

BROADBAND GATE

Internet VPN 対応 BroadbandGate

FutureNet XR-640/CD

ユーザーズガイド

Ver 1.6.7 対応版

release 2



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
改版履歴	11
第1章 XR-640の概要	12
. XR-640の特長	13
. 各部の名称と機能	16
. 動作環境	19
第2章 XR-640の設置	20
XR-640の設置	21
第3章 コンピュータのネットワーク設定	23
. Windows 95/98/Meのネットワーク設定	24
. Windows 2000のネットワーク設定	25
. Windows XPのネットワーク設定	26
. Windows Vistaのネットワーク設定	27
. Macintoshのネットワーク設定	28
. IPアドレスの確認と再取得	29
第4章 設定画面へのログイン	30
設定画面へのログイン方法	31
第5章 インターフェース設定	32
. Ethernetポートの設定	33
. Ethernetポートの設定について	35
. VLANタギングの設定	36
. その他の設定	37
第6章 PPPoE設定	40
. PPPoEの接続先設定	41
. PPPoEの接続設定と回線の接続/切断	43
. 副回線の設定	45
. バックアップ回線の設定	46
. PPPoE特殊オプション設定	48
第7章 RS-232/BRIポートを使った接続(リモートアクセス機能)	50
. XR-640とアナログモデム/TAの接続	51
. BRIポートを使ったXR-640とTA/DSUの接続	52
. リモートアクセス回線の接続先設定	53
. リモートアクセス回線の接続と切断	55
. 副回線接続とバックアップ回線接続	57
. 回線への自動発信の防止について	58
第8章 複数アカウント同時接続設定	59
複数アカウント同時接続の設定	60
第9章 各種サービスの設定	64
各種サービス設定	65
第10章 DNSリレー/キャッシュ機能	66
DNS機能の設定	67
第11章 DHCPサーバ/リレー機能	68
. DHCP関連機能について	69
. DHCPサーバ機能の設定	70
. IPアドレス固定割り付け設定	72

第 12 章 IPsec 機能	73
. XR-640 の IPsec 機能について	74
. IPsec 設定の流れ	75
. IPsec 設定	76
. IPSec Keep-Alive 設定	83
. 「X.509 デジタル証明書」を用いた電子認証	86
. IPsec 通信時のパケットフィルタ設定	88
. IPsec がつながらないとき	89
第 13 章 UPnP 機能	92
. UPnP 機能の設定	93
. UPnP とパケットフィルタ設定	95
第 14 章 ダイナミックルーティング	96
. ダイナミックルーティング機能	97
. RIP の設定	98
. OSPF の設定	100
. DVMRP の設定	107
第 15 章 PPPoE to L2TP	109
. PPPoE to L2TP 機能について	110
第 16 章 SYSLOG 機能	112
. syslog 機能の設定	113
第 17 章 攻撃検出機能	116
. 攻撃検出機能の設定	117
第 18 章 SNMP エージェント機能	118
. SNMP エージェント機能の設定	119
第 19 章 NTP サービス	121
. NTP サービスの設定方法	122
第 20 章 VRRP サービス	124
. VRRP の設定方法	125
. VRRP の設定例	126
第 21 章 アクセスサーバ機能	127
. アクセスサーバ機能について	128
. XR-640 とアナログモデム /TA の接続	129
. BRI ポートを使った XR-640 と TA/DSU の接続	130
. アクセスサーバ機能の設定	131
第 22 章 スタティックルート	134
. スタティックルート設定	135
第 23 章 ソースルーティング機能	137
. ソースルーティング設定	138
第 24 章 NAT 機能	140
. XR-640 の NAT 機能について	141
. バーチャルサーバ設定	142
. 送信元 NAT 設定	143
. バーチャルサーバの設定例	144
. 送信元 NAT の設定例	147
. 補足：ポート番号について	148
第 25 章 パケットフィルタリング機能	149
. 機能の概要	150
. XR-640 のフィルタリング機能について	151
. パケットフィルタリングの設定	152

. パケットフィルタリングの設定例	154
. 外部から設定画面にアクセスさせる設定	160
補足：NAT とフィルタの処理順序について	161
補足：ポート番号について	162
補足：フィルタのログ出力内容について	163
第 26 章 スケジュール設定	164
スケジュール機能の設定方法	165
第 27 章 ネットワークイベント機能	167
. 機能の概要	168
. 各トリガテーブルの設定	170
. 実行イベントテーブルの設定	174
. 実行イベントのオプション設定	176
. ステータスの表示	178
第 28 章 仮想インターフェース機能	179
仮想インターフェース機能の設定	180
第 29 章 GRE 設定	181
GRE の設定	182
第 30 章 QoS 機能	184
. QoS について	185
. QoS 機能の各設定画面について	189
. 各キューイング方式の設定手順について	190
. 各設定画面での設定方法について	191
. ステータスの表示	198
. 設定の編集・削除方法	199
. ステータス情報の表示例	200
. クラスの階層構造について	204
. TOS について	205
. DSCP について	207
第 31 章 ゲートウェイ認証機能	208
ゲートウェイ認証機能の設定	209
第 32 章 ネットワークテスト	215
ネットワークテスト	216
第 33 章 システム設定	220
システム設定	221
時計の設定	221
ログの表示	222
ログの削除	222
パスワードの設定	223
ファームウェアのアップデート	224
設定の保存と復帰	225
設定のリセット	226
再起動	226
セッションライフタイムの設定	227
設定画面の設定	228
ISDN 設定	228
オプション CF カード	229
ARP filter 設定	230
第 34 章 情報表示	231
本体情報の表示	232

第 35 章 詳細情報表示	233
各種情報の表示	234
第 36 章 運用管理設定	235
. INIT ボタンの操作	236
. 携帯電話による制御	237
付録 A インタフェース名一覧	239
付録 B 工場出荷設定一覧	242
付録 C サポートについて	244

はじめに

ご注意

- 1 本装置の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸したために生じた損害などの純粋経済損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。
- 2 通信情報が漏洩した事による経済的、精神的損害につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。
- 3 本書の内容の一部または全部を無断で転載、複写することを禁じます。
- 4 本書およびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。
- 5 本書の内容については万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきの点がありましたらご連絡ください。

商標の表示

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

「FutureNet」はセンチュリー・システムズ株式会社の商標です。

下記製品名等は米国Microsoft Corporationの登録商標です。

Microsoft、Windows、Windows 95、Windows 98、Windows NT3.51、Windows NT4.0
Windows 2000、Windows Me、Windows XP、Windows Vista

Macintosh、Mac OS Xは、アップル社の登録商標です。

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

ご使用にあたって

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

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

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



危険

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



警告

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



注意

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

次の絵表示の区分は、お守りいただく内容を説明しています。



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



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

危険



必ず本体に付属している電源ケーブルをご使用ください。



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



ストーブのそばなど高温の場所で使用したり、放置しないでください。











火の中に投入したり、加熱したりしないでください。



製品の隙間から針金などの異物を挿入しないでください。










ご使用にあたって

警告

-  万一、異物(金属片・水・液体)が製品の内部に入った場合は、まず電源を外し、お買い上げの販売店にご連絡ください。そのまま使用すると火災の原因となります。
-  万一、発熱していたり、煙が出ている、変な臭いがするなどの異常状態のまま使用すると、火災の原因となります。すぐに電源を外し、お買い上げの販売店にご連絡ください。
-  本体を分解、改造しないでください。けがや感電などの事故の原因となります。
-  本体または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ください。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、ご使用をお控えください。落雷が火災・感電・故障の原因となることがあります。
-  電源ケーブルのプラグを本体に差し込んだ後に電源ケーブルケーブルを左右および上下に引っ張ったり、ねじったり、曲げたりしないでください。緩みがある状態にしてください。
-  本製品に乗らないでください。本体が壊れて、けがの原因となることがあります。
-  高出力のアンテナや高圧線などが近くにある環境下では、正常な通信ができない場合があります。

パッケージの内容物の確認

本製品のパッケージには以下のものが同梱されております。本製品をお使いいただく前に、内容物がすべて揃っているかご確認ください。

万が一不足がありましたら、お買い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-640/CD 同梱物一覧>

XR-640/CD 本体	1 台
はじめにお読みください	1 部
安全にお使いいただくために	1 部
UTPケーブル(ストレート、1m)	1 本
電源ケーブル	1 本
海外使用禁止シート	1 部
保証書	1 部

改版履歴

改版履歴

release番号	変更内容
1	初版
2	<p>第8章 複数アカウント同時接続設定 複数アカウント同時接続の設定 「マルチPPPoEセッション」・・・マルチ回線にて設定不可能な設定を修正</p> <p>第11章 DHCPサーバ/リレー機能 ・ DHCP関連機能について DHCPサーバ機能・・・「VLAN対応」の記述を削除</p> <p>・ IPアドレス固定割り付け設定 IPアドレス固定割り付け時のDHCPサーバ設定について・・・補足説明を削除</p> <p>第19章 NTPサービス NTPサービスの設定方法 時刻同期タイムアウト時間・・・注釈を追加</p> <p>第21章 アクセスサーバ機能 ・ アクセスサーバ機能の設定 アカウント毎に別IPを割り当てる場合・・・機能制限を追加</p>

第1章

XR-640 の概要

XR-640の特長

高速ネットワーク環境に余裕で対応

XR-640 /CD(以下、XR-640)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行うCATVインターネット接続サービスでも利用できます。また、LAN側ポートではDHCPサーバ機能を搭載しており、LAN側のPCに自動的にIPアドレス等のTCP/IP設定を行なえます。

NAT/IPマスカレード機能

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

ステートフルパケットインスペクション機能

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

静的パケットフィルタリング機能

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

ISDN用BRIポートを搭載

XR-640は「ISDN U点ポート」と「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-640の「副回線接続」を使うと、ISDN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。

第1章 XR-640の概要

XR-640の特長

ローカルルータ / ブリッジ機能

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

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。

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行うことができます。

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行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 / 優先制御を行うことができます。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行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-640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-640を遠隔管理することも可能です。

・ XR-640 の特長

ログ機能

XR-640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

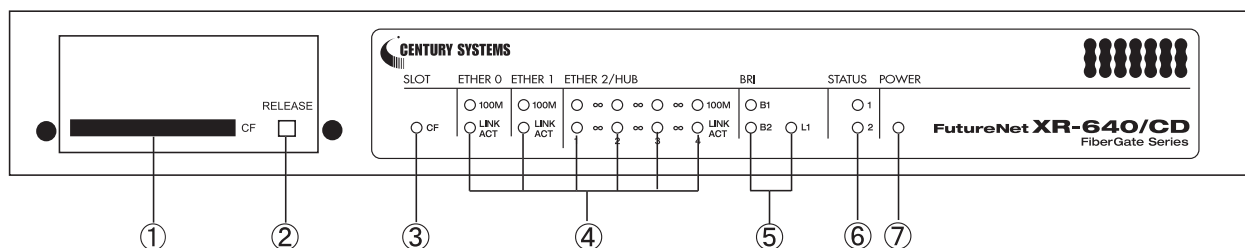
本体の設定内容を一括してファイルにバックアップすることが可能です。また設定の復元も、ブラウザ上から簡単にできます。

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。

各部の名称と機能

製品前面



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。

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、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。

SLOT CF LED

CFカードが挿入され動作しているときに、CF(緑)が点灯します。

CFカードをスロットに挿入しカードが使用可能状態になるまでの間は、CF(緑)は点滅します。

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

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

「LINK/ACT」(緑)ランプが点灯します。

「100M」(緑)ランプは、10Base-Tで接続した場合に消灯、100Base-TXで接続した場合点に点灯します。データ通信時は「LINK/ACT」ランプが消灯します。

BRI LED

「L1」(緑)ランプは、本装置のBRI U点・S/T点ポートがリンクアップしているときに点灯します。

「B1」「B2」(緑)ランプは、本装置のBRIポートを使って回線接続しているときに点灯します。回線接続していないときは消灯しています。

STATUS1(赤)/STATUS2(緑) LED

本装置の全てのサービスが動作開始状態になっているときに、STATUS1(赤)は消灯します。

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

ファームウェアのアップデート作業中は、STATUS1(赤)が点滅します。

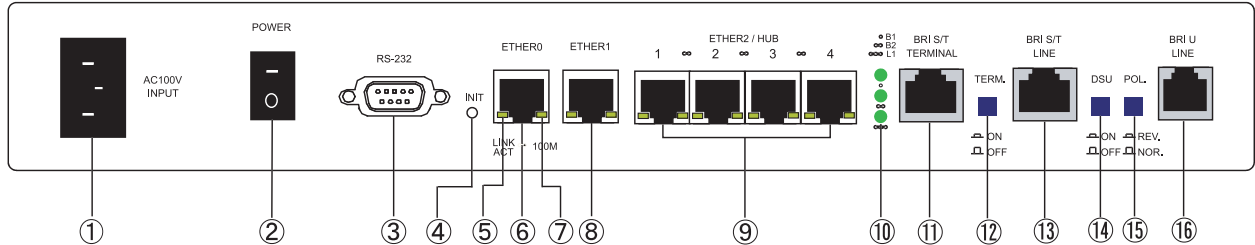
ファームウェアのアップデートに失敗した場合など、本装置が正常に起動できない状態になったときは、STATUS1(赤)とSTATUS2(緑)のどちらも点滅します。

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。

各部の名称と機能

製品背面



電源ケーブル差込口

製品付属の電源ケーブルを接続するコネクタです。ケーブルは必ず付属のものをご使用ください。

電源スイッチ

電源をオン/オフするためのスイッチです。

RS-232ポート

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

INITボタン

本装置を工場出荷時の設定に戻して起動するとき、およびオプションCFカードの設定から起動するときに使用します。

LINK/ACT(緑) LED

Ethernetポートの状態を表示します。ランプ(緑)は以下のパターンで点灯/消灯します。

LANケーブルが正常に接続 : 点灯

データ通信時 : 点滅

本装置のすべてのEthernetポートに実装されています。

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。

100M(橙) LED

Ethernetの接続速度を示します。

ランプ(橙)は以下のパターンで点灯/消灯します。

10Base-Tモード : 消灯

100Base-TXモード : 点灯

本装置のすべてのEthernetポートに実装されています。

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。

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。

BRI LED

「L1」(緑)ランプは、本装置のBRIポートと回線・機器が正常に接続されているときに点灯します。

「B1」「B2」(緑)ランプは、Bチャンネルで通信時に点灯します。MP接続時は「B1」「B2」ランプの両方が点灯します。

BRI S/T TERMINALポート

外部ISDN端末機器を接続する際にISDNケーブルを用いて、このポートと他のISDN機器のBRI S/T点ポートを接続します。

第1章 XR-640の概要

各部の名称と機能

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。BRI S/T点ポートを使って他のISDN機器のDSU機器を接続している場合は、XR-640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。

BRI S/T LINE ポート

XR-640のDSU機能を使わずに外部のDSUを使う場合に、ISDNケーブルでこのポートと外部DSUのBRI S/T点ポートを接続します。

DSU スイッチ

本装置の内蔵DSUを使用する際は「ON」(ボタンを押した状態)に、外部DSUを使用する際は「OFF」(ボタンを押していない状態)にしてください。

本装置の内蔵DSUを使用してISDN接続する場合は、本装置の「BRI S/T LINE」ポートは使用しません。

POL. スイッチ

BRI U点でISDN接続する場合の、回線の極性を切り替えます。極性がリバースの場合は「REV.」(ボタンを押した状態)に、ノーマルの場合は「NOR.」(ボタンを押していない状態)にしてください。

BRI U ポート

本装置の内蔵DSUを使用してISDN接続するときは、回線をこのポートに接続します。また回線の極性に合わせて「POL. スイッチ」を切り替えてください。

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-640の設置

第2章 XR-640 の設置

XR-640 の設置

本装置の各設定方法について説明します。

下記は設置に関する注意点です。よくご確認いただいてから設置してください。



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



電源ケーブルのプラグを本体に差し込んだ後にケーブルを左右および上下に引っ張らず、緩みがある状態にしてください。

抜き差しもケーブルを引っ張らず、コネクタを持って行ってください。

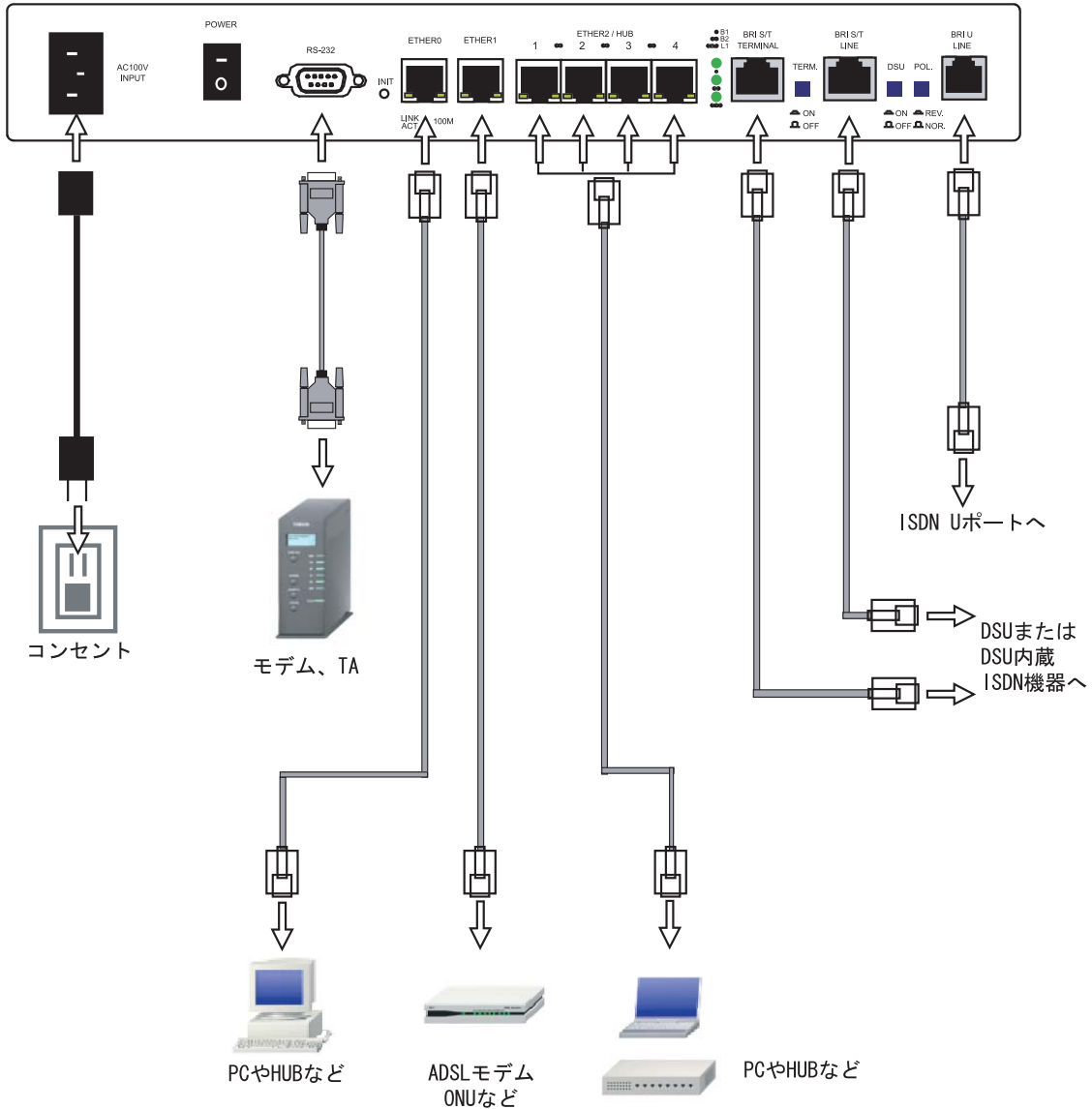
また、ケーブルを足などで引っ掛けてプラグ部に異常な力が掛からないように配線にご注意ください。



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

XR-640 の設置

XR-640 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。接続に使うケーブルの種類は、各機器の説明書等をご覧ください。

3 本装置の設定が工場出荷状態の場合、Ether0 ポートと PC を LAN ケーブルで接続してください。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 本装置と電源ケーブル、電源ケーブルとコンセントを接続してください。

6 全ての接続が完了しましたら、本装置と各機器の電源を投入してください。

第3章

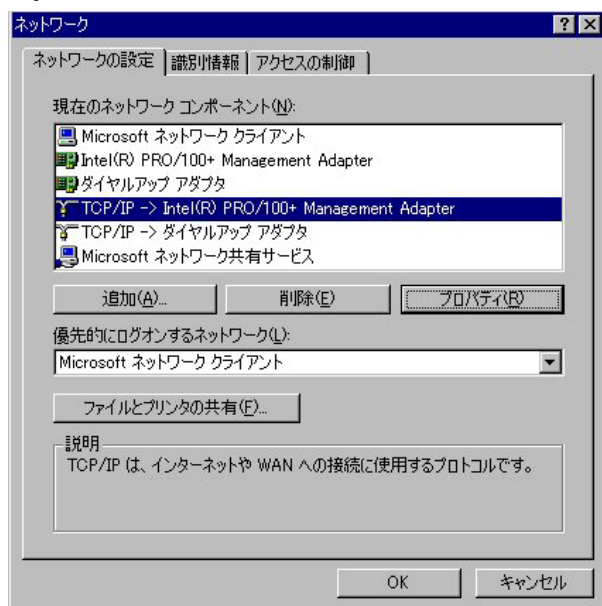
コンピュータのネットワーク設定

第3章 コンピュータのネットワーク設定

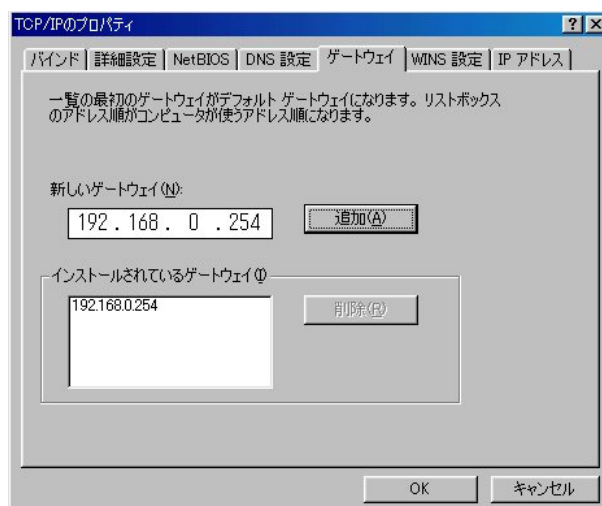
Windows 95/98/Me のネットワーク設定

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。

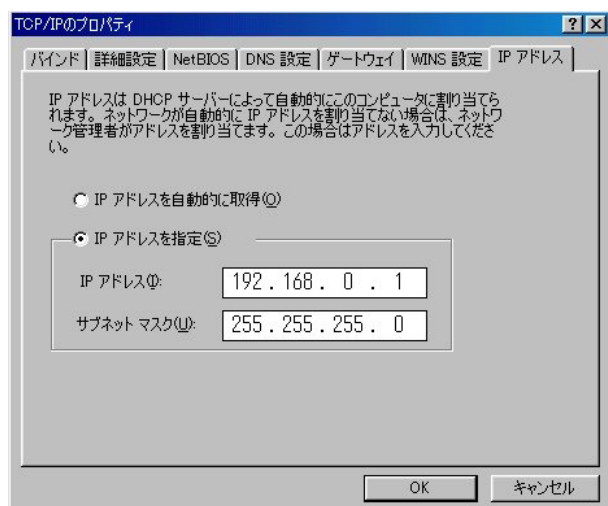
1 「コントロールパネル」 「ネットワーク」の順で開き、「ネットワークの設定」タブの「現在のネットワーク構成」から、コンピュータに装着されたLANボード(カード)のプロパティを開きます。



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。



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設定を行います。「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。



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-640の設定画面へのログインが可能になります。

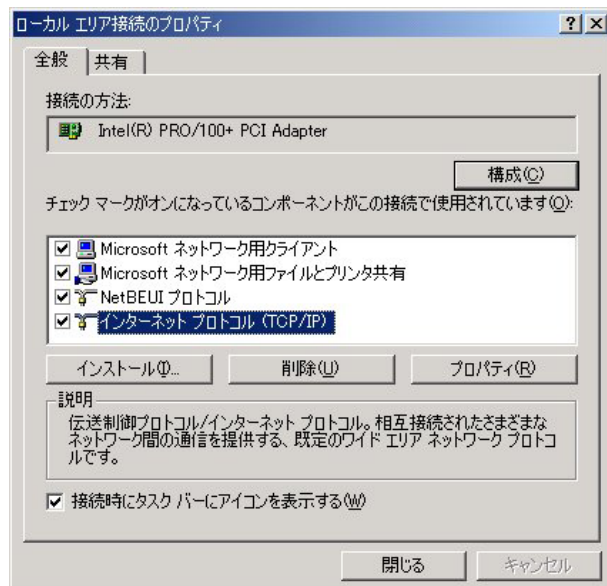
第3章 コンピュータのネットワーク設定

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。

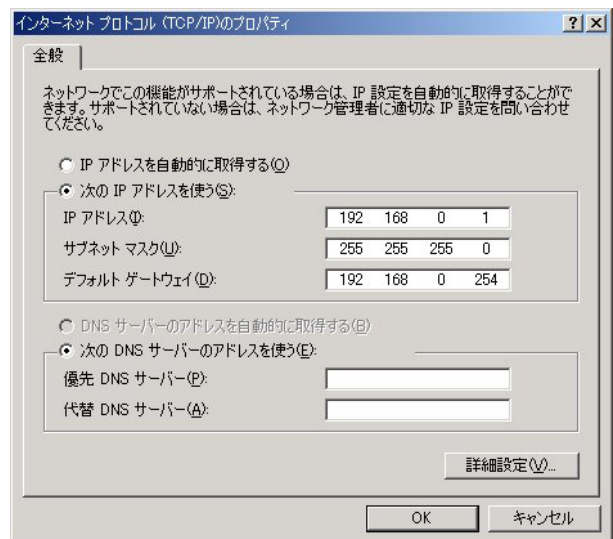


3 「全般」の画面では、「次の IP アドレスを使う」にチェックを入れて以下のように入力します。

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-640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

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。

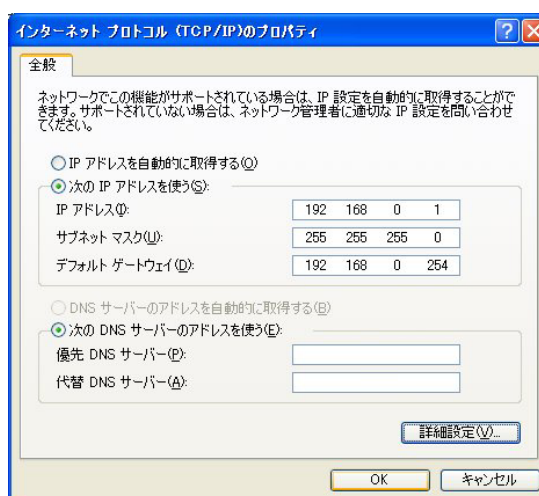


4 「インターネットプロトコル(TCP/IP)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

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」



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。



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-640へのログインの準備が整いました。

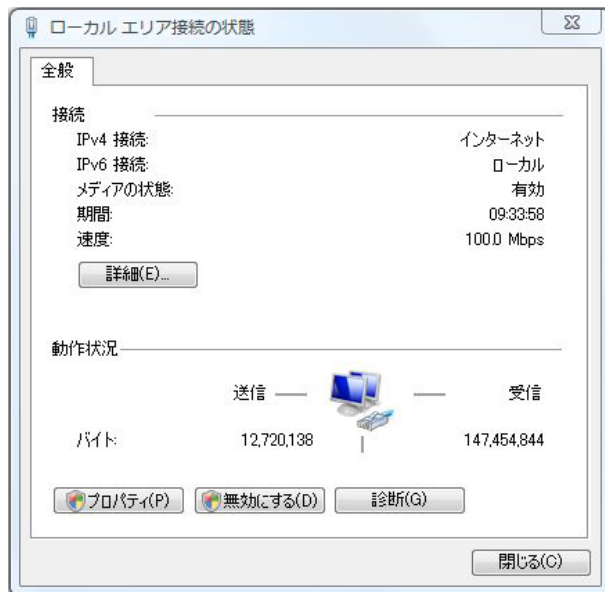
第3章 コンピュータのネットワーク設定

Windows Vistaのネットワーク設定

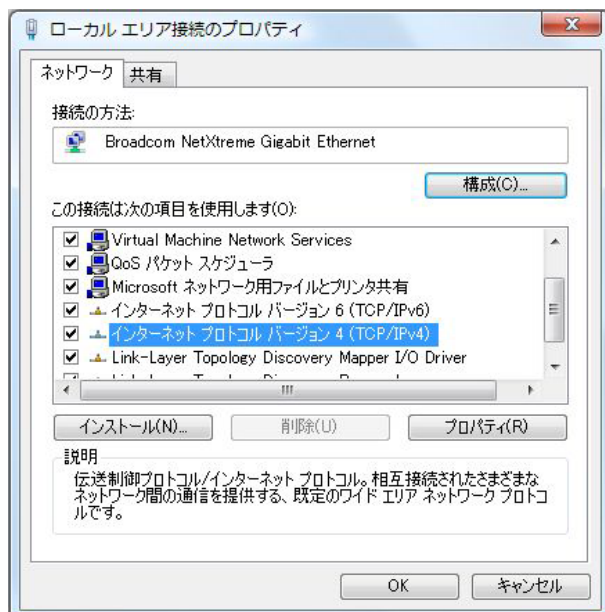
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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。

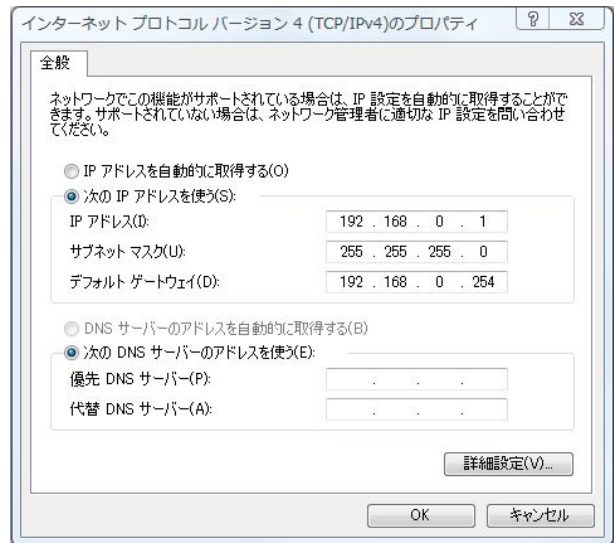


4 「インターネットプロトコルバージョン4(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

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

Macintosh のネットワーク設定

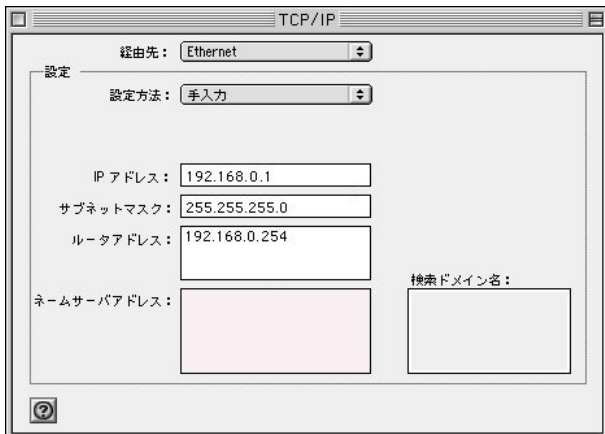
ここではMacintoshのネットワーク設定について説明します。

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-640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。

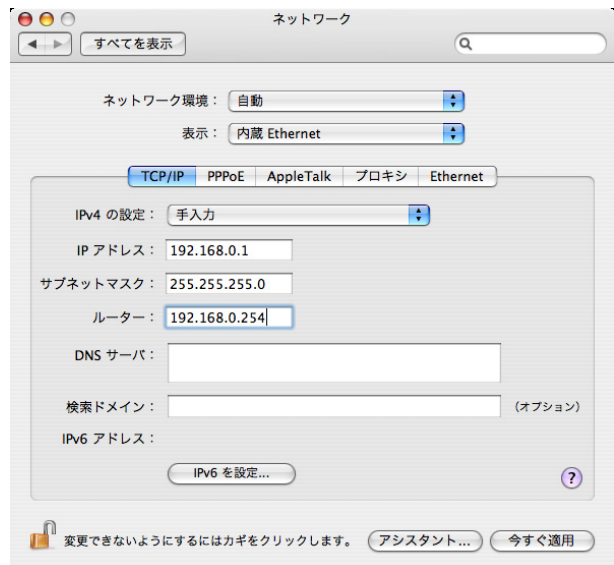
1 「システム環境設定」から「ネットワーク」を開きます。

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

・ 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行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-640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。

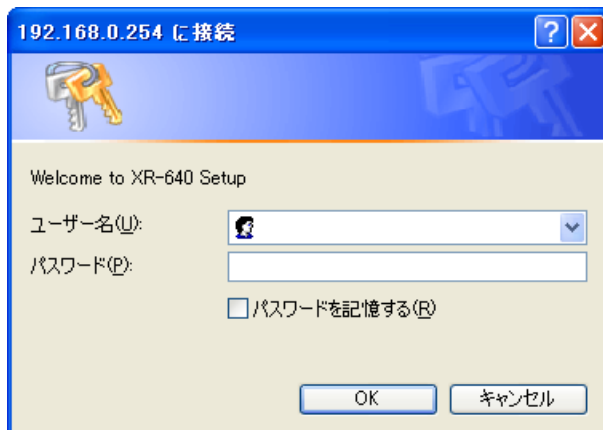
http://192.168.0.254:880/

「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。

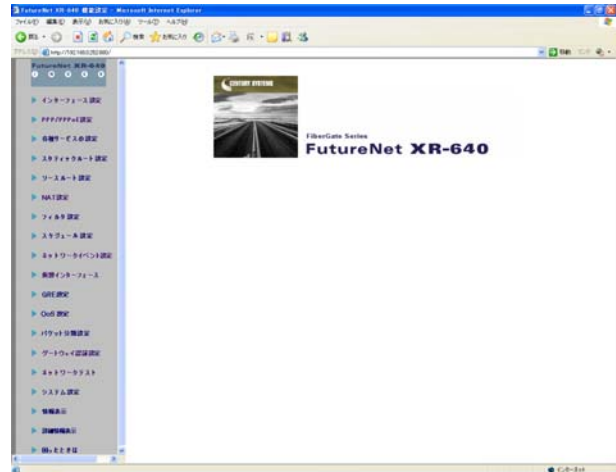
4 ダイアログ画面にパスワードを入力します。
工場出荷設定のユーザー名とパスワードはともに「admin」です。ユーザー名・パスワードを変更している場合は、それに合わせてユーザー名・パスワードを入力します。



3 次のような認証ダイアログが表示されます。



5 ブラウザ設定画面が表示されます。



第5章

インターフェース設定


第5章 インターフェイス設定

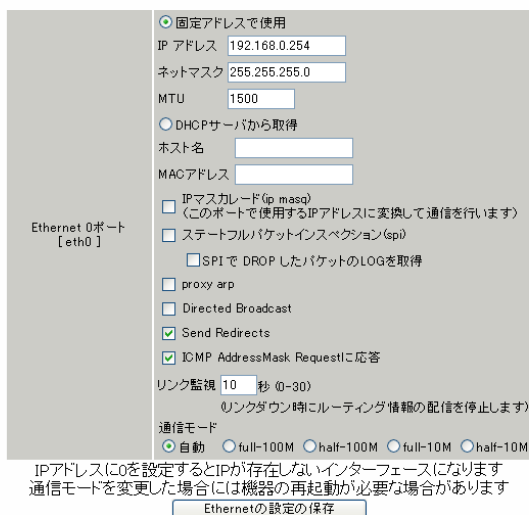
Ethernet ポートの設定

各 Ethernet ポートの設定

各インターフェイスについて、それぞれ必要な情報を入力します。

Web 設定画面「インターフェイス設定」
「Ethernet0(または1、2)の設定」をクリックして設定します。


[eth0] の設定を変更した場合ブラウザからアクセス出来なくなる可能性があります



Ethernet 0 ポート
[eth0]

固定アドレスで使用
IP アドレス 192.168.0.254
ネットマスク 255.255.255.0
MTU 1500

DHCPサーバから取得
ホスト名
MACアドレス

IPマスカレード (ip masq)
(このポートで使用するIPアドレスに変換して通信を行います)

ステートフルパケットインスペクション (spi)
 SPI で DROP したパケットの LOG を取得

proxy arp
 Directed Broadcast
 Send Redirects
 ICMP AddressMask Request に応答

リンク監視 10 秒 (0-30)
(リンクダウン時にルーティング情報の配信を停止します)

通信モード
 自動 full-100M half-100M full-10M half-10M

IPアドレスに0を設定するとIPが存在しないインターフェイスになります
通信モードを変更した場合には機器の再起動が必要な場合があります

Ethernetの設定の保存

(画面は「Ethernet0 の設定」の表示例)

[固定アドレスで使用]

IP アドレス
ネットマスク

IPアドレスが固定割り当ての場合にチェックして、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、そのインターフェイスは IP アドレス等が設定されず、ルーティング・テーブルに載らなくなります。OSPF などで使用していないインターフェイスの情報を配信したくないときなどに "0" を設定してください。

MTU

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

[DHCP から取得]

ホスト名
MAC アドレス

IP アドレスが DHCP で割り当ての場合にチェックして、必要であればホストネームと MAC アドレスを設定します。

「Ethernet2 の設定」にはありません。

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

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

SPI で DROP したパケットの LOG を取得
チェックを入れると、SPI が適用され破棄 (DROP) したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、「第25章 補足：フィルタのログ出力内容について」をご覧ください。

proxy arp
Proxy ARP を使う場合にチェックを入れます。

Direct Broadcast
チェックを入れると、そのインターフェイスにおいて Direct Broadcast の転送を許可します。

Directed Broadcast

IP アドレスのホスト部がすべて 1 のアドレスのことです。

ex. 192.168.0.0/24 の Directed Broadcast は 192.168.0.255 です。

Send Redirects
チェックを入れると、そのインターフェイスにおいて 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 インターフェース設定

. Ethernet ポートの設定

ICMP AddressMask Request に応答

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

チェックをしない場合は、Request に対して応答しません。

リンク監視

チェックを入れると、Ethernet ポートのリンク状態の監視を定期的に行います。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。

通信モード

XR-640 の Ethernet ポートの通信速度・方式を選択します。工場出荷設定では「自動」(オートネゴシエーション)となっていますが、必要に応じて通信速度・方式を選択してください。

選択モードは「自動」、「full-100M」、「half-100M」、「full-10M」、「half-10M」です。

「Ethernet2 の設定」にはありません。

Ethernet2 ポートは自動設定のみとなります。

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

XR-640 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。

第5章 インターフェース設定

. Ethernet ポートの設定について

[ステートフルパケットインスペクション]

ステートフルパケットインスペクションは、パケットを監視してパケットフィルタリング項目を随時変更する機能で、動的パケットフィルタリング機能とも言えるものです。

通常はWANからのアクセスを全て遮断し、WAN方向へのパケットに対応するLAN方向へのパケット(WANからの戻りパケット)に対してのみポートを開放します。これにより、自動的にWANからの不要なアクセスを制御でき、簡単な設定でより高度な安全性を保つことができます。

ステートフルパケットインスペクション機能を有効にすると、原則としてそのインタフェースへのアクセスは一切不可能となります。ステートフルパケットインスペクション機能とバーチャルサーバ機能を同時に使う場合等は、パケットフィルタリングの設定を行って、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。

設定については、本書「**第25章 パケットフィルタリング機能**」をご参照ください。

[PPPoE 接続時の Ethernet ポート設定]

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

XR-640 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 接続を行うためです。

物理的な Ethernet ポートとは独立して動作していますので、「DHCP サーバから取得」の設定やグローバル IP アドレスの設定はしません。PPPoE に接続しているインタフェースでこれらの設定を行うと、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-640 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 通信を行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-640 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 通信を行う相手側のネットワークが 192.168.1.0/24 で、且つ、XR-640 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-640 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 インターフェース設定

VLAN タギングの設定

各 802.1Q Tagged VLAN の設定

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

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

802.1Q Tagged VLAN の設定

設定情報

No.1~

VLAN の設定の保存

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	<input checked="" type="checkbox"/>	192.168.10.254	255.255.255.0	1500	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
2	eth0.2	<input checked="" type="checkbox"/>	192.168.11.254	255.255.255.0	1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	eth0.3	<input checked="" type="checkbox"/>	192.168.12.254	255.255.255.0	1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

VLAN インターフェースの名称は [eth0.TagID] になります
64 個まで登録できます
Tag ID (ID) を登録するとその設定を削除します
設定は有効な TagID をもったものから上方につめられます

VLAN の設定の保存

(Ethernet0 ポートの表示例です)

dev.Tag ID

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

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

enable

チェックを入れることで設定を有効にします。

IP アドレス

ネットマスク

VLAN インタフェースの IP アドレスとサブネットマスクを設定します。

MTU

VLAN インタフェースの MTU 値を設定します。
初期設定値は 1500byte になります。
指定可能範囲 : 68-1500byte です。

ip masq

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

spi

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

drop log

チェックを入れると、SPI により破棄 (DROP) されたパケットの情報を syslog に出力します。
SPI が有効の場合のみ設定可能です。

proxy arp

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

icmp

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

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

設定の削除

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

設定情報の表示

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

第5章 インターフェース設定

その他の設定

ここでは、インターフェースに関するその他の設定を行います。

デフォルトゲートウェイの設定

ARP テーブル

Ether2 HUB の設定

設定方法

各種設定は、Web 設定画面「インターフェース設定」「その他の設定」にて設定します。

インターフェースの設定

[Ethernet0の設定](#) [Ethernet1の設定](#) [Ethernet2の設定](#) [その他の設定](#)

デフォルトゲートウェイの設定

設定の保存

ARPテーブル

IP address	HW type	Flags	HW address	Mask	Device
192.168.0.10	0x1	0x2	00:A0:B0:86:A0:2A	*	eth0

Ether2 HUB の設定

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ペアの組み合わせ

	Port 1	Port 2	Port 3	Port 4
VLAN A	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
VLAN B	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VLAN C	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VLAN D	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

設定の保存

デフォルトゲートウェイの設定

デフォルトゲートウェイの設定は「その他の設定」にある以下の画面で設定します。

デフォルトゲートウェイの設定

設定の保存

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

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

ARP テーブル

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



(画面は表示例です)

[現在のARP テーブル]

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

ARP エントリの固定化

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

ARP エントリの削除

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

[新しいARP エントリ]

ARP エントリを手動で登録するときは、ここから登録します。

ARP エントリの追加

入力欄にIPアドレスとMACアドレスを入力後、ボタンをクリックして登録します。

<エントリの入力例>

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

[固定のARP エントリ]

ARP エントリを固定するときは、ここから登録します。

固定ARP エントリの編集

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

ARP テーブルの確認

「その他の設定」画面中央で、現在のARP テーブルの内容を確認できます。

ARPテーブル					
IP address	HW type	Flags	HW address	Mask	Device
192.168.0.10	0x1	0x2	00:90:99:BB:30:7A	*	eth0
192.168.0.1	0x1	0x8	00:00:00:4D:B0:CB	*	eth0

(画面は表示例です)

Ether2 HUB 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 VLAN A ~ VLAN D の 4 つとなります。

「その他の設定」にある以下の画面で設定します。

Ether2 HUB の設定

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	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
VLAN B	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VLAN C	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
VLAN D	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Port VLAN 機能を使用しない

Port VLAN 機能を使用する

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

各ポートと VLAN メンバの組み合わせ

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。

第 6 章

PPPoE 設定

第6章 PPPoE 設定

1. PPPoE の接続先設定

はじめに、接続先の設定（ISP のアカウント設定）を行います。

Web 設定画面「PPP/PPPoE 設定」 「接続先設定1～5」のいずれかをクリックします。
設定は5つまで保存しておくことができます。

接続先設定

PPP/PPPoE接続設定					
接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
プロバイダ名	<input type="text"/>				
ユーザID	<input type="text"/>				
パスワード	<input type="password"/>				
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>				
LCPキープアライブ	チェック間隔 <input type="text"/> 秒 3回確認出来なくなると回線を切断します 0秒を入力するところの機能は無効になります				
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はPnP-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	<input type="text"/> 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	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 <input type="text"/> Byte (有効時にMSS値が0又は空の場合は、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。)				
BR1/PPPシリアル回線使用時に設定して下さい					
電話番号	<input type="text"/>				
ダイヤルタイムアウト	<input type="text"/> 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	<input type="radio"/> 9600 <input type="radio"/> 19200 <input type="radio"/> 38400 <input type="radio"/> 57600 <input checked="" type="radio"/> 115200 <input type="radio"/> 230400				
初期化用ATコマンド	<input type="text"/> ATQ0V1				
回線種別	<input checked="" type="radio"/> 無指定 <input type="radio"/> トーン <input type="radio"/> パルス				
BR1/PPPシリアル回線使用時に設定して下さい					
ON-DEMAND接続用切断タイマー	<input type="text"/> 180 秒				
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	<input type="text"/> 接続するネットワークを指定して下さい				
ネットマスク	<input type="text"/> 上記のネットワークのネットマスクを指定して下さい				

設定の保存

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ID
プロバイダから指定されたユーザIDを入力してください。

パスワード
プロバイダから指定された接続パスワードを入力してください。

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

<例>

abc(def)g ' h abc¥(def¥)g¥ ' h

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

LCPキープアライブ
キープアライブのためのLCP echoパケットを送出する間隔を指定します。設定した間隔でLCP echoパケットを3回送出してreplyを検出しなかったときに、XR-640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。

第6章 PPPoE 設定

PPPoE の接続先設定

Ping による接続確認

回線によっては、LCP echo を使ったキープアライブを使うことができないことがあります。その場合は、Ping を使ったキープアライブを使用します。「使用するホスト」欄には、Ping の宛先ホストを指定します。

空欄にした場合は P-t-P Gateway 宛に Ping を送出します。

通常は空欄にしておきます。

[UnNumbered-PPP 回線使用時に設定できます]

IP アドレス

固定 IP アドレスを割り当てられる接続の場合 (unnumbered 接続を含む)、ここにプロバイダから割り当てられた IP アドレスを設定します。

IP アドレスを自動的に割り当てられる形態での接続の場合は、ここには何も入力しないでください。

[PPPoE 回線使用時に設定して下さい]

MSS 設定

「有効」を選択すると、XR-640 が MSS 値を自動的に調整します。「MSS 値」は任意に設定できます。最大値は 1452Byte です。

「0」にすると最大 1414byte に自動調整します。

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

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

[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

[PPP シリアル回線使用時に設定して下さい]

シリアル DTE

初期化用 AT コマンド

回線種別

[BRI/PPP シリアル回線使用時に設定して下さい]

ON-DEMAND 接続用切断タイマー

上記項目は、PPPoE 接続の場合は設定の必要はありません。

[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

ネットマスク

<例>

ネットワーク「172.26.0.0」

ネットマスク「255.255.0.0」

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

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

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

最後に「設定の保存」ボタンをクリックして、設定完了です。

設定はすぐに反映されます。

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

第6章 PPPoE 設定

PPPoE の接続設定と回線の接続 / 切断

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

接続設定

PPP/PPPoE接続設定					
接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
回線状態	回線は接続されていません				
接続先の選択	<input checked="" type="radio"/> 接続先1	<input type="radio"/> 接続先2	<input type="radio"/> 接続先3	<input type="radio"/> 接続先4	<input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C				
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続 <input type="radio"/> スケジューラ接続				
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続				
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得				
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				
接続IP変更お知らせメール	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する				
お知らせメールの宛先	<input type="text"/>				
お知らせメールのFromアドレス	<input type="text" value="xr640"/>				
中継するメールサーバのアドレス	<input type="text"/>				

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-640 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25章 補足：フィルタのログ出力内容について」をご覧ください。

デフォルトルートの設定

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

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

通常は「有効」設定にしておきます。

ICMP AddressMask Request

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

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

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

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。

以下の箇所を設定します。

接続IP変更 お知らせメール	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する
お知らせメールの宛先	<input type="text"/>
お知らせメールの Fromアドレス	xx640 <input type="text"/>
中継するメールサーバの アドレス	<input type="text"/>

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。

<入力例> @mail.centurysys.co.jp

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ください。

副回線の設定

副回線設定

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。

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	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> 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 または 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

バックアップ回線の設定

バックアップ回線設定

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

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

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

回線状態の確認は、ping または OSPF を用います。OSPF については、「第14章 ダイナミックルーティング」をご覧ください。

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	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input checked="" type="radio"/> RS232C
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IP マスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROP したパケットの LOG を取得
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 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	<input type="radio"/> PING <input checked="" type="radio"/> OSPF <input type="radio"/> IPSEC+PING
Ping 使用時の宛先アドレス	<input type="text"/>
Ping 使用時の送信元アドレス	<input type="text"/>
Ping fail 時のリトライ回数	0
Ping 使用時の device	<input type="radio"/> 主回線#1 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input checked="" type="radio"/> その他 <input type="text"/>
IPSEC+Ping 使用時の IPSEC ポリシーの NO	<input type="text"/>
復旧時のバックアップ回線の強制切断	<input checked="" type="radio"/> する <input type="radio"/> しない
接続お知らせメール	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する
お知らせメールの宛先	<input type="text"/>
お知らせメールの From アドレス	sr640 <input type="text"/>
中継するメールサーバのアドレス	<input type="text"/>

バックアップ回線 の使用

バックアップ回線を利用する場合は「有効」を選択します。

接続先の選択

バックアップ回線接続で利用する接続先設定を選択します。

接続ポート

バックアップ回線を接続しているインタフェースを選択します。

RS232C/BRI 接続タイプ

RS232C または BRI インタフェースを使ってバックアップ回線接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

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

IP マスカレード

バックアップ回線接続時の IP マスカレードの動作を選択します。

ステートフルパケットインスペクション

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

ICMP AddressMask Request

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

主回線接続確認のインターバル

主回線接続の確認のためにパケットを送出する間隔を設定します。30-999(秒)の間で設定できます。

第6章 PPPoE 設定

バックアップ回線の設定

主回線の回線断の確認方法

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

Ping 使用時の宛先アドレス

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

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

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12章 IPsec 機能」や IPsec 設定ガイドをご覧ください。

復旧時のバックアップ回線の強制切断

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

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。

接続お知らせメール機能

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

以下の箇所を設定します。

接続IP変更 お知らせメール	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する
お知らせメールの宛先	<input type="text"/>
お知らせメールの Fromアドレス	xx640
中継するメールサーバの アドレス	<input type="text"/>

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。

<入力例> @mail.centurysys.co.jp

・ 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。

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

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

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

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

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。

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 を強制送出生
- 非接続 Session の IPv4 Packet 受信時に PADT を強制送出生
- 非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出生

回線接続時に前回の PPPoE セッションの PADT を強制送出生する。

非接続 Session の IPv4 Packet 受信時に PADT を強制送出生する。

非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出生する。

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 を送出生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。

、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 を送出生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う事象を回避するためにも、PPPoE 特殊オプション機能を有効にした上で PPPoE 接続をしていただくことを推奨します。

(次ページへ続きます)

第6章 PPPoE 設定

・ PPPoE 特殊オプション設定

ただし、次の場合には、PPPoE 特殊オプションを無効にしてください。

PPPoE to L2TP 機能を使用している場合

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

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

PPPoE特殊オプション (全回線共通)	<input checked="" type="checkbox"/> 回線接続時に前回のPPPoEセッションのPADTを強制送出
	<input type="checkbox"/> 非接続SessionのIPv4Packet受信時にPADTを強制送出
	<input type="checkbox"/> 非接続SessionのLCP-EchoRequest受信時にPADTを強制送出

PPPoE to L2TP 機能を使用しているときに設定を有効にした場合、XR-640 配下のクライアントが正常に PPPoE 接続できなくなります。

第7章

RS-232/BRI ポートを使った接続
(リモートアクセス機能)

第7章 RS-232/BRIポートを使った接続(リモートアクセス機能)

XR-640 とアナログモデム /TA の接続

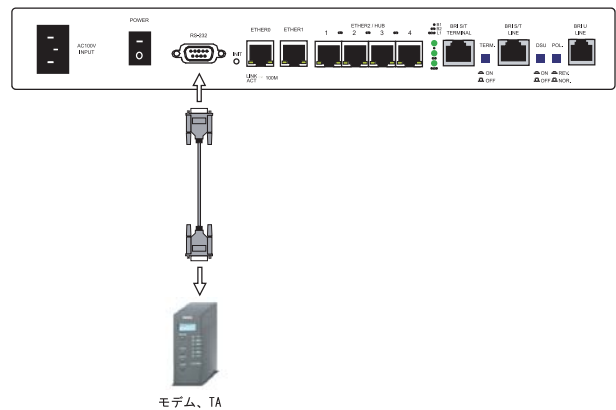
XR-640 は、RS-232ポート、ISDN U点ポート、ISDN S/T点ポート(BRIポート)を搭載しています。これらの各ポートにアナログモデムやターミナルアダプタを接続し、XR-640 のPPP 接続機能を使うことでリモートアクセスが可能となります。

また XR-640 の副回線接続機能で、PPP 接続を副回線として設定しておく、リモートアクセスを障害時のバックアップ回線として使うこともできます。

アナログモデム /TA のシリアル接続

- 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ください。
- 3 全ての接続が完了しましたら、モデムの電源を投入してください。

接続図



第7章 RS-232/BR1ポートを使った接続(リモートアクセス機能)

. BRIポートを使ったXR-640とTA/DSUの接続

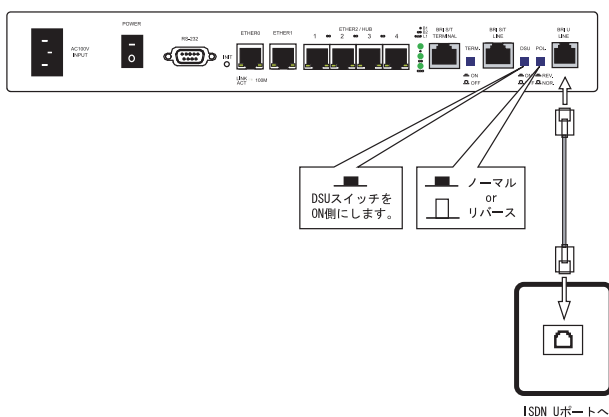
XR-640内蔵のDSUを使う場合

- 1 本装置の電源をオフにします。
- 2 ISDN U点ジャックと本装置の「BRI U」ポートをモジュラーケーブルで接続します。モジュラーケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「ON」側にします。
- 4 本体背面の「POL.」スイッチを、ISDN回線の極性に合わせます。
- 5 全ての接続が完了しましたら、本装置とTAの電源を投入してください。

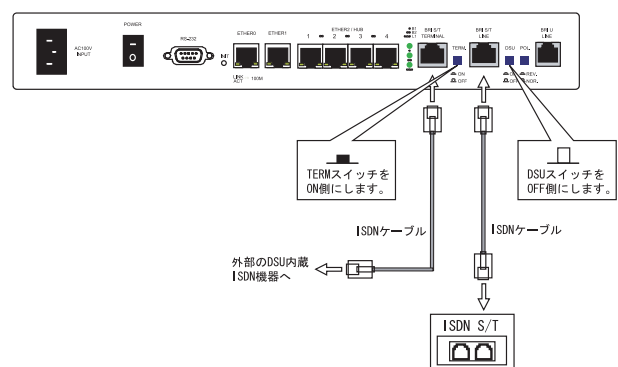
外付けTAに内蔵のDSUを使う場合

- 1 本装置の電源をオフにします。
- 2 外部のDSUと本装置の「BRI S/T LINE」ポートをISDN回線ケーブルで接続します。ISDNケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「OFF」側にします。
- 4 本体背面の「TERM.」スイッチを「ON」側にします。
- 5 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。
- 6 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



接続図



第7章 RS-232/BRI ポートを使った接続(リモートアクセス機能)

リモートアクセス回線の接続先設定

PPP(リモートアクセス)接続の接続先設定を行いません。

Web 設定画面「PPP/PPPoE 設定」の画面上部にある「接続先設定 1 ~ 5」のいずれかをクリックして、接続先の設定を行います。

設定は5つまで保存しておくことができます。

PPP/PPPoE接続設定					
接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
プロバイダ名	<input type="text"/>				
ユーザID	<input type="text"/>				
パスワード	<input type="text"/>				
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>				
LCPキープアライブ	チェック間隔 <input type="text"/> 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				
Pinetによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はPTP-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	<input type="text"/> 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	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 <input type="text"/> 0 Byte (有効時にMSS値が0又は空の場合は、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	<input type="text"/>				
ダイヤルタイムアウト	<input type="text"/> 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	<input type="radio"/> 9600 <input type="radio"/> 19200 <input type="radio"/> 38400 <input type="radio"/> 57600 <input checked="" type="radio"/> 115200 <input type="radio"/> 230400				
初期化用ATコマンド	<input type="text"/> ATQ0V1				
回線種別	<input checked="" type="radio"/> 無指定 <input type="radio"/> トーン <input type="radio"/> バルス				
BRI/PPPシリアル回線使用時に設定して下さい					
ON-DEMAND接続用切断タイムアウト	<input type="text"/> 180 秒				
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	<input type="text"/> 接続するネットワークを指定して下さい				
ネットマスク	<input type="text"/> 上記のネットワークのネットマスクを指定して下さい				

設定の保存

プロバイダ名

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

ユーザID

プロバイダから指定されたユーザIDを入力してください。

パスワード

プロバイダから指定された接続パスワードを入力してください。

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

<例> abc(def)g'h abc¥(def¥)g¥'h

DNSサーバ

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

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

LCPキープアライブ pingによる接続確認

[UnNumbered-PPP回線使用時に設定できます]

IPアドレス

[PPPoE回線使用時に設定して下さい]

MSS設定

上記項目は、リモートアクセス接続の場合は設定の必要はありません。

第7章 RS-232/BR1 ポートを使った接続(リモートアクセス機能)

リモートアクセス回線の接続先設定

[BR1/PPPシリアル回線使用時に設定して下さい]

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。

ダイアルタイムアウト

アクセス先にログインするときのタイムアウト時間を設定します。単位は秒です。

[PPPシリアル回線使用時に設定して下さい]

シリアルDTE

XR-640 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、発信するとき初期化が必要なものもあります。その際のコマンドをここに入力します。

回線種別

回線のダイアル方法を選択します。

[BR1/PPPシリアル回線使用時に設定して下さい]

ON-DEMAND 接続用切断タイマー

PPP/PPPoE 接続設定の RS232C/BR1 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、RS232C/BR1 接続を切断します。

[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

ネットマスク

<例>

ネットワーク「172.26.0.0」

ネットマスク「255.255.0.0」

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

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

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

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

続いて PPP の接続設定を行ないます。

第7章 RS-232/BRI ポートを使った接続(リモートアクセス機能)

リモートアクセス回線の接続と切断

接続先設定に続いて、リモートアクセス接続のために接続設定を行います。

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

PPP/PPPoE接続設定						
接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5	
回線状態	回線は接続されていません					
接続先の選択	<input checked="" type="radio"/> 接続先1	<input type="radio"/> 接続先2	<input type="radio"/> 接続先3	<input type="radio"/> 接続先4	<input type="radio"/> 接続先5	
接続ポート	<input type="radio"/> Ether0	<input type="radio"/> Ether1	<input type="radio"/> Ether2	<input type="radio"/> BRI(64K)	<input type="radio"/> BRI MP(128K)	<input checked="" type="radio"/> RS232C
接続形態	<input type="radio"/> 手動接続	<input checked="" type="radio"/> 常時接続	<input type="radio"/> スケジューラ接続			
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常	<input type="radio"/> On-Demand接続				
IPマスカレード	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効				
ステートフルパケットインスペクション	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効	<input type="checkbox"/> DROPしたパケットのLOGを取得			
デフォルトルートの設定	<input type="radio"/> 無効	<input checked="" type="radio"/> 有効				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する					
接続IP変更お知らせメール	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する					
お知らせメールの宛先	<input type="text"/>					
お知らせメールのFromアドレス	<input type="text" value="xr640"/>					
中継するメールサーバのアドレス	<input type="text"/>					

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「RS232C」ポートを選択します。

接続形態

「手動接続」リモートアクセスの接続 / 切断を手動で切り替えます。

「常時接続」XR-640 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」を選択すると、接続形態設定にあわせて接続します。

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

IPマスカレード

リモートアクセス接続時に IP マスカレードを有効にするかどうかを選択します。unnumbered 接続時以外は、「有効」を選択してください。

ステートフルパケットインスペクション

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25章 補足: フィルタのログ出力内容について](#)」をご覧ください。

デフォルトルートの設定

「有効」を選択すると、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。「インターフェース設定」でデフォルトルートが設定されていても、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。「インターフェース設定」でデフォルトルートが設定されていれば、その設定がそのままデフォルトルートとして採用されます。

通常は「有効」設定にしておきます。

ICMP AddressMask Request

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

第7章 RS-232/BRI ポートを使った接続(リモートアクセス機能)

・ リモートアクセス回線の接続と切断

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。

リモートアクセス接続についても、PPPoE 接続と同様に、「接続 IP お知らせメール」機能設定が可能です。

設定方法については、

「第6章 PPPoE 設定」をご参照ください。

「11.PPPoE の接続設定と回線の接続 / 切断」

第7章 RS-232/BRI ポートを使った接続(リモートアクセス機能)

．副回線接続とバックアップ回線接続

リモートアクセス接続についても、PPPoE 接続と同様に、

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

が可能です。

設定方法については、

「**第6章 PPPoE 設定**」の各ページをご参照ください。

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

第7章 RS-232/BRI ポートを使った接続(リモートアクセス機能)

・ 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RS232ポートやBRI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-640ではあらかじめ以下のフィルタリングを設定しています。

(入力フィルタ)

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

(転送フィルタ)

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

第8章

複数アカウント同時接続設定

第8章 複数アカウント同時接続設定

複数アカウント同時接続の設定

XR-640 は、同時に複数の PPPoE 接続を行うことができます。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)を同時に行う

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

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。

XR-640 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
- ・接続確認として、IPsec + PING を設定する

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

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

また XR-640 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、またはフィルタリング設定をしてください。

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

この機能を利用する場合は以下のステップに従って設定してください。

STEP 1 主接続の接続先設定

1 つ目のプロバイダの接続設定を行います。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 RS-232/BRI ポートを使った接続(リモートアクセス機能)」をご覧ください。

第8章 複数アカウント同時接続設定

複数アカウント同時接続の設定

STEP 2 マルチ接続用の接続先設定

マルチ接続(同時接続)用の接続先設定を行います。

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

設定方法については「第6章 PPPoE 接続」をご参照ください。

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

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

ネットワーク
ネットマスク

< 例 >

ネットワーク 「172.26.0.0」

ネットマスク 「255.255.0.0」

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

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

このどちらも設定しないと、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。

STEP 3 PPPoE 接続の設定

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

「PPP/PPPoE 設定」 「接続設定」を開きます。

[主接続用の接続設定]

以下の部分で設定します。

PPP/PPPoE接続設定					
接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
回線状態	回線は接続されていません				
接続先の選択	<input checked="" type="radio"/> 接続先1	<input type="radio"/> 接続先2	<input type="radio"/> 接続先3	<input type="radio"/> 接続先4	<input type="radio"/> 接続先5
接続ポート	<input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> BRI(64K) <input type="radio"/> BRI MP(128K) <input type="radio"/> RS232C				
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続 <input type="radio"/> スケジュール接続				
RS232C/BRI接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続				
IPマスカーレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ステータフルバケット インスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたバケットのLOGを取得				
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				
接続IP変更 お知らせメール	<input checked="" type="radio"/> 送信しない <input type="radio"/> 送信する				
お知らせメールの宛先	<input type="text"/>				
お知らせメールの Fromアドレス	xr640 <input type="text"/>				
中継するメールサーバの アドレス	<input type="text"/>				

回線状態

現在の回線状態を表示します。

接続先の選択

主接続用の設定を選択します。

接続先ポート

主接続で使用する本装置のインター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・切断の操作を行ってください。

第8章 複数アカウント同時接続設定

複数アカウント同時接続の設定

RS232C/BRI 接続タイプ

「通常」を選択すると、接続形態に合わせて接続します。

「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接続タイムアワーは「接続先設定」で設定します。

IP マスカレード

通常は「有効」を選択します。

LAN 側をグローバル IP で運用している場合は「無効」を選択します。

ステートフルパケットインスペクション

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

ログの出力内容については、「第25章 パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

デフォルトルートの設定

「有効」を選択します。

ICMP AddressMask Request

任意で選択します。

「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) を返送しません。

接続 IP 変更お知らせメール

任意で設定します。

続いてマルチ接続用の接続設定を行います。

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

マルチ接続 #2 ~ #4

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

接続先の選択

マルチ接続用の接続先設定を選択します。

接続ポート

マルチ接続で使用する、XR-640 のインタフェースを選択します。B フレッツ回線で複数の同時接続を行う場合は、主接続の設定と同じインタフェースを選択します。

第8章 複数アカウント同時接続設定

複数アカウント同時接続の設定

RS232C/BRI 接続タイプ

RS232 または BRI インタフェースを使って複数アカウント同時接続するときの接続タイプを選択します。

「通常」を選択すると主回線の接続形態に合わせて接続します。

「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

任意で選択します。
通常は「有効」にします。
LAN 側をグローバル IP で運用している場合は「無効」を選択します。

ステートフルパケットインスペクション任意で選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。

ログの出力内容については、「**第25章 パケットフィルタリング機能 補足：フィルタのログ出力内容について**」をご覧ください。

ICMP AddressMask Request

任意で選択します。

「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。

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となります。

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-640 の「DNS キャッシュ機能」を「有効」にし、各 PC の DNS サーバ設定を XR-640 の IP アドレスに設定してください。

XR-640 に名前解決要求をリレーさせないと、同時接続ができません。

第9章

各種サービスの設定

第9章 各種サービスの設定

各種サービス設定

XR-640 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。

サービスの起動・停止・設定

現在のサービス稼働状況に応じて、
各種設定はサービス項目名をクリックして下さい

DNSキャッシュ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
DHCP/Relayサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
UPnPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 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	
PPPoEtoL2TP	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
攻撃検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
VRRPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 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	

動作変更

ここでは

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

を行います。

サービスの設定

それぞれのサービスの設定を行うには、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 リレー / キャッシュ機能

DHCP サーバ / リレー機能

IPsec 機能

UPnP 機能

ダイナミックルーティング

PPPoE to L2TP

SYSLOG サービス

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 10 章

DNS リレー / キャッシュ機能

DNS 機能の設定

DNS リレー機能

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

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

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

DNSキャッシュの設定

プライマリ DNS IPアドレス	<input type="text"/>
セカンダリ DNS IPアドレス	<input type="text"/>
root server	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
タイムアウト	<input type="text" value="30"/> 秒

プライマリ DNS IPアドレス

セカンダリ DNS IPアドレス

任意の DNS サーバの IP アドレスを入力してください。ISP から指定された DNS サーバへリレーする場合は本設定の必要はありません。

root server

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

タイムアウト

DNS サーバへの問い合わせが無応答の場合のタイムアウトを設定します。

5-30 秒で設定できます。初期設定は 30 秒です。

使用環境によっては、DNS キャッシュのタイムアウトよりもブラウザなどのアプリケーションのタイムアウトが早く発生する場合があります。

この場合は、DNS キャッシュのタイムアウトを調整してください。

設定後に「設定の保存」をクリックして設定完了です。

設定はすぐに反映されます。

DNS キャッシュ機能

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

第 11 章

DHCP サーバ / リレー機能

第 11 章 DHCP サーバ / リレー機能

1. DHCP 関連機能について

本装置は、以下の 4 つの DHCP 関連機能を搭載しています。

DHCP クライアント機能

本装置のインターネット / WAN 側ポートは DHCP クライアントとなることができ、IP アドレスの自動割り当てを行う CATV インターネット接続サービスで利用できます。

また既存 LAN に仮設 LAN を接続したい場合などに、本装置の IP アドレスを決めなくても既存 LAN から IP アドレスを自動的に取得でき、LAN 同士の接続が容易に可能となります。

DHCP クライアント機能の設定は「第 5 章 インターフェイス設定」を参照してください。

DHCP サーバ機能

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

IP アドレスの固定割り当て

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

DHCP リレー機能

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

DHCP リレー機能は NAT 機能を利用している場合の利用はできません。

第11章 DHCPサーバ/リレー機能

. 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行います。

DHCPサーバの設定

DHCPリレーサーバ機能設定

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サーバを使用する DHCPリレーを使用する

DHCPリレーサーバ使用時に設定して下さい

上位DHCPサーバのIPアドレス

DHCP relay over XXX 使用しない 使用する

XXX: PPPoE / IPsec / IPsec over PPPoEでDHCP Relayをする場合、「使用する」に設定して下さい

設定の保存

サーバの選択

DHCPサーバ機能/リレー機能のどちらを使うかを選択します。サーバ機能とリレー機能を同時に使うことはできません。

上位DHCPサーバのIPアドレス

上記の「サーバの選択」で「DHCPリレーを使用する」を選択した場合に、上位のDHCPサーバのIPアドレスを指定します。複数のサーバを登録するときは、IPアドレスごとに改行して設定します。

DHCP relay over XXX

上記「サーバの選択」で「DHCPリレーを使用する」を選択した場合に設定を行います。

PPPoE・IPsec・PPPoE接続時のIPsec上でDHCPリレー機能を利用する場合は「使用する」を選択します。

DHCPサーバ機能設定

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WINSサーバ	
セカンダリWINSサーバ	
scopeID	

サブネット1～3

DHCPサーバ機能の動作設定を行います。

- 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-640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

リース終了アドレス

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

ルータアドレス

DHCPクライアントのデフォルトゲートウェイとなるアドレスを入力してください。通常は、XR-640のインタフェースのIPアドレスを指定します。

第11章 DHCP サーバ/リレー機能

. DHCP サーバ機能の設定

ドメイン名

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

プライマリ DNS

セカンダリ DNS

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

標準リース時間 (秒)

DHCPクライアントに IPアドレスを割り当てる時間を指定します。

初期設定では 600 秒です。1 秒から 999999 秒まで設定できます。

最大リース時間 (秒)

DHCPクライアント側が割り当て時間を要求してきたときの、最大限の割り当て時間を指定します。

初期設定は 7200 秒です。「標準リース時間」+ 1 秒から 999999 秒までの間で設定してください。

プライマリ WINS サーバー

セカンダリ WINS サーバー

DHCPクライアントに割り当てる WINS サーバアドレスを指定します。

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」)を行ってください。

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。

IPアドレス固定割り付け設定

DHCP IPアドレス固定割付け設定

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

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行います。

256まで設定可能です。「[IPアドレス固定割り当て設定インデックス](#)」のリンクをクリックしてください。

DHCP IPアドレス固定割り当て設定

DHCPサーバの設定

DHCP IPアドレス固定割り付け設定

No.1~16まで

No.	MACアドレス	IPアドレス	削除
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

入力のやり直し

設定/削除の実行

[IPアドレス固定割り当て設定インデックス](#)

[\[01-16\]](#) [\[17-32\]](#) [\[33-48\]](#) [\[49-64\]](#) [\[65-80\]](#) [\[81-96\]](#) [\[97-112\]](#) [\[113-128\]](#)
[\[129-144\]](#) [\[145-160\]](#) [\[161-176\]](#) [\[177-192\]](#) [\[193-208\]](#) [\[209-224\]](#) [\[225-240\]](#) [\[241-256\]](#)

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
MACアドレスに固定で割り当てるIPアドレスを入力します。

入力が終わりましたら「設定/削除の実行」をクリックして設定完了です。

固定割り当て機能は、DHCPサーバ機能を再起動してから有効になります。

DHCP IPアドレス固定割り付け設定の削除

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アドレス固定割り付け時のDHCPサーバ設定について

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

第 12 章

IPsec 機能

XR-640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-640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-640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-640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トラバーサルに対応

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

他の機器との接続実績について

以下のルータとの接続を確認しています。

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

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 通信を行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 通信を行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-640 の設定を行います。

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 ポリシー設定を行います。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行います。

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行います。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 通信を行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 通信を行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-640 の設定を行います。

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 ポリシーの設定を行います。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行います。

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行います。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。

第12章 IPsec機能

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。

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
IKE17	IKE18	IKE19	IKE20	IPsec 17	IPsec 18	IPsec 19	IPsec 20

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

(画面は表示例です)

IPsecに関する設定・確認は、全てこの設定画面からおこなえます。

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

STEP 1,2 鍵の作成・交換

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

PSK共通鍵方式を用いてIPsec通信を行う場合は、「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。

現在の鍵の作成状況
現在、鍵を作成できます。

作成する鍵の長さ bit
(512から2048までで、16の倍数の数値に限る)
鍵の長さが長いと、作成に時間がかかる場合があります。

- 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「現在、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。

鍵の作成を開始しました。

鍵の長さが長いと作成に時間がかかる場合があります。

作成が終了すると、本装置のRSA鍵設定に反映されます。

鍵を作成しました。

上記のメッセージが表示されると、鍵の生成が完了です。

生成した鍵は、後述する「本装置側の設定」に自動的に反映されます。

またこの鍵は公開鍵となりますので、相手側にも通知してください。

IPsec 設定

STEP 3 本装置側の設定を行う

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。

本装置の設定

[本装置の設定1](#)
[本装置の設定2](#)
[本装置の設定3](#)
[本装置の設定4](#)
[本装置の設定5](#)

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	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
Virtual Private 設定1	<input type="text"/>
Virtual Private 設定2	<input type="text"/>
Virtual Private 設定3	<input type="text"/>
Virtual Private 設定4	<input type="text"/>

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)	<input type="text"/>

MTU の設定

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

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>

本装置を NAT トラバーサル のホストとして使用する場合に設定します。クライアントとして使用する場合は空欄のままにします。

鍵の表示

RSA 鍵の作成をおこなった場合ここに、作成した 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。

[本装置側の設定]

「本装置側の設定 1 ~ 8」のいずれかをクリックします。ここで XR-640 自身の IP アドレスやインターフェース ID を設定します。

本装置側の設定1

[本装置側の設定1](#)
[本装置側の設定2](#)
[本装置側の設定3](#)
[本装置側の設定4](#)
[本装置側の設定5](#)
[本装置側の設定6](#)
[本装置側の設定7](#)
[本装置側の設定8](#)

IKE/ISAKMP の設定1	
インターフェースのIPアドレス	<input type="text"/>
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	<input type="text"/> (例:@xr.centurysys)

(画面は「本装置側の設定1」です)

インターフェースの IP アドレス

[固定アドレスの場合]

本装置に設定されている IP アドレスをそのまま入力します。

[動的アドレスの場合]

「%ppp0」と入力します。動的アドレスでの接続は、PPP/PPPoE 接続でのみ可能です。

上位ルータの IP アドレス

本装置から見て1つ上位のルータ(ゲートウェイ)の IP アドレスを入力します。

[固定アドレスの場合]

上位ルータの IP アドレスをそのまま入力します。PPP/PPPoE 接続の場合は「%ppp0」と入力してください。

[動的アドレスの場合]

空欄のままにします。

IPsec 設定

インターフェースの ID

本装置への IP アドレスの割り当てが動的割り当ての場合 (aggressive モードで接続する場合) は、インターフェースの 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 ポリシーの設定を行います。

STEP 4 IKE/ISAKMP ポリシーの設定

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

IKE/ISAKMP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

(画面は「IKE/ISAKMP の設定 1」です)

[IKE/ISAKMP の設定]

IKE/ISAKMP ポリシー名

設定名を任意で設定します。(省略可)

接続する本装置側の設定

接続で使用する「本装置側の設定」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
 相手側装置から見て1つ上位のルータ(主にゲートウェイ)IPアドレスを入力します。
 本装置への 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]

上位ルータの IP アドレスをそのまま入力します。

相手側装置が PPP、PPPoE 接続の場合は、空欄にしておきます。

[相手側装置が動的アドレスの場合]

空欄のままにします。

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「agressive モード」のどちらかから選択します。

transform の選択

ISAKMP SA の折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。XR-640 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)

接続相手の機器に合わせて transform を選択する必要があります。

「agressive モード」の場合

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

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

IKE のライフタイム

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

[鍵の設定]

PSK を使用する

PSK 方式の場合にチェックして、相手側と任意に決定した共通鍵を入力してください。

半角英数字のみ使用可能です。最大 2047 文字まで設定できます。

RSA を使用する

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

[X509 の設定]

接続先の証明書の設定

「X.509」設定で IPsec 通信を行う場合は、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 ポリシーの設定を行います。

STEP 5 IPsec ポリシーの設定

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

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ポリシーの設定1

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:

PFS: 使用する 使用しない

DH Groupの選択(PFS使用時に有効):

SAのライフタイム: 秒 (1081~86400秒まで)

DISTANCE: (1~255まで)

(画面は「IPsec ポリシーの設定1」です)

最初に IPsec の起動状態を選択します。

「使用する」

initiator にも responder にもなります。

「使用しない」

その IPsec ポリシーを使用しません。

「Responder として使用する」

サービス起動時や起動中の IPsec ポリシー追加時に、responder として IPsec 接続を待ちます。本装置が固定 IP アドレス設定で、接続相手が動的 IP アドレス設定の場合に選択してください。

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

「On-Demand で使用する」

IPsec をオンデマンド接続します。切断タイマーは SA のライフタイムとなります。

使用する IKE ポリシー名の選択

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

本装置側の LAN 側のネットワークアドレス 自分側の XR-640 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。「本装置側の LAN 側のネットワークアドレス」と同様です。

また NAT Traversal 機能を使用し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 条件と同じ DH Group 条件を接続相手に送ります。

第12章 IPsec 機能

IPsec 設定

SA のライフタイム

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

DISTANCE

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

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

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

[IPsec 通信時の Ethernet ポート設定について]

IPsec 設定を行う場合は、Ethernet ポートの設定に注意してください。

IPsec 通信を行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-640 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 通信を行う相手側のネットワークが 192.168.1.0/24 の設定で、且つ、XR-640 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-640 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。

サービスの起動/停止/設定

現在のサービス稼働状況を表示しています
各種設定はサービス項目名をクリックして下さい

DNS キャッシュ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
DHCP(Relay)サーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
UPnPサービス	<input type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
ダイヤルアップルーティング	起動停止はダイヤルアップルーティングの設定から行って下さい		停止中
PPPoEtoL2TP	<input type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
変換検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
SNMPサービス	<input type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
NTPサービス	<input type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
VRPPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 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

動作変更

動作状態の制御

IPsec サーバ項目、「起動」にチェックして「動作変更」をクリックすると、IPsec 機能が起動します。以降は、XR-640 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。

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 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
IKE17	IKE18	IKE19	IKE20	IPSec 17	IPSec 18	IPSec 19	IPSec 20

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、
本装置側 相手側 接続

IPsec	LAN側	IPアドレス	接続NG	IKEポリシー名	IPアドレス	LAN側	SA

現在の状態 停止中

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 12 章 IPsec 機能

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し、IPsecSAの再起動またはバックアップSAを起動することで、IPsecの再接続性を高めます。

[IPsec Keep-Alive 設定]

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

設定は 128 まで可能です。「ページインデックス」のリンクをクリックしてください。

IPsec Keep-Alive 設定
No.1~16まで

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作Option 1 *	動作Option 2 *	interface	backup SA	remove?
1	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
2	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
3	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
4	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
5	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
6	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
7	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
8	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
9	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
10	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
11	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
12	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
13	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
14	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
15	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>
16	<input type="checkbox"/>			30	3	60	<input type="checkbox"/>	<input checked="" type="checkbox"/>	ipsec0		<input type="checkbox"/>

設定/削除の実行

ページインデックス

[1](#) - [16](#) [17](#) - [32](#) [33](#) - [48](#) [49](#) - [64](#) [65](#) - [80](#) [81](#) - [96](#) [97](#) - [112](#) [113](#) - [128](#)

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 option 1」の設定に応じて、入力値の意味が異なります。

・動作 option 1 が有効の場合

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

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 option 1 が無効の場合

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

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

・ IPsec Keep-Alive 設定

動作 option 1

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

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

注) 本オプションにチェックを入れない場合、IPsec ネゴシエーションと Keep-Alive が非同期に行われるため、タイミングによっては 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。

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 option 1 を有効にした場合、各フェーズと同期した Keep-Alive 動作を行います。

・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 の送出手は行いません。

・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 option 2

本オプションは「動作 option 1」が無効の場合のみ、有効になります。

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

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

interface

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

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

backup SA

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

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

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

<入力例>
1_2_3

またここに、以下のような設定もできます。

ike<n> <n> は 1 ~ 128 の整数

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

<例>
使用する IKE ポリシー IKE/ISAKMP1 番

IPsec ポリシー IPsec2 IPsec4 IPsec5

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

remove ?
設定を削除したいときにチェックします。

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

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

設定番号について

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

第12章 IPsec 機能

「X.509 デジタル証明書」を用いた電子認証

XR-640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-640は証明書署名要求の発行や証明書の発行ができませんので、あらかじめCA局から証明書の発行を受けておく必要があります。

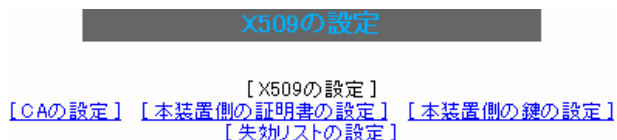
電子証明の仕組みや証明書発行の詳しい手順につきましては関連書籍等をご参考ください。

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

設定は、IPsec設定画面内の「X.509の設定」から行えます。

[X.509の設定]

IPsec設定画面上部の「X509の設定」「X509の設定」を開きます。



X509の設定	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
設定した接続先の証明書のみを使用する	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
証明書のパスワード	<input type="password"/>

入力のやり直し

設定の保存

X509の設定

X.509の使用 / 不使用を選択します。

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

証明書のパスワード
証明書のパスワードを入力します。

入力が終わりましたら「設定の保存」をクリックします。

「X.509 デジタル証明書」を用いた電子認証

[CA の設定]

ここでは、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]

ここでは、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]

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

[失効リストの設定]

失効リストを作成している場合は、その内容をコピーして貼り付けます。

各設定にコピーを貼り付けましたら、「設定の保存」をクリックします。

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

その際、「IKE/ISAKMP 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。

第12章 IPsec 機能

・ IPsec 通信時のパケットフィルタ設定

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

IPsec では、以下の2種類のプロトコル・ポートを使用します。

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

但し、NAT トラバーサルを使用する場合は、IKE の一部のトラフィックおよび暗号化ペイロードはUDP の4500番ポートの packets にカプセル化されています。

よって、以下の2種類のプロトコル・ポートに対するフィルタ設定の追加が必要になります。

- ・プロトコル「UDP」のポート「500」番
IKE(IPsecの鍵交換)のトラフィックに必要です
- ・プロトコル「UDP」のポート「4500」番
一部の IKE トラフィックおよび暗号化ペイロードのトラフィックに必要です

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

< 設定例 >

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

・ 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
```

. IPsec がつながらないとき

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

[正常に IPsec が確立したときの表示例]

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

これらのログやメッセージ内に

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

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

・ 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、「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 がつながらなくなりました。

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-640 には IPsec のログが出ているのに、こちらの XR-640 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、確認方法はありますか？

固定 IP - 動的 IP 間での IPsec 接続を行う場合、固定 IP 側(受信者側)の XR-640 ではログが表示されることがあります。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 13 章

UPnP 機能

第13章 UPnP 機能

UPnP 機能の設定

XR-640 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-640 の UPnP 機能の設定は以下の手順で行ってください。

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。

UPnP サービスの設定

WAN側インターフェース	<input type="text" value="eth1"/>
LAN側インターフェース	<input type="text" value="eth0"/>
切断検知タイマー	<input type="text" value="5"/> 分 (0~60分)

設定の保存

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

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

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

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-640 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」)を行ってください。

第13章 UPnP 機能

UPnP 機能の設定

UPnP の接続状態の確認

各コンピュータが XR-640 と正常に UPnP で接続されているかどうかを確認します。

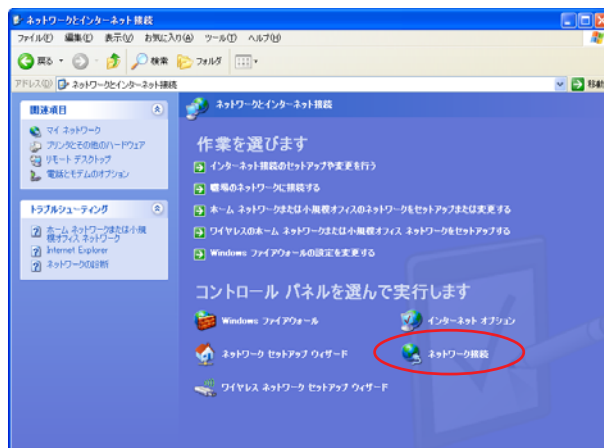
1 「スタート」「コントロールパネル」を開きます。



2 「ネットワークとインターネット接続」を開きます。



3 「ネットワーク接続」を開きます。



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



(画面は Windows XP での表示例です)

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

第13章 UPnP 機能

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ください)

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

UPnP 機能使用時の推奨フィルタ設定

Microsoft Windows 上の UPnP サービスのバッファオーバーフローを狙った 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-640は工場出荷設定で以下のようなフィルタをあらかじめ設定しています。

(入力フィルタ)

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

(転送フィルタ)

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

UPnP 使用時は上記フィルタ設定を作動させておくことを推奨いたします。

第14章

ダイナミックルーティング

第14章 ダイナミックルーティング

ダイナミックルーティング機能

XR-640のダイナミックルーティング機能は以下のプロトコルをサポートしています。

- RIP
- OSPF
- DVMRP

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

設定の開始

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

サービスの起動/停止/設定

現在のサービス稼働状況を反映しています
各種設定はサービス項目名をクリックして下さい

DNSキャッシュ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
DHCP(Relay)サーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
UPnPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 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
PPPoEtoL2TP	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
攻撃検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
VRPPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 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

動作変更

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

ダイナミックルーティング設定

※各種設定は項目名をクリックして下さい。

RIP	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
OSPF	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
DVMRP	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動

動作変更 再起動

第14章 ダイナミックルーティング

RIPの設定

RIPの設定

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

RIP設定

RIP設定	
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	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
再配信時のメトリック設定	<input type="text"/> (0-16) 指定しない場合は空白
staticルートの再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
staticルート再配信時のメトリック設定	<input type="text"/> (0-16) 指定しない場合は空白
default-informationの送信	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

Ether0ポート、Ether1ポート、Ether2ポートXR-640の各Ethernetポートで、RIPを「使用しない」か、使用する（「送受信」）を選択します。

また、使用する場合のRIPバージョン（「バージョン1」、「バージョン2」、「Both 1 and 2」）を選択します。

Administrative Distance設定

RIPとOSPFを併用していて全く同じ経路を学習する場合がありますが、その際は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

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

再配信時のメトリック設定

OSPFルートをRIPで配信するときのメトリック値を設定します。

staticルートの再配信

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

staticルート再配信時のメトリック設定

staticルートをRIPで配信するときのメトリック値を設定します。

default-informationの送信

デフォルトルート情報をRIPで配信したいときに「有効」にしてください。

選択、入力後は「設定」をクリックして設定完了です。

設定後は「ダイナミックルーティング設定」画面に戻り、「起動」を選択して「動作変更」をクリックしてください。

また設定を変更した場合には、「再起動」をクリックしてください。

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

第14章 ダイナミックルーティング

. RIPの設定

RIPフィルタの設定

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

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

NO.	インタフェース	方向	ネットワーク	編集 削除
現在設定はありません				

フィルタの追加

NO.

設定番号を指定します。1-64の間で指定します。

インタフェース

RIPフィルタを実行するインタフェースを選択します。

方向

「in-coming」

本装置がRIP情報を受信する際にRIPフィルタリングします(受信しない)。

「out-going」

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

ネットワーク

RIPフィルタリングの対象となるネットワークアドレスを指定します。

<入力形式>

ネットワークアドレス/サブネットマスク値

入力後は「追加」をクリックしてください。

「取消」をクリックすると、入力内容がクリアされます。

RIPフィルタ設定後は、ただちに設定が有効となります。

設定後は、画面上部に設定内容が一覧表示されます。

NO.	インタフェース	方向	ネットワーク	編集 削除
1	Ether0ポート	in-coming	192.168.0.0/16	編集 削除

「削除」をクリックすると、設定が削除されます。

「編集」をクリックすると、その設定について内容を編集できます。

第14章 ダイナミックルーティング

OSPF の設定

OSPF の設定

OSPFはリンクステート型経路制御プロトコルです。

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

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

これにより、トラフィックのロードバランシングが可能となっています。

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

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

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

OSPF設定

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

インタフェースへのOSPFエリア設定

どのインタフェースでOSPF機能を動作させるかを設定します。

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。

指定インタフェースへのOSPFエリア設定

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

設定

[ダイナミックルーティング設定画面へ](#)

ネットワークアドレス

XR-640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14章 ダイナミックルーティング

OSPFの設定

OSPF エリア設定

各AREA(エリア)ごとの機能設定を行います。

設定画面上部の「OSPF エリア設定」をクリックします。



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

AREA番号	<input type="text" value="0-4294967295"/>
スタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
トータルスタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
default-cost	<input type="text" value="0-16777215"/>
認証設定	使用しない <input type="button" value="v"/>
エリア間ルートの経路集約設定	<input type="text"/> <input type="text"/> <input type="text"/> <input type="text"/>

AREA 番号

機能設定を行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。

トータルスタブ設定

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

default-cost 設定

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

認証設定

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

エリア間ルートの経路集約設定

経路情報を集約して送信したいときに設定します。

< 設定例 >

128.213.64.0 ~ 128.213.95.0のレンジのサブネットを渡すときに1つずつ渡すのではなく、128.213.64.0/19に集約して渡す、といったときに使用します。ただし、連続したサブネットであればなりません(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	無効	無効	無効	128.213.64.0/19	Edit, Remove

(画面は表示例です)

[Configure]項目の

Edit

クリックすることで、それぞれ設定内容の「編集」を行えます。

Remove

クリックすると設定の「削除」を行えます。

第14章 ダイナミックルーティング

OSPF の設定

Virtual Link 設定

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

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

設定画面上部の「Virtual Link 設定」をクリックして設定します。

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

OSPF Virtual-Link設定

Transit AREA番号	<input type="text" value="0-4294967295"/>
Remote-ABR Router-ID設定	<input type="text" value="例192.168.0.1"/>
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)
認証パスワード設定	<input type="text" value=""/> (英数字で最大8文字)
MD KEY-ID設定(1)	<input type="text" value=""/> (1-255)
MD5パスワード設定(1)	<input type="text" value=""/> (英数字で最大16文字)
MD KEY-ID設定(2)	<input type="text" value=""/> (1-255)
MD5パスワード設定(2)	<input type="text" value=""/> (英数字で最大16文字)

Transit AREA 番号

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

Remote-ABR Router-ID 設定

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

Helloインターバル設定

Helloパケットの送出間隔を設定します。

Deadインターバル設定

Deadタイムを設定します。

Retransmit インターバル設定

LSAを送出する間隔を設定します。

transmit delay 設定

LSUを送出する際の遅延間隔(delay)を設定します。

認証パスワード設定

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

MD5 KEY-ID 設定(1)

MD5認証使用時のKEY IDを設定します。

MD5 パスワード設定(1)

エリア内でMD5認証を使用する際のMD5パスワードを設定します。

MD5 KEY-ID 設定(2)

MD5 パスワード設定(2)

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

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

入力後は「設定」をクリックしてください。

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

Virtual Link設定

AREA番号	Remote-ABR ID	Hello	Dead	Retransmit	Transmit Delay	認証 Password	MD5 KEY-ID	MD5 Password	Configure
1	192.168.0.1	10	40	5	1	aaa	1	bbb	Edit Remove

(画面は表示例です)

「Configure」項目の

Edit

をクリックすることで、それぞれ設定内容の「編集」を行えます。

Remove

をクリックすると設定の「削除」を行えます。

第14章 ダイナミックルーティング

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。

OSPF 機能設定	
Router-ID設定	<input type="text" value="192.168.0.1"/> (例:192.168.0.1)
Connected再配信	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value="16777214"/> (0-16777214)
staticルート再配信	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効 メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value="16777214"/> (0-16777214)
RIPルートの再配信	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value="16777214"/> (0-16777214)
Administrative Distance設定	<input type="text" value="110"/> (1-255) デフォルト110
Externalルート Distance設定	<input type="text" value="1"/> (1-255)
Inter-areaルート Distance設定	<input type="text" value="1"/> (1-255)
Intra-areaルート Distance設定	<input type="text" value="1"/> (1-255)
Default-information	<input type="text" value="送信しない"/> メトリックタイプ <input type="text" value="2"/> メトリック値設定 <input type="text" value="16777214"/> (0-16777214)
SPF計算Delay設定	<input type="text" value="5"/> (0-4294967295) デフォルト5s
2つのSPF計算の最小間隔設定	<input type="text" value="10"/> (0-4294967295) デフォルト10s
バックアップ切替え監視対象 Remote Router-ID設定	<input type="text" value="192.168.0.2"/> (例:192.168.0.2)

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 で配信するかどうかを選択します。

「有効」にした場合は以下の2項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

staticルートの再配信

staticルートを OSPF で配信するかどうかを選択します。

IPsecルートを再配信する場合も、この設定を「有効」にする必要があります。

「有効」にした場合は以下の2項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

入力しない場合はメトリック値20となります。

RIPルートの再配信

RIPが学習したルート情報を OSPF で配信するかどうかを選択します。

「有効」にした場合は以下の2項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

入力しない場合はメトリック値20となります。

Administrative Distance 設定

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

External ルート Distance 設定

OSPF 以外のプロトコルで学習した経路のディスタンス値を設定します。

Inter-area ルート Distance 設定

エリア間の経路のディスタンス値を設定します。

Intra-area ルート Distance 設定

エリア内の経路のディスタンス値を設定します。

第14章 ダイナミックルーティング

. OSPF の設定

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が、たとえば PPPoE セッションが切断してデフォルトルート情報がなくなってしまったときは配信されなくなります。

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

「送信する」「常に送信する」の場合は、以下の2項目についても設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

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

SPF 計算 Delay 設定

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

2つの SPF 計算の最小間隔設定

連続して SPF 計算を行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14章 ダイナミックルーティング

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。

OSPFインタフェース設定

インタフェース名	eth0
Passive-Interface設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
コスト値設定	<input type="text"/> (1-65535)
帯域設定	<input type="text"/> (1-10000000kbps)
Helloインターバル設定	<input type="text"/> (1-65535s)
Deadインターバル設定	<input type="text"/> (1-65535s)
Retransmitインターバル設定	<input type="text"/> (3-65535s)
Transmit Delay設定	<input type="text"/> (1-65535s)
認証キー設定	<input type="text"/> (英数字で最大8文字)
MD KEY-ID設定(1)	<input type="text"/> (1-255)
MD5パスワード設定(1)	<input type="text"/> (英数字で最大16文字)
MD KEY-ID設定(2)	<input type="text"/> (1-255)
MD5パスワード設定(2)	<input type="text"/> (英数字で最大16文字)
Priority設定	<input type="text"/> (0-255)
MTU-Ignore設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

インタフェース名

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

Passive-Interface 設定

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

コスト値設定

コスト値を設定します。

帯域設定

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

Helloインターバル設定

Helloパケットを送出する間隔を設定します。

Deadインターバル設定

Deadタイムを設定します。

Retransmit インターバル設定

LSAの送出間隔を設定します。

Transmit Delay 設定

LSUを送出する際の遅延間隔を設定します。

認証キー設定

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

MD KEY-ID 設定(1)

MD5 認証使用時のKEY IDを設定します。

MD5 パスワード設定(1)

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。半角英数字で最大16文字まで使用できます。

MD KEY-ID 設定(2)

MD5 パスワード設定(2)

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

Priority 設定

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

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

第14章 ダイナミックルーティング

OSPF の設定

MTU-Ignore 設定

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

入力後は「設定」をクリックしてください。

設定後は「インターフェース設定」画面に、設定内容が一覧で表示されます。

インターフェース名	Passive	Cost	Hello	Dead	Retransmit	Transmit Delay	DR Priority	MD5 Password	MD5 Key-ID	MD5 Password	Priority	MTU Ignore	Configure
e#0	on	10	1000000	10	40	5	1	cankey	150	cankeysystem	50	off	Edit Remove

現在バックアップ回線は待機中です

New Entry

「Configure」項目の

Edit

をクリックすることで、それぞれ設定内容の「編集」を行えます。

Remove

をクリックすると設定の「削除」を行えます。

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。

ステータス表示

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	
ネイバーリスト情報の表示 (現在のネイバー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	
インターフェース情報の表示 (表示したいインターフェースを指定して下さい)	表示する	<input type="text"/>

ダイナミックルーティング設定画面へ

OSPF データベース表示

LinkState 情報が表示されます。

ネイバーリスト情報の表示

現在のネイバー状態が表示されます。

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

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

インターフェース情報の表示

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

表示したい情報の項目にある「表示する」をクリックしてください。

第14章 ダイナミックルーティング

. DVMRP の設定

DVMRP の設定

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

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

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

DVMRP 設定

[インタフェース設定](#)

[全体設定](#)

[ステータス表示](#)

インタフェース設定

XR-640 の設定画面上部の「インタフェース設定」をクリックして設定します。

256 まで設定可能です。「インターフェイス設定 Index」のリンクをクリックしてください。

インターフェイス設定

インターフェイス設定 Index

[1-](#) [17-](#) [33-](#) [49-](#) [65-](#) [81-](#) [97-](#) [113-](#)
[129-](#) [145-](#) [161-](#) [177-](#) [193-](#) [209-](#) [225-](#) [241-](#)

No.	Interface	Metric	Threshold	Disable	Del
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

設定の保存

入力のやり直し

Interface

DVMRP を実行する、本装置のインタフェース名を指定します。本装置のインタフェース名については、本マニュアルの「付録A インタフェース名一覧」をご参照ください。

Metric

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

Threshold

TTL の“しきい値”を設定します。この値とデータグラム内の TTL 値とを比較して、そのデータグラムを転送または破棄します。

「Threshold > データグラムの TTL」のときはデータグラムを破棄、「Threshold ≤ データグラムの TTL」のときはデータグラムをルーティングします。

Disable

チェックを入れて設定を保存すると、その設定は無効となります。

Del

チェックを入れて設定を保存すると、その設定は削除されます。

入力後は「設定の保存」をクリックしてください。

全体設定

設定画面上部の「全体設定」をクリックして設定します。

全体設定

インターフェイスのデフォルト	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Cache Lifetime (sec) (300s - 86400s)	<input style="width: 100%;" type="text" value="300"/>

設定の保存
入力のやり直し

(画面は表示例です)

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

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

入力後は「設定の保存」をクリックしてください。

ステータス表示

設定画面上部の「ステータス表示」をクリックして表示します。

DVMRP ステータス表示								
UP TIME: 290:24:44								
Neighbors: 0								
DVMRP Interface 表示								
Virtual Interface Table								
Vif	Name	Local-Address	M	Thr	Rate	Flags		
0	eth0	192.168.120.237 subnet: 192.168.120/24	1	1	0	leaf		
1	eth2	192.168.2.254 subnet: 192.168.2/24	1	1	0	querier leaf		
DVMRP Routing 表示								
Multicast Routing Table (2 entries)								
Origin-Subnet	From-Gateway	Metric	Tmr	Fl	In-Vif	Out-Vifs		
192.168.120/24		1	145	..	0	1*		
192.168.2/24		1	145	..	1	0*		
DVMRP Cache 表示								
Multicast Routing Cache Table (2 entries)								
1	Origin	Mcast-group	OTmr	Age	Ptmr	Rx	IVif	Forwifs
2	(prunesrcvif[id]/tmr)	prunebitmap						
3	Source	Lifetime	SavPkt	Pkts	Bytes	RPFf		
1	192.168.120/24	239.255.2.2	0:04:52	0:02:22	-	-	0	
3	192.168.120.161	0:02:22	0	1	47	0		
1	192.168.120/24	239.255.255.250	0:02:43	0:04:36	-	-	0	
3	192.168.120.101	0:04:36	0	36	13710	0		

(画面は表示例です)

「ステータス表示」画面では、DVMRP が動作しているインタフェースの状態、マルチキャストルーティングテーブルの内容、ルーティングテーブルキャッシュの内容が表示されます。

DVMRP サービスが起動していない場合は表示画面はありません。

第 15 章

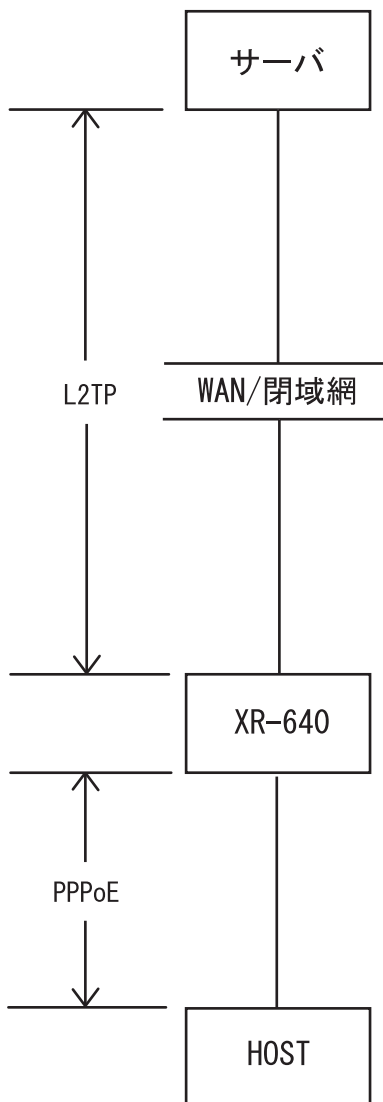
PPPoE to L2TP

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 接続を行います。XR-640 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-640 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」をクリックして行います。

L2TP Tunnel 設定

PPPoE to L2TP 設定

L2TP Tunnel 設定 | PPPoE to L2TP オプション設定 | L2TP ステータス表示

L2TP Tunnel 設定

Description	Peer IP	パスワード	ポート番号	AVP Hiding	Hello Interval	Configure
-------------	---------	-------	-------	------------	----------------	-----------

現在設定はありません

New Entry

「L2TP Tunnel 設定」 「New Entry」をクリックします。

L2TP Tunnel 設定

Description	<input type="text"/>
Peer アドレス	<input type="text"/> (例:192.168.0.1)
パスワード	<input type="text"/> (英数字95文字まで)
ポート番号	<input type="text"/> 1701 (default 1701)
AVP Hiding 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Hello Interval 設定	<input type="text"/> 60 [0-1000s] (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。半角英数字で 95 文字まで設定できます。

ポート番号

ポート番号を入力します。通常は初期設定 1701 を使用します。

AVP Hiding 設定

AVP Hiding の使用 / 不使用を選択します。

Hello Interval 設定

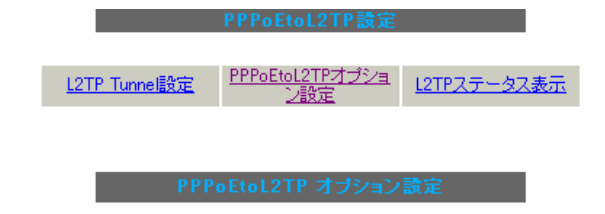
Hello パケットの送信間隔を設定します(単位:秒)。

最後に「設定」をクリックします。

PPPoE to L2TP 機能について

PPPoEtoL2TP オプション設定

「PPPoEtoL2TP オプション設定」をクリックします。



Local hostname	<input type="text" value="localhost"/>
PPPoE Frame受信インタフェース設定	<input checked="" type="radio"/> eth0 <input type="radio"/> eth1 <input type="radio"/> eth2
MAX Session数	<input type="text" value="256"/> (max 256)
Path MTU Discovery	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Debug設定 (Syslogメッセージ出力設定)	<input type="checkbox"/> Tunnel Debug出力 <input type="checkbox"/> Session Debug出力 <input checked="" type="checkbox"/> L2TPエラーメッセージ出力 <input type="checkbox"/> PPPoE Debug出力

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

本機能を有効にした場合は、常にIPヘッダのDFビットをONにして転送します。

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。

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

最後に「設定」をクリックします。

「L2TP Tunnel 設定」「PPPoEtoL2TP オプション設定」を設定した場合、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」）を行ってください。

L2TP ステータス表示

「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。

第 16 章

SYSLOG 機能

syslog 機能の設定

XR-640 は、syslog を出力・表示することが可能です。また、他の syslog サーバに送信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行います。

<ログの取得>

出力先

syslog の出力先を選択します。

「本装置」

本装置で syslog を取得する場合に選択します。

「SYSLOG サーバ」

syslog サーバに送信するときに選択します。

「本装置と SYSLOG サーバ」

本装置と syslog サーバの両方で syslog を管理します。

送信先 IP アドレス

syslog サーバの IP アドレスを指定します。

取得プライオリティ

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

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

--MARK-- を出力する時間間隔

syslog が動作していることを表す「-- MARK --」ログを送出する間隔を指定します。

初期設定は 20 分です。

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

<システムメッセージ>

本装置のシステム情報を定期的に出力することができます。

以下から選択してください。

出力しない

システムメッセージを出力しません。

MARK 出力時

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

1 時間ごとに出力

1 時間ごとにシステムメッセージを出力します。

出力される情報は下記の内容です。

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

・ cpu:0.00

cpu のロードアベレージです。

1 に近いほど高負荷を表し、1 を超えている場合は過負荷の状態を表します。

・ mem:28594176

113 空きメモリ量(byte)です。

syslog 機能の設定

・ session:0/2 (XX/YY)

本装置内部で保持している NAT および IP マスカレード のセッション情報数です。

0 (XX)

現在 Establish している TCP セッションの数

2 (YY)

本装置が現在キャッシュしている全てのセッション数

< ログのメール送信 >

ログの内容を電子メールで送信したい場合の設定です。

送信しない

送信する

ログメール機能を使うときは「送信する」を選択してください。

ログのメールを「送信する」場合は、以下の項目を任意で指定できます。

送信先メールアドレス

ログメッセージの送信先メールアドレスを指定します。

送信元メールアドレス

何も指定しない場合は以下のアドレスで送信されます。

ただし、「中継するサーバアドレス」の設定の有無で異なったアドレスが使用されます。

・「中継するサーバアドレス」設定しない場合

「root@mailto.localhost」

・「中継するサーバアドレス」設定した場合

「root@mailto.localdomain.co.jp」

件名

半角英数字のみ使用できます。

何も指定しないときは「件名は無し」で送信されます。

中継するサーバアドレス

お知らせメールを中継する任意のメールサーバを設定します。

IP アドレス、ドメイン名のどちらでも設定できます。ただしドメイン名で指定するときは、下記の記述で設定してください。

<入力例> mail.centurysys.co.jp

< 検出文字列の指定 >

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

文字列の指定は、1 行につき 255 文字まで、かつ最大 32 行までです。空白・大小文字も判別します。

一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したログのみ抽出して送信します。**なお「検出文字列の指定」項目は、「ログのメール送信」機能のみ有効です。**

「設定の保存」をクリックして設定完了です。

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

syslog 機能の設定

ファシリティと監視レベルについて

本装置で設定されている syslog のファシリティ・監視レベルは以下のようになっています。

[ファシリティ：監視レベル]

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

ログファイルの取得

ログは「システム設定」「ログの表示」に表示されます。

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

ログファイルの取得

ブラウザの「リンクを保存する」を使用して取得して下さい

[最新ログ](#)

[バックアップログ1](#)

[バックアップログ2](#)

[バックアップログ3](#)

[バックアップログ4](#)

[バックアップログ5](#)

[バックアップログ6](#)

第 17 章

攻撃検出機能

攻撃検出機能の設定

攻撃検出機能の概要

攻撃検出機能とは、外部から LAN への侵入や XR-640 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-640 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。

攻撃検出サービスの設定

使用するインターフェース	<input type="radio"/> Ether 0で使用する <input checked="" type="radio"/> Ether 1で使用する <input type="radio"/> Ether 2で使用する <input type="radio"/> PPP/PPPoEで使用する
検出対象となる IP アドレス	<input style="width: 100%;" type="text" value="any"/>

入力のやり直し
設定の保存

使用するインターフェース

DoSの検出を行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

攻撃を検出したいホストの IP アドレスか、ネットワークアドレスを指定します。

<入力例>

ホスト単体の場合

192.168.0.1/32 (“/32”を付ける)

ネットワーク単位の場合

192.168.0.0/24 (“/マスクビット値”を付ける)

「any」と入力すると、すべての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」)を行ってください。

第 18 章

SNMP エージェント機能

第18章 SNMP エージェント機能

SNMP エージェント機能の設定

SNMP エージェントを起動すると、SNMP マネージャから XR-640 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 機能の設定

SNMP マネージャ	192.168.0.0/24 <small>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。</small>
コミュニティ名	community
SNMP TRAP	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
SNMP TRAP の送信先アドレス	<input type="text"/>
SNMP TRAP の送信元	<input checked="" type="radio"/> 指定しない <input type="radio"/> IPアドレス <input type="radio"/> インターフェース
送信元	<input type="text"/>

SNMP マネージャ

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

コミュニティ名

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

SNMP TRAP

「使用する」を選択すると、SNMP TRAP を送信できるようになります。

SNMP TRAP の送信先 IP アドレス

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

SNMP TRAP の送信元

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

「指定しない」

SNMP TRAP の送信元アドレスが自動的に設定されます。

「IP アドレス」

SNMP TRAP の送信元アドレスを指定します。

「インターフェース」

SNMP TRAP の送信元アドレスとなるインターフェース名を指定します。指定可能なインターフェースは、本装置の Ethernet ポートと PPP インターフェースのみです。

送信元

SNMP RESPONSE パケットの送信元アドレスを設定できます。

IPsec 接続を通して、リモート拠点のマネージャから SNMP を取得したい場合は、ここに IPsecSA の LAN 側アドレスを指定してください。

通常の LAN 内でマネージャを使用する場合には設定の必要はありません。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

SNMP 設定

SNMP の設定を保存し、再読み込みしました。

SNMP TRAP の送信元、送信元を変更した場合は、再起動を行って下さい。
[\[各種サービスの設定へ\]](#)

[\[設定画面へ\]](#)

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

なお、設定を変更した場合は、即時設定が反映されませんが、「SNMP TRAP の送信元」および「送信元」を変更した場合には、「動作変更」をクリックしてください。

SNMP エージェント機能の設定

MIB 項目について

以下の MIB に対応しております。

- MIB II (RFC 1213)
- UCD-SNMP MIB
- RFC2011 (IP-MIB)
- RFC2012 (TCP-MIB)
- RFC2013 (UDP-MIB)
- RFC2863 (IF-MIB)

SNMP TRAP を送信するトリガーについて

以下のものに関して、SNMP TRAP を送信します。

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

第 19 章

NTP サービス

第19章 NTP サービス

NTP サービスの設定方法

XR-640 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。

NTP機能の設定
情報表示

問合せ先NTPサーバ (IPアドレス/FQDN)	1.	<input type="text"/>	Polling間隔 (Min)	<input type="text" value="6"/>	(Max)	<input type="text" value="10"/>
	2.	<input type="text"/>	Polling間隔 (Min)	<input type="text" value="6"/>	(Max)	<input type="text" value="10"/>
Polling間隔にX(sec)を指定すると、指定したNTPサーバへのポーリング間隔は2×秒となります。 ex. (4: 16sec, 6: 64sec,... 10: 1024sec)						
時刻同期タイムアウト時間	<input type="text" value="1"/>	(秒-1-10)	NTPサービス起動時に適用されます			
<input type="button" value="入力のやり直し"/> <input type="button" value="設定の保存"/>						

問合せ先 NTP サーバ

NTPサーバのIPアドレスもしくはFQDNを「設定1」もしくは「設定2」に入力します。

NTPサーバの場所は2箇所設定できます。

これにより、XR-640がNTPクライアント/サーバとして動作できます。

NTPサーバのIPアドレスもしくはFQDNを入力しない場合は、XR-640はNTPサーバとしてのみ動作します。

Polling 間隔

NTPサーバと通信を行う間隔を設定します。

サーバとの接続状態により、指定した最小値(Min)と最大値(Max)の範囲でポーリングの間隔を調整します。

Polling 間隔 X(sec)を指定した場合、秒単位での間隔は2のX乗(秒)となります。

<例 4: 16秒、 6: 64秒、... 10: 1024秒>

数字は、4 ~ 17(16-131072秒)の間で設定出来ます。

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

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

時刻同期タイムアウト時間

サーバ応答の最大待ち時間を設定できます。

1-10秒の間で設定できます。

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

入力が終わりましたら「設定の保存」をクリックして設定完了です。

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

情報表示

クリックすると、現在のNTPサービスの動作状況を確認できます。

基準NTPサーバについて

基準となるNTPサーバには以下のようなものがあります。

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

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

NTPクライアントの設定方法

各ホスト/サーバをNTPクライアントとしてXR-640と時刻同期させる方法は、OSにより異なります。

Windows 9x/Me/NTの場合

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

Windows 2000の場合

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

Windows XPの場合

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

Macintoshの場合

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

Linuxの場合

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

第 20 章

VRRP サービス

第20章 VRRP サービス

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)を行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。

VRRPの設定
現在の状態

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	使用しない	使用しない	51	100		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	

使用するインターフェース

VRRPを作動させるインタフェースを選択します。

仮想MACアドレス

VRRP機能を運用するとき、仮想MACアドレスを使用する場合は「使用する」を選択します。「使用しない」設定の場合は、本装置の実MACアドレスを使ってVRRPが動作します。

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

ルータID

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

優先度

VRRPグループ内での優先度を設定します。数字が大きい方が優先度が高くなります。優先度の値が最も大きいものが、VRRPグループ内の「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行ってください。

ステータスの表示

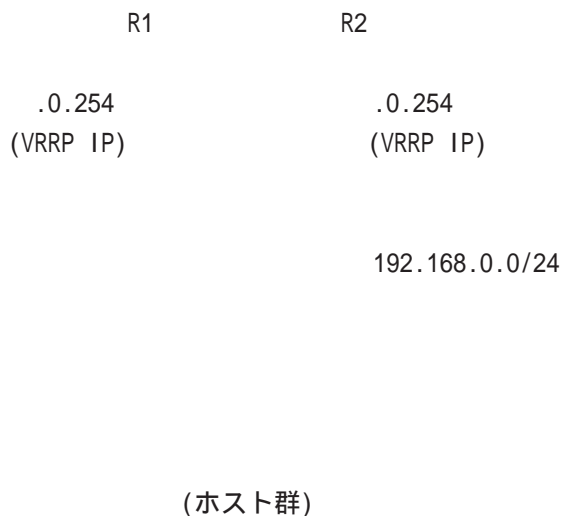
VRRP機能設定画面上部にある「現在の状態」をクリックすると、VRRP機能の動作状況を表示するウィンドウがポップアップします。

第20章 VRRP サービス

VRRP の設定例

下記のネットワーク構成でVRRPサービスを利用するときの設定例です。

ネットワーク構成



設定条件

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

ルータ「R1」の設定例

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
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

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
Ether 0	使用しない	1	50	192.168.0.254	1	指定しない	

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

第 21 章

アクセスサーバ機能

第21章 アクセスサーバ機能

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-640を会社に設置すると、モデムを接続した外出先のコンピュータから会社のLANに接続できます。これは、モバイルコンピューティングや在宅勤務を可能にします。クライアントはモデムによるPPP接続を利用できるものであれば、どのようなPCでもかまいません。この機能を使って接続したクライアントは、接続先のネットワークにハブで接続した場合と同じようにネットワークを利用できます。

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



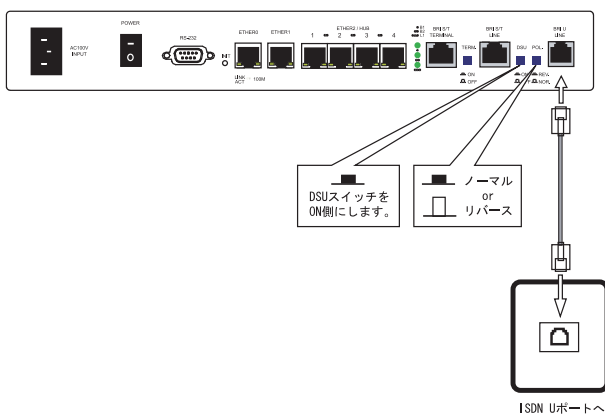
第21章 アクセスサーバ機能

BRI ポートを使った XR-640 と TA/DSU の接続

XR-640 内蔵の DSU を使う場合

- 1 本装置の電源をオフにします。
- 2 ISDN U点ジャックと本装置の「BRI U」ポートをモジュラーケーブルで接続します。モジュラーケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「ON」側にします。
- 4 本体背面の「POL.」スイッチを、ISDN 回線の極性に合わせます。
- 5 全ての接続が完了しましたら、本装置と TA の電源を投入してください。

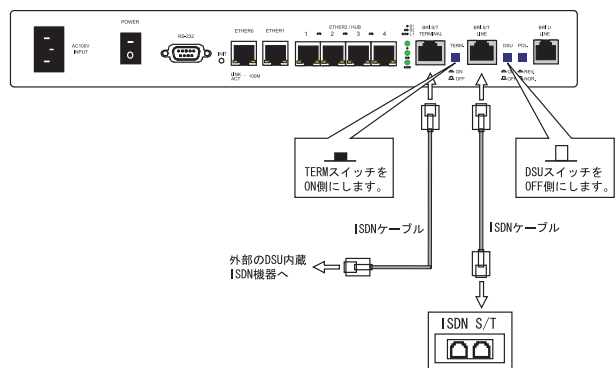
接続図



外付け TA に内蔵の DSU を使う場合

- 1 本装置の電源をオフにします。
- 2 外部の DSU と本装置の「BRI S/T LINE」ポートを ISDN 回線ケーブルで接続します。ISDN ケーブルは別途ご用意ください。
- 3 本体背面の「DSU」スイッチを「OFF」側にします。
- 4 本体背面の「TERM.」スイッチを「ON」側にします。
- 5 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。
- 6 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21章 アクセスサーバ機能

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	<input checked="" type="radio"/> 許可しない <input type="radio"/> 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	<input type="radio"/> 9600 <input type="radio"/> 19200 <input type="radio"/> 38400 <input checked="" type="radio"/> 57600 <input type="radio"/> 115200 <input type="radio"/> 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-640 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-640 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一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-640 とモデム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	<input checked="" type="radio"/> 許可しない <input type="radio"/> 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	<input checked="" type="radio"/> 許可しない <input type="radio"/> 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	<input checked="" type="radio"/> しない <input type="radio"/> する
本装置のホスト名	localhost

回線1 着信 / 回線2 着信

BRI 回線で着信したい場合は、「許可する」を選択します。

アクセスサーバ(本装置)の IP アドレス
リモートアクセスされた時の XR-640 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-640 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一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。

続けてユーザアカウントの設定を行います。

第21章 アクセスサーバ機能

アクセスサーバ機能の設定

ユーザアカウントの設定

設定画面の下側でユーザアカウントの設定を行います。

[1-10] [11-20] [21-30] [31-40] [41-50]

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	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="password"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

アカウント

パスワード

外部からリモートアクセスする場合の、ユーザアカウントとパスワードを登録してください。そのまま、リモートアクセス時のユーザアカウント・パスワードとなります。50アカウントまで登録しておけます。

アカウント毎に別IPを割り当てる場合

(BRI 回線着信時のみ)

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

削除

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

また「BRI 回線の設定」で「発信番号認証」を「する」にしている場合は下記の設定を行ってください。

No.	許可する着信番号	着信する回線	削除
1	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
2	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
3	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
4	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
5	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
6	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
7	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
8	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
9	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>
10	<input type="text"/>	すべて <input type="button" value="v"/>	<input type="checkbox"/>

許可する着信番号

発信者の電話番号を入力してください。

着信する回線

「すべて」、「回線1」、「回線2」の中から選択してください。

削除

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

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

アカウント設定上の注意

ユーザアカウント設定のユーザ名と、PPP/PPPoE設定の接続先設定で設定してあるユーザ名に同じユーザ名を登録した場合、そのユーザは**着信できません**。

ユーザ名が重複しないように設定してください。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

設定が反映されます。

スタティックルートについて

クライアントへのスタティックルートを設定する場合

アクセスサーバ回線でスタティックルートを設定する場合、インタフェース指定によるスタティックルート設定はできません。

「クライアントの IP アドレス」をゲートウェイアドレスとしたルートを設定してください。

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

< 設定例 >

- ・クライアントのネットワークアドレス
192.168.20.0/24
- ・BRI 回線 1 のクライアントの IP アドレス
192.168.251.171
- ・BRI 回線 2 のクライアントの IP アドレス
192.168.251.172

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

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

着信するインタフェース向けにスタティックルートを設定する場合

通常のスタティックルート設定では「インターフェース / ゲートウェイ」のどちらかひとつの項目のみ設定可能ですが、アクセスサーバ機能で着信するインタフェース向けにスタティックルート設定を行う場合は、以下の両項目ともに設定が必要になりますのでご注意ください。

< 設定例 >

- ・インターフェース
ppp6 (固定)
- ・ゲートウェイ
アクセスサーバ設定画面にて指定した着信時のクライアントの IP アドレス

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>	
1	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	ppp6	192.168.251.171	1
2	xxx.xxx.xxx.xxx	xxx.xxx.xxx.xxx	ppp6	192.168.252.172	2

第 22 章

スタティックルート

第22章 スタティックルート

スタティックルート設定

XR-640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。

[スタティックルート設定](#)
[経路情報表示](#)
No.1~16まで

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					<input type="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>
11					<input type="checkbox"/>
12					<input type="checkbox"/>
13					<input type="checkbox"/>
14					<input type="checkbox"/>
15					<input type="checkbox"/>
16					<input type="checkbox"/>

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。

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

スタティックルート設定画面インデックス
[001- 017- 033- 049- 065- 081- 097- 113-](#)
[129- 145- 161- 177- 193- 209- 225- 241-](#)

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>

29ビットマスクの場合 : **255.255.255.248**

単一ホストで指定した場合 : **255.255.255.255**

インターフェース/ゲートウェイ

ルーティングを行うインタフェース名、もしくは上位ルータのIPアドレスを設定します。

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

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

・インターフェース

“ppp6”

・ゲートウェイ

“クライアントに割り当てるIPアドレス”

通常は、インターフェース/ゲートウェイのどちらかのみ設定できます。

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

ディスタンス

経路選択の優先順位を指定します。1～255の間で指定します。値が低いほど優先度が高くなります。**スタティックルートのデフォルトディスタンス値は1です。**

ディスタンス値を変更することで、フローティングスタティックルート設定とすることも可能です。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

設定を挿入する

ルーティング設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行から行います。

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。

スタティックルート設定

設定を削除する

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

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。

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>
1	0.0.0.0	0.0.0.0	ge1	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 23 章

ソースルーティング機能

第23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いますが、ソースルーティングはパケットの送信元アドレスをもとにルーティングを行います。

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行って負荷分散が可能となります。

ソースルート設定は、Web 設定画面「ソースルート設定」で行います。

1 はじめに、ソースルートのテーブル設定を行います。Web 設定画面「ソースルート設定」を開き、「ソースルートのテーブル設定へ」のリンクをクリックしてください。

ソースルートのルール設定

[ソースルートのテーブル設定へ](#)

ソースルートのテーブル設定

[ソースルートのルール設定へ](#)

※NOが赤色の設定は現在無効です

テーブルNO	IP	DEVICE
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>

入力のやり直し

設定の保存

IP

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

DEVICE

デフォルトゲートウェイが存在する回線に接続しているインタフェースのインタフェース名を設定します(情報表示で確認できます。"eth0" や "ppp0" などの表記のものです)。省略することもできます。

設定後は「設定の保存」をクリックします。

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

ソースルートのルール設定

[ソースルートのテーブル設定へ](#)

※NOが赤色の設定は現在無効です

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	<input type="text"/>	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>

入力のやり直し

設定の保存

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。

ソースルーティング設定

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-640
のインタフェースが含まれていると、設定後は XR-
640 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-640
の設定画面にアクセスできなくなります。

第 24 章

NAT 機能

XR-640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-640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-640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となります。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、「インターフェース設定」もしくは「PPP/PPPoE接続」の接続設定画面で設定します。

送信元NAT機能

IPマスカレードとは異なり、プライベートアドレスをどのグローバルIPアドレスに変換するかをそれぞれ設定できるのが送信元NAT機能です。例えば、プライベートアドレスAをグローバルアドレスXに、プライベートアドレスBをグローバルアドレスYに、プライベートアドレスC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行うことで、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。

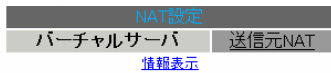
バーチャルサーバ設定

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行います。

256まで設定できます。「[バーチャルサーバ設定画面インデックス](#)」のリンクをクリックしてください。

設定方法

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



バーチャルサーバ機能を使って複数のグローバルIPアドレスを公開する場合は、[\[仮想インターフェースの設定画面\]](#)で公開用インターフェースの任意の仮想インターフェースごとに各グローバルIPアドレスを割り当ててください。
[No.1~16まで] ※No.赤色の設定は現在無効です

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			<input type="checkbox"/>
2			全て			<input type="checkbox"/>
3			全て			<input type="checkbox"/>
4			全て			<input type="checkbox"/>
5			全て			<input type="checkbox"/>
6			全て			<input type="checkbox"/>
7			全て			<input type="checkbox"/>
8			全て			<input type="checkbox"/>
9			全て			<input type="checkbox"/>
10			全て			<input type="checkbox"/>
11			全て			<input type="checkbox"/>
12			全て			<input type="checkbox"/>
13			全て			<input type="checkbox"/>
14			全て			<input type="checkbox"/>
15			全て			<input type="checkbox"/>
16			全て			<input type="checkbox"/>

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。

設定/削除の実行

バーチャルサーバ設定画面インデックス
001- 017- 033- 049- 065- 081- 097- 113-
129- 145- 161- 177- 193- 209- 225- 241-

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指定します。

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

入力が終わりましたら「設定/削除の実行」をクリックして設定完了です。

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

設定情報の確認

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

設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行から行います。

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

設定/削除の実行

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。

・バーチャルサーバの設定例

WWWサーバを公開する際のNAT設定例

NATの条件

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

LAN構成

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

設定画面での入力方法

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

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
1	192.168.0.1	211.xxx.xxx.102	tcp	80	eth1

設定の解説

No.1 :

WAN側から、211.xxx.xxx.102へポート80番(http)でアクセスがあれば、LAN内のサーバ192.168.0.1へ通す。(WAN側からTCPのポート80番以外でアクセスがあっても破棄される)

FTPサーバを公開する際のNAT設定例

NATの条件

- ・WAN側のグローバルアドレスにTCPのポート20番(ftpdata)、21番(ftp)でのアクセスを通す。
- ・LANからWANへのアクセスは自由にできる。
- ・WANはEther1、LANはEther0ポートに接続する。
- ・Ether1ポートはPPPoEでADSL接続する。

LAN構成

- ・LAN側ポートのIPアドレス「192.168.0.254」
- ・FTPサーバのアドレス「192.168.0.2」
- ・グローバルアドレスは「211.xxx.xxx.103」のみ

設定画面での入力方法

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

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
1	192.168.0.2	211.xxx.xxx.103	tcp	20	ppp0
2	192.168.0.2	211.xxx.xxx.103	tcp	21	ppp0

設定の解説

No.1 :

WAN側から、211.xx.xx.103へポート20番(ftpdata)でアクセスがあれば、LAN内のサーバ192.168.0.2へ通す。

No.2 :

WAN側から、211.xxx.xxx.103へポート21番(ftp)でアクセスがあれば、LAN内のサーバ192.168.0.2へ通す。

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくにステートフルパケットインスペクション機能を使っている場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

・ バージョナルサーバの設定例

PPTP サーバを公開する際の NAT 設定例

NAT の条件

- ・ WAN 側のグローバルアドレスにプロトコル「gre」と TCP のポート番号 1723 を通す。
- ・ WAN は Ether1、LAN は Ether0 ポートに接続する。
- ・ WAN 側ポートは PPPoE で ADSL 接続する。

LAN 構成

- ・ LAN 側ポートの IP アドレス「192.168.0.254」
- ・ PPTP サーバのアドレス「192.168.0.3」
- ・ 割り当てられるグローバルアドレスは 1 つのみ。

設定画面での入力方法

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

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
1	192.168.0.3		tcp	1723	ppp0
2	192.168.0.3		gre		ppp0

バーチャルサーバ設定以外に、適宜パケットフィルタ設定を行ってください。とくにステートフルパケットインスペクション機能を使っている場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

バーチャルサーバの設定例

DNS、メール、WWW、FTPサーバを公開する際の
NAT設定例(複数グローバルアドレスを利用)

NATの条件

- WAN側からは、LAN側のメール、WWW、FTPサーバへアクセスできるようにする。
- LAN内のDNSサーバがWANと通信できるようにする。
- LANからWANへのアクセスは自由にできる。
- WANはEther1、LANはEther0ポートに接続。
- グローバルアドレスは複数使用する。

LAN構成

- LAN側ポートのIPアドレス「192.168.0.254」
- WWWサーバのアドレス「192.168.0.1」
- 送受信メールサーバのアドレス「192.168.0.2」
- FTPサーバのアドレス「192.168.0.3」
- DNSサーバのアドレス「192.168.0.4」
- WWWサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.104」
- 送受信メールサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.105」
- FTPサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.106」
- DNSサーバに対応させるグローバルIPアドレスは「211.xxx.xxx.107」

設定画面での入力方法

1 まず最初に、使用する複数のグローバルアドレスを、仮想インターフェースとして登録します。Web設定画面にある「仮想インターフェース設定」を開き、以下のように設定しておきます。

No.	インターフェース	仮想I/F番号	IPアドレス	ネットマスク
1	eth1	1	211.xxx.xxx.104	255.255.255.248
2	eth1	2	211.xxx.xxx.105	255.255.255.248
3	eth1	3	211.xxx.xxx.106	255.255.255.248
4	eth1	4	211.xxx.xxx.107	255.255.255.248

2 IPマスカレードを有効にします。

「第5章 インターフェース設定」を参照してください。

3 「バーチャルサーバ設定」で以下の様に設定してください。

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
1	192.168.0.1	211.xxx.xxx.104	tcp	80	eth1
2	192.168.0.2	211.xxx.xxx.105	tcp	25	eth1
3	192.168.0.2	211.xxx.xxx.105	tcp	110	eth1
4	192.168.0.3	211.xxx.xxx.106	tcp	21	eth1
5	192.168.0.3	211.xxx.xxx.106	tcp	20	eth1
6	192.168.0.4	211.xxx.xxx.107	tcp	53	eth1
7	192.168.0.4	211.xxx.xxx.107	udp	53	eth1

設定の解説

No.1

WAN側から211.xxx.xxx.104へポート80番(http)でアクセスがあれば、LAN内のサーバ192.168.0.1へ通す。

No.2、3

WAN側から211.xxx.xxx.105へポート25番(smtp)か110番(pop3)でアクセスがあれば、LAN内のサーバ192.168.0.2へ通す。

No.4、5

WAN側から211.xxx.xxx.106へポート20番(ftpdata)か21番(ftp)でアクセスがあれば、LAN内のサーバ192.168.0.3へ通す。

No.6、7

WAN側から211.xxx.xxx.107へ、tcpポート53番(domain)かudpポート53番(domain)でアクセスがあれば、LAN内のサーバ192.168.0.4へ通す。

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

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

送信元 NAT の設定例

送信元 NAT 設定では、LAN 側のコンピュータのアドレスをどのグローバルアドレスに変換するかを個々に設定することができます。

No.	送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
1	192.168.0.1	61.xxx.xxx.101	ppp0
2	192.168.0.2	61.xxx.xxx.102	ppp0
3	192.168.10.0/24	61.xxx.xxx.103	ppp0

例えば上記のような送信元 NAT 設定を行うと、

- ・送信元アドレス 192.168.0.1 を 61.xxx.xxx.101 に変換して WAN へアクセスする
- ・送信元アドレス 192.168.0.2 を 61.xxx.xxx.102 に変換して WAN へアクセスする
- ・送信元アドレスとして 192.168.10.0/24 からのアクセスを 61.xxx.xxx.103 に変換して WAN へアクセスする

という設定になります。

送信元のアドレスは、ホスト単位かネットワーク単位で指定できます。範囲指定はできません。ネットワークで指定するときは、以下のように設定してください。

<設定例> 192.168.254.0/24

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

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

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

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

第 25 章

パケットフィルタリング機能

第 25 章 パケットフィルタリング機能

機能の概要

XR-640 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-640 自身が受信するパケットを制限する。
- ・XR-640 自身から送信するパケットを制限する。
- ・ゲートウェイ認証機能を使用しているときにアクセス可能にする。

またフィルタリングは以下の情報に基づいて条件を設定することができます。

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

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

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

XR-640のフィルタリング機能について

XR-640は、以下の4つの基本ルールについてフィルタリングの設定を行います。

- ・入力(input)
- ・転送(forward)
- ・出力(output)
- ・ゲートウェイ認証フィルタ(authgw)

入力(input)フィルタ

外部からXR-640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-640へのアクセスについて制御したい場合には、この入力ルールにフィルタ設定を行います。

転送(forward)フィルタ

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-640で内部転送する(XR-640がルーティングする)アクセスを制御する場合には、この転送ルールにフィルタ設定を行います。

出力(output)フィルタ

XR-640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行います。

パケットが「転送されるもの」か「XR-640自身へのアクセス」か「XR-640自身からのアクセス」かをチェックしてそれぞれのルールにあるフィルタ設定を実行します。

ゲートウェイ認証(authgw)フィルタ

「ゲートウェイ認証機能」を使用しているときに設定するフィルタです。

ゲートウェイ認証を必要とせずに外部と通信可能にするフィルタ設定を行います。ゲートウェイ認証機能については「第31章 ゲートウェイ認証機能」をご覧ください。

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

フィルタの初期設定について

本装置の工場出荷設定では、「入力フィルタ」と「転送フィルタ」において、以下のフィルタ設定がセットされています。

- ・NetBIOSを外部に送出不いフィルタ設定
- ・外部からUPnPで接続されないようにするフィルタ設定

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

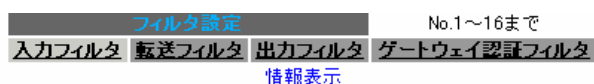
第25章 パケットフィルタリング機能

パケットフィルタリングの設定

入力・転送・出力・ゲートウェイ認証フィルタの4種類ありますが、設定方法はすべて同様となります。設定可能な各フィルタの最大数は256です。各フィルタ設定画面の最下部にある「[フィルタ設定画面インデックス](#)」のリンクをクリックしてください。

設定方法

Web 設定画面にログインします。「フィルタ設定」「入力フィルタ」「転送フィルタ」「出力フィルタ」「ゲートウェイ認証フィルタ」のいずれかをクリックして、以下の画面から設定します。



※No.赤色の設定は現在無効です

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	LOG	削除	No.
1	eth0	パケット受信時	破棄	tcp				137:139	<input type="checkbox"/>	<input type="checkbox"/>	1
2	eth0	パケット受信時	破棄	udp				137:139	<input type="checkbox"/>	<input type="checkbox"/>	2
3	eth0	パケット受信時	破棄	tcp		137			<input type="checkbox"/>	<input type="checkbox"/>	3
4	eth0	パケット受信時	破棄	udp		137			<input type="checkbox"/>	<input type="checkbox"/>	4
5	eth1	パケット受信時	破棄	udp				1900	<input type="checkbox"/>	<input type="checkbox"/>	5
6	ppp0	パケット受信時	破棄	udp				1900	<input type="checkbox"/>	<input type="checkbox"/>	6
7	eth1	パケット受信時	破棄	tcp				5000	<input type="checkbox"/>	<input type="checkbox"/>	7
8	ppp0	パケット受信時	破棄	tcp				5000	<input type="checkbox"/>	<input type="checkbox"/>	8
9	eth1	パケット受信時	破棄	tcp				2869	<input type="checkbox"/>	<input type="checkbox"/>	9
10	ppp0	パケット受信時	破棄	tcp				2869	<input type="checkbox"/>	<input type="checkbox"/>	10
11		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	11
12		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	12
13		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	13
14		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	14
15		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	15
16		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	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。

		パケット受信時	許可	全て					<input type="checkbox"/>	<input type="checkbox"/>	
--	--	---------	----	----	--	--	--	--	--------------------------	--------------------------	--

設定/削除の実行

入力フィルタ設定画面インデックス
[001- 017- 033- 049- 065- 081- 097- 113-](#)
[129- 145- 161- 177- 193- 209- 225- 241-](#)
 (画面は「入力フィルタ」です)

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

方向
 ポートがパケットを受信するときにフィルタリングするか、送信するときにフィルタリングするかを選択します。

入力フィルタでは「パケット受信時」、出力フィルタでは「パケット送信時」のみとなります。

第 25 章 パケットフィルタリング機能

．パケットフィルタリングの設定

動作

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

プロトコル

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

送信元アドレス

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

<入力例>

単一の IP アドレスを指定する：

192.168.253.19

192.168.253.19/32

(“アドレス/32”の書式 “/32”は省略可能です。)

ネットワーク単位で指定する：

192.168.253.0/24

(“ネットワークアドレス/マスクビット値”の書式)

送信元ポート

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

<入力例>

ポート 1024 番から 65535 番を指定する場合。

1024:65535

ポート番号を指定するときは、プロトコルもあわせて選択しておかなければなりません。

(「全て」のプロトコルを選択して、ポート番号を指定することはできません。)

あて先アドレス

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

入力方法は、送信元アドレスと同様です。

あて先ポート

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

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行います。



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25章 パケットフィルタリング機能

．パケットフィルタリングの設定例

インターネットからLANへのアクセスを破棄する設定

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

フィルタの条件

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

LAN構成

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

設定画面での入力方法

「入力フィルタ」で以下のように設定します。

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

「転送フィルタ」で以下のように設定します。

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

フィルタの解説

「入力フィルタ」「転送フィルタ」

No.1、2：

WANから来る、あて先ポートが1024から65535の packets を通す。

No.3：

WANから来る、ICMP packets を通す。

No.4：

上記の条件に合致しない packets を全て破棄する。

第25章 パケットフィルタリング機能

パケットフィルタリングの設定例

WWWサーバを公開する際のフィルタ設定例

フィルタの条件

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

LAN構成

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

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

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

フィルタの解説

No.1 :

192.168.0.1のサーバにHTTPのパケットを通す。

No.2、3 :

WANから来る、あて先ポートが1024から65535のパケットを通す。

No.4 :

上記の条件に合致しないパケットを全て破棄する。

FTPサーバを公開する際のフィルタ設定例

フィルタの条件

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

LAN構成

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

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

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

フィルタの解説

No.1 :

192.168.0.2のサーバにftpのパケットを通す。

No.2 :

192.168.0.2のサーバにftpdataのパケットを通す。

No.3、4 :

WANから来る、あて先ポートが1024から65535のパケットを通す。

No.5 :

上記の条件に合致しないパケットを全て破棄する。

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

第25章 パケットフィルタリング機能

．パケットフィルタリングの設定例

WWW、FTP、メール、DNSサーバを公開する際の フィルタ設定例

フィルタの条件

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

LAN構成

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

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

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

フィルタの解説

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

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

第25章 パケットフィルタリング機能

パケットフィルタリングの設定例

NetBIOSパケットが外部へ出るのを防止する フィルタ設定

フィルタの条件

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

LAN構成

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

設定画面での入力方法

「入力フィルタ」

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

「転送フィルタ」

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

フィルタの解説

「入力フィルタ」「転送フィルタ」

No.1 :

あて先ポートがtcpの137から139のパケットをEther0ポートで破棄する。

No.2 :

あて先ポートがudpの137から139のパケットをEther0ポートで破棄する。

No.3 :

送信先ポートがtcpの137のパケットをEther0ポートで破棄する。

No.4 :

送信先ポートがudpの137のパケットをEther0ポートで破棄する。

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

フィルタの条件

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

LAN構成

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

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

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

フィルタの解説

No.1 :

210.xxx.xxx.32/32 (210.xxx.xxx.32/28のネットワークアドレス)宛てのパケットを受け取らない。

No.2 :

210.xxx.xxx.47/32 (210.xxx.xxx.32/28のネットワークのブロードキャストアドレス)宛てのパケットを受け取らない。

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

第25章 パケットフィルタリング機能

パケットフィルタリングの設定例

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

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

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

フィルタの解説

No.1、2、3：

WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。

WAN 上にプライベートアドレスは存在しない。

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

外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			
4	ppp0	パケット受信時	破棄	全て			202.xxx.xxx.112/28	

「出力フィルタ設定」で以下のように設定します。

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

フィルタの解説

「入力フィルタ」

No.1、2、3：

WAN から来る、送信元 IP アドレスがプライベートアドレスのパケットを受け取らない。

WAN 上にプライベートアドレスは存在しない。

No.4：

WANからのブロードキャストパケットを受け取らない。 smurf 攻撃の防御

「出力フィルタ」No1、2、3：

送信元 IP アドレスが不正なパケットを送出しない。

WAN 上にプライベートアドレスは存在しない。

第25章 パケットフィルタリング機能

．パケットフィルタリングの設定例

PPTPを通すためのフィルタ設定

フィルタの条件

- ・WAN側からのPPTPアクセスを許可する。

LAN構成

- ・WAN側はPPPoE回線に接続する。

設定画面での入力方法

「転送フィルタ設定」で以下のように設定します。

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

フィルタの解説

PPTPでは以下のプロトコル・ポートを使って通信します。

- ・プロトコル「GRE」
- ・プロトコル「tcp」のポート「1723」

したがって、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行っています。

第 25 章 パケットフィルタリング機能

外部から設定画面にアクセスさせる設定

以下は、PPPoE で接続した場合の設定方法です。

1 まず設定画面にログインし、パケットフィルタ設定の「入力フィルタ」画面を開きます。

2 「入力フィルタ」設定の中で、以下のような設定を追加してください。

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

上記設定では、221.xxx.xxx.105 の IP アドレスを持つホストだけが、外部から本装置の設定画面へのアクセスが可能になります。

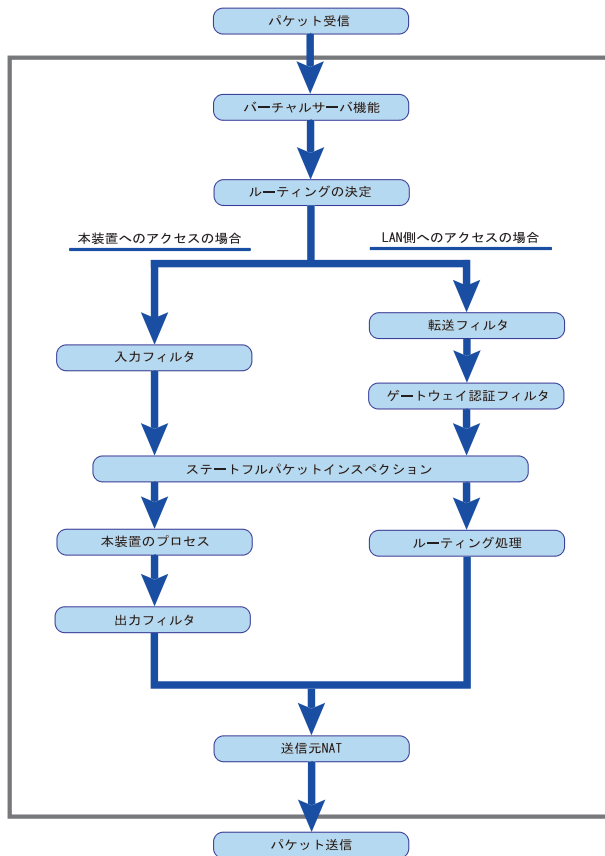
また「送信元アドレス」を空欄にすると、すべてのインターネット上のホストから、本装置にアクセス可能になります。

(セキュリティ上たいへん危険ですので、この設定は推奨いたしません。)

第25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-640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を行うとします。)

- 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-640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-640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。その場合のあと先アドレスは「(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-640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せん。
- 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25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25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 WIN-DOW=48000 ACK URGP=0
```

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

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

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

第 26 章

スケジュール設定

第26章 スケジュール設定

スケジュール機能の設定方法

XR-640には、主回線を接続または切断する時間を管理するスケジュール機能があります。

スケジュールの設定は10個まで設定できます

Web設定画面の「スケジュール設定」をクリックします。

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

2007年 1月 1日 以降

2007年 1月 1日 まで

2007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26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。

入力が終わりましたら、「設定 / 削除の実行」をクリックします。

設定内容は画面上のスケジュール設定欄に反映されます。

スケジュール設定欄の項目について

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

< 例 >

スケジュール設定

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

上の画面で「時間」項目をクリックします。

下の画面のように、「時間」の早い順番に並べ替えられます。

スケジュール設定

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

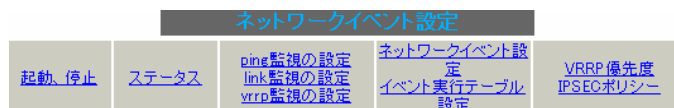
第27章

ネットワークイベント機能

第27章 ネットワークイベント機能

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。

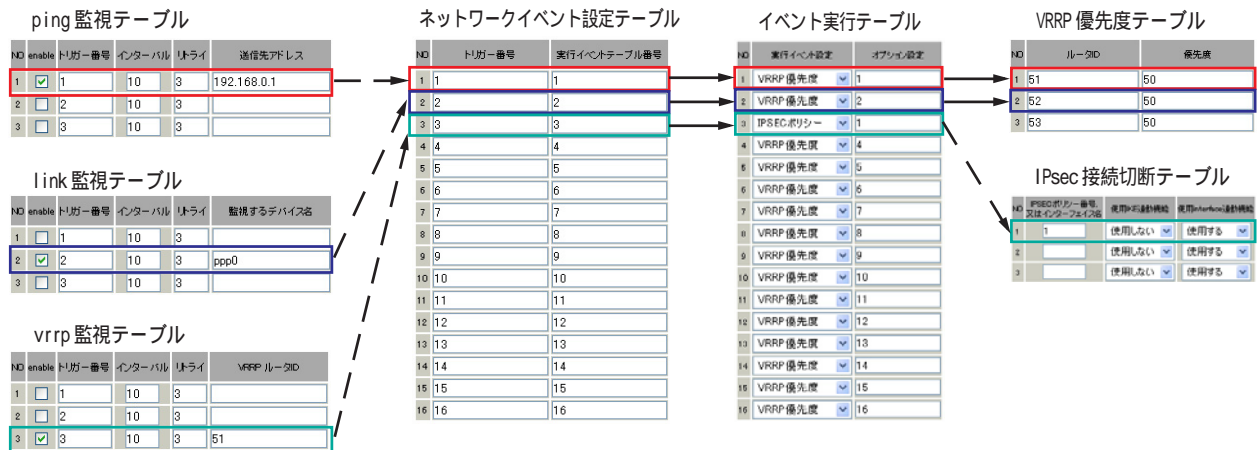
例えば、vrrp 監視と連動して、2台のVRRP ルータのマスタールータの切り替わりに応じて、IPsec 接続を繋ぎかえる、といった使い方ができます。

第27章 ネットワークイベント機能

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。



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「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。

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「イベント実行テーブル」のインデックス番号になります。

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「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「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、テーブルのインデックス番号になります。

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。

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。

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	<input type="checkbox"/>	1	10	3	
2	<input type="checkbox"/>	2	10	3	
3	<input type="checkbox"/>	3	10	3	
4	<input type="checkbox"/>	4	10	3	
5	<input type="checkbox"/>	5	10	3	
6	<input type="checkbox"/>	6	10	3	
7	<input type="checkbox"/>	7	10	3	
8	<input type="checkbox"/>	8	10	3	
9	<input type="checkbox"/>	9	10	3	
10	<input type="checkbox"/>	10	10	3	
11	<input type="checkbox"/>	11	10	3	
12	<input type="checkbox"/>	12	10	3	
13	<input type="checkbox"/>	13	10	3	
14	<input type="checkbox"/>	14	10	3	
15	<input type="checkbox"/>	15	10	3	
16	<input type="checkbox"/>	16	10	3	

入力のやり直し

設定の保存

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せん。

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。

各トリガテーブルの設定

Link 監視の設定方法

設定画面上部の「Link 監視の設定」をクリックして、以下の画面から設定します。

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	<input type="checkbox"/>	1	10	3	
2	<input type="checkbox"/>	2	10	3	
3	<input type="checkbox"/>	3	10	3	
4	<input type="checkbox"/>	4	10	3	
5	<input type="checkbox"/>	5	10	3	
6	<input type="checkbox"/>	6	10	3	
7	<input type="checkbox"/>	7	10	3	
8	<input type="checkbox"/>	8	10	3	
9	<input type="checkbox"/>	9	10	3	
10	<input type="checkbox"/>	10	10	3	
11	<input type="checkbox"/>	11	10	3	
12	<input type="checkbox"/>	12	10	3	
13	<input type="checkbox"/>	13	10	3	
14	<input type="checkbox"/>	14	10	3	
15	<input type="checkbox"/>	15	10	3	
16	<input type="checkbox"/>	16	10	3	

入力のやり直し

設定の保存

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ください。

最後に「設定の保存」をクリックして設定完了です。

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	<input type="checkbox"/>	1	10	3	
2	<input type="checkbox"/>	2	10	3	
3	<input type="checkbox"/>	3	10	3	
4	<input type="checkbox"/>	4	10	3	
5	<input type="checkbox"/>	5	10	3	
6	<input type="checkbox"/>	6	10	3	
7	<input type="checkbox"/>	7	10	3	
8	<input type="checkbox"/>	8	10	3	
9	<input type="checkbox"/>	9	10	3	
10	<input type="checkbox"/>	10	10	3	
11	<input type="checkbox"/>	11	10	3	
12	<input type="checkbox"/>	12	10	3	
13	<input type="checkbox"/>	13	10	3	
14	<input type="checkbox"/>	14	10	3	
15	<input type="checkbox"/>	15	10	3	
16	<input type="checkbox"/>	16	10	3	

入力のやり直し

設定の保存

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。

第27章 ネットワークイベント機能

各トリガテーブルの設定

各種監視設定の起動と停止方法

各監視機能（ping監視、link監視、vrrp監視）を有効にするには、Web画面「ネットワークイベント設定」画面「起動、停止」の以下のネットワークイベントサービス設定画面で、「起動」ボタンにチェックを入れ、「動作変更」をクリックしてサービスを起動してください。

また設定の変更、追加、削除を行った場合は、サービスの再起動を行ってください。

ネットワークイベント設定				
起動、停止	ステータス	ping監視の設定 link監視の設定 vrrp監視の設定	ネットワークイベント設定 イベント実行テーブル設定	VRRP優先度 IPSECポリシー

ネットワークイベントサービス設定

※各種設定は項目名をクリックして下さい。

ネットワークイベント	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
ping監視	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
link監視	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
vrrp監視	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動

動作変更

動作変更と再起動

(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。

実行イベントテーブルの設定

ネットワークイベント設定テーブルの設定

設定画面上部の「ネットワークイベント設定」をクリックして、以下の画面から設定します。

(「イベント実行テーブル設定」画面のリンクをクリックしても以下の画面を開くことができます。)

ネットワークイベント設定

[イベント実行テーブル設定](#)

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

入力のやり直し

設定の保存

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。

(「ネットワークイベント設定」画面のリンクをクリックしても以下の画面を開くことができます。)

イベント実行テーブル設定

[ネットワークイベント設定へ](#)

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	VRRP 優先度 ▼	3
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

入力のやり直し

設定の保存

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。

・ 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。

最後に「設定の保存」をクリックして設定完了です。

VRRP 優先度変更設定

現在のVRRPの状態

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

入力のやり直し

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 の間で設定してください。

なお、トリガ復旧時には「VRRP サービス」で設定されている元の値に戻ります。

実行イベントのオプション設定

IPSEC 接続切断設定 テーブルの設定

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

IPSEC 接続切断設定

現在のIPSECの状態

NO	IPSECポリシー番号、 又はインターフェース名	使用IKE連動機能	使用interface連動機能
1	<input type="text"/>	使用しない ▼	使用する ▼
2	<input type="text"/>	使用しない ▼	使用する ▼
3	<input type="text"/>	使用しない ▼	使用する ▼
4	<input type="text"/>	使用しない ▼	使用する ▼
5	<input type="text"/>	使用しない ▼	使用する ▼
6	<input type="text"/>	使用しない ▼	使用する ▼
7	<input type="text"/>	使用しない ▼	使用する ▼
8	<input type="text"/>	使用しない ▼	使用する ▼
9	<input type="text"/>	使用しない ▼	使用する ▼
10	<input type="text"/>	使用しない ▼	使用する ▼
11	<input type="text"/>	使用しない ▼	使用する ▼
12	<input type="text"/>	使用しない ▼	使用する ▼
13	<input type="text"/>	使用しない ▼	使用する ▼
14	<input type="text"/>	使用しない ▼	使用する ▼
15	<input type="text"/>	使用しない ▼	使用する ▼
16	<input type="text"/>	使用しない ▼	使用する ▼

入力のやり直し

設定の保存

IPSEC ポリシー番号、又はインターフェース名
トリガ検知時に切断する IPsec ポリシーの番号、または IPsec インタフェース名を指定します。

ポリシー番号は、範囲で指定することもできます。

<例> IPsec ポリシー 1 から 20 を切断する **1:20**

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

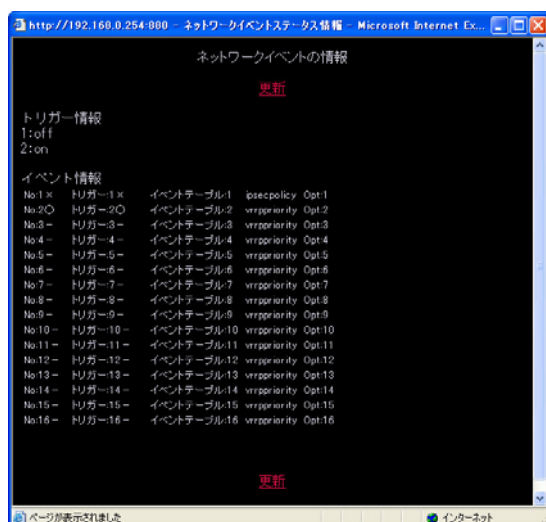
現在の設定状態の確認

VRRP 優先度変更設定画面の上部の、「現在の IPSEC の状態」リンクをクリックすると、「VRRP の情報」を表示するウィンドウがポップアップします。

IPSEC 接続切断設定画面の上部の、「現在の IPSEC の状態」リンクをクリックすると、「IPSEC の情報」を表示するウィンドウがポップアップします。

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。

“x”の表示は、トリガ検知し、イベントを実行している状態を表します。

“ ”の表示は、トリガ検知がなく、イベントが実行されていない状態を表します。

“-”の表示は、無効なイベントです。

・トリガー

イベント実行の条件となるトリガ番号とその状態を表します。

・イベントテーブル

左からイベント実行テーブルのインデックス番号、実行イベント種別、オプションテーブル番号を表します。

第 28 章

仮想インターフェース機能

第28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、仮想インタフェースを設定します。

128まで設定できます。「[仮想インターフェース設定画面インデックス](#)」のリンクをクリックしてください。

設定方法

Web 設定画面「仮想インターフェース」をクリックして、以下の画面から設定します。

仮想インターフェース設定

バーチャルサーバ機能や送信元NAT機能を使って複数のグローバルIPアドレスを公開する際に使用します。公開する側のインタフェースを指定して、任意(0-127)の仮想I/F番号を指定し、各々に公開するグローバルIPアドレスとそのネットマスク値を設定して下さい。

※No.赤色の設定は現在無効です

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	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

[仮想インターフェース設定画面インデックス](#)
[001-](#) [017-](#) [033-](#) [049-](#) [065-](#) [081-](#) [097-](#) [113-](#)

設定/削除の実行

インターフェース

仮想インタフェースを作成するインタフェース名を指定します。

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

仮想 I/F 番号

作成するインタフェースの番号を指定します。

0 ~ 127 の間で設定します。

IP アドレス

作成するインタフェースの IP アドレスを指定します。

ネットマスク

作成するインタフェースのネットマスクを指定します。

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 29 章

GRE 設定

第 29 章 GRE 設定

GRE の設定

GRE は Generic Routing Encapsulation の略で、リモート側にあるルータまで仮想的なポイントツーポイント リンクを張って、多種プロトコルのパケットを IP トンネルにカプセル化するプロトコルです。

また IPsec トンネル内に GRE トンネルを生成することもできますので、GRE を使用する場合でもセキュアな通信を確立することができます。

GRE の設定

設定画面「GRE 設定」 [GRE インタフェース設定:] のインタフェース名「GRE1」～「GRE64」をクリックして設定します。

GRE の設定								
GRE 設定 Index: 一覧表示 [1-32] [33-64]								
GRE インタフェース 設定	GRE1	GRE2	GRE3	GRE4	GRE5	GRE6	GRE7	GRE8
	GRE9	GRE10	GRE11	GRE12	GRE13	GRE14	GRE15	GRE16
	GRE17	GRE18	GRE19	GRE20	GRE21	GRE22	GRE23	GRE24
	GRE25	GRE26	GRE27	GRE28	GRE29	GRE30	GRE31	GRE32

GRE1 設定	
インタフェースアドレス	<input type="text" value=""/> (例192.168.0.1/30)
リモート(宛先)アドレス	<input type="text" value=""/> (例192.168.1.1)
ローカル(送信元)アドレス	<input type="text" value=""/> (例192.168.2.1)
PEERアドレス	<input type="text" value=""/> (例192.168.0.2/30)
TTL	<input type="text" value="255"/> (1-255)
MTU	<input type="text" value="1476"/> (最大値 1500)
Path MTU Discovery	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
ICMP AddressMask Request	<input checked="" type="radio"/> 応答する <input type="radio"/> 応答しない
TOS設定 (ECN Field設定不可)	<input checked="" type="radio"/> TOS値の指定 <input type="text" value=""/> (0x0-0xfc) <input type="radio"/> inherit(TOS値のコピー)
GREoverIPsec	<input type="radio"/> 使用する <input type="text" value="ipsec0"/> <input checked="" type="radio"/> Routing Tableに依存
IDキーの設定	<input type="text" value=""/> (0-4294967295)
End-to-End Checksumming	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 MSS値 <input type="text" value="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。)

現在の状態 Tunnel is down, Link is down

インタフェースアドレス

GRE トンネルを生成するインタフェースの仮想アドレスを設定します。任意で指定します。

リモート(宛先)アドレス

GRE トンネルのエンドポイントの IP アドレス(対向側装置の WAN 側 IP アドレス)を設定します。

ローカル(送信元)アドレス

本装置の WAN 側 IP アドレスを設定します。

PEER アドレス

GRE トンネルを生成する対向側装置のインタフェースの仮想アドレスを設定します。「インタフェースアドレス」と同じネットワークに属するアドレスを指定してください。

TTL

GRE パケットの TTL 値を設定します。

MTU

MTU 値を設定します。最大値は 1500byte です。

Path MTU Discovery

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

Path MTU Discovery を「無効」にした場合、TTL は常にカプセル化されたパケットの TTL 値がコピーされます。従って、GRE 上で OSPF を動かす場合には、TTL が 1 に設定されてしまうため、Path MTU Discovery を有効にしてください。

ICMP AddressMask Request

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

TOS 設定

GRE パケットの TOS 値を設定します。

GRE の設定

GREover IPsec

IPsec を使用して GRE パケットを暗号化する場合に「使用する」を選択します。またこの場合には別途、IPsec の設定が必要です。

Routing Table に合わせて暗号化したい場合には「Routing Table に依存」を選択してください。ルートが IPsec の時は暗号化、IPsec でない時は暗号化しません。

ID キーの設定

この機能を有効にすると、KEY Field の 4byte が GRE ヘッダに付与されます。

End-to-End Checksumming

チェックサム機能の有効 / 無効を選択します。この機能を有効にすると、

checksum field (2byte) + offset (2byte) の計 4byte が GRE パケットに追加されます。

MSS 設定

GRE トンネルに対して、clamp to MSS 機能を有効にしたり、MSS 値の設定が可能です。

入力後は「追加 / 変更」ボタンをクリックします。直ちに設定が反映され、GRE が実行されます。

GRE の削除

「GRE インタフェース設定:GRE1」～「GRE64」の画面の「削除」ボタンをクリックすると、その設定に該当する GRE トンネルが無効化されます(設定自体は保存されています)。

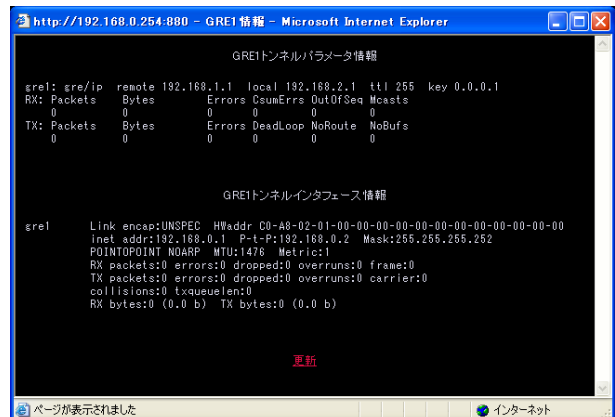
再度有効とするときは「追加 / 変更」ボタンをクリックしてください。

GRE の状態表示

「GRE インタフェース設定:GRE1」～「GRE64」の画面下部にある「現在の状態」では GRE の動作状況が表示されます。

現在の状態 Tunnel is down, Link is down

また、実行しているインタフェースでは、「現在の状態」リンクをクリックするとウィンドウポップアップして、「GRE1 トンネルパラメータ情報」と「GRE1 トンネルインタフェース情報」が表示されます。



GRE の再設定

GRE 設定を行うと、設定内容が一覧表示されます。

GRE 一覧表示

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

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 30 章

QoS 機能

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行います。

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

クラスフル/クラスレスなキューイング

キューイングには、クラスフルなものと同様にクラスレスなものがあります。

クラスレス キューイング

クラスレスなキューイングは、内部に設定可能なトラフィック分割用のバンド(クラス)を持たず、到着するすべてのトラフィックを同等に取り扱います。

PFIFO、TBF、SFQがクラスレスなキューイングです。

クラスフル キューイング

クラスフルなキューイングでは、内部に複数のクラスを持ち、選別器(クラス分けフィルタ)によって、パケットを送り込むクラスを決定します。各クラスはそれぞれに帯域を持つため、クラス分けすることで帯域制御ができるようになります。またキューイング方式によっては、あるクラスがさらに自分の配下にクラスを持つこともできます。さらに、各クラス内でそれぞれキューイング方式を決めることもできます。

PQとCBQがクラスフルなキューイングです。

QoS について

1. SFQ

SFQはパケットの流れ(トラフィック)を整形しません。パケットを送り出す順番を決めるだけです。

SFQでは、トラフィックを多数の内部キューに分割して収納します。そして各キューをラウンドロビンで回り、各キューからパケットをFIFOで順番に送信していきます。

ラウンドロビンで順番にトラフィックが送信されることから、ある特定のトラフィックが他のトラフィックを圧迫してしまうことがなくなり、どのトラフィックも公平に送信されるようになります(複数のトラフィックを平均化できる)。

整形とは、トラフィック量が一定以上にならないように転送速度を調節することを指します。「シェーピング」とも呼ばれます。

2. PFIFO

もっとも単純なキューイング方式です。あらかじめキューのサイズを決定しておき、どのパケットも区別なくキューに収納していきます。キューからパケットを送信するとき、送信するパケットはFIFOにしたがって選別されます。

キューのサイズを超えてパケットが到着したとき、超えた分のパケットは全て破棄されてしまいます。

キューのサイズが大きすぎると、キューイングによる遅延が発生する可能性があります。

キューとは、データの入り口と出口を一つだけ持つバッファのことを指します。

FIFOとは「First In First Out」の略で、「最初に入ったものが最初に出る」、つまり最も古いものが最初に取り出されることを指します。

QoS について

3. TBF

帯域制御方法の1つです。

トークンパケットにトークンを、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)。

またパケット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パケット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パケットのトークンがすぐになくなってしまい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となります。

4. CBQ

CBQは帯域制御の1つです。複数のクラスを作成しクラスごとに帯域幅を設定することで、パケットの種類に応じて使用できる帯域を割り当てる方式です。

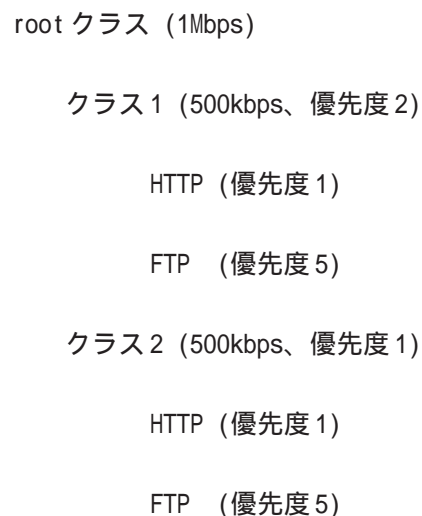
CBQにおけるクラスは、階層的に管理されます。最上位には root クラスが置かれ、利用できる総帯域幅を定義しておきます。root クラスの下に子クラスが置かれ、それぞれの子クラスには root で定義した総帯域幅の一部を利用可能帯域として割り当てます。子クラスの下には、さらにクラスを置くこともできます。

各クラスへのパケットの振り分けは、フィルタ (クラス分けフィルタ) の定義に従っておこなわれます。

各クラスには帯域幅を割り当てます。兄弟クラス間で割り当てている帯域幅の合計が、上位クラスで定義している帯域幅を超えないように設計しなければなりません。

また、それぞれのクラスには優先度を割り振り、優先度に従ってパケットを送信していきます。

<クラス構成図(例)>



(次ページに続きます)

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行うこともできます(クラスキューイング)。

CBQの特徴として、各クラス内において、あるクラスが兄弟クラスから帯域幅を借りることができます。たとえば図のクラス1において、トラフィックが500kbpsを超えていて、且つ、クラス2の使用帯域幅が500kbps以下の場合に、クラス1はクラス2で余っている帯域幅を借りてパケットを送信することができます。

5.PQ

PQは優先制御の1つです。トラフィックのシェーピングは行いません。

PQでは、パケットを分類して送り込むクラスに優先順位をつけておきます。そしてフィルタによってパケットをそれぞれのクラスに分類したあと、優先度の高いクラスから優先的にパケットを送信します。なお、クラス内のパケットはFIFOで取り出されます。

優先度の高いクラスに常にパケットがキューイングされているときには、より優先度の低いクラスからはパケットが送信されなくなります。

・ QoS機能の各設定画面について

本装置では下記の各種設定画面で設定を行います。
設定方法については各設定の説明ページをご参照ください。

Interface Queuing 設定画面

本装置の各インタフェースで行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を行う場合の、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を行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を行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行います。

ステータス表示

QoS機能の各種ステータスが表示されます。

各キューイング方式の設定手順について

各キューイング方式の基本的な設定手順は以下の通りです。

SFQ の設定手順

「Interface Queueing 設定」で設定します。

pfifo の設定手順

「Interface Queueing 設定」でキューのサイズを設定します。

TBF の設定手順

「Interface Queueing 設定」で、トークンのレート、パケットサイズ、キューのサイズを設定します。

CBQ の設定手順

1. ルートクラスの設定

「Interface Queueing 設定」で、ルートクラスの設定を行います。

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行うときには「CLASS Queueing 設定」でキューイング設定を行います。

PQ の設定手順

1. インタフェースの設定

「Interface Queueing 設定」で、Band 数、Priority-map、Marking Filter を設定します。

2. CLASS 分けのためのフィルタ設定

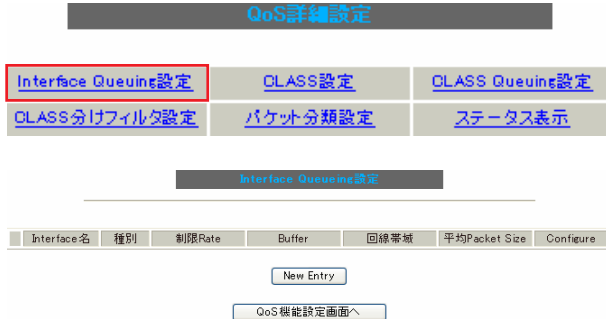
「CLASS 分けフィルタ設定」で、Mark 値によるフィルタを設定します。

3. パケット分類のための設定

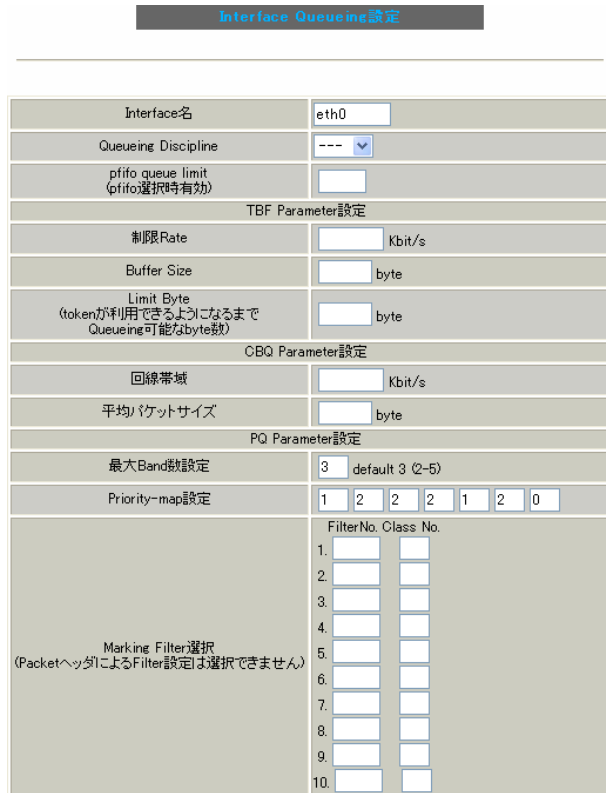
「パケット分類設定」で、TOS 値または MARK 値の付与設定を行います。

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。



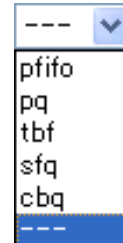
設定 戻る

Interface 名
キューイングを行うインタフェース名を入力します。
インタフェース名は「付録A インタフェース名一覧」を参照してください。

Queueing Discipline

プルダウンからキューイング方式を選択します。

- sfq
- pfifo
- tbf
- cbq
- pq



SFQ の設定

Queueing Discipline で「sfq」を選択するだけです。

PFIFO の設定

pfifo queue limit (pfifo 選択時有効)
パケットをキューイングするキューの長さを設定します。**パケットの数**で指定します。
1-999 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

パケット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

パケット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。

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

パケットの平均サイズを設定します。バイト単位で設定します。

PQの設定

[PQ Parameter 設定]について設定します。

最大 Band 数設定

生成するバンド数を設定します。ここでいう band 数はクラス数のことです。

本装置で設定されるクラス ID は 1001:、1002:、1003:、1004:、1005: となります。

初期設定は3です(クラス ID 1001: ~ 1003:)。最大数は5(クラス ID 1001: ~ 1005:)です。初期設定外の数値に設定した場合は、Priority-map 設定を変更します。

Priority-map 設定

Priority-map には7つの入れ物が用意されています(左から0、1、2、3、4、5、6という番号が付けられています)。そしてそれぞれに Band を設定します。最大 Band 数で設定した範囲で、それぞれに Band を設定できます。

Marking Filter 選択

パケットの Marking 情報によって振り分けを決定するときに設定します。

・Filter No.

Class 分けフィルタの設定番号を指定します。

・Class No.

パケットをおくるクラス番号を指定します。(1001: が Class No.1、1002: が Class No.2、1003: が Class No.3、1004: が Class No.4、1005: が Class No.5 となります。)

Priority-map の箱に付けられている番号は、TOS 値の「Linuxにおける扱い番号(パケットの優先度)」とリンクしています。本章の「 . TOS について」をご参照ください。

インタフェースに届いたパケットは、2つの方法でクラス分けされます。

- ・TOS フィールドの「Linuxにおける扱い番号(パケットの優先度)」を参照し、同じ番号の Priority-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。

設定後は「設定」ボタンをクリックします。

各設定画面での設定方法について

CLASS 設定



設定を追加するときは「New Entry」をクリックします。



Description
設定名を付けることができます。半角英数字のみ使用可能です。

Interface 名
キューイングを行うインタフェース名を入力します。
インタフェース名は「付録A インタフェース名一覧」を参照してください。

Class ID
クラス ID を設定します。クラスの階層構造における <minor 番号> となります。

親 class ID
親クラスの ID を指定します。クラスの階層構造における <major 番号> となります。

Priority
複数の CLASS 設定での優先度を設定します。値が小さいものほど優先度が高くなります。
1-8の間で設定します。

Rate 設定
クラスの帯域幅を設定します。設定は kbit/s 単位となります。

Class 内 Average Packet Size 設定
クラス内のパケットの平均サイズを指定します。設定はバイト単位となります。

Maximum Burst 設定
一度に送信できる最大パケット数を指定します。

Bounded 設定
「有効」を選択すると、兄弟クラスから余っている帯域幅を借りようとはしなくなります (Rate 設定値を超えて通信しません)。
「無効」を選択すると、その逆の動作となります。

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

設定後は「設定」ボタンをクリックします。

各設定画面での設定方法について

CLASS Queueing 設定

QoS詳細設定

Interface Queueing設定 CLASS設定 **CLASS Queueing設定**

CLASS分けフィルタ設定 パケット分類設定 ステータス表示

CLASS Queueing設定

Description	Interface名	QDISC番号	種別	CLASS ID	MAJOR番号	Configure

New Entry

QoS機能設定画面へ

設定を追加するときは「New Entry」をクリックします。

CLASS Queueing設定

Description	<input type="text"/>
Interface名	eth0
QDISC番号	<input type="text"/>
MAJOR ID	1
class ID	<input type="text"/>
Queueing Discipline	---
pfifo limit (PFIFO選択時有効)	<input type="text"/>
TBF Parameter設定	
制限Rate	<input type="text"/> Kbit/s
Buffer Size	<input type="text"/> byte
Limit Byte (tokenが利用できるようになるまで queueing可能なbyte数)	<input type="text"/> 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の選択 (PacketヘッダによるFilter設定は選択できません)	FilterNo. Class No.
	1. <input type="text"/> <input type="text"/>
	2. <input type="text"/> <input type="text"/>
	3. <input type="text"/> <input type="text"/>
	4. <input type="text"/> <input type="text"/>
	5. <input type="text"/> <input type="text"/>
	6. <input type="text"/> <input type="text"/>
	7. <input type="text"/> <input type="text"/>
	8. <input type="text"/> <input type="text"/>
	9. <input type="text"/> <input type="text"/>
10. <input type="text"/> <input type="text"/>	

設定 戻る

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
キューイングを行うインタフェース名を選択します。
インタフェース名は「付録A インタフェース名一覧」を参照してください。

QDISC番号
このクラスが属しているQDISC番号を指定します。

MAJOR ID
親のクラスIDを指定します。クラスの階層構造における <major 番号> となります。

class ID
親クラスのIDを指定します。クラスの階層構造における <minor 番号> となります。

以下は、「Interface Queueing設定」と同様に設定します。

Queueing Discipline
「CLASS Queueing設定」では「cbq」方式の選択はできません。

pfifo limit (PFIFO選択時有効)

[TBF Parameter設定]

制限Rate

Buffer Size

Limit Byte

[PQ Parameter設定]

最大Band数設定

priority-map設定

Marking Filterの選択

設定後は「設定」ボタンをクリックします。

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。

CLASS分けフィルタ設定

設定番号	1
Description	<input type="text"/>
Priority	<input type="text"/> (1-999)
<input type="checkbox"/> パケットヘッダ情報によるフィルタ	
プロトコル	<input type="text"/> (Protocol番号)
送信元アドレス	<input type="text"/>
送信元ポート	<input type="text"/> (ポート番号)
宛先アドレス	<input type="text"/>
宛先ポート	<input type="text"/> (ポート番号)
TOS値	<input type="text"/> (hex.0-fe)
DSCP値	<input type="text"/> (hex.0-3f)
<input type="checkbox"/> Marking情報によるフィルタ	
Mark値	<input type="text"/> (1-999)

設定番号
自動で未使用の設定番号が振られます。

Description
設定名を付けることができます。半角英数字のみ使用可能です。

Priority
複数のCLASS分けフィルタ間での優先度を設定します。値が小さいものほど優先度が高くなります。1-999の間で設定します。

パケットヘッダ情報によるフィルタ
パケットヘッダ情報でCLASS分けを行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を行うときは、パケットヘッダによるフィルタはできません。

プロトコル
プロトコルを指定します。プロトコル番号で指定してください。

送信元アドレス
送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。範囲での指定はできません。

送信元ポート
送信元ポート番号を指定します。範囲で指定するときは、**始点ポート：終点ポート**の形式で指定します。

宛先アドレス
宛先 IP アドレスを指定します。指定方法は送信元 IP アドレスと同様です。

宛先ポート
宛先ポート番号を指定します。指定方法は送信元ポートと同様です。

TOS 値
TOS 値を指定します。16進数で指定します。

DSCP 値
DSCP 値を設定します。16進数で指定します。

Marking 情報によるフィルタ
MARK 値によってCLASS分けを行うときにチェックします。

Mark 値
マッチ条件となる Mark 値を、1-999の間で指定します。PQでフィルタを行うときはMarking情報によるもののみ有効です。

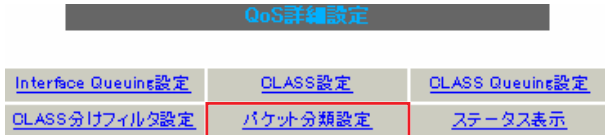
設定後は「設定」ボタンをクリックします。

各設定画面での設定方法について

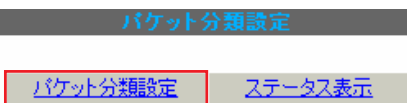
パケット分類設定

本機能の設定画面は以下の方法で表示されます。

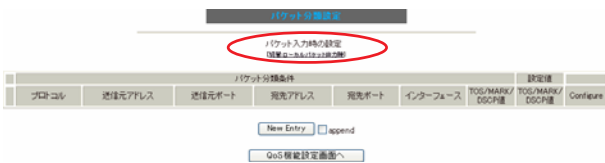
- Web画面「QoS設定」 「パケット分類設定」



- Web画面「パケット分類設定」 「パケット分類設定」



どちらも同様の設定画面が開きます。「パケット入力時の設定」か「ローカルパケット出力時の設定」かを、[切替:]をクリックして選択します。



設定を追加するときは「New Entry」をクリックします。



設定番号	1	
パケット分類条件		
プロトコル	<input type="text" value=""/> (Protocol番号)	<input type="checkbox"/> Not条件
送信元アドレス	<input type="text" value=""/>	<input type="checkbox"/> Not条件
送信元ポート	<input type="text" value=""/> (ポート番号/範囲指定で番号連結)	<input type="checkbox"/> Not条件
宛先アドレス	<input type="text" value=""/>	<input type="checkbox"/> Not条件
宛先ポート	<input type="text" value=""/> (ポート番号/範囲指定まで番号連結)	<input type="checkbox"/> Not条件
インターフェース	<input type="text" value=""/>	<input type="checkbox"/> Not条件
TOS/MARK/DSCP値	<input type="radio"/> TOS <input type="radio"/> MARK <input type="radio"/> DSCP <input checked="" type="radio"/> マッチ条件無効 <input type="text" value=""/> 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	<input type="radio"/> TOS/Precedence <input type="radio"/> MARK <input type="radio"/> DSCP	
設定値	・MARK設定 (1-999) <input type="text" value=""/> ・TOS/Precedence設定 選択して下さい ▼ TOS Bit 選択して下さい ▼ Precedence Bit ・DSCP設定 選択して下さい ▼ DSCP Bit	

設定番号
自動で未使用の設定番号が振られます。

[パケット分類条件]

パケット選別のマッチ条件を定義します。

プロトコル
プロトコルを指定します。プロトコル番号で指定してください。

送信元アドレス
送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。範囲での指定はできません。

送信元ポート
送信元ポート番号を指定します。範囲で指定するときは、**始点ポート:終点ポート**の形式で指定します。

宛先アドレス
宛先 IP アドレスを指定します。指定方法は送信元 IP アドレスと同様です。

宛先ポート
宛先ポート番号を指定します。指定方法は送信元ポートと同様です。

インターフェース
インタフェースを選択します。インタフェース名は「付録A インタフェース名一覧」を参照してください。

各項目について「Not条件」にチェックを付けると、その項目で指定した値以外のものがマッチ条件となります。

TOS/MARK/DSCP 値
マッチングする TOS/MARK/DSCP 値を指定します。TOS、MARK、DSCP のいずれかを選択し、その値を指定します。これらをマッチ条件としないときは「マッチ条件無効」を選択します。

・ 各設定画面での設定方法について

[TOS/MARK/DSCP の値]

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

設定対象

TOS/Precedence、MARK、DSCP のいずれかを選択します。

設定値

設定対象で選択したものについて、設定値を指定します。

設定後は「設定」ボタンをクリックします。

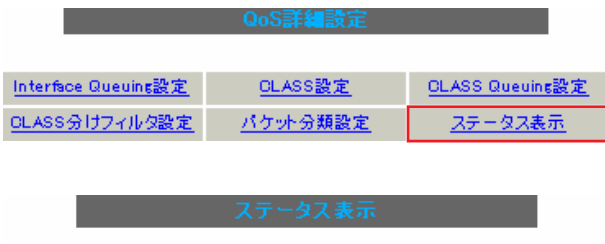
TOS/Precedence および DSCP については章末をご参照ください。

ステータスの表示

ステータス表示

本機能の設定画面は以下の方法で表示されます。

- Web画面「QoS設定」「ステータス表示」



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	<input type="text"/>

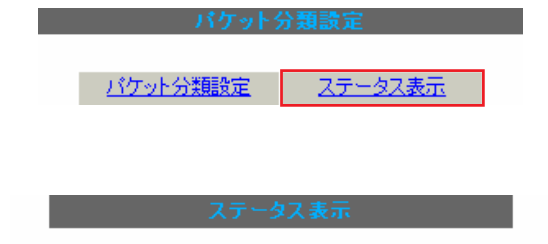
インターフェース指定後、表示するボタンを押下してください
(Packet分類設定ステータス表示時は、インターフェースの指定無くても可)

[QoS機能設定画面へ](#)

QoS機能の各種ステータスを表示します。
表示したい項目について「表示する」ボタンをクリックしてください。

「Packet 分類設定ステータス表示」以外では、必ず
Interface 名を「Interface の指定」に入力してか
ら「表示する」ボタンをクリックしてください。

- Web画面「パケット分類設定」「ステータス表示」



Packet分類設定ステータス表示	表示する
Interfaceの指定(指定無くても可)	<input type="text"/>

パケット分類設定のステータス表示では、「Packet 分類設定ステータス表示」のみになります。

「Interface の指定」は必要な場合に入力してください。指定がなくてもステータスは表示されます。

. 設定の編集・削除方法

各 QoS 設定を行うと、設定内容が一覧で表示されます。

CLASS 設定

	Description	Interface名	ID	親 CLASS ID	Priority	Rate	平均 Packet Size	Maximum Burst	Configure
1		eth0	1	0	1	100000Kbit/s	1000	100	Edit , Remove

(「CLASS 設定」画面の表示例)

設定の編集を行う場合

Configure 欄の「Edit」をクリックすると設定画面に遷移し、その設定を修正できます。

設定の削除を行う場合

Configure 欄の「Remove」をクリックすると、その設定が即座に削除されます。

・ 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	過負荷の状態に届いたパケット数

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個のパケットが用意され、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	パケットのサイズ
mpu	最小パケットサイズ
lat	パケットがtbfに留まっていられる時間

qdisc cbq 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8 weight 1000Kbit allot 1514b

level 2 ewma 5 avpkt 1000b maxidle 242us

Sent 2420755 bytes 3945 pkts (dropped 0, overlimits 0)

borrowed 0 overactions 0 avgidle 6399 undertime 0

bounded,isolated	bounded,isolated設定がされている (boundedは帯域を借りない、isolatedは帯域を貸さない)
prio	優先度(上記ではrootクラスなので、prio値はありません)
weight	ラウンドロビンプロセスの重み
allot	送信できるデータサイズ
ewma	指数重み付け移動平均
avpkt	平均パケットサイズ
maxidle	パケット送信時の最大アイドル時間
borrowed	帯域幅を借りて送信したパケット数
avgidle	EMWAで測定した値から、計算したアイドル時間を差し引いた数値 通常は数字がカウントされていますが、負荷で一杯の接続の状態では"0"、 過負荷の状態ではマイナスの値になります

・ 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

ステータス情報の表示例

[CLASS分けフィルタ設定情報]表示例

クラス分けフィルタの設定情報を表示します。

その1 <CBQでの表示例>

```
[ PARENT 1: ]
filter protocol ip pref 1 u32
filter protocol ip pref 1 u32 fh 805: ht divisor 1
filter protocol ip pref 1 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 1 u32 fh 804: ht divisor 1
filter protocol ip pref 1 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32
filter protocol ip pref 3 u32 fh 805: ht divisor 1
filter protocol ip pref 3 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32 fh 804: ht divisor 1
filter protocol ip pref 3 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
```

protocol	マッチするプロトコル
pref	優先度
u32	パケット内部のフィールド(発信元IPアドレスなど)に基づいて処理すべきクラスの決定を行います。
at 8、at16	マッチの開始は、指定した数値分のオフセットからであることを示します。 at 8であれば、ヘッダの9バイトめからマッチします。
flowid	マッチしたパケットを送るクラス

その2 <PQでの表示例>

```
[ PARENT 1: ]
filter protocol ip pref 1 fw
filter protocol ip pref 1 fw handle 0x1 classid 1:3
filter protocol ip pref 2 fw
filter protocol ip pref 2 fw handle 0x2 classid 1:2
filter protocol ip pref 3 fw
filter protocol ip pref 3 fw handle 0x3 classid 1:1
```

pref	優先度
handle	TOSまたはMARK値
classid	マッチパケットを送るクラスID クラスID 1:(n) のとき、100(n):に送られます。

・ 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      MARK set
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

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。

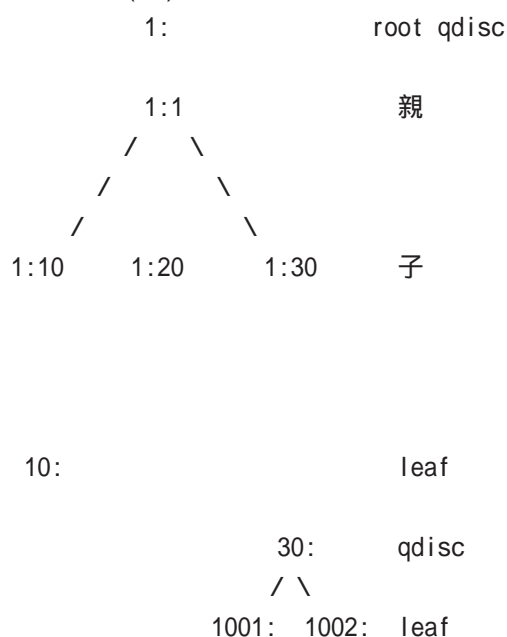
[クラス ID について]

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)>



. 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

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。

. 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。

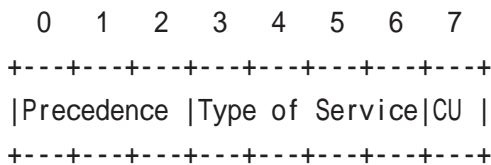
TOS値は定義があいまいで相互運用できない、正しい値が設定されている保証がない、悪用される可能性があるなどの要因により、現在までほとんど使われていません。

. DSCPについて

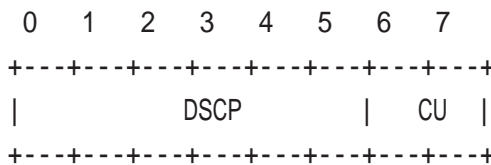
本装置ではDS(DiffServ)フィールドの設定・書き換えも可能です。DSフィールドとは、IPパケット内のTOSの再定義フィールドであり、DiffServに対応したネットワークにおいてQoS制御動作の基準となる値が設定されます。DiffServ対応機器では、DSフィールド内のDSCP値だけを参照してQoS制御を行うことができます。

TOSとDSフィールドのビット定義

【TOSフィールド構造】



【DSCPフィールド構造】



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)		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)
AF11/AF12/AF13	0x0a / 0x0c / 0x0e	<ul style="list-style-type: none"> ・送出優先度 (高) 1 > 2 > 3 > 4 (低) ・廃棄優先度 (高) 1 > 2 > 3 (低)
AF21/AF22/AF23	0x12 / 0x14 / 0x16	
AF31/AF32/AF33	0x1a / 0x1c / 0x1e	
AF41/AF42/AF43	0x22 / 0x24 / 0x26	
CS(Class Selector)		既存のTOS互換による優先制御を行います。
CS1	0x08	Precedence1(Priority)
CS2	0x10	Precedence2(Immediate)
CS3	0x18	Precedence3(Flash)
CS4	0x20	Precedence4(Flash Override)
CS5	0x28	Precedence5(Critic/ESP)
CS6	0x30	Precedence6(Internet Control)
CS7	0x38	Precedence7(Network Control)
BE (Best Effort)	0x00	ベストエフォート(優先制御なし)

第31章

ゲートウェイ認証機能

ゲートウェイ認証機能の設定

「ゲートウェイ認証機能」は、本装置を経由して外部にアクセスをする場合に、本装置での認証を必要とする機能です。

この機能を使うことで、外部へアクセスできるユーザを管理できるようになります。

ゲートウェイ認証設定 (基本設定)		
基本設定	ユーザ設定	RADIUS設定
フィルタ設定	ログ設定	

基本設定

基本設定		
本機能	<input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する
認証	<input type="radio"/> しない (URL転送のみ)	<input checked="" type="radio"/> する
80/tcp 監視	<input checked="" type="radio"/> 行わない	<input type="radio"/> 行う

URL転送		
URL	<input type="text"/>	
通常認証後	<input checked="" type="radio"/> 行わない (デフォルト)	<input type="radio"/> 行う
強制認証後	<input checked="" type="radio"/> 行わない (エンドユーザ要求URL)	<input type="radio"/> 行う

認証方法	
<input checked="" type="radio"/> ローカル	<input type="radio"/> RADIUSサーバ

接続許可時間	
<input checked="" type="radio"/> アイドルタイムアウト	<input type="text" value="30"/> 分 (1~43200)
<input type="radio"/> セッションタイムアウト	<input type="text"/> 分 (1~43200)
<input type="radio"/> 認証を受けたWebブラウザのウィンドウを閉じるまで	

設定変更

[基本設定]

本機能

ゲートウェイ認証機能を使う場合は「使用する」を選択します。

認証

当機能を使用していて、かつ認証を行うときは「する」を選択します。

認証を行わないときは「しない」を選択します。このときは、外部へのアクセスをリダイレクトするだけの動作となります。

80/tcp 監視

「行う」を選択した場合、認証を受けていないIPアドレスからのTCPポート80番のコネクションを監視し、このコネクションがあったときに、強制的にゲートウェイ認証を行います。

[URL転送]

URL

転送先のURLを設定します。

通常認証後

「行う」を選択すると、ゲートウェイ認証後に「URL」で指定したサイトに転送させることができます。

強制認証後

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

[認証方法]

ローカル

XR-640でアカウントを管理/認証します。

RADIUSサーバ

外部のRADIUSサーバでアカウントを管理/認証します。

[接続許可時間]

認証したあとの、ユーザの接続形態を選択できます。

アイドルタイムアウト

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

セッションタイムアウト

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

ゲートウェイ認証機能の設定

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

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

最後に「設定変更」をクリックしてください。

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

ユーザ設定

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

No.1~16まで

No.	ユーザID	パスワード	削除
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

設定/削除の実行

ユーザ設定画面インデックス

[001-](#) [017-](#) [033-](#) [049-](#)

ユーザ ID

パスワード

ユーザアカウントを登録します。
 ユーザ ID・パスワードには半角英数字が使用できません。空白やコロン(:)は含めることができません。

削除

チェックすると、その設定が削除対象となります。

最後に「設定 / 削除の実行」をクリックしてください。

ゲートウェイ認証機能の設定

RADIUS 設定

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

プライマリサーバ設定	
IPアドレス	<input type="text"/>
ポート番号	<input checked="" type="radio"/> 1645 <input type="radio"/> 1812 <input type="radio"/> 手動設定 <input type="text"/>
secret	<input type="text"/>
セカンダリサーバ設定	
IPアドレス	<input type="text"/>
ポート番号	<input checked="" type="radio"/> 1645 <input type="radio"/> 1812 <input type="radio"/> 手動設定 <input type="text"/>
secret	<input type="text"/>
サーバ共通設定	
NAS-IP-Address	<input type="text"/>
NAS-Identifier	<input type="text"/>
接続許可時間 (RADIUSサーバから送信されるアトリビュートの指定)	
アイドルタイムアウト	<input type="text" value="指定しない"/> ▼
セッションタイムアウト	<input type="text" value="指定しない"/> ▼

[プライマリサーバ設定]

プライマリサーバ項目の設定は必須です。

IP アドレス
ポート番号
secret

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

[セカンダリサーバ設定]

セカンダリ項目の設定はなくてもかまいません。

IP アドレス
ポート番号
secret

設定はプライマリサーバ設定と同様です。

[サーバ共通設定]

RADIUS サーバへ問い合わせをする際に送信する NAS の情報を設定します。RADIUS サーバが、どの NAS かを識別するために使います。どちらかの設定が必須です。

NAS-IP-Address

通常は XR-640 の IP アドレスを設定します。

NAS-Identifier

任意の文字列を設定します。
半角英数字が使用できます。

[接続許可時間 (RADIUSサーバから送信されるアトリビュートの指定)]

それぞれ、基本設定で選択されているものが有効となります。

アイドルタイムアウト

プルダウンの以下の項目から選択してください。

- ・ 指定しない

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

- ・ Idle-Timeout_28

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

- ・ Ascend-Idle-Limit_244/529

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

- ・ Ascend-Idle-Limit_244

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

セッションタイムアウト

プルダウンの以下の項目から選択してください。

- ・ 指定しない

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

第31章 ゲートウェイ認証機能

ゲートウェイ認証機能の設定

• Session-Timeout_27

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

• Ascend-Maximum-Time_194/529

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

• Ascend-Maximum-Time_194

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

アトリビュートとは、RADIUSで設定されるパラメータのことを指します。

最後に「設定変更」をクリックしてください。

フィルタ設定

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

設定画面「フィルタ設定」をクリックします。

[「フィルタ設定」のゲートウェイ認証設定フィルタ設定画面](#)にて設定して下さい。

上記のメッセージが表示されたらリンクをクリックしてフィルタ設定画面に移ります。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート	LOG	削除	No.
1		パケット受信時	許可	全て							1
2		パケット受信時	許可	全て							2
3		パケット受信時	許可	全て							3
4		パケット受信時	許可	全て							4
5		パケット受信時	許可	全て							5
6		パケット受信時	許可	全て							6
7		パケット受信時	許可	全て							7
8		パケット受信時	許可	全て							8
9		パケット受信時	許可	全て							9
10		パケット受信時	許可	全て							10
11		パケット受信時	許可	全て							11
12		パケット受信時	許可	全て							12
13		パケット受信時	許可	全て							13
14		パケット受信時	許可	全て							14
15		パケット受信時	許可	全て							15
16		パケット受信時	許可	全て							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。

設定/削除の実行

ゲートウェイ認証フィルタ設定画面のアドレス
001: 017, 023, 045, 046, 081, 087, 113,
122, 145, 161, 177, 193, 202, 225, 241-

ここで設定した IP アドレスやポートについては、ゲートウェイ認証機能によらず、通信可能になります。

設定方法については「第25章 パケットフィルタリング機能」をご参照ください。

ゲートウェイ認証下のアクセス方法

ログ設定

ゲートウェイ認証機能のログを本装置のシステムログに出力できます。

エラーログ	<input checked="" type="radio"/> 使用しない	<input type="radio"/> syslogに取る
アクセスログ	<input checked="" type="radio"/> 使用しない	<input type="radio"/> syslogに取る

ログを取得するかどうかを選択します。

エラーログ

ゲートウェイ認証時のログインエラーを出力します。

<エラーログの表示例>

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

アクセスログ

ゲートウェイ認証時のアクセスログを出力します。

<アクセスログの表示例>

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

ホストからのアクセス方法

ホストから本装置にアクセスします。以下の形式でアドレスを指定してアクセスします。

http://<本装置の IP アドレス>/login.cgi

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

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

<認証成功時の表示例>

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

```
Date: Mon Apr 7 10:06:51 2005
```

設定画面へのアクセスについて

ゲートウェイ認証機能を使用していて認証を行っていない場合でも、本装置の設定画面にはアクセスすることができます。アクセス方法は、通常と同じです。

RADIUS 設定について

認証方法を「RADIUS サーバ」に選択した場合、XR-640 は RADIUS サーバに対して認証要求のみを送信します。

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

認証について

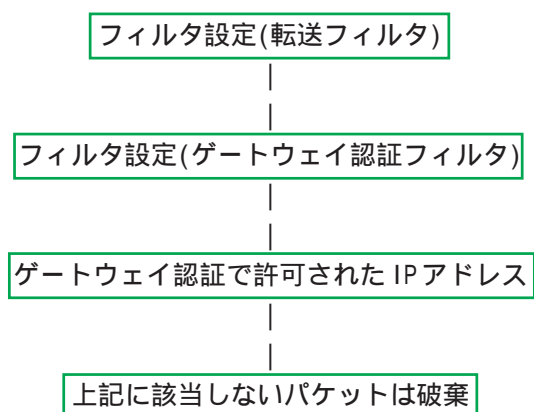
認証方法が「ローカル」、「RADIUS サーバ」のどちらの場合でも、クライアント - 本装置間の認証には、HTTP Basic 認証が用いられます。

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

ゲートウェイ認証の制御方法について

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

フィルタリング制御の順番は以下の通りです。



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

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

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

第 32 章

ネットワークテスト

ネットワークテスト

XR-640 の運用時において、ネットワークテストを行うことができます。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。

ネットワークテスト

Ping	<p>FQDNまたはIPアドレス <input type="text"/></p> <p>インターフェースの指定(省略可)</p> <p> <input type="radio"/> 主回線 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input checked="" type="radio"/> その他 <input type="text"/> </p> <p>オプション count <input type="text" value="10"/> size <input type="text" value="56"/> timeout <input type="text" value="30"/> </p> <p style="text-align: center;"><input type="button" value="実行"/></p>
Trace Route	<p>FQDNまたはIPアドレス <input type="text"/></p> <p>オプション <input checked="" type="radio"/> UDP <input type="radio"/> ICMP </p> <p style="text-align: center;"><input type="button" value="実行"/></p>
パケットダンプ	<p> <input type="radio"/> 主回線 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4 <input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> その他 <input type="text"/> </p> <p style="text-align: center;"><input type="button" value="実行"/> <input type="button" value="結果表示"/></p>
PacketDump TypePcap	<p>Device <input type="text"/> CapCount <input type="text"/> CapSize <input type="text"/></p> <p>Dump Filter <input type="text"/></p> <p>生成ファイルの最大サイズは圧縮後で約4Mbyteです 高帯域下での使用はパケットロスを生じる場合があります</p> <p style="text-align: center;"><input type="button" value="実行"/> <input type="button" value="結果表示"/></p>

[Ping テスト]

指定した相手に本装置から Ping を発信します。

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

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

オプション

・count
 送信する ping パケット数を指定します。
 入力可能な範囲：1-10 です。初期値は 10 です。

・size
 送信するデータサイズ(byte)を指定します。
 入力可能な範囲：56-1500 です。初期値は 56 です
 (8 バイトの ICMP ヘッダが追加されるため、64 バイトの ICMP データが送信されます)。

・timeout
 ping コマンドの起動時間を指定します。
 入力可能な範囲：1-30 です。初期値は 30 です。

入力が終わりましたら「実行」をクリックします。

実行結果例

実行結果

```

PING 211.14.13.66 (211.14.13.66): 56 data bytes
 84 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=49.5 ms
 84 bytes from 211.14.13.66: icmp_seq=1 ttl=52 time=65.7 ms
 84 bytes from 211.14.13.66: icmp_seq=2 ttl=52 time=11.7 ms
 84 bytes from 211.14.13.66: icmp_seq=3 ttl=52 time=12.0 ms
 84 bytes from 211.14.13.66: icmp_seq=4 ttl=52 time=69.0 ms
 84 bytes from 211.14.13.66: icmp_seq=5 ttl=52 time=58.3 ms
 84 bytes from 211.14.13.66: icmp_seq=6 ttl=52 time=12.0 ms
 84 bytes from 211.14.13.66: icmp_seq=7 ttl=52 time=71.4 ms
 84 bytes from 211.14.13.66: icmp_seq=8 ttl=52 time=12.0 ms
 84 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
  
```


第32章 ネットワークテスト

ネットワークテスト

[Trace Route テスト]

指定した宛先までに経由するルータの情報を表示します。

FQDN または IP アドレス

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

オプション

・UDP

UDP パケットを使用する場合に指定します。初期設定は UDP です。

・ICMP

ICMP パケットを使用する場合に指定します。

入力が終わりましたら「実行」をクリックします。

実行結果例

```
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 21.159 ms 19.949 ms
 4 210.195.192.108 (210.195.192.108) 9.205 ms 9.953 ms 9.810 ms
 5 210.195.208.34 (210.195.208.34) 35.538 ms 19.923 ms 14.744 ms
 6 210.195.208.10 (210.195.208.10) 41.641 ms 40.476 ms 63.293 ms
 7 210.171.224.115 (210.171.224.115) 48.948 ms 27.255 ms 36.767 ms
 8 211.14.3.238 (211.14.3.238) 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) 58.573 ms 19.889 ms 50.057 ms
11 211.14.2.193 (211.14.2.193) 33.777 ms 11.380 ms 17.282 ms
12 * * *
13 211.14.12.249 (211.14.12.249) 19.692 ms !X * 15.219 ms !X
```

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

[パケットダンプテスト]

パケットのダンプを取得できます。

ダンプを取得したいインタフェースを選択して「実行」をクリックします。

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

その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例

```
実行結果

192.168.120.15: 192.168.120.15: 56 data bytes
64 bytes from 192.168.120.15: icmp_seq=0 ttl=64 time=12.4 ms

--- 192.168.120.15 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 192.168.120.15 (192.168.120.15), 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 21.159 ms 19.949 ms
 4 210.195.192.108 (210.195.192.108) 9.205 ms 9.953 ms 9.810 ms
 5 210.195.208.34 (210.195.208.34) 35.538 ms 19.923 ms 14.744 ms
 6 210.195.208.10 (210.195.208.10) 41.641 ms 40.476 ms 63.293 ms
 7 210.171.224.115 (210.171.224.115) 48.948 ms 27.255 ms 36.767 ms
 8 211.14.3.238 (211.14.3.238) 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) 58.573 ms 19.889 ms 50.057 ms
11 211.14.2.193 (211.14.2.193) 33.777 ms 11.380 ms 17.282 ms
12 * * *
13 211.14.12.249 (211.14.12.249) 19.692 ms !X * 15.219 ms !X
```

「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)

ネットワークテスト

[PacketDump TypePcap テスト]

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

Device

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

CapCount

パケットダンプの取得数を指定します。
1-99999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。

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]

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

ダンプ実行結果はありません。

まだ指定パケット数を記録していません
記録用ストレージ使用率 約3%

[再表示] [実行中断]

パケットダンプが実行終了したときの画面

実行結果(.gzファイル)

ダンプファイルを消去

[設定画面へ]

「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。

ネットワークテスト

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

PacketDump TypePcapの注意点

- 取得したパケットダンプ結果は、libcap形式でgzip圧縮して保存されます。
- 取得できるデータサイズは、gzip圧縮された状態で最大約4MBです。
- 本装置上にはパケットダンプ結果を1つだけ記録しておけます。パケットダンプ結果を消去せずにPacketDump TypePcapを再実行して実行結果ファイルを作成したときは、それまでに記録されていたパケットダンプ結果に上書きされません。
- 本装置のインターフェース名については本書「付録A インターフェース名一覧」をご参照ください。

第 33 章

システム設定

システム設定

「システム設定」ページでは、XR-640の運用に関する制御を行います。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
- ・ファームウェアのアップデート
- ・設定の保存・復帰
- ・設定のリセット
- ・本体の再起動
- ・セッションライフタイムの設定
- ・設定画面の設定
- ・ISDN設定
- ・オプションCFカードの操作
- ・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。

システム設定						
時計の設定	ログの表示 ログの削除	パスワードの 設定	ファームウェアの アップデート	設定の保存・ 復帰	設定のリセット	再起動
セッション ライフタイムの 設定	設定画面の 設定	ISDN設定	オプションCF カード	ARP filter 設定		

時計の設定

XR-640内蔵時計の設定を行います。

「時計の設定」をクリックして設定画面を開きます。

内蔵時計の設定

2007年 11月 23日 金曜日

18時 40分 00秒

※時刻は24時間形式で入力してください。

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 00:26:11 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 RNXD=0
RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROts=0 SSysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIO=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNXD=0
Apr 26 01:06:09 localhost -- MARK --
Apr 26 01:26:09 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 RNXD=0
RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROts=0 SSysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIO=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNXD=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 RNXD=0
RFwdR=0 RDupR=0 RFail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROts=0 SSysQ=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RQ=3 RIO=0 RFwdQ=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
最大1000行まで表示できます
```

表示の更新

ログファイルの取得

ブラウザの「リンクを保存する」を使用して取得して下さい
[最新ログ](#)

XR-640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。

保存されるログファイルは最大で6つです。
 ログファイルが作成されたときは画面上にリンクが生成されます。
 古いログファイルから順に削除されていきます。

ログファイルの取得

ブラウザの「リンクを保存する」を使用して取得して下さい
[最新ログ](#)

- [バックアップログ1](#)
- [バックアップログ2](#)
- [バックアップログ3](#)
- [バックアップログ4](#)
- [バックアップログ5](#)
- [バックアップログ6](#)

「攻撃検出機能」を使用している場合は、そのログも併せてここで表示されます。

本体の再起動を行った場合、それまでのログは全てクリアされます。

ログの削除

ログ情報は最大2MBまでのサイズで保存されます。また再起動時にログ情報は削除されます。手動で削除する場合は次のようにしてください。

実行方法

「ログの削除」をクリックして画面を開きます。

ログの削除

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。

パスワードの設定

XR-640の設定画面にログインする際のユーザ名、パスワードを変更します。ルータ自身のセキュリティのためにパスワードを変更されることを推奨します。

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。

パスワード設定	
新しいユーザ名	<input type="text"/>
新しいパスワード	<input type="password"/>
もう一度入力してください	<input type="password"/>
<input type="button" value="入力のやり直し"/>	<input type="button" value="設定の保存"/>

ユーザ名とパスワードの設定ができます。

新しいユーザ名

半角英数字で1から15文字まで設定可能です。

新しいパスワード

半角英数字で1から8文字まで設定可能です。
大文字・小文字も判別しますのでご注意ください。

もう一度入力してください

確認のため再度「新しいパスワード」を入力してください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。

次回のログインからは、新しく設定したユーザ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-640は、ブラウザ上からファームウェアのアップデートを行います。

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。

ファームウェアのアップデート

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...

アップデート実行

「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ので、バージョン等が正しければ「実行する」をクリックしてください。

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-640 Series ver 1.6.6

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-640 Series ver 1.6.7

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

左下の画面が表示されたままで3分間経過した後、「実行する」ボタンをクリックすると、以下の画面が表示され、アップデートが実行されません。

ファームウェアのアップデート

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

[\[設定画面へ\]](#)

アップデートを実行した場合は以下の画面が表示され、ファームウェアの書き換えが始まります。

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。

ファームウェアのアップデート作業中は、STATUS1(赤)が点滅します。

この間は、アクセスを行わずにそのままお待ちください。

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

アップデート実行中は、本装置やインターネットへのアクセス等は行わないでください。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-640 の設定の保存および、保存した設定の復帰を行います。

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。

設定の保存・復帰(確認)

--- 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てから、「設定の保存・復帰」のリンクをクリックします。

[設定の保存]

設定を保存するときは、テキストのエンコード形式と保存形式を選択します。

設定の保存・復帰

現在の設定を保存することができます。	
コードの指定	<input type="radio"/> EUC(LF) <input checked="" type="radio"/> SJIS(CR+LF) <input type="radio"/> SJIS(CR)
形式の指定	<input type="radio"/> 全設定(zip) <input checked="" type="radio"/> 初期値との差分(text)
<input type="button" value="設定ファイルの作成"/>	

全設定

本装置のすべての設定を zip 形式で圧縮して保存します。

初期値との差分

初期値と異なる設定のみを抽出して、テキスト形式で保存します。このテキストファイルの内容を直接書き換えて設定を変更することもできます。

選択したら、「設定ファイルの作成」をクリックします。

クリックすると以下のメッセージが表示されます。

設定の保存・復帰

設定の保存作業を行っています。

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

[設定画面へ]

「バックアップファイルのダウンロード」リンクから、設定をテキストファイルで保存しておきます。

[設定の復帰]

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 zip 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	<input type="text"/> <input type="button" value="参照..."/>
<input type="button" value="設定の復帰"/>	

設定の復帰が正しく行われると本機器は自動的に再起動します

その後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、XR-640 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-640 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。

設定のリセット

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。

再起動

XR-640 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。

本体の再起動

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。

本体の再起動を行った場合、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

本装置内部では、NAT/IP マスカレードの通信を高速化するために、セッション生成時に NAT/IP マスカレードのセッション情報を記憶し、一定時間保存しています。

ここでは、そのライフタイムを設定します。

「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。

セッションライフタイムの設定

UDP	<input type="text" value="30"/>	秒 (0 - 8640000)
UDP stream	<input type="text" value="180"/>	秒 (0 - 8640000)
TCP	<input type="text" value="3600"/>	秒 (0 - 8640000)
セッション最大数	<input type="text" value="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。

設定の保存

UDP

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

UDP stream

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

TCP

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

セッション最大数

本装置で保持できる NAT/IP マスカレードのセッション情報の最大数を設定します。

UDP/UDPstream/TCP のセッション情報を合計した最大数になります。

4096 ~ 16384 の間で設定します。

初期設定は 8192 です。

なお、本装置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 16 章 SYSLOG 機能」のシステムメッセージの項を参照してください。

それぞれの項目で “0” を設定すると、初期値で動作します。

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

システム設定

設定画面の設定

WEB 設定画面へのアクセスログについての設定をします。

実行方法

「設定画面の設定」をクリックして画面を開きます。

設定画面の設定	
アクセスログ	<input checked="" type="radio"/> 使用しない <input type="radio"/> syslogに取る
エラーログ	<input checked="" type="radio"/> 使用しない <input type="radio"/> syslogに取る

アクセスログ

(アクセス時の)エラーログ

取得するかどうかを指定します。

「設定の保存」をクリックします。

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

ISDN 設定

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

実行方法

「ISDN の設定」をクリックして画面を開きます。

ISDN設定	
ISDN番号	<input type="text"/>
サブアドレス	<input type="text"/>

ISDN 番号

ISDN 発信者番号を入力します。

サブアドレス

サブアドレスを指定します。

「設定の保存」をクリックします。

システム設定

オプションCFカード

XR-640にオプションで用意されているコンパクトフラッシュ(CF)カードを装着している場合の、CFカードの操作を行います。

ここでは以下の設定を行うことができます。

- ・CFカードの初期化
- ・CFカードへの設定のバックアップ

実行方法

コンパクトフラッシュ(CF)カードを装着してから「オプションCFカード」をクリックして画面を開きます。

画面には、装着したCFカードの情報が表示されます。

CFカードの初期化

はじめてCFカードを装着したときは、必ずCFカードを初期化する必要があります。初期化を行わないとCFカードを使用できません。

CFカードを初期化するときは「オプションCFカードの初期化」をクリックします。

オプションCFカード

このオプションCFカードは初期化しないと使用出来ません

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

CFカードへの設定のバックアップ

設定のバックアップをCFカードにコピーするときは「設定ファイルをコピーする」をクリックしてコピーを実行します。

オプションCFカード

オプションCFカードの状況

総容量 [124906 kbyte] 空容量 [121898 kbyte] 使用率 [2%]

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

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

オプションCFカード

オプションCFカードの状況

総容量 [124906 kbyte] 空容量 [121822 kbyte] 使用率 [2%]

機器設定のバックアップ日時

Sep 4 15:27

[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カードを挿入すると、本体前面のCF(緑)ランプが点滅します。

その後CFランプが点灯すると、CFカードが使用できる状態となります。

CFカードを本装置から取り外すときは、必ず本体前面のCFカードスロット横にある「RELEASE」ボタンを数秒押し続けてください。

CFランプが消灯します。

消灯を確認いただきましたら、CFカードは安全に取り外せます。

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

ARP filter 設定

ARP filter 設定を行います。

実行方法

「ARP filter 設定」をクリックして画面を開きます。



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

選択しましたら「設定の保存」をクリックしてください。設定が完了します。
設定はすぐに反映されます。

第 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。
- ・ **インターフェース情報**
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。

The screenshot shows a web browser window titled "http://192.168.0.254:880 - 機器情報 - Microsoft Internet Explorer". The page content is as follows:

```

ファームウェアバージョン
Century Systems XR-640 Series ver 1.6.7
更新
インターフェース情報
eth0 Link encap:Ethernet HWaddr 00:80:6D:69:05:14
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:774 errors:0 dropped:0 overruns:0 frame:0
TX packets:577 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:134855 (131.6 Kb) TX bytes:315644 (308.2 Kb)
Interrupt:60
eth1 Link encap:Ethernet HWaddr 00:80:6D:69:05:16
inet addr:192.168.1.254 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST 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:62
eth2 Link encap:Ethernet HWaddr 00:80:6D:69:05:18
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:26 Base address:0xaf00
リンク情報
eth0 Link:up AutoNegotiation:on Speed: 100M Duplex:full
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
192.168.0.252 0x1 0x0 00:00:00:00:00:00 * eth0
192.168.0.10 0x1 0x2 00:40:80:86:A0:2A * 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

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

以下の項目を表示します。

• ルーティング情報

本装置のルーティングテーブル、ルーティングテーブルの内部情報、ルートキャッシュの情報、デフォルトゲートウェイ情報が表示できます。

このうち、ルーティングテーブルの内部情報とルートキャッシュの情報はここでのみ表示できます。

• OSPF 情報

• RIP 情報

• IPsec サーバ情報

• DHCP サーバ情報

• NTP サービス情報

• VRRP サービス情報

• PPPoE to L2TP 情報

• QoS 情報

実行方法

Web 設定画面「詳細情報表示」をクリックすると、次の画面が表示されます。

詳細情報の表示

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
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 <input type="text"/>
RIP	RIP 情報
IPsecサーバ	IPsec 情報
DHCPサーバ	DHCPアドレスリスト情報
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 <input type="text"/>
全ての詳細情報を表示する	

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

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

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

第 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 ボタンは押しっぱなしにしておきます。
- 3 本体前面の「STATUS1(赤) LED」ランプが点灯、他の STATUS ランプが消灯するまで INIT ボタンを押し続けます。
- 4 3. 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 ボタンは押しっぱなしにしておきます。
- 3 本体前面の「SLOT CF LED」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-640にグローバルアドレスが割り当てられていて、インターネットに接続している状態ならば、iモードおよびEZウェブに対応した携帯電話から以下のような操作が可能です。

- ・ ルータとしてのサービスを停止する
- ・ ルータとしてのサービスを再開する
- ・ 本装置を再起動する

この機能を利用する際は、パケットフィルタリング設定によってWAN側からの設定変更を許す設定になっていることが必要になります。WAN側から本装置の設定変更を許すフィルタ設定については「第25章 パケットフィルタ機能」項目をご覧ください。

実際に操作画面にアクセスするためには、iモード端末から次のURLをしてしてください。

<iモード端末からアクセスする場合>

http:// 装置の IP アドレス:880/i/

<EZウェブ端末からアクセスする場合>

**http:// 装置の IP アドレス:880/ez/
index.html**

アクセスすると認証画面が表示されますので、ユーザ名とパスワードを入力してください。

「iフィルタ起動」を実行すると、ルータ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-640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-640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-640に割り当てられたグローバルアドレスが変わってしまう場合があります。もしアドレスが変わってしまったときはiモードからの制御ができなくなってしまうことが考えられますので(アドレスが分からなくなるため)、運用には十分ご注意ください。

PPPoEで接続している場合に限り、「アドレス変更お知らせメール」機能を使って現在のIPアドレスを任意のアドレスにメール通知することができます。

携帯電話による操作方法

- 1 携帯電話端末から XR-640 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

インタフェース名一覧

インタフェース名一覧

本装置は、以下の設定においてインタフェース名を直接指定する必要があります。

- ・ OSPF 機能
- ・ IPsec 機能
- ・ SNMP エージェント機能
- ・ UPnP 機能
- ・ スタティックルート設定
- ・ ソースルート設定
- ・ NAT 機能
- ・ パケットフィルタリング機能
- ・ ネットワークイベント機能
- ・ 仮想インターフェース機能
- ・ QoS 機能
- ・ ネットワークテスト

本装置のインタ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。

インタフェース名一覧

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
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
ipsec7	eth2上のipsec
gre<n>	gre (<n>は設定番号)
eth0.<n>	eth0上のVLANインタフェース (<n>はタグID)
eth1.<n>	eth1上のVLANインタフェース (<n>はタグID)
eth2.<n>	eth2上のVLANインタフェース (<n>はタグID)
eth0:<n>	eth0上の仮想インタフェース (<n>は仮想IF番号)
eth1:<n>	eth1上の仮想インタフェース (<n>は仮想IF番号)
eth2:<n>	eth1上の仮想インタフェース (<n>は仮想IF番号)

表左：インタフェース名
表右：実際の接続デバイス

付録 B

工場出荷設定一覧

工場出荷設定一覧

IPアドレス設定	IPアドレス/サブネットマスク値
Ether0ポート	192.168.0.254/255.255.255.0
Ether1ポート	192.168.1.254/255.255.255.0
Ether2ポート	192.168.2.254/255.255.255.0
DHCPクライアント機能	無効 (Ethernet2は機能なし)
IPマスカレード機能	無効
ステートフルパケットインスペクション機能	無効
デフォルトゲートウェイ設定	設定なし
リモートアクセス機能	設定なし
DNSリレー/キャッシュ機能	有効
DHCPサーバ/リレー機能	有効
IPsec機能	無効
UPnP機能	無効
ダイナミックルーティング機能	無効
PPPoEtoL2TP機能	無効
SYSLOG機能	有効
攻撃検出機能	無効
SNMPエージェント機能	無効
NTP機能	無効
VRRP機能	無効
アクセスサーバ機能	無効
スタティックルート設定	設定なし
ソースルーティング設定	設定なし
NAT機能	設定なし
パケットフィルタリング機能	NetBIOSからの漏洩を防止するフィルタ設定 (入力・転送フィルタ設定) 外部からのUPnPパケットを遮断する設定 (入力・転送フィルタ設定)
スケジュール機能	設定なし
ネットワークイベント機能	無効
仮想インターフェース機能	設定なし
GRE機能	無効
QoS機能	設定なし
パケット分類機能	設定なし
ゲートウェイ認証機能	無効
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。必ずユーザ登録していただきますよう、お願いいたします。

サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。

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

故障と思われる場合は

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

ご連絡をいただく前に

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

- ・ファームウェアのバージョンと MAC アドレス
(バージョンの確認方法は「**第 34 章 情報表示**」をご覧ください)
- ・ネットワークの構成 (図)
どのようなネットワークで運用されているかを、差し支えのない範囲でお知らせください。
- ・不具合の内容または、不具合の再現手順
何をしたときにど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ください。
- ・エラーメッセージ
エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
- ・XR-640 の設定内容、およびコンピュータの IP 設定
- ・可能であれば、「**設定のバックアップファイル**」をお送りください。

サポート情報

弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。また製品の FAQ も掲載しておりますので、是非ご覧ください。

XR-640 製品サポートページ : <http://www.centurysys.co.jp/support/xr640cd.html>

製品の保証について

本製品の保証期間は、お買い上げ日より1年間です。保証期間をすぎたもの、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承ください。保証規定については、同梱の保証書をご覧ください。

XR-640/CD ユーザーズガイド 1.6.7対応版 release 2

2008年3月版

発行 センチュリー・システムズ株式会社

Copyright (c) 2002-2008 Century Systems Co., Ltd. All rights reserved.
