BROADBAND GATE

インターネットVPN対応ブロードバンドルータ

FutureNet XR-410/TX series

ユーザーズガイド

Ver1.6.10対応版

CENTURY SYSTEMS

目次

はじめに 5
ご使用にあたって 6
パッケージの内容物の確認 8
第 1 章 XR-410 の概要 9
Ⅰ. XR-410/TX シリーズの特長 10
Ⅱ. 各部の名称と機能 12
Ⅲ. 動作環境 14
第 2 章 XR-410 の設置 15
XR-410 の設置 16
第 3 章 コンピュータのネットワーク設定 17
Ⅰ. Windows XP のネットワーク設定 18
Ⅱ. Windows Vista のネットワーク設定 19
Ⅲ. Macintosh のネットワーク設定 20
Ⅳ. IP アドレスの確認と再取得 21
第 4 章 設定画面へのログイン 22
設定画面へのログイン方法 23
第 5 章 インターフェース設定 24
Ⅰ. Ethernet ポートの設定 25
Ⅱ. Ethernet ポートの設定について 27
Ⅲ. Ethernet ブリッジの設定 28
Ⅳ. 通常接続(CATV など)での接続設定例 29
Ⅴ. ローカルルータ設定 30
第 6 章 PPPoE 設定 31
Ⅰ. PPPoE の接続先設定 32
Ⅱ. PPPoE の接続設定と回線の接続 / 切断 34
Ⅲ. その他の接続設定 35
Ⅳ. 副回線とバックアップ回線 36
Ⅴ. PPPoE 特殊オプション設定について 40
第 7 章 ダイヤルアップ接続 41
Ⅰ. XR-410 とアナログモデム /TA の接続 42
Ⅱ. ダイヤルアップの接続先設定 43
Ⅲ. ダイヤルアップの接続と切断 45
Ⅳ. 副回線接続とバックアップ回線接続 46
第 8 章 複数アカウント同時接続設定 47
複数アカウント同時接続の設定 48
第 9 章 各種サービスの設定 53
各種サービス設定 54
第 10 章 DNS リレー / キャッシュ機能 55
DNS 機能の設定 56
第 11 章 DHCP サーバ / リレー機能 57
Ⅰ. XR-410 の DHCP 関連機能について 58
Ⅱ. DHCP サーバ機能の設定 59
Ⅲ. IP アドレス固定割り当て設定 61
第 12 章 IPsec 機能 62
Ⅰ. XR-410 の IPsec 機能について 63
Ⅱ. IPsec 設定の流れ 64
Ⅲ. IPsec 設定 65
Ⅳ. IPsec Keep-Alive 機能 73

Ⅴ.「X.509 デジタル証明書」を用いた電子認証 77
Ⅵ. IPsec 通信時のパケットフィルタ設定 79
Ⅶ. IPsec がつながらないとき 80
第 13 章 UPnP 機能 83
Ⅰ. UPnP 機能の設定 84
Ⅱ. UPnP とパケットフィルタ設定 86
第 14 章 ダイナミックルーティング(RIP と OSPF の設定) 87
Ⅰ. ダイナミックルーティング機能 88
Ⅱ. RIP の設定 89
Ⅲ. OSPF の設定 91
第 15 章 SYSLOG 機能 98
syslog 機能の設定 99
第 16 章 帯域制御(QoS)機能 102
Ⅰ. QoS 機能の概要 103
Ⅱ. QoS 機能の設定 104
第 17 章 攻撃検出機能 105
攻撃検出機能の設定 106
第 18 章 SNMP エージェント機能 107
SNMP エージェント機能の設定 108
第 19 章 NTP サービス 110
NTP サービスの設定方法 111
第 20 章 VRRP 機能 113
Ⅰ. VRRP の設定方法 114
Ⅱ. VRRP の設定例 115
第 21 章 アクセスサーバ機能 116
Ⅰ. アクセスサーバ機能について 117
Ⅱ. XR-410 とアナログモデム /TA の接続 118
Ⅲ. アクセスサーバ機能の設定 119
第 22 章 スタティックルーティング 120
スタティックルーティング設定 121
第 23 章 ソースルーティング 123
ソースルーティング設定 124
第 24 章 NAT 機能 126
Ⅰ. XR-410 の NAT 機能について 127
Ⅱ. バーチャルサーバ設定 128
Ⅲ. 送信元 NAT 設定 129
Ⅳ. バーチャルサーバの設定例 130
Ⅴ. 送信元 NAT の設定例 133
補足：ポート番号について 134
第 25 章 パケットフィルタリング機能 135
Ⅰ. 機能の概要 136
Ⅱ. XR-410 のフィルタリング機能について 137
Ⅲ. パケットフィルタリングの設定 138
Ⅳ. パケットフィルタリングの設定例 140
Ⅴ. 外部から設定画面にアクセスさせる設定 146
補足：NAT とフィルタの処理順序について 147
補足：ポート番号について 148
補足：フィルタのログ出力内容について 149

第 26 章 ネットワークイベント機能 150
Ⅰ. 機能の概要 151
Ⅱ. 各トリガーテーブルの設定 153
Ⅲ. 実行イベントテーブルの設定 157
Ⅳ. 実行イベントのオプション設定 159
Ⅴ. ステータスの表示 161
第 27 章 仮想インターフェース機能 162
仮想インターフェースの設定 163
第 28 章 GRE 機能 164
GRE の設定 165
第 29 章 パケット分類設定 167
Ⅰ. XR-410 のパケット分類設定について 168
Ⅱ. パケット分類設定の設定 169
Ⅲ. ステータスの表示 171
Ⅳ. ステータス情報の表示例 172
Ⅴ. TOS について 173
Ⅵ. DSCP について 175
第 30 章 ゲートウェイ認証機能 176
Ⅰ. ゲートウェイ認証機能の設定 177
Ⅱ. ゲートウェイ認証下のアクセス方法 183
Ⅲ. ゲートウェイ認証の制御方法について 184
第 31 章 ネットワークテスト 185
ネットワークテスト 186
第 32 章 各種システム設定 190
各種システム設定 191
◆時計の設定 191
◆ログの表示 192
◆ログの削除 192
◆パスワードの設定 193
◆ファームウェアのアップデート 194
◆設定の保存と復帰 195
◆設定のリセット 196
◆本体再起動 196
◆セッションライフタイムの設定 197
◆設定画面の設定 198
◆ARP filter 設定 198
第 33 章 情報表示 199
本体情報の表示 200
第 34 章 詳細情報表示 201
各種情報の表示 202
第 35 章 運用管理設定 203
Ⅰ. 一時的に工場出荷設定に戻す方法 204
Ⅱ. 携帯電話による制御 205
Ⅲ. 携帯電話による操作方法 206
付録 A インタフェース名一覧 207
付録 B 工場出荷設定一覧 209
付録 C サポートについて 211

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-410 梱包物＞

XR-410/TX2、XR-410/TX2DES、またはXR-410/TX4　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
RJ-45/D-sub9ピン変換アダプタ（ストレート）	１個
ACアダプタ	１個
電源ケーブル固定部品	１個
接続用ケーブル類の固定方法	１部
海外使用禁止シート	１部
保証書	１部

第1章

XR-410の概要

Ⅰ．XR-410/TX シリーズの特長

XR-410/TX2、XR-410/TX2DES、XR-410/TX4 からなる、
XR-410/TX シリーズ(以下 XR-410 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
Ethernet インターフェースは全て 10BASE-T/100BASE-TX となっており、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と機能を備えています。

◆シリアルポートを搭載
XR-410 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-410 を遠隔管理することも可能です。

◆ PPPoE クライアント機能
XR-410 は 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。
さらに XR-410 では複数のグローバルアドレスを NAT で設定できます。

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

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

第１章 XR-410の概要

Ⅰ．XR-410/TXシリーズの特長

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

◆ IPsec通信
IPsecを使うと、通信相手の認証と通信の暗号化により簡単に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。最大対地数は64です。
また、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。

◆ 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。

◆ルーティング機能
スタティックルート設定とRIPはもちろん、OSPFを用いたダイナミックルーティングが可能です。

◆障害時のバックアップ回線接続機能
VRRPによる機器冗長機能だけでなく、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。

◆ QoS機能
IPアドレスとポートによる、帯域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帯域を割り当てることが可能になります。

◆ゲートウェイ認証機能
XR-410をインターネットゲートウェイとして運用するときに、インターネットへアクセスするための認証をおこなう機能を搭載しています。パスワード認証によって外部への不正なアクセスを制限することができます。

◆ログ機能
XR-410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。

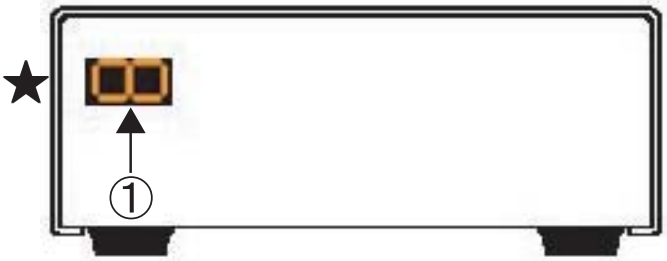
◆バックアップ機能
本体の設定内容を一括してファイルにバックアップすることが可能です。
また設定の復元も、ブラウザ上から簡単にできます。

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

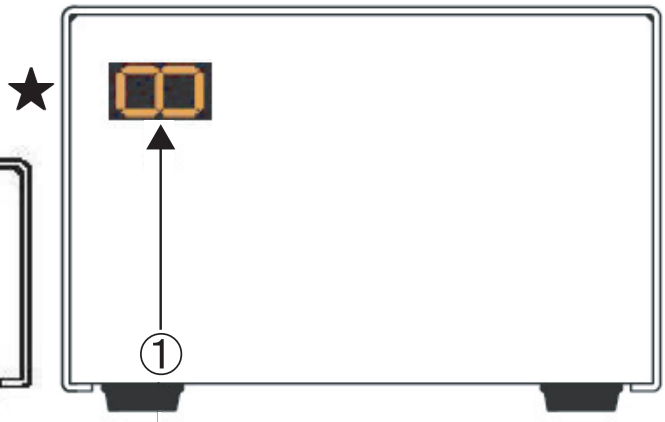
II．各部の名称と機能

◆製品前面

＜XR-410/TX2＞
＜XR-410/TX2DES＞



＜XR-410/TX4＞



① 7セグメント LED
本装置の状態を以下のように表示します。

起動中の LED
＜XR-410/TXseries 共通＞
★印を上に見て、「2 → 3 → 4 → 5 → 6 → 7」の順に表示されます。

各インタフェースのリンク状態の LED
各表示の状態については、下記をご覧ください。

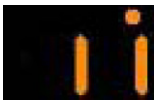
＜XR-410/TX2＞＜XR-410/TX2DES＞


システムが動作している状態。右上にある「・」が点滅します。


Ether0 ポートが Linkup している状態。


Ether1 ポートが Linkup している状態。


RS-232 ポートが Linkup している状態。


ケーブルを接続して 動作している状態の表示例。

＜XR-410/TX4＞
上記の表示に加えて、下記の状態を表示します。


Ether2 ポートが Linkup している状態。


Ether3 ポートが Linkup している状態。


XR-410/TX4 の Ether ポートが全て Linkup している状態。

ファームウェアのアップデート中の LED
＜XR-410/TX2＞＜XR-410/TX2DES＞


インタフェースのリンク状態に関係なく表示されます。

その後の再起動時には、起動中を示す「2 → 3 → 4 → 5 → 6 → 7」が順に表示されます。

＜XR-410/TX4＞
Ether2ポートとEther3ポートのリンク状態により表示が異なります。


Ether2 ポートと Ether3 ポートが共に Linkdown している状態でのアップデート実行時。


Ether2ポートのみLinkupしている状態でのアップデート実行時。


Ether3ポートのみLinkupしている状態でのアップデート実行時。


Ether2 ポートと Ether3 ポートが共に Linkup している状態でのアップデート実行時。

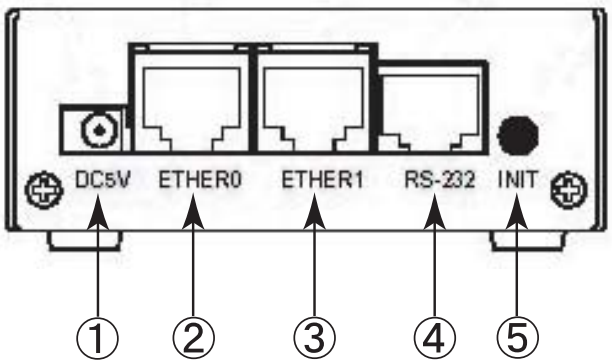
その後の再起動時には、起動中を示す「2 → 3 → 4 → 5 → 6 → 7」が順に表示されます。

「2」「6」「8」等の数字を表示したまま止まっているときは、システム故障により本装置が正常にが起動できない状態となっています。
弊社にてシステムの復旧が必要となりますので、この状態になったときは弊社までご連絡ください。

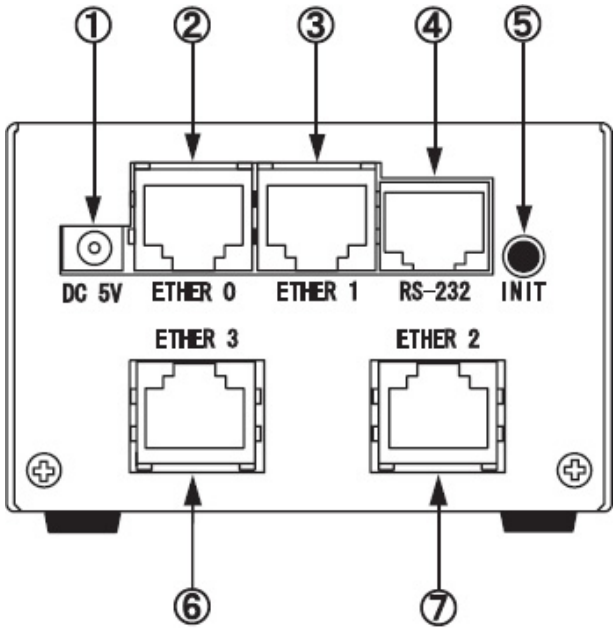
II．各部の名称と機能

◆製品背面

＜XR-410/TX2＞
＜XR-410/TX2DES＞



＜XR-410/TX4＞



① 電源コネクタ
製品付属の AC アダプタを接続します。

② Ether0 ポート
主に LAN との接続に使用します。
イーサネット規格のUTP 100BASE-TXケーブルを接続します。
ポートは Auto-MDIX 対応です。

③ Ether1 ポート
WAN 側ポートとして、また Ether0 ポート、XR-410/TX4 では Ether2 ポート、Ether3 ポートとは別セグメントを接続するポートとして使います。
イーサネット規格のUTP 100BASE-TXケーブルを接続します。
ポートは Auto-MDIX 対応です。

④ RS-232 ポート
リモートアクセスやアクセスサーバー機能を使用するときにモデムを接続します。
ストレートタイプの LAN ケーブルと製品添付の変換アダプタを用いてモデムと接続してください。

⑤ INIT スイッチ
本装置を工場出荷時の設定に戻して起動するときに押します。
操作方法については「第 35 章 運用管理設定」をご覧ください。

⑥ Ether3 ポート（※ XR-410/TX4 のみ）
主に LAN 側ポートとして、また、Ether0、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 100BASE-TXケーブルを接続します。
ポートは Auto-MDIX に対応していません。

⑦ Ether2 ポート（※ XR-410/TX4 のみ）
主に LAN 側ポートとして、また、Ether0、Ether1、Ether3ポートとは別セグメントを接続するポートとして使います。
イーサネット規格のUTP 100BASE-TXケーブルを接続します。
ポートは Auto-MDIX に対応していません。

III. 動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

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

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

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

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

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

◆ソフトウェア環境

・TCP/IP を利用できる OS がインストールされていること。

・接続されている全てのコンピュータの中で少なくとも 1 台に、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-410の設置

XR-410 の設置

XR-410 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 本装置の背面にある Ether0 ポートと HUB や PC を、LAN ケーブルで接続してください。
本装置のEthernet0,1ポートはAuto-MDIX対応です。

XR-410/TX4の場合は、本装置の背面にあるEther2,3ポートと HUB や PC を、LAN ケーブルで接続してください。
XR-410/TX4 の Ethernet2,3 ポートは Auto-MDIX には対応していません。

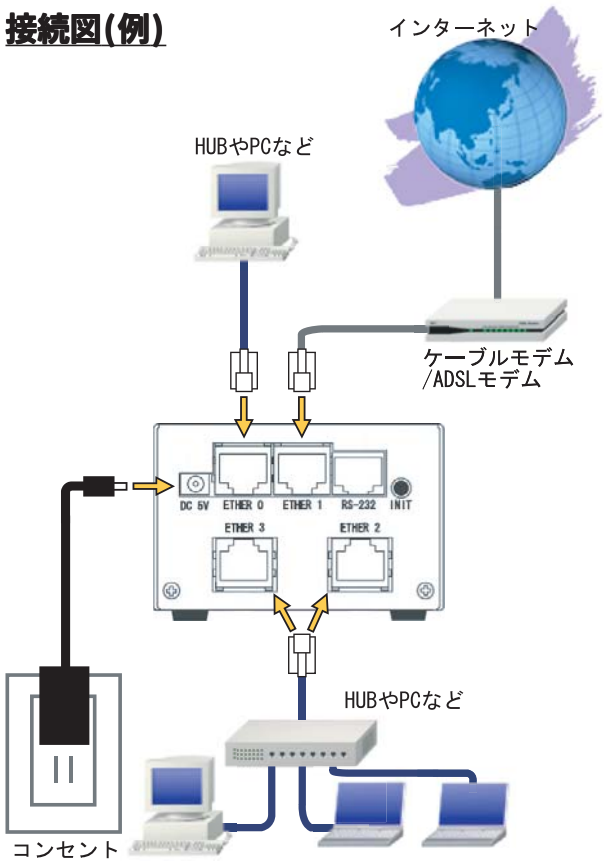
4 本装置と AC アダプタ、AC アダプタとコンセントを接続してください。

5 全ての接続が完了しましたら、各機器の電源を投入してください。

注意！

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

接続図(例)



（XR-410/TX4 の接続例です）

注意！

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

注意！

XR-410 側でも各ポートで ARP table を管理しているため、PC を接続しているポートを変更するとその PC から通信ができなくなる場合があります。
このような場合は、XR-410 側の ARP table が更新されるまで(数秒～数十秒)通信できなくなりますが、故障ではありません。

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

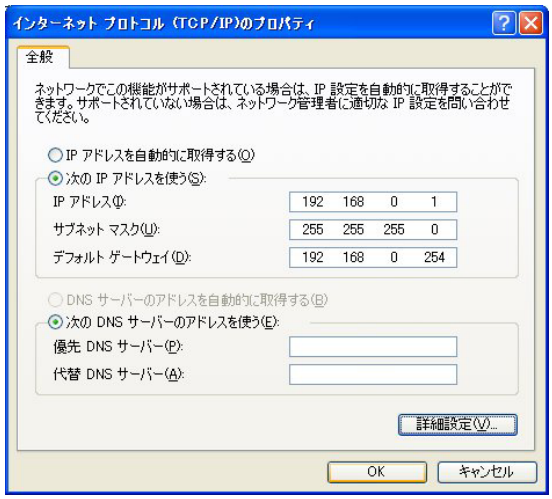
ここではWindows XPが搭載されたコンピュータのネットワーク設定について説明します。

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」



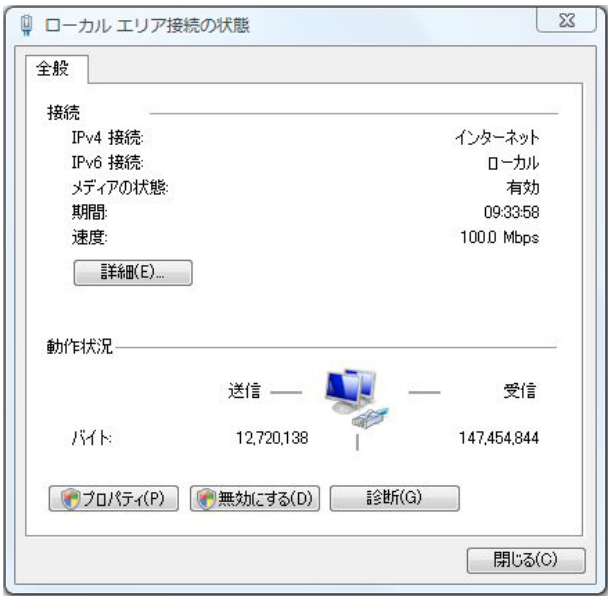
5 最後にOKボタンをクリックして設定完了です。これでXR-410へのログインの準備が整いました。

Ⅱ．Windows Vistaのネットワーク設定

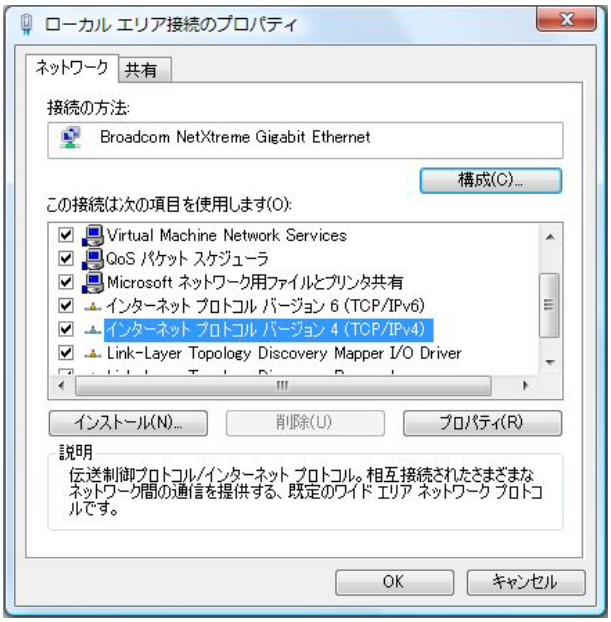
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

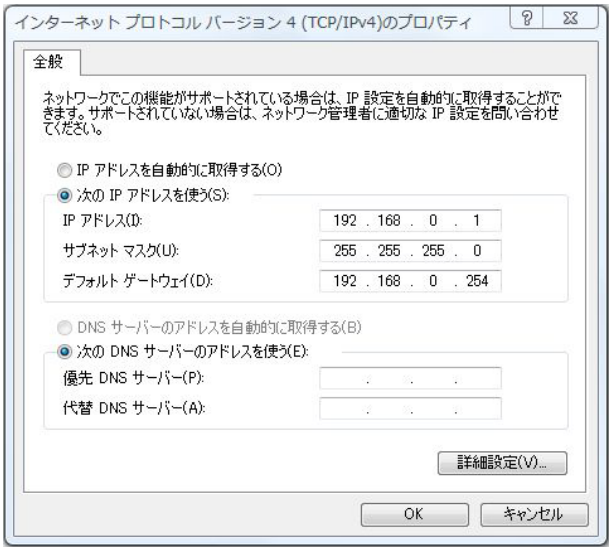


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



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

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



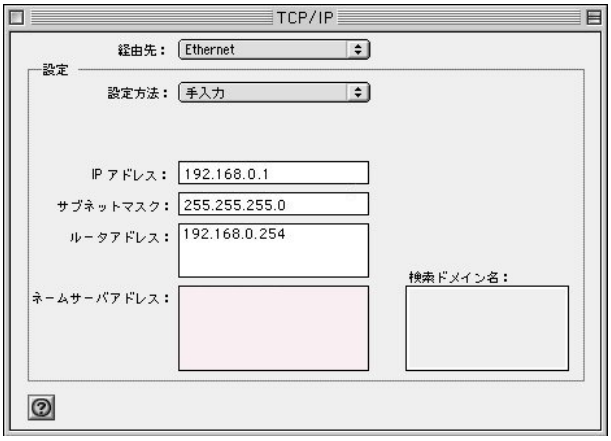
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

III. Macintoshのネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

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

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

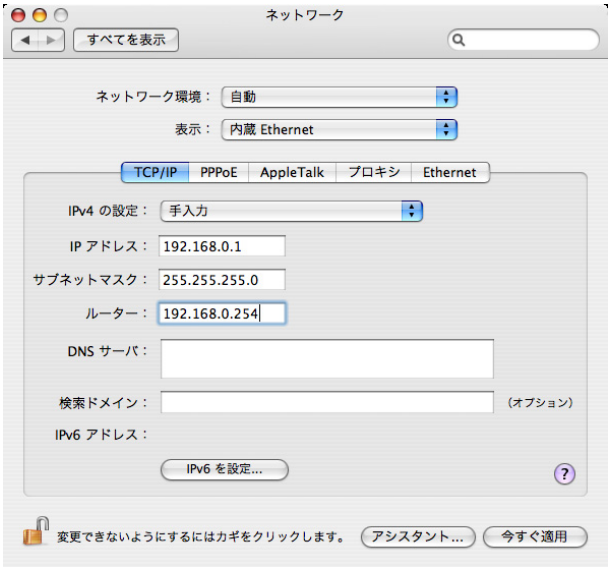


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これで本装置へログインする準備が整いました。

ここでは、Mac OS Xのネットワーク設定について説明します。

1 「システム環境設定」から「ネットワーク」を開きます。

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



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

Ⅳ．IPアドレスの確認と再取得

◆Windows XP/Vistaの場合

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

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

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

3 IP設定のクリアと再取得をするには以下のコマンドを入力してください。

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

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

◆Macintoshの場合

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

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

第4章

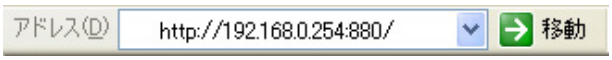
設定画面へのログイン

設定画面へのログイン方法

1 各種ブラウザを開きます。

2 ブラウザから設定画面にアクセスします。

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

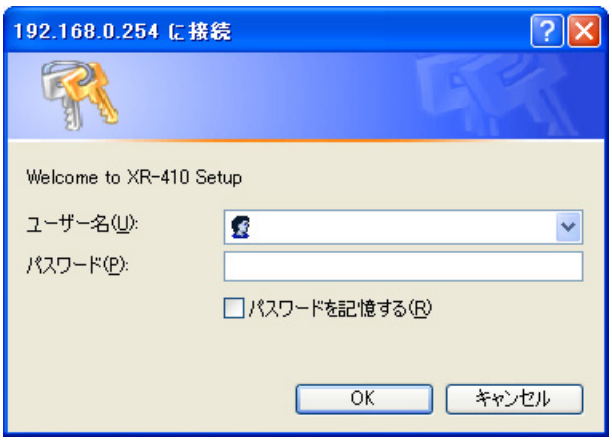


「192.168.0.254」は、Ether0 ポートの工場出荷時の IP アドレスです。
アドレスを変更した場合は、変更後の IP アドレスを指定してください。
設定画面のポート番号 880 は変更することができません。

本装置の工場出荷時の設定では、Ether0ポート以外のインタフェースは、**ステートフルパケットインスペクションが有効**になっています。
そのため **Ether0 ポート以外のインタフェースからは設定画面にアクセスできません。**

Ether0ポート以外のインターフェースから設定できるようにするには、それぞれのインタフェースのステートフルパケットインスペクションを無効にするか、パケットフィルタリング設定をおこなってください。

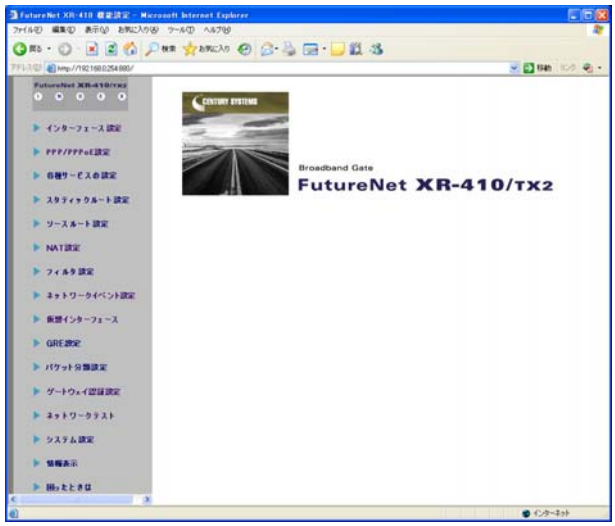
3 次のような認証ダイアログが表示されます。



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、変更後のユーザー名・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。



（画面は XR-410/TX2）

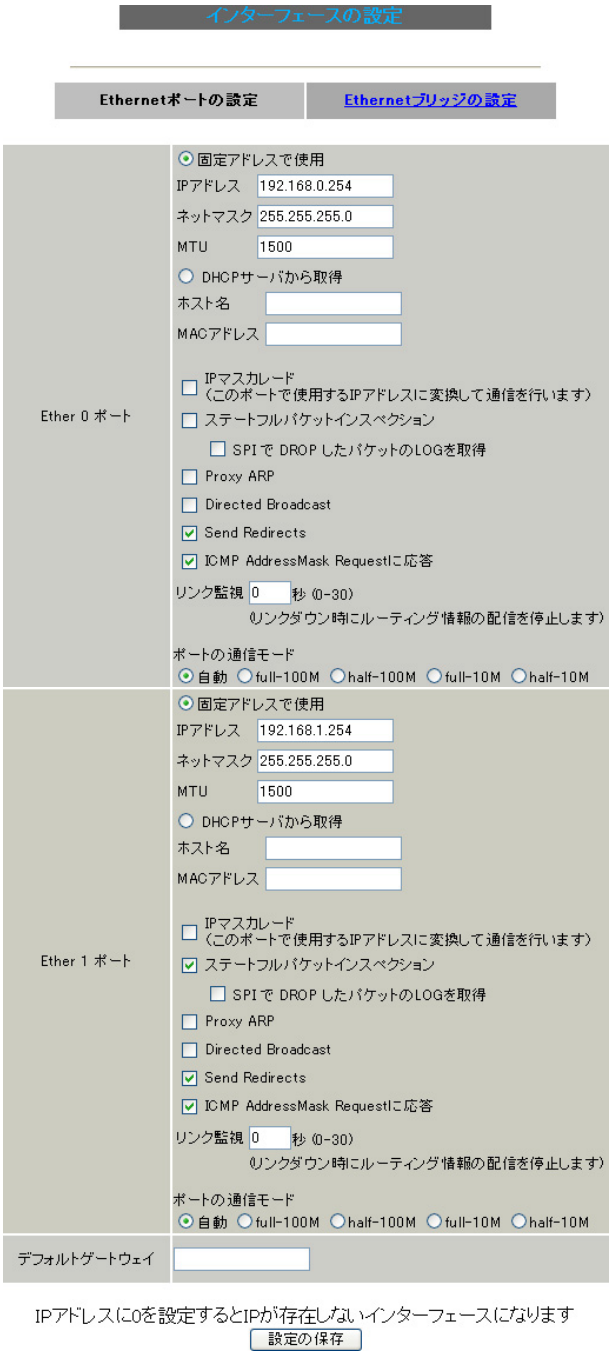
第5章

インターフェース設定

第５章 インターフェース設定

Ⅰ．Ethernet ポートの設定

本装置の各Ethernetポートの設定をおこないます。
Web 設定画面「インターフェース設定」→
「Ethernet ポートの設定」をクリックして以下の画面で設定します。



(画面は XR-410/TX2)

各インターフェースについて、それぞれ必要な情報を入力します。

[固定アドレスで使用]

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

○ MTU
「Path-MTU-Black-HOLE」現象が発生した場合等は、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。

＜MAC アドレスの入力例＞
00:11:22:33:44:55（コロンで区切ります）

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

○ステートフルパケットインスペクション
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。
本設定は、Ether0 以外の Ethernet ポートで、「有効」設定となっています。

○ 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 25 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。

Ⅰ．Ethernet ポートの設定

○ Proxy ARP
ProxyARP を使う場合はチェックします。

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

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

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

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

○ 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、そのインターフェースにて受信した ICMP AddressMask Request(type=17)に対して、Reply(type=18)を返送し、インターフェースのサブネットマスク値を通知します。
チェックをしない場合は、Request に対して応答しません。

○リンク監視
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の使用時にリンクのダウンを検知した場合、そのインタフェースに関連付けられたルーティング情報の配信を停止します。
再度リンク状態がアップした場合には、そのインタフェースに関連付けられたルーティング情報の配信を再開します。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。

○ポートの通信モード
各 Ether 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、通信速度・方式を固定できますので、必要に応じて選択します。
選択モードは「自動」、「full-100M」、「half-100M」、「full-10M」、「half-10M」です。

○デフォルトゲートウェイ
本装置のデフォルトルートとなる IP アドレスを入力してください。
（本項目は、「Ethernet ポートの設定」画面最下部にあります。）

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。
設定はすぐに反映されます。

本装置のインタフェースのアドレスを変更すると、設定は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 アドレス等も本装置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（SPI)]

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

ステートフルパケットインスペクション機能を有効にすると、そのインタフェースへのアクセスは一切不可能となります。
ステートフルパケットインスペクション機能とバーチャルサーバ機能を同時に使う場合等は、パケットフィルタリングの設定をおこなって、外部からアクセスできるように設定する必要があります
「第25章 パケットフィルタリング機能」を参照してください。

[PPPoE 接続時の Ethernet ポート設定]

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

XR-410 が PPPoE で接続する場合には “ ppp ” という論理インターフェースを自動的に生成し、この ppp 論理インターフェースを使ってPPPoE接続をおこなうためです。

物理的なEthernetポートとは独立して動作していますので、「DHCP サーバから取得」の設定やグローバル IP アドレスの設定はしません。
PPPoE に接続しているインタ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-410 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-410のEthernetポートに設定されていると、正常にIPsec通信がおこなえません。

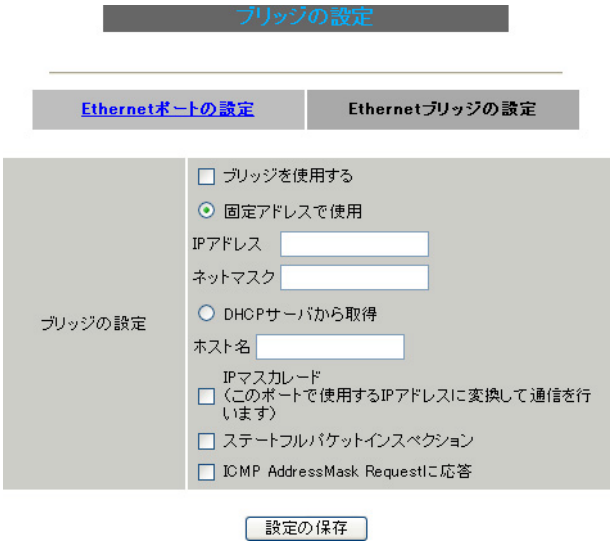
たとえば、IPsec通信をおこなう相手側のネットワークが192.168.1.0/24で、且つ、XR-410のEther1ポートに192.168.1.254が設定されていると、正常にIPsec通信がおこなえません。

このような場合はXR-410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．Ethernet ブリッジの設定

本装置をブリッジとして運用するための設定をおこないます。

Web 設定画面「インターフェース設定」→「Ethernet ブリッジの設定」をクリックして、以下の画面で設定します。



○ブリッジを使用する
チェックすると、本装置の Ethernet ポートはブリッジインタフェースとなります。

[固定アドレスで使用]
○ IP アドレス
○ネットマスク
ブリッジインタフェースの IP アドレスを固定アドレスで設定する場合はこちらをチェックして、IP アドレスとネットマスクを入力します。

[DHCP サーバから取得]
○ホスト名
ブリッジインターフェースの IP アドレスを DHCP から取得する場合はこちらをチェックして、必要であればホスト名を入力します。

○ IP マスカレード
チェックすると、ブリッジインターフェースから出ていくパケットについて 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
チェックを入れたポートから出ていくパケットについて、ステートフルパケットインスペクションが適用されます。

○ ICMP AddressMask Reply に応答
チェックを入れると、そのインターフェイスにて受信した 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「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．通常接続(CATVなど)での接続設定例

ここではNATを使ったCATVインターネット接続の設定について説明します。
CATVのほかにも、Yahoo!BBなどルータ型ADSLモデムを用いて接続する場合もこちらをご覧ください。

接続環境

・WAN側IPアドレスはDHCPで自動取得
・LAN側IPアドレスは工場出荷設定のまま
・Ether0ポートをLAN、Ether1ポートをWANに接続する

設定方法

「インターフェース設定」→「Ethernetポートの設定」画面を開きます。

◯ Ether0ポート
・「固定アドレスで使用」にチェック
・IPアドレス「192.168.0.254」
・サブネットマスク「255.255.255.0」
・「IPマスカレード」「ステートフルパケットインスペクション」にはチェックしません。

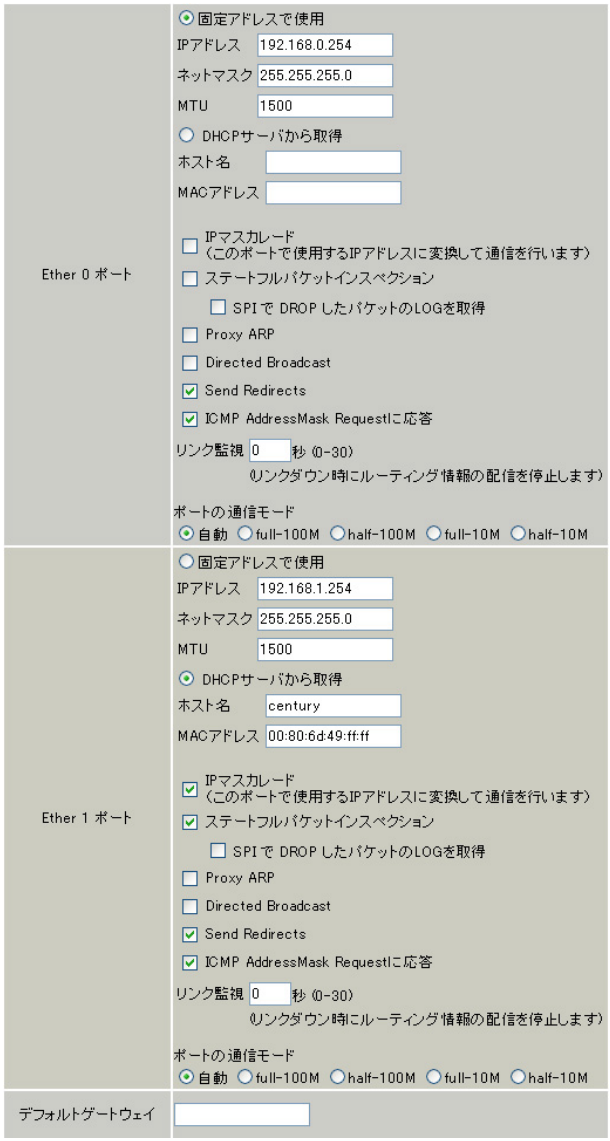
◯ Ether1ポート
・「DHCPから取得」にチェック
・必要であれば「ホスト名」を入力
・任意でMACアドレスを指定することもできます。
　＜入力例＞　00:80:6d:49:ff:ff
・「IPマスカレード」にチェック
・任意で「ステートフルパケットインスペクション」にチェックしてください。
　ステートフルパケットインスペクション機能を使わない場合は、詳細なパケットフィルタの設定をおこなってください。

その他項目については任意で設定してください。

◯デフォルトゲートウェイ
入力しません。

WAN側ポートを固定アドレスで接続する場合は、IPアドレス・ネットマスク・デフォルトゲートウェイについて入力します。
ルータタイプのADSLモデムに接続する場合などは、ルータモデムのIPアドレスがデフォルトゲートウェイとなります。

画面での入力例



Ether0ポートの設定を変更したときは、必ず各コンピュータのIPアドレス設定も変更してください。

また、各コンピュータをDHCPクライアントとして使用する場合は、DHCPサーバ機能の設定をおこなう必要があります。
DHCPサーバ機能については「第11章 DHCPサーバ/リレー機能」をご覧ください。

Ｖ．ローカルルータ設定

ここでは本装置をローカルルータとして使うための設定について説明します。

接続環境

・Ether0 側 IP アドレスは「192.168.0.254]
・Ether0 側サブネットマスクは「255.255.255.0」
・Ether1 側 IP アドレスは「192.168.1.254]
・Ether1 側サブネットマスクは「255.255.255.0」

設定方法

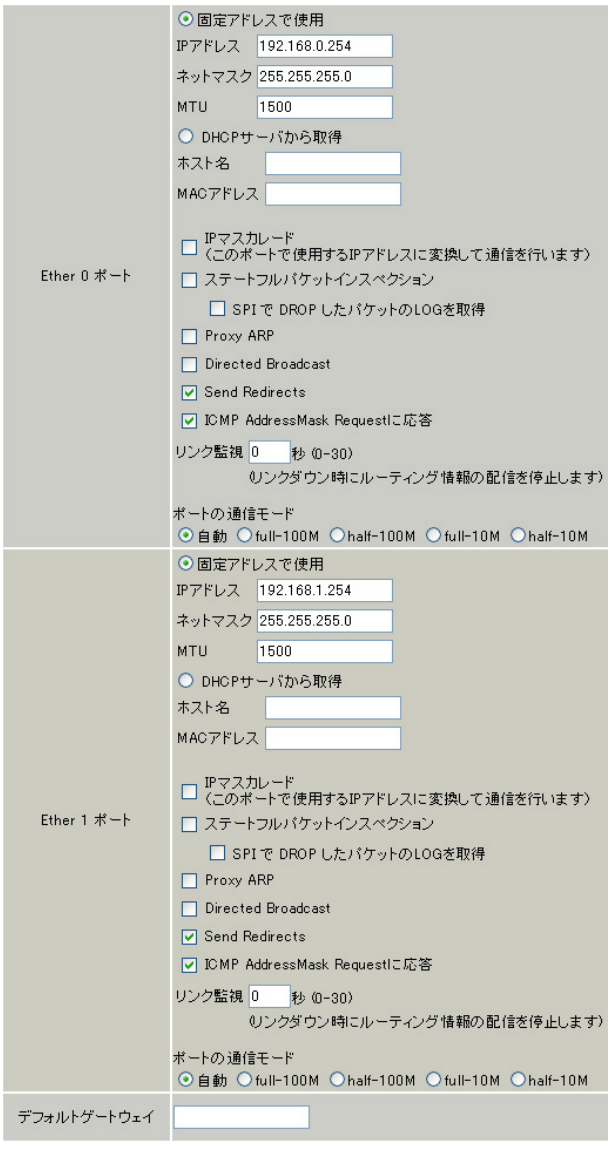
「インターフェース設定」→「Ethernet ポートの設定」画面を開きます。

○ Ether0 ポート
・「固定アドレスで使用」にチェック
・IP アドレス「192.168.0.254」
・サブネットマスク「255.255.255.0」
・「IP マスカレード」「ステートフルパケットインスペクション」にはチェックしません。
・「ポートの通信モード」は任意で選択してください。

○ Ether1 ポート
・「固定アドレスで使用」にチェック
・IP アドレス「192.168.1.254」
・サブネットマスク「255.255.255.0」
・「IP マスカレード」「ステートフルパケットインスペクション」にはチェックしません。
・「ポートの通信モード」は任意で選択してください。

○デフォルトゲートウェイ
必要に応じて指定してください。

画面での入力例



第 6 章

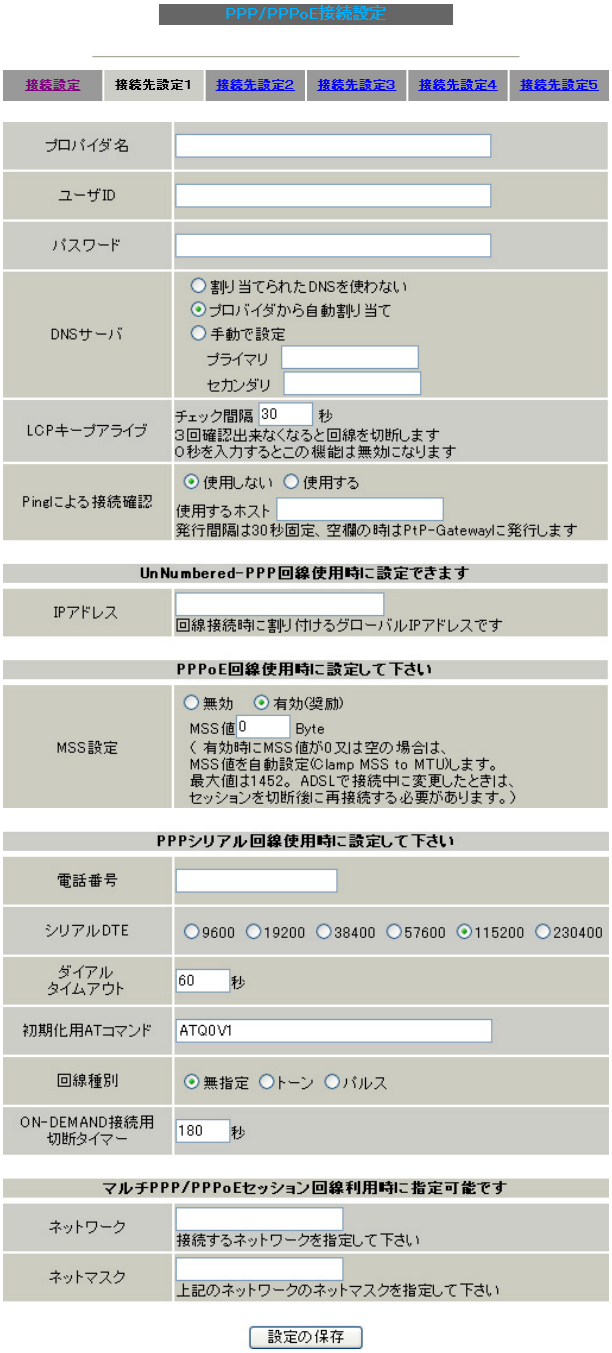
PPPoE 設定

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。



○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ー ID を入力してください。

○パスワード
プロバイダから指定された接続パスワードを入力してください。

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

＜例＞
abc(def)g’h → abc\(def\)g\’h

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

○ LCP キープアライブ
キープアライブのための LCP echo パケットを送出する間隔を指定します。設定した間隔で LCP echo パケットを 3 回送出して reply を検出しなかったときに、XR-410 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。

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

○ MSS 設定
「有効」を選択すると、XR-410 が MSS 値を自動的に調整します。「MSS 値」は任意に設定できます。最大値は 1452 バイトです。
「0」にすると最大 1414byte に自動調整します。
特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします。
(それ以外では正常にアクセスできなくなる場合があります。)

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

上記項目は、PPPoE 接続の場合、設定の必要はありません。

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

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

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

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

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

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。

「常時接続」XR-410 が起動すると自動的に PPPoE 接続を開始します。

○ RS232C 接続タイプ
PPPoE 接続では「通常」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 25 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。

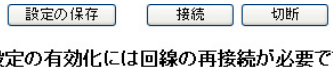
○デフォルトルートの設定
「有効」を選択すると、PPPoE 接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。「インターフェース設定」でデフォルトルートが設定されていても、PPPoE 接続で通知されるものに置き換えられます。

「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。

○ 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。

画面最下部の「設定の保存」ボタンをクリックして、設定完了です。



設定の有効化には回線の再接続が必要です

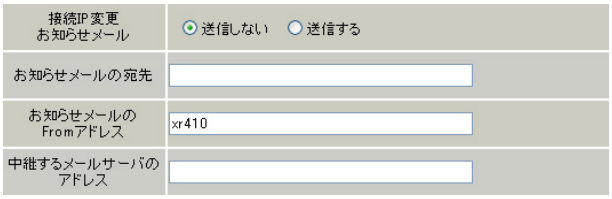
この後は「接続」「切断」ボタンで回線の接続を制御してください。
「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

III．その他の接続設定

接続 IP 変更お知らせメール機能

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

設定は「PPP/PPPoE 接続設定」→「接続設定」画面にある以下の箇所でおこないます。



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

○お知らせメールの宛先
お知らせメールを送るメールアドレスを入力します。

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

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

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

入力が終わりましたら画面最下部の「設定の保存」ボタンをクリックして、設定完了です。

Ⅳ．副回線とバックアップ回線

PPPoE 接続では、「副回線接続」設定と、「バックアップ回線接続」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。

[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 14 章 ダイナミックルーティング」をご覧ください。

Ⅳ．副回線とバックアップ回線

副回線設定

「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。

副回線使用時に設定して下さい	
副回線の使用	◉無効 ○有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1
RS232C 接続タイプ	◉通常 ○On-Demand 接続

○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 接続タイプ
RS-232C 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。

上記 4 項目以外の接続設定は、すべてそのまま引き継がれます。

入力が終わりましたら画面最下部の「設定の保存」ボタンをクリックして、設定完了です。

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。

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。

バックアップ回線使用時に設定して下さい	
バックアップ回線 の使用	○無効 ◉有効
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	◉RS232C ○Ether0 ○Ether1
RS232C 接続タイプ	◉通常 ○On-Demand 接続
IP マスカレード	◉無効 ○有効
ステートフルパケットインスペクション	◉無効 ○有効 □DROP したパケットの LOG を取得
ICMP AddressMask	○応答しない ◉応答する
主回線接続確認のインターバル	30 秒
主回線の回線断の確認方法	○PING ◉OSPF ○IPSEC+PING
Ping 使用時の宛先アドレス	
Ping 使用時の送信元アドレス	
Ping fail 時のリトライ回数	0
Ping 使用時の device	○主回線#1 ○マルチ#2 ○マルチ#3 ○マルチ#4 ◉その他
IPSEC+Ping 使用時の IPSEC ポリシーの NO	
復旧時のバックアップ回線の強制切断	◉する ○しない

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

○接続先の選択
バックアップ回線接続で利用する接続先設定を選択します。

○接続ポート
バックアップ回線で使用するインタフェースを選択します。

○ RS232C 接続タイプ
RS-232C 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。

Ⅳ．副回線とバックアップ回線

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

○ステートフルパケットインスペクション
PPPoE 接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。
SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。
SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 25 章 補足：フィルタのログ出力内容について」をご覧ください。

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

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

○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 を選択したときの、ping パケットの宛先 IP アドレスを設定します。
ここから ping の Reply が帰ってこなかった場合に、バックアップ回線接続に切り替わります。

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

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

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

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

入力が終わりましたら画面最下部の「設定の保存」ボタンをクリックして、設定完了です。

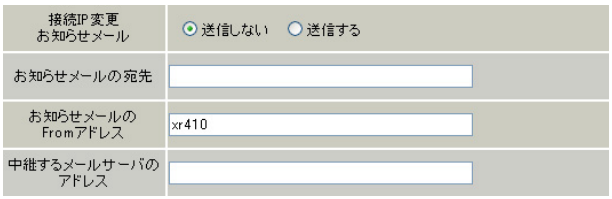
バックアップ回線接続機能は、「接続接定」で「常時接続」に設定してある場合のみ有効です。
また「接続設定」を変更した場合には、回線を一度切断して再接続した際に変更が反映されます。

Ⅳ．副回線とバックアップ回線

バックアップ回線への接続変更お知らせメール機能

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

設定は「PPP/PPPoE 接続設定」→「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**］にある以下の箇所でおこないます。



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

○お知らせメールの宛先
お知らせメールを送るメールアドレスを入力します。

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

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

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

入力が終わりましたら画面最下部の「設定の保存」ボタンをクリックして、設定完了です。

V．PPPoE 特殊オプション設定について

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

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

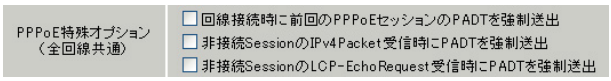
ここで PPPoE 特殊オプション機能を使うことにより、本装置が PPPoE セッションを確立していないことを検知し、強制的に PADT パケットを地域 IP 網側へ送信して、地域 IP 網側に PPPoE セッションの終了を通知します。

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

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

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。



①回線接続時に前回の PPPoE セッションの PADT を強制送出する。

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

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

①の動作について
XR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
XRがLCPキープアライブにより断を検知しても網側が断と判断していない状況下において、網側から

- IPv4 パケット
- LCP エコーリクエスト

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

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

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

第7章

ダイヤルアップ接続

Ⅰ．XR-410 とアナログモデム /TA の接続

XR-410 は、RS-232C ポートを搭載しています。
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-410 の PPP 接続機能を使うことでリモートアクセスが可能となります。

またXR-410 の副回線接続機能で、PPP 接続を副回線として設定しておくと、リモートアクセスを障害時のバックアップ回線として使うこともできます。

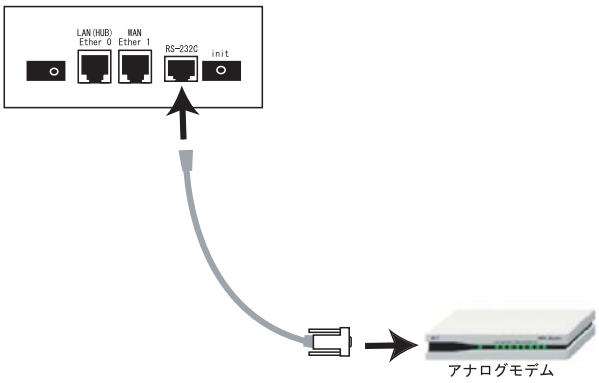
◆アナログモデム /TA の接続

1 XR-410 本体背面の「RS-232C」ポートと製品付属の変換アダプタとを、ストレートタイプの LAN ケーブルで接続してください。

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

3 全ての接続が完了しましたら、モデムの電源を投入してください。

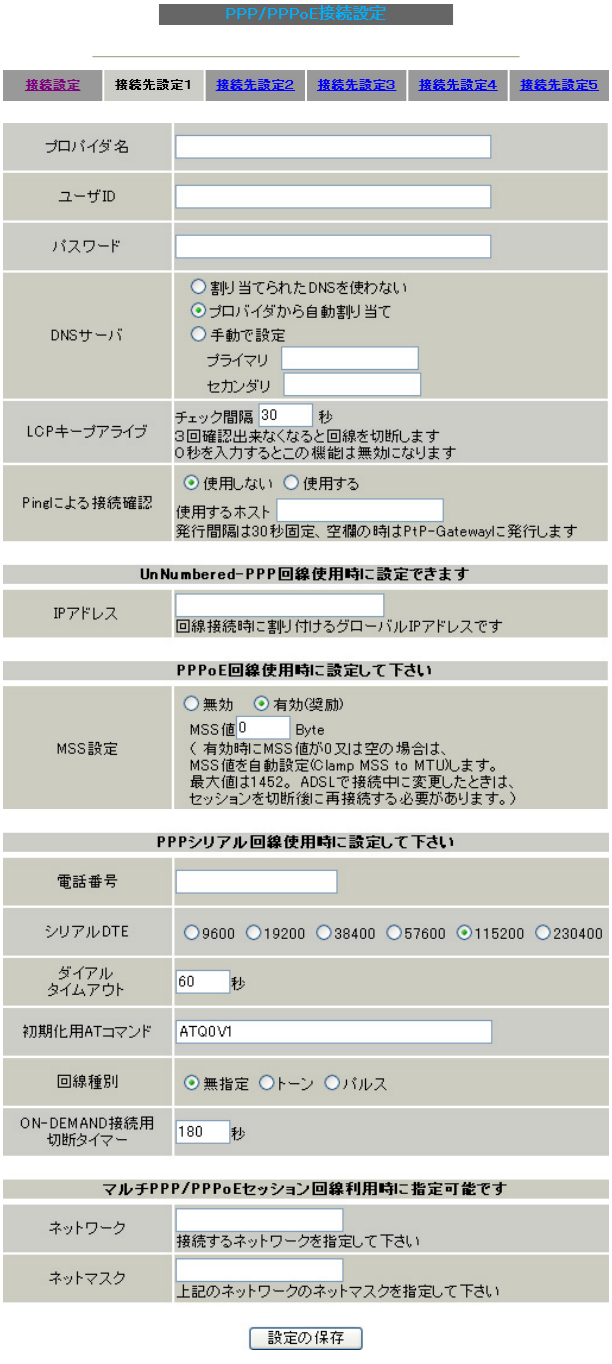
接続図



Ⅱ．ダイヤルアップの接続先設定

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。

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、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ー IDを入力してください。

○パスワード
プロバイダから指定された接続パスワードを入力してください。

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

＜例＞　abc(def)g’h → abc\(def\)g\’h

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

○LCP キープアライブ
○ping による接続確認
○IP アドレス
○MSS 設定

上記項目は、リモートアクセス接続の場合は設定の必要はありません。

Ⅱ．ダイヤルアップの接続先設定

○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。

○シリアル DTE
XR-410 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。

○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。

○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 RS-232C 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、RS-232C 接続を切断します。

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

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

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

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

続いて PPP の接続設定をおこないます。

Ⅲ．ダイヤルアップの接続と切断

接続先設定に続いて、ダイヤルアップ接続のために接続設定をおこないます。
Web 設定画面「PPP/PPPoE 接続設定」を開き「接続設定」をクリックして、以下の画面から設定します。

接続設定

PPP/PPPoE接続設定

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

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

○回線状態
現在の回線状態を表示します。

○接続先の選択
どの接続先設定を使って接続するかを選択します。

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

○接続形態
「手動接続」ダイヤルアップの接続 / 切断を手動で切り替えます。
「常時接続」XR-410 が起動すると自動的にダイヤルアップ接続を開始します。

○ RS232C 接続タイプ
「通常接続」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 接続時以外は、「有効」を選択してください。

○ステートフルパケットインスペクション
PPPoE 接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。
SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。
SPI が有効のときだけ動作可能です。
ログの出力内容については、「第 25 章 補足：フィルタのログ出力内容について」をご覧ください。

○デフォルトルートの設定
「有効」を選択すると、ダイヤルアップ接続時に IP アドレスとともに ISP から通知されるデフォルトルートを自動的に設定します。
「インターフェース設定」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。

画面最下部の「設定の保存」ボタンをクリックして、設定完了です。

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

Ⅳ．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、以下の設定が可能です。

- 副回線接続設定
- バックアップ回線接続設定

設定方法については、「第 6 章　PPPoE 設定」の「Ⅳ . 副回線とバックアップ回線」をご参照ください。

第8章

複数アカウント同時接続設定

複数アカウント同時接続の設定

XR-410/TX シリーズは、同時に複数の PPPoE 接続をおこなうことができます。
以下のような運用が可能です。

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

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

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。
XR-410 のマルチ PPPoE セッション機能は、主回線 1 セッションと、マルチ接続 3 セッションの合計 4 セッションまでの同時接続をサポートしています。なお、以下の項目については主回線では設定できますが、マルチ接続（#2 ～ #4）では設定できませんので、ご注意ください。

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

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

ただし、マルチリンクには対応していませんので、帯域を広げる目的で利用することはできません。
また XR-410 のマルチ PPPoE セッション機能は、PPPoE で接続しているすべてのインターフェースがルーティングの対象となります。したがいまして、それぞれのインターフェースにステートフルパケットインスペクション、またはフィルタリング設定をしてください。

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

この機能を利用する場合は以下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。

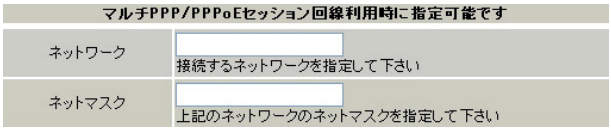
Web 設定画面「PPP/PPPoE 設定」をクリックし、「接続先設定」のいずれかをクリックして設定します。
詳しい設定方法は、「第 6 章」をご覧ください。

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。
設定方法については、「第 6 章」をご参照ください。

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



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

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

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

最後に「設定の保存」をクリックして接続先設定は完了です。

複数アカウント同時接続の設定

STEP 3 PPPoE 接続の設定

複数同時接続のための接続設定をおこないます。
主接続とマルチ接続それぞれについて接続設定をおこないます。
「PPP/PPPoE 設定」→「接続設定」を開きます。

[主接続用の接続設定]
以下の部分で設定します。

PPP/PPPoE接続設定

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

回線状態	回線は接続されていません
接続先の選択	◉接続先1 ○接続先2 ○接続先3 ○接続先4 ○接続先5
接続ポート	○RS232C ○Ether0 ◉Ether1
接続形態	◉手動接続 ○常時接続
RS232C接続タイプ	◉通常 ○On-Demand接続
IPマスカレード	○無効 ◉有効
ステートフルパケットインスペクション	○無効 ◉有効 □DROPしたパケットのLOGを取得
デフォルトルートの設定	○無効 ◉有効
ICMP AddressMask Request	○応答しない ◉応答する
接続IP変更お知らせメール	◉送信しない ○送信する
お知らせメールの宛先	
お知らせメールのFromアドレス	xr410
中継するメールサーバのアドレス	

○回線状態
現在の回線状態を表示します。

○接続先の選択
主接続用の設定を選択します。

○接続先ポート
主接続で使用する、XR-410 のインタフェースを選択します。

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

○ RS232C 接続タイプ
主接続がPPPoE接続の場合は、「通常」を選択します。
主接続がRS-232C接続の場合は、「通常」を選択すると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。

○デフォルトルート
「有効」を選択します。

○ ICMP AddressMask Request
任意で選択します。

○接続 IP 変更お知らせメール
任意で設定します。

続いてマルチ接続用の接続設定をおこないます。

複数アカウント同時接続の設定

[マルチ接続用の設定]
以下の部分で設定します。

マルチPPP/PPPoEセッション機能を利用する際は以下を設定して下さい

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

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

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

○マルチ接続 #2 ～ #4
マルチ PPPoE セッション用の回線として使うものに「有効」を選択します。

○接続先の選択
マルチ接続用の接続先設定を選択します。

○接続ポート
マルチ接続で使用する、XR-410 のインタフェースを選択します。B フレッツ回線で複数の同時接続をおこなう場合は、主接続の設定と同じインタフェースを選択します。

○ RS232C 接続タイプ
マルチ接続が PPPoE 接続の場合は、「通常」を選択します。
マルチ接続が RS-232C 接続の場合は、「通常」を選択すると主回線の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。

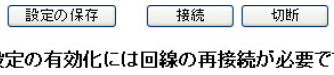
○ ICMP AddressMask Request
任意で選択します。

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。

第9章

各種サービスの設定

各種サービス設定

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

ここでは

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

をおこないます。

サービスの設定

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

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

サービスの起動と停止

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

第 10 章

DNS リレー / キャッシュ機能

DNS 機能の設定

◆DNS リレー機能

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

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

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

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

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

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

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

ただし、「フィルタ設定」で以下の設定を実行している場合には注意が必要です。

DNSのポート番号を指定してフィルタしている場合

<「出力フィルタ」設定例>

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

↓

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

<「出力フィルタ」設定例>

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	eth1	パケット送信時	許可	udp		10000:199		53
2	eth1	パケット送信時	破棄	udp				

または、

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

UDP のポート番号 10000-65535 をフィルタしている場合

<「出力フィルタ」設定例>

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

↓

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

<「出力フィルタ」設定例>

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

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

◆DNS キャッシュ機能

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

第 11 章

DHCP サーバ / リレー機能

第 11 章 DHCP サーバ / リレー機能

Ⅰ．XR-410 の DHCP 関連機能について

本装置は、以下の 4 つの DHCP 関連機能を搭載しています。

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

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

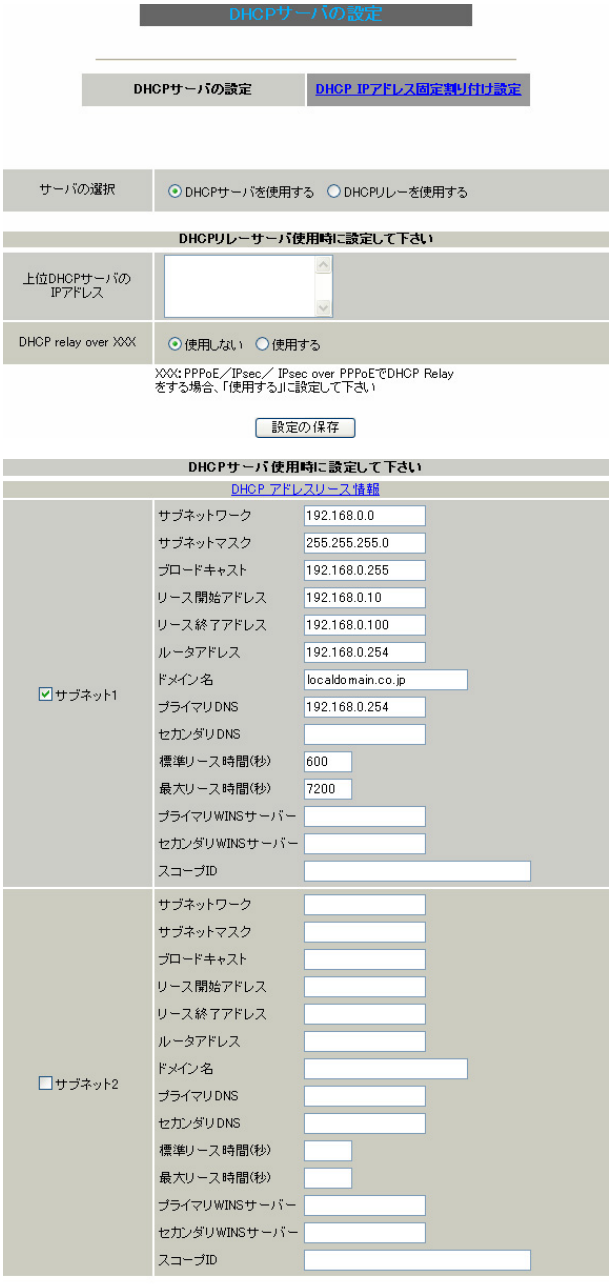
◆ IP アドレスの固定割り当て
DHCP サーバ機能では通常、使用されていない IP アドレスを順に割り当てる仕組みになっていますので、DHCP クライアントの IP アドレスは変動することがあります。
しかし、固定割り当ての設定をすることで、DHCP クライアントのMACアドレス毎に常に同じIPアドレスを割り当てることができます。

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

NAT機能を利用している場合、DHCP リレー機能は利用はできません。

II．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。



（画面は XR-410/TX2 です）

DHCP サーバ / リレーの機能設定

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用するかを選択します。
サーバ機能とリレー機能を同時に使うことはできません。

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

○上位 DHCP サーバの IP アドレス
上位の DHCP サーバの IP アドレスを指定します。
複数のサーバを登録するときは、IP アドレスごとに改行して設定します。

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

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

○サブネット 1
○サブネット 2
○サブネット 3 （※ XR-410/TX4 のみ）
○サブネット 4 （※ XR-410/TX4 のみ）
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-430 のインターフェースに設定された IP アドレスを参照の上、同じサブネットとなる設定を使います。**
- **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次の通りです。

II．DHCP サーバ機能の設定

○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。

○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-410のインタフェースのIPアドレスを指定します。

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

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

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

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

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

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

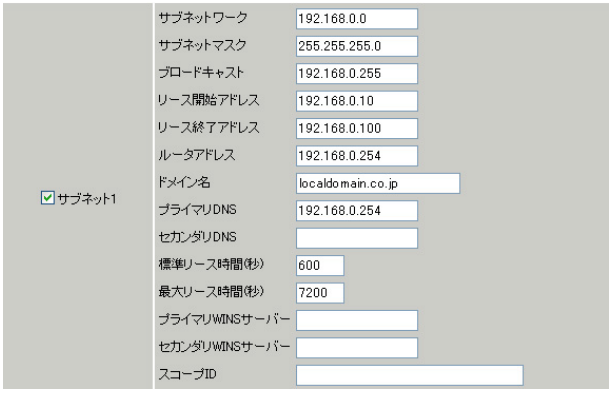
入力が終わりましたら「設定の保存」をクリックして設定完了です。

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、サービスの再起動をおこなってください。

DHCP サーバ機能の初期設定

本装置では「DHCP サーバを使用する」が初期設定で、以下の内容で初期設定されています。

- LAN は 192.168.0.0/24 のネットワーク
- 192.168.0.10 から 100 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 10 分間
- 最大リース時間は 2 時間

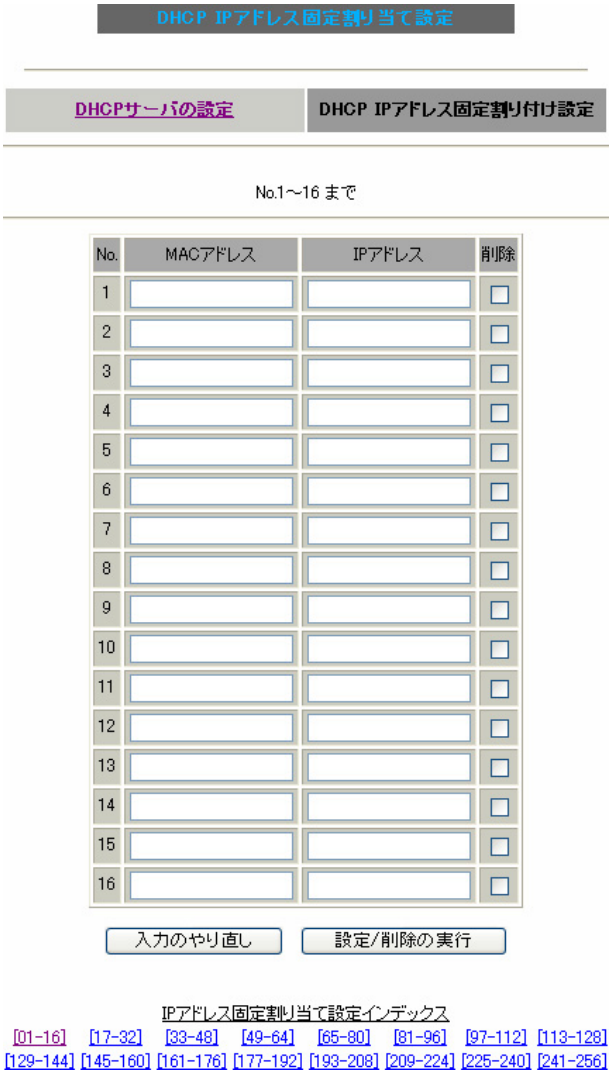


III. IP アドレス固定割り当て設定

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。



○ 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。

最大設定数は 256 です。
設定画面の最下部にある「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してください。

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。
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

一覧の「削除」項目にチェックして「設定 / 削除の実行」をクリックすると、そのエントリが削除されます。

第 12 章

IPsec 機能

Ⅰ．XR-410 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-410/TX シリーズでは「共通鍵方式」「RSA 公開鍵方式」「X.509」による認証に対応しています。ただしアグレッシブモードは「共通鍵方式」にのみ対応、「X.509」はメインモードにのみ対応しています。

◆暗号化アルゴリズム
シングル DES とトリプル DES、AES128bit をサポートしています。暗号化処理は XR-410/TX2・XR-410/TX4 ではソフトウェア、XR-410/TX2DES 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-410 は ESP の認証機能を利用していますので、AH での認証はおこなっていません。

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

◆ IPsec 使用時の通信可能対地数
本装置は最大 128 拠点と IPsec 接続が可能です。

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

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

他の機器との接続実績について

以下のルータとの接続を確認しています。

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

II．IPsec 設定の流れ

◆PreShared(共通鍵)方式での IPsec 通信

STEP 1　共通鍵の決定

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

STEP 2　共通鍵の交換

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

STEP 3　本装置側の設定

自分側の XR-410 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」画面でのインターフェースとルーティングテーブル、ログで確認します。

◆RSA(公開鍵)方式での IPsec 通信

STEP 1　公開鍵・暗号鍵の生成

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

STEP 2　公開鍵の交換

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

STEP 3　本装置側の設定

自分側の XR-410 の設定をおこないます。

STEP 4　IKE/ISAKMP ポリシーの設定

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

STEP 5　IPsec ポリシー設定

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

STEP 6　IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7　IPsec 接続の確認

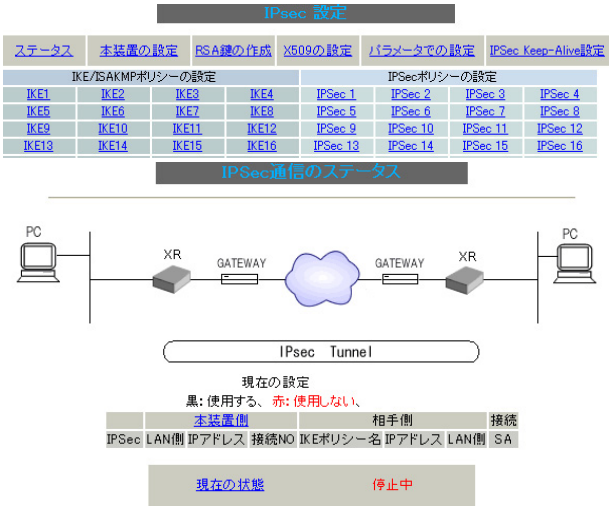
IPsec起動後に、正常にIPsec通信ができるかどうかを確認します。
「情報表示」画面でのインターフェースとルーティングテーブル、ログで確認します。

III. IPsec 設定

STEP 0 設定画面を開く

1 Web 設定画面にログインします。

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



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

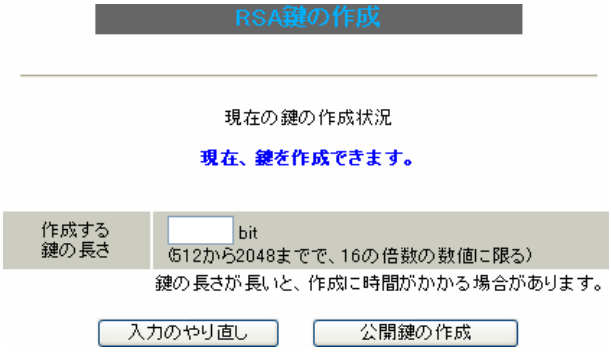
IPsec に関する設定・確認は、全てこの設定画面からおこなえます。

STEP 1,2 鍵の作成・交換

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

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

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



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

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

III. IPsec 設定

STEP 3 本装置側の設定をおこなう

IPsec 設定画面上部の「本装置の設定」をクリックして設定します。

[本装置の設定]
「本装置の設定」をクリックします。

[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 環境で 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。
下記のいずれの場合も「使用する」を選択してください。
- 本装置が NAT 内の IPsec クライアントの場合
- 本装置が NAT 外の IPsec サーバの場合

○ Virtual Private 設定～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。
以下のような書式で入力してください。

%v4:<ネットワーク>/<マスクビット値>

<設定例> %v4:192.168.0.0/24

本装置が NAT の外側の IPsec サーバとして動作する場合に設定します。
最大 4 箇所までの NAT 環境の接続先ネットワークを設定できます。
本装置が NAT 背後の IPsec クライアントとして動作する場合は空欄のままにします。

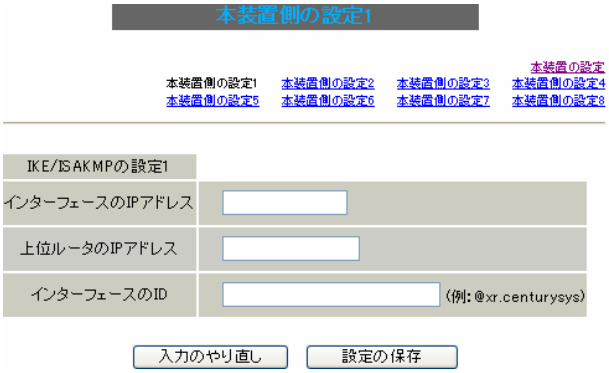
[鍵の表示]
○本装置の RSA 鍵
RSA 鍵の作成をおこなった場合ここに、作成した本装置の RSA 公開鍵が表示されます。
PSK 方式や X.509 電子証明を使う場合はなにも表示されません。

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-410 自身の IP アドレスやインタフェース ID を設定します。



[IKE/ISAKMP の設定 1～8]

○インターフェースの IP アドレス

- **固定アドレスの場合**
  本装置に設定されている IP アドレスをそのまま入力します。
- **動的アドレスの場合**
  PPP/PPPoE 主回線接続の場合は「%ppp0」と入力します。
  Ether0(Ether1)ポートで接続している場合は「%eth0(%eth1)」と入力します。

○上位ルータの IP アドレス
空欄にしておきます。

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

＜入力形式＞ **@＜任意の文字列＞**
＜入力例＞ @centurysystems

@の後は、任意の文字列でかまいません。

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

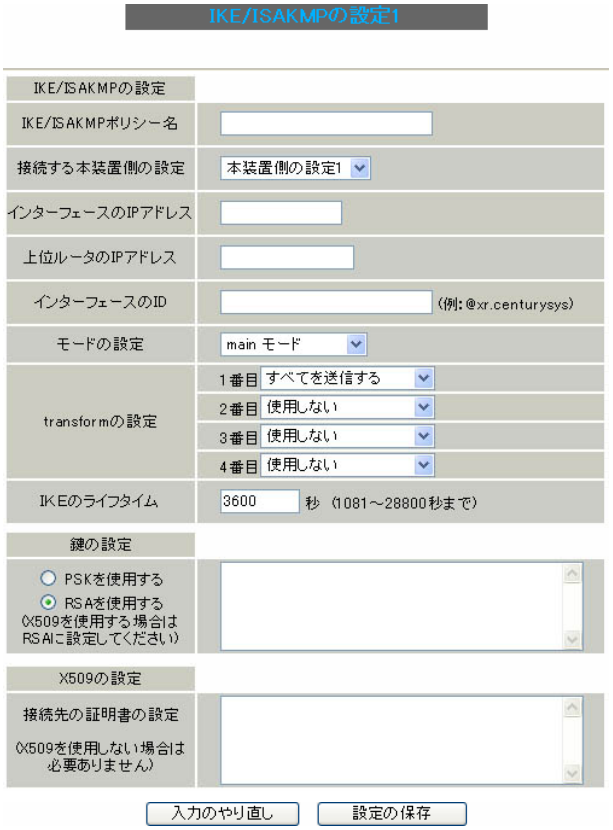
最後に「設定の保存」をクリックして設定完了です。

続いて **IKE/ISAKMP ポリシー**の設定をおこないます。

III. IPsec 設定

STEP 4 IKE/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。



[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。

○インタフェースの ID

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

また、NAT トラバーサルを使用し、対向側装置が NAT 内にある場合にも ID を設定します。

＜入力形式＞ **@＜任意の文字列＞**

＜入力例＞ @centurysystems

@ の後は、任意の文字列でかまいません。

対向側装置への割り当てが固定アドレスの場合は設定の必要はありません。

○モードの設定

IKE のフェーズ 1 モードを「main モード」と「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-410 は、以下のものの組み合わせが選択できます。

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

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

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

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

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

○ 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。
X.509を使用しない場合は設定の必要はありません。

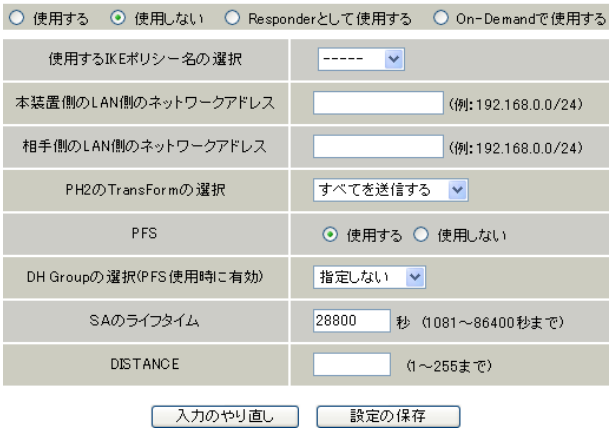
最後に「設定の保存」をクリックして設定完了です。

続いて、**IPsec ポリシーの設定**をおこないます。

III．IPsec 設定

STEP 5　IPsec ポリシーの設定

IPsec 設定画面上部の「IPsec ポリシーの設定」の「IPsec 1」～「IPsec 128」いずれかをクリックして、以下の画面から設定します。



○最初に IPsec の起動状態を選択します。

「使用する」
initiator にも responder にもなります。

「使用しない」
その IPsec ポリシーを使用しません。

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

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

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

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

○相手側の LAN 側のネットワークアドレス
対向の IPsec 装置が接続している LAN 側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。「本装置側の LAN 側のネットワークアドレス」と同様です。
ただし、NAT Traversal 機能を使用し、接続相手が NAT 内にある場合に限っては、“**vhost:%priv**”と設定します。

○ PH2 の TransForm の選択
IPsec SA の折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。

- すべてを送信する
- 暗号化アルゴリズム　(3des、des、aes128)
- 認証アルゴリズム　　(md5、sha1)

通常は「すべてを送信する」の選択で構いません。

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

III. IPsec 設定

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

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

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

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

最後に「設定の保存」をクリックして設定完了です。

続いて、**IPsec 機能の起動**をおこないます。

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

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが XR-410 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-410 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-410 の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

STEP 6 IPsec 機能を起動する

「各種サービスの設定」をクリックして、以下の画面を開きます。

○動作状態の制御
IPsec サーバ項目、「起動」にチェックして「動作変更」をクリックすると、IPsec 機能が起動します。以降は、XR-410 を起動するたびに IPsec 機能が自動起動します。
IPsec 機能を止める場合は「停止」にチェックして「動作変更」をクリックしてください。

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

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

III．IPsec 設定

STEP 7　IPsec 接続を確認する

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

ログの中で、以下のメッセージが含まれているかを確認してください。

（ログメッセージは「メインモード」で通信した場合の表示例です。）

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

および

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

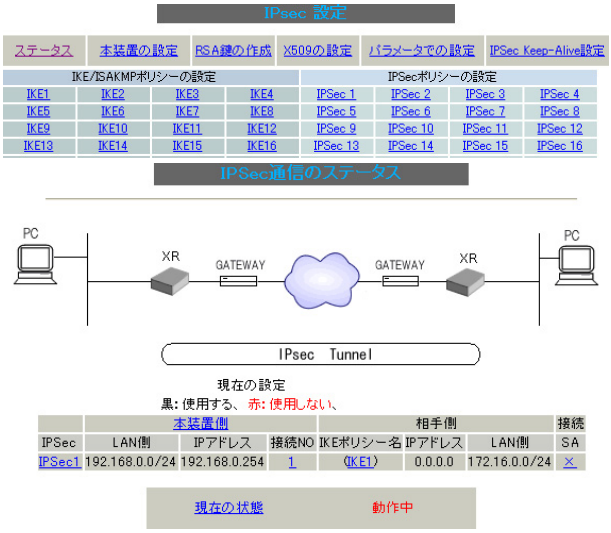
上記 2 つのメッセージが表示されていれば、IPsec が正常に接続されています。

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

(2)のメッセージ
IPsec SAが正常に確立したことを示しています。

STEP 8　IPsec ステータス確認の確認

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



（画面は表示例です）

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

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

また、それぞれの設定番号をクリックすると、設定画面に移ることができます。

Ⅳ. IPsec Keep-Alive 機能

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

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

[IPsec Keep-Alive 設定]
IPsec 設定画面上部の「IPsecKeep-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、本装置の LAN 側インタフェースの IP アドレスを入力します。

IV. IPsec Keep-Alive機能

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

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

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

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

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

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

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

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

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

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

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

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

IV. IPsec Keep-Alive 機能

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

○ interface
Keep-Alive 機能を使う、本装置の IPsec インタフェース名を入力します。
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。

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

<例>
使用する IKE ポリシー　IKE/ISAKMP1 番

IPsec ポリシー　IPsec2　IPsec4　IPsec5

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

○ remove?
設定を削除したいときにチェックします。

IV. IPsec Keep-Alive 機能

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

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

設定番号について

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

IPsec トンネルの障害を検知する条件

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

動的アドレスの場合の本機能の利用について

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

Ⅴ.「X.509 デジタル証明書」を用いた電子認証

本装置は X.509 デジタル証明書を用いた電子認証方式に対応しています。

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

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

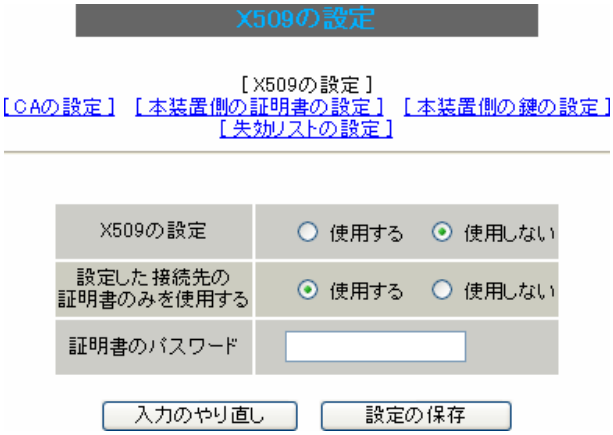
情報処理振興事業協会セキュリティセンター
http://www.ipa.go.jp/security/pki/

設定は、IPsec 設定画面内の「X.509 の設定」からおこなえます。

設定方法

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

[X.509 の設定]



○ X509 の設定
X.509 の使用 / 不使用を選択します。

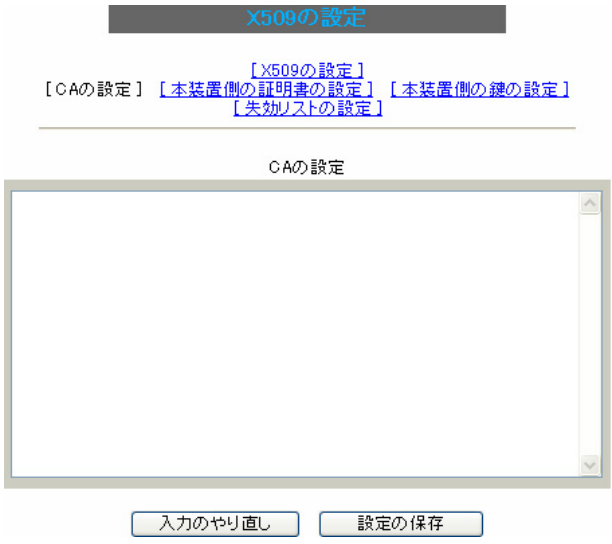
○設定した接続先の証明書のみを使用する
設定した接続先の証明書のみの使用 / 不使用を選択します。

○証明書のパスワード
証明書のパスワードを入力します。

入力後、「設定の保存」をクリックします。

[CA の設定]

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



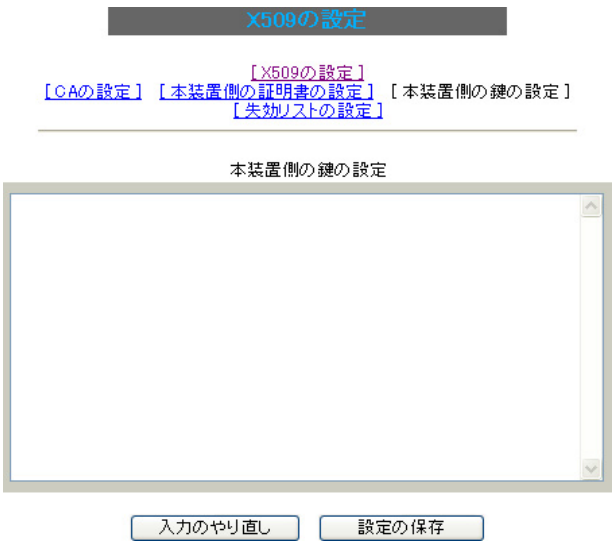
コピーを貼り付けましたら、「設定の保存」をクリックします。

V．「X.509 デジタル証明書」を用いた電子認証

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

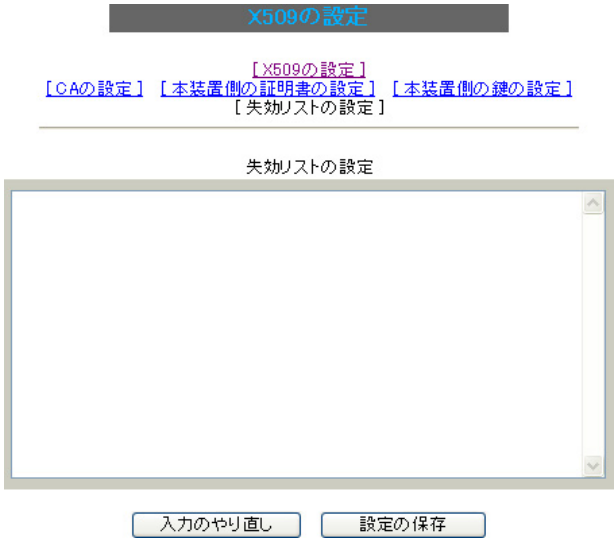
コピーを貼り付けましたら、「設定の保存」をクリックします。

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



コピーを貼り付けましたら、「設定の保存」をクリックします。

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



コピーを貼り付けましたら、「設定の保存」をクリックします。

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

- 「RSA を使用する」　チェック
- 設定欄　空欄

(「本装置の設定」画面の[鍵の表示]欄も空欄にしておきます。)

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

- 設定欄　相手側のデジタル証明書の貼付

以上で X.509 の設定は完了です。

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

VI．IPsec 通信時のパケットフィルタ設定

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

IPsec では、以下の 2 種類のプロトコル・ポートを使用します。

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

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

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

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

- **プロトコル「UDP」のポート「4500」番**
  → 一部の IKE トラヒックおよび、暗号化ペイロードのトラフィックに必要です

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

<設定例>

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

Ⅶ. IPsec 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
```

Ⅶ. 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; newest
ISAKMP
```

これらのログやメッセージ内に

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

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

Ⅶ. 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 XR-410 には IPsec のログが出ているのに、こちらの XR-410 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 XR-410 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 13 章

UPnP 機能

Ⅰ．UPnP 機能の設定

XR-410 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。

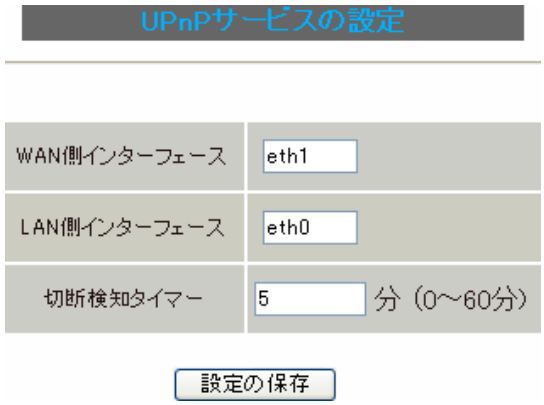
Windows OS の UPnP サービス

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-410 の UPnP 機能の設定は以下の手順でおこなってください。

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



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

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

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

○切断検知タイマー
UPnP 機能使用時の無通信切断タイマーを設定します。
ここで設定した時間だけ無通信時間が経過すると、XR-410 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、サービスの再起動をおこなってください。

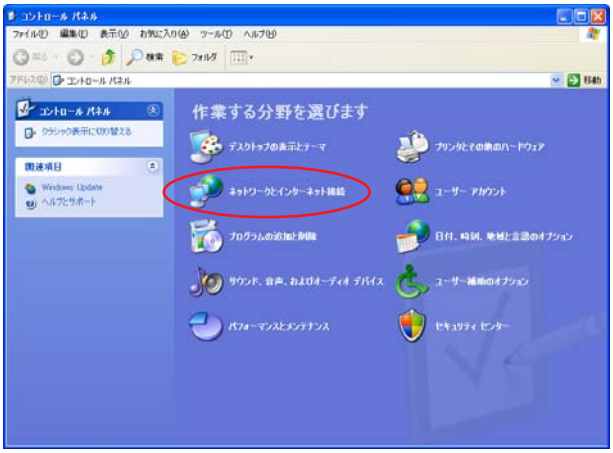
Ⅰ．UPnP 機能の設定

◆UPnP の接続状態の確認

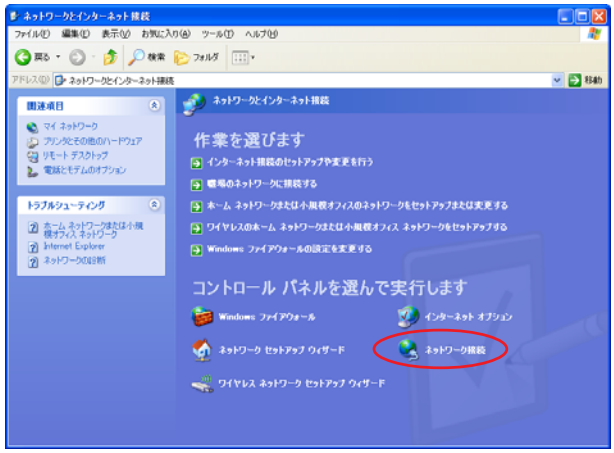
各コンピュータが本装置と正常に UPnP で接続されているかどうかを確認します。

1 「スタート」→「コントロール パネル」を開きます。

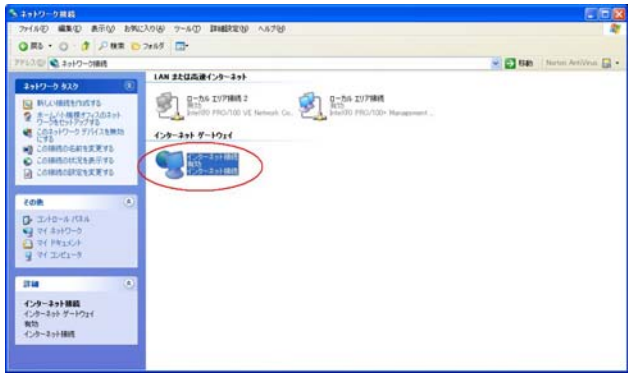
2 「ネットワークとインターネット接続」を開きます。



3 「ネットワーク接続」を開きます。



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



(画面は Windows XP での表示例です)

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

II．UPnP とパケットフィルタ設定

◆UPnP 機能使用時の注意

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

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

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

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

◆UPnP 機能使用時の推奨フィルタ設定

Microsoft Windows 上の UPnP サービスのバッファオーバフローを狙った DoS(サービス妨害)攻撃からの危険性を緩和する為の措置として、XR-410 は工場出荷設定で以下のようなフィルタをあらかじめ設定しています。

(入力フィルタ)

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

(転送フィルタ)

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

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

第 14 章

ダイナミックルーティング
(RIP と OSPF の設定)

第14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

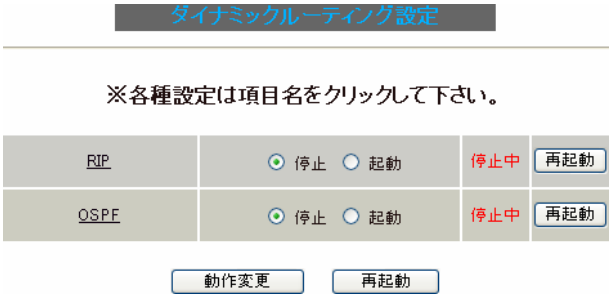
XR-410/TXシリーズのダイナミックルーティング機能は、下記のプロトコルをサポートしています。

- RIP
- OSPF

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」をクリックします。



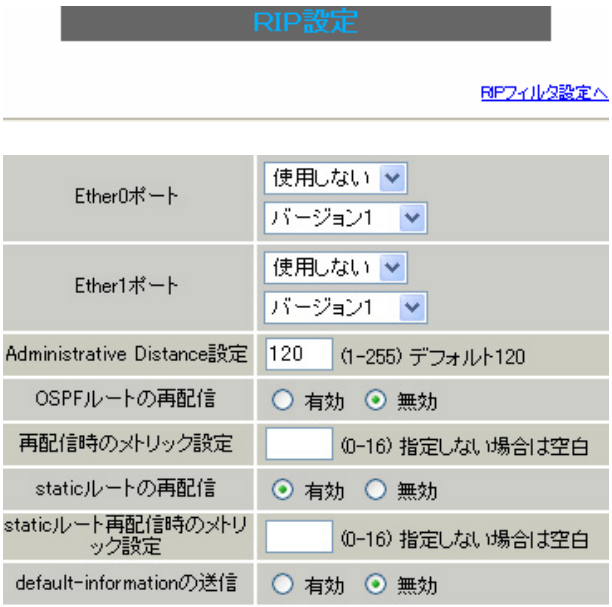
2　「RIP」、「OSPF」をクリックして、それぞれの機能の設定画面を開いて設定をおこないます。

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設定」→「RIP」をクリックして、以下の画面から設定します。

◆RIP 設定



（画面は XR-410/TX2）

○Ether0 ポート
○Ether1 ポート
○Ether2 ポート（※ XR-410/TX4 のみ）
○Ether3 ポート（※ XR-410/TX4 のみ）
本装置の各 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、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の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。

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したくないときに設定します。

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

○ NO.
設定番号を指定します。1～64 の間で指定します。

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

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

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

○ネットワーク
RIP フィルタリングの対象となるネットワークアドレスを指定します。

< 入力形式 >
　ネットワークアドレス / サブネットマスク値

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

RIP フィルタ設定後は、ただちに設定が有効となります。

設定後は、画面上部に設定内容が一覧表示されます。

(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。

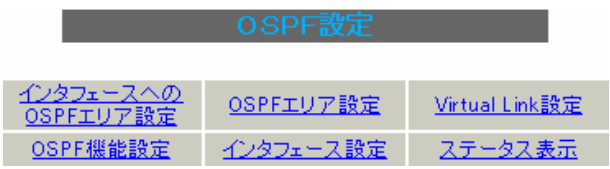
OSPF では各ルータがリンクステートを交換し合い、そのリンクステートをもとに、他のルータがどこに存在するか、どのように接続されているか、というデータベースを生成し、ネットワークトポロジを学習します。

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。

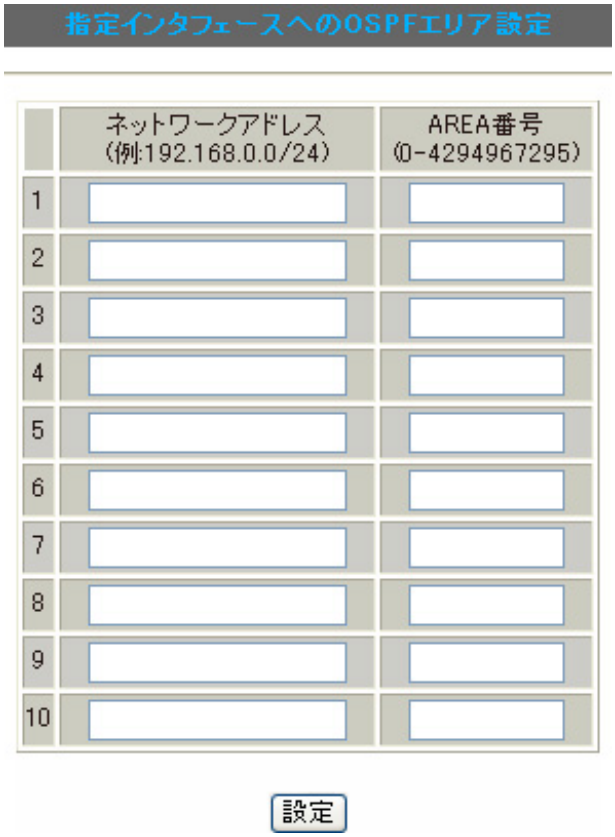


◆インタフェースへの OSPF エリア設定
◆OSPF エリア設定
◆Virtual Link 設定
◆OSPF 機能設定
◆インタフェース設定
◆ステータス表示

◆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
XR-410 に接続しているネットワークのネットワークアドレスを指定します。
ネットワークアドレス/マスクビット値の形式で入力します。

○ AREA 番号
そのネットワークのエリア番号を指定します。

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

入力後は「設定」をクリックして設定完了です。

III．OSPF の設定

◆OSPF エリア設定

各AREA(エリア)ごとの機能設定をおこないます。

設定画面上部の「OSPF エリア設定」をクリックします。

初めて設定するとき、もしくは設定を追加するときは「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指定しない場合、設定内容一覧では空欄で表示されますが、実際は 1 で機能します。

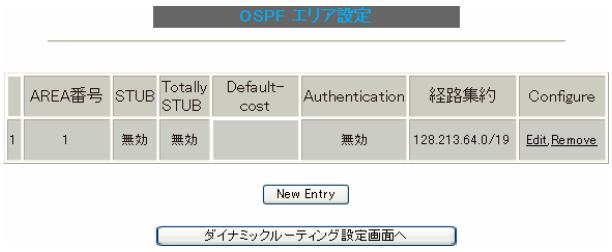
○認証設定
該当エリアでパスワード認証か MD5 認証をおこなうかどうかを選択します。
デフォルト設定は「使用しない」です。

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

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

入力後は「設定」をクリックしてください。

設定後は「OSPF エリア設定」画面に、設定内容が一覧で表示されます。



(画面は表示例です)

[Configure]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VirtualLinkを設定して、論理的にバックボーンエリアに接続させます。

設定画面上部の「VirtualLink設定」をクリックして設定します。

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

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

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

○Hello インターバル設定
Helloパケットの送出間隔を設定します。

○Dead インターバル設定
Deadタイムを設定します。

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

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

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

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

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

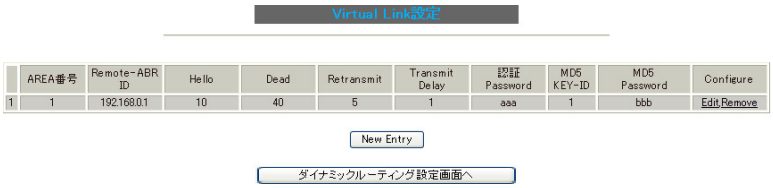
○MD5 KEY-ID 設定(2)
○MD5 パスワード設定(2)
MD5 KEY-IDとパスワードは2つ同時に設定可能です。その場合は(2)に設定します。

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

入力後は「設定」をクリックしてください。

III．OSPF の設定

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



(画面は表示例です)

[Configure]欄

○ Edit

クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○ Remove

クリックすると設定の「削除」をおこなえます。

◆OSPF 機能設定

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

○ Router-ID 設定

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

○ Connected 再配信

connected ルートを OSPF で配信するかどうかを選択します。
「有効」にした場合は以下の 2 項目も設定します。

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

b. メトリック値
配信する際のメトリック値を設定します。

III．OSPF の設定

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

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

b. メトリック値
配信する際のメトリック値を設定します。

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

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

b. メトリック値
配信する際のメトリック値を設定します。

○ 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。

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

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

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

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

b. メトリック値
配信する際のメトリック値を設定します。

○ 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。

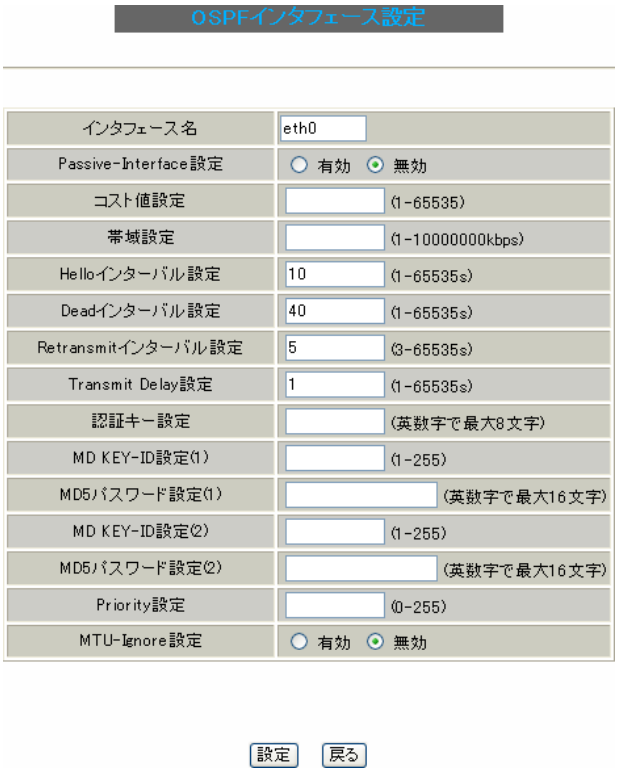
III．OSPF の設定

◆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、本マニュアルの「付録 A」をご参照ください。

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

○コスト値設定
コスト値を設定します。

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

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

○ Dead インターバル設定
Dead タイムを設定します。

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

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

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

○ 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。
半角英数字で最大 16 文字まで使用できます。

○ 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。

III．OSPF の設定

○ Priority 設定
DR、BDR の設定の際に使用する priority を設定します。priority 値が高いものが DR に、次に高いものが BDR に選ばれます。“ 0 ” を設定した場合は DR、BDR の選定には関係しなくなります。

DR、BDR の選定は、priority が同じであれば、IP アドレスの大きいものが DR、BDR になります。

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

入力後は「設定」をクリックしてください。

設定後は「インタフェース設定」画面に、設定内容が一覧で表示されます。

(画面は表示例です)

[Configure]欄

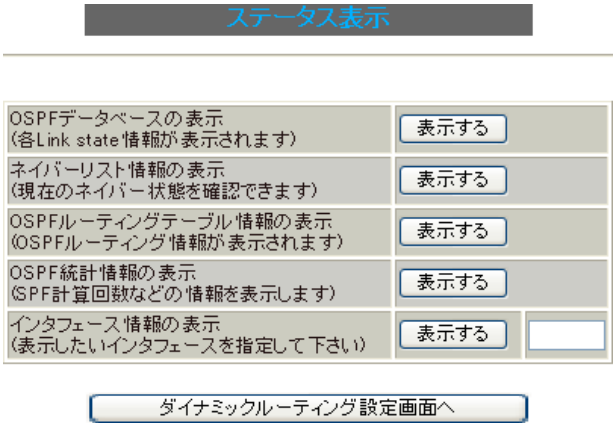
○ Edit
クリックすることで、それぞれ設定内容の「編集」をおこなえます。

○ Remove
クリックすると設定の「削除」をおこなえます。

◆ステータス表示

OSPF の各種ステータスを表示します。

設定画面上部の「ステータス表示」をクリックして設定します。



○ OSPF データベース表示
LinkState 情報が表示されます。

○ネイバーリスト情報の表示
現在のネイバー状態が表示されます。

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

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

○インタフェース情報の表示
現在のインタフェースの状態が表示されます。表示したいインタフェース名を指定してください。指定しない場合は全てのインタフェースについて表示されます。

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。

第 15 章

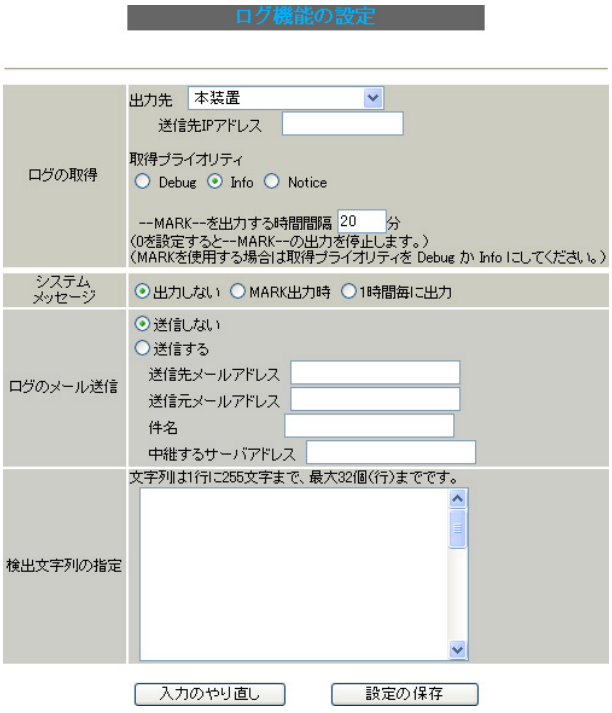
SYSLOG 機能

syslog 機能の設定

XR-410 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。

syslog 機能設定

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



<ログの取得>
○出力先
syslog の出力先を選択します。

「本装置」
本装置で syslog を取得する場合に選択します。

「SYSLOG サーバ」
syslog サーバに送信するときに選択します。

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

○送信先 IP アドレス
syslog サーバの IP アドレスを指定します。

○取得プライオリティ
ログ内容の出力レベルを指定します。プライオリティの内容は以下のようになります。

- Debug ：デバッグ時に有益な情報
- Info ：システムからの情報
- Notice：システムからの通知

○ --MARK-- を出力する時間間隔
syslog が動作していることを表す「-- MARK --」ログを送出する間隔を指定します。
初期設定は 20 分です。

装置本体に記録しておけるログの容量には制限があります。継続的にログを取得される場合は外部の syslog サーバにログを送出するようにしてください。

syslog 機能の設定

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

○出力しない
システムメッセージを出力しません。

○ MARK 出力時
“ -- MARK -- ”の出力と同時にシステムメッセージが出力されます。

○１時間ごとに出力
１時間ごとにシステムメッセージを出力します。

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

<ログのメール送信>
以下の設定は、ログの内容を電子メールで送信したい場合に設定してください。

○送信しない
○送信する
ログメール機能を使うときは「送信する」を選択してください。
ログのメールを「送信する」場合は、以下の項目を任意で指定できます。

○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。

○送信元メールアドレス
ログメッセージの送信元メールアドレスを任意で指定します。
何も指定しないときは「root@localdomain.co.jp」で送信されます。

○件名
半角英数字のみ使用できます。
何も指定しないときは“ 件名は無し ”で送信されます。

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

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

syslog 機能の設定

<検出文字列の指定>
ここで指定した文字列が含まれるログをメールで送信します。
検出文字列には、pppd、IP、DNS など、ログ表示に使用される文字列を指定してください。
なお、文字列の記述に正規表現は使用できません。
文字列を指定しない場合はログメールは送信されません。

文字列の指定は、1 行につき 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、「ログメール機能」のみ有効です。

最後に「設定の保存」をクリックして設定完了です。

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

ファシリティと監視レベルについて

XR-410/TX シリーズで設定されている syslog のファシリティ・監視レベルは以下のようになっています。

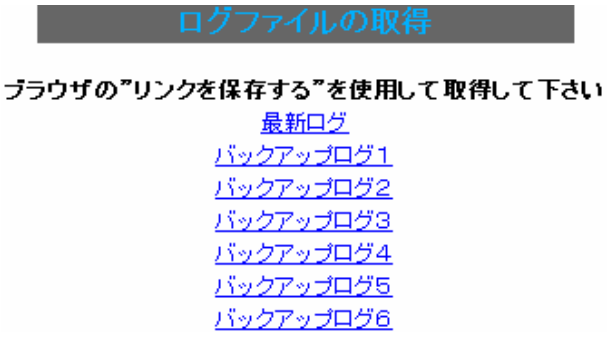
[ファシリティ：監視レベル]
***.info;mail.none;news.none;authpriv.none**

ログファイルの取得

出力されたログは、Web 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。
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。



（ログファイルのリンク表示例）

第 16 章

帯域制御(QoS)機能

第 16 章 帯域制御(QoS)機能

Ⅰ．QoS 機能の概要

QoS 機能について

QoS とは”Quality of Service”の略で、本来はアプリケーションのサービス品質を一定で維持することを意味しています。これが転じて、特定のアプリケーションに対してネットワークの帯域を割り当てる機能のことを QoS と呼びます。

一般的に、ネットワークにおける通信では FTP やストリーミングなどで同時に大量のパケットが伝送されると、各機器において通信のレスポンスが悪くなってしまいます。
(アクセスが増えるごとに、セッションあたりの帯域が狭くなっていきます。)

そこで、アプリケーション毎に占有できる帯域幅を調整することで、レスポンスの低下を防ぎます。
例えば、FTP に 64kbps、その他に 64kbps という帯域幅を設定すれば、FTP アクセスの際には常に最大 64kbpsの帯域を使用してアクセスできるようになります。

XR-410 では、**Ethernet ポートから送出されるトラフィックについて帯域を制御**します。

PPP/PPPoE 論理ポートについて帯域制御をおこなうことはできませんので、例えば PPPoE 接続について帯域制御をおこなう場合も Ether0 ポート側で制御してください。
また、送信元 / あて先の IP アドレス・ポート番号を指定して制御できます。

II．QoS 機能の設定

Web 設定画面「各種サービスの設定」→「帯域制御(QoS)サービス」をクリックして、以下の画面から設定します。

○制御する帯域幅
この条件に合致するパケットに割り当てる帯域幅を設定します。kbps 単位で設定します。
本装置の各 Ethernet ポートから送信されるパケットが帯域制御の対象となります。

○送信元 IP アドレス
送信元ホストの IP アドレスまたは、ネットワークアドレスを設定します。
範囲で設定することはできません。

< 入力例 >
ホスト単体の場合
192.168.0.1/32（“ /32 ”を付ける）

ネットワーク単位の場合
192.168.0.0/24（“ /マスクビット値 ”を付ける）

○送信元ポート番号
送信元ポート番号を設定します。
範囲で設定することはできません。

○あて先 IP アドレス
あて先ホストの IP アドレスまたは、ネットワークアドレスを設定します。
範囲で設定することはできません。
入力方法は、送信元 IP アドレスの場合と同じです。

○あて先ポート番号
あて先ポート番号を設定します。
範囲で設定することはできません。

○インターフェース
帯域制御をおこなうインタフェースを選択します。

○削除
一覧にある「削除」欄のラジオボックスにチェックを入れて「設定 / 削除の実行」をクリックすると、その設定が削除されます。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

一覧の“ No. ”が赤いときは、その番号の設定が正しくないことを示しています。
再度設定し直してください。

帯域制御をおこなう場合は、帯域制御(QoS)サービス機能を起動させる必要があります。
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、サービスの再起動をおこなってください。

第17章

攻撃検出機能

攻撃検出機能の設定

攻撃検出機能の概要

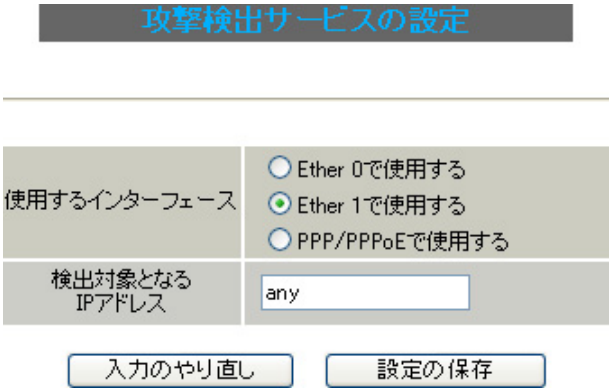
攻撃検出機能とは、外部から LAN への侵入や本装置を踏み台にした他のホスト・サーバ等への攻撃を仕掛けられた時などに、そのログを記録しておくことができる機能です。
検出方法には、統計的な面から異常な状態を検出する方法や、パターンマッチング方法などがあります。
XR-410 ではあらかじめ検出ルールを定めていますので、パターンマッチングによって不正アクセスを検出します。
ホスト単位の他、ネットワーク単位で監視対象を設定できます。

ログの出力

攻撃検出ログも、システムログの中に統合されて出力されますので、「システム設定」内の「ログの表示」やログメール機能で、ログを確認してください。

攻撃検出機能の設定

Web 設定画面「各種サービスの設定」→「攻撃検出サービス」をクリックして、以下の画面で設定します。



○使用するインターフェース
DoSの検出をおこなうインタフェースを選択します。PPP/PPPoE 接続しているインタフェース(主回線のみ)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
攻撃を検出したい送信先ホストの IP アドレス、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 (“ /マスクビット値 ”を付ける)

すべての IP アドレスの場合
any

「any」を設定すると、 すべてのアドレスが検出対象となります。

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

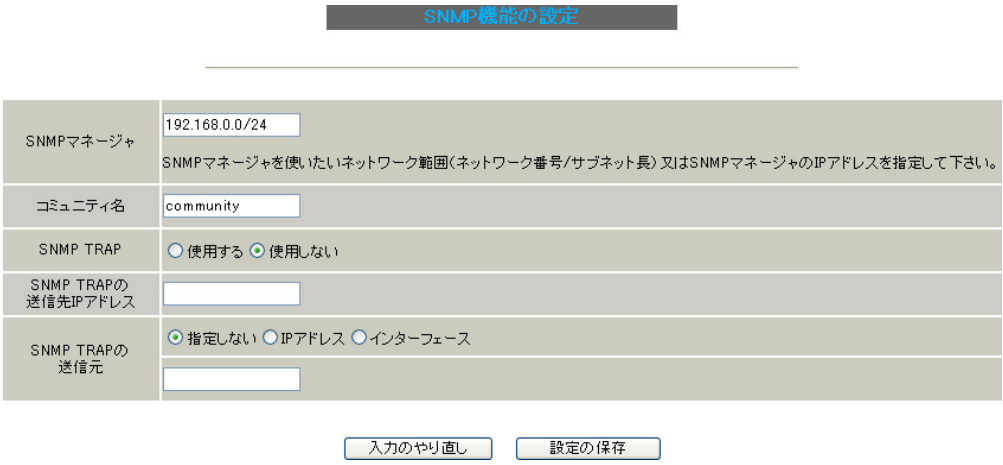
第 18 章

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-410 の MIB Ver.2(RFC1213)の情報を取得することができます。

Web 設定画面「各種サービス設定」→「SNMP サービス」をクリックして、以下の画面で設定します。



◯ SNMP マネージャ
SNMP マネージャを使いたいネットワーク範囲（ネットワーク番号 / サブネット長）または、SNMP マネージャの IP アドレスを指定します。

◯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
「使用する」を選択すると、SNMP TRAP を送信できるようになります。

◯ SNMP TRAP の送信先 IP アドレス
SNMP TRAP を送信する先(SNMP マネージャ)の IP アドレスを指定します。

◯ SNMP TRAP の送信元
SNMP パケット内の ”Agent Address ” に、任意のインタフェースアドレスを指定することができます。

・指定しない
SNMP TRAP の送信元アドレスが自動的に設定されます。

・IP アドレス
ボックス内に ISNMP TRAP の送信元アドレスとなる任意の IP アドレスを設定してください。

・インターフェース
ボックス内に、SNMP TRAP の送信元アドレスとなる任意のインタフェース名を入力してください。
指定可能なインタフェースは本装置の Ethernet または PPP です。

◯ SNMP TRAP の送信元
SNMP RESPONSE パケットの送信元アドレスを設定できます。
IPsec 接続を通して、リモート拠点のマネージャから SNMP を取得したい場合は、ここに IPsecSA の LAN 側アドレスを指定してください。
通常の LAN 内でマネージャを使用する場合には設定の必要はありません。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」トップに戻り、サービスを起動させてください。
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。

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 インターフェースの up、down
- PPP インタフェースの up、down
- 下記の各機能の up、down
  - DNS
  - DHCP サーバー
  - DHCP リレー
  - PLUTO(IPSec の鍵交換をおこなう IKE 機能)
  - UPnP
  - RIP
  - OSPF
  - SYSLOG
  - 攻撃検出
  - NTP
  - VRRP
- SNMP TRAP 自身の起動、停止

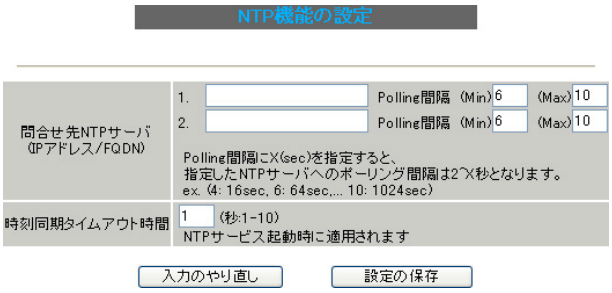
第 19 章

NTP サービス

NTP サービスの設定方法

XR-410 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。

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)]
NTP サーバの IP アドレスまたは FQDN を、設定「1.」もしくは「2.」に入力します。
NTP サーバの場所は２箇所設定できます。
これにより、XR-410 が NTP クライアント / サーバとして動作できます。

NTP サーバの IP アドレスもしくは FQDN を入力しない場合は、XR-410 は NTP サーバとしてのみ動作します。

○ Polling 間隔
NTP サーバと通信をおこなう間隔を設定します。
サーバとの接続状態により、指定した最小値(「Min」)と最大値(「Max」)の範囲でポーリングの間隔を調整します。
Polling 間隔 X(sec)を指定した場合、秒単位での間隔は 2 の X 乗(秒)となります。

＜例 4：16 秒、 6：64 秒、... 10：1024 秒＞

数字は、4～17(16-131072 秒)の間で設定出来ます。
Polling 間隔の初期設定は「Min」6(64 秒)、「Max」10（1024 秒）です。
初期設定のまま NTP サービスを起動させると、はじめは 64 秒間隔で NTP サーバとポーリングをおこない、その後は 64 秒から 1024 秒の間で NTP サーバとポーリングをおこない、時刻のずれを徐々に補正していきます。

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

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

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

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 サーバには以下のようなものがあります。

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

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

NTP クライアントの設定方法

各ホスト / サーバーを NTP クライアントとして XR-410 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 20 章

VRRP 機能

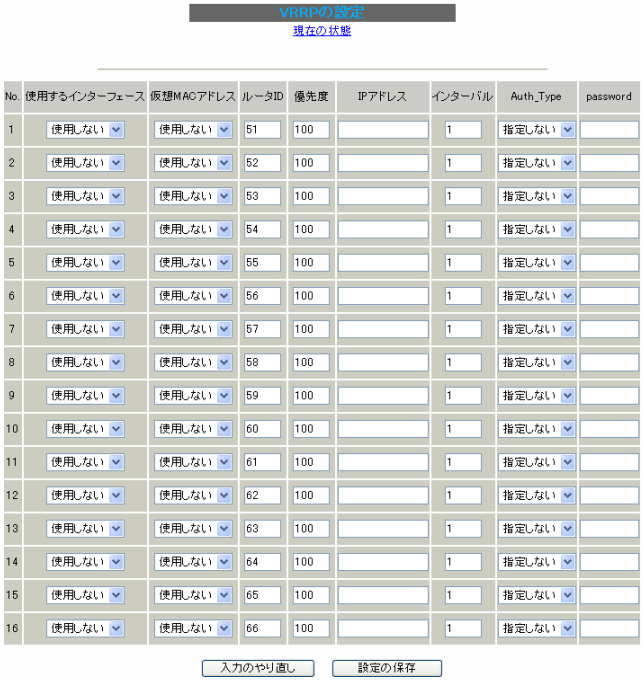
第 18 章 VRRP サービス

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 サービスの設定をします。



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

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

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

○優先度
VRRP グループ内での優先度を設定します。
数字が大きい方が優先度が高くなります。
優先度の値が最も大きいものが、VRRP グループ内での「マスタールータ」となり、他のルータは「バックアップルータ」となります。
1～255 の間で指定します。

○ IP アドレス
VRRP ルータとして作動するときの仮想 IP アドレスを設定します。
VRRP を作動させている環境では、各ホストはこの仮想 IP アドレスをデフォルトゲートウェイとして指定してください。

○インターバル
VRRP パケットを送出する間隔を設定します。
単位は秒です。1～255 の間で設定します。
VRRP パケットの送受信によって、VRRP ルータの状態を確認します。

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

○ Password
認証を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、サービスを起動させてください。また設定を変更した場合には、サービスの再起動をおこなってください。

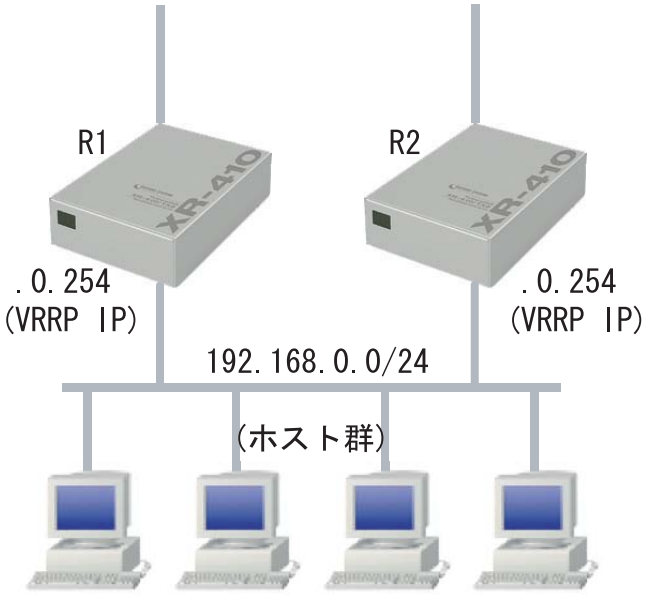
ステータスの表示

VRRP 機能設定画面上部にある「現在の状態」をクリックすると、VRRP 機能の動作状況を表示するウィンドウがポップアップします。

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 21 章

アクセスサーバ機能

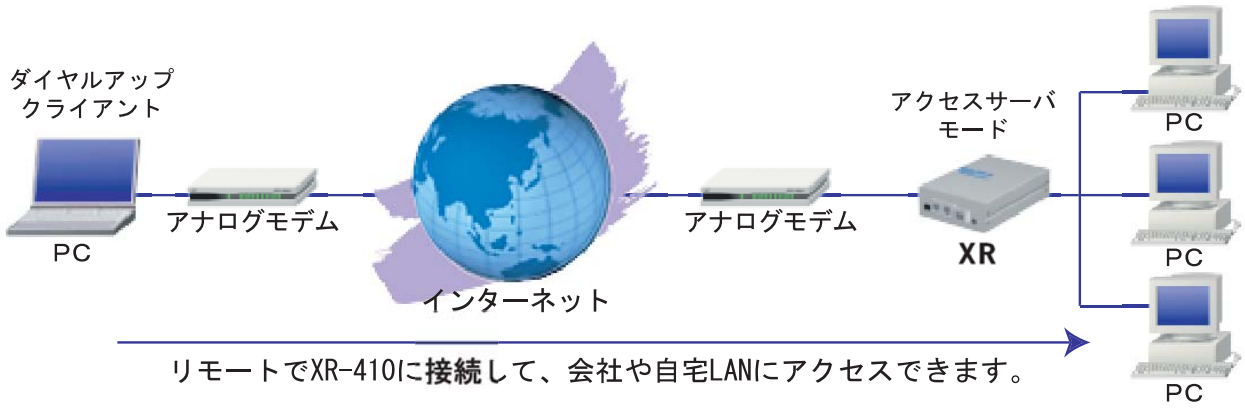
第 21 章 アクセスサーバ機能

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-410 を会社に設置すると、モデムを接続した外出先のコンピュータから会社の LAN に接続できます。
これは、モバイルコンピューティングや在宅勤務を可能にします。
クライアントはモデムによる PPP 接続を利用できるものであれば、どのような PC でもかまいません。
この機能を使って接続したクライアントは、接続先のネットワークにハブで接続した場合と同じようにネットワークを利用できます。

セキュリティは、ユーザー ID・パスワード認証によって確保します。
ユーザー ID・パスワードは、最大 5 アカウント分を登録できます。



II．XR-410 とアナログモデム /TA の接続

リモートアクセス機能を設定する前に、XR-410 とアナログモデムや TA を接続します。以下のように接続してください。

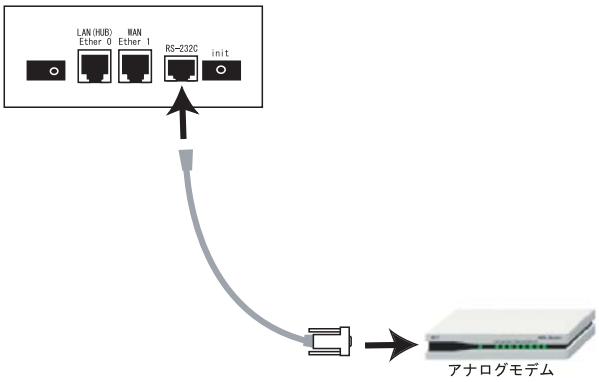
◆アナログモデム /TA の接続

1 XR-410 本体背面の「RS-232」ポートと製品付属の変換アダプタとを、ストレートタイプの LAN ケーブルで接続してください。

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

3 全ての接続が完了しましたら、モデム /TA の電源を投入してください。

接続図



III. アクセスサーバ機能の設定

設定方法

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

○アクセスサーバ
アクセスサーバ機能の使用 / 不使用を選択します。

○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-410 自身の IP アドレスを入力します。
各 Ethernet ポートのアドレスとは異なるプライベートアドレスを設定してください。
なお、サブネットのマスクビット値は 24 ビット(255.255.255.0)に設定されています。

○クライアントの IP アドレス
XR-410 にリモートアクセスしてきたホストに割り当てる IP アドレスを入力します。
上記の「アクセスサーバの IP アドレス」で設定したものと同じネットワークとなるアドレスを設定してください。

○モデムの速度
XR-410 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。

ユーザーアカウントの設定

設定画面の下側でユーザーアカウントの設定をおこないます。

○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。
5 アカウントまで登録しておけます。

○削除
ラジオボックスにチェックして「設定の保存」をクリックすると、その設定が削除されます。

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。

設定後は、外部からダイヤルアップ接続をおこなってください。

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。

アカウント設定上の注意

アクセスサーバ機能のユーザアカウントと、PPP/PPPoE 設定の接続先設定で設定してあるユーザ ID に、同じユーザ名を登録した場合、そのユーザは**着信できません**。
ユーザ名が重複しないように設定してください。

第 22 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-410 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。

○ホスト / ネットワーク
ルーティング先が、「ネットワーク」か、単一「ホスト」かを選択します。

○アドレス
あて先ホストのアドレス、またはネットワークアドレスを入力します。

○ネットマスク
あて先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 ： **255.255.255.2255**

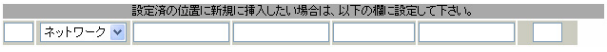
○インターフェース／ゲートウェイ
ルーティングをおこなうインターフェース名、もしくは上位ルータの IP アドレスのどちらかを設定します。
本装置のインターフェース名については、本マニュアルの「付録 A」をご参照ください。

○ディスタンス
経路選択の優先順位を指定します。
1 ～ 255 の間で指定します。値が低いほど優先度が高くなります。
スタティックルートのデフォルトディスタンス値は 1 です。
ディスタンス値を変更することで、フローティングスタティックルート設定とすることも可能です。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

設定を挿入する

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



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

スタティックルーティング設定

設定を削除する

ルーティング設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

デフォルトルートを設定する

スタティックルート設定でデフォルトルートを設定するときは、「アドレス」と「ネットマスク」項目をいずれも ”0.0.0.0 ” として設定してください。

ルーティング情報を確認する

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

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

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

第 23 章

ソースルーティング

ソースルーティング設定

通常のダイナミックルーティングおよびスタティックルーティングでは、パケットのあて先アドレスごとにルーティングをおこないますが、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。

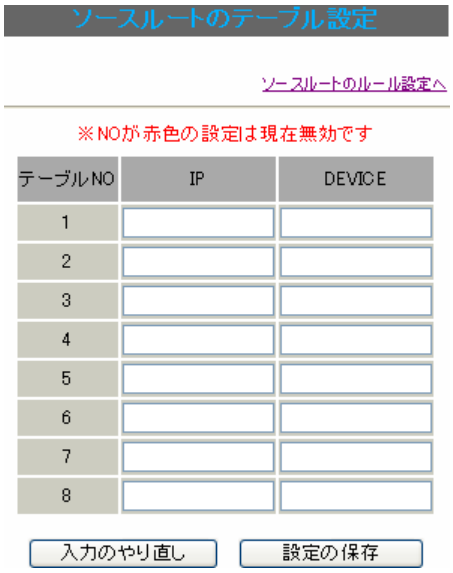
このソースルート機能を使うことで、外部へアクセスするホスト/ネットワークごとにアクセス回線を選択することができますので、複数のインターネット接続をおこなって負荷分散が可能となります。

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(情報表示で確認できます。“ eth0 ”や“ ppp0 ”などの表記のものです)。省略することもできます。

設定後は「設定の保存」をクリックします。

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指定化の画面を開きます。

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

<例>
Ether0ポートのIPアドレスが192.168.0.254で、送信元ネットワークアドレスを192.168.0.0/24と設定すると、192.168.0.0/24内のホストは本装置の設定画面にアクセスできなくなります。

第 24 章

NAT 機能

第24章　NAT機能

Ⅰ．XR-410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-410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-410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。

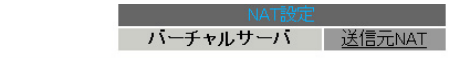
**NetMeetingや各種IM、ネットワークゲームなど、独自のプロトコル・ポートを使用しているアプリケーションについては、NAT機能を使用すると正常に動作しない場合があります。
原則として、NATを介しての個々のアプリケーションの動作についてはサポート対象外とさせていただきます。**

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。
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。

設定方法

Web 設定画面「NAT 設定」→「バーチャルサーバ」をクリックして、以下の画面から設定します。



○サーバのアドレス
インターネットに公開するサーバの、プライベート IP アドレスを入力します。

○公開するグローバルアドレス
サーバのプライベート IP アドレスに対応させるグローバル IP アドレスを入力します。
インターネットからはここで入力したグローバル IP アドレスでアクセスします。
プロバイダから割り当てられている IP アドレスが一つだけの場合は、ここは空欄にします。

○プロトコル
サーバのプロトコルを選択します。

○ポート
サーバが公開するポート番号を入力します。
範囲で指定することも可能です。範囲で指定するときは、ポート番号を ":" で結びます。
　<例>ポート 20 番から 21 番を指定する → **20:21**

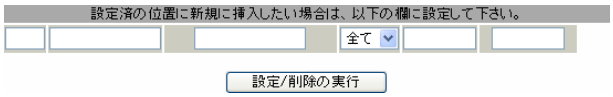
ポート番号を指定して設定するときは、必ずプロトコルも選択してください。
プロトコルが「全て」の選択ではポートを指定することはできません。

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

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

設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。
挿入は、設定テーブルの一番下にある行からおこないます。



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

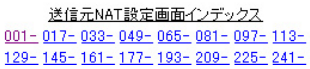
設定を削除する

バーチャルサーバ設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

III．送信元 NAT 設定

設定方法

Web 設定画面「NAT 設定」→「送信元 NAT」をクリックして、以下の画面から設定します。
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。

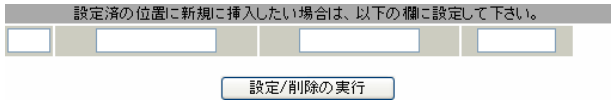
○変換後のグローバルアドレス
プライベート IP アドレスの変換後のグローバル IP アドレスを入力します。
送信元アドレスをここで入力したアドレスに書き換えてインターネット(WAN)へアクセスします。

○インターフェース
どのインターフェースからインターネット(WAN)へアクセスするか、インターフェース名を指定します。
インターネット(WAN)につながっているインターフェースを設定してください。
本装置のインターフェース名については、本マニュアルの「付録 A」をご参照ください。

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

設定を挿入する

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



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

設定を削除する

送信元 NAT 設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

Ⅳ．バーチャルサーバの設定例

◆ WWW サーバを公開する際の NAT 設定例

NAT の条件

・WAN 側のグローバルアドレスに TCP のポート 80 番(http)でのアクセスを通す。
・LAN から WAN へのアクセスは自由にできる。
・WAN は Ether1、LAN は Ether0 ポートに接続。

LAN 構成

・LAN 側ポートの IP アドレス「192.168.0.254」
・WWW サーバのアドレス　　「192.168.0.1」
・グローバルアドレスは「211.xxx.xxx.102」のみ

設定画面での入力方法

・あらかじめ IP マスカレードを有効にします。
・「バーチャルサーバ設定」で以下の様に設定します。

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 25 章

パケットフィルタリング機能

第25章 パケットフィルタリング機能

Ⅰ．機能の概要

XR-410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-410自身が受信するパケットを制限する。
・XR-410自身から送信するパケットを制限する。
・ゲートウェイ認証機能を使用しているときにアクセス可能にする

またフィルタリングは以下の情報に基づいて条件を設定することができます。

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

パケットフィルタリング機能を有効にすると、パケットを単にルーティングするだけでなく、パケットのヘッダ情報を調べて、送信元やあて先のIPアドレス、プロトコルの種類(TCP/UDP/ICMPなどやプロトコル番号)、ポート番号に基づいてパケットを通過させたり破棄させることができます。

このようなパケットフィルタリング機能は、コンピュータやアプリケーション側の設定を変更する必要がないために、個々のコンピュータでパケットフィルタの存在を意識することなく、簡単に利用できます。

II．XR-410 のフィルタリング機能について

XR-410 は、以下の 4 つの基本ルールについてフィルタリングの設定をおこないます。

- **入力(input)**
- **転送(forward)**
- **出力(output)**
- **ゲートウェイ認証（authgw）**

◆入力(input)フィルタ
外部から本装置自身に入ってくるパケットに対して制御します。インターネットや LAN から本装置へのアクセスについて制御したい場合には、この入力ルールにフィルタ設定をおこないます。

◆転送(forward)フィルタ
LAN からインターネットへのアクセスや、インターネットから LAN 内サーバへのアクセス、LAN から LAN へのアクセスなど､本装置で内部転送する(本装置がルーティングする)アクセスを制御するという場合には､この転送ルールにフィルタ設定をおこないます。

◆出力(output)フィルタ
本装置内部からインターネットや LAN などへのアクセスを制御したい場合には、この出力ルールにフィルタ設定をおこないます。
パケットが「転送されるもの」か「本装置自身へのアクセス」か「本装置自身からのアクセス」かをチェックしてそれぞれのルールにあるフィルタ設定を実行します。

◆ゲートウェイ認証（authgw）フィルタ
「ゲートウェイ認証機能」を使用しているときに設定するフィルタです。
ゲートウェイ認証を必要とせずに外部と通信可能にするフィルタ設定をおこないます。
ゲートウェイ認証機能については「第 28 章」をご覧ください。

各ルール内のフィルタ設定は先頭から順番にマッチングされ、最初にマッチした設定がフィルタとして動作することになります。
逆に、マッチするフィルタ設定が見つからなければそのパケットはフィルタリングされません。

**本製品の工場出荷設定では、Ether0 ポート以外はステートフルパケットインスペクション機能が有効になっています。
この機能により、Ether0 ポート以外から XR-410 自身、また LAN 内へのアクセスは一切できないようになっています。**

unnumbered 接続やバーチャルサーバ機能によるサーバ公開を運用される場合は、ステートフルパケットインスペクション機能を無効にするか、パケットフィルタリングの設定をおこない、外部から LAN へのアクセスを許可する設定をおこなってください。

III. パケットフィルタリングの設定

入力・転送・出力・ゲートウェイ認証フィルタの4種類がありますが、設定方法はすべて同じです。
設定可能な各フィルタの最大数は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設定画面にログインします。「フィルタ設定」→「入力フィルタ」「転送フィルタ」「出力フィルタ」「ゲートウェイ認証フィルタ」のいずれかをクリックして、以下の画面から設定します。

(画面は「転送フィルタ」)

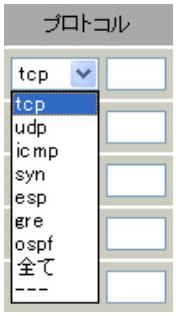
○インターフェース
フィルタリングをおこなうインタフェース名を指定します。
本装置のインターフェース名については、本マニュアルの「付録A インタフェース名一覧」をご参照ください。

○方向
ポートがパケットを受信するときにフィルタリングするか、送信するときにフィルタリングするかを選択します。
入力フィルタでは「パケット受信時」、出力フィルタでは「パケット送信時」のみとなります。

III．パケットフィルタリングの設定

○動作
フィルタリング設定にマッチしたときにパケットを「破棄」するか「通過」させるかを選択します。

○プロトコル
フィルタリング対象とするプロトコルを選択します。
右側の空欄でプロトコル番号による指定もできます。
ポート番号も指定する場合は、ここで必ずプロトコルを選択しておいてください。



○送信元アドレス
フィルタリング対象とする、送信元のIPアドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。

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

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

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

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

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

○あて先アドレス
フィルタリング対象とする、あて先のIPアドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。
入力方法は、送信元 IP アドレスと同様です。

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

○ ICMP type/code
プロトコルで「icmp」を選択した場合に、ICMP の type/code を指定することができます。プロトコルで「icmp」以外を選択した場合は指定できません。

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

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

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

”No.” 項目が赤字で表示されている行は入力内容が正しくありません。再度入力をやり直してください。

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「転送フィルタ」）

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					1024:6553
9	ppp0	パケット受信時	許可	udp					1024:6553
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。

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

◆外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

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

「出力フィルタ設定」で以下のように設定します。

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

フィルタの解説

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

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

Ⅳ．パケットフィルタリングの設定例

◆PPTP を通すためのフィルタ設定

フィルタの条件

・WAN 側からの PPTP アクセスを許可する。

LAN 構成

・WAN 側は PPPoE 回線に接続する。

設定画面での入力方法

「転送フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp				1723
2	ppp0	パケット受信時	許可	gre				

フィルタの解説

PPTP では以下のプロトコル・ポートを使って通信します。

- プロトコル「GRE」
- プロトコル「tcp」のポート「1723」

したがいまして、フィルタ設定では上記 2 つの条件に合致するパケットを通す設定をおこなっています。

Ⅴ．外部から設定画面にアクセスさせる設定

XR-410 の初期設定では Ether1 ポートで、ステートフルパケットインスペクション機能が有効になっています。
そのため、外部から XR-410 の設定画面にアクセスできないようになっています。

しかし、遠隔で XR-410 の設定・制御をおこなう必要がある場合は、「入力フィルタ」で必要な設定をおこなうことで、外部から設定画面にアクセス可能にすることができます。
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。

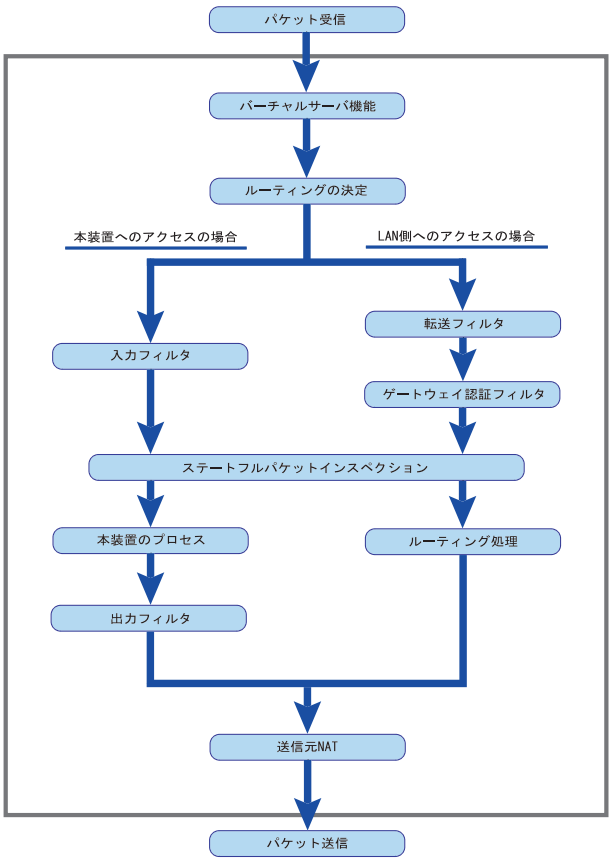
No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	許可	tcp	221.xxx.xxx.105			880

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 XR-410 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-410 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-410 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-410 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-410 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-410 自身へのアクセスはすべて破棄されます。
- ステートフルパケットインスペクションと同時に「入力フィルタ」「転送フィルタ」を設定している場合は、先に「入力フィルタ」「転送フィルタ」にある設定が優先して処理されます。
- 「送信元 NAT 設定」は、一番最後に参照されます。
- LAN 側から WAN 側へのアクセスの場合も、処理の順序は同様です(最初にバーチャルサーバ設定が参照される)。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。
詳細はRFC1700(Oct. 1994)を参照してください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

補足：フィルタのログ出力内容について

フィルタ設定画面で「LOG」にチェックを入れると、その設定に合致したパケットの情報を syslog に出力します。
出力内容は以下のようになります。

<入力パケットを破棄したときのログ出力例>

```
Jan 25 14:14:07 localhost XR-Filter:  FILTER_INPUT_1 IN=eth0 OUT=
MAC=00:80:6d:xx:xx:xx:00:20:ed:yy:yy:yy:80:00  SRC=192.168.xxx.xxx DST=xxx.xxx.xxx.xxx LEN=40
TOS=00 PREC=0x00 TTL=128 ID=43951 CE DF PROTO=TCP SPT=2526 DPT=880 SEQ=4098235374 ACK=1758964579
WINDOW=48000 ACK URGP=0
```

Jan 25 14:14:07	syslog がログを取得した日時です。
XR-Filter:	フィルタのログであることを表します。
FILTER_INPUT_1	入力フィルタの１番目のフィルタで取得されたものです。 「FILTER_FORWARD」は転送フィルタを意味します。 「FILTER_OUTPUT」は出力フィルタを意味します。 「FILTER_AUTHGW」はゲートウェイ認証フィルタを意味します。
IN=	パケットを受信したインタフェースが記されます。
OUT=	パケットを送出したインタフェースが記されます。 何も記載されていないときは、XRのどのインタフェースからもパケットを送出していないことを表わしています。
MAC=	送信元・あて先のMACアドレスが記されます。
SRC=	送信元IPアドレスが記されます。
DST=	送信先IPアドレスが記されます。
LEN=	パケット長が記されます。
TOS=	TOS bitの状態が記されます。
TTL=	TTLの値が記されます。
ID=	IPのIDが記されます。
PROTO=	プロトコルが記されます。

プロトコルが ICMP の時は、以下のような ICMP 用のメッセージも記されます。

TYPE=0	ICMPのタイプが記されます。
CODE=0	ICMPのコードが記されます。
ID=3961	ICMPのIDが記されます。
SEQ=6656	ICMPのシーケンス番号が記されます。

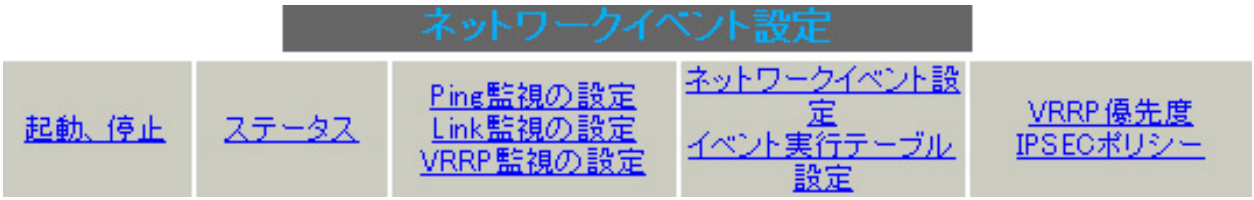
第 26 章

ネットワークイベント機能

第 26 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、それをトリガー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ーとして検知することができます。

- Ping 監視の状態
- Link 監視の状態
- VRRP 監視の状態

◆Ping 監視
本装置から任意の宛先へ ping を送信し、その応答の有無を監視します。
一定時間応答がなかった時にトリガ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。

またこれらのトリガーを検知した際に実行可能なイベントとして以下の 2 つがあります。

- VRRP 優先度変更
- IPsec 接続切断

◆VRRP 優先度変更
トリガー検知時に、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。

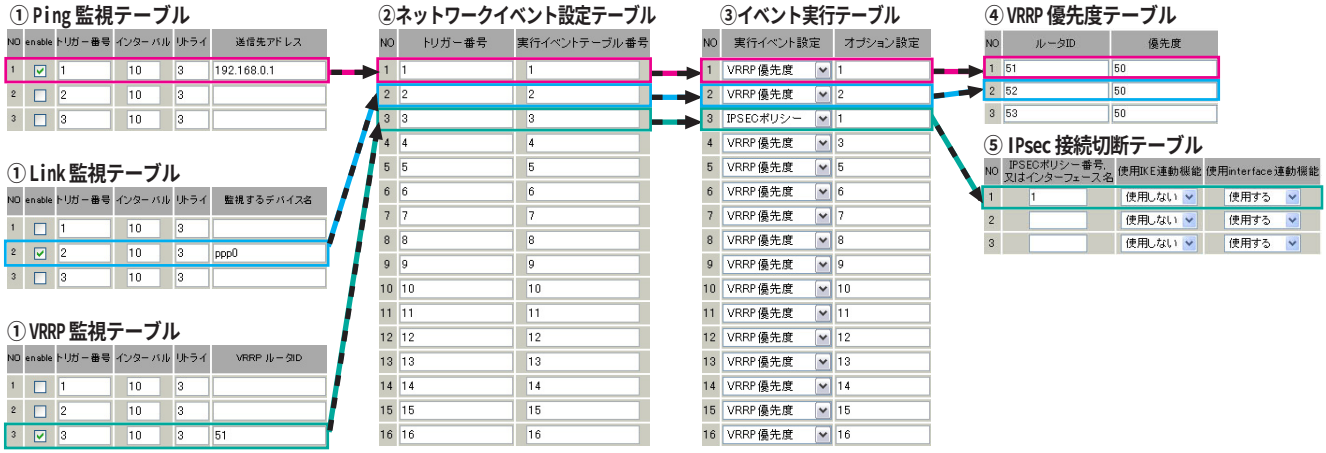
例えば、VRRP 監視と連動して、2 台の VRRP ルータのマスタルータの切り替わりに応じて、IPsec 接続を繋ぎかえる、といった使い方ができます。

第 26 章 ネットワークイベント機能

Ⅰ．機能の概要

本機能で使用する各種テーブルについて

本機能は複数のテーブル定義を連携させることによって実現しています。



①Ping 監視テーブル /Link 監視テーブル /VRRP 監視テーブル

これらのテーブルでは、監視対象、監視周期、障害検出した場合のトリガー番号を設定します。ここで設定を有効(enable)にしたトリガー番号は、次の「②ネットワークイベント設定テーブル」のインデックス番号になります。

②ネットワークイベント設定テーブル

このテーブルでは、トリガー番号とイベント番号の関連付けを定義します。
ここで設定したイベント番号は、次の「③イベント実行テーブル」のインデックス番号になります。

③イベント実行テーブル

このテーブルでは、イベント番号と実行イベント種別 / オプション番号の関連付けを定義します。

イベントの実行種別を「VRRP 優先度」に設定した場合は、次に「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。

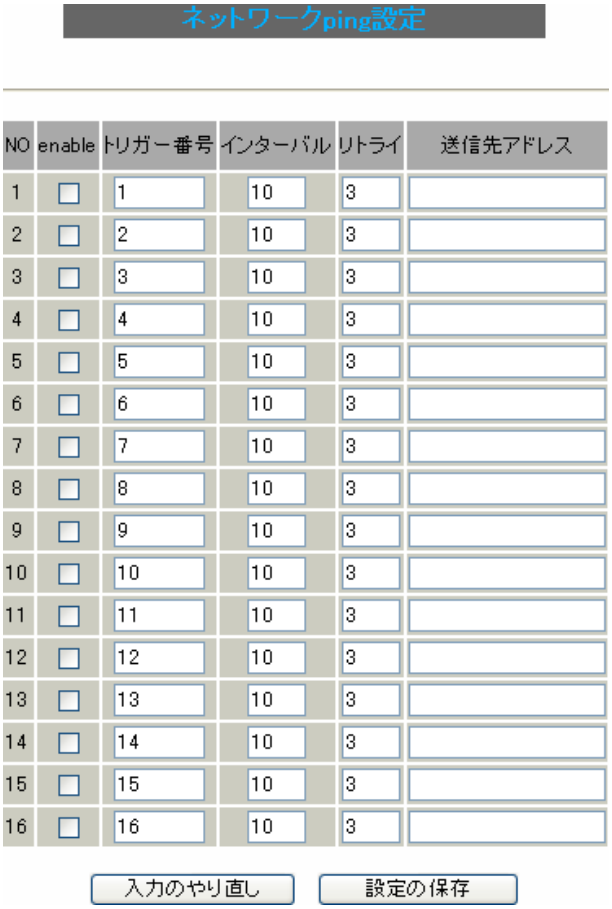
⑤ IPSEC 接続切断テーブル

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．各トリガーテーブルの設定

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。

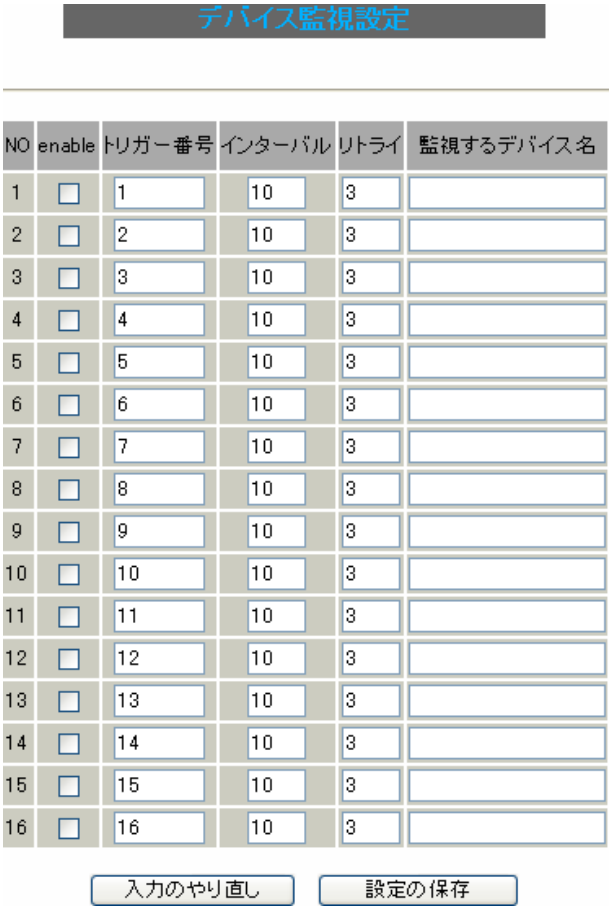
○送信先アドレス
ping を送信する先の IP アドレスを指定します。

最後に「設定の保存」をクリックして設定完了です。

Ⅱ．各トリガーテーブルの設定

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。

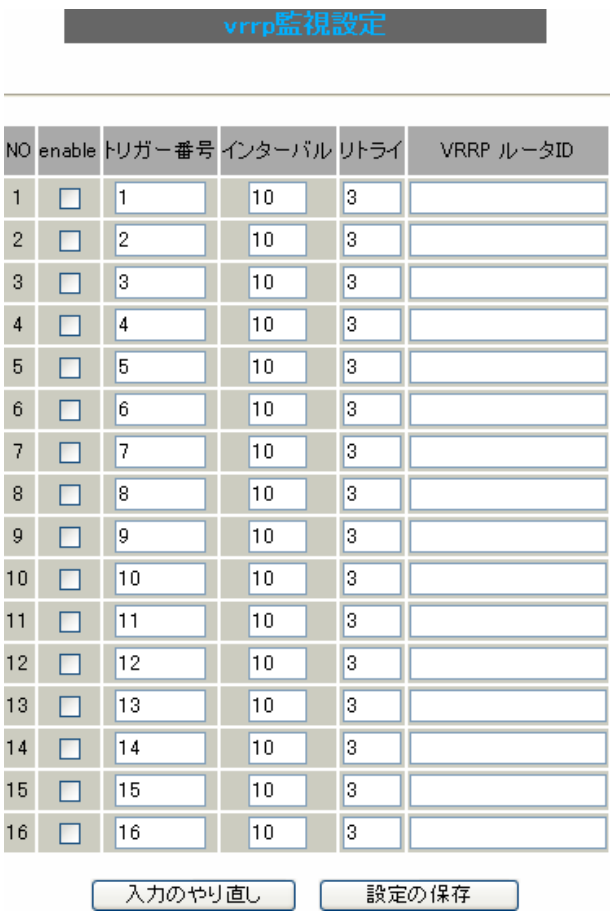
○監視するデバイス名
リンク状態を監視するデバイスのインタフェース名を指定します。
Ethernet インタフェース名、または PPP インタフェース名を入力してください。

最後に「設定の保存」をクリックして設定完了です。

Ⅱ．各トリガーテーブルの設定

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。

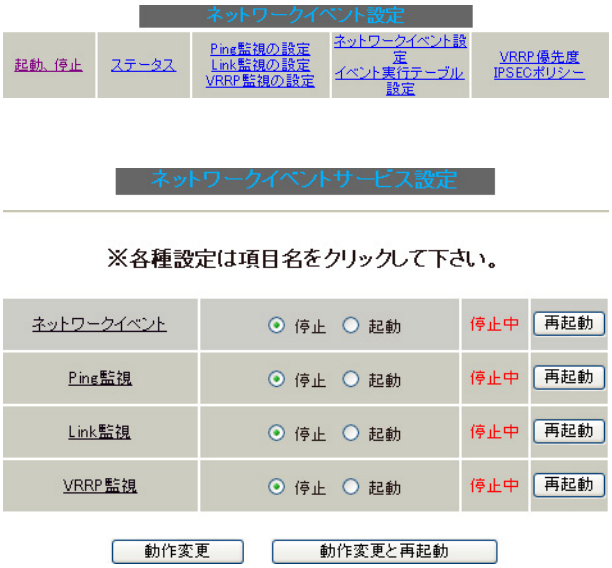
最後に「設定の保存」をクリックして設定完了です。

Ⅱ．各トリガーテーブルの設定

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 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。



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。

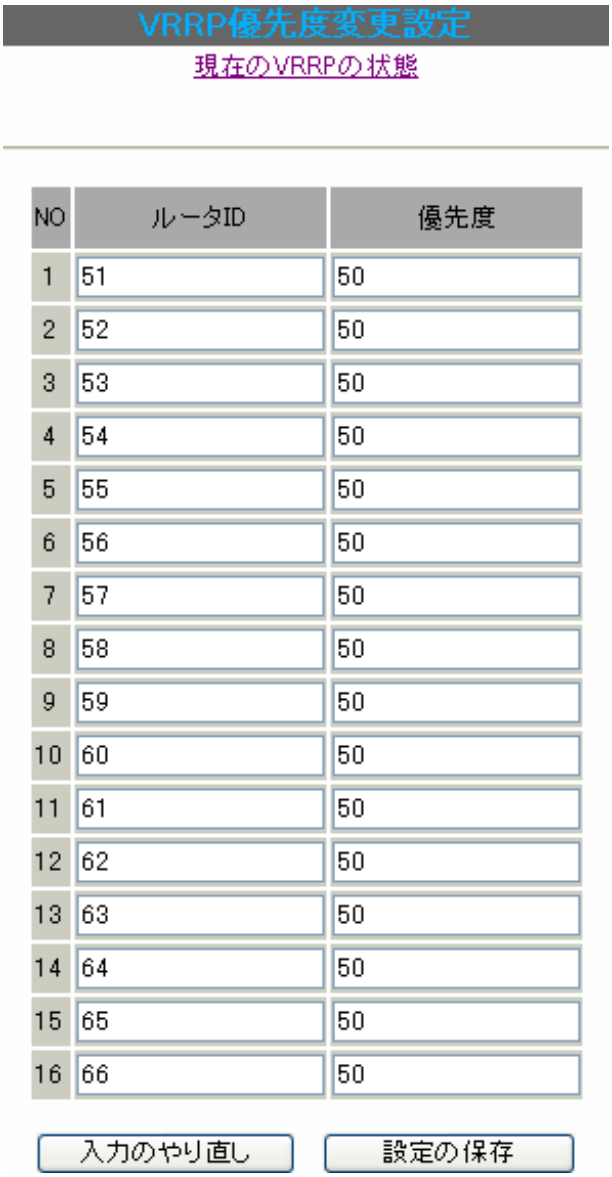
○オプション設定
実行イベントのオプション番号です。
本値は、「VRRP 優先度変更設定」テーブル、または「IPSEC 接続切断設定」テーブルでのインデックス番号となります。

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。

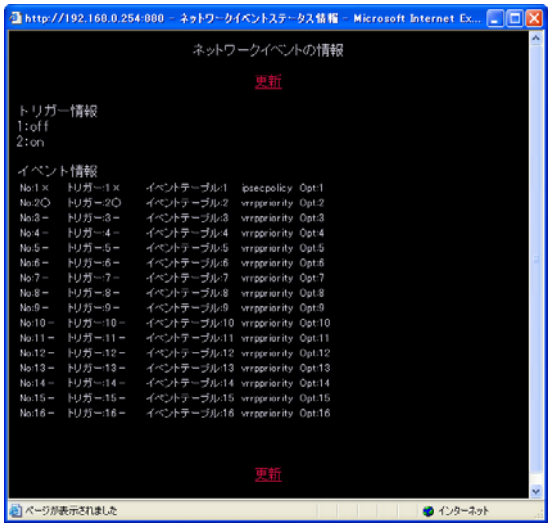
現在の設定状態の確認

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は、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は、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 27 章

仮想インターフェース機能

仮想インターフェースの設定

主にバーチャルサーバ機能を利用する場合に、仮想インタフェースを設定します。
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
仮想インターフェースを作成するインターフェース名を指定します。
本装置のインターフェース名については、本マニュアルの「付録 A」をご参照ください。

○仮想 I/F 番号
作成するインターフェースの番号を指定します。
0～127 の間で設定します。

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

○ネットマスク
作成するインターフェースのネットマスクを指定します。

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

設定を削除する

仮想インターフェース設定を削除する場合は、削除したい設定行の「削除」ボックスにチェックを入れて「設定 / 削除の実行」ボタンをクリックすると削除されます。

第 28 章

GRE 機能

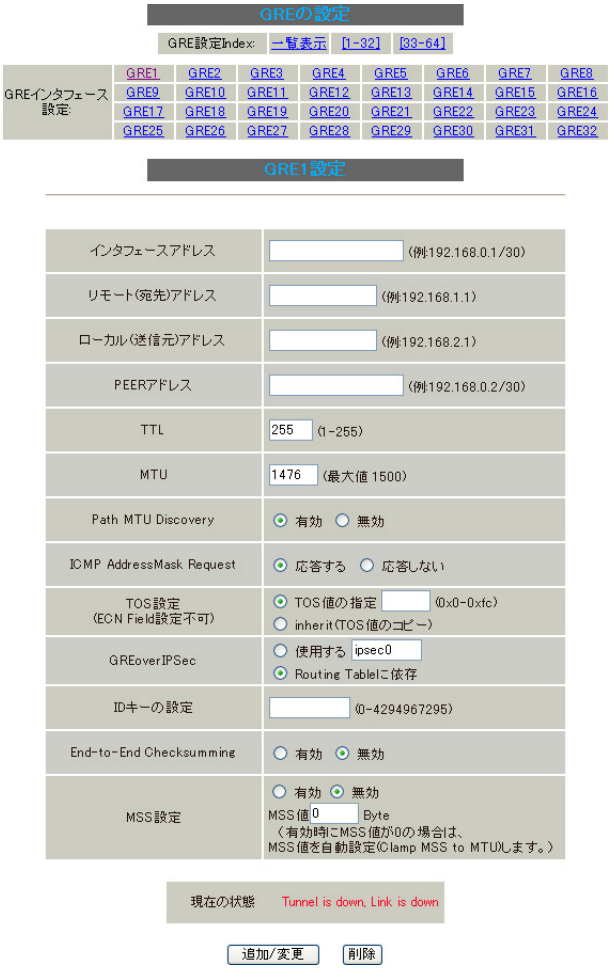
第 28 章 GRE 設定

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。
「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。初期値は 1476byte です。

○ Path MTU Discovery
Path MTU Discovery 機能を有効にするかを選択します。
機能を「有効」にした場合は、常に IP ヘッダの DF ビットを ON にして転送します。
転送パケットの DF ビットが 1 でパケットサイズが MTU を超えている場合は、送信元に ICMP Fragment Needed を返送します。

PathMTU Discovery を「無効」にした場合、TTL は常にカプセル化されたパケットの TTL 値がコピーされます。

従って、GRE 上で OSPF を動かす場合には、TTL が 1 に設定されてしまうため、Path MTU Discovery を「有効」にしてください。

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

GRE の設定

○ ToS
GRE パケットの ToS 値を設定します。

○ GREoverIPsec
IPsec を使用して GRE トンネルを暗号化する場合に「使用する」を選択して IPsec インタフェース名を選択します。
また、この場合には別途 IPsec の設定が必要です。
Routing Table に合わせて暗号化したい場合には「Routing Table に依存」を選択してください。
ルートが IPsec の時は暗号化、IPsec でない時は暗号化しません。

○ 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

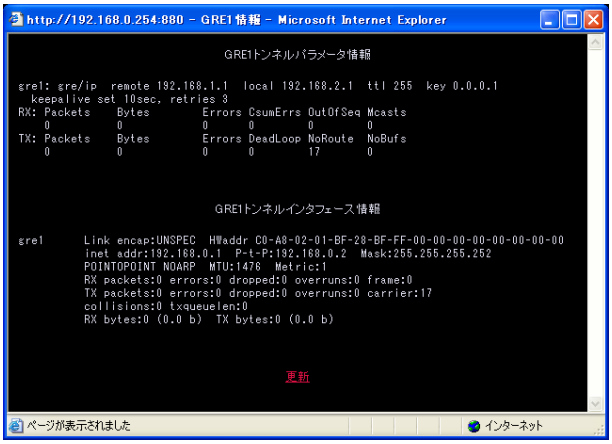
[GRE インタフェース設定:]の「GRE1」～「GRE64」各設定画面にある「削除」をクリックすると、その設定に該当する GRE トンネルが無効化されます(設定自体は保存されています)。
再度有効とするときは「追加/変更」ボタンをクリックしてください。

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。

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。

GRE一覧表示

Interface名	Interface Address	Remote Address	Local Address	Peer Address	MTU	ID Key	Check sum	PMTUD	ICMP	Link State
gre1	192.168.0.1/30	192.168.1.1	192.168.2.1	192.168.0.2/30	1476	1	無効	有効	有効	down

○編集
設定の編集は「Interface 名」をクリックしてください。

○リンク状態
GRE トンネルのリンク状態は「Link State」に表示されます。「up」が GRE トンネルがリンクアップしている状態です。

第 29 章

パケット分類設定

第 29 章 パケット分類設定

Ⅰ．XR-410 のパケット分類設定について

パケット分類設定は、受け取った特定のパケットに対して、TOS/Precedence 値や DSCP 値を付加するための設定です。
XR-410/TX2 シリーズでは、以下の内容によりパケットの分類をおこないます。

プロトコル	プロトコル番号
送信元アドレス	送信元 IP アドレス / プレフィクス
送信元ポート	送信元ポート番号
宛先アドレス	宛先 IP アドレス / プレフィクス
宛先ポート	宛先ポート番号
インタフェース	パケット分類対象インタフェース
TOS 値	受信パケットの TOS 値
DSCP 値	受信パケットの DSCP 値

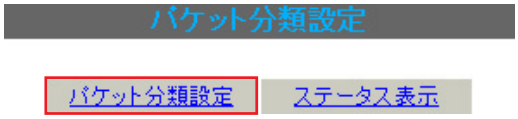
上記の条件に合致するパケットの TOS/Precedence 値、あるいは DSCP 値を書き換えることが可能です。

Ⅱ．パケット分類設定の設定

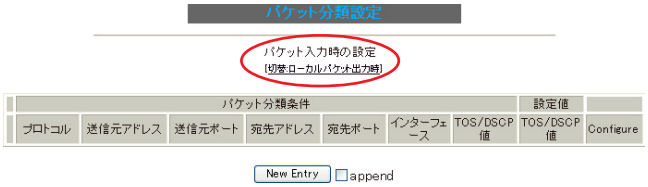
◆パケット分類設定

設定方法

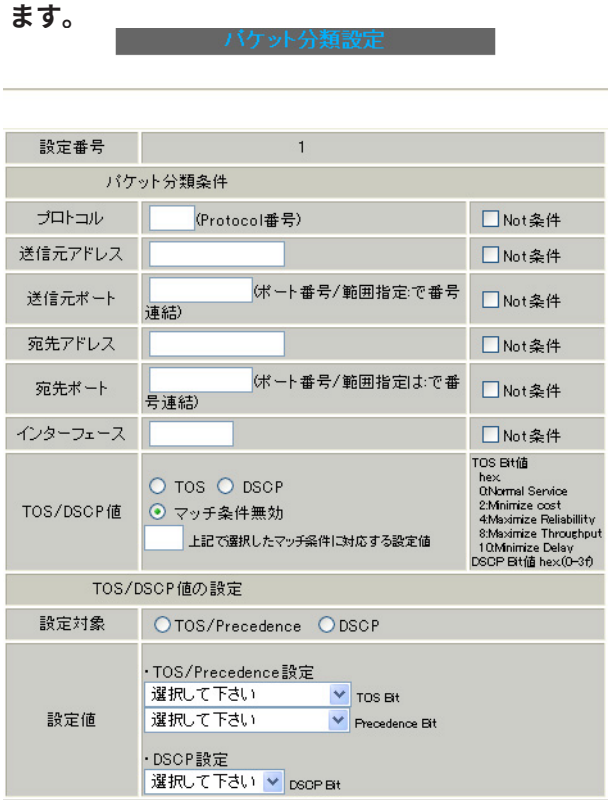
Web 設定画面「パケット分類設定」を開き、「パケット分類設定」をクリックします。



以下の画面が表示されます。
「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、[切替:]をクリックして選選択します。



設定を追加するときは「New Entry」をクリックします。



(画面は表示例です)

○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。

○ Not 条件
[パケット分類条件]の各項目について「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/DSCP 値
マッチングする TOS/DSCP 値を指定します。
TOS、DSCPのどちらかを選択し、その値を指定します。
どちらも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。

II．パケット分類設定の設定

[TOS/DSCP 値の設定]
パケット分類条件で選別したパケットに、あらたに TOS 値または DSCP 値を設定します。

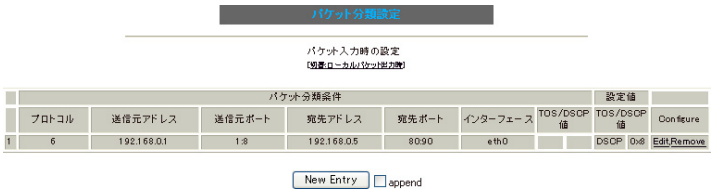
○設定対象
TOS/Precedence、DSCP のいずれかを選択します。

○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。

設定内容は一覧で表示されます。



（画面は表示例です）

○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。

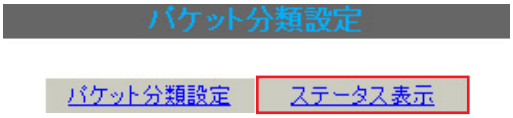
○設定の削除をおこなう場合
Configure 欄の「Remove」をクリックすると、その設定が即座に削除されます。

III．ステータスの表示

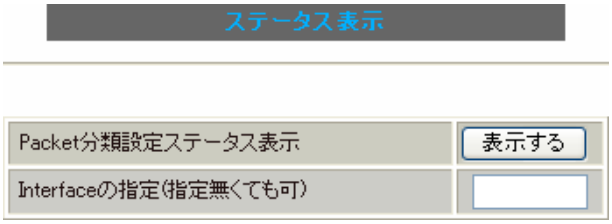
◆ステータス表示

実行方法

Web 設定画面「パケット分類設定」を開き、「ステータス表示」をクリックします。



以下の画面が表示されます。



[Packet 分類設定ステータス表示]
「表示する」ボタンをクリックすると、パケット分類設定のステータスが表示されます。

[Interface の指定]
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。

Ⅳ．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	宛先IPアドレス
MARK set	セットするMARK値
spts	送信元ポート番号
dpt	宛先ポート番号
Type of Service set	セットするTOSビット値

V．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。

V．TOS について

またアプリケーションごとのパケットの取り扱い方法も定義されています(RFC1349)。
アプリケーションの TOS 値は以下のようになっています。<表 3>

アプリケーション	TOSビット値	定義
TELNET	1000	(minimize delay)
FTP		
Control	1000	(minimize delay)
Data	0100	(maximize throughput)
TFTP	1000	(minimize delay)
SMTP		
Command phase	1000	(minimize delay)
DATA phase	0100	(maximize throughput)
Domain Name Service		
UDP Query	1000	(minimize delay)
TCP Query	0000	
Zone Transfer	0100	(maximize throughput)
NNTP	0001	(minimize monetary cost)
ICMP		
Errors	0000	
Requests	0000 (mostly)	
Responses	<same as request>	(mostly)

※表中の TOS ビット値(2 進数表記)が、<表 2> のビットに対応しています。

TOS 値は定義があいまいで相互運用できない、正しい値が設定されている保証がない、悪用される可能性があるなどの要因により、現在までほとんど使われていません。

VI．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 30 章

ゲートウェイ認証機能

第 30 章 ゲートウェイ認証機能

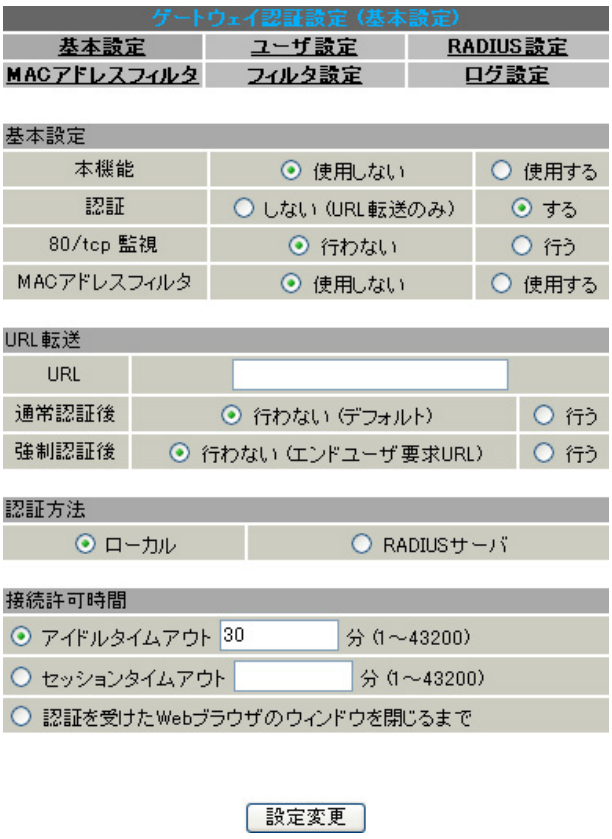
Ⅰ．ゲートウェイ認証機能の設定

「ゲートウェイ認証機能」は、本装置を経由して外部にアクセスをする場合に、本装置での認証を必要とする機能です。
この機能を使うことで、外部へアクセスできるユーザを管理できるようになります。

設定方法

Web 設定画面「ゲートウェイ認証設定」をクリックして、各設定をおこないます。

◆基本設定



[基本設定]

○本機能
ゲートウェイ認証機能を使う場合は「使用する」を選択します。

○認証
当機能を使用していて、かつ認証をおこなうときは「する」を選択します(初期設定)。
認証をおこなわないときは「しない」を選択します。
このときは、外部へのアクセスをリダイレクトするだけの動作となります。

○80/tcp 監視
認証を受けていない IP アドレスからの TCP ポート 80 番のコネクションを監視し、**このコネクションがあったときに、強制的にゲートウェイ認証をおこないます。**
初期設定は監視を「行わない」設定です。

○MAC アドレスフィルタ
MAC アドレスフィルタを有効にする場合は「使用する」を選択します。

[URL 転送]

○URL
転送先の URL を設定します。

○通常認証後
「行う」を選択すると、ゲートウェイ認証後に「URL」で指定したサイトに転送させることができます。
初期設定では URL 転送をおこないません。

○強制認証後
「行う」を選択すると、強制認証後に「URL」で指定したサイトに転送させることができます。
初期設定では URL 転送をおこないません。
この機能を使う場合は「80/tcp 監視」を有効にしてください。

[認証方法]

○ローカル
本装置でアカウントを管理 / 認証します。

○RADIUS サーバ
外部の RADIUS サーバでアカウントを管理 / 認証します。

Ⅰ．ゲートウェイ認証機能の設定

[接続許可時間]
認証したあとの､ユーザの接続形態を選択できます。

○アイドルタイムアウト
認証で許可された通信が無通信状態となってから切断するまでの時間を設定します。
初期設定は 30 分です。

○セッションタイムアウト
認証で許可された通信を強制的に切断するまでの時間を設定します。
認証してからこの時間が経過すると、通信状態にかかわらず通信を切断します。

○認証を受けたWebブラウザのウィンドウを閉じるまで
認証を受けた後にブラウザに表示された画面を閉じたときに、通信を切断します。
通信可能な状態を保つには､認証後の画面を開いたままにしなければなりません。
Web ブラウジングをする場合は、別のブラウザを開く必要があります。

上記設定にしたがって通信が切断した場合は、各ユーザは、再度ゲートウェイ認証を実行する必要があります。

最後に「設定変更」をクリックしてください。

ゲートウェイ認証機能を「使用する」にした場合はただちに機能が有効となりますので、ユーザー設定等から設定をおこなってください。

◆ユーザー設定

設定可能なユーザの最大数は 64 です。
画面最下部にある「ユーザ設定画面インデックス」のリンクをクリックしてください。

○ユーザ ID
○パスワード
ユーザアカウントを登録します。
ユーザ ID・パスワードは半角英数字で指定してください。
空白やコロン(:)は含めることができません。

○削除
チェックすると、その設定が削除対象となります。

最後に「設定/削除の実行」をクリックしてください。

Ⅰ．ゲートウェイ認証機能の設定

◆RADIUS 設定

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

[プライマリサーバ設定]

プライマリ項目の設定は必須です。

○ IP アドレス

○ポート番号

○ secret

RADIUS サーバの IP アドレス、ポート番号、secret を設定します。

[プライマリサーバ設定]

セカンダリ項目の設定はなくてもかまいません。

○ IP アドレス

○ポート番号

○ secret

[サーバ共通設定]

RADIUS サーバへ問い合わせをする際に送信する NAS の情報を設定します。

RADUIS サーバが、どの NAS かを識別するために使います。

どちらかの設定が必須です。

○ NAS-IP-Address

通常は XR-410 の IP アドレスを設定します。

○ NAS-Identifier

任意の文字列を設定します。

半角英数字が使用できます。

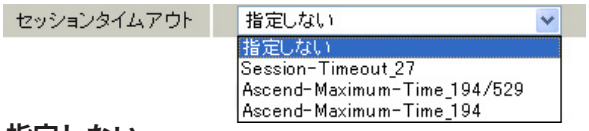
[接続許可時間（RADIUSサーバから送信されるアトリビュートの指定)]

それぞれ、基本設定で選択されているものが有効となります。

※ アトリビュートとは、RADIUS で設定されるパラメータのことを指します。

Ⅰ．ゲートウェイ認証機能の設定

○アイドルタイムアウト
プルダウンの以下の項目から選択してください。



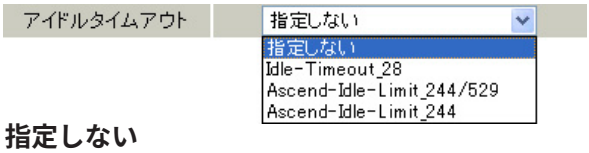
・指定しない
RADIUSサーバからの認証応答に該当のアトリビュートがあればその値を使います。
該当のアトリビュートがなければ「基本設定」で設定した値を使用します。

・Idle-Timeout_28
Idle-Timeout（Type=28)をアイドルタイムアウト値として使用します。

・Ascend-Idle-Limit_244/529
Ascend-Idle-Limit（Vendor-Specific Attribute Type=26，Vendor-Id=529，Attribute Type=244）をアイドルタイムアウト値として使用します。

・Ascend-Idle-Limit_244
Ascend-Idle-Limit（Type=244）をアイドルタイムアウト値として使用します。

○セッションタイムアウト
プルダウンの以下の項目から選択してください。



・指定しない
RADIUSサーバからの認証応答に該当のアトリビュートがあればその値を使います。
該当のアトリビュートがなければ「基本設定」で設定した値を使用します。

・Session-Timeout_27
Session-Timeout（Type=27)をセッションタイムアウト値として使用します。

・Ascend-Maximum-Time_194/529
Ascend-Maximum-Time（Vendor-Specific Attribute Type=26，Vendor-Id=529，Attribute Type=194）をセッションタイムアウト値として使用します。

・Ascend-Maximum-Time_194
Ascend-Maximum-Time（Type=194)をセッションタイムアウト値として使用します。

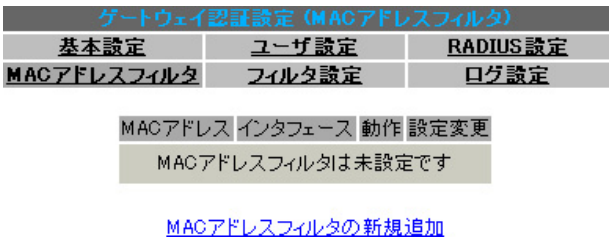
最後に「設定変更」をクリックしてください。

Ⅰ．ゲートウェイ認証機能の設定

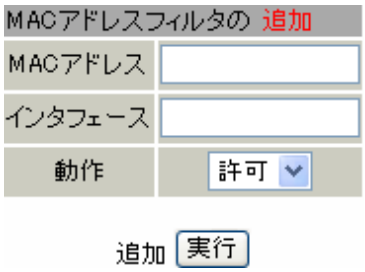
◆MAC アドレスフィルタ

ゲートウェイ認証機能を有効にすると、外部との通信は認証が必要となりますが、MAC アドレスフィルタを設定することによって、認証を必要とせずに通信が可能になります。

本機能で設定した MAC アドレスを送信元 MAC アドレスとする IP パケットの転送がおこなわれると、それ以降はその IP アドレスを送信元/送信先とする IP パケットの転送を許可します。
ここで設定する MAC アドレスは、転送許可を最初に決定する場合に用いられます。



「基本設定」で MAC アドレスフィルタを「使用する」に選択して、「MAC アドレスフィルタ」設定画面「MAC アドレスフィルタの新規追加」をクリックします。



[MAC アドレスフィルタの追加]

○MAC アドレス
フィルタリング対象とする、送信元の MAC アドレスを入力します。

○インタフェース
フィルタリングをおこなうインタフェース名を任意で指定します。
インタフェース名については、本マニュアルの「付録 A」をご参照ください。

○動作
フィルタリング設定にマッチしたときにパケットを破棄するか通過させるかを選択します。

入力が終わりましたら、「実行」をクリックして設定完了です。
設定をおこなうと設定内容が一覧表示されます。

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

一覧表示からは、設定の編集・削除をおこなう事ができます。

○編集
編集したい設定の行にある「編集」ボタンをクリックしてください。
「インタフェース」と「動作」の設定が変更できます。

○削除
削除したい設定の行にある「削除」ボタンをクリックしてください。
削除確認画面が表示されます。「実行」ボタンをクリックすると設定の削除がおこなわれます。

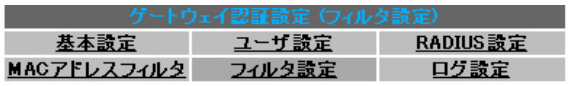
第 30 章 ゲートウェイ認証機能

Ⅰ．ゲートウェイ認証機能の設定

◆フィルタ設定

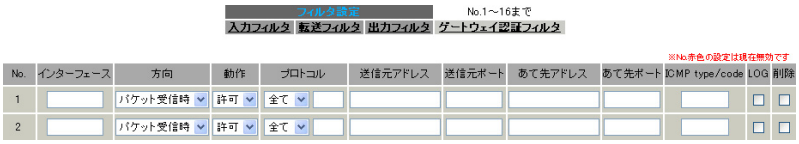
ゲートウェイ認証機能を有効にすると、外部との通信は認証が必要となりますが、フィルタ設定によって認証を必要とせずに通信可能にできます。
「特定のポートだけは常に通信できるようにしたい」といった場合に設定します。

設定画面「フィルタ設定」をクリックします。



「フィルタ設定」のゲートウェイ認証設定フィルタ設定画面にて設定して下さい。

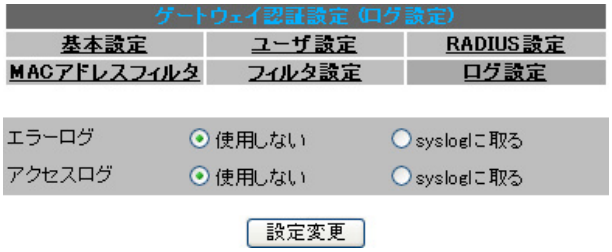
上記のメッセージが表示されるので、リンクをクリックしてください。
Web 設定画面「フィルタ設定」の「ゲートウェイ認証フィルタ」設定画面に移ります。



ここで設定した IP アドレスやポートについては、ゲートウェイ認証機能によらず、通信可能になります。
設定方法については「第 25 章 パケットフィルタリング機能」をご参照ください。

◆ログ設定

ゲートウェイ認証機能のログを本装置のシステムログに出力できます。



ログを取得するかどうかを選択します。

○エラーログ
ゲートウェイ認証時のログインエラーを出力します。

＜エラーログの表示例＞

```
Apr  7 17:04:45 localhost httpd[21529]:
[error] [client 192.168.0.1] user abc: au-
thentication failure for "/": password mis-
match
```

○アクセスログ
ゲートウェイ認証時のアクセスログを出力します。

＜アクセスログの表示例＞

```
Apr  7 17:04:49 localhost authgw: 192.168.0.1
- abc [07/Apr/2003:17:04:49 +0900] "GET /
HTTP/1.1" 200 353
```

II．ゲートウェイ認証下のアクセス方法

ホストからのアクセス方法

1 ホストから本装置にアクセスします。

以下の形式でアドレスを指定してアクセスします。

http://<本装置の IP アドレス>/login.cgi

2 認証画面がポップアップしますので、通知されているユーザ ID とパスワードを入力します。

3 認証に成功すると以下のメッセージが表示され、本装置を経由して外部にアクセスできるようになります。

<認証成功時の表示例>

```
You can connect to the External Network
(abc@192.168.0.1).

Date: Mon Apr 7 10:06:51 2003
```

設定画面へのアクセスについて

ゲートウェイ認証機能を使用していて認証をおこなっていなくても、本装置の設定画面にはアクセスすることができます。
アクセス方法は、通常と同じです。

RADIUS 設定について

認証方法を「RADIUS サーバ」に選択した場合、XR-410 は RADIUS サーバに対して認証要求のみを送信します。

RADIUS サーバへの要求はタイムアウトが 5 秒、リトライが最大 3 回です。
プライマリサーバから応答がない場合は、セカンダリサーバに要求を送信します。

認証について

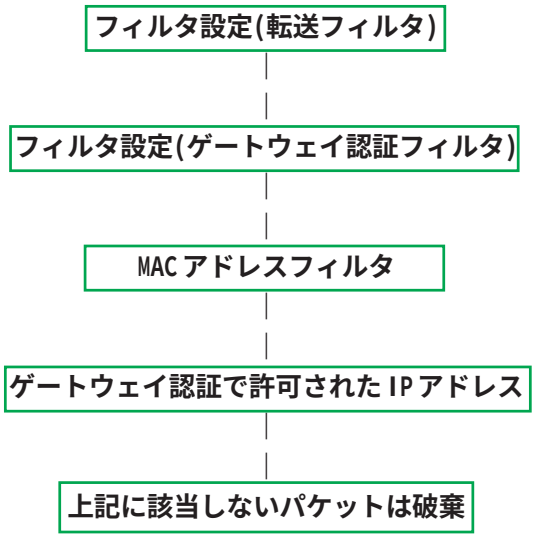
認証方法が「ローカル」、「RADIUS サーバ」のどちらの場合でも、クライアント - 本装置間の認証には、HTTP Basic 認証が用いられます。

また、「RADIUS サーバ」を使用する場合、本装置 - RADIUS サーバ間は User-Password を用いた認証 (PAP)がおこなわれます。

III. ゲートウェイ認証の制御方法について

ゲートウェイ認証機能はパケットフィルタの一種で、認証で許可されたユーザー(ホスト)の IP アドレスを送信元 / あて先に持つ転送パケットのみを通過させます。
制御は、転送フィルタ設定の最後でおこなわれます。

フィルタリング制御の順番は以下の通りです。



ゲートウェイ認証機能を使わない場合は、通常の「転送フィルタ」のみ有効となります。

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

ゲートウェイ認証機能を使用する場合は、「転送フィルタ」には何も設定せずに運用してください。

第 31 章

ネットワークテスト

ネットワークテスト

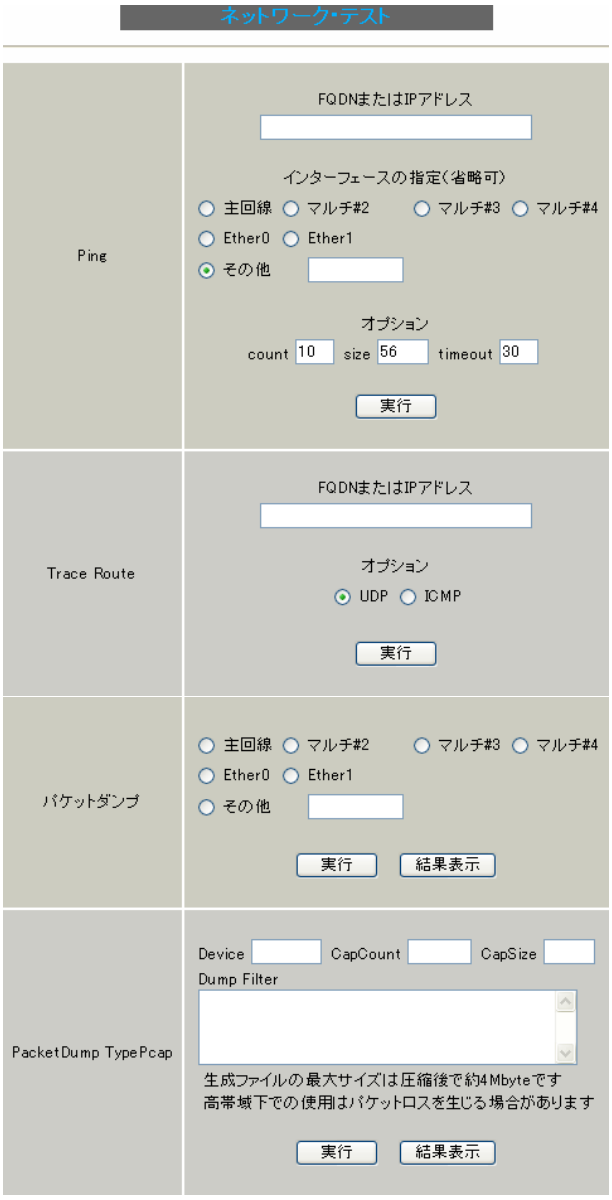
XR-410 の運用時において、ネットワークテストをおこなうことができます。
ネットワークのトラブルシューティングに有効です。

以下の 3 つのテストができます。

- **Ping テスト**
- **Trace Route テスト**
- **パケットダンプの取得**

実行方法

Web 設定画面「ネットワークテスト」をクリックして、以下の画面でテストを実行します。



[Ping テスト]

指定した相手に本装置から Ping を発信します。

◯ FQDN または IP アドレス
FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

◯インターフェースの指定（省略可）
ping パケットを送信するインタフェースを選択できます。省略することも可能です。

◯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=48.5 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 テスト]

指定した宛先までに経由するルータの情報を表示します。

○ FQDN または IP アドレス

FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力します。

○オプション

・UDP

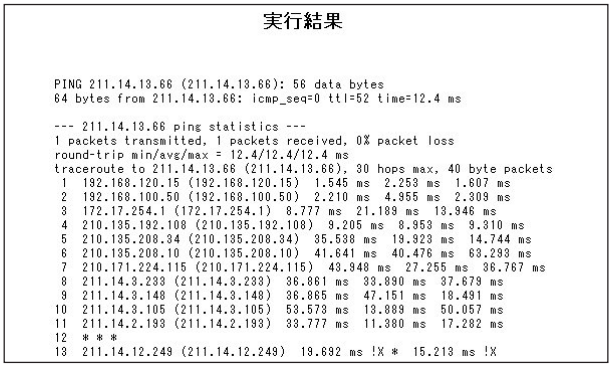
UDP パケットを使用する場合に指定します。
初期設定は UDP です。

・ICMP

ICMP パケットを使用する場合に指定します。

入力が終わりましたら「実行」をクリックします。

実行結果例



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

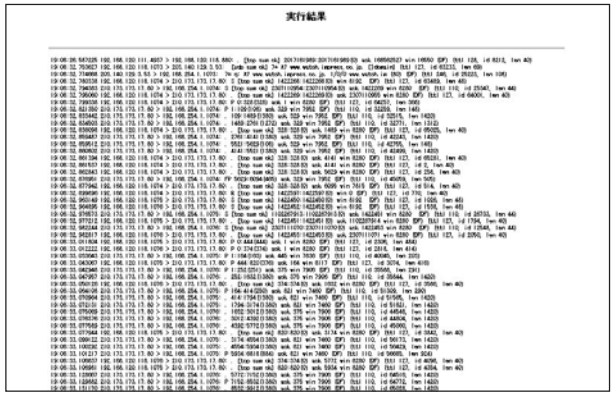
[パケットダンプテスト]

パケットのダンプを取得できます。
ダンプを取得したいインタフェースを選択して「実行」をクリックします。

インタフェースについては「その他」を選択し、直接インタフェースを指定することもできます。
その場合はインタフェース名(「gre1」や「ipsec0」など)を指定してください。

その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例



「結果表示」をクリックするたびに、表示結果が更新されます。
パケットダンプの表示は、最大で 100 パケット分までです。100 パケット分を超えると、古いものから順に表示されなくなります。

ネットワークテスト

[PacketDump TypePcap テスト]
拡張版パケットダンプ取得機能です。
指定したインタフェースで、指定した数のパケットダンプを取得できます。

○ Device
パケットダンプを実行する、本装置のインタフェース名を設定します。インタフェース名は本書**「付録 A インタフェース名一覧」**をご参照ください。

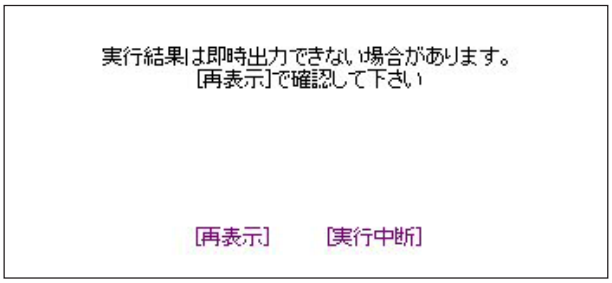
○ CapCount
パケットダンプの取得数を指定します。
1-999999 の間で指定します。

○ CapSize
1パケットごとのダンプデータの最大サイズを指定できます。単位は“ byte ”です。
たとえば 128 と設定すると、128 バイト以上の長さのパケットでも 128 バイト分だけをダンプします。大きなサイズでダンプするときは、本装置への負荷が増加することがあります。また記録できるダンプ数も減少します。

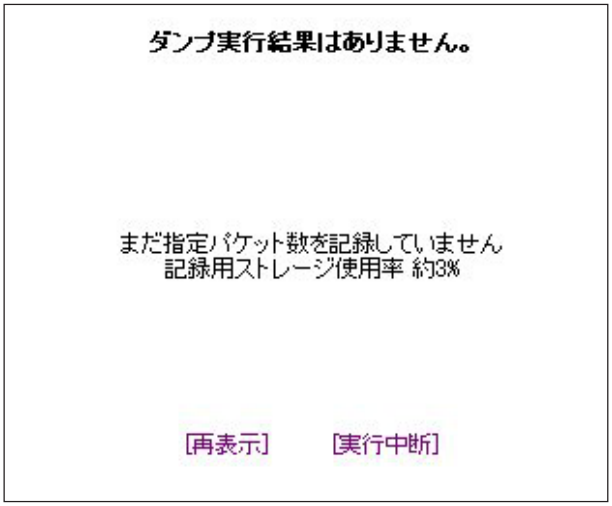
○ Dump Filter
ここに文字列を指定して、それに合致するダンプ内容のみを取得できます。空白・大小文字も判別します。一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したパケットダンプ内容のみ抽出して記録します。

入力後、「実行」ボタンでパケットダンプを開始します。

パケットダンプを開始したときの画面表示

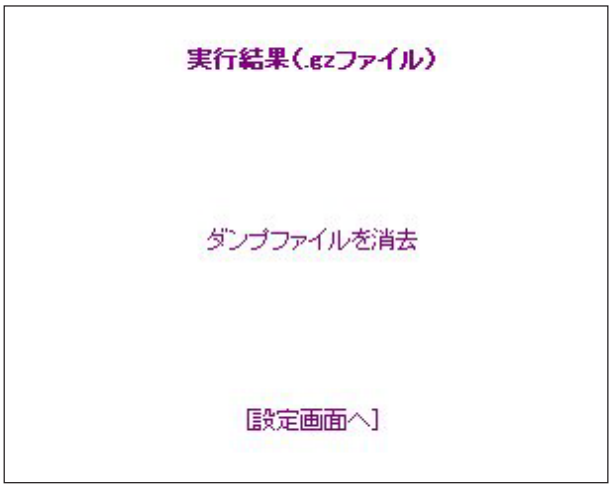


また、パケットダンプ実行中に「再表示」ボタンをクリックすると、下記のような画面が表示されます。



ネットワークテスト

パケットダンプが実行終了したときの画面



「Count」で指定した数のパケットダンプを取得したとき、「実行中断」ボタンをクリックしたとき、またはパケットダンプ取得終了後に「結果表示」をクリックしたとき、上記の画面が表示されます。

「実行結果(.gz ファイル)」リンクから、パケットダンプ結果を圧縮したファイルをローカルホストに保存してください。

ローカルホスト上で解凍してできたファイルは、Ethereal で閲覧することができます。

「ダンプファイルを消去」をクリックすると、本装置に記録されているダンプファイルを消去します。

PacketDump TypePcap の注意点

・取得したパケットダンプ結果は、libcap 形式で gzip 圧縮して保存されます。

・取得できるデータサイズは gzip 圧縮された状態で最大約 4MB です。

・本装置上には、パケットダンプ結果を 1 つだけ記録しておけます。パケットダンプ結果を消去せずに PacketDump TypePcap を再実行して実行結果ファイルを作成したときは、それまでに記録されていたパケットダンプ結果に上書きされます。

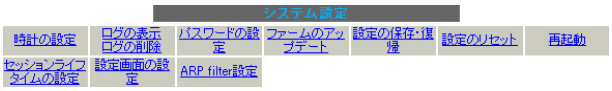
本装置のインタフェース名については、本書の**「付録 A インタフェース名一覧」**をご参照ください。

第 32 章

各種システム設定

各種システム設定

「システム設定」ページでは、XR-410 の運用に関する制御をおこないます。
下記の項目に関して設定・制御が可能です。



- 時計の設定
- ログの表示 / 削除
- パスワード設定
- ファームウェアアップデート
- 設定の保存・復帰
- 設定のリセット
- 本体の再起動
- セッションライフタイムの設定
- 設定画面の設定
- ARP filter 設定

設定・実行方法

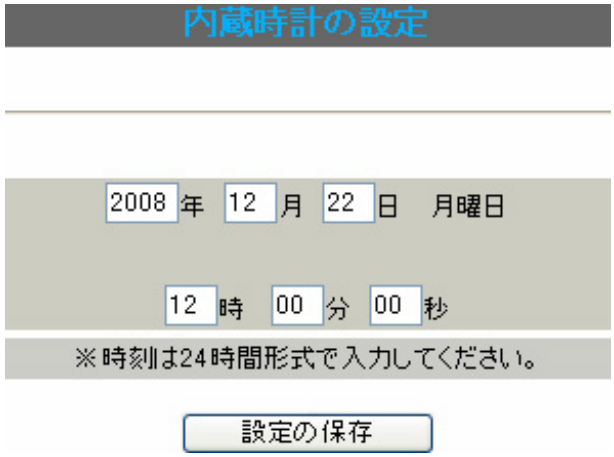
Web 設定画面「システム設定」をクリックします。
各項目のページへは、設定画面上部のリンクをクリックして移動します。

◆時計の設定

XR-410 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。

各種システム設定

◆ログの表示

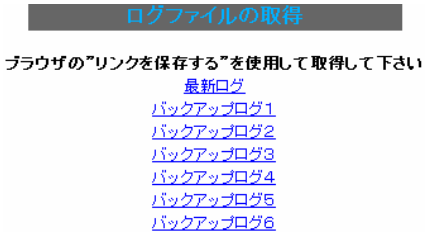
本装置のログが全てここで表示されます。

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。

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。



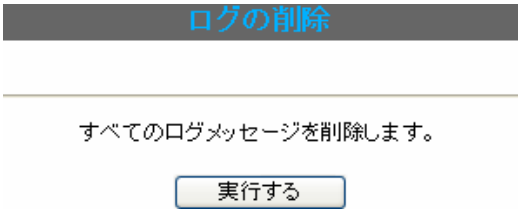
「攻撃検出機能」を使用している場合は、そのログも併せてここで表示されます。
設定方法は「第 17 章 攻撃検出機能」をご参照ください。

◆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。

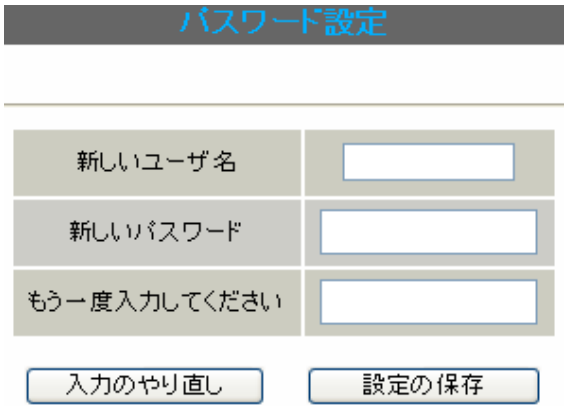
各種システム設定

◆パスワードの設定

XR-410の設定画面にログインする際のユーザ名、パスワードを変更します。
ルータ自身のセキュリティのためにパスワードを変更されることを推奨します。

設定方法

「パスワードの設定」をクリックして設定画面を開きます。



ユーザ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。

各種システム設定

◆ファームウェアのアップデート

XR-410 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

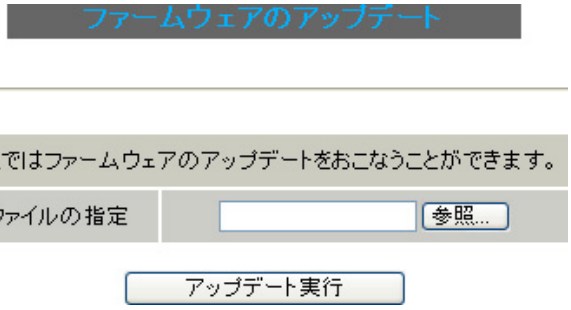
XR-410/TX2
http://www.centurysys.co.jp/support/XR410TX2.html

XR-410/TX2DES
http://www.centurysys.co.jp/support/XR410TX2DES.html

XR-410/TX4
http://www.centurysys.co.jp/support/xr410tx4.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。

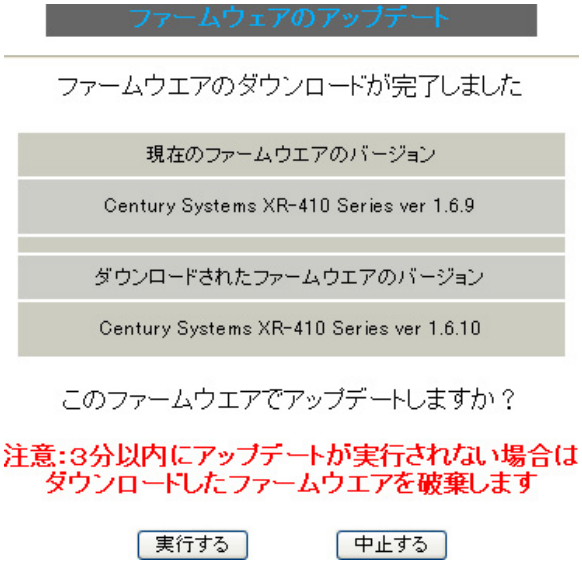


2 「参照」ボタンを押して、弊社ホームページからダウンロードしてきたファームウェアファイルを選択し、「アップデート実行」ボタンを押してください。

3 その後、ファームウェアを本装置に転送します。

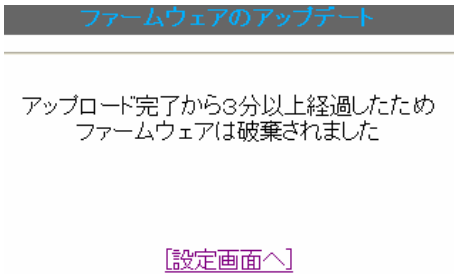
転送が終わるまではしばらく時間がかかります。
転送完了後に、右上のようなアップデートの確認画面が表示されますので、バージョン等が正しければ「実行する」をクリックしてください。

**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。**



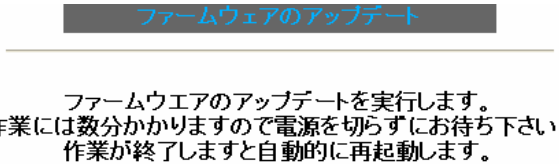
（画面は XR-410/TX2 の表示例です）

上記画面が表示されたままで 3 分間経過した後に「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、アップデートが実行されません。



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、本体前面の「7 セグメント LED」が、アップデート実行状態であることを示す表示をします。
LED 表示の詳細は「第 1 章 XR-410 の概要　II . 各部の名称と機能　◆製品前面」をご参照ください。

ファームウェアの書き換え後に本装置が自動的に再起動されて、アップデートの完了です。

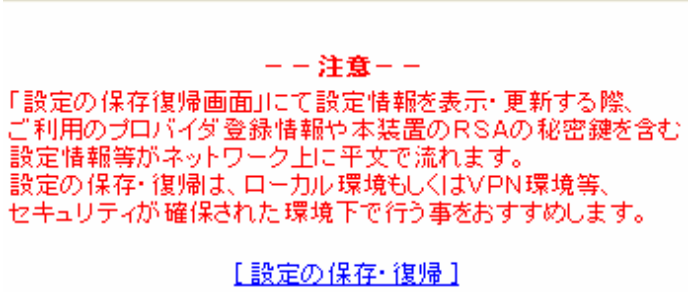
各種システム設定

◆設定の保存と復帰

本装置の設定の保存および、保存した設定の復帰をおこないます。

実行方法

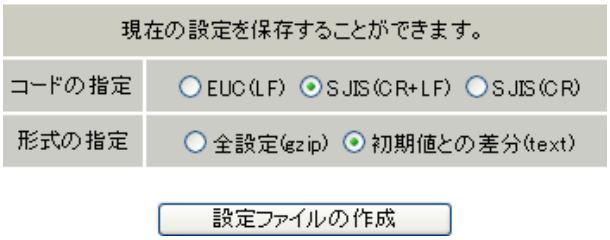
「設定の保存・復帰」をクリックして画面を開きます。



上記のような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します。



○コードの指定

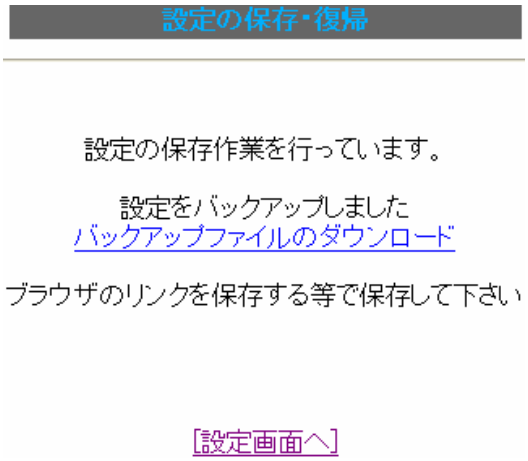
「EUC(LF)」「SJIS(CR+LF)」「SJIS(CR)」のいずれかを選択します。

○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。

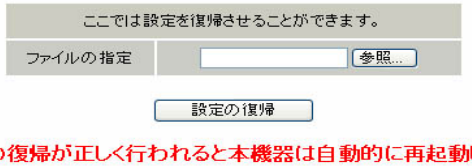
選択後は「設定ファイルの作成」をクリックします。
クリックすると以下のメッセージが表示されます。



「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。

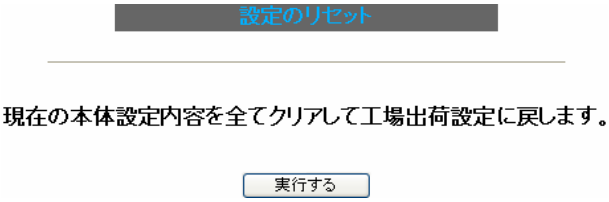
各種システム設定

◆設定のリセット

XR-410 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。

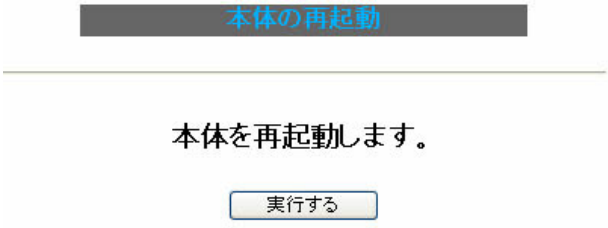
設定のリセットにより全ての設定が失われますので、念のために「設定のバックアップ」を実行しておくようにしてください。

◆本体再起動

XR-410 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。

各種システム設定

◆セッションライフタイムの設定

本装置内部では、NAT/IP マスカレードの通信を高速化するために、セッション生成時に NAT/IP マスカレードのセッション情報を記憶し、一定時間保存しています。
ここでは、そのライフタイムを設定します。

設定方法

「セッションライフタイムの設定」をクリックして画面を開きます。

○ UDP
UDP セッションのライフタイムを設定します。
単位は秒です。0 ～ 8640000 の間で設定します。
初期設定は 30 秒です。

○ UDP stream
UDP streamセッションのライフタイムを設定します。
単位は秒です。0 ～ 8640000 の間で設定します。
初期設定は 180 秒です。

○ TCP
TCP セッションのライフタイムを設定します。単位は秒です。0 ～ 8640000 の間で設定します。
初期設定は 3600 秒です。

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

なお、XR 内部で保持しているセッション数は、周期的に syslog に表示することができます。
詳しくは「第 15 章 SYSLOG 機能」のシステムメッセージの項を参照してください。

それぞれの項目で“ 0 ”を設定すると、初期値で動作します。

「設定の保存」ボタンをクリックすると、設定が保存されます。設定内容はすぐに反映されます。

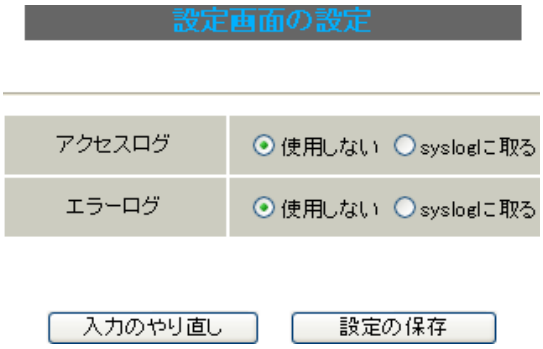
各種システム設定

◆設定画面の設定

WEB設定画面へのアクセスログについての設定をします。

設定方法

「設定画面の設定」をクリックして画面を開きます。



○アクセスログ
○(アクセス時の)エラーログ
取得するかどうかを指定します。

「設定の保存」をクリックします。

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

◆ARP filter 設定

ARP filter設定をおこないます。

設定方法

「ARP filter設定」をクリックして画面を開きます。

ARP filterを「無効」にするか、「有効」にするかを選択します。

有効にすると、同一IPアドレスのARPを複数のインタフェースで受信したときに、受信したそれぞれのインタフェースからARP応答を出さないようにできます。

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。

第 33 章

情報表示

本体情報の表示

本体の機器情報を表示します。
以下の項目を表示します。

- **ファームウェアバージョン情報**
  現在のファームウェアバージョンを確認できます。

- **インターフェース情報**
  各インターフェースの IP アドレスや MAC アドレスなどです。
  PPP/PPPoE や IPsec 論理インタフェースもここに表示されます。

- **リンク情報**
  本装置の各 Ethernet ポートのリンク状態および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。

- **DHCP クライアント情報**
  DHCP クライアントとして設定しているインタフェースがサーバから取得した IP アドレス等の情報を表示します。

実行方法

Web 設定画面「情報表示」をクリックすると、新しいウィンドウが開いて本体情報表示されます。

（画面は XR-410/TX2 での表示例）

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 34 章

詳細情報表示

各種情報の表示

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

- **ルーティング情報**
  本装置のルーティングテーブル、ルーティングテーブルの内部情報、ルートキャッシュの情報、デフォルトゲートウェイ情報が表示できます。
  このうち、ルーティングテーブルの内部情報とルートキャッシュの情報はここでのみ表示できます。
- **OSPF 情報**
- **RIP 情報**
- **IPsec サーバ情報**
- **DHCP サーバ情報**
- **NTP サービス情報**
- **VRRP サービス情報**
- **QoS 情報**

実行方法

Web 設定画面「詳細情報表示」をクリックすると、次の画面が表示されます。

左列の機能名をクリックすると、新しいウィンドウが開いて、その機能に関する情報がまとめて表示されます。

右列の小項目名をクリックした場合は、その小項目のみの情報が表示されます。
なお、「OSPF のインターフェース情報」および QoS の各情報については、ボックス内に表示したいインタ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 35 章

運用管理設定

Ⅰ．一時的に工場出荷設定に戻す方法

XR-410 の背面にある「INIT スイッチ」を使用して、本装置の設定を**一時的に工場出荷設定に戻す**ことができます。

1 本装置を電源 OFF の状態にします。

2 本体背面にある「INIT」スイッチを押します。

3 「INIT」スイッチを押したままの状態で電源を投入し、電源投入後も 5 秒ほど「INIT」スイッチを押しつづけます。

以上の動作で本装置は工場出荷時の設定で再起動します。

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

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

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。

II．携帯電話による制御

本装置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、EZweb 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

これらの機能を利用する際は、パケットフィルタリング設定にて、WAN側からの設定変更を可能にする必要があります。
WAN側から本装置の設定変更を許可するフィルタ設定については「第 25 章 パケットフィルタリング機能」をご覧ください。

i モード端末および、EZweb 端末から、本装置の操作画面にアクセスする場合は、以下の URL を入力してください。

<i モード端末からアクセスする場合>

http:// 本装置の IP アドレス(WAN側):880/i/

<EZweb 端末からアクセスする場合>

http:// 本装置の IP アドレス(WAN 側):880/ez/index.hdml

指定した URL へアクセスすると、認証画面が表示されますので、ユーザー名とパスワードを入力してログインしてください。

ログインすると、本装置の操作メニューが表示されます。

○フィルタ状態
本装置の現在の状態を表示します。

○ 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-410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。

○ 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 モード端末および、EZweb 端末から本装置へアクセスするには、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-410 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-410 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、「アドレス変更お知らせメール」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

以下は、i モード端末から本装置へアクセスした場合の表示例です。

1 携帯電話端末から XR-410 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 ユーザー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
- 仮想インターフェース機能
- ネットワークテスト

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

表左：インタフェース名
表右：実際の接続デバイス

＜XR-410/TX2＞
＜XR-410/TX2DES＞

eth0	Ether0ポート
eth1	Ether1ポート
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
gre<n>	gre(<n>は設定番号)
eth0:<n>	eth0上の仮想インタフェース(<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インタフェース(<n>は仮想IF番号)

＜XR-410/TX4＞

eth0	Ether0ポート
eth1	Ether1ポート
eth2	Ether2ポート
eth3	Ether3ポート
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
ipsec7	eth2上のipsec
ipsec8	eth3上のipsec
gre<n>	gre(<n>は設定番号)
eth0:<n>	eth0上の仮想インタフェース(<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インタフェース(<n>は仮想IF番号)
eth2:<n>	eth2上の仮想インタフェース(<n>は仮想IF番号)
eth3:<n>	eth3上の仮想インタフェース(<n>は仮想IF番号)

付録 B

工場出荷設定一覧

付録 B

工場出荷設定一覧

IPアドレス設定	IPアドレス/サブネットマスク値
Ether0ポート	192.168.0.254/255.255.255.0
Ether1ポート	192.168.1.254/255.255.255.0
Ether2ポート(※ XR-410/TX4のみ)	192.168.2.254/255.255.255.0
Ether3ポート(※ XR-410/TX4のみ)	192.168.3.254/255.255.255.0

DHCPクライアント機能	無効
IPマスカレード機能	無効
ステートフルパケットインスペクション機能	Ether0ポート　無効 Ether0以外のポート　有効
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
SYSLOG機能	有効
帯域制御（QoS）機能	無効
攻撃検出機能	無効
SNMPエージェント機能	無効
NTP機能	無効
VRRP機能	無効
アクセスサーバ機能	無効
スタティックルート設定	設定なし
ソースルーティング設定	設定なし
NAT機能	設定なし
パケットフィルタリング機能	NetBIOSからの漏洩を防止するフィルタ設定 （入力・転送フィルタ設定） 外部からのUPnPパケットを遮断する設定 （入力・転送フィルタ設定）
ネットワークイベント機能	無効
仮想インターフェース機能	設定なし
GRE機能	無効
パケット分類機能	設定なし
ゲートウェイ認証機能	無効

設定画面ログインID	admin
設定画面ログインパスワード	admin

付録 C

サポートについて

付録 C

サポートについて

◆本製品に関してのサポートは、ユーザー登録をされたお客様に限らせていただきます。
必ずユーザー登録していただきますよう、お願いいたします。

◆サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。

・サポートデスク
e-mail　：support@centurysys.co.jp
電話　：0422-37-8926
FAX　：0422-55-3373
受付時間　：10:00～17:00　(土日祝祭日、および弊社の定める休日を除きます)
・ホームページ　http://www.centurysys.co.jp/

◆故障と思われる場合は
製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。
事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

◆ご連絡をいただく前に
スムーズなユーザーサポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。

・ファームウェアのバージョンとＭＡＣアドレス
(バージョンの確認方法は「第 33 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-410 の設定内容、およびコンピュータの IP 設定
・可能であれば、「設定のバックアップファイル」をお送りください。

◆サポート情報
弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。
また製品の FAQ も掲載しておりますので、是非ご覧ください。
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ご使用の製品名（XR-410/TX2、XR-410/TX2DES、XR-410/TX4）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-410/TX シリーズ ユーザーズガイド　v1.6.10 対応版
2008 年 12 月版
発行 センチュリー・システムズ株式会社