
Internet VPN 対応 BROADBAND GATE

FutureNet XR-440/C

ユーザーズガイド

Ver1.7.7 対応版



目次

はじめに	6
ご使用にあたって	7
パッケージの内容物の確認	10
第1章 XR-440 の概要	11
I. XR-440 の特長	12
II. 各部の名称と機能	14
III. 動作環境	16
第2章 XR-440 の設置	17
XR-440 の設置	18
第3章 コンピュータのネットワーク設定	19
I. Windows 95/98/Me のネットワーク設定	20
II. Windows 2000 のネットワーク設定	21
III. Windows XP のネットワーク設定	22
IV. Windows Vista のネットワーク設定	23
V. Macintosh のネットワーク設定	24
VI. IP アドレスの確認と再取得	25
第4章 設定画面へのログイン	26
設定画面へのログイン方法	27
第5章 インタフェース設定	28
I. Ethernet ポートの設定	29
II. VLAN タギングの設定	31
III. その他の設定	32
第6章 PPPoE 設定	36
I. PPPoE の接続先設定	37
II. PPPoE の接続設定と回線の接続 / 切断	39
III. その他の接続設定	41
IV. 副回線とバックアップ回線	42
V. PPPoE 特殊オプション設定	46
第7章 ダイアルアップ接続	47
I. RS-232C ポートとアナログモデム / TA の接続	48
II. BRI ポートと TA/DSU の接続	49
III. 接続先設定	50
IV. ダイアルアップの接続と切断	52
V. 副回線接続とバックアップ回線接続	54
VI. 回線への自動発信の防止について	55
第8章 専用線接続	56
I. BRI ポートと TA/DSU の接続	57
II. 専用線設定	58
III. 専用線の接続と切断	59
第9章 複数アカウント同時接続設定	61
複数アカウント同時接続の設定	62
第10章 各種サービスの設定	68
各種サービス設定	69
第11章 DNS リレー / キャッシュ機能	70
DNS リレー / キャッシュ機能の設定	71
第12章 DHCP サーバ / リレー機能	72
I. DHCP サーバ機能の設定	73
II. DHCP サーバ機能の設定例	74
III. IP アドレス固定割り当て設定	75

第 13 章 IPsec 機能	76
I. XR-440 の IPsec 機能について	77
II. IPsec 設定の流れ	78
III. IPsec 設定	79
IV. IPsec Keep-Alive 設定	88
V. 「X.509 デジタル証明書」を用いた電子認証	91
VI. IPsec 通信時のパケットフィルタ設定	93
VII. IPsec 設定例 1 (センター／拠点間の 1 対 1 接続)	94
VIII. IPsec 設定例 2 (センター／拠点間の 2 対 1 接続)	98
IX. IPsec がつながらないとき	105
第 14 章 UPnP 機能	108
I. UPnP 機能 の設定	109
II. UPnP とパケットフィルタ設定	111
第 15 章 ダイナミックルーティング (RIP/OSPF/BGP4)	112
I. ダイナミックルーティング機能	113
II. RIP の設定	114
III. OSPF の設定	115
IV. BGP4 の設定	122
第 16 章 PPPoE to L2TP	130
PPPoE to L2TP 機能について	131
第 17 章 SYSLOG サービス	133
syslog 機能の設定	134
第 18 章 攻撃検出機能	137
攻撃検出機能の設定	138
第 19 章 SNMP エージェント機能	139
SNMP エージェント機能の設定	140
第 20 章 NTP サービス	142
NTP サービスの設定方法	143
第 21 章 VRRP サービス	145
I. VRRP の設定方法	146
II. VRRP の設定例	147
第 22 章 アクセスサーバ機能	148
I. アクセスサーバ機能について	149
II. XR-440 とアナログモデム /TA の接続	150
III. BRI ポートを使った XR-440 と TA/DSU の接続	151
IV. アクセスサーバ機能の設定	152
第 23 章 スタティックルーティング	154
スタティックルーティング設定	155
第 24 章 ソースルーティング機能	157
ソースルーティング設定	158
第 25 章 NAT 機能	159
I. XR-440 の NAT 機能について	160
II. バーチャルサーバ設定	161
III. 送信元 NAT 設定	162
IV. バーチャルサーバの設定例	163
◆ WWW サーバを公開する際の NAT 設定例	163
◆ FTP サーバを公開する際の NAT 設定例	163
◆ PPTP サーバを公開する際の NAT 設定例	164
◆ 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)	165

V. 送信元 NAT の設定例	166
補足：ポート番号について	167
第 26 章 パケットフィルタリング機能	168
I. 機能の概要	169
II. XR-440 のフィルタリング機能について	170
III. パケットフィルタリングの設定	171
IV. パケットフィルタリングの設定例	173
◆インターネットから LAN へのアクセスを破棄する設定	173
◆WWW サーバを公開する際のフィルタ設定例	174
◆FTP サーバを公開する際のフィルタ設定例	174
◆WWW、FTP、メール、DNS サーバを公開する際のフィルタ設定例	175
◆NetBIOS パケットが外部へ出るのを防止するフィルタ設定	176
◆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)	176
◆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)	177
◆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	177
◆PPTP を通すためのフィルタ設定	178
V. 外部から設定画面にアクセスさせる設定	179
補足：NAT とフィルタの処理順序について	180
補足：ポート番号について	181
補足：フィルタのログ出力内容について	182
第 27 章 スケジュール設定	183
スケジュール機能の設定方法	184
第 28 章 ネットワークイベント機能	186
I. 機能の概要	187
II. 各トリガテーブルの設定	189
III. 実行イベントテーブルの設定	191
IV. 実行イベントのオプション設定	192
V. ステータスの表示	193
第 29 章 仮想インタフェース機能	194
仮想インタフェース機能の設定	195
第 30 章 GRE 設定	196
GRE の設定	197
第 31 章 QoS 機能	199
I. QoS について	200
II. QoS 機能の各設定画面について	204
III. 各キューイング方式の設定手順について	205
IV. 各設定画面での設定方法について	206
V. ステータスの表示	213
VI. 設定の編集・削除方法	214
VII. ステータス情報の表示例	215
VIII. クラスの階層構造について	219
IX. TOS について	220
X. DSCP について	222
第 32 章 ネットワークテスト	223
ネットワークテスト	224
第 33 章 システム設定	227
システム設定	228
◆時計の設定	228
◆ログの表示	229

◆ログの削除	229
◆パスワードの設定	230
◆ファームウェアのアップデート	231
◆設定の保存と復帰	232
◆設定のリセット	233
◆本体再起動	233
◆セッションライフタイムの設定	234
◆設定画面の設定	235
◆ISDN 設定	235
◆オプション CF カード	236
◆ARP filter 設定	237
第 34 章 情報表示	238
本体情報の表示	239
第 35 章 詳細情報表示	240
各種情報の表示	241
第 36 章 運用管理設定	243
INIT ボタンの操作	244
◆本装置の設定を初期化する	244
◆C F カードの設定で起動する	244
補足：バージョンアップ後の設定内容について	244
携帯電話による制御	245
付録 A インタフェース名について	247
付録 B 工場出荷設定一覧	249
付録 C サポートについて	251

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下さい。

◆商標の表示

- ☐ 「BROADBAND GATE」はセンチュリー・システムズ株式会社の登録商標です。
 - ☐ 「FutureNet」はセンチュリー・システムズ株式会社の商標です。
 - ☐ 下記製品名等は米国 Microsoft Corporation の登録商標です。
Microsoft、Windows、Windows 95、Windows 98、Windows NT4.0
Windows 2000、Windows Me、Windows XP、Windows Vista
 - ☐ Macintosh、Mac OS X は、アップル社の登録商標です。
- その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

ご使用にあたって

本製品を安全にお使いいただくために、まず以下の注意事項を必ずお読み下さい。

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

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



危険

この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う危険が差し迫って生じることが想定される内容を示しています。



警告

この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。



注意

この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。

次の絵表示の区分は、お守りいただく内容を説明しています。



このような絵表示は、してはいけない「禁止」を意味するものです。それぞれに具体的な禁止内容が書かれています。



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



危険



必ず本体に付属している電源ケーブルをご使用ください。



使用温度範囲は0℃～40℃です。この温度範囲以外では使用しないでください。



ストーブのそばなど高温の場所で使用したり、放置しないでください。



火の中に投入したり、加熱したりしないでください。



製品の間隙から針金などの異物を挿入しないでください。

ご使用にあたって

警告

-  万一、異物(金属片・水・液体)が製品の内部に入った場合は、まず電源を外し、お買い上げの販売店にご連絡下さい。そのまま使用すると火災の原因となります。
-  万一、発熱していたり、煙が出ている、変な臭いがするなどの異常状態のまま使用すると、火災の原因となります。すぐに電源を外し、お買い上げの販売店にご連絡下さい。
-  本体を分解、改造しないでください。けがや感電などの事故の原因となります。
-  本体または電源ケーブルを直射日光の当たる場所や、調理場や風呂場など湿気が多い場所では絶対に使用しないでください。火災・感電・故障の原因となります。
-  電源ケーブルの電源プラグについたほこりはふき取ってください。火災の原因になります。
-  濡れた手で電源ケーブル、コンセントに触れないでください。感電の原因となります。
-  電源ケーブルのプラグにドライバなどの金属が触れないようにしてください。火災・感電・故障の原因となります。
-  AC100V の家庭用電源以外では絶対に使用しないでください。火災・感電・故障の原因となります。

ご使用にあたって

注意

-  湿気やほこりの多いところ、または高温となるところには保管しないでください。故障の原因となります。
-  乳幼児の手の届かないところに保管してください。けがなどの原因となります。
-  長期間使用しないときには、電源ケーブルをコンセントおよび本体から外してください。
-  電源ケーブルの上に重いものを乗せたり、ケーブルを改造したりしないで下さい。また、電源ケーブルを無理に曲げたりしないでください。火災・感電・故障の原因となることがあります。
-  電源ケーブルは必ず電源プラグを持って抜いてください。ケーブルを引っ張ると、ケーブルに傷が付き、火災・感電・故障の原因となることがあります。
-  近くに雷が発生したときには、電源ケーブルをコンセントから抜いて、ご使用をお控え下さい。落雷が火災・感電・故障の原因となることがあります。
-  本製品に乗らないでください。本体が壊れて、けがの原因となることがあります。
-  高出力のアンテナや高圧線などが近くにある環境下では、正常な通信ができない場合があります。

パッケージの内容物の確認

本製品のパッケージには以下のものが同梱されております。本製品をお使いいただく前に、内容物がすべて揃っているかご確認ください。万が一不足がありましたら、お買いあげいただいた店舗または弊社サポートデスクまでご連絡ください。

XR-440/C 本体	1 台
はじめにお読みください	1 部
UTP ケーブル（ストレート、1m）	1 本
海外使用禁止シート	1 部
保証書	1 部

第1章

XR-440 の概要

第1章 XR-440 の概要

I. XR-440 の特長

◆高速ネットワーク環境に余裕で対応

XR-440/C(以下、XR-440)は通常のルーティングスピードおよび PPPoE 接続時に最大 100Mbps の通信速度を実現していますので、高速 ADSL や FTTH 等の高速インターネット接続や LAN 環境の構成に十分な性能を備えています。

◆PPPoE クライアント機能

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

◆unnumbered 接続対応

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

◆DHCP クライアント / サーバ機能

DHCP クライアント機能によって、IP アドレスの自動割り当てをおこなう CATV インターネット接続サービスでも利用できます。また、LAN 側ポートでは DHCP サーバ機能を搭載しており、LAN 側の PC に自動的に IP アドレス等の TCP/IP 設定を行なえます。

◆NAT/IP マスカレード機能

IP マスカレード機能を搭載していることにより、グローバルアドレスが1つだけしか利用できない場合でも、複数のコンピュータから同時にインターネットに接続できます。
また静的 NAT 設定によるバーチャルサーバ機能を使えば、プライベート LAN 上のサーバをインターネットに公開することができます。

◆ステートフルパケットインスペクション機能

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

◆静的パケットフィルタリング機能

送信元 / 宛先の 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。

◆ISDN 用 BRI ポートを搭載

XR-440 は「ISDN S/T 点ポート」を搭載しています。これにより本装置から直接、もしくは他の ISDN 機器を接続して ISDN 回線に接続できます。

XR-440 の「副回線接続」を使うと、ISDN 回線回線の接続を緊急時のバックアップ回線として運用することもできます。

◆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。

◆UPnP 機能

UPnP(ユニバーサル・プラグアンドプレイ)機能に対応しています。

第1章 XR-440 の概要

I. XR-440 の特長

◆ IPsec 通信

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

◆ GRE トンネリング機能

仮想的なポイントツーポイントリンクを張って各種プロトコルのパケットを IP トンネルにカプセル化する GRE トンネリングに対応しています。

◆ ダイナミックルーティング機能

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

◆ ソースルート機能

送信元アドレスによってルーティングをおこなうソースルーティングが可能です。

◆ 多彩な冗長化構成が実現可能

VRRP 機能による機器冗長化機能だけではなく、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

帯域制御 / 優先制御をおこなうことができます。これにより、ストリーミングデータを利用する通信などに優先的に帯域を割り当てることが可能になります。

◆ スケジュール機能

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

◆ シリアルポートを搭載

XR-440 は RS-232 ポートを備えています。常時接続のルータとして使いながら、同時にモデムや TA を接続してアクセスサーバや、リモートルータとして利用することができます。また、電話回線経由で XR-440 を遠隔管理することも可能です。

◆ ログ機能

XR-440 のログを取得する事ができ、ブラウザ上でログを確認することが可能です。ログを電子メールで送信することも可能です。また攻撃検出設定を行えば、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

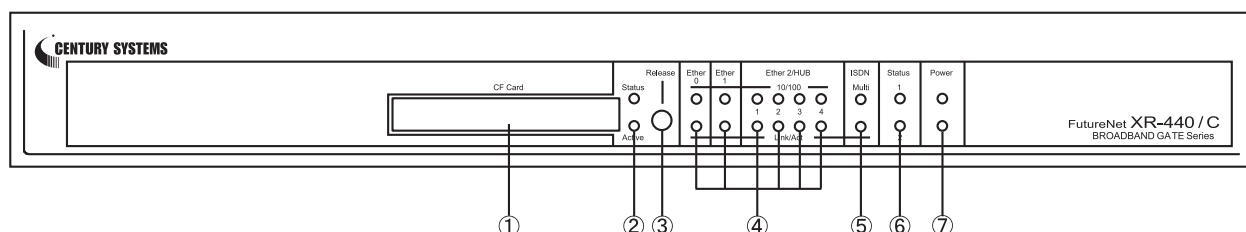
本体の設定内容を一括してファイルにバックアップすることが可能です。
また設定の復元も、ブラウザ上から簡単にできます。

◆ 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



① CFカードスロット

オプションで用意されているCFカードを挿入します。

② STATUS(橙) /ACTIVE(緑)LED

CFカードが挿入され動作しているときに、STATUS(橙)が点灯します。

CFカードをスロットに挿入してカードが使用可能状態になると、ACTIVE(緑)が点灯します。

CFカードが挿入されていないとき、また③の操作をおこないCFカードを安全に取り外せる状態になったときは、STATUS(橙)は消灯します。

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

③ RELEASE ボタン

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

④ Ethernet ポート LED

各Ethernetポートの状態を表示します。

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

⑤ BRI MULTI LED

本装置のBRIポートを使ってISDN接続をしているときに、下段の「LINK」(緑)が点灯します。さらにMP128接続の場合は「MULTI」(橙)が同時に点灯します。

回線切断時は、ランプは消灯しています。

⑥ STATUS 1/2 LED

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

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

ファームウェアのアップデート作業中は、STATUS1(橙)が点滅します。

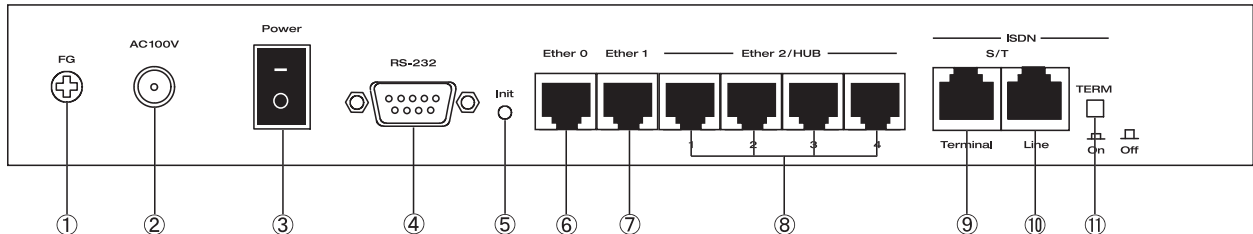
ファームウェアのアップデートに失敗した場合など、本装置が正常に起動できない状態になったときは、STATUS1(橙)とSTATUS2(緑)のどちらも点滅します。

⑦ POWER LED

本装置に電源が投入されているときに点灯(緑)します。

II. 各部の名称と機能

◆製品背面



① FG(アース)端子

保安用接地端子です。必ずアース線を接続してください。

② 電源ケーブル

③ 電源スイッチ

電源をオン/オフするためのスイッチです。

④ RS-232 ポート

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

⑤ INIT ボタン

本装置を一時的に工場出荷時の設定に戻して起動するときに押します。

⑥ Ether0 ポート

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

⑦ Ether1 ポート

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

⑧ Ether2 ポート

4 ポートのスイッチング HUB です。

主に LAN との接続に使用します。イーサネット規格の UTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

⑨ ISDN S/T TERMINAL ポート

このポートと ISDN 機器を ISDN ケーブルで接続します。

⑩ ISDN S/T LINE ポート

このポートと外部 DSU を ISDN ケーブルで接続します。

⑪ TERM. スイッチ

「ISDN S/T 点ポート」接続時の終端抵抗の ON/OFF を切替えます。外部 DSU 機器を接続している場合は、XR-440 を含めていずれか 1 つの機器の終端抵抗を ON にしてください。

III. 動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

- 本製品に接続するコンピュータの全てに、10Base-T または 100Base-TX の LAN ボード / カードがインストールされていること。
- ADSL モデムまたは CATV モデムに、10Base-T または 100Base-TX のインタフェースが搭載されていること。
- 本製品と全てのコンピュータを接続するためのハブやスイッチングハブが用意されていること。
- 本製品と全てのコンピュータを接続するために必要な種類のネットワークケーブルが用意されていること。
- シリアルポートを使う場合は、接続に必要なシリアルケーブルが用意されていること。

◆ソフトウェア環境

- TCP/IP を利用できる OS がインストールされていること。
- 接続されている全てのコンピュータの中で少なくとも 1 台に、Internet Explorer 5.0 以降か Netscape Navigator 6.0 以降がインストールされていること。

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

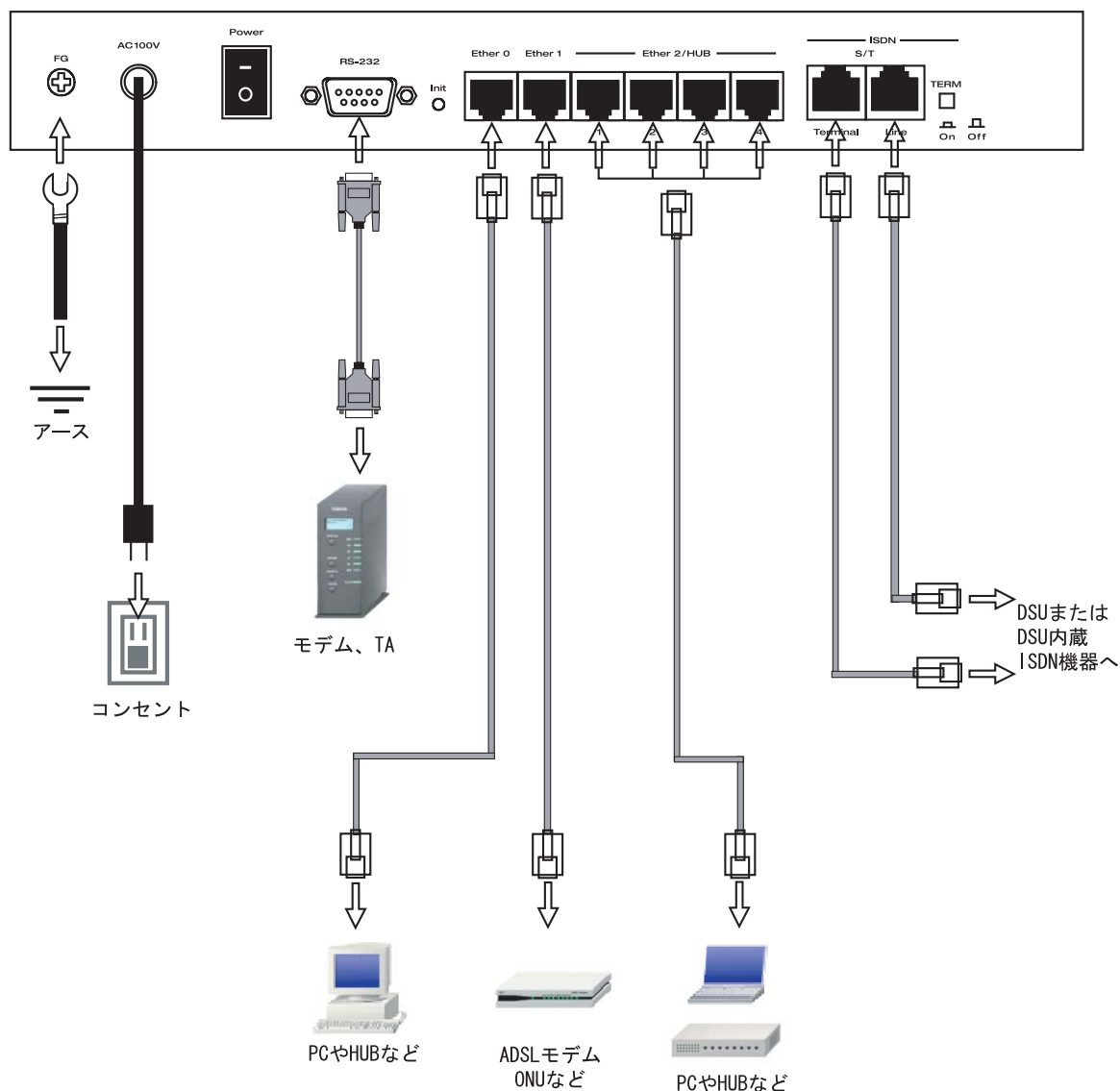
第2章

XR-440 の設置

第2章 XR-440 の設置

XR-440 の設置

XR-440 と xDSL/ ケーブルモデムやコンピュータは、以下の手順で接続してください。



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

2 本装置の背面にある Ether1 ポートと xDSL/ ケーブルモデムや ONU を、LAN ケーブルで接続してください。ケーブルの極性は自動判別します。

3 本装置の設定が工場出荷状態の場合、Ether0 ポートと PC を LAN ケーブルで接続してください。ケーブルの極性は自動判別します。

4 本装置の背面にある Ether2(HUB) ポート(1～4 のいずれかのポート)と PC を LAN ケーブルで接続してください。ケーブルの極性は自動判別します。

5 電源ケーブルとコンセントを接続して下さい。

6 全ての接続が完了しましたら、本装置と各機器の電源を投入してください。

第3章

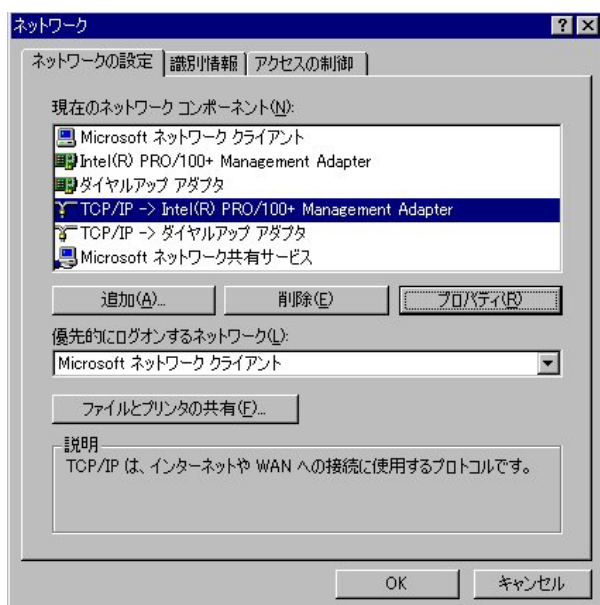
コンピュータのネットワーク設定

第3章 コンピュータのネットワーク設定

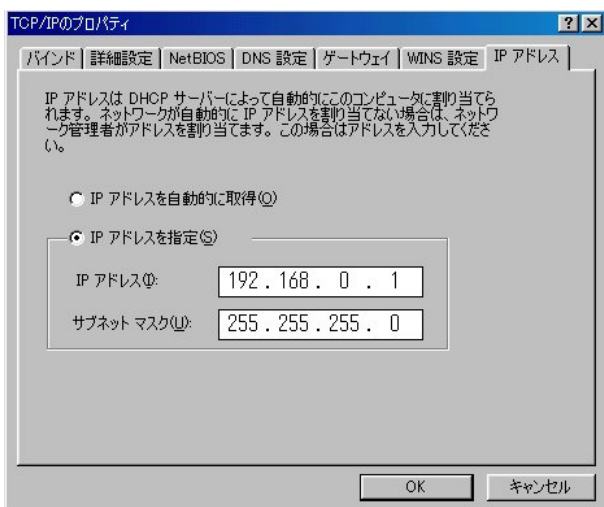
1. Windows 95/98/Me のネットワーク設定

ここではWindows95/98/Meが搭載されたコンピュータのネットワーク設定について説明します。

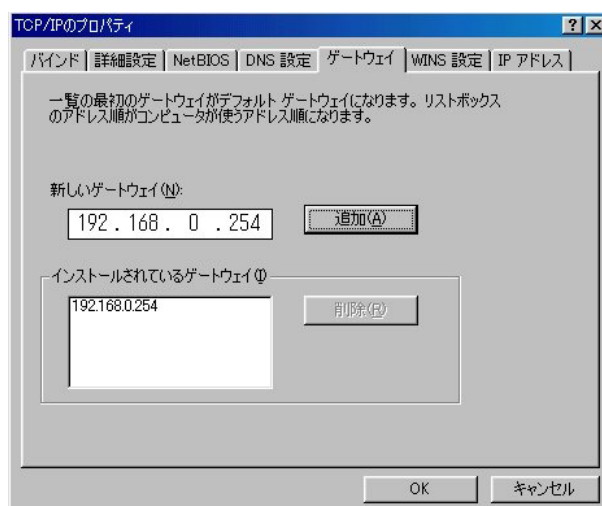
1 「コントロールパネル」→「ネットワーク」の順で開き、「ネットワークの設定」タブの「現在のネットワーク構成」から、コンピュータに装着されたLANボード(カード)のプロパティを開きます。



2 「TCP/IPのプロパティ」が開いたら、「IPアドレス」タブをクリックしてIP設定をおこないます。「IPアドレスを指定」にチェックを入れて、IPアドレスに「192.168.0.1」、サブネットマスクに「255.255.255.0」と入力します。



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



4 最後にOKボタンをクリックするとコンピュータが再起動します。再起動後に、XR-440の設定画面へのログインが可能になります。

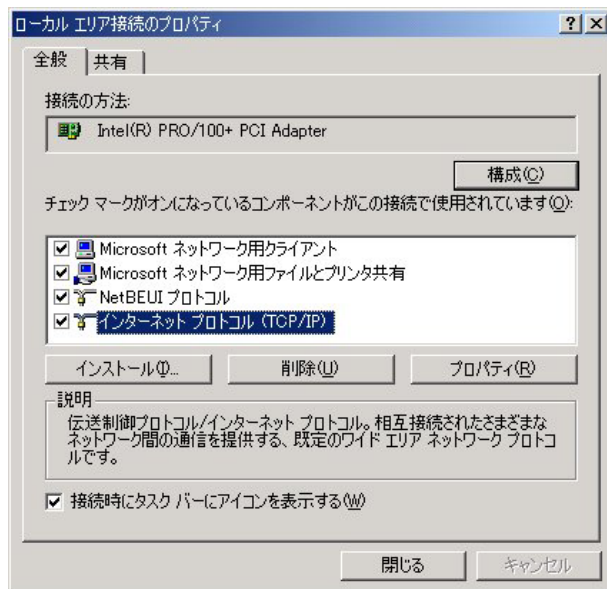
第3章 コンピュータのネットワーク設定

II. Windows 2000 のネットワーク設定

ここではWindows2000が搭載されたコンピュータのネットワーク設定について説明します。

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

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

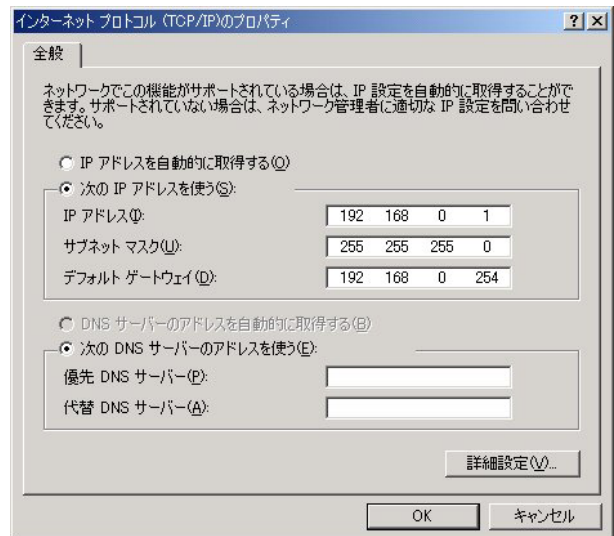


3 「全般」の画面では、「次の IP アドレスを使う」にチェックを入れて以下のように入力します。

IP アドレス 「192.168.0.1」

サブネットマスク 「255.255.255.0」

デフォルトゲートウェイ 「192.168.0.254」



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

第3章 コンピュータのネットワーク設定

III. Windows XP のネットワーク設定

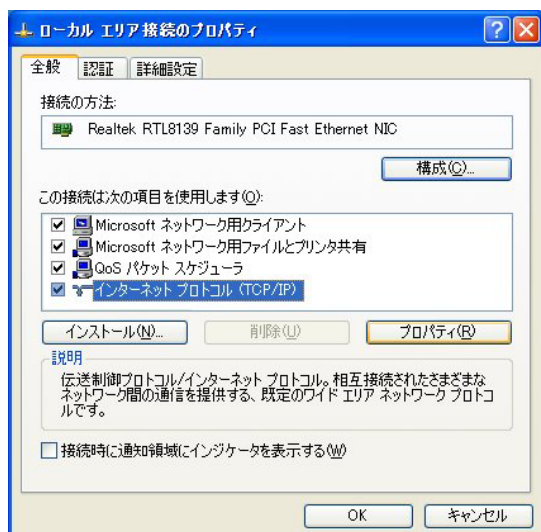
ここではWindowsXPが搭載されたコンピュータのネットワーク設定について説明します。

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

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。



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

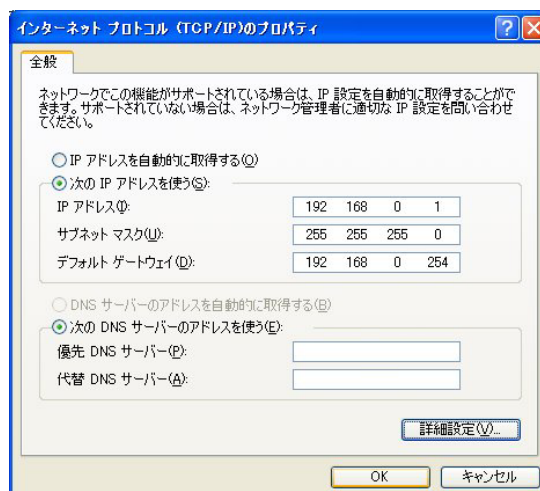


4 「インターネットプロトコル(TCP/IP)」の画面では、「次の IP アドレスを使う」にチェックを入れて以下のように入力します。

IP アドレス 「192.168.0.1」

サブネットマスク 「255.255.255.0」

デフォルトゲートウェイ 「192.168.0.254」



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

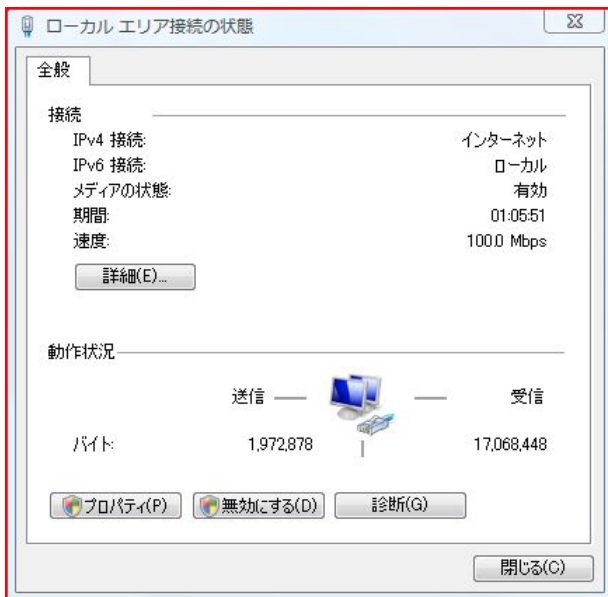
第3章 コンピュータのネットワーク設定

IV.Windows Vista のネットワーク設定

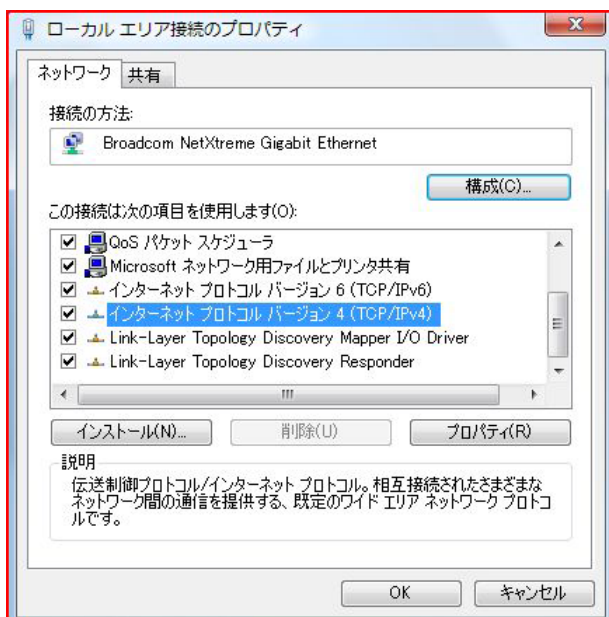
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。



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

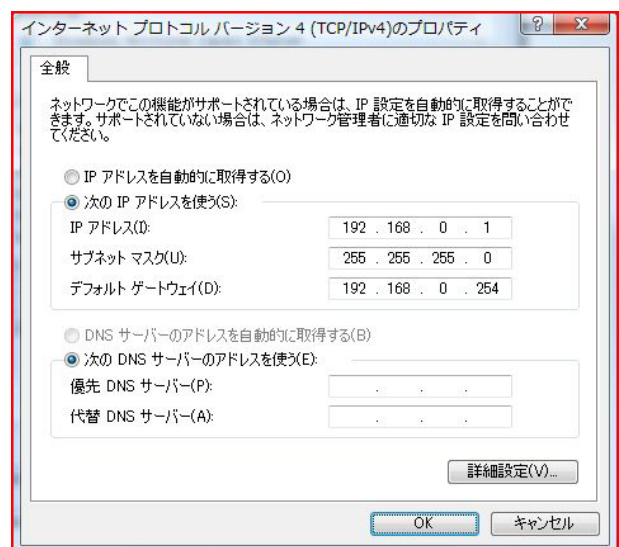


4 「インターネットプロトコルバージョン4 (TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IP アドレス 「192.168.0.1」

サブネットマスク 「255.255.255.0」

デフォルトゲートウェイ 「192.168.0.254」



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

第3章 コンピュータのネットワーク設定

V. Macintosh のネットワーク設定

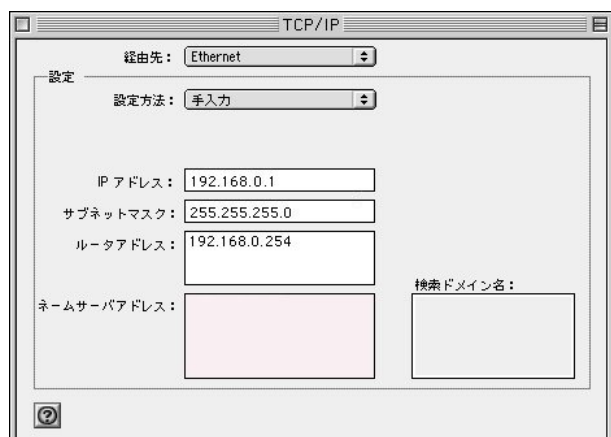
ここではMacintoshのネットワーク設定について説明します。

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

2 経由先を「Ethernet」、設定方法を「手入力」にして、以下のように入力してください。

IP アドレス「192.168.0.1」

サブネットマスク「255.255.255.0」



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

ここでは、Mac OS Xのネットワーク設定について説明します。

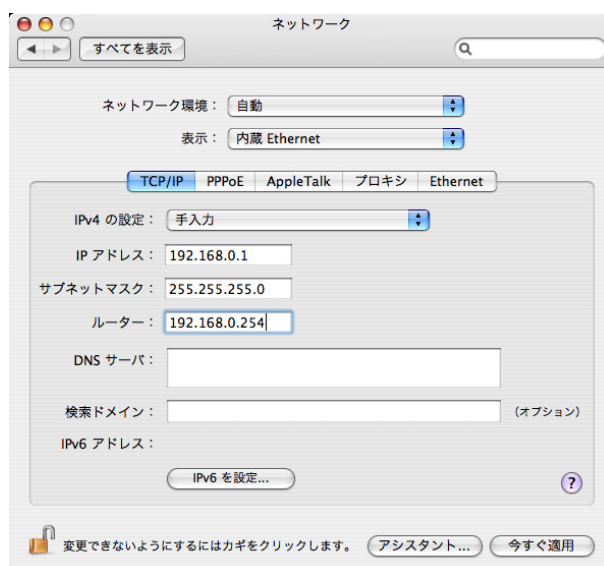
1 「システム環境設定」から「ネットワーク」を開きます。

2 ネットワーク環境を「自動」、表示を「内蔵 Ethernet」、IPv4 の設定を「手入力」にして、以下のように入力してください。

IP アドレス「192.168.0.1」

サブネットマスク「255.255.255.0」

ルーター「192.168.0.254」



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

第3章 コンピュータのネットワーク設定

VI. IP アドレスの確認と再取得

◆ Windows95/98/Me の場合

1 「スタート」→「ファイル名を指定して実行」を開きます。

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

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



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

◆ WindowsNT3.51/4.0/2000 の場合

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

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

```
c:|>ipconfig /all
```

3 IP 設定のクリアと再取得をするには以下のコマンドを入力してください。

```
c:|>ipconfig /release (IP 設定のクリア)
```

```
c:|>ipconfig /renew (IP 設定の再取得)
```

◆ Macintosh の場合

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

XR-440 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

第4章 設定画面へのアクセス

設定画面へのログイン方法

1 各種ブラウザを開きます。

2 ブラウザから設定画面にアクセスします。
ブラウザのアドレス欄に、以下の IP アドレスと
ポート番号を入力してください。

http://192.168.0.254:880/

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

3 次のような認証ダイアログが表示されます。



4 ダイアログ画面にパスワードを入力します。
工場出荷設定のユーザー名とパスワードはともに
「admin」です。ユーザー名・パスワードを変更し
ている場合は、それに合わせてユーザー名・パス
ワードを入力します。



5 ブラウザ設定画面が表示されます。



第5章

インタフェース設定

第5章 インタフェース設定

1. Ethernet ポートの設定

◆各 Ethernet ポートの設定

Web 設定画面「インタフェース設定」->

「Ethernet0(または1、2)の設定」をクリックして設定します。

○ IP アドレスが固定割り当ての場合は「固定アドレスで使用」にチェックして、IP アドレスとネットマスクを入力します。

IP アドレスに "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 などを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。

○ IP アドレスが DHCP で割り当ての場合は「DHCP から取得」にチェックして、必要であればホストネームと MAC アドレスを設定します (Ether2 ポートは対応していません)。

○ MTU

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

○ IP マスカレード

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

○ステートフルパケットインスペクション

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

○ SPI で DROP したパケットの LOG を取得

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

○ Proxy ARP

Proxy ARP を使う場合にチェックを入れます。

○ Directed Broadcast

チェックを入れない場合、そのインタフェースにおいて Directed Broadcast の送信は行いますが、受信した Directed Broadcast は破棄されます。チェックを入れた場合には、受信した Directed Broadcast を転送します。

Directed Broadcast

IP アドレスのホスト部が全て 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。

第5章 インタフェース設定

I.Ethernet ポートの設定

○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行います。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行いません。

○リンクダウン時にインタフェースへの通信不可
チェックを入れると、リンクがダウンした時にそのインタフェースに対する通信ができなくなります。これにより、リモートの拠点から、ping などを使って本装置の LAN インタフェースのリンク状態を監視することができます。リンク監視が有効の場合のみ、本設定も有効になります。

但し、本設定を有効にしたインタフェースがリモートの拠点での IPsec KeepAlive の送信先アドレスに指定された場合、リンクダウンが発生した時に IPsec トンネルの障害として検出されてしまいます。回避の方法など、詳細については、第13章「IPsec 機能 IV. IPsec Keep-Alive 設定」をご覧ください。

○ポートの通信モード

XR-440 の Ethernet ポートの通信速度・方式を選択します。工場出荷設定では「自動」(オートネゴシエーション)となっていますが、必要に応じて通信速度・方式を選択してください。

Ether2 ポートは自動設定のみとなります。

XR-440 のインタフェースのアドレスを変更した後は設定が直ちに反映されます。設定画面にアクセスしているホストやその他クライアントの IP アドレス等も XR の設定にあわせて変更し、変更後の IP アドレスで設定画面に再ログインしてください。

[ステートフルパケットインスペクション]

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

[PPPoE 接続時の Ethernet ポート設定]

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

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

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

[IPsec 通信時の Ethernet ポート設定]

XR-440 を IPsec ゲートウェイとして使う場合は、Ethernet ポートの設定に注意してください。

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが XR-440 の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 で、且つ、XR-440 の Ether1 ポートに 192.168.1.254 が設定されていると、正常に IPsec 通信がおこなえません。

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

第5章 インタフェース設定

II.VLAN タギングの設定

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

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

No.	dev.Tag ID	enable	IPアドレス	ネットマスク	MTU	ip masq	spi	drop log	proxy arp	icmp
1	eth0. 1	☒	192.168.222.1	255.255.255.0	1500	☒	☒	☐	☐	☐
2	eth0. 2	☒	192.168.221.1	255.255.255.0	1500	☒	☒	☐	☐	☐
3	eth0. 3	☒	192.168.223.1	255.255.255.0	1500	☒	☒	☐	☐	☐

(Ether0 ポートでの表示例です)

○ devTag ID.

VLAN のタグ ID を設定します。1 から 4094 の間で設定します。各 Ethernet ポートごとに 64 個までの設定ができます。

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

○ enable

チェックを入れることで設定を有効にします。

○ IP アドレス、サブネットマスク

VLAN インタフェースの IP アドレスとサブネットマスクを設定します。

○ MTU

VLAN インタフェースの MTU 値を設定します。

○ ip masq.

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

○ spi

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

○ proxy arp

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

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

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

設定情報の表示

VLAN 設定項目にある「設定情報」リンクをクリックすると、現在の VLAN 設定情報が表示されます。

III. その他の設定

◆デフォルトゲートウェイの設定

デフォルトゲートウェイは「その他の設定」画面で設定します。「デフォルトゲートウェイの設定」欄に IP アドレスを設定します (PPPoE 接続時は設定の必要はありません)。

デフォルトゲートウェイの設定

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

◆Dummy Interface の設定

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

Dummy Interfaceの設定

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。

III. その他の設定

◆ ARP エントリの設定

「その他の設定」画面中央にある「ARP テーブル」をクリックすると、本装置の ARP テーブルについて設定することができます。

現在のARPテーブル

192.168.0.100 00...

ARPエントリの固定化

ARPエントリの削除

新しいARPエントリ

ARPエントリの追加

固定のARPエントリ

固定ARPエントリの編集

(画面は表示例です)

○現在の ARP テーブル

本装置に登録されている ARP テーブルの内容を表示します。

初期状態では動的な ARP エントリが表示されています。

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

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

○新しい ARP エントリ

ARP エントリを手動で登録するときは、ここから登録します。

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

エントリの入力例：

192.168.0.1 00:11:22:33:44:55

○固定の ARP エントリ

ARP エントリを固定するときは、ここから登録します。

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

エントリの入力方法は「新しい ARP エントリ」と同様です。

第5章 インタフェース設定

III. その他の設定

ARP テーブルの確認

「その他の設定」画面中央で、現在の ARP テーブルの内容を確認できます。

IP address	HW type	Flags	HW address	Mask	Device
192.168.0.100	0x1	0x2	00:90: [input field]	*	eth0

(画面は表示例です)

「Flags」に、ARP エントリの状態が表示されます。

- 0x2 : 自動的に登録されたARP エントリ
- 0x6 : 手動で登録されたARP エントリ
- 0x0 : 無効となっているARP エントリ

第5章 インタフェース設定

III. その他の設定

◆ポートベース VLAN の設定

Ethernet2 ポートで、ポートベース VLAN 設定ができます。

設定できる VLAN グループは A～D の 4 つとなります。

「その他の設定」画面下にある「Ether2 HUB の設定」画面を開きます。

☒ Port VLAN機能を使用しない
☐ Port VLAN機能を使用する

各ポートとVLANメンバの組み合わせ

	Port 1	Port 2	Port 3	Port 4
VLAN A	☒	☒	☒	☒
VLAN B	☐	☐	☐	☐
VLAN C	☐	☐	☐	☐
VLAN D	☐	☐	☐	☐

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

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

入力が終わりましたら「設定の保存」をクリックして設定完了です。

◆ PPPoE ブリッジの設定

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

この機能は XR 自身が PPPoE 接続している時も同時に利用できますので、PPPoE マルチセッションでの接続が可能です。

「PPPoE ブリッジ機能」の「使用する」を選択します。

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

「PPPoE ブリッジの設定の保存」をクリックして設定完了です。

「その他の設定」画面下にある「PPPoE ブリッジの設定」画面を開きます。

PPPoE ブリッジの設定

PPPoEブリッジ機能 ☐ 使用しない ☒ 使用する

インターフェースの選択 ☒ Ethernet0 ☒ Ethernet1 ☐ Ethernet2

PPPoEブリッジの設定の保存

第 6 章

PPPoE 設定

第6章 PPPoE 設定

I. PPPoE の接続先設定

Web 設定画面「PPP/PPPoE 設定」をクリックします。

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

プロバイダ名	
ユーザID	
パスワード	
DNS サーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCP キープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は30秒固定、空欄の時はP-t-P Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(奨励) MSS値 Byte (有効時にMSS値が0の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1462。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)

○プロバイダ名

任意で設定名を付けることができます。半角英数字のみ使用できます。

○ユーザー ID

プロバイダから指定されたユーザー IDを入力してください。

○パスワード

プロバイダから指定された接続パスワードを入力してください。

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

<例>

abc(def)g'h → abc\(def\)g\'h

○DNS サーバ

特に指定のない場合は「プロバイダから自動割り当て」をチェックします。

指定されている場合は「手動で設定」をチェックして、DNS サーバのアドレスを入力します。

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

○LCP キープアライブ

キープアライブのための LCP echo パケットを送出する間隔を指定します。設定した間隔で LCP echo パケットを3回送出してreplyを検出しなかったときに、XR-440 が PPPoE セッションをクローズします。「0」を指定すると、LCP キープアライブ機能は無効となります。

○Ping による接続確認

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

第6章 PPPoE 設定

I. PPPoE の接続先設定

○ IP アドレス

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

○ MSS 設定

「有効」を選択すると、XR-440 が MSS 値を自動的に調整します。「MSS 値」は任意に設定できます。最大値は 1452 バイトです。

「0」にすると最大 1414byte に自動調整します。特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします (それ以外では正常にアクセスできなくなる場合があります)。

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

MSS 設定項目以下は設定しません。

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。

第6章 PPPoE 設定

II. PPPoE の接続設定と回線の接続 / 切断

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

回線状態	回線は接続されていません
接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケット インスペクション	☒ 無効 ☐ 有効 ☐ DROP したパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効
ICMP AddressMask Request	☐ 応答しない ☒ 応答する
接続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	xr440
中継するメールサーバのアド レス	

接続設定

○回線状態

現在の回線状態を表示します。

○接続先の選択

どの接続先設定を使って接続するかを選択します。

○接続ポート

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

○接続形態

「手動接続」 PPPoE(PPP)の接続 / 切断を手動で切り替えます。
「常時接続」 XR-440 が起動すると自動的に PPPoE 接続を開始します。また PPPoE セッションが切断しても、自動的に再接続します。
「スケジューラ接続」 BRI ポートでの接続をする時に選択できます。

○RS232C/BRI 接続タイプ

PPPoE 接続では「通常接続」を選択します。

○IP マスカレード

PPPoE 接続時に IP マスカレードを有効にするかどうかを選択します。

○ステートフルパケットインスペクション

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

II. PPPoE の接続設定と回線の接続 / 切断

○デフォルトルートの設定

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

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

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

III. その他の接続設定

接続 IP 変更お知らせメール機能

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

以下の箇所で設定します。

接続 IP 変更 お知らせメール	☒ 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	xr440
中継するメールサーバのアド レス	

○接続 IP 変更お知らせメール

お知らせメール機能を使う場合は、「送信する」を選択します。

○お知らせメールの宛先

お知らせメールを送るメールアドレスを入力します。

○お知らせメールの From アドレス

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

○中継するメールサーバのアドレス

お知らせメールを中継する任意のメールサーバを設定できます。IP アドレス、ドメイン名のどちらでも設定できます。

ただしドメイン名で指定するときは、下記の記述で設定してください。

<入力形式> @ <ドメイン名>

<入力例> @mail.xxxxxx.co.jp

第6章 PPPoE 設定

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 15 章ダイナミックルーティング III. OSPF の設定」をご覧ください。

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	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ RS232C
RS232C/BRI 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/BRI 接続タイプ

RS232C/BRI インタフェースを使って副回線接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

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

上記3項目以外の接続設定は、すべてそのまま引き継がれます。

副回線での自動接続機能は、「接続設定」で「常時接続」に設定してある場合のみ有効です。また「接続設定」を変更した場合には、回線を一度切断して再接続した際に変更が反映されます。

第6章 PPPoE 設定

IV. 副回線とバックアップ回線

バックアップ回線設定

PPPoE 接続設定画面の「バックアップ回線使用時に設定して下さい」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	☐ Ether0 ☐ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☒ RS232C
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケット インスペクション	☒ 無効 ☐ 有効 ☐ DROPしたパケットのLOGを取得
ICMP AddressMask Request	☐ 応答しない ☒ 応答する
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
接続お知らせメール	☒ 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	xr440
中継するメールサーバのア ドレス	

○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

副回線を接続しているインタフェースを選択します。

○RS232C/BRI 接続タイプ

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

○IP マスカレード

バックアップ回線接続時の IP マスカレードの動作を選択します。

第6章 PPPoE 設定

IV. 副回線とバックアップ回線

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

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

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

○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 が返ってこなかった場合に、バックアップ回線接続に切り替わります。

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

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

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

○Ping 使用時の device
ping を使用する際に ping を発行する、本装置のインタフェースを選択します。「IPSEC+PING」の場合には「その他」を選択して ipsec インタフェース名を指定します(EX. 主回線上の IPsec インタフェースは "ipsec0" です)。

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

○復旧時のバックアップ回線の強制切断
主回線の接続が復旧したときに、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、主回線の接続が復旧しても、バックアップ回線接続の設定に従ってバックアップ回線の接続を維持します。

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

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

IV. 副回線とバックアップ回線

接続変更お知らせメール機能

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

以下の箇所で設定します。

接続お知らせメール	☒ 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	xr440
中継するメールサーバのアドレス	

○接続お知らせメール

お知らせメール機能を使う場合は、「有効」を選択します。

○お知らせメールの宛先

お知らせメールを送るメールアドレスを入力します。

○お知らせメールの From アドレス

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

○中継するメールサーバのアドレス

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

<入力形式> @ <ドメイン名>

<入力例> @mail.xxxxxx.co.jp

第6章 PPPoE 設定

V.PPPoE 特殊オプション設定

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

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

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

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

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

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。

PPPoE 特殊オプション
(全回線共通)

- ☐ 回線接続時に前回の PPPoE セッションの PADT を強制送出
- ☐ 非接続 Session の IPv4Packet 受信時に PADT を強制送出
- ☐ 非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出

- 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-EchoRequest 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、XR 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、XR 側から再接続を行います。

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 XR が受信すると、XR 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、XR 側から再接続を行います。

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

地域 IP 網の工事後に PPPoE 接続ができなくなってしまふ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

第7章 ダイヤルアップ接続

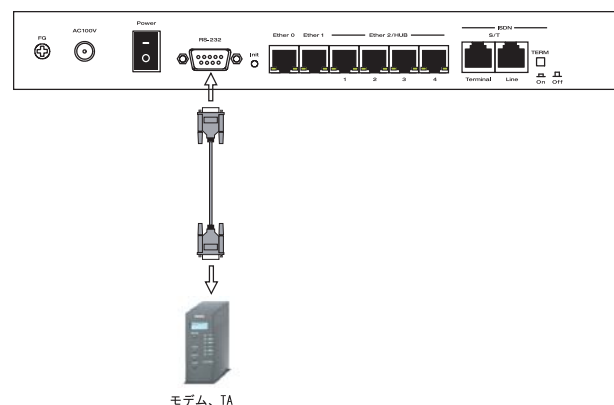
1. RS-232ポートとアナログモデム/TAの接続

XR-440 は、RS-232 ポート、ISDN S/T 点ポート (BRI 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-440 の PPP 接続機能を使うことでダイヤルアップ接続ができます。

◆アナログモデム/TAのシリアル接続

- 1 本装置の電源をオフにします。
- 2 本装置の「RS-232C」ポートとモデム/TAのシリアルポートをシリアルケーブルで接続します。シリアルケーブルは別途ご用意下さい。
- 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



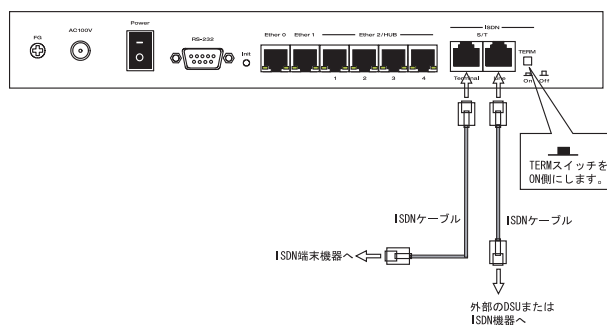
第7章 ダイヤルアップ接続

II. BRI ポートと TA/DSU の接続

◆外部の DSU を使う場合

- 1 本装置の電源をオフにします。
- 2 外部の DSU と本装置の「BRI S/T LINE」ポートを ISDN 回線ケーブルで接続します。ISDN ケーブルは別途ご用意下さい。
- 3 本体背面の「TERM.」スイッチを「ON」側にします。
- 4 別の ISDN 機器を接続する場合は「BRI S/T TERMINAL」ポートと接続してください。
- 5 全ての接続が完了しましたら、本装置と TA の電源を投入します。

接続図



第7章 ダイヤルアップ接続

III. 接続先設定

PPP 接続の接続先設定を行ないます。以下の手順で設定してください。

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

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

プロバイダ名	
ユーザID	
パスワード	
DNSサーバ	☐ 割り当てられたDNSを使わない ☒ プロバイダから自動割り当て ☐ 手動で設定 プライマリ セカンダリ
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	☒ 使用しない ☐ 使用する 使用するホスト 発行間隔は30秒固定、空欄の時はPing-Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	 回線接続時に割り付けるグローバルIPアドレスです
PPPoE回線使用時に設定して下さい	
MSS設定	☐ 無効 ☒ 有効(強制) MSS値 0 Byte (有効時にMSS値が0の場合は、MSS値を自動設定(Clamp MSS to MTU)します。最大値は1452。ADSLで接続中に変更したときは、セッションを切断後に再接続する必要があります。)
BRI/PPPシリアル回線使用時に設定して下さい	
電話番号	
ダイヤルタイムアウト	60 秒
PPPシリアル回線使用時に設定して下さい	
シリアルDTE	☐ 9600 ☐ 19200 ☐ 38400 ☐ 57600 ☒ 115200 ☐ 230400
初期化用ATコマンド	ATQ0V1
回線種別	☒ 無指定 ☐ トーン ☐ パルス

○プロバイダ名

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

○ユーザーID

プロバイダから指定されたユーザーIDを入力してください。

○パスワード

プロバイダから指定された接続パスワードを入力してください。

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

<例> abc(def)g'h → abc\(\def\)g\'h

○DNSサーバ

特に指定のない場合は「プロバイダから自動割り当て」をチェックします。指定されている場合は「手動で設定」をチェックして、DNSサーバのアドレスを入力します。

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

○LCPキープアライブ

○pingによる接続確認

○IPアドレス

○MSS設定

上記項目は、ダイヤルアップ接続、ISDN専用線接続の場合は設定しません。

III. 接続先設定

○電話番号

アクセス先の電話番号を入力します。
市外局番から入力してください。

○電話番号

アクセス先の電話番号を入力します。
市外局番から入力してください。

○ダイヤルタイムアウト

アクセス先にログインするときのタイムアウト時間を設定します。単位は秒です。

○シリアル DTE

XR-440 とモデム /TA 間の DTE 速度を選択します。
工場出荷値は 115200bps です。

○初期化用 AT コマンド

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

○回線種別

回線のダイヤル方法を選択します。

○ON-DEMAND 接続用切断タイマー

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

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

続いて PPP の接続設定を行ないます。

第7章 ダイアルアップ接続

IV. ダイアルアップの接続と切断

接続先設定に続いて、ダイアルアップ接続のために接続設定をおこないます。

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

回線状態	回線は接続されていません
接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケット インスペクション	☒ 無効 ☐ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効
ICMP AddressMask Request	☐ 応答しない ☒ 応答する
接続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	xr440
中継するメールサーバのアド レス	

接続設定

○回線状態

現在の回線状態を表示します。

○接続先の選択

どの接続先設定を使って接続するかを選択します。

○接続ポート

どのポートを使って接続するかを選択します。
リモートアクセス接続では「BRI」または「RS232」
ポートを選択します。

ISDN 専用線を使う場合は、「Leased Line(64K)」
または「Leased Line(128K)」を選択して下さい。

○接続形態

「手動接続」リモートアクセスの接続 / 切断を手動
で切り替えます。

「常時接続」XR-440 が起動すると自動的にリモート
アクセス接続を開始します。

「スケジューラ接続」スケジュール接続設定に従っ
て接続します。

○RS232C/BRI 接続タイプ

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

○IP マスカレード

リモートアクセス接続時に IP マスカレードを有効
にするかどうかを選択します。unnumbered 接続以
外のときと ISDN 専用線接続のときは、「有効」を
選択してください。

第7章 ダイアルアップ接続

IV. ダイアルアップの接続と切断

○ステートフルパケットインスペクション

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

○デフォルトルートの設定

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

「無効」を選択すると、ISPから通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。特に必要のない限り「有効」設定にしておきます。

○ICMP AddressMask Request

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

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

第7章 ダイアルアップ接続

V. 副回線接続とバックアップ回線接続

ダイアルアップ接続については、PPPoE 接続と同様に、接続 IP お知らせメール機能、副回線接続設定およびバックアップ回線接続設定が可能です。

設定方法については、第6章「PPPoE 設定」をご覧ください。

第7章 ダイヤルアップ接続／ISDN 専用線接続

VI. 回線への自動発信の防止について

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

そのためISDNポートで他のISDN機器と接続していて、かつ、「On-Demand 接続」機能を使っている場合には、ISDN回線に自動接続してしまう問題が起こります。

この意図しない発信を防止するために、XR-440ではあらかじめ以下のフィルタリングを設定しています。

(入力フィルタ)

eth0	パケット受信時	破棄	tcp				137:139
eth0	パケット受信時	破棄	udp				137:139
eth0	パケット受信時	破棄	tcp		137		
eth0	パケット受信時	破棄	udp		137		

(転送フィルタ)

eth0	パケット受信時	破棄	tcp				137:139
eth0	パケット受信時	破棄	udp				137:139
eth0	パケット受信時	破棄	tcp		137		
eth0	パケット受信時	破棄	udp		137		

第 8 章

専用線接続

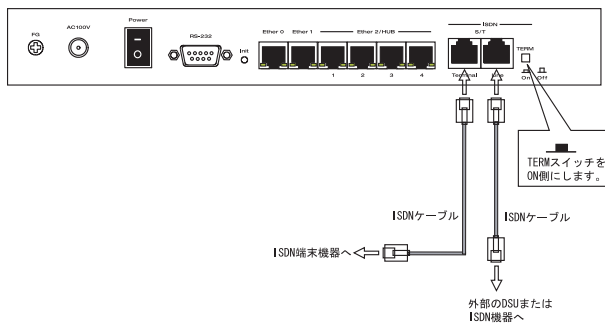
第8章 専用線接続

1. BRI ポートと TA/DSU の接続

◆外部の DSU を使う場合

- 1 本装置の電源をオフにします。
- 2 外部の DSU と本装置の「BRI S/T LINE」ポートを ISDN 回線ケーブルで接続します。ISDN ケーブルは別途ご用意下さい。
- 3 本体背面の「TERM.」スイッチを「ON」側にします。
- 4 別の ISDN 機器を接続する場合は「BRI S/T TERMINAL」ポートと接続してください。
- 5 全ての接続が完了しましたら、本装置と TA の電源を投入します。

接続図



第8章 専用線接続

II. 専用線設定

XR-440/C 同士を ISDN 専用線で接続し、LAN 間通信ができます。

本装置の専用線接続機能の制限について

- unnumbered 接続 (LAN 型払い出し) には対応していません。
- DA128、OCN エコノミー接続には対応していません。

専用線設定

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

プロバイダ名	
専用線設定	
本装置のIPアドレス	
接続先のIPアドレス	
同期PPP	☐ 無効 ☒ 有効
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります

○プロバイダ名

プロバイダ名を任意で設定します。半角英数字で64文字まで使用できます。

○本装置の IP アドレス

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

○接続先の IP アドレス

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

○同期 PPP

同期 PPP を使用するかどうかを選択します。

○LCP キープアライブ

PPPoE 接続のキープアライブのための LCP echo パケットを送出する間隔を指定します。設定した間隔で LCP echo パケットを3回送出して reply を検出しなかったときに、XR-440 が PPPoE セッションをクローズします。「0」を指定すると、LCP キープアライブ機能は無効となります。

設定後は「保存」をクリックしてください。
続いて「接続設定」を行ってください。

専用線設定では、「接続先設定」は行いません。

第8章 専用線接続

III. 専用線の接続と切断

続いて、専用線の接続設定をおこないます。Web 設定画面「PPP/PPPoE 接続設定」→「接続設定」をクリックして、以下の画面から設定します。

回線状態	回線は接続されていません
接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☐ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☒ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☐ 無効 ☒ 有効
ステートフルパケット インスペクション	☐ 無効 ☒ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効
ICMP AddressMask Request	☐ 応答しない ☒ 応答する

接続設定

○回線状態

現在の回線状態を表示します。

○接続先の選択

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

○接続ポート

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

○接続形態

専用線接続では「常時接続」を選択してください。

○RS232C/BRI 接続タイプ

専用線接続では「通常」を選択してください。

○IP マスカレード

専用線接続時に IP マスカレードを有効にするかどうかを選択します。

○ステートフルパケットインスペクション

専用線接続時に、ステートフルパケットインスペクション(SPI)を有効にするかどうかを選択します。

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

○デフォルトルートの設定

「有効」を選択すると、専用線接続時に ISP から通知されるデフォルトルートを自動的に設定します。「インタフェース設定」でデフォルトルートが設定されていても、専用線接続で通知されるものに置き換えられます。

「無効」を選択すると、ISP から通知されるデフォルトルートを無視し、自動設定しません。「インタフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。**特に必要のない限り「有効」設定にしておきます。**

○ 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。

III. 専用線の接続と切断

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

「接続設定」を変更した場合は、回線を一度切断して再接続した際に変更が反映されます。

第9章

複数アカウント同時接続設定

第9章 複数アカウント同時接続設定

複数アカウント同時接続の設定

XR-440 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
- フレッツ ADSL での接続と、ISDN 接続(リモートアクセス)を同時におこなう

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。

XR-440 のマルチ PPPoE セッション機能は、主回線 1 セッションと、マルチ接続 3 セッションの合計 4 セッションまでの同時接続をサポートしています。なお、以下の項目については主回線では設定できませんが、マルチ接続（#2 ～ #4）では設定できませんので、ご注意ください。

- デフォルトルートとして指定する
- 副回線を指定する
- 接続 IP アドレス変更のお知らせメールを送る
- IPsec を設定する

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

ただし、マルチリンクには対応していませんので、帯域を広げる目的で利用することはできません。

また XR-440 のマルチ PPPoE セッション機能は、PPPoE で接続しているすべてのインタフェースがルーティングの対象となります。したがって、それぞれのインタフェースにステートフルパケットインスペクション、又はフィルタリング設定をしてください。

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

第9章 複数アカウント同時接続設定

複数アカウント同時接続の設定

STEP 1 主接続の接続先設定

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

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

STEP 2 マルチ接続用の接続先設定

マルチ接続(同時接続)用の接続先設定をおこないます。

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

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

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

例えば

○ネットワークアドレスに「172.26.0.0」

○ネットマスクに「255.255.0.0」

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

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

このどちらも設定しないと、マルチ接続側にルーティングされず、すべて主接続にルーティングされます。

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。

第9章 複数アカウント同時接続設定

複数アカウント同時接続の設定

STEP 3 PPPoE 接続の設定

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

「PPP/PPPoE 設定」->「接続設定」を開きます。

[主接続用の接続設定]

以下の部分で設定します。

回線状態	回線は接続されていません
接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
接続形態	☐ 手動接続 ☒ 常時接続 ☐ スケジューラ接続
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケットインスペクション	☒ 無効 ☐ 有効 ☐ DROPしたパケットのLOGを取得
デフォルトルートの設定	☐ 無効 ☒ 有効
ICMP AddressMask Request	☐ 応答しない ☒ 応答する
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	xr440
中継するメールサーバのアドレス	

○接続先の選択

主接続用の設定を選択します。

○接続先ポート

主接続で使用する、XR-440のインタフェースを選択します。

○接続形態

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

○IPマスカレード

通常は「有効」を選択します。

LAN側をグローバルIPで運用している場合は「無効」を選択します。

○ステートフルパケットインスペクション

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

第9章 複数アカウント同時接続設定

複数アカウント同時接続の設定

○ ICMP AddressMask Request

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

○ 接続 IP 変更お知らせメール

任意で設定します。

第9章 複数アカウント同時接続設定

複数アカウント同時接続の設定

続いてマルチ接続用の接続設定をおこないます

[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	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケット インスペクション	☒ 無効 ☐ 有効 ☐ DROPしたパケットのLOGを取得
ICMP AddressMask Request	☐ 応答しない ☒ 応答する
マルチ接続 #3	☒ 無効 ☐ 有効
接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケット インスペクション	☒ 無効 ☐ 有効 ☐ DROPしたパケットのLOGを取得
ICMP AddressMask Request	☐ 応答しない ☒ 応答する
マルチ接続 #4	☒ 無効 ☐ 有効
接続先の選択	☒ 接続先1 ☐ 接続先2 ☐ 接続先3 ☐ 接続先4 ☐ 接続先5
接続ポート	☐ Ether0 ☒ Ether1 ☐ Ether2 ☐ BRI(64K) ☐ BRI MP(128K) ☐ Leased Line(64K) ☐ Leased Line(128K) ☐ RS232C
RS232C/BRI接続タイプ	☒ 通常 ☐ On-Demand接続
IPマスカレード	☒ 無効 ☐ 有効
ステートフルパケット インスペクション	☒ 無効 ☐ 有効 ☐ DROPしたパケットのLOGを取得
ICMP AddressMask Request	☐ 応答しない ☒ 応答する

第9章 複数アカウント同時接続設定

複数アカウント同時接続の設定

○マルチ接続 #2 ～ #4

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

○接続先の選択

マルチ接続用の接続先設定を選択します。

○接続ポート

マルチ接続で使用する、XR-440 のインター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ーフェースを選択します。

○RS232C/BRI 接続タイプ

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

「通常」を選択すると常時接続となります。

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

○IP マスカレード

任意で選択します。通常は「有効」にします。

○ステートフルパケットインスペクション

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

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)。

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。

など表示されます。

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

複数アカウント同時接続時の注意点

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

XR-440 に名前解決要求をリレーさせないと、同時接続ができません。

第 10 章

各種サービスの設定

第10章 各種サービスの設定

各種サービス設定

XR-440 の設定画面「各種サービスの起動・停止・設定」をクリックすると、以下の画面が表示されます。

DNSサーバ	☐ 停止 ☒ 起動	動作中	動作変更
DHCP(Relay)サーバ	☐ 停止 ☒ 起動	停止中	動作変更
IPsecサーバ	☒ 停止 ☐ 起動	停止中	動作変更
UPnPサービス	☒ 停止 ☐ 起動	停止中	動作変更
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい		停止中
PPPoE to L2TP	☒ 停止 ☐ 起動	停止中	動作変更
SYSLOGサービス	☐ 停止 ☒ 起動	動作中	動作変更
攻撃検出サービス	☒ 停止 ☐ 起動	停止中	動作変更
SNMPサービス	☒ 停止 ☐ 起動	停止中	動作変更
NTPサービス	☒ 停止 ☐ 起動	停止中	動作変更
VRRPサービス	☒ 停止 ☐ 起動	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい		停止中

ここで

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

をおこないます。

サービスの設定

それぞれのサービスの設定をおこなうには、画面中の各サービス名をクリックしてください。そのサービスの設定画面が表示されます。

それぞれの設定方法については、各機能についてのページを参照してください。

DNSサーバ機能

DHCPサーバ機能

DHCPリレー機能

IPsec接続機能

UPnP機能

ダイナミックルーティング機能

PPPoE to L2TP機能

SYSLOG機能

攻撃検出機能

SNMPエージェント機能

NTPサービス

VRRPサービス

アクセスサーバ機能

サービスの起動と停止

それぞれのサービスを起動・停止するときは、それぞれのサービス項目で「停止」か「起動」を選択し、「動作変更」ボタンをクリックしてください。これにより、サービスの稼働状態が変更されます。またサービスの稼働状態は、各項目ごとに表示されます。

第 11 章

DNS リレー / キャッシュ機能

第11章 DNS リレー / キャッシュ機能

DNS リレー / キャッシュ機能の設定

◆ DNS リレー機能

各種サービス設定画面の「DNS サーバ」を起動させてください。

DNS サーバが「停止」のときは、DNS リレー機能も停止します。

◆ DNS キャッシュ機能

Web 設定画面「各種サービスの設定」->「DNS サーバ」をクリックして、以下の画面で設定します。

DNS キャッシュを使用する	☒ 使用しない	☐ 使用する
以下はDNS キャッシュを使用する際に設定して下さい		
プライマリDNS IPアドレス		
セカンダリDNS IPアドレス		

○ DNS キャッシュ機能の ON/OFF を選択します。
また DNS キャッシュ機能を使う場合は、ISP から指定されたもの、もしくは任意の DNS サーバの IP アドレスを指定してください。

◆ DNS のキャッシュについて

本装置は、DNS リレー・DNS キャッシュのどちらでも DNS の結果をキャッシュします。

設定によるキャッシュの動作は以下のようになります。

- ・「(DNS キャッシュを)使用する、(DNS)サーバ指定あり」の設定の場合。
→指定 DNS が解決した情報を XR がキャッシュします。
- ・「使用する、サーバ指定なし」の設定の場合。
→設定できません。
- ・「使用しない、サーバ指定あり」の設定の場合。
→XR がキャッシュオンリーサーバとなります。
XR 自身が名前解決した情報のみキャッシュします。
- ・「使用しない、サーバ指定なし」の設定の場合。
→XR がキャッシュオンリーサーバとなります。
XR 自身が名前解決した情報のみキャッシュします。

設定後に「設定の保存」をクリックして設定完了です。

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

第 12 章

DHCP サーバ / リレー機能

第12章 DHCP サーバ / リレー機能

1. DHCP サーバ機能の設定

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

DHCPサーバ使用時に設定して下さい	
DHCP アドレスリース情報	
サブネットワーク	192.168.0.0
サブネットマスク	255.255.255.0
ブロードキャスト	192.168.0.255
リース開始アドレス	192.168.0.10
リース終了アドレス	192.168.0.100
ルータアドレス	192.168.0.254
ドメイン名	localdomain.co.jp
プライマリDNS	192.168.0.254
セカンダリDNS	
標準リース時間(秒)	600
最大リース時間(秒)	7200
プライマリDNSサーバ	
セカンダリDNSサーバ	
スコープID	

(上記は表示例です)

DHCP サーバ / リレー機能設定

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うかを選択します。サーバ機能とリレー機能を同時に使うことはできません。

○上位 DHCP サーバの IP アドレス

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

○DHCP relay over XXX

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

○サブネット

DHCP サーバ機能の動作設定をおこないます。

- 複数のサブネットを設定することができます。
- どのサブネットを使うかは、XR-440 のインタフェースに設定された IP アドレスを参照の上、自動的に決定されます。

- ラジオボックスにチェックを入れたサブネット設定が、参照・動作の対象となります。

各サブネットごとの詳細設定は以下の通りです。

○サブネットワーク

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

○サブネットマスク

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

○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 / 終了アドレス

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

○ルータアドレス

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

○ドメイン名

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

○プライマリ / 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。

(次のページに続きます)

第12章 DHCP サーバ / リレー機能

II. DHCP サーバ機能の設定例

○標準リース時間

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

○最大リース時間

DHCP クライアント側が割り当て時間を要求してきたときの、最大限の割り当て時間を指定します。単位は秒です。初期設定では 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 / セカンダリ WINS サーバ

DHCP クライアントに割り当てる WINS サーバアドレスを指定します。

○スコープ ID

NetBIOS スコープ ID を配布できます。

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

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

DHCP リレー機能について

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

DHCP サーバ機能の設定例

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

上記条件の場合の設定例です。

☑ サブネット1	サブネットワーク	192.168.0.0
	サブネットマスク	255.255.255.0
	ブロードキャスト	192.168.0.255
	リース開始アドレス	192.168.0.10
	リース終了アドレス	192.168.0.30
	ルータアドレス	192.168.0.254
	ドメイン名	localdomain.co.jp
	プライマリDNS	192.168.0.254
	セカンダリDNS	
	標準リース時間(秒)	600
	最大リース時間(秒)	7200
	プライマリWINSサーバー	
セカンダリWINSサーバー		
スコープID		

DHCP 情報の表示

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

第12章 DHCP サーバ / リレー機能

III. IP アドレス固定割り当て設定

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

設定方法

Web 設定画面「各種サービスの設定」→「DHCP (Relay)サーバ」→画面上部の「DHCP IP アドレス固定割り付け設定」をクリックして、以下の画面で設定をおこないます。

No.	MACアドレス	IPアドレス	削除
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐
11			☐
12			☐
13			☐
14			☐
15			☐
16			☐

○ MAC アドレス

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

<入力例> **00:80:6d:49:ff:ff**

○ IP アドレス

その MAC アドレスに固定で割り当てる IP アドレスを入力します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

固定割り当て機能は、DHCP サーバ機能を再起動してから有効になります。

エントリの削除方法

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。

IP アドレス固定割り当て設定について

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

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

第 13 章

IPsec 機能

I.XR-440 の IPsec 機能について

◆鍵交換について

IKEを使用しています。IKE フェーズ1ではメインモード、アグレッシブモードの両方をサポートしています。フェーズ2ではクイックモードをサポートしています。

固定 IP アドレス同士の接続はメインモード、固定 IP アドレスと動的 IP アドレスの接続はアグレッシブモードで設定してください。

◆認証方式について

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

◆暗号化アルゴリズム

シングル DES とトリプル DES、AES128bit をサポートしています。暗号化はハードウェア処理で行ないます。

◆ハッシュアルゴリズム

SHA1 と MD-5 を使用しています。

◆認証ヘッダ

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

◆DH 鍵共有アルゴリズムで使用するグループ

group1、group2、group5 をサポートしています。

◆IPsec 使用時の通信可能対地数

XR-440 は最大 128 拠点と IPsec トンネルを構築できます。また VPN 接続できる LAN/ ホストは最大 128 となります。

◆NAT トラバーサル機能を使用した IPsec 接続が可能です。

II. IPsec 設定の流れ

◆ PreShared(共通鍵)方式での IPsec 通信

STEP 1 共通鍵の決定

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

STEP 2 共通鍵の交換

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

STEP 3 本装置側の設定

自分側の XR-440 の設定をおこないます。

STEP 4 IKE/ISAKMP ポリシーの設定

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

STEP 5 IPsec ポリシー設定

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

STEP 6 IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7 IPsec 接続の確認

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

◆ RSA(公開鍵)方式での IPsec 通信

STEP 1 公開鍵・暗号鍵の生成

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

STEP 2 公開鍵の交換

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

STEP 3 本装置側の設定

自分側の XR-440 の設定をおこないます。

STEP 4 IKE/ISAKMP ポリシーの設定

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

STEP 5 IPsec ポリシー設定

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

STEP 6 IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7 IPsec 接続の確認

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

III. IPsec 設定

STEP 0 設定画面を開く

- 1 Web 設定画面にログインします。
- 2 「各種サービスの設定」→「IPsec サーバ」をクリックして、以下の画面から設定します。

IPsec 設定

ステータス	本装置の設定	RSA鍵の作成	X509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			
IKE1	IKE2	IKE3	IKE4	IPSec 1	IPSec 2	IPSec 3	IPSec 4
IKE5	IKE6	IKE7	IKE8	IPSec 5	IPSec 6	IPSec 7	IPSec 8
IKE9	IKE10	IKE11	IKE12	IPSec 9	IPSec 10	IPSec 11	IPSec 12
IKE13	IKE14	IKE15	IKE16	IPSec 13	IPSec 14	IPSec 15	IPSec 16

IPsec 通信のステータス



IPsec Tunnel

現在の設定
黒:使用する、赤:使用しない、

	本装置側			相手側			接続
IPsec	LAN側	IPアドレス	接続NO	IKEポリシー名	IPアドレス	LAN側	SA

現在の状態
停止中

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

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。

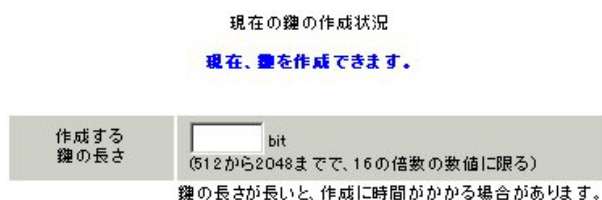
III. IPsec 設定

STEP 1,2 鍵の作成・交換

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

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

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



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

3 鍵を生成します。「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	
主回線使用時のipsecインターフェイスのMTU値	1500
マルチ#2回線使用時のipsecインターフェイスのMTU値	1500
マルチ#3回線使用時のipsecインターフェイスのMTU値	1500
マルチ#4回線使用時のipsecインターフェイスのMTU値	1500
バックアップ回線使用時のipsecインターフェイスのMTU値	1500
Ether 0ポート使用時のipsecインターフェイスのMTU値	1500
Ether 1ポート使用時のipsecインターフェイスのMTU値	1500
Ether 2ポート使用時のipsecインターフェイスのMTU値	1500
NAT Traversalの設定	
NAT Traversal	☐ 使用する ☒ 使用しない
Virtual Private設定	
Virtual Private設定2	
Virtual Private設定3	
Virtual Private設定4	
鍵の表示	
本装置のRSA鍵 (PSKを使用する場合は 必要ありません)	

○ MTU の設定

IPsec 接続時の MTU 値を設定します。
各インタフェースごとに設定できます。
通常は初期設定のままでかまいません。

○ NAT Traversal の設定

NAT トラバーサル機能を使うことで、NAT 環境下にあるクライアントと IPsec 通信を行えるようになります。

「NAT Traversal」

NAT トラバーサル機能を使うかどうかを選択します。

「Virtual Private 設定」

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>

○ 鍵の表示

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

PSK 方式や X.509 電子証明を使う場合はなにも表示されません。

III. IPsec 設定

[本装置側の設定]

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

インタフェースのIPアドレス	
上位ルータのIPアドレス	
インタフェースのID	(例: @xr.centurysys)

○インタフェースの 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。

○インタフェースの ID

本装置への IP アドレスの割り当てが動的割り当ての場合(aggressive モードで接続する場合)は、インタフェースの ID を設定します (必須)。

<入力形式> @ < 任意の文字列 >

<入力例> @centurysystems

@ の後は、任意の文字列(半角英数字のみ使用可能)でかまいません。

最後に「設定の保存」をクリックして設定完了です。続いて 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/ISAKMP ポリシーの設定」1～32の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 ポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	
上位ルータのIPアドレス	
インターフェースのID	(例: @centurysystems)
モードの設定	main モード
transformの設定	1番目 すべてを送信する
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081～28800秒まで)
鍵の設定 ☐ PSKを使用する ☒ RSAを使用する (X509を使用する場合はRSAに設定してください)	
X509の設定 接続先の証明書の設定 (X509を使用しない場合は必要ありません)	

32個以上のIKE/ISAKMPポリシーを設定する場合は、画面上部の「パラメータの設定」をクリックして、パラメータでの設定を行ってください。

○IKE/ISAKMP ポリシー名
設定名を任意で設定します。(省略可)

○接続する本装置側の設定
接続で使用する「本装置側の設定」を選択します。

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

[相手側装置が固定アドレスの場合]
IPアドレスをそのまま入力します。

[相手側装置が動的アドレスの場合]
「0.0.0.0」を入力します。

○上位ルータのIPアドレス
空欄にしておきます。

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

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

@の後は、任意の文字列(半角英数字のみ使用可能)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。

(次ページに続きます)

III. IPsec 設定

○ transform の選択

ISAKMP SA の折衝に必要な暗号化アルゴリズム等の組み合わせを選択します。XR-440 は、以下の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 方式の場合]

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

[RSA 公開鍵方式の場合]

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

○ X509 の設定

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

最後に「設定の保存」をクリックして設定完了です。

続いて、IPsec ポリシーの設定をおこないます。

III. IPsec 設定

STEP 5 IPsec ポリシーの設定

IPsec 設定画面上部の「IPsec ポリシーの設定」をクリックして、以下の画面から設定します。

☐ 使用する ☒ 使用しない ☐ Responderとして使用する ☐ On-Demandで使用する	
使用するIKEポリシー名の選択	-----
本装置側のLAN側のネットワークアドレス	(例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	(例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	秒 (1081～86400秒まで)
DISTANCE	(1～255まで)

(画面は表示例です)

32個以上のIPsecポリシーを設定する場合は、画面上部の「パラメータの設定」をクリックして、パラメータでの設定を行なってください。

○最初にIPsecの起動状態を選択します。

「使用する」はinitiatorにもresponderにもなります。「使用しない」は、そのIPsecポリシーを使用しません。「Responderとして使用する」は、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。XR-1100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下さい。

但し、後述するIPsec KeepAlive機能において、backupSAとして使用する場合もこの選択にして下さい。メイン側のIPsecで障害を検知した場合に、Initiatorとして接続を開始します。

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

○使用するIKEポリシー名の選択

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

○本装置側のLAN側のネットワークアドレス
自分側のXR-440に接続しているLANのネットワークアドレスを入力します。ネットワークアドレス/マスクビット値の形式で入力します。

[入力例] **192.168.0.0/24**

○相手側のLAN側のネットワークアドレス
相手側のIPsec装置に接続されているLANのネットワークアドレスを入力します。ネットワークアドレス/マスクビット値の形式で入力します。

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

○PH2のTransFormの選択

IPsec SAの折衝に必要な暗号化アルゴリズム等の組み合わせを選択します。

- ・暗号化アルゴリズム (des、3des、aes)
- ・認証アルゴリズム (md5、sha1)

通常は「すべてを送信する」の選択で構いません。

○PFS

PFS(PerfectForwardSecrecy)を「使用する」か「使用しない」かを選択します。

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

○DH Groupの選択(PFS使用時に有効)

「PFSを使用する」場合に使用するDH Groupを選択します。ただし「指定しない」を選択しても構いません。その場合は、PH1の結果、選択されたDH Groupを接続相手に送ります。

○SAのライフタイム

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

(次のページに続きます)

第13章 IPsec 機能

III. IPsec 設定

○ DISTANCE

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

なお、設定は省略可能です。省略した場合は「1」として扱います。

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

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

[IPsec 通信時の Ethernet ポート設定について]

IPsec 設定をおこなう場合は、Ethernet ポートの設定に注意してください。

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが XR-440 の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 の設定で、且つ、XR-440 の Ether1 ポートに 192.168.1.254 が設定されていると、正常に IPsec 通信がおこなえません。

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

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。

DNS サーバ	☐ 停止 ☒ 起動	動作中	動作変更
DHCP(Relay)サーバ	☐ 停止 ☒ 起動	停止中	動作変更
IPsecサーバ	☒ 停止 ☐ 起動	停止中	動作変更
UPnPサービス	☒ 停止 ☐ 起動	停止中	動作変更
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい		停止中
FTPtoEnoL2TP	☒ 停止 ☐ 起動	停止中	動作変更
SYNLOGサービス	☐ 停止 ☒ 起動	動作中	動作変更
攻撃検出サービス	☒ 停止 ☐ 起動	停止中	動作変更
SNMPサービス	☒ 停止 ☐ 起動	停止中	動作変更
NTPサービス	☒ 停止 ☐ 起動	停止中	動作変更
VRRPサービス	☒ 停止 ☐ 起動	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい		停止中

○動作状態の制御

IPsec サーバ項目、「起動」にチェックして「動作変更」をクリックすると、IPsec 機能が起動します。以降は、本装置を起動するたびに IPsec 機能が自動起動します。

IPsec 機能を止める場合は「停止」にチェックして「動作変更」をクリックしてください。

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

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

III. IPsec 設定

STEP 7 IPsec 接続を確認する

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

ログの中で、以下のメッセージが含まれているかを確認してください（ログメッセージは「メインモード」で通信した場合の表示例です）。

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

及び

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

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

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

(2)のメッセージは、IPsec SAが正常に確立したことを示しています。

STEP 8 IPsec ステータス確認の確認

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。

IPsec 設定

ステータス	本装置の設定	PSA鍵の作成	X509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		
IKE1	IKE2	IKE3	IKE4	IPSec 1	IPSec 2
IKE5	IKE6	IKE7	IKE8	IPSec 5	IPSec 6
IKE9	IKE10	IKE11	IKE12	IPSec 9	IPSec 10
IKE13	IKE14	IKE15	IKE16	IPSec 13	IPSec 14
				IPSec 15	IPSec 16

IPsec 通信のステータス

現在の設定
黒: 使用する、赤: 使用しない

IPSec	本装置側			相手側			接続
	LAN側	IPアドレス	接続NO	IKEポリシー名	IPアドレス	LAN側	
IPSec1	192.168.0.0/24	192.168.1.254	1	QKE1	192.168.1.253	192.168.2.0/24	SA

現在の状態 動作中

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。

第13章 IPsec 機能

IV. IPsec Keep-Alive 設定

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

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

IPsec 設定画面上部の「IPsec Keep-Alive 設定」をクリックして設定します。

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	operation 1	operation 2	interface	local SA	remote
1	☐			10	3	100	0	0	eth0		
2	☐			10	3	100	0	0	eth0		
3	☐			10	3	100	0	0	eth0		
4	☐			10	3	100	0	0	eth0		
5	☐			10	3	100	0	0	eth0		
6	☐			10	3	100	0	0	eth0		
7	☐			10	3	100	0	0	eth0		
8	☐			10	3	100	0	0	eth0		
9	☐			10	3	100	0	0	eth0		
10	☐			10	3	100	0	0	eth0		
11	☐			10	3	100	0	0	eth0		
12	☐			10	3	100	0	0	eth0		
13	☐			10	3	100	0	0	eth0		
14	☐			10	3	100	0	0	eth0		
15	☐			10	3	100	0	0	eth0		
16	☐			10	3	100	0	0	eth0		

○ enable

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

○ source address

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

○ destination address

IPsec 通信を行う際の、XR の対向側装置の LAN 側のインタフェースの IP アドレスを入力します。

○ interval(sec)

○ watch count

ping を発行する間隔を設定します。

「『interval(sec)』間に『watch count』回 ping を発行する」という設定になります。

○ timeout/delay(sec)

後述の「動作オプション1」の設定に応じて、入力値の意味が異なります。

・動作オプション1が有効の場合

入力値は timeout(秒)として扱います。timeout とは ping 送出時の reply 待ち時間です。

但し、timeout 値が (interval/watch count) より大きい場合は、reply 待ち時間は (interval/watch count) となります。

・動作オプション1が無効の場合

入力値は delay(秒)として扱います。delay とは IPsec が起動してから ping 送信を開始するまでの待ち時間です。IPsec が確立するまでの時間を考慮して設定します。

また ping の reply 待ち時間は、(interval/watch count) 秒となります。

○動作オプション1

IPsec ネゴシエーションと同期して Keep-Alive を行う場合は、チェックを入れます。

チェックを入れない場合は、IPsec ネゴシエーションと非同期に Keep-Alive を行います。

注) 本オプションは v1.7.0 での新規追加オプションです。チェックを入れない場合、IPsec ネゴシエーションと Keep-Alive が非同期に行われるため、タイミングによっては IPsec SA 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 IPsec SA を切断してしまう場合があります。このような事象を防ぐために、本オプションを有効にすることを推奨します。

IV. IPsec Keep-Alive 設定

■ IPsec ネゴシエーションとの同期について

IPsec ポリシーのネゴシエーションは下記のフェーズを遷移しながら行います。動作オプション1を有効にした場合、各フェーズと同期した Keep-Alive 動作を行います。

・フェーズ1 (イニシエーションフェーズ)

ネゴシエーションを開始し、IPsec ポリシー確立中の状態です。

この後、正常に IPsec ポリシーが確立できた場合はフェーズ3へ移行します。

また、要求に対して対向装置からの応答がない場合はタイムアウトによりフェーズ2へ移行します。

※フェーズ3に移行するまでpingの送出は行いません。

・フェーズ2 (ネゴシエーションT.O. フェーズ)

フェーズ1におけるネゴシエーションが失敗、またはタイムアウトした状態です。

この時、バックアップ SA を起動し、フェーズ1に戻ります。

・フェーズ3 (ポリシー確立フェーズ)

IPsec ポリシーが正常に確立した状態です。

確立した IPsec ポリシー上を通過できる ping を使用して IPsec ポリシーの疎通確認を始めます。

この時、マスター SA として確立した場合は、バックアップ SA のダウンを行います。

また、同じ IKE を使う他の IPsec ポリシーがある場合は、それらのネゴシエーションを開始します。

この後、ping の応答がタイムアウトした場合は、フェーズ4に移行します。

・フェーズ4 (ポリシーダウンフェーズ)

フェーズ3においてpingの応答がタイムアウトした時や対向機器より delete SA を受け取った時には、ping の送出を停止して、監視対象の IPsec ポリシーをダウンさせます。

さらに、バックアップ SA を起動させた後、フェーズ1に戻ります。

○動作オプション2

本オプションは「動作オプション1」が無効の場合のみ、有効になります。

チェックを入れると、delay 後に ping を発行して、ping が失敗したら即座に指定された IPsec トンネルの削除、再折衝を開始します。また Keep-Alive による SA 削除後は、毎回 delay 秒待ってから Keep-Alive が開始されます。

チェックははずすと、delay 後に最初に ping が成功 (IPsec が確立) し、その後に ping が失敗してはじめて指定された IPsec トンネルの削除、再折衝を開始します。IPsec が最初に確立する前に ping が失敗してもなにもしません。また delay は初回のみ発生します。

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

○ interface

Keep-Alive 機能を使う、本装置の IPsec インタフェース名を選択します。

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

○ backup SA

ここに IPsec ポリシーの設定番号を指定しておく、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

(次ページに続きます)

第13章 IPsec 機能

IV. IPsec Keep-Alive 設定

またここに、以下のような設定もできます。

ike<n> ※ <n> は 1-64 の整数

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

<例>



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

○ remove

設定を削除したいときにチェックします。

最後に「設定の保存」ボタンをクリックします。

設定番号について

IPsec Keep-Alive 機能を使う際は、監視する IPsec のポリシー No. と Keep-Alive の Policy 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、センタ側からの通信があるようなケースについては SA の不一致が起こりうるため、拠点側で IPsec Keep-Alive 機能を動作させることを推奨します。

destination アドレスとリンク監視について

本装置が対向 XR の Keep-Alive の destination アドレスに指定されており、かつ、そのインタフェース上で「リンクダウン時にインタフェースへの通信不可」

(第5章「インタフェース設定 1.Ethernet ポートの設定」参照)

を有効にすると、インタフェースがリンクダウンした時に、Keep-Alive にも応答しなくなるため、IPsec ポリシーがダウンしてしまいます。

これを回避するためには、destination アドレスと同じネットワークの仮想 loopback インタフェースを設定し、そのアドレスを対向 XR の Keep-Alive の destination アドレスに指定して下さい。

第13章 IPsec 機能

V. 「X.509 デジタル証明書」を用いた電子認証

< loopback 仮想インタフェース設定例 >

本装置の IPsec の LAN 側インタフェースのアドレスを、” 192.168.20.253 ” とします。

インターフェース	仮想I/F番号	IPアドレス	ネットマスク	削除
lo	0	192.168.20.250	255.255.255.255	☐

・この場合、loopback 仮想インタフェース 「lo:0」 にアドレス ” 192.168.20.250 ” を設定します。但し、サブネットマスクには ” 255.255.255.255 ” を指定して下さい。

< 対向 XR の IPsec Keep-Alive 設定例 >

enable	source address	destination address	intf
☒	192.168.0.254	192.168.20.250	

・destination address として 「lo:0」 に設定したアドレス ” 192.168.20.250 ” を指定します。
XR-440 は X.509 デジタル証明書を用いた電子認証方式に対応しています。

ただし XR-440 は証明書署名要求の発行や証明書の発行ができませんので、あらかじめ CA 局から証明書の発行を受けておく必要があります。

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

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

設定は、IPsec 設定画面内の 「X.509 の設定」 から行えます。

X509の設定	☐ 使用する ☒ 使用しない
設定した接続先の証明書のみを使用する	☒ 使用する ☐ 使用しない
証明書のパスワード	

○ X509 の設定

X.509 の使用 / 不使用を選択します。

○ 設定した接続先の証明書のみを使用する

「IKE/ISAKMP の設定」で X.509 の設定を行った接続先のみ X.509 を使用します。

○ 証明書のパスワード

証明書のパスワードを入力します。

第 13 章 IPsec 機能

V. 「X.509 デジタル証明書」を用いた電子認証

[CA の設定]

ここには、CA 局自身のデジタル証明書の内容をコピーして貼り付けます。

[本装置側の証明書の設定]

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

[本装置側の鍵の設定]

ここにはデジタル証明書と同時に発行された、本装置の秘密鍵の内容をコピーして貼り付けます。

[接続先側の設定]

ここには、IPsec 接続先の装置に対して発行された証明書の内容をコピーして貼り付けます。接続先から証明書を入手してください。

[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。

[その他の設定について]

その他の設定については、通常の IPsec 設定と同様にしてください。

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

以上で X.509 の設定は完了です。

[設定のバックアップ保存について]

設定のバックアップを作成しても、X.509 関連の設定は含まれません。またパラメータによる設定にも反映されません。

バックアップファイルから設定を復帰させる場合でも、X.509 関連の設定は再度おこなってください。

第13章 IPsec 機能

VI. IPsec 通信時のパケットフィルタ設定

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

IPsec では、以下の2種類のプロトコル・ポートを使用します。

- ・プロトコル「UDP」のポート「500」番
->IKE(IPsecの鍵交換)のトラフィックに必要です
- ・プロトコル「ESP」
->ESP(暗号化ペイロード)のトラフィックに必要です

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

< 設定例 >

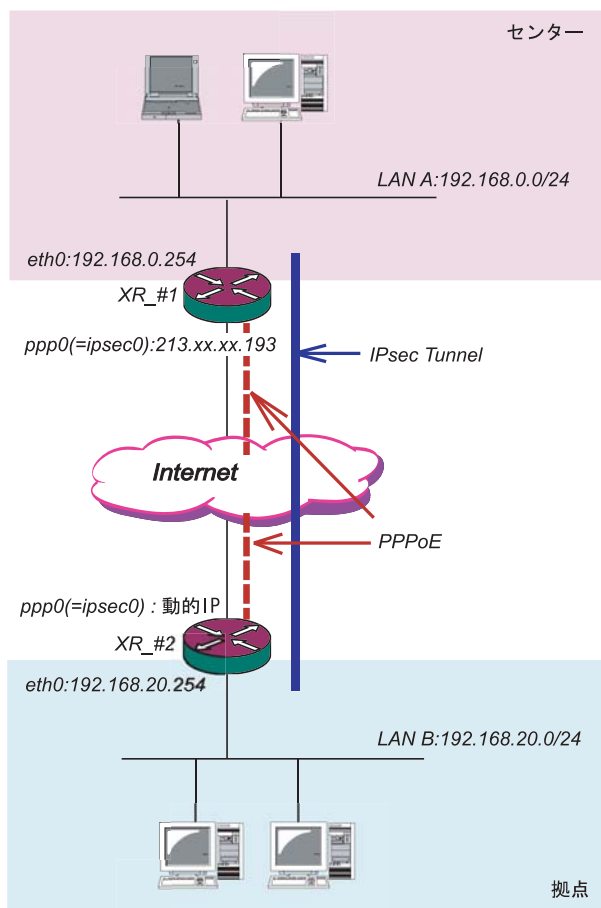
インターフェース	方向	動作	プロトコル	通信元アドレス	通信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	許可	udp				500
ppp0	パケット受信時	許可	esp				

第13章 IPsec 機能

VII. IPsec 設定例 1 (センター／拠点間の1対1接続)

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

<設定例1>



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

「本装置の設定」

「本装置側の設定1」を選択します。

インターフェースのIPアドレス	213.xx.xx.193
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例: @xr.centurysys)

○インタフェースの IP アドレス

「213.xx.xx.193」

○上位ルータの IP アドレス 「%ppp0」

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

○インタフェースの ID 「空欄」

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

<接続条件>

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

第13章 IPsec 機能

VII. IPsec 設定例 1 (センター／拠点間の1対1接続)

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@host (例:@xr.centurysys)
モードの設定	aggressive モード
transformの設定	1番目 group2-3des-sha1
	2番目 使用しない
	3番目 使用しない
	4番目 使用しない
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
☒ PSKを使用する	test_key
☐ RSAを使用する (X509を使用する場合はRSAに設定してください)	
X509の設定	
接続先の証明書の設定	
☐ X509を使用しない場合は必要ありません	

- IKE/ISAKMP ポリシー名 「(任意で設定します)」
- 接続する本装置側の設定 「本装置側の設定1」

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

- 上位ルータの IP アドレス 「空欄」
- インタフェースの ID 「@host」
(@以降は任意の文字列)

※上記の2項目は、対向装置の「本装置の設定」と同じものを設定します。

- モードの設定 「aggressive モード」
- transform の設定 「group2-3des-sha1」
(任意の設定を選択)
- IKE のライフタイム 「3600」 (任意の設定値)

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

「IPsec ポリシーの設定」

「IPsec1」を選択します。

☐ 使用する ☐ 使用しない ☒ Responderとして使用する ☐ On-Demandで使用する	
使用するIKEポリシー名の選択	QKE1
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	(1~255まで)

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

- 使用する IKE ポリシー名の選択 「IKE1」
- 本装置側の LAN 側のネットワークアドレス
「192.168.0.0/24」
- 相手側の LAN 側のネットワークアドレス
「192.168.20.0/24」
- PH2 の TransForm の選択 「すべてを送信する」
- PFS 「使用する」 (推奨)
- DH Group の選択 「指定しない」
- SA のライフタイム 「28800」 (任意の設定値)
- DISTANCE 「空欄」
※省略した場合は、自動的にディスタンス値を「1」として扱います。

「IPsec Keep-Alive の設定」

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

第 13 章 IPsec 機能

VII. IPsec 設定例 1 (センター／拠点間の 1 対 1 接続)

■ XR_#2(拠点側 XR)の設定

各設定画面で下記のように設定します。

「本装置の設定」

「本装置側の設定 1」を選択します。

インターフェースの IP アドレス	%ppp0
上位ルータの IP アドレス	
インターフェースの ID	@host (例: @xr.centurysys)

○ インタフェースの IP アドレス 「%ppp0」

※ PPPoE 接続かつ動的アドレスの場合は、必ずこの設定にします。

○ 上位ルータの IP アドレス 「空欄」

※ PPPoE 接続かつ動的アドレスの場合は、空欄にしてください。

○ インタフェースの ID 「@host」

(@以降は任意の文字列)

※ 動的アドレスの場合は、必ず任意の ID を設定します。

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースの IP アドレス	213.xx.xx.193
上位ルータの IP アドレス	
インターフェースの ID	(例: @xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1 2 番目 使用しない 3 番目 使用しない 4 番目 使用しない
IKE のライフタイム	3600 秒 (1081~28800 秒まで)
鍵の設定	
☒ PSK を使用する ☐ RSA を使用する (X509 を使用する場合は RSA に設定してください)	test_key
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	

○ IKE/ISAKMP ポリシー名 「(任意で設定します)」

○ 接続する本装置側の設定 「本装置側の設定 1」

○ インタフェースの IP アドレス 「213.xx.xx.193」

※ 対向装置の IP アドレスを設定します。

○ 上位ルータの IP アドレス 「空欄」

※ 対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

○ インタフェースの ID 「空欄」

※ 対向装置が固定アドレスなので、設定不要です。

○ モードの設定 「aggressive モード」

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

○ IKE のライフタイム 「3600」(任意の設定値)

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

第13章 IPsec 機能

VII. IPsec 設定例 1 (センター／拠点間の1対1接続)

「IPsec ポリシーの設定」

「IPsec1」を選択します。

☐ 使用する ☐ 使用しない ☒ Responderとして使用する ☐ On-Demandで使用する	
使用するIKEポリシー名の選択	IKE2
本装置側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	2 (1~255まで)

- ☐ 「使用する」を選択します。
※動的アドレスの場合は、必ず initiator として動作します。
- ☐ 使用する IKE ポリシー名の選択 「IKE1」
- ☐ 本装置側の LAN 側のネットワークアドレス
「192.168.20.0/24」
- ☐ 相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」
- ☐ PH2 の TransForm の選択 「すべてを送信する」
- ☐ PFS 「使用する」(推奨)
- ☐ DH Group の選択 「指定しない」
- ☐ SA のライフタイム 「28800」(任意の設定値)
- ☐ DISTANCE 「空欄」
※省略した場合は、自動的にディスタンス値を「1」として扱います。

「IPsec Keep-Alive の設定」

PolicyNo.1 の行に設定します。

Policy No.	enable	source address	destination address	interval	watch count	timeout/delay/sec	Option 1	Option 2	interface	backup SA
1	☒	192.168.0.254	192.168.20.254	30	3	60	☐	☒	ipsec0	

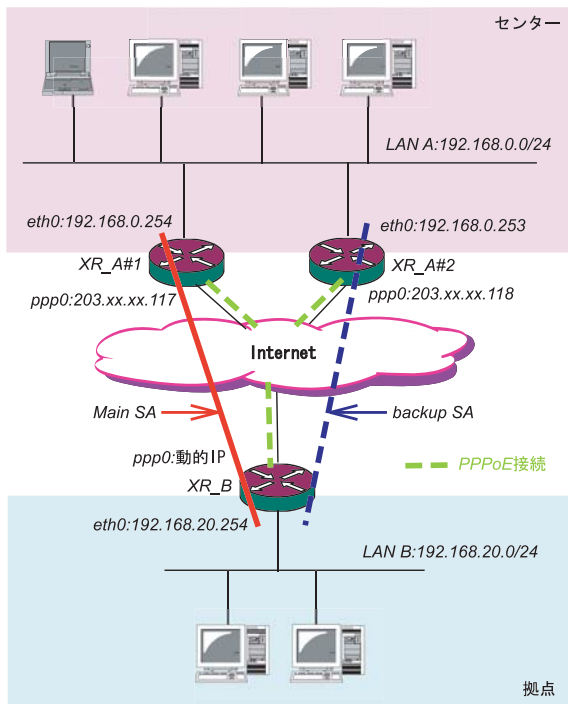
- ☐ enable にチェックを入れます。
- ☐ source address 「192.168.20.254」
- ☐ destination address 「192.168.0.254」
※ source address には本装置側 LAN のインタフェースアドレスを、destination address には相手側 LAN のインタフェースアドレスを設定することを推奨します。
- ☐ interval 「30」(任意の設定値)
- ☐ watch count 「3」(任意の設定値)
- ☐ timeout/delay 「60」(任意の設定値)
※動作オプション2を有効にするため、本値は delay(ping 送出開始待ち時間)=60 秒を意味します。
- ☐ 動作オプション1 「空欄」
- ☐ 動作オプション2 「チェック」
- ☐ interface 「ipsec0」
※ ppp0 上のデフォルトの IPsec インタフェース名は "ipsec0" です。
- ☐ backupSA 「空欄」

第13章 IPsec 機能

VIII.IPsec 設定例 2 (センター／拠点間の2対1接続)

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

<設定例2>



<接続条件>

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

「本装置の設定」

■XR_A#1(センター側XR#1)の設定

「本装置側の設定1」を選択します。

インターフェースのIPアドレス	203.xx.xx.117
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例: @xr.centurysys)

○インタフェースのIPアドレス「203.xx.xx.117」

○上位ルータのIPアドレス「%ppp0」

※ PPPoE 接続かつ固定IPアドレスの場合は、必ずこの設定にします。

○インタフェースのID「空欄」

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

■XR_A#2(センター側XR#2)の設定

「本装置側の設定1」を選択します。

インターフェースのIPアドレス	203.xx.xx.118
上位ルータのIPアドレス	%ppp0
インターフェースのID	(例: @xr.centurysys)

○インタフェースのIPアドレス「203.xx.xx.118」

○上位ルータのIPアドレス「%ppp0」

※ PPPoE 接続かつ固定IPアドレスの場合は、必ずこの設定にします。

○インタフェースのID「空欄」

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

第13章 IPsec 機能

VIII. IPsec 設定例 2 (センター／拠点間の2対1接続)

「IKE/ISAKMPポリシーの設定」

■ XR_A#1, XR_A#2 の IKE/ISAKMP ポリシーの設定

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

「IKE1」を選択します。

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	
インターフェースのID	@host (例: @xr.centurysys)
モードの設定	aggressive モード
transformの設定	1 番目 group2-3des-sha1 2 番目 使用しない 3 番目 使用しない 4 番目 使用しない
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
☒ PSKを使用する ☐ RSAを使用する (X509を使用する場合はRSAに設定してください)	test_key
X509の設定	
接続先の証明書の設定 (X509を使用しない場合は必要ありません)	

○ IKE/ISAKMP ポリシー名 「(任意で設定します)」

○ 接続する本装置側の設定 「本装置側の設定1」

○ インタフェースの IP アドレス 「0.0.0.0」

※対向装置が動的アドレスの場合は必ずこの設定にして下さい。

○ 上位ルータの IP アドレス 「空欄」

○ インタフェースの ID 「@host」

(@以降は任意の文字列)

※上記の2項目は、対向装置の「本装置の設定」と同じものを設定します。

○ モードの設定 「aggressive モード」

○ transform の設定 「group2-3des-sha1」

(任意の設定を選択)

○ IKE のライフタイム 「3600」(任意の設定値)

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

「IPSecポリシーの設定」

■ XR_A#1, XR_A#2 の IPSec ポリシーの設定

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

「IPSec1」を選択します。

使用するIKEポリシー名の選択	「IKE1」
本装置側のLAN側のネットワークアドレス	192.168.0.0/24 (例: 192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.20.0/24 (例: 192.168.0.0/24)
PH2のTransformの選択	すべてを送信する
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	(1~255まで)

○ 「Responder として使用する」を選択します。

○ 使用する IKE ポリシー名の選択 「IKE1」

○ 本装置側の LAN 側のネットワークアドレス

「192.168.0.0/24」

○ 相手側の LAN 側のネットワークアドレス

「192.168.20.0/24」

○ PH2 の Transform の選択 「すべてを送信する」

○ PFS 「使用する」(推奨)

○ DH Group の選択 「指定しない」

○ SA のライフタイム 「28800」(任意の設定値)

○ DISTANCE 「空欄」

第13章 IPsec 機能

VIII.IPsec 設定例 2 (センター／拠点間の2対1接続)

「転送フィルタ」の設定

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

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

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	宛て先アドレス	宛て先ポート	LOG	削除
ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.254			☐

- インターフェース 「ipsec0」
※ ppp0 のデフォルトの IPsec インタフェースの ”ipsec0” を設定します。
- 動作 「破棄」
※条件に合致するパケットを破棄。
- 送信元アドレス 「192.168.20.254」
※拠点側メイン SA の KeepAlive の送信元アドレスを設定します。
- 宛て先アドレス 「192.168.0.254」
※拠点側メイン SA の KeepAlive の送信先アドレスを設定します。

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

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	宛て先アドレス	宛て先ポート	LOG	削除
ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.253			☐

- インターフェース 「ipsec0」
※ ppp0 のデフォルトの IPsec インタフェースの ”ipsec0” を設定します。
- 動作 「破棄」
※条件に合致するパケットを破棄。
- 送信元アドレス 「192.168.20.254」
※拠点側バックアップ SA の KeepAlive の送信元アドレスを設定します。
- 宛て先アドレス 「192.168.0.253」
※拠点側バックアップ SA の KeepAlive の送信先アドレスを設定します。

「スタティックルート」の設定

センター側の XR では自分が IPsec 接続していないときに、拠点方向のルートを IPsec 接続中の XR へフローティングさせるために、スタティックルートの設定を行います。

自分が IPsec 接続しているときは、IPsec ルートのディスタンス値 (=1) の方が小さいため、このスタティックルートは無効の状態となっています。

■ XR_A#1 のスタティックルート設定

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

- アドレス 「192.168.20.0」
- ネットマスク 「255.255.255.0」
- ゲートウェイ 「192.168.0.253」
※ XR_A#2 のアドレスを設定します。

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

■ XR_A#2 のスタティックルート設定

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

- アドレス 「192.168.20.0」
- ネットマスク 「255.255.255.0」
- ゲートウェイ 「192.168.0.254」
※ XR_A#1 のアドレスを設定します。

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

第13章 IPsec 機能

VIII. IPsec 設定例 2 (センター／拠点間の2対1接続)

「IPsec Keep-Alive 設定」

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

■ XR_A#1 の IPsec Keep-Alive 設定

Policy No	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作オプション1	動作オプション2	interface	backup SA
1	☒	192.168.0.254	192.168.20.254	30	3	60			ipsec0	

- ☐ enable にチェックを入れます。
- ☐ source address 「192.168.0.254」
- ☐ destination address 「192.168.20.254」
- ☐ interval 「30」(任意の設定値) ※注)
- ☐ watch count 「3」(任意の設定値)
- ☐ timeout/delay 「60」(任意の設定値)
- ※動作オプション2を有効にするため、本値はdelay(ping送出開始待ち時間)=60秒を意味します。
- ☐ 動作オプション1 「空欄」
- ☐ 動作オプション2 「チェック」
- ☐ interface 「ipsec0」
- ☐ backupSA 「空欄」

■ XR_A#2 の IPsec Keep-Alive 設定

Policy No	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作オプション1	動作オプション2	interface	backup SA
1	☒	192.168.0.253	192.168.20.254	30	3	60		☒	ipsec0	

- ☐ enable にチェックを入れます。
- ☐ source address 「192.168.0.253」
- ☐ destination address 「192.168.20.254」
- ☐ interval 「30」(任意の設定値) ※注)
- ☐ watch count 「3」(任意の設定値)
- ☐ timeout/delay 「60」(任意の設定値)
- ※動作オプション2を有効にするため、本値はdelay(ping送出開始待ち時間)=60秒を意味します。
- ☐ 動作オプション1 「空欄」
- ☐ 動作オプション2 「チェック」
- ☐ interface 「ipsec0」
- ☐ backupSA 「空欄」

※注)

センター側と拠点側の interval が同じ値の場合、Keep-Aliveの周期が同期してしまい、障害時のIPsec切り替え直後に、切り替えた先でもすぐに障害を検出して、IPsec通信が不安定になることがあります。

これを防ぐために、センター側の interval は拠点側のメインSA、バックアップSAのいずれの interval と異なる値を設定することを推奨します。

但し、センター内のXR同士は同じ interval 値でも構いません。

第13章 IPsec 機能

VIII.IPsec 設定例 2 (センター／拠点間の2対1接続)

■ XR_B(拠点側 XR)の設定

「本装置の設定」

「本装置側の設定1」を選択します。

インターフェースのIPアドレス	%ppp0
上位ルータのIPアドレス	
インターフェースのID	@host (例:@xr.centurysys)

○インターフェースの IP アドレス 「%ppp0」

※ PPPoE 接続かつ動的アドレスの場合は、必ずこの設定にします。

○上位ルータの IP アドレス 「空欄」

※ PPPoE 接続かつ動的アドレスの場合は、空欄にして下さい。

○インターフェースの ID 「@host」

(@以降は任意の文字列)

※動的アドレスの場合は、必ず任意の ID を設定します。

メイン SA 用の IKE/ISAKMP ポリシーの設定を行います。

「IKE/ISAKMP ポリシーの設定」

「IKE1」を選択します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	203.xx.xx.117
上位ルータのIPアドレス	
インターフェースのID	(例:@xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1 2 番目 使用しない 3 番目 使用しない 4 番目 使用しない
IKE のライフタイム	3600 秒 (1081~28800 秒まで)
鍵の設定	
☒ PSK を使用する ☐ RSA を使用する (X509 を使用する場合は RSA に設定してください)	test_key
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	

○ IKE/ISAKMP ポリシー名 「(任意で設定します)」

○接続する本装置側の設定 「本装置側の設定1」

○インターフェースの IP アドレス 「203.xx.xx.117」

※対向装置が固定アドレスなので、その IP アドレスを設定します。

○上位ルータの IP アドレス 「空欄」

※対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

○インターフェースの ID 「空欄」

※対向装置が固定アドレスなので、設定不要です。

○モードの設定 「aggressive モード」

○transform の設定

1 番目 「group2-3des-sha1」 (任意の設定を選択)

2 ~ 4 番目 「使用しない」

○IKE のライフタイム 「3600」 (任意の設定値)

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

第13章 IPsec 機能

VIII. IPsec 設定例 2 (センター／拠点間の2対1接続)

バックアップ SA 用の IKE/ISAKMP ポリシーの設定を行います。

「IKE/ISAKMP ポリシーの設定」

「IKE2」を選択します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	
接続する本装置側の設定	本装置側の設定1
インターフェースの IP アドレス	203.xx.xx.118
上位ルータの IP アドレス	
インターフェースの ID	(例: @xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1 2 番目 使用しない 3 番目 使用しない 4 番目 使用しない
IKE のライフタイム	3600 秒 (1081～28800 秒まで)
鍵の設定	
☒ PSK を使用する ☐ RSA を使用する (X509 を使用する場合は RSA に設定してください)	test_key
X509 の設定	
接続先の証明書の設定 (X509 を使用しない場合は必要ありません)	

○IKE/ISAKMP ポリシー名 「(任意で設定します)」

○接続する本装置側の設定 「本装置側の設定1」

○インターフェースの IP アドレス 「203.xx.xx.118」

※対向装置が固定アドレスなので、その IP アドレスを設定します。

○上位ルータの IP アドレス 「空欄」

※対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

○インターフェースの ID 「空欄」

※対向装置が固定アドレスなので、設定不要です。

○モードの設定 「aggressive モード」

○transform の設定

1 番目 「group2-3des-sha1」 (任意の設定を選択)

2～4 番目 「使用しない」

○IKE のライフタイム 「3600」 (任意の設定値)

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

メイン SA 用の IPsec ポリシーの設定を行います。

「IPsec ポリシーの設定」

「IPsec1」を選択します。

☒ 使用する ☐ 使用しない ☐ Responder として使用する ☐ On-Demand で使用する	
使用するIKEポリシー名の選択	(IKE1)
本装置側のLAN側のネットワークアドレス	192.168.20.0/24 (例: 192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例: 192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081～86400 秒まで)
DISTANCE	1 (1～255 まで)

SA 用の IPsec ポリシーであるため、「使用する」を選択します。

○使用する IKE ポリシー名の選択 「IKE1」

○本装置側の LAN 側のネットワークアドレス

「192.168.20.0/24」

○相手側の LAN 側のネットワークアドレス

「192.168.0.0/24」

○PH2 の TransForm の選択 「すべてを送信する」

○PFS 「使用する」 (推奨)

○DH Group の選択 「指定しない」

○SA のライフタイム 「28800」 (任意の設定値)

○DISTANCE 「1」

※メイン側のディスタンス値は最小値(=1)を設定します。

第13章 IPsec 機能

VIII.IPsec 設定例 2 (センター／拠点間の2対1接続)

バックアップ SA 用の IPsec ポリシーの設定を行います。

「IPsec ポリシーの設定」

「IPsec2」を選択します。

☐ 使用する ☐ 使用しない ☒ Responderとして使用する ☐ On-Demandで使用する	
使用するIKEポリシー名の選択	IKE2
本装置側のLAN側のネットワークアドレス	192.168.20.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	192.168.0.0/24 (例:192.168.0.0/24)
PH2のTransFormの選択	すべてを送信する
PFS	☒ 使用する ☐ 使用しない
DH Groupの選択(PFS使用時に有効)	指定しない
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	2 (1~255まで)

☐ 「Responderとして使用する」を選択します。
※本装置は Initiator として動作しますが、バックアップ SA 用の IPsec ポリシーであるため、「Responderとして使用する」を選択して下さい。

- ☐ 使用する IKE ポリシー名の選択 「IKE2」
- ☐ 本装置側の LAN 側のネットワークアドレス
「192.168.20.0/24」
- ☐ 相手側の LAN 側のネットワークアドレス
「192.168.0.0/24」
- ☐ PH2 の TransForm の選択 「すべてを送信する」
- ☐ PFS 「使用する」(推奨)
- ☐ DH Group の選択 「指定しない」
- ☐ SA のライフタイム 「28800」(任意の設定値)
- ☐ DISTANCE 「2」

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

「IPsec Keep-Aliveの設定」

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

Policy No	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作オプション1	動作オプション2	interface	backup SA
1	☒	192.168.20.254	192.168.0.254	45	3	60	☐	☒	ipsec0	2
2	☒	192.168.20.254	192.168.0.253	60	3	60	☐	☒	ipsec0	

■メイン SA 用の KeepAlive の設定

PolicyNo.1の行に設定します。

- ☐ source address 「192.168.20.254」
- ☐ destination address 「192.168.0.254」
- ☐ interval 「45」(任意の設定値)
- ☐ watch count 「3」(任意の設定値)
- ☐ timeout/delay 「60」(任意の設定値)
- ☐ 動作オプション1 「空欄」
- ☐ 動作オプション2 「チェック」
- ☐ interface 「ipsec0」
- ☐ backupSA 「2」

※ Keep-Alive により障害検知した場合に、IPsec2 のポリシーに切り替えるため、「2」を設定します。

■バックアップ SA 用の KeepAlive の設定

PolicyNo.2の行に設定します。

- ☐ source address 「192.168.20.254」
- ☐ destination address 「192.168.0.253」
- ☐ interval 「60」(任意の設定値)
- ☐ watch count 「3」(任意の設定値)
- ☐ timeout/delay 「60」(任意の設定値)
- ☐ 動作オプション1 「空欄」
- ☐ 動作オプション2 「チェック」
- ☐ interface 「ipsec0」
- ☐ backupSA 「空欄」

※注)

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

IX. IPsec がつながらないとき

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

本体ログは、「システム設定」内の「ログ表示」で確認します。

[正常に IPsec 接続できたときのログメッセージ]

メインモードの場合

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

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

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

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

```
Aug 3 12:00:20 localhost ipsec__plutorun:
004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP SA
established
```

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

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

アグレッシブモードの場合

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

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

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

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

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

IX. IPsec がつながらないとき

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

[正常に IPsec が確立したときの表示例]

```
000 interface ipsec0/eth1 218.xxx.xxx.xxx
000
000 "xripsec1": 192.168.xxx.xxx/24
===218.xxx.xxx.xxx[@<id>]---218.xxx.xxx.xxx...
000 "xripsec1": ...219.xxx.xxx.xxx
===192.168.xxx.xxx.xxx/24
000 "xripsec1":  ike_life: 3600s; ipsec_life:
28800s; rekey_margin: 540s; rekey_fuzz: 100%;
keyingtries: 0
000 "xripsec1":  policy: PSK+ENCRYPT+TUNNEL+PFS;
interface: eth1; erouted
000 "xripsec1":  newest ISAKMP SA: #1; newest
IPsec SA: #2; eroute owner: #2
000
000 #2: "xripsec1" STATE_QUICK_I2 (sent QI2, IPsec
SA established); EVENT_SA_REPLACE in 27931s;
newest IPSEC; eroute owner
000 #2: "xripsec1" esp.32a406c4@219.xxx.xxx.xxx
esp.1be9611c@218.xxx.xxx.xxx
tun.1002@219.xxx.xxx.xxx tun.1001@218.xxx.xxx.xxx
000 #1: "xripsec1" STATE_MAIN_I4 (ISAKMP SA
established); EVENT_SA_REPLACE in 2489s; 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。設定を再確認して下さい。

IX. IPsec がつながらないとき

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

この場合は、接続相手との IKE 鍵交換が正常に行えていません。

IPsec 設定の「IKE/ISAKMP ポリシーの設定」項目で相手側機器についての設定を確認してください。

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

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

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

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

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

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

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

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

固定 IP - 動的 IP 間での main モード接続と aggressive モード接続を共存させることはできません。

このようなトラブルを避けるために、固定 IP - 動的 IP 間で IPsec 接続する場合は aggressive モードで接続するようにしてください。

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

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

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

これらの理由によって、IPsec 通信がなかなか復帰しない現象となります。

すぐに IPsec 通信を復帰させたいときは、動的 IP アドレス側の IPsec サービスも再起動する必要があります。

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

○相手の XR-440 には IPsec のログが出ているのに、こちらの XR-440 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-440 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 の状態が表示されます。

第 14 章

UPnP 機能

第14章 UPnP 機能

I. UPnP 機能 の設定

XR-440 は UPnP(Universal Plug and Play)に対応していますので、UPnP に対応したアプリケーションを使うことができます。

対応している Windows OS とアプリケーション

Windows OS

- Windows XP
- Windows Me

アプリケーション

- Windows Messenger

利用できる Messenger の機能について

以下の機能について動作を確認しています。

- インスタントメッセージ
- 音声チャット
- ビデオチャット
- リモートアクセス
- ホワイトボード

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

Windows OS の UPnP サービス

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

◆ UPnP 機能の設定

XR-440 の UPnP 機能の設定は以下の手順でおこなってください。

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

WAN側インターフェース	eth1
LAN側インターフェース	eth0
切断検知タイマー	5 分 (1～60分)

○ 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を設定します。本装置の各インターフェース名をそのまま入力してください。

○ LAN 側インターフェース

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

インターフェース名は、「付録 A インターフェース名について」を参照してください。

○ 切断検知タイマー

UPnP 機能使用時の無通信切断タイマーを設定します。ここで設定した時間だけ無通信時間が経過すると、XR-440 が保持する Windows Messenger のセッションが強制終了されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

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

第14章 UPnP 機能

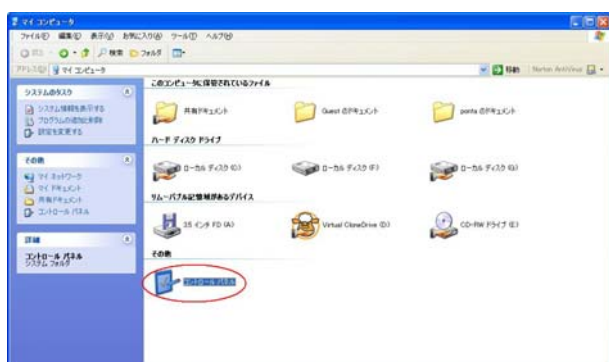
1. UPnP 機能 の設定

◆UPnP の接続状態の確認

各コンピュータがXR-440と正常にUPnPで接続されているかどうかを確認します。

1 「スタート」→「マイコンピュータ」を開きます。

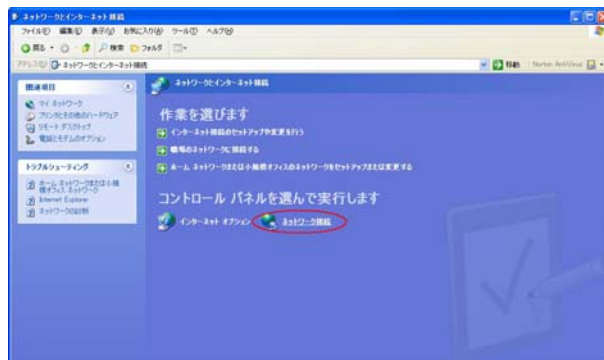
2 「コントロールパネル」を開きます。



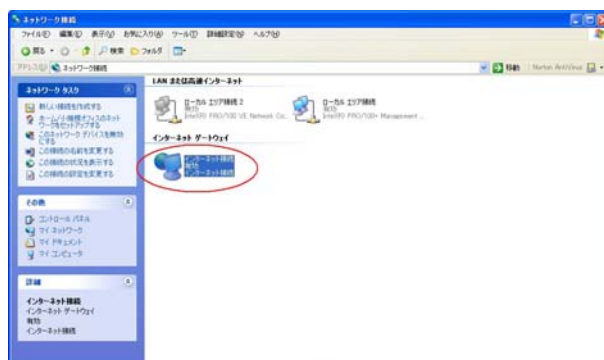
3 「ネットワークとインターネット接続」を開きます。



4 「ネットワーク接続」を開きます。



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



(画面はWindows XPでの表示例です)

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

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 東日本にお問い合わせ下さい)

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

◆ UPnP 機能使用時の推奨フィルタ設定

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

(入力フィルタ)

eth1	パケット受信時	破棄	udp				1900
ppp0	パケット受信時	破棄	udp				1900
eth1	パケット受信時	破棄	tcp				5000
ppp0	パケット受信時	破棄	tcp				5000
eth1	パケット受信時	破棄	tcp				2869
ppp0	パケット受信時	破棄	tcp				2869

(転送フィルタ)

eth1	パケット受信時	破棄	udp				1900
ppp0	パケット受信時	破棄	udp				1900
eth1	パケット受信時	破棄	tcp				5000
ppp0	パケット受信時	破棄	tcp				5000
eth1	パケット受信時	破棄	tcp				2869
ppp0	パケット受信時	破棄	tcp				2869

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

第 15 章

ダイナミックルーティング
(RIP/OSPF/BGP4)

第15章 ダイナミックルーティング

1. ダイナミックルーティング機能

XR-440シリーズのダイナミックルーティング機能は、RIP および OSPF をサポートしています。

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

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。

RIP	☒ 停止 ☐ 起動	停止中
OSPF	☒ 停止 ☐ 起動	停止中

「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。

第15章 ダイナミックルーティング

II. 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。

Ether0ポート	使用しない	バージョン1
Ether1ポート	使用しない	バージョン1
Ether2ポート	使用しない	バージョン1
Administrative Distance設定	120 (1-255) デフォルト120	
OSPFルートの再配信	☐ 有効 ☒ 無効	
再配信時のメトリック設定	(0-16) 指定しない場合は空白	
staticルートの再配信	☒ 有効 ☐ 無効	
staticルート再配信時のメトリック設定	(0-16) 指定しない場合は空白	
default-informationの送信	☐ 有効 ☒ 無効	

○ Ether0、Ether1、Ether2 ポート

XR-440 の各 Ethernet ポートで、RIP の使用 / 不使用、また使用する場合の RIP バージョンを選択します。

○ Administrative Distance 設定

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

○ OSPF ルートの再配信

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。

○ BGP ルートの再配信

BGP で学習したルーティング情報を RIP で配信したいときに「有効」にしてください。RIP のみを使う場合は「無効」にします。

○ 再配信時のメトリック設定

BGP ルートを RIP で配信するときのメトリック値を設定します。

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。

第15章 ダイナミックルーティング

III. OSPF の設定

OSPFはリンクステート型経路制御プロトコルです。

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

また OSPF は主に帯域幅からコストを求め、コストがもっとも低いものを最適な経路として採用します。

これにより、トラフィックのロードバランシングが可能となっています。

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

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

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

◆インタフェースへの OSPF エリア設定

どのインタフェースで OSPF 機能を動作させるかを設定します。

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

	ネットワークアドレス (例:192.168.0.0/24)	AREA番号 (0-4294967295)
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

○ネットワークアドレス

XR-440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。

第15章 ダイナミックルーティング

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	1 (0-4294967295)
スタブ設定	☐ 有効 ☒ 無効
トータルリースタブ設定	☐ 有効 ☒ 無効
default-cost	1 (0-16777215)
認証設定	使用しない
エリア間ルートの経路集約設定	

○ 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。

○トータルリースタブ設定

LSA type5に加え、type3、4も送信しないエリアに指定するときに「有効」にします。

○ default-cost 設定

スタブエリアに対してデフォルトルート情報を送信する際のコスト値を指定します。指定しない場合は1です。

○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。
Ex: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。

	AREA番号	STUB	Totally STUB	Default-cost	Authentication	経路集約	Configure
1	1	有効	無効	10	無効	192.168.10.1/29	Edit Remove

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

第15章 ダイナミックルーティング

III. OSPF の設定

◆ OSPF VirtualLink 設定

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

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

設定画面上部の「VirtualLink 設定」をクリックして設定します。

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

Transit AREA番号	0 (0-4294967295)
Remote-ABR Router-ID設定	192.168.0.1 (例:192.168.0.1)
Hello-インターバル設定	10 (1-65535)
Dead-インターバル設定	40 (1-65535)
Retransmit-インターバル設定	5 (3-65535)
transmit delay設定	1 (1-65535)
認証パスワード設定	(英数字で最大8文字)
MD5 KEY-ID設定(1)	(1-255)
MD5 パスワード設定(1)	(英数字で最大16文字)
MD5 KEY-ID設定(2)	(1-255)
MD5 パスワード設定(2)	(英数字で最大16文字)

○ 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。半角英数字のみ使用できます。

○ MD5 KEY-ID 設定(1)

MD5 認証使用時のKEY IDを設定します。

○ MD5 パスワード設定(1)

エリア内でMD5 認証を使用する際のMD5 パスワードを設定します。半角英数字のみ使用できます。

○ MD5 KEY-ID 設定(2)

○ MD5 パスワード設定(2)

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

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

入力後は「設定」をクリックしてください。

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

AREA番号	Remote-ABR ID	Hello	Dead	Retransmit	Transmit Delay	Auth Password	MD5 KEY-ID	MD5 Password	Configure
0	192.168.0.1	10	40	5	1	***	111	111-000	Edit/Remove

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

第 15 章 ダイナミックルーティング

III. OSPF の設定

◆ OSPF 機能設定

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

AS Number : 10 Remove	
Router-ID	(ex:192.168.0.1)
Scan Time	5 (5~60s)
connected再配信	☐ 有効 ☒ 無効 route-map設定
staticルート再配信	☐ 有効 ☒ 無効 route-map設定
RIPルート再配信	☐ 有効 ☒ 無効 route-map設定
OSPFルート再配信	☐ 有効 ☒ 無効 route-map設定
Distance for routes external to the AS	20 (1~255)
Distance for routes internal to the AS	200 (1~255)
Distance for local routes	200 (1~255)
network import-check	☐ 有効 ☒ 無効
always-compare-med	☐ 有効 ☒ 無効
enforce-first-as	☐ 有効 ☒ 無効
Bestpath AS-PATH ignore	☐ 有効 ☒ 無効
Bestpath med missing-as-worst	☐ 有効 ☒ 無効
default local-pref	(0~4294967295)

○ 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 の再配信

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

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

○ static ルートの再配信

static ルートを OSPF で配信するかどうを選択します。**IPsec ルートを再配信する場合も、この設定を「有効」にする必要があります。**

「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

○ RIP ルートの再配信

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

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

○ BGP ルートの再配信

BGP で学習したルート情報を OSPF で配信するかどうを選択します。「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。

第15章 ダイナミックルーティング

III. OSPF の設定

○ 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」の場合、ルータがデフォルトルートを持っていれば送信されます。

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

「送信する」「常に送信する」の場合は、以下の2項目についても設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

○ 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。

第15章 ダイナミックルーティング

III. OSPF の設定

◆インタフェース設定

各インタフェースごとの OSPF 設定を行ないます。

設定画面上部の「インタフェース設定」をクリックして設定します。

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

インタフェース名	eth0
Passive-Interface設定	☐ 有効 ☒ 無効
コスト値設定	(1~65535)
帯域設定	(1~1000000000kbps)
Hello-インターバル設定	10 (1~65535s)
Dead-インターバル設定	40 (1~65535s)
Retransmit-インターバル設定	5 (3~65535s)
Transmit Delay設定	1 (1~65535s)
認証キー設定	(英数字で最大8文字)
MD KEY-ID設定(1)	(1~255)
MD5 パスワード設定(1)	(英数字で最大16文字)
MD KEY-ID設定(2)	(1~255)
MD5 パスワード設定(2)	(英数字で最大16文字)
Priority設定	(0~255)
MTU-Ignore設定	☐ 有効 ☒ 無効

○インタフェース名

設定する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 インタフェース名について」を参照してください。

○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。

○認証パスワード設定

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。半角英数字のみ使用できます。

○MD5 KEY-ID 設定(1)

MD5 認証使用時の KEY ID を設定します。

○MD5 パスワード設定(1)

VirtualLink 上で MD5 認証を使用する際の MD5 パスワードを設定します。半角英数字のみ使用できます。

○MD5 KEY-ID 設定(2)

○MD5 パスワード設定(2)

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

○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 になる)。どうしても MTU を合わせることができないときには、この MTU 値の不一致を無視して Neighbor (Full) を確立させるための MTU-Ignore を「有効」にしてください。

第15章 ダイナミックルーティング

III. OSPF の設定

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。

インタフェース名	Passive	Cost	帯域	Hello	Dead	Retransmit	Transmit Delay	パスワード	MD5 KEY-ID	MD5 Password	Priority	MTU	Configure
eth0	on	10	1000000	10	40	5	1	century	150	centurysystem	50	off	Edit Remove

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

◆ステータス表示

OSPF の各種ステータスを表示します。

設定画面上部の「ステータス表示」をクリックして設定します。

OSPF データベースの表示 (各 Link state 情報が表示されます)	表示する
ネイバリスト情報の表示 (現在のネイバ状態を確認できます)	表示する
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)	表示する
OSPF 統計情報の表示 (SPF 計算回数などの情報を表示します)	表示する
インタフェース情報の表示 (表示したいインタフェースを指定して下さい)	表示する

○ OSPF データベース表示

LinkState 情報が表示されます。

○ ネイバリスト情報の表示

現在のネイバ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。

第 15 章 ダイナミックルーティング

IV. BGP4 の設定

◆ BGP4 の起動

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

「各種サービスの設定」→「ダイナミックルーティング」を開いて、起動 / 停止をおこないます。

RIP	☒ 停止 ☐ 起動	停止中	再起動
OSPF	☒ 停止 ☐ 起動	停止中	再起動
BGP4	☐ 停止 ☒ 起動	動作中	再起動

動作変更

再起動

○ BGP の起動

「BGP4」行で「起動」にチェックし、「動作変更」ボタンをクリックします。

○ BGP の停止

「BGP4」行で「停止」にチェックし、「動作変更」ボタンをクリックします。

○ BGP の再起動

「BGP4」行で「再起動」ボタンをクリックします。

○ダイナミックルーティングの全てを再起動する
「動作変更」ボタンの右隣にある「再起動」ボタンをクリックします。

○表中の「BGP4」をクリックすると、BGP の設定画面に移ることができます。

◆ BGP4 設定

はじめに BGP4 の AS 番号を設定し、各種設定をおこないます。BGP4 Configuration MENU 画面上部の「BGP Setup」をクリックします。

AS Number	(1-65535)
-----------	--

Commit

○ AS Number

AS 番号を設定します。

設定後に「commit」ボタンをクリックします。

AS 番号を設定した後は、引き続き「BGP4 機能設定」「BGP4 Aggregate Setup」「BGP4 Neighbor Setup」「BGP4 Network Setup」の設定ができるようになります。

第15章 ダイナミックルーティング

IV. BGP4 の設定

BGP4 機能設定(BGP4 Setup 画面)

Router-IDやルート情報再配信などの設定をおこないます。

BGP4 Setup 画面上部の「BGP 機能設定」をクリックして設定します。

AS Number: 10 Remove	
Router-ID	(ex:192.168.0.1)
Scan Time	5 (5-60s)
connected再配信	☐ 有効 ☒ 無効 route-map設定
staticルート再配信	☐ 有効 ☒ 無効 route-map設定
RIPルート再配信	☐ 有効 ☒ 無効 route-map設定
OSPFルート再配信	☐ 有効 ☒ 無効 route-map設定
Distance for routes external to the AS	20 (1-255)
Distance for routes internal to the AS	200 (1-255)
Distance for local routes	200 (1-255)
network import-check	☐ 有効 ☒ 無効
always-compare-med	☐ 有効 ☒ 無効
enforce-first-as	☐ 有効 ☒ 無効
Bestpath AS-PATH ignore	☐ 有効 ☒ 無効
Bestpath med missing-as-worst	☐ 有効 ☒ 無効
default local-pref	(0-4294967295)

○ Router-ID

Router-IDをIPアドレス形式で設定します。

○ Scan Time

Scan Timeを設定します。

○ connected再配信

ConnectedルートをBGP4で再配信したい場合には「有効」を選択します。また routemap を適用するときは、「routemap」欄に routemap 名を設定して下さい。

○ staticルート再配信

StaticルートをBGP4で再配信したい場合には「有効」を選択します。また routemap を適用するときは、「routemap」欄に routemap 名を設定して下さい。

○ RIP ルート再配信

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

○ OSPF ルート再配信

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

○ Distance for routes external to the AS

eBGPルートのadministrativeディスタンス値を設定します。

○ Distance for routes internal to the AS

iBGPルートのadministrativeディスタンス値を設定します。

○ Distance for local routes

local route(aggregate設定によってBGPが学習したルート情報)のadministrative Distance値を設定します。

○ network import-check

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

○ always-compare-med

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

○ enforce-first-as

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

IV. BGP4 の設定

○ Bestpath AS-PATH ignore

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

○ Bestpath med missing-as-worst

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

○ default local-pref

local preference 値のデフォルト値を変更します。デフォルト値は「100」です。

設定後は「Commit」ボタンをクリックしてください。

設定の削除は、BGP4 機能設定画面上部にある「Remove」をクリックしてください。

BGP4 Aggregate Setup(BGP4 Setup 画面)

Aggregate Address の設定を行います。

BGP4 Setup 画面上部の「BGP Aggregate Address Setup」をクリックして設定します。

	Aggregate Address	Summary	Configure
1	192.168.0.0/16	有効	Edit, Remove

New Entry

(画像は一覧表示の例です)

新規に設定するときは「New Entry」を、設定内容を変更するときは一覧表示の「Edit」をクリックして、Aggregate Address の設定を行います。設定を削除するときは、一覧表示の「Remove」をクリックして下さい。

[設定画面]

Aggregate Address	192.168.0.0/16 (ex 192.168.0.0/16)
summary only	☐ 有効 ☒ 無効

○ Aggregate Address

集約したいルートを設定します。

○ summary only

集約ルートのみを配信したい場合に「有効」を選択して下さい。

設定後は「設定」ボタンをクリックしてください。

第15章 ダイナミックルーティング

IV. BGP4 の設定

BGP4 neighbor Setup(BGP4 Setup 画面)

Neighbor Address の設定を行います。

BGP4 Setup 画面上部の「BGP neighbor Setup」をクリックして設定します。

Neighbor Address	Remote as	keepalive interval	hold time	connect time	default originate	next hop self	update source	ebgp multihop	soft reconf in	incoming routemap	outgoing routemap	Filter incoming updates	Filter outgoing updates	Configure
192.168.22.2	5	60	180	120	no	no	eth0	20	no	maptest	maptest	test	test	Edit/Remove

(画像は一覧表示の例です)

新規に設定するときは「New Entry」を、設定内容を変更するときは一覧表示の「Edit」をクリックして、Neighbor Address の設定を行います。設定を削除するときは、一覧表示の「Remove」をクリックして下さい。

[設定画面]

Neighbor Address	192.168.1.1 (ex:192.168.1.1)
Remote AS Number	1 (1-65535)
Keepalive interval	60 (0-65535)
Holdtime	180 (0-65535)
Next Connect Timer	120 (0-65535)
default-originate	☐ 有効 ☒ 無効
next hop-self	☐ 有効 ☒ 無効
update-source	(interfaceを指定)
ebgp-multihop	1 (1-255)
soft-reconfiguration inbound	☐ 有効 ☒ 無効
Apply map to incoming routes	(routemap名指定)
Apply map to outbound routes	(routemap名指定)
Filter incoming updates	(ACL名指定)
Filter outgoing updates	(ACL名指定)

○ Neighbor Address

BGP Neighbor のアドレスを設定します。

○ Remote AS Number

対向装置の AS Number を設定します。

○ Keepalive Interval

Keepalive の送信間隔を設定します。

○ Holdtime

Holdtime を設定します。

○ default-originate

デフォルトルートを送信する場合に「有効」を選択します。

○ next hop-self

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

○ update-source

BGP パケットのソースアドレスを、指定したインタフェースの IP アドレスに変更します。

○ ebgp-multihop

「有効」を選択すると、eBGP の Neighbor ルータが直接接続されていない場合に、ホップ数を設定します。

○ soft-reconfiguration inbound

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

○ Apply map to incoming routes/Apply map to outbound routes

incoming route/outbound route に適用する routemap を指定します。

○ Filter incoming updates/Filter outgoing updates

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

設定後は「設定」ボタンをクリックしてください。

IV. BGP4 の設定

BGP4 network Setup(BGP4 Setup 画面)

Network Address の設定を行います。

BGP4 Setup 画面上部の「BGP network Setup」をクリックして設定します。

	Network Address	Backdoor	Configure
1	192.168.1.0/24	無効	Edit, Remove

New Entry

(画像は一覧表示の例です)

新規に設定するときは「New Entry」を、設定内容を変更するときは一覧表示の「Edit」をクリックして、Network Address の設定を行います。設定を削除するときは、一覧表示の「Remove」をクリックして下さい。

[設定画面]

Specify a network to announce via BGP	192.168.0.0/24 (ex:192.168.0.0/24)
backdoor	☐ 有効 ☒ 無効

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

☐ backdoor
backdoor 機能を使用したい場合に有効にします。

設定後は「設定」ボタンをクリックしてください。

◆ BGP4 ROUTE-MAP Setup

Route-MAP の設定を行います。

BGP4 Configuration MENU 画面上部にある「BGP Route-MAP Setup」をクリックして設定します。

RouteMap (name, permit/deny, sequence)	Rules	
map1, permit, 1 Edit, Remove	match ip address ACL1 set ip 10.10.10.2 Add	Edit, Remove Edit, Remove
map2, permit, 2 Edit, Remove	match ip next-hop ACL2 set as-path 10000 Add	Edit, Remove Edit, Remove
map3, permit, 3 Edit, Remove	match metric 100 set as-precedence 15000 10.10.10.3 Add	Edit, Remove Edit, Remove

New Route-MAP Entry

(画像は一覧表示の例です)

新規に設定するときは「New Route-MAP Entry」を、設定内容を変更するときは一覧表示の RouteMap 列から「Edit」を選択して RouteMap の設定を行います。設定を削除するときは、一覧表示の「Remove」をクリックして下さい。

[設定画面]

route-map name	
permit/deny	☒ permit ☐ deny
sequence number	1 (1-65535)

☐ route-map name
Route-MAP の名前を設定します。

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

"match" 条件、"set" アクションの設定については「BGP4 Route-MAP rules」設定画面で設定します。

☐ sequence number
すでに設定されている Route-MAP のリストの中で、新しい Route-MAP リストの位置を示す番号です。
若い番号のリストが上位に置かれます。

最後に設定ボタンをクリックしてください。再度「BGP Route-MAP Setup」を開くと、Route-Map 一覧表示画面が表示されます。
続いて BGP4 Route-MAP rules の設定を行います。

IV. BGP4 の設定

BGP4 Route-MAP rules の設定は、設定画面上部の「BGP Route-MAP Setup」の一覧表示から、Rules 列の「Add」または「Edit」をクリックして行います。設定を削除するときは、Rules 列の「Remove」をクリックして下さい。

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

「match」は match 条件を設定します。

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

○ match

match 条件を設定するときにチェックを入れてください。条件は以下の3つのものが設定できます。

• ip address

アクセスリストで指定した IP アドレスを match 条件とします。また match 条件となるアクセスリスト名を「ACL NAME」欄に入力してください。

• ip next-hop

next-hop の IP アドレスがアクセスリストで指定した IP アドレスと同じものを match 条件とします。また match 条件となるアクセスリスト名を「ACL NAME」欄に入力してください。

• metric

ここで指定した metric 値を match 条件とします。

○ set

match 条件にヒットしたときの属性値を設定します。以下のものが設定できます。

• aggregator

アグリゲータ属性を付加します。アグリゲータ属性は、集約経路を生成した AS や BGP ルータを示します。

AS Number 欄に AS 番号を、Aggregator Address 欄に IP アドレスを設定します。

• as-path

AS 番号を付加します。AS Number 欄に AS 番号を設定します。

• atomic-aggregate

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

• ip

ネクストホップの IP アドレスを付加します。next-hop 欄に IP アドレスを設定してください。

• local-preference

Local Preference 属性を付加します。これは、同一 AS 内部で複数経路の優先度を表すために用いられる値で、大きいほど優先されます。

IV. BGP4 の設定

• metric

metric属性を付加します。

• origin

origin属性を付加します。origin属性は、経路の生成元を示す属性です。

「IGP」は経路情報をAS内から学習したことを示します。

「EGP」は経路情報をEGPから学習したことを示します。

「Incomplete」は経路情報を上記以外から学習したことを示します。

◆ BGP4 ACL 設定

BGP4 のACL (ACCESS-LIST)設定を行います。

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

新規に設定を開始するときは「New Entry」をクリックしたときは、はじめにACL名を設定します。access-list name欄に任意のACL名を設定してください。半角英数字で32文字まで設定できます。その後、設定ボタンをクリックします。

access-list name	
------------------	----------------------

ACL名の設定後、またはすでにACL設定をしているときは、「BGP network Setup」をクリックするとACL設定一覧表示画面になります。

ACL Name	Rules
test Edit,Remove	deny 192.168.1.0/24 Add

New ACL Entry

(画像は一覧表示の例です)

一覧表示からRule列の「Edit」をクリックして、Network Addressの設定を行います。

acl name : test	
permit/deny	permit
prefix to match	(ex:192.168.0.0/24)

○ permit/deny

permit(許可)/deny(拒否)条件を選択します。

○ prefix to match

マッチング対象とするネットワークアドレスを設定します。「IPアドレス/マスクビット値」の形式で設定します。

ACL設定を削除するときは、一覧表示の「Remove」をクリックして下さい。

◆ BGP4 情報表示

BGP4の各種情報表示を行います。

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

○ BGP Table

BGPのルーティングテーブル情報を表示します。
入力欄でネットワークを指定すると、指定されたネットワークのみ表示します。

○ Detailed information BGP Neighbor

BGP Neighborの詳細情報を表示します。

「advertised-routes」はBGP Neighbor ルータへ配信しているルート情報を表示します。

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

「route」はBGP Neighbor から学習したルート情報を表示します。Neighbor Addressを指定すると、指定されたNeighbor に関係した情報のみ表示されます。

○ Summary of BGP neighbor status

BGP Neighborのステータスを表示します。

○ Clear BGP peers

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

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

第 16 章

PPPoE to L2TP

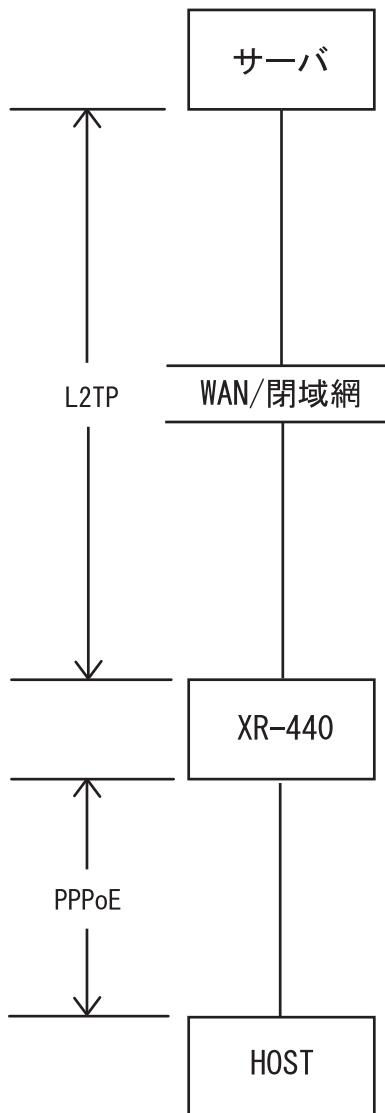
第16章 PPPoE to L2TP

PPPoE to L2TP 機能について

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

構成は以下のようなものになります。

構成図



- HOST からサーバへ PPPoE 接続をおこないますが、XR-440 とサーバ間は L2TP での通信に変換します。HOST は PPPoE 接続を維持します。
- XR-440 は上記構成図におけるサーバになることはできません。

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

L2TP トンネルの設定

「L2TP Tunnel 設定」→「New Entry」をクリックします。

Description	
Peerアドレス	(例:192.168.0.1)
パスワード	(英数字95文字まで)
ポート番号	1701 (default 1701)
AVP Hiding設定	☐ 有効 ☒ 無効
Hello Interval設定	60 (default 60s)

○ Description

任意の設定名をつけます(省略可能)。

○ Peer アドレス

L2TP で接続するサーバの IP アドレスを入力します。

○ パスワード

L2TP 接続時のパスワードを入力します。

○ ポート番号

ポート番号を入力します。通常は初期設定 1701 を使用します。

○ AVP Hiding 設定

AVP Hiding の使用 / 不使用を選択します。

○ Hello Interval 設定

Hello パケットの送信間隔を設定します(単位:秒)。

最後に「設定」をクリックします。

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

第16章 PPPoE to L2TP

PPPoE to L2TP 機能について

オプション設定

「L2TP Tunnel 設定」→「PPPoEtoL2TP オプション設定」をクリックします。

Local hostname	localhost
PPPoE Frame受信インタフェース設定	☒ eth0 ☐ eth1 ☐ eth2
MAX Session数	256 (max 256)
Debug設定 (Syslogメッセージ出力設定)	☐ Tunnel Debug出力 ☐ Session Debug出力 ☒ L2TPエラーメッセージ出力 ☐ PPPoE Debug出力

ステータス表示

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

○ Local hostname

任意の Local hostname 名をつけます。

○ PPPoE Frame 受信インタフェース設定

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

○ MAX session 数

PPPoE to L2TP 接続での最大セッション数を設定します。

○ Path MTU Discovery

Path MTU Discovery 機能を有効にするかを選択します。本機能を有効にした場合は、本装置が送信する L2TP パケットの DF(Don't Fragment)ビットを 1 にします。無効にした場合は、DF ビットを常に 0 にして送信します。

○ Debug 設定(Syslog メッセージ出力設定)

syslog に出力する Debug ログの種類を選択します。

最後に「設定」をクリックします。

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

第 17 章

SYSLOG サービス

第17章 SYSLOG サービス

syslog 機能の設定

XR-440 は、syslog を出力・表示することが可能です。また、他の syslog サーバに送出することもできます。さらに、ログの内容を電子メールで送ることもできます。

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 本装置 送信先IPアドレス 取得プライオリティ ☐ Debug ☒ Info ☐ Notice --MARK--を出力する時間間隔 20 分 (0を設定すると--MARK--の出力を停止します。) (MARKを使用する場合は取得プライオリティを Debug か Info にしてください。)
システムメッセージ	☒ 出力しない ☐ MARK出力時 ☐ 1時間毎に出力
ログのメール送信	☒ 送信しない ☐ 送信する 送信先メールアドレス 送信元メールアドレス 件名 中継するサーバアドレス
検出文字列の指定	文字列は1行に255文字まで、最大32個(行)までです。

ログの取得

○出力先

ログの出力先を「本装置」「SYSLOG サーバ」「本装置と SYSLOG サーバ」から選択します。

○送信先 IP アドレス

出力先で「SYSLOG サーバ」または「本装置と SYSLOG サーバ」を指定した場合に、SYSLOG サーバの IP アドレスを指定します。

○取得プライオリティ

ログ内容の出力レベルを指定します。プライオリティの内容は右の通りです。

• Debug：デバッグ時に有益な情報

• Info：システムからの情報

• Notice：システムからの通知

○--MARK-- を出力する時間間隔

syslog が動作していることを表す「--MARK--」ログを送出する間隔を指定します。取得プライオリティを Info または Debug に設定したときのみ MARK が出力されます。初期設定は 20 分です。

XR-440 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。「出力しない」「MARK 出力時」「1 時間毎に出力」から選択します。

○出力しない

システム情報を出力しません。

○MARK 出力時

システム情報を ”--MARK-- ” の出力と同時に出力します。

○1 時間毎に出力

システム情報を 1 時間毎に出力します。

出力される情報は下記の内容です。

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

- cpu : cpu のロードアベレージです。
1 に近いほど高負荷を表し、1 を超えている場合は過負荷の状態を表します。
- mem : 空きメモリ量(byte)です。
- session:XX/YY
XR 内部で保持している NAT/IP マスカレードのセッション情報数です。
XX: 現在 Establish している TCP セッションの数
YY: XR が現在キャッシュしている全てのセッション数

ログメール機能設定

○送信しない / 送信する

ログの内容を電子メールで送信するかどうか選択します。

○送信先メールアドレス

ログメッセージの送信先メールアドレスを指定します。

○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指定します（任意で指定）。

○件名

ログメッセージの件名を指定します（任意で指定）。半角英数字のみ使用できます。

○中継するサーバアドレス

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

<入力形式> @ <ドメイン名>

<入力例> @mail.xxxxxx.co.jp

「送信元メールアドレス」「件名」「中継するサーバアドレス」を何も指定しないときは

送信元アドレス: 「root@localdomain.co.jp」
件名: 空欄

で送信されます。

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検出して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。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ので注意してください。**

文字列の指定は、1 行につき 256 文字まで、かつ最大 32 行までです。空白・大文字 / 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（「**検出文字列の指定**」項目は、「**ログメール機能**」でのみ有効です）。

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（「停止」→「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-440 シリーズで設定されている syslog のファシリティ・監視レベルおよび出力先は以下のようになっています。

[ファシリティ：監視レベル]

***.info;mail.none;news.none;authpriv.none**

[出力先]

/var/log/messages

<オプションCFカード装着時の syslog 機能について>

オプションCFカードを装着している場合は、システムログは自動的にCFカードに記録されます。

ログはローテーションしてCFカードに記録されていきます。記録のタイミングは

- ・1週間ごと
- ・CFカードの空き容量が20%に達したとき

のいずれか早い方です。

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4つです。以降は古いログファイルから順に削除されていきます。

ログファイルが作成されたときは画面上にリンクが生成され、各端末にダウンロードして利用できます。

第 18 章

攻撃検出機能

攻撃検出機能の設定

攻撃検出機能の概要

攻撃検出機能とは、外部から LAN への侵入や XR-440 を踏み台にした他のホスト・サーバ等への攻撃を仕掛けられた時などに、そのログを記録しておくことができる機能です。検出方法には、統計的な面から異常な状態を検出する方法やパターンマッチング方法などがあります。XR-440 ではあらかじめ検出ルールを定めていますので、パターンマッチングによって不正アクセスを検出します。ホスト単位その他、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	☐ Ether 0 で使用する ☒ Ether 1 で使用する ☐ Ether 2 で使用する ☐ PPP/PPPoE で使用する
検出対象となる IP アドレス	any

○使用するインターフェース

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

○検出対象となる IP アドレス

攻撃を検出する、本装置のインターフェースの IP アドレスネットワークアドレスを指定します。

<入力例>

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

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

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

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

第 19 章

SNMP エージェント機能

第19章 SNMP エージェント機能

SNMP エージェント機能の設定

SNMP エージェントを起動すると、SNMP マネージャから XR-440 の MIB Ver.2(RFC1213)の情報を取得することができます。

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	192.168.0.0/24 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)又はSNMP マネージャのIPアドレスを指定して下さい。
コミュニティ名	community
SNMP TRAP	☐ 使用する ☒ 使用しない
SNMP TRAP の送信先 IP アドレス	
SNMP TRAP の送信元	☒ 指定しない ☐ IP アドレス ☐ インタフェース
送信元	☒ 指定しない ☐ IP アドレス

○ 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) 又は SNMP マネージャの IP アドレスを指定します。

○ コミュニティ名

任意のコミュニティ名を指定します。
ご使用の SNMP マネージャの設定に合わせて入力してください。

○ SNMP TRAP

SNMP TRAP を送信する場合は「使用する」選択します。

○ SNMP TRAP の送信先 IP アドレス

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

○ SNMP TRAP の送信元

Trap フレーム内の Agent address を指定することができます。

・ 指定しない

本装置の IP アドレスが自動的に設定されます。

・ IP アドレス

IP アドレスで指定します。入力欄に本装置の IP アドレスを設定して下さい。

・ インタフェース

インタフェースで指定します。入力欄に本装置のインタフェース名を入力して下さい(入力可能なインタフェース: Ether/PPP)。

○ 送信元

SNMP RESPONSE パケットの送信元アドレスを設定します。IPsec 接続を通して、リモート拠点のマネージャから SNMP を取得したい場合は、ここに IPsec SA の LAN 側アドレスを指定して下さい。

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。

SNMP エージェント機能の設定

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。

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

SNMP TRAPを送信するトリガーについて

以下のものに関して、SNMP TRAP を送信します。

- Ethernet インタフェースの up、down
(但し eth2 は除きます)
- PPP インタフェースの up、down
- 下記の各機能の up、down
 - DNS
 - DHCP サーバー
 - DHCP リレー
 - PLUTO(IPSec の鍵交換を行う IKE 機能)
 - UPnP
 - RIP
 - OSPF
 - SYSLOG
 - PPPoE to L2TP
 - 攻撃検出
 - NTP
 - VRRP
- SNMP TRAP 自身の起動、停止

第 20 章

NTP サービス

第20章 NTP サービス

NTP サービスの設定方法

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

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

問合せ先 NTP サーバ (IP アドレス/FQDN)	1.	Polling 間隔 (Min) 6 (Max) 10
	2.	Polling 間隔 (Min) 6 (Max) 10
Polling 間隔 X を指定した場合、秒単位の間隔は 2^X (sec) ex. (4: 16sec, 6: 64sec, ... 10: 1024sec)		
時刻同期タイムアウト時間	1 (秒:1~10) NTP サービス起動時に適用されます	

○問い合わせ先 NTP サーバ

NTP サーバの IP アドレスもしくは FQDN を入力欄に記入します (2 箇所設定可)。これにより、本装置が NTP クライアント / サーバとして動作できます。

指定しない場合は、本装置は NTP サーバとしてのみ動作します。

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。

(現在の NTP サービスの動作状況は「情報表示」で確認できます)

○Polling 間隔

NTP サーバと通信を行う間隔を設定します。
サーバとの接続状態により、指定した最小値と最大値の範囲でポーリングの間隔を調整します。

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

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

例 X=4 : 16 秒、X=6 : 64 秒、... X=10 : 1024 秒

初期設定は (Min)6 (64 秒)、(Max)10 (1024 秒) です。

初期設定のまま NTP サービスを起動させると、はじめは 64 秒間隔で NTP サーバとポーリングをおこない、その後は 64 秒から 1024 秒の間で NTP サーバとポーリングをおこない、時刻のずれを徐々に補正していきます。

○時刻同期タイムアウト時間

サーバ応答の最大待ち時間を設定できます (指定可能な範囲 : 1 ~ 10 秒)。

NTP サービスの設定方法

基準 NTP サーバについて

基準となる NTP サーバには次のようなものがあります。

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

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

NTP クライアントの設定方法

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

○Windows 9x/Me/NT の場合

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

○Windows 2000 の場合

「net time」コマンドを実行することにより時刻の同期を取ることができます。コマンドの詳細については Microsoft 社にお問い合わせ下さい。

○Windows XP の場合

Windows 2000 と同様のコマンドによるか、「日付と時刻のプロパティ」で NTP クライアントの設定ができます。詳細については Microsoft 社にお問い合わせください。

○Macintosh の場合

コントロールパネル内の NTP クライアント機能で設定してください。詳細は Apple 社にお問い合わせください。

○Linux の場合

Linux 用 NTP サーバをインストールして設定してください。詳細は NTP サーバの関連ドキュメント等をご覧ください。

第 21 章

VRRP サービス

第21章 VRRP サービス

I.VRRP の設定方法

VRRP は動的な経路制御ができないネットワーク環境において、複数のルータのバックアップ(ルータの多重化)をおこなうためのプロトコルです。

「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。

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	51	100	192.168.0.251	1	指定しない	
2	使用しない	使用しない	52	100		1	指定しない	
3	使用しない	使用しない	53	100		1	指定しない	
4	使用しない	使用しない	54	100		1	指定しない	
5	使用しない	使用しない	55	100		1	指定しない	
6	使用しない	使用しない	56	100		1	指定しない	
7	使用しない	使用しない	57	100		1	指定しない	
8	使用しない	使用しない	58	100		1	指定しない	
9	使用しない	使用しない	59	100		1	指定しない	
10	使用しない	使用しない	60	100		1	指定しない	
11	使用しない	使用しない	61	100		1	指定しない	
12	使用しない	使用しない	62	100		1	指定しない	
13	使用しない	使用しない	63	100		1	指定しない	
14	使用しない	使用しない	64	100		1	指定しない	
15	使用しない	使用しない	65	100		1	指定しない	
16	使用しない	使用しない	66	100		1	指定しない	

○使用するインタフェース

VRRP を作動させるインタフェースを選択します。

注) v1.7.6版の時点ではインタフェースにEther2を選択した場合、正常にマスター化ができません。Ether0 または Ether1 を使用して下さい。

○仮想 MAC アドレス

VRRP 機能を運用するときに、仮想 MAC アドレスを使用する場合は「使用する」を選択します。「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

認証を行なう場合のパスワードを設定します。半角英数字で8文字まで設定できます。
Auth_Type を「指定しない」にした場合は、パスワードは設定しません。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

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

ステータスの表示

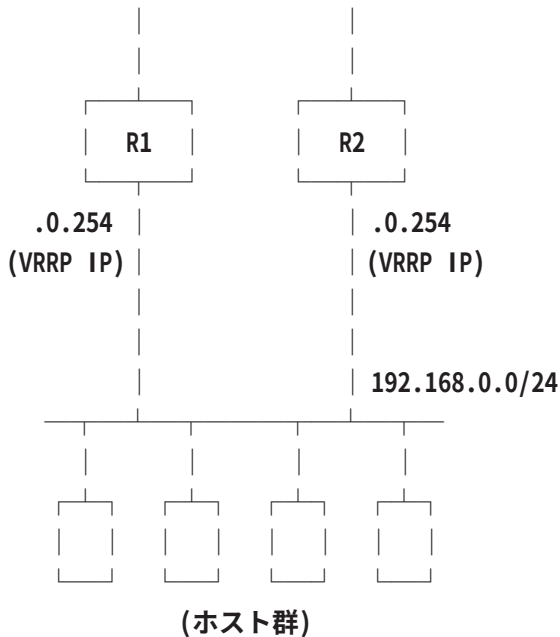
VRRP 機能設定画面上部にある「現在の状態」をクリックすると、VRRP 機能の動作状況を表示するウィンドウがポップアップします。

第 21 章 VRRP サービス

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



ルータ「R1」の設定例

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

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。

設定条件

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

第 22 章

アクセスサーバ機能

第22章 アクセスサーバ機能

1. アクセスサーバ機能について

アクセスサーバとは、電話回線などを使った外部からの接続要求を受けて、LAN に接続する機能です。例えば、アクセスサーバとして設定した XR-440 を会社で設置すると、モデムを接続した外出先のコンピュータから会社の LAN に接続できます。これは、モバイルコンピューティングや在宅勤務を可能にします。クライアントはモデムによる PPP 接続を利用できるものであれば、どのような PC でもかまいません。この機能を使って接続したクライアントは、接続先のネットワークにハブで接続した場合と同じようにネットワークを利用できます。

セキュリティは、ユーザー ID・パスワード認証、BRI 着信ではさらに着信番号によって確保します。ユーザー ID・パスワードは、最大5アカウント分を登録できます。



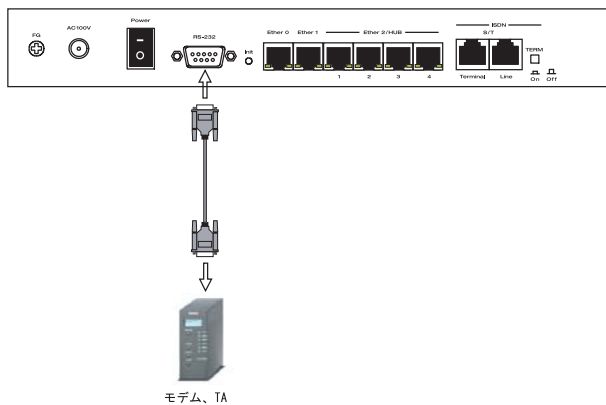
第 22 章 アクセスサーバ機能

II. XR-440 とアナログモデム /TA の接続

◆アナログモデム /TA のシリアル接続

- 1 本装置の電源をオフにします。
- 2 本装置の「RS-232C」ポートとモデム /TA のシリアルポートをシリアルケーブルで接続します。
シリアルケーブルは別途ご用意下さい。
- 3 全ての接続が完了しましたら、モデムの電源を投入してください。

接続図

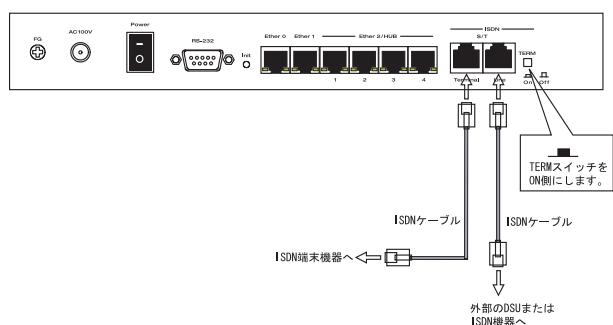


III. BRI ポートを使った XR-440 と TA/DSU の接続

◆外部の DSU を使う場合

- 1 本装置の電源をオフにします。
- 2 外部の DSU と本装置の「BRI S/T LINE」ポートを ISDN 回線ケーブルで接続します。ISDN ケーブルは別途ご用意下さい。
- 3 本体背面の「TERM.」スイッチを「ON」側にします。
- 4 別の ISDN 機器を接続する場合は「BRI S/T TERMINAL」ポートと接続してください。
- 5 全ての接続が完了しましたら、本装置と TA の電源を投入します。

接続図



第 22 章 アクセスサーバ機能

IV. アクセスサーバ機能の設定

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

シリアル回線で着信する場合

「シリアル回線」欄で設定します。

シリアル回線	
着信	☒ 許可しない ☐ 許可する
アクセスサーバ(本装置)の IP アドレス	192.168.253.254
クライアントの IP アドレス	192.168.253.170
モデムの速度	☐ 9600 ☐ 19200 ☐ 38400 ☒ 57600 ☐ 115200 ☐ 230400
受信のための AT コマンド	

○着信

シリアル回線で着信したい場合は「許可する」を選択します。

○アクセスサーバ(本装置)の IP アドレス

リモートアクセスされた時の XR-440 自身の IP アドレスを入力します。各 Ethernet ポートのアドレスとは異なるプライベートアドレスを設定してください。なお、サブネットマスクビット値は 24 ビット(255.255.255.0)に設定されています。

○クライアントの IP アドレス

XR-440 にリモートアクセスしてきたホストに割り当てる IP アドレスを入力します。上記の「アクセスサーバの IP アドレス」で設定したものと同じネットワークとなるアドレスを設定してください。

○モデムの速度

XR-440 とモデムの間の通信速度を選択します。

○着信のための AT コマンド

モデムが外部から着信する場合、AT コマンドが必要な場合があります。その場合は、ここで AT コマンドを入力してください。コマンドについては、各モデムの説明書をご確認ください。

BRI 回線で着信する場合

「BRI 回線」欄で設定します。2 チャンネル分の設定が可能です。

BRI 回線	
回線 1 着信	☒ 許可しない ☐ 許可する
アクセスサーバ(本装置)の IP アドレス	192.168.251.254
クライアントの IP アドレス	192.168.251.171
回線 2 着信	☒ 許可しない ☐ 許可する
アクセスサーバ(本装置)の IP アドレス	192.168.252.254
クライアントの IP アドレス	192.168.252.172
発信者番号認証	☒ しない ☐ する
本装置のホスト名	localhost

○回線 1、回線 2 着信

BRI 回線で着信したい場合は、「許可する」を選択します。

○アクセスサーバ(本装置)の IP アドレス

リモートアクセスされた時の XR-440 自身の IP アドレスを入力します。各 Ethernet ポートのアドレスとは異なるプライベートアドレスを設定してください。なお、サブネットマスクビット値は 24 ビット(255.255.255.0)に設定されています。

○クライアントの IP アドレス

XR-440 にリモートアクセスしてきたホストに割り当てる IP アドレスを入力します。上記の「アクセスサーバの 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。

○発信者番号認証

発信者番号で認証する場合は「する」を選択します。

○本装置のホスト名

本装置のホスト名を任意で設定可能です。

続けてユーザーアカウントの設定をおこないます。

第22章 アクセスサーバ機能

IV. アクセスサーバ機能の設定

ユーザーアカウントの設定

設定画面の下側でユーザーアカウントの設定をおこないます。

No.	アカウント	パスワード	アカウント毎に別IPを割り当てる場合		削除
			本装置のIP	クライアントのIP	
1					☐
2					☐
3					☐
4					☐
5					☐

外部からリモートアクセスする場合の、ユーザーアカウントとパスワードを登録してください。そのまま、リモートアクセス時のユーザーアカウント・パスワードとなります。5アカウントまで登録しておけます。

またアカウントごとに、割り当てる IP アドレスを個別に指定することも可能です。その場合は「本装置の IP」と「クライアントの IP」のどちらか、もしくは両方を設定します。

また BRI 回線の設定で発信番号認証を「する」にしている場合は、「許可する着信番号」欄に、発信者の電話番号を入力し、着信する回線を選択してください。

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

入力後、「設定の保存」をクリックしてください。設定が反映されます。

アカウント設定覧の「削除」ラジオボックスにチェックして「設定 / 削除の実行」をクリックすると、その設定が削除されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

第 23 章

スタティックルーティング

第23章 スタティックルーティング

スタティックルーティング設定

XR-440 は、最大 256 エントリのスタティックルートを登録できます。

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。

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1~255>	削除
1	192.168.10.0	255.255.255.0		192.168.120.15	☐
2	192.168.20.1	255.255.255.0	gre1		☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐
9					☐
10					☐
11					☐
12					☐
13					☐
14					☐
15					☐
16					☐

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

(画面は設定例です)

入力方法

○アドレス

あて先ホストのアドレス、またはネットワークアドレスを入力します。

○ネットマスク

あて先ネットワークのサブネットマスクを入力します。IP アドレス形式で入力してください。

入力例 : 255.255.255.248

また、あて先アドレスを単一ホストで指定した場合には、「255.255.255.255」と入力します。

○インターフェース / ゲートウェイ

ルーティングをおこなうインターフェース名、もしくは上位ルータの IP アドレスを設定します。

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

○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。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

----------------------	----------------------	----------------------	----------------------	----------------------	----------------------

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1つずつ設定番号がずれて設定が更新されます。

設定を削除する

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

インターフェース名は「付録A インターフェース名について」を参照してください。

第23章 スタティックルーティング

スタティックルーティング設定

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。

アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>
0.0.0.0	0.0.0.0	gre1	1

(画面は設定例です)

ルーティング情報を確認する

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

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

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

第 24 章

ソースルーティング機能

第24章 ソースルーティング機能

ソースルーティング設定

通常のダイナミックルーティングおよびスタティックルーティングでは、パケットのあて先アドレスごとにルーティングを行ないませんが、ソースルーティングはパケットの送信元アドレスをもとにルーティングをおこないます。

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

ソースルート設定は、設定画面「ソースルート設定」でおこないます。

1 はじめに、ソースルートのテーブル設定をおこないます。「ソースルートのテーブル設定へ」をクリックしてください。

テーブルNO	IP	DEVICE
1		
2		
3		
4		
5		
6		
7		
8		

○ IP

デフォルトゲートウェイ(上位ルータ)の IP アドレスを設定します。必ず明示的に設定しなければなりません。

○ DEVICE

デフォルトゲートウェイが存在する回線に接続しているインタフェースのインタフェース名を設定します

(インタフェース名は「付録A インタフェース名について」を参照してください)。

省略することもできます。

設定後は「設定の保存」をクリックします。

2 画面右上の「ソースルートのルール設定へ」をクリックします。

ルールNO	送信元ネットワークアドレス	送信先ネットワークアドレス	ソースルートのテーブルNO
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			

○送信元ネットワークアドレス

送信元のネットワークアドレスもしくはホストの IP アドレスを設定します。ネットワークアドレスで設定する場合は、

ネットワークアドレス / マスクビット値
の形式で設定してください。

○送信先ネットワークアドレス

送信先のネットワークアドレスもしくはホストの IP アドレスを設定します。ネットワークアドレスで設定する場合は、

ネットワークアドレス / マスクビット値
の形式で設定してください。

○ソースルートのテーブル No.

使用するソースルートテーブルの番号(1～8)を設定します。

最後に「設定の保存」をクリックして設定完了です。

※送信元ネットワークアドレスをネットワークアドレスで指定した場合、そのネットワークに XR-440 のインタフェースが含まれていると、設定後は XR-440 の設定画面にアクセスできなくなります。

<例>Ether0 ポートの IP アドレスが 192.168.0.254 で、送信元ネットワークアドレスを 192.168.0.0/24 と設定すると、192.168.0.0/24 内のホストは XR-440 の設定画面にアクセスできなくなります。

第 25 章

NAT 機能

第25章 NAT 機能

I. XR-440 の NAT 機能について

NAT(Network Address Translation)は、プライベートアドレスをグローバルアドレスに変換してインターネットにアクセスできるようにする機能です。また1つのプライベートアドレス・ポートと、1つのグローバルアドレス・ポートを対応させて、インターネット側からLANのサーバへアクセスさせることもできます。

XR-440 は以下の3つの NAT 機能をサポートしています。

◆ IP マスカレード機能

複数のプライベートアドレスを、ある1つのグローバルアドレスに変換する機能です。グローバルアドレスはXR-440のインターネット側ポートに設定されたものを使います。またLANのプライベートアドレス全てが変換されることになります。この機能を使うと、グローバルアドレスを1つしか持っていなくても複数のコンピュータからインターネットにアクセスできるようになります。

なお IP マスカレード (NAT 機能) では、プライベートアドレスからグローバルアドレスだけではなく、プライベートアドレスからプライベートアドレス、グローバルアドレスからグローバルアドレスの変換も可能です。IP マスカレード機能については、「インタフェース設定」もしくは「PPP/PPPoE 接続」の接続設定画面で設定します。

◆ 送信元 NAT 機能

IP マスカレードとは異なり、プライベートアドレスをどのグローバル IP アドレスに変換するかをそれぞれ設定できるのが送信元 NAT 機能です。例えば、プライベートアドレス A をグローバルアドレス X に、プライベートアドレス B をグローバルアドレス Y に、プライベートアドレス C から F をグローバルアドレス Z に変換する、といった設定が可能になります。IP マスカレード機能を設定せずに送信元 NAT 機能だけを設定した場合は、送信元 NAT 機能で設定されたアドレスを持つコンピュータしかインターネットにアクセスできません。

◆ バーチャルサーバ機能

インターネット上から LAN 上のサーバ等にアクセスさせることができる機能です。通常はインターネット側から LAN へアクセスする事はできませんが、送信先グローバルアドレスをプライベートアドレスへ変換する設定をおこなうことで、見かけ上はインターネット上のサーバへアクセスできているかのようにすることができます。設定上ではプライベートアドレスとグローバルアドレスを1対1で関連づけます。また同時に、プロトコルとTCP/UDP ポート番号も指定しておきます。ここで指定したプロトコル・TCP/UDP ポート番号でアクセスされた時にグローバルアドレスからプライベートアドレスへ変換され、LAN 上のサーバに転送されます。

これらの NAT 機能は同時に設定・運用が可能です。

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

II. バーチャルサーバ設定

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

設定方法

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

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	削除
1			全て			☐
2			全て			☐
3			全て			☐
4			全て			☐
5			全て			☐
6			全て			☐
7			全て			☐
8			全て			☐
9			全て			☐
10			全て			☐
11			全て			☐
12			全て			☐
13			全て			☐
14			全て			☐
15			全て			☐
16			全て			☐

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

			全て			
--	--	--	----	--	--	--

○サーバのアドレス

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

○公開するグローバルアドレス

サーバのプライベート IP アドレスに対応させるグローバル IP アドレスを入力します。インターネットからはここで入力したグローバル IP アドレスでアクセスします。

プロバイダから割り当てられている IP アドレスが一つだけの場合は、ここは空欄にします。

○プロトコル

サーバのプロトコルを選択します。

○ポート

サーバが公開するポート番号を入力します。範囲で指定することも可能です。範囲で指定するときは、ポート番号を「:」で結びます。

<例> ポート 20 番から 21 番を指定する → 20:21

○インターフェース

外部からのアクセスを受信するインターフェース名を設定します。外部に接続しているインターフェース名を設定してください。

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。

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

設定情報の確認

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

設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

			全て			
--	--	--	----	--	--	--

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1つずつ設定番号がずれて設定が更新されます。

設定を削除する

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

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

III. 送信元 NAT 設定

設定方法

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

No.	送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース	削除
1				☐
2				☐
3				☐
4				☐
5				☐
6				☐
7				☐
8				☐
9				☐
10				☐
11				☐
12				☐
13				☐
14				☐
15				☐
16				☐

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

				☐
----------------------	----------------------	----------------------	----------------------	--------------------------

○送信元のプライベートアドレス

NAT の対象となる LAN 側コンピュータのプライベート IP アドレスを入力します。ネットワーク単位での指定も可能です。

○変換後のグローバルアドレス

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

○インターフェース

外部につながっているインターフェース名を設定してください。

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。

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

設定情報の確認

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

設定を挿入する

送信元 NAT 設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

				☐
----------------------	----------------------	----------------------	----------------------	--------------------------

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。

設定を削除する

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

IV. バーチャルサーバの設定例

◆ WWW サーバを公開する際の NAT 設定例

NAT の条件

- WAN 側のグローバルアドレスに TCP のポート 80 番(http)でのアクセスを通す。
- 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」
- 割り当てられるグローバルアドレスは1つのみ。

設定画面での入力方法

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

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.1		tcp	80	eth1

設定の解説

No.1 :

WAN 側から本装置の IP アドレスへポート 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。
- 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」
- 割り当てられるグローバルアドレスは1つのみ。

設定画面での入力方法

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

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.2		tcp	20	ppp0
192.168.0.2		tcp	21	ppp0

設定の解説

No.1 :

WAN 側から本装置の IP アドレスへポート 21 番 (ftp)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。

No.2 :

WAN 側から本装置の IP アドレスへポート 20 番 (ftpdata)でアクセスがあれば、LAN 内のサーバ 192.168.0.2 へ通す。

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくにステートフルインスペクション機能を使っている場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

IV. バーチャルサーバの設定例

◆ PPTP サーバを公開する際の NAT 設定例

NAT の条件

- WAN 側のグローバルアドレスにプロトコル「gre」と TCP のポート番号 1723 を通す。
- WAN は Ether1、LAN は Ether0 ポートに接続する。
- WAN 側ポートは PPPoE で ADSL 接続する。

LAN 構成

- LAN 側ポートの IP アドレス「192.168.0.254」
- PPTP サーバのアドレス「192.168.0.3」
- 割り当てられるグローバルアドレスは1つのみ。

設定画面での入力方法

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

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.3		tcp	1723	ppp0
192.168.0.3		gre		ppp0

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくにステートフル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。
- WAN 側は PPPoE 接続する。

LAN 構成

- LAN 側ポートの IP アドレス「192.168.0.254」
- WWW サーバのアドレス「192.168.0.1」
- 送受信メールサーバのアドレス「192.168.0.2」
- FTP サーバのアドレス「192.168.0.3」
- DNS サーバのアドレス「192.168.0.4」
- WWW サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.104」
- 送受信メールサーバに対応させるグローバル IP アドレスは「211.xxx.xxx.105」
- FTP サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.106」
- DNS サーバに対応させるグローバル IP アドレスは「211.xxx.xxx.107」

設定画面での入力方法

1 まず最初に、使用する複数のグローバルアドレスを、仮想インタフェースとして登録します。メニューにある「仮想インタフェース設定」を開き、以下のように設定しておきます。

インターフェース	仮想I/F番号	IPアドレス	ネットマスク
ppp0	1	211.xxx.xxx.104	255.255.255.248
ppp0	2	211.xxx.xxx.105	255.255.255.248
ppp0	3	211.xxx.xxx.106	255.255.255.248
ppp0	4	211.xxx.xxx.107	255.255.255.248

2 「バーチャルサーバ設定」で以下の様に設定してください。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.1	211.xxx.xxx.104	tcp	80	ppp0
192.168.0.2	211.xxx.xxx.105	tcp	25	ppp0
192.168.0.2	211.xxx.xxx.105	tcp	110	ppp0
192.168.0.3	211.xxx.xxx.106	tcp	21	ppp0
192.168.0.3	211.xxx.xxx.106	tcp	20	ppp0
192.168.0.4	211.xxx.xxx.107	tcp	53	ppp0
192.168.0.4	211.xxx.xxx.107	udp	53	ppp0

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 (ftppdata) か 21 番 (ftp) でアクセスがあれば、LAN 内のサーバ 192.168.0.3 へ通す。

No.6、7

WAN 側から 211.xxx.xxx.107 へ、tcp ポート 53 番 (domain) か udp ポート 53 番 (domain) でアクセスがあれば LAN 内のサーバ 192.168.0.4 へ通す。

複数のグローバルアドレスを使ってバーチャルサーバ設定をおこなうときは、必ず「仮想インタフェース機能」において使用するグローバルアドレスを設定しておく必要があります。

V. 送信元 NAT の設定例

送信元 NAT 設定では、LAN 側のコンピュータのアドレスをどのグローバルアドレスに変換するかを個々に設定することができます。

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.0.1	61.xxx.xxx.101	ppp0
192.168.0.2	61.xxx.xxx.102	ppp0
192.168.10.0/24	61.xxx.xxx.103	ppp0

例えば上記のような送信元 NAT 設定をおこなうと、

- 送信元アドレス 192.168.0.1 を 61.xxx.xxx.101 に変換して WAN へアクセスする
- 送信元アドレス 192.168.0.2 を 61.xxx.xxx.102 に変換して WAN へアクセスする
- 送信元アドレスとして 192.168.0.0/24 からのアクセスを 61.xxx.xxx.103 に変換して WAN へアクセスする

という設定になります。

送信元のアドレスは、ホスト単位かネットワーク単位で指定できます。範囲指定はできません。ネットワークで指定するときは、以下のように設定して下さい。

< 設定例 > **192.168.254.0/24**

複数のグローバルアドレスを使って送信元 NAT 設定をおこなうときは、必ず「仮想インターフェース機能」で使用する IP アドレスを設定しておく必要があります。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

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

第 26 章

パケットフィルタリング機能

第 26 章 パケットフィルタリング機能

1. 機能の概要

XR-440はパケットフィルタリング機能を搭載しています。パケットフィルタリング機能を使うと、以下のようなことができます。

- 外部から LAN に入ってくるパケットを制限する。
- LAN から外部に出ていくパケットを制限する。
- XR-440 自身が受信するパケットを制限する。
- XR-440 自身から送信するパケットを制限する。

またフィルタリングは以下の情報に基づいて条件を設定することができます。

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

パケットフィルタリング機能を有効にすると、パケットを単にルーティングするだけでなく、パケットのヘッダ情報を調べて、送信元やあて先の IP アドレス、プロトコルの種類 (TCP/UDP/ICMP など)、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。

第 26 章 パケットフィルタリング機能

II.XR-440 のフィルタリング機能について

XR-440 は、3つの基本ルールについてフィルタリングの設定をおこないます。この3つの項目は以下の通りです。

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

◆転送(forward)フィルタ

LANからインターネットへのアクセスや、インターネットからLAN内サーバへのアクセス、LANからLANへのアクセスなど、XR-440で内部転送する(XR-440がルーティングする)アクセスを制御するという場合には、この転送ルールにフィルタ設定をおこないます。

◆入力(input)フィルタ

外部からXR-440自身に入ってくるパケットに対して制御します。インターネットやLANからXR-440へのアクセスについて制御したい場合には、この入力ルールにフィルタ設定をおこないます。

◆出力(output)フィルタ

XR-440内部からインターネットやLANなどへのアクセスを制御したい場合には、この出力ルールにフィルタ設定をおこないます。

パケットが「転送されるもの」か「XR-440自身へのアクセス」か「XR-440自身からのアクセス」かをチェックしてそれぞれのルールにあるフィルタ設定を実行します。

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

フィルタの初期設定について

工場出荷設定では、「入力フィルタ」と「転送フィルタ」において、以下のフィルタ設定がセットされています。

- NetBIOSを外部に送出しないフィルタ設定
- 外部からUPnPで接続されないようにするフィルタ設定

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

第26章 パケットフィルタリング機能

III. パケットフィルタリングの設定

入力・転送・出力フィルタの3種類ありますが、設定方法はすべて同様となります。

設定方法

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

[illegible]

(画面は「転送フィルタ」です)

○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指定します。

インタフェース名は「付録A インタフェース名について」を参照してください。

○方向

ポートがパケットを受信するときにフィルタリングするか、送信するときにフィルタリングするかを選択します。

入力フィルタでは「パケット受信時」、
出力フィルタでは「パケット送信時」
のみとなります。

○動作

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

○プロトコル

フィルタリング対象とするプロトコルを選択します。

右側の空欄でプロトコル番号による指定もできます。

ポート番号も指定する場合は、ここで必ずプロトコルを選択しておいてください。

○送信元アドレス

フィルタリング対象とする、送信元の IP アドレス
を入力します。

ホストアドレスのほか、ネットワークアドレス、ドメイン名での指定が可能です。

< 入力例 >

単一の IP アドレスを指定する：

192.168.253.19/32

(" アドレス /32" の書式)

ネットワーク単位で指定する：

192.168.253.0/24

(“ネットワークアドレス / マスクビット値” の書式)

○送信元ポート

フィルタリング対象とする、送信元のポート番号を入力します。

範囲での指定も可能です。範囲で指定するときは
”:”でポート番号を結びます。

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

ポート番号を指定するときは、プロトコルもあわせて選択しておかなければなりません。

(「全て」のプロトコルを選択して、ポート番号を指定することはできません。)

○あて先アドレス

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

第 26 章 パケットフィルタリング機能

III. パケットフィルタリングの設定

○あて先ポート

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

○送信元 MAC アドレス

[入力・転送フィルタのみ]

フィルタリング対象とする、送信元の MAC アドレスを入力します。

半角英数字、':', '*', '/', ' ' のみ入力することが出来ます。

入力可能な最大文字数は 35 文字です。

送信元 MAC アドレスは、XX:XX:XX:XX:XX:XX 形式で設定します。

以下の形式でも指定することが出来ます。

-XX:XX:XX:XX:*. * (wildcard 形式)

-XX:XX:XX:XX:XX/XX:XX:XX:XX:XX:XX
(マスク形式)

○LOG

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

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

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

設定情報の確認

「情報表示」をクリックすると、現在のフィルタ設定の情報が一覧表示されます。

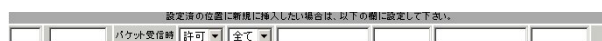
設定を挿入する

フィルタ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

その番号以降に設定がある場合は、1 つずつ設定番号がずれて設定が更新されます。



設定を削除する

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

第 26 章 パケットフィルタリング機能

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

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。
- XR-440 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。
- ステートフルインスペクションは無効とする。

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「192.168.0.1」

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。

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	宛て先アドレス	宛て先ポート
eth1	パケット受信時	許可	tcp				1024-65535
eth1	パケット受信時	許可	udp				1024-65535
eth1	パケット受信時	破棄	全て				

「入力フィルタ」で以下のように設定します。

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	宛て先アドレス	宛て先ポート
eth1	パケット受信時	許可	tcp				1024-65535
eth1	パケット受信時	許可	udp				1024-65535
eth1	パケット受信時	破棄	全て				

フィルタの解説

「転送フィルタ」「入力フィルタ」

No.1 :

WAN から来る、宛て先ポートが 1024 から 65535 のパケットを通す。

No.2 :

上記の条件に合致しないパケットを全て破棄する。

第 26 章 パケットフィルタリング機能

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。

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」
- ステートフルインスペクションは無効とする。

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。

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	宛て先アドレス	宛て先ポート
eth1	パケット受信時	許可	tcp			192.168.0.1/32	80
eth1	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
eth1	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
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 :

WAN から来る、宛て先ポートが 1024 から 65535 のパケットを通す。

No.3 :

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。

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」
- ステートフルインスペクションは無効とする。

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。

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	宛て先アドレス	宛て先ポート
jpp0	パケット受信時	許可	tcp			192.168.0.2/32	21
jpp0	パケット受信時	許可	tcp			192.168.0.2/32	20
jpp0	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
jpp0	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
jpp0	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、宛て先ポートが 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下さい。

第 26 章 パケットフィルタリング機能

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。
- ステートフルインスペクションは無効とする。

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」
- WWW サーバのアドレス「192.168.0.1」
- メールサーバのアドレス「192.168.0.2」
- FTP サーバのアドレス「192.168.0.3」
- DNS サーバのアドレス「192.168.0.4」

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	方向	動作	プロトコル	通信元アドレス	通信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	許可	tcp			192.168.0.1/32	80
ppp0	パケット受信時	許可	tcp			192.168.0.2/32	25
ppp0	パケット受信時	許可	tcp			192.168.0.2/32	110
ppp0	パケット受信時	許可	tcp			192.168.0.3/32	21
ppp0	パケット受信時	許可	tcp			192.168.0.3/32	20
ppp0	パケット受信時	許可	tcp			192.168.0.4/32	53
ppp0	パケット受信時	許可	udp			192.168.0.4/32	53
ppp0	パケット受信時	許可	tcp			192.168.0.0/24	1024-65535
ppp0	パケット受信時	許可	udp			192.168.0.0/24	1024-65535
ppp0	パケット受信時	破棄	全て				

フィルタの解説

No.1 :

192.168.0.1 のサーバに HTTP のパケットを通す。

No.2,3 :

192.168.0.2 のサーバに SMTP と POP3 のパケット
を通す。

No.4,5 :

192.168.0.3 のサーバに ftp と ftpdata のパケッ
トを通す。

No.6,7 :

192.168.0.4 のサーバに、domain のパケット
(tcp,udp)を通す。

No.8、9 :

WAN から来る、あて先ポートが 1024 から 65535
のパケットを通す。

No.10 :

上記の条件に合致しないパケットを全て破棄す
る。

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

第 26 章 パケットフィルタリング機能

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」

eth0	パケット受信時	破棄	tcp				137:139
eth0	パケット受信時	破棄	udp				137:139
eth0	パケット受信時	破棄	tcp			137	
eth0	パケット受信時	破棄	udp			137	

「転送フィルタ」

eth0	パケット受信時	破棄	tcp				137:139
eth0	パケット受信時	破棄	udp				137:139
eth0	パケット受信時	破棄	tcp			137	
eth0	パケット受信時	破棄	udp			137	

フィルタの解説

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.2 :

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。

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
ppp0	パケット受信時	破棄	全て			210.xxx.xxx.32/32	
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(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.32のネットワークのブロードキャスト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。

第26章 パケットフィルタリング機能

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。

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	宛先アドレス	宛先ポート
ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
ppp0	パケット受信時	破棄	全て	192.168.0.0/16			

フィルタの解説

No.1,2,3:

- WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。
→ WAN 上にプライベートアドレスは存在しない。

◆外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

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	宛先アドレス	宛先ポート
ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
ppp0	パケット受信時	破棄	全て	192.168.0.0/16			
ppp0	パケット受信時	破棄	全て			202.xxx.xxx.112/3	
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。

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	宛先アドレス	宛先ポート
ppp0	パケット受信時	破棄	全て			10.0.0.0/8	
ppp0	パケット受信時	破棄	全て			172.16.0.0/16	
ppp0	パケット受信時	破棄	全て			192.168.0.0/16	

フィルタの解説

入力フィルタの 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。

入力フィルタの No.4, 5:

- 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

出力フィルタの 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 上にプライベートネットワーク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。

第 26 章 パケットフィルタリング機能

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。

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	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	許可	tcp				1723
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」

したがって、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ただきます。

第26章 パケットフィルタリング機能

V. 外部から設定画面にアクセスさせる設定

XR-440 の初期設定では、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。そのため、外部から XR-440 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-440 の設定・制御をおこなうことも可能です。その場合は「入力フィルタ」で必要な設定をおこないます。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。

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	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	許可	tcp	xxx.xxx.xxx.xxx			880

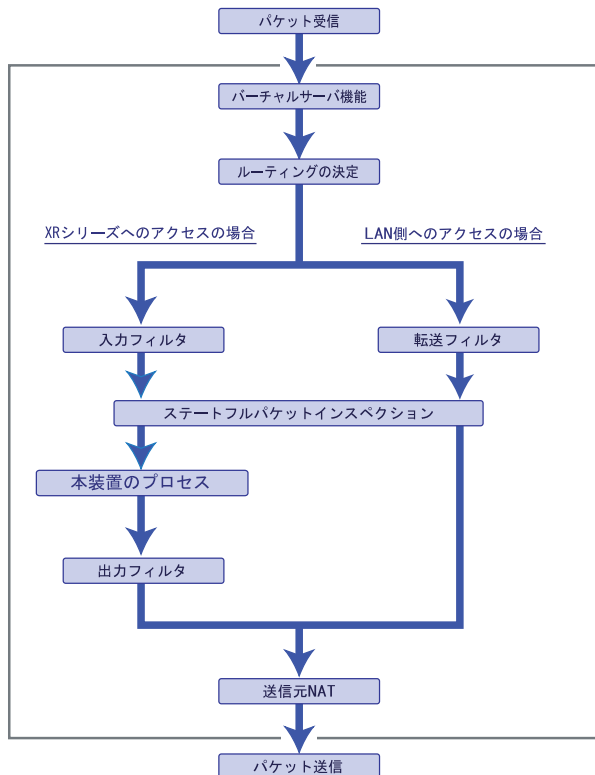
上記設定では、xxx.xxx.xxx.xxx の IP アドレスを持つホストだけが、外部から XR-440 の設定画面へのアクセスが可能になります。

また「送信元アドレス」を空欄にすると、すべてのインターネット上のホストから、XR-440 にアクセス可能になります(**セキュリティ上たいへん危険ですので、この設定は推奨いたしません**)。

第26章 パケットフィルタリング機能

補足：NAT とフィルタの処理順序について

XR-440 における、NAT とフィルタリングの処理方法は以下のようになっています。



(図の上部を WAN 側、下部を LAN 側とします。また LAN → WAN へ NAT をおこなうとします。)

- WAN 側からパケットを受信したとき、最初に「バーチャルサーバ設定」が参照されます。
- 「バーチャルサーバ設定」で静的 NAT 変換したあとに、パケットがルーティングされます。
- XR-440 自身へのアクセスをフィルタするときは「入力フィルタ」、XR-440 自身からのアクセスをフィルタするときは「出力フィルタ」で設定します。
- WAN 側から LAN 側へのアクセスをフィルタするときは「転送フィルタ」で設定します。その場合のあて先アドレスは「(LAN 側の)プライベートアドレス」になります (NAT の後の処理となるため)。
- ステートフルパケットインスペクションだけを有効にしている場合、WAN から LAN、また XR-440 自身へのアクセスはすべて破棄されます。
- ステートフルパケットインスペクションと同時に「転送フィルタ」「入力フィルタ」を設定している場合は、先に「転送フィルタ」「入力フィルタ」にある設定が優先して処理されます。
- 「送信元 NAT 設定」は、一番最後に参照されます。
- LAN 側から WAN 側へのアクセスの場合も、処理の順序は同様です。(最初にバーチャルサーバ設定が参照される)

第 26 章 パケットフィルタリング機能

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

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

第 26 章 パケットフィルタリング機能

補足：フィルタのログ出力内容について

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

<入力パケットを破棄したときのログ出力例>

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

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

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

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

第 27 章

スケジュール設定

第 27 章 スケジュール設定

スケジュール機能の設定方法

XR-440 には、主回線を接続または切断する時間を管理するスケジュール機能があります。

スケジュールの設定は 10 個まで設定できます

○ Web 設定画面「スケジュール設定」をクリックし、以下の画面でスケジュール機能の設定をします。

スケジュール設定				
時間	動作	実行	有効期限	スケジュール
1	スケジュールは設定されていません			
2	スケジュールは設定されていません			
3	スケジュールは設定されていません			
4	スケジュールは設定されていません			
5	スケジュールは設定されていません			
6	スケジュールは設定されていません			
7	スケジュールは設定されていません			
8	スケジュールは設定されていません			
9	スケジュールは設定されていません			
10	スケジュールは設定されていません			

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

スケジュール No.1

時刻 --時-- --分-- 動作 [選択してください]

実行日

☒ 毎日

☐ 毎週

☐ 毎月

有効期限

☒ なし

☐ 1月1日～1月1日の期間

☐ 2002年1月1日以降

☐ 2002年1月1日まで

☐ 2002年1月1日に実行

スケジュールを [無効にする]

設定/削除の実行

[スケジュール]

実行させる「時刻」「動作」を設定します。

「時刻」

実行させる時刻を設定します。

「動作」

動作内容を設定します。

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

[実行日]

実行する日を「毎日」「毎週」「毎月」の中から選択します。

「毎日」

毎日同じ時間に接続 / 切断するように設定する場合に選択します。

「毎週」

毎週同じ曜日の同じ時間に接続 / 切断するように設定する場合に選択します。

なお、複数の曜日を選択することができます。

「毎月」

毎月同じ日の同じ時間に接続 / 切断するように設定する場合に選択します。

なお、複数の日を選択することができます。

複数選択する場合

【Windows の場合】

Control キーを押しながらクリックします。

【Macintosh の場合】

Command キーを押しながらクリックします。

第27章 スケジュール設定

スケジュール機能の設定方法

[有効期限]

実行有効期限を設定します。有効期限は、常に設定する年から10年分まで設定できます。

有効期限で「xxxx年xx月xx日に実行」を選択した場合、実行日は「毎日」のみ選択できます。

「なし」

特に実行する期限を定めない場合に選択します。

「xx月xx日～x月x日の期間」

実行する期間を定める場合に選択し、有効期限を設定します。

「xxxx年xx月xx日以降」

実行する期間の開始日を設定したい場合に選択します。

「xxxx年xx月xx日まで」

実行する期間の終了日を設定したい場合に選択します。

「xxxx年xx月xx日に実行」

実行する日時を設定したい場合に選択します。

○設定したスケジュール内容の実行・削除・保存を決定します。

「スケジュールを有効にする」

設定したスケジュールを起動する場合に選択します。

「スケジュールを無効にする」

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

「スケジュールを削除する」

スケジュールの設定内容を削除する場合に選択します。

○設定 / 削除の実行をクリックします。

○画面上のスケジュール設定欄に設定内容が反映されます。

スケジュール設定欄の項目について

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

<例>

スケジュール設定				
時間	動作	実行	有効期限	スケジュール
1 08:00	主回線切断	毎週 月、水曜日	2002年3月30日以降	有効
2 15:51	主回線接続	毎日	なし	無効
3 17:59	主回線切断	毎日	なし	無効
4 23:00	主回線接続	毎週 日、火曜日	2002年3月30日以降	有効
5	スケジュールは設定されていません			
6	スケジュールは設定されていません			
7	スケジュールは設定されていません			
8	スケジュールは設定されていません			
9	スケジュールは設定されていません			
10	スケジュールは設定されていません			

上の画面で「時間」項目をクリックします。

下の画面のように、「時間」の早い順番に並べ替えられます。

スケジュール設定				
時間	動作	実行	有効期限	スケジュール
1 15:51	主回線接続	毎日	なし	無効
2 08:00	主回線切断	毎週 月、水曜日	2002年3月30日以降	有効
3 17:59	主回線切断	毎日	なし	無効
4 23:00	主回線接続	毎週 日、火曜日	2002年3月30日以降	有効
5	スケジュールは設定されていません			
6	スケジュールは設定されていません			
7	スケジュールは設定されていません			
8	スケジュールは設定されていません			
9	スケジュールは設定されていません			
10	スケジュールは設定されていません			

第 28 章

ネットワークイベント機能

第 28 章 ネットワークイベント機能

I. 機能の概要

ネットワークイベントは、回線障害などのネットワーク状態の変化を検知し、それをトリガとして特定のイベントを実行する機能です。

本装置では、以下のネットワーク状態の変化をトリガとして検知することができます。

- ping 監視の状態
- link 監視の状態
- vrrp 監視の状態

◆ ping 監視

本装置から任意の宛先へ ping を送信し、その応答の有無を監視します。一定時間応答がなかった時にトリガとして検知します。また、再び応答を受信した時は、復旧トリガとして検知します。

◆ link 監視

Ethernet インタフェースや ppp インタフェースのリンク状態を監視します。監視するインタフェースのリンクがダウンした時にトリガとして検知します。また再びリンクがアップした時は復旧トリガとして検知します。

◆ vrrp 監視

本装置の VRRP ルータ状態を監視します。指定したルータ ID の VRRP ルータがバックアップルータへ切り替わった時にトリガとして検知します。また、再びマスタールータへ切り替わった時は復旧トリガとして検知します。

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

- VRRP 優先度変更
- IPsec 接続切断

◆ VRRP 優先度変更

トリガ検知時に、指定した VRRP ルータの優先度を変更します。またトリガ復旧時には、元の VRRP 優先度に変更します。

例えば、ping 監視と連動して、PPPoE 接続先がダウンした時に、自身は VRRP バックアップルータに移行し、新マスタールータ側の接続へ切り替える、といった使い方ができます。

◆ IPsec 接続 / 切断

トリガ検知時に、指定した IPsec ポリシーを切断します。またトリガ復旧時には、IPsec ポリシーを再び接続します。

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

第28章 ネットワークイベント機能

1. 機能の概要

本機能で使用する各種テーブルについて

本機能は複数のテーブル定義を連携させることによって実現しています。

① ping 監視テーブル

NO	enable	トリガー番号	インターバル	リトライ	送信先アドレス
1	☒	1	10	3	192.168.0.1
2	☐	2	10	3	
3	☐	3	10	3	

① link 監視テーブル

NO	enable	トリガー番号	インターバル	リトライ	監視するデバイス名
1	☒	1	10	3	
2	☒	2	10	3	ppp0
3	☐	3	10	3	

① vrrp 監視テーブル

NO	enable	トリガー番号	インターバル	リトライ	VRRP ルータID
1	☐	1	10	3	
2	☐	2	10	3	
3	☒	3	10	3	51

② ネットワークイベント設定テーブル

NO	トリガー番号	実行イベントテーブル番号
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8	8	8
9	9	9
10	10	10
11	11	11
12	12	12
13	13	13
14	14	14
15	15	15
16	16	16

③ イベント実行テーブル

NO	実行イベント設定	オプション設定
1	VRRP 優先度	1
2	VRRP 優先度	2
3	IPSEC ポリシー	1
4	VRRP 優先度	4
5	VRRP 優先度	5
6	VRRP 優先度	6
7	VRRP 優先度	7
8	VRRP 優先度	8
9	VRRP 優先度	9
10	VRRP 優先度	10
11	VRRP 優先度	11
12	VRRP 優先度	12
13	VRRP 優先度	13
14	VRRP 優先度	14
15	VRRP 優先度	15
16	VRRP 優先度	16

④ VRRP 優先度テーブル

NO	IPSEC ポリシー番号 又は インターフェイス名	使用可否の接続状態	使用可否の接続状態
1	1	使用しない	使用する
2		使用しない	使用する
3		使用しない	使用する

⑤ IPsec 接続切断テーブル

NO	IPSEC ポリシー番号 又は インターフェイス名	使用可否の接続状態	使用可否の接続状態
1	1	使用しない	使用する
2		使用しない	使用する
3		使用しない	使用する

① ping 監視テーブル / link 監視テーブル / vrrp 監視テーブル

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

② ネットワークイベント設定テーブル

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

③ イベント実行テーブル

このテーブルでは、イベント番号と実行イベント種別 / オプション番号の関連付けを定義します。イベントの実行種別を「VRRP 優先度」に設定した場合は、次に「④ VRRP 優先度テーブル」を索引します。設定したオプション番号は、テーブル④のインデックス番号になります。

また、イベントの実行種別を「IPSEC ポリシー」に設定した場合は、次に「⑤ IPsec 接続切断テーブル」を索引します。設定したオプション番号は、テーブル⑤のインデックス番号になります。

④ VRRP 優先度テーブル

このテーブルでは、VRRP 優先度を変更するルータ ID とその優先度を定義します。

⑤ IPsec 接続切断テーブル

このテーブルでは、IPsec 接続 / 切断を行う IPsec ポリシー番号、または IPsec インタフェース名を定義します。

第 28 章 ネットワークイベント機能

II. 各トリガテーブルの設定

ping 監視の設定方法

設定画面上部の「ping 監視の設定」をクリックして、以下の画面から設定します。

ネットワークping設定

NO	enable	トリガー番号	インターバル	リトライ	送信先アドレス
1	☐	1	10	3	
2	☐	2	10	3	
3	☐	3	10	3	
4	☐	4	10	3	
5	☐	5	10	3	
6	☐	6	10	3	
7	☐	7	10	3	
8	☐	8	10	3	
9	☐	9	10	3	
10	☐	10	10	3	
11	☐	11	10	3	
12	☐	12	10	3	
13	☐	13	10	3	
14	☐	14	10	3	
15	☐	15	10	3	
16	☐	16	10	3	

○ enable

チェックを入れることで設定を有効にします。

○トリガー番号

ping送信先から応答が無かった場合に検知するトリガーの番号(1～16)を指定します。本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

○インターバル(秒)

○リトライ

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

○送信先アドレス

pingを送信する先の IP アドレスを指定します。

最後に「設定の保存」をクリックして設定完了です。

link 監視の設定方法

設定画面上部の「link 監視の設定」をクリックして、以下の画面から設定します。

デバイス監視設定

NO	enable	トリガー番号	インターバル	リトライ	監視するデバイス名
1	☐	1	10	3	
2	☐	2	10	3	
3	☐	3	10	3	
4	☐	4	10	3	
5	☐	5	10	3	
6	☐	6	10	3	
7	☐	7	10	3	
8	☐	8	10	3	
9	☐	9	10	3	
10	☐	10	10	3	
11	☐	11	10	3	
12	☐	12	10	3	
13	☐	13	10	3	
14	☐	14	10	3	
15	☐	15	10	3	
16	☐	16	10	3	

○ 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下さい。

最後に「設定の保存」をクリックして設定完了です。

第28章 ネットワークイベント機能

II. 各トリガテーブルの設定

vrrp 監視の設定方法

設定画面上部の「vrrp 監視の設定」をクリックして、以下の画面から設定します。

vrrp監視設定

NO	enable	トリガー番号	インターバル	リトライ	VRRP ルータID
1	☐	1	10	3	
2	☐	2	10	3	
3	☐	3	10	3	
4	☐	4	10	3	
5	☐	5	10	3	
6	☐	6	10	3	
7	☐	7	10	3	
8	☐	8	10	3	
9	☐	9	10	3	
10	☐	10	10	3	
11	☐	11	10	3	
12	☐	12	10	3	
13	☐	13	10	3	
14	☐	14	10	3	
15	☐	15	10	3	
16	☐	16	10	3	

○ enable

チェックを入れることで設定を有効にします。

○トリガー番号

監視する VRRP ルータがバックアップへ切り替わった場合に検知するトリガーの番号(1～16)を指定します。本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

○インターバル(秒)

○リトライ

VRRP ルータの状態を監視する間隔を設定します。
『インターバル』秒間に、『リトライ』回、VRRP のルータ状態を監視する」という設定になります。
この間、監視した状態が全てバックアップ状態であった場合にトリガとして検知されます。

○ VRRP ルータ ID

VRRP ルータ状態を監視するルータ ID を指定します。

最後に「設定の保存」をクリックして設定完了です。

各監視機能を有効にするにはネットワークイベントサービス設定画面で、「起動」ボタンにチェックを入れ、「動作変更」をクリックしてサービスを起動して下さい。

また設定の変更、追加、削除を行った場合は、サービスの再起動を行ってください。

(注) 各監視設定で指定したトリガー番号は、「ネットワークイベント設定」テーブルでのインデックス番号となるため、それぞれの監視設定の間で同じトリガー番号が有効にならないように設定してください。

注) v1.7.6版の時点ではインタフェースに Ether2 を選択した VRRP は、正常にトリガ検出ができません。Ether0 または Ether1 を選択した VRRP を使用して下さい。

第28章 ネットワークイベント機能

III. 実行イベントテーブルの設定

ネットワークイベント設定テーブルの設定

設定画面上部の「ネットワークイベント設定」をクリックして、以下の画面から設定します。

○トリガー番号

「ping 監視の設定」、「link 監視の設定」、「vrrp 監視の設定」で設定したトリガー番号を指定します。なお、複数のトリガー検知の組み合わせによって、イベントを実行させることも可能です。

<例>

- ・トリガー番号1とトリガー番号2のどちらかを検知した時にイベントを実行させる場合
1&2
- ・トリガー番号1とトリガー番号2の両方を検知した時、またはトリガー番号3を検知した時にイベントを実行させる場合
[1]2]&3

○実行イベントテーブル番号

そのトリガー番号を検知した時に実行されるイベント番号(1～16)を指定します。本値は、イベント実行テーブルでのインデックス番号となります。なお、複数のイベントを同時に実行させることも可能です。その場合は”_”でイベント番号を繋ぎます。

<例> イベント番号1,2,3を同時に実行させる場合
1_2_3

最後に「設定の保存」をクリックして設定完了です。

イベント実行テーブルの設定

設定画面上部の「イベント実行テーブル設定」をクリックして、以下の画面から設定します。

○実行イベント設定

実行されるイベントの種類を選択します。

「IPsec ポリシー」は、IPsec ポリシーの切断を行います。

「VRRP 優先度」は、VRRP ルータの優先度を変更します。

○オプション設定

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

最後に「設定の保存」をクリックして設定完了です。

第28章 ネットワークイベント機能

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。

VRRP 優先度変更設定
現在のVRRPの状況

NO	ルータID	優先度
1	51	50
2	52	50
3	53	50
4	54	50
5	55	50
6	56	50
7	57	50
8	58	50
9	59	50
10	60	50
11	61	50
12	62	50
13	63	50
14	64	50
15	65	50
16	66	50

入力やり直し 設定の保存

○ルータ ID

トリガ検知時に VRRP 優先度を変更する VRRP ルータ ID を指定します。

○優先度

トリガ検知時に変更する VRRP 優先度を指定します。1～255の間で設定して下さい。
なお、トリガ復旧時には「VRRP サービス」で設定されている元の値に戻ります。

最後に「設定の保存」をクリックして設定完了です。

IPSEC 接続切断設定 テーブルの設定

設定画面上部の「IPSEC ポリシー」をクリックして、以下の画面から設定します。

IPSEC 接続切断設定
現在のIPSECの状況

NO	IPSECポリシー番号 又はインタフェース名	使用IKE連動機能	使用interface連動機能
1		使用しない	使用する
2		使用しない	使用する
3		使用しない	使用する
4		使用しない	使用する
5		使用しない	使用する
6		使用しない	使用する
7		使用しない	使用する
8		使用しない	使用する
9		使用しない	使用する
10		使用しない	使用する
11		使用しない	使用する
12		使用しない	使用する
13		使用しない	使用する
14		使用しない	使用する
15		使用しない	使用する
16		使用しない	使用する

入力やり直し 設定の保存

- IPSEC ポリシー番号、又はインタフェース名
トリガ検知時に切断する IPsec ポリシーの番号、又は IPsec インタ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。
トリガ復旧時には再度 IPsec 接続されます。

○使用 IKE 連動機能

切断する IPsec ポリシーが使用する IKE と同じ IKE を使用する IPsec ポリシーが設定されている場合において、トリガ検知時にその IKE を使用する全ての IPsec ポリシーを切断する場合は、「使用する」を選択します。ここで設定した IPsec ポリシーのみを切断する場合は「使用しない」を選択します。

○使用 interface 連動機能

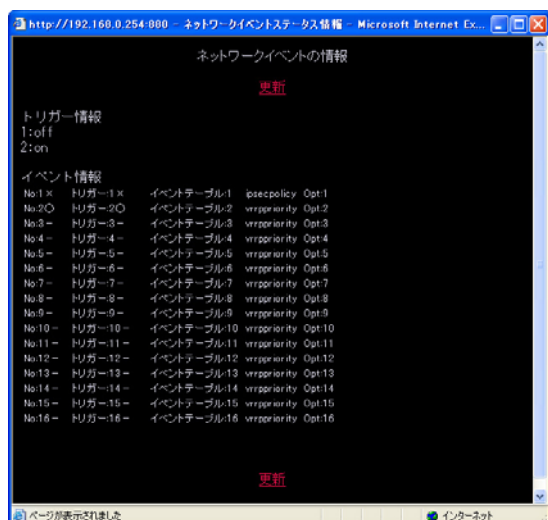
本装置では、PPPoE 上で IPsec 接続している場合、PPPoE 接続時に自動的に IPsec 接続も開始されます。ネットワークイベント機能を使った IPsec 二重化において、バックアップ側の PPPoE 接続時に IPsec を自動接続させたくない場合には「使用しない」を選択します。

最後に「設定の保存」をクリックして設定完了です。

V. ステータスの表示

ステータスの表示

設定画面上部の「ステータス」をクリックして表示します。



○トリガー情報

設定が有効なトリガー番号とその状態を表示します。

”ON”と表示されている場合は、トリガを検知していない、またはトリガが復旧している状態を表します。

“OFF”と表示されている場合は、トリガ検知している状態を表します。

○イベント情報

・No.

イベント番号とその状態を表します。

“×”の表示は、トリガ検知し、イベントを実行している状態を表します。

“○”の表示は、トリガ検知がなく、イベントが実行されていない状態を表します。

“-”の表示は、無効なイベントです。

・トリガー

イベント実行の条件となるトリガ番号とその状態を表します。

・イベントテーブル

左からイベント実行テーブルのインデックス番号、実行イベント種別、オプションテーブル番号を表します。

第 29 章

仮想インタフェース機能

第 29 章 仮想インターフェース機能

仮想インターフェース機能の設定

主にバーチャルサーバ機能を利用する場合に、仮想インターフェースを設定します。

設定方法

Web 設定画面「仮想インターフェース」をクリックして、以下の画面から設定します。

No.	インターフェース	仮想I/F番号	IPアドレス	ネットマスク	削除
1	ppp0	1	192.168.0.254	255.255.255.0	☐
2					☐
3					☐
4					☐
5					☐
6					☐
7					☐
8					☐
9					☐
10					☐
11					☐
12					☐
13					☐
14					☐
15					☐
16					☐

(画面は設定例です)

○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。

インターフェース名は「付録A インターフェース名について」を参照してください。

○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 の間で設定できます。

○IP アドレス

作成するインターフェースの IP アドレスを指定します。

○ネットマスク

作成するインターフェースのネットマスクを指定します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

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

設定を削除する

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

第 30 章

GRE 設定

第30章 GRE 設定

GRE の設定

GRE は Generic Routing Encapsulation の略で、リモート側にあるルータまで仮想的なポイントツーポイント リンクを張って、多種プロトコルのパケットを IP トンネルにカプセル化するプロトコルです。

また IPsec トンネル内に GRE トンネルを生成することもできますので、GRE を使用する場合でもセキュアな通信を確立することができます。

設定画面「GRE 設定」→ GRE インタフェース設定をクリックして設定します。

インタフェースアドレス	172.10.10.1/30 (例: 192.168.0.1/30)
リモート(宛先)アドレス	192.168.121.1 (例: 192.168.1.1)
ローカル(送信元)アドレス	192.168.121.2 (例: 192.168.2.1)
PEERアドレス	172.10.10.2/30 (例: 192.168.0.2/30)
TTL	255 (0~255)
MTU	1476 (最大値 1476)
TOS設定	☒ TOS値の指定 (0~0~0xfe) ☐ inherit(TOS値のコピー)
GREoverIPsec	☐ 使用する IPsec0 ☒ Routing Table に依存
IDキーの設定	(0~4294967295)
End-to-End Checksumming	☐ 有効 ☒ 無効
MSS設定	☐ 有効 ☒ 無効 MSS 値 Byte (有効時に MSS 値が 0 の場合は、MSS 値を自動設定(Clamp MSS to MTU)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。

例) 192.168.90.2/30

○TTL

GRE パケットの TTL 値を設定します。

○MTU

MTU 値を設定します。最大値は 1500byte です。

○Path MTU Discovery

Path MTU Discovery 機能を有効にするかを選択します。本機能を有効にした場合は、本装置が送信する GRE パケットの DF(Don't Fragment)ビットを 1 にします。無効にした場合は、DF ビットを常に 0 にして送信します。

○ToS

GRE パケットの ToS 値を設定します。

○GREoverIPsec

IPsec を使用して GRE パケットを暗号化する場合に「使用する」を選択します。またこの場合には別途、IPsec の設定が必要です。「Routing Table に依存」は GRE トンネルを暗号化して使わないときに選択してください。

GRE トンネルを暗号化するときの IPsec 設定は以下のようにしてください。

- ・本装置側設定 通常通り
- ・IKE/ISAKMP ポリシー設定 通常通り
- ・IPsec ポリシー設定

本装置側の LAN 側のネットワークアドレス：
GRE 設定のローカルアドレス /32

相手側の LAN 側のネットワークアドレス：
GRE 設定のリモートアドレス /32

○ID キーの設定

GRE パケットの識別用の ID を設定します。

GRE の設定

○ 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。

「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。

「現在の状態」では GRE の動作状況が表示されます。

現在の状態 Tunnel is down, Link is down

GRE 設定を行うと、設定内容が一覧表示されます。

Interface名	Interface Address	Remote Address	Local Address	Peer Address	MTU	ID Key	Checksum	Link State
gre1	172.16.1.1/24	192.168.1.1	192.168.1.2	172.16.1.2/24	1476		無効	down

設定の編集は「Interface 名」をクリックしてください。また GRE トンネルのリンク状態は「Link State」に表示されます。「UP」が GRE トンネルがリンクアップしている状態です。

第 31 章

QoS 機能

I.QoS について

本装置の優先制御・帯域制御機能(以下、QoS 機能)は以下の 5 つのキューイング方式で、トラフィック制御をおこないます。

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

クラスフル/クラスレスなキューイング

キューイングには、クラスフルなものとクラスレスなものがあります。

クラスレスなキューイングは、内部に設定可能なトラフィック分割用のバンド(クラス)を持たず、到着するすべてのトラフィックを同等に取り扱います。PFIFO、TBF、SFQ がクラスレスなキューイングです。

クラスフルなキューイングでは、内部に複数のクラスを持ち、選別器(クラス分けフィルタ)によって、パケットを送り込むクラスを決定します。各クラスはそれぞれに帯域を持つため、クラス分けすることで帯域制御ができるようになります。またキューイング方式によっては、あるクラスがさらに自分の配下にクラスを持つこともできます。さらに、各クラス内でそれぞれキューイング方式を決めることもできます。PQ と CBQ がクラスフルなキューイングです。

I. QoS について

1. PFIFO

もっとも単純なキューイング方式です。

あらかじめキューのサイズを決定しておき、どのパケットも区別なくキューに収納していきます。キューからパケットを送信するとき、送信するパケットはFIFOにしたがって選別されます。

キューのサイズを超えてパケットが到着したとき、超えた分のパケットは全て破棄されてしまいます。

キューのサイズが大きすぎると、キューイングによる遅延が発生する可能性があります。

※キューとは、データの入り口と出口を一つだけ持つバッファのことを指します。

※FIFOとは「First In First Out」の略で、「最初に入ったものが最初に出る」、つまり最も古いものが最初に取り出されることを指します。

2. TBF

帯域制御方法の1つです。

トークンバケツにトークンを、ある一定の速度(トークン速度)で収納していきます。このトークン1個ずつがパケットを1個ずつつかみ、トークン速度を超えない範囲でパケットを送信していきます(送信後はトークンは削除されます)。

またバケツに溜まっている余分なトークンは、突発的なバースト状態(パケットが大量に届く状態)でパケットが到着しているときに使われます。バーストが起きているときはすでにバケツに溜まっている分のトークンを使ってパケットを送信しますので、溜まった分のトークンを使い切らないような短期的なバーストであれば、トークン速度(制限Rate)を超えたパケット送信が可能です。

バースト状態が続くとバケツのトークンがすぐになくなってしまうため遅延が発生していき、最終的にはパケットが破棄されてしまうことになります。

1. QoS について

3. SFQ

SFQはパケットの流れ(トラフィック)を整形しません。パケットを送り出す順番を決めるだけです。

SFQでは、トラフィックを多数の内部キューに分割して収納します。そして各キューをラウンドロビンで回り、各キューからパケットをFIFOで順番に送信していきます。

ラウンドロビンで順番にトラフィックが送信されることから、ある特定のトラフィックが他のトラフィックを圧迫してしまうことがなくなり、どのトラフィックも公平に送信されるようになります(複数のトラフィックを平均化できる)。

※整形とは、トラフィック量が一定以上にならないように転送速度を調節することを指します。
「シェーピング」とも呼ばれます。

4. PQ

PQは優先制御の1つです。トラフィックのシェーピングは起こりません。

PQでは、パケットを分類して送り込むクラスに優先順位をつけておきます。そしてフィルタによってパケットをそれぞれのクラスに分類したあと、優先度の高いクラスから優先的にパケットを送信します。なお、クラス内のパケットはFIFOで取り出されます。

優先度の高いクラスに常にパケットがキューイングされているときには、より優先度の低いクラスからはパケットが送信されなくなります。

I.QoS について

5.CBQ

CBQは帯域制御の1つです。複数のクラスを作成しクラスごとに帯域幅を設定することで、パケットの種類に応じて使用できる帯域を割り当てる方式です。

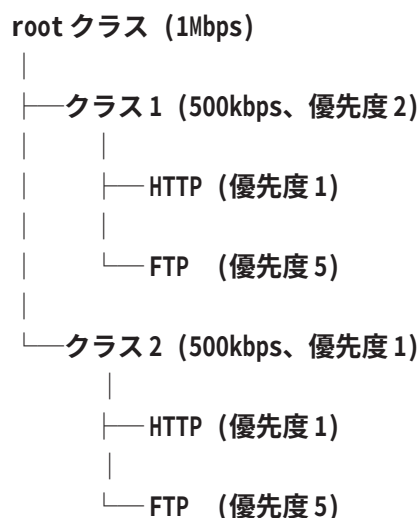
CBQにおけるクラスは、階層的に管理されます。最上位にはrootクラスが置かれ、利用できる総帯域幅を定義しておきます。rootクラスの下に子クラスが置かれ、それぞれの子クラスにはrootで定義した総帯域幅の一部を利用可能帯域として割り当てます。子クラスの下には、さらにクラスを置くこともできます。

各クラスへのパケットの振り分けは、フィルタ(クラス分けフィルタ)の定義に従っておこなわれます。

各クラスには帯域幅を割り当てます。兄弟クラス間で割り当てている帯域幅の合計が、上位クラスで定義している帯域幅を超えないように設計しなければなりません。

また、それぞれのクラスには優先度を割り振り、優先度に従ってパケットを送信していきます。

<クラス構成図(例)>



子クラスからはFIFOでパケットが送信されますが、子クラスの下にキューイングを定義し、クラス内でのキューイングをおこなうこともできます(クラスキューイング)。

CBQの特徴として、各クラス内において、あるクラスが兄弟クラスから帯域幅を借りることができます。たとえば図のクラス1において、トラフィックが500kbpsを超えていて、且つ、クラス2の使用帯域幅が500kbps以下の場合に、クラス1はクラス2で余っている帯域幅を借りてパケットを送信することができます。

II.QoS 機能の各設定画面について

Interface Queuing 設定画面

本装置の各インタフェースでおこなうキューイング方式を定義します。すべてのキューイング方式で設定が必要です。

CLASS 設定

CBQ をおこなう場合の、各クラスについて設定します。

CLASS Queuing 設定

各クラスにおけるキューイング方式を定義します。CBQ 以外のキューイング方式について定義できません。

CLASS 分けフィルタ設定

パケットを各クラスに振り分けるためのフィルタ設定を定義します。PQ、CBQ をおこなう場合に設定が必要です。

パケット分類設定

各パケットに TOS 値や MARK 値を付加するための設定です。PQ をおこなう場合に設定します。PQ では IP ヘッダによる CLASS 分けフィルタリングができないため、TOS 値または MARK 値によってフィルタリングをおこないます。

III. 各キューイング方式の設定手順について

各キューイング方式の基本的な設定手順は以下の通りです。

◆ pfifo の設定手順

「Interface Queueing 設定」でキューのサイズを設定します。

◆ TBF の設定手順

「Interface Queueing 設定」で、トークンのレート、バケツサイズ、キューのサイズを設定します。

◆ SFQ の設定手順

「Interface Queueing 設定」で設定します。

◆ PQ の設定手順

1. インタフェースの設定

「Interface Queueing 設定」で、Band 数、Priority-map、Marking Filter を設定します。

2. CLASS 分けのためのフィルタ設定

「CLASS 分けフィルタ設定」で、Mark 値によるフィルタを設定します。

3. パケット分類のための設定

「パケット分類設定」で、TOS 値または MARK 値の付与設定をおこないます。

◆ CBQ の設定手順

1. ルートクラスの設定

「Interface Queueing 設定」で、ルートクラスの設定をおこないます。

2. 各クラスの設定

- ・「CLASS 設定」で、全てのクラスの親となる親クラスについて設定します。

- ・「CLASS 設定」で、親クラスの下に置く子クラスについて設定します。

- ・「CLASS 設定」で、子クラスの下に置くリーフクラスを設定します。

3. クラス分けの設定

「CLASS 分けフィルタ設定」で、CLASS 分けのマッチ条件を設定します。

4. クラスキューイングの設定

クラス内でさらにキューイングをおこなうときには「CLASS Queueing 設定」でキューイング設定をおこないます。

IV. 各設定画面での設定方法について

◆ Interface Queueing 設定

すべてのキューイング方式において設定が必要です。設定を追加するときは「New Entry」をクリックします。

Interface 名	eth0																						
Queueing Discipline	---																						
pfifo queue limit (pfifo選択時有効)																							
TBF Parameter 設定																							
制限 Rate	Kbit/s																						
Buffer Size	byte																						
Limit Byte (tokenが利用できるようになるまで Queueing可能なbyte数)	byte																						
CBQ Parameter 設定																							
回線帯域	Kbit/s																						
平均パケットサイズ	byte																						
PQ Parameter 設定																							
最大Band数設定	3 default 3 (2-5)																						
Priority-map設定	1 2 2 2 1 2 0																						
Marking Filter 選択 (PacketヘッダによるFilter設定は選択できません)	<table border="1"> <thead> <tr> <th>FilterNo.</th> <th>Class No.</th> </tr> </thead> <tbody> <tr><td>1.</td><td></td></tr> <tr><td>2.</td><td></td></tr> <tr><td>3.</td><td></td></tr> <tr><td>4.</td><td></td></tr> <tr><td>5.</td><td></td></tr> <tr><td>6.</td><td></td></tr> <tr><td>7.</td><td></td></tr> <tr><td>8.</td><td></td></tr> <tr><td>9.</td><td></td></tr> <tr><td>10.</td><td></td></tr> </tbody> </table>	FilterNo.	Class No.	1.		2.		3.		4.		5.		6.		7.		8.		9.		10.	
FilterNo.	Class No.																						
1.																							
2.																							
3.																							
4.																							
5.																							
6.																							
7.																							
8.																							
9.																							
10.																							

○ Interface 名

キューイングをおこなうインタフェース名を入力します。

インタフェース名は「付録A インタフェース名について」を参照してください。

○ Queueing Discipline

キューイング方式を選択します。

[pfifo の設定]

○ pfifo queue limit

パケットをキューイングするキューの長さを設定します。**パケットの数**で指定します。1～999 の範囲で設定してください。

[TBF の設定]

「TBF Parameter 設定」について設定します。

○ 制限 Rate

バケツにトークンを入れていく速度を設定します。

回線の実効速度を上限に設定してください。

○ Buffer Size

バケツのサイズを設定します。これは瞬間的に利用できるトークンの最大値となります。帯域の制限幅を大きくするときは、Buffer Size を大きく設定しておきます。

○ Limit Byte

トークンを待っている状態でキューイングするときの、キューのサイズを設定します。

[SFQ の設定]

Queueing Discipline で「SFQ」を選択するだけです。

IV. 各設定画面での設定方法について

[PQ の設定]

「PQ Parameter 設定」について設定します。

○最大 Band 数設定

生成するバンド数を設定します。ここでいう band 数はクラス数のことです。

本装置で設定されるクラス ID は 1001:、1002:、1003:、1004:、1005: となります。

初期設定は 3 です(クラス ID 1001:～1003:)。最大数は 5(クラス ID 1001:～1005:)です。初期設定外の数値に設定した場合は、Priority-map 設定を変更します。

○Priority-map 設定

Priority-map には 7 つの入れ物が用意されています(左から 0、1、2、3、4、5、6 という番号が付けられています)。そしてそれぞれに Band を設定します。最大 Band 数で設定した範囲で、それぞれに Band を設定できます。

○Marking Filter 設定

パケットの Marking 情報によって振り分けを決定するときに設定します。

Filter No. には Class 分けフィルタの設定番号を指定します。

Class No. には、パケットをおくるクラス番号を指定します(1001:が Class No.1、1002:が Class No.2、1003:が Class No.3、1004:が Class No.4、1005:が Class No.5 となります)。

○Priority-map の箱に付けられている番号は、TOS 値の「Linux における扱い番号(パケットの優先度)」とリンクしています。('TOS 値について」を参照ください)

○インタフェースに届いたパケットは、2 つの方法でクラス分けされます。

- ・TOS フィールドの「Linux における扱い番号(パケットの優先度)」を参照し、同じ番号の Priority-map の箱にパケットを送ります。

- ・Marking Filter 設定に従って、各クラスにパケットを送る

○Prioritymap の箱に付けられる Band はクラスのことです。箱に設定されている値のクラスに属することを意味します。より Band 数が小さい方が優先度が高くなります。

○クラス分けされたあとのパケットは、優先度の高いクラスから FIFO で送信されていきます。
各クラスの優先度は 1001: > 1002: > 1003: > 1004: > 1005: となります。

○より優先度の高いクラスにパケットがあると、その間は優先度の低いクラスからはパケットが送信されなくなります。

IV. 各設定画面での設定方法について

【CBQ の設定】

「CBQ Parameter 設定」について設定します。

○回線帯域

root クラスの帯域幅を設定します。接続回線の物理的な帯域幅を設定します(10Base-TXで接続しているときは10000kbits/s)。

○平均パケットサイズ設定

パケットの平均サイズを設定します。バイト単位で設定します。

IV. 各設定画面での設定方法について

◆ CLASS 設定

設定を追加するときは「New Entry」をクリックします。

Description	user_1
Interface名	eth0
Class ID	10
親 class ID	1
Priority	1
Rate設定	1000 Kbit/s
Class内 Average Packet Size設定	1000 byte
Maximum Burst設定	20
Bounded設定	☒ 有効 ☐ 無効
Filter設定 (Filter番号を入力してください)	1. 2. 3. 4. 5. 6. 7. 8. 9. 10.

(画面は表示例です)

○ Description

設定名を付けることができます。半角英数字のみ使用可能です。

○ Interface 名

キューイングをおこなうインタフェース名を入力します。

インタフェース名は「付録A インタフェース名について」を参照してください。

○ Class ID

クラス ID を設定します。クラスの階層構造における <minor 番号> となります。

○ 親 Class ID

親クラスの ID を指定します。クラスの階層構造における <major 番号> となります。

○ Rate 設定

クラスの帯域幅を設定します。設定は kbit/s 単位となります。

○ Class 内 Average Packet Size 設定

クラス内のパケットの平均サイズを指定します。設定はバイト単位となります。

○ Maximum Burst 設定

一度に送信できる最大パケット数を指定します。

○ bounded 設定

「有効」を選択すると、兄弟クラスから余っている帯域幅を借りようとはしなくなります (Rate 設定値を超えて通信しません)。

「無効」を選択すると、その逆の動作となります。

○ Filter 設定

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

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

◆ 「CLASS Queueing 設定」

設定を追加するときは「New Entry」をクリックします。

Description																							
Interface 名	eth0																						
QDISC 番号																							
MAJOR ID	1																						
class ID																							
Queueing Discipline	---																						
pfifo limit (PFIFO 選択時有効)																							
TBF Parameter 設定																							
制限 Rate	Kbit/s																						
Buffer Size	byte																						
Limit Byte (token が利用できるようになるまで queueing 可能な byte 数)																							
PQ Parameter 設定																							
最大 Band 数 設定	3 default 3 (2-5)																						
priority-map 設定	1 2 2 2 1 2 0																						
Marking Filter の選択 (Packet ヘッダ による Filter 設定 は 選択 できません)	<table border="1"> <thead> <tr> <th>FilterNo.</th> <th>Class No.</th> </tr> </thead> <tbody> <tr><td>1.</td><td> </td></tr> <tr><td>2.</td><td> </td></tr> <tr><td>3.</td><td> </td></tr> <tr><td>4.</td><td> </td></tr> <tr><td>5.</td><td> </td></tr> <tr><td>6.</td><td> </td></tr> <tr><td>7.</td><td> </td></tr> <tr><td>8.</td><td> </td></tr> <tr><td>9.</td><td> </td></tr> <tr><td>10.</td><td> </td></tr> </tbody> </table>	FilterNo.	Class No.	1.		2.		3.		4.		5.		6.		7.		8.		9.		10.	
FilterNo.	Class No.																						
1.																							
2.																							
3.																							
4.																							
5.																							
6.																							
7.																							
8.																							
9.																							
10.																							

(画面は表示例です)

○ MAJOR ID

親のクラス ID を指定します。クラスの階層構造における <major 番号> となります。

○ Class ID

親クラスの ID を指定します。クラスの階層構造における <minor 番号> となります。

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

○ Description

設定名を付けることができます。半角英数字のみ使用可能です。

○ Interface 名

キューイングをおこなうインタフェース名を選択します。

インタフェース名は「付録 A インタフェース名について」を参照してください。

○ QDISC 番号

このクラスが属している QDISC 番号を指定します。

IV. 各設定画面での設定方法について

◆「CLASS 分けフィルタ設定」

設定を追加するときは「New Entry」をクリックします。

設定番号	1
Description	host_1
Priority	1 (1-999)
☒ パケットヘッダ情報によるフィルタ	
プロトコル	6 (Protocol番号)
送信元アドレス	192.168.0.1/32
送信元ポート	(ポート番号)
宛先アドレス	10.10.10.10/32
宛先ポート	80 (ポート番号)
TOS 値	2 (hex:0-fe)
DSCP 値	(hex:0-3f)
☐ Marking情報によるフィルタ	
Mark 値	(1-999)

(画面は表示例です)

○Description

設定名を付けることができます。半角英数字のみ使用可能です。

○Priority

複数の CLASS 分けフィルタ間での優先度を設定します。値が小さいものほど優先度が高くなります。

○パケットヘッダによるフィルタ

パケットヘッダ情報で CLASS 分けをおこなうときにチェックします。以下、マッチ条件を設定していきます。ただし PQ をおこなうときは、パケットヘッダによるフィルタはできません。

○プロトコル

プロトコルを指定します。プロトコル番号で指定してください。

○送信元アドレス

送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。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。

○TOS 値

TOS 値を指定します。16 進数で指定します。

○DSCP 値

DSCP 値を設定します。16 進数で指定します。

○Marking 情報によるフィルタ

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

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

◆「パケット分類設定」

設定を追加するときは「New Entry」をクリックします。

設定番号	1		
パケット分類条件			
プロトコル	6 (Protocol番号)	☐ Not条件	
送信元アドレス	192.168.0.1/32	☐ Not条件	
送信元ポート	1024:65535 (ポート番号/範囲指定で番号連結)	☐ Not条件	
宛先アドレス	10.10.10.10/32	☐ Not条件	
宛先ポート	80 (ポート番号/範囲指定で番号連結)	☐ Not条件	
インターフェース	ppp1	☐ Not条件	
TOS/MARK/DSCP値	☒ TOS ☐ MARK ☐ DSCP ☐ マッチ条件無効 8 上記で選択したマッチ条件に対応する設定値		
TOS Bit値 hex: 0:Normal Service 2:Minimize cost 4:Maximize Reliability 8:Maximize Throughput 10:Minimize Delay MARK値 (1-999) DSCP Bit値 hex(0-3f)			
TOS/MARK/DSCP値の設定			
設定対象	☒ TOS/Precedence ☐ MARK ☐ DSCP		
設定値	・MARK設定 (1-999) ・TOS/Precedence設定 Minimize cost(1) TOS Bit Internetwork Control(6) Precedence Bit ・DSCP設定 選択して下さい DSCP Bit		

(画面は表示例です)

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

[パケット分類条件]

パケット選別のマッチ条件を定義します。

○プロトコル

プロトコルを指定します。プロトコル番号で指定してください。

○送信元アドレス

送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。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

インターフェースを選択します。

インターフェース名は「付録A インターフェース名について」を参照してください。

各項目について「Not 条件」にチェックを付けると、その項目で指定した値以外のものがマッチ条件となります。

○TOS/MARK/DSCP 値

マッチングする TOS/MARK/DSCP 値を指定します。TOS、MARK、DSCP のいずれかを選択し、その値を指定します。これらをマッチ条件としないときは「マッチ条件無効」を選択します。

[TOS/MARK/DSCP 値]

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

○設定対象

TOS/Precedence、MARK、DSCP のいずれかを選択します。

○設定値

設定対象で選択したものについて、設定値を指定します。

設定後は「設定」ボタンをクリックします。

TOS/Precedence および DSCP については章末をご参照下さい。

V. ステータスの表示

「ステータス表示」をクリックすると、以下の画面に移ります。

Queueing Discipline ステータス表示	表示する
CLASS設定 ステータス表示	表示する
CLASS分けルール ステータス表示	表示する
各インターフェースの上記ステータスをすべて表示	表示する
Packet分類設定 ステータス表示	表示する
Interfaceの指定	eth0

QoS機能の各種ステータスを表示します。

「Packet 分類設定ステータス表示」以外では、必ずInterface 名を「Interface の指定」に入力してから「表示する」ボタンをクリックしてください。

VI. 設定の編集・削除方法

設定をおこなうと、設定内容が一覧で表示されます。

	FilterType	Description	Priority	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート	TOS値	MARK値	Configure
1	Mark		1							1	Edit,Remove
2	Mark		2							2	Edit,Remove
3	Mark		3							3	Edit,Remove

(「クラス分けフィルタ設定」画面の表示例)

Configure の「Edit」をクリックすると設定画面に遷移し、その設定を修正できます。

「Remove」をクリックすると、その設定が削除されます。

VII. ステータス情報の表示例

[Queueing 設定情報]表示例

各クラスで設定したキューイング方式や設定パラメータの他、送信したパケット数・送信データサイズ等の情報を表示します。

```
qdisc pfifo 1: limit 300p  
Sent 9386 bytes 82 pkts (dropped 0, overlimits 0)
```

qdisc -> キューイング方式
1: -> キューイングを設定しているクラス ID
limit -> キューイングできる最大パケット数
Sent (nnn) byte (mmm)pkts -> 送信したデータ量とパケット数
dropped -> 破棄したパケット数
overlimits -> 過負荷の状態で届いたパケット数

```
qdisc sfq 20: limit 128p quantum 1500b flows 128/1024 perturb 10sec  
Sent 140878 bytes 206 pkts (dropped 0, overlimits 0)
```

limit (nnn)p -> キューに待機できるパケット数
quantum -> パケットのサイズ
flows (nnn)/(mmm) -> mmm 個のバケツが用意され、同時にアクティブになるのは nnn 個まで
perturb (n)sec -> ハッシュの更新間隔

```
qdisc tbf 1: rate 500Kbit burst 1499b/8 mpu 0b lat 4295.0s  
Sent 73050 bytes 568 pkts (dropped 2, overlimits 17)
```

rate -> 設定している帯域幅
burst -> バケツのサイズ
mpu -> 最小パケットサイズ
lat -> パケットが tbf に留まっていられる時間

```
qdisc cbq 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8 weight  
1000Kbit allot 1514b
```

```
level 2 ewma 5 avpkt 1000b maxidle 242us  
Sent 2420755 bytes 3945 pkts (dropped 0, overlimits 0)  
borrowed 0 overactions 0 avgidle 6399 undertime 0
```

bounded,isolated -> bounded,isolated 設定がされている (bounded は帯域を借りない、isolated は帯域を貸さない)
prio -> 優先度(上記では root クラスなので、prio 値はありません)
weight -> ラウンドロビンプロセスの重み
allot -> 送信できるデータサイズ
ewma -> 指数重み付け移動平均
avpkt -> 平均パケットサイズ
maxidle -> パケット送信時の最大アイドル時間
borrowed -> 帯域幅を借りて送信したパケット数
avgidle -> EMMA で測定した値から、計算したアイドル時間を差し引いた数値。
通常は数字がカウントされていますが、負荷で一杯の接続の状態では "0"、
過負荷の状態ではマイナスの値になります

VII. ステータス情報の表示例

[CLASS 設定情報]表示例

設定している各クラスの情報を表示します。

その1(CBQでの表示例)

```
class cbq 1: root rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8
weight 1000Kbit allot 1514b
level 2 ewma 5 avpkt 1000b maxidle 242us
  Sent 33382 bytes 108 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 6399 undertime 0
class cbq 1:10 parent 1:1 rate 500Kbit cell 8b mpu 64b prio 1/1 weight 50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
  Sent 0 bytes 0 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 181651 undertime 0
class cbq 1:1 parent 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio 3/3 weight
100Kbit allot 1500b
level 1 ewma 5 avpkt 1000b maxidle 242us
  Sent 2388712 bytes 3843 pkts (dropped 0, overlimits 0)
  borrowed 2004 overactions 0 avgidle 6399 undertime 0
class cbq 1:20 parent 1:1 leaf 20: rate 500Kbit cell 8b mpu 64b (bounded) prio 2/2 weight
50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
  Sent 142217 bytes 212 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 174789 undertime 0
```

parent -> 親クラス ID

その2(PQでの表示例)

```
class prio 1: parent 1: leaf 1001:
class prio 1: parent 1: leaf 1002:
class prio 1: parent 1: leaf 1003:
```

prio -> 優先度

parent -> 親クラス ID

leaf -> leaf クラス ID

VII. ステータス情報の表示例

[CLASS 分けフィルタ設定情報]表示例

クラス分けフィルタの設定情報を表示します。

その1(CBQ での表示例)

```
[ PARENT 1: ]
filter protocol ip pref 1 u32
filter protocol ip pref 1 u32 fh 805: ht divisor 1
filter protocol ip pref 1 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 1 u32 fh 804: ht divisor 1
filter protocol ip pref 1 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32
filter protocol ip pref 3 u32 fh 805: ht divisor 1
filter protocol ip pref 3 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32 fh 804: ht divisor 1
filter protocol ip pref 3 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8

protocol -> マッチするプロトコル
pref -> 優先度
u32 -> パケット内部のフィールド (発信元 IP アドレスなど) に基づいて
      処理すべきクラスの決定を行います
at 8、at16 -> マッチの開始は、指定した数値分のオフセットからであることを示します。
              at 8であれば、ヘッダの9バイトめからマッチします。
flowid -> マッチしたパケットを送るクラス
```

その2(PQ での表示例)

```
[ PARENT 1: ]
filter protocol ip pref 1 fw
filter protocol ip pref 1 fw handle 0x1 classid 1:3
filter protocol ip pref 2 fw
filter protocol ip pref 2 fw handle 0x2 classid 1:2
filter protocol ip pref 3 fw
filter protocol ip pref 3 fw handle 0x3 classid 1:1

pref -> 優先度
handle -> MARK 値
classid -> マッチパケットを送るクラス ID
```

VII. ステータス情報の表示例

[Packet 分類設定情報]表示例

パケット分類設定の情報を表示します。

pkts	bytes	target	prot	opt	in	out	source	destination	
272	39111	MARK	all	--	eth0	any	192.168.120.111	anywhere	MARK set 0x1
83	5439	MARK	all	--	eth0	any	192.168.120.113	anywhere	MARK set 0x2
447	48695	MARK	all	--	eth0	any	192.168.0.0/24	anywhere	MARK set 0x3
0	0	FTOS	tcp	--	eth0	any	192.168.0.1	111.111.111.111	tcp spts:1024:

65535 dpt:450 Type of Service set 0x62

pkts -> 入力(出力)されたパケット数

bytes -> 入力(出力)されたバイト数

target -> 分類の対象(MARK か TOS か)

prot -> プロトコル

in -> パケット入力インタフェース

out -> パケット出力インタフェース

source -> 送信元 IP アドレス

destination -> あて先 IP アドレス

MARK set -> セットする MARK 値

spts -> 送信元ポート番号

dpt -> あて先ポート番号

Type of Service set -> セットする TOS ビット値

VIII. クラスの階層構造について

CBQにおけるクラスの階層構造は以下のようになります。

◆ root クラス

ネットワークデバイス上のキューイングです。
本装置のシステムが直接的に対話するのはこのクラスです。

◆ 親クラス

すべてのクラスのベースとなるクラスです。帯域幅を 100% として定義します。

◆ 子クラス

親クラスから分岐するクラスです。親クラスの持つ帯域幅を分割して、それぞれの子クラスの帯域幅として持ちます。

◆ leaf(葉)クラス

leaf クラスは自分から分岐するクラスがないクラスです。

◆ qdisc

キューイングです。ここでキューを管理・制御します。

[クラス ID について]

各クラスはクラス ID を持ちます。クラス ID は MAJOR 番号と MINOR 番号の 2 つからなります。表記は以下のようになります。

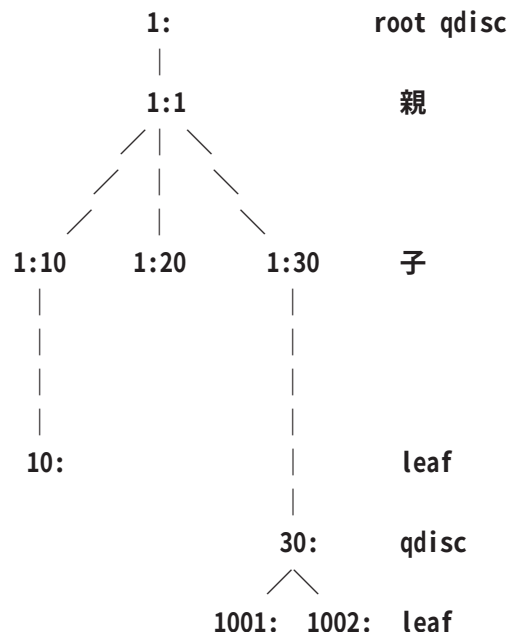
<MAJOR 番号> : <MINOR 番号>

・ root クラスは「1:0」というクラス ID を持ちます。

・ 子クラスは、親と同じ MAJOR 番号を持つ必要があります。

・ MINOR 番号は、他のクラスと qdisc 内で重複しないように定義する必要があります。

<クラス構成図(例)>



IX.TOS について

IP パケットヘッダには TOS フィールドが設けられています。ここにパケットの優先度情報を付与しておくことで、優先度にあわせて機器がパケットを適切に扱えることを期待します。

IP ヘッダ内の TOS フィールドの各ビットは、以下のように定義されています。<表 1>

バイナリ 10 進数 意味

1000	8	Minimize delay (md)
0100	4	Maximize throughput (mt)
0010	2	Maximize reliability (mr)
0001	1	Minimize monetary cost (mmc)
0000	0	Normal Service

md は最小の遅延、mt は最高のスループット、mr は高い信頼性、mmc は低い通信コスト、を期待するパケットであることを示します。

各ビットの組み合わせによる TOS 値は以下のように定義されます。<表 2>

TOS	ビット	意味	Linux での扱い	バンド
0x0	0	Normal Service	0 Best Effort	1
0x2	1	Minimize Monetary Cost	1 Filler	2
0x4	2	Maximize Reliability	0 Best Effort	1
0x6	3	mmc+mr	0 Best Effort	1
0x8	4	Maximize Throughput	2 Bulk	2
0xa	5	mmc+mt	2 Bulk	2
0xc	6	mr+mt	2 Bulk	2
0xe	7	mmc+mr+mt	2 Bulk	2
0x10	8	Minimize Delay	6 Interactive	0
0x12	9	mmc+md	6 Interactive	0
0x14	10	mr+md	6 Interactive	0
0x16	11	mmc+mr+md	6 Interactive	0
0x18	12	mt+md	4 Int. Bulk	1
0x1a	13	mmc+mt+md	4 Int. Bulk	1
0x1c	14	mr+mt+md	4 Int. Bulk	1
0x1e	15	mmc+mr+mt+md	4 Int. Bulk	1

バンドは優先度です。0 が最も優先度が高いものです。初期値ではバンド数は 3 (優先度は 3 段階) です。本装置では、PQ Paramater 設定の「最大 Band 数設定」でバンド数を変更できます (0 ~ 4)。

Linux での扱いの数値は、Linux での TOS ビット列の解釈です。これは PQ Paramater 設定の「Priority-map 設定」の箱にリンクしており、対応する Priority-map の箱に送られます。

IX.TOS について

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

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

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

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

X.DSCP について

本装置ではDS(DiffServ)フィールドの設定・書き換えも可能です。DSフィールドとは、IPパケット内のTOSの再定義フィールドであり、DiffServに対応したネットワークにおいてQoS制御動作の基準となる値が設定されます。DiffServ対応機器では、DSフィールド内のDSCP値だけを参照してQoS制御を行うことができます。

○TOSとDSフィールドのビット定義

【TOS フィールド構造】

```

  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+
|Precedence|Type of Service|CU|
+---+---+---+---+---+---+---+

```

【DSCP フィールド構造】

```

  0   1   2   3   4   5   6   7
+---+---+---+---+---+---+---+
|           DSCP           | CU |
+---+---+---+---+---+---+---+

```

DSCP: differentiated services code point

CU: currently unused (現在未使用)

DSCPビットのとりうる値とその制御方法の定義は以下のようになっています。

定義名	DSCP 値	制御方法
EF(Expedited Forwarding)	0x2e	パケットを最優先で転送(RFC3246)
AF(Assured Forwarding) AF11/AF12/AF13 AF21/AF22/AF23 AF31/AF32/AF33 AF41/AF42/AF43	0x0a / 0x0c / 0x0e 0x12 / 0x14 / 0x16 0x1a / 0x1c / 0x1e 0x22 / 0x24 / 0x26	4つの送出優先度と3つの廃棄優先度を持ち、数字の上位桁は送出優先度(クラス)、下位桁は廃棄優先度を表します。(RFC2597) ・送出優先度 (高) 1 > 2 > 3 > 4 (低) ・廃棄優先度 (高) 1 > 2 > 3 (低)
CS(Class Selector) CS1 CS2 CS3 CS4 CS5 CS6 CS7	0x08 0x10 0x18 0x20 0x28 0x30 0x38	既存のTOS互換による優先制御を行います。 Precedence1(Priority) Precedence2(Immediate) Precedence3(Flash) Precedence4(Flash Override) Precedence5(Critic/ESP) Precedence6(Internetwork Control) Precedence7(Network Control)
BE (Best Effort)	0x00	ベストエフォート(優先制御なし)

第 32 章

ネットワークテスト

第 32 章 ネットワークテスト

ネットワークテスト

XR-440 の運用時において、ネットワークテストをおこなうことができます。ネットワークのトラブルシューティングに有効です。以下の3つのテストができます。

- ping テスト
- traceroute テスト
- パケットダンプの取得

実行方法

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

Ping	FQDNまたはIPアドレス インターフェースの指定(省略可) ☐ 主回線 ☐ マルチ#2 ☐ マルチ#3 ☐ マルチ#4 ☐ Ether0 ☐ Ether1 ☐ Ether2 ☒ その他 実行
Trace Route	FQDNまたはIPアドレス 実行
パケットダンプ	☒ 主回線 ☐ マルチ#2 ☐ マルチ#3 ☐ マルチ#4 ☐ Ether0 ☐ Ether1 ☐ Ether2 ☐ その他 実行 結果表示

○pingテスト

指定した相手に XR-440 から Ping を発信します。FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力して「実行」をクリックします。また ping を送出するインターフェースを指定することもできます(省略化)

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=49.5 ms
64 bytes from 211.14.13.66: icmp_seq=1 ttl=52 time=65.7 ms
64 bytes from 211.14.13.66: icmp_seq=2 ttl=52 time=11.7 ms
64 bytes from 211.14.13.66: icmp_seq=3 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=4 ttl=52 time=69.0 ms
64 bytes from 211.14.13.66: icmp_seq=5 ttl=52 time=58.3 ms
64 bytes from 211.14.13.66: icmp_seq=6 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=7 ttl=52 time=71.4 ms
64 bytes from 211.14.13.66: icmp_seq=8 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=9 ttl=52 time=11.8 ms

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

○traceroute テスト

指定した宛先までに経由するルータの情報を表示します。ping と同様に、FQDN もしくは IP アドレスを入力して「実行」をクリックします。

実行結果例

実行結果

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

--- 211.14.13.66 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.4/12.4/12.4 ms
traceroute to 211.14.13.66 (211.14.13.66), 30 hops max, 40 byte packets
 1 192.168.120.15 (192.168.120.15) 1.545 ms 2.253 ms 1.607 ms
 2 192.168.100.50 (192.168.100.50) 2.210 ms 4.955 ms 2.309 ms
 3 172.17.254.1 (172.17.254.1) 8.777 ms 21.189 ms 13.946 ms
 4 210.135.192.108 (210.135.192.108) 9.205 ms 8.953 ms 9.310 ms
 5 210.135.208.34 (210.135.208.34) 35.538 ms 19.923 ms 14.744 ms
 6 210.135.208.10 (210.135.208.10) 41.641 ms 40.476 ms 63.293 ms
 7 210.171.224.115 (210.171.224.115) 43.948 ms 27.255 ms 36.767 ms
 8 211.14.3.233 (211.14.3.233) 36.861 ms 33.890 ms 37.679 ms
 9 211.14.3.148 (211.14.3.148) 36.865 ms 47.151 ms 18.491 ms
10 211.14.3.105 (211.14.3.105) 53.573 ms 13.889 ms 50.057 ms
11 211.14.2.193 (211.14.2.193) 33.777 ms 11.980 ms 17.282 ms
12 * * *
13 211.14.12.249 (211.14.12.249) 19.892 ms !X * 15.213 ms !X
```

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

第32章 ネットワークテスト

ネットワークテスト

○パケットダンプ

パケットのダンプを取得できます。

ダンプを取得したいインタフェースを選択して「実行」をクリックします。その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例

実行結果

```
19-08-26 587215 192.168.120.111.4837 > 192.168.120.118.800: [tcp sum ok] 2017161989:2017161989.0) seq:19865257 win:16550 (DF) (tl) 120, id 8212, len 40
19-08-32 759827 192.168.120.116.1070 > 200.140.128.53: [udp sum ok] 7+37 www.mechatronics.co.jp [checksum] (tl) 127, id 52533, len 59
19-08-32 716680 200.140.128.53.59 > 192.168.254.1:0000: [p < 0] www.mechatronics.co.jp [checksum] (tl) 127, id 52533, len 1000
19-08-32 760338 192.168.120.116.1074 > 210.173.173.17.80: 8 [tcp sum ok] 1422286:1422286.0) win:8182 (DF) (tl) 127, id 85486, len 40
19-08-32 764553 210.173.173.17.80 > 192.168.254.1:0000: [tcp sum ok] 2307110964:230711096.0) seq:1422289 win:8280 (DF) (tl) 110, id 25547, len 44
19-08-32 795580 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 1422289:1422289.0) seq:2307110965 win:8280 (DF) (tl) 127, id 54001, len 40
19-08-32 821350 210.173.173.17.80 > 192.168.254.1:0000: [p 1102100] seq:329 win:7982 (DF) (tl) 110, id 52559, len 148
19-08-32 835442 210.173.173.17.80 > 192.168.254.1:0000: [p 0] seq:1481 win:8280 (DF) (tl) 110, id 52565, len 1420
19-08-32 834003 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 329:329 win:7982 (DF) (tl) 110, id 42345, len 1312
19-08-32 836096 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 329:329 win:7982 (DF) (tl) 110, id 42356, len 1420
19-08-32 859487 210.173.173.17.80 > 192.168.254.1:0000: [p 2301414] seq:329 win:7982 (DF) (tl) 110, id 42345, len 1420
19-08-32 869512 210.173.173.17.80 > 192.168.254.1:0000: [p 5652] seq:329 win:7982 (DF) (tl) 110, id 42356, len 1420
19-08-32 880602 210.173.173.17.80 > 192.168.254.1:0000: [p 4141552] seq:329 win:7982 (DF) (tl) 110, id 42356, len 1420
19-08-32 881584 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 329:329 win:7982 (DF) (tl) 110, id 42356, len 1420
19-08-32 881537 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 329:329 win:7982 (DF) (tl) 110, id 42356, len 1420
19-08-32 882481 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 329:329 win:7982 (DF) (tl) 110, id 42356, len 1420
19-08-32 877942 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 329:329 win:7982 (DF) (tl) 110, id 42356, len 1420
19-08-32 899696 192.168.120.116.1074 > 210.173.173.17.80: [tcp sum ok] 1422287:1422287.0) win:8182 (DF) (tl) 127, id 770, len 40
19-08-32 905149 192.168.120.116.1074 > 210.173.173.17.80: 8 [tcp sum ok] 1422287:1422287.0) win:8182 (DF) (tl) 127, id 1020, len 40
19-08-32 904896 192.168.120.116.1074 > 210.173.173.17.80: 8 [tcp sum ok] 1422287:1422287.0) win:8182 (DF) (tl) 127, id 1020, len 40
19-08-32 979673 210.173.173.17.80 > 192.168.254.1:0000: [p 1102297916] seq:1102297916.0) seq:1422483 win:8280 (DF) (tl) 110, id 25733, len 44
19-08-32 977212 192.168.120.116.1070 > 210.173.173.17.80: [tcp sum ok] 1422483:1422483.0) seq:1102297916 win:8280 (DF) (tl) 127, id 1794, len 40
19-08-32 982544 210.173.173.17.80 > 192.168.254.1:0000: [p 0] seq:1102297916.0) seq:1422483 win:8280 (DF) (tl) 110, id 12544, len 44
19-08-32 982617 192.168.120.116.1070 > 210.173.173.17.80: [tcp sum ok] 1422483:1422483.0) seq:1102297916 win:8280 (DF) (tl) 127, id 2050, len 40
19-08-32 011634 192.168.120.116.1070 > 210.173.173.17.80: [p 0] seq:1481 win:8280 (DF) (tl) 127, id 2050, len 40
19-08-32 012222 192.168.120.116.1070 > 210.173.173.17.80: [p 0] seq:1481 win:8280 (DF) (tl) 127, id 2050, len 40
19-08-32 025663 210.173.173.17.80 > 192.168.254.1:0000: [p 11061160] seq:445 win:7906 (DF) (tl) 110, id 50564, len 300
19-08-32 043087 192.168.120.116.1070 > 210.173.173.17.80: [p 444820370] seq:164 win:6117 (DF) (tl) 127, id 3074, len 416
19-08-32 042445 210.173.173.17.80 > 192.168.254.1:0000: [p 11061160] seq:445 win:7906 (DF) (tl) 110, id 50564, len 300
19-08-32 047993 210.173.173.17.80 > 192.168.254.1:0000: [p 2521052] seq:376 win:7906 (DF) (tl) 110, id 50544, len 1420
19-08-32 050120 192.168.120.116.1070 > 210.173.173.17.80: [tcp sum ok] 376:376 win:7906 (DF) (tl) 110, id 51309, len 290
19-08-32 064108 210.173.173.17.80 > 192.168.254.1:0000: [p 1644142250] seq:821 win:7400 (DF) (tl) 110, id 51309, len 290
19-08-32 070064 210.173.173.17.80 > 192.168.254.1:0000: [p 4141794] seq:821 win:7400 (DF) (tl) 110, id 51309, len 290
19-08-32 072131 210.173.173.17.80 > 192.168.254.1:0000: [p 179431741330] seq:821 win:7400 (DF) (tl) 110, id 51309, len 290
19-08-32 075665 210.173.173.17.80 > 192.168.254.1:0000: [p 5652] seq:376 win:7906 (DF) (tl) 110, id 44504, len 1420
19-08-32 075676 210.173.173.17.80 > 192.168.254.1:0000: [p 30124382] seq:376 win:7906 (DF) (tl) 110, id 44504, len 1420
19-08-32 077659 210.173.173.17.80 > 192.168.254.1:0000: [p 43523772] seq:376 win:7906 (DF) (tl) 110, id 44504, len 1420
19-08-32 077944 192.168.120.116.1070 > 210.173.173.17.80: [tcp sum ok] 820:820 win:3174 win:8280 (DF) (tl) 127, id 3842, len 40
19-08-32 096122 210.173.173.17.80 > 192.168.254.1:0000: [p 5144554] seq:821 win:7400 (DF) (tl) 110, id 56675, len 1420
19-08-32 100292 210.173.173.17.80 > 192.168.254.1:0000: [p 4554594] seq:821 win:7400 (DF) (tl) 110, id 56675, len 1420
19-08-32 101517 210.173.173.17.80 > 192.168.254.1:0000: [p 5994584] seq:821 win:7400 (DF) (tl) 110, id 56675, len 1420
19-08-32 106837 192.168.120.116.1070 > 210.173.173.17.80: [tcp sum ok] 374:374 win:8280 (DF) (tl) 127, id 4026, len 40
19-08-32 109041 192.168.120.116.1070 > 210.173.173.17.80: [tcp sum ok] 820:820 win:3174 win:8280 (DF) (tl) 127, id 4254, len 40
19-08-32 128892 210.173.173.17.80 > 192.168.254.1:0000: [p 57123182] seq:376 win:7906 (DF) (tl) 110, id 64510, len 1420
19-08-32 128892 210.173.173.17.80 > 192.168.254.1:0000: [p 57123182] seq:376 win:7906 (DF) (tl) 110, id 64510, len 1420
19-08-32 131170 210.173.173.17.80 > 192.168.254.1:0000: [p 85322912] seq:376 win:7906 (DF) (tl) 110, id 65020, len 1420
```

「結果表示」をクリックするたびに、表示結果が更新されます。

パケットダンプの表示は、最大で100パケット分までです。100パケット分を超えると、古いものから順に表示されなくなります。

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

○PacketDump TypePcap

拡張版パケットダンプ取得機能です。

指定したインタフェースで、指定した数のパケットダンプを取得できます。

「Device」：パケットダンプを実行する、本装置のインタフェース名を設定します。

インタフェース名は本書「付録A インタフェース名について」をご参照下さい。

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

「CapSize」

1パケットごとのダンプデータの最大サイズを指定できます。単位は”byte”です。

たとえば128と設定すると、128バイト以上の長さのパケットでも128バイト分だけをダンプします。

大きなサイズでダンプするときは、本装置への負荷が増加することがあります。また記録できるダンプ数も減少します。

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

上記項目を入力後、「実行」ボタンでパケットダンプを開始します。

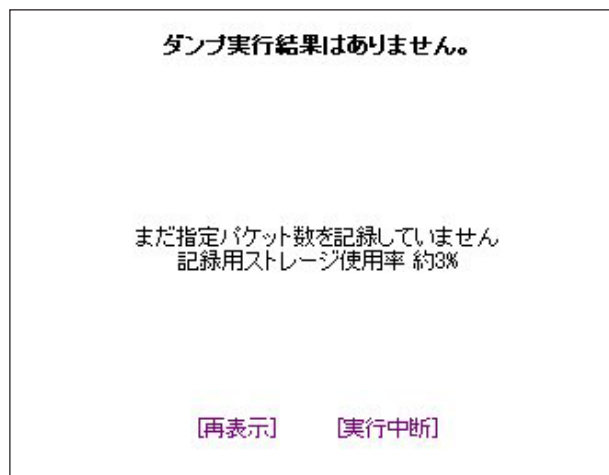
パケットダンプを開始したときの画面表示

実行結果は即時出力できない場合があります。
[再表示]で確認して下さい

[再表示] [実行中断]

ネットワークテスト

パケットダンプ結果を表示できないときの画面



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、上記のような画面が表示されます。

[PacketDump TypePcapの注意点]

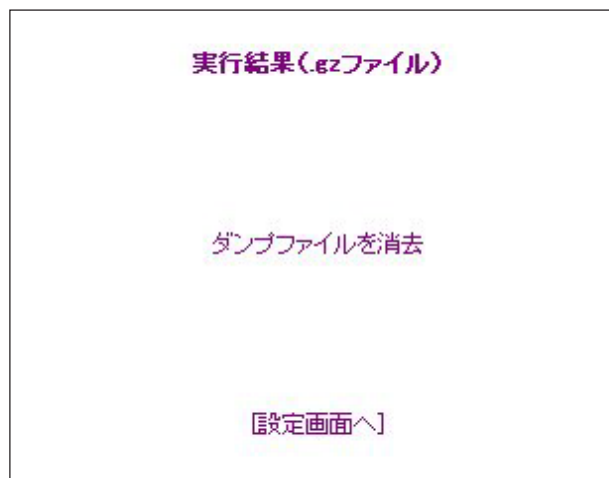
- 取得したパケットダンプ結果は、libcap形式でgzip圧縮して保存されます。

- 取得できるデータサイズは、gzip圧縮された状態で最大約1MB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「付録A インタフェース名について」をご参照下さい。

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。

第 33 章

システム設定

システム設定

「システム設定」ページでは、XR-440 の運用に関する制御をおこないます。下記の項目に関して設定・制御が可能です。

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

実行方法

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

◆時計の設定

XR-440 内蔵時計の設定をおこないます。

「時計の設定」をクリックして設定画面を開きます。

○24 時間単位で時刻を設定してください。

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

システム設定

◆ログの表示

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。

```
Apr 26 00:05:11 localhost -- MARK --
Apr 26 00:25:11 localhost -- MARK --
Apr 26 00:37:59 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 00:37:59 localhost named[436]: USAGE 1019749079 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 00:37:59 localhost named[436]: NSTATS 1019749079 1019556843 A=3
Apr 26 00:37:59 localhost named[436]: XSTATS 1019749079 1019556843 RR=0 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNKD=0
Apr 26 01:08:09 localhost -- MARK --
Apr 26 01:28:09 localhost -- MARK --
Apr 26 01:38:57 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 01:38:57 localhost named[436]: USAGE 1019752737 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 01:38:57 localhost named[436]: NSTATS 1019752737 1019556843 A=3
Apr 26 01:38:57 localhost named[436]: XSTATS 1019752737 1019556843 RR=0 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNKD=0
Apr 26 02:07:06 localhost -- MARK --
Apr 26 02:27:06 localhost -- MARK --
Apr 26 02:39:54 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 02:39:54 localhost named[436]: USAGE 1019756394 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 02:39:54 localhost named[436]: NSTATS 1019756394 1019556843 A=3
Apr 26 02:39:54 localhost named[436]: XSTATS 1019756394 1019556843 RR=0 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 SSysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIQ=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNKD=0
```

○XR-440のログが全てここで表示されます。

○「表示の更新」ボタンをクリックすると表示が更新されます。

◆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。

すべてのログメッセージを削除します。

実行する

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

システム設定

◆パスワードの設定

XR-440の設定画面にログインする際のユーザー名、パスワードを変更します。ルータ自身のセキュリティのためにパスワードを変更されることを推奨します。

実行方法

「パスワードの設定」をクリックして設定画面を開きます。

新しいユーザ名	
新しいパスワード	
もう一度入力してください	

○新しいユーザー名とパスワードを設定します。半角英数字で1から8文字まで設定可能です。大文字・小文字も判別しますのでご注意ください。

入力が終わりましたら「設定」ボタンをクリックして設定完了です。次回のログインからは、新しく設定したユーザー名とパスワードを使います。

システム設定

◆ファームウェアのアップデート

XR-440 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。

実行方法

「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。

ここではファームウェアのアップデートをおこなうことができます。

ファイルの指定		参照...
---------	----------------------	--------------------------------------

「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。

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

ファームウェアのアップデート	
ファームウェアのダウンロードが完了しました	
現在のファームウェアのバージョン	
Century Systems XR-440 Series ver 1.6.0	
ダウンロードされたファームウェアのバージョン	
Century Systems XR-440 Series ver 1.7.6	

このファームウェアでアップデートしますか？

注意: 3分以内にアップデートが実行されない場合はダウンロードしたファームウェアを破棄します

実行する	中止する
-------------------------------------	-------------------------------------

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

アップロード完了から3分以上経過したため
ファームウェアは破棄されました

時間内に「実行する」をクリックすると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。

ファームウェアのアップデート

ファームウェアのアップデートを実行します。
作業には数分かかりますので電源を切らずにお待ち下さい。
作業が終了しますと自動的に再起動します。

[一度ブラウザを閉じてからご利用下さい](#)

アップデート中は、本体の STATUS 1 (赤)が点滅します。この間は、アクセスをおこなわずにそのままお待ちください。

書き換えが終了すると本装置が自動的に再起動されて、アップデートの完了です。

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

システム設定

◆設定の保存と復帰

XR-440 の設定の保存および、保存した設定の復帰をおこないます。

実行方法

「設定の保存・復帰」をクリックして画面を開きます。

――注意――

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

[\[設定の保存・復帰\]](#)

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

[設定の保存]

設定を保存するときは、テキストのエンコード形式と保存形式を選択して「設定ファイルの作成」をクリックします。

現在の設定を保存することができます。	
コードの指定	☐ EUC (LF) ☒ S.JIS (CR+LF) ☐ S.JIS (CR)
形式の指定	☐ 全設定 (gzip) ☒ 初期値との差分 (text)

クリックすると以下のメッセージが表示されます。

設定をバックアップしました。
バックアップファイルのダウンロード

ブラウザのリンクを保存する等で保存して下さい。

「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。

「全設定」を選択すると、すべてのXR-440の設定をgzip形式で圧縮して保存します。

「初期値との差分」を選択すると、初期値と異なる設定のみを抽出して、テキスト形式で保存します。

このテキストファイルの内容を直接書き換えて設定を変更することもできます。

[設定の復帰]

上記項目から「参照」をクリックして、保存しておいた設定ファイルを選択します。全設定の保存ファイルはgzip圧縮形式のまま、復帰させることができます。

ここでは設定を復帰させることができます。	
ファイルの指定	参照...

その後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、XR-440 が自動的に再起動されます。

――注意――

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

システム設定

◆設定のリセット

XR-440 の設定を全てリセットし、工場出荷時の設定に戻します。

実行方法

「設定のリセット」をクリックして画面を開きます。

現在の本体設定内容を全てクリアして工場出荷設定に戻します。

実行する

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

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

◆本体再起動

XR-440 を再起動します。設定内容は変更されません。

実行方法

「再起動」をクリックして画面を開きます。

本体を再起動します。

実行する

「実行する」ボタンをクリックすると、リセットが実行されます。

本体の再起動をおこなった場合、それまでのログは全てクリアされます。

システム設定

◆セッションライフタイムの設定

NAT/IP マスカレードのセッションライフタイムを設定します。

それぞれの項目で "0" を設定すると、初期値で動作します。

「セッションライフタイムの設定」をクリックして画面を開きます。

「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。

UDP	30	秒 (0 - 8640000)
UDP stream	180	秒 (0 - 8640000)
TCP	3600	秒 (0 - 8640000)
セッション最大数	8192	セッション (0, 4096 - 16384)
0を入力した場合、デフォルト値を設定します。		

○ UDP

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

○ UDP stream

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

○ TCP

TCP セッションのライフタイムを設定します。単位は秒です。0 ～ 8640000 の間で設定します。初期設定は 432000 秒です。

○ セッション最大数

XR-440 で保持できる NAT/IP マスカレードのセッション情報の最大数を設定します。UDP/UDPstream/TCP のセッション情報を合計した最大数になります。4096 ～ 16384 の間で設定します。初期設定は 4096 です。

なお、XR-440 内部で保持しているセッション数は、周期的に syslog に表示することができます。詳しくは第 17 章「SYSLOG サービス」のシステムメッセージの項を参照してください。

システム設定

◆設定画面の設定

WEB設定画面へのアクセスログについての設定をします。

実行方法

「設定画面の設定」をクリックして画面を開きます。

アクセスログ	☒ 使用しない ☐ syslogに取る
エラーログ	☒ 使用しない ☐ syslogに取る

設定画面の

- アクセスログ
- (アクセス時の)エラーログ

を取得するかどうかを選択して、「設定の保存」をクリックします。

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

◆ISDN 設定

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

実行方法

「ISDN 設定」をクリックして画面を開きます。

ISDN番号	
サブアドレス	

○ ISDN 番号

ISDN 発信者番号を入力します。

○サブアドレス

サブアドレスを指定します。

最後に「設定の保存」をクリックします。

システム設定

◆オプションCFカード

XR-440シリーズにオプションで用意されているコンパクトフラッシュ(CF)カードを装着している場合にCFカードの操作を行ないます。

- ・CFカードの初期化
- ・CFカードへの設定のバックアップ

ができます。

「オプションCFカード」をクリックして画面を開きます。
画面上部には、装着したCFカードの情報が表示されます。

オプションCFカードの状況
総容量 [62436 kbyte] 空容量 [59370 kbyte] 使用率 [5%]
機器設定のバックアップはありません

オプションCFカードに現在の設定をコピーします

設定ファイルをコピーする

オプションCFカードを初期化します

オプションCFカードの初期化

○設定ファイルをコピーする

設定のバックアップをCFカードにコピーするときに実行します。

○オプションCFカードの初期化

CFカードを初期化するときに実行します。

また、CFカードを本装置から取り外すときは、**か**
ならず「本体の停止」を実行するか、本体前面の
「RELEASE」ボタンを使用してから取り外してくだ
さい。この作業を行わずにCFカードを取り外す
と、本装置およびCFカードが破損する場合があります。

はじめてCFカードを装着したときは、CFカードを初期化する必要がありますので、必ず「CFカードの初期化」を実行してください。初期化しないとCFカードを使用できません。

またCFカードが初期化されていないときは、「オプションCFカードに現在の設定をコピーします」項目は表示されません。

システム設定

[CFカードの取り扱いについて]

オプション CF カードは、本装置前面パネルの CF カードスロットに挿入してください。

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

CF カードを取り外すときは、CF カードスロット横にある RELEASE ボタンを数秒押し続けてください。その後 CF ランプが消灯しましたら、CF カードを安全に取り外せます。

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

◆ ARP filter 設定

ARP filter 設定をおこないます。

実行方法

「ARP filter 設定」をクリックして画面を開きます。

ARP filter	☒ 無効	☐ 有効
------------	-------------------------------------	--------------------------

「有効」を選択して保存すると、ARP filter が動作します。

ARP filter を有効にすることで、同一 IP アドレスの ARP を複数のインタフェースで受信したときに、当該 MAC アドレス以外のインタフェースから ARP 応答を出さないようにできます。

第 34 章

情報表示

本体情報の表示

本体の機器情報を表示します。
以下の項目を表示します。

- **ファームウェアバージョン情報**
現在のファームウェアバージョンを確認できます。
- **インタフェース情報**
各インタフェースの IP アドレスや MAC アドレスなどです。
PPP/PPPoE や IPsec 論理インタフェースもここに表示されます。
- **リンク情報**
本装置の各 Ethernet ポートのリンク状態、リンク速度が表示されます。
- **ルーティング情報**
直接接続、スタティックルート、ダイナミックルートに関するルーティング情報です。
- **Default Gateway 情報**
デフォルトルート情報です。
- **ARP テーブル情報**
XR が保持している ARP テーブルです。
- **DHCP クライアント取得情報**
DHCP クライアントとして設定しているインタフェースがサーバから取得した IP アドレス等の情報を表示します。

実行方法

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

ファームウェアバージョン

Century Systems XR-440 Series ver 1.7.6

更新

インタフェース情報

eth0

Link encap:Ethernet HWaddr 00:80:6D:6E:0A:C0
inet addr:192.168.0.254 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:881 errors:0 dropped:0 overruns:0 frame:0
TX packets:554 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:117245 (114.4 Kb) TX bytes:423039 (413.1 Kb)
Interrupt:28

eth1

Link encap:Ethernet HWaddr 00:80:6D:6E:0A:C1
inet addr:192.168.1.254 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:3 errors:3 dropped:0 overruns:0 carrier:6
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:180 (180.0 b)
Interrupt:29

eth2

Link encap:Ethernet HWaddr 00:80:6D:6E:0A:C2
inet addr:192.168.2.254 Bcast:192.168.2.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:0 errors:0 dropped:0 overruns:0 frame:0
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:0 (0.0 b) TX bytes:0 (0.0 b)
Interrupt:1

リンク情報

eth1

Link:down

eth2

Port1 Link:down

Port2 Link:down

Port3 Link:down

Port4 Link:down

ルーティング情報

Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth2
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1
192.168.0.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

Default Gateway 情報

ARP テーブル情報

IP address	HW type	Flags	HW address	Mask	Device
192.168.0.100	0x1	0x2	00:90:99:17:00:1E	*	eth0

更新

anchor for reload-button

画面中の「更新」をクリックすると、表示内容が更新されます。

第 35 章

詳細情報表示

各種情報の表示

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。

ルーティング	ルーティング詳細情報
	ルーティングキャッシュ情報
	デフォルトゲートウェイ情報
PPPoEブリッジ	PPPoEブリッジ情報
OSPF	データベース情報
	ネイバー情報
	ルート情報
	統計情報
	インターフェース情報
RIP	RIP情報
IPsecサーバ	IPsec情報
DHCPサーバ	DHCPアドレスリース情報
NTPサービス	NTP情報
VRRPサービス	VRRP情報
PPPoE to L2TP	L2TP情報
QoS	Queueing設定情報
	CLASS設定情報
	CLASS分けフィルタ設定情報
	Packet分類設定情報
	Interfaceの指定
全ての詳細情報を表示する	

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。

左列の機能名をクリックすると、新しいウィンドウが開いて、その機能に関する情報がまとめて表示されます。右列の小項目名をクリックした場合は、その小項目のみの情報が表示されます。

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

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

各種情報の表示

表示される内容は以下のとおりです。

- **ルーティング情報**

XR のルーティングテーブル、ルーティングテーブルの内部情報、ルートキャッシュの情報、デフォルトゲートウェイ情報が表示できます。

このうち、ルーティングテーブルの内部情報とルートキャッシュの情報はここでのみ表示できます。

- **PPPoE ブリッジ情報**

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

PPPoE Bridge: [On/Off]
Bridging Port: [ethx], [ethx]
Bridging Packet Count: 0 - 2³²-1

例)

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

- **OSPF 情報**
- **RIP 情報**
- **IPsec 情報**
- **DHCP アドレスリース情報**
- **NTP 情報**
- **VRRP 情報**
- **QoS 情報**

第 36 章

運用管理設定

INIT ボタンの操作

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

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

◆本装置の設定を初期化する

- 1 本装置が停止状態になっていることを確認します。
- 2 本体背面にある「INIT」ボタンを押しながら、電源スイッチをオンにします。INIT ボタンは押したままにしておきます。
- 3 本体前面の STATUS1 ランプが点灯、他の STATUS ランプが消灯するまで INIT ボタンを押し続けます。
- 4 3. の状態になったら INIT ボタンを放します。その後、本装置が工場出荷設定で起動します。

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

◆CF カードの設定で起動する

- 1 本装置にオプション CF カードが挿入されていることを確認します。
- 2 本体背面にある「INIT」ボタンを押しながら、パワースwitchをオンにします。INIT ボタンは押したままにしておきます。
- 3 本体前面の「STATUS」ランプの点滅が止まるまで INIT ボタンを押し続けます。
- 4 点滅が止まったら INIT ボタンを放します。その後、本装置が CF カードに保存されている設定内容で起動します。

補足：バージョンアップ後の設定内容について

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

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

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

携帯電話による制御

XR-440 にグローバルアドレスが割り当てられていて、インターネットに接続している状態ならば、i モードおよび EZ ウェブに対応した携帯電話から以下のような操作が可能です。

- ・ルータとしてのサービスを停止する
- ・ルータとしてのサービスを再開する
- ・本装置を再起動する

この機能を利用する際は、パケットフィルタリング設定によって WAN 側からの設定変更を許す設定になっていることが必要になります。WAN 側から本装置の設定変更を許すフィルタ設定については「パケットフィルタ機能」項目をご覧ください。

実際に操作画面にアクセスするためには、i モード端末から次の URL をしてしてください。

<i モード端末からアクセスする場合>

http:// 装置の IP アドレス:880/i/

<EZ ウェブ端末からアクセスする場合>

**http:// 装置の IP アドレス:880/ez/
index.html**

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ください。

「i フィルタ起動」を実行すると、ルーターとしてのサービスが停止します。

この状態では、WAN から LAN へのアクセスはできません。WAN 側からは XR-440 自身の設定画面もしくは i モード画面にしかアクセスできなくなります。

また LAN 側からインターネット側へアクセスしても、アクセス先からの応答を受け取ることができなくなります。

「i フィルタ停止」を実行すると、以前の設定状態に戻り、ルーター機能が再開されます。

i モードからアクセスするには、パケットフィルタの「入力フィルタ設定」で、インターネット側から XR-440 の設定画面にログインできるように設定しておく必要があります。

IP アドレス自動割り当ての契約でインターネットに接続されている場合、XR-440 に割り当てられたグローバルアドレスが変わってしまう場合があります。もしアドレスが変わってしまったときは i モードからの制御ができなくなってしまうことが考えられますので(アドレスが分からなくなるため)、運用には十分ご注意下さい。

⇒ 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。

第 36 章 運用管理設定

携帯電話による操作方法

1 携帯電話端末から XR-440 の WAN 側に割り当てられたグローバルアドレスを指定してアクセスします。



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。

2 ユーザー名とパスワードを入力して「OK」を選択します。



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

インタフェース名について

インタフェース名について

本装置は、以下の設定においてインタフェース名を直接指定する必要があります。

- OSPF 機能
- スタティックルート設定
- ソースルート設定
- NAT 機能
- パケットフィルタリング機能
- 仮想インタフェース機能
- QoS 機能
- ネットワークテスト

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

eth0	Ether0ポート
eth1	Ether1ポート
eth2	Ether2ポート
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ppp6	アクセスサーバ(シリアル接続)
ppp7	アクセスサーバ(BRI接続)
ppp8	アクセスサーバ(BRI接続)
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
ipsec7	eth2上のipsec
gre<n>	gre(<n>は設定番号)

表左：インタフェース名
表右：実際の接続デバイス

付録 B

工場出荷設定一覧

IPアドレス設定	IPアドレス/サブネットマスク値
Ether0ポート	192.168.0.254/255.255.255.0
Ether1ポート	192.168.1.254/255.255.255.0
Ether2ポート	192.168.2.254/255.255.255.0

DHCPサーバ機能	有効
DHCPクライアント機能	無効
デフォルトゲートウェイ	設定無し
IPマスカレード機能	Ether0ポート以外で有効
NAT機能	設定無し
パケットフィルタ機能	NetBIOSの漏洩を防止するフィルタ設定 (入力・転送フィルタ設定) 外部からのUPnPパケットを遮断する設定 (入力・転送フィルタ設定)
DNSリレー機能	有効
DNSキャッシュ機能	無効
スタティックルーティング設定	設定無し
ダイナミックルーティング設定	無効
ソースルーティング設定	設定無し
IPsec機能	設定無し
GRE機能	設定無し
UPnP機能	有効
ログ機能	無効
攻撃検出機能	無効
QoS機能	設定無し
仮想インタフェース機能	無効
アクセスサーバ機能	無効
SNMPエージェント機能	無効
NTP機能	無効
スケジュール機能	設定無し

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

サポートについて

◆本製品に関するサポートは、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、下記へご連絡下さい。

・サポートデスク

電話 0422-37-8926

受付時間 10:00～16:30（土日祝祭日、及び弊社の定める休日を除きます）

・FAX 0422-55-3373

・e-mail support@centurysys.co.jp

・ホームページ <http://www.centurysys.co.jp/>

◆故障と思われる場合は

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

◆ご連絡をいただく前に

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

・ファームウェアのバージョンとMACアドレス

（バージョンの確認方法は第34章「情報表示」をご覧ください）

・ネットワークの構成(図)

どのようなネットワークで運用されているかを、差し支えない範囲でお知らせ下さい。

・不具合の内容または、不具合の再現手順

何をしたときにどのような問題が発生するのか、できるだけ具体的にお知らせ下さい。

・エラーメッセージ

エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。

・XR-440の設定内容、およびコンピュータのIP設定

・「設定のバックアップファイル」を電子メール等でお送り下さい。

◆サポート情報

弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。また製品のFAQも掲載しておりますので、是非ご覧ください。

XR-440 製品サポートページ

<http://www.centurysys.co.jp/support/xr440c.html>

◆製品の保証について

本製品の保証期間は、お買い上げ日より1年間です。保証期間をすぎたもの、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承下さい。保証規定については、同梱の保証書をご覧ください。

XR-440/C ユーザーズガイド 1.7.7 対応版

2007 年 7 月版

発行 センチュリー・システムズ株式会社

Copyright (c) 2002-2007 Century Systems Co., Ltd. All rights reserved.
