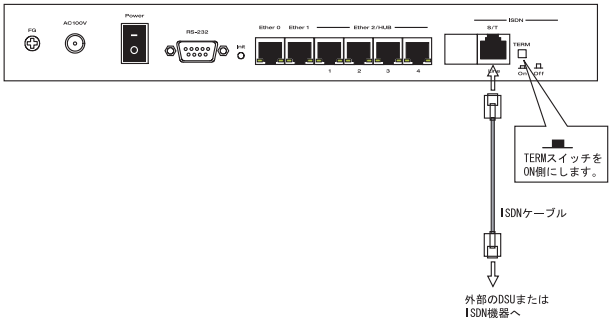
1 XR-540 の電源をオフにします。

2 外部の DSU と本装置の「BRI S/T LINE」ポートを ISDN 回線ケーブルで接続します。ISDN ケーブルは別途ご用意ください。

3 本体背面の「TERM.」スイッチを「ON」側にします。

4 全ての接続が完了しましたら、モデムの電源を投入してください。

接続図

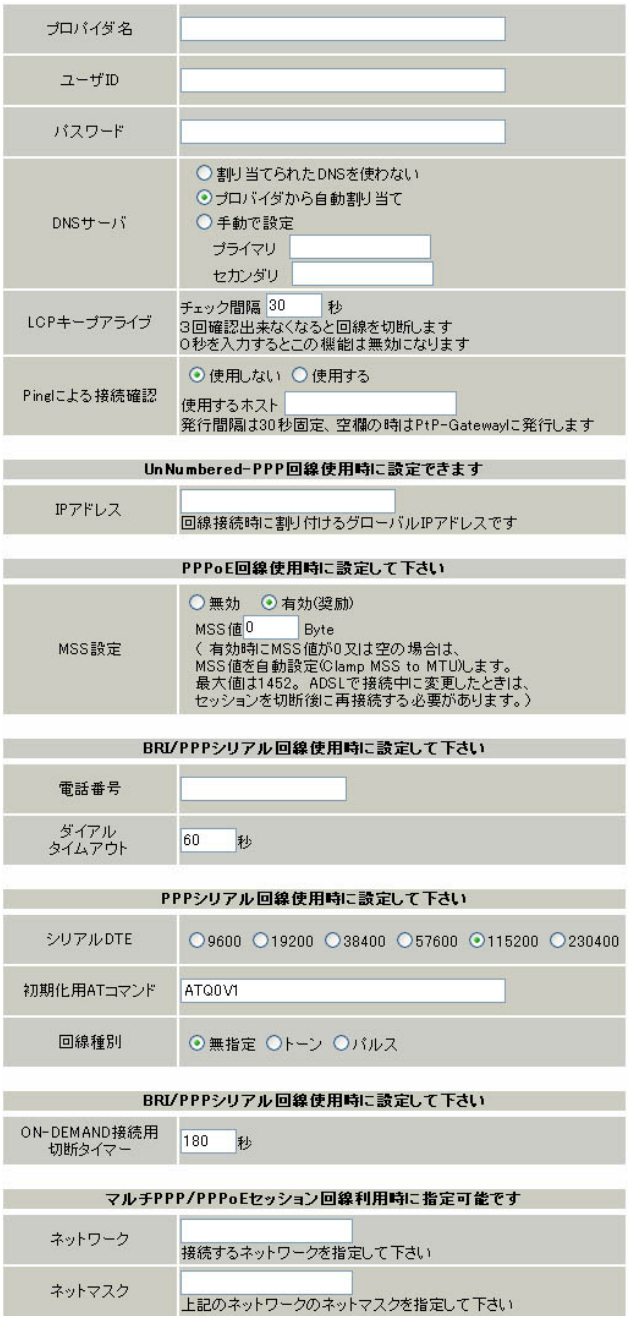


III．接続先設定

PPP 接続の接続先設定を行ないます。以下の手順で設定してください。

Web 設定画面「PPP/PPPoE 設定」をクリックして接続先の設定をおこないます。

右画面上部「接続先設定」１～５のいずれかをクリックします(5つまで設定を保存しておくことができます)。



（画面は XR-540）

○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。

○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。

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必要はありません。

III. 接続先設定

○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。

○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
例えば
　ネットワークアドレス「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 の接続設定を行ないます。

IV. ダイヤルアップの接続と切断

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」をクリックします。右画面の「接続設定」をクリックして、以下の画面から設定します。

（画面は XR-540）

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。
リモートアクセス接続では「RS232C」ポートを選択します。

○接続形態
「手動接続」
リモートアクセスの接続 / 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リモートアクセス接続を開始します。

「スケジューラ接続」（※ **XR-540 のみ**）
BRI ポートでの接続をする時に選択できます。

○ RS232C 接続タイプ
（※ **XR-540 のみ**　RS232C/BRI 接続タイプ）
「通常接続」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
リモートアクセス接続時に 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
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 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、リモートアクセス接続時に 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、リモートアクセス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。**特に必要のない限り「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、そのインター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。

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。

V. 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、接続 IP お知らせメール機能、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　IV. バックアップ回線」**をご覧ください。

VI．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、XR 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

専用線接続
（※ XR-540のみ）

第 8 章　専用線接続(※ XR-540 のみ)

Ⅰ．BRI ポートと TA/DSU の接続

XR-540 は、ISDN S/T 点ポート(BRI ポート)を搭載しています。このポートにターミナルアダプタを接続することによって、専用線接続を行うことが出来ます。

◆外部の DSU を使う場合

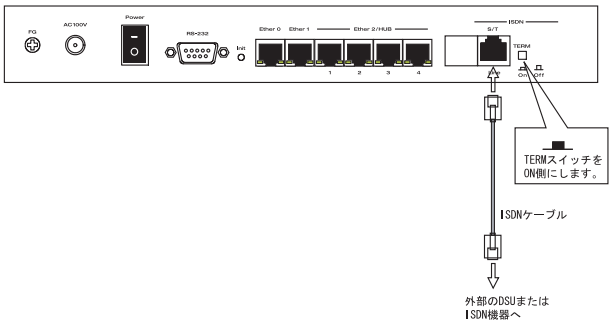
1 XR-540 の電源をオフにします。

2 外部の DSU と本装置の「BRI S/T LINE」ポートを ISDN 回線ケーブルで接続します。ISDN ケーブルは別途ご用意ください。

3 本体背面の「TERM.」スイッチを「ON」側にします。

4 全ての接続が完了しましたら、モデムの電源を投入してください。

接続図



第 8 章　専用線接続(※ XR-540 のみ)

II．専用線設定

専用線設定を行ないます。以下の手順で設定してください。

Web 設定画面「PPP/PPPoE 設定」→「専用線設定」をクリックして接続先の設定をおこないます。

○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。

○本装置の IP アドレス
プロバイダから指定された IP アドレスを入力してください。

○接続先の IP アドレス
プロバイダから指定された IP アドレスを入力してください。
指定された IP アドレスがない場合は、「0.0.0.0」を入力してください。

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/PPPoE 接続設定を行ないます。

III．専用線の接続と切断

続いて、専用線の接続設定をおこないます。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。

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	○Ether0 ○Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ◉Leased Line(64K) ○Leased Line(128K) ○RS232C
接続形態	○手動接続 ◉常時接続 ○スケジューラ接続
RS232C/BRI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

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
専用線接続では、任意の接続先を選択してください（実際の接続先は、「II．専用線設定」の設定内容が反映されます)。

○接続ポート
専用線接続では、「Leased Line(64K)」、または「Leased Line(128K)」を選択してください。

○接続形態
専用線接続では「常時接続」を選択してください。

○ RS232C/BRI 接続タイプ
専用線接続では「通常」を選択してください。

○ IP マスカレード
専用線接続時に 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
専用線接続時に、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 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、専用線接続時に 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、専用線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。**特に必要のない限り「有効」設定にしておきます。**

III．専用線の接続と切断

○ ICMP AddressMask Request
「応答する」にチェックを入れると、そのインター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。

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。

第9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(リモートアクセス)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
・バックアップ回線を指定する
・IPsec 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ー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、それぞれのインターフェースにステートフルパケットインスペクション、又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下のステップに従って設定してください。

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。

Web 設定画面「PPP/PPPoE 設定」をクリックし、「接続先設定」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 接続」**または**第 7 章「ダイヤルアップ接続」**をご覧ください。

複数アカウント同時接続の設定

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」をクリックし、「接続先設定」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 接続」**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。

マルチPPP/PPPoEセッション回線利用時に指定可能です	
ネットワーク	接続するネットワークを指定して下さい
ネットマスク	上記のネットワークのネットマスクを指定して下さい

○ネットワークアドレス
○ネットマスク
例えば
　ネットワークアドレスに「172.26.0.0」
　ネットマスクに「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」をクリックして接続先設定は完了です。

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	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	○Ether0 ⊙Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○Leased Line(64K) ○Leased Line(128K) ○RS232C
接続形態	⊙手動接続 ○常時接続 ○スケジューラ接続
RS232C/BRI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

（画面は XR-540）

○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
（※ **XR-540 のみ** RS232C/BRI 接続タイプ）
「通常接続」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。

複数アカウント同時接続の設定

○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 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」を選択します。

○ ICMP AddressMask Request
任意で選択します。

○接続 IP 変更お知らせメール
任意で設定します。

続いてマルチ接続用の接続設定をおこないます。

（画面は XR-540）

[マルチ接続用の設定]
以下の部分で設定します。

○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
(※ **XR-540 のみ** RS232C/BRI 接続タイプ)
「通常接続」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 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。

○ 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)。

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 10 章

各種サービスの設定

各種サービス設定

Web 設定画面「各種サービスの設定」をクリックすると、以下の画面が表示されます。

ここでは

・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 機能
- 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「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 11 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。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行うかどうかを指定します。

設定後に「設定の保存」をクリックして設定完了です。

◆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。

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は、サービスの再起動(「停止」→「起動」)をおこなってください。

第 12 章

DHCP サーバ / リレー機能

第 12 章 DHCP サーバ / リレー機能

Ⅰ. 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 インターフェース設定」を参照してください。

◆ 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 サーバ機能（VLAN 対応）
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。
また、VLAN ごとに DHCP サーバ機能の設定を行うこともできます。

◆ 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 XR 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(XR 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)。

DHCP リレー機能は NAT 機能を利用している場合の利用はできません。

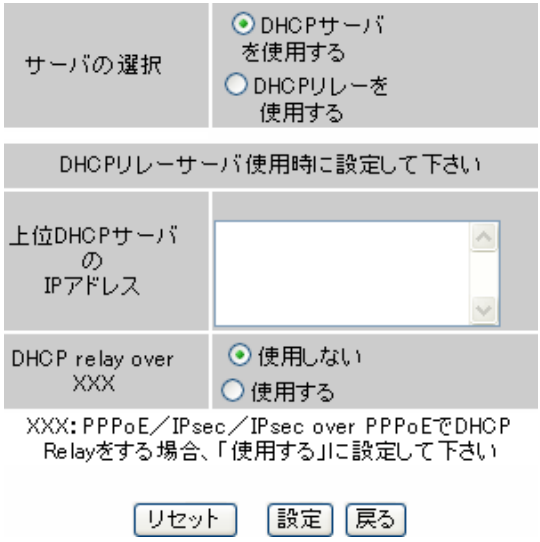
第 12 章 DHCP サーバ / リレー機能

11. DHCP 設定

DHCP サーバ / リレー機能の設定を行います。

Web 設定画面「各種サービスの設定」→「DHCP (Relay)サーバ」をクリックして、以下の画面で設定をおこないます。

[DHCP 設定]



○サーバの選択
DHCP サーバ機能 / リレー機能のどちらを使うかを選択します。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。

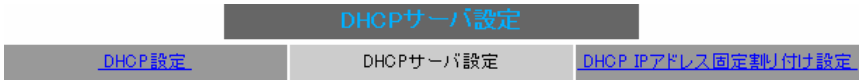
○上位 DHCP サーバの IP アドレス
上記「サーバの選択」で「DHCP リレーを使用する」を選択した場合に、上位の DHCP サーバの IP アドレスを指定します。

○ DHCP relay over xxx
上記「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をおこないます。PPPoE・IPsec・PPPoE 接続時の IPsec 上で DHCP リレー機能を利用する場合は「使用する」を選択します。

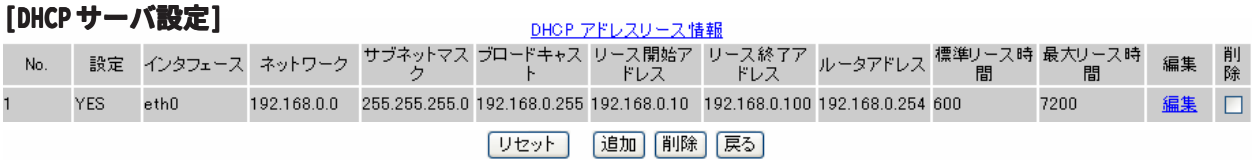
最後に「設定」をクリックして完了です。

III. DHCP サーバ設定

DHCP サーバ機能を使用する場合は、Web 設定画面の「DHCP サーバ設定」をクリックし、以下の画面で設定を行います。



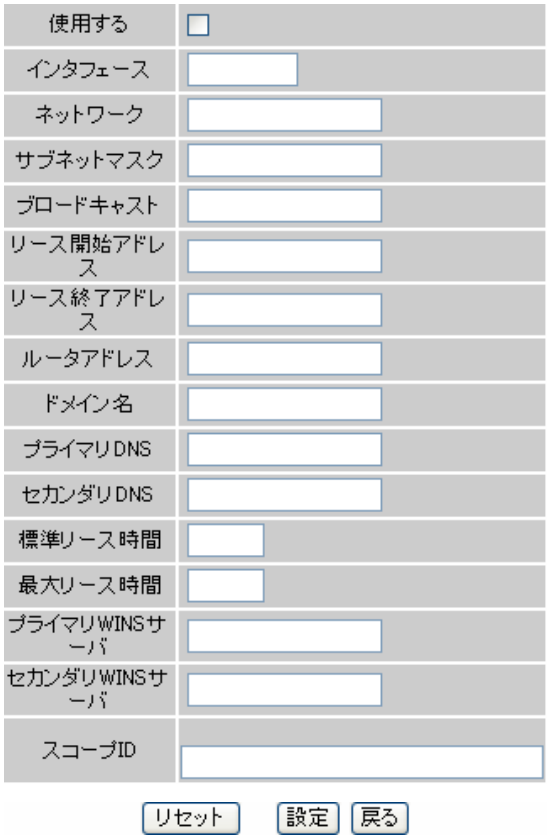
[DHCP サーバ設定]



現在の DHCP サーバ設定の一覧が表示されます。「DHCP アドレスリース情報」をクリックすると、現在のリース情報を確認できます。

DHCP サーバ設定の追加・編集

「編集」または「追加」ボタンをクリックして、以下の画面を開きます。



○使用する
この設定を DHCP サーバ機能に反映させる場合は、チェックを入れます。

○インターフェース
DHCP サーバを動作させるインターフェースを指定します。
指定可能なインターフェースは、Ethernet・VLAN の各インターフェースです。インターフェース名については「付録 A」をご覧ください。

設定を旧バージョンのファームウェアから引き継ぐ場合に、本装置がインターフェースの特定が出来ず DHCP サービスを起動できないことがあります。その場合には、インターフェース名の手動設定が必要です。

○ネットワーク
DHCP サーバを動作させる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 サーバを動作させるネットワーク空間のサブネットマスクを指定します。

○ブロードキャスト
DHCP サーバを動作させる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。両項目で設定した範囲の IP アドレスが、DHCP クライアントに割り当てられます。

III. DHCP サーバ設定

○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、XR 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指定します（任意で指定）。

○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（任意で指定）。

○標準リース時間
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：秒）。

○最大リース時間
DHCP クライアントが割り当て時間を要求した時の最大割り当て時間を指定します（単位：秒）。指定した値以上のリース時間を要求された場合、リース時間は指定値で設定されます。

○プライマリ WINS サーバ
○セカンダリ WINS サーバ
DHCP クライアントに割り当てる WINS サーバの IP アドレスを指定します。

○スコープ ID
NetBIOS スコープ ID を配布できます。TCP/IP を介して NetBIOS を実行しているコンピュータでは、同じ NetBIOS スコープ ID を使用するほかのコンピュータとのみ NetBIOS 情報を交換することができます。

入力後、「設定」をクリックして設定完了です。
設定を変更した場合はサービスの再起動が必要です。

DHCP サーバ設定の削除

DHCP サーバ設定の一覧画面で、右側の「削除」欄にチェックを入れ「削除」ボタンをクリックします。

DHCP リレー機能について

本装置を DHCP リレー先の DHCP サーバとして運用するときは、リレー元のネットワーク向けサブネット設定とともに、本装置直下に接続された LAN に対して有効なサブネット設定を行う必要があります(DHCP サーバとして動作させるためには、最低 1 つの、有効なサブネット設定が必要です)。

IV. DHCP IP アドレス固定割り付け設定

DHCP サーバ機能で固定 IP アドレスを割り当てる場合の設定をおこないます。

Web 設定画面の「DHCP IP アドレス固定割り付け設定」をクリックし、以下の画面を開きます。

[DHCP IP アドレス固定割り付け設定]

○ 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

割り当てる IP アドレスを指定します。

入力後、「設定」をクリックして設定完了です。

設定を有効にするにはサービスの再起動が必要です。

DHCP IP アドレス固定割り付け設定の削除

設定画面右側の「削除」欄にチェックを入れて「設定」ボタンをクリックします。

IP アドレス固定割り当て時の DHCP サーバ設定について

DHCP サーバ機能で IP アドレス固定割り付け設定のみを使用する場合でも、DHCP サーバ設定は必要です。

その場合は「DHCP サーバ設定」画面の「リース開始アドレス」「リース終了アドレス」に、「DHCP IP アドレス固定割り付け設定」で指定したアドレス範囲の先頭と末尾の IP アドレスを指定してください。

第 13 章

IPsec 機能

1．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。暗号化処理はハードウェア処理で行ないます。

◆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
XR-510 は 64 拠点まで IPsec 接続が可能です。
XR-540、XR-730 は最大 128 拠点と IPsec トンネルを構築できます。また VPN 接続できる LAN/ ホストは最大 128 となります。

◆ 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
本装置同士の場合、NAT 内のプライベートアドレス環境においても IPsec 接続を行うことができます。

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)**

11. 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通信を行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」画面でのインター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 XR 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

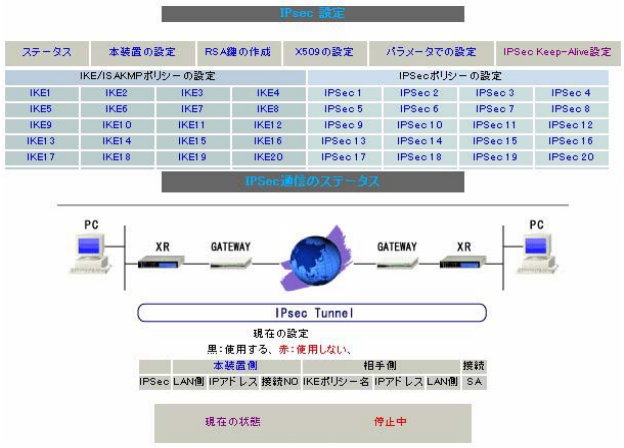
IPsec 起動後に、正常に IPsec 通信ができるかどうかを確認します。「情報表示」画面でのインターフェースとルーティングテーブル、ログで確認します。

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。



(画面は表示例です)

- **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**

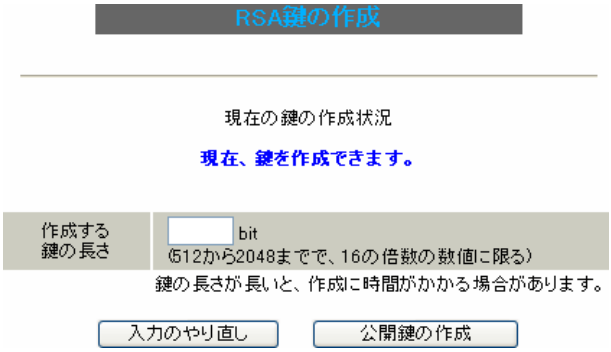
IPsec に関する設定・確認は、全てこの設定画面からおこなえます。

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。

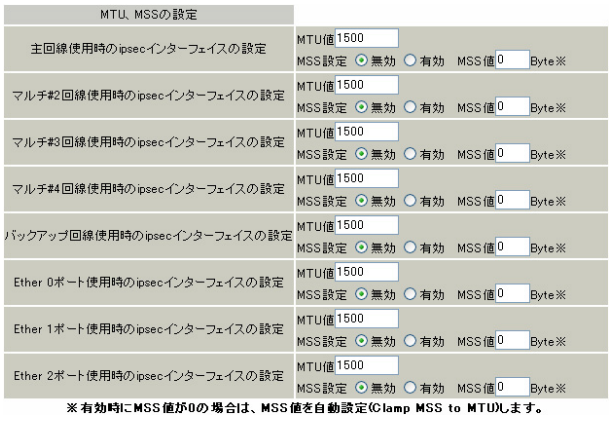
III. IPsec 設定

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。

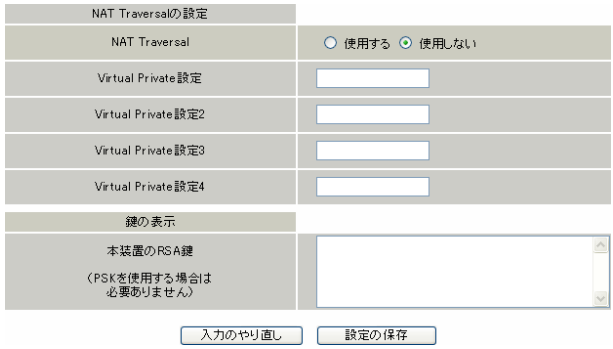


（画面は XR-540）

（画面は XR-730）

○ MTU、MSS の設定

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。
指定可能な範囲は、MTU が 68-1500、MSS は 1-1460 です。



○ 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 通信を行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。下記のいずれの場合も「使用する」を選択してください。

- 本装置が NAT 内の IPsec クライアントの場合
- 本装置が NAT 外の IPsec サーバの場合

「Virtual Private 設定」

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。

%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

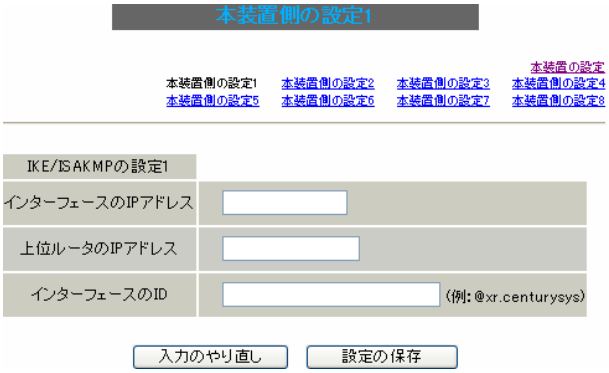
RSA 鍵の作成をおこなった場合ここに、作成した本装置の RSA 公開鍵が表示されます。
PSK 方式や X.509 電子証明を使う場合はなにも表示されません。

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」の 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。



○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]

「%ppp0」と入力します。Ether0(Ether1)ポートで接続している場合は「%eth0(%eth1、または %eth2)」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。

○インターフェースの 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「インターフェースの IP アドレス」を ID として使用します。

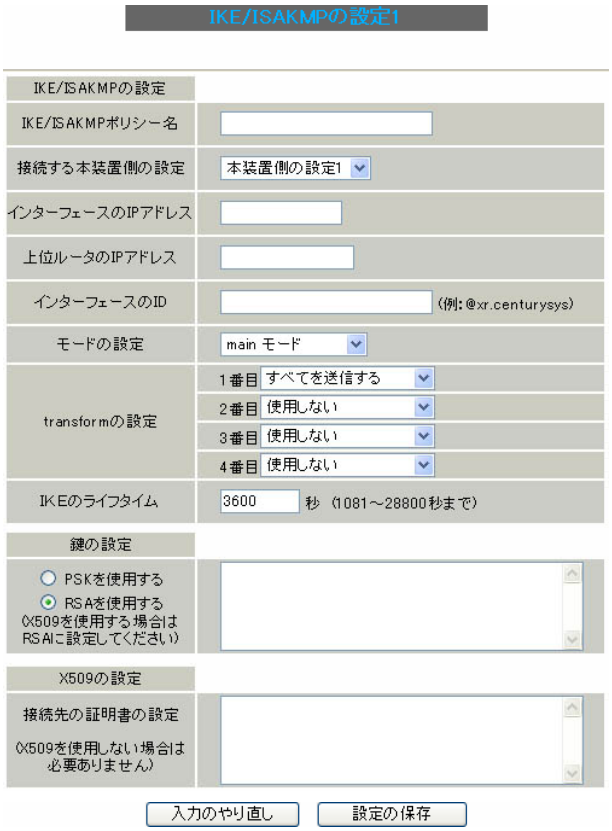
最後に「設定の保存」をクリックして設定完了です。

続いて **IKE/ISAKMP ポリシー**の設定をおこないます。

III. IPsec 設定

STEP 4 IKE/ISAKMAP ポリシーの設定

IPsec 設定画面上部の「IKE/ISAKAMP ポリシーの設定」の「IKE1」～「IKE128」いずれかをクリックして、以下の画面から設定します。



(画面は表示例です)

○ 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」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。また NAT トラバーサルを使用し、対向側装置が NAT 内にある場合にも 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「agressive モード」のどちらかから選択します。

○ 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)

「agressive 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。agressive 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。

III. IPsec 設定

○鍵の設定

[PSK 方式の場合]

「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。最大 2047 文字まで設定できます。

[RSA 公開鍵方式の場合]

「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。

○ X.509 の設定

「X.509」設定で IPsec 通信をおこなう場合は、相手側装置に対して発行されたデジタル証明書をテキストボックス内に貼り付けます。

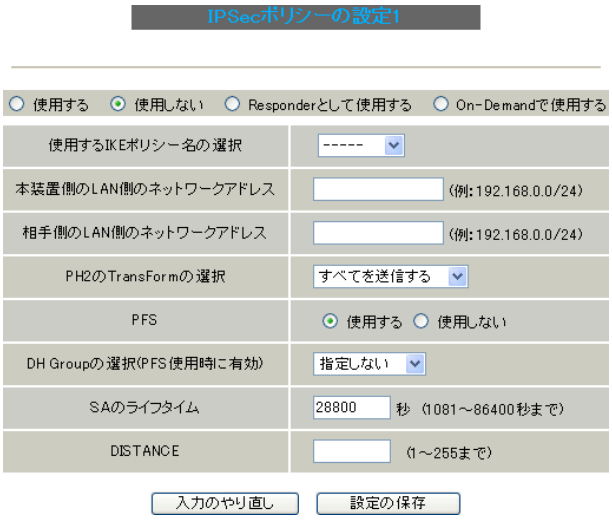
最後に「設定の保存」をクリックして設定完了です。

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 128」いずれかをクリックして、以下の画面から設定します。



(画面は表示例です)

○最初に IPsec の起動状態を選択します。

「使用する」
initiater 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
自分側の本装置に接続している 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
相手側の IPsec 装置に接続されている 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。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。

また、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 (3des、des、aes128)
- 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。

○ 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。

III. IPsec 設定

○ 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XR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、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。

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（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)**

及び

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)のメッセージは、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)のメッセージは、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。

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

○ 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 通信を行う際の、XR の LAN 側インターフェースの IP アドレスを入力します。

○ destination address
IPsec 通信を行う際の、XR の対向側装置の LAN 側のインターフェースの 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「動作オプション 1」の設定に応じて、入力値の意味が異なります。

・動作オプション 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。
但し、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。

・動作オプション 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。

IV. IPsec Keep-Alive 機能

○動作オプション 1
IPsecネゴシエーションと同期してKeep-Aliveを行う場合は、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 を行います。

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が非同期に行われるため、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行います。動作オプション1を有効にした場合、各フェーズと同期したKeep-Alive動作を行います。

・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の送出は行いません。

・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 のダウンを行います。
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。

○動作オプション 2
本オプションは「動作オプション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 インターフェース名を選択します。本装置のインター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。

○ 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。

IV. IPsec Keep-Alive 機能

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。

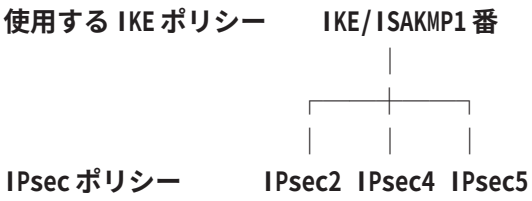
＜入力例＞
1_2_3

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 S A 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行います。

＜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 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。

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。

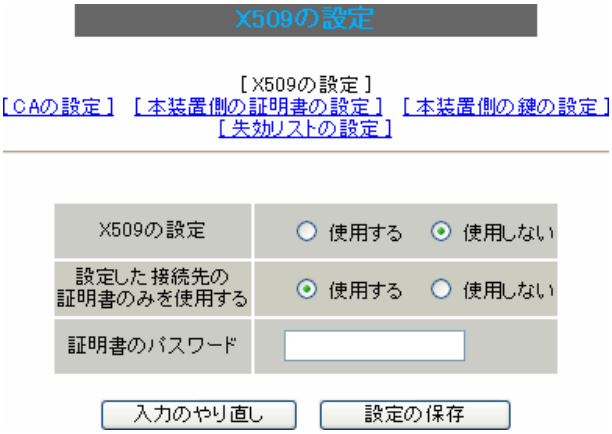
ただし本装置は証明書署名要求の発行や証明書の発行ができませんので、あらかじめ CA 局から証明書の発行を受けておく必要があります。

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」から行えます。

[X.509 の設定]
「X.509 の設定」画面→「X.509 の設定」を開きます。



○X.509 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
使用するか、使用しないかを選択します。

○証明書のパスワード
証明書のパスワードを入力します。

入力が終わりましたら「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

[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。

[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。

[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。

[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。

各設定に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。

注） その他の設定については、通常の IPsec 設定と同様にしてください。

その際、「IKE/ISAKMAP ポリシーの設定」画面内の鍵の設定項目は、「RSA を使用する」にチェックします。鍵は空欄のままにします。
(「本装置の設定」画面の鍵表示も空欄のままです)。

以上で X.509 の設定は完了です。

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

但し、NAT トラバーサルを使用する場合は、IKE の一部のトラフィックおよび暗号化ペイロードは UDP の 4500 番ポートのパケットにカプセリングされています。よって、以下の 2 種類のプロトコル・ポートに対するフィルタ設定の追加が必要になります。

- **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「UDP」のポート「4500」番**
  →一部の IKE トラフィックおよび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。

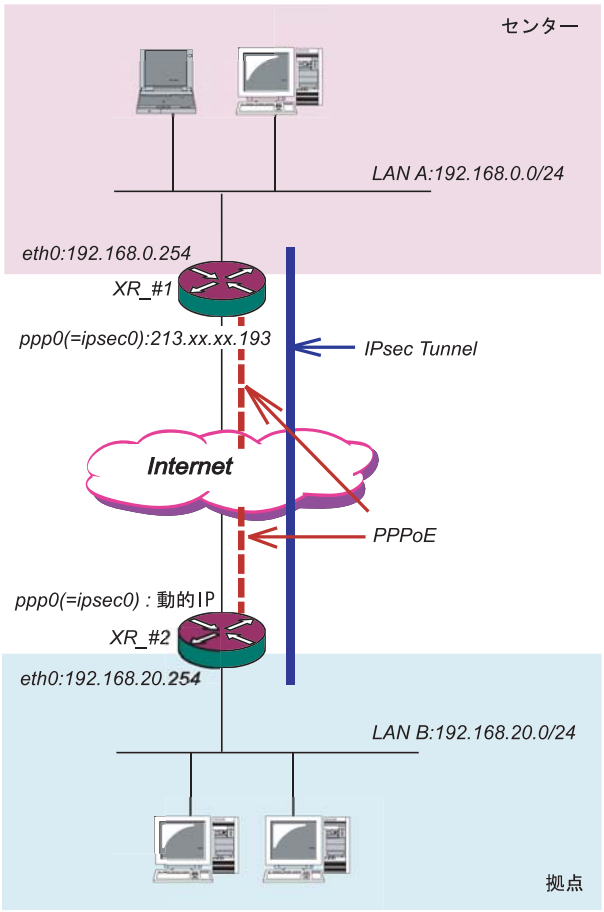
< 設定例 >

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、インター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。

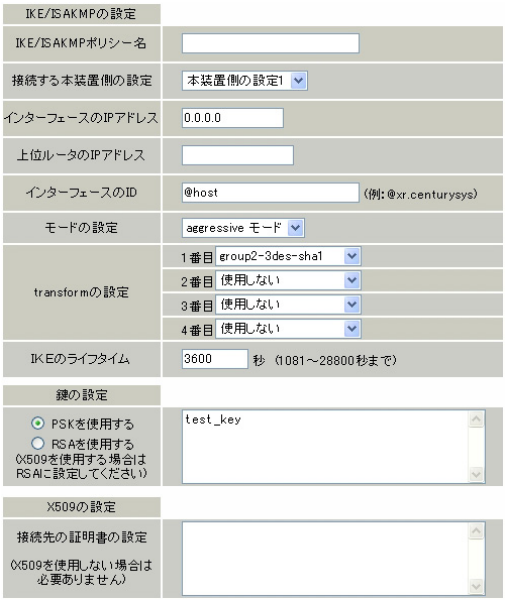
○インターフェースの IP アドレス
「213.xx.xx.193」

○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。

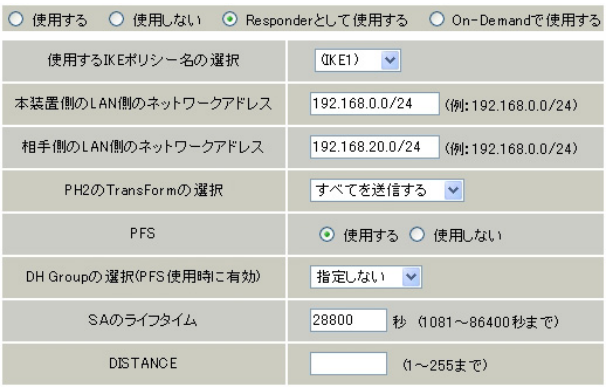
○モードの設定 「aggressive モード」

○ 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)

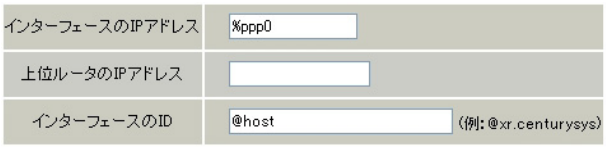
○ DISTANCE 「空欄」
※省略した場合は、自動的にディスタンス値を「1」として扱います。

「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。

「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」

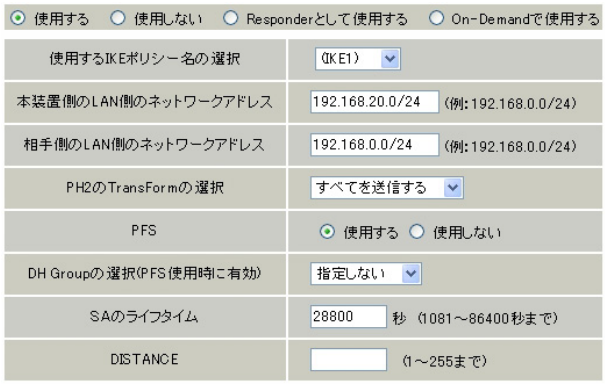
○ transform の設定 「group2-3des-sha1」
(任意の設定を選択)

○ 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 のインターフェースアドレスを、destination address には相手側 LAN のインター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）
※動作オプション 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。

○動作オプション 1
「空欄」

○動作オプション 2
「チェック」

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

○ backup SA
「空欄」

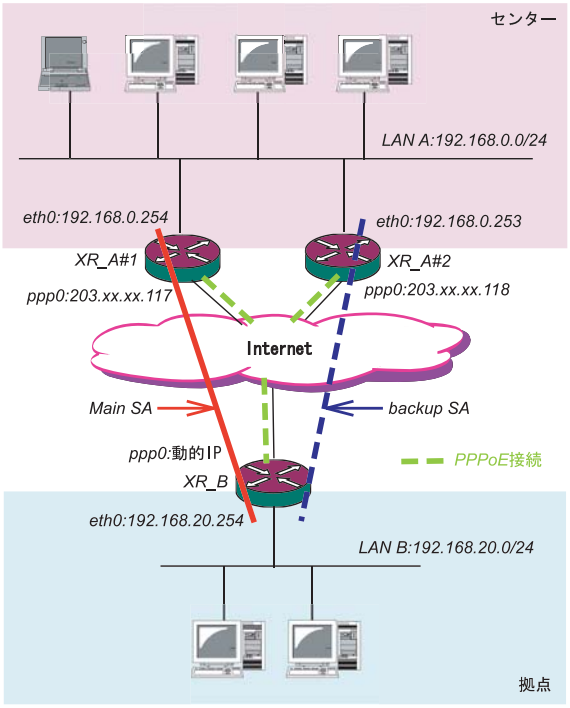
「IPsec Keep-Alive の設定」
PolicyNo.1 の行に設定します。

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、インター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.xx.xx.117
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

「203.xx.xx.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.xx.xx.118
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

「203.xx.xx.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。

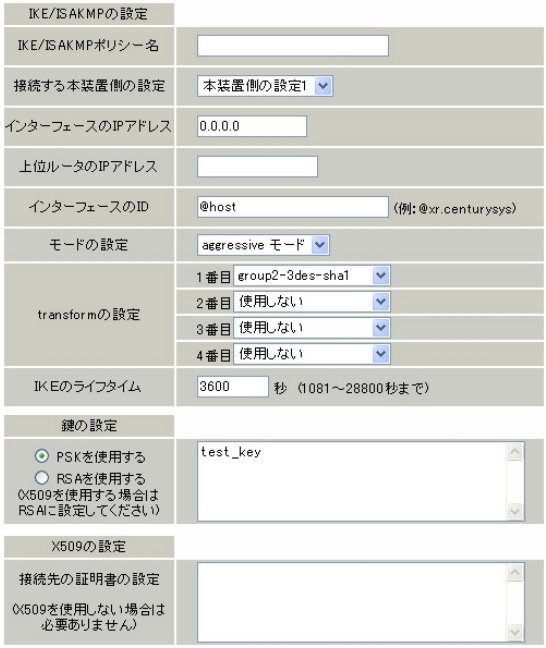
VIII. IPsec 設定例 2（センター／拠点間の 2 対 1 接続)

「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)

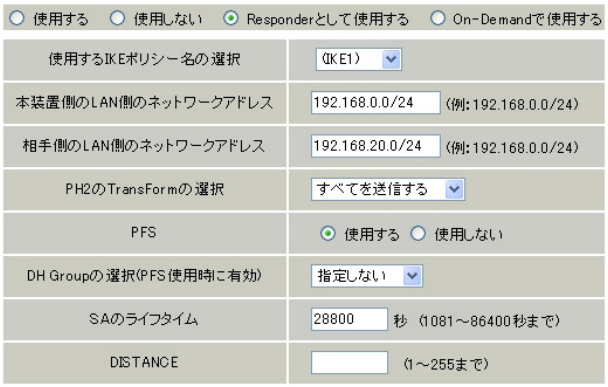
○鍵の設定
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

「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 インターフェースの“ 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 インターフェースの“ 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行います。
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)
※ 動作オプション 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。
○動作オプション 1 「空欄」
○動作オプション 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)
※ 動作オプション 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。
○動作オプション 1 「空欄」
○動作オプション 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。
但し、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	%ppp
上位ルータのIPアドレス	
インターフェースのID	@host （例: @xr.centurysys）

○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 ポリシーの設定を行います。

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	
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
上位ルータのIPアドレス	
インターフェースのID	（例: @xr.centurysys）
モードの設定	aggressive モード
transformの設定	1番目 group2-3des-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081～28800秒まで)
鍵の設定	
PSKを使用する / RSAを使用する (X509を使用する場合はRSAに設定してください)	test_key
X509の設定	
接続先の証明書の設定 (X509を使用しない場合は必要ありません)	

○ 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）

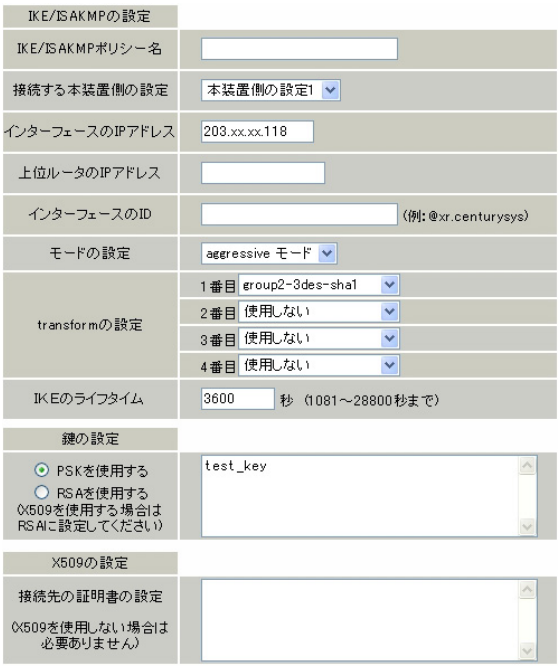
○鍵の設定
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

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 ポリシーの設定を行います。

「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」

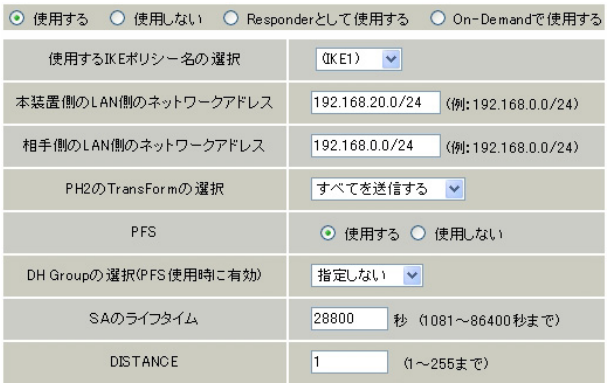
○ IKE のライフタイム 「3600」（任意の設定値）

○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 ポリシーの設定を行います。

「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）

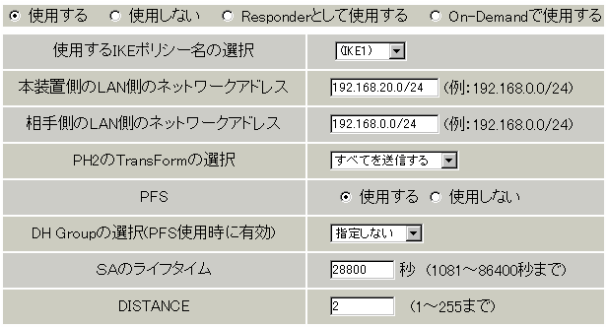
○ DISTANCE
「1」
※メイン側のディスタンス値は最小値(=1)を設定します。

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 ポリシーの設定を行います。

「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）
○動作オプション 1「空欄」
○動作オプション 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）
○動作オプション 1「空欄」
○動作オプション 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、「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 SA
 established

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.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; new-
est 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 鍵交換が正常に行えていません。
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)を行ってください。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。

○aggressiveモードで接続しようとしたら、今までつながっていたIPsecがつながらなくなってしまいました。

固定 IP - 動的 IP 間での main モード接続と aggressive モード接続を共存させることはできません。
このようなトラブルを避けるために、固定 IP - 動的 IP 間で IPsec 接続する場合は aggressive モードで接続するようにしてください。

○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 サービスも再起動する必要があります。

また、「IPsec Keep-Alive機能」を使うことで IPsec の再接続性を高めることができます。

○相手の装置には IPsecのログが出ているのに、こちらの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」をクリックしてください。ここに現在の IPsec の状況が表示されます。

第 14 章

UPnP 機能

第 14 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

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
- リモートアクセス
- ホワイトボード

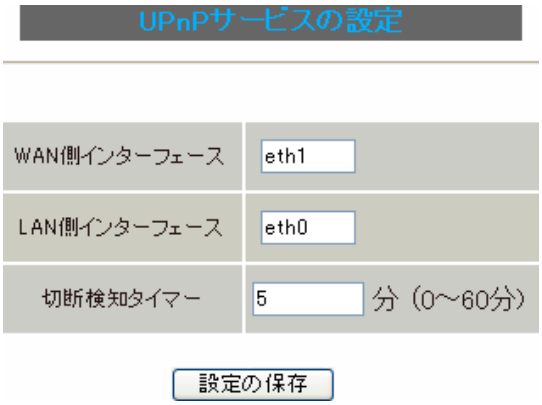
「ファイルまたは写真の送受信」および「アプリケーションの共有」については現在使用できません。

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ー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ーフェース名を指定します。

本装置のインター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。

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。

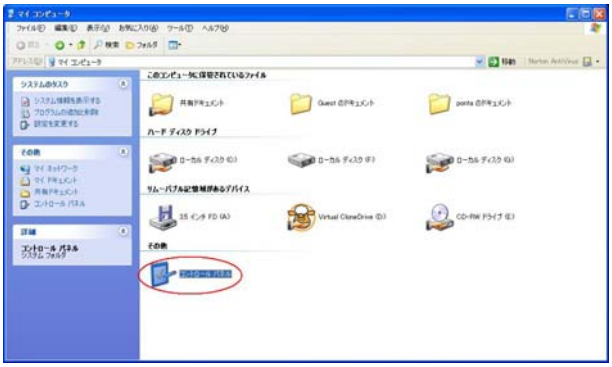
Ⅰ. UPnP 機能の設定

◆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。

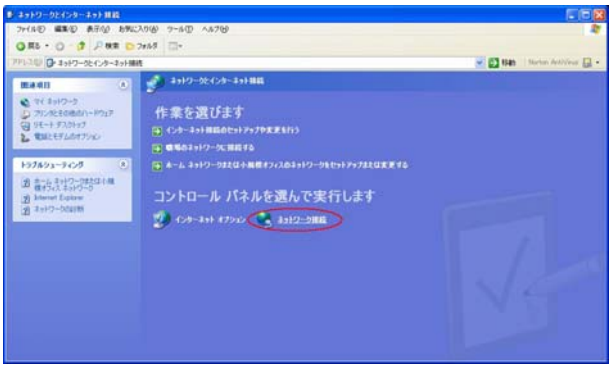
1 「スタート」→「マイコンピュータ」を開きます。

2 「コントロールパネル」を開きます。

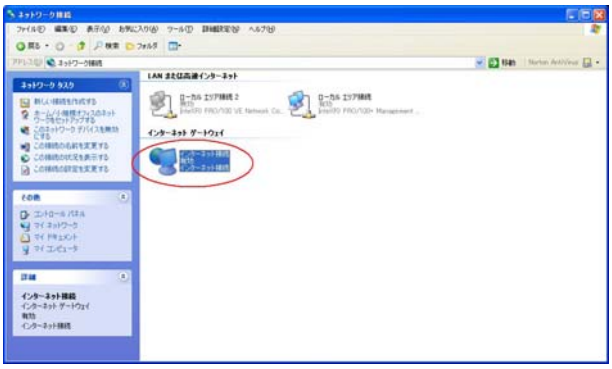


3 「ネットワークとインターネット接続」を開きます。

4 「ネットワーク接続」を開きます。



5 「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。

11. 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さま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	LOG	削除
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	LOG	削除
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 15 章

ダイナミックルーティング

第 15 章 ダイナミックルーティング

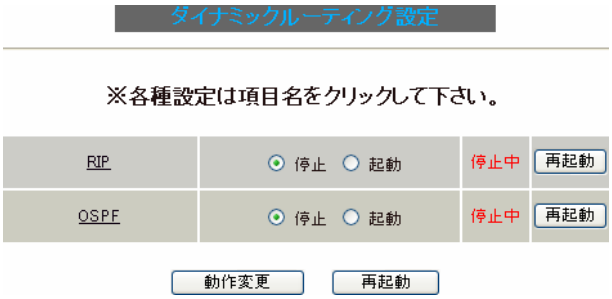
Ⅰ．ダイナミックルーティング機能

本装置のダイナミックルーティング機能は、RIP および OSPF をサポートしています。
さらに、XR-540 と XR-730 では BGP4 と DVMRP もサポートしています。

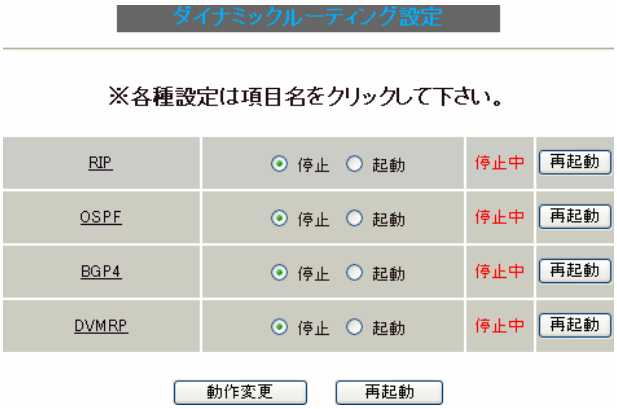
RIP 機能のみで運用することはもちろん、RIP で学習した経路情報を OSPF で配布することなどもできます。

◆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。



（画面は XR-510）



（画面は XR-540、XR-730）

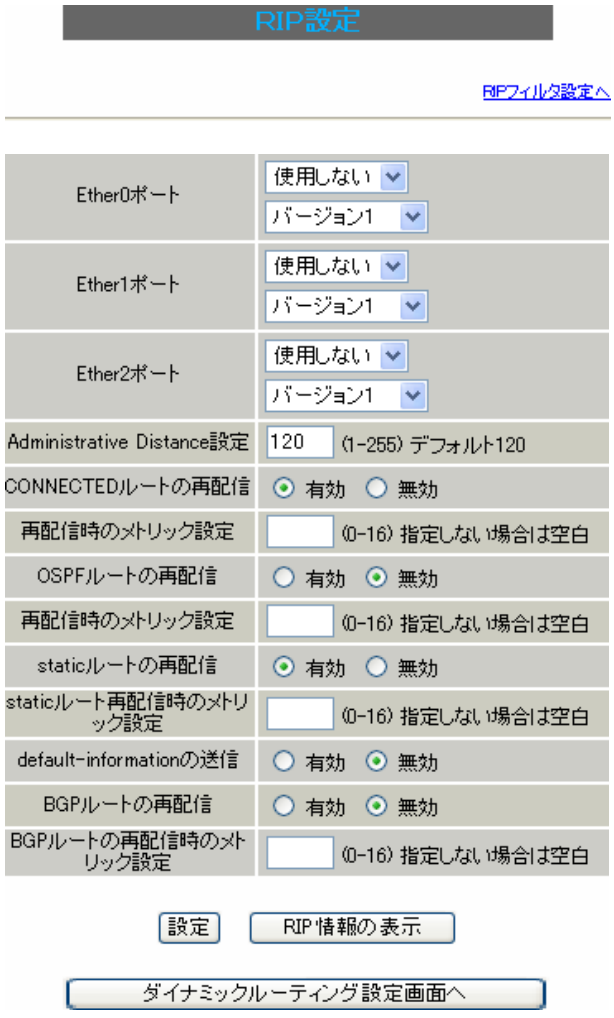
※ XR-540、XR-730 では「BGP4」「DVMRP」の設定も行えます。

2 「RIP」、「OSPF」（XR-540、XR-730 では「BGP4」、「DVMRP」）をクリックして、それぞれの機能の設定画面を開いて設定をおこないます。

11. 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設定」→「RIP」をクリックして、以下の画面から設定します。



（画面は XR-540）

○ Ether0、Ether1 ポート、Ether2 ポート、Ether3 ポート
本装置の各Ethernetポートで、RIPの使用/不使用、また、使用する場合の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(インター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。

○ static 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（※ **XR-510 にはありません**）
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
（※ **XR-510 にはありません**）
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。

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 フィルターの設定

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」→画面左「ダイナミックルーティング設定」→「RIP フィルタ設定」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選択します。

○方向
「in-coming」は本装置が 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」は本装置から 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「保存」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。

「削除」をクリックすると、設定が削除されます。
「編集」をクリックすると、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。

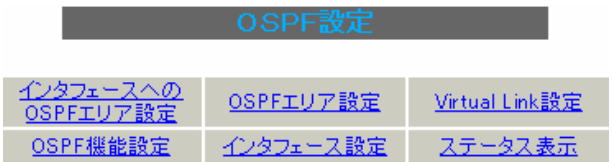
OSPF では各ルータがリンクステートを交換しあい、そのリンクステートをもとに、他のルータがどこに存在するか、どのように接続されているか、というデータベースを生成し、ネットワークトポロジを学習します。

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。**

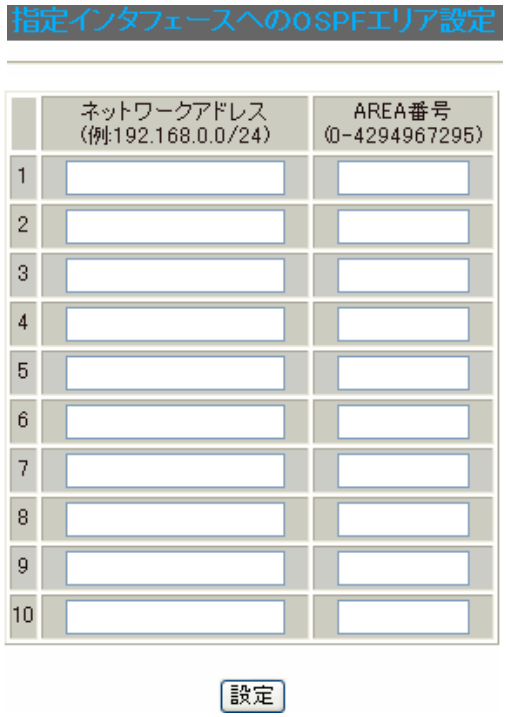
OSPF 設定は、Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング設定」→「OSPF」をクリックします。



◆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。

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。

設定画面上部の「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。

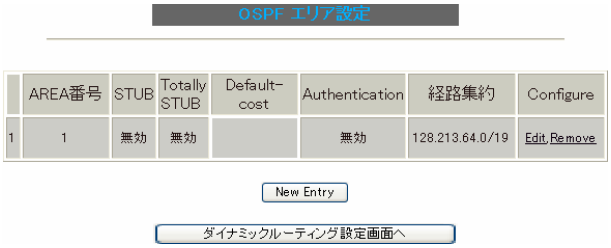
○認証設定
該当エリアでパスワード認証か MD5 認証をおこなうかどうかを選択します。デフォルト設定は「使用しない」です。

○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」項目の
○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

◆OSPF VirtualLink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VirtualLink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「VirtualLink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
VirtualLink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
VirtualLink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
VirtualLink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。

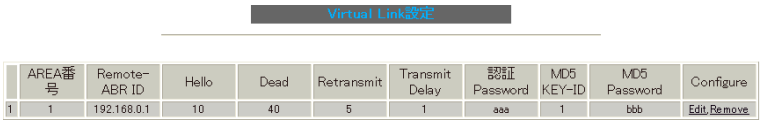
○MD5 パスワード設定(1)
エリア内でMD5認証を使用する際のMD5パスワードを設定します。

○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。

VirtualLink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。

設定後は「VirtualLink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」項目の
○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

◆OSPF 機能設定

OSPF の動作について設定します。設定画面上部の「OSPF 機能設定」をクリックして設定します。

○ 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。

○ 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。

III. OSPFの設定

○ 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。

「送信する」の場合、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。

「常に送信」の場合、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。

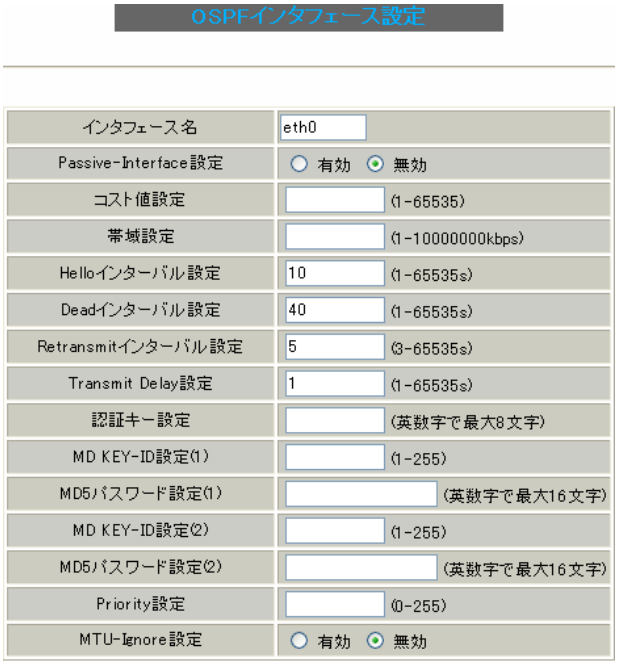
III. OSPF の設定

◆インタフェース設定

各インタフェースごとの OSPF 設定を行ないます。

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、本マニュアルの「付録 A」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。

○ 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。

○ 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。

III．OSPF の設定

○ 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 になる)。
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)

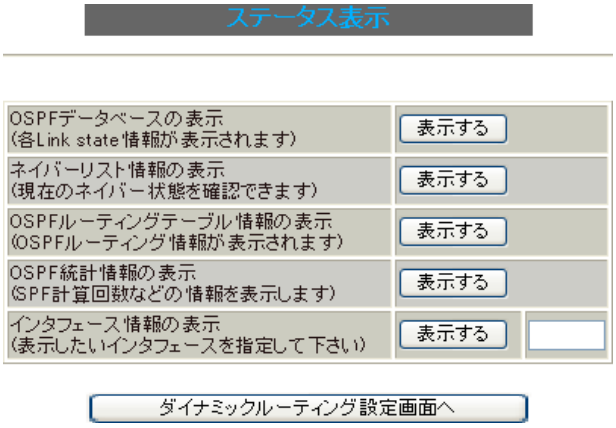
「Configure」項目の
○ Edit
クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○ 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（※ XR-510 にはありません）

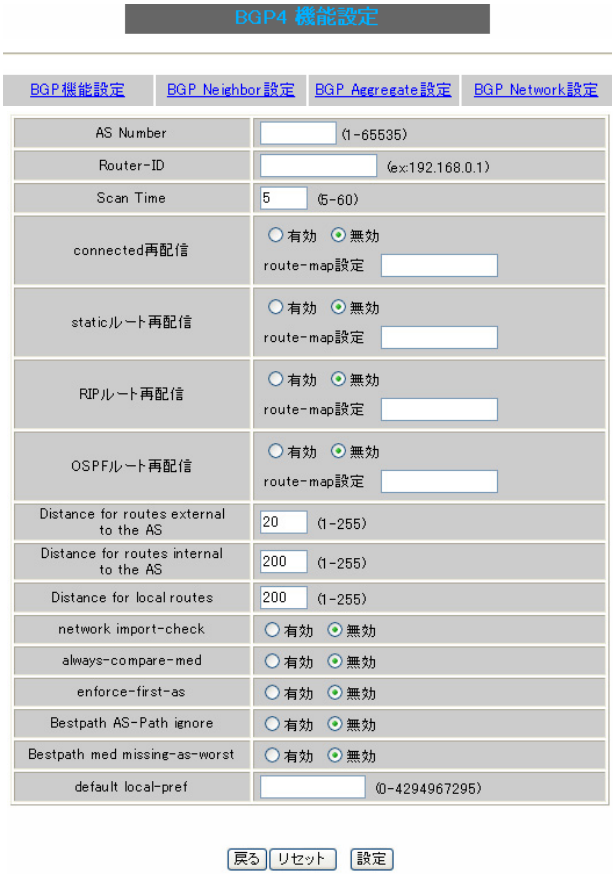
◆BGP4 機能設定

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。ここで各種設定を行います。

BGP 機能設定

Router-ID やルート情報再配信などの設定を行います。

BGP 機能設定をクリックして、以下の画面で設定を行います。



◯AS Number

AS 番号を設定します。入力可能な範囲は 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。指定可能な範囲は 5-60 秒です。

◯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。

IV．BGP4 の設定（※ XR-510 にはありません）

○ 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。入力可能な範囲は 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。入力可能な範囲は 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。入力可能な範囲は 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。入力可能な範囲は 0-4294967295 です。デフォルト値は「100」です。

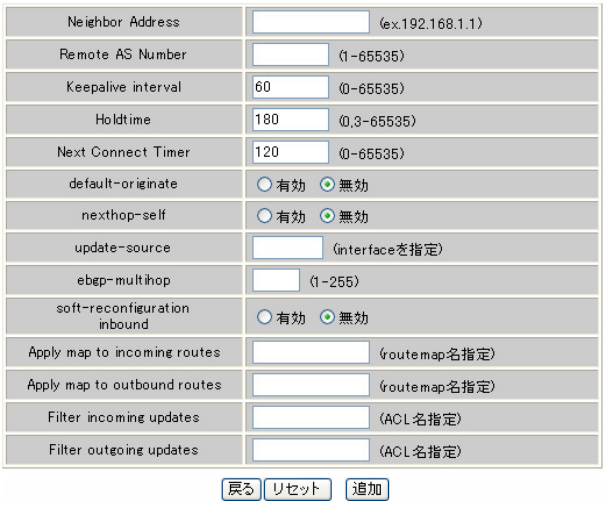
入力後「設定」ボタンをクリックし、設定を保存します。

IV. BGP4の設定（※ XR-510にはありません）

BGP4 Neighbor設定

Neighbor Addressの設定を行います。
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。

新規に設定を行う場合は、「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。入力可能な範囲は1-65535です。

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

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

○ Next Connect Timer
Next Connect Timerを設定します。入力可能な範囲は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。インターフェース名を指定してください。

本装置のインター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。

○ 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。入力可能な範囲は1-255です。

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

○ 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。

IV. BGP4 の設定（※ XR-510 にはありません）

○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。
設定内容の変更を行う場合は、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 の設定を行います。
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。

新規に設定を行う場合は、「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。

設定内容の変更を行う場合は、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 の設定を行います。
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。

新規に設定を行う場合は、「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。

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

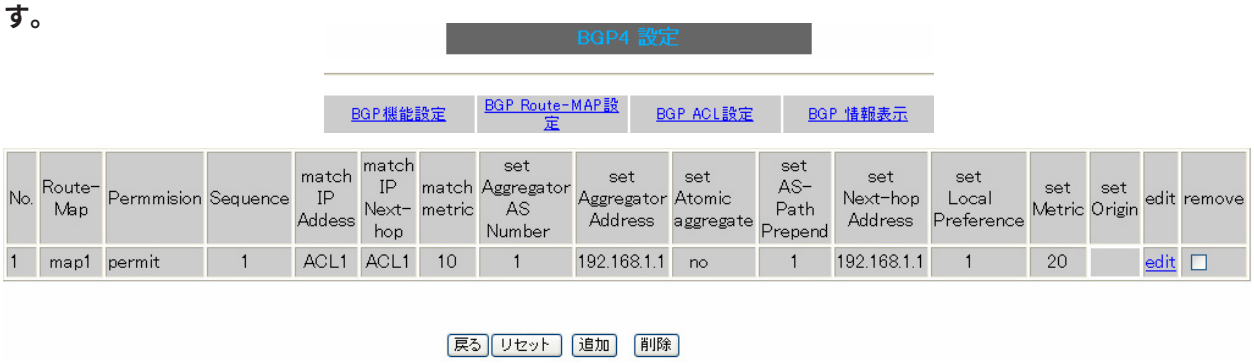
設定を削除する場合は、一覧表示画面「Remove」下の空欄にチェックを入れて「削除」ボタンをクリックしてください。

IV. BGP4 の設定（※ XR-510 にはありません）

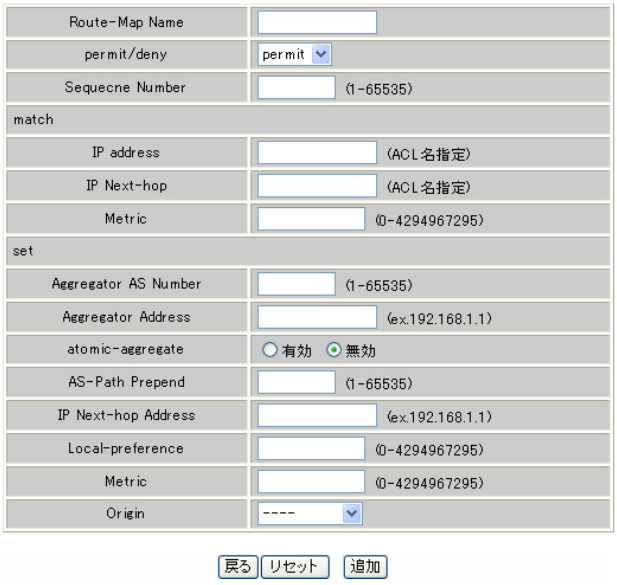
◆ BGP4 Route-MAP 設定

Route-MAP の設定を行います。

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。



新規に設定を行う場合は「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。入力可能な範囲は 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。入力可能な範囲は 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。入力可能な範囲は 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。入力可能な範囲は 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。入力可能な範囲は 0-4294967295 です。

・Metric
metric 属性を付加します。入力可能な範囲は 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。

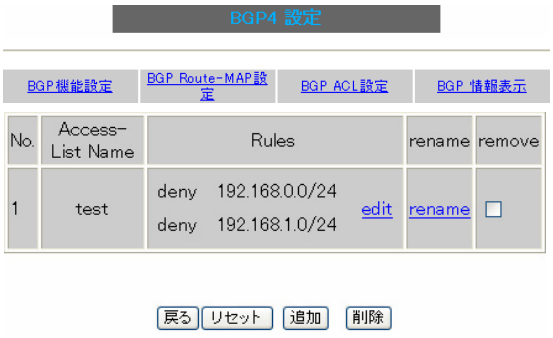
入力後「追加」ボタンをクリックし、設定を保存します。
設定内容の変更を行う場合は、Route-Map 一覧表示画面の「Edit」をクリックしてください。

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。

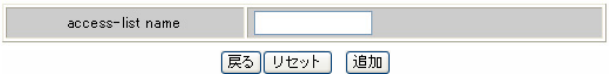
IV. BGP4 の設定（※ XR-510 にはありません）

◆BGP4 ACL 設定

BGP4 の ACL(ACCESS-LIST)設定を行います。
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。



新規に設定を行う場合は「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。
入力可能な範囲は 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。

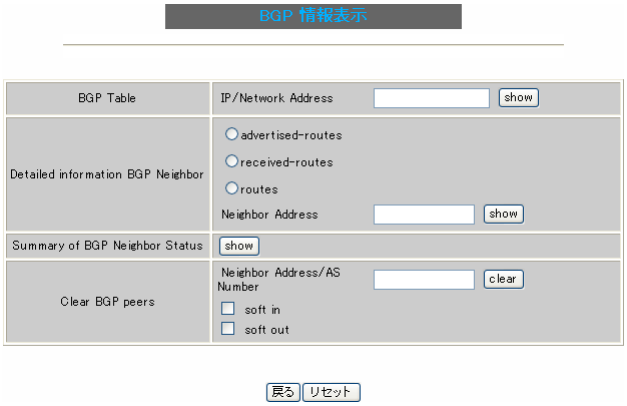
設定済みのルールを削除する場合は、ルールの一覧表示画面で「remove」下の空欄にチェックを入れ、「削除」ボタンをクリックしてください。

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（※ XR-510 にはありません）

◆BGP 情報表示

BGP4 の各種情報表示を行います。
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
設定の変更を行った場合などに 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。

V. DVMRP の設定（※ XR-510 にはありません）

◆DVMRP の設定

DVMRP はルータ間で使用される、マルチキャストデータグラムの経路を制御するプロトコルです。

DVMRP も他のダイナミックルーティングプロトコル同様にルータ間で経路情報を交換して、自動的にマルチキャストパケットの最適なルーティングを実現します。

ユニキャスト・ブロードキャストデータグラムについては DVMRP は経路制御しません。RIP や OSPF を利用してください。

DVMRP 設定

インタフェース設定 | 全体設定 | ステータス表示

◆インターフェース設定

XR-540 または XR-730 の設定画面上部の「インタフェース設定」をクリックして設定します。

インターフェイス設定

インターフェイス設定 Index

1- 17- 33- 49- 65- 81- 97- 113-
129- 145- 161- 177- 193- 209- 225- 241-

No.	Interface	Metric	Threshold	Disable	Del
1				☐	☐
2				☐	☐
3				☐	☐
4				☐	☐
5				☐	☐
6				☐	☐
7				☐	☐
8				☐	☐
9				☐	☐
10				☐	☐
11				☐	☐
12				☐	☐
13				☐	☐
14				☐	☐
15				☐	☐
16				☐	☐

設定の保存　入力のやり直し

（画面は表示例です）

○ Interface

DVMRP を実行する、本装置のインターフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録 A インターフェース名について」をご参照ください。

○ Metric

メトリックを指定します。経路選択時のコストとなり、Metric 値が大きいほどコストが高くなります。

○ Threshold

TTL の ” しきい値 ” を設定します。この値とデータグラム内の TTL 値とを比較して、そのデータグラムを転送または破棄します。
「Threshold ＞データグラムの TTL」のときはデータグラムを破棄、「Threshold ≦データグラムの TTL」のときはデータグラムをルーティングします。

○ Disable

チェックを入れて設定を保存すると、その設定は無効となります。

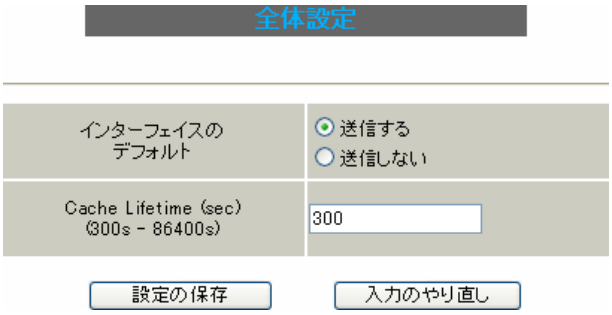
○ Del

チェックを入れて設定を保存すると、その設定は削除されます。

V．DVMRP の設定（※ XR-510 にはありません）

◆全体設定

設定画面上部の「全体設定」をクリックして設定します。



(画面は表示例です)

○インターフェイスのデフォルト
インターフェースのデフォルトの送信 / 非送信を設定します。

○ Cache Lifetime（sec）
マルチキャスト・ルーティングテーブルのキャッシュ保持時間を指定します。300 秒～ 86400 秒の間で指定します。

◆ステータス表示

設定画面上部の「ステータス表示」をクリックして表示します。

DVMRP ステータス表示

UP TIME: 0:00:34

Neighbors: 0

DVMRP Interface 表示

Virtual Interface Table

Vif	Name	Local-Address	M	Thr	Rate	Flags
0	eth0	192.168.0.254 subnet: 192.168.0/24	1	1	0	disabled
1	eth1	192.168.1.254 subnet: 192.168.1/24	1	1	0	querier leaf
2	eth2	192.168.2.254 subnet: 192.168.2/24	1	1	0	querier leaf

DVMRP Routing 表示

Multicast Routing Table (2 entries)

Origin-Subnet	From-Gateway	Metric	Tmr	Fl	In-Vif	Out-Vifs
192.168.2/24		1	40	..	2	1*
192.168.1/24		1	40	..	1	2*

DVMRP Cache 表示

Multicast Routing Cache Table (0 entries)

1	Origin	Mcast-group	CTmr	Age	Ptmr	Rx	IVif	Forwvifs
2	(prunesrc:vif[idx]/tmr)	prunebitmap						
3	Source	Lifetime	SavPkt	Pkts	Bytes	RPFf		

(画面は表示例です)

「ステータス表示」画面では、DVMRP が動作しているインターフェースの状態、マルチキャストルーティングテーブルの内容、ルーティングテーブルキャッシュの内容が表示されます。
※ DVMRP サービスが起動していない場合は表示画面はありません。

第 16 章

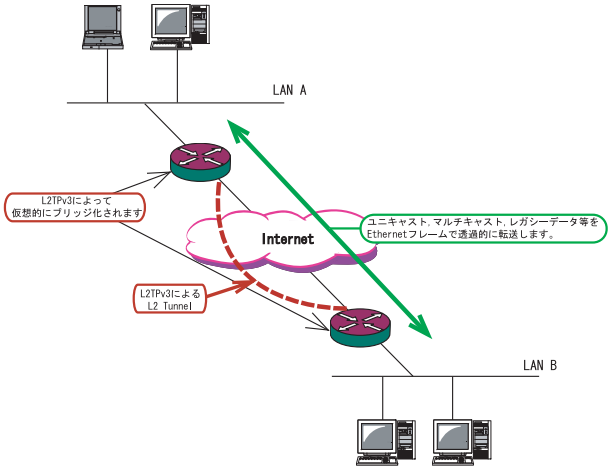
L2TPv3 機能

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出来ます。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。



- **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。

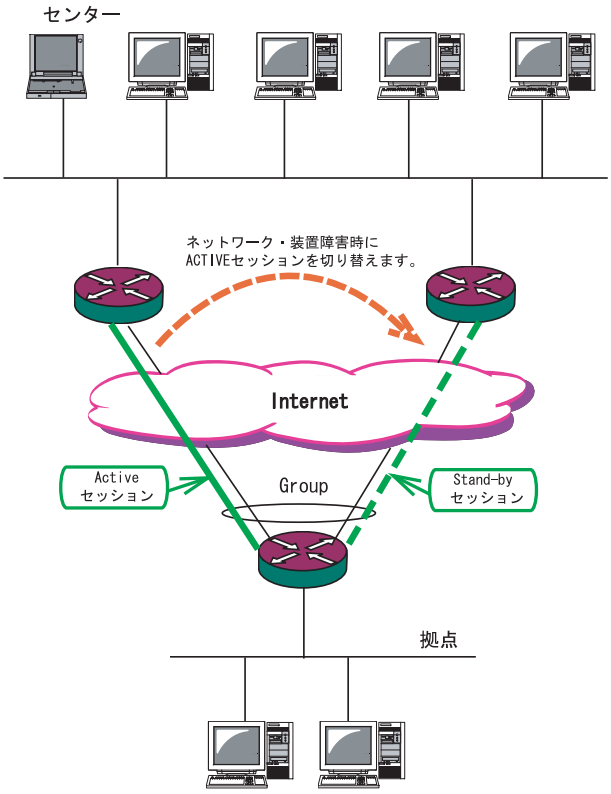
また Point to Multi-Point に対応しており、1 つの Xconnect Interface に対して複数の L2TP session を関連づけすることが可能です。

◆ 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。

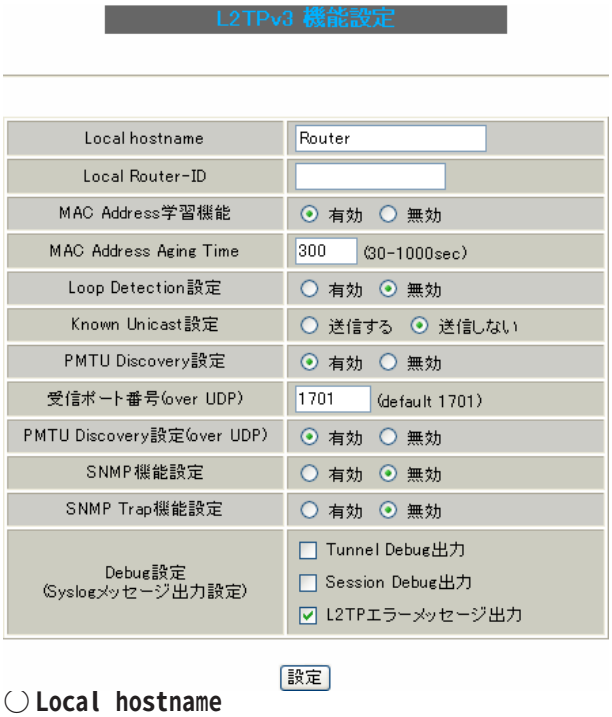
・L2TPv3 セッション二重化の例

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。



11. 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行います。



○ Local hostname
本装置のホスト名を設定します（使用可能な文字：半角英数字）。対向 LCCE(※ 1)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。

○ 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(ex.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(※ 2)
MAC アドレス学習機能を有効にするかを選択します。

○ 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：30 ～ 1000 秒）

○ Loop Detection 設定(※ 3)
LoopDetect 機能を有効にするかを選択します。

○ Known Unicast 設定(※ 4)
Known Unicast 送信機能を有効にするかを選択します。

○ PMTU 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。但し、カプセリングしたフレーム長が送信インターフェースの 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 20 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。

(※ 1)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。

(※ 2)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 インター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 インターフェース毎に 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。

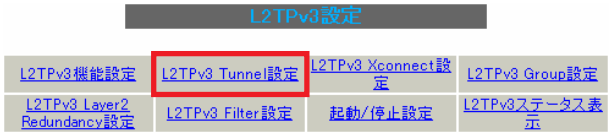
(※ 3) Loop Detection 機能
フレームの転送がループしてしまうことを防ぐ機能です。この機能が有効になっているときは、以下の２つの場合にフレームの転送を行いません。
- Xconnect インターフェースより受信したフレームの送信元 MAC アドレスが FDB に存在するとき
- L2TP セッションより受信したフレームの送信元 MAC アドレスが Local MAC テーブルに存在するとき

(※ 4) 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 フレームの転送を行いません。
- Xconnect インター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

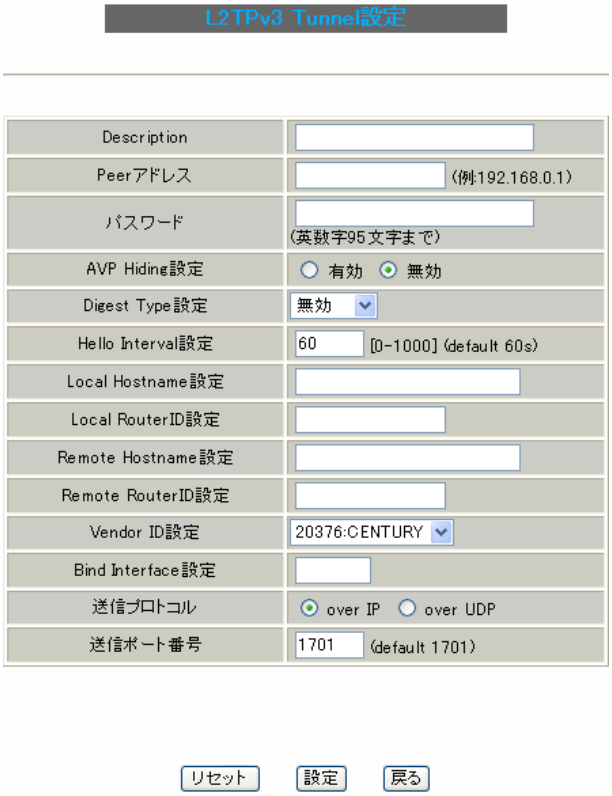
III. L2TPv3　Tunnel 設定

L2TPv3 のトンネル(制御コネクション)のための設定を行います。

「各種サービスの設定」->「L2TPv3」の「L2TPv3 Tunnel 設定」をクリックします。



新規に設定を行うときは「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。
但し、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。パスワードは設定しなくてもかまいません。

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。

○AVP Hiding(※)
AVP Hiding を有効にするかを選択します。

○Digest Type
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：0-1100 秒)。「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
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。

○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
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。

III. L2TPv3 Tunnel 設定

○ Vender ID 設定
対向 LCCE のベンダー ID を設定します。
「0」は RFC 3931 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。
「over UDP」を選択した場合、PPPoE to L2TP 機能を同時に動作させることはできません。

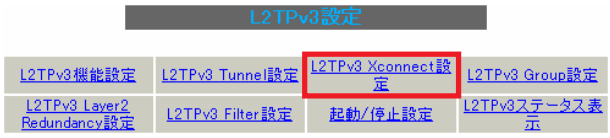
○送信ポート番号
L2TPv3 over UDP 使用時（上記「送信プロトコル」で「over UDP」を選択した場合）に、対向装置のポート番号を指定します。

(※)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。

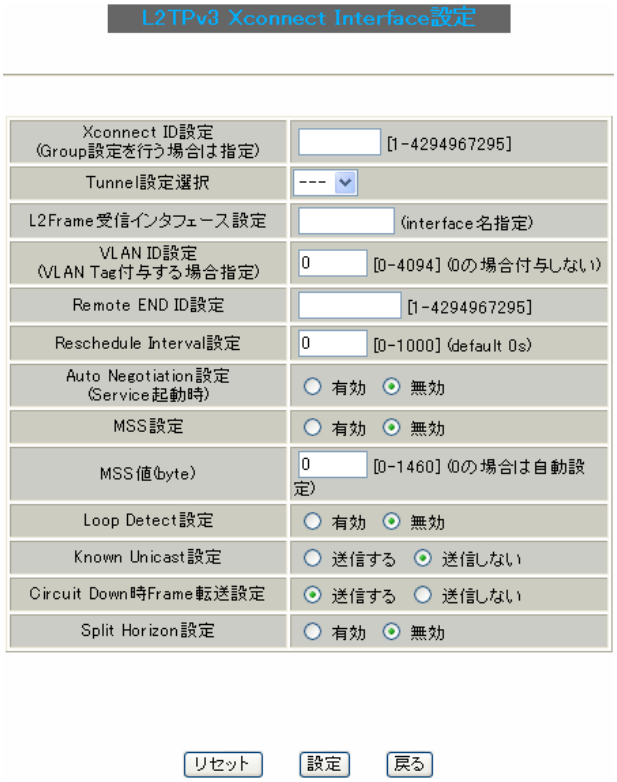
IV. L2TPv3　Xconnect(クロスコネクト)設定

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行います。

「各種サービスの設定」->「L2TPv3」の「L2TPv3 Xconnect 設定」をクリックします。



新規に設定を行うときは「New Entry」をクリックして、以下の画面で設定します。



○ Xconnect ID 設定
「L2TPv3 Group 設定」で使用する ID を任意で設定します。

○ Tunnel 設定
「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、本装置のイーサネットポートと VLAN インタフェースのみです。

Point to Multi-point 接続を行う場合は、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。

但し、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 設定を行うときの例：
「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
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
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。但し、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 re-schedule(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設定します。0 ～ 1000(秒)で設定します。

また、「0」を設定したときは自動再接続は行われません。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。

IV. L2TPv3 Xconnect(クロスコネクト)設定

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。

○ Auto Negotiation 設定
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）。
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。

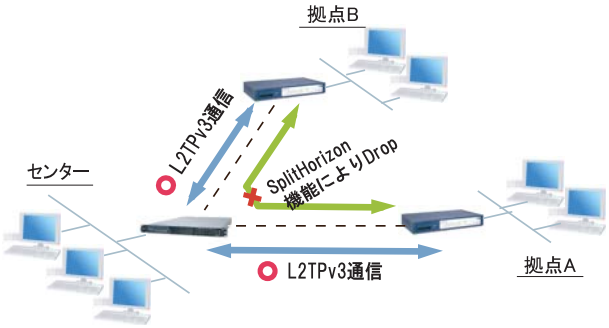
○ Known Unicast 設定
この Xconnect において、Known Unicast 送信機能を有効にするかを選択します。

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。

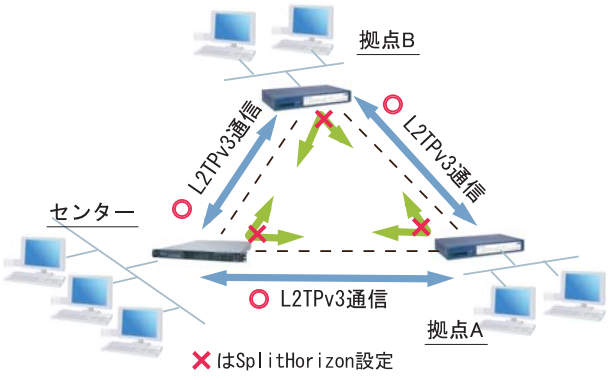
○ Split Horizon 設定
Point-to-Multi-Point 機能によって、センターと２拠点間を接続しているような構成において、センターと拠点間の L2TPv3 通信は行うが、拠点同士間の通信は必要ない場合に、センター側でこの機能を有効にします。
センター側では、Split Horizon 機能が有効の場合、一方の拠点から受信したフレームをもう一方のセッションへは転送せず、Local Interface に対してのみ転送します。

※ 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

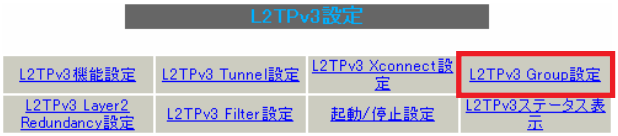


V. L2TPv3 Group 設定

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行います。

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。

「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行うときは、「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：1～4095)。他の Group と重複しない値を設定してください。

○ Primary Xconnect 設定
Primary 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。

○ Secondary Xconnect 設定
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行わず、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。

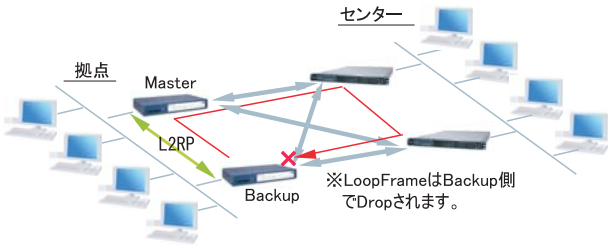
1vs1 の二重化構成の場合、対向 LCCE で Link Down が発生した際に、Primary から Secondary へ Active セッションを切り替えたとしても、通信できない状態は変わりません。よってこの構成においては、不要なセッションの切り替えを抑止するために本機能を有効に設定することを推奨します。

VI．Layer2 Redundancy 設定

Layer2 Redundancy Protocol 機能（以下、L2TP 機能）とは、装置の冗長化を行い、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



「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」をクリックすると以下の設定画面が開きます。

(画面は XR-540)

○ L2RP ID
L2RP の ID です。対になる LCCE の L2RP と同じ値を設定します。

○ 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。

○ 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（指定可能な範囲：1～255）。

○ Advertisement Interval 設定
Advertise Frame を送信する間隔を設定します（指定可能な範囲：1～60 秒）。

※ 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

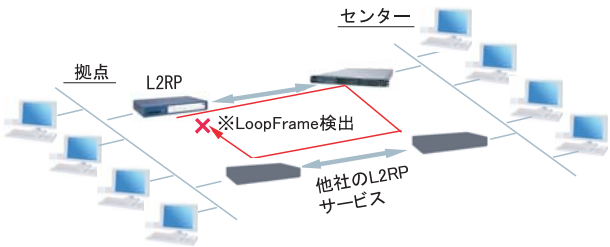
○ Preempt 設定
Priority 値が低いものが Master で高いものが Backup となることを許可するかどうかの設定です。

○ Xconnect インターフェース設定
Xconnect インター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 の転送を行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。

○ FDB Reset 設定（※ **XR-540 のみ**）
XR が HUB ポートを持っている場合に、自身の HUB ポートの MAC テーブルをフラッシュします。

○ 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。

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行ってください。

- 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」

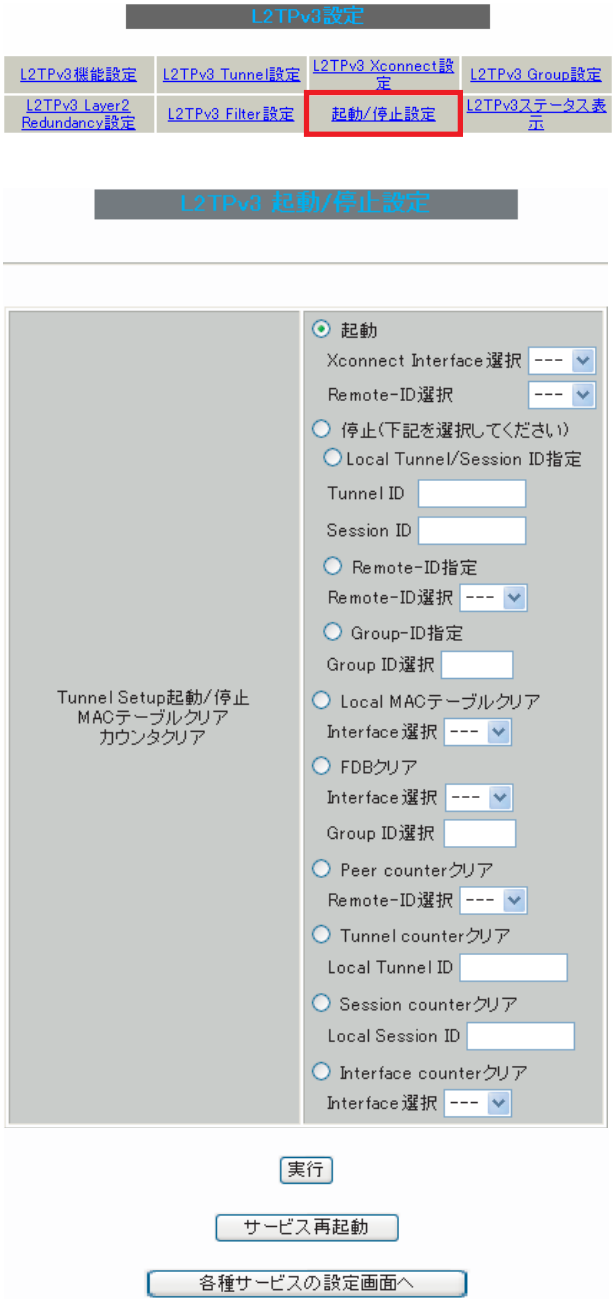
VII. L2TPv3 Filter 設定

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行います。

「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

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。

また、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。

○停止

トンネル / セッションの停止を行います。停止したい方法を以下から選択してください。

・Tunnel/SessionID 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 TunnelID/SessionID を指定してください。

・RemoteID 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。

・GroupID 指定

グループ内のセッションを全て停止したい場合は、停止するグループ 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。

VIII. 起動 / 停止設定

○ 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 Tunnel ID を指定してください。

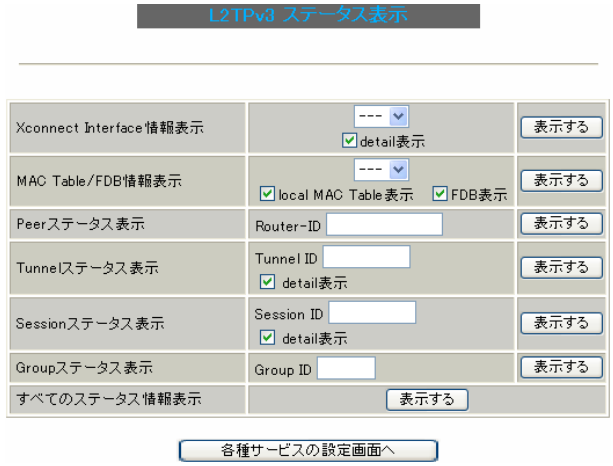
○ Session counter クリア
「L2TPv3 ステータス表示」で表示される「Session ステータス」のカウンタをクリアします。クリアしたいセッション ID を指定してください。

○ 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インタフェース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。

IX. L2TPv3　ステータス表示

L2TPv3 の各種ステータスを表示します。

「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 インタフェース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インタフェースを選択してください。
「detail 表示」に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。

なお、ローカル側で保持する MAC テーブルを表示したい場合は、「local MAC Table 表示」にチェックを入れ、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、「FDB 表示」にチェックを入れてください。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。表示したいセッション 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」に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。表示したいセッション 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」に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。
表示したいグループ ID を選択してください。選択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。

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。

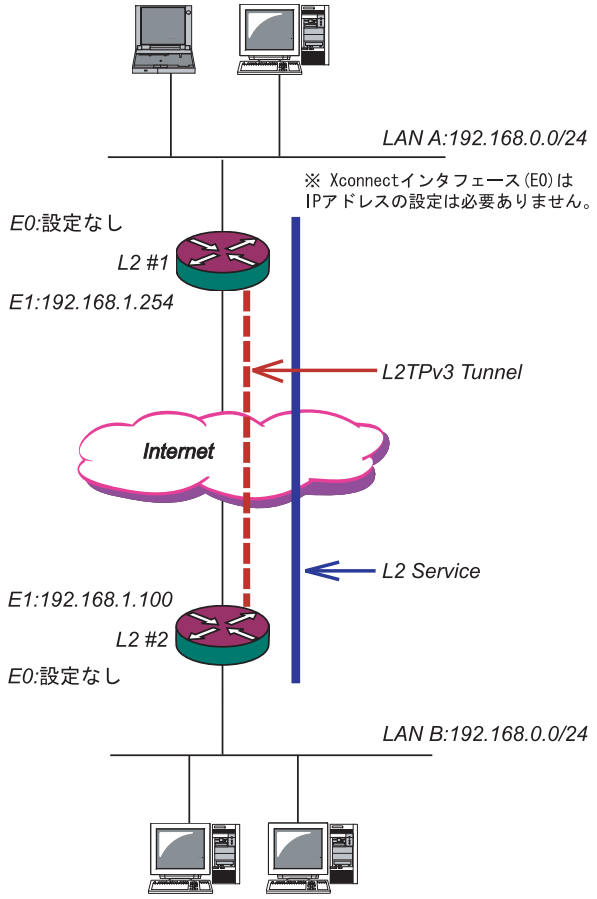
ICCN：Incoming-Call-Connected
ICRP に対する応答メッセージ。このメッセージにより、L2TP セッションが確立した状態になったことを示します。

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。

DNSキャッシュ	○停止 ○起動	停止中	動作変更
DHCP(Relay)サーバ	○停止 ○起動	停止中	動作変更
IPsecサーバ	○停止 ○起動	停止中	動作変更
UPnPサービス	○停止 ○起動	停止中	動作変更
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい	停止中	
L2TPv3	○停止 ○起動	動作中	動作変更
SYSLOGサービス	○停止 ○起動	動作中	動作変更
攻撃検出サービス	○停止 ○起動	停止中	動作変更
SNMPサービス	○停止 ○起動	停止中	動作変更
NTPサービス	○停止 ○起動	停止中	動作変更
VRRPサービス	○停止 ○起動	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい	停止中	

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。

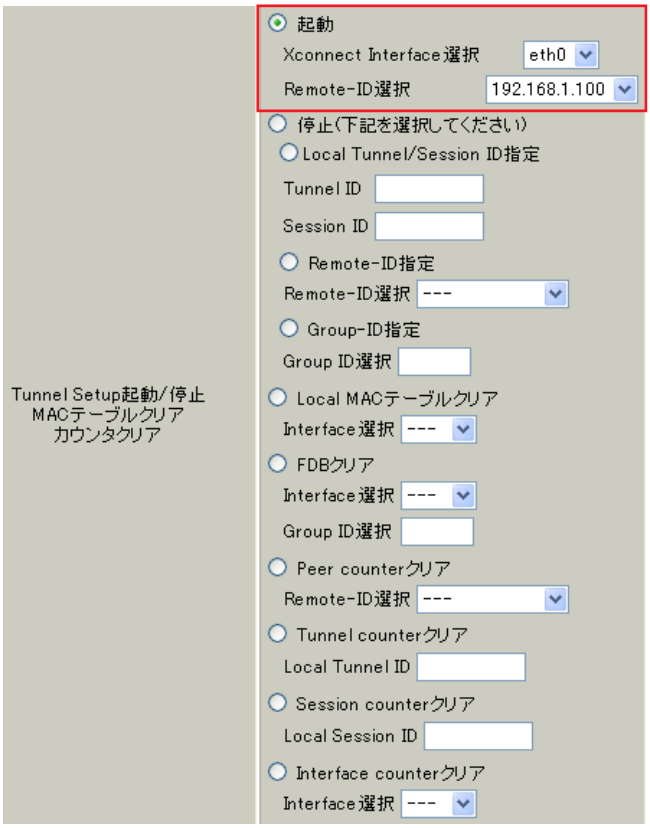
Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.254
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	◉ 有効 ○ 無効
MSS設定	◉ 有効 ○ 無効
MSS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。

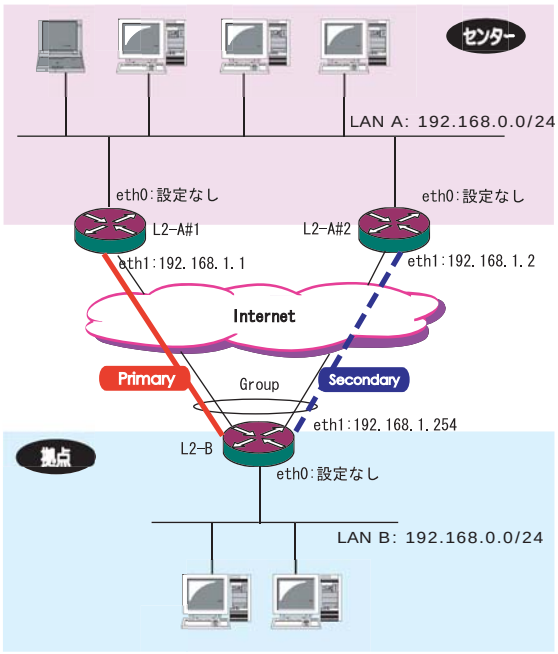


L2TPv3 接続を停止するときは、「起動 / 停止設定」画面で停止するか、各種サービス設定画面で L2TPv3 を停止します。

XII．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行います。

構成図（例）



XII．L2TPv3　設定例 2（L2TP トンネル二重化）

L2-A#1/L2-A#1(センター側)ルータの設定

L2-A#1（Primary）ルータの 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）ルータの 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

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

L2-A#1（Primary）ルータの 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	192.168.1.254 (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#2（Secondary）ルータの 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)

L2-A#1（Primary）ルータの Xconnect Interface 設定をおこないます。

・「Xconnect ID 設定」は Group 設定を行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 受信インターフェース」は LAN 側のインターフェースを指定します。**LAN 側インターフェースには 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

XII. L2TPv3　設定例 2（L2TP トンネル二重化）

L2-A#2（Secondary）ルータの 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

L2TPv3 Group 設定について

- Primary、Secondary ルータともに、L2TP セッションの Group 化は行わないので、設定の必要はありません。

XII．L2TPv3　設定例 2（L2TP トンネル二重化）

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

Primary セッション側の 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 を行います。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)

XII．L2TPv3　設定例 2（L2TP トンネル二重化）

Secondary セッション側の 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)

Primary セッション側の 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 受信インターフェース」は LAN 側のインターフェースを指定します。**LAN 側インターフェースには 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。但し、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行います。

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

XII. L2TPv3　設定例 2（L2TP トンネル二重化）

Secondary セッション側の 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

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

XII. L2TPv3　設定例 2（L2TP トンネル二重化）

L2TPv3TunnelSetup の起動

設定後が終わりましたら L2TPv3 機能の起動 / 停止設定を行います。

「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 17 章

L2TPv3 フィルタ機能

第 17 章 L2TPv3 フィルタ機能

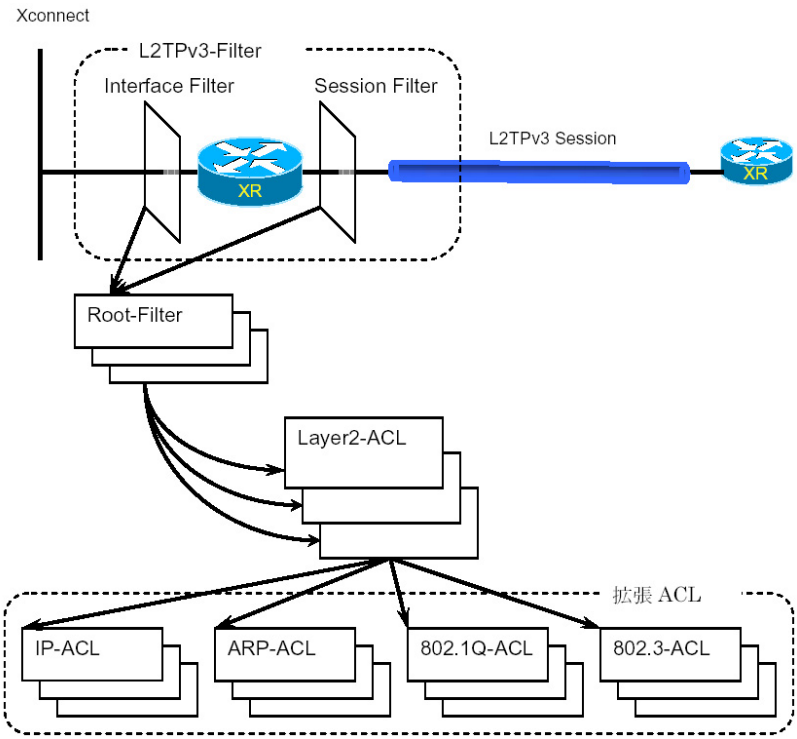
Ⅰ．L2TPv3 フィルタ 機能概要

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行ないます。
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 17 章 L2TPv3 フィルタ機能

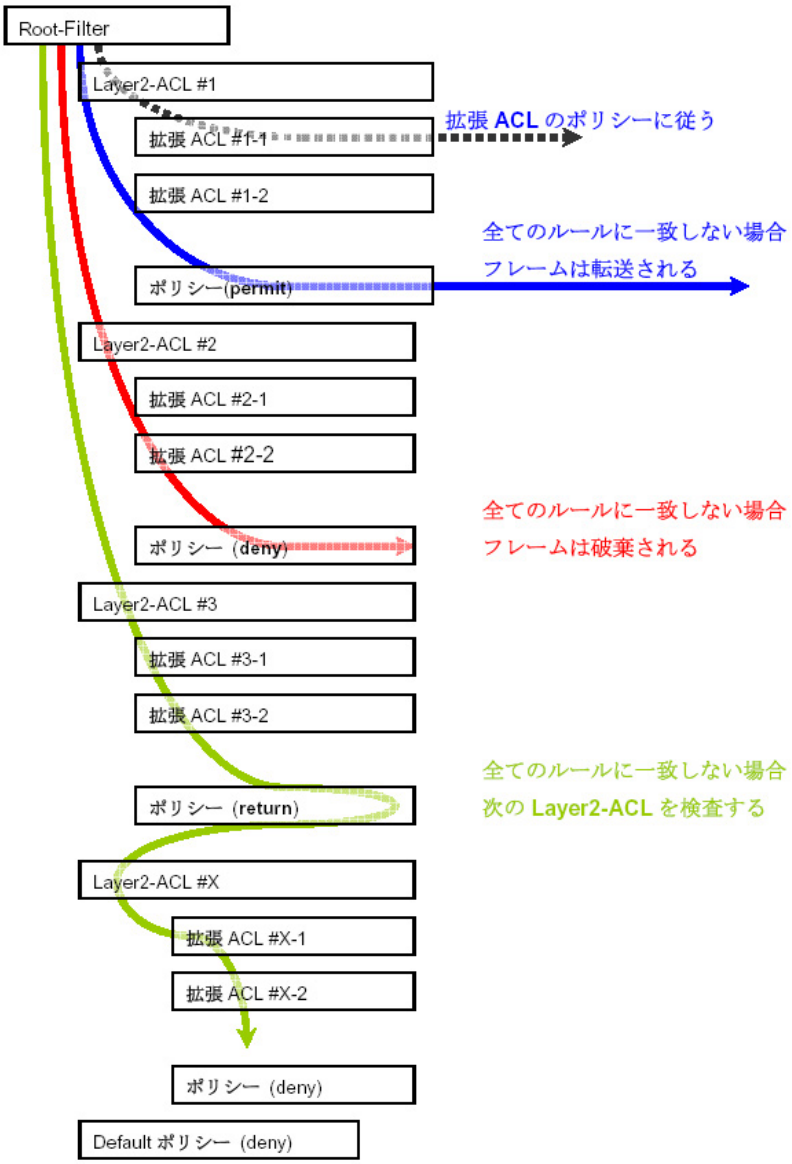
Ⅰ．L2TPv3 フィルタ 機能概要

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行います。

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 17 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行い、最初に条件に一致したもの（1st match）に対して以下の評価を行います。

・拡張 ACL がない場合
　該当 Layer2 ACL のポリシーに従い、deny/permit/return を行います。
・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 にて検索を行い、以下の評価を行います。
　1) 拡張 ACL に一致する場合、拡張 ACL の policy に従い deny/permit を行います。
　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 を行います。

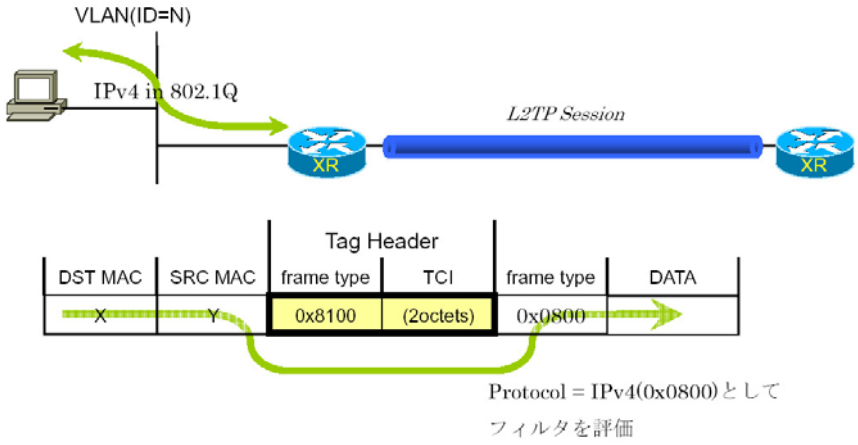
フレームが配下に設定された全ての Layer2 ACL に一致しなかった場合は、Default ポリシーによりフレームを deny または permit します。

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行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、フレームの転送は行われませんのでご注意ください。

802.1Q タグヘッダ

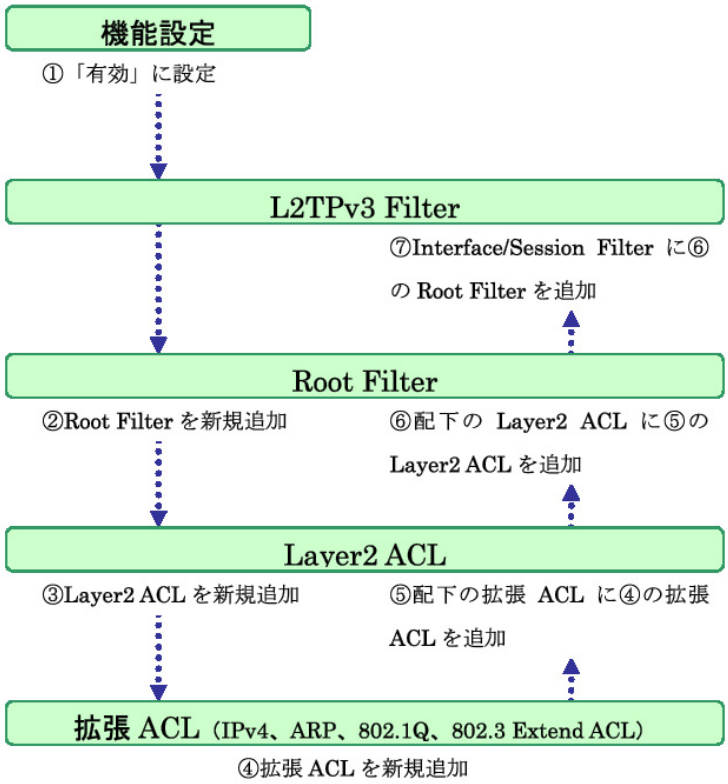
Xconnect Interface が VLAN(802.1Q)であるフレームをフィルタリングする場合、タグヘッダについては、フィルタの評価対象から除外し、タグヘッダに続くフィールドから再開します(下図参照)。



11. 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

「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行います。

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。

○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。

*** 設定で可能な文字について**

Root Filter・ACL 名で使用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。

IV. L2TPv3 Filter 設定

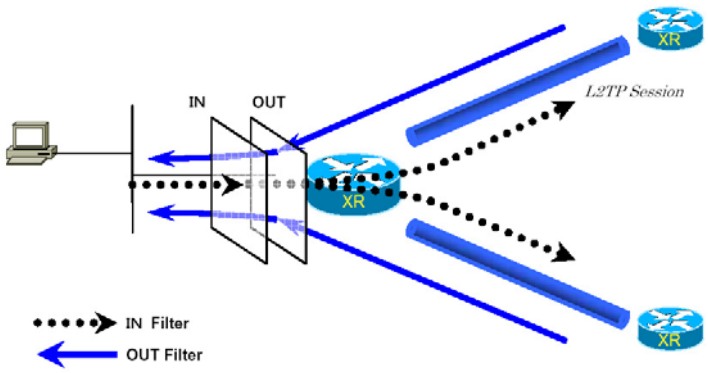
L2TPv3 Filter 設定画面の「L2TPv3 Filter 設定」をクリックします。
現在設定されている Interface Filter と Session Filter が一覧表示されます。

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行います。
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

Interface Filter を編集する

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 に設定したインター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。

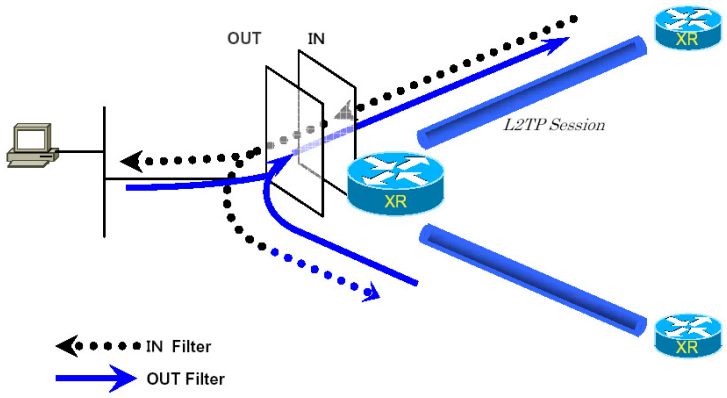
IV. L2TPv3 Filter 設定

Session Filter

Session Filter

Index	Peer ID	Remote END 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行いますので、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

Session Filter を編集する

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

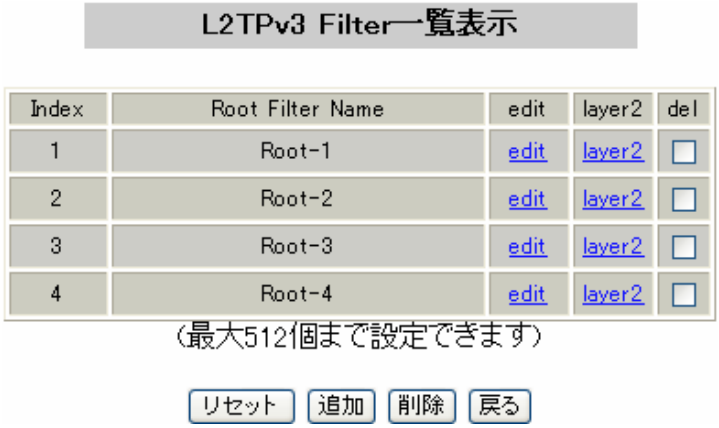
○ PeerID : RemoteEndID
対向側の Xconnect Interface ID と Remote End ID が表示されます。

○ 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

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 を追加する

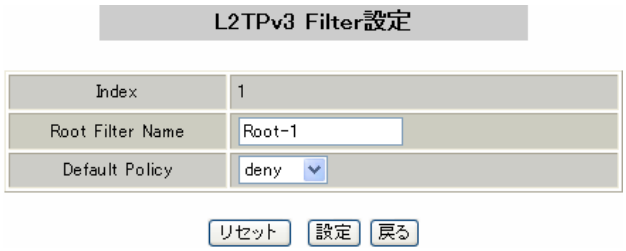
画面下の「追加」ボタンをクリックします。

○ Root Filter Name
Root Filter を識別するための名前を入力します(*)。

○ 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 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。

Root Filter 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。

V. Root Filter 設定

配下に Layer2 ACL を設定する

一覧表示内の「layer2」をクリックします。
現在設定されている配下の Layer2 ACL が一覧表示されます。

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 を追加する

画面下の「追加」ボタンをクリックします。

Seq.No.	
Layer2 ACL Name	----

○ 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 を編集する

一覧表示内の「edit」をクリックします。

Seq.No.	1
Layer2 ACL Name	L2ACL-1

追加画面と同様に設定してください。

配下の Layer2 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。

VI. 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 を追加する

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(*)。

○ 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。
指定可能な範囲は 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 を編集する

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 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。

VI．Layer2 ACL 設定

配下に拡張 ACL を設定する

一覧表示内の「extend」をクリックします。
現在設定されている配下の拡張 ACL が一覧表示されます。

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 を追加する

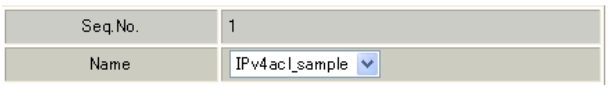
画面下の「追加」ボタンをクリックします。

○ 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 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。

配下の拡張 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。

VII. 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 を追加する

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(*)。

○ 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。
指定可能な範囲は 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。
指定可能な範囲は 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。

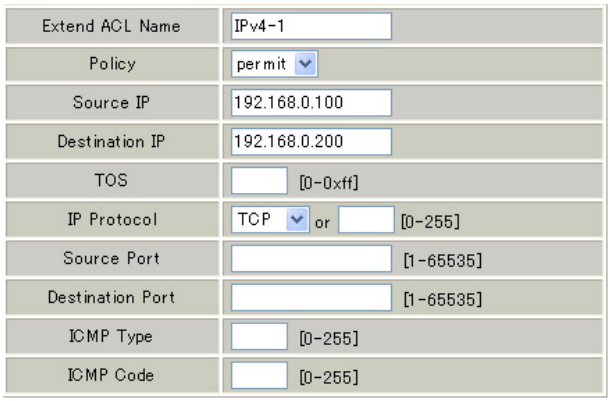
○ ICMP Type
ICMP Type の指定が可能です。IP Protocol に ICMP を指定した場合のみ設定可能です。
指定可能な範囲は 0-255 です。

○ 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。
指定可能な範囲は 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

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 を追加する

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(*)。

○ 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。
指定可能な範囲は 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 を編集する

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 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。

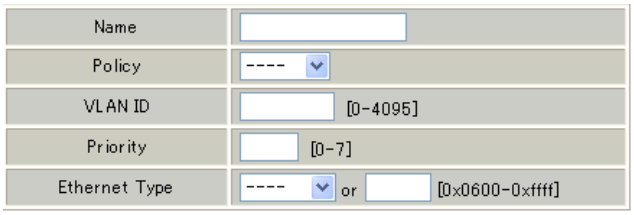
IX. 802.1Q Extend ACL 設定

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 を追加する

画面下の「追加」ボタンをクリックします。



◯ Name
拡張 ACL を識別するための名前を入力します(*)。

◯ Policy
deny（破棄）/permit（許可）のいずれかを選択します。

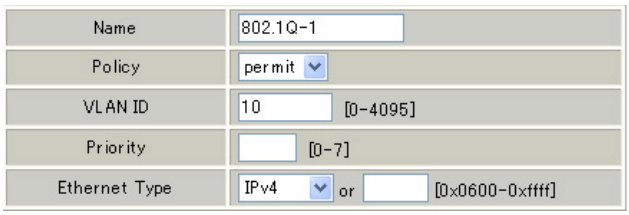
◯ VLAN ID
VLAN ID を指定します。
範囲設定が可能です。指定可能な範囲は 0-4095 です。
＜フォーマット＞
xxx（VLAN ID：xx）
xxx:yyy（xxx 以上、yyy 以下の VLAN ID）

◯ Priority
IEEE 802.1P で規定されている Priority Field を判定します。
指定可能な範囲は 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。
指定可能な範囲は 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 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。

802.1Q 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。

IX. 802.1Q Extend ACL 設定

配下に拡張 ACL を設定する

一覧表示内の「extend」をクリックします。
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 を追加する

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 を編集する

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 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。

X. 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 を追加する

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(*)。

◯ 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。
指定可能な範囲は 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。
指定可能な範囲は 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 を編集する

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]

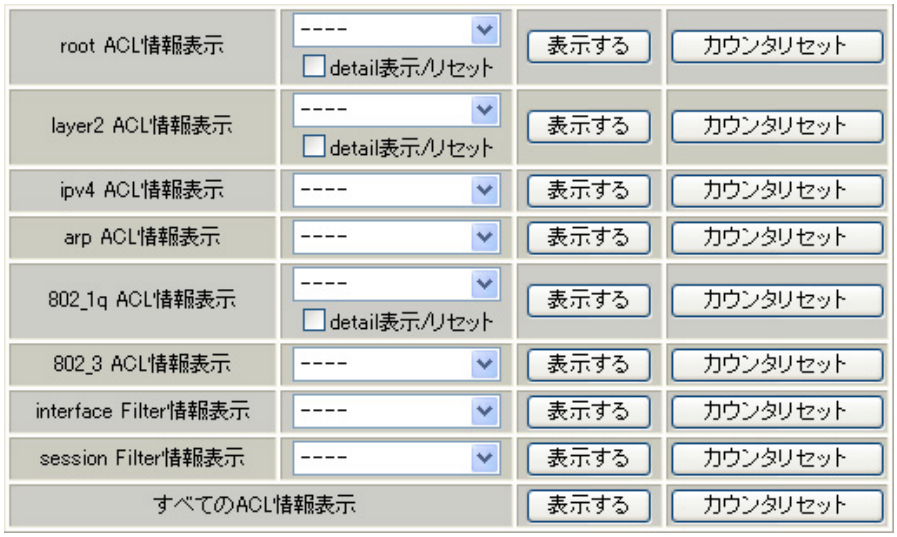
追加画面と同様に設定してください。

802.3 Extend ACL 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。

XI．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）※

○ 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

XI. 情報表示

○ 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

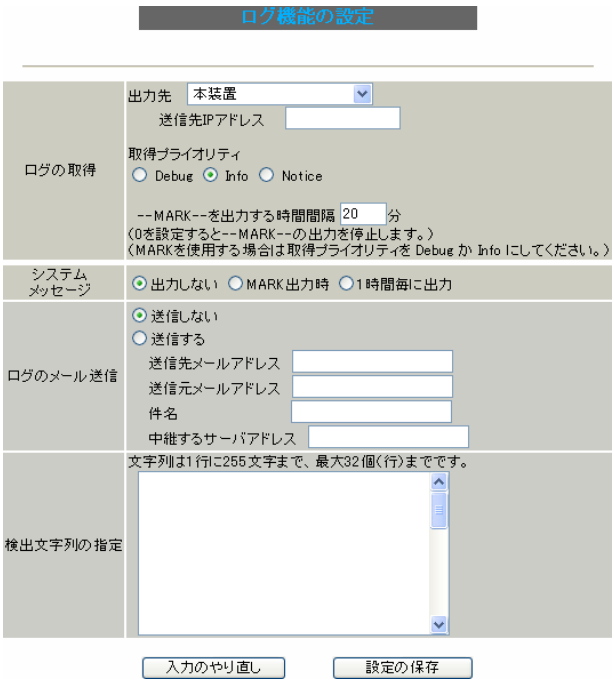
第 18 章

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できます。

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。



<SYSLOG 機能設定>

○「ログの取得」項目で設定します。

「取得する」
本装置で syslog を取得する場合に選択します。

「他の syslog サーバに送信する」
syslog を他のサーバに送信するときに選択します。このとき、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。「MARK 出力時」を選択した場合は "--MARK--" の出力と同時に出力されます。

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 ： 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 ： 空きメモリ量(byte)です。
- session:XX/YY
  XR 内部で保持している NAT/IP マスカレードのセッション情報数です。
  XX: 現在 Establish している TCP セッションの数
  YY: XR が現在キャッシュしている全てのセッション数

SYSLOG 機能の設定

<ログメール機能設定>
○ログの内容を電子メールで送信したいときの設定です。「ログメールの送信」項目で設定します。

ログメール機能を使うときは「送信する」を選択し、「ログメッセージ送信先のメールアドレス」を指定します。さらに、
　「ログメッセージ送信元のメールアドレス」
　「件名」
　「中継するサーバアドレス」
を任意で指定できます。「件名」は半角英数字のみ使用できます。

何も指定しないときは
　送信元アドレス「root@localhost」
　件名は無し
で送信されます。

「中継するメールサーバのアドレス」は、お知らせメールを中継する任意のメールサーバを設定します。IP アドレス、ドメイン名のどちらでも設定できます。ただしドメイン名で指定するときは、下記の記述で設定してください。

<入力形式>　**< ドメイン名 >**
<入力例>　　mail.xxxxxx.co.jp

○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、1 行につき 256 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、「ログメール機能」のみ有効です。**

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。

ファシリティと監視レベルについて
XR 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**

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 4 つです。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。

第 19 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

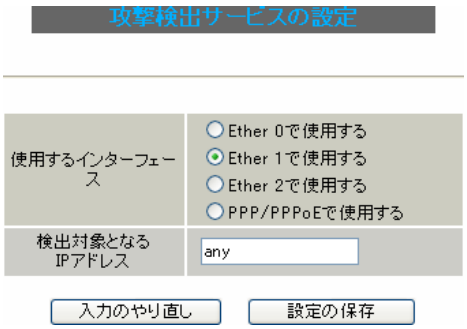
攻撃検出機能とは、外部から LAN への侵入や本装置を踏み台にした他のホスト・サーバ等への攻撃を仕掛けられた時などに、そのログを記録しておくことができる機能です。検出方法には、統計的な面から異常な状態を検出する方法やパターンマッチング方法などがあります。本装置ではあらかじめ検出ルールを定めていますので、パターンマッチングによって不正アクセスを検出します。ホスト単位の他、ネットワーク単位で監視対象を設定できます。

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。



（画面は XR-540）

○使用するインターフェース
DoS の検出をおこなうインター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
攻撃を検出したいホストの IP アドレスか、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***
（”/マスクビット値”を付ける）

「any」と入力すると、すべてのホスト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 20 章

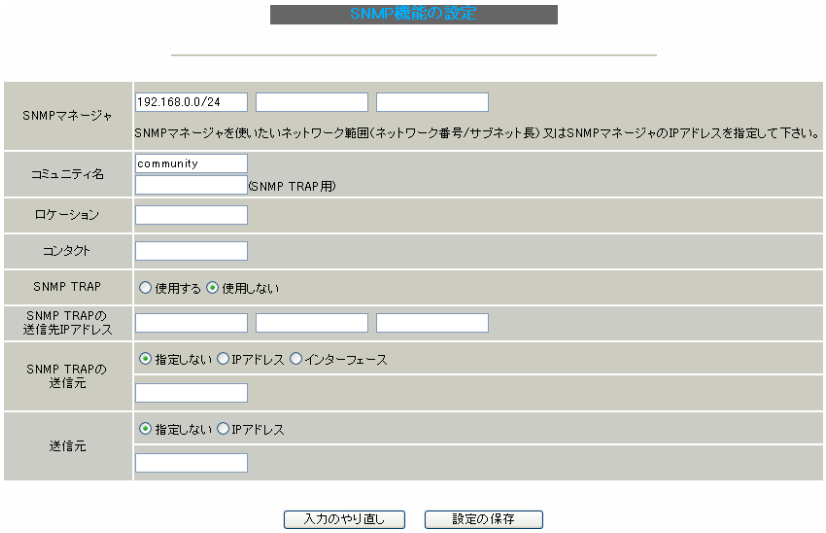
SNMP エージェント機能

第 20 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、任意のインター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」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」で指定する場合
SNMP TRAP の送信元アドレスを指定します。

「インターフェース」で指定する場合
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。

Ⅰ．SNMP エージェント機能の設定

○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。

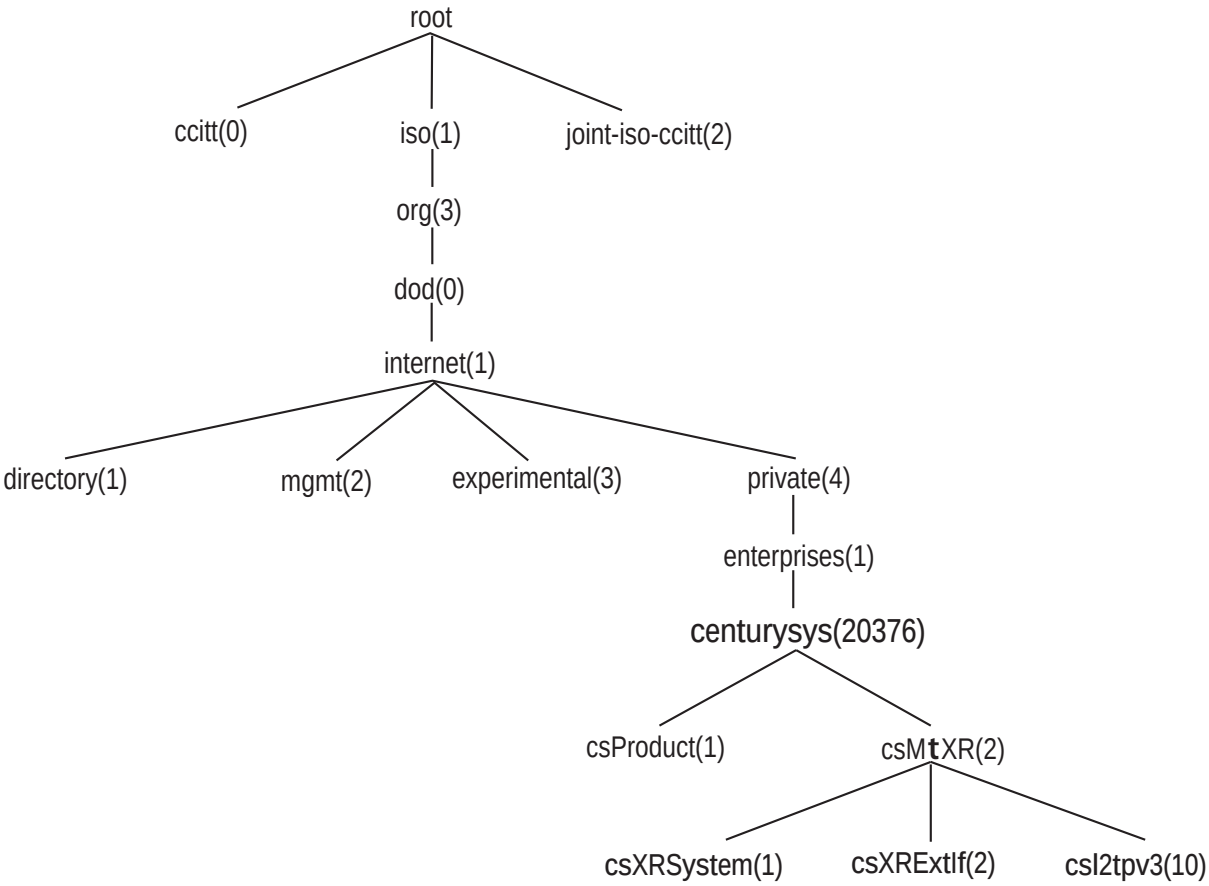
機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動させてください。
なお、設定を変更した場合は、即時設定が反映されますが、「SNMP TRAP の送信元」および「送信元」を変更した場合には、「動作変更」をクリックしてください。

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 インターフェースの up、down
  （XR-540 の場合は、eth2 を除きます）
- 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
  - SYSLOG
  - 攻撃検出
  - NTP
  - VRRP
- SNMP TRAP 自身の起動、停止

11. 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 インターフェース用 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
インターフェースに関する XR 独自の定義 MIB です。各インターフェースの状態や 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ください。

注) システム、インターフェース、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。

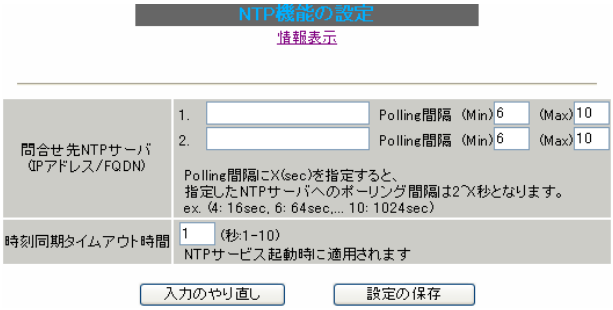
第 21 章

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 サーバと通信を行い、時刻を同期させることができます。

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
NTP サーバの IP アドレスもしくは FQDN を「設定 1」もしくは「設定 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
NTP サーバと通信を行う間隔を設定します。
サーバとの接続状態により、指定した最小値と最大値の範囲でポーリングの間隔を調整します。
Polling 間隔 X 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設定できます。1～10 秒の間で設定できます。

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。

○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。

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 サービスの設定方法

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ください。

○ 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 社にお問い合わせください。

○ 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ください。

第 22 章

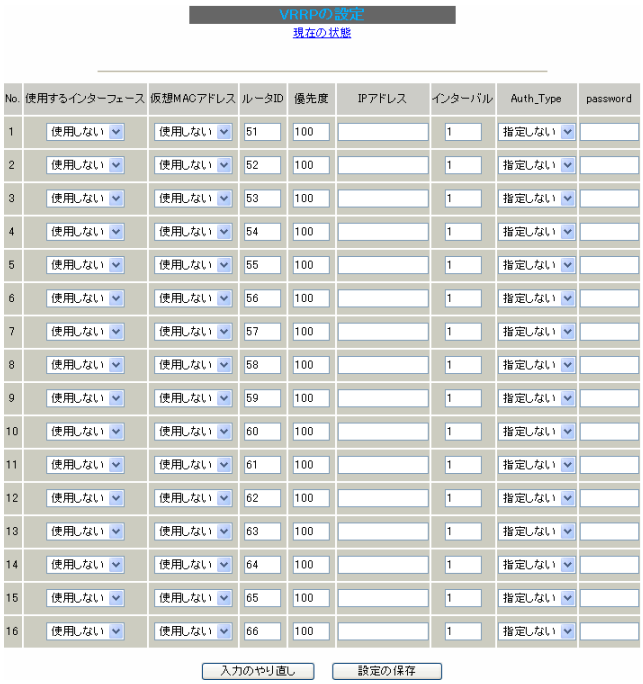
VRRP 機能

第 22 章 VRRP サービス

Ⅰ．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。

「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。「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。
注）仮想 MAC アドレスは一つのインターフェースにつき、一つの VRRP しか設定できません。

○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。
1～255 の間で指定します。

○ 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。

○ Auth_Type
認証形式を選択します。「PASS」または「AH」を選択できます。

○ Password
認証を行なう場合のパスワードを設定します。半角英数字で 8 文字まで設定できます。
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。

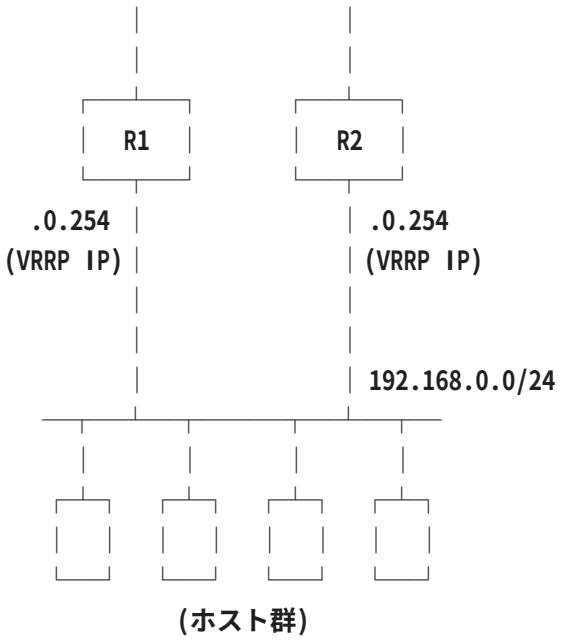
入力が終わりましたら「設定の保存」をクリックして設定完了です。
機能を有効にするには「各種サービスの設定」トップに戻り、サービスを有効にしてください。また設定を変更した場合には、サービスの再起動をおこなってください。

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。

11. VRRP の設定例

下記のネットワーク構成で VRRP サービスを利用するときの設定例です。

ネットワーク構成



設定条件

・ルータ「R1」をマスタルータとする。
・ルータ「R2」をバックアップルータとする。
・ルータの仮想 IP アドレスは「192.168.0.254」
・「R1」「R2」ともに、Ether0 インタフェースで VRRP を作動させる。
・各ホストは「192.168.0.254」をデフォルトゲートウェイとする。
・VRRP ID は「1」とする。
・インターバルは 1 秒とする。
・認証は行なわない。

ルータ「R1」の設定例

No.	使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
1	Ether 0	使用しない	1	100	192.168.0.254	1	指定しない	

ルータ「R2」の設定例

No.	使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
1	Ether 0	使用しない	1	50	192.168.0.254	1	指定しない	

ルータ「R1」が通信不能になると、「R2」が「R1」の仮想 IP アドレスを引き継ぎ、ルータ「R1」が存在しているように動作します。

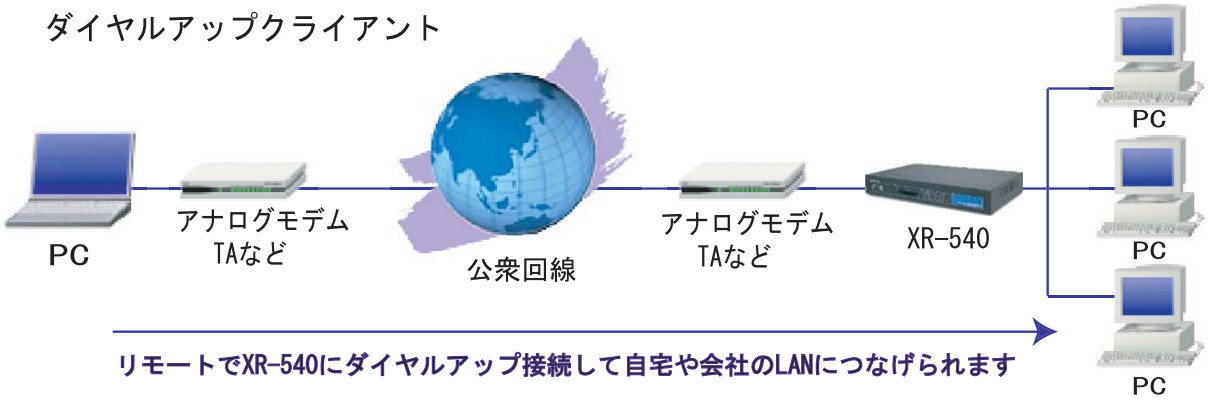
第 23 章

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・BRI 着信(※ **XR-540 のみ**)ではさらに着信番号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。



（図は XR-540 の場合）

11．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。

<XR-510 の場合 >

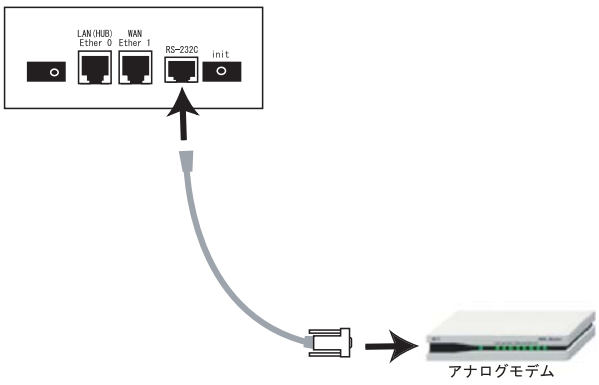
◆アナログモデム /TA の接続

1 XR-510 本体背面の「RS-232」ポートと製品付属の変換アダプタとを、ストレートタイプの LAN ケーブルで接続してください。

2 変換アダプタのコネクタを、アナログモデム /TA のシリアルポートに接続してください。シリアルポートのコネクタが 25 ピンタイプの場合は別途、変換コネクタをご用意ください。

3 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



<XR-540、XR-730 の場合 >

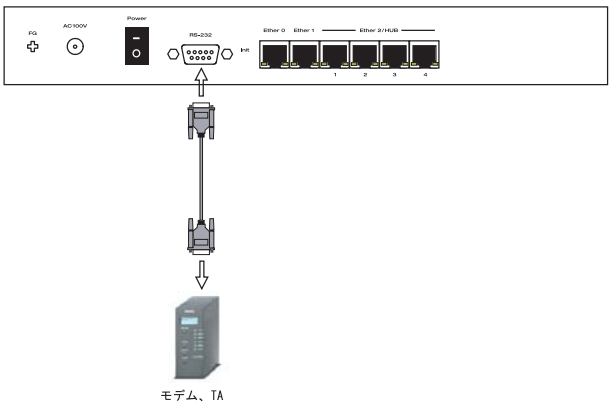
◆アナログモデム /TA のシリアル接続

1 XR-540 の電源をオフにします。

2 XR-540 の「RS-232C」ポートとモデム /TA のシリアルポートをシリアルケーブルで接続します。シリアルケーブルは別途ご用意ください。

3 全ての接続が完了しましたら、モデム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。

シリアル回線で着信する場合

（画面は XR-510）

※ XR-540 では「シリアル回線」欄で設定します。

（画面は XR-540）

○アクセスサーバ（※ XR-510 のみ）
アクセスサーバ機能の使用 / 不使用を選択します。

○着信（※ XR-540 のみ）
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
リモートアクセス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、サブネットのマスクビット値は 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
本装置にリモートアクセス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。

BRI 回線で着信する場合(※ XR-540 のみ)
「BRI 回線」欄で設定します。2 チャンネル分の設定が可能です。

○回線 1 着信 / 回線 2 着信
BRI 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
リモートアクセスされた時の XR-540 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
本装置にリモートアクセス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。

III．アクセスサーバ機能の設定

○発信者番号認証
発信者番号で認証する場合は「する」を選択します。

○本装置のホスト名
本装置のホスト名を任意で設定可能です。

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					☐
6					☐
7					☐
8					☐
9					☐
10					☐

（画面は XR-540）

○アカウント
○パスワード
外部からリモートアクセスする場合の、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、リモートアクセス時のユーザーアカウント・パスワードとなります。
50 アカウントまで登録しておけます。

○アカウント毎に別 IP を割り当てる場合
（※ **XR-540 のみ**）
・本装置の OP
・クライアントの IP
アカウントごとに、割り当てる IP アドレスを個別に指定することも可能です。その場合は「本装置の IP」と「クライアントの IP」のどちらか、もしくは両方を設定します。

○削除
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「設定の保存」をクリックすると、その設定が削除されます。

また、「BRI 回線の設定」（※ **XR-540 のみ**）で発信番号認証を「する」にしている場合は下記の画面の設定を行ってください。

No.	許可する着信番号	着信する回線	削除
1		すべて	☐
2		すべて	☐
3		すべて	☐
4		すべて	☐
5		すべて	☐
6		すべて	☐
7		すべて	☐
8		すべて	☐
9		すべて	☐
10		すべて	☐

（画面は XR-540）

○許可する着信番号（※ **XR-540 のみ**）
発信者の電話番号を入力してください。

○着信する回線（※ **XR-540 のみ**）
「すべて」、「回線 1」、「回線 2」の中から選択してください。

○削除
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「設定の保存」をクリックすると、その設定が削除されます。

※外部からダイヤルアップ接続されていないときには、「各種サービスの設定」画面の「アクセスサーバ」が「待機中」の表示となります。

アカウント設定上の注意

ユーザーアカウント設定のユーザー名と、PPP/PPPoE 設定の接続先設定で設定してあるユーザー名に同じユーザ名を登録した場合、そのユーザは**着信できません**。
ユーザー名が重複しないように設定してください。

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。

III．アクセスサーバ機能の設定

クライアントへのスタティックルート設定について（XR-510 の場合）

リモートアクセスしてきたホストに対するスタティックルートを設定する場合、必ず下記のように設定します。

・インターフェース “ ppp6 ”
・ゲートウェイ “ クライアントの IP アドレス ”

クライアントへのスタティックルートについて（XR-540 の場合）

アクセスサーバ回線でスタティックルートを設定する場合、インターフェース指定によるスタティックルート設定はできません。
「クライアントの IP アドレス」をゲートウェイアドレスとしたルートを設定してください。

なお、BRI 回線 1,2 両方の着信を許可している場合は、両方の「クライアント IP アドレス」をゲートウェイアドレスとしたルートを設定します。

BRI 着信時のスタティックルート設定例)
・クライアントのネットワークアドレス
　192.168.20.0/24
・BRI 回線 1 のクライアントの IP アドレス
　192.168.251.171
・BRI 回線 2 のクライアントの IP アドレス
　192.168.251.172

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		192.168.251.171	1
192.168.20.0	255.255.255.0		192.168.251.172	1

注）アクセスサーバ着信用スタティックルートに限り、着信後にルートが有効になるまで経路情報表示では表示されません。

◆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「インターフェース / 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ー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ください。

インターフェース：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

前々ページ「BRI 回線で着信する場合（※ **XR-540 のみ**）」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	192.168.251.171	1
2	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	ppp6	192.168.252.172	2

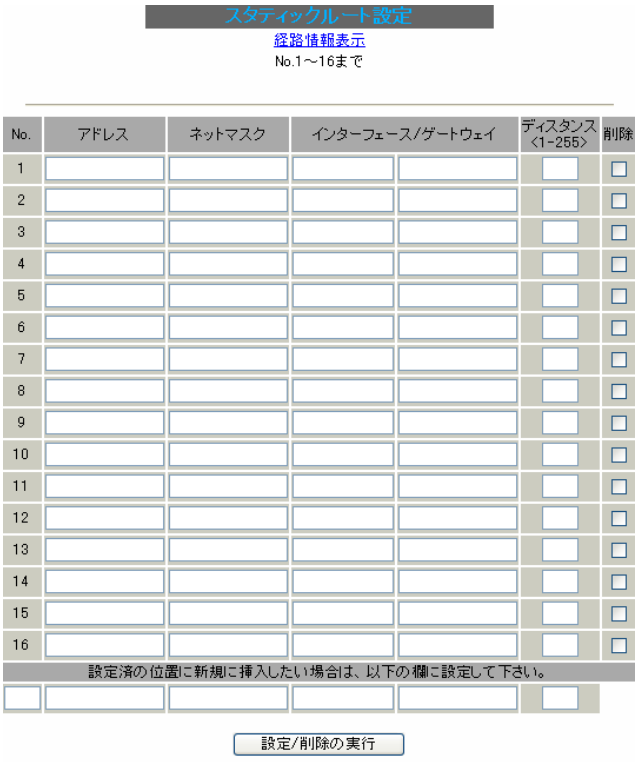
第 24 章

スタティックルート

スタティックルート設定

本装置は、最大 256 エントリのスタティックルートを登録できます。

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

○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。

○インターフェース／ゲートウェイ

ルーティングをおこなうインターフェース名、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。

※ PPP/PPPoE や GRE インタフェースを設定するときはインタフェース名だけの設定となります。

注)但し、リモートアクセス接続のクライアントに対するスタティックルートを設定する場合のみ、下記のように設定してください。

- **インターフェース “ ppp6 ”**
- **ゲートウェイ**
  “ クライアントに割り当てる IP アドレス ”

通常は、インターフェース / ゲートウェイのどちらかのみ設定できます。

本装置のインター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。

○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。

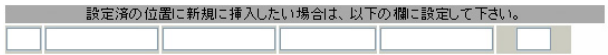
設定を挿入する

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

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。

インタフェース名は「付録 A」を参照してください。

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 25 章

ソースルーティング

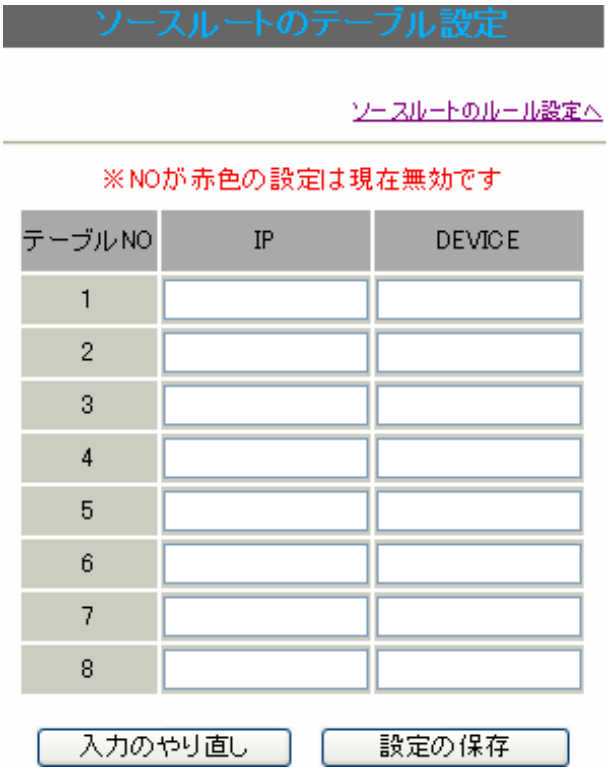
ソースルーティング設定

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。



○ 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。

○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。

ソースルーティング設定

○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 26 章

NAT 機能

第 26 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、「インターフェース設定」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。

11．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。

No.	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
1			全て			□
2			全て			□
3			全て			□
4			全て			□
5			全て			□
6			全て			□
7			全て			□
8			全て			□
9			全て			□
10			全て			□
11			全て			□
12			全て			□
13			全て			□
14			全て			□
15			全て			□
16			全て			□
設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。						
			全て			

○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***

○インターフェース
インターネットからのアクセスを受信するインターフェース名を指定します。本装置のインター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。

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。

設定情報の確認

「情報表示」をクリックすると、現在のバーチャルサーバ設定の情報が一覧表示されます。

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。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。					
			全て		

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。

ポート番号を指定して設定するときは、必ずプロトコルも選択してください。「全て」の選択ではポートを指定することはできません。

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。

No.	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	削除
1				☐
2				☐
3				☐
4				☐
5				☐
6				☐
7				☐
8				☐
9				☐
10				☐
11				☐
12				☐
13				☐
14				☐
15				☐
16				☐
設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。				

○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。

○インターフェース
どのインターフェースからインターネット(WAN)へアクセスするか、インター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ーフェースを設定してください。
本装置のインター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。

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。

設定情報の確認

「情報表示」をクリックすると、現在の送信元 NAT 設定の情報が一覧表示されます。

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。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。				

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.xx.xx.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。

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくに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る場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

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
192.168.0.3		tcp	1023	ppp0
192.168.0.3		gre		ppp0

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくに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る場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

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、仮想インターフェースとして登録します。メニューにある「仮想インターフェース設定」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 インターフェース設定」**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
192.168.0.3	211.xxx.xxx.105	tcp	110	eth1
192.168.0.4	211.xxx.xxx.106	tcp	21	eth1
192.168.0.5	211.xxx.xxx.106	tcp	20	eth1
192.168.0.6	211.xxx.xxx.107	tcp	53	eth1
192.168.0.7	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。

Ethernet で直接 WAN に接続する環境で、WAN 側に複数のグローバルアドレスを指定してバーチャルサーバ機能を使用する場合、[公開するグローバルアドレス]で指定した IP アドレスを、「仮想インターフェース設定」にも必ず指定してください。

ただし、PPPoE 接続の場合は、仮想インターフェースを作成する必要はありません。

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ください。
＜設定例＞　***192.168.254.0/24***

Ethernetで直接WANに接続する環境で、WAN側に複数のグローバルアドレスを指定して送信元 NAT 機能を使用する場合、[変換後のグローバルアドレス]で指定したIPアドレスを、「仮想インターフェース設定」にも必ず指定してください。

ただし、PPPoE接続の場合は、仮想インターフェースを作成する必要はありません。

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 27 章

パケットフィルタリング機能

第 27 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。
・ゲートウェイ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。

・送信元 / あて先 IP アドレス
・プロトコル(TCP/UDP/ICMP など)・番号
・送信元 / あて先ポート番号
・入出力方向(入力 / 転送 / 出力)
・インターフェース

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)・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。

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)**
- **ゲートウェイ認証フィルタ**

◆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。

◆ゲートウェイ認証フィルタ
「ゲートウェイ認証機能」を使用しているときに設定するフィルタです。ゲートウェイ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。ゲートウェイ認証機能については
「第 34 章 ゲートウェイ認証機能」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

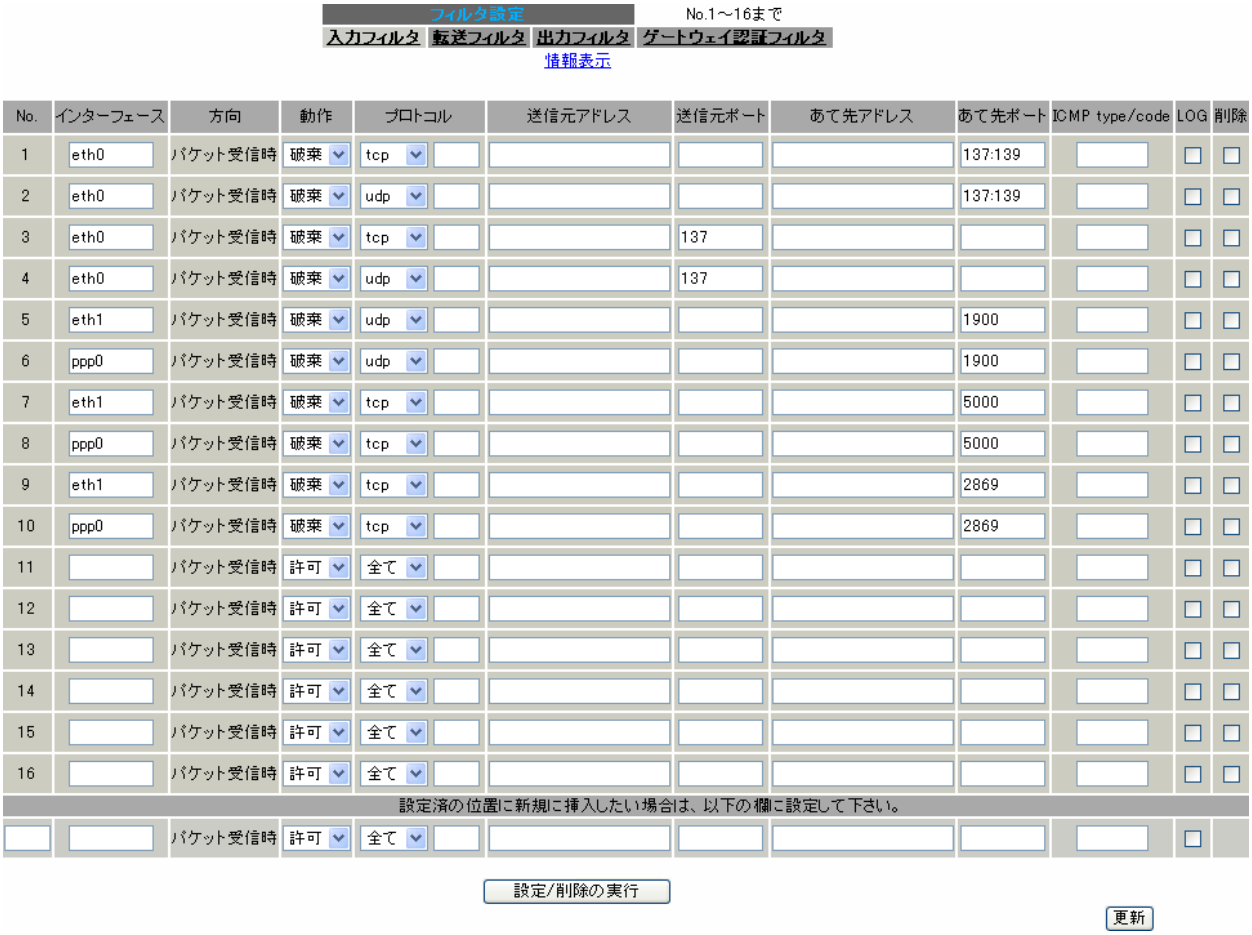
Windows ファイル共有をする場合は、NetBIOS 用のフィルタを削除してお使いください。

III. パケットフィルタリングの設定

入力・転送・出力・ゲートウェイ認証フィルタの 4 種類ありますが、設定方法はすべて同様となります。

設定方法

Web 設定画面にログインします。「フィルタ設定」→「入力フィルタ」「転送フィルタ」「出力フィルタ」「ゲートウェイ認証フィルタ」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ーフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名について」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。

○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。

III．パケットフィルタリングの設定

○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、ドメイン名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　(” アドレス /32 ” の書式)
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、プロトコルもあ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、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での指定が可能です。
入力方法は、送信元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、送信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。

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。

○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行います。通常は DNS の TTL の値が 0 になるタイミングで名前解決が行われますが、更新タイミング以外で名前解決を行いたい場合にクリックしてください。

また、IP アドレスをドメイン名、FQDN で指定した場合は「更新」ボタンをクリックし、名前解決を実行してください。

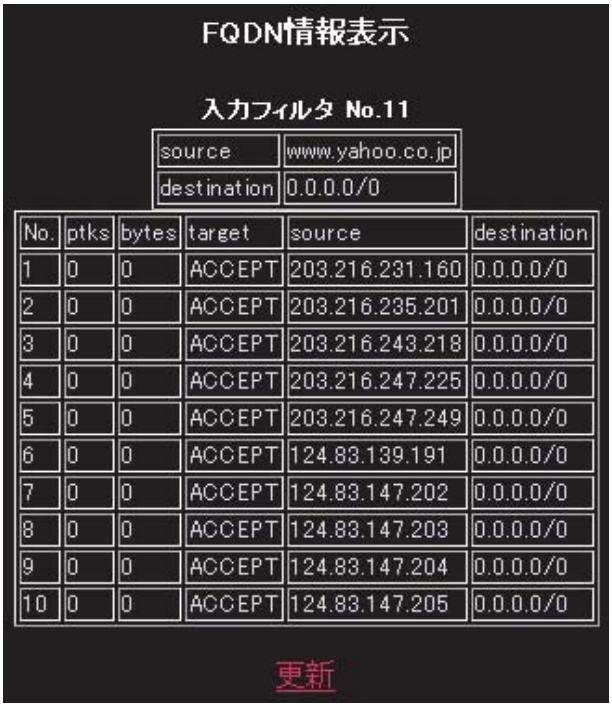
送信元アドレス、または、あて先アドレスとして FQDN 形式を指定する場合、各フィルタ設定（入力、転送、出力、ゲートウェイ認証）を含めた指定数の合計は 64 個まで可能とします。
（１行の設定で送信元アドレスとあて先アドレスの両方を AQDN 指定した場合の指定数は 2 です。）

III. パケットフィルタリングの設定

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。

IP アドレス指定を FQDN で行った場合は、「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。



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。

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

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「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. 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 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」

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					

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。

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。

◆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」No1、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。

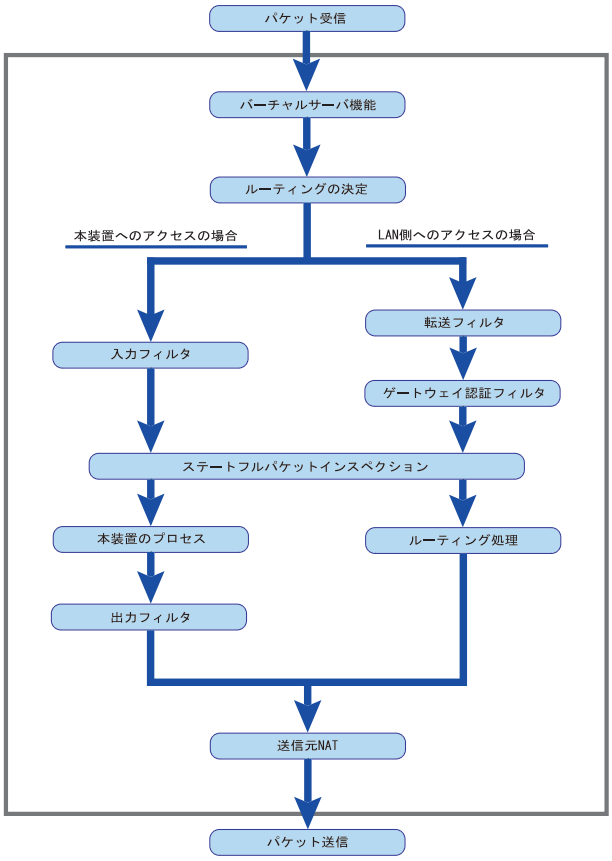
No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp	221.xxx.xxx.105			880

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「入力フィルタ」「転送フィルタ」を設定している場合は、先に「入力フィルタ」「転送フィルタ」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。
IN=	パケットを受信したインターフェイスが記されます。
OUT=	パケットを送出したインターフェイスが記されます。なに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 28 章

ブリッジフィルタ機能

第 28 章 ブリッジフィルタ機能

Ⅰ．機能の概要

本装置はブリッジフィルタ機能を搭載しています。ブリッジされた Ethernet インターフェースや VLAN インターフェースにおいて、MAC ヘッダを使ったフィルタリングを行うことができます。
同一 LAN の特定エリアをブリッジで分離して、ブリッジフィルタを設定することによって、LAN 内のセキュリティをきめ細かく制御することができます。

以下のようなブリッジフィルタリングをレイヤ２レベルで実現できます。

- ブリッジされた２つのインターフェース間のフレームをレイヤ２レベルで制限する。
- ブリッジの一方のインターフェースから本装置自身が受信するフレームをレイヤ２レベルで制限する。
- 本装置からブリッジの一方のインターフェースへ出て行くフレームをレイヤ２レベルで制限する。
- STP フレームの送受信を制限する。

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。

- 送信元 / 宛先 MAC アドレス
- Ethernet タイプ(IP/ARP/IEEE802.1Q など)
  ※さらに IP アドレス / ポート番号、ARP-Opcode、VLAN Priority Tag といったプロトコル毎の詳細設定も可能
- 入出力方向(入力 / 転送 / 出力)
- インターフェース

注） 本機能はブリッジされていないインターフェース上での L2 フィルタとして動作することはできません。

パケットフィルタと同様に、ブリッジフィルタでも以下の３つの基本ルールについてフィルタリングの設定を行います。

- **入力(input)**
- **転送(forward)**
- **出力(output)**

◆入力(input)フィルタ
ブリッジされたインターフェースから本装置自身に入ってくるフレームに対してレイヤ 2 レベルで制御します。ブリッジに接続されたホスト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行います。

◆転送(forward)フィルタ
本装置がブリッジされたインターフェース間でフレーム転送するアクセスをレイヤ 2 レベルで制御する場合には、この転送ルールにフィルタ設定を行います。

◆出力(output)フィルタ
本装置自身からブリッジされたインターフェースへのアクセスをレイヤ 2 レベルで制御したい場合には、この出力ルールにフィルタ設定を行います。

制御したいフレームが「ブリッジ内で転送されるもの」、「本装置自身へのアクセス」、「本装置自身からのアクセス」かを確認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。

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優先的にフィルタとして動作することになります。
つまりアクセスを許可するフィルタと、それ以外を破棄するフィルタを設定したい場合は、必ず許可する方のフィルタを先に設定してください。

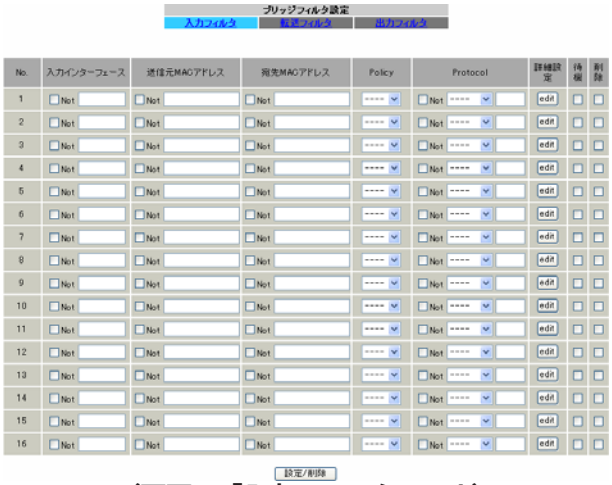
マッチするフィルタ設定が見つからない場合は、そのフレームはフィルタリングされません。

II. ブリッジフィルタの設定

入力・転送・出力フィルタの３種類がありますが、設定方法は全て同様となります。

設定方法

Web 設定画面にログインします。「ブリッジフィルタ設定」→「入力フィルタ」「転送フィルタ」「出力フィルタ」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）

○入力インターフェース(入力 / 転送フィルタのみ)
フィルタリング対象とする入力インターフェースを指定します。

○出力インターフェース(転送 / 出力フィルタのみ)
フィルタリングを行う出力インターフェース名を指定します。

※指定可能なインターフェースは入力、出力共にイーサネット(ethN),VLAN インターフェース(ethX.Y)のいずれかです。

○送信元 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。ワイルドカード指定はできません。

○宛先 MAC アドレス
フィルタリング対象とする宛先 MAC アドレスを入力します。ワイルドカード指定はできません。

※ MAC アドレスはマルチキャスト MAC アドレス、ブロードキャスト MAC アドレスの指定も可能です。

○ Policy
フィルタリング設定にマッチしたときにフレームを破棄するか許可するかを選択します。

○ Protocol
フィルタリング対象とするイーサネットタイプを指定します。「IPv4」「ARP」「802.1q」のいずれかをプルダウンから選択するか、またはボックス内に直接数値を入力してください。
数値で入力する場合は、頭に 0x を付与しない 16 進数で指定します。設定可能な範囲は 0600 ～ ffff です。
　例）　IPX を指定する場合： 8137

○詳細設定
次ページにて説明します。

入力が終わりましたら、「設定 / 削除」をクリックして設定完了です。

注） 各項目の「Not」チェックボックスはフィルタリング条件を Not 条件にしたい場合にチェックしてください。
Not 条件にした場合は、指定した条件以外の全てがフィルタリング対象となります。

設定の削除

不要なフィルタリング条件を削除したい場合は右端の「削除」チェックボックスにチェックを入れ、「設定 / 削除」をクリックします。

設定の待機

設定したフィルタリング条件を一時的に無効にしたい場合は右側の「待機」チェックボックスにチェックを入れてください。画面上の設定は残りますが、フィルタリングは無効になります。

III. ブリッジフィルタの詳細設定

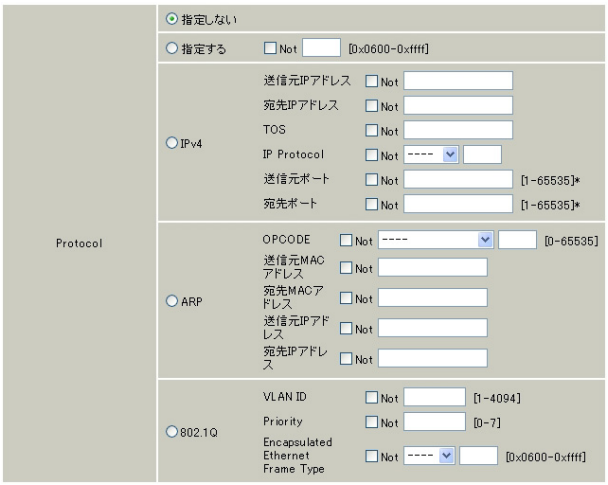
本装置では、プロトコル別のより詳細な設定や STP に対するフィルタ設定も可能です。
これらはブリッジフィルタ詳細設定画面で設定します。

設定方法

ブリッジフィルタ画面の各フィルタ項目の右側にある ” 詳細設定 ” 欄の「edit」をクリックすると、ブリッジフィルタ詳細設定画面が開きます。

プロトコル別詳細設定

ブリッジフィルタ詳細設定の以下の画面から設定します。



[IPv4 設定]

IPv4 パケットをフィルタする場合、以下のような詳細設定ができます。

○送信元 IP アドレス
フィルタリング対象とする送信元 IP アドレスを指定します。

○宛先 IP アドレス
フィルタリング対象とする宛先 IP アドレスを指定します。

○ TOS
特定のサービスタイプ(TOS)が設定された IPv4 パケットをフィルタリングしたい場合に指定します。ボックス内にフィルタリング対象とする ToS 値を入力してください。16 進数で指定します。設定可能な範囲は 00 ～ ff です。

○ IP Protocol
フィルタリング対象とする IP プロトコルを指定します。ICMP/TCP/UDP/GRE/ESP/OSPF のいずれかをプルダウンから選択するか、またはボックス内にプロトコル番号を数値で入力してください。数値で入力する場合は 10 進数で指定します。設定可能な範囲は 0 ～ 255 です。

○送信元ポート (*)
フィルタリング対象とする送信元ポート番号を指定します。IP Protocol に「TCP」または「UDP」を指定した場合のみ設定可能です。
また設定可能な範囲は 1 ～ 65535 です。

○宛先ポート (*)
フィルタリング対象とする宛先ポート番号を指定します。IP Protocol に「TCP」または「UDP」を指定した場合のみ設定可能です。
また設定可能な範囲は 1 ～ 65535 です。

[ARP 設定]

ARP パケットをフィルタする場合、以下のような詳細設定ができます。

○ OPCODE
特定の ARP オペレーションコードが設定された ARP パケットをフィルタリングしたい場合に指定します。ARP オペレーションコードをプルダウンから選択するか、またはボックス内に ARP オペレーションコードを数値で入力してください。数値で入力する場合は 10 進数で入力し、設定可能な範囲は 0 ～ 65535 です。

○送信元 MAC アドレス
フィルタリング対象とする ARP プロトコル部の送信元 MAC アドレスを指定します。

(次ページに続きます)

III．ブリッジフィルタの詳細設定

○宛先 MAC アドレス
フィルタリング対象とする ARP プロトコル部の宛先 MAC アドレスを指定します。

送信元 MAC アドレス、宛先 MAC アドレスは単一指定、またはマスク表記によるワイルドカード指定ができます。
マスク指定の例)
・「00:80:6D:**:**:**」を指定する場合
00:80:6D:00:00:00/FF:FF:FF:00:00:00

○送信元 IP アドレス
フィルタリング対象とする ARP プロトコル部の送信元 IP アドレスを指定します。

○宛先 IP アドレス
フィルタリング対象とする ARP プロトコル部の宛先 IP アドレスを指定します。

[IEEE802.1Q 設定]

VLAN タギングされたパケットをフィルタする場合、以下のような詳細設定ができます。Ethernet ブリッジでのみ有効です。

○ VLAN ID
フィルタリング対象とする VLAN ID を指定します。設定可能な範囲は、1 ～ 4094 です。

○ Priotiry
フィルタリング対象とする UserPriority 値を指定します。設定可能な範囲は 0 ～ 7 です。

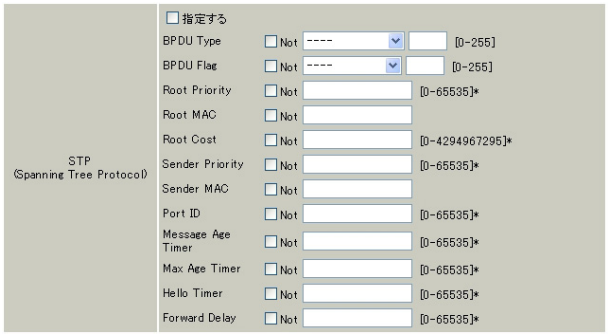
注) VLAN ID と Priority は同時に指定することはできません。

○ Encapsulated Ethernet Frame Type
フィルタリング対象とするオリジナルフレームのタイプを指定します。プルダウンから「IPv4」「ARP」を選択するか、またはボックス内に直接数値を入力してください。
数値で入力する場合は、16 進数で指定します。設定可能な範囲は 0600 ～ ffff です。

STP 詳細設定

STP フィルタを設定する場合、宛先 MAC アドレスに「01:80:c2:00:00:00」を設定してください。

その他の STP 詳細設定は、ブリッジフィルタ詳細設定の以下の画面から設定します。



○指定する
STP の詳細設定を行う場合はチェックを入れます。

○ BPDU Type
フィルタリング対象とする BPDU タイプを指定します。プルダウンから「CONFIG BPDU」(=0)、「TCN BPDU」(=1)のいずれかを選択するか、または、ボックス内に直接数値を入力してください。
数値で入力する場合は、10 進数で指定します。設定可能な範囲は 0 ～ 255 です。

○ BPDU Flag
フィルタリング対象とする BPDU フラグを指定します。プルダウンから「CHANGE」(=1)、「CHANGE ACK」(=128)のいずれかを選択するか、または、ボックス内に直接数値を入力してください。
数値で入力する場合は、10 進数で指定します。設定可能な範囲は 0 ～ 255 です。

○ Root Priority (*)
フィルタリング対象とするルートブリッジプライオリティを指定します。設定可能な範囲は 0 ～ 65535 です。

○ Root MAC
フィルタリング対象とするルートブリッジ MAC アドレスを指定します。

III．ブリッジフィルタの詳細設定

○ Root Cost (*)
フィルタリング対象とするルートブリッジへのパスコストを指定します。設定可能な範囲は、0～4294967295 です。

○ Sender Priority (*)
フィルタリング対象とする送信元ブリッジのプライオリティを指定します。設定可能な範囲は 0～65535 です。

○ Sender MAC
フィルタリング対象とする送信元ブリッジの MAC アドレスを指定します。

○ Port ID (*)
フィルタリング対象とする送信元ブリッジのポート識別子を指定します。設定可能な範囲は 0～65535 です。

○ Message Age Timer (*)
フィルタリング対象とする Message Age Timer (BPDU 有効時間)を指定します。設定可能な範囲は 0～65535 です。

○ Max Age (*)
フィルタリング対象とする Max Age(BPDU 最大監視時間)を指定します。設定可能な範囲は 0～65535 です。

○ Hello Timer (*)
フィルタリング対象とする Hello Timer(BPDU 送信間隔)を指定します。設定可能な範囲は 0～65535 です。

○ Forward Delay (*)
フィルタリング対象とする Forward Delay(Forward 遷移遅延時間)を指定します。設定可能な範囲は 0～65535 です。

注） 各項目の「Not」チェックボックスはフィルタリング条件を Not 条件にしたい場合にチェックしてください。
Not 条件にした場合は、指定した条件以外の全てがフィルタリング対象となります。

注 ） 文中に(*)のついた項目は数値入力時に範囲指定ができます。範囲指定したい場合は、下限値と上限値を ”: ” で結んでください。
＜入力例＞ 1000 から 1020 をフィルタリング対象とする場合。 「1000:1020」

第 29 章

スケジュール設定
（※ XR-540 のみ）

第 29 章 スケジュール設定（※ XR-540 のみ）

スケジュール機能の設定方法

XR-540 には、主回線を接続または切断する時間を管理するスケジュール機能があります。
スケジュールの設定は 10 個まで設定できます

Web 設定画面の「スケジュール設定」をクリックします。

1～10 のいずれかをクリックし、以下の画面でスケジュール機能の詳細を設定します。

○スケジュール
実行させる「時刻」「動作」を設定します。

「時刻」
実行させる時刻を設定します。

「動作」
動作内容を設定します。
「時刻」項目で設定した時間に主回線を接続する場合は「主回線接続」、切断する場合は「主回線切断」を選択します。

○実行日
実行する日を「毎日」「毎週」「毎月」の中から選択します。

「毎日」
毎日同じ時間に接続 / 切断するように設定する場合に選択します。

「毎週」
毎週同じ曜日の同じ時間に接続 / 切断するように設定する場合に選択します。
なお、複数の曜日を選択することができます。

「毎月」
毎月同じ日の同じ時間に接続 / 切断するように設定する場合に選択します。
なお、複数の日を選択することができます。

複数選択する場合
【Windows の場合】
Control キーを押しながらクリックします。
【Macintosh の場合】
Command キーを押しながらクリックします。

○有効期限
実行有効期限を設定します。有効期限は、常に設定する年から 10 年分まで設定できます。
有効期限で「xxxx 年 xx 月 xx 日に実行」を選択した場合、実行日は「毎日」のみ選択できます。

「なし」
特に実行する期限を定めない場合に選択します。

「xx 月 xx 日～ x 月 x 日の期間」
実行する期間を定める場合に選択し、有効期限を設定します。

「xxxx 年 xx 月 xx 日以降」
実行する期間の開始日を設定したい場合に選択します。

「xxxx 年 xx 月 xx 日まで」
実行する期間の終了日を設定したい場合に選択します。

「xxxx 年 xx 月 xx 日に実行」
実行する日時を設定したい場合に選択します。

○設定したスケジュール内容の実行・削除・保存を決定します。

「スケジュールを有効にする」
設定したスケジュールを起動する場合に選択します。

「スケジュールを無効にする」
スケジュールの設定内容を残しておきたい場合に選択します（スケジュールは起動しません）。

「スケジュールを削除する」
スケジュールの設定内容を削除する場合に選択します。

入力が終わりましたら、「設定 / 削除の実行」をクリックします。
設定内容は画面上のスケジュール設定欄に反映されます。

スケジュール設定欄の項目について

スケジュール設定欄にある項目（「時間」「動作」「実行」「有効期間」「スケジュール」）のリンクをクリックすると、クリックした項目を基準にしたソートがかかります。

＜例＞

スケジュール設定

	時間	動作	実行	有効期限	スケジュール
1	15 : 51	主回線接続	毎日	なし	無効
2	08 : 00	主回線切断	毎週 月,水曜日	2007年 9月 1日以降	有効
3	18 : 10	主回線切断	毎日	なし	無効
4	23 : 00	主回線接続	毎週 日,火曜日	2007年 9月30日以降	有効
5	スケジュールは設定されていません				
6	スケジュールは設定されていません				
7	スケジュールは設定されていません				
8	スケジュールは設定されていません				
9	スケジュールは設定されていません				
10	スケジュールは設定されていません				

上の画面で「時間」項目をクリックします。
下の画面のように、「時間」の早い順番に並べ替えられます。

スケジュール設定

	時間	動作	実行	有効期限	スケジュール
1	08 : 00	主回線切断	毎週 月,水曜日	2007年 9月 1日以降	有効
2	15 : 51	主回線接続	毎日	なし	無効
3	18 : 10	主回線切断	毎日	なし	無効
4	23 : 00	主回線接続	毎週 日,火曜日	2007年 9月30日以降	有効
5	スケジュールは設定されていません				
6	スケジュールは設定されていません				
7	スケジュールは設定されていません				
8	スケジュールは設定されていません				
9	スケジュールは設定されていません				
10	スケジュールは設定されていません				

第 30 章

ネットワークイベント機能

第 30 章 ネットワークイベント機能

1．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

◆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。監視するインターフェースのリンクがダウンした時にトリガとして検知します。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として検知します。

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。

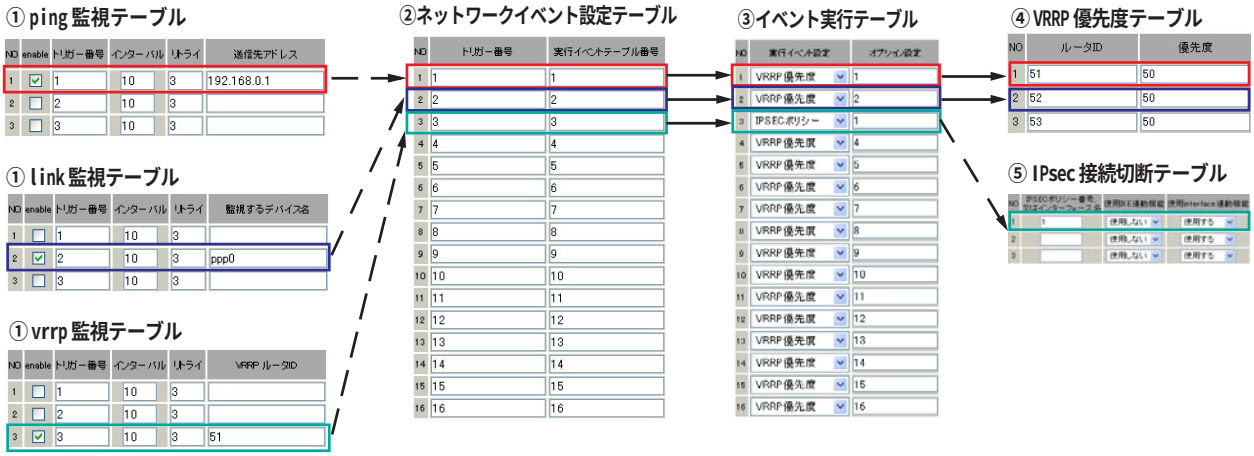
例えば、vrrp 監視と連動して、2 台の VRRP ルータのマスタルータの切り替わりに応じて、IPsec 接続を繋ぎかえる、といった使い方ができます。

第 30 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

　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「④ VRRP 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 / 切断を行う 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。

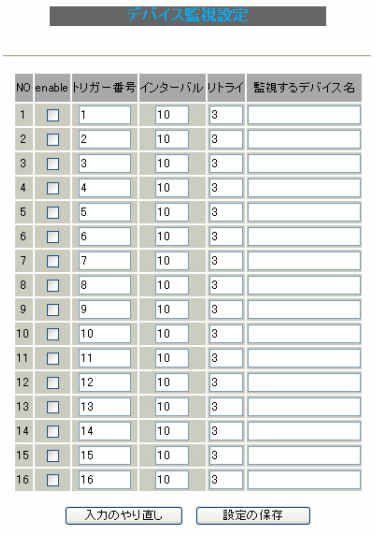
○インターバル(秒)
○リトライ
ping を発行する間隔を設定します。
「『インターバル』秒間に、『リトライ』回 ping を発行する」という設定になります。この間、一度も応答が無かった場合にトリガとして検知されます。

○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。

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ーフェース名を指定します。Ethernet インターフェース名、または PPP インター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。

II. 各トリガテーブルの設定

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。

各監視機能を有効にするにはネットワークイベント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、削除を行った場合は、サービスの再起動を行ってください。

(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。

○トリガー番号
「ping 監視の設定」、「link 監視の設定」、「vrrp 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。

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。

○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 ポリシーの切断を行います。
「VRRP 優先度」は、VRRP ルータの優先度を変更します。

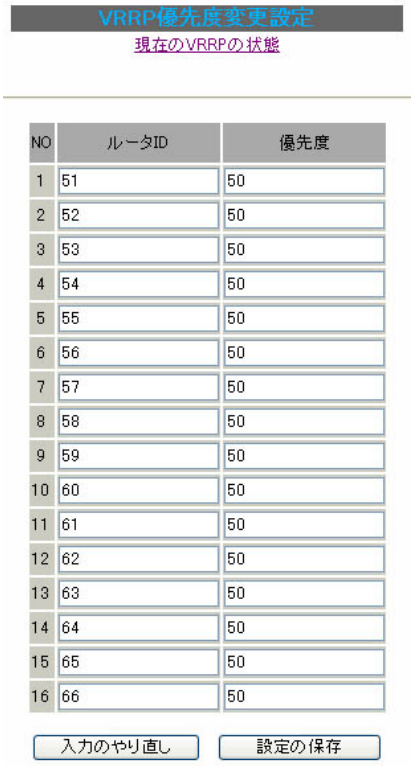
○オプション設定
実行イベントのオプション番号です。本値は、「VRRP 優先度変更設定」テーブル、または「IPSEC 接続切断設定」テーブルでのインデックス番号となります。

最後に「設定の保存」をクリックして設定完了です。

Ⅳ．実行イベントのオプション設定

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。

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
トリガ検知時に切断する IPsec ポリシーの番号、又は IPsec インター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**

インターフェース名を指定した場合は、そのインターフェースで接続する IPsec は全て切断されます。トリガ復旧時には再度 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。

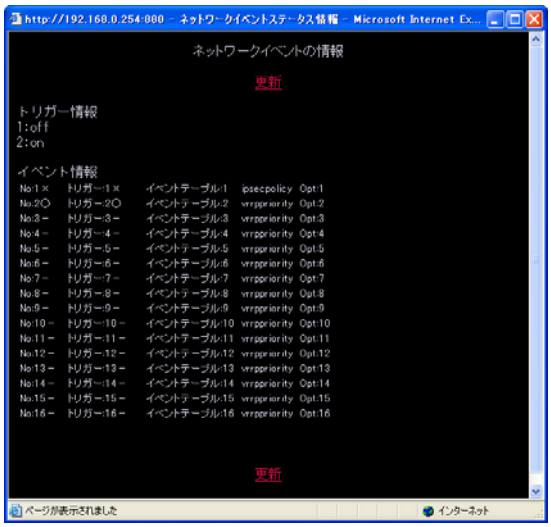
○使用 interface 連動機能
本装置では、PPPoE 上で IPsec 接続している場合、PPPoE 接続時に自動的に IPsec 接続も開始されます。ネットワークイベント機能を使った IPsec 二重化において、バックアップ側の PPPoE 接続時に IPsec を自動接続させたくない場合には「使用しない」を選択します。

最後に「設定の保存」をクリックして設定完了です。

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 31 章

仮想インターフェース機能

仮想インターフェースの設定

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。

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
仮想インターフェースを作成するインターフェース名を指定します。本装置のインター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。

○仮想 I/F 番号
作成するインターフェースの番号を指定します。
自由に設定できます。

○ IP アドレス
作成するインターフェースの IP アドレスを指定します。

○ネットマスク
作成するインターフェースのネットマスクを指定します。

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。

”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。

設定を削除する

仮想インター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。

第 32 章

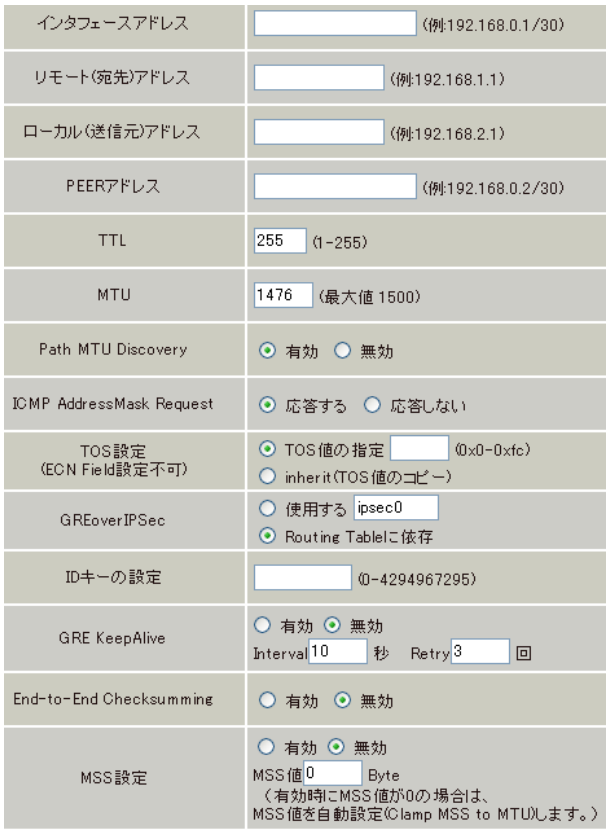
GRE 機能

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ーフェース名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。

○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。

○ 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、Path MTU 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 インター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 over IPsec
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」を選択してください。
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 の設定

○ 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行います。「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」には、GRE キープアライブパケットの送信間隔を設定します。
指定可能な範囲は 1 ～ 32767 秒です。
「Retry」には、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。
指定可能な範囲は 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行われます。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 送信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 が実行されます。

◆ GRE の削除

「削除」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

「現在の状態」では GRE の動作状況が表示されます。

現在の状態	Tunnel is down, Link is down

◆ 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（下記設定画面）。
設定の編集は「Interface 名」をクリックしてください。また 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。

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

第 33 章

QoS 機能

第 33 章 QoS 機能

1. 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.PFIFO
2.TBF
3.SFQ
4.PQ
5.CBQ

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。

1. QoS について

1.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。

2.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。

1. QoS について

3.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。

4.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。

I. QoS について

5.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)>

```
root クラス（1Mbps）
 |
 ├──クラス 1（500kbps、優先度 2）
 |      |
 |      ├── HTTP（優先度 1）
 |      |
 |      └── FTP （優先度 5）
 |
 └──クラス 2（500kbps、優先度 1）
        |
        ├── HTTP（優先度 1）
        |
        └── FTP （優先度 5）
```

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。

11. QoS 機能の各設定画面について

Interface Queuing 設定画面
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。

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。

◆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。

◆SFQ の設定手順

「Interface Queueing 設定」で設定します。

◆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。

◆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。

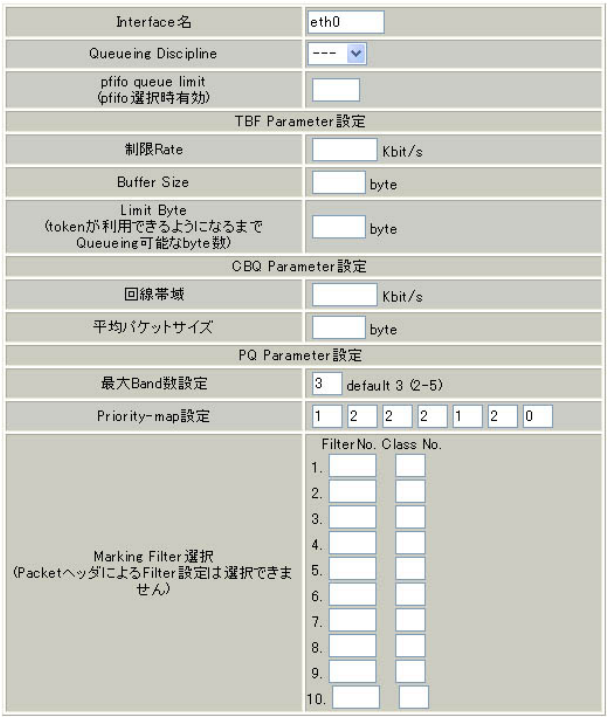
4. クラスキューイングの設定

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。

IV. 各設定画面での設定方法について

◆ 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」を参照してください。**

○ Queueing Discipline

キューイング方式を選択します。

[pfifo の設定]

○ pfifo queue limit

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。1～999 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。

[SFQ の設定]

Queueing Discipline で「SFQ」を選択するだけです。

IV. 各設定画面での設定方法について

[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 設定

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. には Class 分けフィルタの設定番号を指定します。

Class No. には、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。(「TOS 値について」を参照ください)

○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。

Ⅳ. 各設定画面での設定方法について

[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)。

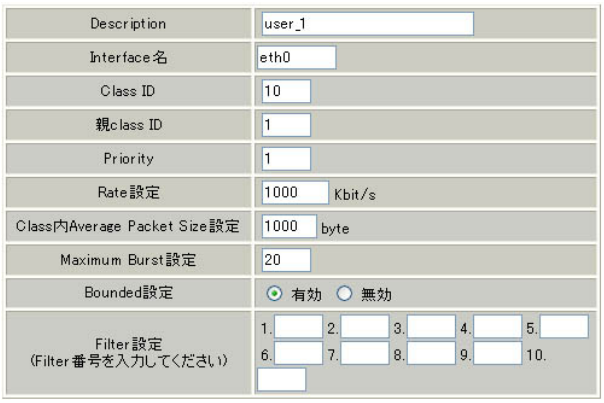
○平均パケットサイズ設定

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。

IV. 各設定画面での設定方法について

◆CLASS 設定

設定を追加するときは「New Entry」をクリックします。



(画面は表示例です)

○ 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」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。

○ 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

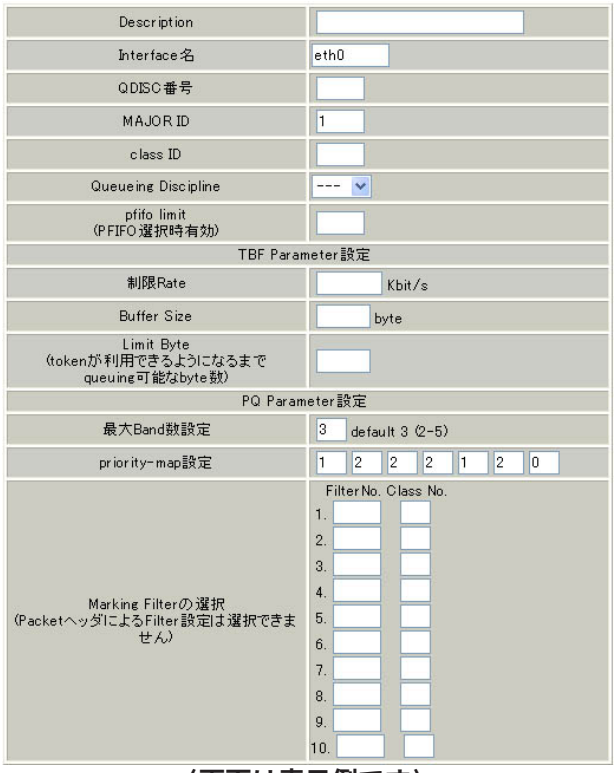
CLASS 分けフィルタの設定番号を指定します。ここで指定したフィルタにマッチングしたパケットが、このクラスに送られてきます。

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

◆「CLASS Queueing 設定」

設定を追加するときは「New Entry」をクリックします。



(画面は表示例です)

○ 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」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。

○ Queueing Discipline 以下は、Interface Queueing 設定と同様に設定します。

IV. 各設定画面での設定方法について

◆「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。

(画面は表示例です)

○ 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。

○パケットヘッダによるフィルタ
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。

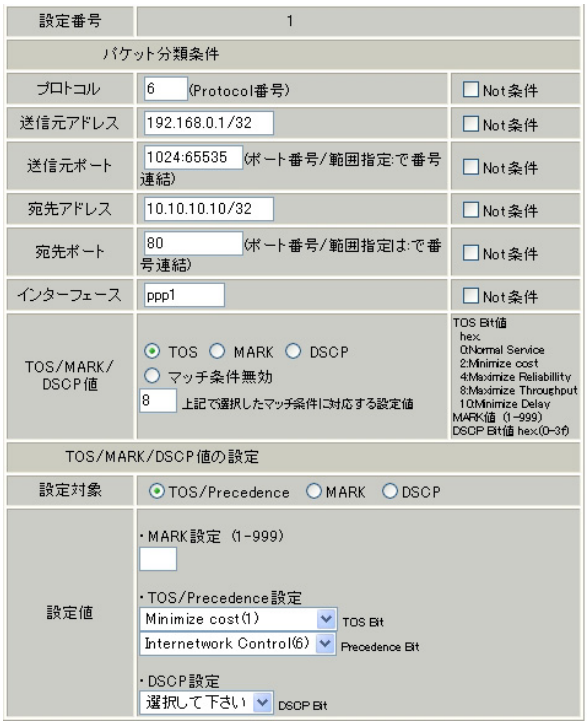
○ Marking 情報によるフィルタ
MARK 値によって CLASS 分けをおこなうときにチェックします。以下、「Mark 値」欄にマッチ条件となる Mark 値を指定します。PQ でフィルタをおこなうときは Marking 情報によるもののみ有効です。

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

◆「パケット分類設定」

設定を追加するときは「New Entry」をクリックします。



(画面は表示例です)

「ローカルパケット出力時の設定」か「パケット入力時の設定」をクリックして選択します。

[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。

○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」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 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

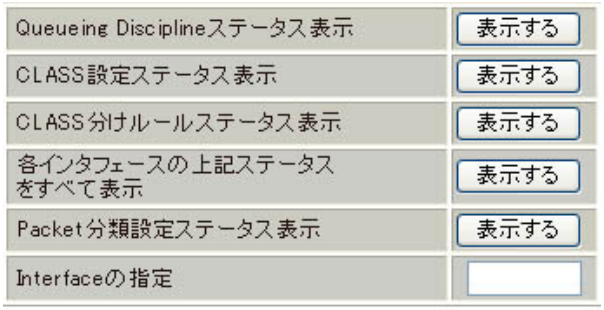
設定対象で選択したものについて、設定値を指定します。

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。

V．ステータスの表示

「ステータス表示」をクリックすると、以下の画面に移ります。



QoS機能の各種ステータスを表示します。

「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。

VI．設定の編集・削除方法

設定をおこなうと、設定内容が一覧で表示されます。

	Filter Type	Description	Priority	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート	TOS値	DSCP値	MARK値	Configure
1	Mark		1								1	Edit, Remove

(「クラス分けフィルタ設定」画面の表示例)

Configure 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。

「Remove」をクリックすると、その設定が削除されます。

VII. 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

VII. 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

VII．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行います。
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。

VII. 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ーフェース
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

VIII. 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。

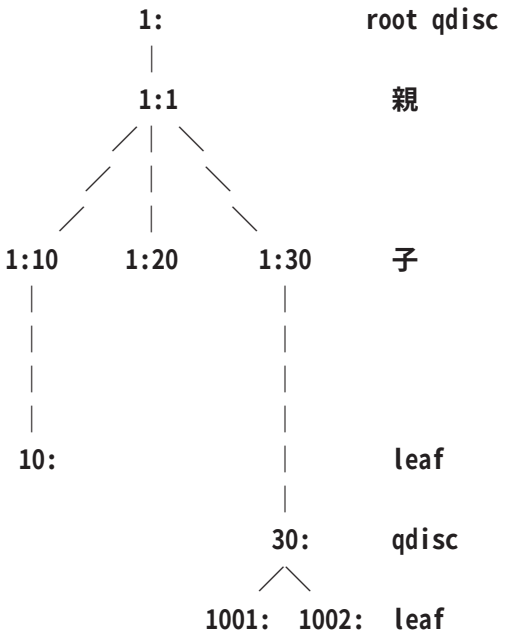
<MAJOR 番号>:<MINOR 番号>

・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)>



IX. 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。

IX. 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。

X. 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 制御を行うことができます。

○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行います。 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 34 章

ゲートウェイ認証機能

1．ゲートウェイ認証機能の設定

「ゲートウェイ認証機能」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。

◆基本設定

[基本設定]

基本設定

本機能	○ 使用しない	○ 使用する
認証	○ しない（URL転送のみ）	◉ する
80/tcp 監視	◉ 行わない	○ 行う
MACアドレスフィルタ	○ 使用しない	◉ 使用する

○本機能
ゲートウェイ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)。
認証を行わないときは「しない」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、強制的にゲートウェイ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

URL		
通常認証後	◉ 行わない（デフォルト）	○ 行う
強制認証後	◉ 行わない（エンドユーザ要求URL）	○ 行う

○ URL
転送先の URL を設定します。

○通常認証後
「はい」を選択すると、ゲートウェイ認証後に「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 転送を行いません。

○強制認証後
「はい」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 転送を行いません。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]

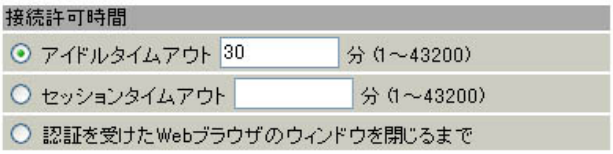
認証方法

◉ ローカル	○ RADIUSサーバ→ローカル	○ RADIUSサーバ

○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→ローカル」外部の RADIUS サーバと通信できず認証できなかった場合に、本装置で認証を行います。
「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．ゲートウェイ認証機能の設定

[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、各ユーザーは再度ゲートウェイ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。

ゲートウェイ認証機能を「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

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			☐

○ユーザー ID・パスワード
ユーザーアカウントを登録します。
ユーザー ID・パスワードには半角英数字が使用できます。空白やコロン(:)は含めることができません。
「削除」をチェックすると、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。

1．ゲートウェイ認証機能の設定

◆RADIUS 設定

「基本設定」において、認証方法を「RADIUS サーバ」に選択した場合にのみ設定します。

○プライマリ / セカンダリサーバ設定
RADIUS サーバの IP アドレス、ポート番号、secret を設定します。プライマリ項目の設定は必須です。セカンダリ項目の設定はなくてもかまいません。

○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”は IP アドレスです。通常は XR-510 の IP アドレスを設定します。

”NAS-Identifier”は任意の文字列を設定します。半角英数字が使用できます。

○アイドルタイムアウト
○セッションタイムアウト
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。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。

Idle-Timeout：アイドルタイムアウト
Ascend-Maximum-Time：セッションタイムアウト
Ascend-Idle-Limit：アイドルタイムアウト

※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。

第 34 章 ゲートウェイ認証機能

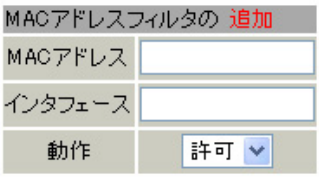
Ⅰ．ゲートウェイ認証機能の設定

◆MAC アドレスフィルタ

ゲートウェイ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 パケットの転送が行われると、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。

○インターフェース
フィルタリングをおこなうインターフェース名を入力します（任意で指定）。インターフェース名については、本マニュアルの「付録 A」をご覧ください。

○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。

MACアドレス	インタフェース	動作	設定変更	
00:01:02:03:04:05	eth0	許可	編集	削除

設定の編集には「編集」を、削除するには「削除」をクリックしてください。

1．ゲートウェイ認証機能の設定

◆フィルタ設定

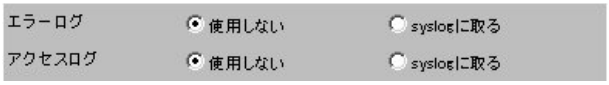
ゲートウェイ認証機能を有効にすると外部との通信は認証が必要となりますが、フィルタ設定によって認証を必要とせずに通信可能にできます。特定のポートだけはつねに通信できるようにしたいといった場合に設定します。

設定画面「フィルタ設定」をクリックします。
”**「フィルタ設定」のゲートウェイ認証設定フィルタ設定画面 にて設定してください。**”というメッセージが表示されたらリンクをクリックして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、ゲートウェイ認証機能によらず、通信可能になります(設定方法については「第 27 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

ゲートウェイ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 ： ゲートウェイ認証時のログインエラーを出力します。
・アクセスログ ： ゲートウェイ認証時のアクセスログを出力します。

<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．ゲートウェイ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

ゲートウェイ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

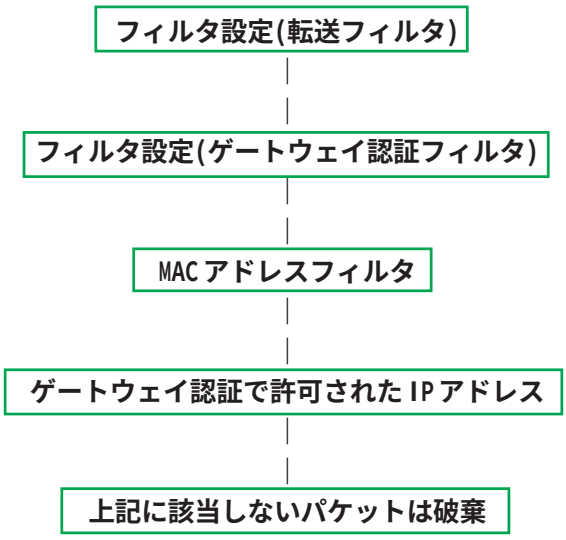
認証方法が「ローカル」の場合、HTTP Basic 認証を使って認証されます。
「RADIUS サーバ」の場合は、PAP で認証要求を送信します。

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) が行われます

III. ゲートウェイ認証の制御方法について

ゲートウェイ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。



ゲートウェイ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、ゲートウェイ認証よりも優先してそのフィルタが参照されてしまい、ゲートウェイ認証が有効に機能しなくなる恐れがあります。

ゲートウェイ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 35 章

検疫フィルタ機能

検疫フィルタ機能の設定

本装置は Windows サーバ上で稼動する「XR 検疫管理サービス」プログラムからの外部指示に基づき、フィルタルールを更新する機能を持っています。検疫フィルタの全体動作概要については「XR 検疫管理サービス」の付属ドキュメントをご覧ください。

Web 設定画面「検疫フィルタ設定」をクリックして設定をします。

◆検疫フィルタ設定

検疫フィルタ	○使用しない ◉使用する
Log	○使用しない ◉使用する
ユーザ	demo
パスワード	demo

○検疫フィルタ
検疫フィルタ機能を使う場合は「使用する」を選択します。
検疫フィルタ機能を「使用する」にした場合、フィルタのデフォルトポリシーは DROP に変更されます。いずれかのフィルタ設定で明示的に許可されていない通信パケットは破棄されます。

○ Log
検疫フィルタ関連のログ情報を記録する場合には「使用する」を選択します。ログ情報には検疫フィルタルールの追加削除の記録や、検疫フィルタにより破棄されたパケットなどが記録されます。

○ユーザ
検疫フィルタ機能に外部からアクセスするための管理用のユーザ名を指定します。「XR 検疫管理サービス」側の設定と一致している必要があります。

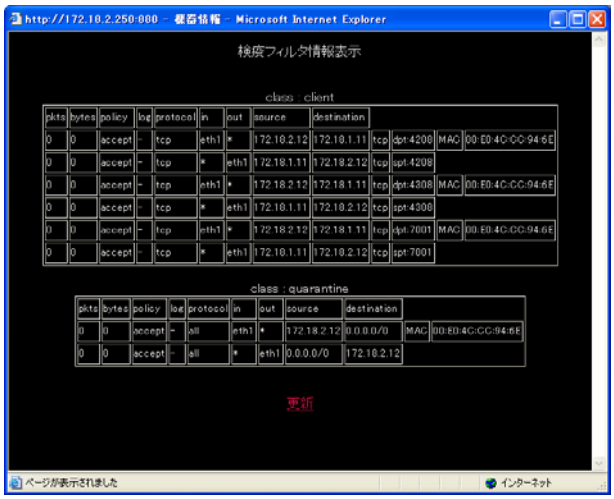
○検疫フィルタ
検疫フィルタ機能に外部からアクセスするための管理用のパスワードを指定します。「XR 検疫管理サービス」側の設定と一致している必要があります。

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。以降「XR 検疫管理サービス」からの指示に基づきフィルタルールが追加削除されるようになります。

◆管理機能

現在設定されている検疫フィルタルールの確認および削除をおこなうことができます。

○表示
表示ボタンを押すことで、現在「XR 検疫管理サービス」の指示に基づいて設定されているフィルタルールが表示されます。



上段が登録済みの PC を検疫サーバに接続するためのルールになります。下段が検疫に合格した PC の通信を許可するルールになります。

○削除
削除ボタンを押すことで設定されている全ての検疫フィルタルールが削除されます。

※ゲートウェイ認証機能の 80/tcp 監視および URL 転送と併用する場合、以下の動作となります。
「ゲートウェイ認証フィルタ」の設定に合致する通信は「ゲートウェイ認証フィルタ」が優先されて適用されます。URL 転送はされません。
「転送フィルタ」の設定に合致する通信のうち TCP80 番ポート宛のものはフィルタが適用されず、URL 転送されます。

第 36 章

ネットワークテスト

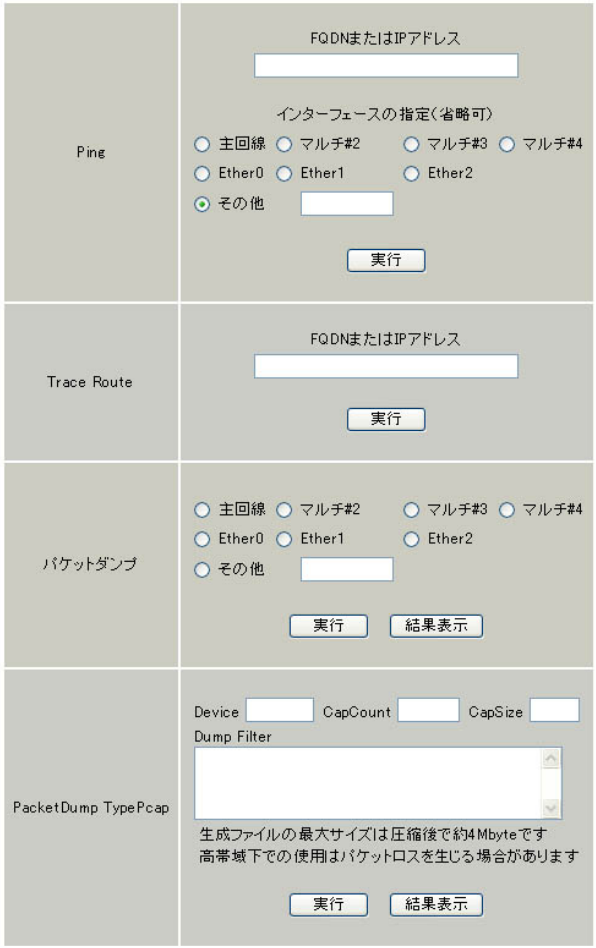
ネットワークテスト

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
- traceroute 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。



(画面は XR-540)

○ping テスト

指定した相手に本装置から Ping を発信します。FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力して「実行」をクリックします。

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=49.5 ms
64 bytes from 211.14.13.66: icmp_seq=1 ttl=52 time=65.7 ms
64 bytes from 211.14.13.66: icmp_seq=2 ttl=52 time=11.7 ms
64 bytes from 211.14.13.66: icmp_seq=3 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=4 ttl=52 time=68.0 ms
64 bytes from 211.14.13.66: icmp_seq=5 ttl=52 time=58.3 ms
64 bytes from 211.14.13.66: icmp_seq=6 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=7 ttl=52 time=71.4 ms
64 bytes from 211.14.13.66: icmp_seq=8 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=9 ttl=52 time=11.8 ms

--- 211.14.13.66 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 11.7/37.3/71.4 ms
```

○ traceroute 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。ping と同様に、FQDN もしくは IP アドレスを入力して「実行」をクリックします。

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=12.4 ms

--- 211.14.13.66 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.4/12.4/12.4 ms
traceroute to 211.14.13.66 (211.14.13.66), 30 hops max, 40 byte packets
 1  192.168.120.15 (192.168.120.15)  1.545 ms  2.253 ms  1.607 ms
 2  192.168.100.50 (192.168.100.50)  2.210 ms  4.955 ms  2.309 ms
 3  172.17.254.1 (172.17.254.1)  8.777 ms  21.189 ms  13.946 ms
 4  210.135.192.108 (210.135.192.108)  8.205 ms  8.953 ms  9.310 ms
 5  210.135.208.34 (210.135.208.34)  35.538 ms  19.923 ms  14.744 ms
 6  210.135.208.10 (210.135.208.10)  41.641 ms  40.476 ms  63.293 ms
 7  210.171.224.115 (210.171.224.115)  43.948 ms  27.255 ms  36.767 ms
 8  211.14.3.233 (211.14.3.233)  36.861 ms  33.890 ms  37.679 ms
 9  211.14.3.148 (211.14.3.148)  36.865 ms  47.151 ms  18.491 ms
10  211.14.3.105 (211.14.3.105)  53.573 ms  13.889 ms  50.057 ms
11  211.14.2.193 (211.14.2.193)  33.777 ms  11.380 ms  17.282 ms
12  * * *
13  211.14.12.249 (211.14.12.249)  19.692 ms !X *  15.213 ms !X
```

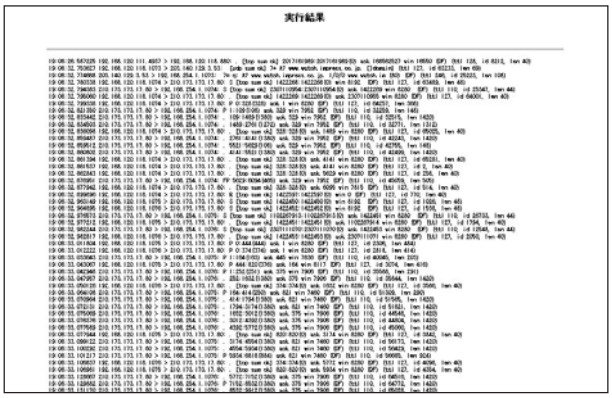
ping・traceroute テストで応答メッセージが表示されない場合は、DNS で名前解決ができていない可能性があります。その場合はまず、IP アドレスを直接指定してご確認ください。

ネットワークテスト

○パケットダンプ

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ーフェースを選択して「実行」をクリックします。その他を選択し、直接インタフェース名を指定することもできます。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。

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を指定してください(「gre1」や「ipsec0」など)

○ PacketDump TypePcap

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」をご参照ください。

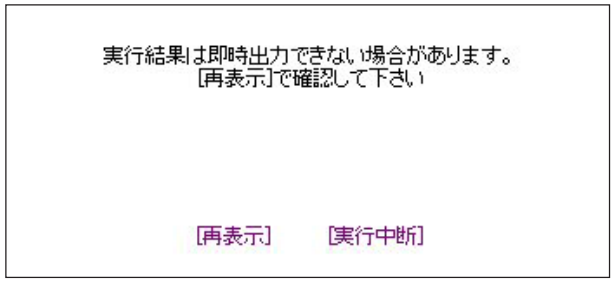
「CapCount」：パケットダンプの取得数を指定します。1 ～ 99999 の間で指定します。

「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。

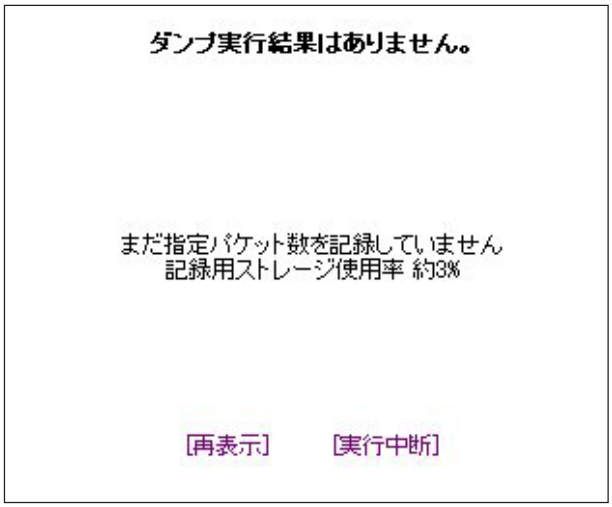
上記項目を入力後、「実行」ボタンでパケットダンプを開始します。

パケットダンプを開始したときの画面表示

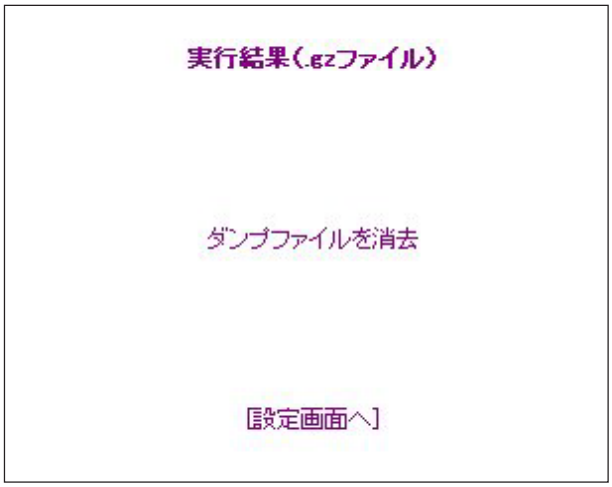


ネットワークテスト

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。



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。

[PacketDump TypePcap の注意点]

本装置のインタフェース名については、「付録 A」をご参照ください。

第 37 章

各種システム設定

システム設定

「システム設定」ページでは、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
- 本体の再起動
- セッションライフタイムの設定
- 設定画面の設定
- ISDN 設定(※ XR-540 のみ)
- オプションCFカード(※ XR-510にはありません)
- ARP Filter 設定

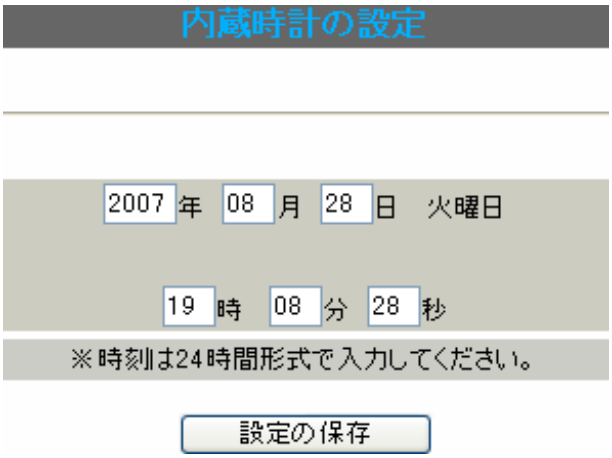
実行方法

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。

「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

「ログの表示」をクリックして表示画面を開きます。

本装置のログが全てここで表示されます。

「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。

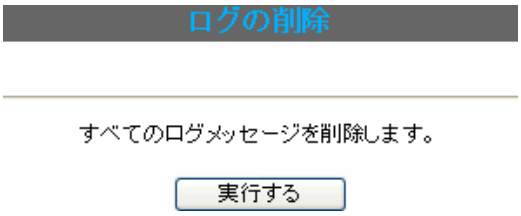
「攻撃検出機能」を使用している場合は、そのログも併せてここで表示されます。

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。

◆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。

「ログの削除」をクリックして画面を開きます。



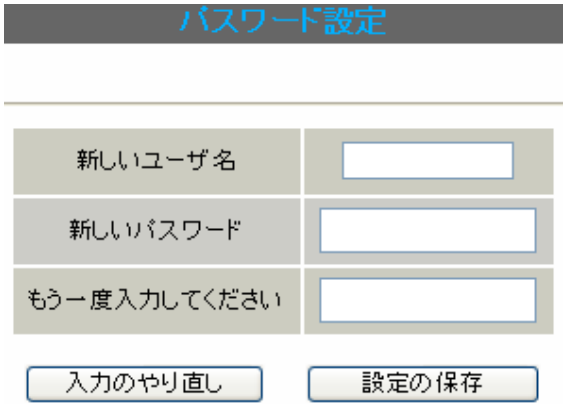
「実行する」ボタンをクリックすると、保存されているログが**全て削除**されます。

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ー名、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。

「パスワードの設定」をクリックして設定画面を開きます。



新しいユーザー名とパスワードの設定ができます。
○ユーザー名
半角英数字で 1 から 15 文字まで設定可能です。

○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。

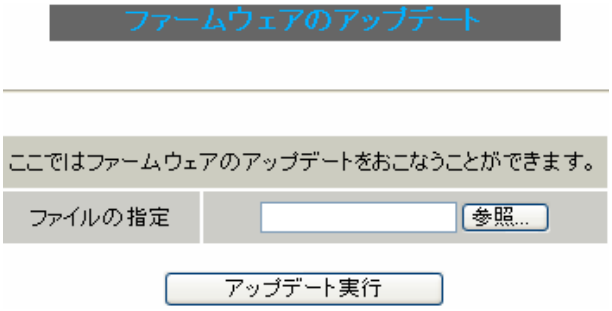
入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。

次回のログインからは、新しく設定したユーザー名とパスワードを使います。

◆ファームウェアのアップデート

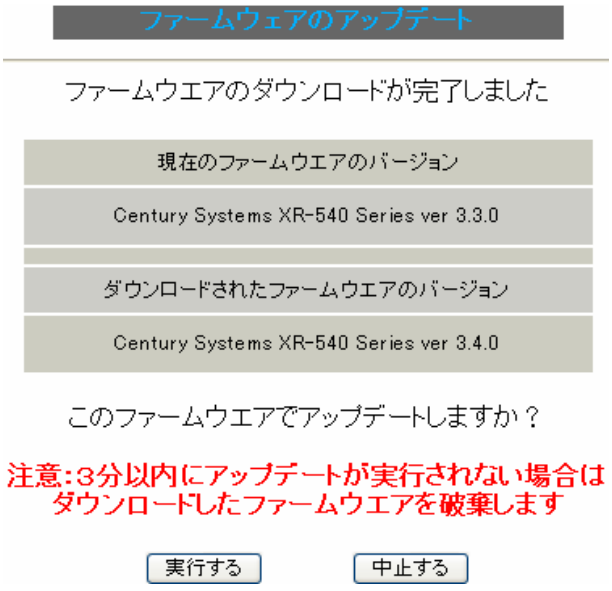
本装置は、ブラウザ上からファームウェアのアップデートをおこないます。

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。

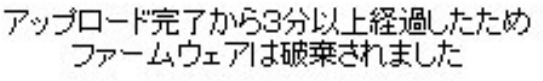


2 「参照」ボタンを押して、弊社ホームページからダウンロードしてきたファームウェアファイルを選択し、「アップデート実行」ボタンを押してください。

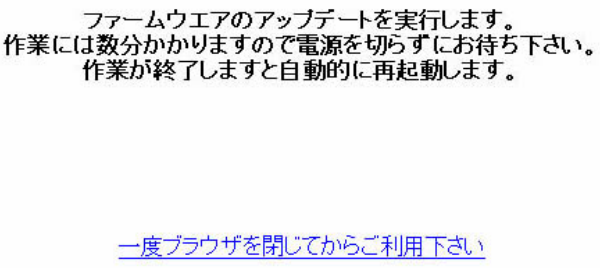
3 その後、ファームウェアを本装置に転送します(転送が終わるまではしばらく時間がかかります)。転送完了後に、以下のようなアップデートの確認画面が表示されますので、バージョン等が正しければ「実行する」をクリックしてください。



上記画面が表示されたままで 3 分間経過すると、以下の画面が表示され、アップデートが実行されません。



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、本体の STATUS 1 (赤)が点滅します。この間は、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後に本装置が自動的に再起動されて、アップデートの完了です。

アップデート実行中は、本装置やインターネットへのアクセス等は行なわないでください。アップデート失敗の原因となることがあります。

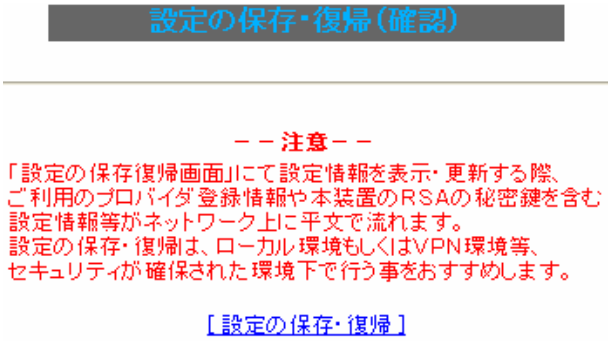
システム設定

◆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

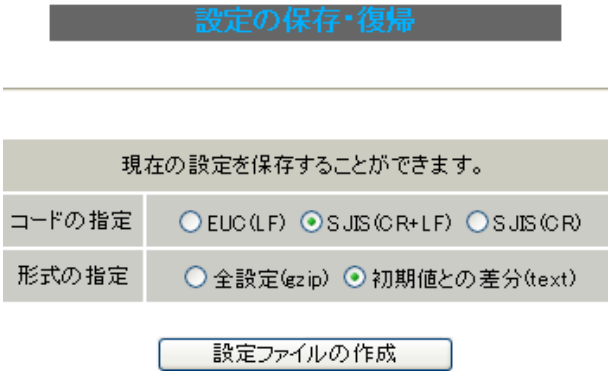
「設定の保存・復帰」をクリックして画面を開きます。



上記のようなメッセージが表示されてから、「設定の保存・復帰」のリンクをクリックします。

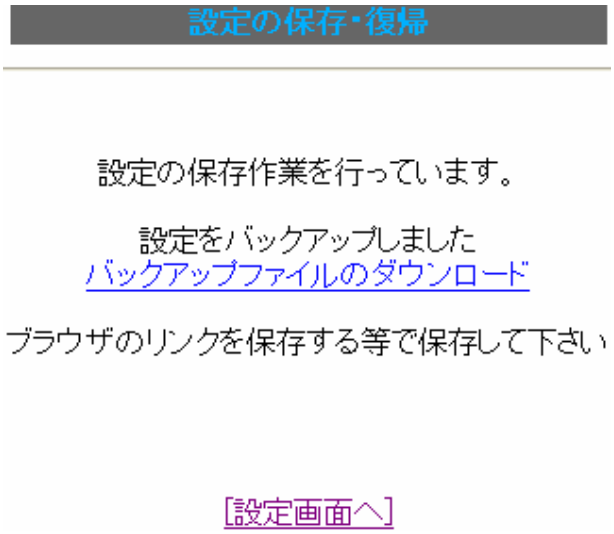
[設定の保存]

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。



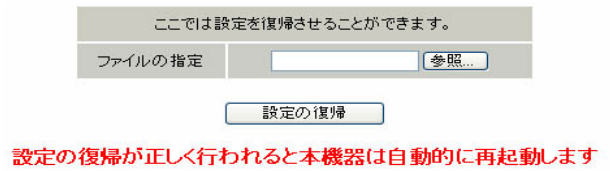
「全設定」を選択すると、本装置のすべての設定をgzip形式で圧縮して保存します。
「初期値との差分」を選択すると、初期値と異なる設定のみを抽出して、テキスト形式で保存します。このテキストファイルの内容を直接書き換えて設定を変更することもできます。

選択したら「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。



[設定の復帰]

上記項目から「参照」をクリックして、保存しておいた設定ファイルを選択します。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。



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。

－－注意－－

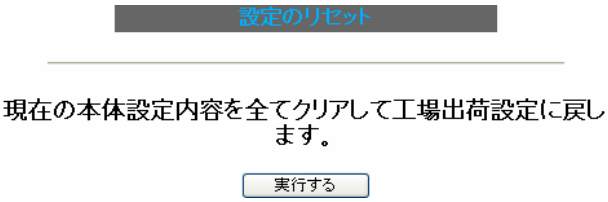
「設定の保存復帰画面」にて設定情報を表示・更新する際、ご利用のプロバイダ登録情報や本装置のＲＳＡの秘密鍵を含む設定情報等がネットワーク上に平文で流れます。設定の保存・復帰は、ローカル環境もしくはＶＰＮ環境等、セキュリティが確保された環境下で行う事をおすすめします。

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。

「設定のリセット」をクリックして画面を開きます。



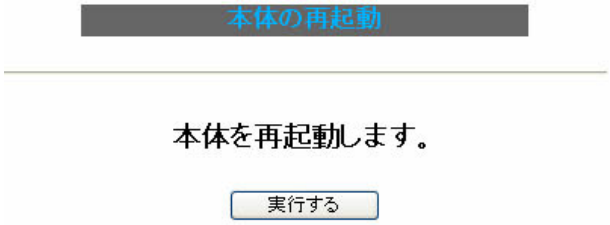
「実行する」ボタンをクリックするとリセットが実行され、本体の全設定が工場出荷設定に戻ります。

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。

◆本体再起動

本装置を再起動します。設定内容は変更されません。

「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

◆セッションライフタイムの設定

XR 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。

「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。

（画面は XR-540 です）

○ 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。

○セッション最大数
XR で保持できる NAT/IP マスカレードのセッション情報の最大数を設定します。UDP/UDPstream/TCP のセッション情報を合計した最大数になります。
4096 ～ 16384 の間で設定します。
XR-510 の初期設定は 4096 です。
XR-540、XR-730 での初期設定は 8192 です。

なお、XR 内部で保持しているセッション数は、周期的に syslog に表示することができます。詳しくは**「第 18 章 SYSLOG 機能」のシステムメッセージの項を参照してください。**

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。

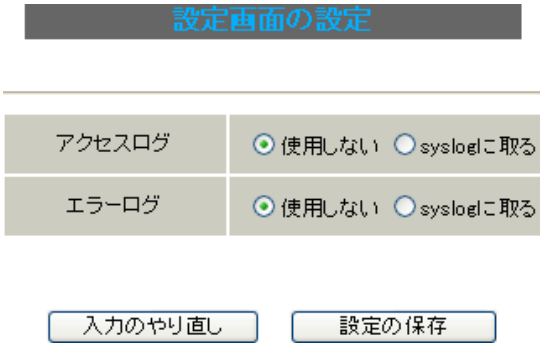
システム設定

◆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。

実行方法

「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。

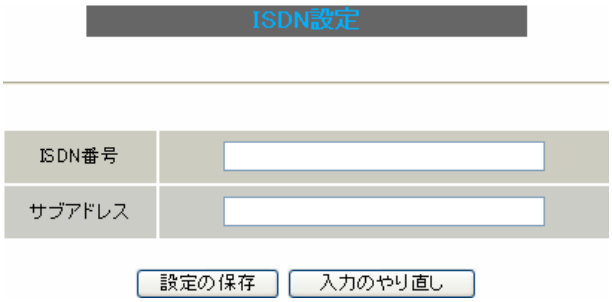
アクセスログ・エラーログは、「syslog」サービスの設定にしたがって出力されます。

◆ ISDN 設定(※ XR-540 のみ)

BRI を使った ISDN 回線接続を行なうときの「ISDN 発信者番号」を設定します。

実行方法

「ISDN の設定」をクリックして画面を開きます。



○ ISDN 番号
ISDN 発信者番号を入力します。

○サブアドレス
サブアドレスを指定します。

「設定の保存」をクリックします。

システム設定

◆オプション CF カード (※ XR-510 にはありません)

XR-540 シリーズにオプションで用意されているコンパクトフラッシュ(CF)カードを装着している場合の、CF カードの操作を行ないます。
ここでは以下の設定を行うことができます。

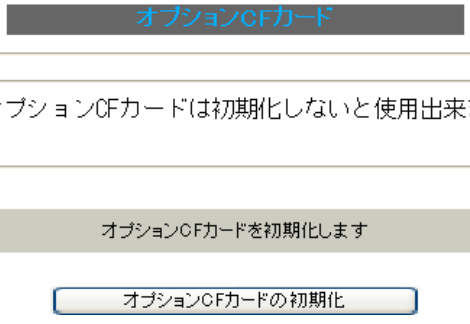
- CF カードの初期化
- CF カードへの設定のバックアップ

実行方法

コンパクトフラッシュ(CF)カードを装着してから「オプション CF カード」をクリックして画面を開きます。
画面には、装着した CF カードの情報が表示されます。

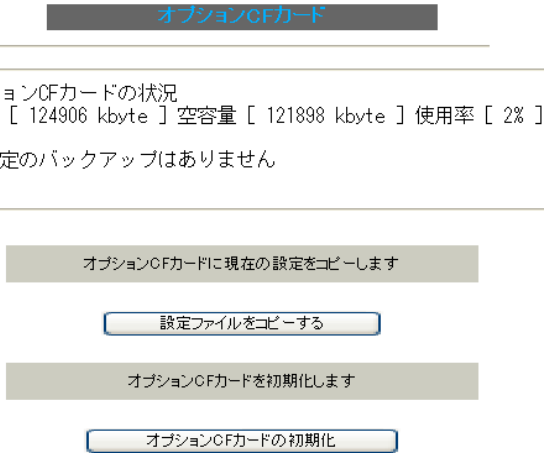
○CF カードの初期化

はじめて CF カードを装着したときは、必ず CF カードを初期化する必要があります。初期化を行わないと CF カードを使用できません。
CFカードを初期化するときは「オプションCFカードの初期化」をクリックします。

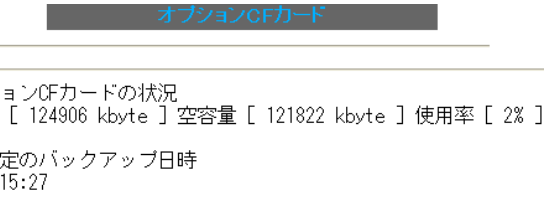


○CF カードへの設定のバックアップ

設定のバックアップをCFカード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。



設定のバックアップがある場合は、画面上部に、装着したCFカードの状況とバックアップ情報が表示されます。



[CF カードの取り扱いについて]
オプション CF カードは、XR-540、XR-730 前面パネルの CF カードスロットに挿入してください。

XR-540 では、
- CF カードを挿入され動作しているときは本体前面の STATUS(橙)LED が点灯します。
- CF カードが使用可能状態になると ACTIVE(緑)LED ランプが点灯します。

XR-730 では、CF LED(緑)ランプが点灯します。

**CF カードを本装置から取り外すときは、必ず本体前面の CF カードスロット横にある「RELEASE」ボタンを数秒押し続けてください。CF ランプが消灯します。
消灯を確認いただきましたら、CF カードは安全に取り外せます。**

上記の手順以外で CF カードを取り扱った場合、本装置および CF カードが故障する場合がありますのでご注意ください。

システム設定

◆ARP filter 設定

ARP filter 設定をおこないます。

実行方法

「ARP filter 設定」をクリックして画面を開きます。

ARP filter を有効にすると、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、受信したそれぞれ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。

第 38 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。

- **インターフェース情報**
  各インターフェースの 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**
  直接接続、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**
  デフォルトゲートウェイ情報です。

- **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「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。

（画面は XR-540）

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 39 章

詳細情報表示

第 39 章 詳細情報表示

各種情報の表示

ここではルーティング情報や各種サービス情報をまとめて表示することができます。
以下の項目を表示します。

- **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。

- **IPv6 ブリッジ情報**
  取得できる項目は、実行状態、使用しているインターフェイス名、転送できたパケットカウントの３項目です。また、取得できる値のフォーマットは以下の通りです。

```
IPv6 Bridge:              [On/Off]
Bridging Port:            [ethx], [ethx]
Bridging Packet Count: 0 - 2^32-1
```

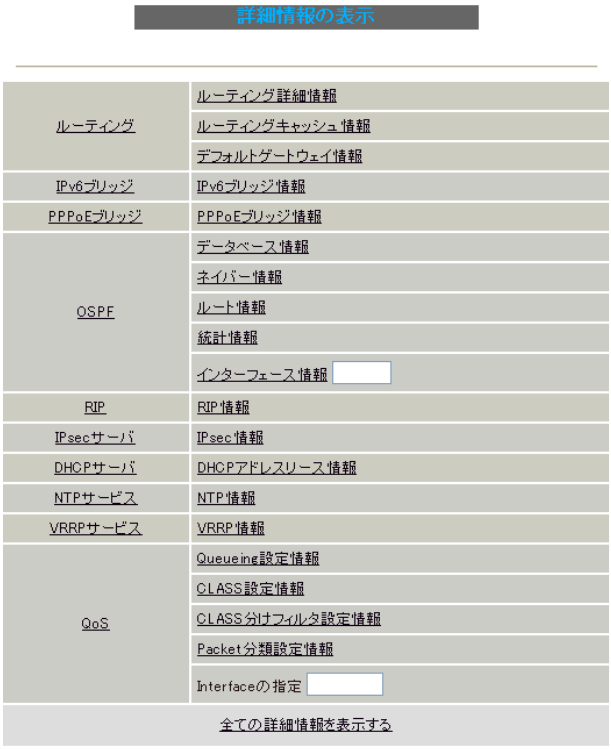
例)

```
IPv6 Bridge:              On
Bridging Port:            eth0, eth1
Bridging Packet Count: 31
```

- **PPPoE ブリッジ情報**
- **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**

実行方法

Web 設定画面「詳細情報表示」をクリックすると、次の画面が表示されます。



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。なお、「OSPF のインターフェース情報」および QoS の各情報については、ボックス内に表示したいインターフェース名を入力してください。

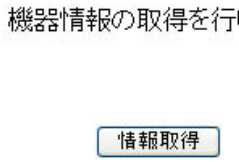
一番下の「全ての詳細情報を表示する」をクリックすると、全ての機能の全ての項目についての情報が一括表示されます。

第 40 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。



「情報取得」をクリックします。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 37 章　各種システム設定
　◆ログの表示 / 削除」をご覧ください。

○設定ファイル
詳細は、「第 37 章　各種システム設定
　◆設定の保存・復帰」をご覧ください。

○本体の機器情報
詳細は、「第 38 章　情報表示」をご覧ください。

第41章

運用管理設定

INIT ボタンの操作

本装置の背面にある「INIT ボタン」を使用することで、以下の操作ができます。

- 本装置の設定を一時的に初期化する (ソフトウェアリセット)
- オプション CF カードに保存された設定で起動する（※ XR-510 にはありません）

◆本装置の設定を初期化する

＜XR-510 の場合＞

INIT ボタンを押したまま電源切断→電源投入し、電源投入後も 5 秒ほど INIT ボタンを押しつづけると、XR-510 は工場出荷時の設定で再起動します。

ただしこのとき、工場出荷時の設定での再起動前の設定は別の領域に残っています。

この操作後にもう一度再起動すると、それまでの設定が復帰します。工場出荷時の設定で戻したあとに設定を変更していれば、変更した設定が反映された上で復帰します。

＜XR-540、XR-730 の場合＞

1 **本装置が停止状態になっていることを確認します。**

2 本体背面にある「INIT」ボタンを押しながら、電源スイッチをオンにします。INIT ボタンは押したままにしておきます。

3 本体前面の「STATUS1(赤) LED」ランプが点灯、他の STATUS ランプが消灯するまで INIT ボタンを押し続けます。

4 3 状態になったら INIT ボタンを放します。その後、XR-540、XR-730 が工場出荷設定で起動します。

設定を完全にリセットする場合は、「システム設定」→「設定のリセット」でリセットを実行してください。

◆ＣＦカードの設定で起動する (※ XR-510 にはありません)

1 XR-540、XR-730 にオプション CF カードが挿入されていることを確認します。

2 本体背面にある「INIT」ボタンを押しながら、電源スイッチをオンにします。
INIT ボタンは押したままにしておきます。

3 本体前面にある、XR-540「STATUS(橙) LED」、XR-730「CF LED(緑)」の点滅が止まるまで INIT ボタンを押し続けます。

4 点滅が止まったら INIT ボタンを放します。その後、XR-540、XR-730 が CF カードに保存されている設定内容で起動します。

補足：バージョンアップ後の設定内容について

本装置をバージョンアップしたとき、CF カード内の設定ファイルは旧バージョンの形式で保存されたままです。

ただしバージョンアップ後に本装置を電源 OFF→CF カードの設定内容で起動しても、旧バージョンの設定内容を自動的に新バージョン用に変換して起動できます。

CF カード内の設定を新バージョン用にするためには、新バージョンで CF カードの設定から起動し、あらためて CF カードへ設定の保存を行ってください。

付録 A

インターフェース名一覧

付録 A

インターフェース名一覧

本装置は、以下の設定においてインターフェース名を直接指定する必要があります。

- OSPF 機能
- DHCP サーバ機能
- 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
- 仮想インターフェース機能
- QoS 機能
- ネットワークテスト

本装置のインターフェース名と実際の接続インターフェースの対応付けは次の表の通りとなります。

XR-510

eth0	Ether0ポート
eth1	Ether1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
ppp6	リモートアクセス回線
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
gre<n>	gre (<n>は設定番号)
eth0.<n>	eth0上のVLANインターフェース (<n>はVLAN ID)
eth1.<n>	eth1上のVLANインターフェース
eth0:<n>	eth0上の仮想インターフェース (<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インターフェース
br<n>	Bridgeインターフェース (<n>は設定番号)

表左：インターフェース名
表右：実際の接続デバイス

付録 A

インターフェース名一覧

XR-540

eth0	Ether0ポート
eth1	Ether1ポート
eth2	Ether2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
ppp6	アクセスサーバ(シリアル接続)
ppp7	アクセスサーバ(BRI接続)
ppp8	アクセスサーバ(BRI接続)
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
gre<n>	gre (<n>は設定番号)
eth0.<n>	eth0上のVLANインターフェース (<n>はVLAN ID)
eth1.<n>	eth1上のVLANインターフェース
eth2.<n>	eth2上のVLANインターフェース
eth0:<n>	eth0上の仮想インターフェース (<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インターフェース
eth2:<n>	eth2上の仮想インターフェース
br<n>	Bridgeインターフェース (<n>は設定番号)
dummy0	Dummy Interface

XR-730

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
ppp6	リモートアクセス回線
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インターフェース (<n>はVLAN ID)
eth1.<n>	eth1上のVLANインターフェース
eth2.<n>	eth2上のVLANインターフェース
eth3.<n>	eth3上のVLANインターフェース
eth0:<n>	eth0上の仮想インターフェース (<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インターフェース
eth2:<n>	eth2上の仮想インターフェース
eth3:<n>	eth3上の仮想インターフェース
br<n>	Bridgeインターフェース (<n>は設定番号)
dummy0	Dummy Interface

表左：インターフェース名
表右：実際の接続デバイス

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（※ XR-510にはありません）	192.168.2.254/255.255.255.0
ETHER3ポート（※ XR-730のみ）	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	無効
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）
ブリッジフィルタ機能	設定なし
スケジュール機能(※ XR-540のみ)	設定なし
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
ゲートウェイ認証機能	無効
検疫フィルタ機能	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
　電話 0422-37-8926
　受付時間　10:00～17:00　(土日祝祭日、及び弊社の定める休日を除きます)
・FAX　0422-55-3373
・e-mail　support@centurysys.co.jp
・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「第 38 章 情報表示」をご覧ください)
・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ください。
・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ください。
・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、是非ご覧ください。
XR-510 製品サポートページ　http://www.centurysys.co.jp/support/xr510c.html
XR-540 製品サポートページ　http://www.centurysys.co.jp/support/xr540c.html
XR-730 製品サポートページ　http://www.centurysys.co.jp/support/xr730c.html

◆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。保証期間をすぎたもの、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ください。保証規定については、同梱の保証書をご覧ください。

XR-510/C XR-540/C XR-730/C ユーザーズガイド v3.4.0対応版
2007年09月版
発行 センチュリー・システムズ株式会社