

GIGABIT GATE

L2TPv3 対応 GigabitGate

FutureNet XR-1100 series

ユーザズガイド

Ver1.6.2 対応版



目次

はじめに	6
ご使用にあたって	7
パッケージの内容物の確認	10
第1章 本装置の概要	11
I. 本装置の特長	12
II. 各部の名称と機能	13
III. 動作環境	16
第2章 本装置の設置	17
本装置の設置	18
第3章 コンピュータのネットワーク設定	19
I. Windows 95/98/Meのネットワーク設定	20
II. Windows 2000のネットワーク設定	21
III. Windows XPのネットワーク設定	22
IV. Windows Vistaのネットワーク設定	23
V. Macintoshのネットワーク設定	24
VI. IPアドレスの確認と再取得	25
第4章 設定画面へのログイン	26
設定画面へのログイン方法	27
第5章 インタフェース設定	28
I. Ethernetポートの設定	29
II. Ethernetポートの設定について	31
III. VLAN タギングの設定	32
IV. その他の設定	33
第6章 PPPoE 設定	35
I. PPPoE の接続先設定	36
II. PPPoE の接続設定と回線の接続 / 切断	38
III. その他の接続設定	39
IV. バックアップ回線	40
V. PPPoE 特殊オプション設定	43
第7章 RS-232 ポートを使った接続(リモートアクセス機能)	44
I. 本装置とアナログモデム / TA の接続	45
II. リモートアクセス回線の接続先設定	46
III. リモートアクセス回線の接続と切断	48
IV. バックアップ回線接続	49
第8章 複数アカウント同時接続設定	50
複数アカウント同時接続の設定	51
第9章 各種サービスの設定	55
各種サービス設定	56
第10章 DNS リレー / キャッシュ機能	57
DNS リレー / キャッシュ機能の設定	58
第11章 DHCP サーバ / リレー機能	59
I. 本装置の DHCP 関連機能について	60
II. DHCP サーバ機能の設定	61
III. DHCP サーバ機能の設定例	62
IV. IP アドレス固定割り当て設定	63
第12章 IPsec 機能	64
I. 本装置の IPsec 機能について	65
II. IPsec 設定の流れ	66

III. IPsec 設定	67
IV. IPsec Keep-Alive 機能	74
V. 「X.509 デジタル証明書」を用いた電子認証	77
VI. IPsec 通信時のパケットフィルタ設定	78
VII. IPsec 設定例 1 (センター / 拠点間の 1 対 1 接続)	79
VIII. IPsec 設定例 2 (センター / 拠点間の 2 対 1 接続)	83
IX. IPsec がつながらないとき	90
第 13 章 L2TPv3 機能	93
I. L2TPv3 機能概要	94
II. L2TPv3 機能設定	95
III. L2TPv3 Tunnel 設定	97
IV. L2TPv3 Xconnect (クロスコネクト) 設定	99
V. L2TPv3 Group 設定	102
VI. Layer2 Redundancy 設定	103
VII. L2TPv3 Filter 設定	105
VIII. 起動 / 停止設定	106
IX. L2TPv3 ステータス表示	108
X. 制御メッセージ一覧	109
XI. L2TPv3 設定例 1 (2 拠点間の L2TP トンネル)	110
XII. L2TPv3 設定例 2 (L2TP トンネル二重化)	114
第 14 章 L2TPv3 フィルタ機能	122
I. L2TPv3 フィルタ 機能概要	123
II. 設定順序について	126
III. 機能設定	127
IV. L2TPv3 Filter 設定	128
V. Root Filter 設定	130
VI. Layer2 ACL 設定	132
VII. IPv4 Extend ACL 設定	134
VIII. ARP Extend ACL 設定	136
IX. 802.1Q Extend ACL 設定	137
X. 802.3 Extend ACL 設定	139
XI. 情報表示	140
第 15 章 PPPoE to L2TP	142
PPPoE to L2TP 機能について	143
第 16 章 SYSLOG 機能	145
syslog 機能の設定	146
第 17 章 攻撃検出機能	149
攻撃検出機能の設定	150
第 18 章 SNMP エージェント機能	151
I. SNMP エージェント機能の設定	152
II. Century Systems プライベート MIB について	154
第 19 章 NTP サービス	155
NTP サービスの設定方法	156
第 20 章 VRRP 機能	158
VRRP の設定方法	159
第 21 章 アクセスサーバ機能	160
I. アクセスサーバ機能について	161
II. 本装置とアナログモデム / TA の接続	162
III. アクセスサーバ機能の設定	163

第22章 UPnP 機能	165
I. UPnP 機能 の設定	166
II. UPnP とパケットフィルタ設定	168
第23章 ダイナミックルーティング(RIP と OSPF)	169
I. ダイナミックルーティング機能	170
II. RIP の設定	171
III. OSPF の設定	172
第24章 スタティックルート設定	179
スタティックルート設定方法	180
第25章 ソースルート機能	182
ソースルート設定	183
第26章 NAT 機能	184
I. 本装置の NAT 機能について	185
II. バーチャルサーバ設定	186
III. 送信元 NAT 設定	187
IV. バーチャルサーバの設定例	188
V. 送信元 NAT の設定例	191
補足：ポート番号について	192
第27章 パケットフィルタリング機能	193
I. 機能の概要	194
II. 本装置のフィルタリング機能について	195
III. パケットフィルタリングの設定	196
IV. パケットフィルタリングの設定例	199
V. 外部から設定画面にアクセスさせる設定	205
補足：NAT とフィルタの処理順序について	206
補足：ポート番号について	207
補足：フィルタのログ出力内容について	208
第28章 ネットワークイベント機能	209
I. 機能の概要	210
II. 各トリガテーブルの設定	212
III. 実行イベントテーブルの設定	214
IV. 実行イベントのオプション設定	215
V. ステータスの表示	216
第29章 仮想インタフェース機能	217
仮想インタフェース機能の設定	218
第30章 GRE 設定	219
GRE の設定	220
第31章 QoS 設定	222
I. QoS について	223
II. QoS 機能の各設定画面について	227
III. 各キューイング方式の設定手順について	228
IV. 各設定画面での設定方法について	229
V. ステータスの表示	236
VI. 設定の編集・削除方法	237
VII. ステータス情報の表示例	238
VIII. クラスの階層構造について	242
IX. TOS について	243
X. DSCP について	245

第 32 章 ゲートウェイ認証機能	246
I. ゲートウェイ認証機能の設定	247
II. ゲートウェイ認証下のアクセス方法	252
III. ゲートウェイ認証の制御方法について	253
第 33 章 検疫フィルタ機能	254
検疫フィルタ機能の設定	255
第 34 章 ネットワークテスト	256
ネットワークテスト	257
第 35 章 簡易 CLI 機能	261
I. 簡易 CLI 機能の概要	262
II. 簡易 CLI 機能のアクセス設定	263
第 36 章 システム設定	267
システム設定	268
時計の設定	268
ログの表示	269
ログの削除	269
パスワードの設定	270
ファームウェアのアップデート	271
設定の保存と復帰	272
設定のリセット	273
再起動	273
本体停止	274
セッションライフタイムの設定	274
設定画面の設定	275
オプション USB フラッシュディスク	276
CLI 設定	277
ARP filter 設定	277
第 37 章 情報表示	278
本体情報の表示	279
第 38 章 詳細情報表示	280
各種情報の表示	281
第 39 章 テクニカルサポート	282
テクニカルサポート	283
第 40 章 運用管理設定	284
I. 各種ボタンの操作	285
II. オプション USB フラッシュディスクの操作	287
付録 A インタフェース名一覧	288
付録 B 工場出荷設定一覧	290
付録 C サポートについて	292

はじめに

ご注意

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

商標の表示

「GIGABIT 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下さい。

絵表示について

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

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



危険

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



警告

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



注意

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

次の絵表示の区分は、お守りいただく内容を説明しています。



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



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

危険



必ず本体に付属している電源ケーブルをご使用ください。



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



ストーブのそばなど高温の場所で使用したり、放置しないでください。











火の中に投入したり、加熱したりしないでください。



製品の隙間から針金などの異物を挿入しないでください。










ご使用にあたって

警告

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

ご使用にあたって

注意

-  湿気やほこりの多いところ、または高温となるところには保管しないでください。故障の原因となります。
-  乳幼児の手の届かないところに保管してください。けがなどの原因となります。
-  長期間使用しないときには、電源ケーブルをコンセントおよび本体から外してください。電源ケーブルの上に重いものを乗せたり、ケーブルを改造したりしないで下さい。また、
-  電源ケーブルを無理に曲げたりしないでください。火災・感電・故障の原因となることがあります。
-  電源ケーブルは必ず電源プラグを持って抜いてください。ケーブルを引っ張ると、ケーブルに傷が付き、火災・感電・故障の原因となることがあります。
-  近くに雷が発生したときには、電源ケーブルをコンセントから抜いて、ご使用をお控え下さい。落雷が火災・感電・故障の原因となることがあります。
-  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品が同梱されております。本製品をお使いいただく前に、内容物が全て揃っているかご確認ください。
万が一、不足がありましたら、お買い上げいただいた店舗、または、弊社サポートデスクまでご連絡くださいますようお願いいたします。

同梱品一覧

品名	数量
本体	1台
AC電源ケーブル	1本
UTPケーブル(CAT5, ストレート 1m)	1本
海外使用禁止シート	1枚
はじめにお読み下さい	1枚
ラックマウント用レール	1式
ラック組み立てマニュアル	1枚
保証書	1枚

第1章

本装置の概要

第1章 本装置の概要

1. 本装置の特長

XR-1100/C、XR-1100/CT(以下、本装置)は次のような特長を持っています。

ギガビット対応

本装置はギガビット対応のインタフェースを4ポート保有しており、最大1Gpbsの高速ルーティングを提供します。

Century Systems 独自 MIB に対応

本製品は標準 MIB-II の他、当社独自の MIB/Trap をサポートしています。独自 MIB/Trap ではシステムや各種サービス、L2TPv3 サービスに関する情報が取得でき、保守性やメンテナンス性に優れた運用が可能になります。

簡易 CLI 機能を搭載

本装置では、表示コマンドを中心とした簡易 CLI (Command Line Interface) 機能を実装しています。ブラウザベースの GUI に比べ、よりスピーディな運用監視が可能です。

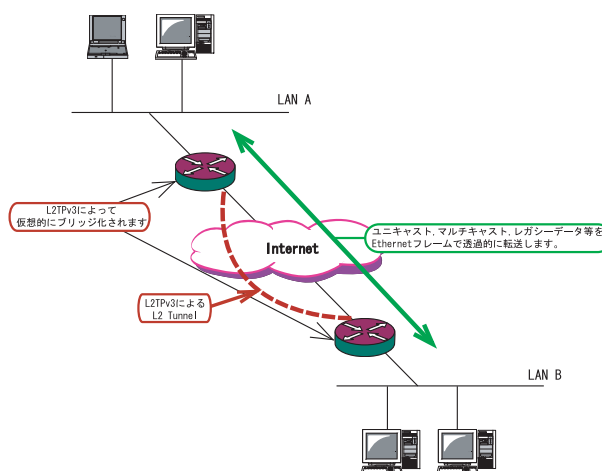
L2TPv3 機能を搭載

本製品は次世代ネットワークのトンネリング及び VPN における主要技術になりつつある L2TPv3 機能を搭載しています。

L2TPv3 機能は、IP ネットワーク上のルータ間で L2TP トンネルを構築します。これにより本製品が仮想的なブリッジとなり、遠隔のネットワーク間でレイヤ2通信が可能となります。

レイヤ2でトンネリングするため、2つのネットワークは HUB で繋がった1つの Ethernet ネットワークとして使うことができます。また上位プロトコルに依存せずにネットワーク通信ができ、TCP/IP だけでなく、任意の上位プロトコル(IPX、AppleTalk、SNA 等)を透過的に転送することができます。

また L2TPv3 機能は、従来の専用線やフレームリレー網ではなく IP 網で利用できますので、低コストな運用が可能です。



L2TPv3 機能につきましては、
第13章「L2TPv3 機能」をご参照下さい。

IPsec 機能を搭載

本製品の IPsec 機能を使うことで、インターネット上で複数の拠点をつなぐ IP 仮想専用線(インターネット VPN)の構築に利用できます。

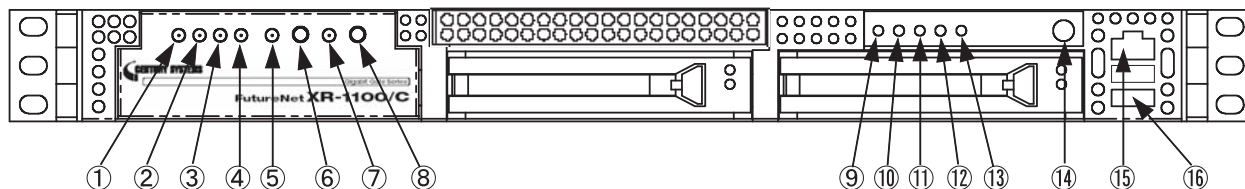
802.1q VLAN に対応

本製品の各 Ethernet ポートで VLAN ID が最大1024 個までの 802.1q マルチプル VLAN を構築できます。インタフェース毎に複数の VLAN セグメントを設定し、LAN 内でのセキュリティを強化することができます。

第1章 本装置の概要

II. 各部の名称と機能

製品前面



システムステータスLED(緑)

本装置が動作状態にあるとき点灯します。

AUX LED(緑)

本装置では使用しません。

Ether3 LED(緑)

Ether3ポートの状態を示します。Linkup時には点灯します。

Ether2 LED(緑)

Ether2ポートの状態を示します。Linkup時には点灯します。

USBステータス LED(橙)

オプションUSBフラッシュディスクが接続され動作状態にあるとき点灯します。USBフラッシュディスクを接続したときは「消灯 点滅 点灯」、Releaseボタンを押したときは「点灯 点滅 消灯」の順序で遷移します。

RELEASEスイッチ

本装置に接続しているオプションUSBフラッシュディスクを取り外すときに押します。詳細は第40章「運用管理設定」をご参照ください。

INITステータス LED(橙)

INITスイッチにより本装置を初期化するときに、本装置の状態を示します。

INITスイッチ

このスイッチを押すことで、本装置を工場出荷状態に戻します。詳細は第40章「運用管理設定」をご参照ください。

Temp LED(赤)

本装置の温度が一定以上になると点灯します。

Ether1 LED(緑)

Ether1ポートの状態を示します。Linkup時には点灯します。

Ether0 LED(緑)

Ether0ポートの状態を示します。Linkup時には点灯します。

CF LED(橙)

CFカードの状態を示します。

パワー LED(緑)

本装置に電源を投入しているときに点灯します。

電源スイッチ

電源スイッチを押すと、動作が停止して待機状態になります。待機状態とは、電源オフ状態と同じですが、本装置には通電している状態です。

ただし、通常は設定画面の「システム設定」「本体停止」画面で待機状態にしてください。待機状態にするのは、本装置がハングアップしたときなどの非常時のみにしてください。

完全に電源をオフにする場合は、電源スイッチを4秒以上押してください。

RS-232 インタフェース(RJ-45コネクタ)

このポートは、使用できません。

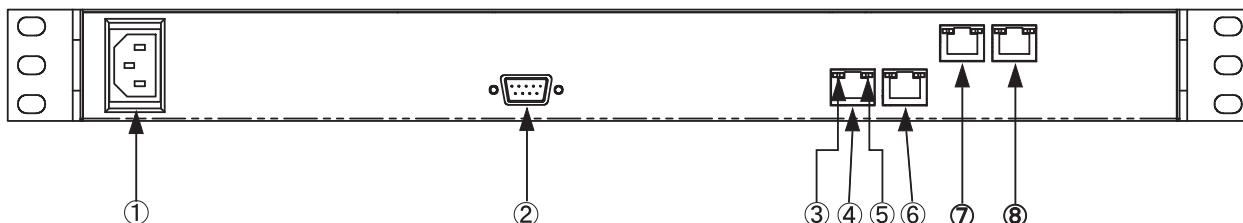
USBインタフェース

オプションのUSBフラッシュデバイスを接続します。下段のみ使用可能です。オプションUSBフラッシュデバイス以外の機器を接続することはできません。

第1章 本装置の概要

II. 各部の名称と機能

製品背面(XR-1100/CT)



電源ケーブル差し込み口

RS-232ポート(D-Sub 9ピン)

モデム /TA を接続します。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使用します。

速度表示ランプ

Ethernet の接続速度を示します。ランプは以下のようなパターンで点灯 / 消灯します。

- 10Base-Tモード : 消灯
- 100Base-TXモード : 緑 点灯
- 1000Base-Tモード : 橙 点灯

Ether0ポート(RJ-45)

Ethernet 規格の UTP ケーブル(LAN ケーブル) を接続します。極性を自動判別します。

LINKランプ

Ethernet ケーブルのリンク状態を示します。ランプは各ポートで以下のようなパターンで点灯 / 消灯します。

- Ether0ポート、Ether1ポート
- Link UP : 橙 点灯
 - Link Down : 消灯
 - データ送受信時 : 橙 点灯

- Ether2ポート、Ether3ポート
- Link UP : 緑 点灯
 - Link Down : 消灯
 - データ送受信時 : 緑 点滅

Ether1ポート(RJ-45)

Ethernet 規格の UTP ケーブル(LAN ケーブル) を接続します。極性を自動判別します。

Ether2ポート(RJ-45)

Ethernet 規格の UTP ケーブル(LAN ケーブル) を接続します。極性を自動判別します。

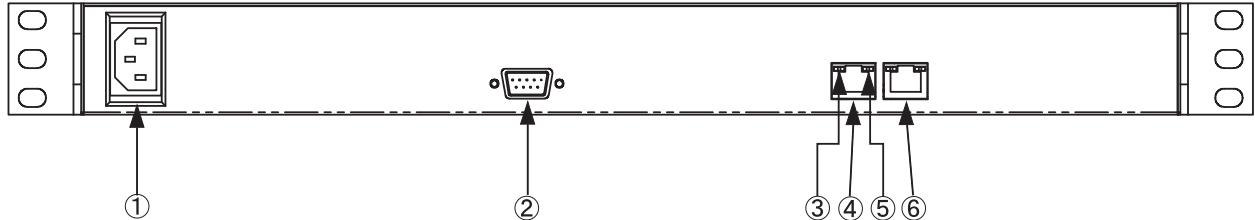
Ether3ポート(RJ-45)

Ethernet 規格の UTP ケーブル(LAN ケーブル) を接続します。極性を自動判別します。

搭載されているインタフェース / ポートは、上記のもの以外は使用できません。

II. 各部の名称と機能

製品背面(XR-1100/C)



電源ケーブル差し込み口

RS-232ポート(D-Sub 9ピン)

モデム / TA を接続します。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使用します。

速度表示ランプ

Ethernet の接続速度を示します。ランプは以下のようなパターンで点灯 / 消灯します。

- 10Base-T モード : 消灯
- 100Base-TX モード : 緑点灯
- 1000Base-T モード : 橙点灯

Ether0ポート(RJ-45)

Ethernet 規格の UTP ケーブル(LAN ケーブル)を接続します。極性を自動判別します。

LINKランプ(緑)

Ethernet ケーブルのリンク状態を示します。ランプは以下のようなパターンで点灯 / 消灯します。

- Link UP : 橙点灯
- Link Down : 消灯

Ether1ポート(RJ-45)

Ethernet 規格の UTP ケーブル(LAN ケーブル)を接続します。極性を自動判別します。

搭載されているインタフェース / ポートは、上記のもの以外は使用できません。

III. 動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

ハードウェア環境

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

本装置の設置

第2章 本装置の設置

本装置の設置

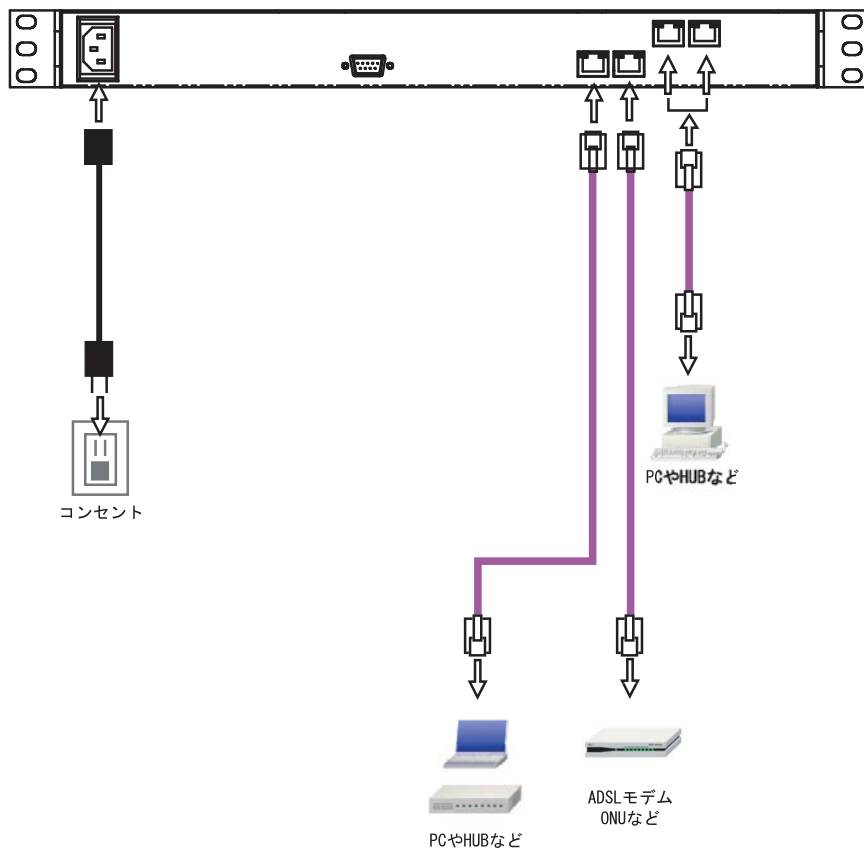
本装置とADSL/ケーブルモデムやコンピュータは、以下の手順で接続してください。

1. 本装置とADSL/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EthernetポートとADSL/ケーブルモデムやONUを、LANケーブルで接続してください。**本装置のEthernetポートは極性を自動判別します。**
3. 本装置の背面にある各EthernetポートとHUBをLANケーブルで接続してください。**本装置のEthernetポートは極性を自動判別します。**
4. 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下さい。
5. 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。

注意点

通信事業者が設置したADSLモデム/ONU等を直接接続できるインタフェースはEther0、Ether1ポートのみとなります。

接続図(例)



(上図はXR-1100/CTでの接続例です)

第3章

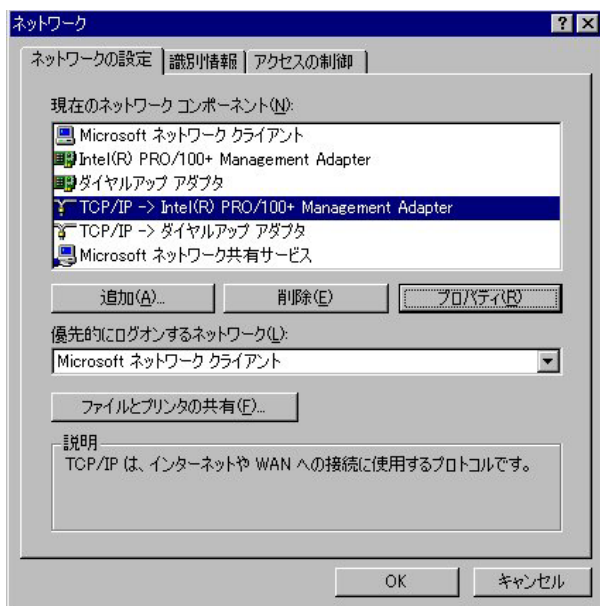
コンピュータのネットワーク設定

第3章 コンピュータのネットワーク設定

1. Windows 95/98/Me のネットワーク設定

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

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

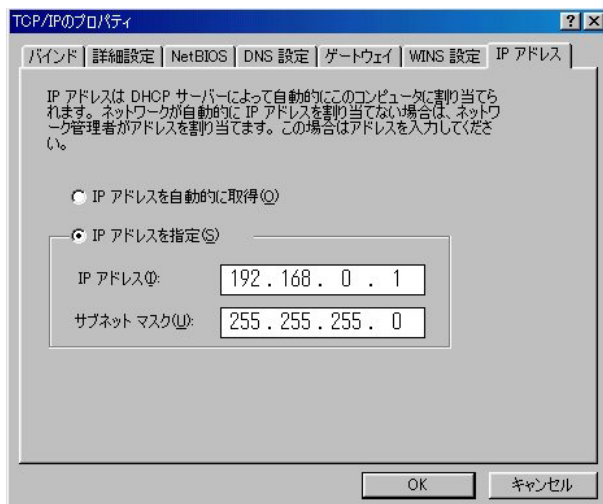


3 続いて「ゲートウェイ」タブをクリックして、新しいゲートウェイに「192.168.0.254」と入力して追加ボタンをクリックしてください。



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

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



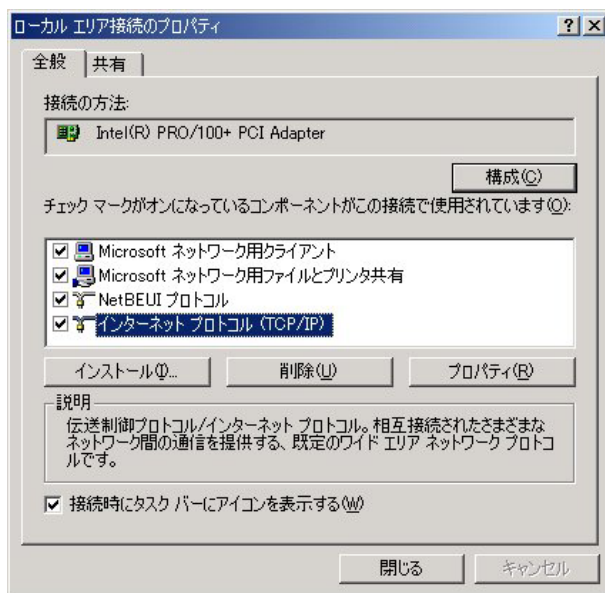
第3章 コンピュータのネットワーク設定

11. Windows 2000 のネットワーク設定

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

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

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

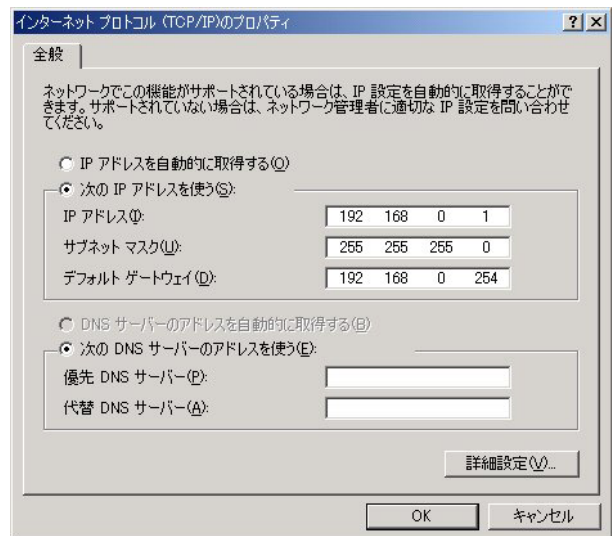


3 「全般」の画面では、「次の IP アドレスを使う」にチェックを入れて以下のように入力します。

IP アドレス 「192.168.0.1」

サブネットマスク 「255.255.255.0」

デフォルトゲートウェイ 「192.168.0.254」



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

第3章 コンピュータのネットワーク設定

III. Windows XPのネットワーク設定

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

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

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

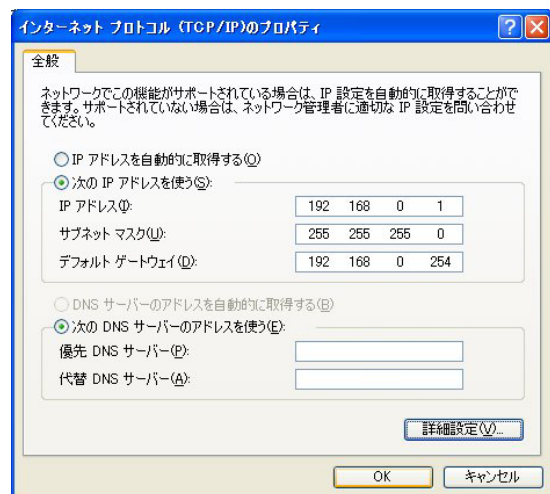


4 「インターネットプロトコル(TCP/IP)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

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。



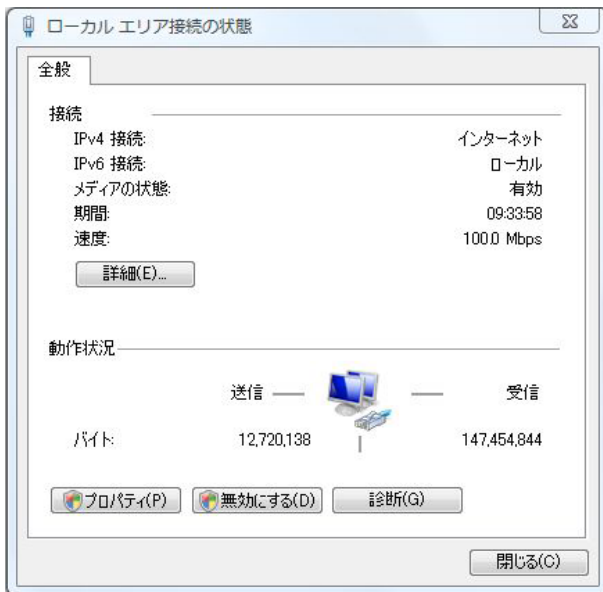
第3章 コンピュータのネットワーク設定

IV. Windows Vistaのネットワーク設定

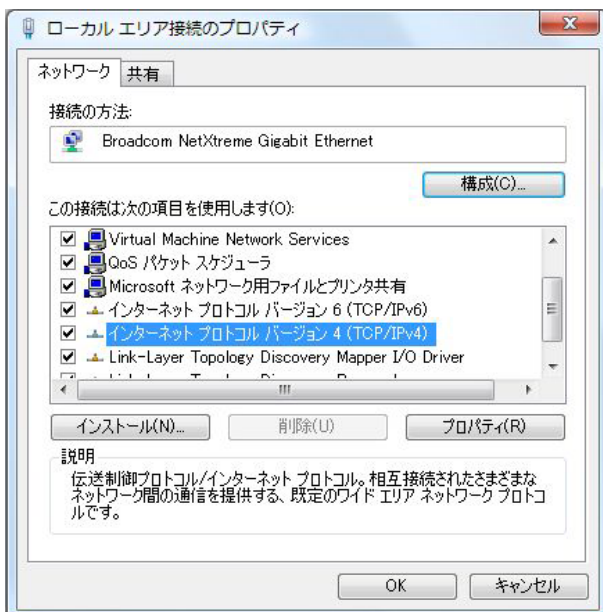
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。



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

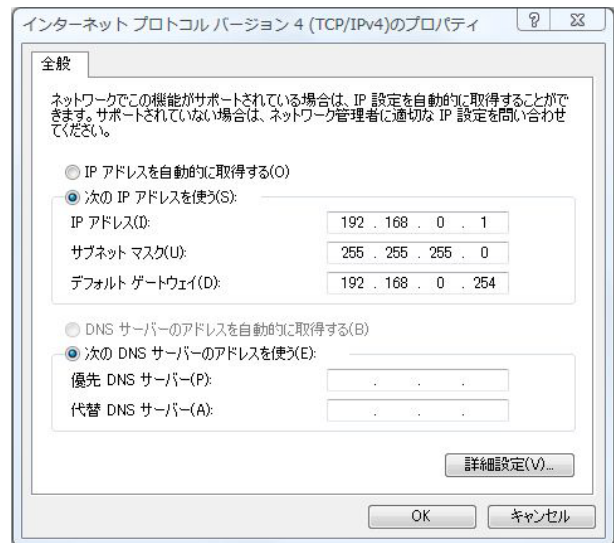


4 「インターネットプロトコルバージョン4 (TCP/IPv4)」の画面では、「次の IP アドレスを使う」にチェックを入れて以下のように入力します。

IP アドレス「192.168.0.1」

サブネットマスク「255.255.255.0」

デフォルトゲートウェイ「192.168.0.254」



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

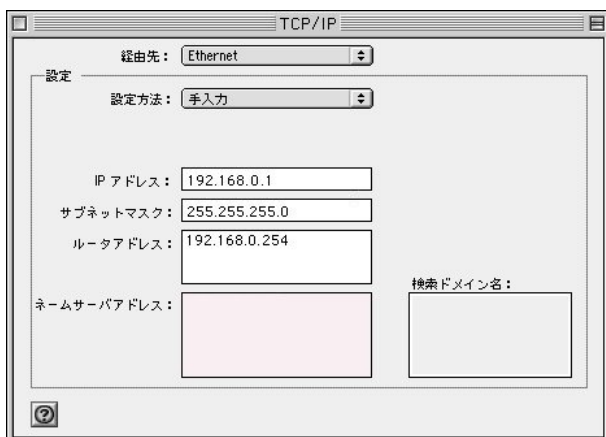
第3章 コンピュータのネットワーク設定

V. Macintosh のネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

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

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

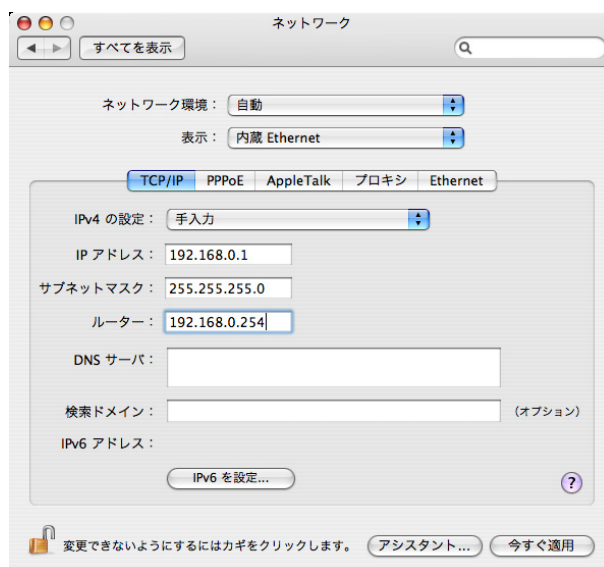


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これで本装置へログインする準備が整いました。

ここでは、Mac OS Xのネットワーク設定について説明します。

1 「システム環境設定」から「ネットワーク」を開きます。

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



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

第3章 コンピュータのネットワーク設定

VI. IPアドレスの確認と再取得

Windows95/98/Me の場合

1 「スタート」 「ファイル名を指定して実行」を開きます。

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

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



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

WindowsNT3.51/4.0/2000 の場合

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

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

```
c:¥>ipconfig /all
```

3 IP 設定のクリアと再取得をするには以下のコマンドを入力してください。

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

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

Macintosh の場合

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

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

第4章

設定画面へのログイン

第4章 設定画面へのログイン

設定画面へのログイン方法

1 各種ブラウザを開きます。

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

http://192.168.0.254:880/

「192.168.0.254」は、Ether0ポートの工場出荷時のアドレスです。アドレスを変更した場合は、そのアドレスを指定してください。

設定画面のポート番号880は変更することができません。

5 ブラウザ設定画面が表示されます。



3 次のような認証ダイアログが表示されます。



4 ダイアログ画面にパスワードを入力します。

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



第5章

インタフェース設定

第5章 インタフェース設定

1. Ethernet ポートの設定

ここでは本装置の各 Ethernet ポートの設定をおこないます。

Web 設定画面「インタフェース設定」->

「Ethernet0(または1、2、3)の設定」をクリックして以下の画面で設定します。

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

リンク監視 0 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)
 リンクダウン時にインターフェースへの通信不可

通信モード
 自動 full-1000M full-100M half-100M full-10M half-10M

(画面はEthernet0での表示例です)

各インタフェースについて、それぞれ必要な情報を入力します。

Ether2、Ether3ポートはXR-1100/CTのみ表示され、設定可能です。

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

IPアドレスに"0"を設定すると、そのインタフェースはIPアドレス等が設定されず、ルーティング・テーブルに載らなくなります。OSPFなどで使用していないインタフェースの情報を配信したくないときなどに"0"を設定してください。

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

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。

IPマスカレード

チェックを入れると、そのEthernetポートでIPマスカレードされます。

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

SPIでDROPしたパケットのLOGを取得チェックを入れると、SPIが適用され破棄(DROP)したパケットの情報をsyslogに出力します。SPIが有効のときだけ動作可能です。ログの出力内容については、第27章「パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

Proxy ARP

Proxy ARPを使う場合にチェックを入れます。

Directed Broadcast

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

Directed Broadcast

IPアドレスのホスト部がすべて1のアドレスのことです。

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

Send Redirects

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

ICMP Redirects

他に適切な経路があることを通知するICMPパケットのことです。

(次ページへ続く)

第5章 インタフェース設定

1. Ethernet ポートの設定

リンク監視

チェックを入れると、Ethernet ポートのリンク状態の監視を定期的に行います。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(ルーティングテーブルから該当のルーティング情報を削除する)。再度リンク状態がアップした場合には、そのインタフェースに関連付けられたルーティング情報の配信を再開します。

監視間隔は1～30秒の間で設定できます。また、0を設定するとリンク監視を行いません。

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

但し、本設定を有効にしたインタフェースがリモートの拠点でのIPsec KeepAliveの送信先アドレスに指定された場合、リンクダウンが発生した時にIPsecトンネルの障害として検出されてしまいます。

回避の方法など、詳細については、第12章「IPsec機能 IV. IPsec Keep-Alive機能」をご覧ください。

ポートの通信モード

XR-1100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。

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

本装置のインタフェースのアドレスを変更した後は、設定画面にアクセスしているホストやその他のクライアントのIP設定もそれにあわせて変更し、変更したIPアドレスの設定画面に再ログインしてください。

11. Ethernet ポートの設定について

[ステートフルパケットインスペクション]

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

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

ステートフルパケットインスペクション機能を有効にすると、そのインタフェースへのアクセスは一切不可能となります。ステートフルパケットインスペクション機能とバーチャルサーバ機能を同時に使う場合等は、パケットフィルタリングの設定をおこなって、外部からアクセスできるように設定する必要があります(第27章「パケットフィルタリング機能」参照)。

[PPPoE 接続時の Ethernet ポート設定]

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

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

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

[IPsec 通信時の Ethernet ポート設定]

本装置を IPsec ゲートウェイとして使う場合は、Ethernet ポートの設定に注意してください。IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが本装置の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

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

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

第5章 インタフェース設定

III. VLAN タギングの設定

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

Web 設定画面「インタフェース設定」-> 「Ethernet0(または1、2、3)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
1	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	eth0.	<input type="checkbox"/>			1500	<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"/>
5	eth0.	<input type="checkbox"/>			1500	<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"/>
7	eth0.	<input type="checkbox"/>			1500	<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"/>
9	eth0.	<input type="checkbox"/>			1500	<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"/>
11	eth0.	<input type="checkbox"/>			1500	<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"/>
13	eth0.	<input type="checkbox"/>			1500	<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"/>
15	eth0.	<input type="checkbox"/>			1500	<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"/>

VLAN-インターフェースの名称は[eth0.TagID]になります
1024個まで登録できます
Tag IDに0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

(Ether0 ポートの表示例です)

devTag ID.

VLAN のタグ ID を設定します。1 から 4094 の間で設定します。各 Ethernet ポートごとに 1024 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>」「eth3.<ID>」となります。

enable

チェックを入れることで設定を有効にします。

IP アドレス、サブネットマスク

VLAN インタフェースの IP アドレスとサブネットマスクを設定します。

MTU

VLAN インタフェースの MTU 値を設定します。

ip masq.

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

spi

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

drop log

チェックを入れると、SPI により破棄(DROP)したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第 27 章「パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

proxy arp

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

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

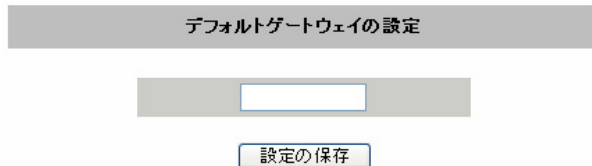
また、VLAN 設定を削除する場合は、dev.Tag ID 欄に「0」を入力して「VLAN の設定の保存」をクリックしてください。

設定情報の表示

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

デフォルトゲートウェイの設定

Web 設定画面「インタフェース設定」->「その他の設定」をクリックして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 エントリの設定

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



(画面は表示例です)

現在の ARP テーブル

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

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

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

新しい ARP エントリ

ARP エントリを手動で登録するときは、ここから登録します。

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

エントリの入力例：

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

固定の ARP エントリ

ARP エントリを固定するときは、ここから登録します。

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

エントリの入力方法は「新しい ARP エントリ」と同様です。

ARP テーブルの確認

「その他の設定」画面中央で、現在の ARP テーブルの内容を確認できます。

ARPテーブル

IP address	HW type	Flags	HW address	Mask	Device
192.168.0.60	0x1	0x0	00:00:00:00:00:00	*	eth0
192.168.0.10	0x1	0x6	00:90:99:BB:30:7A	*	eth0

(画面は表示例です)

第 6 章

PPPoE 設定

第6章 PPPoE 設定

1. PPPoE の接続先設定

Web 設定画面「PPP/PPPoE 設定」をクリックします。

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

プロバイダ名	<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" value="30"/> 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<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P-t-P Gatewayに発行します
UnNumbered-PPP回線使用時に設定できます	
IPアドレス	<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" value="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。)

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、「'」「()」「|」「¥」等の特殊記号については使用できません。

ユーザー ID

プロバイダから指定されたユーザー IDを入力してください。1～63文字まで入力可能です。

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。1～63文字まで入力可能です。

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

<例>

abc(def)g'h abc¥(def¥)g¥'h

DNSサーバ

特に指定のない場合は「プロバイダから自動割り当て」をチェックします。

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

LCPキープアライブ

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

Pingによる接続確認

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

通常は空欄にしておきます。

第6章 PPPoE 設定

1. PPPoE の接続先設定

IP アドレス

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

MSS 設定

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

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

MSS 設定項目以下は設定しません。

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

第6章 PPPoE 設定

11. PPPoE の接続設定と回線の接続 / 切断

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

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"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続
RS232C 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
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
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="xr"/>
中継するメールサーバの アドレス	<input type="text"/>

(画面は XR-1100/CT での表示例です)

接続設定

回線状態

現在の回線状態を表示します。

接続先の選択

どの接続先設定を使って接続するかを選択します。

接続ポート

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

接続形態

「手動接続」 PPPoE (PPP) の接続 / 切断を手動で切り替えます。

「常時接続」本装置が起動すると自動的に PPPoE 接続を開始します。

RS232C 接続タイプ

PPPoE 接続では「通常」を選択します。

IP マスカレード

PPPoE 接続時に IP マスカレードを有効にするかどうかを選択します。

ステートフルパケットインスペクション

PPPoE 接続時に、ステートフルパケットインスペクション (SPI) を有効にするかどうかを選択します。SPI を有効にして「DROP したパケットの LOG を取得」にチェックを入れると、SPI が適用され破棄 (DROP) したパケットの情報を syslog に出力します。SPI が有効のときだけ動作可能です。ログの出力内容については、第 27 章「パケットフィルタリング機能 補足：フィルタのログ出力内容について」をご覧ください。

デフォルトルートの設定

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

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

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

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

III. その他の接続設定

接続 IP 変更お知らせメール機能

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

以下の箇所を設定します。

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	xx <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。

<入力形式> @ <ドメイン名>

<入力例> @mail.xxxxxx.co.jp

IV. バックアップ回線

PPPoE 接続では、「バックアップ回線接続」設定ができます。

[バックアップ回線接続]

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

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

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

回線状態の確認は、ping または OSPF を用います。OSPF については、第 23 章「ダイナミックルーティング (RIP と OSPF)」をご覧ください。

IV. バックアップ回線

バックアップ回線設定

PPPoE 接続設定画面の「バックアップ回線使用時に設定して下さい」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 checked="" type="radio"/> RS232C <input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3
RS232C 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
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 checked="" type="radio"/> PING <input 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	xx <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 接続タイプ

RS232C 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ムは「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のステートフルパケット
インスペクションの動作を選択します。

主回線接続確認のインターバル

主回線接続の確認ためにパケットを送出する間隔を設定します。

主回線の回線断の確認方法

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

Ping 使用時の宛先アドレス

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

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

Ping 使用時の送信元アドレス

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

Ping 発行のリトライインターバルの間隔
Ping をリトライ発行する間隔を指定します。秒単位で指定します。

Ping 使用時の device

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

第6章 PPPoE 設定

IV. バックアップ回線

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なってください。

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

接続変更お知らせメール機能

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

以下の箇所を設定します。

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	<input type="text" value="xr"/>
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。

<入力形式> @ <ドメイン名>

<入力例> @mail.xxxxxx.co.jp

第6章 PPPoE 設定

V. PPPoE 特殊オプション設定

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

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

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

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

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

PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。

PPPoE 特殊オプション
(全回線共通)

- 回線接続時に前回の PPPoE セッションの PADT を強制送出手
- 非接続 Session の IPv4 Packet 受信時に PADT を強制送出手
- 非接続 Session の LCP-EchoRequest 受信時に PADT を強制送出手

回線接続時に前回の PPPoE セッションの PADT を強制送出手する。

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

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

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 を送出手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 を送出手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。

第7章

RS-232 ポートを使った接続
(リモートアクセス機能)

第7章 RS-232ポートを使った接続(リモートアクセス機能)

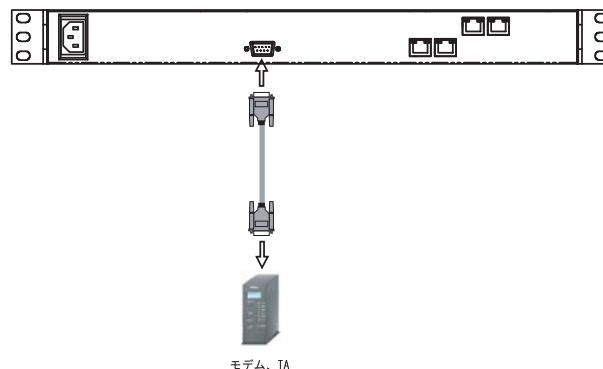
1. 本装置とアナログモデム/TAの接続

本装置は、RS-232ポートを搭載しています。こ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、本装置の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。

アナログモデム/TAのシリアル接続

- 1 本装置本体背面の「RS-232」ポートとアナログモデム/TAのシリアルポートをシリアルケーブルで接続してください。シリアルケーブルは別途ご用意ください。
- 2 全ての接続が完了しましたら、本装置とモデム/TAの電源を投入してください。

接続図



(図はXR-1100/CTでの例です)

第7章 RS-232ポートを使った接続(リモートアクセス機能)

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

プロバイダ名	<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" value="30"/> 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります
Pingによる接続確認	<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PitP-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" value="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。)
-------	--

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"/>
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
ダイヤルタイムアウト	<input type="text" value="60"/> 秒
初期化用ATコマンド	<input type="text" value="AT00V1"/>
回線種別	<input checked="" type="radio"/> 無指定 <input type="radio"/> トーン <input type="radio"/> パルス
ON-DEMAND接続用切断タイマー	<input type="text" value="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

プロバイダ名

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

ユーザー ID

プロバイダから指定されたユーザー IDを入力してください。1～63文字まで入力可能です。

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。1～63文字まで入力可能です。

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

<例> abc(def)g'h abc¥(def¥)g¥'h

DNSサーバ

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

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

LCPキープアライブ pingによる接続確認 IPアドレス MSS設定

上記項目は、リモートアクセス接続の場合は設定のしません。

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。

第7章 RS-232ポートを使った接続(リモートアクセス機能)

II. リモートアクセス回線の接続先設定

ダイヤルタイムアウト

アクセス先にログインするときのタイムアウト時間を設定します。単位は秒です。

シリアルDTE

本装置とモデム /TA間のDTE速度を選択します。
工場出荷値は115200bpsです。

初期化用ATコマンド

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

回線種別

回線のダイヤル方法を選択します。

ON-DEMAND 接続用切断タイマー

PPP 接続設定のRS232C 接続タイプをOn-Demand 接続にした場合の、自動切断タイマーを設定します。
ここで設定した時間を過ぎて無通信状態のときに、PPP 接続を切断します。

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の接続設定を行いません。

第7章 RS-232ポートを使った接続(リモートアクセス機能)

111. 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おこないます。

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

回線状態	回線は接続されていません
接続先の選択	<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"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続
RS232C 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
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
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	xx <input type="text"/>
中継するメールサーバのアドレス	<input type="text"/>

(画面は XR-1100/CT での表示例です)

接続設定

回線状態

現在の回線状態を表示します。

接続先の選択

どの接続先設定を使って接続するかを選択します。

接続ポート

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

接続形態

「手動接続」リモートアクセスの接続 / 切断を手動で切り替えます。

「常時接続」本装置が起動すると自動的にリモートアクセス接続を開始します。

RS232C 接続タイプ

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

IP マスカレード

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を有効にするかどうかを選択します。

デフォルトルートの設定

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

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

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

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

第7章 RS-232ポートを使った接続(リモートアクセス機能)

IV. 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、接続IPお知らせメール機能、バックアップ回線接続設定が可能です。

設定方法については、第6章「PPPoE設定」をご覧ください。

第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

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

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

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

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。

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

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

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

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

またマルチ接続側(主回線ではない側)はフレッツスクエアのように閉じた空間を想定しているため、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下さい。

STEP 1 主接続の接続先設定

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

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 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)用の接続先設定をおこないます。

Web 設定画面「PPP/PPPoE 設定」をクリックし、「接続先設定」のいずれかをクリックして設定します。設定方法については、第6章「PPPoE 設定」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

例えば

ネットワークアドレスに「172.26.0.0」

ネットマスクに「255.255.0.0」

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

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

このどちらも設定しない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」をクリックして接続先設定は完了です。

STEP 3 PPPoE 接続の設定

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

「PPP/PPPoE 設定」->「接続設定」を開きます。

[主接続用の接続設定]

以下の部分で設定します。

回線状態	回線は接続されていません
接続先の選択	<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"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3
接続形態	<input checked="" type="radio"/> 手動接続 <input type="radio"/> 常時接続
RS232C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
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
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	xr <input type="text"/>
中継するメールサーバのアドレス	<input type="text"/>

(画面はXR-1100/CTでの表示例です)

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、本装置のインタフェースを選択します。

接続形態

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

IPマスカレード

通常は「有効」を選択します。

LAN側をグローバルIPで運用している場合は「無効」を選択します。

ステートフルパケットインスペクション

任意で選択します。

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

デフォルトルート

「有効」を選択します。

接続 IP 変更お知らせメール

任意で設定します。

続いてマルチ接続用の接続設定をおこないます。

[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"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3
RS232C 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
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"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3
RS232C 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
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"/> RS232C <input type="radio"/> Ether0 <input checked="" type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3
RS232C 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

(画面はXR-1100/CTでの表示例です)

マルチ接続 #2 ~ #4

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

接続先の選択

マルチ接続用の接続先設定を選択します。

接続ポート

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

RS232C 接続タイプ

RS232C を使って複数アカウント同時接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

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

IP マスカレード

任意で選択します。通常は「有効」にします。

ステートフルパケットインスペクション

任意で選択します。

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)。

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 4 PPPoE 接続の開始

すべて設定した後、「接続」をクリックして PPPoE 接続を開始します。

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

接続に成功した場合：

主回線で接続しています。

マルチセッション回線1で接続しています。

接続できていない場合：

主回線で接続を試みています。

マルチセッション回線1で接続を試みています。

などと表示されます。

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

複数アカウント同時接続時の注意点

通常の ISP とフレッツスクエアへの同時接続をするには、本装置の「DNS キャッシュ機能」を「有効」にし、各 PC の DNS サーバ設定を本装置の IP アドレスに設定してください。

本装置に名前解決要求をリレーさせないと、同時接続ができません。

第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

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

DNSキャッシュ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
DHCP(Relay)サーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
UPnPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
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
L2TPv3	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
攻撃検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
VRRPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい	停止中

ここで

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

をおこないます。

サービスの設定

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

DNS キャッシュ機能

DHCP サーバ機能

DHCP リレー機能

IPsec 機能

UPnP 機能

ダイナミックルーティング機能

PPPoE toL2TP 機能

L2TPv3 機能

SYSLOG 機能

攻撃検出機能

SNMP エージェント機能

NTP サービス

VRRP サービス

アクセスサーバ機能

サービスの起動と停止

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

第 10 章

DNS リレー / キャッシュ機能

第10章 DNSサーバ機能

DNS リレー / キャッシュ機能の設定

DNS リレー機能

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キャッシュ機能」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 type="radio"/> 使用する <input checked="" type="radio"/> 使用しない

設定の保存

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下さい。ISPから指定されたDNSサーバへリレーする場合は本設定の必要はありません。

root server

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

設定後に「設定の保存」をクリックして設定完了です。

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

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. 本装置のDHCP関連機能について

本装置は、以下の4つのDHCP関連機能を搭載しています。

DHCPクライアント機能

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

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

DHCPクライアント機能の設定は第5章「インタフェース設定」を参照してください。

DHCPサーバ機能

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

IPアドレスの固定割り当て

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

DHCPリレー機能

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

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

11. DHCPサーバ機能の設定

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

サブネット	サブネットワーク	サブネットマスク	ブロードキャスト	リース開始アドレス	リース終了アドレス	ルータアドレス	ドメイン名	プライマリDNS	セカンダリDNS	標準リース時間(秒)	最大リース時間(秒)	プライマリWINSサーバー	セカンダリWINSサーバー	スコープID
<input checked="" type="checkbox"/> サブネット1	192.168.0.0	255.255.255.0	192.168.0.255	192.168.0.10	192.168.0.100	192.168.0.254	localdomain.co.jp	192.168.0.254		600	7200			
<input type="checkbox"/> サブネット2														
<input type="checkbox"/> サブネット3														
<input type="checkbox"/> サブネット4														

(画面はXR-1100/CTでの表示例です)

DHCPサーバ/リレー機能設定

画面上部「DHCPサーバの設定」をクリックします。

サーバの選択

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

上位DHCPサーバのIPアドレス

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

DHCP relay over PPPoE

PPPoE接続を経由してDHCPリレー機能をおこなうときに「PPPoE上で使用する」を選択してください。主にNTT東西の提供する「フレッツオフィス」の閉域網環境において利用します。

サブネット

DHCPサーバ機能の動作設定をおこないます。

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

各サブネットごとの詳細設定は以下の通りです。

サブネットワーク

DHCPサーバ機能を有効にするサブネットワーク空間のアドレスを指定します。

サブネットマスク

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

ブロードキャスト

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

リース開始アドレス/終了アドレス

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

第11章 DHCPサーバ/リレー機能

11.1. DHCPサーバ機能の設定例

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、本装置のインタフェースのIPアドレスを指定します。

ドメイン名

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

プライマリ/セカンダリDNS

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

標準リース時間

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

最大リース時間

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

プライマリ/セカンダリWINSサーバー

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。必要であれば指定してください。

スコープID

DHCPクライアントに通知するNetBIOSスコープIDを指定します。WINSサーバー設定時に有効になります。

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

DHCPサーバ機能の設定例

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

上記条件の場合の設定例です。

サブネットワーク	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	192.168.0.1
リース終了アドレス	192.168.0.30
ルータアドレス	192.168.0.254
ドメイン名	
<input checked="" type="checkbox"/> サブネット1	
プライマリDNS	192.168.0.254
セカンダリDNS	
標準リース時間(秒)	3600
最大リース時間(秒)	18000
プライマリWINSサーバー	
セカンダリWINSサーバー	
スコープID	

第11章 DHCPサーバ/リレー機能

IV. IPアドレス固定割り当て設定

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

設定方法

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

No.	MACアドレス	IPアドレス	削除
1	<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"/>

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

<入力例> **00:80:6d:49:ff:ff**

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

入力が終わりましたら「設定/削除の実行」をクリックして設定完了です。

固定割り当て機能は、DHCPサーバ機能を再起動してから有効になります。

エントリの削除方法

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

第 12 章

IPsec 機能

1. 本装置の IPsec 機能について

鍵交換について

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

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

認証方式について

XR-1100 シリーズでは「共通鍵方式」「RSA 公開鍵方式」「X.509」による認証に対応しています。ただしアグレッシブモードは「共通鍵方式」にのみ対応、「X.509」はメインモードにのみ対応しています。

暗号化アルゴリズム

シングル DES とトリプル DES、AES128bit をサポートしています。暗号化はソフト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-1100 は ESP の認証機能を利用していますので、AH での認証はおこなっていません。

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

IPsec 使用時の通信可能対地数

512 拠点まで IPsec 接続が可能です。

IPsec とインターネット接続

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

NAT トラバーサルに対応しています。

他の機器との接続実績について

2005 年 1 月現在、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 Client (SSH Sentinel)
- Linux サーバ (FreeS/WAN)

11. IPsec 設定の流れ

PreShared(共通鍵)方式での IPsec 通信

STEP 1 共通鍵の決定

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

STEP 2 共通鍵の交換

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

STEP 3 本装置側の設定

自分側の本装置の設定をおこないます。

STEP 4 IKE/ISAKMP ポリシーの設定

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

STEP 5 IPsec ポリシー設定

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

STEP 6 IPsec の起動

本装置の IPsec 機能を起動します。

STEP 7 IPsec 接続の確認

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

RSA(公開鍵)方式での IPsec 通信

STEP 1 公開鍵・暗号鍵の生成

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

STEP 2 公開鍵の交換

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

STEP 3 本装置側の設定

自分側の本装置の設定をおこないます。

STEP 4 IKE/ISAKMP ポリシーの設定

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

STEP 5 IPsec ポリシー設定

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

STEP 6 IPsec の起動

本装置の IPsec 機能を起動します。

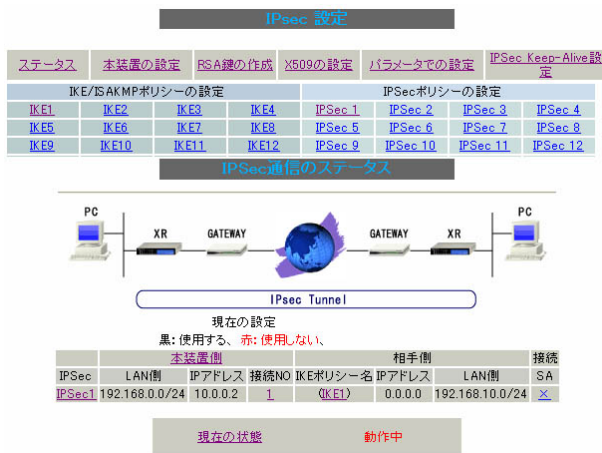
STEP 7 IPsec 接続の確認

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

III. IPsec 設定

STEP 0 設定画面を開く

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



(画面は表示例です)

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

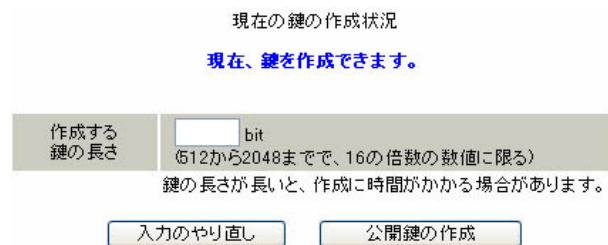
IPsec に関する設定・確認は、全てこの設定画面からおこなえます。

STEP 1,2 鍵の作成・交換

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

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

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



- 2 作成する鍵の長さを指定して「公開鍵の作成」をクリックします。

鍵の長さは512bit から 2048bit までで、16 の倍数となる数値が指定可能です。

現在の鍵の作成状況が「鍵を作成できます」の表示の時に限り、作成可能です。

- 3 鍵を生成します。「鍵を作成しました。」のメッセージが表示されると、鍵の生成が完了です。

生成した鍵は、後述する「本装置側の設定」に自動的に反映されます。

またこの鍵は公開鍵となりますので、相手側にも通知してください。

III. IPsec 設定

STEP 3 本装置側の設定をおこなう

IPsec 設定画面上部の「本装置の設定」をクリックして設定します。

[本装置の設定]

「本装置の設定」をクリックします。

MTU, MSS の設定	
主回線使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
マルチ#2 回線使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
マルチ#3 回線使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
マルチ#4 回線使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
バックアップ回線使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
Ether 0 ポート使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
Ether 1 ポート使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
Ether 2 ポート使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
Ether 3 ポート使用時の ipsec インターフェイスの設定	MTU 値 <input type="text" value="1500"/> MSS 設定 <input type="radio"/> 無効 <input type="radio"/> 有効 MSS 値 <input type="text"/> Byte
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	<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"/>
<input type="button" value="入力のやり直し"/> <input type="button" value="設定の保存"/>	

MTU, MSS の設定

IPsec 接続時の MTU/MSS 値を設定します。各インターフェイスごとに設定できます。(指定可能範囲 MTU:68-1500, MSS:1-1460)

NAT Traversal の設定

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

「NAT Traversal」

NAT トラバーサル機能を使うかどうかを選択します。

「Virtual Private 設定」

接続相手のクライアントが属しているネットワークと同じネットワークアドレスを入力します。以下のような書式で入力してください。

%v4:<ネットワーク>/<マスクビット値>

「鍵の表示」

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

PSK 方式や X.509 電子証明を使う場合はなにも表示されません。

[本装置側の設定]

「本装置側の設定」の 1 ~ 8 のいずれかをクリックします。ここで本装置の IP アドレスやインターフェイス ID を設定します。

IKE/ISAKMP の設定1	
インターフェイスの IP アドレス	<input type="text" value="%ppp0"/>
上位ルータの IP アドレス	<input type="text"/>
インターフェイスの ID	<input type="text" value="@ejitsu"/> (例: @xr.centurysys)

インターフェイスの IP アドレス

[固定アドレスの場合]

本装置に設定されている IP アドレスをそのまま入力します。

[動的アドレスの場合]

PPP/PPPoE 主回線接続の場合は「%ppp0」と入力します。Ether0(Ether1)ポートで接続している場合は「%eth0(%eth1)」と入力します。

上位ルータの IP アドレス

空欄にしておきます。

III. IPsec 設定

インタフェースの ID

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

<入力形式> @ <任意の文字列>

<入力例> @centurysystems

(@ の後は、任意の文字列でかまいません。)

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

最後に「設定の保存」をクリックして設定完了です。続いて **IKE/ISAKMP ポリシー** の設定をおこないます。

STEP 4 IKE/ISAKMP ポリシーの設定

IPsec 設定画面上部の「IKE/ISAKMP ポリシーの設定」1 ~ 1024 のいずれかをクリックして、以下の画面から設定します。

IKE/ISAKMP の設定	
IKE/ISAKMP ポリシー名	center-A
接続する本装置側の設定	本装置側の設定1
インタフェースの IP アドレス	60.43.36.244
上位ルータの IP アドレス	
インタフェースの ID	(例: @xr.centurysys)
モードの設定	aggressive モード
transform の設定	1 番目 group2-3des-sha1
	2 番目 使用しない
	3 番目 使用しない
	4 番目 使用しない
IKE のライフタイム	3600 秒 (1081 ~ 28800 秒まで)
鍵の設定	
<input checked="" type="radio"/> PSK を使用する <input type="radio"/> RSA を使用する <small>(X509 を使用する場合は RSA に設定してください)</small>	NgsIPsecA
X509 の設定	
接続先の証明書の設定 <small>(X509 を使用しない場合は必要ありません)</small>	

(画面は表示例です)

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

IKE/ISAKMP ポリシー名

設定名を任意で設定します。(省略可)

インタフェースの 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。

III. IPsec 設定

上位ルータの IP アドレス
空欄にしておきます。

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

<入力形式> @ <任意の文字列>

<入力例> @centurysystems

@の後は、任意の文字列でかまいません。

**対向側装置への割り当てが固定アドレスの場合は
設定の必要はありません。**

モードの設定

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

transform の選択

ISAKMP SA の折衝に必要な暗号化アルゴリズム等の
組み合わせを選択します。本装置は、以下のもの
の組み合わせが選択できます。

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

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

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

IKE のライフタイム

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

鍵の設定

[PSK 方式の場合]

「PSK を使用する」にチェックして、相手側と任意
に決定した共通鍵を入力してください。

[RSA 公開鍵方式の場合]

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

X509 の設定

「X.509」設定で IPsec 通信をおこなう場合は、相
手側のデジタル証明書をテキストボックス内に貼
り付けます。

最後に「設定の保存」をクリックして設定完了です。

続いて、IPsec ポリシーの設定をおこないます。

III. IPsec 設定

STEP 5 IPsec ポリシーの設定

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

<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない <input type="radio"/> Responderとして使用する <input type="radio"/> On-Demandで使用する	
使用するIKEポリシー名の選択	center-A (IKE1) ▼
本装置側のLAN側のネットワークアドレス	172.28.20.0/24 (例:192.168.0.0/24)
相手側のLAN側のネットワークアドレス	0.0.0.0/0 (例:192.168.0.0/24)
PH2のTransFormの選択	3des-sha1 ▼
PFS	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
DH Groupの選択(PFS使用時に有効)	group2 ▼
SAのライフタイム	28800 秒 (1081~86400秒まで)
DISTANCE	1 (1~255まで)

(画面は表示例です)

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

最初にIPsecの起動状態を選択します。

「使用する」はinitiatorにもresponderにもなりません。

「使用しない」は、そのIPsecポリシーを使用しません。

「Responderとして使用する」は、サービス起動時や起動中のIPsecポリシー追加時に、responderとしてIPsec接続を待ちます。XR-1100が固定IPアドレス設定で接続相手が動的IPアドレス設定の場合は、本値を選択して下さい。

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下さい。メイン側のIPsecSAで障害を検知した場合、Initiatorとして接続を開始します。

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

使用するIKEポリシー名の選択

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

本装置側のLAN側のネットワークアドレス
自分側のXR-1100に接続しているLANのネットワークアドレスを入力します。ネットワークアドレス/マスクビット値の形式で入力します。

[入力例] **192.168.0.0/24**

相手側のLAN側のネットワークアドレス
相手側のIPsec装置に接続されているLANのネットワークアドレスを入力します。ネットワークアドレス/マスクビット値の形式で入力します。設定の要領は「本装置側のLAN側のネットワークアドレス」と同様です。

但し、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を接続相手に送ります。

(次ページに続きます)

第12章 IPsec 機能

III. IPsec 設定

SA のライフタイム

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

DISTANCE

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

なお、本設定は省略可能です。省略した場合は「1」として扱います。

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

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

[IPsec 通信時の Ethernet ポート設定について]

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

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが XR-1100 の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 の設定で、且つ、XR-1100 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-1100 の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

STEP 6 IPsec 機能を起動する

「各種サービスの設定」をクリックして、以下の画面を開きます。

DNSキャッシュ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
DHCP(Relay)サーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
UPnPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
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
L2TPv3	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
SYNLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中
攻撃検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
VRBPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい	停止中

動作状態の制御

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

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

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

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

III. IPsec 設定

STEP 7 IPsec 接続を確認する

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

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

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

及び

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

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

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

(2)のメッセージは、IPsec SA が正常に確立したことを示しています。

STEP 8 IPsec ステータス確認の確認

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

IPsec 設定

ステータス	本装置の設定	ISA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			
IK E1	IK E2	IK E3	IK E4	IPSec 1	IPSec 2	IPSec 3	IPSec 4
IK E5	IK E6	IK E7	IK E8	IPSec 5	IPSec 6	IPSec 7	IPSec 8
IK E9	IK E10	IK E11	IK E12	IPSec 9	IPSec 10	IPSec 11	IPSec 12

IPsec通信のステータス

現在の設定
黒: 使用する、赤: 使用しない、

IPsec	LAN側	IPアドレス	接続NO	IKEポリシー名	相手側 IPアドレス	LAN側	接続
IPSec1	192.168.0.0/24	10.0.0.2	1	(IKE1)	0.0.0.0	192.168.10.0/24	SA

現在の状態 動作中

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

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

また、それぞれの設定番号をクリックすると、設定画面に移ることができます。

第 12 章 IPsec 機能

IV. IPsec Keep-Alive 機能

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

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

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

Policy No	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	動作オプション 1	動作オプション 2	interface	backup SA	restart
1	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
2	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
3	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
4	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
5	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
6	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
7	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
8	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
9	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
10	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
11	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
12	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
13	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
14	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
15	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>
16	<input type="checkbox"/>			30	3	0	<input type="checkbox"/>	<input type="checkbox"/>	eth0/0		<input type="checkbox"/>

enable

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

source address

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

destination address

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

interval(sec)

watch count

ping を発行する間隔を設定します。

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

timeout/delay(sec)

後述の「動作オプション 1」の設定に応じて、入力値の意味が異なります。

・動作オプション 1 が有効の場合

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

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

・動作オプション 1 が無効の場合

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

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

動作オプション 1

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

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

注) 本オプションは v1.3.0 での新規追加オプションです。チェックを入れない場合、IPsec ネゴシエーションと Keep-Alive が非同期に行われるため、タイミングによっては IPsecSA の確立と ping の応答待ちタイムアウトが重なってしまい、確立直後の IPsecSA を切断してしまう場合があります。

IV. IPsec Keep-Alive 機能

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

・フェーズ1 (イニシエーションフェーズ)

ネゴシエーションを開始し、IPsec ポリシー確立中の状態です。

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

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

フェーズ3に移行するまでpingの送出は行いません。

・フェーズ2 (ネゴシエーションT.O. フェーズ)

フェーズ1におけるネゴシエーションが失敗、またはタイムアウトした状態です。

この時、バックアップSAを起動し、フェーズ1に戻ります。

・フェーズ3 (ポリシー確立フェーズ)

IPsec ポリシーが正常に確立した状態です。

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

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

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

この後、pingの応答がタイムアウトした場合は、フェーズ4に移行します。

・フェーズ4 (ポリシーダウンフェーズ)

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

さらに、バックアップSAを起動させた後、フェーズ1に戻ります。

動作オプション2

本オプションは「動作オプション1」が無効の場合のみ、有効になります。

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

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

注) 本オプションはv1.3.0以前での「flag」オプションと同じものです。

interface

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

backup SA

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

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

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

< 入力例 >
1_2_3

(次ページに続きます)

第12章 IPsec 機能

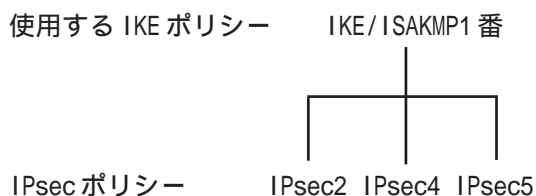
IV. IPsec Keep-Alive 機能

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>



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

remove

設定を削除したいときにチェックします。

最後に「設定 / 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。

destination アドレスとリンク監視について

本装置が対向 XR の Keep-Alive の destination アドレスに指定されており、かつ、そのインタフェース上で「リンクダウン時にインタフェースへの通信不可」(第5章「インタフェース設定 1. Ethernet ポートの設定」参照) を有効にすると、インタフェースがリンクダウンした時に、Keep-Alive にも応答しなくなるため、IPsec ポリシーがダウンしてしまいます。

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

< loopback 仮想インタフェース設定例 >

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

インタフェース	仮想V/F番号	IPアドレス	ネットマスク	削除
lo	0	192.168.20.250	255.255.255.255	<input type="checkbox"/>

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

< 対向 XR の IPsec Keep-Alive 設定例 >

enable	source address	destination address	intf
<input checked="" type="checkbox"/>	192.168.0.254	192.168.20.250	

・destination address として「lo:0」に設定したアドレス「192.168.20.250」を指定します。

第12章 IPsec機能

V. 「X.509 デジタル証明書」を用いた電子認証

本装置はX.509 デジタル証明書を用いた電子認証方式に対応しています。

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

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

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

設定は、IPsec 設定画面内の「X.509 の設定」から行えます。

[X.509 の設定]

「X.509 の設定」画面 「X.509 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"/>

X509 の設定

X.509 の使用 / 不使用を選択します。

設定した接続先の証明書のみを使用する

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

証明書のパスワード

証明書のパスワードを入力します。

[CA の設定]

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

[本装置側の証明書の設定]

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

[本装置側の鍵の設定]

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

[失効リストの設定]

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

[その他の設定について]

「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。さらにその下の「X.509」設定で、IPsec 通信をおこなう場合は、相手側のデジタル証明書をテキストボックス内に貼り付けます。

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。

以上でX.509 の設定は完了です。

第12章 IPsec機能

VI. IPsec通信時のパケットフィルタ設定

ステートフルパケットインスペクション機能を使っていたり、パケットフィルタの設定によっては、IPsec通信ができない場合があります。

このような場合はIPsec通信でのデータをやりとりできるように、パケットフィルタの設定を追加する必要があります。

IPsecでは、以下の2種類のプロトコル・ポートを使用します。

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

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

<設定例>

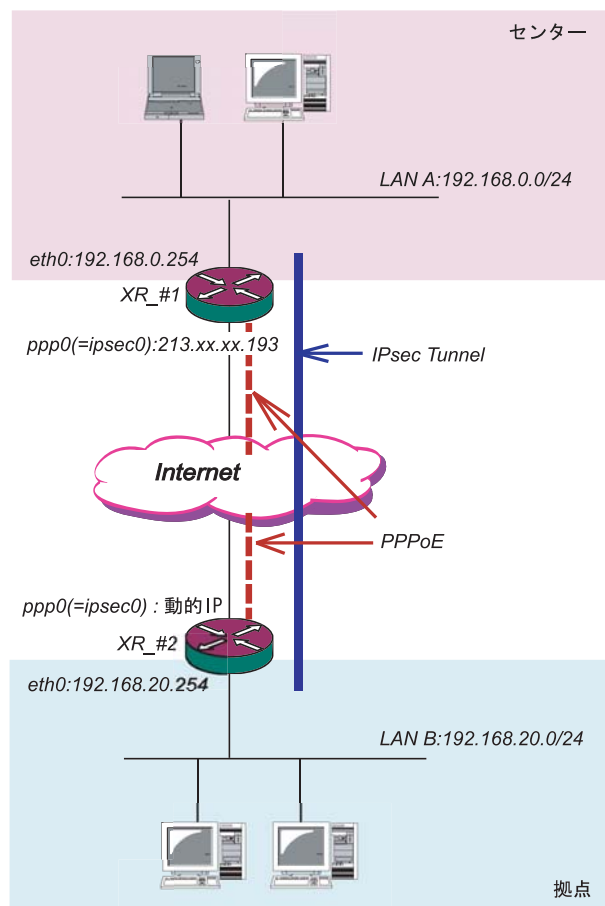
No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート	LOG	削除
1	ppp0	パケット受信時	許可	udp				500	<input type="checkbox"/>	<input type="checkbox"/>
2	ppp0	パケット受信時	許可	esp					<input type="checkbox"/>	<input type="checkbox"/>

第12章 IPsec 機能

VII. IPsec 設定例 1 (センター / 拠点間の1対1接続)

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

< 設定例 1 >



< 接続条件 >

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

XR_#1(センター側 XR)の設定
各設定画面で下記のように設定します。

「本装置の設定」

「本装置側の設定 1」を選択します。

インターフェースの IP アドレス	213.xx.xx.193
上位ルータの IP アドレス	%ppp0
インターフェースの ID	<input type="text"/> (例:@xr.centurysys)

インターフェースの IP アドレス

「213. x x . x x . 193」

上位ルータの IP アドレス

「%ppp0」

PPPoE 接続かつ、固定 IP アドレスの場合は、必ずこの設定にします。

インターフェースの ID

[空欄]

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

第12章 IPsec機能

VII. IPsec設定例 1 (センター / 拠点間の1対1接続)

「IKE/ISAKMPポリシーの設定」

「IKE1」を選択します。

IKE/ISAKMPの設定	
IKE/ISAKMPポリシー名	<input type="text"/>
接続する本装置側の設定	本装置側の設定1
インターフェースのIPアドレス	0.0.0.0
上位ルータのIPアドレス	<input type="text"/>
インターフェースのID	@host (例:@x.centurysys)
モードの設定	aggressiveモード
transformの設定	1番目 group2-3des-sha1 2番目 使用しない 3番目 使用しない 4番目 使用しない
IKEのライフタイム	3600 秒 (1081~28800秒まで)
鍵の設定	
<input checked="" type="radio"/> PSKを使用する <input type="radio"/> RSAを使用する <small>×509を使用する場合はRSAに設定してください</small>	test_key
×509の設定	
接続先の証明書の設定 <small>×509を使用しない場合は必要ありません</small>	<input type="text"/>

IKE/ISAKMPポリシー名 「(任意で設定します)」

接続する本装置側の設定 「本装置側の設定1」

インターフェースのIPアドレス 「0.0.0.0」

対向装置が動的アドレスの場合は必ずこの設定に
して下さい。

上位ルータのIPアドレス [空欄]

インターフェースのID
「@host」(@以降は任意の文字列)

上記の2項目は、対向装置の「本装置の設定」と
同じものを設定します。

モードの設定 「aggressiveモード」

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

IKEのライフタイム 「3600」(任意の設定値)

鍵の設定

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

「IPsecポリシーの設定」

「IPsec1」を選択します。

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

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

使用するIKEポリシー名の選択 「IKE1」

本装置側のLAN側のネットワークアドレス
「192.168.0.0/24」

相手側のLAN側のネットワークアドレス
「192.168.20.0/24」

PH2のTransFormの選択 「すべてを送信する」

PFS 「使用する」(推奨)

DH Groupの選択 「指定しない」

SAのライフタイム 「28800」(任意の設定値)

DISTANCE [空欄]

省略した場合は、自動的にディスタンス値を「1」
として扱います。

「IPsec Keep-Aliveの設定」

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

第12章 IPsec機能

VII. IPsec設定例1 (センター/拠点間の1対1接続)

XR_#2(拠点側XR)の設定
各設定画面で下記のように設定します。

「本装置の設定」

「本装置側の設定1」を選択します。

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

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

上位ルータのIPアドレス [空欄]
PPPoE接続かつ動的アドレスの場合は、空欄にして下さい。

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

「IKE/ISAKMPポリシーの設定」

「IKE1」を選択します。

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

IKE/ISAKMPポリシー名 「(任意で設定します)」

接続する本装置側の設定 「本装置側の設定1」

インターフェースのIPアドレス
「213.xx.xx.193」

対向装置のIPアドレスを設定します。

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

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

モードの設定 「aggressive モード」

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

IKEのライフタイム 「3600」(任意の設定値)

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

第12章 IPsec 機能

VII. IPsec 設定例 1 (センター / 拠点間の1対1接続)

「IPSecポリシーの設定」

「IPSec1」を選択します。

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

「使用する」を選択します。

動的アドレスの場合は、必ず initiator として動作させます。

使用する IKE ポリシー名の選択 「IKE1」

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

相手側のLAN側のネットワークアドレス
「192.168.0.0/24」

PH2のTransFormの選択 「すべてを送信する」

PFS 「使用する」(推奨)

DH Groupの選択 「指定しない」

SAのライフタイム 「28800」(任意の設定値)

DISTANCE [空欄]

省略した場合は、自動的にディスタンス値を「1」として扱います。

「IPsec Keep-Aliveの設定」

PolicyNo.1の行に設定します。

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	Action 1	Action 2	interface	backup SA
1	<input checked="" type="checkbox"/>	192.168.20.254	192.168.0.254	30	3	60		チェック	ipsec0	

enable にチェックを入れます。

source address 「192.168.20.254」

destination address 「192.168.0.254」

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

interval 「30」(任意の設定値)

watch count 「3」(任意の設定値)

timeout/delay 「60」(任意の設定値)

動作オプション1を無効にするため、本値はdelay (ping送出開始待ち時間)=60秒を意味します。

動作オプション1 [空欄]

動作オプション2 「チェック」

interface 「ipsec0」

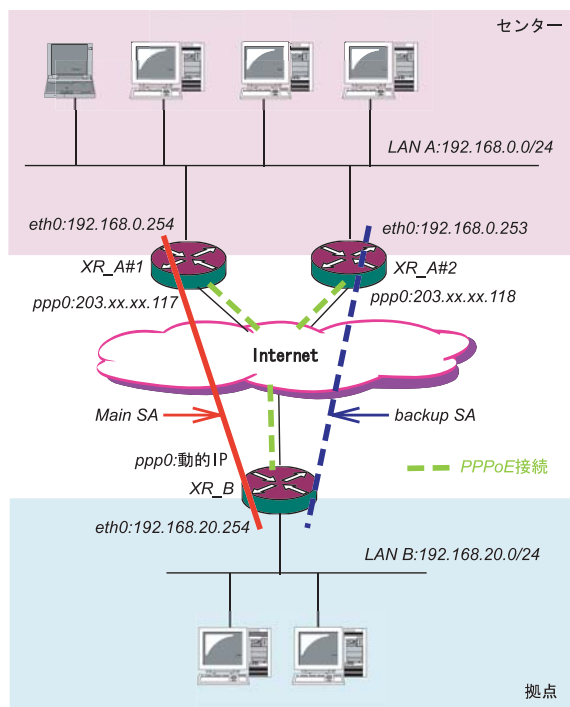
ppp0 上のデフォルトの IPsec インタフェース名は "ipsec0" です。

backupSA [空欄]

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

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

< 設定例 2 >



< 接続条件 >

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

「本装置の設定」

XR_A#1 (センター側 XR#1) の設定

「本装置側の設定 1」を選択します。

インタフェースの IP アドレス	203.xx.xx.117
上位ルータの IP アドレス	%ppp0
インタフェースの ID	<input type="text"/> (例: @xr.centurysys)

インタフェースの IP アドレス

「203.xx.xx.117」

上位ルータの IP アドレス

「%ppp0」

PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

インタフェースの ID

[空欄]

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

XR_A#2 (センター側 XR#2) の設定

「本装置側の設定 1」を選択します。

インタフェースの IP アドレス	203.xx.xx.118
上位ルータの IP アドレス	%ppp0
インタフェースの ID	<input type="text"/> (例: @xr.centurysys)

インタフェースの IP アドレス

「203.xx.xx.118」

上位ルータの IP アドレス

「%ppp0」

PPPoE 接続かつ固定 IP アドレスの場合は、必ずこの設定にします。

インタフェースの ID

[空欄]

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

第12章 IPsec 機能

VIII. IPsec 設定例 2 (センター / 拠点間の2対1接続)

「IKE/ISAKMPポリシーの設定」

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

「IKE1」を選択します。

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

IKE/ISAKMP ポリシー名 「(任意で設定します)」

接続する本装置側の設定 「本装置側の設定1」

インタフェースの IP アドレス 「0.0.0.0」
対向装置が動的アドレスの場合は必ずこの設定に
します。

上位ルータの IP アドレス [空欄]

インタフェースの ID
「@host」(@以降は任意の文字列)

上記の2項目は、対向装置の「本装置の設定」と
同じものを設定します。

モードの設定 「aggressive モード」

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

IKE のライフタイム 「3600」(任意の設定値)

鍵の設定

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

「IPSecポリシーの設定」

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

「IPSec1」を選択します。

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

「Responder として使用する」を選択します。

使用する IKE ポリシー名の選択 「IKE1」

本装置側のLAN側のネットワークアドレス
「192.168.0.0/24」

相手側のLAN側のネットワークアドレス
「192.168.20.0/24」

PH2のTransFormの選択 「すべてを送信する」

PFS 「使用する」(推奨)

DH Groupの選択 「指定しない」

SAのライフタイム 「28800」(任意の設定値)

DISTANCE [空欄]

VIII. IPsec 設定例 2 (センター / 拠点間の2対1接続)

「転送フィルタ」の設定

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

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

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート	LOG	削除
ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.254		<input type="checkbox"/>	<input type="checkbox"/>

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

動作 「破棄」
送信元アドレス 「192.168.20.254」
拠点側メイン SA の KeepAlive の送信元アドレスを設定します。
宛て先アドレス 「192.168.0.254」
拠点側メイン SA の KeepAlive の送信先アドレスを設定します。

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

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート	LOG	削除
ipsec0	パケット受信時	破棄	全て	192.168.20.254		192.168.0.253		<input type="checkbox"/>	<input type="checkbox"/>

インターフェース 「ipsec0」
ppp0 のデフォルトの IPsec インタフェースの "ipsec0" を設定します。
動作 「破棄」
送信元アドレス 「192.168.20.254」
拠点側バックアップ SA の KeepAlive の送信元アドレスを設定します。
宛て先アドレス 「192.168.0.253」
拠点側バックアップ SA の KeepAlive の送信先アドレスを設定します。

「スタティックルート」の設定

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

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

XR_A#1 のスタティックルート設定

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

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

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

XR_A#2 のスタティックルート設定

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

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

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

第12章 IPsec機能

VIII. IPsec設定例2 (センター/拠点間の2対1接続)

「IPsec Keep-Alive設定」

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

XR_A#1のIPsec Keep-Alive設定

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	Action 1	Action 2	interface	backup SA
1	<input checked="" type="checkbox"/>	192.168.0.254	192.168.20.254	30	3	60			ipsec0	

enableにチェックを入れます。

source address 「192.168.0.254」

destination address 「192.168.20.254」

interval 「30」(任意の設定値)

watch count 「3」(任意の設定値)

timeout/delay 「60」(任意の設定値)

動作オプション1を無効にするため、本値はdelay (ping送出delay時間)=60秒を意味します。

動作オプション1 [空欄]

動作オプション2 「チェック」

interface 「ipsec0」

backupSA [空欄]

XR_A#2のIPsec Keep-Alive設定

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	Action 1	Action 2	interface	backup SA
1	<input checked="" type="checkbox"/>	192.168.0.253	192.168.20.254	30	3	60			ipsec0	

enableにチェックを入れます。

source address 「192.168.0.253」

destination address 「192.168.20.254」

interval 「30」(任意の設定値) **注)**

watch count 「3」(任意の設定値)

timeout/delay 「60」(任意の設定値)

動作オプション1を無効にするため、本値はdelay (ping送出delay時間)=60秒を意味します。

動作オプション1 [空欄]

動作オプション2 「チェック」

interface 「ipsec0」

backupSA [空欄]

注)

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

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

但し、センター内のXR同士は同じinterval値でも構いません。

第12章 IPsec機能

VIII. IPsec設定例 2 (センター / 拠点間の2対1接続)

XR_B(拠点側XR)の設定

「本装置の設定」

「本装置側の設定1」を選択します。

インターフェースのIPアドレス	<input type="text" value="%ppp0"/>
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" value="@host"/> (例: @xr.centurysys)

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

上位ルータのIPアドレス [空欄]
PPPoE 接続かつ動的アドレスの場合は、空欄にして下さい。

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

メインSA用のIKE/ISAKMPポリシーの設定を行います。

「IKE/ISAKMPポリシーの設定」

「IKE1」を選択します。

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

IKE/ISAKMPポリシー名 「(任意で設定します)」
接続する本装置側の設定 「本装置側の設定1」
インターフェースのIPアドレス

「203.xx.xx.117」

対向装置が固定アドレスなので、そのIPアドレスを設定します。

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

インターフェースのID [空欄]
対向装置が固定アドレスなので、設定不要です。
モードの設定 「aggressive モード」
transformの設定

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

IKEのライフタイム 「3600」(任意の設定値)
鍵の設定

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

第12章 IPsec機能

VIII. IPsec設定例2 (センター/拠点間の2対1接続)

バックアップ SA 用の IKE/ISAKMP ポリシーの設定を行います。

「IKE/ISAKMPポリシーの設定」

「IKE2」を選択します。

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

IKE/ISAKMP ポリシー名 「(任意で設定します)」

接続する本装置側の設定 「本装置側の設定1」

インタフェースの IP アドレス

「203.xx.xx.118」

対向装置が固定アドレスなので、その IP アドレスを設定します。

上位ルータの IP アドレス [空欄]

対向装置が PPPoE 接続かつ固定アドレスなので、設定不要です。

インタフェースの ID [空欄]

対向装置が固定アドレスなので、設定不要です。

モードの設定 「aggressive モード」

transform の設定

1 番目 「group2-3des-sha1」(任意の設定を選択)

2 ~ 4 番目 「使用しない」

IKE のライフタイム 「3600」(任意の設定値)

鍵の設定

「PSK を使用する」を選択し、対向装置との共通鍵

「test_key」を入力します。

メイン SA 用の IPsec ポリシーの設定を行います。

「IPSecポリシーの設定」

「IPSec1」を選択します。

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

「使用する」を選択します。

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

使用する IKE ポリシー名の選択 「IKE1」

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

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

PH2 の TransForm の選択 「すべてを送信する」

PFS 「使用する」(推奨)

DH Group の選択 「指定しない」

SA のライフタイム 「28800」(任意の設定値)

DISTANCE 「1」

メイン側のディスタンス値は最小値(=1)を設定します。

第12章 IPsec 機能

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

バックアップ SA 用の IPsec ポリシーの設定を行います。

「IPsec ポリシーの設定」

「IPSec2」を選択します。

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

「Responderとして使用する」を選択します。
バックアップ SA 用の IPsec ポリシーであるため、
「Responderとして使用する」を選択して下さい。

使用する IKE ポリシー名の選択 「IKE2」

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

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

PH2 の TransForm の選択 「すべてを送信する」

PFS 「使用する」(推奨)

DH Group の選択 「指定しない」

SA のライフタイム 「28800」(任意の設定値)

DISTANCE 「2」
バックアップ側のディスタンス値は、メイン側の
ディスタンス値より大きな値を設定します。

「IPsec Keep-Alive の設定」

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

Policy No.	enable	source address	destination address	interval(sec)	watch count	timeout/delay(sec)	RTT(Typoon 1.0)	RTT(Typoon 2.0)	interface	backup SA
1	<input checked="" type="checkbox"/>	192.168.20.254	192.168.0.254	45	3	60			ipsec0	2
2	<input checked="" type="checkbox"/>	192.168.20.254	192.168.0.253	60	3	60			ipsec0	

メイン SA 用の KeepAlive の設定

PolicyNo.1 の行に設定します。

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

Keep-Alive により障害検知した場合に、IPSec2 のポリシーに切り替えるため、「2」を設定します。

バックアップ SA 用の KeepAlive の設定

PolicyNo.2 の行に設定します。

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

注)

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

IX. IPsec がつながらないとき

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

本体ログは、「システム設定」内の「ログ表示」で確認します。

[正常に IPsec 接続できたときのログメッセージ]

メインモードの場合

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

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

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

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

```
Aug 3 12:00:20 localhost ipsec_plutorun:
004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP
SAestablished
```

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

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

アグレッシブモードの場合

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

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

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

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

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

IX. IPsec がつながらないとき

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

[正常に IPsec が確立したときの表示例]

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

これらのログやメッセージ内に

- ISAKMP SA established
- IPsec SA established

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

IX. IPsec がつながらないとき

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

この場合は、接続相手との IKE 鍵交換が正常に行えていません。

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

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

S

「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。

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 サービスも再起動してください。

動的 IP アドレス側の IPsec サービスの再起動が困難な環境でお使いの場合は、IPsec SA のライフタイムを短くして運用してください。

相手の本装置には IPsec のログが出ているのに、こちらの本装置にはログが出ていません。IPsec は確立しているようなのですが、確認方法はありますか？

固定 IP - 動的 IP 間での IPsec 接続をおこなう場合、固定 IP 側(受信者側)の本装置ではログが表示されないことがあります。その場合は「各種サービスの設定」「IPsec サーバ」「ステータス」を開き、「現在の状態」をクリックして下さい。ここに現在の IPsec の状況が表示されます。

第 13 章

L2TPv3 機能

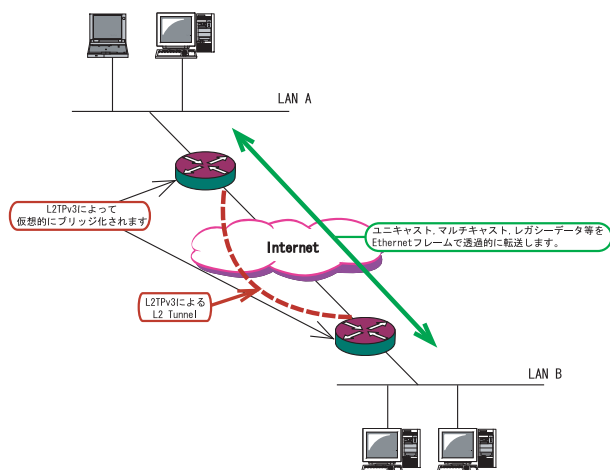
第13章 L2TPv3 機能

1. L2TPv3 機能概要

L2TPv3 機能は、IP ネットワーク上のルータ間で L2TPv3 トンネルを構築します。これにより本製品が仮想的なブリッジとなり、遠隔のネットワーク間でレイヤ2通信が可能となります。

レイヤ2レベルでトンネリングするため、2つのネットワークは HUB で繋がった1つの Ethernet ネットワークのように使うことができます。また上位プロトコルに依存せずにネットワーク通信ができ、TCP/IP だけでなく、任意の上位プロトコル (IPX、AppleTalk、SNA 等) を透過的に転送することができます。

また L2TPv3 機能は、従来の専用線やフレームリレー網ではなく IP 網で利用できますので、低コストな運用が可能です。



- End to Endで Ethernet フレームを転送したい
- FNA や SNA などのレガシーデータを転送したい
- ブロードキャスト / マルチキャストパケットを転送したい
- IPX や AppleTalk 等のデータを転送したい

このような、従来の IP-VPN やインターネット VPN では通信させることができなかったものも、L2TPv3 を使うことで通信できるようになります。

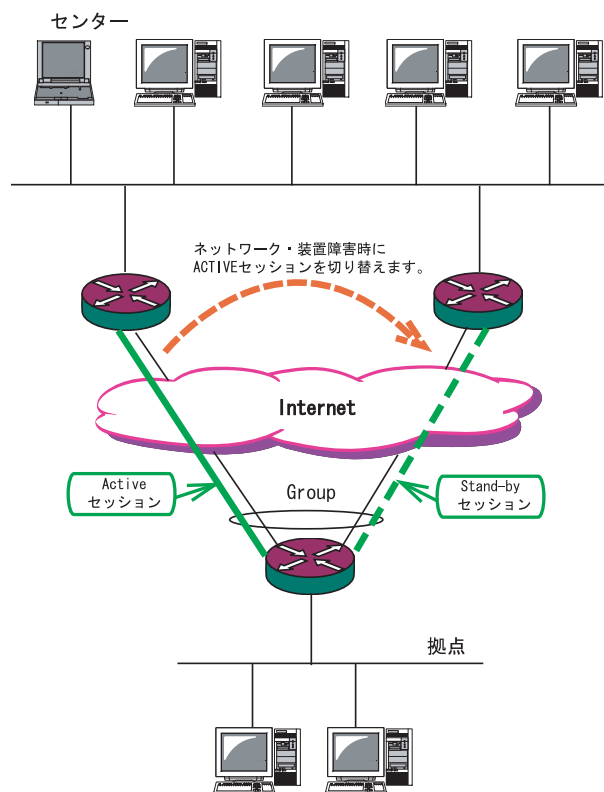
また Point to Multi-Point に対応しており、1つの Xconnect Interface に対して複数の L2TP session を関連づけることが可能です。

L2TPv3 セッションの二重化機能

本装置では、L2TPv3 Group 機能 (L2TPv3 セッションの二重化機能) を具備しています。ネットワーク障害や対向機器の障害時に二重化された L2TPv3 セッションの Active セッションを切り替えることによって、レイヤ2通信の冗長性を高めることができます。

・L2TPv3 セッション二重化の例

センター側を2台の冗長構成にし、拠点側の XR で、センター側への L2TPv3 セッションを二重化します。



11. L2TPv3 機能設定

本装置の ID やホスト名、MAC アドレスに関する設定を行います。

Local hostname	<input type="text" value="Router"/>
Local Router-ID	<input type="text"/>
MAC Address 学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	<input type="text" value="300"/> (30-1000sec)
Loop Detection 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast 設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
受信ポート番号 (over UDP)	<input type="text" value="1701"/> (default 1701)
PMTU Discovery 設定 (over UDP)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP 機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap 機能設定	<input type="radio"/> 有効 <input checked="" 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

Localhostname

本装置のホスト名を設定します。半角英数字のみ使用可能です。対向 LCCE (1) の ” リモートホスト名 ” 設定と同じものにします。設定は必須ですが、後述の 「 L2TPv3 Tunnel 設定 」 で設定した場合はそちらが優先されます。

Local Router-ID

本装置のルータ ID を設定します。LCCE のルータ ID の識別に使用します。対向 LCCE の ” リモートルータ ID ” 設定と同じものにします。ルータ ID は IP アドレス形式で設定して下さい。(ex. 192.168.0.1 など) 設定は必須ですが、後述の 「 L2TPv3 Tunnel 設定 」 で設定した場合はそちらが優先されます。

MAC Address 学習機能 (2)

MAC アドレス学習機能を有効にするかを選択します。

MAC Address Aging Time

本装置が学習した MAC アドレスの保持時間を設定します。30 ~ 1000 (秒) で設定します。

Loop Detection 設定 (3)

LoopDetect 機能を有効にするかを選択します。

Known Unicast 設定 (4)

Known Unicast 送信機能を有効にするかを選択します。

Path MTU Discovery

Path MTU Discovery 機能を有効にするかを選択します。本機能を有効にした場合は、送信する L2TPv3 パケットの DF (Don ' t Fragment) ビットを 1 にします。無効にした場合は、DF ビットを常に 0 にして送信します。但し、カプセル化されたフレーム長が送信インタフェースの MTU 値を超過する場合は、この設定に関係なく、フラグメントされ、DF ビットを 0 にして送信します。

受信ポート番号 (over UDP)

L2TPv3 over UDP 使用時の L2TP パケットの受信ポートを指定します。

11. L2TPv3 機能設定

PMTU Discovery 設定 (over UDP)

L2TPv3 over UDP 使用時に Path MTU Discovery 機能を有効にするかを選択します。

SNMP 機能設定

L2TPv3 用の SNMP エージェント機能を有効にするかを選択します。L2TPv3 に関する MIB の取得が可能になります。

SNMP Trap 機能設定

L2TPv3 用の SNMP Trap 機能を有効にするかを選択します。L2TPv3 に関する Trap 通知が可能になります。

これらの SNMP 機能を使用する場合は、SNMP サービスを起動させて下さい。

また、MIB や Trap に関する詳細は第 18 章「SNMP エージェント機能」を参照してください。

Debug 設定

syslog に出力するデバッグ情報の種類を選択します。トンネルのデバッグ情報、セッションのデバッグ情報、L2TP エラーメッセージの 3 種類を選択できます。

(1) LCCE (L2TP Control Connection Endpoint)
L2TP コネクションの末端にある装置を指す言葉。

(2) MAC Address 学習機能

本装置が受信したフレームの MAC アドレスを学習し、不要なトラフィックの転送を抑制する機能です。ブロードキャスト、マルチキャストについては MAC アドレスに関係なく、すべて転送されます。

Xconnect インタフェースで受信した MAC アドレスはローカル側 MAC テーブル(以下、Local MAC テーブル)に、L2TP セッション側で受信した MAC アドレスはセッション側 MAC テーブル(以下、FDB)にてそれぞれ保存されます。

さらに本装置は Xconnect インタフェース毎に Local MAC テーブル / FDB を持ち、それぞれの Local MAC テーブル / FDB につき、最大 65535 個の MAC アドレスを学習することができます。

学習した MAC テーブルは手動でクリアすることができます。

(3) Loop Detection 機能

フレームの転送がループしてしまうことを防ぐ機能です。この機能が有効になっているときは、以下の 2 つの場合にフレームの転送を行いません。

- Xconnect インタフェースより受信したフレームの送信元 MAC アドレスが FDB に存在するとき
- L2TP セッションより受信したフレームの送信元 MAC アドレスが Local MAC テーブルに存在するとき

(4) Known Unicast 送信機能

Known Unicast とは、既に MAC アドレス学習済みの Unicast フレームのことを言います。この機能を「無効」にしたときは、以下の場合に Unicast フレームの転送を行いません。

- Xconnect インタフェースより受信した Unicast フレームの送信先 MAC アドレスが Local MAC テーブルに存在するとき

III. L2TPv3 Tunnel 設定

L2TPv3のトンネル(制御コネクション)のための設定を行います。新規に設定を行うときは「New Entry」をクリックします。

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)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効 <input type="button" value="v"/>
Hello Interval設定	<input type="text" value="60"/> [0-1000] (default 60s)
Local Hostname設定	<input type="text"/>
Local RouterID設定	<input type="text"/>
Remote Hostname設定	<input type="text"/>
Remote RouterID設定	<input type="text"/>
Vendor ID設定	20376:CENTURY <input type="button" value="v"/>
Bind Interface設定	<input type="text"/>
送信プロトコル	<input checked="" type="radio"/> over IP <input type="radio"/> over UDP
送信ポート番号	<input type="text" value="1701"/> (default 1701)

Description

このトンネル設定についてのコメントや説明を付記します。この設定はL2TPv3の動作には影響しません。

Peer アドレス

対向 LCCE の IP アドレスを設定します。但し、対向 LCCE が動的 IP アドレスの場合には空欄にしてください。

パスワード

CHAP 認証やメッセージダイジェスト、AVP Hiding で利用する共有鍵を設定します。パスワードは設定しなくてもかまいません。

パスワードは、制御コネクションの確立時における対向 LCCE の識別、認証に使われます。

AVP Hiding()

AVP Hiding を有効にするかを選択します。

Digest Type

メッセージダイジェストを使用する場合に設定します。

Hello Interval 設定

Hello パケットの送信間隔を設定します。「0」を設定すると Hello パケットを送信しません。

Hello パケットは、L2TPv3 の制御コネクションの状態を確認するために送信されます。

L2TPv3 二重化機能で、ネットワークや機器障害を自動的に検出したい場合は必ず設定して下さい。

Local Hostname 設定

本装置のホスト名を設定します。LCCE の識別に使用します。設定しない場合は「L2TPv3 機能設定」での設定が有効になります。

Local Router ID

対向 LCCE のルータ ID を設定します。LCCE のルータ ID の識別に使用します。設定しない場合は「L2TPv3 機能設定」での設定が有効になります。

Remote Hostname 設定

対向 LCCE のホスト名を設定します。LCCE の識別に使用します。設定は必須となります。

III. L2TPv3 Tunnel 設定

Remote Router ID

対向 LCCE のルータ ID を設定します。LCCE のルータ ID の識別に使用します。設定は必須となります。

Vender ID 設定

対向 LCCE のベンダー ID を設定します。「0」は IETF 機器 (XR-410-L2、XR-640L2)、「9」は Cisco Router となります。

Bind Interface 設定

バインドさせる本装置のインタフェースを設定します。指定可能なインタフェースは「PPP インタフェース」のみです。

この設定により、PPP/PPPoE の接続 / 切断に伴って、L2TP トンネルとセッションの自動確立 / 解放がおこなわれます。

送信プロトコル

L2TP パケット送信時のプロトコルを「over IP」「over UDP」から選択します。接続する対向装置と同じプロトコルを指定する必要があります。「over UDP」を選択した場合、PPPoE to L2TP 機能を同時に動作させることはできません。

送信ポート番号

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

() AVP Hiding

L2TPv3 では、AVP (Attribute Value Pair) と呼ばれる、属性と値のペアでトンネルの確立や解放、維持などの制御メッセージをやりとりします。

AVP は通常、平文で送受信されますが、AVP Hiding 機能を使うことで AVP 中のデータを暗号化します。

IV. L2TPv3 Xconnect (クロスコネクト) 設定

主にL2TPセッションを確立するとき使用するパラメータの設定を行います。

Xconnect ID設定 (Group設定を行う場合は指定)	<input type="text"/> [1-4294967295]
Tunnel設定選択	--- ▾
L2Frame受信インタフェース設定	<input type="text"/> (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	<input type="text"/> [0-4094] (0の場合付与しない)
Remote END ID設定	<input type="text"/> [1-4294967295]
Reschedule Interval設定	<input type="text"/> [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<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(byte)	<input type="text"/> [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

Xconnect ID 設定

「L2TPv3 Group 設定」で使用する ID を任意で設定します。

Tunnel 設定

「L2TPv3 Tunnel 設定」で設定したトンネル設定を選択して、トンネルの設定とセッションの設定を関連づけます。

プルダウンメニューには、「L2TPv3 Tunnel 設定」の「Remote Router ID」で設定された値が表示されます。

L2Frame 受信インタフェース設定

レイヤー2フレーム(Ethernet フレーム)を受信するインタフェース名を設定します。設定可能なインタフェースは、本装置のイーサネットポートとVLANインタフェースのみです。

Point to Multi-point 接続を行う場合は、1つのインタフェースに対し、複数のL2TPv3セッションの関連付けが可能です。

但し、本装置のEthernetインタフェースとVLANインタフェースを同時に設定することはできません。

2つ(以上)のXconnect 設定を行うときの例:

「eth0.10」と「eth0.20」・・・設定可能
 「eth0.10」と「eth0.10」・・・設定可能()
 「eth0」と「eth0.10」・・・設定不可

Point to Multi-point 接続、もしくはL2TPv3二重化の場合のみ設定可能。

VLAN ID

本装置でVLANタギング機能を使用する場合に設定します。本装置の配下にVLANに対応していないL2スイッチが存在するときに使用できます。0～4094まで設定でき、「0」のときはVLANタグを付与しません。

Remote END ID

対向LCCEのEND IDを設定します。END IDは1～4294967295の任意の整数値です。対向LCCEのEND ID設定と同じものにします。但し、L2TPv3セッション毎に異なる値を設定して下さい。

第 13 章 L2TPv3 機能

IV. L2TPv3 Xconnect (クロスコネクト) 設定

Reschedule Interval 設定

L2TP トンネル / セッションが切断したときに re-schedule(自動再接続)することができます。自動再接続するときにはここで、自動再接続を開始するまでの間隔を設定します。0 ~ 1000(秒)で設定します。

また、「0」を設定したときは自動再接続は行われません。このときは手動による接続か対向 LCCE からのネゴシエーションによって再接続します。

L2TPv3 二重化機能で、ネットワークや機器の復旧時に自動的にセッション再接続させたい場合は必ず設定して下さい。

Auto Negotiation 設定

この設定が有効になっているときは、L2TPv3 機能が起動後に自動的に L2TPv3 トンネルの接続が開始されます。

この設定は Ethernet 接続時に有効です。PPP/PPPoE 環境での自動接続は、「L2TPv3 Tunnel 設定」の「Bind Interface 設定」で ppp インタフェースを設定して下さい。

MSS 設定

MSS 値の調整機能を有効にするかどうかを選択します。

MSS 値 (byte)

MSS 設定を「有効」に選択した場合、MSS 値を指定することができます (指定可能範囲 0-1460)。0 を指定した場合、自動的に計算された値を設定します。

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

Loop Detection 設定

この Xconnect において、Loop Detection 機能を有効にするかを選択します。

Known Unicast 設定

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

注) LoopDetect 設定、Known Unicast 設定は、「L2TPv3 機能設定」でそれぞれ有効にしていない場合、ここでの設定は無効となります。

Circuit Down 時 Frame 転送設定

Circuit Status が Down 状態の時に、対向 LCCE に対して Non-Unicast Frame を送信するかを選択します。

第13章 L2TPv3 機能

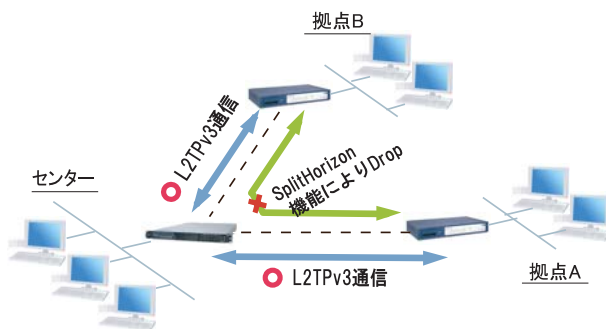
IV. L2TPv3 Xconnect (クロスコネクト) 設定

Split Horizon 設定

Point-to-Multi-Point 機能によって、センターと2拠点間を接続しているような構成において、センターと拠点間のL2TPv3通信は行うが、拠点同士間の通信は必要ない場合に、センター側でこの機能を有効にします。

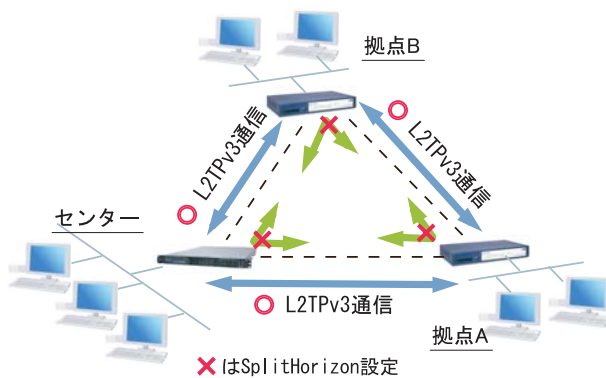
センター側では、Split Horizon 機能が有効の場合、一方の拠点から受信したフレームをもう一方のセッションへは転送せず、Local Interface に対してのみ転送します。

Split Horizon の使用例 1



また、この機能は、拠点間でフルメッシュの構成をとる様な場合に、フレームのLoopの発生を防ぐための設定としても有効です。この場合、全ての拠点においてSplit Horizon 機能を有効に設定します。LoopDetect 機能を有効にする必要はありません。

Split Horizon の使用例 2



V. L2TPv3 Group 設定

L2TPv3セッション二重化機能を使用する場合に、二重化グループのための設定を行います。新規のグループ設定を行うときは、「New Entry」をクリックします。
二重化機能を使用しない場合は、設定する必要はありません。

Group ID	<input type="text" value=""/> [1-4095]
Primary Xconnect設定選択	---
Secondary Xconnect設定選択	---
Preempt設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Primary active時の Secondary Session強制切断設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Active Hold設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

Group ID 設定

Groupを識別する番号を設定します。他のGroupと重複しない値を設定して下さい。設定可能な値は、1～4095の任意の整数値です。

Primary Xconnect 設定

Primaryとして使用したいXconnectをプルダウンから選択します。プルダウンには「L2TPv3 Xconnect 設定」の「Xconnect ID 設定」で設定した値が表示されます。

既に他のGroupで使用されているXconnectを指定することはできません。

Secondary Xconnect 設定

Secondaryとして使用したいXconnectをプルダウンから選択します。プルダウンには「L2TPv3 Xconnect 設定」の「Xconnect ID 設定」で設定した値が表示されます。

既に他のGroupで使用されているXconnectを指定することはできません。

Preempt 設定

GroupのPreemptモード()を有効にするかどうかを設定します。

Preempt モード

SecondaryセッションがActiveとなっている状態で、Primaryセッションが確立したときに、通常SecondaryセッションがActiveな状態を維持し続けませんが、Preemptモードが「有効」の場合は、PrimaryセッションがActiveになり、SecondaryセッションはStand-byとなります。

Primary active時のSecondary Session強制切断設定
この設定が「有効」となっている場合、PrimaryセッションがActiveに移行した際に、Secondaryセッションを強制的に切断します。本機能を「有効」にする場合、「Preempt 設定」も「有効」に設定して下さい。

SecondaryセッションをISDNなどの従量回線で接続する場合には「有効」にすることを推奨します。

Active Hold 設定

GroupのActive Hold機能()を有効にするかどうかを設定します。

Active Hold 機能

対向のLCCEからLink Downを受信した際に、Secondaryセッションへの切り替えを行わず、PrimaryセッションをActiveのまま維持する機能のことを言います。

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

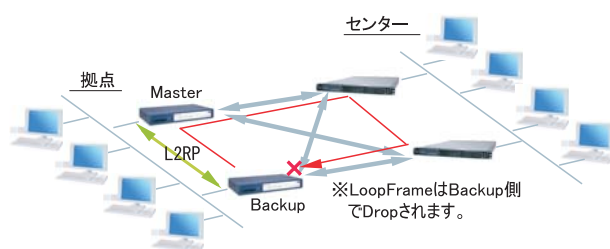
VI. Layer2 Redundancy 設定

Layer2 Redundancy Protocol 機能 (以下、L2TP 機能)とは、装置の冗長化を行い、Frame の Loop を抑止するための機能です。

L2RP 機能では、2 台の LCCE で Master/Backup 構成を取り、Backup 側は受信 Frame を全て Drop させることによって、Loop の発生を防ぐことができます。また機器や回線の障害発生時には、Master/Backup を切り替えることによって拠点間の接続を維持することができます。

下図のようなネットワーク構成では、フレームの Loop が発生し得るため、本機能を有効にしてください。

L2RP 機能の使用例



L2RP の設定方法

「L2TPv3 Layer2 Redundancy 設定」画面から「New Entry」をクリックすると以下の設定画面が開きます。

L2RP ID	<input type="text" value="100"/> [1-255]
Type 設定	<input checked="" type="radio"/> Priority <input type="radio"/> Active Session
Priority 設定	<input type="text" value="100"/> [1-255] (default 100)
Advertisement Interval 設定	<input type="text" value="1"/> [1-60] (default 1)
Preempt 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Xconnect インタフェース 設定	<input type="text" value=""/> (interface 名 指定)
Forward Delay 設定	<input type="text" value="0"/> [0-60] (default 0s)
Port Down Time 設定	<input type="text" value="0"/> [0.5-10] (default 0s)
Block Reset 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効

L2RP ID

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

Type 設定

Master/Backup を決定する判定方法を選択します。「Priority」は Priority 値の高い方が Master となります。「Active Session」は Active Session 数の多い方が Master となります。

Type 設定

Master/Backup を決定する判定方法を選択します。「Priority」は Priority 値の高い方が Master となります。「Active Session」は Active Session 数の多い方が Master となります。

Priority 設定

Master の選定に使用する Priority 値です。1 ~ 255 の間で設定します。

Advertisement Interval 設定

Advertise Frame を送信する間隔です。1 ~ 60(秒) の間で設定します。

Advertise Frame

Master 側が定期的に出す情報フレームです。Backup 側ではこれを監視し、一定時間受信しない場合に Master 側の障害と判断し、自身が Master へ遷移します。

Preempt 設定

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

Xconnect インタフェース 設定

Xconnect インタフェース名を指定して下さい。Advertise Frame は Xconnect 上で送受信されます。

VI. Layer2 Redundancy 設定

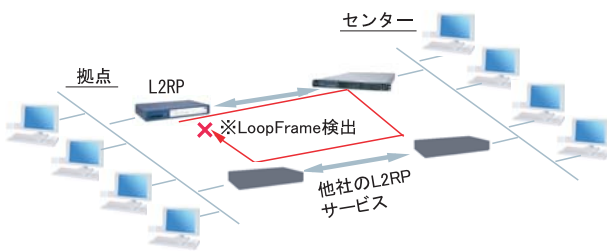
Forward Delay 設定

Forward Delay とは、L2TP セッション確立後、指定された Delay Time の間、Frame の転送を行わない機能のことです。

例えば、他の L2 サービスと併用し、L2RP の対向が存在しないような構成において、L2RP 機能では自身が送出した Advertise フレームを受信することで Loop を検出しますが、Advertise フレームを受信するまでは一時的に Loop が発生する可能性があります。このような場合に Forward Delay を有効にすることによって、Loop の発生を抑止することができます。

delay Time の設定値は Advertisement Interval より長い時間を設定することを推奨します。

他の L2RP サービスとの併用例



Port Down Time 設定

L2RP 機能によって、Active セッションの切り替えが発生した際、配下のスイッチにおける MAC アドレスのエントリが、以前 Master だった機器の Port を向いているために最大約5分間通信ができなくなる場合があります。

これを回避するために、Master から Backup の切り替え時に自身の Port のリンク状態を一時的にダウンさせることによって配下のスイッチの MAC テーブルをフラッシュさせることができます。

設定値は、切り替え時に Port をダウンさせる時間です。0 を指定すると本機能は無効になります。

L2RP Group Blocking 状態について

他の L2 サービスと併用している場合に、自身が送出した Advertise Frame を受信したことによって、Frame の転送を停止している状態を Group Blocking 状態と言います。この Group Blocking 状態に変化があった場合にも、以下の設定で、機器の MAC テーブルをフラッシュすることができます。

FDB Reset 設定

XR が HUB ポートを持っている場合に、自身の HUB ポートの MAC テーブルをフラッシュします。

Block Reset 設定

自身の Port のリンク状態を一時的に Down させ、配下のスイッチの MAC テーブルをフラッシュします。Group Blocking 状態に遷移した場合のみ動作します。

L2RP 機能使用時の注意

L2RP 機能を使用する場合は、Xconnect 設定において以下のオプション設定を行って下さい。

- Loop Detect 機能 「無効」
- known-unicast 機能 「送信する」
- Circuit Down 時 Frame 転送設定 「送信する」

L2TPv3 Filter 設定については、第14章「L2TPv3 フィルタ機能」で説明します。

VIII. 起動 / 停止設定

L2TPv3 トンネル / セッションの起動や停止、MAC テーブルのクリア等を行います。

Tunnel Setup起動/停止
MACテーブルクリア
カウンタクリア

起動

Xconnect Interface 選択 ---- ▾

Remote-ID 選択 ---- ▾

停止(下記を選択してください)

Local Tunnel/Session ID指定

Tunnel ID

Session ID

Remote-ID指定

Remote-ID 選択 ---- ▾

Group-ID指定

Group ID 選択

Local MACテーブルクリア

Interface 選択 ---- ▾

FDBクリア

Interface 選択 ---- ▾

Group ID 選択

Peer counterクリア

Remote-ID 選択 ---- ▾

Tunnel counterクリア

Local Tunnel ID

Session counterクリア

Local Session ID

Interface counterクリア

Interface 選択 ---- ▾

起動

トンネル / セッション接続を実行したい Xconnect インタフェースを選択します。プルダウンには、「L2TPv3 Xconnect 設定」で設定したインタフェースが表示されます。

また、Point to Multi-point 接続や L2TPv3 二重化の場合に、1セッションずつ接続したい場合は、接続したい Remote-ID をプルダウンから選択してください。

画面下部の「実行」ボタンを押下すると、接続を開始します。

停止

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

- Tunnel/SessionID 指定
- 1セッションのみ切断したい場合は、切断するセッションの Tunnel ID/SessionID を指定して下さい。
- RemoteID 指定
- ある LCCE に対するセッションを全て切断したい場合は、対向 LCCE の Remote-ID を選択して下さい。
- GroupID 指定

グループ内のセッションを全て停止したい場合は、停止するグループ ID を指定して下さい。

Local MAC テーブルクリア

L2TPv3 機能で保持しているローカル側の MAC テーブル(Local MAC テーブル)をクリアします。クリアしたい Xconnect Interface をプルダウンから選択してください。

FDB クリア

L2TPv3 機能で保持している L2TP セッション側の MAC テーブル(FDB)をクリアします。Group ID を選択した場合は、そのグループで持つ FDB のみクリアします。Xconnect Interface をプルダウンから選択した場合は、その Interface で持つ全てのセッション ID の FDB をクリアします。

なお、Local MAC テーブル / FDB における MAC テーブルは、本装置の「情報表示」で表示される ARP テーブルとは別です。

VIII. 起動 / 停止設定

Peer counter クリア

「L2TPv3 ステータス表示」で表示される「Peer ステータス表示」のカウンタをクリアします。プルダウンからクリアしたいRemote-IDを選択して下さい。プルダウンには、「L2TPv3 Xconnect 設定」で設定したPeer IDが表示されます。

Tunnel Counter クリア

「L2TPv3 ステータス表示」で表示される「Tunnel ステータス表示」のカウンタをクリアします。クリアしたいTunnel IDを指定して下さい。

Session counter クリア

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

Interface counter クリア

「L2TPv3 ステータス表示」で表示される「Xconnect Interface 情報表示」のカウンタをクリアします。プルダウンからクリアしたいインタフェースを選択して下さい。プルダウンには、「L2TPv3 Xconnect 設定」で設定したインタフェースが表示されます。

IX. L2TPv3 ステータス表示

L2TPv3 の各種ステータスを表示します。

Xconnect Interface 情報表示	<input type="text" value="---"/> <input checked="" type="checkbox"/> detail 表示	表示する
MAC Table/FDB 情報表示	<input type="text" value="---"/> <input checked="" type="checkbox"/> local MAC Table 表示 <input checked="" type="checkbox"/> FDB 表示	表示する
Peer ステータス表示	Router-ID <input type="text"/>	表示する
Tunnel ステータス表示	Tunnel ID <input type="text"/> <input checked="" type="checkbox"/> detail 表示	表示する
Session ステータス表示	Session ID <input type="text"/> <input checked="" type="checkbox"/> detail 表示	表示する
Group ステータス表示	Group ID <input type="text"/>	表示する
すべてのステータス情報表示	表示する	

Xconnect Interface 情報表示

Xconnect インタフェースのカウンタ情報を表示します。プルダウンから表示したいインタフェースを選択して下さい。

「detail 表示」にチェックを入れると詳細情報を表示することができます。

MAC Table/FDB 情報表示

L2TPv3 機能が保持している MAC アドレステーブルの内容を表示します。プルダウンから表示したい Xconnect インタフェースを選択して下さい。

なお、ローカル側で保持する MAC テーブルを表示したい場合は、「local MAC Table 表示」にチェックを入れ、L2TP セッション側で保持する MAC テーブルを表示したい場合は、「FDB 表示」にチェックを入れてください。両方にチェックを入れることもできます。

Peer ステータス表示

Peer ステータス情報を表示します。表示したい Router-ID を指定して下さい。

Tunnel ステータス表示

L2TPv3 トンネルの情報のみを表示します。

「detail 表示」にチェックを入れると詳細情報を表示することができます。

Session ステータス表示

L2TPv3 セッションの情報とカウンタ情報を表示します。表示したいセッション ID を指定して下さい。指定しない場合は全てのセッションの情報を表示します。

「detail 表示」にチェックを入れると詳細情報を表示することができます。

Group ステータス表示

L2TPv3 グループの情報を表示します。プライマリ・セカンダリの Xconnect / セッション情報と現在 Active のセッション ID が表示されます。表示したいグループ ID をプルダウンから選択して下さい。選択しない場合は全てのグループの情報を表示します。

すべてのステータス情報表示

上記 5 つの情報を一覧表示します。

X. 制御メッセージ一覧

L2TPのログには各種制御メッセージが表示されます。メッセージの内容については、下記を参照して下さい。

[制御コネクション関連メッセージ]

SCCRQ : Start-Control-Connection-Request

制御コネクション(トンネル)の確立を要求するメッセージ。

SCCRP : Start-Control-Connection-Reply

SCCRQ に対する応答メッセージ。トンネルの確立に同意したことを示します。

SCCCN : Start-Control-Connection-Connected

SCCRP に対する応答メッセージ。このメッセージにより、トンネルが確立したことを示します。

StopCCN : Stop-Control-Connection-Notification

トンネルを切断するメッセージ。これにより、トンネル内のセッションも切断されます。

HELLO : Hello

トンネルの状態を確認するために使われるメッセージ。

[呼管理関連メッセージ]

ICRQ : Incoming-Call-Request

リモートクライアントから送られる着呼要求メッセージ。

ICRP : Incoming-Call-Reply

ICRQ に対する応答メッセージ。

ICCN : Incoming-Call-Connected

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

CDN : Call-Disconnect-Notify

L2TP セッションの切断を要求するメッセージ。

第13章 L2TPv3 機能

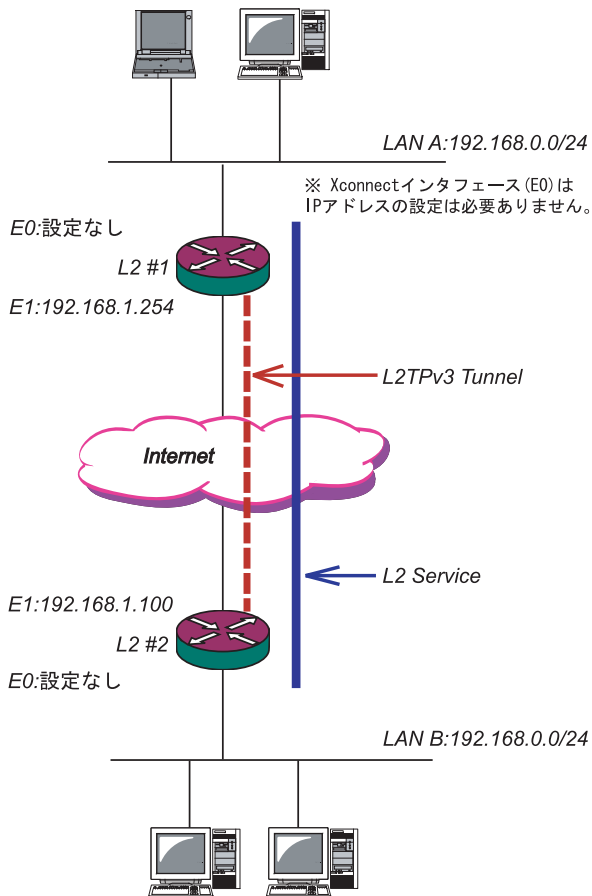
XI. L2TPv3 設定例 1 (2 拠点間の L2TP トンネル)

2 拠点間で L2TP トンネルを構築し、End to End で Ethernet フレームを透過的に転送する設定例です。

L2TPv3 サービスの起動

L2TPv3 機能を設定するときは、はじめに「各種サービス」の「L2TPv3」を起動してください。

構成図 (例)



DNS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
ダイナミックルーティング	起動停止はダイナミックルーティングの設定から行って下さい		停止中
L2TPv3	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
SYSLOGサーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	動作変更
SNMPサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	動作変更
NTPサーバ	<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

第13章 L2TPv3 機能

XI. L2TPv3 設定例 1(2拠点間のL2TPトンネル)

L2 #1 ルータの設定

L2TPv3 機能設定をします。

- ・Local Router-IDはIPアドレス形式で設定します(この設定例ではEther1ポートのIPアドレスとしています)。

Local hostname	L2-1
Local Router-ID	192.168.1.254
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" 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

L2TPv3 Xconnect Interface設定をします。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.100
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

L2TPv3 Tunnel 設定をします。

- ・「AVP Hiding」「Digest type」を使用するときは、「パスワード」を設定する必要があります。
- ・PPPoE接続とL2TPv3接続を連動させるときは、「Bind Interface」にPPPインタフェース名を設定します。

Description	sample
Peerアドレス	192.168.1.100 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-2
Remote RouterID設定	192.168.1.100
Vendor ID設定	20376:CENTURY
Bind Interface設定	

第13章 L2TPv3 機能

XI. L2TPv3 設定例 1(2 拠点間の L2TP トンネル)

L2 #2 ルータの設定

L2TPv3 機能設定をします。

Local hostname	L2-2
Local Router-ID	192.168.1.100
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP 機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" 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

L2TPv3 Xconnect Interfaceの設定をします。

Xconnect ID設定 (Group設定を行う場合は指定)	[] [1-4294967295]
Tunnel設定選択	192.168.1.254
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

L2TPv3 Tunnel 設定をします。

Description	sample
Peerアドレス	192.168.1.254 (例:192.168.0.1)
パスワード	[] (英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	[]
Local RouterID設定	[]
Remote Hostname設定	L2-1
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376-CENTURY
Bind Interface設定	[]

XI.L2TPv3 設定例1 (2拠点間のL2TPトンネル)

L2TPv3TunnelSetupの起動

ルータの設定後、「起動 / 停止設定」画面でL2TPv3接続を開始させます。

下の画面で「起動」にチェックを入れ、Xconnect InterfaceとRemote-IDを選択します。

画面下の「実行」ボタンをクリックするとL2TPv3接続を開始します。

Tunnel Setup起動/停止
MACテーブルクリア
カウンタクリア

- 起動
 - Xconnect Interface 選択
 - Remote-ID 選択
- 停止(下記を選択してください)
 - Local Tunnel/Session ID 指定
 - Tunnel ID
 - Session ID
 - Remote-ID 指定
 - Remote-ID 選択
 - Group-ID 指定
 - Group ID 選択
 - Local MACテーブルクリア
 - Interface 選択
 - FDBクリア
 - Interface 選択
 - Group ID 選択
 - Peer counterクリア
 - Remote-ID 選択
 - Tunnel counterクリア
 - Local Tunnel ID
 - Session counterクリア
 - Local Session ID
 - Interface counterクリア
 - Interface 選択

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

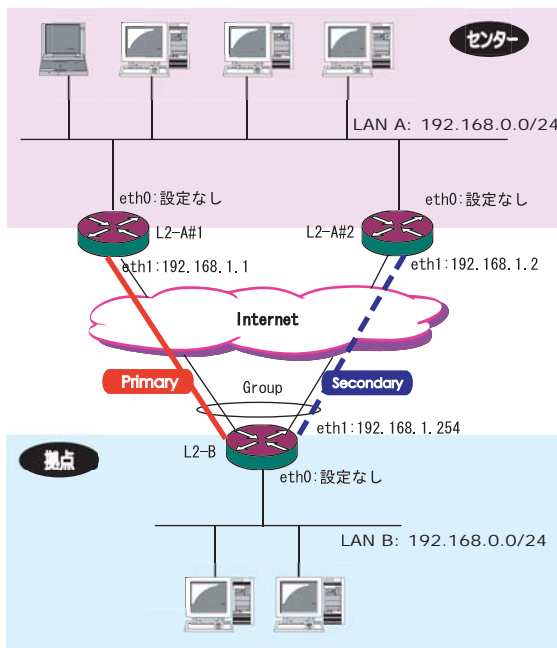
第 13 章 L2TPv3 機能

XII. L2TPv3 設定例 2 (L2TP トンネル二重化)

次に、センター側を 2 台の冗長構成にし、拠点 / センター間の L2TP トンネルを二重化する場合の設定例です。

本例では、センター側の 2 台の XR のそれぞれに対し、拠点側 XR から L2TPv3 セッションを張り、Secondary 側セッションは STAND-BY セッションとして待機させるような設定を行います。

構成図 (例)



第13章 L2TPv3 機能

XII. L2TPv3 設定例2 (L2TPトンネル二重化)

L2-A#1/L2-A#1(センター側)ルータの設定

L2-A#1 (Primary) ルータのL2TPv3 機能設定をします。

- ・「LocalHostName」には任意のホスト名を設定します。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。

Local hostname	L2-A1
Local Router-ID	192.168.1.1
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" 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

L2-A#2 (Secondary) ルータのL2TPv3 機能設定をします。

- ・Primaryルータと同じ要領で設定して下さい。

Local hostname	L2-A2
Local Router-ID	192.168.1.2
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" 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

L2-A#1 (Primary) ルータのTunnel 設定をします。

- ・「Peerアドレス」には拠点側ルータのWAN側のIPアドレスを設定します。
- ・「LocalHostName」「Local Router-ID」が未設定の場合は、機能設定で設定した値が使用されます。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。
- ・「RemoteHostName」「Remote Router-ID」は、それぞれ拠点側ルータで設定する「LocalHostName」「Local Router-ID」と同じものを設定します。

Description	primary
Peerアドレス	192.168.1.254 (例192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-B
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376-CENTURY
Bind Interface設定	

第13章 L2TPv3 機能

XII. L2TPv3 設定例2 (L2TP トンネル二重化)

L2-A#2 (Secondary) ルータの Tunnel 設定をします。

- Primaryルータと同じ要領で設定して下さい。本例の場合、Primaryルータと同じ設定になります。

Description	secondary
Peerアドレス	192.168.1.254 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-B
Remote RouterID設定	192.168.1.254
Vendor ID設定	20376:CENTURY
Bind Interface設定	

L2-A#1 (Primary) ルータの Xconnect Interface 設定をします。

- 「Xconnect ID設定」はGroup設定を行わないので設定不要です。
- 「Tunnel設定選択」はプルダウンから拠点側ルータのPeerアドレスを選択します。
- 「L2Frame受信インタフェース」はLAN側のインタフェースを指定します。**LAN側インタフェースにはIPアドレスを設定する必要はありません。**
- 「Remote End ID設定」は任意のEND IDを設定します。必ず拠点側ルータのPrimaryセッションと同じ値を設定して下さい。

Xconnect ID設定 (Group設定を行う場合は指定)	[1-4294967295]
Tunnel設定選択	192.168.1.254
L2Frame受信インタフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	1 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

第13章 L2TPv3 機能

XII. L2TPv3 設定例2 (L2TP トンネル二重化)

L2-A#2 (Secondary) ルータの Xconnect Interface 設定をします。

- Primary ルータと同じ要領で設定して下さい。
- 「Remote End ID 設定」は、拠点側ルータの Secondary セッションと同じ値を設定します。

L2TPv3 Group 設定について

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

Xconnect ID 設定 (Group 設定を行う場合は指定)	<input type="text" value=""/> [1-4294967295]
Tunnel 設定選択	192.168.1.254 ▼
L2Frame 受信インターフェース設定	eth0 (interface 名指定)
VLAN ID 設定 (VLAN Tag 付与する場合指定)	0 [0-4094] 0 の場合付与しない)
Remote END ID 設定	2 [1-4294967295]
Reschedule Interval 設定	0 [0-1000] (default 0s)
Auto Negotiation 設定 (Service 起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS 値(byte)	0 [0-1460] 0 の場合は自動設定)
Loop Detect 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast 設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down 時 Frame 転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

第13章 L2TPv3 機能

XII. L2TPv3 設定例2 (L2TP トンネル二重化)

L2-B(拠点側ルータ)の設定

L2TPv3 機能設定をします。

- ・「LocalHostName」には任意のホスト名を設定します。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。

Local hostname	L2-B
Local Router-ID	192.168.1.254
MAC Address学習機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MAC Address Aging Time	300 (30-1000sec)
Loop Detection設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
PMTU Discovery設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
SNMP機能設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
SNMP Trap機能設定	<input type="radio"/> 有効 <input checked="" 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

Primaryセッション側のL2TPv3 Tunnel設定をします。

- ・「Peerアドレス」にはセンター側PrimaryルータのWAN側のIPアドレスを設定します。
- ・「Hello Interval設定」を設定した場合、L2TPセッションのKeep-Aliveを行います。回線または対向LCCEの障害を検出し、ACTIVEセッションをSecondary側へ自動的に切り替えることができます。
- ・「LocalHostName」「Local Router-ID」が未設定の場合は、機能設定で設定した値が使用されます。
- ・「Local Router-ID」にはWAN側のIPアドレスを設定します。
- ・「RemoteHostName」「Remote Router-ID」は、それぞれセンター側Primaryルータで設定する「LocalHostName」「Local Router-ID」と同じものを設定します。

Description	primary
Peerアドレス	192.168.1.1 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type設定	無効
Hello Interval設定	60 [0-1000] (default 60s)
Local Hostname設定	
Local RouterID設定	
Remote Hostname設定	L2-A1
Remote RouterID設定	192.168.1.1
Vendor ID設定	20376:CENTURY
Bind Interface設定	

X11. L2TPv3 設定例2 (L2TP トンネル二重化)

Secondary セッション側の L2TPv3 Tunnel 設定をします。

- ・Primary セッションと同じ要領で設定して下さい。

Description	secondary
Peer アドレス	192.168.1.2 (例:192.168.0.1)
パスワード	(英数字95文字まで)
AVP Hiding 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Digest Type 設定	無効
Hello Interval 設定	60 [0-1000] (default 60s)
Local Hostname 設定	
Local RouterID 設定	
Remote Hostname 設定	L2-A2
Remote RouterID 設定	192.168.1.2
Vendor ID 設定	20376:CENTURY
Bind Interface 設定	

Secondary セッション側の L2TPv3 Xconnect 設定をします。

- ・「Xconnect ID 設定」は任意の Xconnect ID を設定します。必ず Secondary 側と異なる値を設定して下さい。
- ・「Tunnel 設定選択」はプルダウンから Primary セッションの Peer アドレスを選択します。
- ・「L2Frame 受信インタフェース」は LAN 側のインタフェースを指定します。**LAN 側インタフェースには IP アドレスを設定する必要はありません。**
- ・「Remote End ID 設定」は任意の END ID を設定します。必ずセンター側 Primary ルータで設定する End ID と同じ値を設定します。但し、Secondary 側と同じ値は設定できません。
- ・「Reschedule Interval 設定」に任意の Interval 時間を設定して下さい。この場合、L2TP セッションの切断検出時に自動的に再接続を行います。

Xconnect ID 設定 (Group 設定を行う場合は指定)	1 [1-4294967295]
Tunnel 設定選択	192.168.1.1
L2Frame 受信インタフェース 設定	eth0 (interface 名指定)
VLAN ID 設定 (VLAN Tag 付与する場合指定)	0 [0-4094] (0 の場合付与しない)
Remote END ID 設定	1 [1-4294967295]
Reschedule Interval 設定	0 [0-1000] (default 0s)
Auto Negotiation 設定 (Service 起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS 設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS 値(byte)	0 [0-1460] (0 の場合は自動設定)
Loop Detect 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast 設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down 時 Frame 転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

第13章 L2TPv3 機能

XII. L2TPv3 設定例2 (L2TP トンネル二重化)

Secondary セッション側の L2TPv3 Xconnect 設定をします。

- Primary セッションと同じ要領で設定して下さい。

Xconnect ID設定 (Group設定を行う場合は指定)	2 [1-4294967295]
Tunnel設定選択	192.168.1.2
L2Frame受信インターフェース設定	eth0 (interface名指定)
VLAN ID設定 (VLAN Tag付与する場合指定)	0 [0-4094] (0の場合付与しない)
Remote END ID設定	2 [1-4294967295]
Reschedule Interval設定	0 [0-1000] (default 0s)
Auto Negotiation設定 (Service起動時)	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
MSS設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
MSS値(byte)	0 [0-1460] (0の場合は自動設定)
Loop Detect設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Known Unicast設定	<input type="radio"/> 送信する <input checked="" type="radio"/> 送信しない
Circuit Down時Frame転送設定	<input checked="" type="radio"/> 送信する <input type="radio"/> 送信しない
Split Horizon設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

L2TPv3 Group 設定をします。

- 「Group ID」は任意のグループ ID を設定します。
- 「Primary Xconnect 設定選択」はプルダウンから Primary セッションの Xconnect ID を選択します。
- 「Secondary Xconnect 設定選択」はプルダウンから Secondary セッションの Xconnect ID を選択します。
- 本例では「Preempt 設定」「Primary active 時の Secondary Session 強制切断設定」をそれぞれ「無効」に設定しています。常に Primary/Secondary セッションの両方が接続された状態となり、Secondary セッション側は Stand-by 状態として待機しています。Primary セッションの障害時には、Secondary セッションを即時に Active 化します。

Group ID	1 [1-4095]
Primary Xconnect設定選択	1
Secondary Xconnect設定選択	2
Preempt設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Primary active時の Secondary Session強制切断設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Active Hold設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

XII. L2TPv3 設定例2 (L2TPトンネル二重化)

L2TPv3 Tunnel Setup の起動

設定後が終わりましたら L2TPv3 機能の起動 / 停止設定を行います。

「起動 / 停止」画面で Xconnect Interface と Remote-ID を選択し、画面下の「実行」ボタンをクリックすると L2TPv3 接続を開始します。

本例では、拠点側から Primary/Secondary の両方の L2TPv3 接続を開始し、Primary 側が ACTIVE セッション、Secondary 側は STAND-BY セッションとして確立します。

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

第 14 章

L2TPv3 フィルタ機能

1. L2TPv3 フィルタ 機能概要

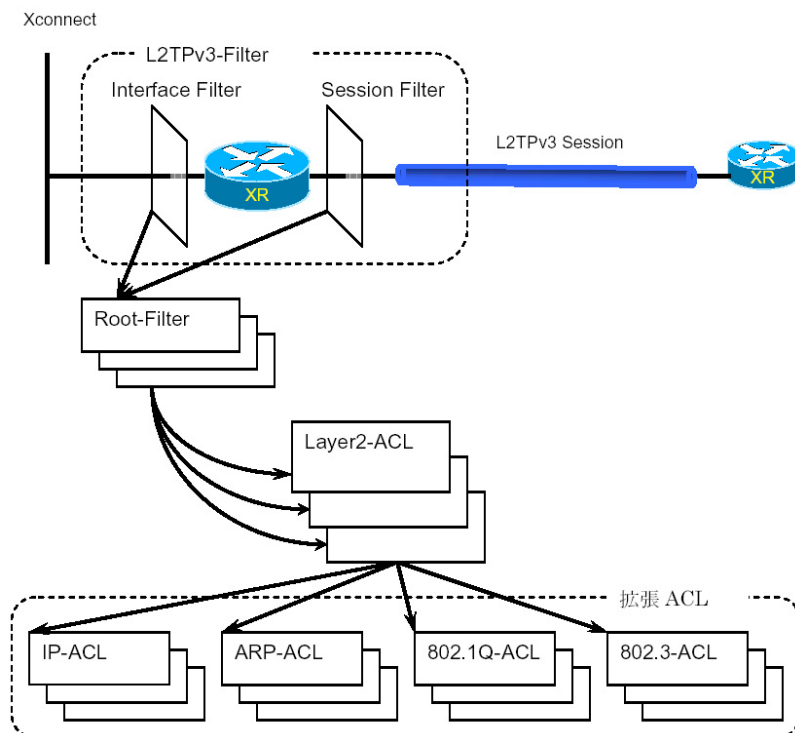
L2TPv3 フィルタ概要

XR の L2TPv3 フィルタ機能は、ユーザが設定したフィルタリングルールに従い、Xconnect Interface 上もしくは Session 上でアクセス制御を行ないます。

アクセス制御は、MAC アドレスや IPv4、ARP、802.1Q、TCP/UDP など L2-L4 での詳細な指定が可能です。

L2TPv3 フィルタ設定概要

L2TPv3 フィルタは以下の要素で構成されています。



(1) Access Control List (ACL)

Layer2 レベルでルールを記述する「Layer2 ACL」およびプロトコル毎に詳細なルールを記述する拡張 ACL として IP-ACL、ARP-ACL、802.1Q-ACL、802.3-ACL があります。

(2) Root-Filter

Root-Filter では Layer2 ACL を検索する順にリストします。各 Root Filter にはユーザによりシステムでユニークな名前を付与し、識別します。

Root Filter では、配下に設定された全ての Layer2 ACL に一致しなかった場合の動作を Default ポリシーとします。Default ポリシーとして定義可能な動作は、deny (破棄) / permit (許可) です。

(3) L2TPv3-Filter

Xconnect Interface、Session それぞれに適用する Root-Filter を設定します。Xconnect Interface に関しては Interface Filter、Session に関しては Session Filter で設定します。

1. L2TPv3 フィルタ 機能概要

L2TPv3 フィルタの動作 (ポリシー)

設定条件に一致した場合、L2TPv3 フィルタは以下の動作を行います。

1) 許可 (permit)

フィルタルールに一致した場合、検索を中止してフレームを転送します。

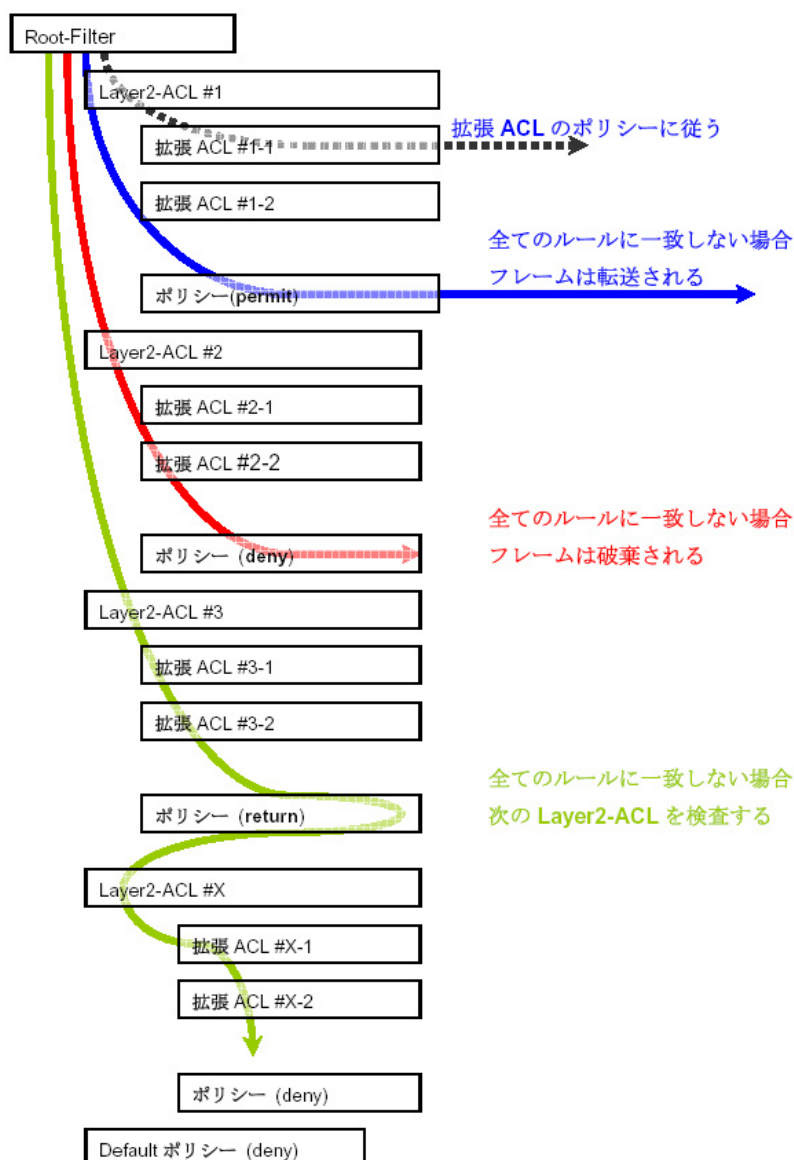
2) 破棄 (deny)

フィルタルールに一致した場合、検索を中止してフレームを破棄します。

3) 復帰 (return)

Layer2 ACL でのみ指定可能です。フィルタルールに一致しない場合、該当 Layer2 ACL での検索を中止して呼び出し元の次の Layer2 ACL から検索を再開します。

フィルタ評価のモデル図



1. L2TPv3 フィルタ 機能概要

フィルタの評価

Root-Filter の配下に設定された Layer2 ACL の検索は、定義された上位から順番に行い、最初に条件に一致したものの (1st match) に対して以下の評価を行います。

- ・ 拡張 ACL がない場合
該当 Layer2 ACL のポリシーに従い、deny/permit/return を行います。
- ・ 拡張 ACL がある場合
Layer2 ACL の配下に設定された拡張 ACL の検索は、1st match にて検索を行い、以下の評価を行います。
 - 1) 拡張 ACL に一致する場合、拡張 ACL の policy に従い deny/permit を行います。
 - 2) 全ての拡張 ACL に一致しない場合、該当 Layer2 ACL のポリシーに従い、deny/permit/return を行います。

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

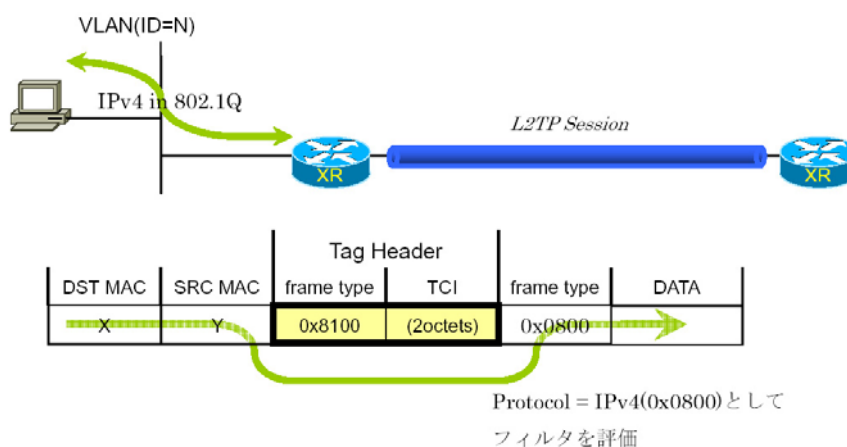
フィルタ処理順序

L2TPv3 フィルタにおける処理順序は、IN 側フィルタでは送信元 / 宛先 MAC アドレスのチェックを行ったあとになります。

「Known Unicast 設定」や「Circuit Down 時の Frame 転送」によりフレームの転送が禁止されている状態で permit 条件に一致するフレームを受信しても、フレームの転送は行われませんのでご注意ください。

802.1Q タグヘッダ

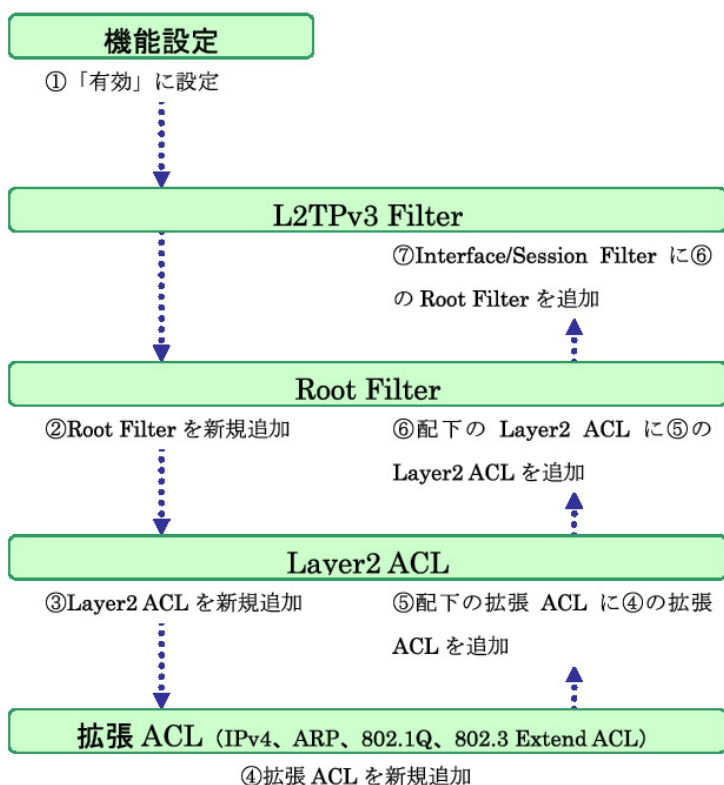
Xconnect Interface が VLAN (802.1Q) であるフレームをフィルタリングする場合、タグヘッダについては、フィルタの評価対象から除外し、タグヘッダに続くフィールドから再開します (下図参照)。



11. 設定順序について

L2TPv3 Filter の設定順序は、下の表を参考にして下さい。

【L2TPv3 Filter の設定順序】



第14章 L2TPv3 フィルタ機能

III. 機能設定

「各種サービスの設定」 「L2TPv3」をクリックして、画面上部の「L2TPv3 Filter 設定」をクリックします。

L2TPv3 フィルタは以下の画面で設定を行います。



機能設定

L2TPv3 フィルタ設定画面の「機能設定」をクリックします。



本機能

L2TPv3 Filter 機能の有効 / 無効を選択し、設定ボタンを押します。

* 設定で可能な文字について

Root Filter・ACL名で使用可能な文字は英数字、ハイフン(-)、アンダースコア(_)、ピリオド(.)です。1～64文字の間で設定できます。ただし、1文字目は英数字に限ります。

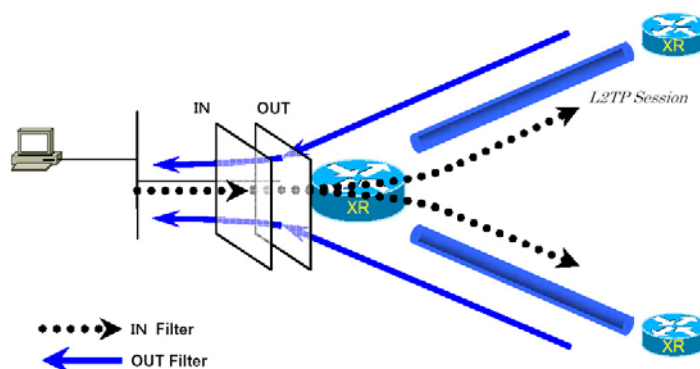
IV. L2TPv3 Filter 設定

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

Interface Filter

Index	Interface	IN Filter	OUT Filter	edit
1	eth0	Root-1	Root-2	edit

Interface Filter は、Root Filter を Xconnect Interface に対応づけてフィルタリングを行います。IN Filter は外側のネットワークから Xconnect Interface を通して XR が受信するフレームをフィルタリングします。OUT Filter は XR が Xconnect Interface を通して送信するフレームをフィルタリングします。



Interface Filter のモデル図

Interface Filter を編集する

Interface Filter 一覧表示内の「edit」ボタンをクリックします。

Interface	eth0
ACL(in)	Root-1
ACL(out)	Root-2

Interface

Xconnect Interface に設定したインターフェース名が表示されます。

ACL(in)

IN 方向に設定する Root Filter 名を選択します。

ACL(out)

OUT 方向に設定する Root Filter 名を選択します。

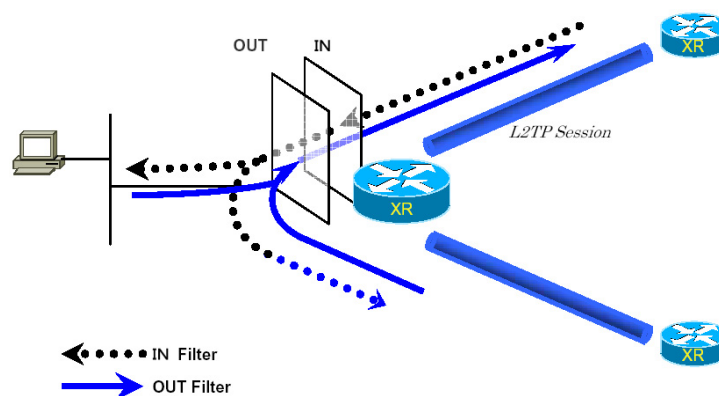
IV. L2TPv3 Filter 設定

Session Filter

Index	Peer ID	RemoteEND ID	IN Filter	OUT Filter	edit
1	192.168.1.253	1	Root-3	Root-4	edit

Session Filter は、Root Filter を Session に関連づけてフィルタリングを行いますので、Session から Session への通信を制御することが出来ます。

下の図で、IN Filter は XR が L2TP Session A から受信するフレームをフィルタリングしています。OUT Filter は XR が L2TP Session A へ送信するフレームをフィルタリングしています。



Session Filter のモデル図

Session Filter を編集する

Session Filter 一覧表示内の「edit」ボタンをクリックします。

PeerID : RemoteEndID	192.168.1.253:1
ACL(in)	Root-3
ACL(out)	Root-4

PeerID : RemoteEndID

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

ACL(in)

IN 方向に設定したい Root Filter 名を選択します。

ACL(out)

OUT 方向に設定したい Root Filter 名を選択します。

V. Root Filter 設定

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

Index	Root Filter Name	edit	layer2	del
1	Root-1	edit	layer2	<input type="checkbox"/>

Root Filter を追加する

画面下の「追加」ボタンをクリックします。

Root Filter Name	<input type="text"/>
Default Policy	<input type="text" value="deny"/>

Root Filter Name

Root Filter を識別するための名前を入力します
 (*).

Default Policy

受け取ったフレームが、その Root Filter の配下
 にある Layer2 ACL のすべてに一致しなかった場合
 の動作を設定します。Permit/Deny のどちらかを選
 択して下さい。

Root Filter を編集する

一覧表示内の「edit」をクリックします。

Index	1
Root Filter Name	<input type="text" value="FILTER-1"/>
Default Policy	<input type="text" value="permit"/>

追加画面と同様に設定してください。

Root Filter を削除する

一覧表示内の「del」にチェックを入れて画面下の
 「削除」ボタンをクリックします。

V. Root Filter 設定

配下に Layer2 ACL を設定する

一覧表示内の「layer2」をクリックします。

現在設定されている配下の Layer2 ACL が一覧表示されます。

Seq.No.	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length	edit	del
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4	edit	<input type="checkbox"/>
*	default	deny					

配下の Layer2 ACL を追加する

画面下の「追加」ボタンをクリックします。

Seq.No.	<input type="text"/>
Layer2 ACL Name	<input type="text" value="----"/>

Seq.No.

配下の Layer2 ACL を検索する際の順番 (シーケンス番号) を指定します。無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

Layer2 ACL Name

その Root Filter の配下に設定したい Layer2 ACL を選択します。同一 Root Filter 内で重複する Layer2 ACL を設定することはできません。

配下の Layer2 ACL を編集する

一覧表示内の「edit」をクリックします。

Seq.No.	1
Layer2 ACL Name	<input type="text" value="L2ACL-1"/>

追加画面と同様に設定してください。

配下の Layer2 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

第 14 章 L2TPv3 フィルタ機能

VI. Layer2 ACL 設定

L2TPv3 Filter 設定画面の「Layer2 ACL 設定」をクリックします。
現在設定されている Layer2 ACL が一覧表示されます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length	edit	extend	del
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4	edit	extend	<input type="checkbox"/>

Layer2 ACL を追加する

画面下の「追加」ボタンをクリックします。

Layer2 ACL Name	<input type="text"/>
Policy	---- ▾
Source MAC	<input type="text"/>
Destination MAC	<input type="text"/>
Type/Length	---- ▾ or <input type="text"/> [0x0600-0xffff]

Layer2 ACL Name

ACLを識別するための名前を入力します(*)。

Policy

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

Source MAC

送信元 MAC アドレスを指定します (マスクによるフィルタリングも可能です)。

<フォーマット>

XX:XX:XX:XX:XX:XX

XX:XX:XX:XX:XX:XX/MM:MM:MM:MM:MM:MM

Destination MAC

あて先 MAC アドレスを指定します。Source MAC 設定と同様に設定して下さい。

Type/Length

IPv4、IPv6、ARP、802.1Q、length または 16 進数指定の中から選択します (無指定でも可)。16 進数指定の場合は右側の入力欄に指定値を入力します。(指定可能な範囲 : 0600-ffff)。

IPv4、ARP、802.1Q を指定すると配下の拡張 ACL に IPv4 Extend ACL、ARP Extend ACL、802.1Q Extend ACL を指定することが出来ます。16 進数で length を指定すると、802.3 Extend ACL を指定することが出来ます。

Layer2 ACL を編集する

一覧表示内の「edit」をクリックします。

Layer2 ACL Name	L2ACL-1
Policy	permit ▾
Source MAC	00:11:22:33:44:55
Destination MAC	<input type="text"/>
Type/Length	IPv4 ▾ or <input type="text"/> [0x0600-0xffff]

追加画面と同様に設定してください。

Layer2 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

VI. Layer2 ACL 設定

配下に拡張 ACL を設定する

一覧表示内の「extend」をクリックします。

現在設定されている配下の拡張 ACL が一覧表示されます。

Index	Layer2 ACL Name	Policy	Source MAC	Destination MAC	Type/Length
1	L2ACL-1	permit	00:11:22:33:44:55		IPv4

Seq.No.	Extend ACL Name	edit	del
1	IPv4-1	edit	<input type="checkbox"/>

配下の拡張 ACL を追加する

画面下の「追加」ボタンをクリックします。

Seq.No.	<input type="text"/>
Name	---- <input type="button" value="v"/>

Seq.No.

配下の拡張 ACL を検索する際の順番（シーケンス番号）を指定します。無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

Name

設定可能な拡張 ACL 名を選択します。同一 Layer2 ACL 内で重複する拡張 ACL を設定することはできません。

配下の拡張 ACL を編集する

一覧表示内の「edit」をクリックします。

Seq.No.	1
Name	IPv4acl_sample <input type="button" value="v"/>

追加画面と同様に設定してください。

配下の拡張 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

第 14 章 L2TPv3 フィルタ機能

VII. IPv4 Extend ACL 設定

L2TPV3 Filter 設定画面の「IPv4 Extend ACL 設定」をクリックします。
現在設定されている IPv4 Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	Source IP	Destination IP	TOS	Protocol	option	edit	del
1	IPv4-1	permit	192.168.0.100	192.168.0.200		tcp		edit	<input type="checkbox"/>

オプション欄表示の意味は次の通りです。

- ・src-port=X 送信元ポート番号が X
- ・dst-port=X:Y あて先ポート番号の範囲が X ~ Y

IPv4 Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Extend ACL Name	<input type="text"/>
Policy	---- <input type="button" value="v"/>
Source IP	<input type="text"/>
Destination IP	<input type="text"/>
TOS	<input type="text"/> [0-0xff]
IP Protocol	---- <input type="button" value="v"/> or <input type="text"/> [0-255]
Source Port	<input type="text"/> [1-65535]
Destination Port	<input type="text"/> [1-65535]
ICMP Type	<input type="text"/> [0-255]
ICMP Code	<input type="text"/> [0-255]

Extend ACL Name

拡張ACLを識別するための名前を入力します(*)。

Policy

deny (破棄) / permit (許可) を選択します。

Source IP

送信元 IP アドレスを指定します (マスクによる指定も可)。

<フォーマット>

A.B.C.D

A.B.C.D/M

Destination IP

あて先 IP アドレスを指定します。Source IP と同様に設定して下さい。

TOS

TOS 値を 16 進数で指定します。

(指定可能な範囲 : 00-ff)

IP Protocol

TCP/UDP/ICMP または 10 進数指定の中から選択します (無指定でも可)。

10 進数指定の場合は右側の入力欄に指定値を入力して下さい。

(指定可能な範囲 : 0-255)

Source Port

送信元ポートを指定します。IP Protocol に TCP/UDP を指定した時のみ設定可能です。

範囲設定が可能です。

<フォーマット>

xxx (ポート番号 xx)

xxx:yyy (xxx 以上、yyy 以下のポート番号)

Destination Port

あて先ポートを指定します。設定方法は Source Port と同様です。

ICMP Type

ICMP Type の指定が可能です。IP Protocol に ICMP を指定した場合のみ設定可能です。

(指定可能な範囲 : 0-255)

ICMP Code

ICMP Code の指定が可能です。ICMP Type が指定されていないと設定できません。

(指定可能な範囲 : 0-255)

VII. IPv4 Extend ACL 設定

IPv4 Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Extend ACL Name	<input type="text" value="IPv4-1"/>
Policy	<input type="text" value="permit"/>
Source IP	<input type="text" value="192.168.0.100"/>
Destination IP	<input type="text" value="192.168.0.200"/>
TOS	<input type="text"/> [0-0xff]
IP Protocol	<input type="text" value="TCP"/> or <input type="text"/> [0-255]
Source Port	<input type="text"/> [1-65535]
Destination Port	<input type="text"/> [1-65535]
ICMP Type	<input type="text"/> [0-255]
ICMP Code	<input type="text"/> [0-255]

追加画面と同様に設定してください。

IPv4 Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

第14章 L2TPv3 フィルタ機能

VIII. ARP Extend ACL 設定

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

Index	Extend ACL Name	Policy	OPCODE	Source MAC	Destination MAC	Source IP	Destination IP	edit	del
1	ARP-1	permit		00:11:22:33:44:55			192.168.0.200	edit	<input type="checkbox"/>

ARP Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Extend ACL Name	<input type="text"/>
Policy	---- <input type="button" value="v"/>
OPCODE	---- <input type="button" value="v"/> or <input type="text"/> [0-65535]
Source MAC	<input type="text"/>
Destination MAC	<input type="text"/>
Source IP	<input type="text"/>
Destination IP	<input type="text"/>

Extend ACL Name

拡張 ACL を識別するための名前を入力します(*)。

Policy

deny (破棄) / permit (許可) を選択します。

OPCODE

Request、Reply、Request_Reverse、
Reply_Reverse、DRARP_Request、DRARP_Reply、
DRARP_Error、InARP_Request、ARP_NAK または 10
進数指定の中から選択します (無指定でも可)。
10 進数指定の場合は右側の入力欄に指定値を入力
して下さい (指定可能な範囲 : 0-65535)。

Source MAC

送信元 MAC アドレスを指定します (マスクによる
フィルタリングも可)。

<フォーマット>

XX:XX:XX:XX:XX:XX

XX:XX:XX:XX:XX:XX/MM:MM:MM:MM:MM:MM

Destination MAC

あて先 MAC アドレスを指定します。Source MAC 設
定と同様に設定して下さい。

Source IP

送信元 IP アドレスを指定します (マスクによる
フィルタリングも可)。

<フォーマット>

A.B.C.D

A.B.C.D/M

Destination IP

あて先 IP アドレスを指定します。Source IP 設定
と同様に設定して下さい。

ARP Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Extend ACL Name	ARP-1
Policy	permit <input type="button" value="v"/>
OPCODE	---- <input type="button" value="v"/> or <input type="text"/> [0-65535]
Source MAC	00:11:22:33:44:55
Destination MAC	<input type="text"/>
Source IP	<input type="text"/>
Destination IP	192.168.0.200

追加画面と同様に設定してください。

ARP Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の
「削除」ボタンをクリックします。

第 14 章 L2TPv3 フィルタ機能

IX. 802.1Q Extend ACL 設定

L2TPv3 Filter 設定画面の「802.1Q Extend ACL 設定」をクリックします。
現在設定されている 802.1Q Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	VLAN ID	Priority	Ethernet Type	edit	extend	del
1	802.1Q-1	permit	10		IPv4	edit	extend	<input type="checkbox"/>

802.1Q Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Name	<input type="text"/>
Policy	---- ▾
VLAN ID	<input type="text"/> [0-4095]
Priority	<input type="text"/> [0-7]
Ethernet Type	---- ▾ or <input type="text"/> [0x0600-0xffff]

Name
拡張 ACL を識別するための名前を入力します(*)。

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

VLAN ID
VLAN ID を指定します。
範囲設定が可能です。
(指定可能な範囲 : 0-4095)

<フォーマット>
xxx (VLAN ID : xx)
xxx:yyy (xxx 以上、yyy 以下の VLAN ID)

Priority
IEEE 802.1P で規定されている Priority Field を判定します。
(指定可能な範囲 : 0 - 7)

Ethernet Type

カプセル化されたフレームの Ethernet Type を指定します。IPv4、IPv6、ARP または 16 進数指定の中から選択します (無指定でも設定可)。16 進数指定の場合は右側の入力欄に指定値を入力して下さい。

(指定可能な範囲 : 0600-ffff)

IPv4、ARP を指定すると配下の拡張 ACL に IPv4 Extend ACL、ARP Extend ACL を指定することができます。

802.1Q Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Name	802.1Q-1
Policy	permit ▾
VLAN ID	10 [0-4095]
Priority	<input type="text"/> [0-7]
Ethernet Type	IPv4 ▾ or <input type="text"/> [0x0600-0xffff]

追加画面と同様に設定してください。

802.1Q Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

IX. 802.1Q Extend ACL 設定

配下に拡張 ACL を設定する

一覧表示内の「extend」をクリックします。
 現在設定されている配下の拡張 ACL の一覧が表示されます。

Index	Extend ACL Name	Policy	VLAN ID	Priority	Ethernet Type
1	802.1Q-1	deny	10		ARP

Seq.No.	Extend ACL Name	edit	del
1	ARP-1	edit	<input type="checkbox"/>

配下の拡張 ACL を追加する

画面下の「追加」ボタンをクリックします。

Seq.No.	<input type="text"/>
Name	---- <input type="button" value="v"/>

Seq.NO.

配下の拡張 ACL を検索する際の順番（シーケンス番号）を指定します。無指定またはすでに設定されている数を越えた数値を入力した場合、末尾に追加されます。

Name

設定可能な拡張 ACL 名を選択します。同一 802.1Q Extend ACL 内で重複する拡張 ACL を設定することはできません。

配下の拡張 ACL を編集する

一覧表示内の「edit」をクリックします。

Seq.No.	1
Name	ARP-1 <input type="button" value="v"/>

追加画面と同様に設定してください。

配下の拡張 ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

X. 802.3 Extend ACL 設定

L2TPv3 Filter 設定画面の「802.3 Extend ACL 設定」をクリックします。
現在設定されている 802.3 Extend ACL が一覧表示されます。

Index	Extend ACL Name	Policy	DSAP/SSAP	type	edit	del
1	802.3-1	permit	0xaa		edit	<input type="checkbox"/>

802.3 Extend ACL を追加する

画面下の「追加」ボタンをクリックします。

Name	<input type="text"/>
Policy	---- ▾
DSAP/SSAP	0x <input type="text"/> [0x00-0xff]
Type	0x <input type="text"/> [0x0600-0xffff]

Name

拡張 ACL を識別するための名前を入力します(*)。

Policy

deny (破棄) / permit (許可) のいずれかを選択します。

DSAP/SSAP

16 進数で DSAP/SSAP を指定します。

(指定可能な範囲 : 00-ff)

DSAP/SSAP は等値なので 1byte で指定します。

Type

16 進数で 802.3 with SNAP の type field を指定します。

(指定可能な範囲 : 0600-ffff)

DSAP/SSAP を指定した場合は設定できません。

この入力欄で Type を指定した場合の DSAP/SSAP は 0xaa/0xaa として判定されます。

802.3 Extend ACL を編集する

一覧表示内の「edit」をクリックします。

Name	ACL-802_3-1
Policy	permit ▾
DSAP/SSAP	0x aa [0x00-0xff]
Type	0x <input type="text"/> [0x0600-0xffff]

追加画面と同様に設定してください。

802.3 Extend ACL を削除する

一覧表示内の「del」にチェックを入れて画面下の「削除」ボタンをクリックします。

XI. 情報表示

L2TPv3 Filter 設定画面の「情報表示」をクリックします。

root ACL情報表示	---- <input type="checkbox"/> detail表示/リセット	表示する	カウンタリセット
layer2 ACL情報表示	---- <input type="checkbox"/> detail表示/リセット	表示する	カウンタリセット
ipv4 ACL情報表示	----	表示する	カウンタリセット
arp ACL情報表示	----	表示する	カウンタリセット
802_1q ACL情報表示	---- <input type="checkbox"/> detail表示/リセット	表示する	カウンタリセット
802_3 ACL情報表示	----	表示する	カウンタリセット
interface Filter情報表示	----	表示する	カウンタリセット
session Filter情報表示	----	表示する	カウンタリセット
すべてのACL情報表示		表示する	カウンタリセット

表示する

「表示する」ボタンをクリックすると ACL 情報を表示します。プルダウンから ACL 名を選択して個別に表示することもできます。

「detail 表示 / リセット」にチェックを入れてクリックすると、設定した全ての ACL 情報が表示されます。

カウンタリセット

「カウンタリセット」ボタンをクリックすると ACL のカウンタをリセットします。プルダウンから ACL 名を選択して個別にリセットすることもできます。

「detail 表示 / リセット」にチェックを入れてクリックすると、配下に設定されている ACL のカウンタも同時にリセットできます。

「表示する」ボタンで表示される情報は以下の通りです。

(は detail 表示にチェックを入れた時に表示されます。)

Root ACL 情報表示

Root Filter 名 総カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
(+ 拡張 ACL 名)

(カウンタ (frame 数、 byte 数) Policy)

+Default Policy カウンタ (frame 数、 byte 数) Default Policy

layer2 ACL 情報表示

Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、送信元 MAC アドレス、あて先 MAC アドレス、Protocol
(+ 拡張 ACL 名)

(カウンタ (frame 数、 byte 数) Policy)

ipv4 ACL 情報表示

IPv4 ACL 名

カウンタ (frame 数、 byte 数) Policy、送信元 IP アドレス、あて先 IP アドレス、TOS、Protocol、オプション

XI. 情報表示

arp ACL 情報表示

ARP ACL 名

カウンタ (frame 数、 byte 数) Policy、 Code、 送信元 MAC アドレス、 あて先 MAC アドレス、
送信元 IP アドレス、 あて先 IP アドレス

802_1q ACL 情報表示

802.1Q ACL 名

カウンタ (frame 数、 byte 数) Policy、 VLAN-ID、 Priority、 encap-type
(+ 拡張 ACL 名)
(カウンタ (frame 数、 byte 数) Policy)

802_3 ACL 情報表示

802.3 ACL 名

カウンタ (frame 数、 byte 数) Policy、 DSAP/SSAP、 type

interface Filter 情報表示

interface、 in : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

interface、 out : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

session Filter 情報表示

Peer ID、 RemoteEND-ID、 in : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

Peer ID、 RemoteEND-ID、 out : カウンタ (frame 数、 byte 数) : Root Filter 名

Root Filter 名、 カウンタ (frame 数、 byte 数)

+Layer2 ACL 名

カウンタ (frame 数、 byte 数) Policy、 送信元 MAC アドレス、 あて先 MAC アドレス、 Protocol
+Default Policy カウンタ (frame 数、 byte 数) Default Policy

第 15 章

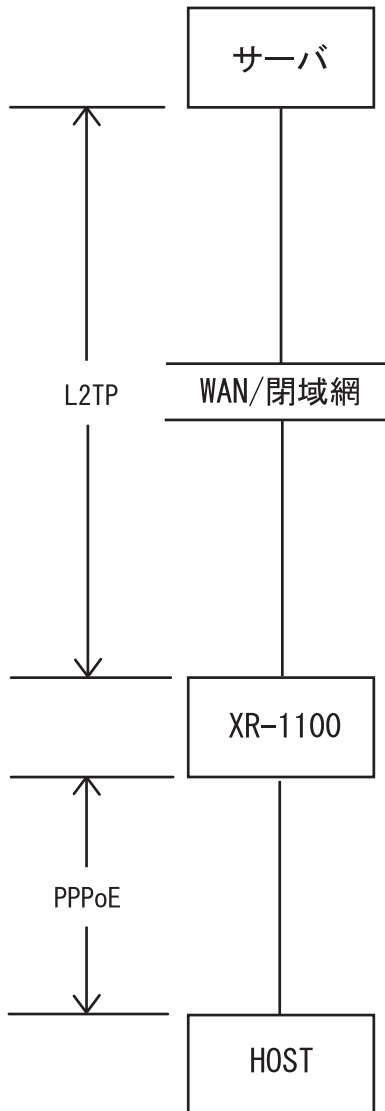
PPPoE to L2TP

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

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

L2TP トンネルの設定

「L2TP Tunnel 設定」 「New Entry」をクリックします。

Description	<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	1701 (default 1701)
AVP Hiding設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
Hello Interval設定	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。

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

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

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

最後に「設定」をクリックします。

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

PPPoE to L2TP 機能について

オプション設定

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

Local hostname	localhost
PPPoE Frame 受信インターフェース設定	<input checked="" type="radio"/> eth0 <input type="radio"/> eth1 <input type="radio"/> eth2 <input type="radio"/> eth3
MAX Session 数	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 受信インターフェース設定

PPPoE フレームを受信するインター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ーフェースを選択してください。

MAX session 数

PPPoE to L2TP 接続での最大セッション数を設定します。

Path MTU Discovery

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

Debug 設定(Syslog メッセージ出力設定)

syslog に出力する Debug ログの種類を選択します。

最後に「設定」をクリックします。

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

ステータス表示

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

第 16 章

SYSLOG 機能

syslog 機能の設定

XR-1100 は、syslog を出力・表示することが可能です。また、他の syslog サーバに送出することも出来ます。さらに、ログの内容を電子メールで送ることも出来ます。

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

ログの取得

出力先

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

送信先 IP アドレス

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

取得プライオリティ

ログ内容の出力レベルを指定します。プライオリティの内容は右の通りです。

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

--MARK-- を出力する時間間隔

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

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

syslog 機能の設定

システムメッセージ

本装置のシステム情報を定期的に出力することができます。「出力しない」「MARK 出力時」「1 時間毎に出力」から選択します。

出力しない
システム情報を出しません。

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

1 時間毎に出力
システム情報を 1 時間毎に出力します。

出力される情報は下記の内容です。

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

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

ログメール機能設定

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

ログメール機能を使うときは「送信する」を選択し、「ログメッセージ送信先のメールアドレス」を指定します。さらに、

「ログメッセージ送信元のメールアドレス」
「件名」
「中継するサーバアドレス」

を任意で指定できます。「件名」は半角英数字のみ使用できます。

何も指定しないときは

送信元アドレス「root@localdomain.co.jp」
件名は無し

で送信されます。

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

<入力形式> @ <ドメイン名>

<入力例> @mail.xxxxxx.co.jp

syslog 機能の設定

検出文字列の指定

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

文字列の指定は、1行につき256文字まで、かつ最大32行までです。空白・大小文字も判別します。一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したログのみ抽出して送信します。**なお「検出文字列の指定」項目は、「ログメール機能」のみ有効です。**

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

ファシリティと監視レベルについて

XR-1100シリーズで設定されているsyslogのファシリティ・監視レベルは以下のようになっています。

[ファシリティ：監視レベル]

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

<オプションUSBメモリー装着時のsyslog機能>

オプションUSBメモリーを装着している場合は、システムログは自動的にUSBメモリーに記録されます。

ログはローテーションしてUSBメモリーに記録されていきます。記録のタイミングは

- ・1週間ごと
- ・USBメモリーの空き容量が20%に達したとき

のいずれか早い方です。

ローテーションで記録されたログは圧縮して保存されます。保存されるファイルは最大で4つです。以降は古いログファイルから順に削除されていきます。

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

第 17 章

攻撃検出機能

攻撃検出機能の設定

攻撃検出機能の概要

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

ログの出力

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

攻撃検出機能の設定

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

使用するインターフェース	<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 type="text" value="any"/>

(画面は XR-1100/CT での表示例です)

使用するインタフェース

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

検出対象となる IP アドレス

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

<入力例>

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

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

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

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

第 18 章

SNMP エージェント機能

第18章 SNMP エージェント機能

1. SNMP エージェント機能の設定

SNMP エージェントを起動すると、SNMP マネージャから本装置のMIB Ver.2(RFC1213)および、プライベートMIBの情報を取得することができます。

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

SNMP マネージャ	192.168.0.0/24
コミュニティ名	community <small>SNMP TRAP 用</small>
ロケーション	
コンタクト	
SNMP TRAP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
SNMP TRAP の送信元 IP アドレス	
SNMP TRAP の送信元	<input 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="radio"/> 指定しない <input type="radio"/> IP アドレス

SNMP マネージャ

SNMP マネージャを使いたいネットワーク範囲(ネットワーク番号/サブネット長)または、SNMP マネージャの IP アドレスを指定します。最大3つまで指定することができます。

コミュニティ名

任意のコミュニティ名を指定します。ご使用の SNMP マネージャの設定に合わせて入力してください。Get/Response 用と Trap 用とそれぞれ異なるコミュニティ名が設定可能です。

ロケーション

装置の設置場所を表す標準 MIB “sysLocation” (oid=.1.3.6.1.2.1.1.6.0)に、任意のロケーション名を設定することができます。

コンタクト

装置管理者の連絡先を表す標準 MIB “sysContact” (oid=.1.3.6.1.2.1.1.4.0)に、任意の連絡先情報を設定することができます。

SNMP TRAP

「使用する」を選択すると、SNMP TRAP を送信できるようになります。

SNMP TRAP の送信先 IP アドレス
SNMP TRAP を送信する先(SNMP マネージャ)の IP アドレスを指定します。
最大3つまで指定することができます。

SNMP TRAP の送信元
SNMP パケット内の “Agent Address” に、任意のインタ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」を選択した場合

SNMP TRAP の送信元アドレスが自動的に設定されます。

「IP アドレス」を選択した場合

SNMP TRAP の送信元アドレスを指定します。

「インターフェース」を選択した場合

SNMP TRAP の送信元アドレスとなるインタフェース名を指定します。
指定可能なインタフェースは、本装置のイーサネットポートと PPP インタフェースのみです。

送信元

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

入力が終わりましたら「設定の保存」をクリックして設定完了です。

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

I. 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)

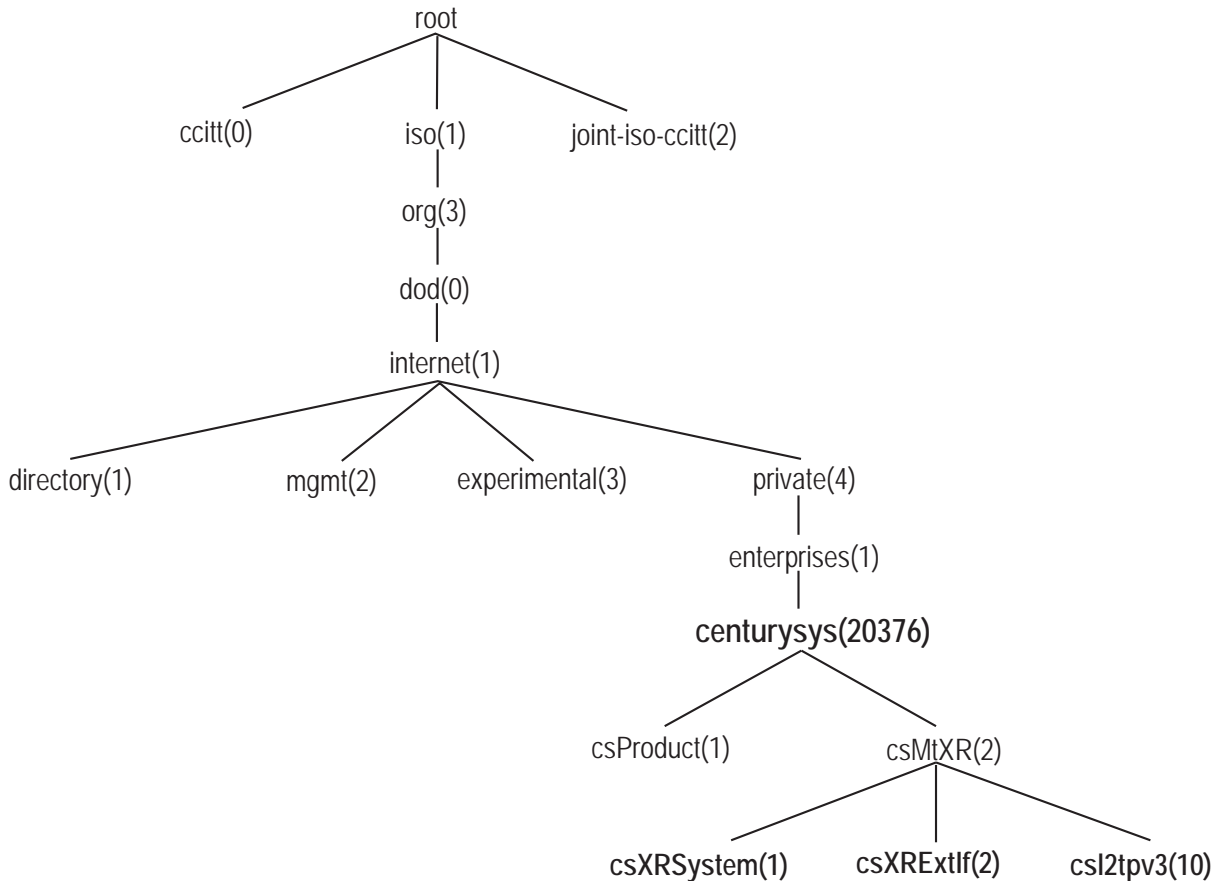
SNMP TRAPを送信するトリガーについて

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
- 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
 - L2TPv3
 - SYSLOG
 - 攻撃検出
 - NTP
 - VRRP
- SNMP TRAP 自身の起動、停止

II. Century Systems プライベートMIBについて

本装置では保守性を高めるために以下のようなプライベートMIB(centurysys)を実装しています。このMIB定義の階層下には、XRシステム用MIB(csXRSystem)、XRインタフェース用MIB(csXRExtIf)、L2TPv3用MIB(csl2tpv3)の3つがあります。



csXRSystem

システム情報に関する XR 独自の定義 MIB です。CPU 使用率、空きメモリ量、コネクショントラッキング数、ファンステータスのシステム情報や、サービスの状態に関する情報を定義しています。また、これらに関する Trap 通知用の MIB 定義も含まれます。なお、主なシステム情報 Trap の通知条件は下記の通りです。

- ・ CPU 使用率 : 90% 超過時
- ・ 空きメモリ量 : 2MB 低下時
- ・ コネクショントラッキング : 総数の 90% 超過時

csXRExtIf

インタフェースに関する XR 独自の定義 MIB です。各インタフェースの状態や IP アドレス情報などを定義しています。また、UP/DOWN やアドレス変更時などの Trap 通知用の MIB 定義も含まれます。

csl2tpv3

L2TPv3 サービスに関する定義 MIB です。Tunnel / Session の状態や、送受信フレームのカウント情報などを定義しています。また、Tunnel / Session の Establish や Down 時などの Trap 通知用の MIB 定義も含まれます。

これらの MIB 定義の詳細については、MIB 定義ファイルを参照して下さい。

注) システム、インタフェース、サービスに関する情報は標準 MIB-II でも取得できますが、Trap については全て独自 MIB によって通知されます。

第 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

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

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

問合せ先NTPサーバ (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 X を指定した場合、秒単位の間隔は2 ^X (sec) ex. (4: 16sec, 6: 64sec,... 10: 1024sec)						
時刻同期タイムアウト時間	<input type="text" value="1"/>	(秒:1-10) NTPサービス起動時に適用されます				

NTPサーバのIPアドレスもしくはFQDNを「設定1」もしくは「設定2」に入力します(NTPサーバの場所は2箇所設定できます)。これにより、本装置がNTPクライアント/サーバとして動作できます。

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

Polling 間隔

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

(例 4 : 16秒、 6 : 64秒、... 10 : 1024秒)

数字は4 ~ 17(16 ~ 131072秒)の間で設定出来ます。

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

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

時刻同期タイムアウト時間

サーバ応答の最大待ち時間を設定できます。1 ~ 10秒の間で設定できます。

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

「情報表示」をクリックすると、現在のNTPサービスの動作状況を確認できます。

基準NTPサーバについて

基準となるNTPサーバには次のようなものがあります。

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

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

NTP クライアントの設定方法

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

Windows 9x/Me/NT の場合

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

Windows 2000 の場合

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

Windows XP の場合

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

Macintosh の場合

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

Linux の場合

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

第 20 章

VRRP 機能

VRRP の設定方法

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

「各種サービスの設定」 「VRRP サービス」をクリックして以下の画面でVRRPサービスの設定をします。

No.	使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
1	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ーフェースを選択します。

仮想MACアドレス

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

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

認証形式に「PASS」または「AH」を選択した場合のパスワードを入力します。設定できる文字数は1 ~ 8文字です。

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

ステータスの表示

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

第21章

アクセスサーバ機能

第21章 アクセスサーバ機能

1. アクセスサーバ機能について

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

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

ダイヤルアップクライアント



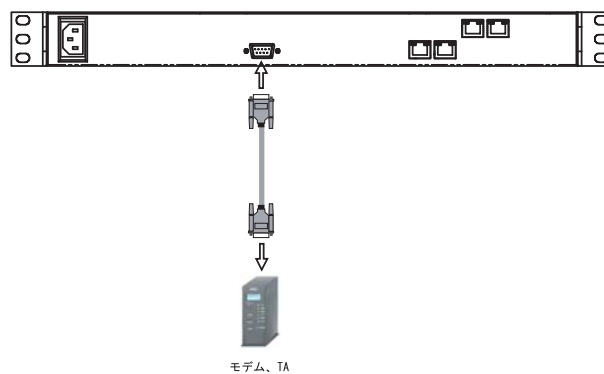
II. 本装置とアナログモデム /TAの接続

アクセスサーバ機能を設定する前に、本装置とアナログモデムやTAを接続します。以下のように接続してください。

アナログモデム /TAの接続

- 1 本装置本体背面の「RS-232」ポートとアナログモデム /TAのシリアルポートをシリアルケーブルで接続してください。シリアルケーブルは別途ご用意ください。
- 2 全ての接続が完了しましたら、モデム /TAの電源を投入してください。

接続図



(画面はXR-1100/CTでの接続例です)

第21章 アクセスサーバ機能

III. アクセスサーバ機能の設定

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

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

クライアントの IP アドレス

本装置にリモートアクセスしてきたホストに割り当てる IP アドレスを入力します。上記の「アクセスサーバの IP アドレス」で設定したものと同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

本装置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。多くの場合、コマンドの入力は必要ありません。

続けてユーザーアカウントの設定をおこないます。

ユーザーアカウントの設定

設定画面の下側でユーザーアカウントの設定をおこないます。

No.	アカウント	パスワード	アカウント毎に別IPを割り当てる場合		削除
			本装置のIP	クライアントのIP	
1	<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"/>

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

入力後、「設定の保存」をクリックしてください。設定が反映されます。

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

入力が終わりましたら「設定の保存」をクリックして設定完了です。

第21章 アクセスサーバ機能

III. アクセスサーバ機能の設定

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。

インタフェース：ppp6（固定）

ゲートウェイ：アクセスサーバ設定画面にて指定した着信時のクライアントのIPアドレス

設定例

前ページ「シリアル回線」設定画面のスタティックルート設定例です。

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

第 22 章

UPnP 機能

第22章 UPnP 機能

I. UPnP 機能 の設定

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

対応している Windows OSとアプリケーション

Windows OS

- ・ Windows XP
- ・ Windows Me

アプリケーション

- ・ Windows Messenger
- ・ MSN 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。
(2004年6月現在)

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

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

Windows OSのUPnPサービス

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

UPnP機能の設定

本装置のUPnP機能の設定は以下の手順でおこなってください。

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

WAN側インターフェース	<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)

WAN側インタフェース

WAN側に接続しているインタフェース名を指定します。

LAN側インタフェース

LAN側に接続してい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」をご参照下さい。

切断検知タイマー

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

切断タイマーを無効にするときは「0」を指定してください。

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。

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

第22章 UPnP 機能

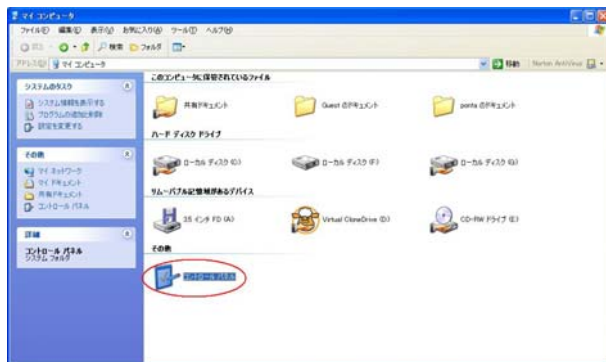
1. UPnP 機能 の設定

UPnP の接続状態の確認

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

1 「スタート」「マイコンピュータ」を開きます。

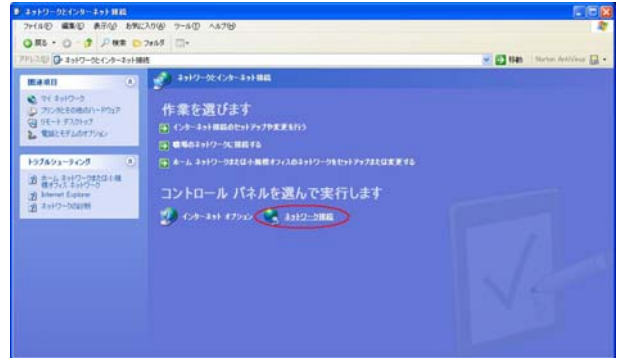
2 「コントロールパネル」を開きます。



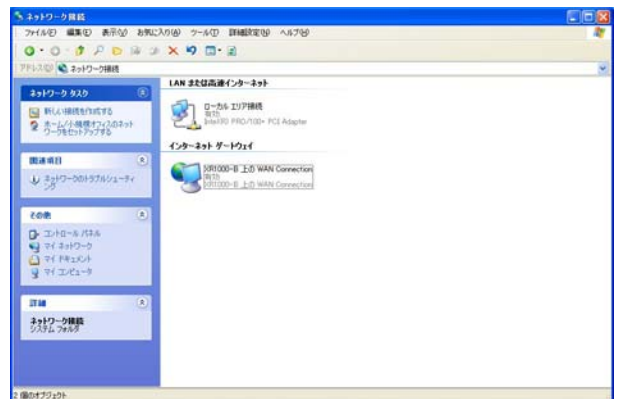
3 「ネットワークとインターネット接続」を開きます。



4 「ネットワーク接続」を開きます。



5 「ネットワーク接続」画面内に、「インターネットゲートウェイ」として「本装置-B上のCnnection 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22章 UPnP 機能

11. UPnP とパケットフィルタ設定

UPnP 機能使用時の注意

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

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

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

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

UPnP 機能使用時の推奨フィルタ設定

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

(入力フィルタ)

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
eth1	パケット受信時	破棄	udp				1900
ppp0	パケット受信時	破棄	udp				1900
eth1	パケット受信時	破棄	tcp				5000
ppp0	パケット受信時	破棄	tcp				5000
eth1	パケット受信時	破棄	tcp				2869
ppp0	パケット受信時	破棄	tcp				2869

(転送フィルタ)

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
eth1	パケット受信時	破棄	udp				1900
ppp0	パケット受信時	破棄	udp				1900
eth1	パケット受信時	破棄	tcp				5000
ppp0	パケット受信時	破棄	tcp				5000
eth1	パケット受信時	破棄	tcp				2869
ppp0	パケット受信時	破棄	tcp				2869

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

第 23 章

ダイナミックルーティング
(RIP と OSPF)

第23章 ダイナミックルーティング機能

1. ダイナミックルーティング機能

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

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

設定の開始

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。

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

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

II. RIPの設定

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

Ether0ポート	<input type="button" value="使用しない"/> <input type="button" value="バージョン1"/>
Ether1ポート	<input type="button" value="使用しない"/> <input type="button" value="バージョン1"/>
Ether2ポート	<input type="button" value="使用しない"/> <input type="button" value="バージョン1"/>
Ether3ポート	<input type="button" value="使用しない"/> <input type="button" value="バージョン1"/>
Administrative Distance 設定	<input type="text" value="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" value=""/> (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" value=""/> (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

(画面はXR-1100/CTでの表示例です)

Ether0、Ether1、Ether2、Ether3ポート
本装置の各Ethernetポートで、RIPの使用/不使用、また使用する場合のRIPバージョンを選択します。(Ether2,3ポートはXR-1100/CTのみ表示され、設定可能です。)

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。

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。

III. OSPF の設定

OSPFはリンクステート型経路制御プロトコルです。

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

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

これにより、トラフィックのロードバランシングが可能となっています。

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

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

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

インタフェースへの OSPF エリア設定

どのインタフェースで OSPF 機能を動作させるかを設定します。

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

	ネットワークアドレス (例:192.168.0.0/24)	AREA番号 (0-4294967295)
1	<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"/>

ネットワークアドレス

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

AREA 番号

そのネットワークのエリア番号を指定します。

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

入力後は「設定」をクリックして設定完了です。

III. OSPFの設定

OSPF エリア設定

各AREA(エリア)ごとの機能設定をおこないます。

設定画面上部の「OSPF エリア設定」をクリックします。

初めて設定するとき、もしくは設定を追加するときは「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"/> <input type="text"/>

AREA 番号
機能設定をおこなうエリアの番号を指定します。

スタブ設定

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

トータルスタブ設定

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

default-cost 設定

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

認証設定

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

エリア間ルートの経路集約設定

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

入力後は「設定」をクリックしてください。

設定後は「OSPF エリア設定」画面に、設定内容が一覧で表示されます。

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

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

第23章 ダイナミックルーティング機能

III. OSPF の設定

OSPF VirtualLink 設定

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

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

設定画面上部の「VirtualLink 設定」をクリックして設定します。

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

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
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"/> <input type="text"/>

Transit AREA 番号

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

Remote-ABR Router-ID 設定

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

Hello インターバル設定

Helloパケットの送出間隔を設定します。

Dead インターバル設定

Deadタイムを設定します。

Retransmit インターバル設定

LSAを送出する間隔を設定します。

transmit delay 設定

LSUを送出する際の遅延間隔(delay)を設定します。

認証パスワード設定

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

MD5 KEY-ID 設定(1)

MD5 認証使用時のKEY IDを設定します。

MD5 パスワード設定(1)

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。

MD5 KEY-ID 設定(2)

MD5 パスワード設定(2)

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

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

入力後は「設定」をクリックしてください。

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

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

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

III. OSPF の設定

OSPF 機能設定

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

Router-ID設定	<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 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)
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

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 ルート再配信

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

「有効」にした場合は以下の 2 項目も設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

RIPルートの再配信

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

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

Administrative Distance 設定

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

External ルート Distance 設定

OSPF 以外のプロトコルで学習した経路のディスタンス値を設定します。

Inter-area ルート Distance 設定

エリア間の経路のディスタンス値を設定します。

intra-area ルート Distance 設定

エリア内の経路のディスタンス値を設定します。

(次のページに続きます)

第23章 ダイナミックルーティング機能

III. OSPF の設定

Default-information

デフォルトルート 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う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に向けるように、OSPF で配信します。

「送信する」「常に送信する」の場合は、以下の2項目についても設定します。

a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

b. メトリック値

配信する際のメトリック値を設定します。

SPF 計算 Delay 設定

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

2つの SPF 計算の最小間隔設定

連続して SPF 計算をおこなう際の間隔を設定します。

バックアップ切替え監視対象 Remote Router-ID 設定

OSPF Hello によるバックアップ回線切り替え機能を使用する際に、Neighbor が切れたかどうかをチェックする対象のルータを判別するために、対象のルータの IP アドレスを設定します。

バックアップ機能を使用しない場合は、設定する必要はありません。

入力後は「設定」をクリックしてください。

III. OSPF の設定

インタフェース設定

各インタフェースごとの OSPF 設定を行ないます。

設定画面上部の「インタフェース設定」をクリックして設定します。

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

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"/> (1-1000000kbps)
Hello-インターバル設定	10 (1-65535s)
Dead-インターバル設定	40 (1-65535s)
Retransmit-インターバル設定	5 (3-65535s)
Transmit Delay設定	1 (1-65535s)
認証キー設定	<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

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

Hello インターバル設定

Hello パケットを送出する間隔を設定します。

Dead インターバル設定

Dead タイムを設定します。

Retransmit インターバル設定

LSA の送出国隔を設定します。

Transmit Delay 設定

LSU を送出国際の遅延間隔を設定します。

認証パスワード設定

simple パスワード認証を使用する際のパスワードを設定します。

MD5 KEY-ID 設定(1)

MD5 認証使用時の KEY ID を設定します。

MD5 パスワード設定(1)

VirtualLink 上で MD5 認証を使用する際の MD5 パスワードを設定します。

MD5 KEY-ID 設定(2)

MD5 パスワード設定(2)

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

Priority 設定

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

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

MTU-Ignore 設定

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

第23章 ダイナミックルーティング機能

III. OSPF の設定

入力後は「設定」をクリックしてください。

設定後は「インタフェース設定」画面に、設定内容が一覧で表示されます。

インタフェース名	Passive	Cost	帯域	Hello	Dead	Retransmit	Transmit Delay	DRB Password	MD5 KEY-ID	MD5 Password	Priority	MTU ignore	Configure
eth0	off	1	1	10	40	5	1	aaa	1	bbb	1	off	Edit Password

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

ステータス表示

OSPFの各種ステータスを表示します。

設定画面上部の「ステータス表示」をクリックして設定します。

OSPFデータベースの表示 (各Link state情報が表示されます)	表示する	
ネイバースト情報の表示 (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	
インタフェース情報の表示 (表示したいインタフェースを指定して下さい)	表示する	<input type="text"/>

OSPF データベース表示

LinkState情報が表示されます。

ネイバースト情報の表示

現在のネイバー状態が表示されます。

OSPF ルーティングテーブル情報の表示

OSPFルーティング情報が表示されます。

OSPF 統計情報の表示

SPFの計算回数やRouter IDなどが表示されます。

インタフェース情報の表示

現在のインタフェースの状態が表示されます。

第24章

スタティックルート設定

第24章 スタティックルート設定

スタティックルート設定方法

Web 設定画面「スタティックルート設定」をクリックして、以下の画面から設定します。

No.	ホスト/ネットワーク	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	ネットワーク					<input type="checkbox"/>
2	ネットワーク					<input type="checkbox"/>
3	ネットワーク					<input type="checkbox"/>
4	ネットワーク					<input type="checkbox"/>
5	ネットワーク					<input type="checkbox"/>
6	ネットワーク					<input type="checkbox"/>
7	ネットワーク					<input type="checkbox"/>
8	ネットワーク					<input type="checkbox"/>
9	ネットワーク					<input type="checkbox"/>
10	ネットワーク					<input type="checkbox"/>
11	ネットワーク					<input type="checkbox"/>
12	ネットワーク					<input type="checkbox"/>
13	ネットワーク					<input type="checkbox"/>
14	ネットワーク					<input type="checkbox"/>
15	ネットワーク					<input type="checkbox"/>
16	ネットワーク					<input type="checkbox"/>
<small>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。</small>						
	ネットワーク					<input type="checkbox"/>

入力方法

ホスト / ネットワーク
ルーティング先が、単一ホストかネットワークかを選択します。

アドレス
あて先ホストのアドレス、またはネットワークアドレスを入力します。

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

入力例 : **255.255.255.248** (29ビットマスク)

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

インターフェース / ゲートウェイ
ルーティングをおこなうインターフェース名、もしくは上位ルータの IP アドレスのどちらかを設定します。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。

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

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

設定を挿入する

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

<small>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。</small>						
	ネットワーク					<input type="checkbox"/>

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方法

設定を削除する

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

デフォルトルートを設定する

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

ルーティング情報を確認する

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

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

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

第 25 章

ソースルート機能

ソースルート設定

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

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

ソースルート設定は、設定画面「ソースルート設定」でおこないます。

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

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

IP

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

DEVICE

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

設定後は「設定の保存」をクリックします。

2 画面右上の「ソースルートのルール設定へ」をクリックします。

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

送信元ネットワークアドレス

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

ネットワークアドレス / マスクビット値

の形式で設定してください。

送信先ネットワークアドレス

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

ネットワークアドレス / マスクビット値

の形式で設定してください。

ソースルートのテーブル No.

使用するソースルートテーブルの番号(1 ~ 8)を設定します。

最後に「設定の保存」をクリックして設定完了です。

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

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

第 26 章

NAT 機能

1. 本装置のNAT機能について

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

本装置は以下の3つのNAT機能をサポートしています。

IPマスカレード機能

複数のプライベートアドレスを、ある1つのグローバルアドレスに変換する機能です。グローバルアドレスは本装置のインターネット側ポートに設定されたものを使います。またLANのプライベートアドレス全てが変換されることとなります。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、「インタフェース設定」もしくは「PPP/PPPoE接続」の接続設定画面で設定します。

送信元NAT機能

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

バーチャルサーバ機能

インターネット上からLAN上のサーバ等にアクセスさせることができる機能です。通常はインターネット側からLANへアクセスする事はできませんが、送信先グローバルアドレスをプライベートアドレスへ変換する設定をおこなうことで、見かけ上はインターネット上のサーバへアクセスできているかのようにすることができます。設定上ではプライベートアドレスとグローバルアドレスを1対1で関連づけます。また同時に、プロトコルとTCP/UDPポート番号も指定しておきます。ここで指定したプロトコル・TCP/UDPポート番号でアクセスされた時にグローバルアドレスからプライベートアドレスへ変換され、LAN上のサーバに転送されます。

これらのNAT機能は同時に設定・運用が可能です。

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

II. バーチャルサーバ設定

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

設定方法

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

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	削除
1	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<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。

<input type="text"/>	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
----------------------	----------------------	----------------------	-------------------------------------	----------------------	----------------------	--------------------------

サーバのアドレス

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

公開するグローバルアドレス

サーバのプライベート IP アドレスに対応させるグローバル IP アドレスを入力します。インターネットからはここで入力したグローバル IP アドレスでアクセスします。

プロバイダから割り当てられている IP アドレスが一つだけの場合は、ここは空欄にします。

プロトコル

サーバのプロトコルを選択します。

ポート

サーバが公開するポート番号を入力します。範囲で指定することも可能です。範囲で指定するときは、ポート番号を “:” で結びます。

<例> ポート 20 番から 21 番を指定する 20:21

インターフェース

インターネットからのアクセスを受信するインターフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名一覧」をご参照下さい。

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下さい。

設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

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。

<input type="text"/>	<input type="text"/>	<input type="text"/>	全て <input type="button" value="v"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
----------------------	----------------------	----------------------	-------------------------------------	----------------------	----------------------	--------------------------

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

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

設定を削除する

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

III. 送信元 NAT 設定

設定方法

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

No.	送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース	削除
1	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16	<input type="text"/>	<input type="text"/>	<input type="text"/>	<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。				
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

送信元のプライベートアドレス

NATの対象となるLAN側コンピュータのプライベートIPアドレスを入力します。ネットワーク単位での指定も可能です。

変換後のグローバルアドレス

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

インターフェース

どのインターフェースからインターネット(WAN)へアクセスするか、インターフェース名を指定します。インターネット(WAN)につながっているインターフェースを設定してください。本装置のインターフェース名については、本マニュアルの「付録A インタフェース名一覧」をご参照下さい。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

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

設定を挿入する

送信元 NAT 設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

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。				
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

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

設定を削除する

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

IV. バーチャルサーバの設定例

WWW サーバを公開する際の NAT 設定例

NAT の条件

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

LAN 構成

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

設定画面での入力方法

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

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.1	211.xxx.xxx.102	tcp	80	eth1

設定の解説

No.1 :

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

FTP サーバを公開する際の NAT 設定例

NAT の条件

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

LAN 構成

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

設定画面での入力方法

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

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース
192.168.0.2	211.xxx.xxx.103	tcp	20	ppp0
192.168.0.2	211.xxx.xxx.103	tcp	21	ppp0

設定の解説

No.1 :

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

No.2 :

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

IV. バーチャルサーバの設定例

PPTP サーバを公開する際の NAT 設定例

NAT の条件

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

LAN 構成

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

設定画面での入力方法

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

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	削除
192.168.0.3	<input type="text"/>	tcp	1723	ppp0	<input type="checkbox"/>
192.168.0.3	<input type="text"/>	gre	<input type="text"/>	ppp0	<input type="checkbox"/>

IV. バーチャルサーバの設定例

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

NATの条件

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

LAN構成

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

設定画面での入力方法

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

インタフェース	仮想V/F番号	IPアドレス	ネットマスク
eth1	1	211.xxx.xxx.104	255.255.255.248
eth1	2	211.xxx.xxx.105	255.255.255.248
eth1	3	211.xxx.xxx.106	255.255.255.248
eth1	4	211.xxx.xxx.107	255.255.255.248

2 IPマスカレードを有効にします。

(第5章「インタフェース設定」参照)

3 「バーチャルサーバ設定」で以下の様に設定してください。

サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インタフェース
192.168.0.1	211.xxx.xxx.104	tcp	80	eth1
192.168.0.2	211.xxx.xxx.105	tcp	25	eth1
192.168.0.2	211.xxx.xxx.105	tcp	110	eth1
192.168.0.3	211.xxx.xxx.106	tcp	20	eth1
192.168.0.3	211.xxx.xxx.106	tcp	21	eth1
192.168.0.4	211.xxx.xxx.107	tcp	53	eth1
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。

複数のグローバルアドレスを使ってバーチャルサーバ設定をおこなうときは、必ず「仮想インタフェース機能」において使用するグローバルアドレスを設定しておく必要があります。

V. 送信元 NAT の設定例

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

送信元のプライベートアドレス	変換後のグローバルアドレス	インターフェース
192.168.0.1	61.xxx.xxx.101	ppp0
192.168.0.2	61.xxx.xxx.102	ppp0
192.168.10.0/24	61.xxx.xxx.103	ppp0

例えば上記のような送信元 NAT 設定をおこなうと、

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

< 設定例 > **192.168.254.0/24**

複数のグローバルアドレスを使って送信元 NAT 設定をおこなうときは、必ず「仮想インターフェース機能」で設定しておく必要がありますので、ご注意下さい。

補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

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

第 27 章

パケットフィルタリング機能

第 27 章 パケットフィルタリング機能

1. 機能の概要

本装置はパケットフィルタリング機能を搭載しています。パケットフィルタリング機能を使うと、以下のようなことができます。

- ・外部から LAN に入ってくるパケットを制限する。
- ・LAN から外部に出ていくパケットを制限する。
- ・本装置自身が受信するパケットを制限する。
- ・本装置自身から送信するパケットを制限する。
- ・ゲートウェイ認証機能を使用しているときにアクセス可能にする

またフィルタリングは以下の情報に基づいて条件を設定することができます。

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

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

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

Xconnect Interface に指定されたインタフェースは、フィルタ設定を適用することができません。L2TP セッション間でのフィルタリングを設定するには、第 14 章「L2TPv3 フィルタ機能」を参考にしてください。

II. 本装置のフィルタリング機能について

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

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

転送(forward)フィルタ

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

入力(input)フィルタ

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

出力(output)フィルタ

本装置内部からインターネットや LAN などへのアクセスを制御したい場合には、この出力ルールにフィルタ設定をおこないます。

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

ゲートウェイ認証フィルタ

「ゲートウェイ認証機能」を使用しているときに設定するフィルタです。ゲートウェイ認証を必要とせずに外部と通信可能にするフィルタ設定をおこないます。ゲートウェイ認証機能については第 32 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下さい。

第27章 パケットフィルタリング機能

III. パケットフィルタリングの設定

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

設定方法

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

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	ICMP type/code	LOG	状態	No.
1	eth0	パケット受信時	破棄	tcp				137-139			<input type="checkbox"/>	1
2	eth0	パケット受信時	破棄	udp				137-139			<input type="checkbox"/>	2
3	eth0	パケット受信時	破棄	tcp		137					<input type="checkbox"/>	3
4	eth0	パケット受信時	破棄	udp		137					<input type="checkbox"/>	4
5	eth1	パケット受信時	破棄	udp				1900			<input type="checkbox"/>	5
6	ppp0	パケット受信時	破棄	udp				1900			<input type="checkbox"/>	6
7	eth1	パケット受信時	破棄	tcp				5000			<input type="checkbox"/>	7
8	ppp0	パケット受信時	破棄	tcp				5000			<input type="checkbox"/>	8
9	eth1	パケット受信時	破棄	tcp				2869			<input type="checkbox"/>	9
10	ppp0	パケット受信時	破棄	tcp				2869			<input type="checkbox"/>	10
11		パケット受信時	許可	全て							<input type="checkbox"/>	11
12		パケット受信時	許可	全て							<input type="checkbox"/>	12
13		パケット受信時	許可	全て							<input type="checkbox"/>	13
14		パケット受信時	許可	全て							<input type="checkbox"/>	14
15		パケット受信時	許可	全て							<input type="checkbox"/>	15
16		パケット受信時	許可	全て							<input type="checkbox"/>	16

(画面は「転送フィルタ」です)

インタフェース

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

方向

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

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

動作

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

プロトコル

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

送信元アドレス

フィルタリング対象とする、送信元の IP アドレスを入力します。

ホストアドレスのほか、ネットワークアドレス、FQDN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)

宛て先アドレス

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、FQDNでの指定が可能です。

入力方法は、送信元 IP アドレスと同様です。

宛て先ポート

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。

第27章 パケットフィルタリング機能

III. パケットフィルタリングの設定

ICMP type/code

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

プロトコルで「icmp」以外を選択した場合は指定できません。

LOG

チェックを入れると、そのフィルタ設定に合致したパケットがあったとき、そのパケットの情報をsyslogに出力します。

許可 / 破棄いずれの場合も出力します。

更新ボタン

IPアドレスをFQDNで指定したフィルタの名前解決を手動で行います。

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

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。

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

送信元アドレス、または、あて先アドレスとしてFQDN形式を指定する場合、各フィルタ設定（入力、転送、出力、ゲートウェイ認証）を含めた指定数の合計は64個まで可能とします。

（1行の設定で送信元アドレスとあて先アドレスの両方をFQDN指定した場合の指定数は2です。）

設定情報の確認

「情報表示」をクリックすると、現在のフィルタ設定の情報が一覧表示されます。

入力フィルタ 情報表示

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

更新

IPアドレス指定をFQDNで行った場合は、「type」欄の「FQDN」リンクをクリックするとクリックしたフィルタ設定の名前解決したIPアドレス一覧が表示されます。

FQDN情報表示

入力フィルタ No.11

source	www.yahoo.co.jp
destination	0.0.0.0/0

No.	pkts	bytes	target	source	destination
1	0	0	ACCEPT	203.216.231.160	0.0.0.0/0
2	0	0	ACCEPT	203.216.235.201	0.0.0.0/0
3	0	0	ACCEPT	203.216.243.218	0.0.0.0/0
4	0	0	ACCEPT	203.216.247.225	0.0.0.0/0
5	0	0	ACCEPT	203.216.247.249	0.0.0.0/0
6	0	0	ACCEPT	124.83.139.191	0.0.0.0/0
7	0	0	ACCEPT	124.83.147.202	0.0.0.0/0
8	0	0	ACCEPT	124.83.147.203	0.0.0.0/0
9	0	0	ACCEPT	124.83.147.204	0.0.0.0/0
10	0	0	ACCEPT	124.83.147.205	0.0.0.0/0

更新

第27章 パケットフィルタリング機能

III. パケットフィルタリングの設定

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ことができます。
挿入は、設定テーブルの一番下にある行からおこないます。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

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

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 27 章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

インターネットから LAN へのアクセスを破棄する設定

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
eth1	パケット受信時	許可	tcp				1024-65535
eth1	パケット受信時	許可	udp				1024-65535
eth1	パケット受信時	破棄	全て				

「入力フィルタ」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
eth1	パケット受信時	許可	tcp				1024-65535
eth1	パケット受信時	許可	udp				1024-65535
eth1	パケット受信時	破棄	全て				

フィルタの解説

「転送フィルタ」「入力フィルタ」

No.1 :

WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.2 :

上記の条件に合致しないパケットを全て破棄する。

第27章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

WWWサーバを公開する際のフィルタ設定例

フィルタの条件

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

LAN構成

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

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
eth1	パケット受信時	許可	tcp			192.168.0.1	80
eth1	パケット受信時	許可	tcp				1024-65535
eth1	パケット受信時	許可	udp				1024-65535
eth1	パケット受信時	破棄	全て				

フィルタの解説

No.1 :

192.168.0.1のサーバにHTTPのパケットを通す。

No.2 :

WANから来る、宛て先ポートが1024から65535のパケットを通す。

No.3 :

上記の条件に合致しないパケットを全て破棄する。

FTPサーバを公開する際のフィルタ設定例

フィルタの条件

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

LAN構成

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

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	許可	tcp			192.168.0.2	21
ppp0	パケット受信時	許可	tcp			192.168.0.2	20
ppp0	パケット受信時	許可	tcp				1024-65535
ppp0	パケット受信時	許可	udp				1024-65535
ppp0	パケット受信時	破棄	全て				

フィルタの解説

No.1 :

192.168.0.2のサーバにftpのパケットを通す。

No.2 :

192.168.0.2のサーバにftpdataのパケットを通す。

No.3、4 :

WANから来る、宛て先ポートが1024から65535のパケットを通す。

No.5 :

上記の条件に合致しないパケットを全て破棄する。

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

第27章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

WWW、FTP、メール、DNS サーバを公開する際の フィルタ設定例

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「転送フィルタ」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	許可	tcp			192.168.0.1	80
ppp0	パケット受信時	許可	tcp			192.168.0.2	25
ppp0	パケット受信時	許可	tcp			192.168.0.2	110
ppp0	パケット受信時	許可	tcp			192.168.0.3	21
ppp0	パケット受信時	許可	tcp			192.168.0.3	20
ppp0	パケット受信時	許可	tcp			192.168.0.4	53
ppp0	パケット受信時	許可	udp			192.168.0.4	53
ppp0	パケット受信時	許可	tcp				1024-65535
ppp0	パケット受信時	許可	udp				1024-65535
ppp0	パケット受信時	破棄	全て				

フィルタの解説

No.1 :

192.168.0.1 のサーバに HTTP のパケットを通す。

No.2,3 :

192.168.0.2 のサーバに SMTP と POP3 のパケットを通す。

No.4,5 :

192.168.0.3 のサーバに ftp と ftpdata のパケットを通す。

No.6,7 :

192.168.0.4 のサーバに、domain のパケット (tcp,udp)を通す。

No.8、9 :

WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.10 :

上記の条件に合致しないパケットを全て破棄する。

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

第 27 章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

NetBIOS パケットが外部へ出るのを防止する フィルタ設定

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「入力フィルタ」

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

「転送フィルタ」

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

フィルタの解説

No.1 :

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

No.2 :

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

No.3 :

送信先ポートが tcp の 137 のパケットを Ether0 ポートで破棄する。

No.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。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
ppp0	パケット受信時	破棄	全て			210.xxx.xxx.32/32	
ppp0	パケット受信時	破棄	全て			210.xxx.xxx.47/32	

フィルタの解説

No.1 :

210.xxx.xxx.32/32 (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27章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

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

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
ppp0	パケット受信時	破棄	全て	192.168.0.0/16			

フィルタの解説

No.1,2,3 :

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

外部からの攻撃を防止する総合的なフィルタリング設定

フィルタの条件

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

LAN 構成

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

設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	破棄	全て	10.0.0.0/8			
ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
ppp0	パケット受信時	破棄	全て	192.168.0.0/16			
ppp0	パケット受信時	破棄	全て			202.xxx.xxx.127/3	

「出力フィルタ設定」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット送信時	破棄	全て			10.0.0.0/8	
ppp0	パケット送信時	破棄	全て			172.16.0.0/16	
ppp0	パケット送信時	破棄	全て			192.168.0.0/16	

フィルタの解説

入力フィルタの No.1,2,3 :

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

入力フィルタの No.4,5 :

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

出力フィルタの No.1,2,3 :

- 送信元 IP アドレスが不正なパケットを送出ししない。
- WAN 上にプライベートネットワークアドレスは存在しない。

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

第27章 パケットフィルタリング機能

IV. パケットフィルタリングの設定例

PPTPを通すためのフィルタ設定

フィルタの条件

- ・WAN側からのPPTPアクセスを許可する。

LAN構成

- ・WAN側はPPPoE回線に接続する。

設定画面での入力方法

「転送フィルタ設定」で以下のように設定します。

インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	宛て先アドレス	宛て先ポート
ppp0	パケット受信時	許可	gre				
ppp0	パケット受信時	許可	tcp				1723

フィルタの解説

PPTPでは以下のプロトコル・ポートを使って通信します。

- ・プロトコル「GRE」
- ・プロトコル「tcp」のポート「1723」

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

第 27 章 パケットフィルタリング機能

V. 外部から設定画面にアクセスさせる設定

以下は、PPPoE で接続した場合の設定方法です。

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

2 「入力フィルタ」設定の中で、以下のような設定を追加してください。

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

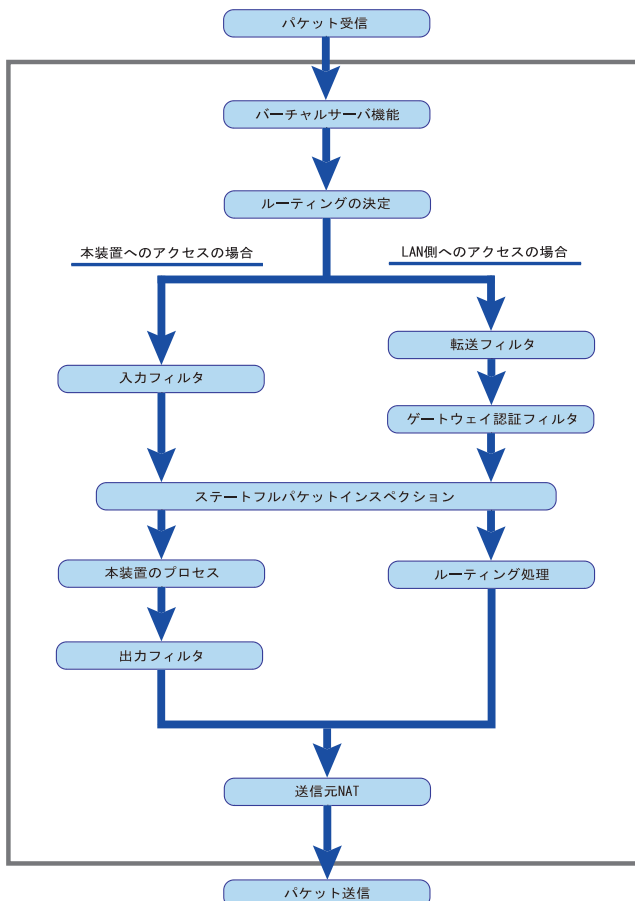
(セキュリティ上、大変危険ですので、この設定は推奨いたしません)。

第27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

本装置における、NATとフィルタリングの処理方法は以下のようになっています。

(図の上部をWAN側、下部をLAN側とします。またLAN → WANへNATをおこなうとします。)



- WAN側からパケットを受信したとき、最初に「バーチャルサーバ設定」が参照されます。
- 「バーチャルサーバ設定」で静的NAT変換したあとに、パケットがルーティングされます。
- 本装置自身へのアクセスをフィルタするときは「入力フィルタ」、本装置自身からのアクセスをフィルタするときは「出力フィルタ」で設定します。
- WAN側からLAN側へのアクセスをフィルタするときは「転送フィルタ」で設定します。その場合のあとに先アドレスは「(LAN側の)プライベートアドレス」になります(NATの後の処理となるため)。
- ステートフルパケットインスペクションだけを有効にしている場合、WANからLAN、また本装置自身へのアクセスはすべて破棄されます。
- ステートフルパケットインスペクションと同時に「転送フィルタ」「入力フィルタ」を設定している場合は、先に「転送フィルタ」「入力フィルタ」にある設定が優先して処理されます。
- 「送信元NAT設定」は、一番最後に参照されます。
- LAN側からWAN側へのアクセスの場合も、処理の順序は同様です(最初にバーチャルサーバ設定が参照される)。

第27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 27 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。出力内容は以下ようになります。

<入力パケットを破棄したときのログ出力例>

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

Jan 25 14:14:07	syslog がログを取得した日時です。
XR-Filter:	フィルタのログであることを表します。
FILTER_INPUT_1	入力フィルタの 1 番目のフィルタで取得されたものです。 FILTER_FORWARD は転送フィルタを意味します。
IN=	パケットを受信したインタ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 28 章

ネットワークイベント機能

第28章 ネットワークイベント機能

1. 機能の概要

ネットワークイベントは、回線障害などのネットワーク状態の変化を検知し、それをトリガとして特定のイベントを実行する機能です。

本装置では、以下のネットワーク状態の変化をトリガとして検知することができます。

- ・ping 監視の状態
- ・link 監視の状態
- ・vrrp 監視の状態

ping 監視

本装置から任意の宛先へpingを送信し、その応答の有無を監視します。一定時間応答がなかった時にトリガとして検知します。また、再び応答を受信した時は、復旧トリガとして検知します。

link 監視

Ethernet インタフェースやpppインタフェースのリンク状態を監視します。監視するインタフェースのリンクがダウンした時にトリガとして検知します。また再びリンクがアップした時は復旧トリガとして検知します。

vrrp 監視

本装置のVRRP ルータ状態を監視します。指定したルータ ID のVRRP ルータがバックアップルータへ切り替わった時にトリガとして検知します。また、再びマスタールータへ切り替わった時は復旧トリガとして検知します。

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

- ・VRRP 優先度変更
- ・IPsec 接続切断

VRRP 優先度変更

トリガ検知時に、指定したVRRP ルータの優先度を変更します。またトリガ復旧時には、元のVRRP 優先度に変更します。

例えば、ping 監視と連動して、PPPoE 接続先がダウンした時に、自身はVRRP バックアップルータに移行し、新マスタールータ側の接続へ切り替える、といった使い方ができます。

IPsec 接続 / 切断

トリガ検知時に、指定したIPsec ポリシーを切断します。またトリガ復旧時には、IPsec ポリシーを再び接続します。

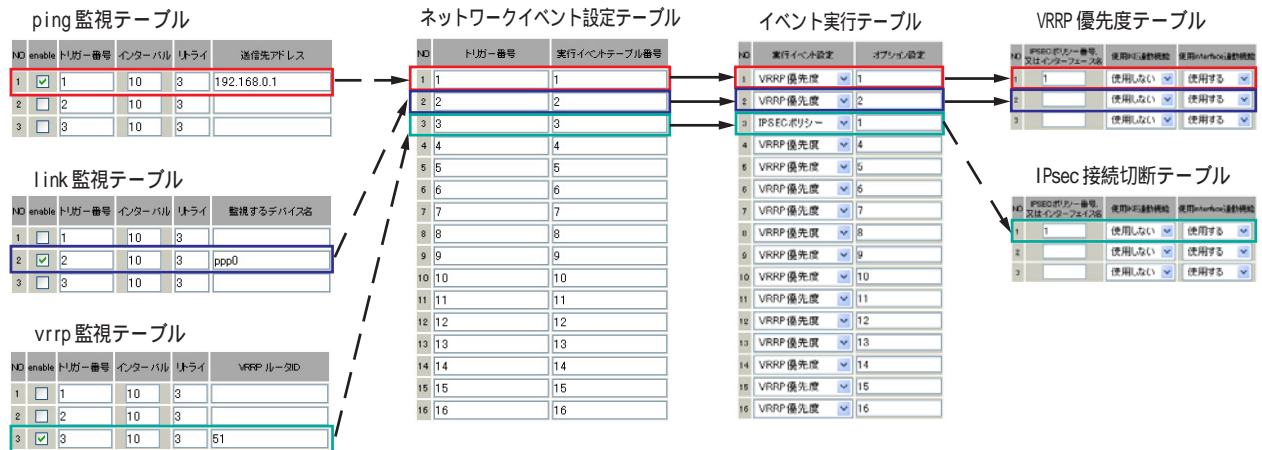
例えば、vrrp 監視と連動して、2台のVRRP ルータのマスタールータの切り替わりに応じて、IPsec 接続を繋ぎかえる、といった使い方ができます。

第28章 ネットワークイベント機能

1. 機能の概要

本機能で使用する各種テーブルについて

本機能は複数のテーブル定義を連携させることによって実現しています。



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。

II. 各トリガテーブルの設定

ping 監視の設定方法

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

ネットワークping設定

NO	enable	トリガー番号	インターバル	リトライ	送信先アドレス
1	<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	

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。

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	

enable

チェックを入れることで設定を有効にします。

トリガー番号

監視するインタフェースのリンクがダウンした場合に検知するトリガーの番号(1 ~ 16)を指定します。本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

インターバル(秒)

リトライ

インタフェースのリンク状態を監視する間隔を設定します。

「『インターバル』秒間に、『リトライ』回、インタフェースのリンク状態をチェックする」という設定になります。この間、監視したリンク状態が全てダウンだった場合にトリガとして検知されます。

監視するデバイス名

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

最後に「設定の保存」をクリックして設定完了です。

II. 各トリガテーブルの設定

vrmp 監視の設定方法

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

vrmp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	

enable

チェックを入れることで設定を有効にします。

トリガー番号

監視する VRRP ルータがバックアップへ切り替わった場合に検知するトリガーの番号(1 ~ 16)を指定します。本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

インターバル(秒)

リトライ

VRRP ルータの状態を監視する間隔を設定します。

「『インターバル』秒間に、『リトライ』回、VRRP のルータ状態を監視する」という設定になります。

この間、監視した状態が全てバックアップ状態であった場合にトリガとして検知されます。

VRRP ルータ ID

VRRP ルータ状態を監視するルータ ID を指定します。

最後に「設定の保存」をクリックして設定完了です。

各監視機能を有効にするにはネットワークイベントサービス設定画面で、「起動」ボタンにチェックを入れ、「動作変更」をクリックしてサービスを起動して下さい。

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

(注) 各監視設定で指定したトリガー番号は、「ネットワークイベント設定」テーブルでのインデックス番号となるため、それぞれの監視設定の間で同じトリガー番号が有効にならないように設定してください。

第28章 ネットワークイベント機能

III. 実行イベントテーブルの設定

ネットワークイベント設定テーブルの設定

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

NO	トリガー番号	実行イベントテーブル番号
1		1
2		2
3		3
4		4
5		5
6		6
7		7
8		8
9		9
10		10
11		11
12		12
13		13
14		14
15		15
16		16

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。

NO	実行イベント設定	オプション設定
1	IPsecポリシー	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

実行イベント設定

実行されるイベントの種類を選択します。

「IPsecポリシー」は、IPsecポリシーの切断を行います。

「VRRP優先度」は、VRRPルータの優先度を変更します。

オプション設定

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

最後に「設定の保存」をクリックして設定完了です。

第 28 章 ネットワークイベント機能

IV. 実行イベントのオプション設定

VRRP 優先度変更設定テーブルの設定

設定画面上部の「VRRP 優先度」をクリックして、以下の画面から設定します。

VRRP 優先度変更設定 現在のVRRPの状態		
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

ルータ ID

トリガ検知時に VRRP 優先度を変更する VRRP ルータ ID を指定します。

優先度

トリガ検知時に変更する VRRP 優先度を指定します。1 ~ 255 の間で設定して下さい。
なお、トリガ復旧時には「VRRP サービス」で設定されている元の値に戻ります。

最後に「設定の保存」をクリックして設定完了です。

IPSEC 接続切断設定 テーブルの設定

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

IPSEC 接続切断設定 現在のIPSECの状態			
NO	IPSECポリシー番号、 又はインタフェース名	使用IKE連動機能	使用Interface連動機能
1		使用しない	使用する
2		使用しない	使用する
3		使用しない	使用する
4		使用しない	使用する
5		使用しない	使用する
6		使用しない	使用する
7		使用しない	使用する
8		使用しない	使用する
9		使用しない	使用する
10		使用しない	使用する
11		使用しない	使用する
12		使用しない	使用する
13		使用しない	使用する
14		使用しない	使用する
15		使用しない	使用する
16		使用しない	使用する

IPSEC ポリシー番号、又はインタフェース名
トリガ検知時に切断する IPsec ポリシーの番号、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。

V. ステータスの表示

ステータスの表示

設定画面上部の「ステータス」をクリックして表示します。



トリガー情報

設定が有効なトリガー番号とその状態を表示します。

“ON”と表示されている場合は、トリガを検知していない、またはトリガが復旧している状態を表します。

“OFF”と表示されている場合は、トリガ検知している状態を表します。

イベント情報

・No.

イベント番号とその状態を表します。

“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 29 章

仮想インタフェース機能

第 29 章 仮想インターフェース機能

仮想インターフェース機能の設定

主にバーチャルサーバ機能を利用する場合に、仮想インターフェースを設定します。

設定方法

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

No.	インターフェース	仮想I/F番号	IPアドレス	ネットマスク	削除
1	<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"/>

インターフェース

仮想インターフェースを作成するインターフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録A インターフェース名一覧」をご参照ください。

仮想 I/F 番号

作成するインターフェースの番号を指定します。
0 ~ 1023 の間で設定します。

IP アドレス

作成するインターフェースの IP アドレスを指定します。

ネットマスク

作成するインターフェースのネットマスクを指定します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

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

設定を削除する

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

第 30 章

GRE 設定

GRE の設定

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

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

設定は設定画面左「GRE設定」でおこないます。

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

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。

例) 192.168.90.1/30

リモート(宛先)アドレス

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

ローカル(送信元)アドレス

本装置のWAN側IPアドレスを設定します。

PEERアドレス

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

例) 192.168.90.2/30

TTL

GREパケットのTTL値を設定します。

MTU

MTU値を設定します。最大値は1500byteです。

Path MTU Discovery

Path MTU Discovery機能を有効にするかを選択します。

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

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

ToS

GREパケットのToS値を設定します。

GREoverIPsec

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

Routing Tableに合わせて暗号化したい場合には「Routing Tableに依存」を選択します。

ルートがIPsecの時は暗号化、IPsecでない時は暗号化しません。

GRE の設定

GRE トンネルを暗号化するときの IPsec 設定は次のように設定してください。

- ・本装置側設定 **通常通り**
- ・IKE/ISAKMP ポリシー設定 **通常通り**
- ・IPsec ポリシー設定

本装置側の LAN 側のネットワークアドレス：

GRE 設定のローカルアドレス /32

相手側の LAN 側のネットワークアドレス：

GRE 設定のリモートアドレス /32

ID キーの設定

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 トンネルが生成されません。

「削除」をクリックすると、その設定に該当する GRE トンネルが無効化されます(設定自体は保存されています)。再度有効とするときは「追加 / 変更」ボタンをクリックしてください。

「現在の状態」では GRE の動作状況が表示されます。

現在の状態

Tunnel is down, Link is down

GRE 設定を行うと、設定内容が一覧表示されます。

Interface名	Interface Address	Remote Address	Local Address	Peer Address	MTU	ID Key	Check sum	PMTUD	Link State
gre1	192.168.90.1/30	192.168.1.253	192.168.1.254	192.168.90.2/30	1476		無効	有効	up

設定の編集は「Interface 名」をクリックして下さい。また GRE トンネルのリンク状態は「Link State」に表示されます。「UP」は GRE トンネルがリンクアップしている状態です。

第 31 章

QoS 設定

1. QoS について

本装置の優先制御・帯域制御機能(以下、QoS 機能)は以下の5つのキューイング方式で、トラフィック制御をおこないます。

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

クラスフル/クラスレスなキューイング

キューイングには、クラスフルなものと同様にクラスレスなものがあります。

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

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

1. QoSについて

1. PFIFO

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

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

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

キューとは、データの入り口と出口を一つだけ持つバッファのことを指します。

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

2. TBF

帯域制御方法の1つです。

トークンバケツにトークンを、ある一定の速度(トークン速度)で収納していきます。このトークン1個ずつがパケットを1個ずつかみ、トークン速度を超えない範囲でパケットを送信していきます(送信後はトークンは削除されます)。

またバケツに溜まっている余分なトークンは、突発的なバースト状態(パケットが大量に届く状態)でパケットが到着しているときに使われます。バーストが起きているときはすでにバケツに溜まっている分のトークンを使ってパケットを送信しますので、溜まった分のトークンを使い切らないような短期的なバーストであれば、トークン速度(制限Rate)を超えたパケット送信が可能です。

バースト状態が続くとバケツのトークンがすぐになくなってしま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。

1. QoS について

3. SFQ

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

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

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

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

4. PQ

PQは優先制御の1つです。トラフィックのシェーピングは起こりません。

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

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

1. QoSについて

5. CBQ

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

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

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

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

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

<クラス構成図(例)>

root クラス (1Mbps)

 クラス 1 (500kbps、優先度 2)

 HTTP (優先度 1)

 FTP (優先度 5)

 クラス 2 (500kbps、優先度 1)

 HTTP (優先度 1)

 FTP (優先度 5)

子クラスからはFIFOでパケットが送信されますが、子クラスの下にキューイングを定義し、クラス内でのキューイングをおこなうこともできます(クラスキューイング)。

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

II. QoS 機能の各設定画面について

Interface Queuing 設定画面

本装置の各インタフェースでおこなうキューイング方式を定義します。すべてのキューイング方式で設定が必要です。

CLASS 設定

CBQをおこなう場合の、各クラスについて設定します。

CLASS Queuing 設定

各クラスにおけるキューイング方式を定義します。CBQ以外のキューイング方式について定義できません。

CLASS 分けフィルタ設定

パケットを各クラスに振り分けるためのフィルタ設定を定義します。PQ、CBQをおこなう場合に設定が必要です。

パケット分類設定

各パケットにTOS値やMARK値を付加するための設定です。PQをおこなう場合に設定します。PQではIPヘッダによるCLASS分けフィルタリングができないため、TOS値またはMARK値によってフィルタリングをおこないます。

III. 各キューイング方式の設定手順について

各キューイング方式の基本的な設定手順は以下の通りです。

pfifoの設定手順

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

TBFの設定手順

「Interface Queueing 設定」で、トークンのレート、バケツサイズ、キューのサイズを設定します。

SFQの設定手順

「Interface Queueing 設定」で設定します。

PQの設定手順

1. インタフェースの設定

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

2. CLASS 分けのためのフィルタ設定

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

3. パケット分類のための設定

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

CBQの設定手順

1. ルートクラスの設定

「Interface Queueing 設定」で、ルートクラスの設定をおこないます。

2. 各クラスの設定

・「CLASS 設定」で、全てのクラスの親となる親クラスについて設定します。

・「CLASS 設定」で、親クラスの下に置く子クラスについて設定します。

・「CLASS 設定」で、子クラスの下に置くリーフクラスを設定します。

3. クラス分けの設定

「CLASS 分けフィルタ設定」で、CLASS 分けのマッチ条件を設定します。

4. クラスキューイングの設定

クラス内でさらにキューイングをおこなうときには「CLASS Queueing 設定」でキューイング設定をおこないます。

IV. 各設定画面での設定方法について

Interface Queueing 設定

すべてのキューイング方式において設定が必要です。設定を追加するときは「New Entry」をクリックします。

Interface名	eth0	
Queueing Discipline	---	
pfifo queue limit (pfifo 選択時有効)	<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
CBQ Parameter 設定		
回線帯域	<input type="text"/>	Kbit/s
平均パケットサイズ	<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 選択 (PacketヘッダによるFilter 設定は選択できません)	Filter No.	Class No.
	1.	<input type="text"/>
	2.	<input type="text"/>
	3.	<input type="text"/>
	4.	<input type="text"/>
	5.	<input type="text"/>
	6.	<input type="text"/>
	7.	<input type="text"/>
	8.	<input type="text"/>
	9.	<input type="text"/>
	10.	<input type="text"/>

Interface 名

キューイングをおこなうインタフェース名を入力します。本装置のインタフェース名については、本マニュアルの「付録A インタフェース名一覧」をご参照ください。

Queueing Discipline

キューイング方式を選択します。

[pfifo の設定]

pfifo queue limit

パケットをキューイングするキューの長さを設定します。**パケットの数**で指定します。1 ~ 999 の範囲で設定してください。

[TBF の設定]

「TBF Parameter 設定」について設定します。

制限Rate

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。

[SFQ の設定]

Queueing Discipline で「SFQ」を選択するだけです。

IV. 各設定画面での設定方法について

[PQの設定]

「PQ Parameter 設定」について設定します。

最大 Band 数設定

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

本装置で設定されるクラス ID は 1001:、1002:、1003:、1004:、1005: となります。バンド番号は 1001: が 1、1002: が 2、1003: が 3、1004: が 4、1005: が 5 となります。

Band 数の初期設定は 3 です (クラス ID 1001: ~ 1003:)。設定可能な band 数は 2 ~ 5 です。初期設定外の数値に設定した場合は、Priority-map 設定を変更します。

Priority-map 設定

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

Marking Filter 設定

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

Filter No. には Class 分けフィルタの設定番号を指定します。

Class No. には、パケットをおくるクラス番号 (= Band 番号) を指定します。

1001: が 1、1002: が 2、1003: が 3、1004: が 4、1005: が 5 となります。

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

インタフェースに届いたパケットは、2 つの方法でクラス分けされます。

- TOS フィールドの「Linux における扱い番号 (パケットの優先度)」を参照し、同じ番号の Priority-map の箱にパケットを送ります。
- Marking Filter 設定に従って、各クラスにパケットを送る

Priority-map の箱に付けられる Band はクラスのことです。箱に設定されている値のクラスに属することを意味します。Band 数が小さい方が、より優先度が高くなります。

クラス分けされたあとのパケットは、優先度の高いクラスから FIFO で送信されていきます。**各クラスの優先度は 1001: > 1002: > 1003: > 1004: > 1005: となります。**

より優先度の高いクラスにパケットがあると、その間は優先度の低いクラスからはパケットが送信されなくなります。

IV. 各設定画面での設定方法について

[CBQの設定]

「CBQ Parameter 設定」について設定します。

回線帯域

root クラスの帯域幅を設定します。接続回線の物理的な帯域幅を設定します(10Base-TXで接続しているときは10000kbits/s)。

平均パケットサイズ設定

パケットの平均サイズを設定します。バイト単位で設定します。

IV. 各設定画面での設定方法について

CLASS 設定

設定を追加するときは「New Entry」をクリックします。

Description	<input type="text"/>
Interface名	eth0
Class ID	<input type="text"/>
親class ID	1
Priority	<input type="text"/>
Rate設定	<input type="text"/> Kbit/s
Class内Average Packet Size設定	1000 byte
Maximum Burst設定	20
Bounded設定	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
Filter設定 (Filter番号を入力してください)	1. <input type="text"/> 2. <input type="text"/> 3. <input type="text"/> 4. <input type="text"/> 5. <input type="text"/> 6. <input type="text"/> 7. <input type="text"/> 8. <input type="text"/> 9. <input type="text"/> 10. <input type="text"/>

(画面は表示例です)

Description

設定名を付けることができます。半角英数字のみ使用可能です。

Interface 名

キューイングをおこなうインタフェース名を入力します。

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

Class ID

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

親 Class ID

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

Rate 設定

クラスの帯域幅を設定します。設定は kbit/s 単位となります。

Class 内 Average Packet Size 設定

クラス内のパケットの平均サイズを指定します。設定はバイト単位となります。

Maximum Burst 設定

一度に送信できる最大パケット数を指定します。

bounded 設定

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

「無効」を選択すると、その逆の動作となります。

Filter 設定

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

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

「CLASS Queueing 設定」

設定を追加するときは「New Entry」をクリックします。

Description	<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 queuing可能なbyte数)	<input type="text"/>
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)	Filter No. 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"/>	

(画面は表示例です)

Description

設定名を付けることができます。半角英数字のみ使用可能です。

Interface名

キューイングをおこなうインタフェース名を入力します。本装置のインタフェース名については、本マニュアルの「付録A」をご参照ください。

QDISC番号

このクラスが属しているQDISC番号を指定します。

MAJOR ID

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

Class ID

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

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

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

「CLASS分けフィルタ設定」

設定を追加するときは「New Entry」をクリックします。

設定番号	1
Description	host_1
Priority	1 (1-999)
<input checked="" type="checkbox"/> パケットヘッダ情報によるフィルタ	
プロトコル	6 (Protocol番号)
送信元アドレス	192.168.0.1/32
送信元ポート	(ポート番号)
宛先アドレス	10.10.10.10/32
宛先ポート	80 (ポート番号)
TOS値	02 (hex0-fe)
<input type="checkbox"/> Marking情報によるフィルタ	
Mark値	100 (1-999)

(画面は表示例です)

Description

設定名を付けることができます。半角英数字のみ使用可能です。

Priority

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

パケットヘッダによるフィルタ

パケットヘッダ情報でCLASS分けをおこなうときにチェックします。以下、マッチ条件を設定していきます。ただしPQをおこなうときは、パケットヘッダによるフィルタはできません。

プロトコル

プロトコルを指定します。プロトコル番号で指定してください。

送信元アドレス

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

送信元ポート

対象とする送信元ポート番号を指定します。範囲での指定はできません。

宛先アドレス

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

宛先ポート

対象とする宛先ポート番号を指定します。範囲での指定はできません。

TOS 値

TOS 値を指定します。16 進数で指定します。

DSCP 値

DSCP 値を設定します。16 進数で指定します。

Marking 情報によるフィルタ

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

設定後は「設定」ボタンをクリックします。

IV. 各設定画面での設定方法について

「パケット分類設定」

設定を追加するときには「New Entry」をクリックします。

設定番号	1	
パケット分類条件		
プロトコル	6 (Protocol番号)	<input type="checkbox"/> Not条件
送信元アドレス	192.168.0.1/32	<input type="checkbox"/> Not条件
送信元ポート	1024:65535 (ポート番号/範囲指定で番号連結)	<input type="checkbox"/> Not条件
宛先アドレス	10.10.10.10/32	<input type="checkbox"/> Not条件
宛先ポート	80 (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	ppp1	<input type="checkbox"/> Not条件
TOS/MARK/DSCP値	<input checked="" type="radio"/> TOS <input type="radio"/> MARK <input type="radio"/> DSCP <input type="radio"/> マッチ条件無効 8 上記で選択したマッチ条件に対応する設定値	TOS Bit値 hex: 0Normal Service 2Minimize cost 4Maximize Reliability 8Maximize Throughput 10Minimize Delay MARK値 (1-999) DSCP Bit値 hex:(0-3f)
TOS/MARK/DSCP値の設定		
設定対象	<input checked="" type="radio"/> TOS/Precedence <input type="radio"/> MARK <input type="radio"/> DSCP	
設定値	・MARK設定 (1-999) <input type="text"/> ・TOS/Precedence設定 Minimize cost(1) TOS Bit Internetwork Control(6) Precedence Bit ・DSCP設定 選択して下さい DSCP Bit	

(画面は表示例です)

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

【パケット分類条件】

パケット選別のマッチ条件を定義します。

プロトコル

プロトコルを指定します。プロトコル番号で指定してください。

送信元アドレス

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

送信元ポート

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

宛先アドレス

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

宛先ポート

宛先ポート番号を指定します。指定方法は送信元ポートと同様です。

インターフェース

インターフェースを選択します。インターフェース名は「付録A インターフェース名一覧」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。

【TOS/MARK/DSCP 値】

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

設定対象

TOS/Precedence、MARK、DSCP のいずれかを選択します。

設定値

設定対象で選択したものについて、設定値を指定します。

設定後は「設定」ボタンをクリックします。

TOS/Precedence および DSCP については章末をご参照下さい。

V. ステータスの表示

「ステータス表示」をクリックすると、以下の画面に移ります。

Queueing Disciplineステータス表示	<input type="button" value="表示する"/>
CLASS設定ステータス表示	<input type="button" value="表示する"/>
CLASS分けルールステータス表示	<input type="button" value="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	<input type="button" value="表示する"/>
Packet分類設定ステータス表示	<input type="button" value="表示する"/>
Interfaceの指定	<input type="text"/>

QoS機能の各種ステータスを表示します。

「Packet分類設定ステータス表示」以外では、必ずInterface名を「Interfaceの指定」に入力してから「表示する」ボタンをクリックしてください。

VI. 設定の編集・削除方法

設定をおこなうと、設定内容が一覧で表示されます。

	FilterType	Description	Priority	プロトコル	送信元アドレス	送信元ポート	宛先アドレス	宛先ポート	TOS値	MARK値	Configure
1	Mark		1							1	Edit/Remove
2	Mark		1							2	Edit/Remove
3	Mark		2							2	Edit/Remove

(「クラス分けフィルタ設定」画面の表示例)

Configureの「Edit」をクリックすると設定画面に遷移し、その設定を修正できます。

「Remove」をクリックすると、その設定が削除されます。

VII. ステータス情報の表示例

[Queueing 設定情報]表示例

各クラスで設定したキューイング方式や設定パラメータの他、送信したパケット数・送信データサイズ等の情報を表示します。

qdisc pfifo 1: limit 300p

Sent 9386 bytes 82 pkts (dropped 0, overlimits 0)

qdisc -> キューイング方式
 1: -> キューイングを設定しているクラス ID
 limit -> キューイングできる最大パケット数
 Sent (nnn) byte (mmm)pkts -> 送信したデータ量とパケット数
 dropped -> 破棄したパケット数
 overlimits -> 過負荷の状態が届いたパケット数

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 個のパケツが用意され、同時にアクティブになるのは nnn 個まで
 perturb (n)sec -> ハッシュの更新間隔

qdisc tbf 1: rate 500Kbit burst 1499b/8 mpu 0b lat 4295.0s

Sent 73050 bytes 568 pkts (dropped 2, overlimits 17)

rate -> 設定している帯域幅
 burst -> バケツのサイズ
 mpu -> 最小パケットサイズ
 lat -> パケットが tbf に留まっていられる時間

qdisc cbq 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8 weight 1000Kbit allot 1514b

level 2 ewma 5 avpkt 1000b maxidle 242us

Sent 2420755 bytes 3945 pkts (dropped 0, overlimits 0)

borrowed 0 overactions 0 avgidle 6399 undertime 0

bounded,isolated -> bounded,isolated 設定がされている (bounded は帯域を借りない、isolated は帯域を貸さない)

prio -> 優先度 (上記では root クラスなので、prio 値はありません)

weight -> ラウンドロビンプロセスの重み

allot -> 送信できるデータサイズ

ewma -> 指数重み付け移動平均

avpkt -> 平均パケットサイズ

maxidle -> パケット送信時の最大アイドル時間

borrowed -> 帯域幅を借りて送信したパケット数

avgidle -> EMWA で測定した値から、計算したアイドル時間を差し引いた数値。

通常は数字がカウントされていますが、負荷で一杯の接続の状態では "0"、過負荷の状態ではマイナスの値になります

VII. ステータス情報の表示例

[CLASS 設定情報]表示例

設定している各クラスの情報を表示します。

その1(CBQでの表示例)

```
class cbq 1: root rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio no-transmit/8
weight 1000Kbit allot 1514b
level 2 ewma 5 avpkt 1000b maxidle 242us
  Sent 33382 bytes 108 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 6399 undertime 0
class cbq 1:10 parent 1:1 rate 500Kbit cell 8b mpu 64b prio 1/1 weight 50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
  Sent 0 bytes 0 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 181651 undertime 0
class cbq 1:1 parent 1: rate 1000Kbit cell 8b mpu 64b (bounded,isolated) prio 3/3 weight
100Kbit allot 1500b
level 1 ewma 5 avpkt 1000b maxidle 242us
  Sent 2388712 bytes 3843 pkts (dropped 0, overlimits 0)
  borrowed 2004 overactions 0 avgidle 6399 undertime 0
class cbq 1:20 parent 1:1 leaf 20: rate 500Kbit cell 8b mpu 64b (bounded) prio 2/2 weight
50Kbit allot 1500b
level 0 ewma 5 avpkt 1000b maxidle 6928us offtime 15876us
  Sent 142217 bytes 212 pkts (dropped 0, overlimits 0)
  borrowed 0 overactions 0 avgidle 174789 undertime 0
```

parent -> 親クラス ID

その2(PQでの表示例)

```
class prio 1: parent 1: leaf 1001:
class prio 1: parent 1: leaf 1002:
class prio 1: parent 1: leaf 1003:
```

prio -> 優先度

parent -> 親クラス ID

leaf -> leafクラス ID

VII. ステータス情報の表示例

[CLASS分けフィルタ設定情報]表示例

クラス分けフィルタの設定情報を表示します。

その1(CBQでの表示例)

```
[ PARENT 1: ]
filter protocol ip pref 1 u32
filter protocol ip pref 1 u32 fh 805: ht divisor 1
filter protocol ip pref 1 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 1 u32 fh 804: ht divisor 1
filter protocol ip pref 1 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32
filter protocol ip pref 3 u32 fh 805: ht divisor 1
filter protocol ip pref 3 u32 fh 805::800 order 2048 key ht 805 bkt 0 flowid 1:20
  match c0a8786f/ffffffff at 16
  match 00060000/00ff0000 at 8
filter protocol ip pref 3 u32 fh 804: ht divisor 1
filter protocol ip pref 3 u32 fh 804::800 order 2048 key ht 804 bkt 0 flowid 1:10
  match c0a87800/ffffff00 at 16
  match 00060000/00ff0000 at 8
```

protocol -> マッチするプロトコル

pref -> 優先度

u32 -> パケット内部のフィールド (発信元 IP アドレスなど) に基づいて処理すべきクラスの決定を行います

at 8、at16 -> マッチの開始は、指定した数値分のオフセットからであることを示します。
at 8であれば、ヘッダの9バイトめからマッチします。

flowid -> マッチしたパケットを送るクラス

その2(PQでの表示例)

```
[ PARENT 1: ]
filter protocol ip pref 1 fw
filter protocol ip pref 1 fw handle 0x1 classid 1:3
filter protocol ip pref 2 fw
filter protocol ip pref 2 fw handle 0x2 classid 1:2
filter protocol ip pref 3 fw
filter protocol ip pref 3 fw handle 0x3 classid 1:1
```

pref -> 優先度

handle -> MARK 値

classid -> マッチパケットを送るクラス ID

VII. ステータス情報の表示例

[Packet 分類設定情報]表示例

パケット分類設定の情報を表示します。

```
pkts bytes target    prot opt in    out    source          destination      MARK set 0x1
272 39111 MARK      all -- eth0 any    192.168.120.111 anywhere
83 5439 MARK      all -- eth0 any    192.168.120.113 anywhere          MARK set 0x2
447 48695 MARK      all -- eth0 any    192.168.0.0/24  anywhere          MARK set 0x3
0 0 FTOS      tcp -- eth0 any    192.168.0.1    111.111.111.111 tcp spts:
1024:65535 dpt:450 Type of Service set 0x62
```

pkts -> 入力(出力)されたパケット数

bytes -> 入力(出力)されたバイト数

target -> 分類の対象(MARK か TOS か)

prot -> プロトコル

in -> パケット入力インタフェース

out -> パケット出力インタフェース

source -> 送信元 IP アドレス

destination -> あて先 IP アドレス

MARK set -> セットする MARK 値

spts -> 送信元ポート番号

dpt -> あて先ポート番号

Type of Service set -> セットする TOS ビット値

VIII. クラスの階層構造について

CBQにおけるクラスの階層構造は以下のようになります。

root クラス

ネットワークデバイス上のキューイングです。本装置のシステムが直接的に対話するのはこのクラスです。

親クラス

すべてのクラスのベースとなるクラスです。帯域幅を 100%として定義します。

子クラス

親クラスから分岐するクラスです。親クラスの持つ帯域幅を分割して、それぞれの子クラスの帯域幅として持ちます。

leaf(葉)クラス

leaf クラスは自分から分岐するクラスがないクラスです。

qdisc

キューイングです。ここでキューを管理・制御します。

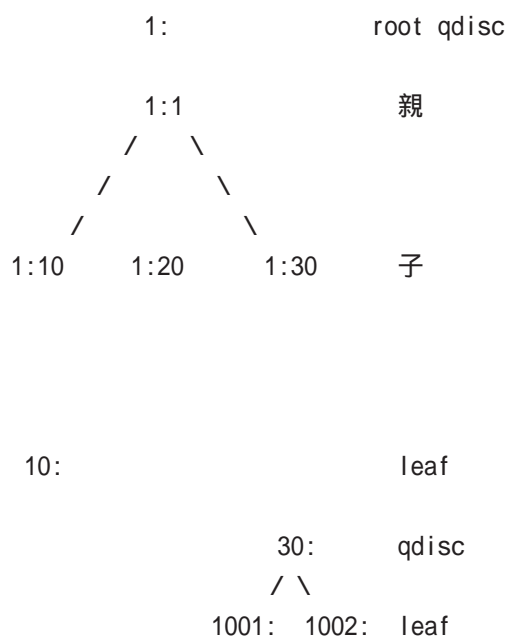
[クラス ID について]

各クラスはクラス ID を持ちます。クラス ID は MAJOR 番号と MINOR 番号の 2 つからなります。表記は以下のようになります。

<MAJOR 番号> : <MINOR 番号>

- ・ root クラスは「1:0」というクラス ID を持ちます。
- ・ 子クラスは、親と同じ MAJOR 番号を持つ必要があります。
- ・ MINOR 番号は、他のクラスと qdisc 内で重複しないように定義する必要があります。

<クラス構成図(例)>



IX. TOSについて

IPパケットヘッダにはTOSフィールドが設けられています。ここにパケットの優先度情報を付与しておくことで、優先度にあわせて機器がパケットを適切に扱えることを期待します。

IPヘッダ内のTOSフィールドの各ビットは、以下のように定義されています。<表1>

バイナリ	10進数	意味
1000	8	Minimize delay (md)
0100	4	Maximize throughput (mt)
0010	2	Maximize reliability (mr)
0001	1	Minimize monetary cost (mmc)
0000	0	Normal Service

mdは最小の遅延、mtは最高のスループット、mrは高い信頼性、mmcは低い通信コスト、を期待するパケットであることを示します。

各ビットの組み合わせによるTOS値は以下のように定義されます。<表2>

TOS	ビット	意味	Linuxでの扱い	バンド
0x0	0	Normal Service	0 Best Effort	1
0x2	1	Minimize Monetary Cost	1 Filler	2
0x4	2	Maximize Reliability	0 Best Effort	1
0x6	3	mmc+mr	0 Best Effort	1
0x8	4	Maximize Throughput	2 Bulk	2
0xa	5	mmc+mt	2 Bulk	2
0xc	6	mr+mt	2 Bulk	2
0xe	7	mmc+mr+mt	2 Bulk	2
0x10	8	Minimize Delay	6 Interactive	0
0x12	9	mmc+md	6 Interactive	0
0x14	10	mr+md	6 Interactive	0
0x16	11	mmc+mr+md	6 Interactive	0
0x18	12	mt+md	4 Int. Bulk	1
0x1a	13	mmc+mt+md	4 Int. Bulk	1
0x1c	14	mr+mt+md	4 Int. Bulk	1
0x1e	15	mmc+mr+mt+md	4 Int. Bulk	1

バンドは優先度です。0が最も優先度が高いものです。初期値ではバンド数は3(優先度は3段階)です。本装置では、PQ Paramater 設定の「最大Band数設定」でバンド数を変更できます(0 ~ 4)。

Linuxでの扱いの数値は、LinuxでのTOSビット列の解釈です。これはPQ Paramater 設定の「Priority-map設定」の箱にリンクしており、対応するPriority-mapの箱に送られます。

IX. TOS について

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

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

表中のTOSビット値(2進数表記)が、<表2>のビットに対応しています。

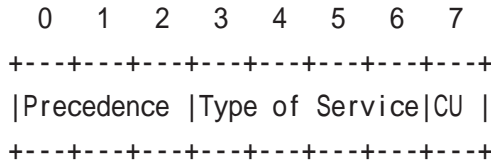
TOS値は定義があいまいで相互運用できない、正しい値が設定されている保証がない、悪用される可能性があるなどの要因により、現在までほとんど使われていません。

X. DSCPについて

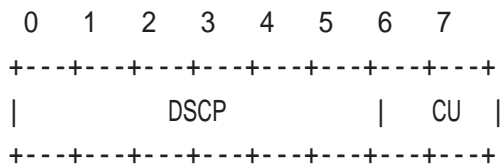
本装置ではDS(DiffServ)フィールドの設定・書き換えも可能です。DSフィールドとは、IPパケット内のTOSの再定義フィールドであり、DiffServに対応したネットワークにおいてQoS制御動作の基準となる値が設定されます。DiffServ対応機器では、DSフィールド内のDSCP値だけを参照してQoS制御を行うことができます。

TOSとDSフィールドのビット定義

【TOSフィールド構造】



【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 32 章

ゲートウェイ認証機能

第32章 ゲートウェイ認証機能

1. ゲートウェイ認証機能の設定

「ゲートウェイ認証機能」は、本装置を経由して外部にアクセスをする場合に、本装置での認証を必要とする機能です。

この機能を使うことで、外部へアクセスできるユーザーを管理できるようになります。

基本設定

[基本設定]

基本設定		
本機能	<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

本機能

ゲートウェイ認証機能を使う場合は「使用する」を選択します。

認証

当機能を使用していて、かつ認証をおこなうときは「する」を選択します(初期設定)。

認証を行わないときは「しない」を選択します。このときは、外部へのアクセスをリダイレクトするだけの動作となります。

80/tcp 監視

認証を受けていないIPアドレスからのTCPポート80番のコネクションを監視し、**このコネクションがあったときに、強制的にゲートウェイ認証をおこないます。**

初期設定は監視を「行わない」設定です。

[URL転送]

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

URL

転送先のURLを設定します。

通常認証後

「行う」を選択すると、ゲートウェイ認証後に「URL」で指定したサイトに転送させることができます。

初期設定ではURL転送を行いません。

強制認証後

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

[認証方法]

認証方法	
<input checked="" type="radio"/> ローカル	<input type="radio"/> RADIUSサーバ

認証方法

「ローカル」本装置でアカウントを管理/認証します。

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

第 32 章 ゲートウェイ認証機能

1. ゲートウェイ認証機能の設定

[接続許可時間]

接続許可時間	
<input checked="" type="radio"/> アイドルタイムアウト	30 分 (1~43200)
<input type="radio"/> セッションタイムアウト	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	

接続許可時間

認証したあとの、ユーザーの接続形態を選択できます。

「アイドルタイムアウト」

認証で許可された通信が無通信状態となってから切断するまでの時間を設定します。

「セッションタイムアウト」

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

「認証を受けたWebブラウザのウィンドウを閉じるまで」

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

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

最後に「設定変更」をクリックしてください。

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

ユーザー設定

No.	ユーザID	パスワード	削除
1	<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"/>

ユーザー ID・パスワード

ユーザーアカウントを登録します。

ユーザー ID・パスワードには半角英数字が使用できません。空白やコロン(:)は含めることができません。

「削除」をチェックすると、その設定が削除対象となります。

最後に「設定 / 削除の実行」をクリックしてください。

1. ゲートウェイ認証機能の設定

RADIUS 設定

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

プライマリサーバ設定	
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 / セカンダリサーバ設定

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

サーバ共通設定

RADIUSサーバへ問い合わせをする際に送信するNASの情報を設定します。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” はIPアドレスです。通常は本装置のIPアドレスを設定します。

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

アイドルタイムアウト

セッションタイムアウト

RADIUSサーバからの認証応答に該当のアトリビュートがあればその値を使います。該当のアトリビュートがなければ「基本設定」で設定した値を使用します。それぞれ、基本設定で選択されているものが有効となります。

Idle-Timeout : アイドルタイムアウト

Ascend-Maximum-Time : セッションタイムアウト

Ascend-Idle-Limit : アイドルタイムアウト

アトリビュートとは、RADIUSで設定されるパラメータのことを指します。

最後に「設定変更」をクリックしてください。

1. ゲートウェイ認証機能の設定

MAC アドレスフィルタ

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

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

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

MACアドレスフィルタの 追加	
MACアドレス	<input type="text"/>
インタフェース	<input type="text"/>
動作	許可 <input type="button" value="v"/>

MAC アドレス

フィルタリング対象とする、送信元 MAC アドレスを入力します。

インタフェース

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

動作

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

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

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

設定の編集には「編集」を、削除するには「削除」をクリックして下さい。

第32章 ゲートウェイ認証機能

1. ゲートウェイ認証機能の設定

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。特定のポートだけの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。」というメッセージが表示されたらリンクをクリックしてフィルタ設定画面に移ります。

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
	パケット受信時	許可	全て				
	パケット受信時	許可	全て				

ここで設定した IP アドレスやポートについては、ゲートウェイ認証機能によらず、通信可能になります(設定方法については第27章「パケットフィルタリング機能」をご参照下さい)。

ログ設定

ゲートウェイ認証機能のログを本装置のシステムログに出力できます。

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。
- ・アクセスログ : ゲートウェイ認証時のアクセスログを出力します。

<エラーログの表示例>

```
Apr 7 17:04:45 localhost httpd[21529]: [error]
[client 192.168.0.1] user abc: authentication
failure for "/": password mismatch
```

<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
```

11. ゲートウェイ認証下のアクセス方法

ホストからのアクセス方法

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ー 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 2003

設定画面へのアクセスについて

ゲートウェイ認証機能を使用していて認証をおこなっていない場合でも、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、本装置は RADIUS サーバに対して認証要求のみを送信します。

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

認証について

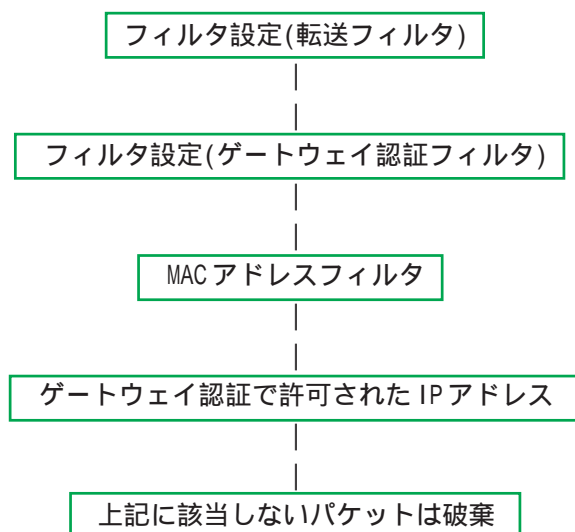
認証方法が「ローカル」、「RADIUS サーバ」のどちらの場合でも、クライアント - 本装置間の認証には、HTTP Basic 認証が用いられます。

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

III. ゲートウェイ認証の制御方法について

ゲートウェイ認証機能はパケットフィルタの一種で、認証で許可されたユーザー(ホスト)の IP アドレスを送信元 / 宛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 33 章

検疫フィルタ機能

第33章 検疫フィルタ機能

検疫フィルタ機能の設定

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

Web 設定画面「検疫フィルタ設定」をクリックして設定をします。

検疫フィルタ設定

検疫フィルタ	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
Log	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する
ユーザ	<input type="text" value="demo"/>
パスワード	<input type="text" value="demo"/>

検疫フィルタ

検疫フィルタ機能を使う場合は「使用する」を選択します。

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

Log

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

ユーザ

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

検疫フィルタ

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

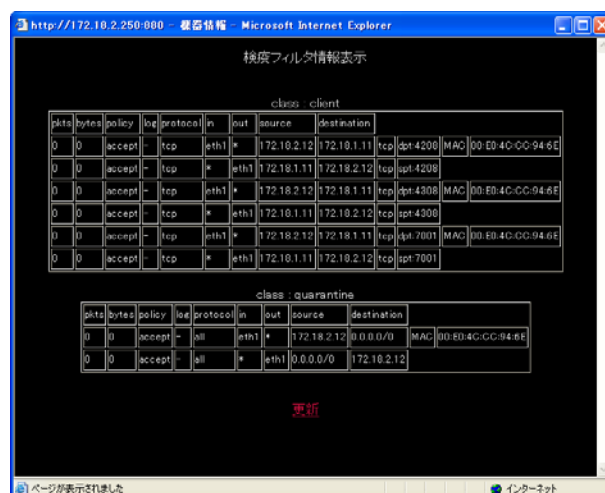
入力が終わりましたら「設定の保存」をクリックして設定完了です。以降「XR 検疫管理サービス」からの指示に基づきフィルタルールが追加削除されるようになります。

管理機能

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

表示

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



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

削除

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

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

第 34 章

ネットワークテスト

第34章 ネットワークテスト

ネットワークテスト

本装置の運用時において、ネットワークテストをおこなうことができます。ネットワークのトラブルシューティングに有効です。以下の3つのテストができます。

- ・pingテスト
- ・tracerouteテスト
- ・パケットダンプの取得

実行方法

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

Ping	<p>FQDNまたはIPアドレス</p> <input type="text"/> <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</p> <p><input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3</p> <p><input checked="" type="radio"/> その他 <input type="text"/></p> <p><input type="button" value="実行"/></p>
Trace Route	<p>FQDNまたはIPアドレス</p> <input type="text"/> <p><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</p> <p><input type="radio"/> Ether0 <input type="radio"/> Ether1 <input type="radio"/> Ether2 <input type="radio"/> Ether3</p> <p><input type="radio"/> その他 <input type="text"/></p> <p><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</p> <input type="text"/> <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><input type="button" value="実行"/> <input type="button" value="結果表示"/></p>

(画面はXR-1100/CTでの表示例です)

pingテスト

指定した相手に本装置から Ping を発信します。FQDN(www.xxx.co.jp などのドメイン名)、もしくは IP アドレスを入力して「実行」をクリックします。また ping を送出するインタフェースを指定することもできます(省略化)

実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=49.5 ms
64 bytes from 211.14.13.66: icmp_seq=1 ttl=52 time=66.7 ms
64 bytes from 211.14.13.66: icmp_seq=2 ttl=52 time=11.7 ms
64 bytes from 211.14.13.66: icmp_seq=3 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=4 ttl=52 time=69.0 ms
64 bytes from 211.14.13.66: icmp_seq=5 ttl=52 time=58.3 ms
64 bytes from 211.14.13.66: icmp_seq=6 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=7 ttl=52 time=71.4 ms
64 bytes from 211.14.13.66: icmp_seq=8 ttl=52 time=12.0 ms
64 bytes from 211.14.13.66: icmp_seq=9 ttl=52 time=11.8 ms

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

traceroute テスト

指定した宛先までに経路するルータの情報を表示します。ping と同様に、FQDN もしくは IP アドレスを入力して「実行」をクリックします。

実行結果例

実行結果

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

--- 211.14.13.66 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.4/12.4/12.4 ms
traceroute to 211.14.13.66 (211.14.13.66), 30 hops max, 40 byte packets
 1 192.168.120.15 (192.168.120.15) 1.545 ms 2.253 ms 1.607 ms
 2 192.168.100.50 (192.168.100.50) 2.210 ms 4.955 ms 2.309 ms
 3 172.17.254.1 (172.17.254.1) 8.777 ms 21.189 ms 13.946 ms
 4 210.135.192.108 (210.135.192.108) 9.205 ms 8.953 ms 9.310 ms
 5 210.135.208.34 (210.135.208.34) 35.538 ms 19.923 ms 14.744 ms
 6 210.135.208.10 (210.135.208.10) 41.641 ms 40.476 ms 63.293 ms
 7 210.171.224.115 (210.171.224.115) 43.948 ms 27.255 ms 36.767 ms
 8 211.14.3.233 (211.14.3.233) 36.861 ms 33.890 ms 37.679 ms
 9 211.14.3.148 (211.14.3.148) 36.865 ms 47.151 ms 18.491 ms
10 211.14.3.105 (211.14.3.105) 53.573 ms 13.889 ms 50.057 ms
11 211.14.2.193 (211.14.2.193) 33.777 ms 11.380 ms 17.282 ms
12 * * *
13 211.14.12.249 (211.14.12.249) 19.692 ms !X * 15.213 ms !X
```

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

第34章 ネットワークテスト

ネットワークテスト

条件式は、" or " , " and " , " not " といった論理条件も指定できます。

(例) 192.168.0.0/24の外から中に入っているパケットを取得する

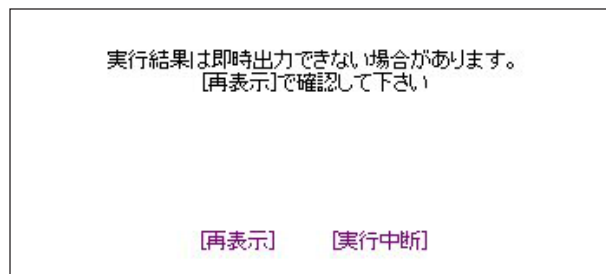
```
src net not 192.168.0.0/24 and dst net 192.168.0.0/24
```

複数の条件を指定したいときは上記のように、論理条件によって一連の条件式として設定してください。

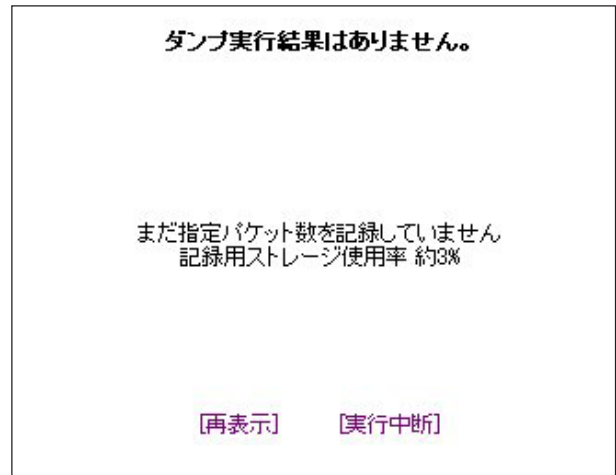
条件式の記述方法が正しくない場合は、「tcpdumpは異常終了しました。filter等を確認してください」と表示され、パケットダンプが取得できません。DumpFilterの設定を見直してください。

上記項目を入力後、「実行」ボタンでパケットダンプを開始します。

パケットダンプを開始したときの画面表示

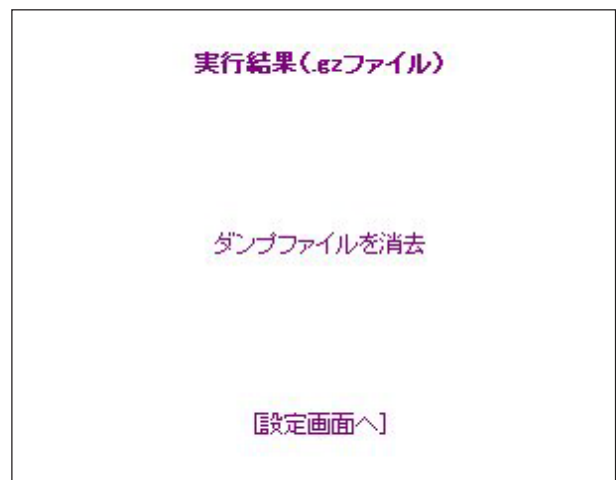


パケットダンプ結果を表示できないときの画面



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

パケットダンプが実行終了したときの画面



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

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

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

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

ネットワークテスト

[PacketDump TypePcapの注意点]

- ・取得したパケットダンプ結果は、libcap形式でgzip圧縮して保存されます。
- ・取得できるデータサイズは、gzip圧縮された状態で最大約4MBです。
- ・本装置上にはパケットダンプ結果を1つだけ記録しておけます。パケットダンプ結果を消去せずにPacketDump TypePcapを再実行して実行結果ファイルを作成したときは、それまでに記録されていたパケットダンプ結果に上書きされます。
- ・本装置のインタ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。

第 35 章

簡易 CLI 機能

I. 簡易 CLI 機能の概要

本装置では、表示コマンドを中心とした簡易 CLI (Command Line Interface) 機能を実装しています。ブラウザベースの GUI に比べ、よりスピーディな運用監視が可能になります。

簡易 CLI では以下のようなコマンド群を実装しています。

- ・システム情報の表示
- ・インタフェース情報の表示
- ・システム内部情報の表示
- ・各種サービス情報の表示
- ・L2TPv3 セッションの開始 / 停止
- ・L2TPv3 フィルタ情報の表示 / クリア
- ・テクニカルサポート機能(情報一括表示)

各コマンドの実行方法などの詳細については、別紙「CLI コマンドリファレンス」を参照してください。

CLI に関する設定

CLI を使用するための本装置へのアクセスは telnet で行いますが、初期状態では全てのアクセスが禁止されています。CLI へアクセスするための設定は以下の画面から行います。

「システム設定」 「CLI 設定」をクリックして設定画面を開きます。

CLI 設定		
機能設定	ユーザ設定	ACL 設定
本機能	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> telnet <input type="checkbox"/> ssh	
ホスト名	xr1100	
Enable パスワード		

CLI へのアクセス設定は以下の手順で行います。

- 1) ユーザ設定
ユーザアカウントの作成
- 2) ACL 設定
アクセスリストの設定
- 3) 機能設定
CLI 接続の受付開始

II. 簡易 CLI 機能のアクセス設定

1. ユーザアカウントの作成

まず CLI にアクセスするためのユーザアカウントを作成します。
アカウントは最大 64 アカウントまで設定可能です。

ユーザアカウントの作成は、「ユーザ設定」をクリックして、以下の設定画面から行います。

No.	ユーザ	パスワード	無効	削除
1	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

ユーザ

任意のユーザ名を設定して下さい。使用可能な文字は、半角英数字、"-"(ハイフン)、“_”(アンダースコア)、“.”(ピリオド)です。最大 64 文字まで入力可能です。

パスワード

任意のパスワードを設定して下さい。使用可能な文字は、半角英数字、“-”(ハイフン)、“_”(アンダースコア)、“.”(ピリオド)です。最大 64 文字まで入力可能です。

無効

設定したアカウントを一時的に使用不可にしたい場合は、このボックスにチェックを入れてください。GUI 上の設定は残りますが、このアカウントからのアクセスはできません。

入力が終わりましたら「設定」をクリックして設定完了です。

II. 簡易 CLI 機能のアクセス設定

2. アクセスリストの設定

次に CLI へのアクセス可能なホスト、ネットワークを制限するために、アクセスリストを設定します。

アクセスリストが未設定の状態では全てのホストからの接続が可能になっています。必ずアクセスリストを設定して下さい。

アクセスリストの設定は、「ACL 設定」をクリックして、以下の設定画面から行います。

No.	パーミッション	送信元アドレス	宛先アドレス	無効	削除
1	----	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	----	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	----	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input type="checkbox"/>

パーミッション

このリストエントリの条件にマッチしたアクセスに対して、許可(permit)または拒否(deny)を選択します。

送信元アドレス

アクセス元のホストアドレスまたはネットワークアドレスを指定します。

宛先アドレス

アクセス先(つまり本装置)のホストアドレスまたはネットワークアドレスを指定します。

送信元アドレス、宛先アドレスの指定はホストアドレス形式(xx.xx.xx.xx)、ネットワーク形式(xx.xx.xx.xx/yy)のいずれの形式でも可能です。

すべてのネットワークを指定する場合は、「0.0.0.0/0」と入力してください。

無効

設定したアクセスリストを一時的に無効にしたい場合は、このボックスにチェックを入れてください。GUI 上の設定は残りますが、このアクセスリストは無効になります。

入力が終わりましたら「設定」をクリックして設定完了です。

アクセスリストの評価順について

CLI アクセス時のアクセス条件の比較は、アクセスリストの上から順に行われます。条件にマッチするアクセスリストが見つかった場合は、そのパーミッション動作に従ってアクセスの許可 / 拒否を決定し、以降のアクセスリストは評価されません。例えば、192.168.0.100 のホストを除く 192.168.0.0/24 のネットワークからのアクセスを禁止したい場合は、以下の並びでアクセスリストを設定します。

No.	パーミッション	送信元アドレス	宛先アドレス
1	permit	192.168.0.100	192.168.0.254
2	deny	192.168.0.0/24	192.168.0.254

暗黙の deny について

アクセスリストを設定した場合、アクセスリストの最後には全てのアクセスを禁止する暗黙の deny が設定されています。

つまり、全てのアクセスリストに対してマッチしないアクセスは禁止されることになります。

II. 簡易 CLI 機能のアクセス設定

3. CLI 接続の受付開始

最後に CLI 機能を有効にすることで、CLI へのアクセスの受け付けを開始します。

CLI 機能の有効は、「機能設定」をクリックして、以下の設定画面から行います。

本機能	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> telnet <input type="checkbox"/> ssh
ホスト名	<input type="text" value="xr1100"/>
Enable パスワード	<input type="text"/>

本機能

「telnet」「ssh」のチェック欄で、CLI へのアクセスを受け付けるポートを選択し、「有効」にチェックを入れます。

ホスト名

任意のホスト名を設定して下さい。CLI のプロンプトとして表示されます。

ENABLE パスワード

特権ユーザ用の「Enable パスワード」を設定します。

CLI には一般ユーザ用の「VIEW モード」と、特権ユーザ用の「ENABLE モード」があり、内部システム情報の表示や実行系のコマンドは ENABLE モードでのみ実行可能です。この Enable パスワードを設定すると、ENABLE モードへ以降する際に、パスワード認証を行います。

詳細は、「CLI コマンドリファレンス」を参照して下さい。

入力が終わりましたら「設定」ボタンをクリックして設定完了です。チェックを入れた telnet/ssh ポートをリッスンし、CLI へのアクセスを受け付けます。

II. 簡易 CLI 機能のアクセス設定

- - 注意 - -

telnet, ssh ポートのフィルタリング

CLI 機能を有効にした場合、全てのインタフェースの telnet ポート (23 番) または ssh ポート (22 番) でリスンしている状態になります。CLI へのアクセスはアクセスリストで制限できますが、telnet, ssh ポートは攻撃の対象とされやすいので、WAN 側の telnet, ssh ポートは入力パケットのフィルタリングを設定することを推奨します。

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	tcp				22
2	ppp0	パケット受信時	破棄	tcp				23

フィルタリングの設定例です

telnet 接続クライアントについて

telnet 接続クライアントは、Windows「MS-DOS プロンプト」や端末エミュレータソフト、UNIX の telnet コマンドなど任意のクライアントが使用できます。

これらのクライアントの使い方については、個々のマニュアル等を参照して下さい。

ssh の対応バージョンについて

ssh 接続は version1, version2 の両方に対応しています。常に両方のバージョンでの接続が可能です。但し、RSA 鍵認証には対応しておりません。パスワード認証による接続のみ可能です。

telnet, ssh セッションのキープアライブ

telnet, ssh クライアントから突然に切断された場合に備え、TCP が無通信の状態でも 120 分を経過すると、自動的に TCP Keepalive を開始します。

Keepalive の応答がない場合は、TCP セッション断と判断し、内部の TCP セッションを解放します。

第 36 章

システム設定

システム設定

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

- ・時計の設定
- ・ログの表示 / 削除
- ・パスワードの設定
- ・ファームウェアアップデート
- ・設定の保存・復帰
- ・設定のリセット
- ・本体の再起動
- ・本体停止
- ・セッションライフタイムの設定
- ・設定画面の設定
- ・オプションUSBフラッシュディスクの操作

実行方法

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

時計の設定

本装置内蔵時計の設定をおこないます。

「時計の設定」をクリックして設定画面を開きます。



The screenshot shows a web interface for setting the clock. At the top, there are input fields for the date: '2006' for the year, '03' for the month, and '31' for the day, followed by '日 金曜日' (Sunday, Friday). Below this, there are input fields for the time: '13' for hours, '42' for minutes, and '15' for seconds. At the bottom, there is a note: '※時刻は24時間形式で入力してください。' (Please input the time in 24-hour format.)

24時間単位で時刻を設定してください。

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

システム設定

ログの表示

実行方法

「ログの表示」をクリックして表示画面を開きます。

```
Apr 26 00:05:11 localhost -- MARK --
Apr 26 00:25:11 localhost -- MARK --
Apr 26 00:37:59 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 00:37:59 localhost named[436]: USAGE 1019749079 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 00:37:59 localhost named[436]: NSTATS 1019749079 1019556843 A=3
Apr 26 00:37:59 localhost named[436]: XSTATS 1019749079 1019556843 RR=0 RNKD=0
RfwdR=0 RdupR=0 Rfail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 Ssys0=1 SAns=0
SFwd0=3 SDup0=19233 SErr=4 R0=3 RI0=0 RfwdQ=0 RdupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNKD=0
Apr 26 01:08:09 localhost -- MARK --
Apr 26 01:28:09 localhost -- MARK --
Apr 26 01:38:57 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 01:38:57 localhost named[436]: USAGE 1019752737 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 01:38:57 localhost named[436]: NSTATS 1019752737 1019556843 A=3
Apr 26 01:38:57 localhost named[436]: XSTATS 1019752737 1019556843 RR=0 RNKD=0
RfwdR=0 RdupR=0 Rfail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 Ssys0=1 SAns=0
SFwd0=3 SDup0=19233 SErr=4 R0=3 RI0=0 RfwdQ=0 RdupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNKD=0
Apr 26 02:07:06 localhost -- MARK --
Apr 26 02:27:06 localhost -- MARK --
Apr 26 02:39:54 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 02:39:54 localhost named[436]: USAGE 1019756394 1019556843
CPU=2.58u/2.34s CHILDCPU=0u/0s
Apr 26 02:39:54 localhost named[436]: NSTATS 1019756394 1019556843 A=3
Apr 26 02:39:54 localhost named[436]: XSTATS 1019756394 1019556843 RR=0 RNKD=0
RfwdR=0 RdupR=0 Rfail=0 RFErr=0 RErr=0 RAXFR=0 RLame=0 ROpts=0 Ssys0=1 SAns=0
SFwd0=3 SDup0=19233 SErr=4 R0=3 RI0=0 RfwdQ=0 RdupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SNaAns=0 SNKD=0
```

本装置のログが全てここで表示されます。

「表示の更新」ボタンをクリックすると表示が更新されます。

「不正アクセス検出機能」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。

ローテーションで記録されたログは圧縮して保存されます。保存されるファイルは最大で4つです。以降は古いログファイルから順に削除されていきます。

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

ログの削除

ログ情報は最大2MBまでのサイズで保存されます。また再起動時にログ情報は削除されます。手動で削除する場合は次のようにしてください。

実行方法

「ログの削除」をクリックして画面を開きます。

すべてのログメッセージを削除します。

実行する

「削除実行」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

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

実行方法

「パスワードの設定」をクリックして設定画面を開きます。

新しいユーザー名	<input type="text"/>
新しいパスワード	<input type="text"/>
もう一度入力してください	<input type="text"/>

新しいユーザー名とパスワードを設定します。半角英数字で1から8文字まで設定可能です。大文字・小文字も判別しますのでご注意ください。

入力が終わりましたら「設定」ボタンをクリックして設定完了です。次回のログインからは、新しく設定したユーザー名とパスワードを使います。

システム設定

ファームウェアのアップデート

本装置は、ブラウザ上からファームウェアのアップデートをおこないます。

実行方法

「ファームウェアのアップデート」をクリックして画面を開きます。

ここではファームウェアのアップデートをおこなうことができます。

ファイルの指定

参照...

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

その後、ファームウェアを本装置に転送します(転送が終わるまではしばらく時間がかかります)。転送完了後に、以下のようなアップデートの確認画面が表示されますので、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
XR-1100 ver 1.1.0
ダウンロードされたファームウェアのバージョン
XR-1100 ver 1.1.0

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

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。

アップデート中は、本体のLEDが時計回りに回転します。この間は、アクセスをおこなわずにそのままお待ちください。

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

システム設定

設定の保存と復帰

本装置の設定の保存および、保存した設定の復帰をおこないます。

実行方法

「設定の保存・復帰」をクリックして画面を開きます。

- - 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勧めします。

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て「設定ファイルの作成」をクリックします。

現在の設定を保存することができます。	
コードの指定	<input type="radio"/> EUC(LF) <input checked="" type="radio"/> S.JIS(CR+LF) <input type="radio"/> S.JIS(CR)
形式の指定	<input type="radio"/> 全設定(gzip) <input checked="" type="radio"/> 初期値との差分(text)

クリックすると以下のメッセージが表示されます。

設定をバックアップしました。
バックアップファイルのダウンロード

ブラウザのリンクを保存する等で保存して下さい。

「バックアップファイルのダウンロード」リンクから、設定をテキストファイルで保存しておきます。

「全設定」を選択すると、本装置のすべての設定を gzip 形式で圧縮して保存します。

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

[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テキストファイルを選択します。

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..."/>

その後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、本装置が自動的に再起動されます。

- - 注意 - -

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

システム設定

設定のリセット

本装置の設定を全てリセットし、工場出荷時の設定に戻します。

実行方法

「設定のリセット」をクリックして画面を開きます。

現在の本体設定内容を全てクリアして工場出荷設定に戻します。

実行する

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

再起動

本装置を再起動します。設定内容は変更されません。

実行方法

「再起動」をクリックして画面を開きます。



「実行する」ボタンをクリックすると、再起動が実行されます。

システム設定

本体停止

本装置を停止状態にします。

停止状態とは、電源オフの状態とほぼ同じですが、本体背面のメインスイッチで操作することなく、本体の動作を停止します。

本装置に CF カードを装着していて、CF カードを本体から取り外すときには必ず「本体停止」を実行してから作業してください。

実行方法

「本体停止」をクリックして画面を開きます。

本体の動作を停止します。

実行する

「実行する」ボタンをクリックすると、本装置は停止状態となります。

停止状態から稼働状態に復帰する場合は、本装置本体前面にあるパワースwitchの「|」側を押してください。

セッションライフタイムの設定

NAT/IP マスカレードのセッションライフタイムを設定します。

「セッションライフタイムの設定」をクリックして画面を開きます。

UDP	<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)
0を入力した場合、デフォルト値を設定します。		

UDP

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

UDP stream

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

TCP

TCP セッションのライフタイムを設定します。単位は秒です。0 ~ 8640000 の間で設定します。初期設定は 432000 秒です。

「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。

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

設定画面の

アクセスログ
(アクセス時の)エラーログ

を取得するかどうかを指定して、「設定の保存」をクリックします。

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

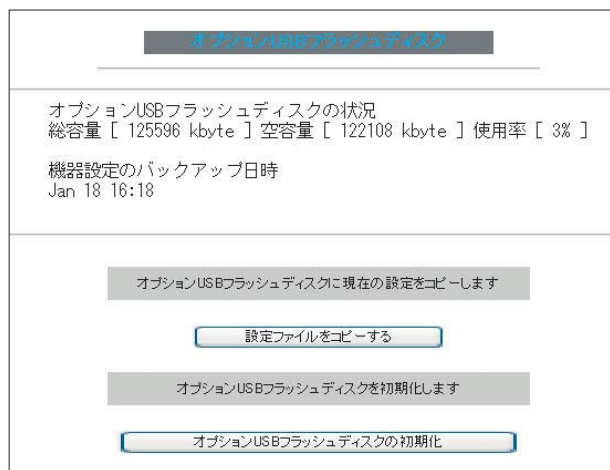
システム設定

オプションUSBフラッシュディスク

XR-1100シリーズにオプションで用意されているUSBフラッシュディスク FutureNet Memory Media USB-128 を装着している場合、USBフラッシュディスクの操作を行ないます。

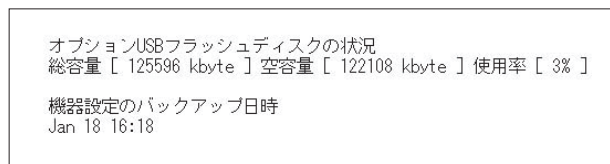
- ・フラッシュディスクの初期化
- ・フラッシュディスクへの設定のバックアップができます。

「オプションUSBフラッシュディスク」をクリックして画面を開きます。



USBフラッシュディスク情報の表示

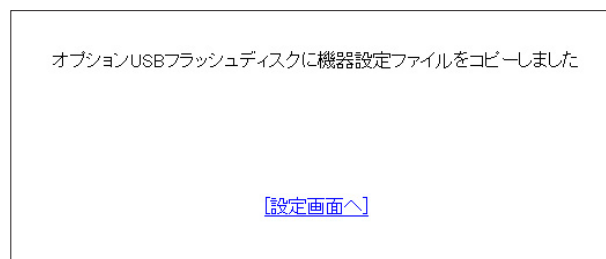
画面上部には、装着したUSBフラッシュディスクのメモリ容量使用状況などの情報が表示されます。



USBフラッシュディスクに設定をコピーする

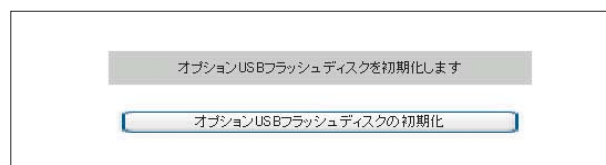
設定のバックアップをUSBフラッシュディスクにコピーするときは「オプションUSBフラッシュディスクに現在の設定をコピーします」項目でコピーを実行します。

コピー完了後は以下のような画面が表示されます。



USBフラッシュディスクの初期化

USBフラッシュディスクを初期化するときは「オプションUSBフラッシュディスクを初期化します」項目で実行します。



はじめてUSBフラッシュディスクを装着したときは必ず「USBフラッシュディスクの初期化」を実行してください。USBフラッシュディスクは初期化しないと使用できません。

またUSBフラッシュディスクが初期化されていないときは、「オプションUSBフラッシュディスクに現在の設定をコピーします」項目は表示されません。

USBフラッシュディスクを本装置から取り外すときは、「本体の停止」を実行するか、本体前面の「Release」ボタンを使用してください。「本体の停止」もしくは「Release」ボタンを使わずにUSBフラッシュディスクを取り外すと、本装置およびUSBフラッシュディスクが破損する場合があります。詳しい取り外し方法は第38章「運用管理設定 オプションUSBフラッシュディスクを取り外す」を参照して下さい。

システム設定

CLI 設定

CLI 設定については、第 34 章「簡易 CLI 機能」で説明します。

ARP filter 設定

ARP filter の設定をおこないます。

ARP filter を有効にすることで、同一 IP アドレスの ARP を複数のインタフェースで受信したときに、当該 MAC アドレス以外のインタフェースから ARP 応答を出さないようにできます。

「ARP filter 設定」をクリックして設定画面を開きます。



「無効」または「有効」を選択して「設定の保存」をクリックします。

第 37 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。

標準ファームと #IRI ファームとの違いは、機種名の後に「IRI」と記されていることで判断できます。

- **インタフェース情報**

各インタフェースの IP アドレスや MAC アドレスなどです。

PPP/PPPoE や IPsec 論理インタフェースもここに表示されます。

- **リンク情報**

本装置の各 Ethernet ポートのリンク状態、リンク速度が表示されます。

- **ルーティング情報**

インタフェースルート、スタティックルート、ダイナミックルートに関するルーティング情報です。

- **Default Gateway 情報**

デフォルトルート情報です。

- **ARP テーブル情報**

XR が保持している ARP テーブルです。

- **DHCP クライアント取得情報**

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

実行方法

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

```

ファームウェアバージョン
Century Systems XR-640 Series ver 1.1.3
更新
インタフェース情報
eth0 Link encap:Ethernet HWaddr 00:80:6D:68:01:E4
    inet addr:192.168.120.237 Bcast:192.168.120.255 Mask:255.255.255.0
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:293557 errors:0 dropped:0 overruns:0 frame:0
    TX packets:2700 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:100
    Interrupt:80
eth1 Link encap:Ethernet HWaddr 00:80:6D:68:01:E5
    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
    Interrupt:82
eth2 Link encap:Ethernet HWaddr 00:80:6D:68:01:E6
    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
    Interrupt:28 Base address:0xf00

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
192.168.120.0 0.0.0.0 255.255.255.0 U 0 0 0 eth0

Default Gateway情報
default via 192.168.120.15 dev eth0

ARPテーブル情報
IP address HW type Flags HW address Mask Device
192.168.120.111 0x1 0x2 00:20:ED:4D:B0:0B * eth0
  
```

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 38 章

詳細情報表示

各種情報の表示

システム設定の「詳細情報表示」をクリックすると、以下の画面が表示されます。

ルーティング	ルーティング詳細情報
	ルーティングキャッシュ情報
	デフォルトゲートウェイ情報
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アドレスリース情報
NTPサービス	NTP情報
VRRPサービス	VRRP 情報
PPPoE to L2TP	L2TP情報
QoS	Queueing設定情報
	CLASS設定情報
	CLASS分けフィルタ設定情報
	Packet分類設定情報
	Interfaceの指定 <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。

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

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

表示される内容は以下のとおりです。

・ルーティング情報

XR のルーティングテーブル、ルーティングテーブルの内部情報、ルートキャッシュの情報、デフォルトゲートウェイ情報が表示できます。

このうち、ルーティングテーブルの内部情報とルートキャッシュの情報はここでのみ表示できます。

- ・OSPF 情報
- ・RIP 情報
- ・IPsec 情報
- ・NTP 情報
- ・VRRP 情報
- ・PPPoE to L2TP
- ・QoS 情報

第 39 章

テクニカルサポート

第 39 章 テクニカルサポート

テクニカルサポート

テクニカルサポートを利用することによって、本体の情報を一括して取得することができます。

機器情報の取得を行います

情報取得

「情報取得」をクリックします。下記の 3 つの情報を一括して取得することができます。

syslog

設定ファイル

本体の機器情報

第 40 章

運用管理設定

1. 各種ボタンの操作

本装置の前面にある各種ボタンを使用して、以下の操作をおこないます。

- ・本装置の設定を初期化する
- ・オプションUSBフラッシュディスクに保存された設定で起動する
- ・本装置をシャットダウンする

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 本体前面にある「Init」ボタンを押しながら、パワー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System statusランプが消灯したらInitボタンを放します。本装置が工場出荷設定で起動します。
- 4 本装置の起動が完了するとSystem statusランプが点灯し、Init Statusランプは消灯します。

1. 各種ボタンの操作

オプションUSBフラッシュディスクの設定で起動する

- 1 本装置にオプションUSBフラッシュディスク FutureNet Memory Media USB-128 が挿入されていることを確認します。
- 2 本体前面にある「Init」ボタンを押しながら、パワースイッチをオンにします。Initボタンは押したままにしておきます。
- 3 本体前面のSystem statusランプが消灯したらInitボタンを放します。その後、本装置がオプションUSBメモリに保存されている設定内容で起動します。
- 4 本装置の起動が完了するとSystem statusランプが点灯し、Init statusランプは消灯します。

本装置をシャットダウンする

本装置のシャットダウンは、「システム設定」画面からおこなうか、本体前面のpowerスイッチを押してください。

電源スイッチを押すと、動作が停止して待機状態になります。待機状態とは、電源オフ状態と同じですが、本装置には通電している状態です。

ただし通常は、設定画面の「システム設定」「本体停止」画面で待機状態にしてください。待機状態にするのは、本装置がハングアップしたときなどの非常時のみにしてください。

完全に電源をオフにする場合は、電源スイッチを4秒以上押してください。

II. オプションUSBフラッシュディスクの操作

オプションUSBフラッシュディスクを接続する

1 オプションUSBフラッシュディスク

FutureNet Memory Media USB-128 を本体前面のUSBインタフェースに差し込みます。下側のインタフェースのみ使用可能です。図柄の印刷されている面が上面です。

2 USB Status ランプの状態が、消灯 -> 点滅 -> 点灯の順序で遷移します。

3 USB Status ランプが点灯した後、オプションUSBフラッシュディスクが使用できる状態となります。

オプションUSBフラッシュディスクを取り外す

本装置からUSBフラッシュディスクを取り外すときは、以下の手順で操作してください。

1 本体前面の「Release」ボタンを押します。

2 USB Status ランプが点灯 点滅 消灯の順序で遷移します。

3 USB Status ランプが消灯したのを確認後、オプションUSBフラッシュディスクを取り外すことができます。

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場合があります。

- OSPF 機能
- IPsec 機能
- L2TPv3 機能
- SNMP エージェント機能
- UPnP 機能
- スタティックルート設定
- ソースルート設定
- NAT 機能
- パケットフィルタリング機能
- ネットワークイベント機能
- 仮想インタフェース機能
- 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付けは次の表の通りとなります。

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

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 (XR-1100/CT のみ)	192.168.2.254/255.255.255.0
ETHER3 ポート (XR-1100/CT のみ)	192.168.3.254/255.255.255.0
DHCP クライアント機能	無効
IP マスカレード機能	無効
ステートフルパケットインスペクション機能	無効
デフォルトゲートウェイ設定	設定なし
リモートアクセス機能	無効
DNS リレー / キャッシュ機能	無効
DHCP サーバ / リレー機能	無効
IPsec 機能	無効
UPnP 機能	無効
ダイナミックルーティング機能	無効
L2TPv3 機能	無効
SYSLOG 機能	有効
攻撃検出機能	無効
SNMP エージェント機能	無効
NTP 機能	無効
VRRP 機能	無効
アクセスサーバ機能	無効
スタティックルート設定	設定なし
ソースルーティング設定	設定なし
NAT 機能	設定なし
パケットフィルタリング機能	NetBIOSからの漏洩を防止するフィルタ設定 (入力・転送フィルタ設定) 外部からの UPnP パケットを遮断する設定 (入力・転送フィルタ設定)
ネットワークイベント機能	無効
仮想インターフェース機能	設定なし
GRE 機能	無効
QoS 機能	設定なし
パケット分類機能	設定なし
ゲートウェイ認証機能	無効
検疫フィルタ機能	無効
設定画面ログイン ID	admin
設定画面ログインパスワード	admin

付録 C

サポートについて

サポートについて

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

サポートに関する技術的なお問い合わせやご質問は、下記へご連絡下さい。

- ・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下さい。事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

ご連絡をいただく前に

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

- ・ファームウェアのバージョンとMACアドレス
(バージョンの確認方法は設定画面「情報表示」でご確認いただけます)
- ・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下さい。
- ・不具合の内容または、不具合の再現手順
何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせ下さい。
- ・エラーメッセージ
エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
- ・本装置の設定内容、およびコンピュータのIP設定
- ・可能であれば、「設定のバックアップファイル」をお送りください。

サポート情報

弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。また製品のFAQも掲載しておりますので、是非ご覧下さい。

XR-1100 製品サポートページ

<http://www.centurysys.co.jp/support/xr1100.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。保証期間を過ぎたもの、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承下さい。保証規定については、同梱の保証書をご覧ください。

XR-1100series ユーザーズガイド 1.6.2対応版

2007年11月版

発行 センチュリー・システムズ株式会社

Copyright (c) 2002-2007 Century Systems Co., Ltd. All rights reserved.
