Internet VPN 対応 BROADBAND GATE

FutureNet XR-440/C

ユーザーズガイド

Ver1.7.8 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 XP、Windows Vista

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

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

ご使用にあたって

安全にお使いいただくために

このたびは、FutureNet シリーズ（以下「本製品」）をお買い上げ頂き、誠にありがとうございます。

ここでは、お使いになる方および周囲の人への危害や財産への損害を未然に防ぎ、本製品を安全に正しくお使い頂くための注意事項を記載していますので、必ずお読み頂き、記載事項をお守り下さい。

また、お読みになった後は、大切に保管して下さい。

絵表示の意味

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想定される内容

注意 この表示を無視して、誤った取り扱いをすると、人が障害を負う可能性及び物的損害の発生が想定される内容

◆FutureNet シリーズ共通

危険 万一、発煙・異常な発熱・異臭・異音等の異常が出た場合は、すぐに、本製品に接続する外部電源装置の電源を切り、使用を中止して下さい。
そのままご使用されると、火災・感電の原因になります。

危険 本製品内部へ異物（金属片・水・液体）を入れないで下さい。

危険 本製品を以下の様な場所で使用したり、放置しないで下さい。
- 直射日光の当たる場所、高温になる場所
- 湿気の多い場所やほこりの多い場所、振動・衝撃の加わる場所
- 温度変化の激しい場所、強い電波・磁界・静電気・ノイズが発生する場所

危険 本製品および電源コード・接続ケーブルは、小さなお子さまの手の届かない場所に設置して下さい。

危険 本製品の仕様で定められた使用温度範囲外では使用しないで下さい。

危険 通気孔のある製品は、本体を重ねたり、物を置いたり、立て掛けたりして通気孔を塞がないで下さい。

危険 本製品を濡らしたり、水がかかる恐れのある場所で使用しないで下さい。
また、結露する様な場所で使用しないで下さい。
結露してしまった場合、十分に乾燥させてからご使用下さい。

危険 本製品は日本国内仕様です。
国外で使用された場合、弊社は責任を一切負いかねます。

危険 本製品の取付け・取外しは、必ず本体と外部電源装置の両方の電源を切ってから行なって下さい。
また、使用中は濡れた手で本製品に触れないで下さい。

危険 本製品の分解、改造は絶対にしないで下さい。
分解したり、改造した場合、保証期間であっても有料修理となる場合がありますので、修理は弊社サポートデスクにご依頼下さい。
また、法令に基づく承認を受けて製造されている製品を、電気的・機械的特性を変更して使用する事は、関係法令により固く禁じられています。

危険 近くに雷が発生した時は、本製品の電源をコンセントなどから抜いて、ご使用をお控え下さい。
また、落雷による感電を防ぐため、本製品やケーブルに触れないで下さい。

危険 本製品の接続ケーブルの上に重量物を載せないで下さい。
また、熱器具のそばに配線をしないで下さい。

危険 本製品の電源コードは、付属の物をご使用下さい。
また、以下の点に注意してお取扱い下さい。
- 物を載せたり、熱器具のそばで使用しないで下さい。
- 引張ったり、ねじったり、折り曲げたりしないで下さい。
- 押し付けたり、加工をしたりしないで下さい。

危険 本製品の電源コードをコンセント等から抜く時は、必ずプラグ部分を持って抜いて頂き、直接コードを引張らないで下さい。

ご使用にあたって

危険 本製品の電源コードが傷ついたり、コンセント等の差込みがゆるい時は使用しないで下さい。

危険 本製品に電源コードが付属されている場合は、必ず付属の物をご使用下さい。
また、付属されている電源コードは、本製品の専用品です。他の製品などには絶対に使用しないで下さい。

危険 本製品の仕様で定められた電源以外には、絶対に接続しないで下さい。
(例：AC100V ± 10V(50/60Hz)，DC 電源など)

危険 電源プラグは、絶対に濡れた手で触れないで下さい。
また、電源プラグにドライバーなどの金属が触れない様にして下さい。

危険 電源プラグは、コンセントの奥まで確実に差し込んで下さい。
また、分岐ソケットなどを使用したタコ足配線にならない様にして下さい。

危険 電源プラグの金属部分およびその周辺にほこり等の付着物がある場合には、乾いた布でよく拭き取ってからご使用下さい。
(時々、電極間にほこりやゴミがたまっていないかご点検下さい)

注意 ご使用の際は取扱説明書に従い、正しくお取り扱い下さい。

注意 万一の異常発生時に、すぐに、本製品の電源および外部電源装置の電源を切れる様に本製品周辺には、物を置かないで下さい。

注意 人の通行の妨げになる場所には設置しないで下さい。

注意 ぐらついた台の上や、傾いたところなど不安定な場所に設置しないで下さい。
また、屋外には設置しないで下さい。

注意 本製品への接続は、コネクタ等の接続部にほこりやゴミなどの付着物が無い事を確認してから行なって下さい。

注意 本製品のコネクタの接点などに、素手で触れないで下さい。

注意 取扱説明書と異なる接続をしないで下さい。
また、本製品への接続を間違えない様に十分注意して下さい。

注意 本製品にディップスイッチがある場合、ディップスイッチの操作は本製品の電源および外部電源装置の電源を切った状態で行なって下さい。
また、先端の鋭利なもので操作したり、必要以上の力を加えないで下さい。

注意 本製品に重い物を載せたり、乗ったり、挟んだり、無理な荷重をかけないで下さい。

注意 本製品をベンジン、シンナー、アルコールなどの引火性溶剤で拭かないで下さい。
お手入れは、乾いた柔らかい布で乾拭きし、汚れのひどい時には水で薄めた中性洗剤を布に少し含ませて汚れを拭取り、乾いた柔らかい布で乾拭きして下さい。

注意 接続ケーブルは足などに引っかからない様に配線して下さい。

注意 本製品を保管する際は、本製品の仕様で定められた保存温度・湿度の範囲をお守り下さい。
また、ほこりや振動の多いところには保管しないで下さい。

注意 本製品を廃棄する時は、廃棄場所の地方自治体の条例・規則に従って下さい。
条例の内容については各地方自治体にお問合せ下さい。

◆AC アダプタを付属する製品の場合

危険 本製品に付属の AC アダプタは AC100V 専用です。AC100V 以外の電圧で使用しないで下さい。

危険 AC アダプタは本製品に付属されたものをご使用下さい。
また、付属された AC アダプタは、本製品以外の機器で使用しないで下さい。

危険 感電の原因になるため、AC アダプタは濡れた手で触れないで下さい。
また、AC アダプタを濡らしたり、湿度の高い場所、水のかかる恐れのある場所では使用しないで下さい。

危険 AC アダプタの抜き差しは、必ずプラグ部分を持って行なって下さい。
また、AC アダプタの金属部分およびその周辺にほこり等の付着物がある場合には、乾いた布でよく拭き取ってからご使用下さい。(時々、電極間にほこりやゴミがたまっていないかご点検下さい)

危険 AC アダプタを保温・保湿性の高いもの（じゅうたん・カーペット・スポンジ・緩衝材・段ボール箱・発泡スチロール等）の上で使用したり、中に包んだりしないで下さい。

パッケージの内容物の確認

本製品のパッケージには以下の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、お買いあ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-440/C 梱包物＞

XR-440/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
LAN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

第1章

XR-440の概要

第１章 XR-440 の概要

Ｉ．XR-440 の特長

XR-440/C(以下、XR-440 または、本装置)には、以下の特徴があります。

◆高速ネットワーク環境に余裕で対応
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。

◆シリアルポートを搭載
XR-440 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 XR-440 を遠隔管理することも可能です。

◆ ISDN 用 BRI ポートを搭載
XR-440 は「ISDN S/T 点ポート」を搭載しています。これにより本装置から直接、もしくは他の ISDN 機器を接続して ISDN 回線に接続できます。
「副回線接続」を使うと、ISDN 回線回線の接続を緊急時のバックアップ回線として運用することもできます。

◆ 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 設定をおこなえます。

◆ 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。

◆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おこなっています。
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。

第 1 章 XR-440 の概要

Ⅰ．XR-440 の特長

◆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。
◆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。

◆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、OSPF 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 ISDN 回線やブロードバンド回線を用いてバックアップする機能を搭載しています。

◆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。

◆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。

◆スケジュール機能
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。

◆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。

◆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。

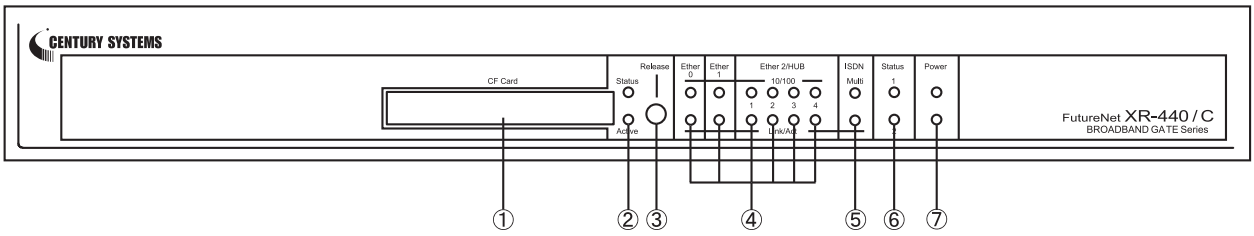
◆ログ機能
XR-440 のログを取得する事ができ、ブラウザ上でログを確認することが可能です。ログを電子メールで送信することも可能です。
また、攻撃検出設定をおこなえば、インターネットからの不正アクセスのログも併せてログに記録されます。

◆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。

◆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。

Ⅱ．各部の名称と機能

◆製品前面



① CF Card 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 Status LED(橙) / Active LED(緑)

CFカードスロットにCFカードが挿入された場合の状態を表示します。

上段「Status LED」(橙)
- 動作しているとき ： ●
- CF カードへのアクセス中 ： ✳ （点滅）
- アクセスがないとき、③ Release 操作実行時、CF カードが未挿入のとき ： ●

下段「Active LED」(緑)
- CF カードが使用可能状態のとき ： ●
- CF カードが挿入されていないとき ： ●
- ③ Release 操作をおこなったとき ： ●

③ 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、②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。

④ Ethernetポート(Ether 0,Ether 1,Ether 2/HUB)
10/100 LED(橙) / Link/Act LED(緑)

各 Ethernet ポートの状態を表示します。

上段「10/100 LED」(橙)
- 10Base-T で接続した場合 ： ●
- 100Base-TX で接続した場合 ： ●

下段「Link/Act LED」(緑)
- LAN ケーブルが正常に接続時 ： ●
- データ通信時 ： ✳ （点滅）

⑤ ISDN (BRI) LED
Multi LED(橙) / Link/Act LED(緑)

本装置のBRIポートを使ってISDN接続をしている場合の状態を表示します。

上段「Multi LED」(橙)
- MP128 接続時 ： ●
- 回線切断時 ： ●

下段「Link/Act LED」(緑)
- BRI ポートを使って ISDN 接続時 ： ●
- 回線切断時 ： ●

⑥ Status 1 LED(橙) / Status 2 LED(緑)

上段「Status 1 LED」(橙)
- 本装置の全サービスが動作開始状態 ： ●
- ファームウェアのアップデート作業中 ： ✳

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。

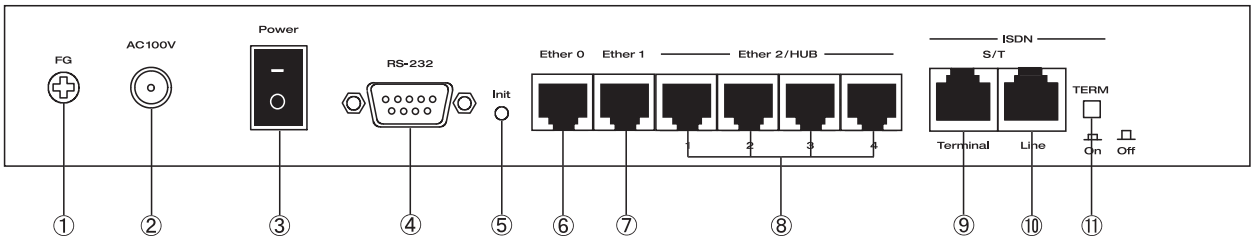
下段「Status 2 LED」(緑)
- PPP/PPPoE 主回線で接続しているとき ： ●
- PPP/PPPoE 主回線で接続していないとき ： ●

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
- 「Status 1 LED」(橙) ： ✳ （点滅）
- 「Status 2 LED」(緑) ： ✳ （点滅）

⑦ Power LED(緑)
- 本装置に電源が投入されているとき ： ●

Ⅱ．各部の名称と機能

◆製品背面



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 AC 100V 電源ケーブル

③ Power 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 Ether 0 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。ポートは Auto-MDIX 対応です。

⑦ Eehter 1 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。ポートは Auto-MDIX 対応です。

⑧ Ether 2/HUB 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。ポートは Auto-MDIX 対応です。

⑨ ISDN S/T Terminal ポート
このポートと ISDN 機器を ISDN ケーブルで接続します。

⑩ ISDN S/T 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。

⑪ TERM. スイッチ
「ISDN S/T 点ポート」接続時の終端抵抗の ON/OFF を切替えます。
外部 DSU 機器を接続している場合は、XR-440 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。

III．動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

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

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

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

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

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

◆ソフトウェア環境

・TCP/IP を利用できる OS がインストールされていること。

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

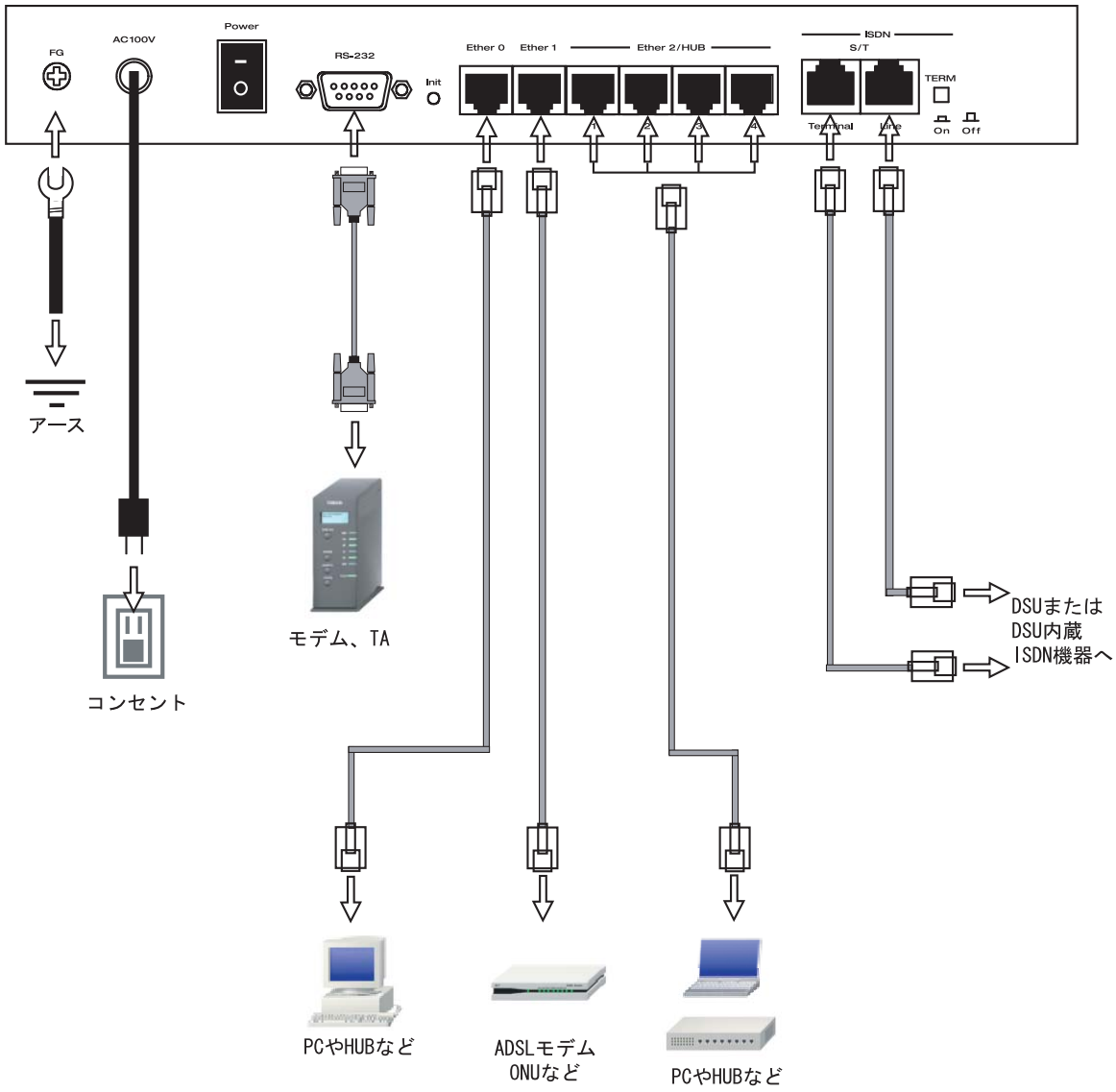
なお、サポートにつきましては、本製品固有の設定項目と本製品の設定に関係する OS 上の設定に限らせていただきます。
OS 上の一般的な設定やパソコンにインストールされた LAN ボード / カードの設定、各種アプリケーションの固有の設定等のお問い合わせについては、サポート対象外とさせていただきますので、あらかじめご了承ください。

第2章

XR-440の設置

XR-440 の設置

XR-440 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。



1 本装置と 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。

2 本装置の背面にある 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 本装置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 本装置の背面にある 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。

本装置の各 Ethernet ポートは Auto-MDIX 対応です。

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、本装置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 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。

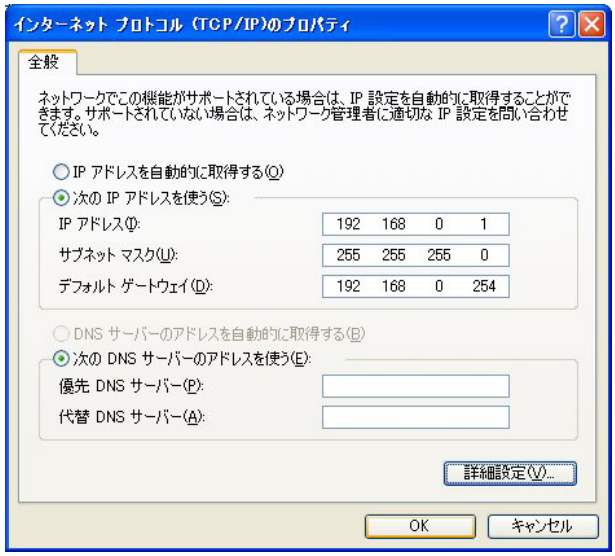
1 「コントロールパネル」→「ネットワーク接続」から、「ローカル接続」を開きます。

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」



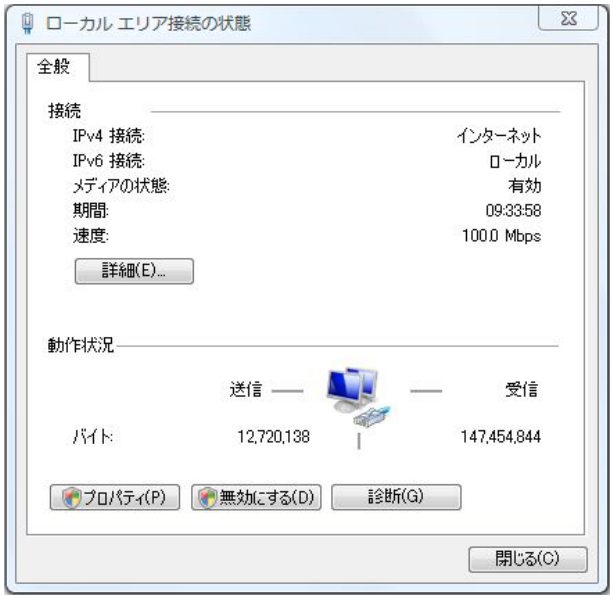
5 最後に OK ボタンをクリックして設定完了です。これで XR-440 へのログインの準備が整いました。

II．Windows Vistaのネットワーク設定

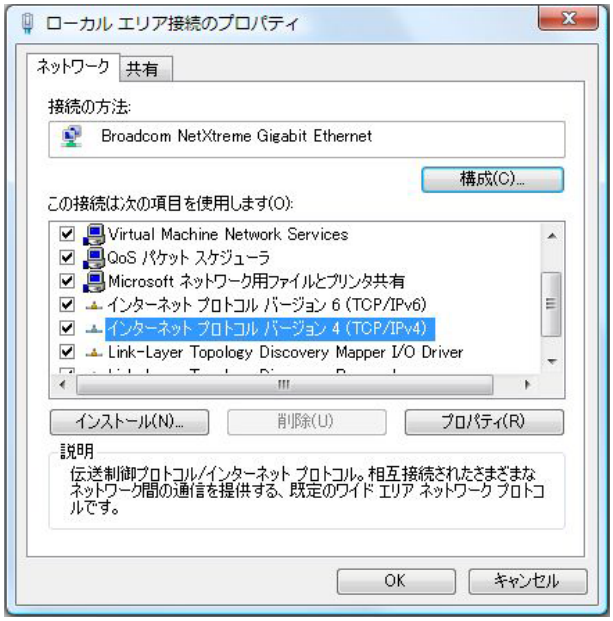
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

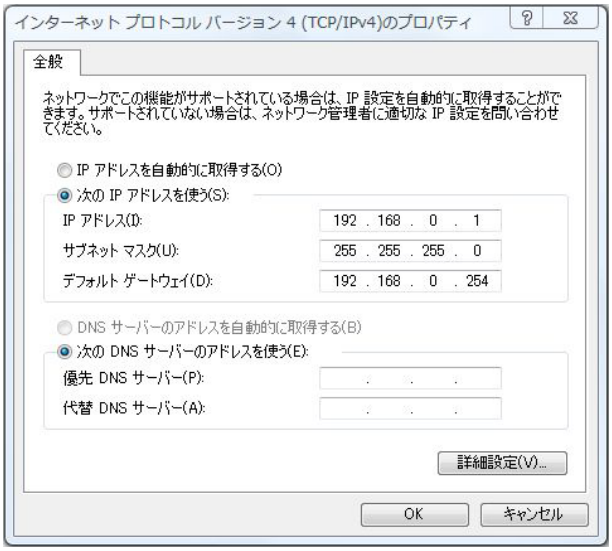


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



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

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



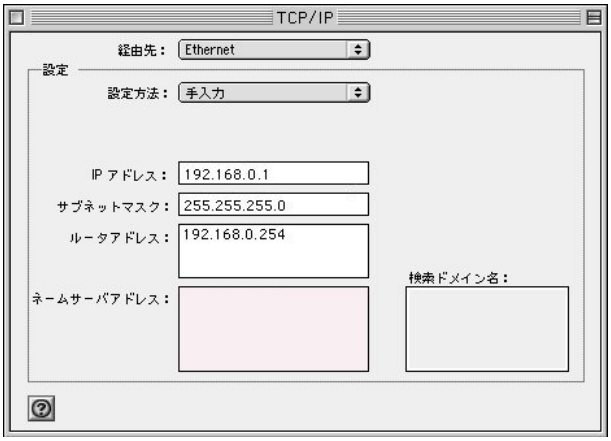
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

III. Macintoshのネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

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

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

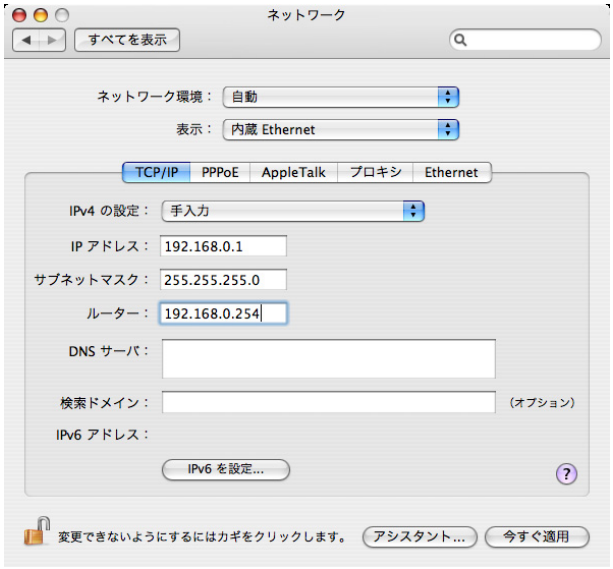


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これでXR-440へログインする準備が整いました。

ここでは、Mac OS Xのネットワーク設定について説明します。

1 「システム環境設定」から「ネットワーク」を開きます。

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



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

Ⅳ．IPアドレスの確認と再取得

◆Windows XP/Vistaの場合

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

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

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

3 IP設定のクリアと再取得をするには以下のコマンドを入力してください。

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

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

◆Macintoshの場合

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

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

第4章

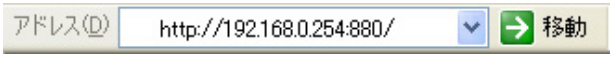
設定画面へのログイン

設定画面へのログイン方法

1 各種ブラウザを開きます。

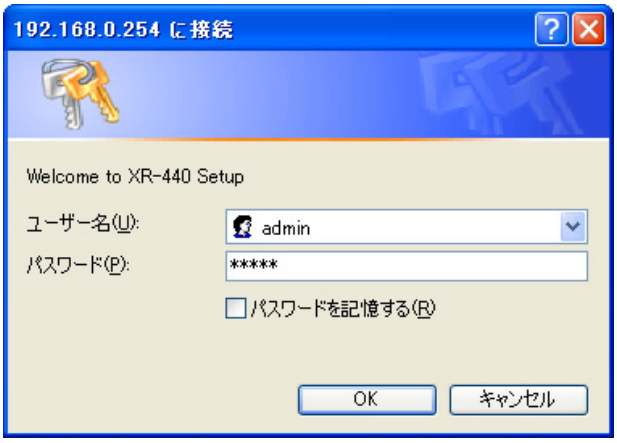
2 ブラウザから設定画面にアクセスします。

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



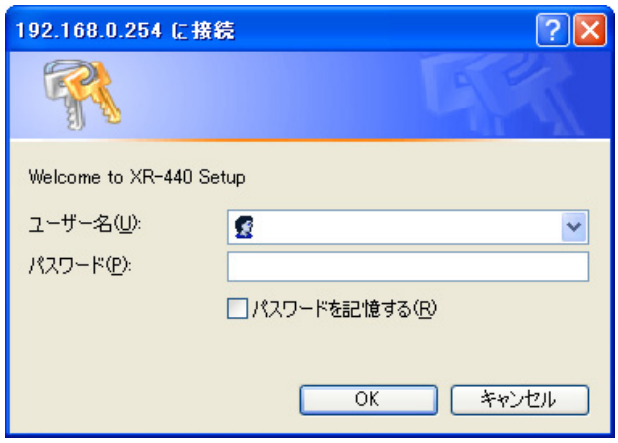
「192.168.0.254」は、Ether0 ポートの工場出荷時のアドレスです。アドレスを変更した場合は、そのアドレスを指定してください。
設定画面のポート番号 880 は変更することができません。

3 次のような認証ダイアログが表示されます。

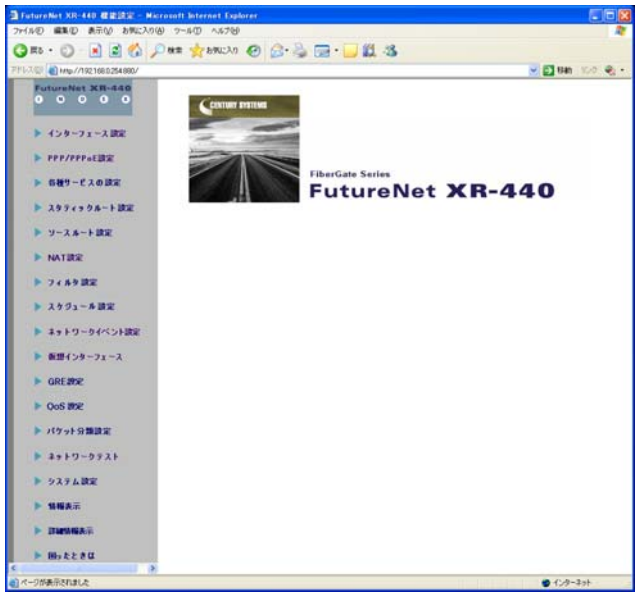


4 ダイアログ画面にパスワードを入力します。

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



5 ブラウザ設定画面が表示されます。



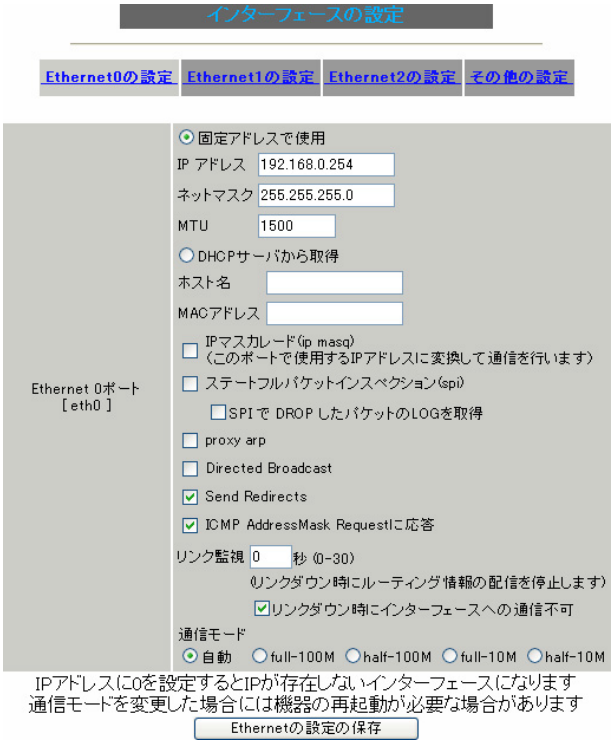
第5章

インターフェース設定

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、2)の設定」をクリックして設定します。



(画面は「Ethernet0 の設定」)

[固定アドレスで使用]

○ IP アドレス

○ネットマスク

IP アドレス固定割り当ての場合にチェックし、IP アドレスとネットマスクを入力します。

IPアドレスに“０”を設定すると、そのインタフェースは IP アドレス等が設定されず、ルーティング・テーブルに載らなくなります。

OSPFなどで使用していないインタフェースの情報を配信したくないときなどは“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、MTU 値を変更することで回避できます。通常は初期設定の 1500byte のままでかまいません。

[DHCP サーバから取得]

○ホスト名

○ MAC アドレス

IPアドレスが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。

※ 「Ethernet2 の設定」は対応していません。

○ IP マスカレード（ip masq）

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

○ステートフルパケットインスペクション(spi)

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

○ SPI で DROP したパケットの LOG を取得

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

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

○ proxy arp

Proxy ARP を使う場合にチェックを入れます。

○ Directed Broadcast

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

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

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

○リンク監視
チェックを入れると、Ethernet ポートのリンク状態の監視を定期的におこないます。
OSPF 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。
監視間隔は 1～30 秒の間で設定できます。
また、0 を設定するとリンク監視をおこないません。

○リンクダウン時にインターフェースへの通信不可
チェックを入れると、リンクがダウンした時にそのインタフェースに対する通信ができなくなります。
これにより、リモートの拠点から ping などを使って本装置の LAN インタフェースのリンク状態を監視することができます。
リンク監視が有効の場合のみ、本設定も有効になります。
ただし、本設定を有効にしたインタフェースがリモートの拠点での IPsec KeepAlive の送信先アドレスに指定された場合、リンクダウンが発生した時に IPsec トンネルの障害として検出されてしまいます。
回避の方法など、詳細については、「第 13 章 IPsec 機能　Ⅳ.IPsec Keep-Alive 設定」をご覧ください。

○通信モード
XR-440 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。
※ Ether2 ポートは自動設定のみとなります。

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。

XR-440 のインタフェースのアドレスを変更した後は設定が直ちに反映されます。
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。

II．Ethernetポートの設定について

[ステートフルパケットインスペクション]

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

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

[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。

XR-440がPPPoEで接続する場合には“ppp”という論理インタフェースを自動的に生成し、このppp論理インタフェースを使ってPPPoE接続をおこなうためです。

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

[IPsec通信時のEthernetポート設定]

XR-440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XR-440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、かつ、XR-440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。

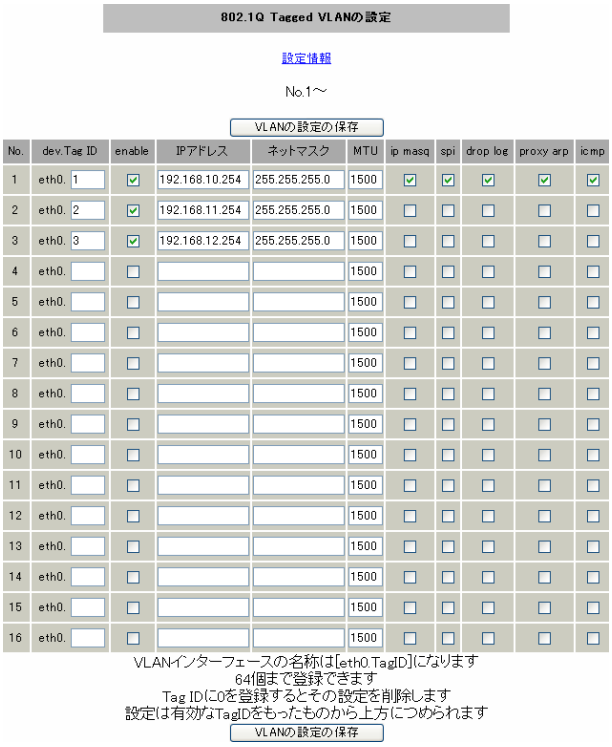
このような場合はXR-440のEthernetポートのIPアドレスを、別のネットワークに属するIPアドレスに設定し直してください。

III. VLAN タギングの設定

◆各 802.1Q Tagged VLAN の設定

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

Web 設定画面「インターフェース設定」→「Ethernet0(または 1、2)の設定」を開き、最下部にある以下の画面で設定します。



(Ether0 ポートでの表示例です)

○ dev.Tag ID
VLAN のタグ ID を設定します。
1～4094 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
○ネットマスク
VLAN インタフェースの IP アドレスとサブネットマスクを設定します。

○ MTU
VLAN インタフェースの MTU 値を設定します。

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

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

○ drop log
チェックを入れると、SPI により破棄(DROP)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。

VLAN 設定の削除

VLAN 設定を削除する場合は、「dev.Tag ID」欄に“0”を入力して「VLAN の設定の保存」をクリックしてください。

設定情報の表示

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

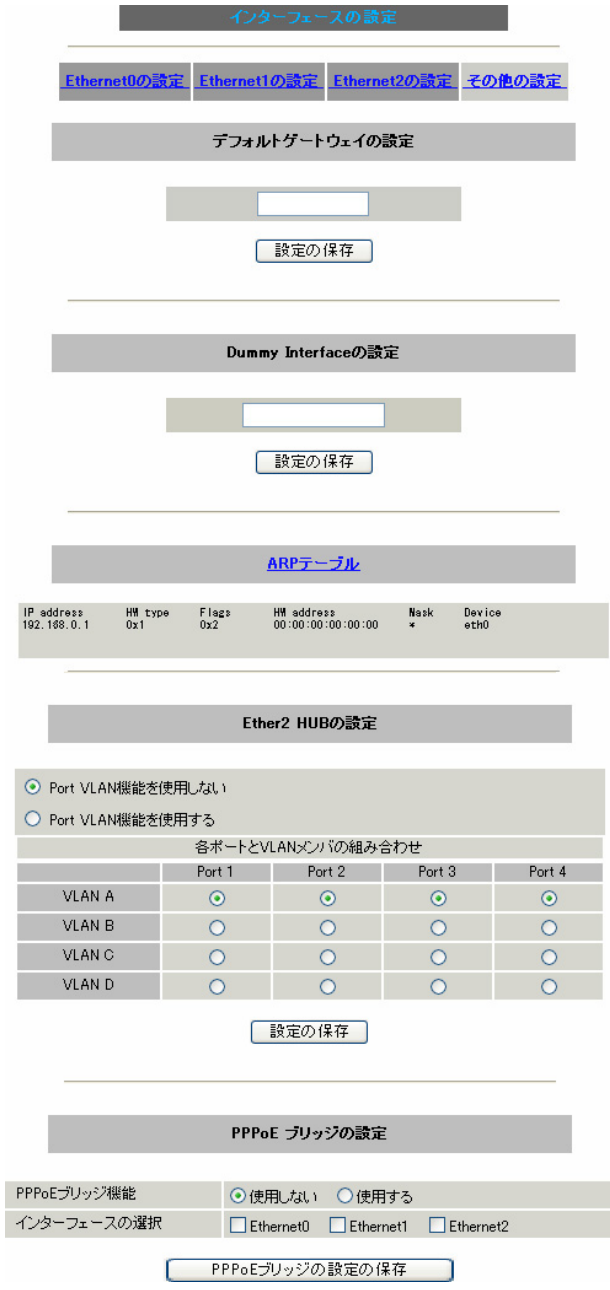
Ⅳ．その他の設定

ここでは、インタフェースに関するその他の設定をおこないます。

- ◆デフォルトゲートウェイの設定
- ◆Dummy Interfaceの設定
- ◆ARPテーブル
- ◆Ether2 HUBの設定
- ◆PPPoE ブリッジの設定

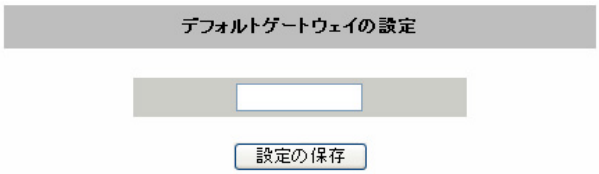
設定方法

各種設定は、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は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アドレスを設定します。
※ 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

以下の画面でDummyInterfaceを設定します。

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

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

Ⅳ．その他の設定

◆ARP テーブル

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

（画面は表示例です）

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

○ ARP エントリの固定化
ARP エントリをクリックして「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 エントリの削除
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。

○ ARP エントリの追加
入力欄に IP アドレスと MAC アドレスを入力後、「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。

○固定 ARP エントリの編集
入力欄に IP アドレスと MAC アドレスを入力後、「固定 ARP エントリの編集」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）

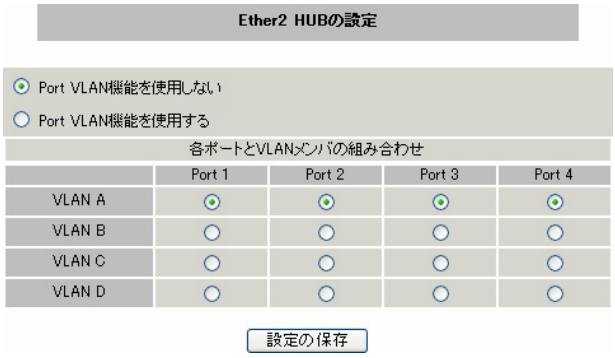
「Flags」に、ARP エントリの状態が表示されます。
0x2 ： 自動的に登録された ARP エントリ
0x6 ： 手動で登録された ARP エントリ
0x0 ： 無効となっている ARP エントリ

Ⅳ．その他の設定

◆Ether2 HUBの設定

本装置のEthernet2ポートで、ポートベースVLAN設定ができます。
設定できるVLANグループはVLAN A～VLAN Dの4つとなります。

「その他の設定」画面下にある「Ether2 HUBの設定」画面で設定します。



○Port VLAN機能を使用する
ポートベースVLAN機能を使う場合「Port VLAN機能を使用する」にチェックします。

○「各ポートとVLANメンバの組み合わせ」で、Ether2の各ポートと所属するVLANグループの組み合わせを設定します。

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。

◆PPPoE ブリッジの設定

PPPoE ブリッジ機能を使用すると、XR自身がおこなうPPPoE接続の他に、XRを経由したLAN側のホストから外部へのPPPoE接続をおこなうことが可能です。
その場合、XRではPPPoEパケットを透過します。
この機能はXR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。

「その他の設定」画面下にある「PPPoE ブリッジの設定」画面で設定します。

○PPPoEブリッジ機能
PPPoEブリッジ機能を使用する場合は「使用する」を選択します。

○インターフェースの選択
PPPoE ブリッジを有効にするインタフェースを２つ選んでチェックを入れます。

「PPPoE ブリッジの設定の保存」をクリックして設定完了です。

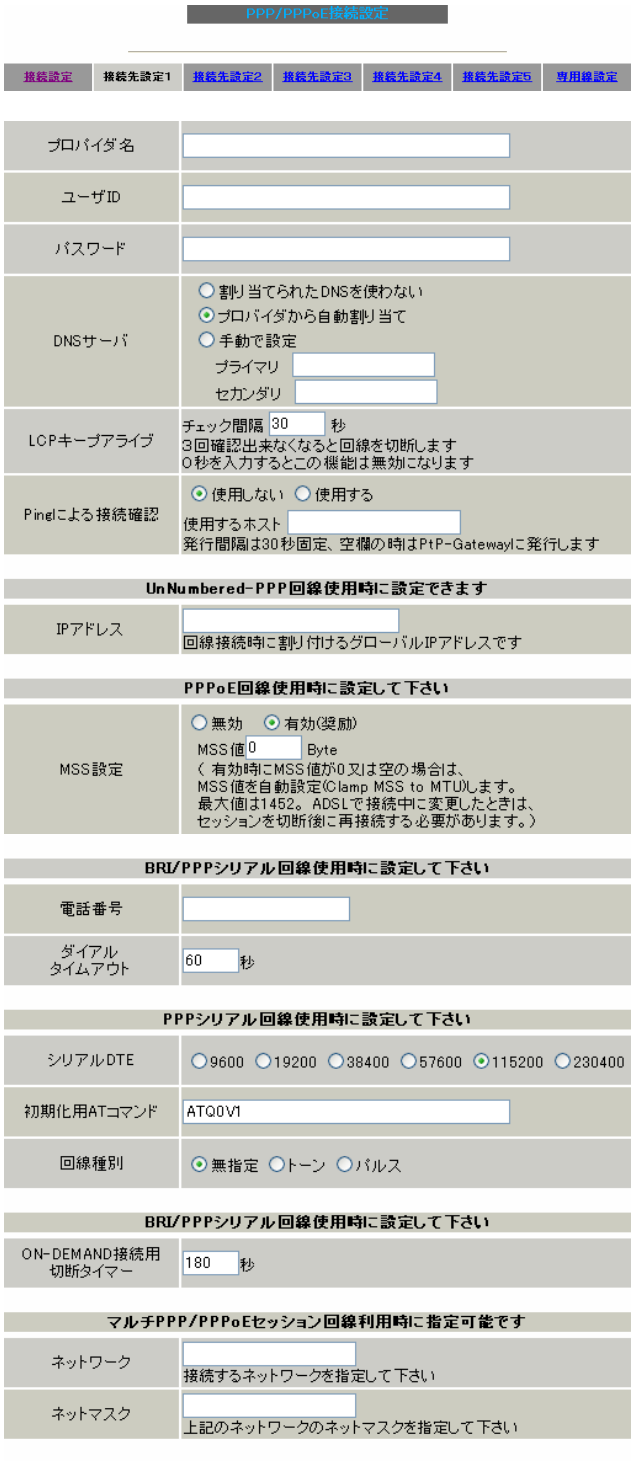
第 6 章

PPPoE 設定

Ⅰ．PPPoE の接続先設定

接続先設定

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



（画面「接続先設定１」）

○プロバイダ名
接続するプロバイダ名を入力します。
任意に入力できますが、半角英数字のみ使用できます。

○ユーザ ID
プロバイダから指定されたユーザ ID を入力してください。

○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。

Ⅰ．PPPoE の接続先設定

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

○ IP アドレス
固定 IP アドレスを割り当てられる接続の場合 (unnumbered 接続を含む)、ここにプロバイダから割り当てられた IP アドレスを設定します。
IP アドレスを自動的に割り当てられる形態での接続の場合は、ここには何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 1452Byte 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 >
　ネットワーク「172.26.0.0」
　ネットマスク「255.255.0.0」
と指定すると、172.26.0.0/16 のネットワークにアクセスするときはマルチ接続を使ってアクセスするようになります。

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

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

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

II．PPPoE の接続設定と回線の接続 / 切断

接続設定

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
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。
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。

「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。また PPPoE セッションが切断しても、自動的に再接続します。

「スケジューラ接続」
BRI ポートでの接続をする時に選択できます。

○ 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 26 章 補足：フィルタのログ出力内容について」**をご覧ください。

○デフォルトルートの設定
「有効」を選択すると、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。
「インターフェース設定」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。

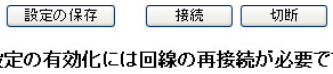
「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。
「インターフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。

通常は「有効」設定にしておきます。

II．PPPoE の接続設定と回線の接続 / 切断

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

最後に「設定の保存」ボタンをクリックして、設定完了です。



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

接続 IP 変更お知らせメール機能

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

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

＜ PPPoE お知らせメール送信＞

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

III．副回線の設定

PPPoE 接続では、「副回線接続」設定ができます。

[副回線接続]

主回線が何らかの理由で切断されてしまったときに、自動的に副回線設定での接続に切り替えて、接続を維持することができます。
また、主回線が再度接続されると、自動的に副回線から主回線の接続に戻ります。

主回線から副回線の接続に切り替わっても、NAT 設定やパケットフィルタ設定、ルーティング設定等の全ての設定が、そのまま副回線接続にも引き継がれます。

回線状態の確認は、セッションキープアライブ機能を用います。

副回線設定

PPP/PPPoE 接続設定画面の**「副回線使用時に設定して下さい」**欄で設定します。

○副回線の使用
副回線を利用する場合は「有効」を選択します。

○接続先の選択
副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
副回線を接続しているインタフェースを選択します。

○ RS232C/BRI 接続タイプ
RS232C/BRI インタフェースを使って副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。

最後に「設定の保存」ボタンをクリックして設定完了です。

上記３項目以外の接続設定は、すべてそのまま引き継がれます。

**副回線での自動接続機能は、「接続設定」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。**

Ⅳ．バックアップ回線の設定

PPPoE 接続では、「バックアップ回線接続」設定も可能です。

[バックアップ回線接続]

副回線接続と同様に、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、副回線接続とは異なり、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 または OSPF を用います。OSPF については、「第 15 章 ダイナミックルーティング　III .OSPF の設定」をご覧ください。

バックアップ回線設定

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

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

○接続先の選択
バックアップ回線接続で利用する接続先設定を選択します。

○接続ポート
バックアップ回線を接続しているインタフェースを選択します。

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

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

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

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

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

Ⅳ．バックアップ回線の設定

○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、「OSPF」は OSPF の Hello パケットにより、「IPSEC+PING」は IPSEC 上での ping により、回線の切断を確認します。

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

OSPF の場合は、OSPF 設定画面「OSPF 機能設定」の「バックアップ切り替え監視対象 Remote Router-ID 設定」で設定した IP アドレスに対して接続確認をおこないます。

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

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

○Ping 使用時の device
ping を使用する際に ping を発行する、本装置のインタフェースを選択します。
「IPSEC+PING」の場合には「その他」を選択して ipsec インタフェース名を指定します。

＜例＞主回線上の IPsec インタフェースは
“ ipsec0 ”です。

○IPSEC+Ping 使用時の IPSEC ポリシーの NO
「IPSEC+PING」で回線断を確認するときは必ず、使用する IPsec ポリシーの設定番号を指定します。
IPsec 設定については「第 13 章 IPsec 機能」や IPsec 設定ガイドをご覧ください。

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

最後に「設定の保存」ボタンをクリックして、設定完了です。

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

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

接続お知らせメール機能

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

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

＜ PPPoE Backup 回線のお知らせメール送信＞

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

Ⅴ．PPPoE 特殊オプション設定

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

これは、ユーザ側が 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、ユーザ側からの新規接続要求を受け入れることができない状態になっていることが原因です。

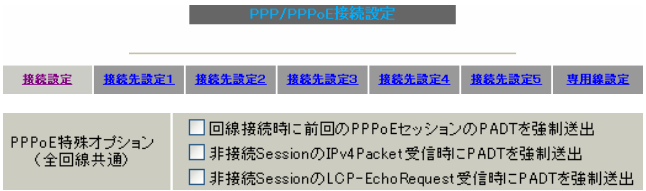
ここでPPPoE特殊オプション機能を使うことにより、本装置がPPPoEセッションを確立していないことを検知し、強制的に PADT パケットを地域 IP 網側へ送信して、地域 IP 網側に PPPoE セッションの終了を通知します。

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

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

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。



①回線接続時に前回の PPPoE セッションの PADT を強制送出する。

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

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

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

②、③の動作について
本装置がLCP キープアライブにより断を検知しても網側が断と判断していない状況下において、
網側から

- IPv4 パケット
- LCP エコーリクエスト

のいずれかを本装置が受信すると、本装置がPADTを送出してセッションの終了を網側に認識させます。
その後、本装置側から再接続をおこないます。

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

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

ただし、次の場合には、PPPoE 特殊オプションを無効にしてください。

→PPPoE to L2TP 機能を使用している場合

この場合には、PPPoE 特殊オプション設定のうち、下記の 2 項目については設定を無効（チェックなし）としてください。

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

PPPoE to L2TP 機能を使用しているときに設定を有効にした場合、XR-440 配下のクライアントが正常に PPPoE 接続できなくなります。

第7章

ダイヤルアップ接続

Ⅰ．RS-232 ポートとアナログモデム /TA の接続

XR-440 は、以下のポートを搭載しています。

- RS-232 ポート
- ISDN S/T 点ポート(BRI ポート)

これらの各ポートに、アナログモデムやターミナルアダプタを接続し、XR-440 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。

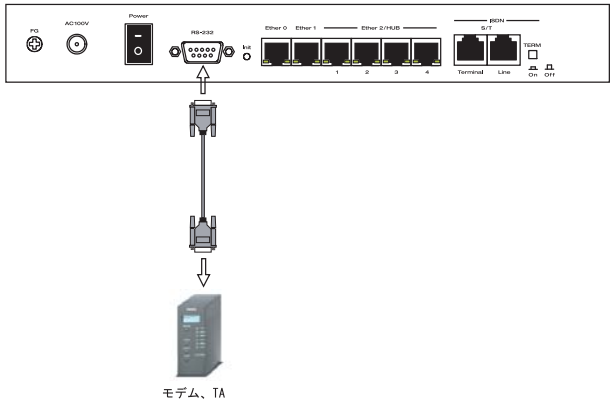
◆アナログモデム /TA のシリアル接続

1 本装置の電源をオフにします。

2 本装置の「RS-232」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

◆外部の DSU を使う場合

1 本装置の電源をオフにします。

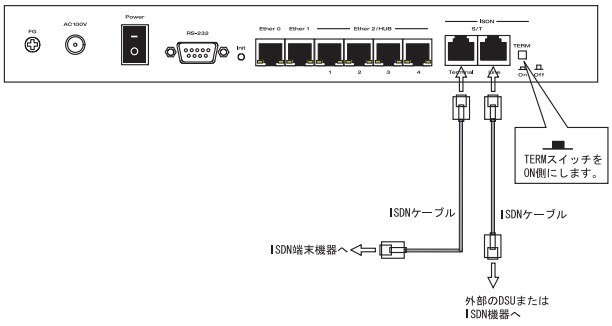
2 外部の DSU と本装置の「BRI S/T Line」ポートを ISDN 回線ケーブルで接続します。
ISDN ケーブルは別途ご用意ください。

3 本体背面の「TERM.」スイッチを「ON」にします。

4 別の ISDN 機器を接続する場合は「BRI S/T Terminal」ポートと接続してください。

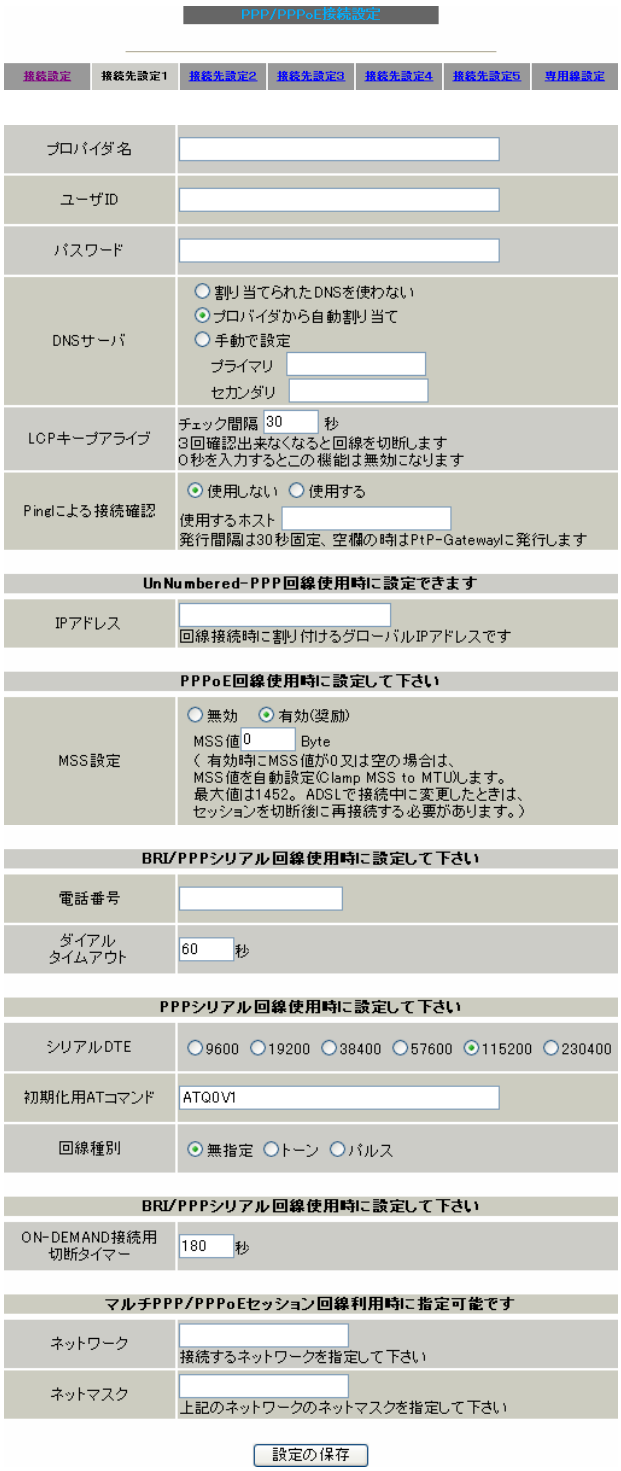
5 全ての接続が完了しましたら、本装置と TA の電源を投入します。

接続図



III．接続先設定

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



（画面は「接続先設定１」）

接続先設定

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

○ユーザ ID
プロバイダから指定されたユーザ IDを入力してください。

○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、ISDN専用線接続の場合は設定しません。

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/BRI 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、BRI 接続を切断します。

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

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

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

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

続いて PPP の接続設定をおこないます。

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」を開き「接続設定」をクリックして、以下の画面から設定します。

接続設定

○回線状態
現在の回線状態を表示します。

○接続先の選択
どの接続先設定を使って接続するかを選択します。

○接続ポート
どのポートを使って接続するかを選択します。
ダイヤルアップ接続では「BRI」または「RS232」ポートを選択します。
ISDN 専用線を使う場合は、「Leased Line(64K)」または「Leased Line(128K)」を選択してください。

○接続形態
「手動接続」
ダイヤルアップの接続/切断を手動で切り替えます。
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。

「常時接続」
本装置が起動すると自動的にダイヤルアップ接続を開始します。

「スケジューラ接続」
スケジュール接続設定に従って接続します。

○ 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
ダイヤルアップ接続時に IP マスカレードを有効にするかどうかを選択します。
unnumbered 接続以外の場合と、ISDN 専用線接続のときは、「有効」を選択してください。

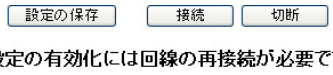
○ステートフルパケットインスペクション
ダイヤルアップ接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。
SPI を有効にして「DROP したパケットのLOGを取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。
SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 26 章 パケットフィルタリング機能　補足：フィルタのログ出力内容について」をご覧ください。

Ⅳ．ダイヤルアップの接続と切断

○デフォルトルートの設定
「有効」を選択すると、ダイヤルアップ接続時にIPアドレスとともにISPから通知されるデフォルトルートを自動的に設定します。
「インターフェース設定」でデフォルトルートが設定されていても、ダイヤルアップ接続で通知されるものに置き換えられます。
「無効」を選択すると、ISPから通知されるデフォルトルートを無視し、自動設定しません。「インターフェース設定」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、そのインタフェースにて受信したICMP AddressMask Request (type=17)に対して、サブネットマスク値を設定したICMP AddressMask Reply(type=18)を返送します。

最後に「設定の保存」ボタンをクリックして、設定完了です。



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

Ⅴ．副回線接続と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、

- 副回線接続設定
- バックアップ回線接続設定
- 接続 IP お知らせメール機能

が可能です。

設定方法については、
「第 6 章 PPPoE 設定」の各ページをご参照ください。

「II .PPPoE の接続設定と回線の接続 / 切断」
「III . 副回線の設定」
「IV . バックアップ回線の設定」

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、ISDNポートで他のISDN機器と接続していて、かつ「On-Demand接続」機能を使っている場合には、ISDN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-440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

Ⅰ．BRI ポートと TA/DSU の接続

◆外部の DSU を使う場合

1 本装置の電源をオフにします。

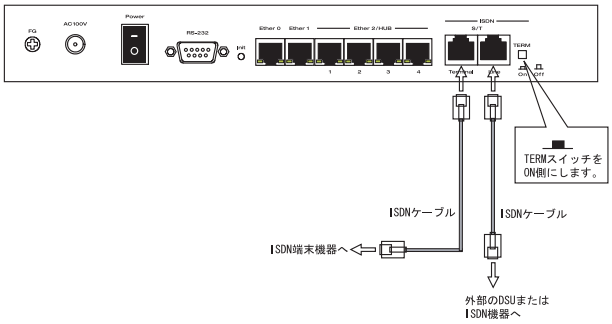
2 外部の DSU と本装置の「BRI S/T Line」ポートを ISDN 回線ケーブルで接続します。
ISDN ケーブルは別途ご用意ください。

3 本体背面の「TERM.」スイッチを「ON」側にします。

4 別の ISDN 機器を接続する場合は
「BRI S/T Terminal」ポートと接続してください。

5 全ての接続が完了しましたら、本装置と TA の電源を投入します。

接続図



Ⅱ．専用線設定

XR-440 同士を ISDN 専用線で接続し、LAN 間通信ができます。

本装置の専用線接続機能の制限について

・unnumbered 接続(LAN 型払い出し)には対応していません。

・OCN エコノミーの 128kb/s 接続には対応していません。

専用線設定

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

○プロバイダ名
プロバイダ名を任意で設定します。
半角英数字で 64 文字まで使用できます。

○本装置の IP アドレス
ISP から通知された、お客様の機器に割り当てられた IP アドレスを設定します。

○接続先の IP アドレス
対向の装置(XR-440)に割り当てられる IP アドレスを設定します。

○同期 PPP
同期 PPP を使用するかどうかを選択します。

○LCP キープアライブ
PPPoE 接続の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、XR-440 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。

設定後は「設定の保存」をクリックしてください。

続いて「接続設定」をおこなってください。
専用線設定では、「接続先設定」はおこないません。

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。

接続設定

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
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 26 章 パケットフィルタリング機能　補足：フィルタのログ出力内容について」をご覧ください。

○デフォルトルートの設定
「有効」を選択すると、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。
「インターフェース設定」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。「インターフェース設定」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、そのインタフェースにて受信した ICMP AddressMask Request (type=17)に対して、サブネットマスク値を設定した ICMP AddressMask Reply(type=18)を返送します。

最後に「設定の保存」ボタンをクリックして、設定完了です。

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

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

XR-440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

・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

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。
XR-440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
・副回線を指定する
・接続IPアドレス変更のお知らせメールを送る
・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、XR-440のマルチPPPoEセッション機能は、PPPoEで接続しているすべてのインタフェースがルーティングの対象となります。
したがいまして、それぞれのインタフェースにステートフルパケットインスペクション、又はフィルタリング設定をしてください。

この機能を利用する場合は次ページからの複数アカウント同時接続の設定のステップに従って設定してください。

複数アカウント同時接続の設定

STEP １●主接続の接続先設定

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

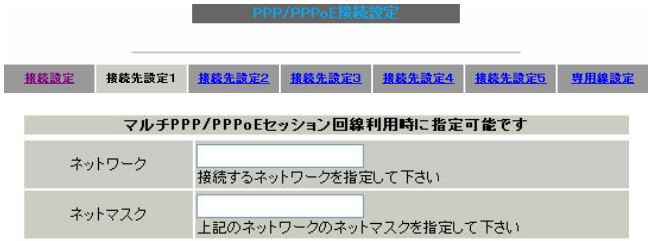
Web 設定画面「PPP/PPPoE 設定」をクリックし、「接続先設定１～５」のいずれかをクリックして設定します。
詳しい設定方法は、「第６章 PPPoE 設定」または「第７章 ダイヤルアップ接続」をご覧ください。

STEP ２●マルチ接続用の接続先設定

マルチ接続(同時接続)用の接続先設定をおこないます。

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

さらに、設定画面最下部にある下図の「**マルチPPP/PPPoEセッション回線利用時に指定可能です**」部分で、マルチ接続を使ってアクセスしたい先のネットワークアドレスとネットマスクを指定します。



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

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

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

最後に「設定の保存」をクリックして接続先設定は完了です。

複数アカウント同時接続の設定

STEP 3 ● PPPoE 接続の設定

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

Web 設定画面「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。

○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 XR-440 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/BRI 接続タイプ
「通常」は接続形態設定にあわせて接続します。

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

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

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

○デフォルトルートの設定
「有効」を選択します。

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

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

続いてマルチ接続用の接続設定をおこないます。

複数アカウント同時接続の設定

[マルチ接続用の設定]

Web 設定画面「PPP/PPPoE 設定」→「接続設定」にある以下の「**マルチ PPP/PPPoE セッション機能を利用する際は以下を設定して下さい**」部分で設定します。

PPP/PPPoE接続設定

接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5	専用線設定

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい

マルチ接続 #2	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○Leased Line(64K) ○Leased Line(128K) ○RS232C
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
ICMP AddressMask Request	○応答しない ◉応答する
マルチ接続 #3	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○Leased Line(64K) ○Leased Line(128K) ○RS232C
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
ICMP AddressMask Request	○応答しない ◉応答する
マルチ接続 #4	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○Ether0 ◉Ether1 ○Ether2 ○BRI(64K) ○BRI MP(128K) ○Leased Line(64K) ○Leased Line(128K) ○RS232C
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
ICMP AddressMask Request	○応答しない ◉応答する

○マルチ接続 #2 ～ #4

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

○接続先の選択

マルチ接続用の接続先設定を選択します。

○接続ポート

マルチ接続で使用する XR-440 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/BRI 接続タイプ

BRI インタフェースを使って複数アカウント同時接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

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

○ IP マスカレード

任意で選択します。

通常は「有効」にします。

○ステートフルパケットインスペクション

任意で選択します。

SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。

SPI が有効のときだけ動作可能です。

ログの出力内容については「第 26 章 パケットフィルタリング機能　補足：フィルタのログ出力内容について」をご覧ください。

○ ICMP AddressMask Request

任意で選択します。

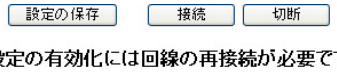
マルチ接続設定は 3 つまで設定可能です。

最大 4 セッションの同時接続が可能です。

複数アカウント同時接続の設定

STEP 4 ● PPPoE 接続の開始

すべて設定した後、「接続」をクリックして PPPoE 接続を開始します。



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

接続に成功した場合:

主回線で接続しています。
マルチセッション回線 1 で接続しています。

接続できていない場合:

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

などと表示されます。

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

複数アカウント同時接続時の注意点

通常の ISP とフレッツスクエアへの同時接続をするには、XR-440 の「DNS サーバ機能」を「有効」にし、各 PC の DNS サーバ設定を XR-440 の IP アドレスに設定してください。

XR-440 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、各機能についてのページを参照してください。

DNS キャッシュ
→「第 11 章 DNS リレー / キャッシュ機能」
DHCP(Relay)サーバ
→「第 12 章 DHCP サーバ / リレー機能」
IPsec サーバ
→「第 13 章 IPsec 機能」
UPnP サービス
→「第 14 章 UPnP 機能」
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 (RIP/OSPF/BGP4)」
PPPoEtoL2TP
→「第 16 章 PPPoE to L2TP」
SYSLOG サービス
→「第 17 章 SYSLOG サービス」
攻撃検出サービス
→「第 18 章 攻撃検出機能」
SNMP サービス
→「第 19 章 SNMP エージェント機能」
NTP サービス
→「第 20 章 NTP サービス」
VRRP サービス
→「第 21 章 VRRP サービス」
アクセスサーバ
→「第 22 章 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、「動作変更」ボタンをクリックしてください。これにより、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、各項目ごとに表示されます。

第 11 章

DNS リレー / キャッシュ機能

第 11 章 DNS リレー / キャッシュ機能

DNS 機能の設定

◆ DNS リレー機能

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

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

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

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

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

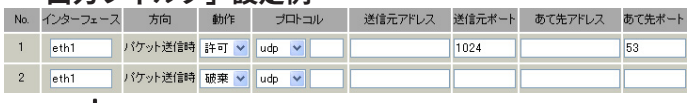
○タイムアウト
DNSサーバへの問い合わせが無応答の場合のタイムアウトを設定します。
5-30 秒で設定できます。初期設定は 30 秒です。
使用環境によっては、DNSキャッシュのタイムアウトよりもブラウザなどのアプリケーションのタイムアウトが早く発生する場合があります。
この場合は、DNSキャッシュのタイムアウトを調整してください。

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

ただし、「フィルタ設定」で以下の設定を実行している場合には注意が必要です。

DNSのポート番号を指定してフィルタしている場合

<「出力フィルタ」設定例>



↓

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

<「出力フィルタ」設定例>

または、

UDP のポート番号 10000-65535 をフィルタしている場合

<「出力フィルタ」設定例>

↓

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

<「出力フィルタ」設定例>

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

◆ DNS キャッシュ機能

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

第 12 章

DHCP サーバ / リレー機能

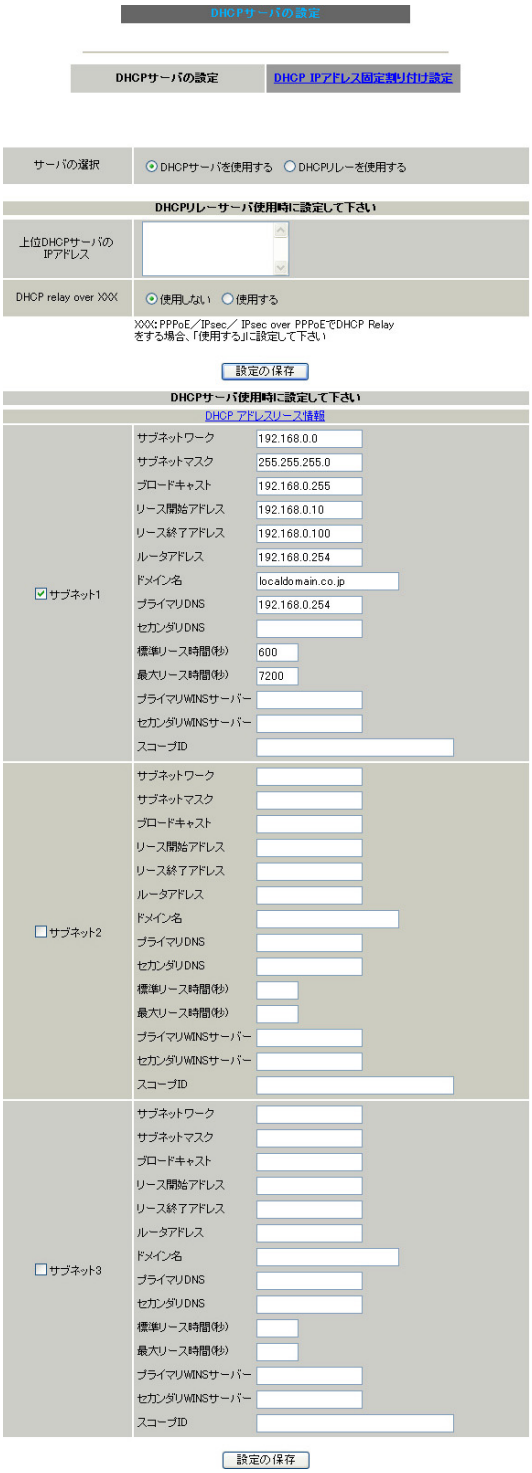
第 12 章 DHCP サーバ / リレー機能

Ⅰ．DHCP サーバ機能の設定

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 サーバの設定

画面上部「DHCP サーバの設定」をクリックします。



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

[DHCP リレーサーバ使用時に設定して下さい]
「サーバの選択」で「DHCP リレーを使用する」を選択した場合に設定します。

○上位 DHCP サーバの IP アドレス
DHCP リレー機能を使う場合に、上位の DHCP サーバの IP アドレスを指定してください。

○ DHCP relay over XXX
通常の Ethernet 接続経由以外(PPPoE/IPsec/PPPoE 接続時の IPsec)で DHCP リレー機能をおこなうときに「使用する」を選択してください。

[DHCP サーバ使用時に設定して下さい]
「サーバの選択」で「DHCP サーバを使用する」を選択した場合に設定をおこないます。

○サブネット 1 ～ 3
DHCP サーバ機能の動作設定をおこないます。

- **複数のサブネットを設定することができます。**
- **どのサブネットを使うかは、XR-440 のインタフェースに設定された IP アドレスを参照の上、自動的に決定されます。**
- **ラジオボックスにチェックを入れたサブネット設定が、参照・動作の対象となります。**

各サブネットごとの詳細設定は以下の通りです。

○サブネットワーク
DHCP サーバ機能を有効にするサブネットワーク空間のアドレスを指定します。

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

Ⅰ．DHCP サーバ機能の設定

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

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

○ルータアドレス
DHCP クライアントのデフォルトゲートウェイとなるアドレスを入力してください。
通常は、XR-440 のインタフェースの IP アドレスを指定します。

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

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

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

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

○プライマリ WINS サーバ
○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。

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

Ⅰ．DHCP サーバ機能の設定

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おこなう必要があります。(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。)

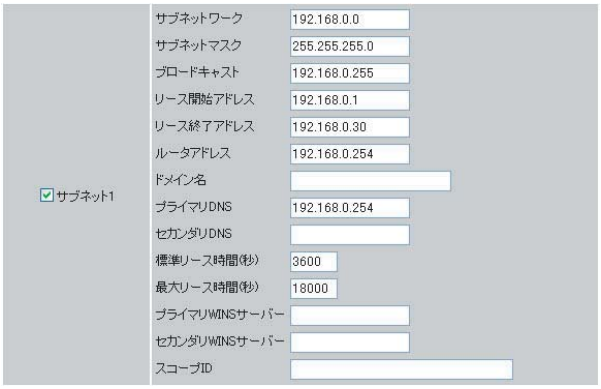
DHCP 情報の表示

設定画面中の「DHCP アドレスリース情報」をクリックすると、クライアントに割り当てているリース情報を確認できます。

DHCP サーバ機能の設定例

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

上記条件の場合の設定例です。



II．IP アドレス固定割り当て設定

◆DHCP IP アドレス固定割り付け設定

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

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

○ MAC アドレス
コンピュータに装着されている LAN ボードなどの MAC アドレスを入力します。

＜入力例＞　**00:80:6d:49:ff:ff**

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

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

エントリの削除方法

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

IP アドレス固定割り当て時の DHCP サーバ設定について

IPアドレス固定割り当てをおこなう場合でも、有効な DHCP サーバ設定をおこなってください。

DHCP サーバ機能で固定割り当てだけをおこなうときには、リース範囲を、割り当てる IP アドレスの先頭と末尾の IP アドレスとしてサブネット設定をおこなってください。

第 13 章

IPsec 機能

Ⅰ．XR-440 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
XR-440 シリーズは「共通鍵方式」「RSA 公開鍵方式」「X.509」による認証に対応しています。
ただし、アグレッシブモードは「共通鍵方式」にのみ対応、「X.509」はメインモードにのみ対応しています。

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

◆ハッシュアルゴリズム
SHA1 と MD-5 を使用しています。

◆認証ヘッダ
XR-440 シリーズは ESP の認証機能を利用しています。AH での認証はサポートしていません。

◆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-440 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。

◆NAT トラバーサル機能を使用した IPsec 接続
XR 同士の場合、NAT 内のプライベートアドレス環境においても IPsec 接続をおこなうことが可能です。

II．IPsec 設定の流れ

◆ PreShared(共通鍵)方式での IPsec 通信

STEP 1　共通鍵の決定

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

STEP 2　共通鍵の交換

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

STEP 3　本装置側の設定

自分側の XR-440 の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

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

STEP 5　IPsec ポリシー設定

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

STEP 6　IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7　IPsec 接続の確認

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

◆ RSA(公開鍵)方式での IPsec 通信

STEP 1　公開鍵・暗号鍵の生成

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

STEP 2　公開鍵の交換

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

STEP 3　本装置側の設定

自分側の XR-440 の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

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

STEP 5　IPsec ポリシー設定

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

STEP 6　IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7　IPsec 接続の確認

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

III. IPsec 設定

STEP 0 設定画面を開く

1 Web 設定画面にログインします。

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

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。

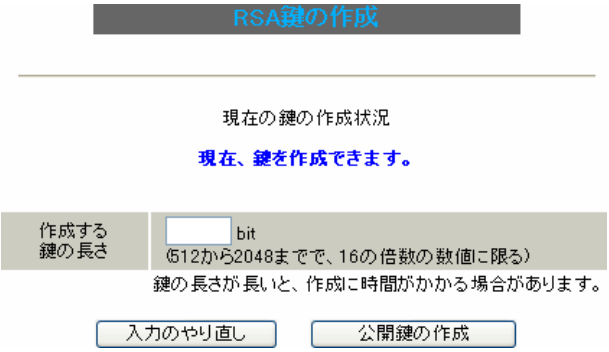
- **ステータスの確認**
- **本装置の設定**
- **RSA 鍵の作成**
- **X.509 の設定**
- **パラメータでの設定**
- **IPsec Keep-Alive 設定**
- **IKE/ISAKMP ポリシーの設定**
- **IPsec ポリシーの設定**

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。

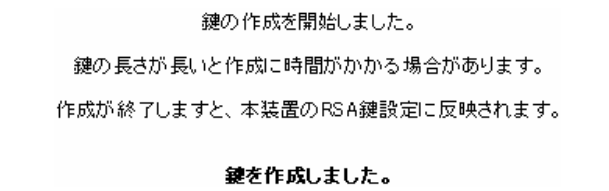
PSK 共通鍵方式を用いて IPsec 通信をおこなう場合は、「鍵の作成」は不要です。
相手側と任意で共通鍵を決定し、交換しておきます。

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。



上記のメッセージが表示されると、鍵の生成が完了です。
生成した鍵は、後述する「本装置側の設定」に自動的に反映されます。
また、この鍵は公開鍵となりますので、相手側にも通知してください。

STEP 3　本装置側の設定をおこなう

IPsec 設定画面上部の「本装置の設定」をクリックして設定します。

[本装置の設定]
「本装置の設定」をクリックします。

[MTU の設定]
○ ipsec インターフェイスの MTU 値
IPsec 接続時の MTU 値を設定します。
各インタフェースごとに設定できます。
通常は初期設定のままでかまいません。

[NAT Traversal の設定]
NAT トラバーサル機能を使うことで、NAT 環境下にあるクライアントと IPsec 通信をおこなえるようになります。

○ NAT Traversal
NAT トラバーサル機能を使うかどうかを選択します。

○ Virtual Private 設定～4
接続相手の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。
最大 4 箇所まで接続先ネットワークを設定できます。
以下のような書式で入力してください。

＜入力形式＞
%v4:＜ネットワーク＞/＜マスクビット値＞

＜設定例＞
%v4:192.168.0.0/24

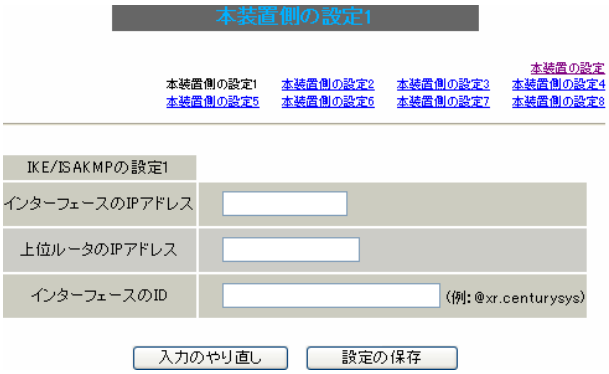
[鍵の表示]
○本装置の RSA 鍵
RSA 鍵の作成をおこなった場合ここに、作成した RSA 鍵の公開鍵が表示されます。
PSK 方式や X.509 電子証明を使う場合はなにも表示されません。

最後に「設定の保存」をクリックして設定完了です。

III. IPsec 設定

[本装置側の設定]

「本装置側の設定 1～8」のいずれかをクリックします。
ここで XR-440 自身の IP アドレスやインタフェース ID を設定します。



（画面は「本装置側の設定 1」です）

○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**
  PPP/PPPoE 主回線接続の場合は「%ppp0」と入力します。
  Ether0(Ether1,Ether2)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）。
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。

＜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。
半角英数字のみ使用可能です。)

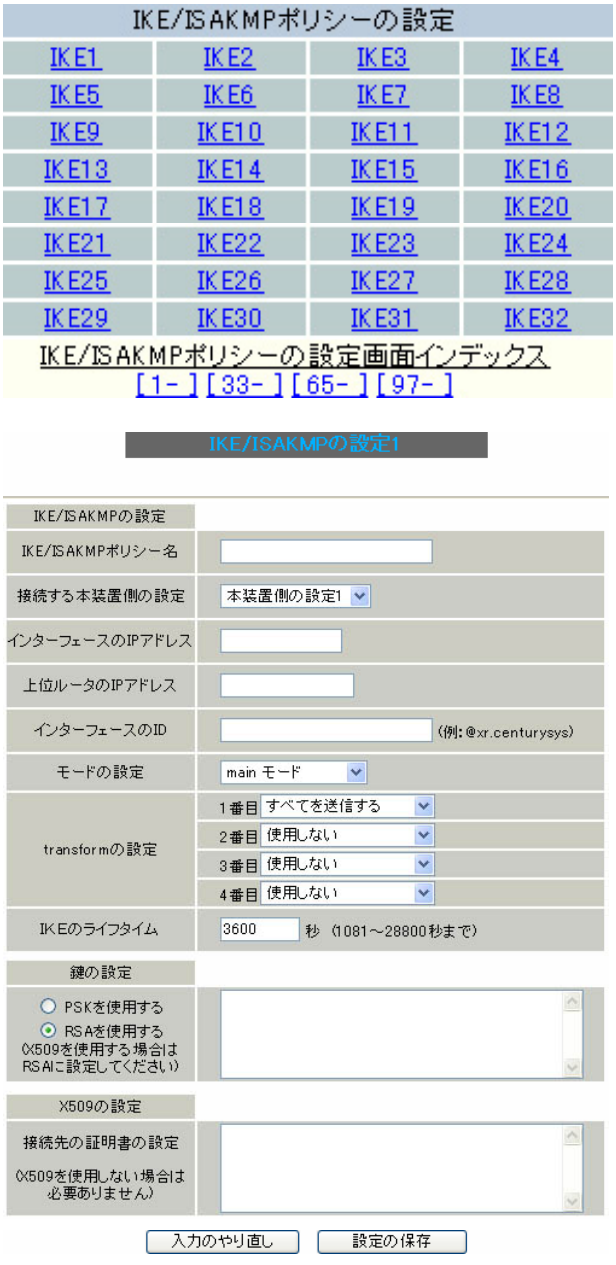
最後に「設定の保存」をクリックして設定完了です。

続いて **IKE/ISAKMP ポリシー**の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

IPsec 設定画面上部の「IKE/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。

32 個以上設定する場合は「IKE/ISAKMP ポリシーの設定画面インデックス」で切り替えてください。



(画面は「IKE/ISAKMP の設定 1」)

[IKE/ISAKMP の設定]

○ IKE/ISAKMP ポリシー名

設定名を任意で設定します。(省略可)

○接続する本装置側の設定

接続で使用する「本装置側の設定 1～8」を選択します。

○インターフェースの IP アドレス

相手側 IPsec 装置の IP アドレスを設定します。

相手側装置への IP アドレスの割り当てが固定か動的かで、入力が異なります。

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

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

○上位ルータの IP アドレス

空欄にしておきます。

○インターフェースの ID

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

＜入力形式＞　**@＜任意の文字列＞**

＜入力例＞　@centurysystems

(@ の後は、任意の文字列でかまいません。
半角英数字のみ使用可能です。)

対向側装置への割り当てが固定アドレスの場合は設定の必要はありません。

○モードの設定

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

III. IPsec 設定

○ transform の選択
ISAKMP SAの折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。
XR-440 は、以下の組み合わせが選択できます。

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

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

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

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

[鍵の設定]
○ PSK を使用する
PSK 方式の場合に、「PSK を使用する」にチェックして、相手側と任意に決定した共通鍵を入力してください。
半角英数字のみ使用可能です。最大 2047 文字まで設定できます。

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

[X509 の設定]
○接続先の証明書の設定
「X.509」設定で IPsec 通信をおこなう場合は、相手側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。

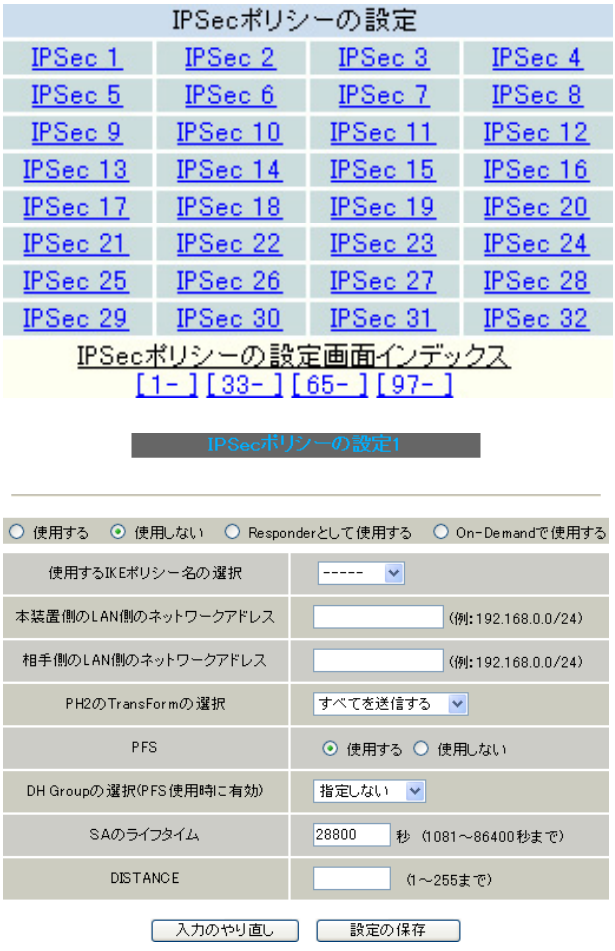
続いて、**IPsec ポリシーの設定**をおこないます。

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ます。

32 個以上設定する場合は「IPSec ポリシーの設定画面インデックス」で切り替えてください。



(画面は「IPSec ポリシーの設定 1」)

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に選択してください。
ただし、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 IPsec 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
XR-440 が接続している LAN のネットワークアドレスを入力します。
ネットワークアドレス / マスクビット値の形式で入力します。
＜入力例＞　**192.168.0.0/24**

○相手側の LAN 側のネットワークアドレス
対向の IPsec 装置に接続されている 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。

また NAT Traversal 機能を使用している場合に限っては、“**vhost:%priv**”と設定します。

III. IPsec 設定

○ 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。
・暗号化アルゴリズム (des、3des、aes)
・認証アルゴリズム (md5、sha1)
通常は「すべてを送信する」の選択で構いません。

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

○ 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 を接続相手に送ります。

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

○ DISTANCE
IPsec ルートの DISTANCE 値を設定します。
同じ内容でかつ DISTANCE 値の小さい IPsec ポリシーが起動したときには、DISTANCE 値の大きいポリシーは自動的に切断されます。
なお、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-440 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、XR-440 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 XR-440 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. IPsec 設定

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。

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。

＜「メインモード」で通信した場合の表示例＞

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

および

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

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

(1)のメッセージ

IKE 鍵交換が正常に完了し、ISAKMP SA が確立したことを示しています。

(2)のメッセージ

IPsec SA が正常に確立したことを示しています。

STEP 8 IPsecステータス確認の確認

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

(画面は表示例です)

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

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

また、それぞれの設定番号をクリックすると、設定画面に移ることができます。

IV. IPSec Keep-Alive 設定

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することで、IPsec の再接続性を高めます。

設定方法

IPsec 設定画面上部の「IPsec Keep-Alive 設定」をクリックして設定します。
設定は 128 まで可能です。画面下部にある「ページインデックス」のリンクをクリックしてください。

IPSec Keep-Alive設定

No.1～16まで

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

設定/削除の実行

ページインデックス

1 - 16 17 - 32 33 - 48 49 - 64 65 - 80 81 - 96 97 -112 113-128

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

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

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

IV. IPSec Keep-Alive 設定

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

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

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

・動作オプション 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。
ただし、timeout 値が(interval/watch count)より大きい場合は、reply 待ち時間は(interval/watch count)となります。

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

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

注) 本オプションは v1.7.0 での新規追加オプションです。
チェックを入れない場合、IPsec ネゴシエーションと Keep-Alive が非同期におこなわれるため、タイミングによっては IPsecSA の確立と ping の応答待ちタイムアウトが重なってしまい、確立直後の IPsecSA を切断してしまう場合があります。
このような事象を防ぐために、本オプションを有効にすることを推奨します。

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

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

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

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

この後、ping の応答がタイムアウトした場合は、フェーズ 4 に移行します。

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

IV. IPSec Keep-Alive 設定

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

注) 本オプションは v1.7.0 以前の「flag」オプションと同じものです。

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

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

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

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

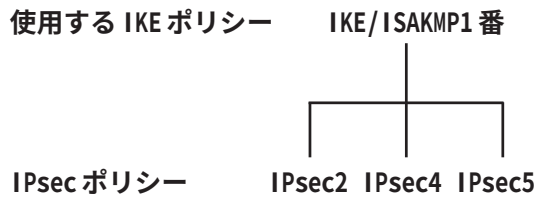
< 入力例 > 1_2_3

またここに、以下のような設定もできます。

ike<n> ※ <n> は 1 ～ 128 の整数

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

< 例 >



上図の設定で backupSA に「ike1」と設定すると、「IPsec2」が使用している IKE/ISAKMP ポリシー設定 1 番を使う、他の IPsec ポリシー(IPsec4 と IPsec5)も同時にネゴシエーションを開始します。

○ remove?
設定を削除したいときにチェックします。

最後に「設定の保存」ボタンをクリックします。
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。

destination addressとリンク監視について

本装置が対向 XR の Keep-Alive の「destination address」に指定されており、かつ、そのインタフェース上で、Web 設定画面「インターフェース設定」→「Ethernet0(1,2)の設定」にある「□ リンクダウン時にインターフェースへの通信不可」(「第5章 インターフェース設定 Ⅰ.Ethernetポートの設定」参照) を「有効」にすると、インタフェースがリンクダウンした時に、Keep-Alive にも応答しなくなるため、IPsec ポリシーがダウンしてしまいます。
これを回避するためには、「仮想インターフェース」設定で、destination address と同じネットワークの **loopback インタフェース**を設定し、そのアドレスを対向 XR の IPsec Keep-Alive の「destination address」に指定してください。

＜例＞

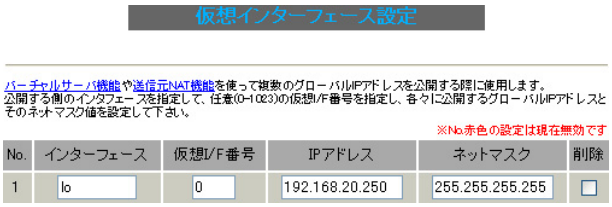
本装置側の設定

ネットワーク構成

IPsecのLAN側インタフェースアドレス：192.168.20.253
loopback インタフェースアドレス　　：192.168.20.250

本装置側の loopback(仮想)インタフェース設定

本装置側の Web 設定画面「仮想インターフェース」を開いて設定します。



○インターフェース　「lo」
○仮想 I/F 番号　「0」
○ IP アドレス　「192.168.20.250」
○ネットマスク　「255.255.255.255」(必須)

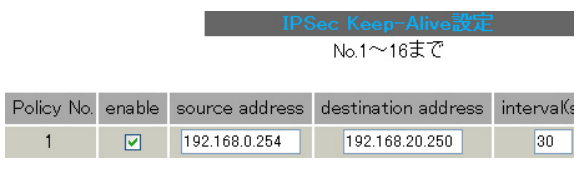
対向 XR 側の設定

ネットワーク構成

IPsecのLAN側インタフェースアドレス：192.168.0.254

対向 XR 側の IPsec Keep-Alive 設定

対向の XR 側で、Web 設定画面「各種サービスの設定」→「IPsec サーバ」→「IPSec Keep-Alive 設定」を開いて設定します。



○source address　対向XR自身のLAN側アドレス
○destination address　「lo:0」に設定したアドレス
→「192.168.20.250」

V.「X.509 デジタル証明書」を用いた電子認証

XR-440 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、XR-440 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/

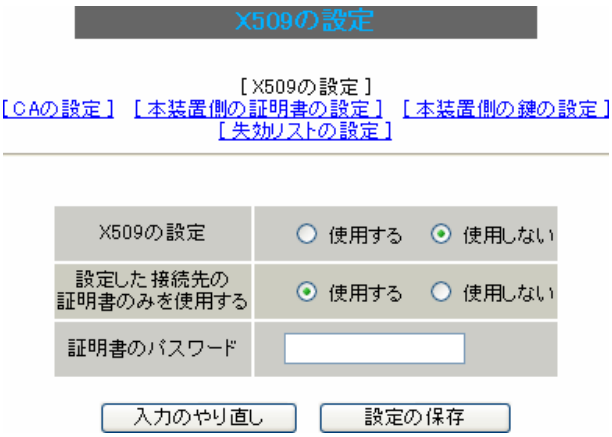
設定方法

IPsec 設定画面上部の「X509 の設定」を開きます。
ここで以下の設定が可能です。

- [X509 の設定]
- [CA の設定]
- [本装置側の証明書の設定]
- [本装置側の鍵の設定]
- [失効リストの設定]

各リンクをクリックすると設定画面が表示されます。

[X.509 の設定]



○ X509 の設定
X.509 の使用 / 不使用を選択します。

○設定した接続先の証明書のみを使用する
「IKE/ISAKMP の設定」で X.509 の設定をおこなった接続先の証明書みの使用 / 不使用を選択します。

○証明書のパスワード
証明書のパスワードを入力します。

入力後「設定の保存」をクリックします。

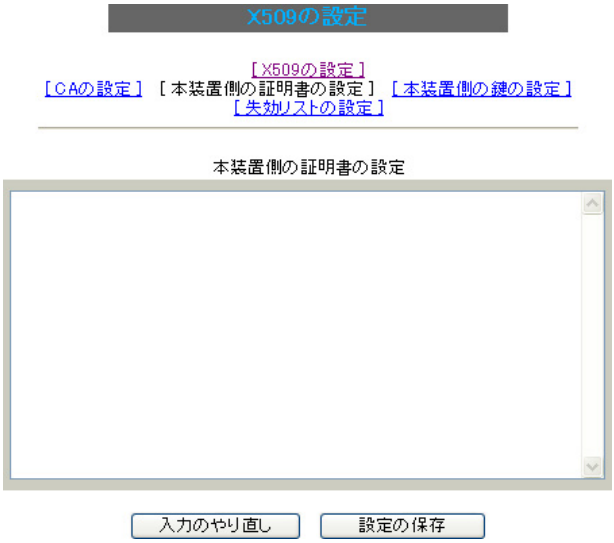
[CA の設定]

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

コピーを貼り付けましたら、「設定の保存」をクリックします。

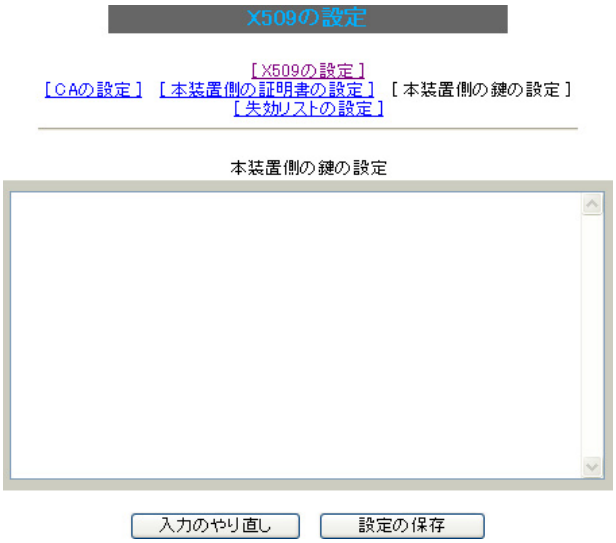
V．「X.509 デジタル証明書」を用いた電子認証

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



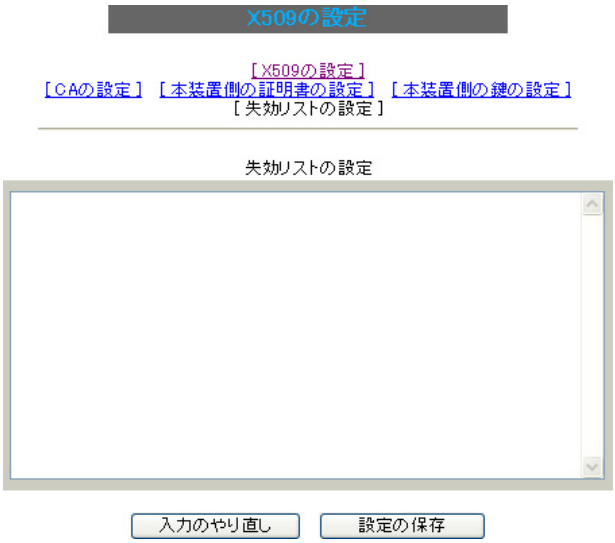
コピーを貼り付けましたら、「設定の保存」をクリックします。

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



コピーを貼り付けましたら、「設定の保存」をクリックします。

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



コピーを貼り付けましたら、「設定の保存」をクリックします。

[接続先の証明書の設定]
「IKE/ISAKMP ポリシーの設定」画面内の[鍵の設定]は下記のように設定してください。

- 「RSA を使用する」　チェック
- 設定欄　空欄

(「本装置の設定」画面の[鍵の表示]欄も空欄にしておきます。)

「IKE/ISAKMP ポリシーの設定」画面内[X509 の設定]の「接続先の証明書の設定」は下記のように設定してください。

- 設定欄　相手側のデジタル証明書の貼付

以上で X.509 の設定は完了です。

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

VI．IPsec 通信時のパケットフィルタ設定

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

IPsec では、以下の 2 種類のプロトコル・ポートを使用します。

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

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

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

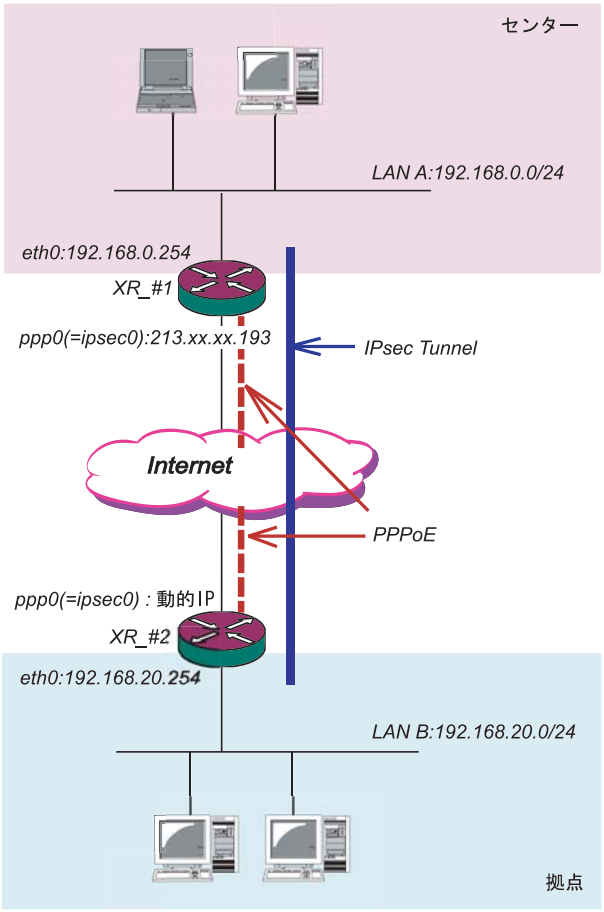
＜設定例＞

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

Ⅶ. IPsec 設定例 1（センター／拠点間の 1 対 1 接続）

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

＜設定例 1＞



＜接続条件＞

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

■ XR_#1(センター側 XR)の設定

各設定画面で下記のように設定します。

「本装置の設定」

「本装置側の設定１」を選択します。

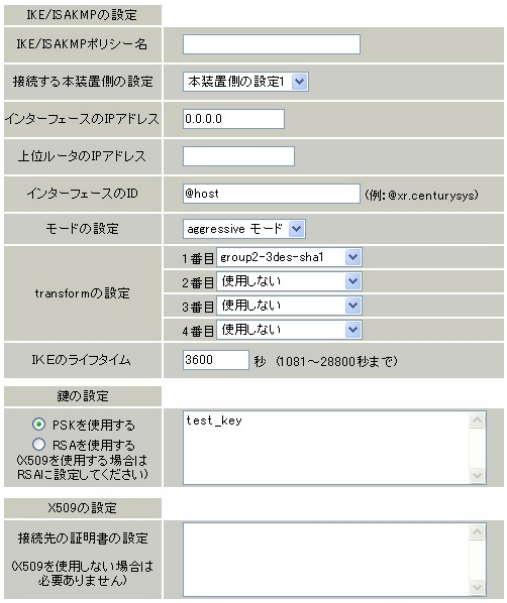
○インターフェースの IP アドレス
「213.xxx.xxx.193」

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

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

Ⅶ．IPsec 設定例 1（センター／拠点間の 1 対 1 接続）

「IKE/ISAKMP ポリシーの設定」
「IKE1」を選択します。



○ IKE/ISAKMP ポリシー名 「(任意で設定します)」

○接続する本装置側の設定 「本装置側の設定 1」

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

○上位ルータの IP アドレス 「空欄」

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

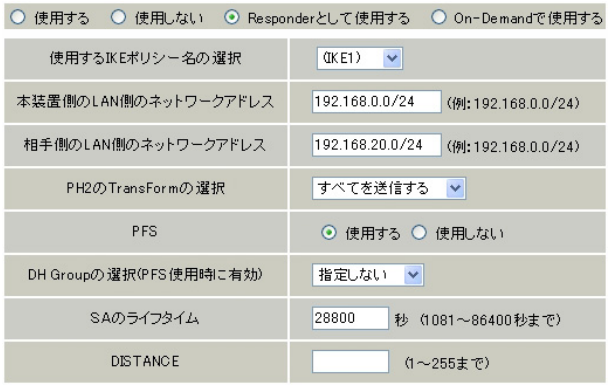
○モードの設定 「aggressive モード」

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

○ IKE のライフタイム 「3600」
(任意の設定値)

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

「IPSec ポリシーの設定」
「IPSec1」を選択します。



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

○使用する IKE ポリシー名の選択 「IKE1」

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

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

○ PH2 の TransForm の選択 「すべてを送信する」

○ PFS 「使用する」（推奨）

○ DH Group の選択 「指定しない」

○ SA のライフタイム 「28800」（任意の設定値）

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

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

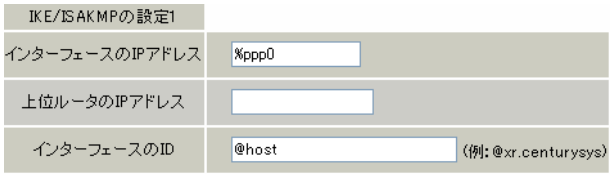
Ⅶ. IPsec 設定例 1（センター／拠点間の 1 対 1 接続）

■ XR_#2(拠点側 XR)の設定

各設定画面で下記のように設定します。

「本装置の設定」

「本装置側の設定１」を選択します。



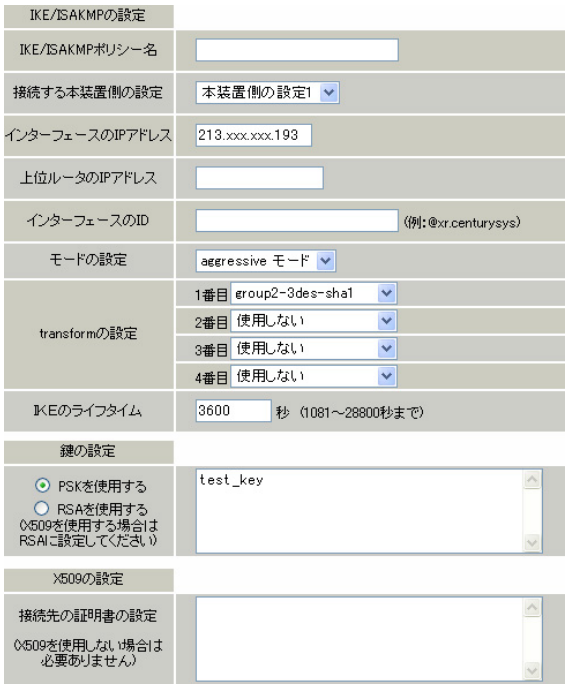
○インターフェースの IP アドレス　「%ppp0」
※ PPPoE 接続かつ動的アドレスの場合は、必ずこの設定にします。

○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.xxx.xxx.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」

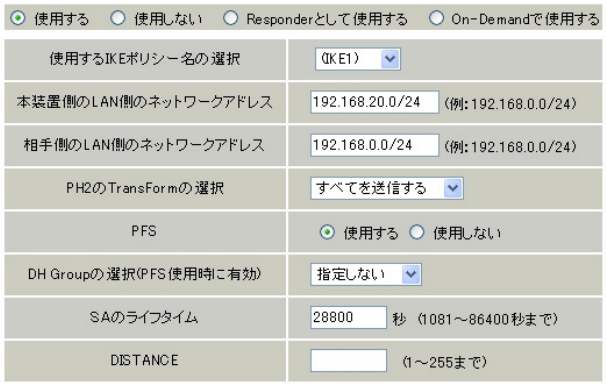
○ transform の設定　「group2-3des-sha1」
(任意の設定を選択)

○ 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。

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

○ interval　「30」（任意の設定値）

○ watch count　「3」（任意の設定値）

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

○動作 option 1　「空欄」

○動作 option 2　「チェック」

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

○ backup SA　「空欄」

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

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

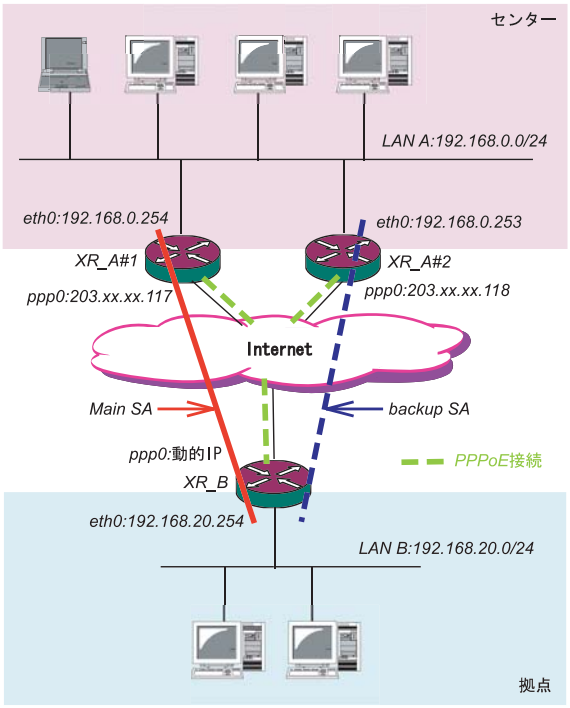
○ enable にチェックを入れます。

○ source address　「192.168.20.254」

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。
- ただし、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 を用いておこないます。
- IP アドレス、ネットワークアドレス、インタフェース名は図中の表記を使用するものとします。
- 拠点側を Initiator、センター側を Responder とします。
- 拠点側が動的アドレスのため、aggressive モードで接続します。
- PSK 共通鍵を用い、鍵は「test_key」とします。
- センター側 LAN では、拠点方向のルートをアクティブの SA にフローティングさせるため、スタティックルートを用います。

■ XR_A#1(センター側 XR#1)の設定

「本装置の設定」

「本装置側の設定１」を選択します。

IKE/ISAKMPの設定1	
インターフェースのIPアドレス	203.xxx.xxx.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.xxx.xxx.117」

○上位ルータの IP アドレス　「%ppp0」

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

○インターフェースの ID　「空欄」

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

■ XR_A#2(センター側 XR#2)の設定

「本装置の設定」

「本装置側の設定１」を選択します。

IKE/ISAKMPの設定1	
インターフェースのIPアドレス	203.xxx.xxx.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.xxx.xxx.118」

○上位ルータの IP アドレス　「%ppp0」

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

○インターフェースの ID　「空欄」

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

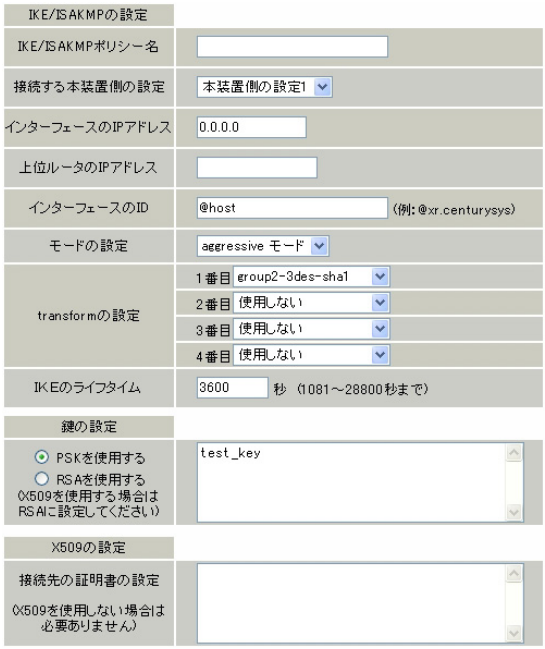
Ⅷ．IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

■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」

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)

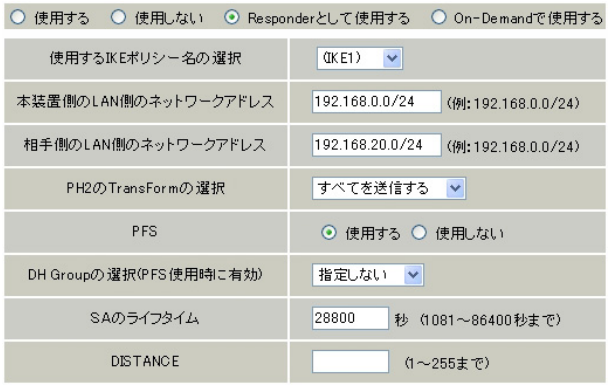
○鍵の設定
「PSK を使用する」を選択し、対向装置との共通鍵「test_key」を入力します。

■ XR_A#1,XR_A#2 の IPsec ポリシーの設定

「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）

■ XR_A#1,XR_A#2 の転送フィルタの設定

「転送フィルタ」の設定

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

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

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

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

○動作　「破棄」
※条件に合致するパケットを破棄。

○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、**メイン側XR(XR_A#1)**にも下記のような転送フィルタを設定してください。

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

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

○動作　「破棄」
※条件に合致するパケットを破棄。

○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。

■XR_A#1,XR_A#2のスタティックルートの設定

「スタティックルート」の設定

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

■ XR_A#1 のスタティックルート設定

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

○アドレス　「192.168.20.0」

○ネットマスク　「255.255.255.0」

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

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

■ XR_A#2 のスタティックルート設定

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

○アドレス　「192.168.20.0」

○ネットマスク　「255.255.255.0」

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

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

Ⅷ. IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

■ XR_A#1,XR_A#2 の IPSec Keep-Alive の設定

「IPSec Keep-Alive 設定」

さらに、障害時にすぐにフローティングスタティックルートへ切り替えるために、IPsec Keep-Alive を設定します。

(KeepAlive 機能を使用しない場合は、Rekey のタイミングまでフローティングできない場合があります。)

■ XR_A#1 の IPsec Keep-Alive 設定

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

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

■ XR_A#2 の IPsec Keep-Alive 設定

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

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

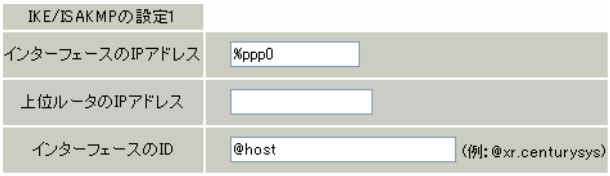
※注)
センター側と拠点側の interval が同じ値の場合、Keep-Alive の周期が同期してしまい、障害時の IPsec 切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec 通信が不安定になることがあります。
これを防ぐために、センター側の interval は拠点側のメイン SA, バックアップ SA のいずれの interval とも異なる値を設定することを推奨します。
ただし、センター内の XR 同士は同じ interval 値でも構いません。

Ⅷ. IPsec 設定例 2（センター／拠点間の 2 対 1 接続)

■ XR_B(拠点側 XR)の設定

「本装置の設定」

「本装置側の設定１」を選択します。



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

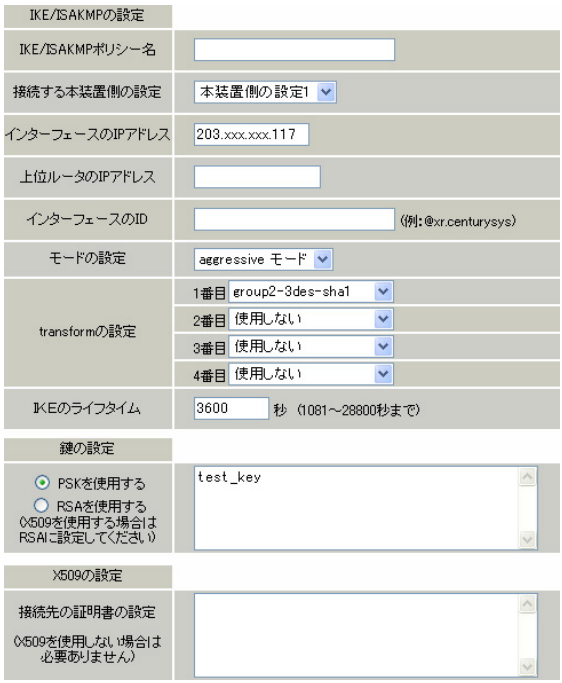
○上位ルータの IP アドレス　「空欄」
※ PPPoE 接続かつ動的アドレスの場合は、空欄にしてください。

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

メイン SA 用の IKE/ISAKMP ポリシーの設定をおこないます。

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。



○ IKE/ISAKMP ポリシー名　「(任意で設定します)」

○接続する本装置側の設定　「本装置側の設定1」

○インターフェースの IP アドレス　「203.xxx.xxx.117」
※対向装置が固定アドレスなので、その IP アドレスを設定します。

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

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

○モードの設定　「aggressive モード」

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

○ IKE のライフタイム　「3600」（任意の設定値）

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

Ⅷ．IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

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

「IKE/ISAKMP ポリシーの設定」

「IKE2」を選択します。

○ IKE/ISAKMP ポリシー名　「(任意で設定します)」

○接続する本装置側の設定　「本装置側の設定 1」

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

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

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

○モードの設定　「aggressive モード」

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

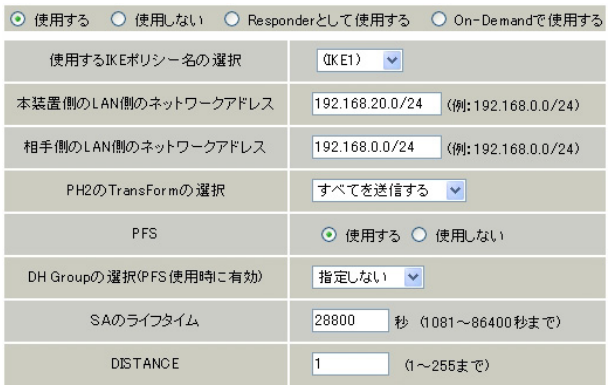
○ IKE のライフタイム　「3600」（任意の設定値）

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

メイン SA 用の IPsec ポリシーの設定をおこないます。

「IPSec ポリシーの設定」

「IPSec1」を選択します。



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

○使用する IKE ポリシー名の選択　「IKE1」

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

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

○ PH2 の TransForm の選択　「すべてを送信する」

○ PFS　「使用する」（推奨）

○ DH Group の選択　「指定しない」

○ SA のライフタイム　「28800」（任意の設定値）

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

Ⅷ．IPsec 設定例 2（センター／拠点間の 2 対 1 接続）

バックアップ SA 用の IPsec ポリシーの設定をおこないます。

「IPSec ポリシーの設定」

「IPSec2」を選択します。

○「Responder として使用する」を選択します。
※本装置は Initiator として動作しますが、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）　**※注)**
○watch count　「3」（任意の設定値）
○timeout/delay　「60」（任意の設定値）
○動作option 1　「空欄」
○動作option 2　「チェック」
○interface　「ipsec0」
○backupSA　「2」
※ Keep-Alive により障害検知した場合に、IPSec2 のポリシーに切り替えるため、“2”を設定します。

■バックアップ SA 用の KeepAlive の設定

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

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

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

IX．IPsec がつながらないとき

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

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

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

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

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

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

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

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

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

○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

XR-440 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。

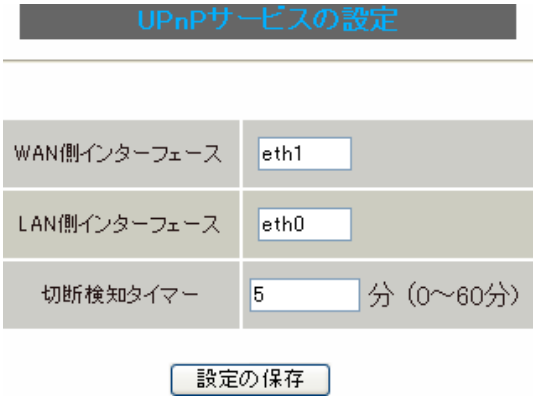
Windows OS の UPnP サービス

Windows XP 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

XR-440 の UPnP 機能の設定は以下の手順でおこなってください。

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



○WAN 側インターフェース
WAN側に接続しているインタフェースを設定します。本装置の各インタフェース名をそのまま入力してください。

○LAN 側インターフェース
LAN側に接続しているインタフェースを設定します。本装置の各インタフェース名をそのまま入力してください。

本装置の各インタフェース名は、「付録 A　インタフェース名一覧」を参照してください。

○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、XR-440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。

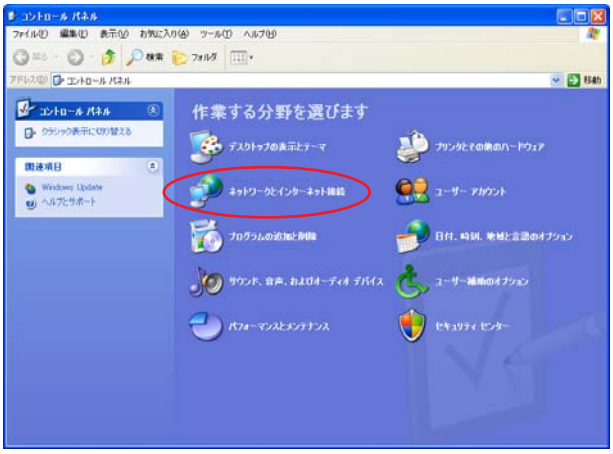
Ⅰ．UPnP 機能 の設定

◆ UPnP の接続状態の確認

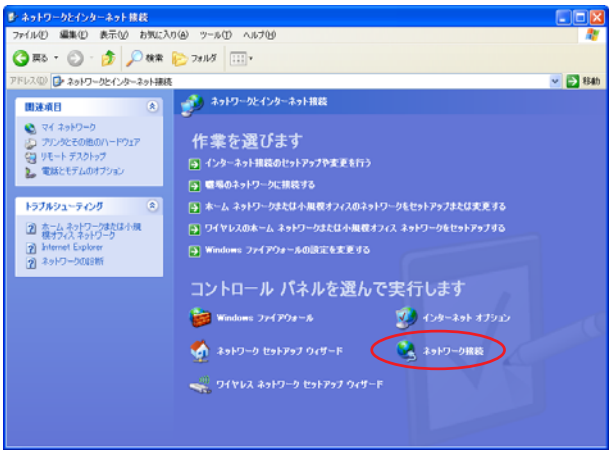
各コンピュータが本装置と正常に UPnP で接続されているかどうかを確認します。

1 「スタート」→「コントロール パネル」を開きます。

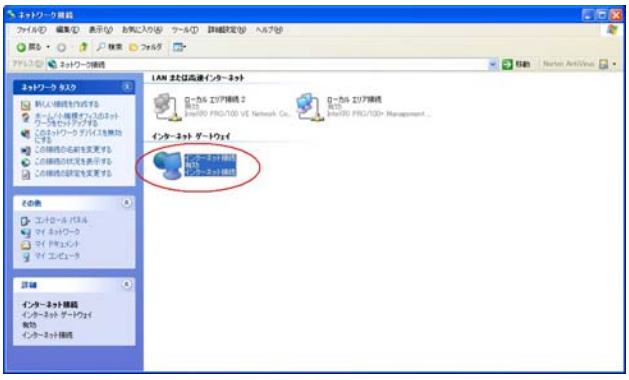
2 「ネットワークとインターネット接続」を開きます。



3 「ネットワーク接続」を開きます。



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



(画面は Windows XP での表示例です)

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

II．UPnP とパケットフィルタ設定

◆UPnP 機能使用時の注意

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

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

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

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

◆UPnP 機能使用時の推奨フィルタ設定

Microsoft Windows 上の UPnP サービスのバッファオーバフローを狙った DoS(サービス妨害)攻撃からの危険性を緩和する為の措置として、XR-440 は工場出荷設定で以下のようなフィルタをあらかじめ設定しています。

(入力フィルタ)

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

(転送フィルタ)

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

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

第 15 章

ダイナミックルーティング
(RIP/OSPF/BGP4)

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下記のプロトコルをサポートしています。

- RIP
- OSPF
- BGP4

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

設定の開始

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

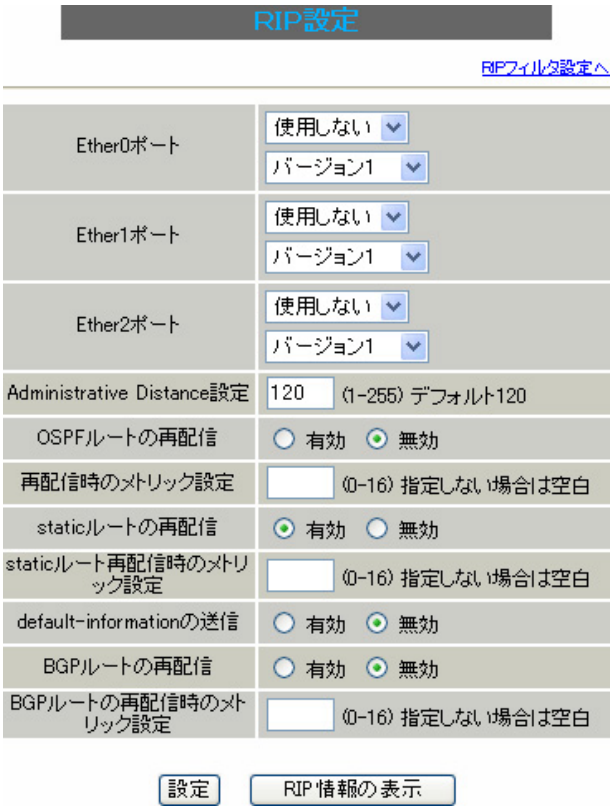
2 「RIP」、「OSPF」、「BGP4」のいずれかをクリックして、それぞれの機能の設定画面で設定をおこないます。

II．RIP の設定

RIP の設定

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

◆RIP 設定



○Ether0 ポート、Ether1 ポート、Ether2 ポート
XR-440 の各 Ethernet ポートで、RIP を「使用しない」か、使用する(「送受信」)を選択します。
また、RIP を使用する場合の RIP バージョン(「バージョン 1」、「バージョン 2」、「Both 1 and 2」）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、その際は本項目の値が小さい方を経路として採用します。

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

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

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

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

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。

II．RIPの設定

◆RIPフィルタの設定

RIPによるroute情報の送信、または受信をおこないたくない場合に設定します。

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

○NO.
設定番号を指定します。1-64の間で指定します。

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

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

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

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

入力後は「追加」をクリックしてください。

「取消」をクリックすると、入力内容がクリアされます。

RIPフィルタ設定後は、ただちに設定が有効となります。

設定後は､画面上部に設定内容が一覧表示されます。

(画面は表示例です)

[編集 削除]欄

○削除
クリックすると、設定が削除されます。

○編集
クリックすると、その設定について内容を編集できます。

III．OSPF の設定

OSPF の設定

OSPF はリンクステート型経路制御プロトコルです。

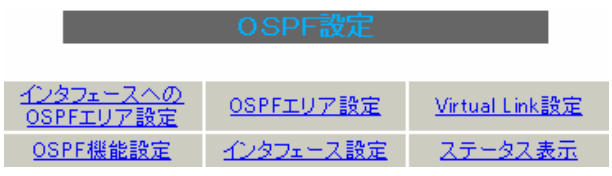
OSPF では各ルータがリンクステートを交換し合い、そのリンクステートをもとに、他のルータがどこに存在するか、どのように接続されているか、というデータベースを生成し、ネットワークトポロジを学習します。

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

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

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

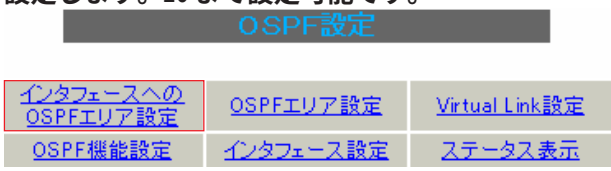
OSPF 設定は、Web 設定画面「各種サービスの設定」→画面左「ダイナミックルーティング」→「OSPF」をクリックします。
ここで各種設定をおこないます。



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

◆インタフェースへの OSPF エリア設定

どのインタフェースで OSPF 機能を動作させるかを設定します。10 まで設定可能です。



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

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

○ AREA 番号
そのネットワークのエリア番号を指定します。

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

入力後は「設定」をクリックして設定完了です。

III．OSPF の設定

◆OSPF エリア設定

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

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

○ AREA 番号
機能設定をおこなうエリアの番号を指定します。

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

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

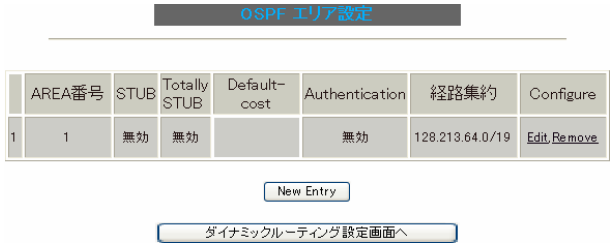
○ default-cost 設定
スタブエリアに対してデフォルトルート情報を送信する際のコスト値を指定します。
指定しない場合、設定内容一覧では空欄で表示されますが、実際は 1 で機能します。

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

○エリア間ルートの経路集約設定
経路情報を集約して送信したいときに設定します。
＜設定例＞
128.213.64.0～128.213.95.0 のレンジのサブネットを渡すときに 1 つずつ渡すのではなく、128.213.64.0/19 に集約して渡す、といったときに使用します。
ただし、連続したサブネットでなければなりません(レンジ内に存在しないサブネットがあってはいけません)。

入力後は「設定」をクリックしてください。

設定後は「OSPF エリア設定」画面に、設定内容が一覧で表示されます。



(画面は表示例です)

[Configure]欄

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

○ Remove
クリックすると設定の「削除」をおこなえます。

III．OSPFの設定

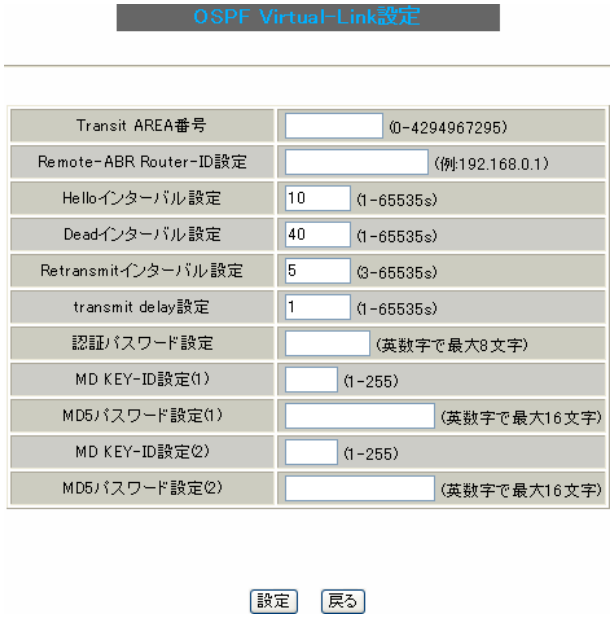
◆Virtual Link設定

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

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

設定画面上部の「Virtual Link設定」をクリックして設定します。

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



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

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

○Helloインターバル設定
Helloパケットの送出間隔を設定します。

○Deadインターバル設定
Deadタイムを設定します。

○Retransmitインターバル設定
LSAを送出する間隔を設定します。

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

○認証パスワード設定
Virtual Link上でsimpleパスワード認証を使用する際のパスワードを設定します。
半角英数字のみ使用できます。

○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。
半角英数字のみ使用できます。

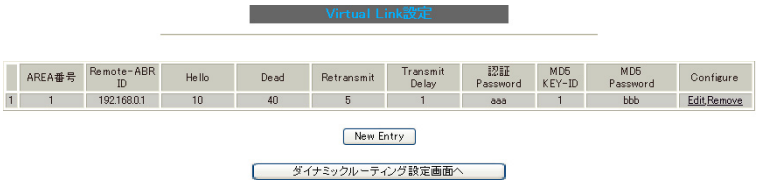
○MD5 KEY-ID設定(2)
○MD5 パスワード設定(2)
MD5 KEY-IDとパスワードは2つ同時に設定可能です。
その場合は(2)に設定します。
半角英数字のみ使用できます。

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。

III．OSPFの設定

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



(画面は表示例です)

[Configure]欄

○ Edit

クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○ Remove

クリックすると設定の「削除」をおこなえます。

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

◆OSPF機能設定

「OSPF機能設定」でOSPFの動作について設定します。

○ Router-ID設定

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

○ Connected再配信

connectedルートをOSPFで配信するかどうかを選択します。

「有効」にした場合は以下の2項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプtype1、type2を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

III．OSPF の設定

○ static ルート再配
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。

○ RIP ルートの再配信
RIP で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。

○ BGP ルートの再配信
BGP で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。

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

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

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

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

○ Default-information
デフォルトルートを OSPF で配信するかどうかを選択します。

・送信しない
・送信する
ルータがデフォルトルートを持っていれば送信されます。
・常に送信
デフォルトルートの有無にかかわらず、自分にデフォルトルートを向けるように、OSPF で配信します。

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

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

b. メトリック値
配信する際のメトリック値を設定します。

○ 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。

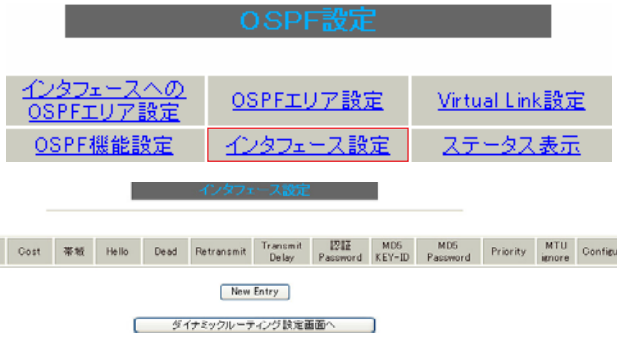
○バックアップ切替え監視対象Remote Router-ID設定
OSPF Helloによるバックアップ回線切り替え機能を使用する際に、Neighbor が切れたかどうかをチェックする対象のルータを判別するために、対象のルータの IP アドレスを設定します。
バックアップ機能を使用しない場合は、設定する必要はありません。

入力後は「設定」をクリックしてください。

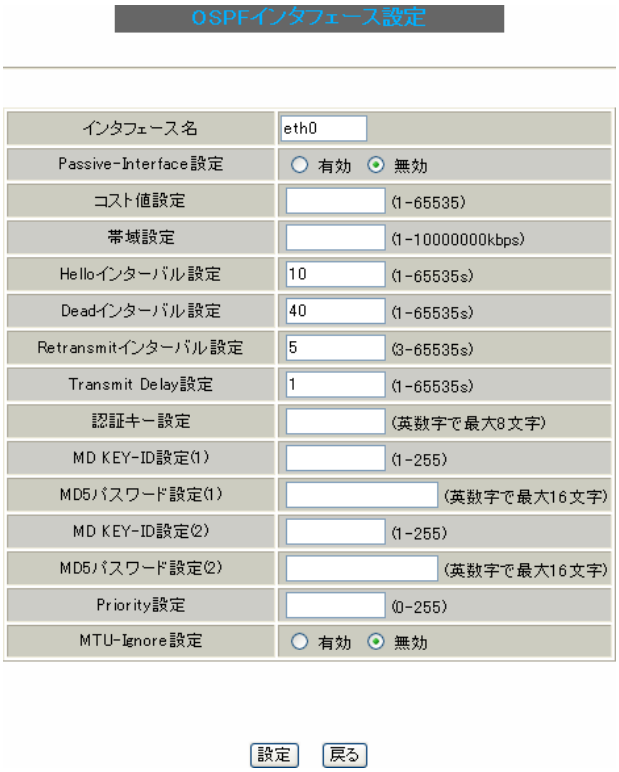
III．OSPFの設定

◆インタフェース設定

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



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



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

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

○コスト値設定
コスト値を設定します。

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

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

○Deadインターバル設定
Deadタイムを設定します。

○Retransmitインターバル設定
LSAの送出間隔を設定します。

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

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

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

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

III．OSPF の設定

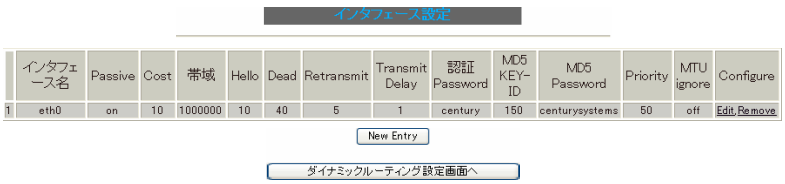
○MD KEY-ID 設定(2)
○MD5 パスワード設定(2)
MD5 KEY-IDとパスワードは2つ同時に設定可能です。
その場合は(2)に設定します。

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

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

入力後は「設定」をクリックしてください。

設定後は「インタフェース設定」画面に、設定内容が一覧で表示されます。



(画面は表示例です)

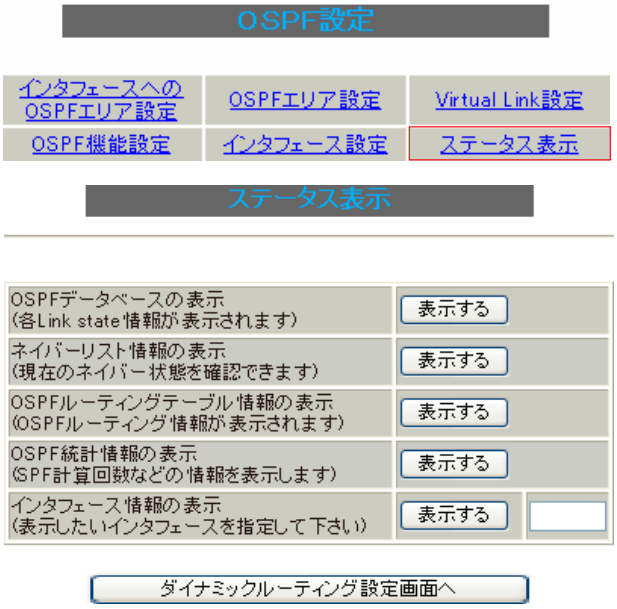
[Configure]欄

○Edit
クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○Remove
クリックすると設定の「削除」をおこなえます。

◆ステータス表示

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



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

○ネイバーリスト情報の表示
現在のネイバー状態が表示されます。

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

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

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

表示したい情報の項目にある「表示する」をクリックしてください。

IV．BGP4 の設定

BGP の設定

ダイナミックルーティングの「BGP4」をクリックして、各種設定をおこないます。

ただし、BGP4 の各種設定をおこなう前に、BGP4 を起動させる必要があります。
BGP4 が起動していないときは、設定はできません。

BGP4 が停止中に「BGP4」設定画面を開くと以下の画面が表示されます。

◆ BGP4 の起動

Web 設定画面「各種サービスの設定」→「ダイナミックルーティング」を開きます。

BGP4 の起動

「BGP4」の「起動」にチェックし、「動作変更」ボタンをクリックします。

BGP4 の停止

「BGP4」の「停止」にチェックし、「動作変更」ボタンをクリックします。

BGP4 の再起動

「BGP4」の「再起動」ボタンをクリックします。

ダイナミックルーティングの全てを再起動する場合は、画面最下部にある「再起動」ボタンをクリックします。

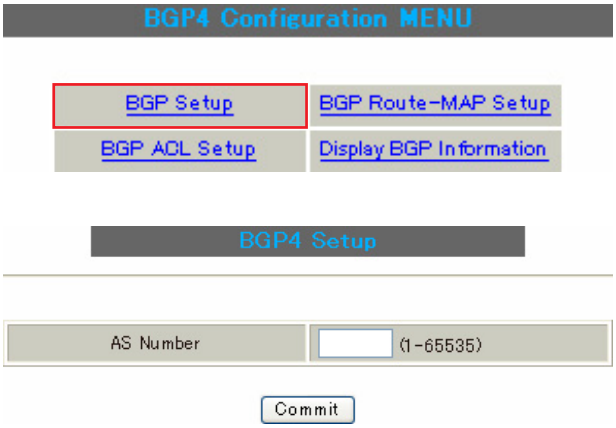
ダイナミックルーティング設定一覧の「BGP4」をクリックすると、BGP4 の各種設定画面に移ることができます。

Ⅳ．BGP4 の設定

◆BGP Setup

はじめに BGP4 の AS 番号を設定し、各種設定をおこないます。

BGP4 Configuration MENU 画面の「BGP Setup」をクリックします。



○AS Number

AS 番号を設定します。

1-65535 の間で設定してください。

入力後は「commit」ボタンをクリックします。

BGP AS 番号を設定すると、引き続き、以下の各種設定ができるようになります。

- **BGP 機能設定**
- **BGP Aggregate Setup**
- **BGP neighbor Setup**
- **BGP network Setup**

BGP4 機能設定（◆BGP4 Setup）

Router-ID やルート情報再配信などの設定をおこないます。

AS 番号を設定後、「BGP4 Setup」画面に表示される「BGP 機能設定」を開き、以下の画面で設定します。

（画面は表示例です）

○AS Number ： X

「BGP4 Setup」で設定したAS番号(X)が表示されます。

○Remove

設定を削除する場合は、「Remove」をクリックしてください。

※ BGP AS 番号自体が削除され、「BGP4 Setup」設定トップ画面に戻ります。

○Router-ID

Router-ID を IP アドレス形式で設定します。

IV．BGP4 の設定

○ Scan Time
Scan Time を設定します。
5-60 秒の間で設定してください。

○ 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、routemap を適用するときは、「route-map 設定」欄に routemap 名を設定してください。

○ static ルート再配信
Static ルートを BGP4 で再配信したい場合には「有効」を選択します。
また、routemap を適用するときは、「route-map 設定」欄に routemap 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、routemap を適用するときは、「route-map 設定」欄に routemap 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、routemap を適用するときは、「route-map 設定」欄に routemap 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。
設定可能な範囲は 0-4294967295 です。デフォルト値は「100」です。

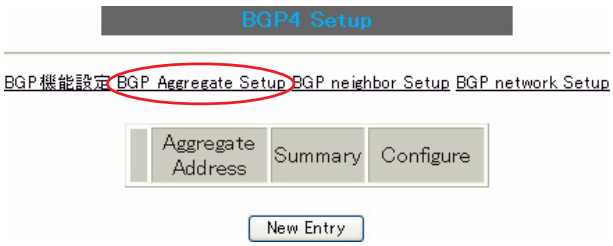
設定後は「Commit」ボタンをクリックしてください。

Ⅳ．BGP4 の設定

BGP Aggregate Setup（◆BGP4 Setup）

Aggregate Address の設定をおこないます。

AS 番号を設定後、「BGP4 Setup」画面に表示される「BGP Aggregate Setup」を開きます。



新規に設定するときは「New Entry」をクリックして「BGP4 Aggregate Setup」設定画面を開きます。

○ 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に「有効」を選択してください。

設定後「設定」ボタンをクリックしてください。
設定後は「BGP Aggregate Setup」画面に、設定内容が一覧で表示されます。

(画面は表示例です)

[Configure]欄

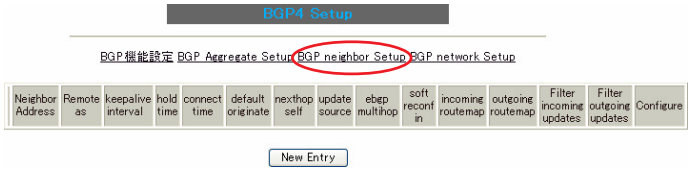
○ Edit
クリックすると設定内容の「編集」をおこなえます。

○ Remove
クリックすると設定の「削除」をおこなえます。

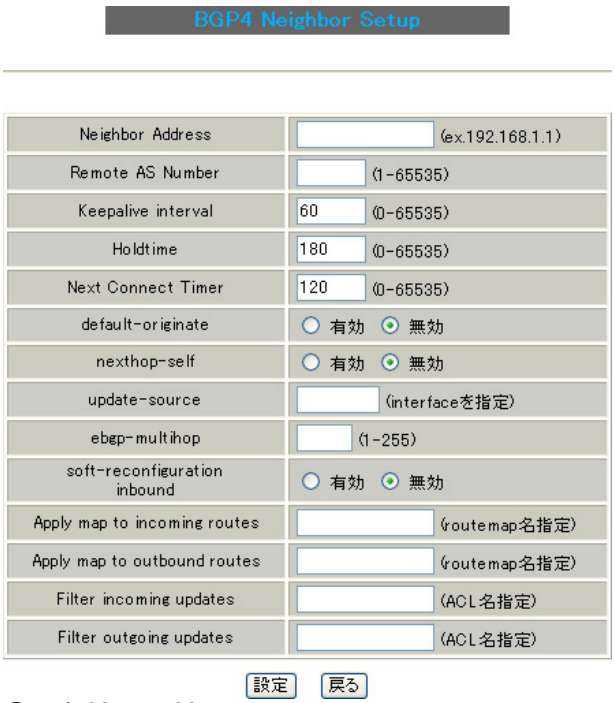
BGP neighbor Setup（◆BGP4 Setup）

Neighbor Address の設定をおこないます。

AS 番号を設定後、「BGP4 Setup」画面に表示される「BGP neighbor Setup」を開きます。



新規に設定するときは「New Entry」をクリックして「BGP neighbor Setup」設定画面を開きます。



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

○ Remote AS Number
対向装置の AS Number 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 です。

○ Holdtime
Holdtime を設定します。
入力可能な範囲は 0.3-65535 です。

IV．BGP4 の設定

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

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

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

○ update-source
BGP パケットのソースアドレスを、指定したインタフェースの IP アドレスに変更します。
インタフェース名を指定してください。本装置のインタフェース名については、「付録 A インタフェース名一覧」をご参照ください。

○ ebgp-multihop
「有効」を選択すると、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。

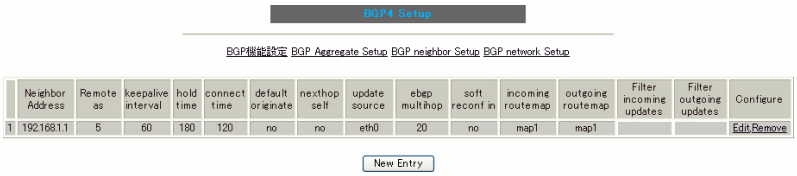
○ soft-reconfiguration inbound
「有効」を選択すると BGP Session をクリアせずに、ポリシーの変更をおこないます。

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

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

設定後「設定」ボタンをクリックしてください。

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



(画面は表示例です)

[Configure]欄
○ Edit
クリックすると設定内容の「編集」をおこなえます。

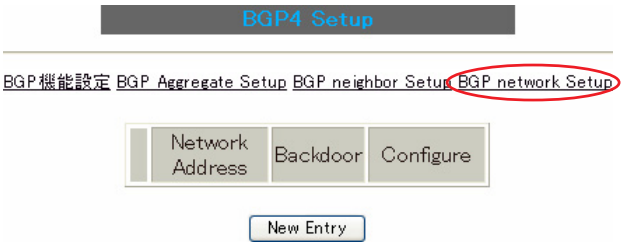
○ Remove
クリックすると設定の「削除」をおこなえます。

Ⅳ．BGP4 の設定

BGP network Setup (◆BGP4 Setup)

Network Address の設定をおこないます。

AS 番号を設定後、「BGP4 Setup」画面に表示される「BGP network Setup」を開きます。



新規に設定するときは「New Entry」をクリックして「BGP network Setup」設定画面を開きます。

○ Speficy a network to announce via BGP
BGPにより配信した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」にします。

設定後は「設定」ボタンをクリックしてください。
設定後は「BGP network Setup」画面に、設定内容が一覧で表示されます。

(画面は表示例です)

[Configure]欄

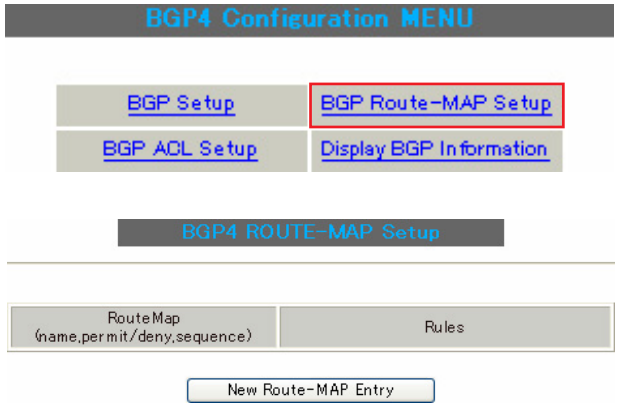
○ Edit
クリックすると設定内容の「編集」をおこなえます。

○ Remove
クリックすると設定の「削除」をおこなえます。

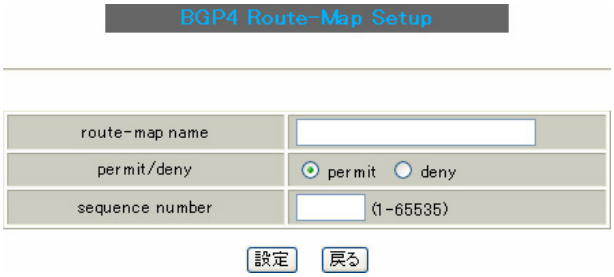
◆BGP Route-MAP Setup

Route-MAP の設定をおこないます。

BGP4 Configuration MENU 画面の「BGP Route-MAP Setup」をクリックして設定します。



新規に設定するときは「New Route-MAP Entry」をクリックしてください。



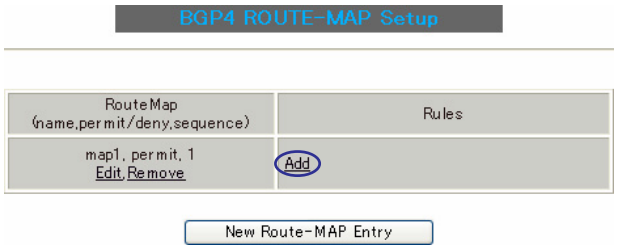
○ route-map name
Route-MAP の名前を設定します。

○ 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。
“match”条件、“set”アクションの設定については後述の「BGP4 Route-MAP Rules」設定画面で設定します。

○ 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。

IV．BGP4 の設定

設定後「設定」ボタンをクリックしてください。
設定後は「BGP4 ROUTE-MAP Setup」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)

[RouteMap]欄

○ Edit

クリックすると設定内容の「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。

続いて「BGP4 Route-MAP Rules」の設定をおこないます。

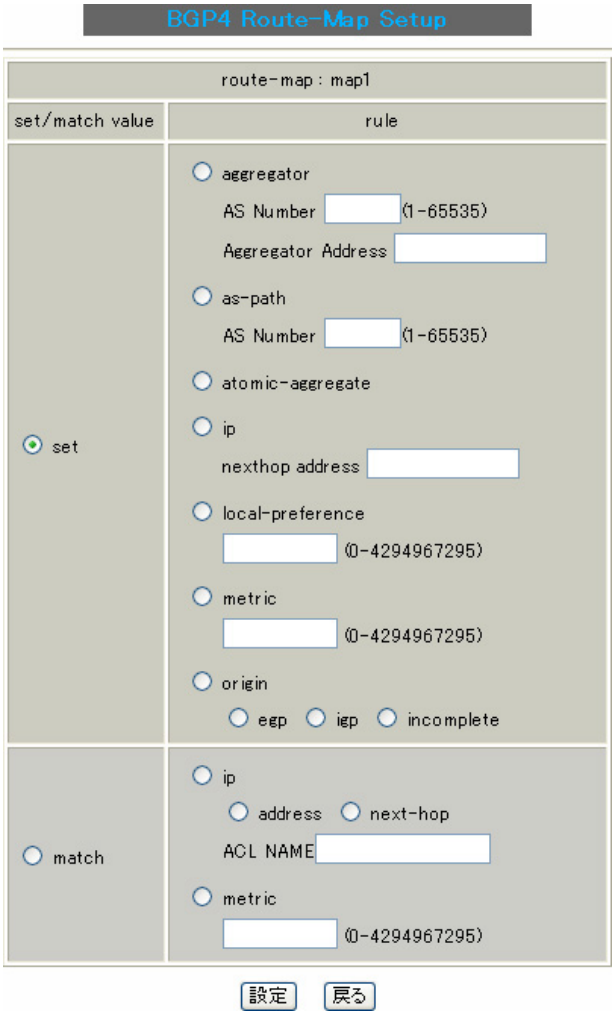
Rules

Route-MAP は、“ match ” と “ set ” 条件設定のリストで作られます。

「match」
match 条件を設定します。

「set」
match 条件によって一致したときの set アクションを設定します。

“ match ” と “ set ” の条件設定は、「BGP4 ROUTE-MAP Setup」設定の一覧表示から、[Rules]欄の「Add」（左図：表示例の青印）をクリックして、以下の画面でおこないます。



○ route-map ： XXXX
「BGP Route-MAP Setup」で設定した Route-MAP 名(XXXX)が表示されます。

○ set
match条件にヒットした場合の属性値を設定します。
以下のものが設定できます。

○ aggregator
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。
「AS Number」欄に AS 番号(1-65535)を、
「Aggregator Address」欄に IP アドレスを設定します。

○ as-path
AS 番号を付加します。
「AS Number」欄にAS番号(1-65535)を設定します。

○ atomic-aggregate
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。

○ ip
ネクストホップの IP アドレスを付加します。
「nexthop address」欄に IP アドレスを設定してください。

○ local-preference
Local Preference 属性を付加します。
Local Preference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 は、経路の生成元を示す属性です。

- egp
  経路情報を EGP から学習したことを示します。
- igp
  経路情報を AS 内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。

○ match
match 条件として設定する場合はチェックを入れてください。条件は以下の 3 つが設定できます。

○ ip
チェックを入れたら「address」か「next-hop」を選択してください。

- 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。また、match 条件となるアクセスリスト名を「ACL NAME」欄に入力してください。
- 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。また、match 条件となるアクセスリスト名を「ACL NAME」欄に入力してください。

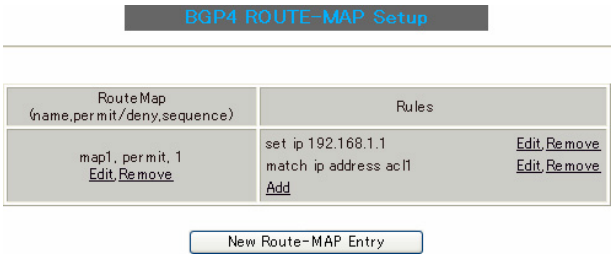
○ metric
ここで指定した metric 値を match 条件とします。
入力可能な範囲は 0-4294967295 です。

設定後「追加」ボタンをクリックし、設定を保存します。

“ match ”または“ set ”は、**１回の設定で１つの条件設定を保存します。**

Ⅳ．BGP4 の設定

設定後は「BGP4 ROUTE-MAP Setup」画面の[Rules]欄に、設定内容が一覧で表示されます。



(画面は表示例です)

[Rules]欄

○ Edit

クリックすると条件設定の内容「編集」をおこなえます。

○ Remove

クリックすると条件設定の「削除」をおこなえます。

○ Add

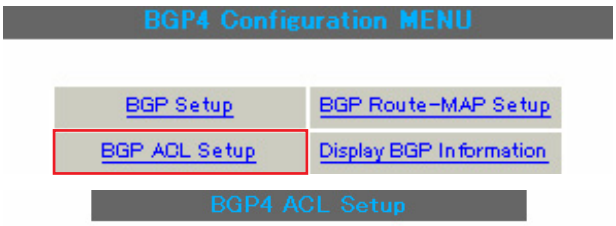
クリックすると新しい条件設定の「追加」をおこなえます。

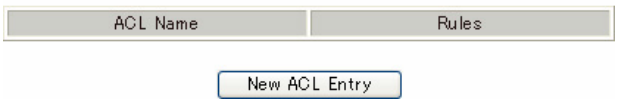
条件リストは、設定した順に表示されます。

◆BGP4 ACL Setup

BGP4 の ACL(ACCESS-LIST)設定をおこないます。

BGP4 Configuration MENU画面の「BGP4 ACL Setup」をクリックします。





新規に設定するときは「New ACL Entry」をクリックして設定します。

○ access-list name

任意の ACL 名を設定してください。

半角英数字で 32 文字まで設定できます。

入力後「設定」ボタンをクリックします。

設定後は「BGP4 ACL Setup」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)

[ACL Name]欄

○ Edit

クリックすると設定内容の「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。

Ⅳ．BGP4 の設定

続いて「BGP4 ACL Rules」の設定をおこないます。

Rules

BGP4 の ACL の条件設定は、「BGP4 ACL Setup」設定の一覧表示から、[Rules]欄の「Add」をクリックして、以下の画面でおこないます。

○acl name : XXXX
「BGP4 ACL Setup」で設定した ACL 名(XXXX)が表示されます。

○permit/deny
permit(許可)/deny(拒否)条件を選択します。

○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」の形式で設定してください。

設定後「追加」ボタンをクリックし、設定を保存します。

設定後は「BGP4 ACL Setup」画面の[Rules]欄に、設定内容が一覧で表示されます。

(画面は表示例です)

[Rules]欄
○Add
クリックすると新しい ACL 設定の「追加」をおこなえます。
ACL は設定した順に表示されます。

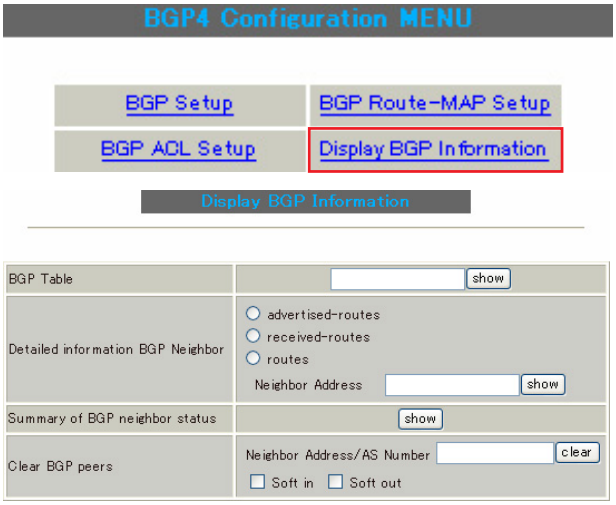
※ ACL Rules 設定を削除する場合は、[ACL Name]欄の「Remove」をクリックして、[ACL Name]ごと削除してください。

IV．BGP4の設定

◆Display BGP Information

BGP4の各種情報表示をおこないます。

BGP4 Configuration MENU画面の「Display BGP Information」をクリックします。



◯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のみ表示します。

◯Detailed information BGP Neighbor

BGP Neighborの詳細情報を表示します。
「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。

・advertised-routes
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
BGP Neighborルータから受け取ったルート情報を表示します。

・routes
BGP Neighborから学習したロート情報を表示します。

◯Summary of BGP neighbor status

BGP Neighborのステータスを表示します。

各表示項目を選択後は「show」ボタンをクリックしてください。新しいウィンドウが開いて選択した設定情報が表示されます。

◯Clear BGP peers

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

また、BGP soft reconfigもできます。
BGP soft reconfigは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します。
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。

選択後は「clear」ボタンをクリックしてください。
BGP peer情報が削除されます。

第 16 章

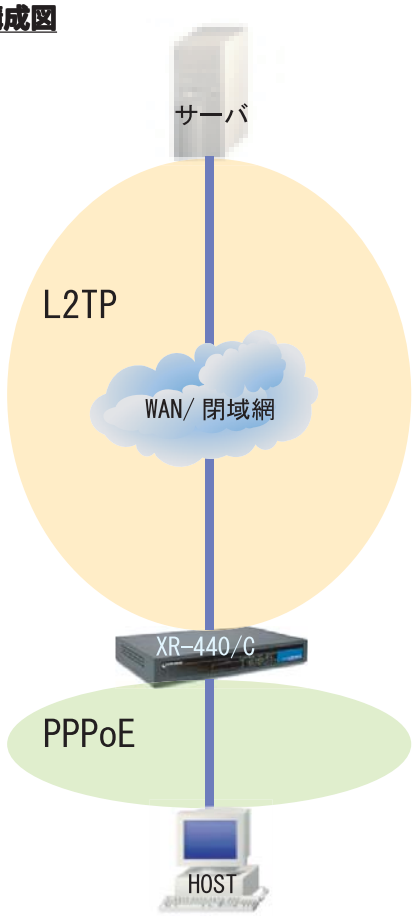
PPPoE to L2TP

PPPoE to L2TP機能について

PPPoE to L2TP機能は、L2TPトンネルを経由してのPPPoE接続を可能にするものです。

構成は以下のようなものになります。

構成図

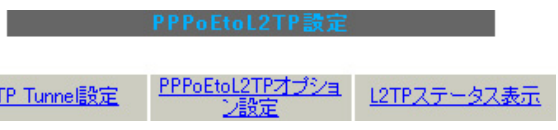


・HOSTからサーバへPPPoE接続をおこないますが、XR-440とサーバ間はL2TPでの通信に変換します。HOSTはPPPoE接続を維持します。

・**XR-440は上記構成図におけるサーバになることはできません。**

PPPoE to L2TP設定

設定はWeb設定画面「各種サービスの設定」→「PPPoE to L2TP」をクリックしておこないます。



◆L2TP Tunnel設定

「PPPoEtoL2TP」設定画面→「L2TP Tunnel設定」を開きます。

新規で設定するときは「New Entry」をクリックします。

○Description
任意の設定名をつけます(省略可能)。

○Peerアドレス
L2TPで接続するサーバのIPアドレスを入力します。

○パスワード
L2TP接続時のパスワードを入力します。

○ポート番号
ポート番号を入力します。
通常は初期設定1701を使用します。

○AVP Hiding設定
AVP Hidingの使用/不使用を選択します。

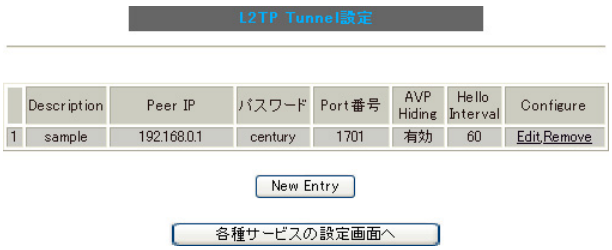
○Hello Interval設定
Helloパケットの送信間隔を設定します(単位:秒)。

最後に「設定」をクリックします。

PPPoE to L2TP 機能について

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。

設定後は「L2TP Tunnel 設定」画面に設定内容が一覧表示されます。



（画面は表示例です）

[Configure]欄

○ Edit
クリックすると設定内容の「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。

◆ PPPoEtoL2TP オプション設定

「PPPoEtoL2TP」→「PPPoEtoL2TP オプション設定」を開きます。

○ Local hostname
任意の Local host 名をつけます。

○ PPPoE Frame 受信インタフェース設定
PPPoE フレームを受信するインタフェースを選択します。
PPPoE クライアントが接続されている側のインタフェースを選択してください。

○ MAX Session 数
PPPoE to L2TP 接続での最大セッション数を設定します。

○ Path MTU Discovery
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、本装置が送信する L2TP 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。

○ Debug 設定(Syslog メッセージ出力設定)
syslog に出力する Debug ログの種類を以下の４つから選択します。

- Tunnel Debug 出力
- Session Debug 出力
- L2TP エラーメッセージ出力
- PPPoE Debug 出力

PPPoE to L2TP 機能について

最後に「設定」をクリックします。

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。

◆L2TP ステータス表示

「PPPoEtoL2TP」→「L2TP ステータス表示」をクリックするとウィンドウがポップアップし、L2TP のステータス情報を確認できます。

第 17 章

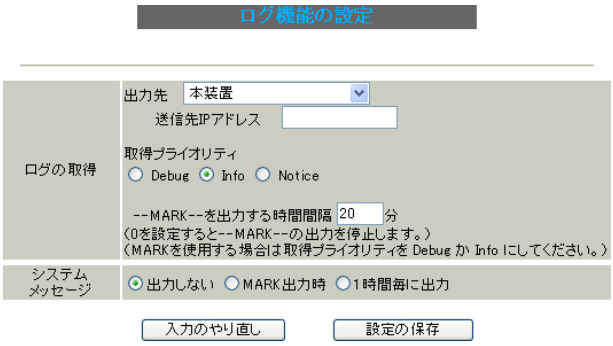
SYSLOG サービス

syslog 機能の設定

XR-440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。
電子メール設定は「第 33 章 各種システム設定」を参照してください。

syslog 取得機能の設定

Web 設定画面「各種サービスの設定」→「SYSLOG サービス」をクリックして、以下の画面から設定をおこないます。



<ログの取得>

○出力先
syslog の出力先を選択します。

「本装置」
本装置で syslog を取得する場合に選択します。

「SYSLOG サーバ」
syslog サーバに送信するときに選択します。

「本装置と SYSLOG サーバ」
本装置と syslog サーバの両方で syslog を管理します。

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。

○送信先 IP アドレス
出力先で「SYSLOG サーバ」または「本装置と SYSLOG サーバ」を指定した場合に、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通りです。

- 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。
取得プライオリティを「Debug」「Info」またはに設定したときのみ MARK が出力されます。
初期設定は 20 分です。

<システムメッセージ>
本装置のシステム情報を定期的に出力することができます。
以下から選択してください。

○出力しない
システム情報を出力しません。

○ MARK 出力時
システム情報を“ --MARK-- ”の出力と同時に出力します。

○１時間毎に出力
システム情報を１時間毎に出力します。

最後に「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを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。

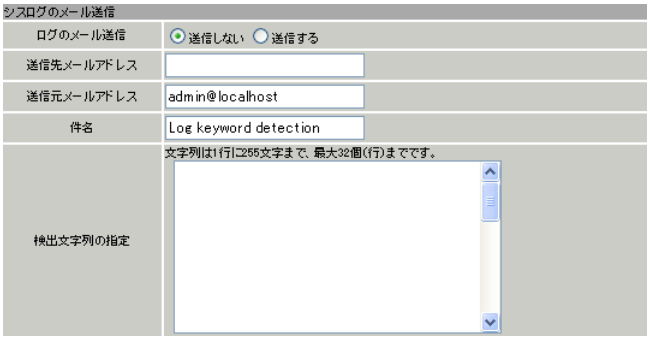
syslog 機能の設定

syslog のメール送信機能の設定

ログの内容を電子メールで送信したい場合の設定です。

Web 設定画面「システム設定」→「メール送信機能の設定」をクリックして以下の画面で設定します。

<シスログのメール送信>



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

ログファイルの取得

記録した syslog は、設定画面「システム設定」→「ログの表示」に表示されます。

ローテーションで記録されたログは圧縮して保存されます。
保存されるファイルは最大で 6 つです。

本装置では、初期化済みのオプション CF カードを装着している場合、ログは自動的に CF カードに記録されます。

保存最大容量を超えると、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。

システムログ内容

本装置で出力される情報は下記の内容です。

```
Nov  7 14:57:44 localhost system: cpu:0.00
mem:28594176 session:0/2
```

・cpu:0.00
cpu のロードアベレージです。
1 に近いほど高負荷を表し、1 を超えている場合は過負荷の状態を表します。

・mem:28594176
空きメモリ量(byte)です。

・session:0/2　(XX/YY)
本装置内部で保持している NAT および IP マスカレード のセッション情報数です。

0 (XX)：現在 Establish している TCP セッションの数

2 (YY)：本装置が現在キャッシュしている全てのセッション数

ファシリティと監視レベルについて

XR-440 で設定されている syslog のファシリティ・監視レベルおよび出力先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**

[出力先]
/var/log/messages

第 18 章

攻撃検出機能

攻撃検出機能の設定

攻撃検出機能の概要

攻撃検出機能とは、外部から LAN への侵入や XR-440 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。

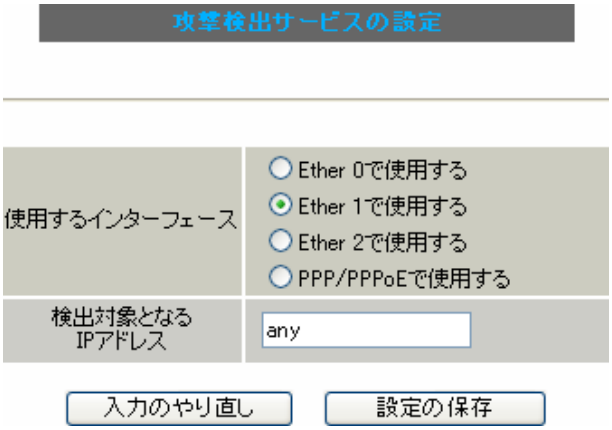
XR-440 ではあらかじめ検出ルールを定めていますので、パターンマッチングによって不正アクセスを検出します。
ホスト単位の他、ネットワーク単位で監視対象を設定できます。

ログの出力

攻撃検出ログは、システムログの中に統合されて出力されます。
「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、以下の画面から設定します。



○使用するインターフェース
DoSの検出をおこなうインタフェースを選択します。PPPoE/PPP 接続しているインタフェースで検出する場合は「PPP/PPPoE で使用する」を選択してください。

○検出対象となる IP アドレス
攻撃を検出したいホストの IP アドレスか、ネットワークアドレスまたは、全ての IP アドレスを指定できます。

< 入力例 >

ホスト単体の場合 ： **192.168.0.1/32**
(“ /32 ” を付ける)

ネットワーク単位の場合 ： **192.168.0.0/24**
(“ / ネットマスク ”を付ける)

すべての IP アドレスの場合 ： **any**
「any」を入力すると、すべてのアドレスが検出対象となります。そのため通常のアクセスも攻撃として誤検知する場合があります。

入力が終わりましたら「設定の保存」をクリックして設定完了です。
機能を有効にするには「各種サービスの設定」トップに戻り、サービスを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 19 章

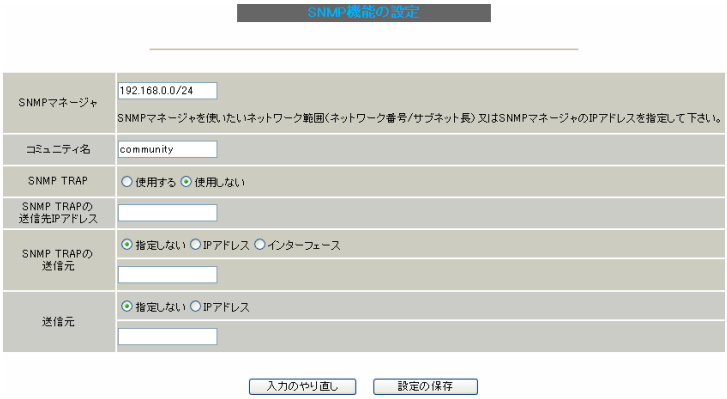
SNMP エージェント機能

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 XR-440 の MIB Ver.2(RFC1213)の情報を取得することができます。

設定方法

Web 設定画面「各種サービスの設定」→「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。

○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。

○ SNMP TRAP
SNMP TRAP を送信する場合は「使用する」選択します。

○ SNMP TRAP の送信先 IP アドレス
SNMP TRAP の送信先(SNMP マネージャ)の IP アドレスを指定します。

○ SNMP TRAP の送信元
Trap フレーム内の Agent address を指定することができます。

・指定しない
本装置の IP アドレスが自動的に設定されます。

・IP アドレス
IP アドレスで指定します。
入力欄に本装置のIPアドレスを設定してください。

・インターフェース
インタフェースで指定します。
入力欄に本装置のインタフェース名を入力してください。入力可能なインタフェースは、本装置の Ethernet と PPP です。

○送信元
SNMP RESPONSE パケットの送信元アドレスを設定します。
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、入力欄に IPsec SA 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。

「SNMP TRAP の送信元」または「送信元」を変更した場合、機能を有効にするにはサービスの再起動が必要です。「各種サービスの設定」トップに戻り、サービスを起動しなおしてください。

SNMP エージェント機能の設定

SNMP TRAP を送信するトリガーについて

以下のものに関して、SNMP TRAP を送信します。

- Ethernet インタフェースの up、down
  (但し、eth2 インタフェースは除きます)
- 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 /DHCP リレー
  PLUTO(IPSec の鍵交換をおこなう IKE 機能)
  UPnP
  RIP
  OSPF
  BGP4
  PPPoE to L2TP
  SYSLOG
  攻撃検出
  NTP
  VRRP
- SNMP TRAP 自身の起動、停止

第 20 章

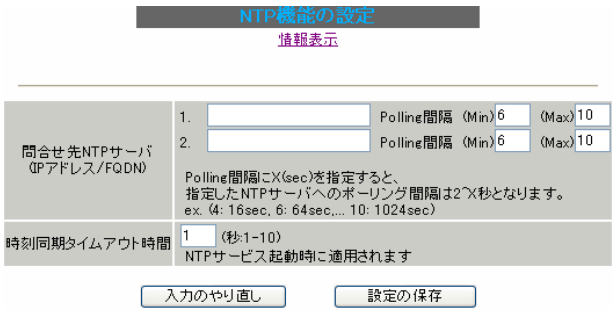
NTP サービス

NTP サービスの設定方法

XR-440 は、NTP クライアント / サーバ機能を持っています。
インターネットを使った時刻同期の手法の一つである NTP(Network Time Protocol)を用いて NTP サーバと通信をおこない、時刻を同期させることができます。

設定方法

Web 設定画面「各種サービスの設定」→「NTP サービス」をクリックして以下の画面で NTP 機能の設定をします。



[問合せ先 NTP サーバ (IP アドレス /FQDN)]
○1.
○2.
NTP サーバの IP アドレスもしくは FQDN を設定「1.」もしくは「2.」入力欄に記入します。
２箇所の NTP サーバ設定が可能です。
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 サーバを指定しない場合、本装置は NTP サーバとしてのみ動作します。

○ Polling 間隔(Min)/(Max)
NTP サーバと通信をおこなう間隔を設定します。
サーバとの接続状態により､指定した最小値(Min)と最大値(Max)の範囲でポーリングの間隔を調整します。

Polling 間隔 X(sec)を指定した場合、秒単位での間隔は 2 の X 乗(秒)となります。
指定可能な範囲は 4 ～ 17(16 ～ 131072 秒)です。

＜例＞ X=4：16 秒、X=6：64 秒、...X=10：1024 秒

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、初め 64 秒間隔で NTP サーバとポーリングをおこない、その後は 64 秒から 1024 秒の間で NTP サーバとポーリングをおこない、時刻のずれを徐々に補正していきます。

[時刻同期タイムアウト時間]
サーバ応答の最大待ち時間を 1-10 秒の間で設定できます。

注）時刻同期の際、内部的には NTP サーバに対する時刻情報のサンプリングを 4 回おこなっています。
本装置から NTP サーバへの同期がおこなえない状態では、サービス起動時に NTP サーバの１設定に対し「(指定したタイムアウト時間)×4」秒程度の同期処理時間が掛かる場合があります。

入力が終わりましたら「設定の保存」をクリックして設定完了です。
機能を有効にするには「各種サービスの設定」トップに戻り、サービスを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。

NTP サービスの設定方法

基準 NTP サーバについて

基準となる NTP サーバには次のようなものがあります。

- ntp1.jst.mfeed.ad.jp (210.173.160.27)
- ntp2.jst.mfeed.ad.jp (210.173.160.57)
- ntp3.jst.mfeed.ad.jp (210.173.160.87)

注）サーバを FQDN で指定するときは、「各種サービスの設定」画面の「DNS サーバ」を起動しておきます。

NTP クライアントの設定方法

各ホスト / サーバーを NTP クライアントとして本装置と時刻同期させる方法は、OS により異なります。

Windows 9x/Me/NT の場合

これらの OS では NTP プロトコルを直接扱うことができません。
フリーウェアの NTP クライアント・アプリケーション等を入手してご利用ください。

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 21 章

VRRP サービス

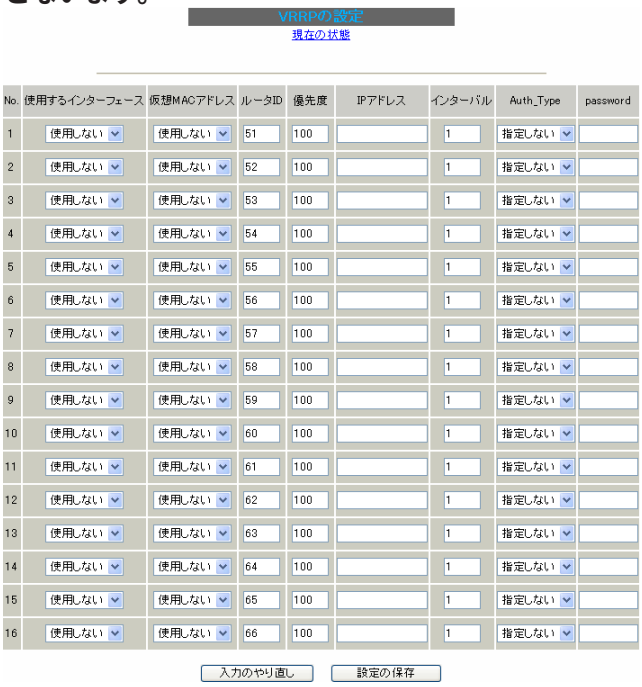
第 21 章 VRRP サービス

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。

設定方法

「各種サービスの設定」→「VRRP サービス」をクリックして以下の画面で VRRP サービスの設定をおこないます。



○使用するインターフェース
VRRP を作動させるインタフェースを選択します。

注) v1.7.6 版の時点では Ether2 を選択した場合、正常にマスター化ができません。Ether0 または Ether1 を使用してください。

○仮想 MAC アドレス
VRRP 機能を運用するときに、仮想 MAC アドレスを使用する場合は「使用する」を選択します。
１つのインタフェースにつき、設定可能な仮想 MAC アドレスは１つです。
「使用しない」設定の場合は、本装置の実 MAC アドレスを使って VRRP が動作します。

○ルータ ID
VRRP グループの ID を入力します。
他の設定 No. と同一のルータ ID を設定すると、同一の VRRP グループに属することになります。
ID が異なると違うグループと見なされます。

○優先度
VRRP グループ内での優先度を設定します。
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。
「指定しない」か、「PASS」または「AH」を選択できます。

○ password
認証をおこ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。

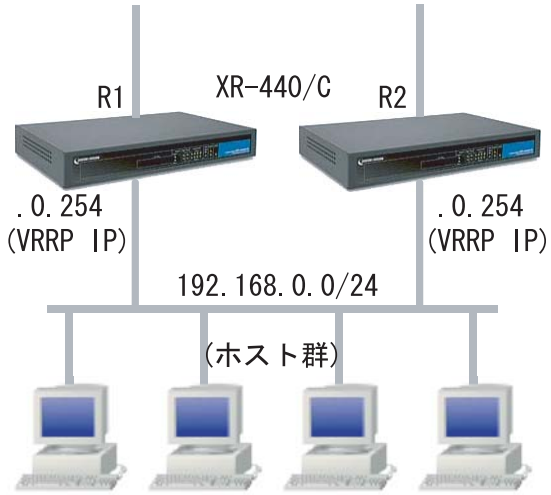
ステータスの表示

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。

II．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。
- 認証はおこなわない。

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 22 章

アクセスサーバ機能

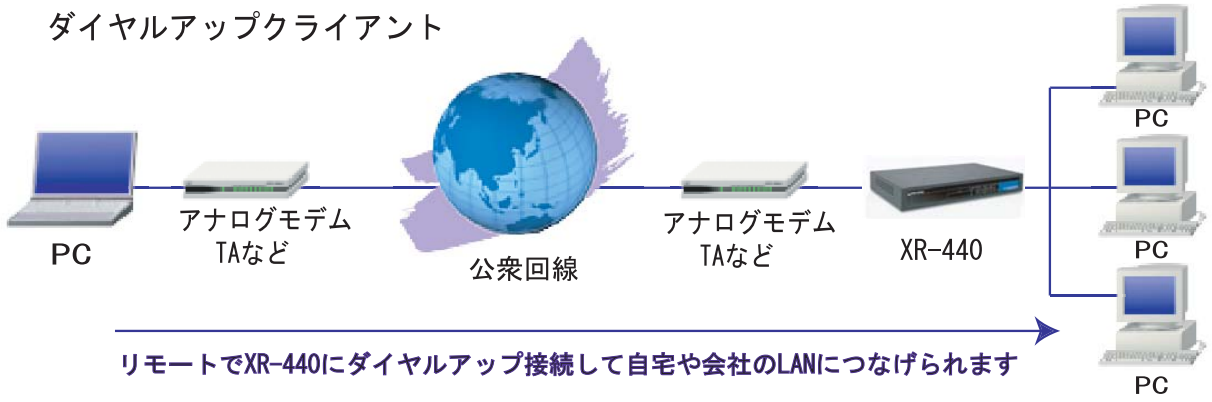
第 22 章 アクセスサーバ機能

Ⅰ．アクセスサーバ機能について

アクセスサーバとは、電話回線などを使った外部からの接続要求を受けて、LAN に接続する機能です。

例えば、アクセスサーバとして設定したXR-440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 ID・パスワード認証を使用します。また、BRI 着信では着信番号によっても確保できます。
ユーザ ID・パスワードは、最大 5 アカウント分を登録できます。



II．XR-440 とアナログモデム /TA の接続

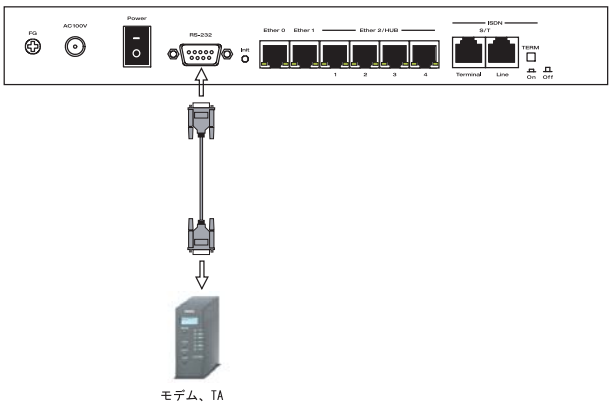
◆アナログモデム /TA のシリアル接続

1 本装置の電源をオフにします。

2 本装置の「RS-232」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．BRI ポートを使った XR-440 と TA/DSU の接続

◆外部の DSU を使う場合

1 本装置の電源をオフにします。

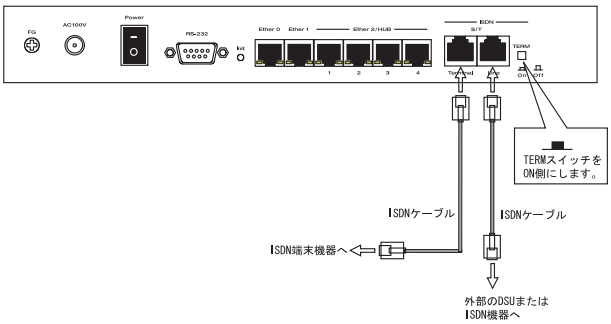
2 外部の DSU と本装置の「BRI S/T Line」ポートを ISDN 回線ケーブルで接続します。
ISDN ケーブルは別途ご用意ください。

3 本体背面の「TERM.」スイッチを「ON」側にします。

4 別の ISDN 機器を接続する場合は
「BRI S/T Terminal」ポートと接続してください。

5 全ての接続が完了しましたら、本装置と TA の電源を投入します。

接続図



Ⅳ．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。

アクセスサーバの設定

XR-440 ではシリアル回線と BRI 回線(２チャンネル)を使用することができます。
着信を受ける回線ごとに設定をおこないます。

◆シリアル回線で着信する場合

以下の「**シリアル回線**」欄で設定します。

○着信
シリアル回線で着信したい場合は「許可する」を選択します。

○アクセスサーバ(本装置)の IP アドレス
リモートアクセスされた時の XR-440 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
XR-440 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(本装置)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
XR-440 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

設定は以下の「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-440 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。

Ⅳ．アクセスサーバ機能の設定

○クライアントの IP アドレス
XR-440 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。
前記の「アクセスサーバ(本装置)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。

○アカウント認証
PPP のネゴシエーションで認証（PAP、CHAP）する場合は「する」を選択します。
アカウント認証をおこなうには、画面下のユーザアカウント設定欄で「アカウント」と「パスワード」を設定する必要があります。

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	user1	pass1			☐

（設定例）

○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。
発信者番号認証をおこなうには、画面下のユーザアカウント設定欄で「着信番号」を設定する必要があります。

No.	許可する着信番号	着信する回線	削除
1	0123456789	すべて	☐

（設定例）

「アカウント認証」「発信者番号認証」項目を設定する際に、アクセスサーバで BRI 回線が接続中の場合は、「回線１着信 / 回線２着信」の両方で「許可しない」を選択し「設定の保存」をクリックして、**一度接続を切断してから設定をおこなってください。BRI 回線の接続中に設定をおこなうと反映はされますが、動作しません。**

○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。

ユーザアカウントの設定

設定画面の下側でユーザアカウントの設定をおこないます。
ユーザは 5 アカウントまで設定可能です。

◆シリアル回線で着信する場合

以下の画面で設定します。

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					☐

○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アカウント・パスワードとなります。
アクセスサーバ設定の「アカウント認証」を「する」にしている場合は必ず設定してください。

○アカウント毎に別 IP を割り当てる場合
・本装置の IP
・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。

本項目で IP アドレスの割り当てをおこなうと、シリアル回線設定欄、BRI 回線設定欄の「アクセスサーバ(本装置)の IP アドレス」、「クライアントの IP アドレス」設定は無効になります。

○削除
アカウント設定覧の「削除」チェック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。

◆BRI 回線で着信する場合

また BRI 回線の設定で「発信番号認証」を「する」にしている場合は、必ず以下の画面の設定をおこなってください。

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	☐

○許可する着信番号
発信者の電話番号を入力してください。

○着信する回線
「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」チェック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。

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。

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。
接続している状態では「接続中」となります。

第 23 章

スタティックルーティング

スタティックルーティング設定

XR-440 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。
画面下部にある「スタティックルート設定画面インデックス」のリンクをクリックしてください。

設定方法

Web 設定画面「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。

○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
あて先アドレス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＞
29 ビットマスクの場合　　：255.255.255.248
単一ホストで指定した場合 ：255.255.255.255

○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フェース名、もしくは上位ルータの IP アドレスを設定します。
※ PPP/PPPoE や GRE インタフェースを設定する場合は、インタフェース名だけの設定となります。

本装置のインタフェース名については「付録 A インタフェース名一覧」をご参照ください。

注)ただし、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。

○ディスタンス
経路選択の優先順位を 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。

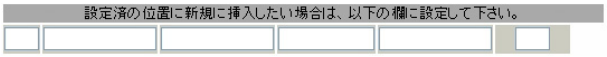
○削除
ルーティング設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れてください。

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。

スタティックルーティング設定

設定を挿入する

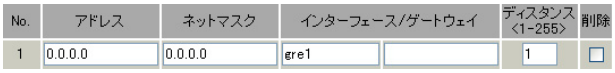
ルーティング設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。



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。

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。



（画面は表示例です）

ルーティング情報を確認する

現在のルーティング情報を確認するには、設定画面上部にある「経路情報表示」をクリックします。
ウィンドウがポップアップし、経路情報が確認できます。

“ inactive ”と表示されている経路は、その時点では有効な経路ではなく、無視されます。

表示されていないものに関しては、正しい設定ではありません。
設定をご確認のうえ、再度設定してください。

第 24 章

ソースルーティング機能

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おこないますが、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。

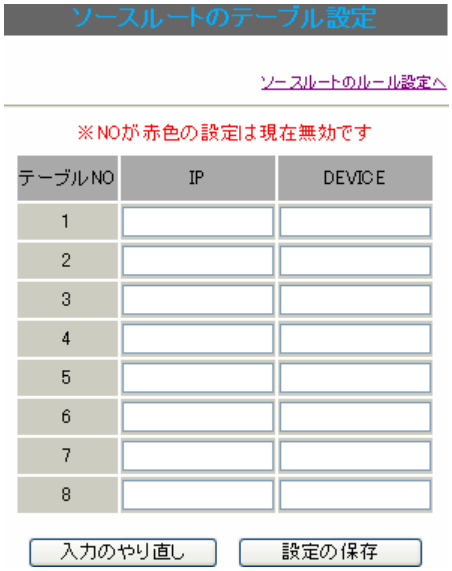
このソースルート機能を使うことで、外部へアクセスするホスト / ネットワークごとにアクセス回線を選択することができますので、複数のインターネット接続をおこなって負荷分散が可能となります。

設定方法

ソースルート設定は、Web 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。
Web 設定画面「ソースルート設定」を開き、「ソースルートのテーブル設定へ」のリンクをクリックしてください。

「ソースルートのテーブル設定」画面が表示されます。



○ 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。
本装置のインタフェース名は「付録 A インタフェース名一覧」を参照してください。
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。

ソースルーティング設定

2 画面右上の「ソースルートのルール設定へ」のリンクをクリックして以下の画面を開きます。

○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 XR-440 のインタフェースが含まれていると、設定後は XR-440 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 XR-440 の設定画面にアクセスできなくなります。

第 25 章

NAT 機能

第 25 章　NAT 機能

Ⅰ．XR-440 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。

XR-440は以下の3つのNAT機能をサポートしています。
これらのNAT機能は、同時に設定・運用が可能です。

◆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XR-440 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、Web 設定画面「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。
プライベートアドレスをグローバルアドレスに変換する、といった設定が可能になります。

＜例＞

プライベートアドレスA…＞グローバルアドレスX
プライベートアドレスB…＞グローバルアドレスY
プライベートアドレスC～F…＞グローバルアドレスZ

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。

NetMeetingや各種IM、ネットワークゲームなど、独自のプロトコル・ポートを使用しているアプリケーションについては、NAT機能を使用すると正常に動作しない場合があります。
原則として、NATを介しての個々のアプリケーションの動作についてはサポート対象外とさせていただきます。

Ⅱ．バーチャルサーバ設定

NAT 環境下において、LAN からサーバを公開するときなどの設定をおこないます。

設定方法

Web 設定画面「NAT 設定」→「バーチャルサーバ」をクリックして、以下の画面から設定します。
256まで設定できます。「バーチャルサーバ設定画面インデックス」のリンクをクリックしてください。

○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 アドレスにアクセスします。
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**

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

○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フェース名を設定します。
外部に接続しているインタフェース名を設定してください。

○削除
設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れてください。

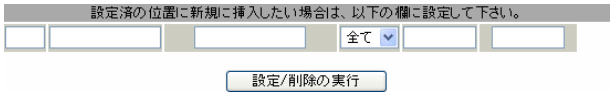
入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
“No.”項目が赤字で表示されている行は入力内容が正しくありません。
再度入力をやり直してください。

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。



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。

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。
256 まで設定できます。「送信元 NAT 設定画面インデックス」のリンクをクリックしてください。

○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
どのインタフェースからインターネット(WAN)へアクセスするか、インタフェース名を指定します。
インターネットにつながっているインタフェースを設定してください。

○削除
設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れてください。

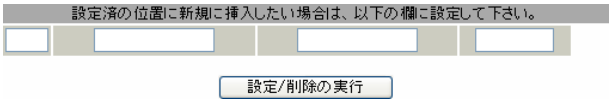
入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
“No.”項目が赤字で表示されている行は入力内容が正しくありません。
再度入力をやり直してください。

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。



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。

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。

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
1	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。

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
1	192.168.0.2	211.xxx.xxx.103	tcp	20	ppp0
2	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 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。
No.2 ：
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。

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おこなってください。
特に、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。

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
1	192.168.0.3		tcp	1723	ppp0
2	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おこなってください。
特に、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、仮想インタフェースとして登録します。
Web 設定画面にある「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。

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
1	eth1	1	211.xxx.xxx.104	255.255.255.248
2	eth1	2	211.xxx.xxx.105	255.255.255.248
3	eth1	3	211.xxx.xxx.106	255.255.255.248
4	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」を参照してください。

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。

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
1	192.168.0.1	211.xxx.xxx.104	tcp	80	eth1
2	192.168.0.2	211.xxx.xxx.105	tcp	25	eth1
3	192.168.0.2	211.xxx.xxx.105	tcp	110	eth1
4	192.168.0.3	211.xxx.xxx.106	tcp	21	eth1
5	192.168.0.3	211.xxx.xxx.106	tcp	20	eth1
6	192.168.0.4	211.xxx.xxx.107	tcp	53	eth1
7	192.168.0.4	211.xxx.xxx.107	udp	53	eth1

設定の解説

No.1
　WAN 側から 211.xxx.xxx.104 へポート 80 番(http)でアクセスがあれば、LAN 内のサーバ 192.168.0.1 へ通す。
No.2、3
　WAN 側から 211.xxx.xxx.105 へポート 25 番(smtp)か 110 番(pop3)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。
No.4、5
　WAN 側から 211.xxx.xxx.106 へポート 20 番(ftpdata)か 21 番(ftp)でアクセスがあれば、LAN 内のサーバ 192.168.0.3 へ通す。
No.6、7
　WAN 側から 211.xxx.xxx.107 へ、tcp ポート 53 番(domain)か udp ポート 53 番(domain)でアクセスがあれば、LAN 内のサーバ 192.168.0.4 へ通す。

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。

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
1	192.168.0.1	61.xxx.xxx.101	ppp0
2	192.168.0.2	61.xxx.xxx.102	ppp0
3	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 26 章

パケットフィルタリング機能

第 26 章 パケットフィルタリング機能

Ⅰ．機能の概要

XR-440 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。
- XR-440 自身が受信するパケットを制限する。
- XR-440 自身から送信するパケットを制限する。

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。

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

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 などや、プロトコル番号)、ポート番号、送信元 MAC アドレスに基づいて、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．XR-440 のフィルタリング機能について

XR-440 は、3 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。
3 つの項目は以下の通りです。

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

◆入力(input)フィルタ
外部から XR-440 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 XR-440 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、XR-440 で内部転送する(XR-440 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
XR-440 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「XR-440 自身へのアクセス」か「XR-440 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。

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

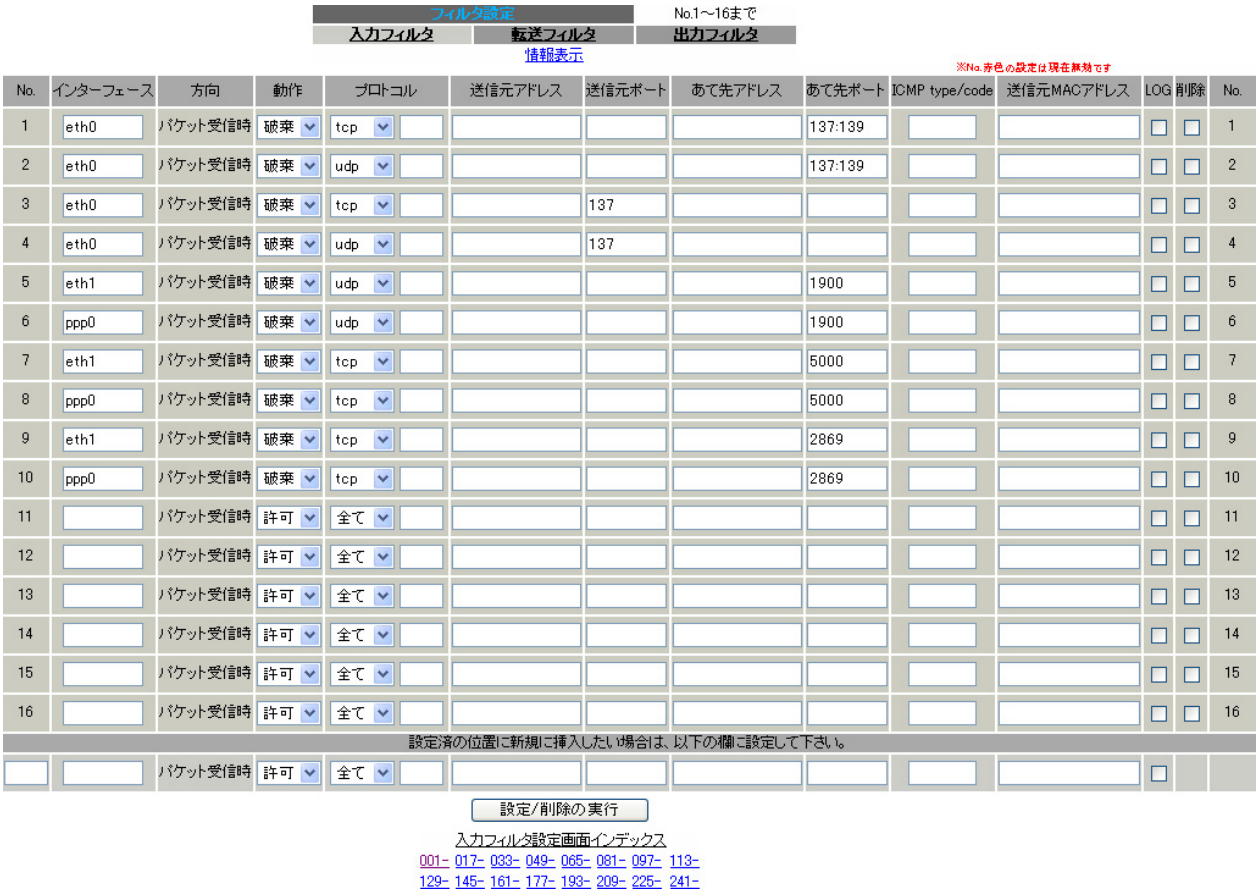
Windows ファイル共有をする場合は、NetBIOS 用のフィルタを削除してお使いください。

III．パケットフィルタリングの設定

入力・転送・出力フィルタの 3 種類ありますが、設定方法はすべて同じです。
各フィルタで設定可能数は最大 256 です。
各フィルタ設定画面の最下部にある「フィルタ設定画面インデックス」のリンクをクリックしてください。

設定方法

Web 設定画面「フィルタ設定」→「入力フィルタ」「転送フィルタ」「出力フィルタ」のいずれかをクリックして、以下の画面から設定します。



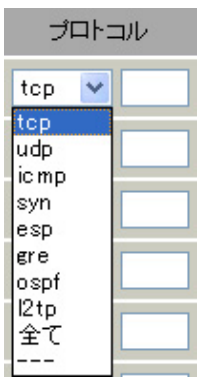
(画面は「入力フィルタ」です)

○インターフェース
フィルタリングをおこなうインタフェース名を指定します。
インタフェース名は「付録 A インタフェース名一覧」を参照してください。

○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」のみ、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、ネットワークアドレスでの指定が可能です。

< 入力例 >
単一の IP アドレスを指定する：
　192.168.253.19
　192.168.253.19/32
（“ アドレス /32 ”の書式 “ /32 ”は省略可能です。）

ネットワーク単位で指定する：
　192.168.253.0/24
（“ ネットワークアドレス / マスクビット値 ”の書式）

○送信元ポート
フィルタリング対象とする、送信元のポート番号を入力します。
範囲での指定も可能です。範囲で指定するときは “ : ” でポート番号を結びます。

< 入力例 >
ポート 1024 番から 65535 番を指定する場合。
　1024:65535

ポート番号を指定するときは、プロトコルも合わせて選択しておかなければなりません。
(「全て」のプロトコルを選択して、ポート番号を指定することはできません。)

○あて先アドレス
フィルタリング対象とする、あて先の IP アドレスを入力します。
ホストアドレス、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 IP アドレスと同様です。

○あて先ポート
フィルタリング対象とする、あて先のポート番号を入力します。
範囲での指定も可能です。指定方法は送信元ポートと同様です。

○ 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。

○送信元 MAC アドレス
※ 本項目は「出力フィルタ」にはありません。
フィルタリング対象とする、送信元の MAC アドレスを入力します。
半角英数字、’: ’、’ * ’、’ / ’ のみ入力できます。
入力可能な最大文字数は 35 文字です。

送信元MACアドレスは、XX:XX:XX:XX:XX:XX形式で設定します。
以下の形式でも指定することが出来ます。
　-XX:XX:XX:XX:*:*　　（wildcard 形式）
　-XX:XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX
　　（マスク形式）

○ LOG
チェックを入れると、そのフィルタ設定に合致したパケットがあったとき、そのパケットの情報を syslog に出力します。
許可 / 破棄いずれの場合も出力します。

○削除
フィルタ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れてください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。
”No.” 項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

III．パケットフィルタリングの設定

設定情報の確認

「情報表示」をクリックすると、現在のフィルタ設定の情報が一覧表示されます。


入力フィルタ 情報表示

No.	type	ptks	bytes	target	log	prot	in	out	source	destination		
1	IP	0	0	DROP	-	tcp	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp	dpts:137:139
2	IP	6	468	DROP	-	udp	eth0	*	0.0.0.0/0	0.0.0.0/0	udp	dpts:137:139
3	IP	0	0	DROP	-	tcp	eth0	*	0.0.0.0/0	0.0.0.0/0	tcp	spt:137
4	IP	0	0	DROP	-	udp	eth0	*	0.0.0.0/0	0.0.0.0/0	udp	spt:137
5	IP	0	0	DROP	-	udp	eth1	*	0.0.0.0/0	0.0.0.0/0	udp	dpt:1900
6	IP	0	0	DROP	-	udp	ppp0	*	0.0.0.0/0	0.0.0.0/0	udp	dpt:1900
7	IP	0	0	DROP	-	tcp	eth1	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:5000
8	IP	0	0	DROP	-	tcp	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:5000
9	IP	0	0	DROP	-	tcp	eth1	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:2869
10	IP	0	0	DROP	-	tcp	ppp0	*	0.0.0.0/0	0.0.0.0/0	tcp	dpt:2869
11	FQDN	---	---	ACCEPT	-	tcp	eth1	*	www.yahoo.co.jp	0.0.0.0/0	tcp	dpt:80

更新

（画面は「入力フィルタ 情報表示」例）

設定を挿入する

フィルタ設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。

（画面は「入力フィルタ」）

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。
その番号以降に設定がある場合は、1つずつ設定番号がずれて設定が更新されます。

Ⅳ．パケットフィルタリングの設定例

◆インターネットからLANへのアクセスを破棄する設定

本製品の工場出荷設定では、インターネット側から LAN へのアクセスは全て通過させる設定となっていますので、以下の設定をおこない、外部からのアクセスを禁止するようにします。

フィルタの条件

- WAN 側からは LAN 側へアクセス不可にする。
- LAN から WAN へのアクセスは自由にできる。
- 本装置から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- LAN から WAN へ IP マスカレードをおこなう。
- ステートフルパケットインスペクションは有効。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス「192.168.0.1」

設定画面での入力方法

「入力フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp				1024:65535
2	eth1	パケット受信時	許可	udp				1024:65535
3	eth1	パケット受信時	許可	--- 1				
4	eth1	パケット受信時	破棄	全て				

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp				1024:65535
2	eth1	パケット受信時	許可	udp				1024:65535
3	eth1	パケット受信時	許可	--- 1				
4	eth1	パケット受信時	破棄	全て				

フィルタの解説

「入力フィルタ」「転送フィルタ」

No.1、2：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.3：
WAN から来る、ICMP（プロトコル番号“1”）パケットを通す。

No.4：
上記の条件に合致しないパケットを全て破棄する。

Ⅳ．パケットフィルタリングの設定例

◆WWW サーバを公開する際のフィルタ設定例

フィルタの条件

・WAN 側からは LAN 側の WWW サーバにだけアクセス可能にする。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続。
・ステートフルパケットインスペクションは有効。

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス 「192.168.0.254」
・WWW サーバのアドレス 「192.168.0.1」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット受信時	許可	tcp				192.168.0.1	80
2	eth1	パケット受信時	許可	tcp					1024:65535
3	eth1	パケット受信時	許可	udp					1024:65535
4	eth1	パケット受信時	破棄	全て					

フィルタの解説

No.1：
192.168.0.1 のサーバに HTTP のパケットを通す。
No.2、3：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。
No.4：
上記の条件に合致しないパケットを全て破棄する。

◆FTP サーバを公開する際のフィルタ設定例

フィルタの条件

・WAN 側からは LAN 側の FTP サーバにだけアクセスが可能にする。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続する。
・NAT は有効。
・Ether1 ポートは PPPoE 回線に接続する。
・ステートフルパケットインスペクションは有効。

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス 「192.168.0.254」
・FTP サーバのアドレス 「192.168.0.2」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp				192.168.0.2	21
2	ppp0	パケット受信時	許可	tcp				192.168.0.2	20
3	ppp0	パケット受信時	許可	tcp					1024:65535
4	ppp0	パケット受信時	許可	udp					1024:65535
5	ppp0	パケット受信時	破棄	全て					

フィルタの解説

No.1：
192.168.0.2 のサーバに ftp のパケットを通す。
No.2：
192.168.0.2 のサーバに ftpdata のパケットを通す。
No.3、4：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。
No.5：
上記の条件に合致しないパケットを全て破棄する。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

Ⅳ．パケットフィルタリングの設定例

◆WWW、FTP、メール、DNS サーバを公開する際のフィルタ設定例

フィルタの条件

- WAN 側からは LAN 側の WWW、FTP、メールサーバにだけアクセスが可能にする。
- DNS サーバが WAN と通信できるようにする。
- LAN から WAN へのアクセスは自由にできる。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- PPPoE で ADSL に接続する。
- NAT は有効。
- ステートフルパケットインスペクションは有効。

LAN 構成

- LAN のネットワークアドレス「192.168.0.0/24」
- LAN 側ポートの IP アドレス「192.168.0.254」
- WWW サーバのアドレス「192.168.0.1」
- メールサーバのアドレス「192.168.0.2」
- FTP サーバのアドレス「192.168.0.3」
- DNS サーバのアドレス「192.168.0.4」

フィルタの解説

No.1：
192.168.0.1 のサーバに HTTP のパケットを通す。
No.2：
192.168.0.2 のサーバに SMTP のパケットを通す。
No.3：
192.168.0.2 のサーバに POP3 のパケットを通す。
No.4：
192.168.0.3 のサーバに ftp のパケットを通す。
No.5：
192.168.0.3 のサーバに ftpdata のパケットを通す。
No.6、7：
192.168.0.4 のサーバに、domain のパケット(tcp,udp)を通す。
No.8、9：
WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。
No.10：
上記の条件に合致しないパケットを全て破棄する。

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル		送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp				192.168.0.1	80
2	ppp0	パケット受信時	許可	tcp				192.168.0.2	25
3	ppp0	パケット受信時	許可	tcp				192.168.0.2	110
4	ppp0	パケット受信時	許可	tcp				192.168.0.3	21
5	ppp0	パケット受信時	許可	tcp				192.168.0.3	20
6	ppp0	パケット受信時	許可	tcp				192.168.0.4	53
7	ppp0	パケット受信時	許可	udp				192.168.0.4	53
8	ppp0	パケット受信時	許可	tcp					1024:65535
9	ppp0	パケット受信時	許可	udp					1024:65535
10	ppp0	パケット受信時	破棄	全て					

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

Ⅳ．パケットフィルタリングの設定例

◆NetBIOS パケットが外部へ出るのを防止するフィルタ設定

フィルタの条件

・LAN 側から送出された NetBIOS パケットを WAN へ出さない。(Windows での自動接続を防止する)

LAN 構成

・LAN のネットワークアドレス「192.168.0.0/24」
・LAN 側ポートの IP アドレス 「192.168.0.254」

設定画面での入力方法

「入力フィルタ」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	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」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	eth0	パケット受信時	破棄	tcp				137:139
2	eth0	パケット受信時	破棄	udp				137:139
3	eth0	パケット受信時	破棄	tcp		137		
4	eth0	パケット受信時	破棄	udp		137		

フィルタの解説

「入力フィルタ」「転送フィルタ」
No.1：
　あて先ポートが tcp の 137 から 139 のパケットを Ether0 ポートで破棄する。
No.2：
　あて先ポートが udp の 137 から 139 のパケットを Ether0 ポートで破棄する。
No.3：
　送信先ポートが tcp の 137 のパケットを Ether0 ポートで破棄する。
No.4：
　送信先ポートが udp の 137 のパケットを Ether0 ポートで破棄する。

◆WAN からのブロードキャストパケットを破棄するフィルタ設定(smurf 攻撃の防御)

フィルタの条件

・WAN 側からのブロードキャストパケットを受け取らないようにする。→ smurf 攻撃を防御する

LAN 構成

・プロバイダから割り当てられたネットワーク空間「210.xxx.xxx.32/28」
・WAN 側は PPPoE 回線に接続する。
・WAN 側ポートの IP アドレス「210.xxx.xxx.33」

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	全て			210.xxx.xxx.32/32	
2	ppp0	パケット受信時	破棄	全て			210.xxx.xxx.47/32	

フィルタの解説

No.1：
　210.xxx.xxx.32/32（210.xxx.xxx.32/28 のネットワークのネットワークアドレス）宛てのパケットを受け取らない。
No.2：
　210.xxx.xxx.47/32（210.xxx.xxx.32/28 のネットワークのブロードキャストアドレス）宛てのパケットを受け取らない。

これらの設定例は説明のためのものです。
これらのフィルタを設定して安全を確保できることを保証するものではありませんのでご注意ください。

Ⅳ．パケットフィルタリングの設定例

◆WAN からのパケットを破棄するフィルタ設定 (IP spoofing 攻撃の防御)

フィルタの条件

・WAN 側からの不正な送信元 IP アドレスを持つパケットを受け取らないようにする。
→ IP spoofing 攻撃を受けないようにする。

LAN 構成

・LAN 側のネットワークアドレス「192.168.0.0/24」
・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			

フィルタの解説

No.1、2、3：
WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。
→WAN 上にプライベートアドレスは存在しない。

◆外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

・WAN 側からの不正な送信元・送信先 IP アドレスを持つパケットを受け取らないようにする。
→WAN からの攻撃を受けない・攻撃の踏み台にされないようにする。

LAN 構成

・プロバイダから割り当てられたアドレス空間「202.xxx.xxx.112/28」
・LAN 側のネットワークアドレス「192.168.0.0/24」
・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			
4	ppp0	パケット受信時	破棄	全て			202.xxx.xxx.127/3	

「出力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット送信時	許可	全て	10.0.0.0/8			
2	ppp0	パケット送信時	許可	全て	172.16.0.0/16			
3	ppp0	パケット送信時	許可	全て	192.168.0.0/16			

フィルタの解説

「入力フィルタ」
No.1、2、3：
WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。
→WAN 上にプライベートアドレスは存在しない。
No.4：
WAN からのブロードキャストパケットを受け取らない。
→ smurf 攻撃の防御

「出力フィルタ」
No.1、2、3：
送信元 IP アドレスが不正なパケットを送出しない。
→WAN 上にプライベートアドレスは存在しない。

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

◆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

遠隔で XR-440 の設定・制御をおこなうことも可能です。
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。

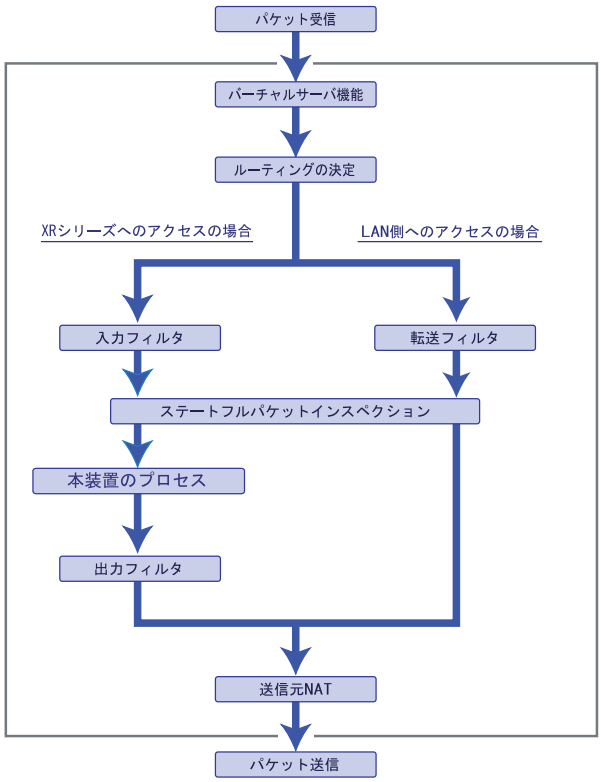
No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp	221.xxx.xxx.105			880

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、XR-440 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

XR-440 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。
- XR-440 自身へのアクセスをフィルタするときは「入力フィルタ」、XR-440 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 XR-440 自身へのアクセスはすべて破棄されます。
- ステートフルパケットインスペクションと同時に「転送フィルタ」「入力フィルタ」を設定している場合は、先に「転送フィルタ」「入力フィルタ」にある設定が優先して処理されます。
- 「送信元 NAT 設定」は、一番最後に参照されます。
- LAN 側から WAN 側へのアクセスの場合も、処理の順序は同様です。
  (最初にバーチャルサーバ設定が参照されます。)

補足：ポート番号について

よく使われるポートの番号については、下記の表
を参考にしてください。
詳細はRFC1700(Oct. 1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

補足：フィルタのログ出力内容について

フィルタ設定画面で「LOG」にチェックを入れると、その設定に合致したパケットの情報を syslog に出力します。
出力内容は以下のようになります。

<入力パケットを破棄したときのログ出力例>

```
Jan 25 14:14:07 localhost XR-Filter:  FILTER_INPUT_1 IN=eth0 OUT=
MAC=00:80:6d:xx:xx:xx:00:20:ed:yy:yy:yy:80:00  SRC=192.168.xxx.xxx DST=xxx.xxx.xxx.xxx
LEN=40 TOS=00 PREC=0x00 TTL=128 ID=43951 CE DF PROTO=TCP SPT=2526 DPT=880 SEQ=4098235374
ACK=1758964579 WINDOW=48000 ACK URGP=0
```

Jan 25 14:14:07	syslog がログを取得した日時です。
XR-Filter:	フィルタのログであることを表します。
FILTER_INPUT_1	入力フィルタの１番目のフィルタで取得されたものです。 「FILTER_FORWARD」は転送フィルタを意味します。 「FILTER_OUTPUT」は出力フィルタを意味します。
IN=	パケットを受信したインタフェースが記されます。
OUT=	パケットを送出したインタフェースが記されます。 何も記載されていないときは、XRのどのインタフェースからもパケットを送出していないことを表わしています。
MAC=	送信元・あて先のMACアドレスが記されます。
SRC=	送信元IPアドレスが記されます。
DST=	送信先IPアドレスが記されます。
LEN=	パケット長が記されます。
TOS=	TOS bitの状態が記されます。
TTL=	TTLの値が記されます。
ID=	IPのIDが記されます。
PROTO=	プロトコルが記されます。

プロトコルが ICMP の時は、以下のような ICMP 用のメッセージも記されます。

TYPE=0	ICMPのタイプが記されます。
CODE=0	ICMPのコードが記されます。
ID=3961	ICMPのIDが記されます。
SEQ=6656	ICMPのシーケンス番号が記されます。

第 27 章

スケジュール設定

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。

スケジュール機能の設定方法

○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保存・実行・削除を決定します。

「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				

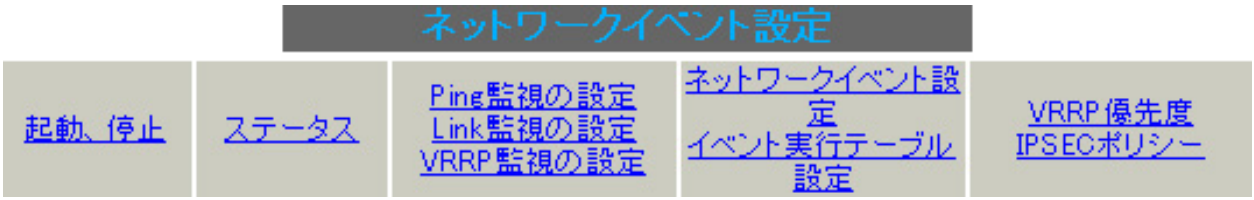
第 28 章

ネットワークイベント機能

第 28 章 ネットワークイベント機能

Ⅰ．機能の概要

ネットワークイベントは、回線障害などのネットワーク状態の変化を検知し、それをトリガとして特定のイベントを実行する機能です。



本装置では、以下のネットワーク状態の変化をトリガとして検知することができます。

- Ping 監視の状態
- Link 監視の状態
- VRRP 監視の状態

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

◆Ping 監視

本装置から任意の宛先へ ping を送信し、その応答の有無を監視します。
一定時間応答がなかった時にトリガーとして検知します。
また再び応答を受信した時は、復旧トリガーとして検知します。

◆Link 監視

Ethernet インタフェースや ppp インタフェースのリンク状態を監視します。
監視するインタフェースのリンクがダウンした時にトリガーとして検知します。
また再びリンクがアップした時は、復旧トリガーとして検知します。

◆VRRP 監視

本装置の VRRP ルータ状態を監視します。
指定したルータ ID の VRRP ルータがバックアップルータへ切り替わった時にトリガーとして検知します。
また再びマスタルータへ切り替わった時は、復旧トリガーとして検知します。

◆VRRP 優先度変更

トリガー検知時に、指定した VRRP ルータの優先度を変更します。
またトリガー復旧時には、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

トリガー検知時に、指定した IPsec ポリシーを切断します。
またトリガー復旧時には、IPsec ポリシーを再び接続します。

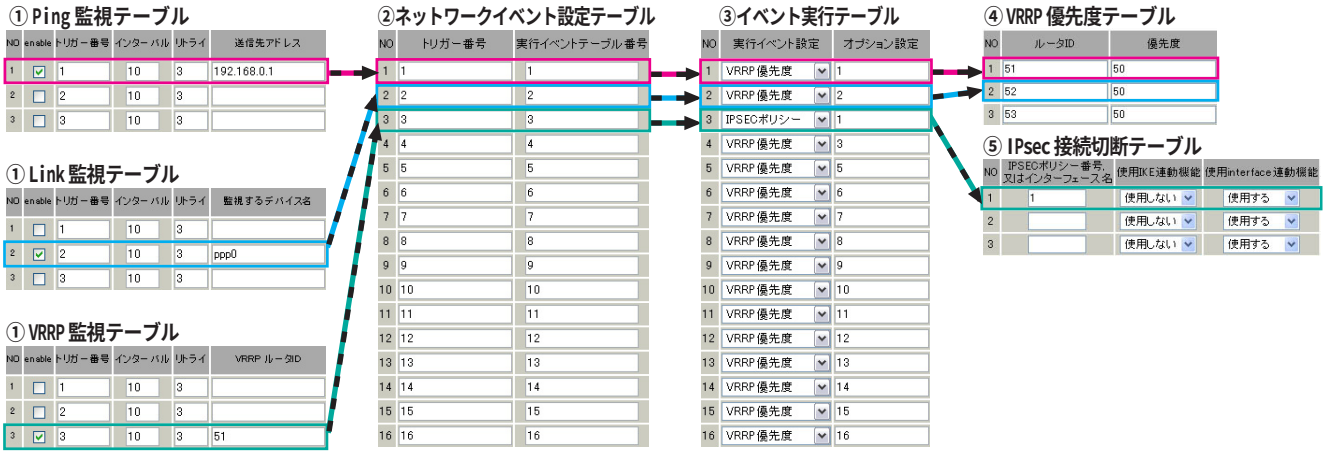
例えば、VRRP 監視と連動して、2 台の VRRP ルータのマスタルータの切り替わりに応じて、IPsec 接続を繋ぎかえる、といった使い方ができます。

第 28 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。



① Ping 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「④VRRP 優先度テーブル」を索引します。
設定したオプション番号は、テーブル④のインデックス番号になります。

また、イベントの実行種別を「IPSEC ポリシー」に設定した場合は、次に「⑤ IPsec 接続切断テーブル」を索引します。
設定したオプション番号は、テーブル⑤のインデックス番号になります。

④ VRRP 優先度テーブル

このテーブルでは、VRRP 優先度を変更するルータ ID とその優先度を定義します。

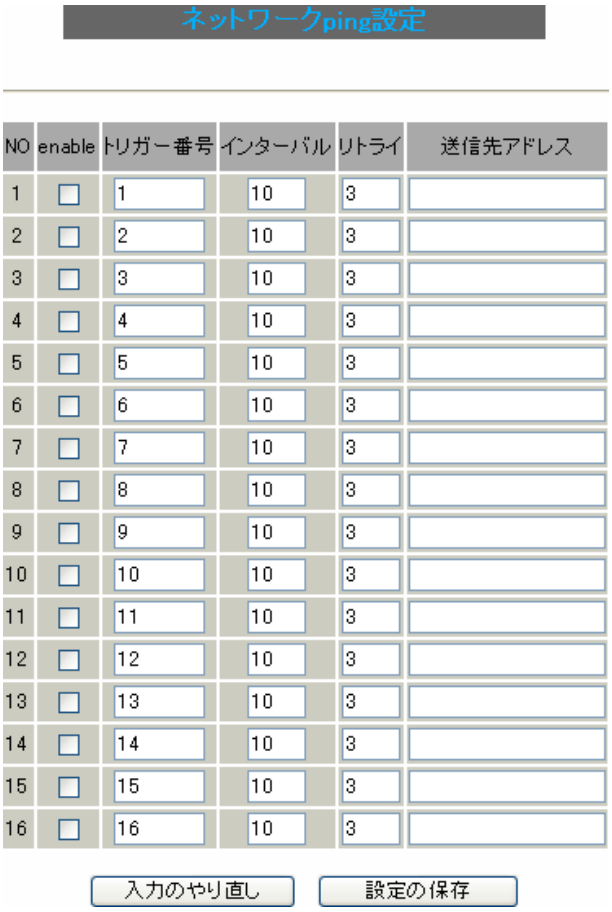
⑤ IPsec 接続切断テーブル

このテーブルでは、IPsec 接続 / 切断をおこなう IPsec ポリシー番号、または IPsec インタフェース名を定義します。

Ⅱ．各トリガテーブルの設定

Ping 監視の設定方法

設定画面上部の「Ping 監視の設定」をクリックして、以下の画面から設定します。



○ enable
チェックを入れることで設定を有効にします。

○トリガー番号
ping送信先から応答が無かった場合に検知するトリガーの番号(1～16)を指定します。
本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

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

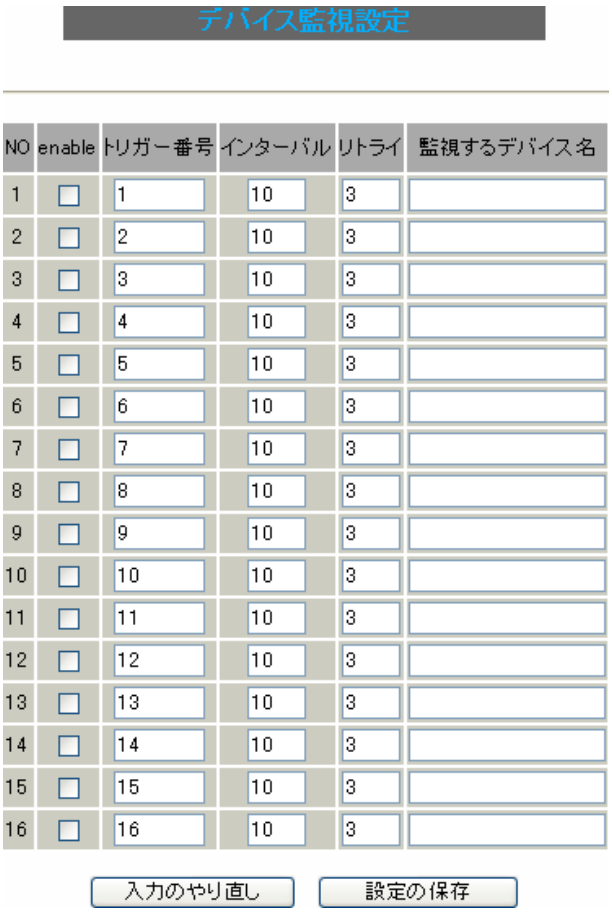
○送信先アドレス
ping を送信する先の IP アドレスを指定します。

最後に「設定の保存」をクリックして設定完了です。

Ⅱ．各トリガテーブルの設定

Link 監視の設定方法

設定画面上部の「Link 監視の設定」をクリックして、以下の画面から設定します。



○ enable
チェックを入れることで設定を有効にします。

○トリガー番号
監視するインタ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、監視したリンク状態が全てダウンだった場合にトリガーとして検知されます。

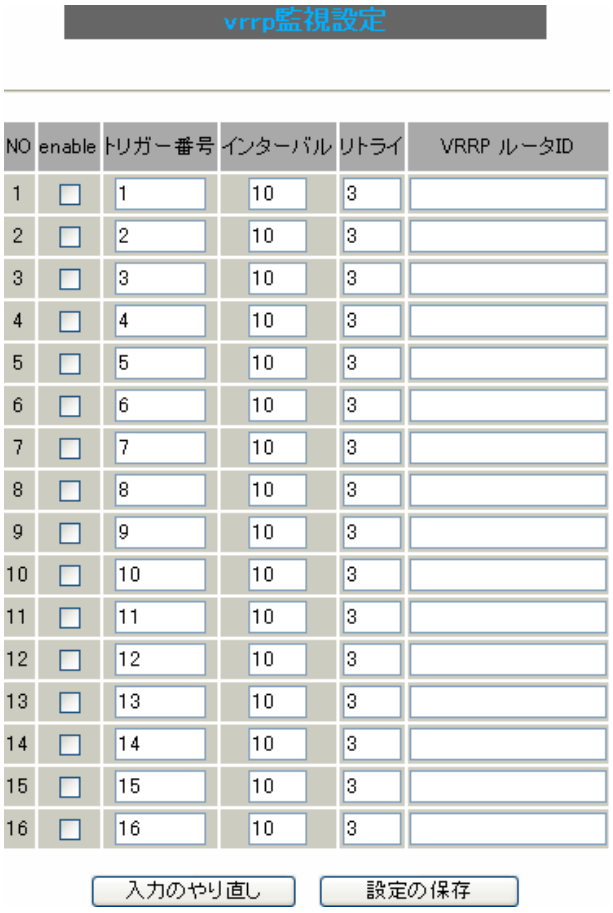
○監視するデバイス名
リンク状態を監視するデバイスのインタフェース名を指定します。
Ethernet インタフェース名、または PPP インタフェース名を入力してください。

最後に「設定の保存」をクリックして設定完了です。

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ーとして検知されます。

○VRRP ルータ ID
VRRP ルータ状態を監視するルータ ID を指定します。

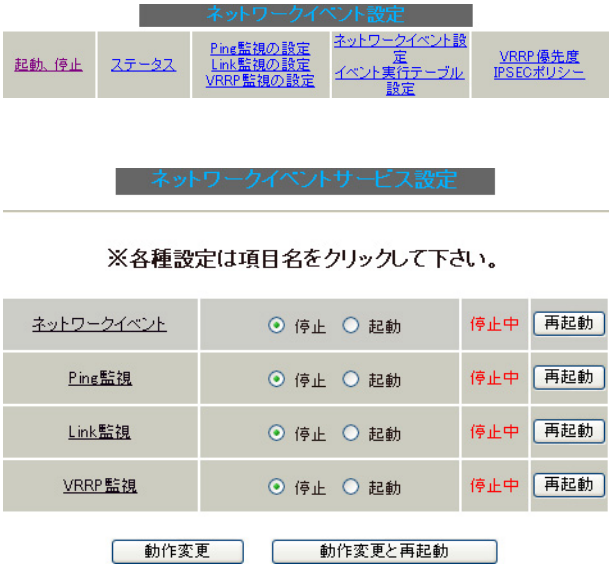
最後に「設定の保存」をクリックして設定完了です。

II．各トリガテーブルの設定

各種監視設定の起動と停止方法

各監視機能（Ping 監視、Link 監視、VRRP 監視）を有効にするには、Web 設定画面「ネットワークイベント設定」画面→「起動、停止」の以下のネットワーク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、削除をおこなった場合は、サービスを再起動させてください。



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。

注）v1.7.6版の時点ではインタフェースにEther2を選択したVRRPは、正常にトリガー検出ができません。
Ether0またはEther1を選択したVRRPを使用してください。

III．実行イベントテーブルの設定

ネットワークイベント設定テーブルの設定

設定画面上部の「ネットワークイベント設定」をクリックして、以下の画面から設定します。

(「イベント実行テーブル設定」画面のリンクをクリックしても以下の画面を開くことができます。)

○トリガー番号

「Ping 監視の設定」、「Link 監視の設定」、「VRRP 監視の設定」で設定したトリガー番号を指定します。
なお、複数のトリガー検知の組み合わせによって、イベントを実行させることも可能です。

＜例＞

・トリガー番号 1 とトリガー番号 2 のどちらかを検知した時にイベントを実行させる場合

1&2

・トリガー番号 1 とトリガー番号 2 の両方を検知した時、またはトリガー番号 3 を検知した時にイベントを実行させる場合

[1|2]&3

○実行イベントテーブル番号

そのトリガー番号を検知した時に実行されるイベント番号(1～16)を指定します。
本値は、イベント実行テーブルでのインデックス番号となります。
なお、複数のイベントを同時に実行させることも可能です。その場合は”_”でイベント番号を繋ぎます。

＜例＞

イベント番号 1,2,3 を同時に実行させる場合

1_2_3

最後に「設定の保存」をクリックして設定完了です。

III. 実行イベントテーブルの設定

イベント実行テーブルの設定

設定画面上部の「イベント実行テーブル設定」をクリックして、以下の画面から設定します。

（「ネットワークイベント設定」画面のリンクをクリックしても以下の画面を開くことができます。）

○実行イベント設定
実行されるイベントの種類を選択します。
「IPsec ポリシー」は、IPsec ポリシーの切断をおこないます。
「VRRP 優先度」は、VRRP ルータの優先度を変更します。

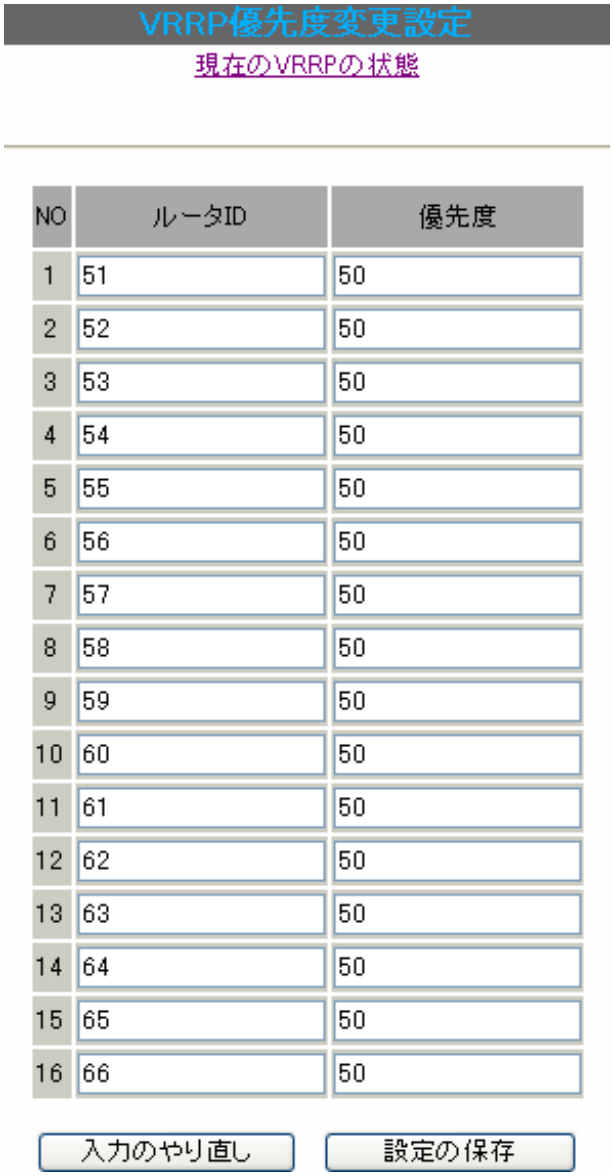
○オプション設定
実行イベントのオプション番号です。
本値は、「VRRP 優先度変更設定」テーブル、または「IPSEC 接続切断設定」テーブルでのインデックス番号となります。

最後に「設定の保存」をクリックして設定完了です。

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
トリガー検知時に VRRP 優先度を変更する VRRP ルータ ID を指定します。

○優先度
トリガー検知時に変更する VRRP 優先度を指定します。1-255 の間で設定してください。
なお、トリガー復旧時には「VRRP サービス」で設定されている元の値に戻ります。

最後に「設定の保存」をクリックして設定完了です。

現在の設定状態の確認

VRRP 優先度変更設定画面の上部の、
「現在の VRRP の状態」リンクをクリックすると、
「VRRP の情報」を表示するウィンドウがポップアップします。

Ⅳ．実行イベントのオプション設定

IPSEC 接続切断設定 テーブルの設定

設定画面上部の「IPSEC ポリシー」をクリックして、次の画面から設定します。

○ IPSEC ポリシー番号、又はインターフェース名
トリガー検知時に切断する IPsec ポリシーの番号、または IPsec インタフェース名を指定します。
ポリシー番号は、範囲で指定することもできます。

＜例＞ IPsec ポリシー 1 から 20 を切断する → **1:20**

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

○使用 IKE 連動機能
切断する IPsec ポリシーが使用する IKE と同じ IKE を使用する IPsec ポリシーが設定されている場合において、トリガー検知時にその IKE を使用する全ての IPsec ポリシーを切断する場合は、「使用する」を選択します。
ここで設定した IPsec ポリシーのみを切断する場合は「使用しない」を選択します。

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

最後に「設定の保存」をクリックして設定完了です。

現在の設定状態の確認

IPSEC 接続切断設定画面の上部の、
「現在の IPSEC の状態」リンクをクリックすると、
「IPSEC の情報」を表示するウィンドウがポップアップします。

Ⅴ．ステータスの表示

ステータスの表示

設定画面上部の「ステータス」をクリックして表示します。

○トリガー情報

設定が有効なトリガー番号とその状態を表示します。

“ ON ”と表示されている場合

トリガーを検知していない、またはトリガー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

トリガー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、トリガー検知し、イベントを実行している状態を表します。

“ ○ ”の表示は、トリガー検知がなく、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ー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 29 章

仮想インターフェース機能

仮想インタフェース機能の設定

主にバーチャルサーバ機能を利用する場合に、仮想インタフェースを設定します。
128 まで設定できます。
「仮想インターフェース設定画面インデックス」のリンクをクリックしてください。

設定方法

Web 設定画面「仮想インターフェース」をクリックして、以下の画面から設定します。

○インターフェース
仮想インタフェースを作成するインタフェース名を指定します。
本装置のインタフェース名については「付録 A インタフェース名一覧」を参照してください。

○仮想 I/F 番号
作成するインタフェースの番号を指定します。
0～127 の間で設定できます。

○ IP アドレス
作成するインタフェースの IP アドレスを指定します。

○ネットマスク
作成するインタフェースのネットマスクを指定します。

○削除
仮想インタフェース設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れてください。

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。

第 30 章

GRE 設定

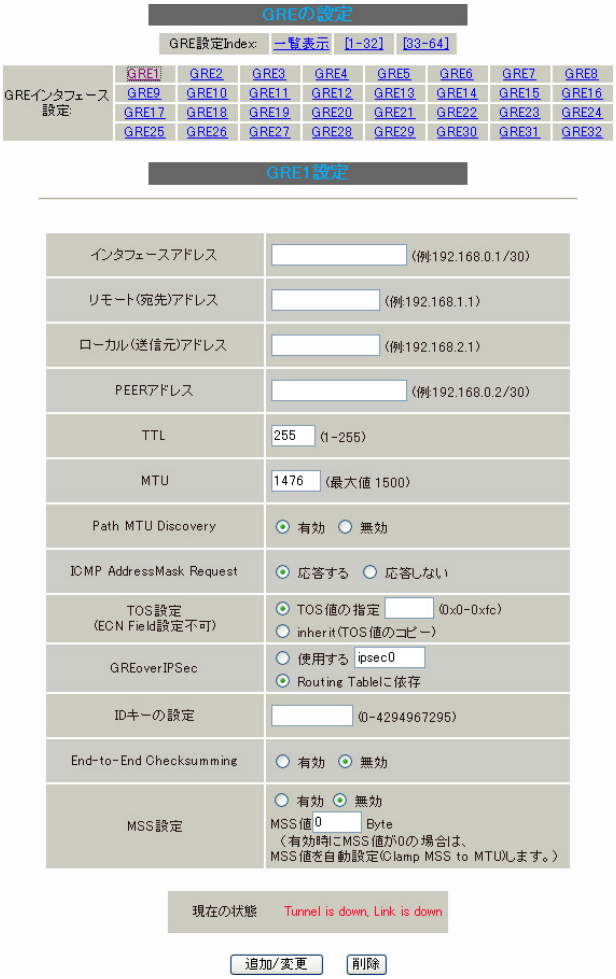
第 30 章 GRE 設定

GRE の設定

GRE は Generic Routing Encapsulation の略で、リモート側にあるルータまで仮想的なポイントツーポイント リンクを張って、多種プロトコルのパケットを IP トンネルにカプセル化するプロトコルです。
また、IPsec トンネル内に GRE トンネルを生成することもできますので、GRE を使用する場合でもセキュアな通信を確立することができます。

設定方法

Web 設定画面「GRE 設定」→[GRE インタフェース設定:]のインタフェース名「GRE1」～「GRE64」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。
前項目の「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。
本機能を「有効」にした場合は、本装置が送信する GRE 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。

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

○ TOS 設定
GRE パケットの ToS 値を設定します。

GRE の設定

○ GREoverIPSec
IPsec を使用して GRE パケットを暗号化する場合に「使用する」を選択します。
また、この場合には別途、IPsec の設定が必要です。
「Routing Table に依存」は GRE トンネルを暗号化して使わないときに選択してください。

GRE トンネルを暗号化するときの「IPsec 設定」は以下のようにしてください。

- 本装置側設定　**通常通り**
- IKE/ISAKMP ポリシー設定　**通常通り**
- IPsec ポリシー設定
  本装置側の LAN 側のネットワークアドレス：
  GRE 設定のローカルアドレス /32
  相手側の LAN 側のネットワークアドレス：
  GRE 設定のリモートアドレス /32

○ ID キーの設定
GRE パケットの識別用の ID を設定します。

○ End-to-End Checksumming
チェックサム機能の有効 / 無効を選択します。
この機能を「有効」にすると、
　checksum field (2byte) + offset (2byte)
の計 4byte が GRE パケットに追加されます。

○ MSS 設定
GRE トンネルに対して、clamp to MSS 機能を有効にしたり、MSS 値の設定が可能です。

入力後は「追加 / 変更」ボタンをクリックします。
直ちに設定が反映され、GRE が実行されます。

GRE の無効化

[GRE インタフェース設定:]の「GRE1」～「GRE64」各設定画面にある「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。

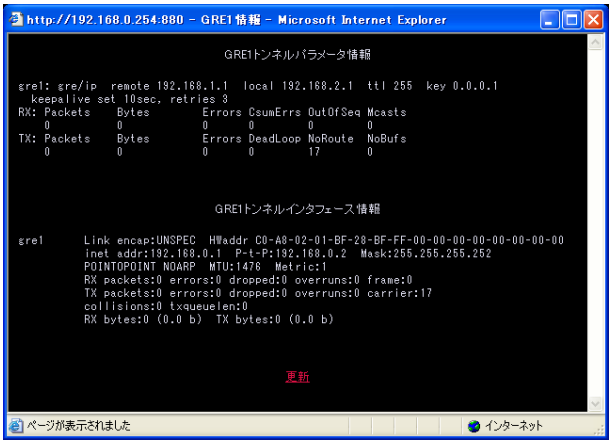
GRE の状態表示

[GRE インタフェース設定:]の「GRE1」～「GRE64」各設定画面下部にある「現在の状態」には、GRE の動作状況が表示されます。

(画面は表示例です)

また、実行しているインタフェースでは、「現在の状態」リンクをクリックすると、ウィンドウポップアップして以下の情報が表示されます。

- GREX トンネルパラメータ情報
- GREX トンネルインタフェース情報



(画面は「GRE1 情報」の表示例)

GRE の一覧表示

GRE 設定をおこなうと、設定内容が一覧表示されます。

○編集
設定の編集は「Interface 名」をクリックしてください。

○リンク状態
GRE トンネルのリンク状態は「Link State」に表示されます。
「up」が GRE トンネルがリンクアップしている状態です。

第 31 章

QoS 機能

第31章 QoS機能

Ⅰ．QoSについて

本装置の優先制御・帯域制御機能(以下、QoS機能)は以下の5つのキューイング方式で、トラフィック制御をおこないます。

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

クラスフル/クラスレスなキューイング
キューイングには、クラスフルなものとクラスレスなものがあります。

クラスレス キューイング
クラスレスなキューイングは、内部に設定可能なトラフィック分割用のバンド(クラス)を持たず、到着するすべてのトラフィックを同等に取り扱います。

SFQ、PFIFO、TBFがクラスレスなキューイングです。

クラスフル キューイング
クラスフルなキューイングでは、内部に複数のクラスを持ち、選別器(クラス分けフィルタ)によって、パケットを送り込むクラスを決定します。各クラスはそれぞれに帯域を持つため、クラス分けすることで帯域制御ができるようになります。またキューイング方式によっては、あるクラスがさらに自分の配下にクラスを持つこともできます。さらに、各クラス内でそれぞれキューイング方式を決めることもできます。

CBQとPQがクラスフルなキューイングです。

1.SFQ
SFQはパケットの流れ(トラフィック)を整形(※)しません。
パケットを送り出す順番を決めるだけです。

SFQでは、トラフィックを多数の内部キュー(※)に分割して収納します。
そして、各キューをラウンドロビンで回り、各キューからパケットをFIFO(※)で順番に送信していきます。

ラウンドロビンで順番にトラフィックが送信されることから、ある特定のトラフィックが他のトラフィックを圧迫してしまうことがなくなり、どのトラフィックも公平に送信されるようになります。
(複数のトラフィックを平均化できます。)

※ 整形
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。

※ キュー
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
「First In First Out」の略で、「最初に入ったものが最初に出る」、つまり最も古いものが最初に取り出されることを指します。

Ⅰ．QoS について

2.PFIFO

もっとも単純なキューイング方式です。
あらかじめキューのサイズを決定しておき、どのパケットも区別なくキューに収納していきます。
キューからパケットを送信するとき、送信するパケットは FIFO にしたがって選別されます。

キューのサイズを超えてパケットが到着したとき、超えた分のパケットは全て破棄されてしまいます。

キューのサイズが大きすぎると、キューイングによる遅延が発生する可能性があります。

3.TBF

帯域制御方法の 1 つです。
トークンバケツにトークンを、ある一定の速度(トークン速度)で収納していきます。
このトークン1個ずつがパケットを1個ずつつつかみ、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。

Ⅰ．QoS について

4.CBQ

CBQ は帯域制御の 1 つです。
複数のクラスを作成しクラスごとに帯域幅を設定することで、パケットの種類に応じて使用できる帯域を割り当てる方式です。

CBQ におけるクラスは、階層的に管理されます。
最上位には root クラスが置かれ、利用できる総帯域幅を定義しておきます。
root クラスの下に子クラスが置かれ、それぞれの子クラスには root で定義した総帯域幅の一部を利用可能帯域として割り当てます。
子クラスの下には、さらにクラスを置くこともできます。

各クラスへのパケットの振り分けは、フィルタ(クラス分けフィルタ)の定義に従っておこなわれます。

各クラスには帯域幅を割り当てます。
兄弟クラス間で割り当てている帯域幅の合計が、上位クラスで定義している帯域幅を超えないように設計しなければなりません。

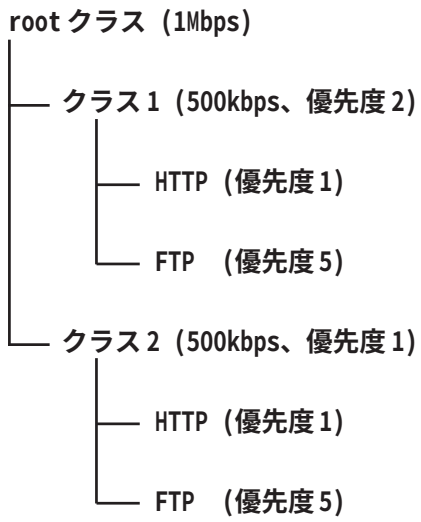
また、それぞれのクラスには優先度を割り振り、優先度に従ってパケットを送信していきます。

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。

例えば、右図<クラス構成図>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。

<クラス構成図　例>



Ⅰ．QoS について

5.PQ

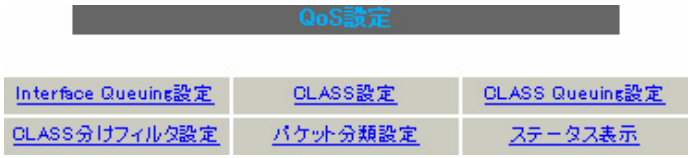
PQ は優先制御の 1 つです。
トラフィックのシェーピングはおこないません。

PQ では、パケットを分類して送り込むクラスに優先順位をつけておきます。
そして、フィルタによってパケットをそれぞれのクラスに分類したあと、優先度の高いクラスから優先的にパケットを送信します。
なお、クラス内のパケットは FIFO で取り出されます。

優先度の高いクラスに常にパケットがキューイングされているときには、より優先度の低いクラスからはパケットが送信されなくなります。

II．QoS 機能の各設定画面について

本装置では下記の各種設定画面で設定をおこないます。
設定方法については各設定の説明ページをご参照ください。



Interface Queuing 設定
本装置の各インタフェースでおこなうキューイング方式を定義します。
すべてのキューイング方式で設定が必要です。

CLASS 設定
CBQ をおこなう場合の、各クラスについて設定します。

CLASS Queuing 設定
各クラスにおけるキューイング方式を定義します。
CBQ 以外のキューイング方式について定義できます。

CLASS 分けフィルタ設定
パケットを各クラスに振り分けるためのフィルタ設定を定義します。
PQ、CBQ をおこなう場合に設定が必要です。

パケット分類設定
各パケットに TOS 値や MARK 値を付加するための設定です。
PQ をおこなう場合に設定します。
PQ では IP ヘッダによる CLASS 分けフィルタリングができないため、TOS 値または MARK 値によってフィルタリングをおこないます。

ステータス表示
QoS 機能の各種ステータスが表示されます。

III. 各キューイング方式の設定手順について

各キューイング方式の基本的な設定手順は以下の通りです。

◆SFQ の設定手順
「Interface Queueing 設定」で設定します。

◆PFIFO の設定手順
「Interface Queueing 設定」でキューのサイズを設定します。

◆TBF の設定手順
「Interface Queueing 設定」で、トークンのレート、バケツサイズ、キューのサイズを設定します。

◆CBQ の設定手順
1. ルートクラスの設定
「Interface Queueing 設定」で、ルートクラスの設定をおこないます。

2. 各クラスの設定
・「CLASS 設定」で、全てのクラスの親となる親クラスについて設定します。

・「CLASS 設定」で、親クラスの下に置く子クラスについて設定します。

・「CLASS 設定」で、子クラスの下に置くリーフクラスを設定します。

3. クラス分けの設定
「CLASS 分けフィルタ設定」で、CLASS 分けのマッチ条件を設定します。

4. クラスキューイングの設定
クラス内でさらにキューイングをおこなうときには「CLASS Queueing 設定」でキューイング設定をおこないます。

◆PQ の設定手順
1. インタフェースの設定
「Interface Queueing 設定」で、Band 数、Priority-map、Marking Filter を設定します。

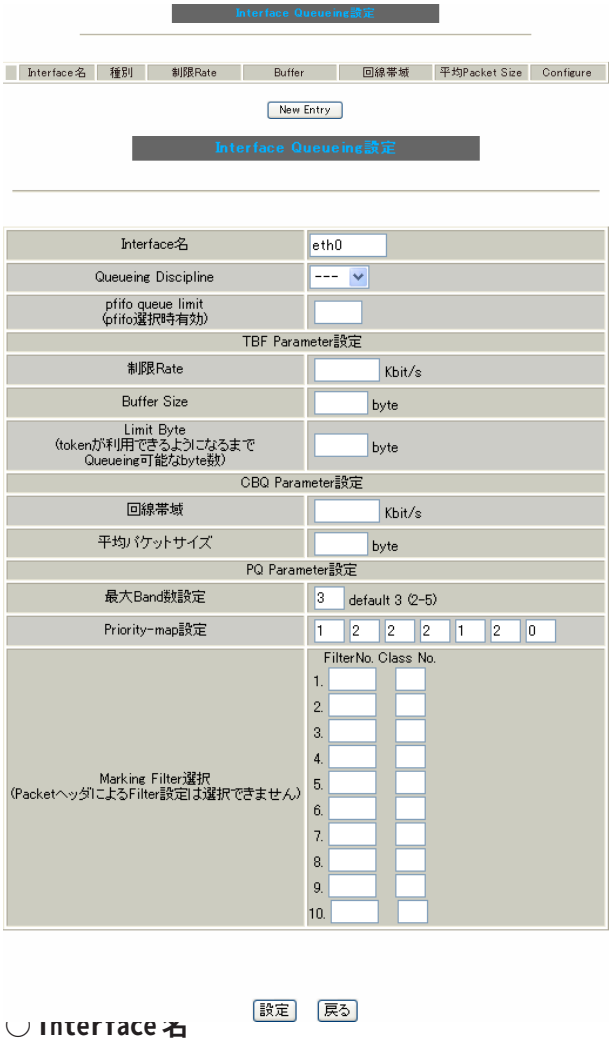
2. CLASS 分けのためのフィルタ設定
「CLASS 分けフィルタ設定」で、Mark 値によるフィルタを設定します。

3. パケット分類のための設定
「パケット分類設定」で、TOS 値または MARK 値の付与設定をおこないます。

Ⅳ．各設定画面での設定方法について

Interface Queueing 設定

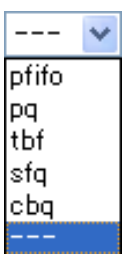
すべてのキューイング方式において設定が必要です。
設定を追加するときは「New Entry」をクリックします。



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

◯ Queueing Discipline
プルダウンからキューイング方式を選択します。

- sfq
- pfifo
- tbf
- cbq
- pq



◆SFQ の設定
Queueing Descipline で「sfq」を選択するだけです。

◆PFIFO の設定
◯ pfifo queue limit （pfifo 選択時有効）
パケットをキューイングするキューの長さを設定します。**パケットの数**で指定します。
1～1000 の範囲で設定してください。

◆TBF の設定
[TBF Paramater 設定]について設定します。

◯制限 Rate
バケツにトークンを入れていく速度を設定します。
回線の実効速度を上限に設定してください。

◯ Buffer Size
バケツのサイズを設定します。
これは瞬間的に利用できるトークンの最大値となります。
帯域の制限幅を大きくするときは、Buffer Size を大きく設定しておきます。

◯ Limit Byte
トークンを待っている状態でキューイングするときの、キューのサイズを設定します。

◆CBQ の設定
[CBQ Parameter 設定]について設定します。

◯回線帯域
root クラスの帯域幅を設定します。
接続回線の物理的な帯域幅を設定します。
(10BASE-TX で接続しているときは 10000kbits/s)

◯平均パケットサイズ
パケットの平均サイズを設定します。
バイト単位で設定します。

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(クラス ID 1001:～1003:)、最大数は 5(クラス ID 1001:～1005:)です。
設定可能な band 数は 2～5 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.
Class分けフィルタの設定番号を指定します。

・Class No.
パケットをおくるクラス番号(＝Band 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。
(「IX .TOS 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ります。

※ 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。
Band数が小さい方が、より優先度が高くなります。

※ クラス分けされたあとのパケットは、優先度の高いクラスから FIFO で送信されていきます。
各クラスの優先度は1001: > 1002: > 1003: > 1004: > 1005:となります。

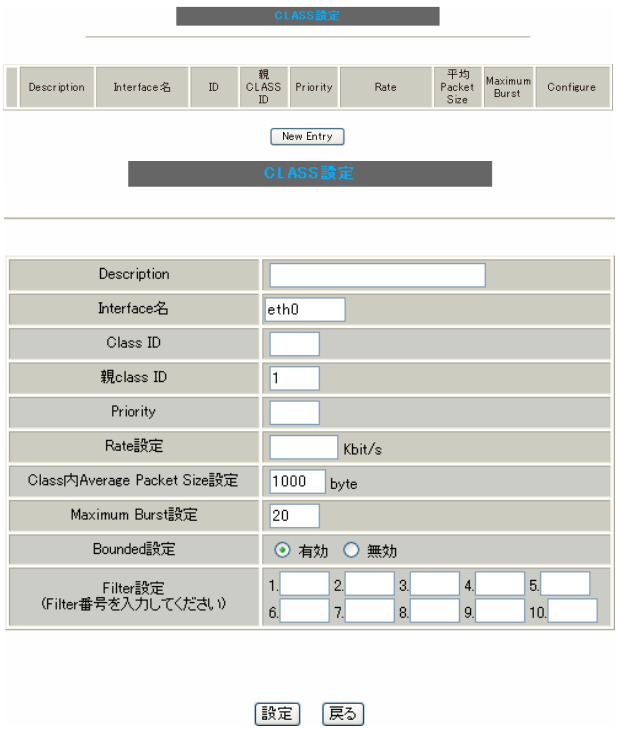
※ より優先度の高いクラスにパケットがあると、その間は優先度の低いクラスからはパケットが送信されなくなります。

設定後は「設定」ボタンをクリックします。

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。



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

○ Class ID
クラス ID を設定します。
クラスの階層構造における <minor 番号> となります。

○親 class ID
親クラスの ID を指定します。
クラスの階層構造における <major 番号> となります。

○ Priority
複数の CLASS 設定での優先度を設定します。
値が小さいものほど優先度が高くなります。
1～8 の間で設定します。

○ Rate 設定
クラスの帯域幅を設定します。
設定は kbit/s 単位となります。

○ Class 内 Average Packet Size 設定
クラス内のパケットの平均サイズを指定します。
設定はバイト単位となります。

○ Maximum Burst 設定
一度に送信できる最大パケット数を指定します。

○ Bounded 設定
「有効」を選択すると、兄弟クラスから余っている帯域幅を借りようとはしなくなります(Rate 設定値を超えて通信しません)。
「無効」を選択すると、その逆の動作となります。

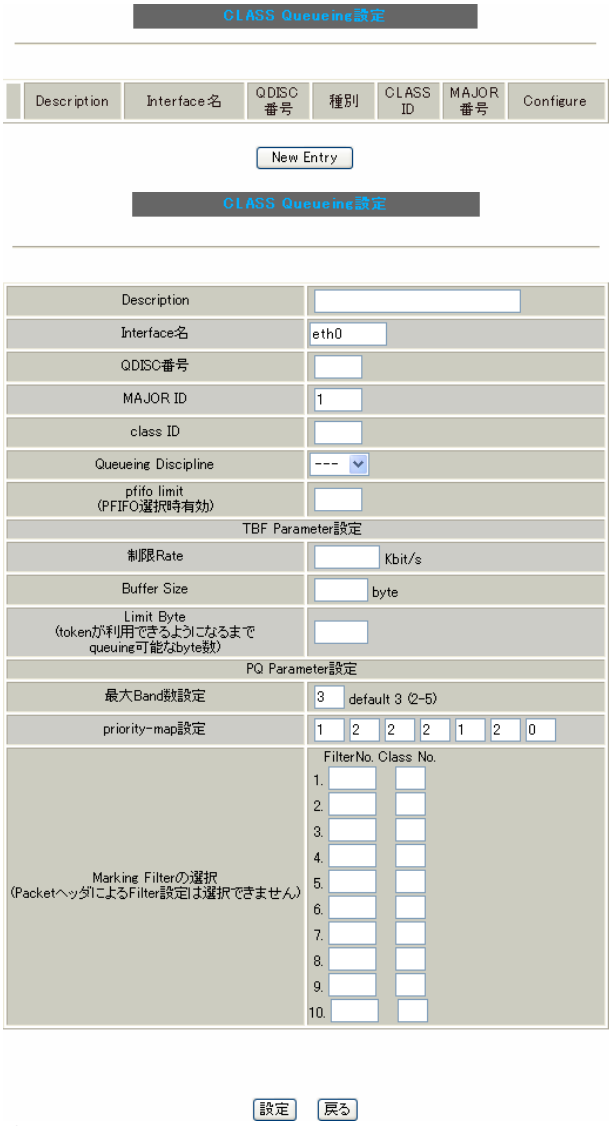
○ Filter 設定
CLASS 分けフィルタの設定番号を指定します。
ここで指定したフィルタにマッチングしたパケットが、このクラスに送られてきます。

設定後は「設定」ボタンをクリックします。

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。



◯ 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
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。

◯ QDISC 番号
このクラスが属している QDISC 番号を指定します。

◯ MAJOR ID
親のクラス ID を指定します。
クラスの階層構造における <major 番号 > となります。

◯ class ID
親クラスの ID を指定します。
クラスの階層構造における <minor 番号 > となります。

以下は、「Interface Queueing 設定」と同様に設定します。

◯ Queueing Discipline
「CLASS Queueing 設定」では「cbq」方式の選択はできません。

◯ pfifo limit (PFIFO 選択時有効)

[TBF Parameter 設定]
◯制限 Rate

◯ Buffer Size

◯ Limit Byte

[PQ Parameter 設定]
◯最大 Band 数設定

◯ priority-map 設定

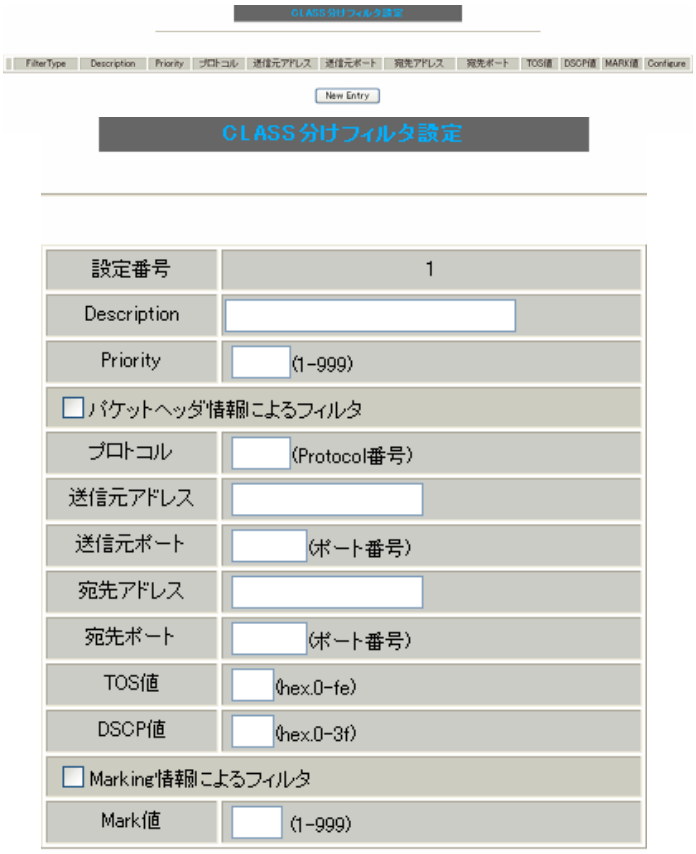
◯ Marking Filter の選択

設定後は「設定」ボタンをクリックします。

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。



○設定番号
自動で未使用の設定番号が振られます。

○ Description
設定名を付けることができます。
半角英数字のみ使用可能です。

○ Priority
複数の CLASS 分けフィルタ間での優先度を設定します。
値が小さいものほど優先度が高くなります。

[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。単一ホストを指定するときは<ホスト IP
アドレス>/32 の形式で指定します。
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。
範囲での指定はできません。

○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。

[Mariking 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。
PQ でフィルタをおこなうときは Mariking 情報によ
るもののみ有効です。

○ Mark 値
マッチ条件となる Mark 値を指定します。

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

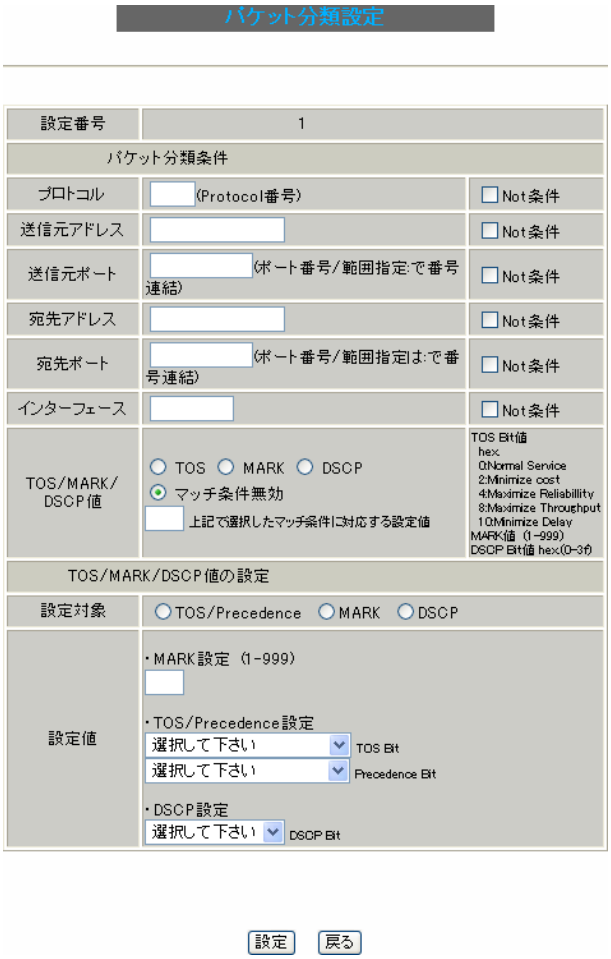
パケット分類設定

「パケット分類設定」の設定画面は以下の方法で開きます。

- Web 設定画面「QoS 設定」→「パケット分類設定」
- Web 設定画面「パケット分類設定」

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

設定を追加するときは「New Entry」をクリックします。



○設定番号
自動で未使用の設定番号が振られます。

[パケット分類条件]
パケット選別のマッチ条件を定義します。

○プロトコル
プロトコルを指定します。
プロトコル番号で指定してください。

○送信元アドレス
送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。単一ホストを指定するときは**<ホスト IP アドレス>/32** の形式で指定します。
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。

○インターフェース
インタフェースを選択します。
インタフェース名は「付録 A インタフェース名一覧」を参照してください。

各項目について「Not条件」にチェックを付けると、**その項目で指定した値以外のもの**がマッチ条件となります。

○ TOS/MARK/DSCP 値
マッチングする TOS/MARK/DSCP 値を指定します。
TOS、MARK、DSCP のいずれかを選択し、その値を指定します。
これらをマッチ条件としないときは「マッチ条件無効」を選択します。

Ⅳ．各設定画面での設定方法について

[TOS/MARK/DSCP 値]
パケット分類条件で選別したパケットに、新たに 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。

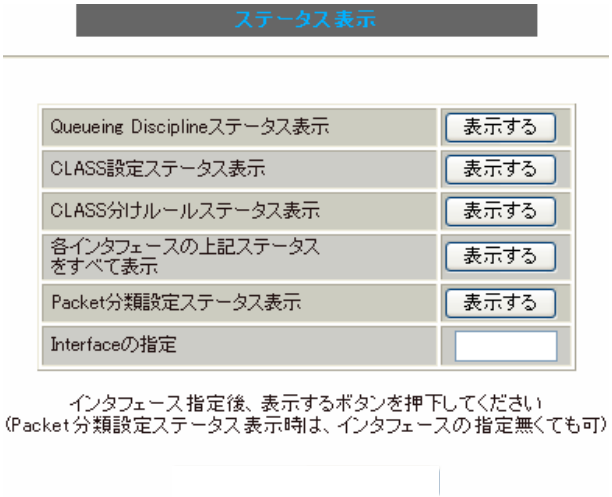
TOS/Precedence および DSCP については章末をご参照ください。

Ⅴ．ステータスの表示

ステータス表示

本機能の設定画面は以下の方法で表示されます。

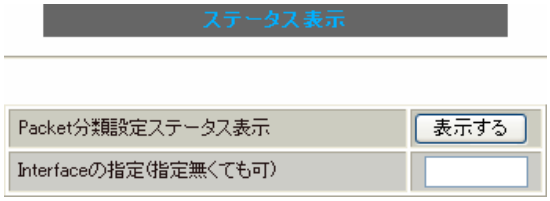
・Web 設定画面「QoS 設定」→「ステータス表示」



QoS 機能の各種ステータスを表示します。
表示したい項目について「表示する」ボタンをクリックしてください。

「Packet 分類設定ステータス表示」以外では、必ず Interface 名を「Interface の指定」に入力してから「表示する」ボタンをクリックしてください。

・Web 設定画面「パケット分類設定」→「ステータス表示」



パケット分類設定のステータス表示では、「Packet 分類設定ステータス表示」のみになります。

「Interface の指定」は必要な場合に入力してください。
指定がなくてもステータスは表示されます。

VI．設定の編集・削除方法

各 QoS 設定をおこなうと、設定内容が一覧で表示されます。


CLASS設定

	Description	Interface名	ID	親 CLASS ID	Priority	Rate	平均 Packet Size	Maximum Burst	Configure
1		eth0	1	0	1	100000Kbit/s	1000	100	Edit,Remove

(「CLASS 設定」画面の表示例)

○設定の編集をおこなう場合
Configure 欄の「Edit」をクリックすると設定画面に遷移し、その設定を修正できます。

○設定の削除をおこなう場合
Configure 欄の「Remove」をクリックすると、その設定が即座に削除されます。

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おこないます。
at 8、at16	マッチの開始は、指定した数値分のオフセットからであることを示します。 at 8であれば、ヘッダの9バイトめからマッチします。
flowid	マッチしたパケットを送るクラス

その 2 <PQ での表示例>

```
[ PARENT 1: ]
filter protocol ip pref 1 fw
filter protocol ip pref 1 fw handle 0x1 classid 1:3
filter protocol ip pref 2 fw
filter protocol ip pref 2 fw handle 0x2 classid 1:2
filter protocol ip pref 3 fw
filter protocol ip pref 3 fw handle 0x3 classid 1:1
```

pref	優先度
handle	TOSまたはMARK値
classid	マッチパケットを送るクラスID クラスID 1:(n) のとき、100(n):に送られます。

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。

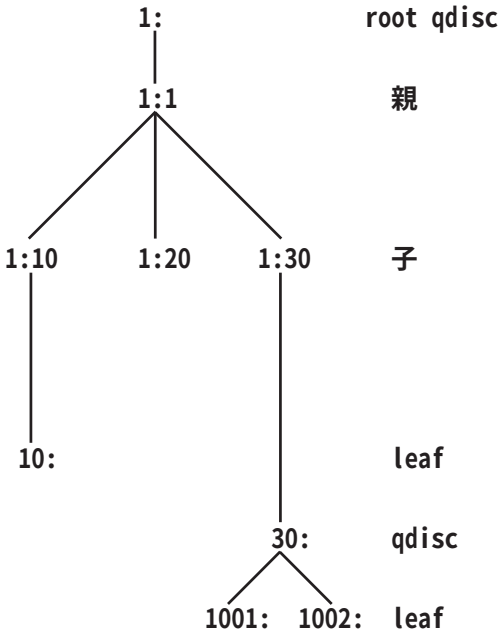
<MAJOR 番号>：<MINOR 番号>

・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 Data	 1000 0100	 (minimize delay) (maximize throughput)
TFTP	1000	(minimize delay)
SMTP Command phase DATA phase	 1000 0100	 (minimize delay) (maximize throughput)
Domain Name Service UDP Query TCP Query Zone Transfer	 1000 0000 0100	 (minimize delay) (maximize throughput)
NNTP	0001	(minimize monetary cost)
ICMP Errors Requests Responses	 0000 0000 <same as request>	 (mostly) (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制御をおこなうことができます。

○TOSとDSフィールドのビット定義

【TOSフィールド構造】

```
   0   1   2   3   4   5   6   7
 +---+---+---+---+---+---+---+---+
 |Precedence |Type of Service|CU |
 +---+---+---+---+---+---+---+---+
```

【DSCPフィールド構造】

```
   0   1   2   3   4   5   6   7
 +---+---+---+---+---+---+---+---+
 |           DSCP            |  CU  |
 +---+---+---+---+---+---+---+---+
 DSCP: differentiated services code point
 CU:   currently unused（現在未使用）
```

DSCPビットのとりうる値とその制御方法の定義は以下のようになっています。

定義名	DSCP値	制御方法
EF(Expedited Forwarding)	0x2e	パケットを最優先で転送(RFC3246)
AF(Assured Forwarding) AF11/AF12/AF13 AF21/AF22/AF23 AF31/AF32/AF33 AF41/AF42/AF43	 0x0a / 0x0c / 0x0e 0x12 / 0x14 / 0x16 0x1a / 0x1c / 0x1e 0x22 / 0x24 / 0x26	4つの送出優先度と3つの廃棄優先度を持ち、数字の上位桁は送出優先度(クラス)、下位桁は廃棄優先度を表します。(RFC2597) ・送出優先度　(高) 1 > 2 > 3 > 4 (低) ・廃棄優先度　(高) 1 > 2 > 3 (低)
CS(Class Selector) CS1 CS2 CS3 CS4 CS5 CS6 CS7	 0x08 0x10 0x18 0x20 0x28 0x30 0x38	既存のTOS互換による優先制御をおこないます。 Precedence1(Priority) Precedence2(Immediate) Precedence3(Flash) Precedence4(Flash Override) Precedence5(Critic/ESP) Precedence6(Internetwork Control) Precedence7(Network Control)
BE (Best Effort)	0x00	ベストエフォート(優先制御なし)

第 32 章

ネットワークテスト

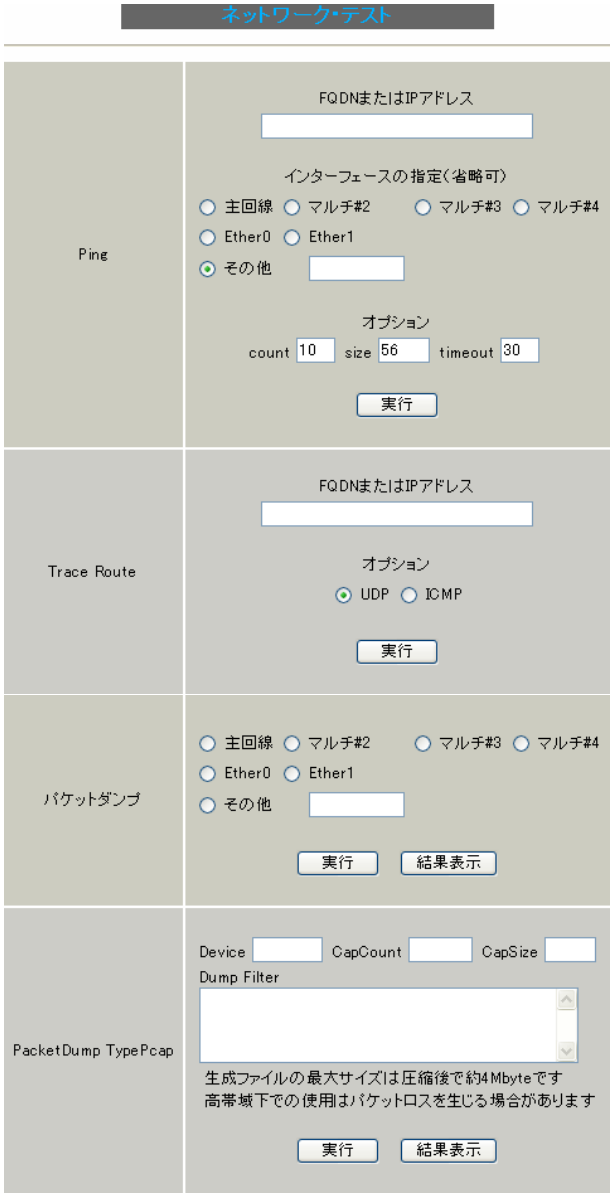
ネットワークテスト

XR-440 の運用時において、ネットワークテストをおこなうことができます。
ネットワークのトラブルシューティングに有効です。
以下の 3 つのテストができます。

- Ping テスト
- Trace Route テスト
- パケットダンプの取得

実行方法

Web 設定画面の「ネットワークテスト」をクリックして、以下の画面で各テストを実行します。



[Ping]

指定した相手に本装置から Ping を発信します。

○ FQDN または IP アドレス

FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

○インターフェースの指定（省略可）

ping パケットを送信するインタフェースを選択できます。
省略することも可能です。

○オプション

・count

送信する ping パケット数を指定します。
入力可能な範囲：1-10 です。初期値は 10 です。

・size

送信するデータサイズ(byte)を指定します。
入力可能な範囲：56-1500 です。初期値は 56 です。
(8 バイトの ICMP ヘッダが追加されるため、64 バイトの ICMP データが送信されます。)

・timeout

ping コマンドの起動時間を指定します。
入力可能な範囲：1-30 です。初期値は 30 です。

入力が終わりましたら「実行」をクリックします。

実行結果例

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=69.0 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
```

ネットワークテスト

[Trace Route]
指定した宛先までに経由するルータの情報を表示します。

○ FQDN または IP アドレス
FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

○オプション

・UDP
UDP パケットを使用する場合に指定します。
初期設定は UDP です。

・ICMP
ICMP パケットを使用する場合に指定します。

入力が終わりましたら「実行」をクリックします。

実行結果例

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)  9.205 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
```

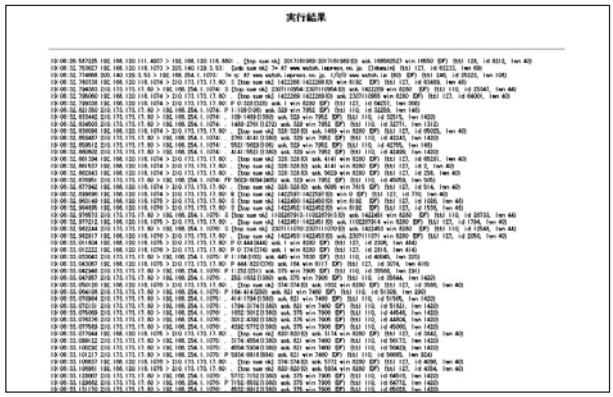
Ping・Trace Route テストで応答メッセージが表示されない場合は、DNS で名前解決ができていない可能性があります。
その場合はまず、IP アドレスを直接指定してご確認ください。

[パケットダンプ]
パケットのダンプを取得できます。
ダンプを取得したいインタフェースを選択して「実行」をクリックします。

インタフェースについては「その他」を選択し、直接インタフェースを指定することもできます。
その場合はインタフェース名(「gre1」や「ipsec0」など)を指定してください。

その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例



「結果表示」をクリックするたびに、表示結果が更新されます。
パケットダンプの表示は、最大で 100 パケット分までです。
100 パケット分を超えると、古いものから順に表示されなくなります。

ネットワークテスト

[PacketDump TypePcap]
拡張版パケットダンプ取得機能です。
指定したインタフェースで、指定した数のパケットダンプを取得できます。

○ Device
パケットダンプを実行する、本装置のインタフェース名を設定します。
インタフェース名は本書「付録A インタフェース名一覧」をご参照ください。

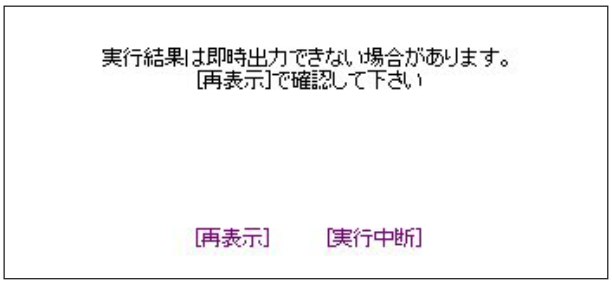
○ CapCount
パケットダンプの取得数を指定します。
1-999999 の間で指定します。

○ CapSize
1パケットごとのダンプデータの最大サイズを指定できます。単位は“ byte ”です。
たとえば 128 と設定すると、128 バイト以上の長さのパケットでも 128 バイト分だけをダンプします。
大きなサイズでダンプするときは、本装置への負荷が増加することがあります。
また、記録できるダンプ数も減少します。

○ Dump Filter
ここに文字列を指定して、それに合致するダンプ内容のみを取得できます。
空白・大小文字も判別します。
一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したパケットダンプ内容のみ抽出して記録します。

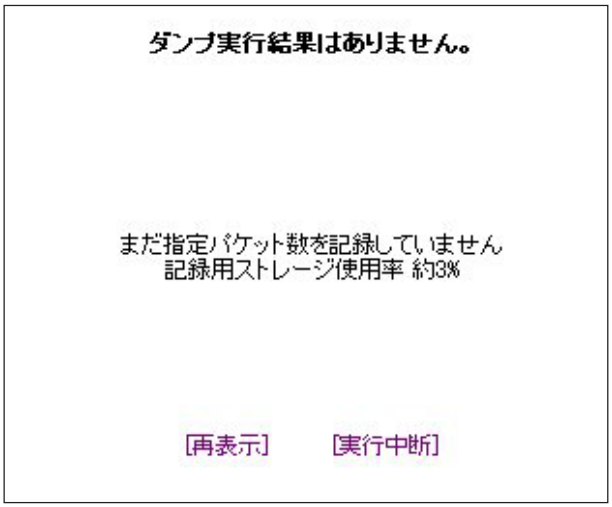
入力後、「実行」ボタンでパケットダンプを開始します。

パケットダンプを開始したときの画面表示



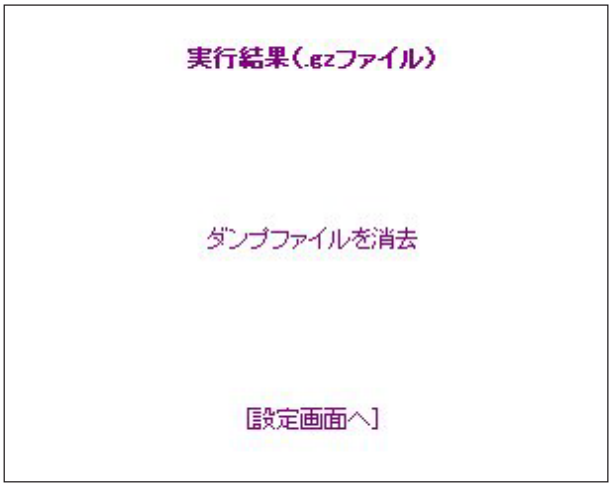
また、パケットダンプ実行中に「再表示」ボタンをクリックすると、下記のような画面が表示されます。

パケットダンプ結果を表示できないときの画面表示



ネットワークテスト

パケットダンプが実行終了したときの画面



上記の画面は以下の場合に表示されます。

- 「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
- 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

「実行結果(.gz ファイル)」リンクから、パケットダンプ結果を圧縮したファイルをローカルホストに保存してください。

ローカルホスト上で解凍してできたファイルは、Ethereal で閲覧することができます。

「ダンプファイルを消去」をクリックすると、本装置に記録されているダンプファイルを消去します。

PacketDump TypePcap の注意点

- 取得したパケットダンプ結果は、libcap 形式で gzip 圧縮して保存されます。
- 取得できるデータサイズは gzip 圧縮された状態で最大約 4MB です。
- 本装置上には、パケットダンプ結果を 1 つだけ記録しておけます。
  パケットダンプ結果を消去せずに PacketDump TypePcap を再実行して実行結果ファイルを作成したときは、それまでに記録されていたパケットダンプ結果に上書きされます。

本装置のインタフェース名については本書の「付録 A インタフェース名一覧」をご参照ください。

第 33 章

システム設定

システム設定

「システム設定」ページでは、XR-440 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 / ログの削除
◆パスワードの設定
◆ファームウェアのアップデート
◆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
◆オプション CF カード
◆ ARP filter 設定
◆メール送信機能の設定

設定・実行方法

Web 設定画面「システム設定」をクリックします。
各項目のページへは、設定画面上部のリンクをクリックして移動します。

◆時計の設定

本装置内蔵時計の設定をおこないます。

設定方法

「時計の設定」をクリックして設定画面を開きます。

24 時間単位で時刻を設定してください。

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

システム設定

◆ログの表示

本装置のログが全てここで表示されます。

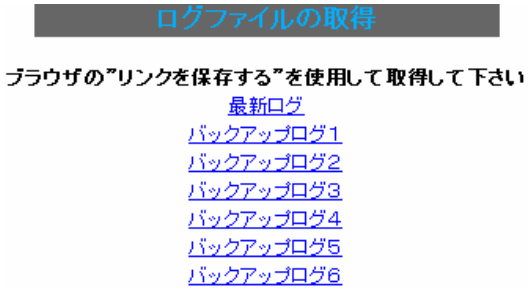
実行方法

「ログの表示」をクリックして表示画面を開きます。

「表示の更新」ボタンをクリックすると表示が更新されます。

記録したログは圧縮して保存されます。
本装置にて初期化済みのオプションCFカードを装着時は、自動的に CF カードにログを記録します。

保存されるログファイルは最大で 6 つです。
ログファイルが作成されたときは画面上にリンクが生成されます。
古いログファイルから順に削除されていきます。

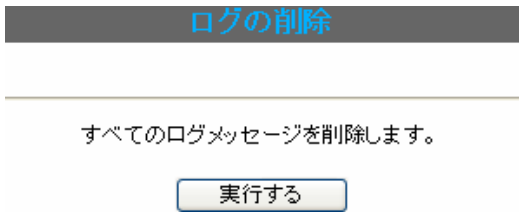


◆ログの削除

ログ情報は最大 2MB までのサイズで保存されます。
また、再起動時にログ情報は削除されます。
手動で削除する場合は次のようにしてください。

実行方法

「ログの削除」をクリックして画面を開きます。



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

本体の再起動をおこなった場合も、それまでのログは全てクリアされます。

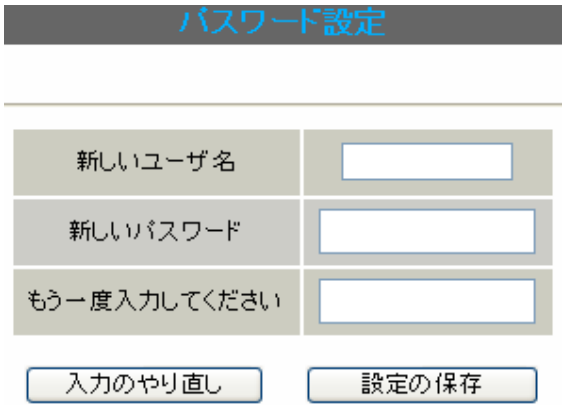
システム設定

◆パスワードの設定

XR-440 の設定画面にログインする際のユーザ名、パスワードを変更します。
ルータ自身のセキュリティのためにパスワードを変更されることを推奨します。

設定方法

「パスワードの設定」をクリックして設定画面を開きます。



新しいユーザ名とパスワードの設定ができます。

○新しいユーザ名
半角英数字で 1 から 15 文字まで設定可能です。

○新しいパスワード
半角英数字で 1 から 8 文字まで設定可能です。
大文字・小文字も判別しますのでご注意ください。

○もう一度入力してください
確認のため再度「新しいパスワード」を入力してください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。

本装置の操作を続行すると、ログイン用のダイアログ画面がポップしますので、新たに設定したユーザ名とパスワードで再度ログインしてください。

システム設定

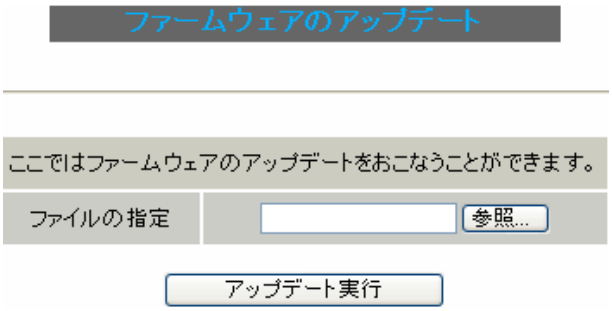
◆ファームウェアのアップデート

本装置は、ブラウザ上からファームウェアのアップデートをおこないます。
ファームウェアは弊社ホームページよりダウンロードできます。

弊社サポートサイト
http://www.centurysys.co.jp/support/xr440c.html

実行方法

1 「ファームウェアのアップデート」をクリックして画面を開きます。

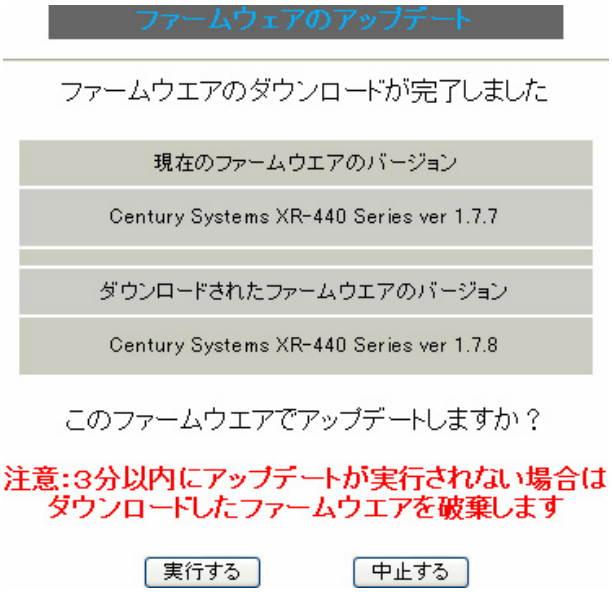


2 「参照」ボタンを押して、弊社ホームページからダウンロードしてきたファームウェアファイルを選択し、「アップデート実行」ボタンを押してください。

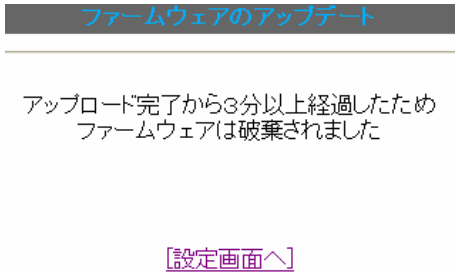
3 その後、ファームウェアを本装置に転送します。
転送が終わるまではしばらく時間がかかります。

転送完了後に、右上のようなアップデートの確認画面が表示されます。
バージョン等が正しければ「実行する」をクリックしてください。

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おこ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。

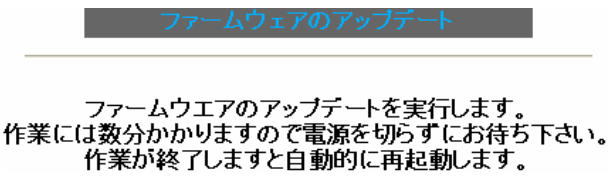


上記画面が表示されたままで3分間以上経過してから、「実行する」ボタンをクリックすると、以下の画面が表示され、アップデートは実行されません。



アップデートを実行するには再度、2 の操作からおこなってください。

4 アップデートを実行した場合は以下の画面が表示され、ファームウェアの書き換えが始まります。



アップデート中は、本体の Status 1 LED(赤)が点滅します。LED が動作中は、アクセスをおこなわずに、そのままお待ちください。
ファームウェアの書き換えが終了すると、本装置は自動的に再起動して、アップデートの完了となります。

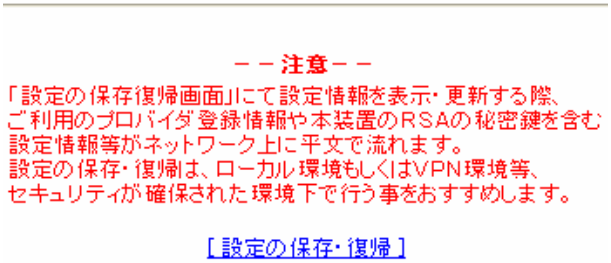
システム設定

◆設定の保存と復帰

XR-440 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

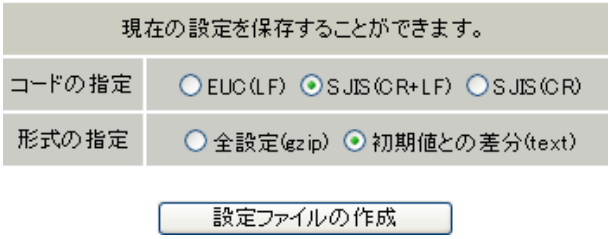
「設定の保存・復帰」をクリックして画面を開きます。



上記のような注意のメッセージが表示されます。
ご確認いただいた上で「設定の保存・復帰」のリンクをクリックしてください。

[設定の保存]

設定を保存するときは、テキストのエンコード方式と保存形式を選択ます。



○コードの指定

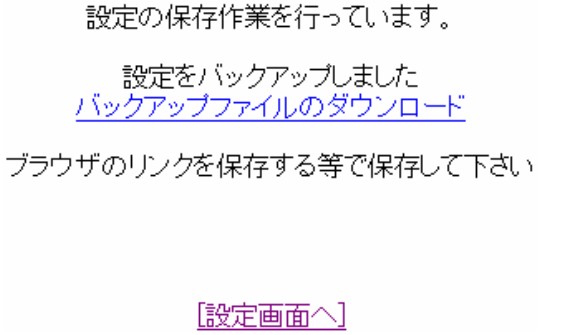
「EUC(LF)」「SJIS(CR+LF)」「SJIS(CR)」のいずれかを選択します。

○形式の指定

・全設定(gzip)
　本装置のすべての設定を gzip 形式で圧縮して保存します。

・初期値との差分(text)
　初期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。

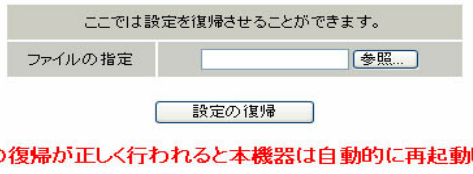
選択後は「設定ファイルの作成」をクリックします。
クリックすると以下のメッセージが表示されます。



「バックアップファイルのダウンロード」リンクから、設定をテキストファイルで保存しておきます。
設定ファイル名は「backup.txt」です。

[設定の復帰]

「参照」をクリックして、保存しておいた設定ファイル(「backup.txt」)を選択します。
保存形式が「全設定」の保存ファイルは、gzip 圧縮形式のまま、復帰させることができます。



設定ファイルを選択後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、本装置が自動的に再起動されます。

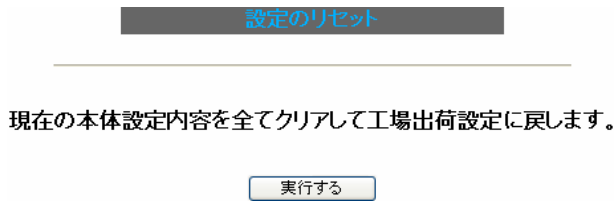
システム設定

◆設定のリセット

XR-440 の設定を全てリセットし、工場出荷時の設定に戻します。

実行方法

「設定のリセット」をクリックして画面を開きます。



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

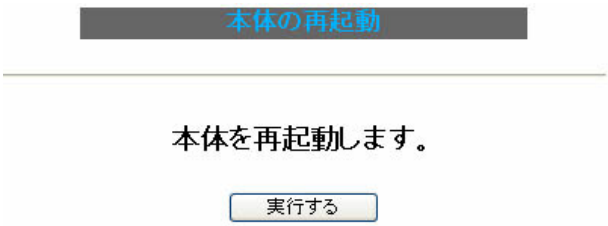
設定のリセットにより全ての設定が失われますので、念のために「設定のバックアップ」を実行しておくようにしてください。

◆本体再起動

XR-440 を再起動します。
設定内容は変更されません。

実行方法

「再起動」をクリックして画面を開きます。



「実行する」ボタンをクリックすると、リセットが実行されます。

本体の再起動をおこなった場合、それまでのログは全てクリアされます。

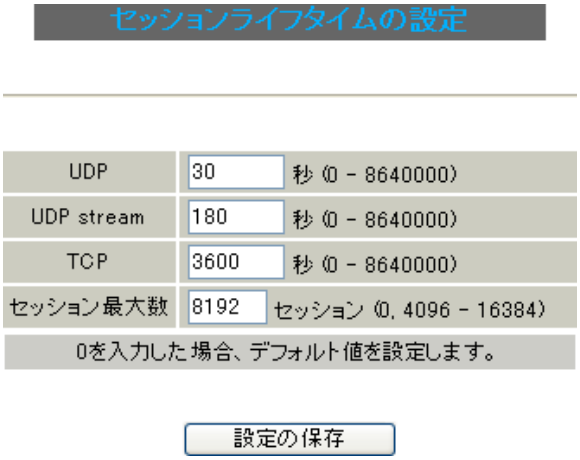
システム設定

◆セッションライフタイムの設定

NAT/IP マスカレードのセッションライフタイムを設定します。

設定方法

「セッションライフタイムの設定」をクリックして画面を開きます。



○ UDP

UDP セッションのライフタイムを設定します。
単位は秒です。0 ～ 8640000 の間で設定します。
初期設定は 30 秒です。

○ UDP stream

UDP streamセッションのライフタイムを設定します。
単位は秒です。0 ～ 8640000 の間で設定します。
初期設定は 180 秒です。

○ TCP

TCP セッションのライフタイムを設定します。
単位は秒です。0 ～ 8640000 の間で設定します。
初期設定は 432000 秒です。

○セッション最大数

XR-440 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。
初期設定は 8192 です。

なお、XR-440 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 17 章 SYSLOG サービス」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。

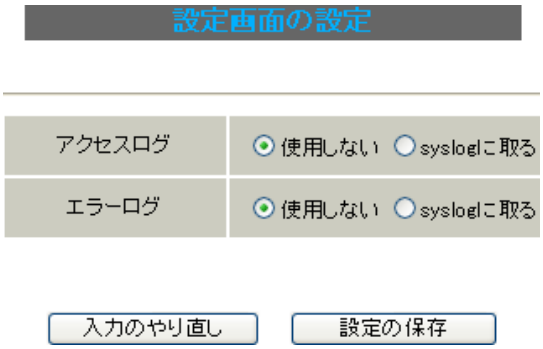
システム設定

◆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。

設定方法

「設定画面の設定」をクリックして画面を開きます。



○アクセスログ
○(アクセス時の)エラーログ
設定画面のアクセスログ / エラーログを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。

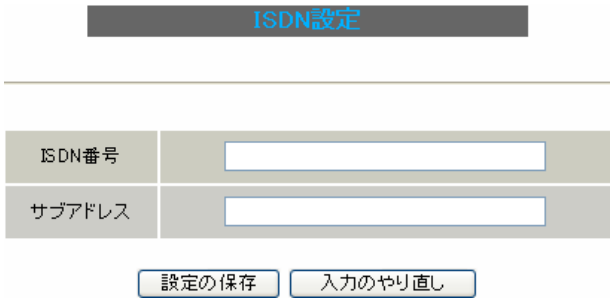
アクセスログ・エラーログは、「syslog」サービスの設定にしたがって出力されます。

◆ ISDN 設定

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

設定方法

「ISDN 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。

最後に「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-440 に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 カードの操作をおこないます。

ここでは以下の設定をおこなうことができます。

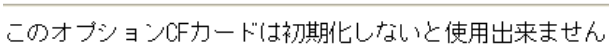
- CF カードの初期化
- CF カードへの設定のバックアップ

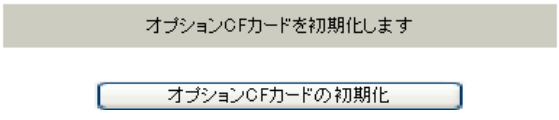
実行方法

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

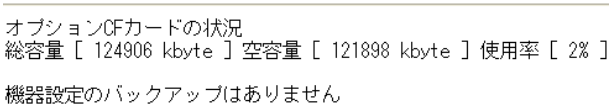
はじめて CF カードを装着したときは、必ず CF カードを初期化する必要があります。
初期化をおこなわないと CF カードを使用できません。
CFカードを初期化するときは「オプションCFカードの初期化」をクリックします。

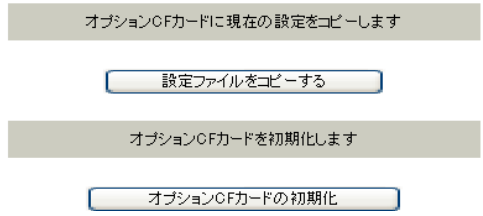




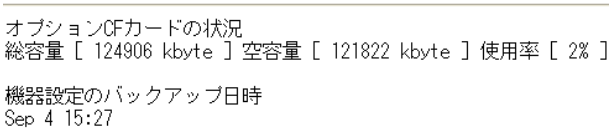
○CF カードへの設定のバックアップ

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。
CF カードが初期化されていないときは、「オプション CF カードに現在の設定をコピーします」項目は表示されません。





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、本装置前面パネルの CF カードスロットに挿入してください。

- CF カードが挿入され、動作している場合
  本体前面の「Status LED」(橙)が点灯します。
- CF カードが使用可能状態の場合
  本体前面の「Active LED」(緑)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。
その後 CF ランプ(「Status LED」/「Active LED」)が消灯しましたら、CF カードを安全に取り外せます。

この作業をおこなわずにCFカードを取り外すと、本装置およびCFカードが破損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。

設定方法

「ARP filter設定」をクリックして画面を開きます。

ARP filter を「無効」にするか、「有効」にするかを選択します。

「有効」を選択して保存すると、ARP filter が動作します。
「有効」にすることで、同一 IP アドレスの ARP を複数のインタフェースで受信したときに、当該 MAC アドレス以外のインタフェースから ARP 応答を出さないようにできます。

選択しましたら「設定の保存」をクリックしてください。設定が完了します。
設定はすぐに反映されます。

システム設定

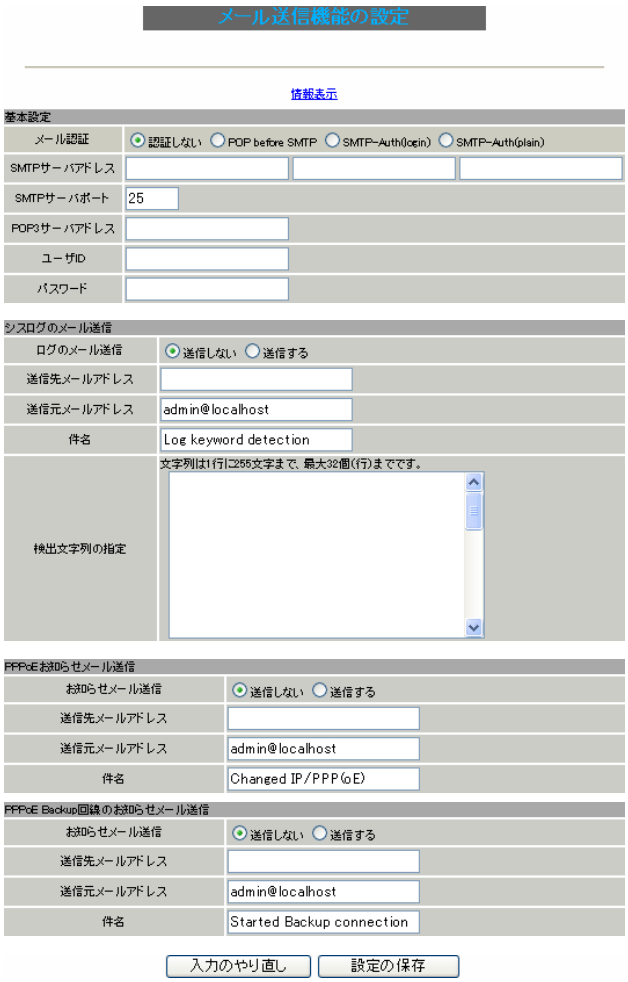
◆メール送信機能の設定

各種メール送信機能の設定をおこないます。
ここでは以下の場合にメール送信を設定出来ます。

- SYSLOG サービスのログメール送信
- PPP/PPPoE 接続設定の主回線 接続 IP 変更 お知らせメール
- PPP/PPPoE 接続設定のバックアップ回線 接続 お知らせメール

設定方法

「メール送信機能の設定」をクリックして画面を開きます。



＜基本設定＞

○メール認証

下記よりいずれかを選択します。

「認証しない」

メールサーバとの認証をおこなわずに、本装置が自律的にメールを送信します。

「POP before SMTP」

指定した POP3 サーバにあらかじめアクセスさせることによって、SMTP によるメールの送信を許可する方式です。

「SMTP-Auth(login)」

メール送信時にユーザ認証をおこない、メールの送信を許可する方法です。
平文によるユーザ認証方式です。

「SMTP-Auth(plain)」

メール送信時にユーザ認証をおこない、メールの送信を許可する方法です。
LOGIN も PLAIN 同様、平文を用いた認証形式です。

○ SMTP サーバアドレス

SMTP サーバアドレスは３箇所まで設定できます。
それぞれの設定箇所において１つの IPv4 アドレス、または FQDN が設定可能です。
FQDN は最大 64 文字で、ドメイン形式とホスト形式のどちらでも設定できます。

ドメイン形式で指定する場合
＜入力例＞ @centurysys.co.jp

ホスト形式で指定する場合
＜入力例＞ smtp.centurysys.co.jp

本設定は、メール認証設定で「認証しない」場合は任意ですが、認証ありの場合は必ず設定してください。

○ SMTP サーバポート

設定されたポートを使用してメールを送信します。
設定可能な範囲：1-65535 です。
初期設定は “ 25 ” です。

システム設定

○ POP3 サーバアドレス
IPv4 アドレス、または FQDN で設定します。
FQDN は最大 64 文字で、ホスト形式のみ設定できます。
認証方式で「POP before SMTP」を指定した場合は必ず設定してください。

○ユーザ ID
ユーザ ID を設定します。
最大文字数は 64 文字です。
認証方式を「認証しない」以外で選択した場合は必ず設定してください。

○パスワード
パスワードを設定します。
半角英数字で 64 文字まで設定可能です。
大文字・小文字も判別しますのでご注意ください。
認証方式を「認証しない」以外で選択した場合は必ず設定してください。

＜シスログのメール送信＞
ログの内容を電子メールで送信したいときの設定です。

○ログのメール送信
ログメール機能を使用する場合は「送信する」を選択します。

○送信先メールアドレス
ログメッセージの送信先メールアドレスを指定します。
最大文字数は 64 文字です。

○送信元メールアドレス
送信元のメールアドレスは任意で指定できます。
最大文字数は 64 文字です。
初期設定は「admin@localhost」です。

○件名
任意で指定できます。
使用可能な文字は半角英数字で、最大 64 文字です。
初期設定は「Log Keyword detection」です。

○検出文字列の指定
ここで指定した文字列が含まれるログをメールで送信します。
検出文字列には、pppd、IP、DNS などログ表示に使用される文字列を指定してください。
なお、文字列の記述に正規表現は使用できません。
文字列を指定しない場合はログメールは送信されません。

文字列の指定は、半角英数字で一行につき 255 文字まで、かつ最大 32 行までです。
空白・大小文字も判別します。
一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したログのみ抽出して送信します。
なお、「検出文字列の指定」項目は、「シスログのメール送信」機能のみ有効です。

システム設定

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

○お知らせメール送信
お知らせメール機能を使用する場合は「送信する」を選択します。

○送信先メールアドレス
お知らせメールの送り先メールアドレスを１箇所入力します。
最大文字数は 64 文字です。

○送信元メールアドレス
お知らせメールの送り元メールアドレスを１箇所入力します。
最大文字数は 64 文字です。
初期設定は「admin@localhost」です。

○件名
送信されるメールの件名を任意で設定できます。使用可能な文字は半角英数字で、最大 64 文字です。
初期設定は「Changed IP/PPP(oE)」です。

＜PPPoE Backup 回線のお知らせメール送信＞
バックアップ回線で接続したときに、それを電子メールによって通知させることができます。

設定内容は＜PPPoE お知らせメール送信＞と同様です。

○お知らせメール送信
○送信先メールアドレス
○送信元メールアドレス
○件名
初期設定は「Started Backup connection」です。

必要項目への入力が終わりましたら「設定の保存」をクリックしてください。

○情報表示
リンクをクリックすると、メール送信の成功 / 失敗に関する情報が表示されます。

第 34 章

情報表示

本体情報の表示

本体の機器情報を表示します。
以下の項目を表示します。

- **ファームウェアバージョン情報**
  現在のファームウェアバージョンを確認できます。

- **インタフェース情報**
  各インタフェースの IP アドレスや MAC アドレスなどです。
  PPP/PPPoE や IPsec 論理インタフェースもここに表示されます。

- **リンク情報**
  本装置の各 Ethernet ポートのリンク状態、リンク速度が表示されます。

- **ルーティング情報**
  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。

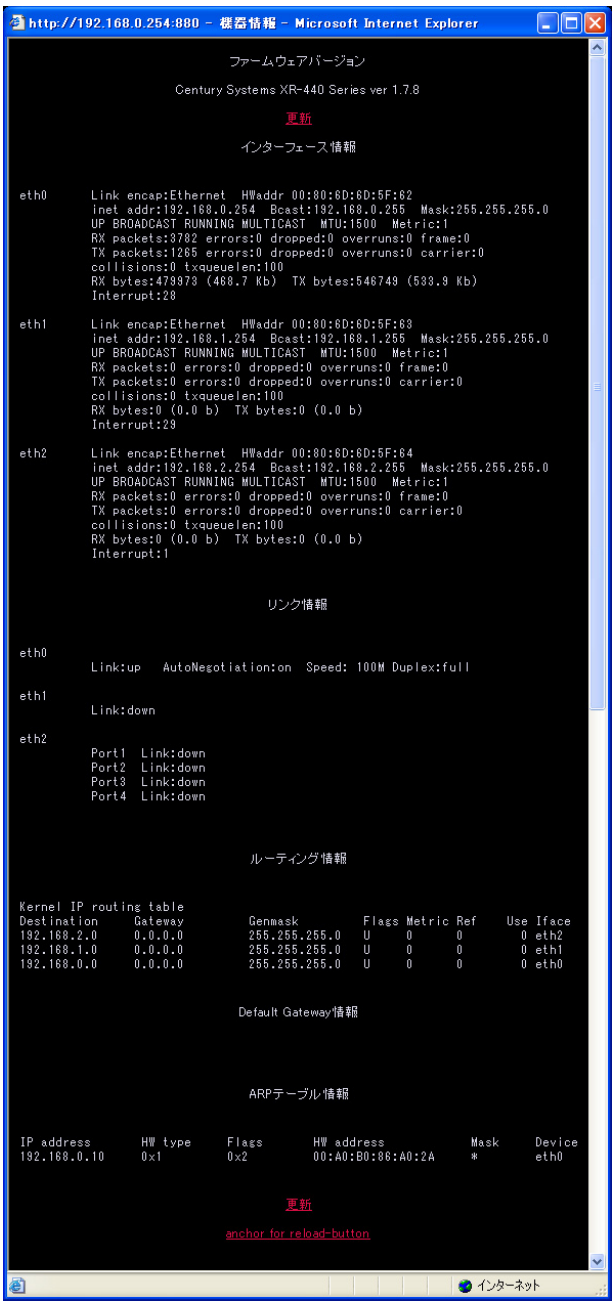
- **Default Gateway 情報**
  デフォルトルート情報です。

- **ARP テーブル情報**
  XR が保持している ARP テーブルです。

- **DHCP クライアント取得情報**
  DHCP クライアントとして設定しているインタフェースがサーバから取得した IP アドレス等の情報を表示します。

実行方法

Web 設定画面の「情報表示」をクリックすると、新しいウィンドウが開いて本体情報表示されます。



画面中の「更新」をクリックすると、表示内容が更新されます。

第 35 章

詳細情報表示

第 35 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。

表示される内容は以下のとおりです。

- **ルーティング情報**
  XR のルーティングテーブル、ルーティングテーブルの内部情報、ルートキャッシュの情報、デフォルトゲートウェイ情報が表示できます。
  このうち、ルーティングテーブルの内部情報とルートキャッシュの情報はここでのみ表示できます。

- **PPPoE 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フェース名、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。

```
PPPoE 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
```

- **OSPF 情報**
- **RIP 情報**
- **IPsec 情報**
- **DHCP アドレスリース情報**
- **NTP 情報**
- **VRRP 情報**
- **PPPoE to L2TP**
- **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 36 章

運用管理設定

Ⅰ．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

◆本装置の設定を初期化する

1 本装置が停止状態になっていることを確認します。

2 本体背面にある「Init」ボタンを押しながら、Power 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 LED」(橙)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 の状態になったら「Init」ボタンを放します。
その後、本装置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

1 本装置が停止状態になっていることを確認します。

2 本装置にオプション CF カードが挿入されていることを確認します。

3 本体背面にある「INIT」ボタンを押しながら、Power 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。

4 本体前面にある「Status LED」(橙)ランプの点滅が止まるまで「Init」ボタンを押し続けます。

5 点滅が止まったら「Init」ボタンを放します。
その後、本装置が 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おこなってください。

II．携帯電話による制御

XR-440にグローバルアドレスが割り当てられていて、インターネットに接続している状態ならば、iモードおよびEZウェブに対応した携帯電話から以下のような操作が可能です。

- **ルータとしてのサービスを停止する**
- **ルータとしてのサービスを再開する**
- **本装置を再起動する**

この機能を利用する際は、パケットフィルタリング設定によってWAN側からの設定変更を許す設定になっていることが必要になります。
WAN側から本装置の設定変更を許すフィルタ設定については**「第26章 パケットフィルタ機能」**項目をご覧ください。

実際に操作画面にアクセスするためには、iモード端末から次のURLをしてしてください。

<i モード端末からアクセスする場合>

http:// 装置の IP アドレス:880/i/

<EZ ウェブ端末からアクセスする場合>

http:// 装置の IP アドレス:880/ez/index.hdml

アクセスすると認証画面が表示されますので、ユーザ名とパスワードを入力してください。

2.i フィルタ起動
実行すると、ルーターとしてのサービスが停止します。

この状態では、WANからLANへのアクセスはできません。
WAN側からはXR-440自身の設定画面もしくはiモード画面にしかアクセスできなくなります。
また、LAN側からインターネット側へアクセスしても、アクセス先からの応答を受け取ることができなくなります。

3.i フィルタ停止
実行すると、以前の設定状態に戻り、ルーター機能が再開されます。

iモードからアクセスするには、パケットフィルタの「入力フィルタ設定」で、インターネット側からXR-440の設定画面にログインできるように設定しておく必要があります。

IPアドレス自動割り当ての契約でインターネットに接続されている場合、XR-440に割り当てられたグローバルアドレスが変わってしまう場合があります。
もし、アドレスが変わってしまったときは、iモードからの制御ができなくなってしまうことが考えられますので(アドレスが分からなくなるため)、運用には十分ご注意ください。

⇒PPPoEで接続している場合に限り、「PPPoEお知らせメール送信」機能を使って現在のIPアドレスを任意のアドレスにメール通知することができます。

III．携帯電話による操作方法

1　携帯電話端末から XR-440 の WAN 側に割り当てられたグローバルアドレスを指定してアクセスします。

2　ユーザ名とパスワードを入力して「OK」を選択します。

3　操作メニューが表示されます。

操作したい項目を選択して実行してください。

4　「フィルタ状態」を選択すると以下のような画面が表示されて、現在の状態を確認できます。

付録 A

インタフェース名一覧

付録 A

インタフェース名一覧

本装置は、以下の設定においてインタフェース名を直接指定する必要があります。

- OSPF 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
- 仮想インタフェース機能
- QoS 機能
- ネットワークテスト

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

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インタフェース (<n>はVLAN ID)
eth1.<n>	eth1上のVLANインタフェース
eth2.<n>	eth2上のVLANインタフェース
eth0:<n>	eth0上の仮想インタフェース (<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インタフェース
eth2:<n>	eth2上の仮想インタフェース
lo:<n>	loopbackインタフェース (<n>は仮想IF番号)

表左：インタフェース名
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	192.168.2.254/255.255.255.0

DHCPクライアント機能	無効 （※ Ether 2は機能なし）
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	有効
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
PPPoE to L2TP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）
スケジュール機能	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	無効
パケット分類機能	無効

設定画面ログインID	admin
設定画面ログインパスワード	admin

付録 C

サポートについて

付録 C

サポートについて

◆本製品に関してのサポートは、ユーザー登録をされたお客様に限らせていただきます。
必ずユーザー登録していただきますよう、お願いいたします。

◆サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。

・サポートデスク
e-mail　：support@centurysys.co.jp
電話　：0422-37-8926
FAX　：0422-55-3373
受付時間　：10:00～17:00　(土日祝祭日、および弊社の定める休日を除きます)
・ホームページ　http://www.centurysys.co.jp/

◆故障と思われる場合は
製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。
事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

◆ご連絡をいただく前に
スムーズなユーザーサポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。

・ファームウェアのバージョンとＭＡＣアドレス
(バージョンの確認方法は第 34 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。
・XR-440 の設定内容、およびコンピュータの IP 設定
・**「設定のバックアップファイル」を電子メール等でお送りください。**

◆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。

FutureNet XR シリーズ 製品サポートページ
http://www.centurysys.co.jp/support/
※ インデックスページから本装置の製品名をクリックしてください。

◆製品の保証について
本製品の保証期間は、お買い上げ日より 1 年間です。保証期間をすぎたもの、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-440/C　ユーザーズガイド　1.7.8対応版

2009年01月版

発行 センチュリー・システムズ株式会社