

# *Mobile VPN Series*

---

モバイルVPN対応ルータ

---

**FutureNet XR-430**

ユーザーズガイド

v1.1.0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
<b>第1章 XR-430 の概要 .....</b>	<b>11</b>
. XR-430 の特長 .....	12
. 各部の名称と機能 .....	14
. 動作環境 .....	16
<b>第2章 XR-430 の設置 .....</b>	<b>17</b>
XR-430 の設置 .....	18
<b>第3章 コンピュータのネットワーク設定 .....</b>	<b>20</b>
. Windows XP のネットワーク設定 .....	21
. Windows Vista のネットワーク設定 .....	22
. Macintosh のネットワーク設定 .....	23
. IP アドレスの確認と再取得 .....	24
<b>第4章 設定画面へのログイン .....</b>	<b>25</b>
設定画面へのログイン方法 .....	26
<b>第5章 インターフェース設定 .....</b>	<b>27</b>
. Ethernet ポートの設定 .....	28
. Ethernet ポートの設定について .....	30
. VLAN タギングの設定 .....	31
. デフォルトゲートウェイの設定 .....	32
<b>第6章 PPPoE 設定 .....</b>	<b>33</b>
. PPPoE の接続先設定 .....	34
. PPPoE の接続設定と回線の接続と切断 .....	36
. バックアップ回線接続設定 .....	39
. PPPoE 特殊オプション設定について .....	42
<b>第7章 ダイヤルアップ接続 .....</b>	<b>43</b>
. ダイヤルアップ回線の接続先設定 .....	44
. ダイヤルアップ回線の接続と切断 .....	46
. バックアップ回線接続 .....	48
. 回線への自動発信の防止について .....	49
<b>第8章 複数アカウント同時接続設定 .....</b>	<b>50</b>
複数アカウント同時接続の設定 .....	51
<b>第9章 各種サービスの設定 .....</b>	<b>56</b>
各種サービス設定 .....	57
<b>第10章 DNS リレー / キャッシュ機能 .....</b>	<b>58</b>
DNS 機能の設定 .....	59
<b>第11章 DHCP サーバ / リレー機能 .....</b>	<b>60</b>
. XR-430 の DHCP 関連機能について .....	61
. DHCP サーバ機能の設定 .....	62
. IP アドレス固定割り当て設定 .....	64
<b>第12章 IPsec 機能 .....</b>	<b>65</b>
. XR-430 の IPsec 機能について .....	66
. IPsec 設定の流れ .....	67
. IPsec 設定 .....	68
. IPsec Keep-Alive 機能 .....	76
. 「X.509 デジタル証明書」を用いた電子認証 .....	80

. IPsec 通信時のパケットフィルタ設定 .....	82
. IPsec がつながらないとき .....	83
<b>第 13 章 UPnP 機能 .....</b>	<b>86</b>
. UPnP 機能の設定 .....	87
. UPnP とパケットフィルタ設定 .....	89
<b>第 14 章 ダイナミックルーティング(RIP と OSPF の設定) .....</b>	<b>90</b>
. ダイナミックルーティング機能 .....	91
. RIP の設定 .....	92
. OSPF の設定 .....	94
<b>第 15 章 L2TPv3 機能 .....</b>	<b>101</b>
. L2TPv3 機能概要 .....	102
. L2TPv3 機能設定 .....	103
. L2TPv3 Tunnel 設定 .....	105
. L2TPv3 Xconnect(クロスコネクト)設定 .....	107
. L2TPv3 Group 設定 .....	109
. Layer2 Redundancy 設定 .....	110
. L2TPv3 Filter 設定 .....	112
. 起動 / 停止設定 .....	113
. L2TPv3 ステータス表示 .....	115
. 制御メッセージ一覧 .....	116
. L2TPv3 設定例 1(2拠点間の L2TP トンネル) .....	117
. L2TPv3 設定例 2 (L2TP トンネル二重化) .....	121
<b>第 16 章 L2TPv3 フィルタ機能 .....</b>	<b>129</b>
. L2TPv3 フィルタ 機能概要 .....	130
. 設定順序について .....	133
. 機能設定 .....	134
. L2TPv3 Filter 設定 .....	135
. Root Filter 設定 .....	137
. Layer2 ACL 設定 .....	139
. IPv4 Extend ACL 設定 .....	141
. ARP Extend ACL 設定 .....	143
. 802.1Q Extend ACL 設定 .....	144
. 802.3 Extend ACL 設定 .....	146
. 情報表示 .....	147
<b>第 17 章 SYSLOG 機能 .....</b>	<b>149</b>
syslog 機能の設定 .....	150
<b>第 18 章 攻撃検出機能 .....</b>	<b>152</b>
攻撃検出機能の設定 .....	153
<b>第 19 章 SNMP エージェント機能 .....</b>	<b>154</b>
SNMP エージェント機能の設定 .....	155
<b>第 20 章 NTP サービス .....</b>	<b>157</b>
NTP サービスの設定方法 .....	158
<b>第 21 章 VRRP 機能 .....</b>	<b>160</b>
. VRRP の設定方法 .....	161
. VRRP の設定例 .....	162
<b>第 22 章 アクセスサーバ機能 .....</b>	<b>163</b>
. アクセスサーバ機能について .....	164
. アクセスサーバ機能の設定 .....	165

<b>第23章 スタティックルーティング</b>	166
スタティックルーティング設定	167
<b>第24章 ソースルーティング</b>	169
ソースルーティング設定	170
<b>第25章 NAT 機能</b>	172
XR-430 の NAT 機能について	173
バーチャルサーバ設定	174
送信元 NAT 設定	175
バーチャルサーバの設定例	176
送信元 NAT の設定例	179
補足：ポート番号について	180
<b>第26章 パケットフィルタリング機能</b>	181
機能の概要	182
XR-430 のフィルタリング機能について	183
パケットフィルタリングの設定	184
パケットフィルタリングの設定例	187
外部から設定画面にアクセスさせる設定	193
補足：NAT とフィルタの処理順序について	194
補足：ポート番号について	195
補足：フィルタのログ出力内容について	196
<b>第27章 ネットワークイベント機能</b>	197
機能の概要	198
各トリガーテーブルの設定	200
実行イベントテーブルの設定	204
実行イベントのオプション設定	206
ステータスの表示	208
<b>第28章 仮想インターフェース機能</b>	209
仮想インターフェースの設定	210
<b>第29章 GRE 機能</b>	211
GRE の設定	212
<b>第30章 パケット分類設定</b>	214
XR-430 のパケット分類設定について	215
パケット分類設定の設定	216
ステータスの表示	217
ステータス情報の表示例	218
TOS について	219
DSCP について	221
<b>第31章 Web 認証機能</b>	222
Web 認証機能の設定	223
Web 認証下のアクセス方法	229
Web 認証の制御方法について	230
<b>第32章 ネットワークテスト</b>	231
ネットワークテスト	232
<b>第33章 各種システム設定</b>	236
各種システム設定	237
時計の設定	237
ログの表示	238
ログの削除	238

パスワードの設定 .....	239
ファームウェアのアップデート .....	240
設定の保存と復帰 .....	242
設定のリセット .....	243
再起動 .....	243
セッションライフタイムの設定 .....	244
設定画面の設定 .....	245
ARP filter 設定 .....	245
メール送信機能の設定 .....	246
モバイル通信インターフェース一覧 .....	249
外部ストレージ管理 .....	251
<b>第 34 章 情報表示 .....</b>	<b>253</b>
本体情報の表示 .....	254
<b>第 35 章 テクニカルサポート .....</b>	<b>255</b>
テクニカルサポート .....	256
<b>第 36 章 運用管理設定 .....</b>	<b>257</b>
INIT ボタンの操作 .....	258
<b>付録 A インタフェース名一覧 .....</b>	<b>259</b>
<b>付録 B 工場出荷設定一覧 .....</b>	<b>261</b>
<b>付録 C サポートについて .....</b>	<b>263</b>

# はじめに

## ご注意

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

## 商標の表示

「FutureNet」はセンチュリー・システムズ株式会社の商標です。

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

Microsoft、Windows、Windows XP、Windows Vista

下記製品名等は米国 Apple Inc. の登録商標です。

Macintosh、Mac OS X

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

# ご使用にあたって

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

## 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になっています。内容をよく理解してから本文をお読みください。

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



### 危険

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



### 警告

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



### 注意

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

次の絵表示の区分は、お守りいただく内容を説明しています。



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



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

## !**危険**



必ず本体に付属している電源ケーブルをご使用ください。



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



ストーブのそばなど高温の場所で使用したり、放置しないでください。



火の中に投入したり、加熱したりしないでください。



製品の隙間から針金などの異物を挿入しないでください。

## ご使用にあたって

### ⚠ 警告

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

## パッケージの内容物の確認

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

万が一不足がありましたら、お買い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。

### < XR-430 梱包物 >

XR-430本体	1台
はじめにお読みください	1部
安全にお使いいただくために	1部
UTPケーブル（ストレート、1m）	1本
ACアダプタ	1個
海外使用禁止シート	1部
保証書	1部
ゴム足	4個
CFスロット塞ぎシール（台紙1枚）	2枚
ナイロンクリップ（ACアダプタ固定用）	1個
小ネジ（ACアダプタ固定用）	1個

# 第1章

---

---

XR-430 の概要

### . XR-430 の特長

**XR-430 (以下、XR-430 または、本装置) には、以下の特徴があります。**

高速ネットワーク環境に余裕で対応

Ethernet インタフェースは全て 10base-T/100Base-TX となっており、高速 ADSL や FTTH 等の高速インターネット接続や LAN 環境の構成に充分な性能と機能を備えています。

PPPoE クライアント機能

XR-430 は PPPoE クライアント機能を搭載していますので、FTTH サービスや NTT 東日本 / 西日本などが提供するフレッツ ADSL・B フレッツサービスに対応しています。また、PPPoE の自動接続機能やリンク監視機能、IP アドレス変更通知機能を搭載しています。

unnumbered 接続対応

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

DHCP クライアント / サーバ機能

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

NAT / IP マスカレード機能

IP マスカレード機能を搭載していることにより、グローバルアドレスが 1 つだけしか利用できない場合でも、複数のコンピュータから同時にインターネットに接続できます。

また、静的 NAT 設定によるバーチャルサーバ機能を使えば、プライベート LAN 上のサーバをインターネットに公開することができます。さらに、複数のグローバルアドレスを NAT で設定できます。

ステートフルパケットインスペクション機能

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

静的パケットフィルタリング機能

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

IPsec 通信

IPsec を使うと、通信相手の認証と通信の暗号化により簡単に VPN(Virtual Private Network) を実現できます。WAN 上の IPsec サーバと 1 対 n で通信が可能です。最大対地数は 64 です。

また、公開鍵の作成から IPsec 用の設定、通信の開始 / 停止まで、ブラウザ上で簡単におこなうことができます。

UPnP 機能

UPnP(ユニバーサル・プラグアンドプレイ)機能に対応しています。

## 第1章 XR-430 の概要

### . XR-430 の特長

#### GRE トンネリング機能

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

#### ダイナミックルーティング機能

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

#### ソースルート機能

送信元アドレスによってルーティングをおこなうソースルーティングが可能です。

#### 多彩な冗長化構成が実現可能

VRRP による機器冗長機能だけでなく、インターフェース状態や Ping によるインターネット VPN のエンド～エンドの監視を実現し、ネットワークの障害時にブロードバンド回線やワイヤレス回線を用いてバックアップする機能を搭載しています。

#### 攻撃検出機能

定められたルールに則り不正アクセスを検出します。監視対象は、ホスト単位・ネットワーク単位で設定できます。攻撃検出した場合にはログを記録します。

#### Web 認証機能

XR-430 をインターネットゲートウェイとして運用するときに、インターネットへアクセスするための認証をおこなう機能を搭載しています。パスワード認証によって外部への不正なアクセスを制限することができます。

#### ログ機能

XR-430 のログを取得する事ができ、ブラウザ上でログを確認することが可能です。

また攻撃検出設定をおこなえば、インターネットからの不正アクセスのログも併せてログに記録されます。

#### バックアップ機能

本体の設定内容を一括してファイルにバックアップすることができます。

また設定の復元も、ブラウザ上から簡単にできます。

#### ファームウェアアップデート

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

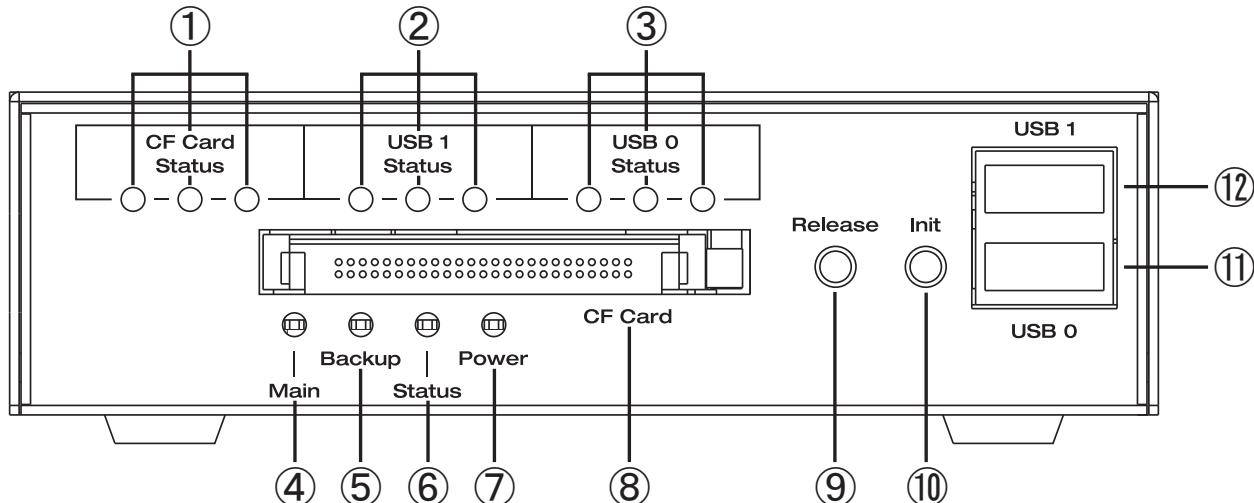
#### ワイヤレス通信対応

本装置に搭載された CF・USB のインターフェース（以下、モバイル通信インターフェース）に通信カードを装着すると、PPP 接続をワイヤレスで実現することができます。

また、着信可能なデータ通信カードを使用すれば、アクセスサーバとして利用することもできます。

## . 各部の名称と機能

## 製品前面



CF Card Status LED (緑)

USB 1 Status LED (緑)

USB 0 Status LED (緑)

CF タイプ・USB タイプのデータ通信モジュールの電波  
状態を 3 つの LED で以下のように表示します。

- ・未装着時 : ● ● ●
- ・未サポート : (点滅: 点灯4秒、消灯1秒)
- ・電波 圏外 : ● ● ●
- ・電波 (弱) : ● ● ●
- ・電波 (中) : ● ● ●
- ・電波 (強) : ● ● ●

Main LED (緑)

PPP/PPPoE 接続の状態を表示します。

- ・主回線接続
  - 接続時 : ●
  - 切断時 : ●
- ・マルチ接続(#2-4)
  - 接続時 : ●
  - 切断時 : ●
- ・主回線、マルチ接続の同時接続
  - 接続時 :
  - 切断時 : ●

Backup LED (緑)

バックアップ回線接続の状態を表示します。

- ・接続時 :
- ・切断時 : ●

Status LED (赤 / 緑)

ファームウェアのアップデート時: (同時点滅)

Power LED (緑)

本装置電源が投入されている状態 :

CF Card スロット

CF タイプのデータ通信モジュールまたは、CF メモリ  
カードを挿入します。

Release ボタン

本装置では使用しません。

Init ボタン

ボタンを押しながら電源を入れると、設定が工場出  
荷時状態で起動します。

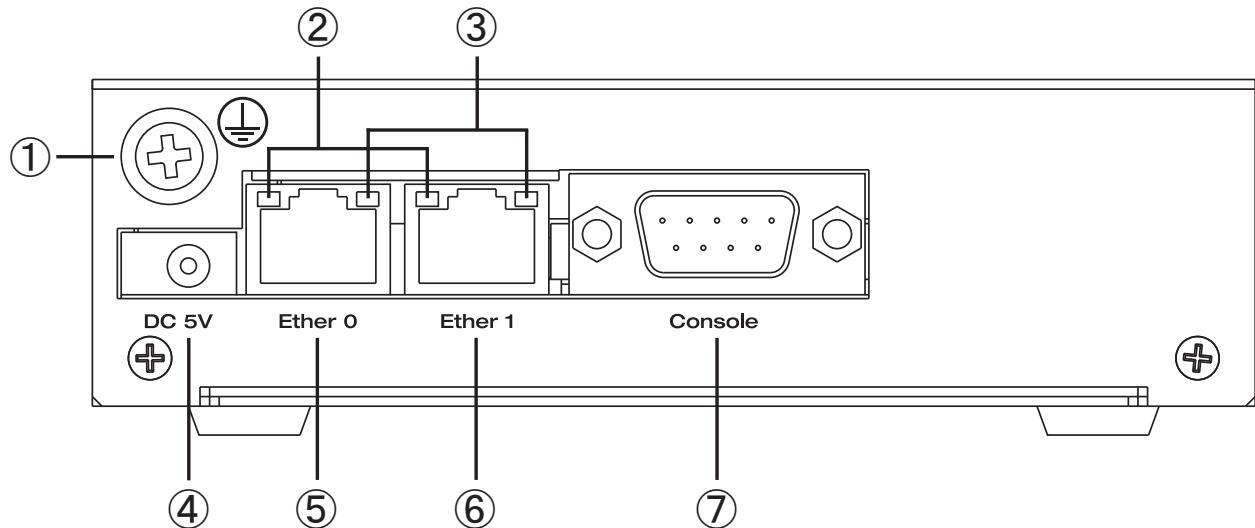
USB 0 ポート

USB 1 ポート

USB タイプのデータ通信モジュールまたは、USB メモ  
リスティックを挿入します。

## . 各部の名称と機能

### 製品背面



#### FG(アース)端子

保安用接地端子です。必ずアース線を接続してください。

#### Link/Active LED (緑)

Ethernet ポートの状態を表示します。

- ・ LAN ケーブルが正常に接続時 : ●
- ・ データ通信時 : - (点滅)

#### Speed LED (オレンジ)

Ethernet ポートの接続速度を表示します。

- ・ 10Base-T で接続時 : ●
- ・ 100BASE-TX で接続時 : ○

#### DC 5V 電源コネクタ

製品付属の AC アダプタを接続します。

#### Ether 0 ポート

#### Ether 1 ポート

10BASE-T/100BASE-TX 対応で、Ether0, Ether1 の 2 ポートが使用可能です。

Auto-MDI/MDIX にも対応しています。

各 Ethernet ポートの状態は、, の LED で表示します。

#### Console

弊社での保守管理用ポートです。使用できません。

### . 動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

#### ハードウェア環境

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

#### 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 Explorer5.0 以降か Netscape Navigator6.0 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

---

---

XR-430 の設置

## XR-430 の設置

本装置の各設置方法について説明します。

下記は設定に関する注意点です。よくご確認いただいてから設定してください。



注意！

本装置は直射日光が当たるところや、温度の高いところには設置しないようにしてください。

内部温度が上がり、動作が不安定になる場合があります。



注意！

ACアダプタのプラグを本体に差し込んだ後にACアダプタのケーブルを左右及び上下に引っ張らず、緩みがある状態にしてください。

抜き差しもケーブルを引っ張らず、コネクタを持っておこなってください。

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



注意！

XR-430 側でも各ポートで ARP table を管理しているため、PC を接続しているポートを変更するとその PC から通信ができない場合があります。このような場合は、XR-430 側の ARP table が更新されるまで(数秒～数十秒)通信できなくなりますが、故障ではありません。

## 第2章 XR-430 の設置

### XR-430 の設置

以下の手順で接続してください。

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

2

#### <有線接続の場合>

本装置の背面にあるEther1ポートとxDSL/ケーブルモデムやONUを、LANケーブルで接続してください。

#### <モバイル接続の場合>

CFタイプのデータ通信モジュールはCF Cardスロットに挿入してください。

USBタイプのデータ通信モジュールはUSB 0、USB 1ポートに挿入してください。

すべてのモバイル通信インターフェースを同時に使用することができますが、同一製品のモジュールを2つ同時に使用することはできません。

3 本装置の背面にあるEther0ポートとHUBやPCを、LANケーブルで接続してください。

**本装置の各EthernetポートはAuto-MDIX対応です。**

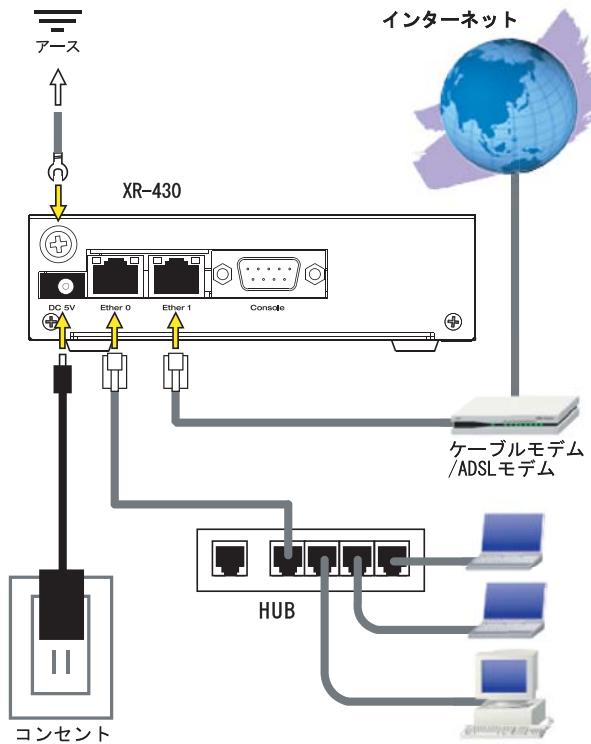
4 本装置とACアダプタ、ACアダプタとコンセントを接続してください。

5 全ての接続が完了しましたら、本装置と各機器の電源を投入してください。

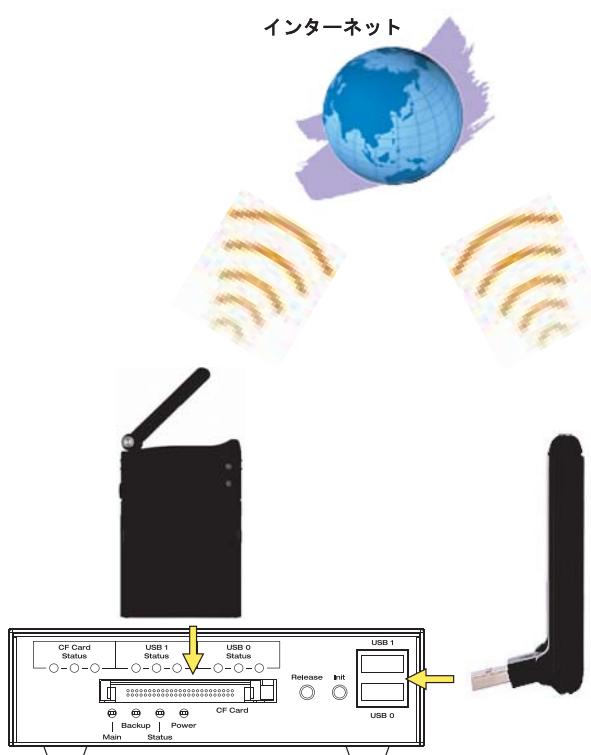
なお、モバイル接続の場合、本装置対応のデータ通信モジュールは以下のとおりです。

タイプ	提供元	型番	XR-430対応
USB	EMOBILE	D02HW	発信のみ
USB	NTT DoCoMo	A2502	発信のみ
CF	NTT DoCoMo	P2403	発着信
CF	NTT DoCoMo	N2502	発着信
CF	KDDI	W04K	発信のみ
CF	KDDI	W05K	発信のみ

#### 有線接続の場合の接続図(例)



#### モバイル接続の場合の接続図(例)



# 第3章

---

---

コンピュータのネットワーク設定

## 第3章 コンピュータのネットワーク設定

### . Windows XP のネットワーク設定

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

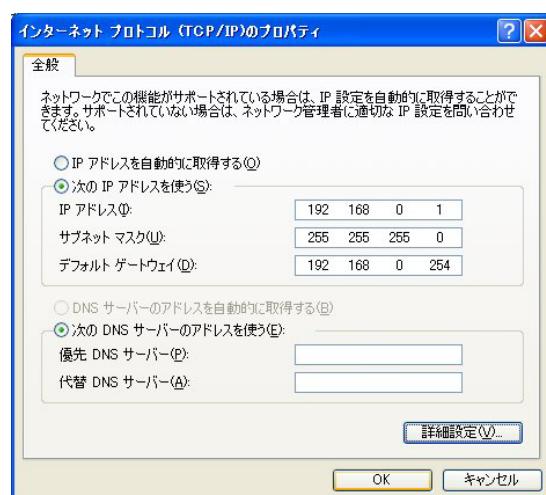
- 1 「コントロールパネル」 「ネットワーク接続」から、「ローカル接続」を開きます。
- 2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。



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



- 4 「インターネットプロトコル(TCP/IP)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。  
IPアドレス「192.168.0.1」  
サブネットマスク「255.255.255.0」  
デフォルトゲートウェイ「192.168.0.254」



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

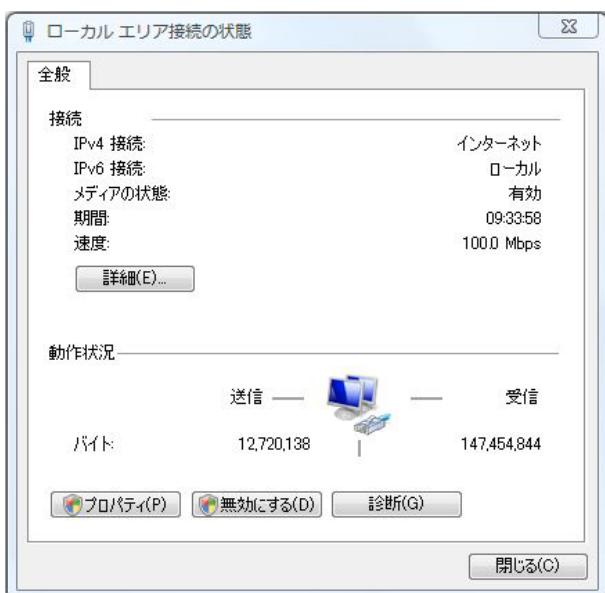
## 第3章 コンピュータのネットワーク設定

### . Windows Vistaのネットワーク設定

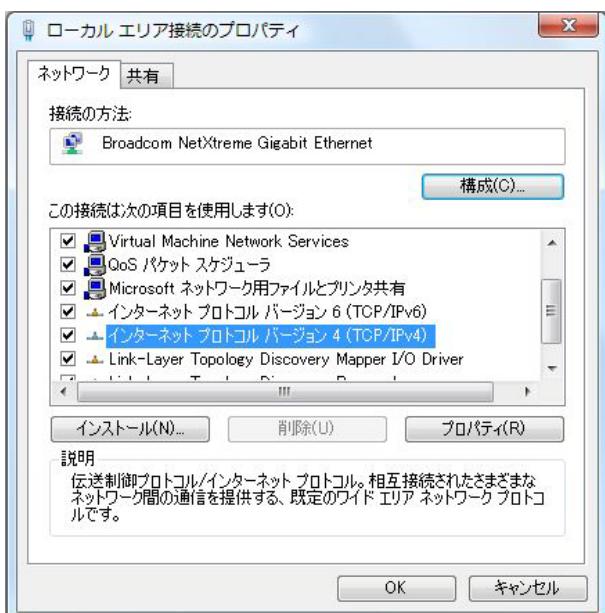
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

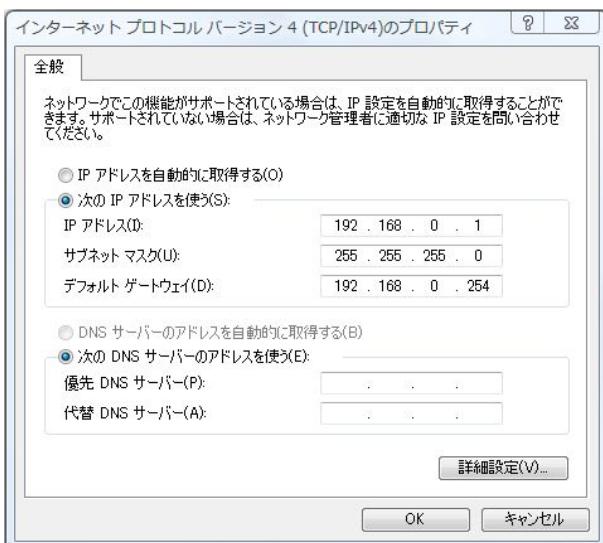


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



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

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



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

## 第3章 コンピュータのネットワーク設定

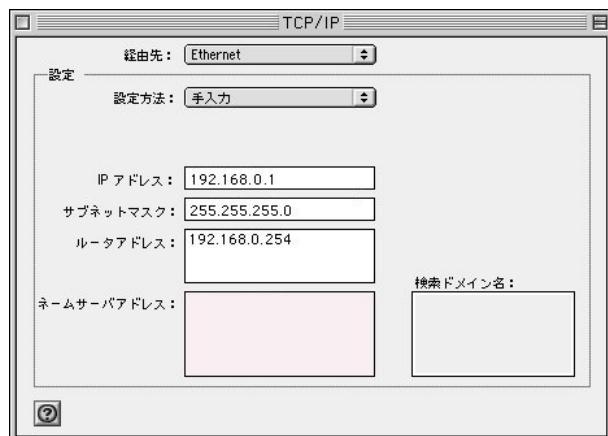
### . Macintosh のネットワーク設定

ここでは Macintosh のネットワーク設定について説明します。

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

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

IP アドレス 「192.168.0.1」  
サブネットマスク 「255.255.255.0」



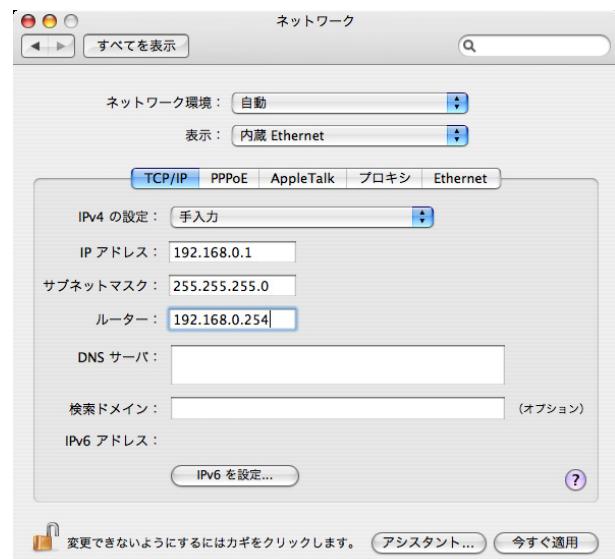
3 ウィンドウを閉じて設定を保存します。その後 Macintosh 本体を再起動してください。これで本装置へログインする準備が整いました。

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

### . IP アドレスの確認と再取得

#### Windows XP/Vista の場合

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

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

```
C:\>ipconfig /all
```

3 IP 設定のクリアと再取得をするには以下のコマンドを入力してください。

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

#### 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ではありませんので、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。

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

# 第4章

---

---

設定画面へのログイン

## 設定画面へのログイン方法

1 各種ブラウザを開きます。

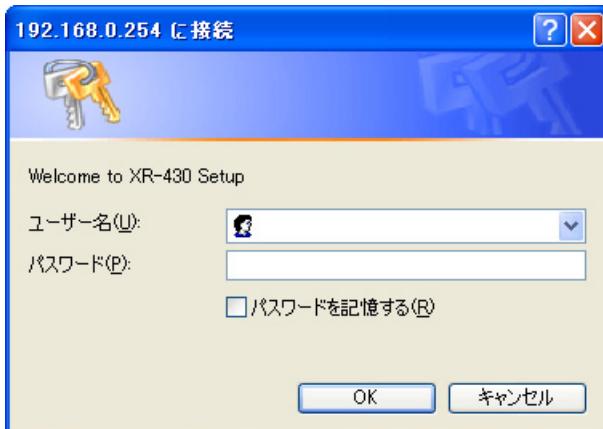
2 ブラウザから設定画面にアクセスします。  
ブラウザのアドレス欄に、以下のIPアドレスとポート番号を入力してください。



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

**設定画面のポート番号880は変更することができません。**

3 次のような認証ダイアログが表示されます。



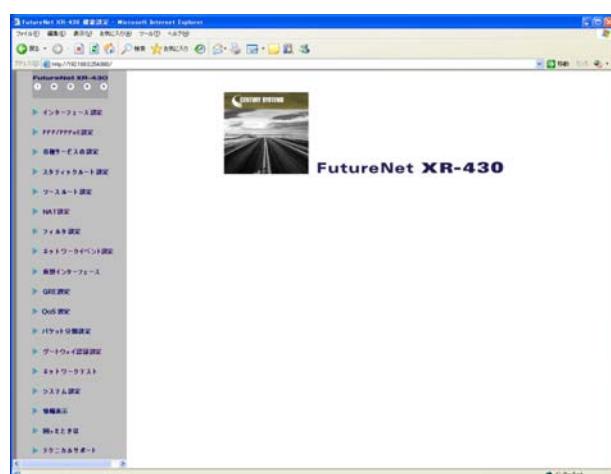
4 ダイアログ画面にパスワードを入力します。

工場出荷設定のユーザー名とパスワードはともに「admin」です。

ユーザー名・パスワードを変更している場合は、それにあわせてユーザー名・パスワードを入力します。



5 ブラウザ設定画面が表示されます。



# 第5章

---

---

インターフェース設定

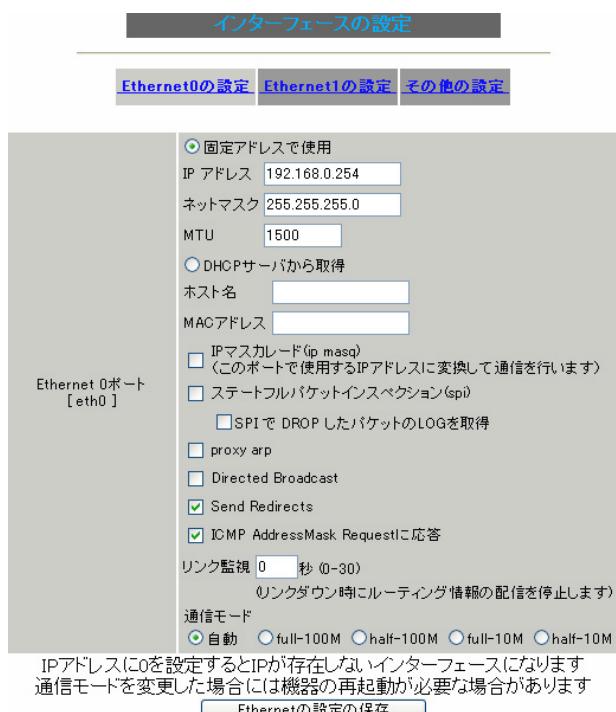
## 第5章 インターフェース設定

### . Ethernet ポートの設定

#### 各 Ethernet ポートの設定

Web 設定画面「インターフェース設定」

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



(画面は「Ethernet0 の設定」)

#### [ 固定アドレスで使用 ]

IP アドレス

ネットマスク

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

IP アドレスに “0” を設定すると、そのインターフェースは 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ーフェースの情報を配信したくないときなどに “0” を設定してください。

MTU

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

#### [ DHCP から取得 ]

ホスト名

MAC アドレス

IP アドレスを DHCP で割り当てる場合にチェックして、必要であればホスト名と MAC アドレスを設定します。

#### IP マスカレード ( ip masq )

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

#### ステートフルパケットインスペクション(spi)

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

#### SPI で DROP したパケットの LOG を取得

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

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

#### proxy arp

Proxy ARP を使う場合にチェックを入れます。

#### Directed Broadcast

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

#### ICMP Redirects

他に適切な経路があることを通知する ICMP パケットのことです。

## 第5章 インターフェース設定

### . Ethernet ポートの設定

#### ICMP AddressMask Request に応答

NW 監視装置によっては、LAN 内装置の監視を ICMP Address Mask の送受信によっておこなう場合があります。

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

#### リンク監視

Ethernet ポートのリンク状態の監視を定期的におこないます。

監視間隔は、1-30 秒の間で設定できます。また、0 秒で設定するとリンク監視をおこないません。  
OSPF の使用時にリンクのダウンを検知した場合、そのインターフェースに関連付けられたルーティング情報の配信を停止します。再度リンク状態がアップした場合には、そのインター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。

#### 通信モード

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

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

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

**本装置のインターフェースのアドレス変更は、直ちに設定が反映されます。**  
**設定画面にアクセスしているホストやその他クラウントの IP アドレス等も本装置の設定に合わせて変更し、変更後の IP アドレスで設定画面に再ログインしてください。**

## 第5章 インターフェース設定

### . Ethernet ポートの設定について

#### [ステートフルパケットインスペクション]

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

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

ステートフルパケットインスペクション機能を有効にすると、そのインターフェースへのアクセスは原則として一切不可能となります。ステートフルパケットインスペクション機能とバーチャルサーバ機能を同時に使う場合等は、パケットフィルタリングの設定をおこなって、外部からアクセスできるように設定する必要があります。

「第26章 パケットフィルタリング機能」を参照してください。

#### [PPPoE 接続時の Ethernet ポート設定]

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

XR-430 が PPPoE で接続する場合には “ppp” という論理インターフェースを自動的に生成し、この ppp 論理インターフェースを使って PPPoE 接続をおこなうためです。

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

#### [IPsec 通信時の Ethernet ポート設定]

XR-430 を IPsec ゲートウェイとして使う場合は、Ethernet ポートの設定に注意してください。

IPsec 通信をおこなう相手側のネットワークと同じネットワークのアドレスが XR-430 の Ethernet ポートに設定されていると、正常に IPsec 通信がおこなえません。

たとえば、IPsec 通信をおこなう相手側のネットワークが 192.168.1.0/24 で、且つ、XR-430 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-430 の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

## 第5章 インターフェース設定

### . VLAN タギングの設定

#### 各 802.1Q Tagged VLAN の設定

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

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

No.	dev.Tag ID	enable	IPアドレス	ネットマスク	MTU	ip masq	spi	drop log	proxy arp	icmp
1	eth0.1	<input checked="" type="checkbox"/>	192.168.10.254	255.255.255.0	1500	<input checked="" type="checkbox"/>				
2	eth0.2	<input checked="" type="checkbox"/>	192.168.11.254	255.255.255.0	1500	<input type="checkbox"/>				
3	eth0.3	<input checked="" type="checkbox"/>	192.168.12.254	255.255.255.0	1500	<input type="checkbox"/>				
4	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
5	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
6	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
7	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
8	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
9	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
10	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
11	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
12	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
13	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
14	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
15	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				
16	eth0.	<input type="checkbox"/>			1500	<input type="checkbox"/>				

VLANインターフェースの名称は[eth0.TagID]になります  
64個まで登録できます  
Tag ID(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並められます

VLANの設定の保存

(画面は「Ethernet0 の設定」の表示例です)

#### dev.Tag ID

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

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

#### enable

チェックを入れることで設定を有効にします。

#### IP アドレス

#### ネットマスク

VLAN インターフェースの IP アドレスとサブネットマスクを設定します。

#### MTU

VLAN インターフェースの MTU 値を設定します。

指定可能範囲 : 68-1500byte です。

初期設定値は 1500byte になります。

#### ip masq

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

#### drop log

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

#### proxy arp

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

#### icmp

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

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

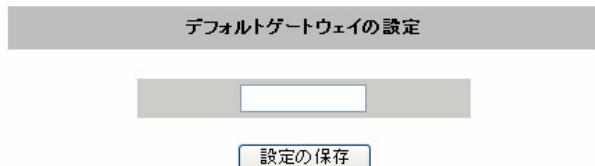
「802.1Q Tagged VLAN の設定」の「設定情報」リンクをクリックすると、現在の VLAN 設定情報が表示されます。

## 第5章 インターフェース設定

### . デフォルトゲートウェイの設定

#### デフォルトゲートウェイの設定

デフォルトゲートウェイの設定は、Web 設定画面  
「インターフェース設定」 「その他の設定」にあ  
る以下の画面から設定します。



#### デフォルトゲートウェイの設定

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。

# 第 6 章

---

---

PPPoE 設定

## . PPPoE の接続先設定

**接続先設定**

はじめに、接続先の設定( ISPのアカウント設定 )をおこないます。

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

設定は 5 つまで保存しておくことができます。

**PPP/PPPoE接続設定**

<b>接続設定</b>	<b>接続先設定1</b>	<b>接続先設定2</b>	<b>接続先設定3</b>	<b>接続先設定4</b>	<b>接続先設定5</b>
プロバイダ名					
ユーザID					
パスワード					
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 ブラウザ セカンダリ				
LCPキープアライブ	チェック間隔 30 秒 3回確認出来なくなると回線を切断します 0秒を入力するとこの機能は無効になります				
Pingによる接続確認	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する 使用するホスト				
発行間隔は30秒固定、空欄の時はPTP-Gatewayに発行します					
<b>Un Numbered-PPP回線使用時に設定できます</b>					
IPアドレス	回線接続時に割り付けるグローバルIPアドレスです				
<b>PPPoE回線使用時に設定して下さい</b>					
MSS設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 0 Byte <small>( 有効時にMSS値が0又は空の場合には、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。 )</small>				
<b>PPPモバイル回線使用時に設定して下さい</b>					
電話番号					
ダイアルタイムアウト	60 秒				
初期化用ATコマンド	ATQ0V1				
ON-DEMAND接続用切断タイマー	180 秒				
<b>マルチPPP/PPPoEセッション回線利用時に指定可能です</b>					
ネットワーク	接続するネットワークを指定して下さい				
ネットマスク	上記のネットワークのネットマスクを指定して下さい				
<b>設定の保存</b>					

**プロバイダ名**

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

**ユーザ ID**

プロバイダから指定されたユーザ ID を入力してください。

**パスワード**

プロバイダから指定された接続パスワードを入力してください。

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

**<例>**

abc(def)g' h      abc¥(def¥)g¥' h

**DNS サーバ**

特に指定のない場合は「プロバイダから自動割り当て」をチェックします。

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

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

**LCP キープアライブ**

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

“ 0 ” を指定すると、LCP キープアライブ機能は無効となります。

## 第6章 PPPoE 設定

### . PPPoE の接続先設定

#### Ping による接続確認

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

#### IP アドレス

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

#### MSS 設定

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

0 にすると最大 1414byte に自動調整します。  
特に必要のない限り、この機能を有効にして、かつ MSS 値を 0 にしておくことを推奨いたします  
(それ以外では正常にアクセスできなくなる場合があります)。  
また ADSL で接続中に MSS 設定を変更したときは、PPPoE セッションを切断後に再接続する必要があります。

#### 電話番号

ダイアルタイムアウト  
初期化用 AT コマンド  
ON-DEMAND 接続用切断タイマー

上記項目は、PPPoE 接続の場合は設定の必要はありません。

#### ネットワーク

#### ネットマスク

<例>

ネットワーク「172.26.0.0」

ネットマスク「255.255.0.0」

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

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

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

最後に「設定の保存」ボタンをクリックして、設定完了です。

設定はすぐに反映されます。

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

## 第6章 PPPoE 設定

### . PPPoE の接続設定と回線の接続と切断

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

#### 接続設定

PPP/PPPoE接続設定

接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
回線状態	主回線で接続しています				
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	指定ポート: USB0 [ 指定可能な接続ポート ]				
接続形態	<input type="radio"/> 手動接続 <input checked="" type="radio"/> 常時接続				
モバイル通信接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続				
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得				
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				

#### 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

プルダウンメニューに現在有効なポートが表示されますので、リストの中から選択してください。

既に設定済の場合には「接続ポート:( 設定されている接続ポート名 )」が表示されます。



( 画面は表示例です )

#### 接続形態

「手動接続」

PPPoE(PPP)の接続 / 切断を手動で切り替えます。同画面最下部のボタンで「接続」「切断」の操作をおこなってください。

#### 「常時接続」

本装置が起動すると自動的に PPPoE 接続を開始します。

#### モバイル通信接続タイプ

無線モジュールを使って主回線接続するときの接続タイプを選択します。

「通常」を選択すると常時接続となります。

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

#### IP マスカレード

PPPoE 接続時に IP マスカレードを有効にするかどうかを選択します。

#### ステートフルパケットインスペクション

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

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

#### デフォルトルートの設定

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

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

**通常は「有効」設定にしておきます。**

#### ICMP AddressMask Request

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

### . PPPoE の接続設定と回線の接続と切断

最後に「設定の保存」ボタンをクリックして、設定完了です。

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

#### 接続 IP 変更お知らせメール機能

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

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

< PPPoE お知らせメール送信 >

PPPoE お知らせメール送信	
お知らせメール送信	<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	admin@localhost
件名	Changed IP/PPPoE

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

## 第6章 PPPoE 設定

### . PPPoE の接続設定と回線の接続と切断

#### syslogへの出力について

本装置で、モバイル通信インターフェースを使用して PPP 接続をおこなった場合、接続時と切断時の電波状態をログへ出力します。

出力形式は以下のとおりです。

##### ・接続時

ppp\_mobile\_on: キャリア名:通信カード名/Antenna Level(アンテナレベル)

##### ・切断時

ppp\_mobile\_off: キャリア名:通信カード名/Antenna Level(アンテナレベル)

##### ・通信カード未装着時

ppp\_mobile\_on: Unplugged/Antenna Level(アンテナレベル)

##### ・未サポートのカード装着時

ppp\_mobile\_on: Not available/Antenna Level(アンテナレベル)

ppp\_mobile\_off: Not available/Antenna Level(アンテナレベル)

##### ・圏外状態の時

ppp\_mobile\_on: キャリア名:通信カード名/No service(アンテナレベル)

圏外の場合、発信 (pppd起動) はおこないません。

なお、アンテナレベル部分の表示形式は以下のとおりです。

- ・ -1 : 電波状態取得未サポート
- ・ 0 : 圏外 / 未装着
- ・ 1 : 弱
- ・ 2 : 中
- ・ 3 : 強

#### PPP接続障害時のリカバリ機能について

PPP接続開始時に電波状態が [ 圏外 ] であった場合、圏外である旨をシステムログへ出力しますが、接続はおこないません。

ただし、接続開始時は圏内だったが、実際の接続発呼時に圏外となった状態で、ATコマンドの発行を繰り返すと、通信カードがハングアップする場合があるため、chatプログラムによるATコマンド発行直前にも電波状態を検査し、圏外の場合は処理を継続しません。

#### < ワイヤレスでの PPP 接続時のログ出力例 >

```
Jun 3 10:38:06 localhost pppd[8460]: e-mobile:D02HW/Antenna Level(3) ※接続時電波状態
Jun 3 10:38:06 localhost pppd[8460]: pppd 2.4.2 started by root, uid 0
Jun 3 10:38:07 localhost chat[8461]: timeout set to 60 seconds
Jun 3 10:38:07 localhost chat[8461]: abort on (BUSY)
Jun 3 10:38:07 localhost chat[8461]: abort on (ERROR)
Jun 3 10:38:07 localhost chat[8461]: abort on (NO CARRIER)
Jun 3 10:38:07 localhost chat[8461]: abort on (NO DIALTONE)
Jun 3 10:38:07 localhost chat[8461]: send (ATZ^M)
Jun 3 10:38:07 localhost chat[8461]: expect (OK)
Jun 3 10:38:07 localhost chat[8461]: ^M
Jun 3 10:38:07 localhost chat[8461]: OK
Jun 3 10:38:07 localhost chat[8461]: -- got it
Jun 3 10:38:07 localhost chat[8461]: send (ATQ0V1^M)
Jun 3 10:38:07 localhost chat[8461]: expect (OK)
Jun 3 10:38:07 localhost chat[8461]: ^M
Jun 3 10:38:07 localhost chat[8461]: T01^M^M
Jun 3 10:38:07 localhost chat[8461]: OK
Jun 3 10:38:07 localhost chat[8461]: -- got it
Jun 3 10:38:07 localhost chat[8461]: send (ATD*99***1#^M)
Jun 3 10:38:07 localhost chat[8461]: expect (CONNECT)
Jun 3 10:38:07 localhost chat[8461]: ^M
Jun 3 10:38:07 localhost chat[8461]: ATD*99***1#^M^M
Jun 3 10:38:07 localhost chat[8461]: CONNECT
Jun 3 10:38:07 localhost chat[8461]: -- got it
Jun 3 10:38:07 localhost pppd[8460]: Serial connection established.
Jun 3 10:38:07 localhost pppd[8460]: Using interface ppp0
Jun 3 10:38:07 localhost pppd[8460]: Connect: ppp0 <-> /dev/ttym0
                                         (PPP 接続中)

Jun 3 10:40:54 localhost dialup_proc[4519]: count: 2, event: alldown, mode: NULL
Jun 3 10:40:54 localhost pppd[8460]: e-mobile:D02HW/Antenna Level(3) ※切断時電波状態
Jun 3 10:40:55 localhost pppd[8460]: Terminating on signal 2.
Jun 3 10:40:55 localhost pppd[8460]: Connection terminated.
```

## 第6章 PPPoE 設定

### . バックアップ回線接続設定

PPPoE 接続では、「バックアップ回線接続」設定のおこなえます。

#### [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 を用います。

#### バックアップ回線設定

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

PPP/PPPoE接続設定

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	指定ポート: <b>None</b> 指定可能な接続ポート
モバイル通信接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続
IPマスカレード	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ステートフルパケットインスペクション	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 <input type="checkbox"/> DROP したパケットのLOGを取得
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する
主回線接続確認のインターバル	30 秒
主回線の回線断の確認方法	<input checked="" type="radio"/> PING <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

#### 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

プルダウンメニューに現在有効なポートが表示されますので、リストの中から選択してください。既に設定済の場合は「接続ポート:(設定されている接続ポート名)」が表示されます。

接続ポート	指定ポート: <b>USB0</b> 指定可能な接続ポート
	<input type="checkbox"/> 指定可能な接続ポート USB0 (A2502) CF (FOMA P2403) Ether0 Ether1

### . バックアップ回線接続設定

#### モバイル通信接続タイプ

無線モジュールを使ってバックアップ回線接続するときの接続タイプを選択します。  
「通常」を選択すると常時接続となります。  
「On-Demand 接続」を選択するとオンデマンド接続となります。オンデマンド接続における切断タイマーは「接続先設定」で設定します。

#### IPマスカレード

バックアップ回線接続時の IP マスカレードの動作を選択します。

#### ステートフルパケットインスペクション

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

#### ICMP AddressMask Request

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

#### 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。30 ~ 999(秒)の間で設定できます。

#### 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、「IPSEC+PING」は IPSEC 上での ping により、回線の切断を確認します。

#### Ping 使用時の宛先アドレス

回線断の確認方法で「PING」「IPSEC+PING」を選択したときの、ping パケットのあて先 IP アドレスを設定します。

ここから ping の Reply が帰ってこなかった場合に、バックアップ回線接続に切り替わります。

#### Ping 使用時の送信元アドレス

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

#### Ping fail 時のリトライ回数

ping のリプライがないときに何回リトライするかを指定します。

#### Ping 使用時の device

ping を使用する際の、ping を発行する回線(インターフェース)を選択します。

「その他」を選択して、インターフェース名を直接指定もできます。

<例>

主回線上の IPsec インタフェースは“ ipsec0 ”です。

#### IPSEC + PING 使用時の IPSEC ポリシーの NO

IPSEC+PING で回線断を確認するときは必ず、使用する IPsec ポリシーの設定番号を指定します。

IPsec 設定については「第 12 章 IPsec 設定」や IPsec 設定ガイドをご覧ください。

#### 復旧時のバックアップ回線の強制切断

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

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

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

### . バックアップ回線接続設定

#### **接続お知らせメール機能**

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

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

< PPPoE Backup 回線のお知らせメール送信 >

PPPoE Backup回線のお知らせメール送信	
お知らせメール送信	<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	admin@localhost
件名	Started Backup connection

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

## 第6章 PPPoE 設定

### . PPPoE 特殊オプション設定について

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

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

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

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

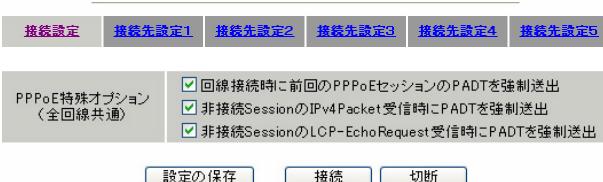
PADT = PPPoE Active Discovery Terminate の略。

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

#### PPPoE 特殊オプション設定

PPP/PPPoE 設定「接続設定」画面の最下部で設定します。

PPP/PPPoE 接続設定



設定の有効化には回線の再接続が必要です

回線接続時に前回の PPPoE セッションの PADT を強制送出する。

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

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

#### の動作について

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

#### 、 の動作について

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

- IPv4 パケット
- LCP エコーリクエスト

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

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

地域 IP 網の工事後に PPPoE 接続ができな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

---

---

ダイヤルアップ接続

## 第7章 ダイヤルアップ接続

### . ダイヤルアップ回線の接続先設定

XR-430 の PPP 接続機能を使う事で、モバイル通信インターフェース経由でダイヤルアップが可能となります。

PPP(ダイヤルアップ)接続の接続先設定をおこないます。

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

設定は5つまで保存しておくことができます。

**PPP/PPPoE接続設定**

接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
プロバイダ名					
ユーザID					
パスワード					
DNSサーバ	<input type="radio"/> 割り当てられたDNSを使わない <input checked="" type="radio"/> プロバイダから自動割り当て <input type="radio"/> 手動で設定 プライマリ <input type="text"/> セカンダリ <input type="text"/>				
LCPキープアライブ	チェック間隔 <input type="text"/> 秒 3回確認出来なくなると回線を切断します。 0秒を入力するとこの機能は無効になります				
Pingによる接続確認	<input type="radio"/> 使用しない <input checked="" type="radio"/> 使用する 使用するホスト <input type="text"/> 発行間隔は30秒固定、空欄の時はPnP-Gatewayに発行します				
<b>Un Numbered-PPP回線使用時に設定できます</b>					
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				
<b>PPPoE回線使用時に設定して下さい</b>					
MSS設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効(奨励) MSS値 <input type="text"/> Byte (有効時にMSS値が0又は空の場合には、 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。)				
<b>PPPモバイル回線使用時に設定して下さい</b>					
電話番号	<input type="text"/>				
ダイアルタイムアウト	60 秒				
初期化用ATコマンド	ATQ0V1				
ON-DEMAND接続用 切断タイマー	180 秒				
<b>マルチPPP/PPPoEセッション回線利用時に指定可能です</b>					
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				
<b>設定の保存</b>					

( 画面は「接続先設定 1 」 )

## 第7章 ダイヤルアップ接続

### . ダイヤルアップ回線の接続先設定

#### プロバイダ名

接続するプロバイダ名を入力します。  
半角英数字のみですが、任意に設定できます。

#### ユーザ ID

プロバイダから指定されたユーザ IDを入力してください。

#### パスワード

プロバイダから指定された接続パスワードを入力してください。

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

<例> abc(def)g ' h abc¥(def¥)g¥ ' h

#### DNS サーバ

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

#### LCP キープアライブ

#### ping による接続確認

#### IP アドレス

#### MSS 設定

上記項目は、ダイヤルアップ接続の場合は設定の必要はありません。

#### 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。

#### ダイアルタイムアウト

アクセス先にログインするときのタイムアウト時間を設定します。単位は秒です。

#### 初期化用 AT コマンド

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

#### ON-DEMAND 接続用切断タイマー

PPP接続設定のモバイル通信接続タイプを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。

#### ネットワーク

#### ネットマスク

<例>

ネットワーク「172.26.0.0」

ネットマスク「255.255.0.0」

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

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

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

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

続いて PPP の接続設定をおこないます。

## 第7章 ダイヤルアップ接続

### . ダイヤルアップ回線の接続と切断

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

PPP/PPPoE接続設定

接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
回線状態	主回線で接続しています				
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	指定ポート: USB0 <input type="button" value="指定可能な接続ポート"/>				
接続形態	<input type="radio"/> 手動接続 <input checked="" type="radio"/> 常時接続				
モバイル通信接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続				
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得				
デフォルトルートの設定	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				

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  
プルダウンメニューに現在有効なポートが表示されますので、リストの中から選択してください。  
既に設定済の場合は「接続ポート:(設定されている接続ポート名)」が表示されます。  
ダイヤルアップ接続ではモバイル通信インターフェースを選択します。



(画面は表示例です)

モバイル通信インターフェースでの接続設定後に通信カードを差替えた場合は、再設定が必要です。

#### 接続形態

##### 「手動接続」

ダイヤルアップの接続/切断を手動で切り替えます。同画面最下部のボタンで「接続」「切断」の操作をおこなってください。

##### 「常時接続」

本装置が起動すると自動的にダイヤルアップ接続を開始します。

#### モバイル通信接続タイプ

無線モジュールでダイヤルアップ接続をおこなう時の接続タイプを選択します。

「通常」接続時は、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

ダイヤルアップ接続時に IPマスカレードを有効にするかどうかを選択します。unnumbered 接続時以外は、「有効」を選択してください。

#### ステートフルパケットインスペクション

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

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

## 第7章 ダイヤルアップ接続

### . ダイヤルアップ回線の接続と切断

#### デフォルトルートの設定

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

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

特に必要のない限り「有効」設定にしておきます。

#### ICMP AddressMask Request

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

最後に「設定の保存」ボタンをクリックして、設定完了です。

この後は画面最下部の「接続」「切断」ボタンで回線の接続を制御してください。

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

### . バックアップ回線接続

ダイヤルアップ接続についても、PPPoE 接続と同様に、

- ・PPPoE お知らせメール送信

および

- ・バックアップ回線接続設定

が可能です。

設定方法については、

「**第6章 PPPoE 設定**」の各ページをご参照ください。

「 . PPPoE の接続設定と回線の接続と切断」

「 . バックアップ回線接続設定」

## 第7章 ダイヤルアップ接続

### . 回線への自動発信の防止について

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

そのため「On-Demand 接続」機能を使っている場合には、ダイヤルアップ回線に自動接続してしまう問題が起こります。

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

(入力フィルタ)

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

(転送フィルタ)

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

# 第8章

---

---

複数アカウント同時接続設定

## 第8章 複数アカウント同時接続設定

### 複数アカウント同時接続の設定

XR-430 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(ダイヤルアップ)を同時におこなう

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

この接続形態は「マルチ PPPoE セッション」と呼ばれることもあります。

XR-430 のマルチ PPPoE セッション機能は、主回線 1 セッションと、マルチ接続 3 セッションの合計 4 セッションまでの同時接続をサポートしています。なお、以下の項目については主回線では設定できますが、マルチ接続 (#2 ~ #4) では設定できませんので、ご注意ください。

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

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

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

また XR-430 のマルチ PPPoE セッション機能は、PPPoE で接続しているすべてのインターフェースがルーティングの対象となります。

したがいまして、それぞれのインターフェースにステートフルパケットインスペクション、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ので、工場出荷設定ではステートフルパケットインスペクションは無効となっています。必要に応じてステートフルパケットインスペクション等の設定をして使用してください。

この機能を利用する場合は以下のステップに従って設定してください。

## 複数アカウント同時接続の設定

### STEP 1 主接続の接続先設定

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

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

### STEP 2 マルチ接続用の接続先設定

マルチ接続(同時接続)用の接続先設定をおこないます。

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

PPP/PPPoE接続設定					
接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
マルチPPP/PPPoEセッション回線利用時に指定可能です					
ネットワーク					
接続するネットワークを指定して下さい					
ネットマスク					
上記のネットワークのネットマスクを指定して下さい					

ネットワーク

ネットマスク

<例>

ネットワーク「172.26.0.0」

ネットマスク「255.255.0.0」

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

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

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

最後に「設定の保存」をクリックして接続先設定は完了です。

## 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 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。  
「PPPoE/PPPoE 設定」 「接続設定」を開きます。

#### [主接続用の接続設定]

以下の部分で設定します。

PPP/PPPoE接続設定

接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
回線状態	主回線で接続しています				
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	指定ポート: USB0 [ 指定可能な接続ポート ]				
接続形態	<input type="radio"/> 手動接続 <input checked="" type="radio"/> 常時接続				
モバイル通信接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続				
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ステートフルパケットインスペクション	<input 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				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				

#### 回線状態

現在の回線状態を表示します。

#### 接続先の選択

主接続用の設定を選択します。

#### 接続ポート

主回線で使用する本装置のインターフェースをプルダウンメニューのリストから選択してください。  
既に設定済の場合は「接続ポート:( 設定されている接続ポート名 )」が表示されます。

接続ポート 指定ポート: USB0 [ 指定可能な接続ポート ]

USB0 ( A2502 )
CF ( FOMA P2403 )
Ether0
Ether1

( 画面は表示例です )

#### 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。

#### モバイル通信接続タイプ

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

#### IPマスカレード

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

#### ステートフルパケットインスペクション

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

#### デフォルトルートの設定

「有効」を選択します。

#### ICMP AddressMask Request

任意で選択します。

#### PPPoE お知らせメール送信

「システム設定」「メール送信機能の設定」にある<PPPoE お知らせメール送信>を任意で設定します。

設定方法については「第33章 各種システム設定」をご覧ください。

続いて、マルチ接続用の接続設定をおこないます。

## 第8章 複数アカウント同時接続設定

### 複数アカウント同時接続の設定

#### [マルチ接続用の設定]

以下の部分で設定します。

PPP/PPPoE接続設定

接続設定	接続先設定1	接続先設定2	接続先設定3	接続先設定4	接続先設定5
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 type="radio"/> 無効 <input checked="" 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	指定ポート: USB1 指定可能な接続ポート ▾				
モバイル通信接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続				
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				
マルチ接続 #3	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効				
接続先の選択	<input checked="" type="radio"/> 接続先1 <input type="radio"/> 接続先2 <input type="radio"/> 接続先3 <input type="radio"/> 接続先4 <input type="radio"/> 接続先5				
接続ポート	指定ポート: USB1 指定可能な接続ポート ▾				
モバイル通信接続タイプ	<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 type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				
マルチ接続 #4	<input type="radio"/> 無効 <input checked="" 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	指定ポート: USB1 指定可能な接続ポート ▾				
モバイル通信接続タイプ	<input checked="" type="radio"/> 通常 <input type="radio"/> On-Demand接続				
IPマスカレード	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効				
ステートフルパケットインスペクション	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効 <input type="checkbox"/> DROPしたパケットのLOGを取得				
ICMP AddressMask Request	<input type="radio"/> 応答しない <input checked="" type="radio"/> 応答する				

#### マルチ接続 #2 ~ #4

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

#### 接続先の選択

マルチ接続用の接続先設定を選択します。

#### 接続ポート

マルチ接続で使用する、本装置のインターフェースをプルダウンメニューのリストから選択してください。既に設定済の場合は「接続ポート:(設定されている接続ポート名)」が表示されます。

Bフレッシュ回線で複数の同時接続をおこなう場合は、主接続の設定と同じインターフェースを選択します。



(画面は表示例です)

#### モバイル通信接続タイプ

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

#### IPマスカレード

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

#### ステートフルパケットインスペクション

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

#### ICMP AddressMask Request

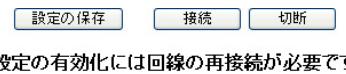
任意で選択します。

マルチ接続設定は3つまで設定可能です。  
最大4セッションの同時接続が可能です。

### 複数アカウント同時接続の設定

#### STEP 4 PPPoE 接続の開始

すべて設定した後、「接続」をクリックして PPPoE 接続を開始します。



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

接続に成功した場合：

**主回線で接続しています。  
マルチセッション回線1で接続しています。**

接続できていない場合：

**主回線で接続を試みています。  
マルチセッション回線1で接続を試みています。**  
などと表示されます。

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

#### 複数アカウント同時接続時の注意点

通常の ISP とフレッツスクエアへの同時接続をするには、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

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

現在のサービス稼働状況を反映しています 各種設定はサービス項目名をクリックして下さい			
DNSキャッシュ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	<a href="#">動作変更</a>
DHCP(Relay)サーバ	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	<a href="#">動作変更</a>
IPsecサーバ	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	<a href="#">動作変更</a>
UPnPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	<a href="#">動作変更</a>
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 checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	<a href="#">動作変更</a>
SYSLOGサービス	<input type="radio"/> 停止 <input checked="" type="radio"/> 起動	動作中	<a href="#">動作変更</a>
攻撃検出サービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	<a href="#">動作変更</a>
SNMPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	<a href="#">動作変更</a>
NTPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	<a href="#">動作変更</a>
VRRPサービス	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	<a href="#">動作変更</a>
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	

ここでは

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

をおこないます。

### サービスの設定

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

それぞれの設定方法については、以下のページを参照してください。

DNS リレー / キャッシュ機能

DHCP サーバ / リレー機能

IPsec 機能

UPnP 機能

ダイナミックルーティング機能

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 リレー / キャッシュ機能

### DNS 機能の設定

#### DNS リレー機能

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

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

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

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

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

#### root server

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

#### タイムアウト

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

設定後に「設定の保存」をクリックして設定完了です。

設定はすぐに反映されます。

#### DNS キャッシュ機能

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

# 第 11 章

---

---

DHCP サーバ / リレー機能

## 第11章 DHCP サーバ / リレー機能

### . XR-430 の DHCP 関連機能について

XR-430 は、以下の 4 つの DHCP 関連機能を搭載しています。

#### DHCP クライアント機能

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

また既存 LAN に仮設 LAN を接続したい場合などに、XR-430 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なります。

DHCP クライアント機能の設定は「[第5章 インターフェース設定](#)」を参照してください。

#### DHCP サーバ機能

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

#### IP アドレスの固定割り当て

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

#### 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 XR-430 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(XR-430 が DHCP クライアントからの要求と DHCP サーバからの応答を中継します)。

NAT 機能を利用している場合、DHCP リレー機能は利用できません。

## 第11章 DHCP サーバ / リレー機能

### . DHCP サーバ機能の設定

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

DHCP サーバの設定

DHCP サーバの設定    DHCP IP アドレス固定割り付け設定

サーバの選択     DHCP サーバを使用する     DHCP リレーを使用する

DHCP リレーサーバ使用時に設定して下さい

上位 DHCP サーバの IP アドレス: [入力欄]

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

設定の保存

DHCP サーバ使用時に設定して下さい

DHCP アドレスリース情報

サブネットワーク: 192.168.0.0  
サブネットマスク: 255.255.255.0  
ブロードキャスト: 192.168.0.255  
リース開始アドレス: 192.168.0.10  
リース終了アドレス: 192.168.0.100  
ルーターアドレス: 192.168.0.254  
ドメイン名: localdomain.co.jp  
プライマリ DNS: 192.168.0.254  
セカンダリ DNS: [入力欄]  
標準リース時間(秒): 600  
最大リース時間(秒): 7200  
プライマリ WINS サーバー: [入力欄]  
セカンダリ WINS サーバー: [入力欄]  
スコープ ID: [入力欄]

サブネット1

サブネットワーク: [入力欄]  
サブネットマスク: [入力欄]  
ブロードキャスト: [入力欄]  
リース開始アドレス: [入力欄]  
リース終了アドレス: [入力欄]  
ルーターアドレス: [入力欄]  
ドメイン名: [入力欄]  
プライマリ DNS: [入力欄]  
セカンダリ DNS: [入力欄]  
標準リース時間(秒): [入力欄]  
最大リース時間(秒): [入力欄]  
プライマリ WINS サーバー: [入力欄]  
セカンダリ WINS サーバー: [入力欄]  
スコープ ID: [入力欄]

サブネット2

サブネットワーク: [入力欄]  
サブネットマスク: [入力欄]  
ブロードキャスト: [入力欄]  
リース開始アドレス: [入力欄]  
リース終了アドレス: [入力欄]  
ルーターアドレス: [入力欄]  
ドメイン名: [入力欄]  
プライマリ DNS: [入力欄]  
セカンダリ DNS: [入力欄]  
標準リース時間(秒): [入力欄]  
最大リース時間(秒): [入力欄]  
プライマリ WINS サーバー: [入力欄]  
セカンダリ WINS サーバー: [入力欄]  
スコープ ID: [入力欄]

設定の保存

### DHCP サーバ / リレーの機能設定

画面上部「DHCP サーバの設定」をクリックします。

#### サーバの選択

DHCP サーバ機能 / リレー機能のどちらを使用するかを選択します。

サーバ機能とリレー機能を同時に使うことはできません。

#### [DHCP リレーサーバ使用時に設定して下さい]

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

#### 上位 DHCP サーバの IP アドレス

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

#### DHCP relay over XXX

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

#### [DHCP サーバ使用時に設定して下さい]

「サーバの選択」で「DHCP サーバを使用する」を選択した場合に設定をおこないます。

#### サブネット1

#### サブネット2

DHCP サーバ機能の動作設定をおこないます。

- ・複数のサブネットを設定することができます。
- ・どのサブネットを使うかは、XR-430 のインターフェースに設定された IP アドレスを参照の上、同じサブネットとなる設定を使います。
- ・チェック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。

## 第11章 DHCP サーバ / リレー機能

### . DHCP サーバ機能の設定

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。

#### プロードキャスト

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

#### リース開始アドレス

#### リース終了アドレス

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

#### ルータアドレス

DHCP クライアントのデフォルトゲートウェイとなるアドレスを入力してください。通常は、XR-430 のインターフェースの IP アドレスを指定します。

#### ドメイン名

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

#### プライマリ DNS

#### セカンダリ DNS

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

#### 標準リース時間(秒)

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

#### 最大リース時間(秒)

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

#### プライマリ WINS サーバー

#### セカンダリ WINS サーバー

DHCP クライアントに割り当てる WINS サーバの IP アドレスを指定します。

#### スコープ ID

NetBIOS スコープ ID を配布できます。

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

入力が終わりましたら「設定の保存」をクリックして設定完了です。

**機能を有効にするには「各種サービスの設定」  
トップに戻り、サービスを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 サーバ機能の初期設定

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

- ・ LAN は 192.168.0.0/24 のネットワーク
- ・ 192.168.0.10 から 100 のアドレスをリース
- ・ ルータアドレスは 192.168.0.254
- ・ ルータは DNS リレー機能が有効
- ・ 標準リース時間は 10 分間
- ・ 最大リース時間は 2 時間

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

## 第11章 DHCP サーバ / リレー機能

### . IP アドレス固定割り当て設定

#### DHCP IP アドレス固定割り付け設定

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

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

**DHCP IP アドレス固定割り当て設定**

		DHCP サーバの設定		DHCP IP アドレス固定割り付け設定	
No.1~16まで					
No.	MAC アドレス	IP アドレス	削除		
1			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
9			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
10			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
11			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
12			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
13			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
14			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
15			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
16			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**IP アドレス固定割り当て設定インデックス**

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

#### MAC アドレス

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

<入力例> 00:80:6d:49:ff:ff

#### IP アドレス

その MAC アドレスに固定で割り当てる IP アドレスを入力します。

最大設定数は 256 です。

設定画面の最下部にある「IP アドレス固定割り当て設定インデックス」のリンクをクリックしてください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

**固定割り当て機能は、DHCP サーバ機能を再起動してから有効になります。**

#### エントリの削除方法

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

#### IP アドレス固定割り当て時の DHCP サーバ設定について

DHCP サーバ機能で IP アドレス固定割り付け設定のみを使用する場合でも、DHCP サーバの設定にある [DHCP リレーサーバ使用時に設定して下さい] の設定は必要です。

# 第 12 章

---

---

IPsec 機能

### . XR-430 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-430 では「共通鍵方式」、「RSA 公開鍵方式」、「X.509」による認証に対応しています。

ただしアグレッシブモードは「共通鍵方式」にのみ対応、「X.509」はメインモードにのみ対応しています。

#### 暗号化アルゴリズム

シングルDES とトリプルDES、AES128bit をサポートしています。暗号化処理はソフトウェア処理でおこないます。

#### ハッシュアルゴリズム

SHA1 と MD-5 を使用しています。

#### 認証ヘッダ

XR-430 は ESP の認証機能を利用していますので、AH での認証はおこなっていません。

#### DH 鍵共有アルゴリズムで使用するグループ

group1、group2、group5 をサポートしています。

#### IPsec 使用時の通信可能対地数

本装置は最大 128 拠点と IPsec 接続が可能です。

#### IPsec とインターネット接続

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

#### NAT トラバーサルに対応

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

#### 他の機器との接続実績について

以下のルータとの接続を確認しています。

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

### . IPsec設定の流れ

#### PreShared(共通鍵)方式でのIPsec通信

##### STEP 1 共通鍵の決定

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

##### STEP 2 共通鍵の交換

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

##### STEP 3 本装置側の設定

自分側のXR-430の設定をおこないます。

##### STEP 4 IKE/ISAKMPポリシーの設定

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

##### STEP 5 IPsecポリシー設定

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

##### STEP 6 IPsecの起動

本装置のIPsec機能を起動します。

##### STEP 7 IPsec接続の確認

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

#### RSA(公開鍵)方式でのIPsec通信

##### STEP 1 公開鍵・暗号鍵の生成

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

##### STEP 2 公開鍵の交換

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

##### STEP 3 本装置側の設定

自分側のXR-430の設定をおこないます。

##### STEP 4 IKE/ISAKMPポリシーの設定

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

##### STEP 5 IPsecポリシー設定

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

##### STEP 6 IPsecの起動

本装置のIPsec機能を起動します。

##### STEP 7 IPsec接続の確認

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

## 第12章 IPsec機能

### . IPsec設定

#### STEP 0 設定画面を開く

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



- ・ステータスの確認

- ・本装置の設定

- ・RSA鍵の作成

- ・X.509の設定

- ・パラメータでの設定

- ・IPsec Keep-Alive設定

- ・IKE/ISAKMPポリシーの設定

- ・IPsecポリシーの設定

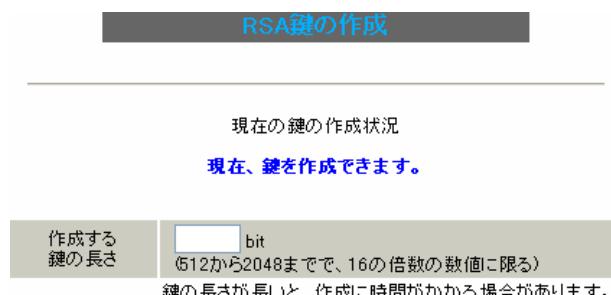
IPsecに関する設定・確認は、全てこの設定画面からおこなえます。

#### STEP 1,2 鍵の作成・交換

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

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

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



- 2 作成する鍵の長さを指定して「公開鍵の作成」をクリックします。

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

現在の鍵の作成状況が「鍵を作成できます」の表示の時に限り、作成可能です。

- 3 鍵を生成します。「鍵を作成しました。」のメッセージが表示されると、鍵の生成が完了です。生成した鍵は、後述する「本装置側の設定」に自動的に反映されます。

またこの鍵は公開鍵となりますので、相手側にも通知してください。

## . IPsec設定

## STEP 3 本装置側の設定をおこなう

IPsec設定画面上部の「本装置の設定」をクリックして設定します。

## [本装置の設定]

「本装置の設定」をクリックします。

MTUの設定	
主回線使用時のipsecインターフェイスのMTU値	1500
マルチ#2回線使用時のipsecインターフェイスのMTU値	1500
マルチ#3回線使用時のipsecインターフェイスのMTU値	1500
マルチ#4回線使用時のipsecインターフェイスのMTU値	1500
バックアップ回線使用時のipsecインターフェイスのMTU値	1500
Ether 0ポート使用時のipsecインターフェイスのMTU値	1500
Ether 1ポート使用時のipsecインターフェイスのMTU値	1500
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	
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)	

[入力のやり直し](#) [設定の保存](#)

## [MTUの設定]

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

## [NAT Traversalの設定]

NATトラバーサル機能を使うことで、NAT環境でIPsec通信をおこなえるようになります。

## NAT Traversal

NATトラバーサル機能を使うかどうかを選択します。

- ・本装置がNAT内のIPsecクライアントの場合
- ・本装置がNAT外のIPsecサーバの場合

## Virtual Private設定

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

%v4:<ネットワーク>/<マスクビット値>

<設定例> %v4:192.168.0.0/24

本装置をNATトラバーサルのホストとして使用する場合に設定します。

クライアントとして使用する場合は空欄のままにします。

## [鍵の表示]

## 本装置のRSA鍵

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

最後に「設定の保存」をクリックして設定完了です。

## . IPsec設定

## [本装置側の設定]

「本装置側の設定」の1～8のいずれかをクリックします。

ここでXR-430自身のIPアドレスやインターフェースIDを設定します。

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

## [ IKE/ISAKMP の設定 1 ~ 8 ]

インターフェースのIPアドレス

## ・固定アドレスの場合

本装置に設定されているIPアドレスをそのまま入力します。

## ・動的アドレスの場合

PPP/PPPoE主回線接続の場合は「%ppp0」と入力します。

Ether0(Ether1)ポートで接続している場合は「%eth0(%eth1)」と入力します。

上位ルータのIPアドレス

本装置から見て1つ上位のルータ(ゲートウェイ)のIPアドレスを入力します。

## ・固定アドレスの場合

上位ルータのIPアドレスをそのまま入力します。

PPP/PPPoE主回線接続の場合は「%ppp0」と入力してください。

## ・動的アドレスの場合

空欄のままにします。

インターフェースのID

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

また、NAT内のクライアントとして接続する場合も必ず設定してください。

<入力形式> @ <任意の文字列>

<入力例> @centurysystems

@の後は、任意の文字列でかまいません。

固定アドレスの場合は、設定を省略できます。

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

最後に「設定の保存」をクリックして設定完了です。

続いてIKE/ISAKMPポリシーの設定をおこないます。

## . IPsec設定

## STEP 4 IKE/ISAKMP ポリシーの設定

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

IKE/ISAKMPポリシーの設定			
<a href="#">IKE1</a>	<a href="#">IKE2</a>	<a href="#">IKE3</a>	<a href="#">IKE4</a>
<a href="#">IKE5</a>	<a href="#">IKE6</a>	<a href="#">IKE7</a>	<a href="#">IKE8</a>
<a href="#">IKE9</a>	<a href="#">IKE10</a>	<a href="#">IKE11</a>	<a href="#">IKE12</a>
<a href="#">IKE13</a>	<a href="#">IKE14</a>	<a href="#">IKE15</a>	<a href="#">IKE16</a>
<a href="#">IKE17</a>	<a href="#">IKE18</a>	<a href="#">IKE19</a>	<a href="#">IKE20</a>
<a href="#">IKE21</a>	<a href="#">IKE22</a>	<a href="#">IKE23</a>	<a href="#">IKE24</a>
<a href="#">IKE25</a>	<a href="#">IKE26</a>	<a href="#">IKE27</a>	<a href="#">IKE28</a>
<a href="#">IKE29</a>	<a href="#">IKE30</a>	<a href="#">IKE31</a>	<a href="#">IKE32</a>

[IKE/ISAKMPポリシーの設定画面インデックス](#)  
[\[1-\]](#) [\[33-\]](#) [\[65-\]](#) [\[97-\]](#)

**IKE/ISAKMPの設定**

IKE/ISAKMPの設定	<input type="text"/>								
接続する本装置側の設定	<input type="button" value="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"/>								
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	<input type="button" value="main モード"/>								
transformの設定	<table border="1"> <tr> <td>1番目</td> <td>すべてを送信する</td> </tr> <tr> <td>2番目</td> <td>使用しない</td> </tr> <tr> <td>3番目</td> <td>使用しない</td> </tr> <tr> <td>4番目</td> <td>使用しない</td> </tr> </table>	1番目	すべてを送信する	2番目	使用しない	3番目	使用しない	4番目	使用しない
1番目	すべてを送信する								
2番目	使用しない								
3番目	使用しない								
4番目	使用しない								
IKEのライフタイム	<input type="text"/> 秒 (1081～28800秒まで)								
鍵の設定	<input checked="" type="radio"/> PSKを使用する <input checked="" 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								
X509の設定	<input type="text"/>								

IKE/ISAKMP ポリシー名  
設定名を任意で設定します。(省略可)

接続する本装置側の設定  
接続で使用する「本装置側の設定1～8」を選択します。

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

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

[相手側装置が動的アドレスの場合]  
「0.0.0.0」を入力します。

上位ルータの IP アドレス  
空欄にしておきます。

インターフェースの ID  
対向側装置への IP アドレスの割り当てが動的割り当てる場合に限り、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。

### . IPsec設定

#### transformの選択

ISAKMP SAの折衝で必要な暗号化アルゴリズム等の組み合わせを選択します。XR-430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、相手側装置に対して発行されたデジタル証明書をテキストボックス内に貼り付けます。

最後に「設定の保存」をクリックして設定完了です。

続いて、IPsecポリシーの設定をおこないます。

## . IPsec設定

## STEP 5 IPsecポリシーの設定

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

IPSecポリシーの設定			
<a href="#">IPSec 1</a>	<a href="#">IPSec 2</a>	<a href="#">IPSec 3</a>	<a href="#">IPSec 4</a>
<a href="#">IPSec 5</a>	<a href="#">IPSec 6</a>	<a href="#">IPSec 7</a>	<a href="#">IPSec 8</a>
<a href="#">IPSec 9</a>	<a href="#">IPSec 10</a>	<a href="#">IPSec 11</a>	<a href="#">IPSec 12</a>
<a href="#">IPSec 13</a>	<a href="#">IPSec 14</a>	<a href="#">IPSec 15</a>	<a href="#">IPSec 16</a>
<a href="#">IPSec 17</a>	<a href="#">IPSec 18</a>	<a href="#">IPSec 19</a>	<a href="#">IPSec 20</a>
<a href="#">IPSec 21</a>	<a href="#">IPSec 22</a>	<a href="#">IPSec 23</a>	<a href="#">IPSec 24</a>
<a href="#">IPSec 25</a>	<a href="#">IPSec 26</a>	<a href="#">IPSec 27</a>	<a href="#">IPSec 28</a>
<a href="#">IPSec 29</a>	<a href="#">IPSec 30</a>	<a href="#">IPSec 31</a>	<a href="#">IPSec 32</a>
<a href="#">IPSecポリシーの設定画面インデックス</a> [1-] [33-] [65-] [97-]			

IPSecポリシーの設定

<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 <input type="button" value="-----"/>			
本装置側のLAN側のネットワークアドレス <input type="text"/> (例:192.168.0.0/24)			
相手側のLAN側のネットワークアドレス <input type="text"/> (例:192.168.0.0/24)			
PH2のTransFormの選択 <input type="button" value="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) <input type="button" value="指定しない"/>			
SAのライタイム <input type="text" value="28800"/> 秒 (1081～86400秒まで)			
DISTANCE <input type="text"/> (1～255まで)			
<input type="button" value="入力のやり直し"/>		<input type="button" value="設定の保存"/>	

最初にIPsecの起動状態を選択します。

「使用する」

initiatorにも responderにもなります。

「使用しない」

そのIPsecポリシーを使用しません。

「Responderとして使用する」

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

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

「On-Demandで使用する」

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

使用するIKEポリシー名の選択

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

本装置側のLAN側のネットワークアドレス  
自分側の本装置に接続しているLANのネットワークアドレスを入力します。

ネットワークアドレス/マスクビット値の形式で入力します。

<入力例> 192.168.0.0/24

相手側のLAN側のネットワークアドレス

相手側のIPsec装置に接続されているLANのネットワークアドレスを入力します。

ネットワークアドレス/マスクビット値の形式で入力します。「本装置側のLAN側のネットワークアドレス」と同様です。

また、NAT Traversal機能を使用し、接続相手がNAT内にある場合に限っては、「vhost:%priv」と設定します。

PH2のTransFormの選択

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

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

通常は「すべてを送信する」の選択で構いません。

PFS

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

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

## 第12章 IPsec機能

### . IPsec設定

#### DH Group の選択(PFS 使用時に有効)

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

#### SAのライフタイム

IPsec SA の有効期間を設定します。IPsecSA とはデータを暗号化して通信するためのトライ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-430 の Ethernet ポートに設定されていると、正常に IPsec 通信があこなえません。

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-430 の Ether1 ポートに 192.168.1.254 が設定されていると、正常に IPsec 通信があこなえません。

このような場合は XR-430 の Ethernet ポートの IP アドレスを、別のネットワークに属する IP アドレスに設定し直してください。

### STEP 6 IPsec 機能を起動する

「各種サービスの設定」をクリックして、以下の画面を開きます。

サービスの起動・停止・設定

現在のサービス稼働状況を反映しています 各種設定はサービス項目名をクリックして下さい				
サービス名	停止	起動	動作中	動作変更
DNSキャッシュ	<input type="radio"/>	<input checked="" type="radio"/>	動作中	動作変更
DHCP(Relay)サービス	<input type="radio"/>	<input checked="" type="radio"/>	動作中	動作変更
IPsecサーバ	<input checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
UPnPサービス	<input checked="" type="radio"/>	<input type="radio"/>	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 checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
SYSLOGサービス	<input type="radio"/>	<input checked="" type="radio"/>	動作中	動作変更
攻撃検出サービス	<input checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
SNMPサービス	<input checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
NTPサービス	<input checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
VRRPサービス	<input checked="" type="radio"/>	<input type="radio"/>	停止中	動作変更
アクセスサーバ	起動停止はアクセスサーバの設定から行って下さい			停止中
動作変更				

#### 動作状態の制御

IPsec サーバ項目、「起動」にチェックして「動作変更」をクリックすると、IPsec 機能が起動します。以降は、XR-430 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。

## 第12章 IPsec機能

### . 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

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

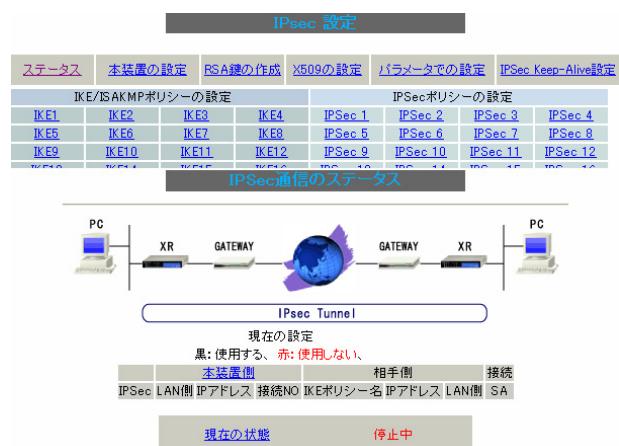
#### (2)のメッセージ

IPsec SAが正常に確立したことを示しています。

#### STEP 8 IPsecステータス確認の確認

IPsecの簡単なステータスを確認できます。

「各種サービスの設定」「IPsecサーバ」「ステータス」をクリックして、画面を開きます。



(画面は表示例です)

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

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

また、それぞれの設定番号をクリックすると、設定画面に移ることができます。

## 第12章 IPsec機能

### . IPsec Keep-Alive機能

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

指定した宛先へIPsecトンネル経由でpingパケットを発行して応答がない場合にIPsecトンネルに障害が発生したと判断し、そのIPsecトンネルを自動的に削除します。

不要なIPsecトンネルを自動的に削除し、IPsecSAの再起動またはバックアップSAを起動することで、IPsecの再接続性を高めます。

#### [IPsec Keep-Alive設定]

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

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

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

設定/削除の実行

ページインデックス

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

#### 動作Optionの説明

##### 動作Option 1 check on

IPsecのネゴシエーション動作と連動して動作します。timeout/delayはicmp echo reply timeout値として認識します。  
timeout値>(interval/count)の場合には実行時にtimeout値は(interval/count)秒となります。

動作Option 2は無視します。

##### 動作Option 1 check off

IPsecのネゴシエーション動作とは非連動、動作Option 2の設定に従って動作します。timeout/delayはdelay値として認識します。

##### 動作Option 2 check on

IPsec SAの状態に依存せず指定したパラメータでkeepalive動作をします。

##### 動作Option 2 check off

IPsec SAがestablishした後の最初のicmp echo replyが確認出来た時点からkeepalive動作を始めます。

enable

設定を有効にする時にチェックします。

IPsec Keep-Alive機能を使いたいIPsecポリシーと

同じ番号にチェックを入れます。

source address

IPsec通信をおこなう際の、本装置のLAN側インターフェースのIPアドレスを入力します。

destination address

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

### . IPsec Keep-Alive機能

interval(sec)

watch count

pingを発行する間隔を設定します。

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

timeout/delay(sec)

後述の「動作option 1」の設定に応じて、入力値の意味が異なります。

- ・動作option 1が有効の場合

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

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

- ・動作option 1が無効の場合

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

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

#### 動作option 1

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

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

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

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

- ・フェーズ1(イニシエーションフェーズ)

ネゴシエーションを開始し、IPSecポリシー確立中の状態です。

この後、正常にIPSecポリシーが確立できた場合はフェーズ3へ移行します。

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

フェーズ3に移行するまでpingの送出はおこないません。

- ・フェーズ2(ネゴシエーションT.0.フェーズ)

フェーズ1におけるネゴシエーションが失敗、またはタイムアウトした状態です。

この時、バックアップSAを起動し、フェーズ1に戻ります。

- ・フェーズ3(ポリシー確立フェーズ)

IPSecポリシーが正常に確立した状態です。

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

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

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

この後、pingの応答がタイムアウトした場合は、フェーズ4に移行します。

- ・フェーズ4(ポリシーダウンフェーズ)

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

さらに、バックアップSAを起動させた後、フェーズ1に戻ります。

## . IPsec Keep-Alive機能

## 動作 option 2

本オプションは「動作option 1」が無効の場合のみ、有効になります。

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

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

## interface

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

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

## backup SA

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

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

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

## &lt;入力例&gt;

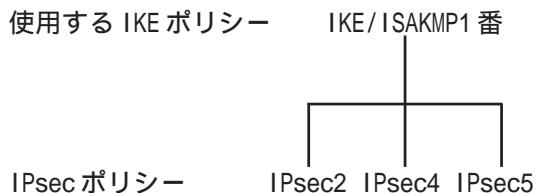
1\_2\_3

またここに、以下のような設定もできます。

ike<n> <n> は 1 ~ 128 の整数

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

## &lt;例&gt;



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

remove ?

設定を削除したいときにチェックします。

### . IPsec Keep-Alive機能

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

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

#### 設定番号について

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

#### IPsecトンネルの障害を検知する条件

IPsec Keep-Alive機能によって障害を検知するのは、「interval/watch count」に従ってpingを発行して、一度も応答がなかったときです。

このとき本装置は、pingの応答がなかったIPsecトンネルを自動的に削除します。

反対に一度でも応答があったときは、本装置はIPsecトンネルを保持します。

#### 動的アドレスの場合の本機能の利用について

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

## 第12章 IPsec機能

### .「X.509デジタル証明書」を用いた電子認証

本装置はX.509デジタル証明書を用いた電子認証方式に対応しています。

ただし、本装置は証明書署名要求の発行や証明書の発行ができません。

あらかじめCA局から証明書の発行を受けておく必要があります。

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

情報処理振興事業協会セキュリティセンター

<http://www.ipa.go.jp/security/pki/>

#### [X.509の設定]

IPsec設定画面上部の「X509の設定」「X509の設定」を開きます。

#### X509の設定

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

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="text"/>

#### X509の設定

X.509の使用 / 不使用を選択します。

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

#### 証明書のパスワード

証明書のパスワードを入力します。

入力が終わりましたら「設定の保存」をクリックします。

## 第12章 IPsec機能

### 「X.509デジタル証明書」を用いた電子認証

#### [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。

X.509の設定

【CAの設定】 【本装置側の証明書の設定】 【本装置側の鍵の設定】  
【失効リストの設定】

CAの設定

失効リストの設定

入力のやり直し 設定の保存

#### [本装置側の鍵の設定]

ここにはデジタル証明書と一緒に発行された、本装置の秘密鍵の内容をコピーして貼り付けます。

X.509の設定

【CAの設定】 【本装置側の証明書の設定】 【本装置側の鍵の設定】  
【失効リストの設定】

失効リストの設定

入力のやり直し 設定の保存

#### [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。

X.509の設定

【CAの設定】 【本装置側の証明書の設定】 【本装置側の鍵の設定】  
【失効リストの設定】

本装置側の証明書の設定

入力のやり直し 設定の保存

#### [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。

X.509の設定

【CAの設定】 【本装置側の証明書の設定】 【本装置側の鍵の設定】  
【失効リストの設定】

本装置側の鍵の設定

入力のやり直し 設定の保存

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

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

各設定にコピーを貼り付けましたら、「設定の保存」をクリックします。

以上で X.509 の設定は完了です。

## 第12章 IPsec機能

### . IPsec通信時のパケットフィルタ設定

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

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

IPsecでは、以下の2種類のプロトコル・ポートを使用します。

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

ただし、NATトラバーサルを使用する場合は、IKEの一部のトラフィックおよび暗号化ペイロードはUDPの4500番ポートのパケットにカプセリングされています。

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

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

これらのパケットを通せるように、「入力フィルタ」に設定を追加してください。

なお、「ESP」については、ポート番号の指定はしません。

<設定例>

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

### . IPsecがつながらないとき

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

本体ログは、「システム設定」内の「ログ表示」で確認します。

#### [正常にIPsec接続できたときのログメッセージ]

##### メインモードの場合

```
Aug 3 12:00:14 localhost ipsec_setup:  
...FreeS/WAN IPsec started  
  
Aug 3 12:00:20 localhost ipsec_plutorun:  
104 "xripsec1" #1: STATE_MAIN_I1: initiate  
  
Aug 3 12:00:20 localhost ipsec_plutorun:  
106 "xripsec1" #1: STATE_MAIN_I2: from  
STATE_MAIN_I1; sent MI2, expecting MR2  
  
Aug 3 12:00:20 localhost ipsec_plutorun:  
108 "xripsec1" #1: STATE_MAIN_I3: from  
STATE_MAIN_I2; sent MI3, expecting MR3  
  
Aug 3 12:00:20 localhost ipsec_plutorun:  
004 "xripsec1" #1: STATE_MAIN_I4: ISAKMP SA  
established  
  
Aug 3 12:00:20 localhost ipsec_plutorun:  
112 "xripsec1" #2: STATE_QUICK_I1: initiate
```

##### アグレッシブモードの場合

```
Apr 25 11:14:27 localhost ipsec_setup:  
...FreeS/WAN IPsec started  
  
Aug 3 11:14:34 localhost ipsec_plutorun:  
whack:ph1_mode=aggressive whack:CD_ID=@home  
whack:ID_FQDN=@home 112 "xripsec1" #1:  
STATE_AGGR_I1: initiate  
  
Aug 3 11:14:34 localhost ipsec_plutorun: 004  
"xripsec1" #1: SAEST(e)=STATE_AGGR_I2: sent  
AI2, ISAKMP SA established  
  
Aug 3 12:14:34 localhost ipsec_plutorun: 117  
"xripsec1" #2: STATE_QUICK_I1: initiate  
  
Aug 3 12:14:34 localhost ipsec_plutorun: 004  
"xripsec1" #2: SAEST(13)=STATE_QUICK_I2: sent  
QI2, IPsec SA established
```

### . IPsecがつながらないとき

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

#### [正常にIPsecが確立したときの表示例]

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

これらのログやメッセージ内に

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

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

### . IPsecがつながらないとき

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

この場合は、接続相手とのIKE鍵交換が正常におこなえています。

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、「第30章 パケット分類設定 . DSCPについて」をご覧ください。

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

この場合は、IPsec SAが正常に確立できていません。

IPsec設定の「IPsecポリシー設定」項目で、自分側と相手側のネットワークアドレスが正しいか、設定を確認してください。

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

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

IPSecは確立していますが、Windowsでファイル共有ができません。

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

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

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

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

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

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

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

これらの理由によって、IPsec通信がなかなか復帰しない現象となります。

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

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

相手のXR-430にはIPsecのログが出ているのに、こちらのXR-430にはログが出ていません。IPsecは確立しているようなのですが、確認方法はありませんか？

固定IP - 動的IP間でのIPsec接続をおこなう場合、固定IP側(受信者側)のXR-430ではログが表示されないことがあります。その場合は「各種サービスの設定」「IPsecサーバ」「ステータス」を開き、「現在の状態」をクリックしてください。ここに現在のIPsecの状況が表示されます。

# 第 13 章

---

---

UPnP 機能

## 第13章 UPnP機能

### . UPnP機能の設定

XR-430はUPnP(Universal Plug and Play)に対応していますので、UPnPに対応したアプリケーションを使うことができます。

#### 対応しているWindows OSとアプリケーション

##### **Windows OS**

- Windows XP
- Windows Me

##### **アプリケーション**

- Windows Messenger

#### 利用できるMessengerの機能について

以下の機能について動作を確認しています。

- インスタントメッセージ
- 音声チャット
- ビデオチャット
- ダイヤルアップ
- ホワイトボード

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

#### Windows OSのUPnPサービス

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

#### UPnP機能の設定

XR-430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。

#### **UPnPサービスの設定**

WAN側インターフェース	eth1
LAN側インターフェース	eth0
切断検知タイマー	5 分 (0~60分)

#### **設定の保存**

##### **WAN側インターフェース**

WAN側に接続しているインターフェース名を指定します。

##### **LAN側インターフェース**

LAN側に接続しているインターフェース名を指定します。

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

##### **切断検知タイマー**

UPnP機能使用時の無通信切断タイマーを設定します。

ここで設定した時間だけ無通信時間が経過すると、XR-430が保持するWindows Messengerのセッションが強制終了されます。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

**機能を有効にするには「各種サービスの設定」  
トップに戻り、サービスを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13章 UPnP機能

### . UPnP機能の設定

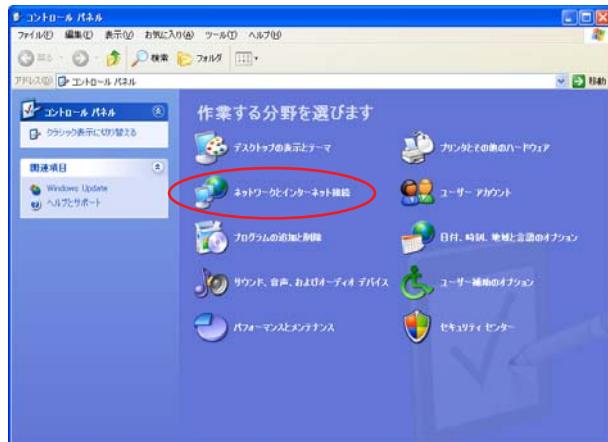
#### UPnPの接続状態の確認

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

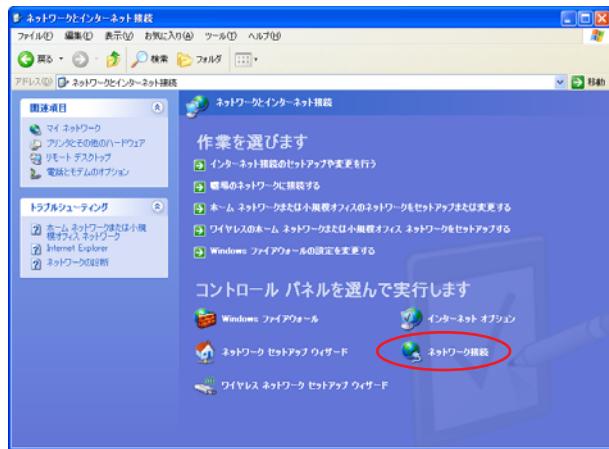
1 「スタート」「コントロール パネル」を開きます。



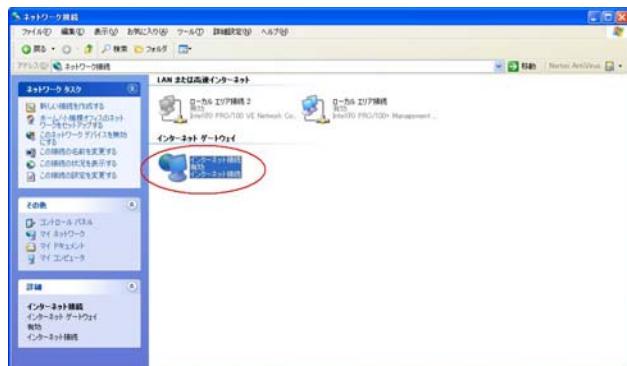
2 「ネットワークとインターネット接続」を開きます。



3 「ネットワーク接続」を開きます。



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



(画面はWindows XPでの表示例です)

Windows OSやWindows Messengerの詳細につきましては、Windowsのマニュアル／ヘルプをご参照ください。

弊社ではWindowsや各アプリケーションの操作法や仕様等についてお答えできかねますので、ご了承ください。

## 第13章 UPnP機能

### . UPnPとパケットフィルタ設定

#### UPnP機能使用時の注意

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

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

参考：NTT東日本のVoIP-TAの利用ポートは、UDP・5060、UDP・5090、UDP・5091です。

(詳細はNTT東日本にお問い合わせください)

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

#### UPnP機能使用時の推奨フィルタ設定

Microsoft Windows上のUPnPサービスのバッファオーバフローを狙ったDoS(サービス妨害)攻撃からの危険性を緩和する為の措置として、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)

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

##### (転送フィルタ)

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

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

# 第 14 章

---

---

ダイナミックルーティング  
(RIP と OSPF の設定)

## 第14章 ダイナミックルーティング

### . ダイナミックルーティング機能

XR-430 のダイナミックルーティング機能は、下記のプロトコルをサポートしています。

- RIP
- OSPF

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

#### 設定の開始

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

**ダイナミックルーティング設定**

※各種設定は項目名をクリックして下さい。

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

**動作変更**

**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。

## 第14章 ダイナミックルーティング

### . RIPの設定

#### RIPの設定

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

**RIP設定**

[RIPフィルタ設定へ](#)

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

[設定](#) [RIP情報の表示](#)

[ダイナミックルーティング設定画面へ](#)

Ether0ポート

Ether1ポート

XR-430 の各 Ethernet ポートで、RIP を「使用しない」か、使用する（「送受信」）を選択します。

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

Administrative Distance 設定

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

OSPF ルートの再配信

RIP と OSPF を併用していて、OSPF で学習したルーティング情報を RIP で配信したいときに「有効」にしてください。

RIPのみを使う場合は「無効」にします。

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

static ルートの再配信

static ルーティング情報を 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。

static ルート再配信時のメトリック設定

static ルートを RIP で配信するときのメトリック値を設定します。

default-information の送信

デフォルトルート情報を RIP で配信したいときに「有効」にしてください。

選択、入力後は「設定」をクリックして設定完了です。

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

また設定を変更した場合には、「再起動」をクリックしてください。

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

## 第14章 ダイナミックルーティング

### . RIPの設定

#### RIP フィルターの設定

RIPによるroute情報の送信または受信をしたくないときに設定します。

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

**RIPフィルター設定**

RIP設定へ

NO.	インターフェース	方向	ネットワーク	編集 削除
現在設定はありません				
[フィルターの追加]				
	-----	-----	(例192.168.0.0/16)	
<b>[取消] [追加]</b>				

ダイナミックルーティング設定画面へ

NO.  
設定番号を指定します。1 ~ 64 の間で指定します。

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

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

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

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

<入力形式>  
ネットワークアドレス / サブネットマスク値

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

RIPフィルタ設定後は、ただちに設定が有効となります。

設定後は、画面上部に設定内容が一覧表示されます。

**RIPフィルター設定**

RIP設定へ

NO.	インターフェース	方向	ネットワーク	編集 削除
1	Ether0ポート	in-comming	192.168.0.0/16	<b>編集 削除</b>

(画面は表示例です)

[編集 削除]欄

**削除**

クリックすると、設定が削除されます。

**編集**

クリックすると、その設定について内容を編集できます。

## 第14章 ダイナミックルーティング

### . OSPF の設定

#### OSPF の設定

OSPFはリンクステート型経路制御プロトコルです。

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

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。

#### インターフェースへの OSPF エリア設定

どのインターフェースで OSPF 機能を動作させるかを設定します。

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

**指定インターフェースへの OSPF エリア設定**

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

**設定**

**ダイナミックルーティング設定画面へ**

ネットワークアドレス

XR-430 に接続しているネットワークのネットワークアドレスを指定します。

ネットワークアドレス / マスクビット値の形式で入力します。

AREA 番号

そのネットワークのエリア番号を指定します。

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

入力後は「設定」をクリックして設定完了です。

## 第14章 ダイナミックルーティング

### . OSPF の設定

#### OSPF エリア設定

各 AREA(エリア)ごとの機能設定をおこないます。

設定画面上部の「OSPF エリア設定」をクリックします。

OSPF エリア設定

AREA番号	STUB	Totally STUB	Default-cost	Authentication	経路集約	Configure
<a href="#">New Entry</a>						
<a href="#">ダイナミックルーティング設定画面へ</a>						

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

OSPF エリア設定

AREA番号	(0-4294967295)
スタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
トータリースタブ設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
default-cost	(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	（複数行入力用）

設定 戻る

AREA 番号

機能設定をおこなうエリアの番号を指定します。

#### スタブ設定

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

#### トータリースタブ設定

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

default-cost 設定

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

#### 認証設定

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

#### エリア間ルートの経路集約設定

経路情報を集約して送信したいときに設定します。

<設定例>

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

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。

OSPF エリア設定

	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 <a href="#">Edit, Remove</a>

New Entry

[ダイナミックルーティング設定画面へ](#)

(画面は表示例です)

[Configure] 欄

[Edit](#)

クリックすることで、それぞれ設定内容の「編集」  
をおこなえます。

[Remove](#)

クリックすると設定の「削除」をおこなえます。

## 第14章 ダイナミックルーティング

### . OSPF の設定

#### Virtual Link 設定

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

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

設定画面上部の「Virtual Link 設定」をクリックして設定します。

Virtual Link設定

New Entry

ダイナミックルーティング設定画面へ

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

OSPF Virtual-Link設定

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

設定 戻る

#### Transit AREA 番号

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

このエリアが「Transit AREA」となります。

#### Remote-ABR Router-ID 設定

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

#### Hello インターバル設定

Helloパケットの送出間隔を設定します。

#### Dead インターバル設定

Deadタイムを設定します。

#### Retransmit インターバル設定

LSAを送出する間隔を設定します。

#### transmit delay 設定

LSUを送出する際の遅延間隔(delay)を設定します。

#### 認証パスワード設定

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

#### MD5 KEY-ID 設定(1)

MD5認証使用時のKEY IDを設定します。

#### MD5 パスワード設定(1)

エリア内でMD5認証を使用する際のMD5パスワードを設定します。

#### MD5 KEY-ID 設定(2)

#### MD5 パスワード設定(2)

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

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

入力後は「設定」をクリックしてください。

## 第14章 ダイナミックルーティング

### . OSPF の設定

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

**Virtual Link 設定**

AREA番号	Remote-ABR ID	Hello	Dead	Retransmit	Transmit Delay	認証 Password	MDS KEY-ID	MDS Password	Configure
1	192.168.0.1	10	40	5	1	aaa	1	bbb	<a href="#">Edit/Remove</a>

[New Entry](#)

[ダイナミックルーティング設定画面へ](#)

(画面は表示例です)

[Configure]欄

Edit

クリックすることで、それぞれ設定内容の「編集」をおこなえます。

Remove

クリックすると設定の「削除」をおこなえます。

### OSPF 機能設定

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

**OSPF機能設定**

Router-ID設定	<input type="text" value="192.168.0.1"/> (例192.168.0.1)
Connected再配信	<input checked="" 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="0-16777214"/>
staticルート再配信	<input checked="" 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="0-16777214"/>
RIPルートの再配信	<input checked="" 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="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="110"/> (1-255)
Inter-areaルート Distance 設定	<input type="text" value="110"/> (1-255)
Intra-areaルート Distance 設定	<input type="text" value="110"/> (1-255)
Default-information	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="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

[設定](#)

[ダイナミックルーティング設定画面へ](#)

### Router-ID 設定

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

#### Connected 再配信

connected ルートを OSPF で配信するかどうかを選択します。

「有効」にした場合は以下の 2 項目も設定します。

##### a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

##### b. メトリック値

配信する際のメトリック値を設定します。

### . OSPF の設定

#### static ルートの再配信

static ルートを OSPF で配信するかどうかを選択します。

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

「有効」にした場合は以下の 2 項目も設定します。

##### a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

##### b. メトリック値

配信する際のメトリック値を設定します。

#### RIP ルートの再配信

RIP が学習したルート情報を OSPF で配信するかどうかを選択します。

「有効」にした場合は以下の 2 項目も設定します。

##### a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

##### b. メトリック値

配信する際のメトリック値を設定します。

#### Administrative Distance 設定

ディスタンス値を設定します。

OSPF と他のダイナミックルーティングを併用していく同じサブネットを学習した際に、この値の小さい方のダイナミックルートを経路として採用します。

#### External ルート Distance 設定

OSPF 以外のプロトコルで学習した経路のディスタンス値を設定します。

#### Inter-area ルート Distance 設定

エリア間の経路のディスタンス値を設定します。

#### Intra-area ルート Distance 設定

エリア内の経路のディスタンス値を設定します。

#### Default-information

デフォルトルートを OSPF で配信するかどうかを選択します。

##### ・送信する

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

##### ・常に送信

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

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

##### a. メトリックタイプ

配信する際のメトリックタイプ type1、type2 を選択します。

##### b. メトリック値

配信する際のメトリック値を設定します。

#### SPF 計算 Delay 設定

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

#### 2 つの SPF 計算の最小間隔設定

連続して SPF 計算をおこなう際の間隔を設定します。

入力後は「設定」をクリックしてください。

## 第14章 ダイナミックルーティング

### . OSPF の設定

#### インターフェース設定

各インターフェースごとの OSPF 設定をおこないます。

設定画面上部の「インターフェース設定」をクリックして設定します。

インターフェース名	Passive	Cost	帯域	Hello	Dead	Retransmit	Transmit Delay	認証 Password	MD5 KEY-ID	MD5 Password	Priority	MTU ignore	Configure
eth0	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	1-65535											

New Entry

インターフェース設定

ダイナミックルーティング設定画面へ

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

インターフェース名	eth0
Passive-Interface設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
コスト値設定	1-65535
帯域設定	1-10000000 kbps
Helloインターバル設定	10 (1-65535s)
Deadインターバル設定	40 (1-65535s)
Retransmitインターバル設定	5 (3-65535s)
Transmit Delay設定	1 (1-65535s)
認証キー設定	(英数字で最大8文字)
MD KEY-ID設定(1)	(1-255)
MD5パスワード設定(1)	(英数字で最大16文字)
MD KEY-ID設定(2)	(1-255)
MD5パスワード設定(2)	(英数字で最大16文字)
Priority設定	0-255
MTU-Ignore設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

設定 戻る

#### インターフェース名

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

#### Passive-Interface 設定

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

#### コスト値設定

コスト値を設定します。

#### 帯域設定

帯域設定をおこないます。この値をもとにコスト値を計算します。コスト値 = 100Mbps / 帯域 kbps です。

コスト値と両方設定した場合は、コスト値設定が優先されます。

#### Hello インターバル設定

Hello パケットを送出する間隔を設定します。

#### Dead インターバル設定

Dead タイムを設定します。

#### Retransmit インターバル設定

LSA の送出間隔を設定します。

#### Transmit Delay 設定

LSU を送出する際の遅延間隔を設定します。

#### 認証キー設定

simple パスワード認証を使用する際のパスワードを設定します。

半角英数字で最大 8 文字まで使用できます。

#### MD KEY-ID 設定(1)

MD5 認証使用時の KEY ID を設定します。

#### MD5 パスワード設定(1)

エリア内で MD5 認証を使用する際の MD5 パスワードを設定します。

半角英数字で最大 16 文字まで使用できます。

#### MD KEY-ID 設定(2)

#### MD5 パスワード設定(2)

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

## 第14章 ダイナミックルーティング

### . OSPF の設定

#### Priority 設定

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

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

#### MTU-Ignore 設定

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

入力後は「設定」をクリックしてください。

設定後は「インターフェース設定」画面に、設定内容が一覧で表示されます。

#### インターフェース設定

インターフェース名	Passive	Cost	帯域	Hello	Dead	Retransmit	Transmit Delay	認証 Password	MD5 KEY-ID	MD5 Password	Priority	MTU Ignore	Configure
1 eth0	on	10	100000	10	40	5	1	century	150	century/systems	50	off	Edit Remove

現在バックアップ回線は待機中です

New Entry

ダイナミックルーティング設定画面へ

(画面は表示例です)

#### [Configure]欄

Edit

クリックすることで、それぞれ設定内容の「編集」をおこなえます。

Remove

クリックすると設定の「削除」をおこなえます。

#### ステータス表示

OSPF の各種ステータスを表示します。

設定画面上部の「ステータス表示」をクリックして設定します。

#### ステータス表示

OSPFデータベースの表示 (各Link state情報が表示されます)	<input type="button" value="表示する"/>
ネイバーリスト情報の表示 (現在のネイバー状態を確認できます)	<input type="button" value="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)	<input type="button" value="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)	<input type="button" value="表示する"/>
インターフェース情報の表示 (表示したいインターフェースを指定して下さい)	<input type="button" value="表示する"/> <input type="text"/>

ダイナミックルーティング設定画面へ

#### OSPF データベース表示

LinkState 情報が表示されます。

#### ネイバーリスト情報の表示

現在のネイバー状態が表示されます。

#### OSPF ルーティングテーブル情報の表示

OSPF ルーティング情報が表示されます。

#### OSPF 統計情報の表示

SPF の計算回数や Router ID などが表示されます。

#### インターフェース情報の表示

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

表示したい情報の項目にある「表示する」をクリックしてください。

# 第 15 章

---

---

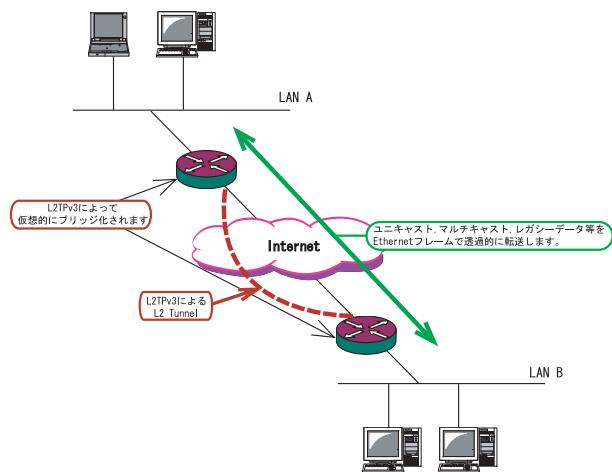
L2TPv3 機能

## . 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出来ます。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つたものも、L2TPv3を使うことで通信が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を関連づけすることが可能です。

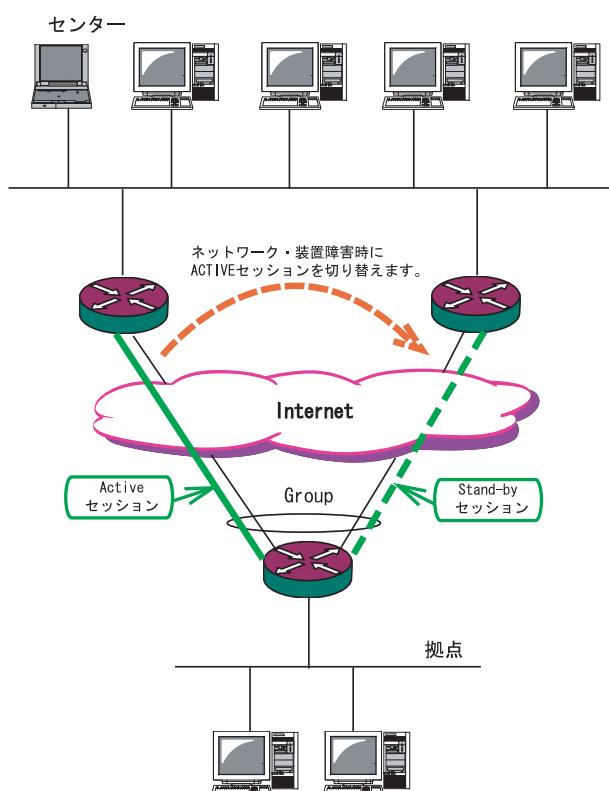
## L2TPv3セッションの二重化機能

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。



## 第15章 L2TPv3機能

### 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おこないます。

「各種サービスの設定」 「L2TPv3」の「L2TPv3 機能設定」をクリックします。

L2TPv3 設定

L2TPv3機能設定	L2TPv3 Tunnel設定	L2TPv3 Xconnect設定	L2TPv3 Group設定
L2TPv3 Layer2 Redundancy設定	L2TPv3 Filter設定	起動/停止設定	L2TPv3ステータス表示

L2TPv3 機能設定

Local hostname	Router
Local Router-ID	
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
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<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

設定

各種サービスの設定画面へ

#### Local hostname

本装置のホスト名を設定します。

使用可能な文字は半角英数字です。

対向 LCCE( 1 )の “ リモートホスト名 ” 設定と同じ文字列を指定してください。  
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、 IP アドレス形式で設定します (ex.192.168.0.1 など ) 。

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 ” 設定と同じ文字列を指定してください。  
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 ( 指定可能な範囲 : 30-1000 秒 )

#### 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

L2TPv3 over IP 使用時に 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。ただし、カプセリングしたフレーム長が送信インターフェースの MTU 値を超過する場合は、こ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。

#### 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。

### . L2TPv3 機能設定

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ください。

また、MIBやTrapに関する詳細は

「第19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、不要なトランジット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インター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インターフェース毎に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おこないません。

- ・Xconnectインター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フレームの転送をおこないません。

- ・Xconnectインター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

## 第15章 L2TPv3 機能

### . L2TPv3 Tunnel 設定

L2TPv3のトンネル(制御コネクション)のための設定をおこないます。

「各種サービスの設定」 「L2TPv3」の「L2TPv3 Tunnel 設定」をクリックします。



新規に設定をおこなうときは「New Entry」をクリックして、以下の画面で設定します。

This screenshot displays the 'L2TPv3 Tunnel設定' configuration form. It consists of a table with various settings:

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 checked="" type="radio"/> 有効 <input type="radio"/> 無効
Digest Type設定	無効 <input type="button" value="▼"/>
Hello Interval設定	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="▼"/>
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	1701 (default 1701)

At the bottom of the form are three buttons: 'リセット' (Reset), '設定' (Set), and '戻る' (Back).

**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。  
ただし、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（指定可能な範囲：0-1100 秒）。「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ください。

#### 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。

#### 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。

### . L2TPv3 Tunnel 設定

#### Vender ID 設定

対向 LCCE のベンダー ID を設定します。「0」は RFC 3931 対応機器、「9」は Cisco Router、「20376」は XR シリーズとなります。

#### Bind Interface 設定

バインドさせる本装置のインターフェースを設定します。指定可能なインターフェースは「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 の中のデータを暗号化します。

## 第15章 L2TPv3 機能

### . 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に使用するパラメータの設定をおこないます。

「各種サービスの設定」 「L2TPv3」の「L2TPv3 Xconnect 設定」をクリックします。



新規に設定をおこなうときは「New Entry」をクリックして、以下の画面で設定します。

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	---
L2Frame受信インターフェース設定	(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	<input type="text" value="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 checked="" type="radio"/> 有効 <input type="radio"/> 無効
Known Unicast設定	<input checked="" type="radio"/> 送信する <input 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 checked="" type="radio"/> 有効 <input type="radio"/> 無効

リセット 設定 戻る

#### 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 受信インターフェース設定

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

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

ただし、本装置のEthernetインターフェースとVLANインター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 設定をおこなうときの例:

「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。ただし、L2TPv3セッション毎に異なる値を設定してください。

#### Reschedule Interval 設定

L2TPトンネル/セッションが切断したときにreschedule(自動再接続)することができます。自動再接続するときはここで、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おこなわれません。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。

## 第15章 L2TPv3機能

### . L2TPv3 Xconnect(クロスコネクト)設定

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ください。

#### 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インターフェースを設定してください。

#### 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です。

“0”を指定すると、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

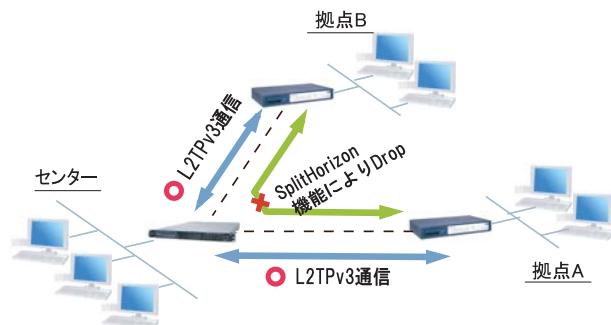
Circuit StatusがDown状態の時に、対向LCCEに対してNon-Unicast Frameを送信するかを選択します。

#### 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通信はおこなうが、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。

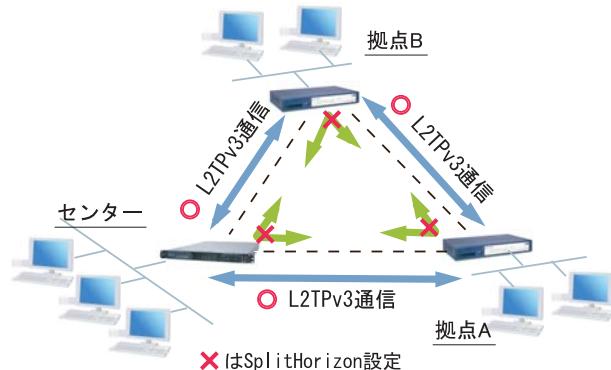
センター側では、Split Horizon機能が有効の場合、一方の拠点から受信したフレームをもう一方のセッションへは転送せず、Local Interfaceに対してのみ転送します。

#### 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



## 第15章 L2TPv3 機能

### . 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おこないます。

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。

「各種サービスの設定」 「L2TPv3」の「L2TPv3 Group 設定」をクリックします。



新規のグループ設定をおこなうときは、「New Entry」をクリックします。

This is a configuration dialog for a new L2TPv3 group. It contains the following fields:

Group ID	[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

リセット 設定 戻る

#### Group ID 設定

Group を識別する番号を設定します（指定可能な範囲：1-4095）。他の Group と重複しない値を設定してください。

#### 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すが、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」に設定してください。

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おこなわず、Primary セッションを Active のまま維持する機能のことと言います。

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止するために本機能を有効に設定することを推奨します。

## 第15章 L2TPv3機能

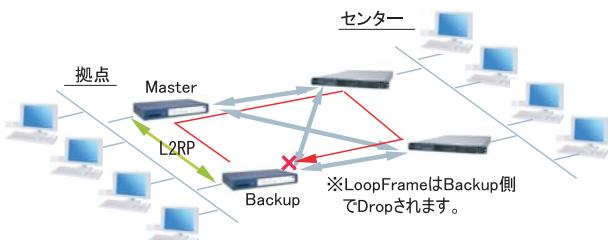
### . Layer2 Redundancy 設定

Layer2 Redundancy Protocol 機能（以下、L2TP 機能）とは、装置の冗長化をおこない、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



「各種サービスの設定」 「L2TPv3」の「L2TPv3 Layer2 Redundancy 設定」をクリックします。



「New Entry」をクリックすると以下の設定画面が開きます。

#### L2TPv3 Layer2 Redundancy 設定

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

[リセット](#) [設定](#) [戻る](#)

#### 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 値を設定します（指定可能な範囲：1-255）。

#### Advertisement Interval 設定

Advertise Frame を送信する間隔を設定します（指定可能な範囲：1-60 秒）。

#### Advertise Frame

Master 側が定期的に送出する情報フレームです。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。

### . Layer2 Redundancy 設定

#### 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ください。  
Advertise Frame は Xconnect 上で送受信されます。

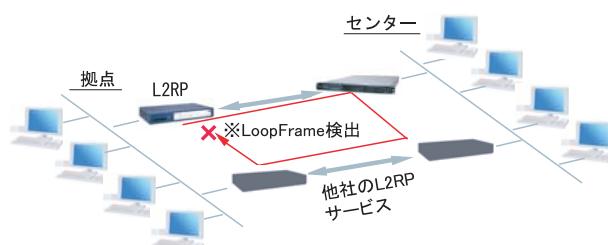
#### Forward Delay 設定

Forward Delay とは、L2TP セッション確立後、指定された Delay Time の間、Frame の転送をおこな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することができます。

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

本装置が 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おこなってください。

- 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

L2TPv3 Filter 設定については、次章で説明します。



### . 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おこないます。

「各種サービスの設定」 「L2TPv3」 の「起動 / 停止設定」をクリックします。



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 ---

実行  
サービス再起動  
各種サービスの設定画面へ

#### 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」で設定したインター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おこないます。停止したい方法を以下から選択してください。

- Tunnel / Session ID 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 / Session ID を指定してください。

- Remote-ID 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 を選択してください。

- Group ID 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 を指定してください。

#### 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。

### . 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を選択してください。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を指定してください。

#### 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を指定してください。

#### 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ーフェースを選択してください。プルダウンには、「L2TPv3 Xconnect 設定」で設定したインターフェースが表示されます。

## 第15章 L2TPv3 機能

### . L2TPv3 ステータス表示

L2TPv3の各種ステータスを表示します。

「各種サービスの設定」 「L2TPv3」の  
「L2TPv3ステータス表示」をクリックします。



#### 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ーフェースを選択してください。

「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ください。

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 を指定してください。

#### 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 を指定してください。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ください。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。

## . 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、下記を参照してください。

## [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。

**SCCRQ : 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**

SCCRQ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**

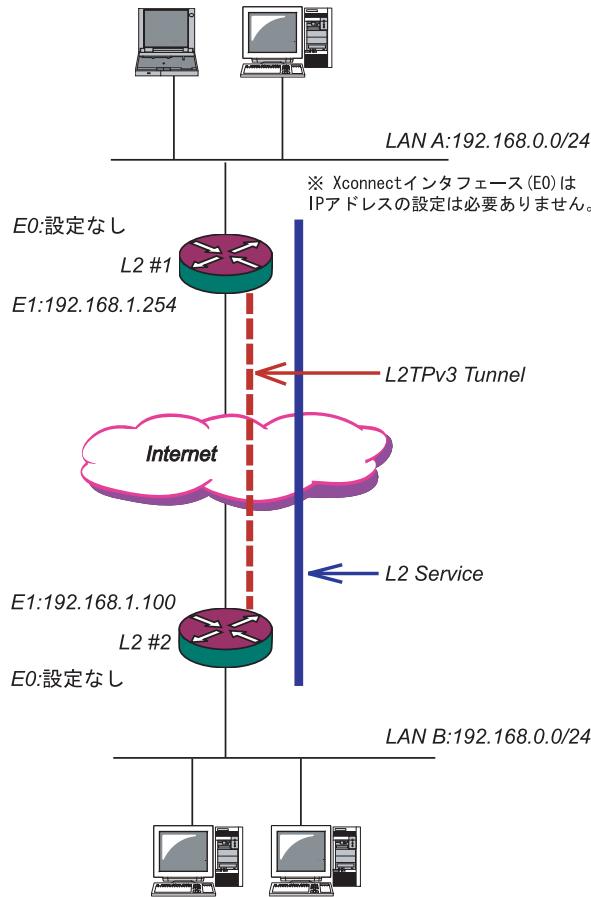
L2TPセッションの切断を要求するメッセージ。

## 第15章 L2TPv3 機能

### . 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。

構成図(例)



#### 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。

サービスの起動・停止・設定			
現在のサービス稼働状況を反映しています 各種設定はサービス項目名をクリックして下さい			
DNSキャッシュ	<input type="radio"/> 停止	<input checked="" type="radio"/> 起動	動作中
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		
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		
動作変更			

## 第15章 L2TPv3機能

### . L2TPv3 設定例1(2拠点間のL2TPトンネル)

#### L2 #1 ルータの設定

L2TPv3機能設定をおこないます。

- 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
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<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

L2TPv3 Xconnect Interface設定をおこないます。

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	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設定をおこないます。

- 「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ときは、「Bind Interface」にPPPインターフェース名を設定します。
- 「Vendor ID」は“0:IETF”に設定してください。

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	0:IETF
Bind Interface設定	
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	1701 (default 1701)

## 第15章 L2TPv3 機能

### . L2TPv3 設定例 1(2拠点間のL2TP トンネル)

#### L2 #2 ルータの設定

L2#1 ルータと同様に設定します。

L2TPv3 機能設定をおこないます。

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
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<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

L2TPv3 Xconnect Interface設定をおこないます。

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	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設定をおこないます。

・「Vendor ID」は“0:IETF”に設定してください。

Description	
Peerアドレス	192.168.1.254 (例192.168.0.1)
パスワード	
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	0:IETF
Bind Interface設定	
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	1701 (default 1701)

### . L2TPv3 設定例1 (2拠点間のL2TPトンネル)

#### L2TPv3 Tunnel Setup 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。

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。

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。



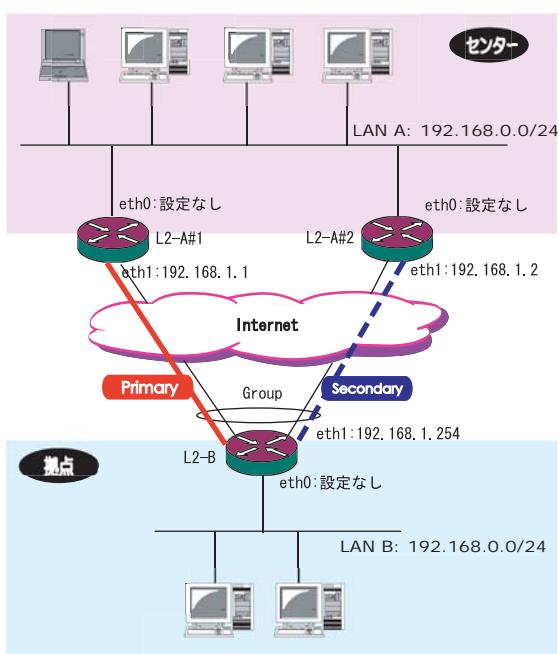
## 第15章 L2TPv3 機能

### . 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おこないます。

構成図(例)



## 第15章 L2TPv3機能

### . L2TPv3 設定例2 (L2TPトンネル二重化)

#### L2-A#1/L2-A#2(センター側)ルータの設定

L2-A#1 (Primary) ルータ

L2TPv3機能設定をおこないます。

- 「Local HostName」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
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<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

L2-A#2 (Secondary) ルータ

L2TPv3機能設定をおこないます。

- Primaryルータと同じ要領で設定してください。

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
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<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

## 第15章 L2TPv3機能

### . L2TPv3 設定例2 (L2TPトンネル二重化)

#### L2-A#1 (Primary) ルータ

**L2TPv3 Tunnel 設定をおこないます。**

- ・「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します。
- 「LocalHostName」「Local Router-ID」と同じものを設定します。
- ・「Vendor ID」は“0:IETF”に設定してください。

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	0:IETF
Bind Interface設定	
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	1701 (default 1701)

#### L2-A#2 (Secondary) ルータ

**L2TPv3 Tunnel 設定をおこないます。**

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

Description	
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	0:IETF
Bind Interface設定	
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	1701 (default 1701)

## 第15章 L2TPv3機能

### . L2TPv3 設定例2 (L2TPトンネル二重化)

#### L2-A#1 (Primary) ルータ

- L2TPv3 Xconnect Interface設定**をおこないます。
- 「Xconnect ID設定」はGroup設定をおこなわないで設定不要です。
  - 「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受信インターフェース」はLAN側のインターフェースを指定します。**LAN側インターフェースには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ください。

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	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

#### L2-A#2 (Secondary) ルータの

- L2TPv3 Xconnect Interface設定**をおこないます。

- Primaryルータと同じ要領で設定してください。
- 「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。

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 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 設定例2 (L2TPトンネル二重化)

#### L2TPv3 Group設定について

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

#### L2-B(拠点側ルータ)の設定

L2TPv3機能設定をおこないます。

- 「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
受信ポート番号(over UDP)	1701 (default 1701)
PMTU Discovery設定(over UDP)	<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

## 第15章 L2TPv3機能

### . L2TPv3 設定例2 (L2TPトンネル二重化)

#### Primaryセッション側

L2TPv3 Tunnel設定をおこないます。

- 「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 をおこないます。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。
- 「Vendor ID」は“0:IETF”に設定してください。

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	0:IETF
Bind Interface設定	
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	1701 (default 1701)

#### Secondaryセッション側

L2TPv3 Tunnel設定をおこないます。

- Primaryセッションと同じ要領で設定してください。

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	0:IETF
Bind Interface設定	
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	1701 (default 1701)

## 第15章 L2TPv3 機能

### . L2TPv3 設定例2 (L2TP トンネル二重化)

#### Primary セッション側

##### L2TPv3 Xconnect 設定をおこないます。

- 「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ください。
- 「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 受信インターフェース」は LAN 側のインターフェースを指定します。**LAN 側インターフェースには 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。ただし、Secondary 側と同じ値は設定できません。
- 「Reschedule Interval 設定」に任意の Interval 時間を設定してください。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おこないます。

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	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

#### Secondary セッション側

##### L2TPv3 Xconnect 設定をおこないます。

- Primary セッションと同じ要領で設定してください。

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 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 設定例2 (L2TPトンネル二重化)

L2TPv3 Group設定をおこないます。

- ・「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	<input type="text" value="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

L2TPv3 Tunnel Setup の起動

設定後が終わりましたら L2TPv3 機能の起動 / 停止設定をおこないます。

「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 16 章

---

---

L2TPv3 フィルタ機能

## . L2TPv3 フィルタ 機能概要

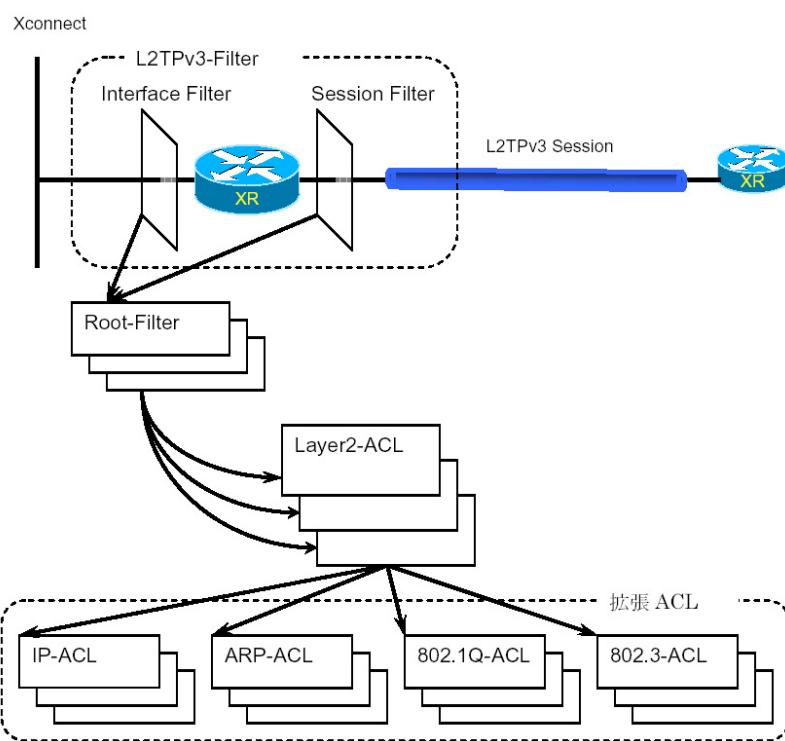
**L2TPv3 フィルタ概要**

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おこないます。

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。

### . 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おこないます。

##### 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。

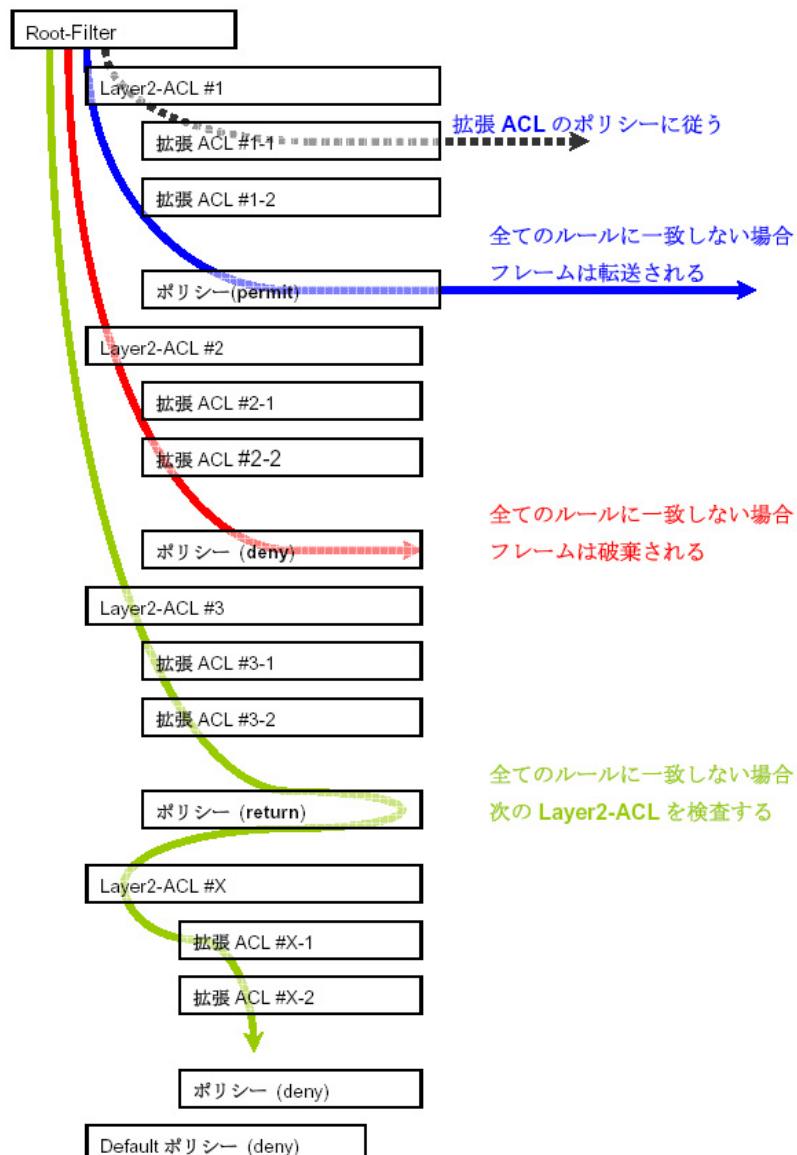
##### 2)破棄(deny)

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



## . 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おこない、最初に条件に一致したもの (1st match) に対して以下の評価をおこないます。

- ・拡張 ACLがない場合

該当 Layer2 ACL のポリシーに従い、deny/permit/returnをおこないます。

- ・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 にて検索をおこない、以下の評価をおこないます。

- 1) 拡張 ACL に一致する場合、拡張 ACL の policy に従い deny/permit をおこないます。

- 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をおこないます。

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。

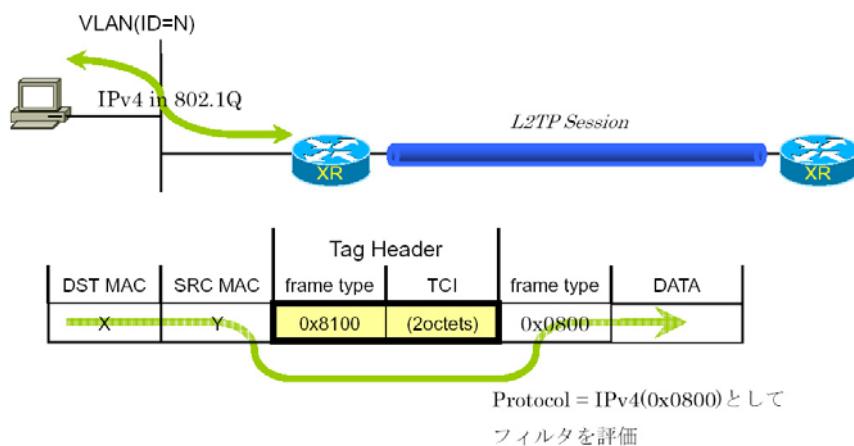
### フィルタ処理順序

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 / あて先 MAC アドレスのチェックをおこな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、フレームの転送はおこなわれませんのでご注意ください。

### 802.1Q タグヘッダ

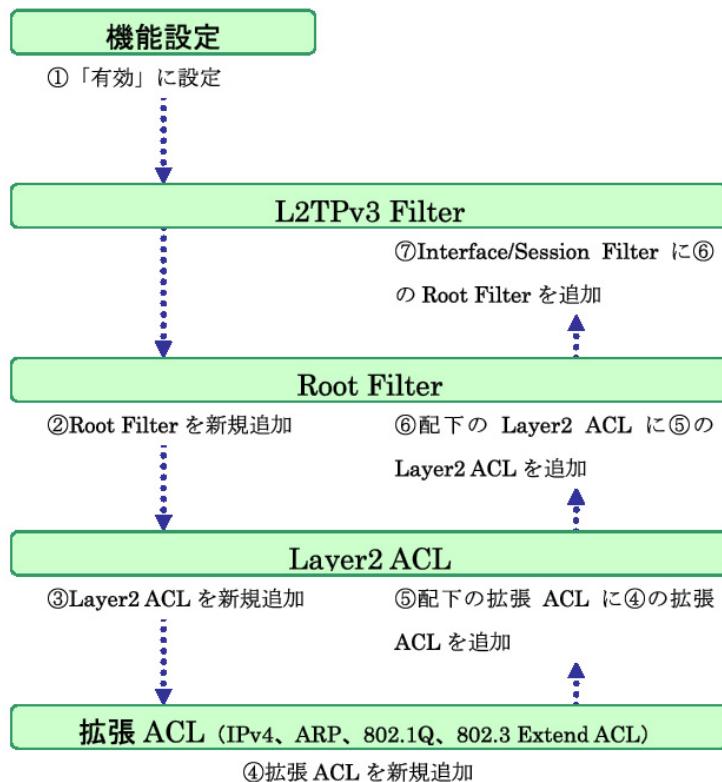
Xconnect Interface が VLAN(802.1Q)であるフレームをフィルタリングする場合、タグヘッダについては、フィルタの評価対象から除外し、タグヘッダに続くフィールドから再開します(下図参照)。



## . 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ください。

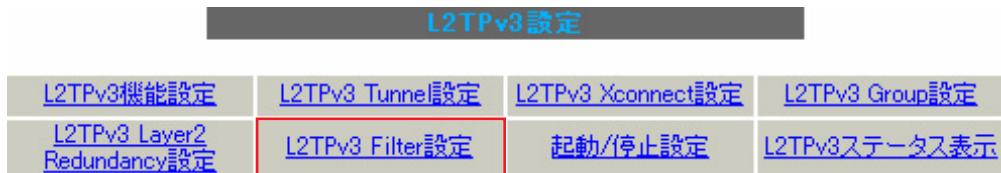
## 【L2TPv3 Filter の設定順序】



## 第16章 L2TPv3 フィルタ機能

### . 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おこないます。



#### 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。

#### 機能設定

##### \* 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。

本機能	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
-----	--

[リセット](#) [設定](#) [戻る](#)

#### 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。

## 第16章 L2TPv3 フィルタ機能

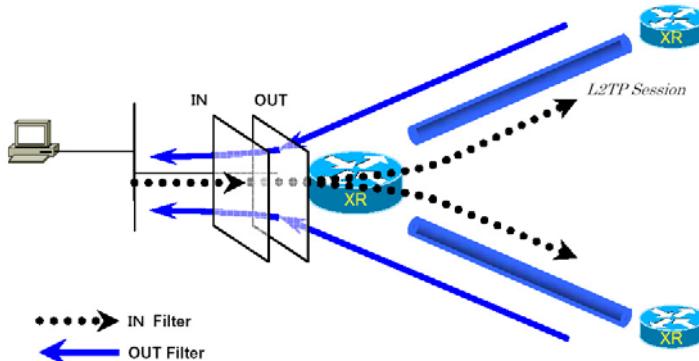
### . L2TPv3 Filter 設定

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

Interface Filter				
Index	Interface	IN Filter	OUT Filter	edit
1	eth0	Root-1	Root-2	<a href="#">edit</a>

Interface Filter は、Root Filter を Xconnect Interface に対応づけてフィルタリングをおこないます。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。

L2TPv3 Filter 適用設定

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

リセット 設定 戻る

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。

## 第16章 L2TPv3 フィルタ機能

### . L2TPv3 Filter 設定

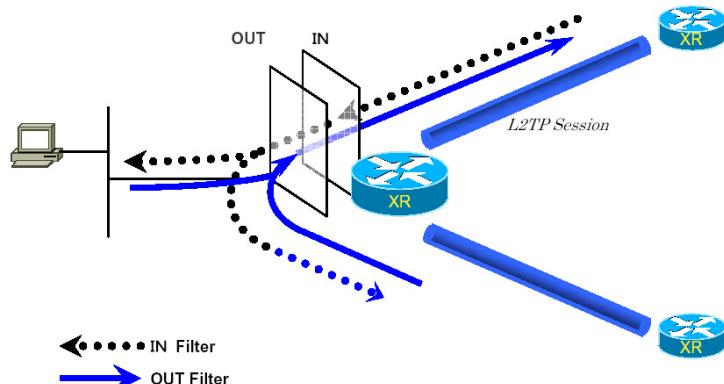
#### Session Filter

Session Filter

Index	Peer ID	RemoteEND ID	IN Filter	OUT Filter	edit
1	192.168.0.1	1	Root-2	Root-3	<a href="#">edit</a>
2	192.168.0.2	2	Root-3	Root-4	<a href="#">edit</a>

Session Filterは、Root FilterをSessionに関連づけてフィルタリングをおこないますので、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。

L2TPv3 Filter適用設定

PeerID : RemoteEndID	192.168.0.1:1
ACL(in)	Root-2
ACL(out)	Root-3

[リセット](#) [設定](#) [戻る](#)

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。

## 第16章 L2TPv3 フィルタ機能

### . 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。

L2TPv3 Filter一覧表示

Index	Root Filter Name	edit	layer2	del
1	Root-1	<a href="#">edit</a>	<a href="#">layer2</a>	<input type="checkbox"/>
2	Root-2	<a href="#">edit</a>	<a href="#">layer2</a>	<input type="checkbox"/>
3	Root-3	<a href="#">edit</a>	<a href="#">layer2</a>	<input type="checkbox"/>
4	Root-4	<a href="#">edit</a>	<a href="#">layer2</a>	<input type="checkbox"/>

(最大512個まで設定できます)

[リセット](#) [追加](#) [削除](#) [戻る](#)

#### Root Filter を追加する

画面下の「追加」ボタンをクリックします。

L2TPv3 Filter設定

Root Filter Name	<input type="text"/>
Default Policy	deny <a href="#">▼</a>

[リセット](#) [設定](#) [戻る](#)

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  
択してください。

#### Root Filter を編集する

一覧表示内の「edit」をクリックします。

L2TPv3 Filter設定

Index	1
Root Filter Name	<input type="text"/> Root-1
Default Policy	deny <a href="#">▼</a>

[リセット](#) [設定](#) [戻る](#)

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。

## . 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	<a href="#">L2ACL-1</a>	permit	00:11:22:33:44:55		IPv4	<a href="#">edit</a>	<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	<a href="#">L2ACL-1</a>

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16章 L2TPv3 フィルタ機能

### . 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	<a href="#">edit</a>	<a href="#">extend</a>	<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	---- <input type="button" value="▼"/>
Source MAC	<input type="text"/>
Destination MAC	<input type="text"/>
Type/Length	---- <input type="button" value="▼"/> 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ください。

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 です。

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 を指定することができます。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	<input type="text" value="L2ACL-1"/>
Policy	permit <input type="button" value="▼"/>
Source MAC	<input type="text" value="00:11:22:33:44:55"/>
Destination MAC	<input type="text"/>
Type/Length	IPv4 <input type="button" value="▼"/> or <input type="text" value="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。

## 第16章 L2TPv3 フィルタ機能

### . 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	<a href="#">edit</a>	<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="▼"/>

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="▼"/>

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16章 L2TPv3 フィルタ機能

### . 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		<a href="#">edit</a>	<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="▼"/>
Source IP	<input type="text"/>
Destination IP	<input type="text"/>
TOS	<input type="text"/> [0-0xff]
IP Protocol	---- <input type="button" value="▼"/> 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能です。)

<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と同様に設定してください。

##### TOS

TOS値を16進数で指定します。

指定可能な範囲：00-ffです。

##### 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ください。

指定可能な範囲：0-255です。

##### 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です。

##### 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です。

### . 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	IPv4-1
Policy	permit ▼
Source IP	192.168.0.100
Destination IP	192.168.0.200
TOS	[ ] [0-0xff]
IP Protocol	TCP ▼ or [ ] [0-255]
Source Port	[ ] [1-65535]
Destination Port	[ ] [1-65535]
ICMP Type	[ ] [0-255]
ICMP Code	[ ] [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16章 L2TPv3 フィルタ機能

### . 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	<a href="#">edit</a>	<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="▼"/>
OPCODE	---- <input type="button" value="▼"/> 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。無指定でも可能です。  
10進数指定の場合は右側の入力欄に指定値を入力してください。  
指定可能な範囲：0-65535です。

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ください。

#### 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能です。)

<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ください。

#### 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="▼"/>
OPCODE	---- <input type="button" value="▼"/> 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16章 L2TPv3 フィルタ機能

### . 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	<a href="#">edit</a>	<a href="#">extend</a>	<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	---- <input type="button" value="▼"/>
VLAN ID	<input type="text"/> [0-4095]
Priority	<input type="text"/> [0-7]
Ethernet Type	---- <input type="button" value="▼"/> 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です。

<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 です。

##### Ethernet Type

カプセリングされたフレームの 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。 無指定でも設定可能です。 16 進数指定の場合は右側の入力欄に指定値を入力してください。

指定可能な範囲 : 0600-f f f f です。

IPv4、 ARP を指定すると配下の拡張 ACL に IPv4 Extend ACL、 ARP Extend ACL を指定することが出来ます。

#### 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 <input type="button" value="▼"/>
VLAN ID	10 [0-4095]
Priority	<input type="text"/> [0-7]
Ethernet Type	IPv4 <input type="button" value="▼"/> 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。

## 第16章 L2TPv3 フィルタ機能

### . 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	<a href="#">edit</a>	<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="▼"/>

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="▼"/>

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16章 L2TPv3 フィルタ機能

### . 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		<a href="#">edit</a>	<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	---- <input type="button" value="▼"/>
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 です。

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 です。

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 <input type="button" value="▼"/>
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。

## 第16章 L2TPv3 フィルタ機能

### . 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	---- <input type="checkbox"/> detail表示 / リセット	表示する	カウンタリセット
arp 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_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	---- <input type="checkbox"/> detail表示 / リセット	表示する	カウンタリセット
interface Filter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
session Filter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
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

## 第16章 L2TPv3 フィルタ機能

### . 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 17 章

---

---

SYSLOG 機能

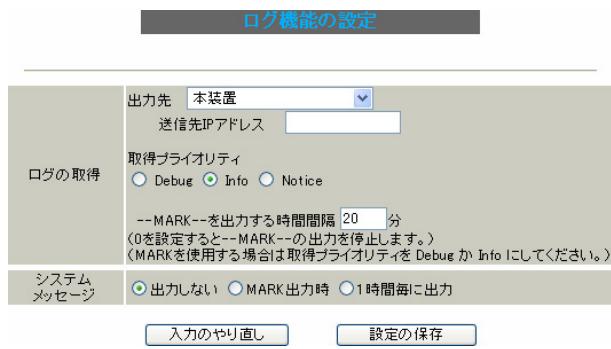
### syslog機能の設定

本装置は、syslogを出力・表示することが可能です。また、他のsyslogサーバに送出することもできます。

さらに、ログの内容を電子メールで送ることも可能です。電子メール設定は、「第33章 各種システム設定」をご参照ください。

#### syslog取得機能の設定

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



#### <ログの取得>

##### 出力先

syslogの出力先を選択します。

##### 「本装置」

本装置でsyslogを取得する場合に選択します。

##### 「SYSLOGサーバ」

syslogサーバに送信するときに選択します。

##### 「本装置とSYSLOGサーバ」

本装置とsyslogサーバの両方でsyslogを管理します。

##### 送信先IPアドレス

syslogサーバのIPアドレスを指定します。

##### 取得プライオリティ

ログ内容の出力レベルを指定します。

プライオリティの内容は以下のようになります。

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

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

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

#### <システムメッセージ>

本装置のシステム情報を定期的に出力することができます。

以下から選択してください。

##### 出力しない

システムメッセージを出力しません。

##### MARK出力時

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

##### 1時間ごとにOutput

1時間ごとにシステムメッセージを出力します。

出力される情報は下記の内容です。

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

- cpu:0.00  
cpuのロードアベレージです。  
1に近いほど高負荷を表し、1を超えている場合は過負荷の状態を表します。
- mem:28594176  
空きメモリ量(byte)です。

## 第17章 syslog機能

### syslog機能の設定

・session:0/2 (XX/YY)

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

0 (XX)

現在EstablishしているTCPセッションの数

2 (YY)

本装置が現在キャッシュしている全てのセッション数

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-430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

#### syslogのメール送信機能の設定

ログの内容を電子メールで送信したい場合の設定です。

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

#### <シスログのメール送信>

シスログのメール送信	
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"/> admin@localhost
件名	<input type="text"/> Log keyword detection 文字列は1行に255文字まで、最大32個(行)までです。
検出文字列の指定	<input type="text"/>

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

#### ログファイルの取得

ログは「システム設定」「ログの表示」に表示されます。

保存されるファイルは最大で6つです。

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。古いログファイルから順に削除されています。

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

#### ログファイルの取得

ブラウザの「リンクを保存する」を使用して取得して下さい

最新ログ

バックアップログ1  
バックアップログ2  
バックアップログ3  
バックアップログ4  
バックアップログ5  
バックアップログ6

# 第 18 章

---

---

攻擊檢出機能

## 攻撃検出機能の設定

### 攻撃検出機能の概要

攻撃検出機能とは、外部から LANへの侵入や XR-430 を踏み台にした他のホスト・サーバ等への攻撃を仕掛けられた時などに、そのログを記録しておくことができる機能です。

検出方法には、統計的な面から異常な状態を検出する方法やパターンマッチング方法などがあります。XR-430ではあらかじめ検出ルールを定めていますので、パターンマッチングによって不正アクセスを検出します。ホスト単位の他、ネットワーク単位で監視対象を設定できます。

### ログの出力

攻撃検出口ログも、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」で、ログを確認してください。

### 攻撃検出機能の設定

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

#### 攻撃検出サービスの設定

使用するインターフェース	<input type="radio"/> Ether 0で使用する <input checked="" type="radio"/> Ether 1で使用する <input type="radio"/> PPP/PPPoEで使用する
検出対象となる IPアドレス	any
<input type="button" value="入力のやり直し"/> <input type="button" value="設定の保存"/>	

#### 使用するインターフェース

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

#### 検出対象となる IP アドレス

攻撃を検出したい送信先ホストの IP アドレス、ネットワークアドレスまたは、全ての IP アドレスを指定できます。

<入力例>

ホスト単体の場合

**192.168.0.1/32** (“ /32 ”を付ける)

ネットワーク単位の場合

**192.168.0.0/24** (“ /マスクビット値 ”を付ける)

すべての IP アドレスの場合

**any**

「any」を設定すると、すべてのアドレスが検出対象となります。

入力が終わりましたら「設定の保存」をクリックして設定完了です。

**機能を有効にするには「各種サービスの設定」トップに戻り、サービスを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 19 章

---

---

SNMP エージェント機能

## 第19章 SNMPエージェント機能

### SNMPエージェント機能の設定

SNMPエージェントを起動すると、SNMPマネージャからXR-430のMIB Ver.2(RFC1213)の情報を取得することができます。

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

**SNMP機能の設定**

SNMPマネージャ	192.168.0.0/24 SNMPマネージャを使いたいネットワーク範囲(ネットワーク番号/サブネット長)又はSNMPマネージャのIPアドレスを指定して下さい。
コミュニティ名	community
SNMP TRAP	<input type="radio"/> 使用する <input checked="" type="radio"/> 使用しない
SNMP TRAPの送信先IPアドレス	[入力欄]
SNMP TRAPの送信元	<input checked="" type="radio"/> 指定しない <input type="radio"/> IPアドレス <input type="radio"/> インターフェース [入力欄]
送信元	<input checked="" type="radio"/> 指定しない <input type="radio"/> IPアドレス [入力欄]

[入力のやり直し](#) [設定の保存](#)

#### SNMPマネージャ

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

#### コミュニティ名

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

#### SNMP TRAP

「使用する」を選択すると、SNMP TRAPを送信できるようになります。

#### SNMP TRAPの送信先IPアドレス

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

#### SNMP TRAPの送信元

Trapフレーム内のAgent addressを指定することができます。

##### ・指定しない

本装置のIPアドレスが自動的に設定されます。

##### ・IPアドレス

ボックス内に本装置の任意のIPアドレスを設定してください。

#### ・インターフェース

ボックス内に本装置の任意のインターフェース名を入力してください。  
入力可能なインターフェースはEthernetまたはPPP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。**

## SNMP エージェント機能の設定

### SNMP TRAP を送信するトリガーについて

以下のものに関して、SNMP TRAP を送信します。

- ・ Ethernet インタフェースの up、down
- ・ PPP インタフェースの up、down
- ・ 下記の各機能の up、down
  - DNS
  - DHCP サーバー
  - DHCP リレー
  - PLUTO(IPSec の鍵交換をおこなう IKE 機能)
  - UPnP
  - RIP
  - OSPF
  - L2TPv3
  - SYSLOG
  - 攻撃検出
  - NTP
  - VRRP
- ・ SNMP TRAP 自身の起動、停止

# 第 20 章

---

---

NTP サービス

## NTP サービスの設定方法

XR-430 は、NTP クライアント / サーバ機能を持っています。インターネットを使った時刻同期の手法の一つである NTP(Network Time Protocol)を用いて NTP サーバと通信をおこない、時刻を同期させることができます。

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

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

### 問合せ先 NTP サーバ (IP アドレス / FQDN)

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

NTP サーバの場所は 2 箇所設定できます。

これにより、XR-430 が NTP クライアント / サーバとして動作できます。

NTP サーバの IP アドレスもしくは FQDN を入力しない場合は、XR-430 は NTP サーバとしてのみ動作します。

### Polling 間隔

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

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

<例 4 : 16 秒、 6 : 64 秒、 ... 10 : 1024 秒>

数字は、4 ~ 17(16-131072 秒)の間で設定出来ます。Polling 間隔の初期設定は (Min)6 (64 秒) (Max)10 (1024 秒) です。

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

### 時刻同期タイムアウト時間

サーバ応答の最大待ち時間を 1-10 秒の間で設定できます。

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

入力が終わりましたら「設定の保存」をクリックして設定完了です。

機能を有効にするには「各種サービスの設定」  
トップに戻り、サービスを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。

### NTP サービスの設定方法

#### 基準 NTP サーバについて

基準となる NTP サーバには以下のようなものがあります。

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

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

#### NTP クライアントの設定方法

各ホスト / サーバーを NTP クライアントとして XR-430 と時刻同期させる方法は、OS により異なります。

##### Windows 9x/Me/NT の場合

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

##### Windows 2000 の場合

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

##### Windows XP の場合

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

##### Macintosh の場合

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

##### Linux の場合

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

# 第 21 章

---

---

VRRP 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	

[ 入力のやり直し ] [ 設定の保存 ]

#### 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 グループ内での「マスター ルータ」となり、他のルータは「バックアップ ルータ」となります。  
1 ~ 255 の間で指定します。

#### IP アドレス

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

#### インターバル

VRRP パケットを送出する間隔を設定します。単位は秒です。1 ~ 255 の間で設定します。

VRRP パケットの送受信によって、VRRP ルータの状態を確認します。

#### Auth\_Type

認証形式を選択します。

「PASS」または「AH」を選択できます。

#### Password

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

入力が終わったら「設定の保存」をクリックして設定完了です。

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

#### ステータスの表示

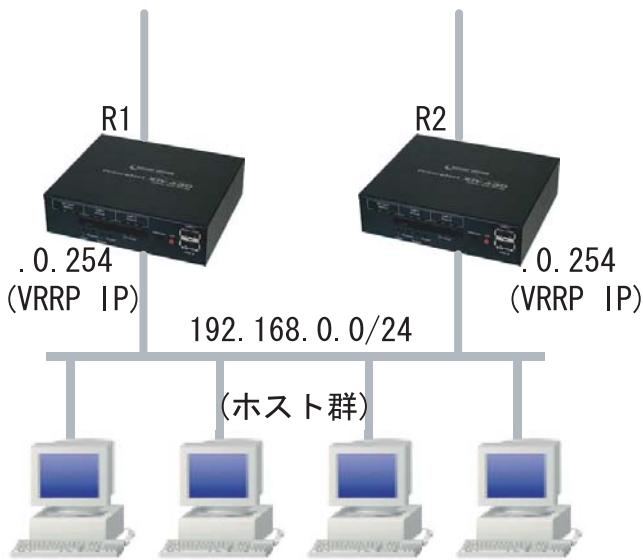
VRRP 機能設定画面上部にある「現在の状態」をクリックすると、VRRP 機能の動作状況を表示するウィンドウがポップアップします。

## 第21章 VRRP サービス

### . VRRP の設定例

下記のネットワーク構成でVRRPサービスを利用するときの設定例です。

#### ネットワーク構成



#### 設定条件

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

#### ルータ「R1」の設定例

No.	使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
1	Ether 0	使用しない	1	100	192.168.0.254	1	指定しない	

#### ルータ「R2」の設定例

No.	使用するインターフェース	仮想MACアドレス	ルータID	優先度	IPアドレス	インターバル	Auth_Type	password
1	Ether 0	使用しない	1	50	192.168.0.254	1	指定しない	

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

# 第 22 章

---

---

アクセスサーバ機能

## 第22章 アクセスサーバ機能

### . アクセスサーバ機能について

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

例えば、アクセスサーバとして設定したXR-430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。



本装置のアクセスサーバ設定で使用するインターフェースはモバイル通信インターフェースです。

使用できるモバイル通信モジュールは“着信対応”的以下の2つです。

タイプ	提供元	型番	着信形態	
			回線交換着信	IPパケット着信
CF	NTT DoCoMo	P2403		
CF	NTT DoCoMo	N2502	×	

#### IPパケット着信について

NTT DoCoMoの以下のサービスを利用して着信をおこないます。

NTTドコモ ビジネスマopera

アクセスプレミアム FOMAタイプ - オプションサービス -

[OPTION] FOMAパケット電話番号着信機能・IP着信機能

サービスの詳細については下記のHPをご覧ください。

[http://www.nttdocomo.biz/b-mopera/intro/prm\\_foma/option.html#d](http://www.nttdocomo.biz/b-mopera/intro/prm_foma/option.html#d)

パケット着信の場合は、既存のアクセスサーバ設定とは動作が異なります。

・ユーザ認証はおこないません。

上記サービス内でIPアドレスと電話番号を制限します。

・アクセスサーバ(本装置)のIPアドレスは、IP着信機能で割当てられた電話番号と紐付いたIPアドレス(ドコモ契約登録必要)を指定します。

・クライアントのIPアドレスは、FOMAネットワーク側に依存するので、設定はおこないません。

## 第22章 アクセスサーバ機能

### . アクセスサーバ機能の設定

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

**アクセスサーバ設定**

アクセスサーバ	<input checked="" type="radio"/> 使用しない <input type="radio"/> 使用する		
着信するモバイル通信インターフェース	None 指定可能な接続ポート <input type="button" value="▼"/>		
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	<input type="text"/>		
No.	アカウント	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"/>

**設定の保存**

#### アクセスサーバの設定

アクセスサーバ

アクセスサーバ機能の使用 / 不使用を選択します。

#### 着信するモバイル通信インターフェース

着信時に使用するモバイル通信インターフェースをプルダウンメニューから選択します。

選択可能なインターフェースは“着信対応”のみです。また、プルダウンに表示されるのは装着時のみです。

着信するモバイル通信インターフェース	None 指定可能な接続ポート <input type="button" value="▼"/>
指定可能な接続ポート CF (FOMA P2403)	

(画面は表示例です)

#### アクセスサーバ(本装置)のIPアドレス

リモートアクセスされた時のXR-430自身のIPアドレスを入力します。各Ethernetポートのアドレスとは異なるプライベートアドレスを設定してください。**なお、サブネットのマスクビット値は24ビット(255.255.255.0)に設定されています。**

#### クライアントのIPアドレス

XR-430にリモートアクセスしてきたホストに割り当てるIPアドレスを入力します。

上記の「アクセスサーバのIPアドレス」で設定したものと同じネットワークとなるアドレスを設定してください。

#### モデムの速度

XR-430とモデムの間の通信速度を選択します。

#### 着信のためのATコマンド

モデムが外部から着信する場合、ATコマンドが必要な場合があります。その場合は、ここでATコマンドを入力してください。

コマンドについては、各モデムの説明書をご確認ください。

#### ユーザーアカウントの設定

設定画面の下側でユーザーアカウントの設定をおこないます。

##### アカウント

##### パスワード

外部からリモートアクセスする場合の、ユーザー 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。

##### 削除

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

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

設定後は、外部からダイヤルアップ接続をおこなってください。

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

#### アカウント設定上の注意

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

ユーザー名が重複しないように設定してください。

# 第 23 章

---

---

スタティックルーティング

## 第23章 スタティックルーティング

### スタティックルーティング設定

本装置は、最大 256 エントリのスタティックルートを登録できます。

Web 設定画面「スタティックルート設定」をクリックして、以下の画面から設定します。

スタティックルート設定

経路情報表示  
No.1~16まで

No.	アドレス	ネットマスク	インターフェース/ゲートウェイ	ディスタンス <1-255>	削除
1					<input type="button" value="□"/>
2					<input type="button" value="□"/>
3					<input type="button" value="□"/>
4					<input type="button" value="□"/>
5					<input type="button" value="□"/>
6					<input type="button" value="□"/>
7					<input type="button" value="□"/>
8					<input type="button" value="□"/>
9					<input type="button" value="□"/>
10					<input type="button" value="□"/>
11					<input type="button" value="□"/>
12					<input type="button" value="□"/>
13					<input type="button" value="□"/>
14					<input type="button" value="□"/>
15					<input type="button" value="□"/>
16					<input type="button" value="□"/>

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

設定/削除の実行

#### 入力方法

##### アドレス

あて先ホストのアドレス、またはネットワークアドレスを入力します。

##### ネットマスク

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

##### <入力例>

29 ビットマスクの場合 : 255.255.255.248

単一ホストで指定した場合 : 255.255.255.255

##### インターフェース / ゲートウェイ

ルーティングを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。

PPP/PPPoE や GRE インタフェースを設定する

ときはインターフェース名だけの設定となります。 167

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

##### ・インターフェース

“ppp6”

##### ・ゲートウェイ

“クライアントに割り当てる IP アドレス”

通常は、インターフェース / ゲートウェイのどちらかのみ設定できます。

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

##### 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。

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つずつ設定番号がズれて設定が更新されます。

### スタティックルーティング設定

#### 設定を削除する

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

#### デフォルトルートを設定する

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

#### ルーティング情報を確認する

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

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

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

# 第 24 章

---

---

ソースルーティング

## ソースルーティング設定

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

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

ソースルート設定は、Web 設定画面「ソースルート設定」でおこないます。

1 はじめに、ソースルートのテーブル設定をおこないます。

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

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。

## 第24章 ソースルーティング

### ソースルーティング設定

2 画面右上の「ソースルートのルール設定へ」のリンクをクリック指定化の画面を開きます。

[ソースルートのルール設定](#)

ソースルートのテーブル設定△

※ NOが赤色の設定は現在無効です

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

[入力のやり直し](#) [設定の保存](#)

送信元ネットワークアドレス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ー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。

**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。

# 第 25 章

---

---

NAT 機能

### . XR-430 の NAT 機能について

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

XR-430 は以下の3つのNAT機能をサポートしています。

#### IPマスカレード機能

複数のプライベートアドレスを、ある1つのグローバルアドレスに変換する機能です。グローバルアドレスはXR-430のインターネット側ポートに設定されたものを使います。またLANのプライベートアドレス全てが変換されることになります。この機能を使うと、グローバルアドレスを1つしか持っていないくとも複数のコンピュータからインターネットにアクセスすることができるようになります。

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

#### 送信元NAT機能

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

## . バーチャルサーバ設定

NAT環境下において、LANからサーバを公開するときなどの設定をおこないます。  
256まで設定できます。「バーチャルサーバ設定画面インデックス」のリンクをクリックしてください。

### 設定方法

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

No.	サーバのアドレス	公開するグローバルアドレス	プロトコル	ポート	インターフェース	削除
1			全て			<input type="checkbox"/>
2			全て			<input type="checkbox"/>
3			全て			<input type="checkbox"/>
4			全て			<input type="checkbox"/>
5			全て			<input type="checkbox"/>
6			全て			<input type="checkbox"/>
7			全て			<input type="checkbox"/>
8			全て			<input type="checkbox"/>
9			全て			<input type="checkbox"/>
10			全て			<input type="checkbox"/>
11			全て			<input type="checkbox"/>
12			全て			<input type="checkbox"/>
13			全て			<input type="checkbox"/>
14			全て			<input type="checkbox"/>
15			全て			<input type="checkbox"/>
16			全て			<input type="checkbox"/>

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

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

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

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

プロトコル  
サーバのプロトコルを選択します。

### ポート

サーバが公開するポート番号を入力します。範囲で指定することも可能です。範囲で指定するときは、ポート番号を“:”で結びます。

<例>ポート20番から21番を指定する 20:21

### インターフェース

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 インタフェース名一覧」をご参照ください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

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

### 設定情報の確認

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

### 設定を挿入する

バーチャルサーバ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

			全て		
--	--	--	----	--	--

最も左の欄に任意の番号を指定して設定すると、その番号に設定が挿入されます。

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

### 設定を削除する

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

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

## . 送信元NAT設定

**設定方法**

Web設定画面「NAT設定」、「送信元NAT」をクリックして、以下の画面から設定します。  
256まで設定できます。「送信元NAT設定画面インデックス」のリンクをクリックしてください。

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

設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。

送信元NAT設定画面インデックス  
001- 017- 033- 049- 065- 081- 097- 113-  
129- 145- 161- 177- 193- 209- 225- 241-

**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」をご参照ください。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

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

**設定情報の確認**

「情報表示」をクリックすると、現在の送信元NAT設定の情報が一覧表示されます。

**設定を挿入する**

送信元NAT設定を追加する場合、任意の場所に挿入することができます。

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。

**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。

## . バーチャルサーバの設定例

## WWWサーバを公開する際のNAT設定例

## NATの条件

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

## LAN構成

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

## 設定画面での入力方法

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

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

## 設定の解説

No.1 :

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

## FTPサーバを公開する際のNAT設定例

## NATの条件

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

## LAN構成

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

## 設定画面での入力方法

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

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

## 設定の解説

No.1 :

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

No.2 :

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

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

## 第25章 NAT機能

### . バーチャルサーバの設定例

#### PPTP サーバを公開する際のNAT設定例

##### NATの条件

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

##### LAN構成

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

##### 設定画面での入力方法

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

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

バーチャルサーバ設定以外に、適宜パケットフィルタ設定をおこなってください。

特にステートフルパケットインスペクション機能を使っている場合には、「転送フィルタ」で明示的に、使用ポートを開放する必要があります。

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

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

2 IPマスカレードを有効にします。

「第5章 インターフェース設定」を参照してください。

3 「バーチャルサーバ設定」で以下の様に設定してください。

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

設定の解説

No.1

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

No.2、3

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

No.4、5

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

No.6、7

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

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

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

## . 送信元NATの設定例

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

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

例えば上記のような送信元NAT設定をおこなうと、

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

という設定になります。

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

<設定例> 192.168.254.0/24

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

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

## 補足：ポート番号について

よく使われるポートの番号については、下記の表

を参考してください。

詳細はRFC1700(Oct. 1994)を参照してください。

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

# 第 26 章

---

---

パケットフィルタリング機能

## 第26章 パケットフィルタリング機能

### . 機能の概要

XR-430はパケットフィルタリング機能を搭載しています。

パケットフィルタリング機能を使うと、以下のようなことができます。

- ・外部から LAN に入ってくるパケットを制限する。
- ・LAN から外部に出ていくパケットを制限する。
- ・XR-430 自身が受信するパケットを制限する。
- ・XR-430 自身から送信するパケットを制限する。
- ・Web 認証機能を使用しているときにアクセス可能にする

またフィルタリングは以下の情報に基づいて条件を設定することができます。

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

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

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

## 第26章 パケットフィルタリング機能

### . XR-430 のフィルタリング機能について

XR-430 は、以下の 4 つの基本ルールについてフィルタリングの設定をおこないます。

- ・入力(input)
- ・転送(forward)
- ・出力(output)
- ・Web 認証フィルタ(authgw)

#### 入力(input)フィルタ

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

#### 転送(forward)フィルタ

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

#### 出力(output)フィルタ

本装置内部からインターネットや LAN などへのアクセスを制御したい場合には、この出力ルールにフィルタ設定をおこないます。

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

#### Web 認証(authgw) フィルタ

「Web 認証設定」機能を使用しているときに設定するフィルタです。

Web 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。

Web 認証機能については「第 31 章 Web 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 を外部に送出しないフィルタ設定
- ・外部から UPnP で接続されないようにする  
フィルタ設定

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

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定

入力・転送・出力・Web 認証フィルタの4種類がありますが、設定方法はすべて同じです。

設定可能な各フィルタの最大数は256です。各フィルタ設定画面の最下部にある「フィルタ設定画面インデックス」のリンクをクリックしてください。

#### 設定方法

Web 設定画面にログインします。「フィルタ設定」「入力フィルタ」「転送フィルタ」「出力フィルタ」「Web 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。

フィルタ設定									No.1~16まで			
No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート	ICMP type/code	LOG	削除	No.
1	eth0	パケット受信時	破棄	tcp				137:139		<input type="checkbox"/>	<input type="checkbox"/>	1
2	eth0	パケット受信時	破棄	udp				137:139		<input type="checkbox"/>	<input type="checkbox"/>	2
3	eth0	パケット受信時	破棄	tcp		137				<input type="checkbox"/>	<input type="checkbox"/>	3
4	eth0	パケット受信時	破棄	udp		137				<input type="checkbox"/>	<input type="checkbox"/>	4
5	eth1	パケット受信時	破棄	udp				1900		<input type="checkbox"/>	<input type="checkbox"/>	5
6	ppp0	パケット受信時	破棄	udp				1900		<input type="checkbox"/>	<input type="checkbox"/>	6
7	eth1	パケット受信時	破棄	tcp				5000		<input type="checkbox"/>	<input type="checkbox"/>	7
8	ppp0	パケット受信時	破棄	tcp				5000		<input type="checkbox"/>	<input type="checkbox"/>	8
9	eth1	パケット受信時	破棄	tcp				2869		<input type="checkbox"/>	<input type="checkbox"/>	9
10	ppp0	パケット受信時	破棄	tcp				2869		<input type="checkbox"/>	<input type="checkbox"/>	10
11		パケット受信時	許可	全て						<input type="checkbox"/>	<input type="checkbox"/>	11
12		パケット受信時	許可	全て						<input type="checkbox"/>	<input type="checkbox"/>	12
13		パケット受信時	許可	全て						<input type="checkbox"/>	<input type="checkbox"/>	13
14		パケット受信時	許可	全て						<input type="checkbox"/>	<input type="checkbox"/>	14
15		パケット受信時	許可	全て						<input type="checkbox"/>	<input type="checkbox"/>	15
16		パケット受信時	許可	全て						<input type="checkbox"/>	<input type="checkbox"/>	16
設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。												
		パケット受信時	許可	全て								
<input type="button" value="設定/削除の実行"/>												
<a href="#">転送フィルタ設定画面インデックス</a> <a href="#">001- 017- 033- 049- 065- 081- 097- 113-</a> <a href="#">129- 145- 161- 177- 193- 209- 225- 241-</a>												
(画面は「転送フィルタ」)												

#### インターフェース

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

#### 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。

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定

#### 送信元アドレス

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

#### LOG

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

#### <入力例>

单一の 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)

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。

#### 送信元ポート

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

#### <入力例>

ポート 1024 番から 65535 番を指定する場合。

**1024:65535**

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

(「全て」のプロトコルを選択して、ポート番号を指定することはできません。)

#### あて先アドレス

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

入力方法は、送信元 IP アドレスと同様です。

#### あて先ポート

フィルタリング対象とする、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。

#### 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。

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定

#### 設定情報の確認

「情報表示」をクリックすると、現在のフィルタ設定の情報が一覧表示されます。

入力フィルタ 情報表示										
No	type	ptks	bytes	target	log	prot	in	out	source	destination
1	IP	0	0	DROP	-	tcp	eth0	*	0.0.0.0/0	0.0.0.0/0 [tcp] dpts:137:139
2	IP	6	468	DROP	-	udp	eth0	*	0.0.0.0/0	0.0.0.0/0 [udp] dpts:137:139
3	IP	0	0	DROP	-	tcp	eth0	*	0.0.0.0/0	0.0.0.0/0 [tcp] spt:137
4	IP	0	0	DROP	-	udp	eth0	*	0.0.0.0/0	0.0.0.0/0 [udp] spt:137
5	IP	0	0	DROP	-	udp	eth1	*	0.0.0.0/0	0.0.0.0/0 [udp] dpt:1900
6	IP	0	0	DROP	-	udp	ppo0	*	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	ppo0	*	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	ppo0	*	0.0.0.0/0	0.0.0.0/0 [tcp] dpt:2869
11	REDIRECT	--	--	ACCEPT	-	tcp	eth1	*	www.yahoo.co.jp	0.0.0.0/0 [tcp] dpt:80

更新

#### 設定を挿入する

フィルタ設定を追加する場合、任意の場所に挿入する事ができます。

挿入は、設定テーブルの一番下にある行からおこないます。

										設定済の位置に新規に挿入したい場合は、以下の欄に設定して下さい。
			パケット受信時	許可	全て					

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つずつ設定番号がズれて設定が更新されます。

#### 設定を削除する

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

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定例

#### インターネットからLANへのアクセスを破棄する設定

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

#### フィルタの条件

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

#### LAN構成

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

#### 設定画面での入力方法

「入力フィルタ」で以下のように設定します。

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

「転送フィルタ」で以下のように設定します。

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

#### フィルタの解説

「入力フィルタ」「転送フィルタ」

No.1、2：

WANから来る、あて先ポートが1024から65535のパケットを通す。

No.3：

WANから来る、ICMPパケットを通す。

No.4：

上記の条件に合致しないパケットを全て破棄する。

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定例

#### WWWサーバを公開する際のフィルタ設定例

##### フィルタの条件

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

##### LAN構成

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

#### 設定画面での入力方法

「転送フィルタ」で以下のように設定します。

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

#### フィルタの解説

No.1 :

192.168.0.1のサーバにHTTPのパケットを通す。

No.2、3 :

WANから来る、あて先ポートが1024から65535のパケットを通す。

No.4 :

上記の条件に合致しないパケットを全て破棄する。

#### FTPサーバを公開する際のフィルタ設定例

##### フィルタの条件

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

##### LAN構成

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

#### 設定画面での入力方法

「転送フィルタ」で以下のように設定します。

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

#### フィルタの解説

No.1 :

192.168.0.2のサーバにftpのパケットを通す。

No.2 :

192.168.0.2のサーバにftpdataのパケットを通す。

No.3、4 :

WANから来る、あて先ポートが1024から65535のパケットを通す。

No.5 :

上記の条件に合致しないパケットを全て破棄する。

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

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定例

#### WWW、FTP、メール、DNS サーバを公開する際の フィルタ設定例

##### フィルタの条件

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

##### LAN 構成

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

##### 設定画面での入力方法

「転送フィルタ」で以下のように設定します。

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

##### フィルタの解説

No.1 :

192.168.0.1 のサーバに HTTP のパケットを通す。

No.2 :

192.168.0.2 のサーバに SMTP のパケットを通す。

No.3 :

192.168.0.2 のサーバに POP3 のパケットを通す。

No.4 :

192.168.0.3 のサーバに ftp のパケットを通す。

No.5 :

192.168.0.3 のサーバに ftpdata のパケットを通す。

No.6、7 :

192.168.0.4 のサーバに、domain のパケット (tcp, udp) を通す。

No.8、9 :

WAN から来る、あて先ポートが 1024 から 65535 のパケットを通す。

No.10 :

上記の条件に合致しないパケットを全て破棄する。

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

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定例

#### NetBIOSパケットが外部へ出るのを防止する フィルタ設定

##### フィルタの条件

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

##### LAN構成

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

##### 設定画面での入力方法

##### 「入力フィルタ」

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

##### 「転送フィルタ」

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

##### フィルタの解説

##### 「入力フィルタ」「転送フィルタ」

No.1 :

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

No.2 :

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

No.3 :

送信先ポートがtcpの137のパケットをEther0ポートで破棄する。

No.4 :

送信先ポートがudpの137のパケットをEther0ポートで破棄する。

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

##### フィルタの条件

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

##### LAN構成

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

##### 設定画面での入力方法

##### 「入力フィルタ設定」で以下のように設定します。

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

##### フィルタの解説

No.1 :

210.xxx.xxx.32/32(210.xxx.xxx.32/28のネットワークアドレス)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26章 パケットフィルタリング機能

### . パケットフィルタリングの設定例

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

##### フィルタの条件

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

##### LAN構成

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

##### 設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット受信時	破棄	全て	10.0.0.8			
2	ppp0	パケット受信時	破棄	全て	172.16.0.0/16			
3	ppp0	パケット受信時	破棄	全て	192.168.0.0/16			

##### フィルタの解説

No.1、2、3：

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

#### 外部からの攻撃を防止する総合的なフィルタリング設定

##### フィルタの条件

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

##### LAN構成

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

##### 設定画面での入力方法

「入力フィルタ設定」で以下のように設定します。

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

「出力フィルタ設定」で以下のように設定します。

No.	インターフェース	方向	動作	プロトコル	送信元アドレス	送信元ポート	あて先アドレス	あて先ポート
1	ppp0	パケット送信時	許可	全て	10.0.0.8			
2	ppp0	パケット送信時	許可	全て	172.16.0.0/16			
3	ppp0	パケット送信時	許可	全て	192.168.0.0/16			

##### フィルタの解説

「入力フィルタ」

No.1、2、3：

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

No.4：

WANからのブロードキャストパケットを受け取らない。smurf攻撃の防御

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。

「出力フィルタ」No1、2、3：

送信元IPアドレスが不正なパケットを送出しない。

WAN上にプライベートアドレスは存在しない。

## 第26章 パケットフィルタリング機能

### . パケットフィルタリングの設定例

#### PPTPを通すためのフィルタ設定

##### フィルタの条件

- WAN側からのPPTPアクセスを許可する。

##### LAN構成

- WAN側はPPPoE回線に接続する。

#### 設定画面での入力方法

「転送フィルタ設定」で以下のように設定します。

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

#### フィルタの解説

PPTPでは以下のプロトコル・ポートを使って通信します。

- プロトコル「GRE」
- プロトコル「tcp」のポート「1723」

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

## 第26章 パケットフィルタリング機能

### . 外部から設定画面にアクセスさせる設定

以下は、PPPoE で接続した場合の設定方法です。

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

2 「入力フィルタ」設定の中で、以下のような設定を追加してください。

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

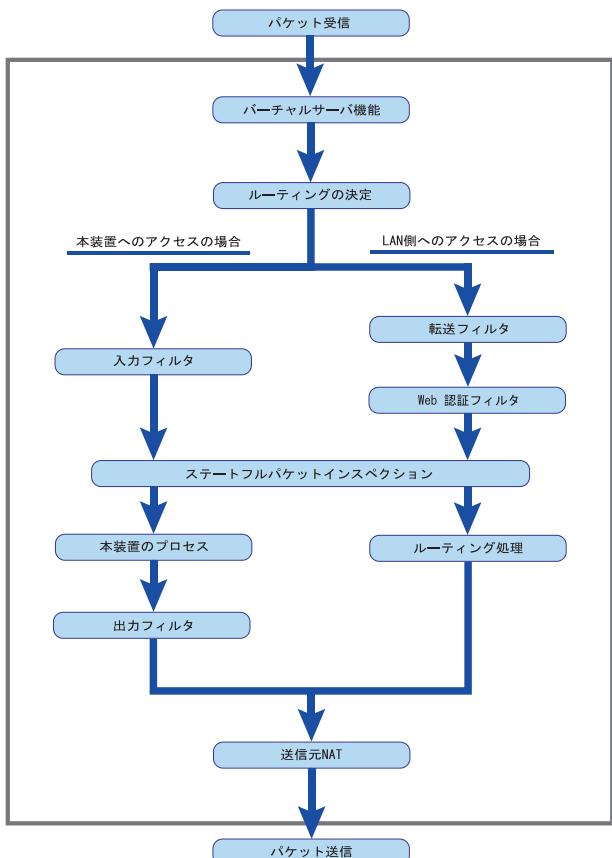
上記設定では、221.xxx.xxx.105 の IP アドレスを持つホストだけが、外部から本装置の設定画面へのアクセスが可能になります。

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

(**セキュリティ上たいへん危険ですので、この設定は推奨いたしません。)**

### 補足：NATとフィルタの処理順序について

XR-430における、NATとフィルタリングの処理方法は以下のようになっています。



(図の上部を WAN 側、下部を LAN 側とします。また LAN → WAN へ NAT をおこなうとします。)

- WAN 側からパケットを受信したとき、最初に「バーチャルサーバ設定」が参照されます。
- 「バーチャルサーバ設定」で静的 NAT 変換したあとに、パケットがルーティングされます。
- XR-430 自身へのアクセスをフィルタするときは「入力フィルタ」、XR-430 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、または XR-430 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)。

## 補足：ポート番号について

よく使われるポートの番号については、下記の表を参考にしてください。

詳細はRFC1700(Oct. 1994)を参照してください。

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

## 補足：フィルタのログ出力内容について

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

<入力パケットを破棄したときのログ出力例>

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

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

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

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

# 第 27 章

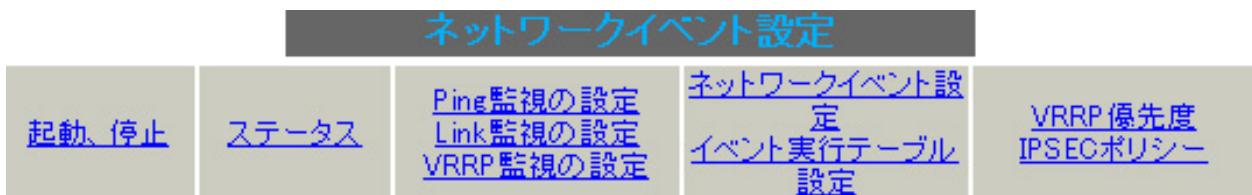
---

---

ネットワークイベント機能

### . 機能の概要

ネットワークイベントは、回線障害などのネットワーク状態の変化を検知し、それをトリガーとして特定のイベントを実行する機能です。



本装置では、以下のネットワーク状態の変化をトリガーとして検知することができます。

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

#### Ping監視

本装置から任意の宛先へ ping を送信し、その応答の有無を監視します。  
一定時間応答がなかった時にトリガーとして検知します。  
また再び応答を受信した時は、復旧トリガーとして検知します。

#### Link監視

Ethernet インタフェースや ppp インタフェースのリンク状態を監視します。  
監視するインターフェースのリンクがダウンした時にトリガーとして検知します。  
また再びリンクがアップした時は、復旧トリガーとして検知します。

#### VRRP監視

本装置の VRRP ルータ状態を監視します。  
指定したルータ ID の VRRP ルータがバックアップルータへ切り替わった時にトリガーとして検知します。  
また再びマスタールータへ切り替わった時は、復旧トリガーとして検知します。

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

- ・ VRRP 優先度変更
- ・ IPsec 接続切断

#### VRRP 優先度変更

トリガー検知時に、指定した VRRP ルータの優先度を変更します。  
またトリガー復旧時には、元の VRRP 優先度に変更します。

例えば、Ping 監視と連動して、PPPoE 接続先がダウンした時に、自身は VRRP バックアップルータに移行し、新マスタールータ側の接続へ切り替える、といった使い方ができます。

#### IPsec接続 / 切断

トリガー検知時に、指定した IPsec ポリシーを切断します。  
またトリガー復旧時には、IPsec ポリシーを再び接続します。

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

## 第27章 ネットワークイベント機能

### . 機能の概要

#### 本機能で使用する各種テーブルについて

本機能は複数のテーブル定義を連携させることによって実現しています。



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

これらのテーブルでは、監視対象、監視周期、障害検出した場合のトリガー番号を設定します。

ここで設定を有効(enable)にしたトリガー番号は、次の「 ネットワークイベント設定テーブル」のインデックス番号になります。

#### ネットワークイベント設定テーブル

このテーブルでは、トリガー番号とイベント番号の関連付けを定義します。

ここで設定したイベント番号は、次の「 イベント実行テーブル」のインデックス番号になります。

#### イベント実行テーブル

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

イベントの実行種別を「VRRP 優先度」に設定した場合は、次に「 VRRP 優先度テーブル」を索引します。設定したオプション番号は、テーブル のインデックス番号になります。

また、イベントの実行種別を「IPSEC ポリシー」に設定した場合は、次に「 IPsec 接続切断テーブル」を索引します。

設定したオプション番号は、テーブル のインデックス番号になります。

#### VRRP 優先度テーブル

このテーブルでは、VRRP 優先度を変更するルータ ID とその優先度を定義します。

#### IPsec 接続切断テーブル

このテーブルでは、IPsec 接続 / 切断をおこなう IPsec ポリシー番号、または IPsec インタフェース名を定義します。

## 第27章 ネットワークイベント機能

### . 各トリガーテーブルの設定

#### Ping監視の設定方法

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

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	

**ネットワークping設定**

enable  
チェックを入れることで設定を有効にします。

トリガー番号  
ping送信先から応答が無かった場合に検知するトリガーの番号(1 ~ 16)を指定します。  
本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

インターバル(秒)  
リトライ  
pingを発行する間隔を設定します。  
『インターバル』秒間に、『リトライ』回pingを発行する」という設定になります。  
この間、一度も応答が無かった場合にトリガーとして検知されます。

送信先アドレス  
pingを送信する先のIPアドレスを指定します。

最後に「設定の保存」をクリックして設定完了です。

## 第27章 ネットワークイベント機能

### . 各トリガーテーブルの設定

#### Link 監視の設定方法

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

**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

監視するインター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

インター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、インターフェースのリンク状態をチェックする」という設定になります。

この間、監視したリンク状態が全てダウンだった場合にトリガーとして検知されます。

#### 監視するデバイス名

リンク状態を監視するデバイスのインターフェース名を指定します。

Ethernet インタフェース名、または PPP インタフェース名を入力してください。

最後に「設定の保存」をクリックして設定完了です。

## . 各トリガーテーブルの設定

**VRRP 監視の設定方法**

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

**vrrp監視設定**

NO	enable	トリガー番号	インターバル	リトライ	VRRP ルータID
1	<input type="checkbox"/>	1	10	3	
2	<input type="checkbox"/>	2	10	3	
3	<input type="checkbox"/>	3	10	3	
4	<input type="checkbox"/>	4	10	3	
5	<input type="checkbox"/>	5	10	3	
6	<input type="checkbox"/>	6	10	3	
7	<input type="checkbox"/>	7	10	3	
8	<input type="checkbox"/>	8	10	3	
9	<input type="checkbox"/>	9	10	3	
10	<input type="checkbox"/>	10	10	3	
11	<input type="checkbox"/>	11	10	3	
12	<input type="checkbox"/>	12	10	3	
13	<input type="checkbox"/>	13	10	3	
14	<input type="checkbox"/>	14	10	3	
15	<input type="checkbox"/>	15	10	3	
16	<input type="checkbox"/>	16	10	3	

enable

チェックを入れることで設定を有効にします。

**トリガー番号**

監視する VRRP ルータがバックアップへ切り替わった場合に検知するトリガーの番号(1 ~ 16)を指定します。

本値は、「ネットワークイベント設定」テーブルでのインデックス番号となります。

**インターバル(秒)****リトライ**

VRRP ルータの状態を監視する間隔を設定します。『『インターバル』秒間に、『リトライ』回、VRRP のルータ状態を監視する』という設定になります。この間、監視した状態が全てバックアップ状態であった場合にトリガーとして検知されます。

**VRRP ルータ ID**

VRRP ルータ状態を監視するルータ ID を指定します。

最後に「設定の保存」をクリックして設定完了です。

## 第27章 ネットワークイベント機能

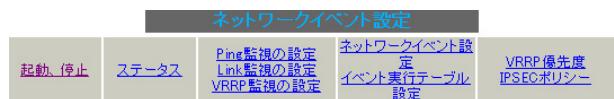
### . 各トリガーテーブルの設定

#### 各種監視設定の起動と停止方法

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

また設定の変更、追加、削除をおこなった場合は、サービスを再起動させてください。

**注)** 各監視設定で指定したトリガー番号は、「ネットワークイベント設定」テーブルでのインデックス番号となるため、それぞれの監視設定の間で同じトリガー番号が有効にならないように設定してください。



#### ネットワークイベントサービス設定

※各種設定は項目名をクリックして下さい。

ネットワークイベント	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
Ping監視	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
Link監視	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動
VRRP監視	<input checked="" type="radio"/> 停止 <input type="radio"/> 起動	停止中	再起動

動作変更

動作変更と再起動

## . 実行イベントテーブルの設定

ネットワークイベント設定テーブルの設定

設定画面上部の「ネットワークイベント設定」をクリックして、以下の画面から設定します。  
 (「イベント実行テーブル設定」画面のリンクをクリックしても以下の画面を開くことができます。)

**ネットワークイベント設定**

[イベント実行テーブル設定](#)

NO	トリガー番号	実行イベントテーブル番号
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5
6	6	6
7	7	7
8	8	8
9	9	9
10	10	10
11	11	11
12	12	12
13	13	13
14	14	14
15	15	15
16	16	16

[入力のやり直し](#) [設定の保存](#)

## トリガー番号

「Ping 監視の設定」、「Link 監視の設定」、「VRRP 監視の設定」で設定したトリガー番号を指定します。なお、複数のトリガー検知の組み合わせによって、イベントを実行させることも可能です。

## &lt;例&gt;

- ・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が、その場合は「\_」でイベント番号を繋ぎます。

## &lt;例&gt;

- ・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。

## 第27章 ネットワークイベント機能

### . 実行イベントテーブルの設定

#### イベント実行テーブルの設定

設定画面上部の「イベント実行テーブル設定」をクリックして、以下の画面から設定します。  
（「ネットワークイベント設定」画面のリンクをクリックしても以下の画面を開くことができます。）

イベント実行テーブル設定

ネットワークイベント設定△

NO	実行イベント設定	オプション設定
1	VRRP 優先度	1
2	VRRP 優先度	2
3	VRRP 優先度	3
4	VRRP 優先度	4
5	VRRP 優先度	5
6	VRRP 優先度	6
7	VRRP 優先度	7
8	VRRP 優先度	8
9	VRRP 優先度	9
10	VRRP 優先度	10
11	VRRP 優先度	11
12	VRRP 優先度	12
13	VRRP 優先度	13
14	VRRP 優先度	14
15	VRRP 優先度	15
16	VRRP 優先度	16

入力のやり直し 設定の保存

#### 実行イベント設定

実行されるイベントの種類を選択します。

「IPsec ポリシー」は、IPsec ポリシーの切断をおこないます。

「VRRP 優先度」は、VRRP ルータの優先度を変更します。

#### オプション設定

実行イベントのオプション番号です。

本値は、「VRRP 優先度変更設定」テーブル、または「IPSEC 接続切断設定」テーブルでのインデックス番号となります。

最後に「設定の保存」をクリックして設定完了です。

## . 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**

トリガー検知時に VRRP 優先度を変更する VRRP ルータ ID を指定します。

**優先度**

トリガー検知時に変更する VRRP 優先度を指定します。1-255 の間で設定してください。

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

最後に「設定の保存」をクリックして設定完了です。

**現在の設定状態の確認**

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

## 第27章 ネットワークイベント機能

### . 実行イベントのオプション設定

#### IPSEC 接続切断設定 テーブルの設定

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

**IPSEC 接続切断設定**  
[現在のIPSECの状態](#)

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

[入力のやり直し](#) [設定の保存](#)

IPSEC ポリシー番号、又はインターフェース名  
トリガー検知時に切断する IPsec ポリシーの番号、  
または IPsec インタフェース名を指定します。  
ポリシー番号は、範囲で指定することもできます。

<例> IPsec ポリシー 1 から 20 を切断する 1:20

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

#### 使用 IKE 連動機能

切断する IPsec ポリシーが使用する IKE と同じ IKE を使用する IPsec ポリシーが設定されている場合において、トリガー検知時にその IKE を使用する全ての IPsec ポリシーを切断する場合は、「使用する」を選択します。

ここで設定した IPsec ポリシーのみを切断する場合は「使用しない」を選択します。

#### 使用 interface 連動機能

本装置では、PPPoE 上で IPsec 接続している場合、  
PPPoE 接続時に自動的に IPsec 接続も開始されます。  
ネットワークイベント機能を使った IPsec 二重化において、バックアップ側の PPPoE 接続時に IPsec を自動接続させたくない場合には「使用しない」を選択します。

最後に「設定の保存」をクリックして設定完了です。

#### 現在の設定状態の確認

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

### . ステータスの表示

#### ステータスの表示

設定画面上部の「ステータス」をクリックして表示します。



#### トリガー情報

設定が有効なトリガー番号とその状態を表示します。

“ON”と表示されている場合は、トリガーを検知していない、またはトリガーが復旧している状態を表します。

“OFF”と表示されている場合は、トリガー検知している状態を表します。

#### イベント情報

##### ・ No.

イベント番号とその状態を表します。

“X”的表示は、トリガー検知し、イベントを実行している状態を表します。

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

“-”の表示は、無効なイベントです。

##### ・ トリガー

イベント実行の条件となるトリガー番号とその状態を表します。

##### ・ イベントテーブル

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

# 第 28 章

---

---

仮想インターフェース機能

## 仮想インターフェースの設定

主にバーチャルサーバ機能を利用する場合に、仮想インタ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="checkbox"/>
2					<input type="checkbox"/>
3					<input type="checkbox"/>
4					<input type="checkbox"/>
5					<input type="checkbox"/>
6					<input type="checkbox"/>
7					<input type="checkbox"/>
8					<input type="checkbox"/>
9					<input type="checkbox"/>
10					<input type="checkbox"/>
11					<input type="checkbox"/>
12					<input type="checkbox"/>
13					<input type="checkbox"/>
14					<input type="checkbox"/>
15					<input type="checkbox"/>
16					<input type="checkbox"/>

**インターフェース**  
仮想インターフェースを作成するインターフェース名を指定します。本装置のインターフェース名については、本マニュアルの「付録A」をご参照ください。

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

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

**ネットマスク**  
作成するインターフェースのネットマスクを指定します。

入力が終わりましたら「設定 / 削除の実行」をクリックして設定完了です。

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

### 設定を削除する

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

# 第 29 章

---

---

GRE 機能

## GRE の設定

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

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

### GRE の設定

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

GRE の設定																																	
GRE 設定 Index: <a href="#">一覧表示 [1-32]</a> <a href="#">[33-64]</a>																																	
GRE インタフェース 設定	GRE1	GRE2	GRE3	GRE4	GRE5	GRE6	GRE7	GRE8																									
	GRE9	GRE10	GRE11	GRE12	GRE13	GRE14	GRE15	GRE16																									
	GRE17	GRE18	GRE19	GRE20	GRE21	GRE22	GRE23	GRE24																									
	GRE25	GRE26	GRE27	GRE28	GRE29	GRE30	GRE31	GRE32																									
GRE1 設定																																	
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 15%;">インターフェース アドレス</td> <td style="width: 85%;"><input type="text"/> (例 192.168.0.1/30)</td> </tr> <tr> <td>リモート(宛先)アドレス</td> <td><input type="text"/> (例 192.168.1.1)</td> </tr> <tr> <td>ローカル(送信元)アドレス</td> <td><input type="text"/> (例 192.168.2.1)</td> </tr> <tr> <td>PEER アドレス</td> <td><input type="text"/> (例 192.168.0.2/30)</td> </tr> <tr> <td>TTL</td> <td><input type="text" value="255"/> (1~255)</td> </tr> <tr> <td>MTU</td> <td><input type="text" value="1476"/> (最大値 1500)</td> </tr> <tr> <td>Path MTU Discovery</td> <td><input checked="" type="radio"/> 有効 <input type="radio"/> 無効</td> </tr> <tr> <td>ICMP AddressMask Request</td> <td><input checked="" type="radio"/> 応答する <input type="radio"/> 応答しない</td> </tr> <tr> <td>TOS 設定 (ECN Field 設定不可)</td> <td><input checked="" type="radio"/> TOS 値の指定 <input type="text" value="0x0xfc"/> <input type="radio"/> inherit (TOS 値のコピー)</td> </tr> <tr> <td>GRE over IPsec</td> <td><input type="radio"/> 使用する ipsec0 <input checked="" type="radio"/> Routing Table に依存</td> </tr> <tr> <td>IDキーの設定</td> <td><input type="text" value="0-4294967295"/></td> </tr> <tr> <td>End-to-End Checksumming</td> <td><input type="radio"/> 有効 <input checked="" type="radio"/> 無効</td> </tr> <tr> <td>MSS 設定</td> <td><input type="radio"/> 有効 <input checked="" type="radio"/> 無効 MSS 値 0 Byte &lt;有效時に MSS 値が 0 の場合は、MSS 値を自動設定(Clamp MSS to MTU)します。&gt;</td> </tr> </table>								インターフェース 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	<input type="text" value="255"/> (1~255)	MTU	<input type="text" value="1476"/> (最大値 1500)	Path MTU Discovery	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効	ICMP AddressMask Request	<input checked="" type="radio"/> 応答する <input type="radio"/> 応答しない	TOS 設定 (ECN Field 設定不可)	<input checked="" type="radio"/> TOS 値の指定 <input type="text" value="0x0xfc"/> <input type="radio"/> inherit (TOS 値のコピー)	GRE over IPsec	<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" value="0-4294967295"/>	End-to-End Checksumming	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効	MSS 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 MSS 値 0 Byte <有效時に MSS 値が 0 の場合は、MSS 値を自動設定(Clamp MSS to MTU)します。>
インターフェース 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	<input type="text" value="255"/> (1~255)																																
MTU	<input type="text" value="1476"/> (最大値 1500)																																
Path MTU Discovery	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効																																
ICMP AddressMask Request	<input checked="" type="radio"/> 応答する <input type="radio"/> 応答しない																																
TOS 設定 (ECN Field 設定不可)	<input checked="" type="radio"/> TOS 値の指定 <input type="text" value="0x0xfc"/> <input type="radio"/> inherit (TOS 値のコピー)																																
GRE over IPsec	<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" value="0-4294967295"/>																																
End-to-End Checksumming	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効																																
MSS 設定	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効 MSS 値 0 Byte <有效時に MSS 値が 0 の場合は、MSS 値を自動設定(Clamp MSS to MTU)します。>																																
現在の状態 <span style="color: red;">Tunnel is down, Link is down</span>																																	
<a href="#">追加/変更</a> <a href="#">削除</a>																																	

### インターフェースアドレス

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

### リモート(宛先)アドレス

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

### ローカル(送信元)アドレス

本装置の WAN 側 IP アドレスを設定します。

### PEER アドレス

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

### TTL

GRE パケットの TTL 値を設定します。

### MTU

MTU 値を設定します。最大値は 1500byte です。

### Path MTU Discovery

Path MTU Discovery 機能を有効にするかを選択します。

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

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

### ICMP AddressMask Request

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

### TOS 設定(ECN Field 設定不可)

GRE パケットの TOS 値を設定します。

## 第29章 GRE 設定

### GRE の設定

#### GREoverIPsec

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

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

#### ID キーの設定

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

#### End-to-End Checksumming

チェックサム機能の有効 / 無効を選択します。  
この機能を有効にすると、

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

#### MSS 設定

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

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

#### GRE の削除

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

再度有効とするときは「追加 / 変更」ボタンをクリックしてください。

#### GRE の状態表示

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

現在の状態      Tunnel is down, Link is down

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



#### GRE の再設定

GRE 設定をおこなうと、設定内容が一覧表示されます。

#### GRE一覧表示

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

#### 編集

設定の編集は「Interface名」をクリックしてください。

#### リンク状態

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

# 第 30 章

---

---

パケット分類設定

## 第30章 パケット分類設定

### . XR-430 のパケット分類設定について

パケット分類設定は、受け取った特定のパケットに対して、TOS/Precedence 値や DSCP 値を付加するための設定です。XR-430 では、以下の内容によりパケットの分類をおこないます。

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

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

## 第30章 パケット分類設定

### . パケット分類設定の設定

#### 「パケット分類設定」

設定を追加するときは「New Entry」をクリックします。

設定番号	1	
パケット分類条件		
プロトコル	6 (Protocol番号)	<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: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/DSCP 値	<input checked="" type="radio"/> TOS <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 DSOP Bit値 hex(0-3f)
TOS/DSCP 値の設定		
設定対象	<input checked="" type="radio"/> TOS/Precedence <input type="radio"/> DSCP	
設定値	<ul style="list-style-type: none"><li>・TOS/Precedence 設定 Minimize cost(1) <input type="radio"/> TOS Bit Internetwork Control(6) <input type="radio"/> Precedence Bit</li><li>・DSCP 設定 選択して下さい <input type="radio"/> DSCP Bit</li></ul>	

(画面は表示例です)

「ローカルパケット出力時の設定」か「パケット入力時の設定」をクリックして選択します。

#### [パケット分類条件]

パケット選別のマッチ条件を定義します。

##### プロトコル

プロトコルを指定します。プロトコル番号で指定してください。

##### 送信元アドレス

送信元 IP アドレスを指定します。サブネット単位、ホスト単位のいずれでも指定可能です。单一ホストを指定するときは<ホスト IP アドレス>/32 の形式で指定します。範囲での指定はできません。

##### 送信元ポート

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

##### 宛先アドレス

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

##### 宛先ポート

宛先ポート番号を指定します。指定方法は送信元ポートと同様です。

##### インターフェース

インターフェースを選択します。

インターフェース名は「付録A」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/DSCP 値

マッチングする TOS/DSCP 値を指定します。TOS、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/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 値または DSCP 値を設定します。

##### 設定対象

TOS/Precedence、DSCP のいずれかを選択します。

##### 設定値

設定対象で選択したものについて、設定値を指定します。

設定後は「設定」ボタンをクリックします。

TOS/Precedence および DSCP については章末「. TOS について」、「. DSCP について」をご参照ください。

## 第30章 パケット分類設定

### . 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。

Packet分類設定ステータス表示	<input type="button" value="表示する"/>
Interfaceの指定(指定無くても可)	<input type="button"/>

パケット分類設定のステータスを表示します。

## 第30章 パケット分類設定

### . ステータス情報の表示例

#### [Packet 分類設定情報]表示例

パケット分類設定の情報を表示します。

pkts	bytes	target	prot	opt	in	out	source	destination	
272	39111	MARK	all	--	eth0	any	192.168.120.111	anywhere	MARK set 0x1
83	5439	MARK	all	--	eth0	any	192.168.120.113	anywhere	MARK set 0x2
447	48695	MARK	all	--	eth0	any	192.168.0.0/24	anywhere	MARK set 0x3
0	0	FTOS	tcp	--	eth0	any	192.168.0.1	111.111.111.111	tcp spts:1024:

65535 dpt:450 Type of Service set 0x62

pkts -> 入力(出力)されたパケット数

bytes -> 入力(出力)されたバイト数

target -> 分類の対象(MARK か TOS か)

prot -> プロトコル

in -> パケット入力インターフェース

out -> パケット出力インターフェース

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

## 第30章 パケット分類設定

### . 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することで、優先度にあわせて機器がパケットを適切に扱えることを期待します。

IPヘッダ内のTOSフィールドの各ビットは、以下のように定義されています。<表1>

バイナリ 10進数 意味

バイナリ	10進数	意味
1000	8	Minimize delay (md)
0100	4	Maximize throughput (mt)
0010	2	Maximize reliability (mr)
0001	1	Minimize monetary cost (mmc)
0000	0	Normal Service

mdは最小の遅延、mtは最高のスループット、mrは高い信頼性、mmcは低い通信コスト、を期待するパケットであることを示します。

各ビットの組み合わせによるTOS値は以下のように定義されます。<表2>

TOS	ビット	意味	Linuxでの扱い	バンド
0x0	0	Normal Service	0 Best Effort	1
0x2	1	Minimize Monetary Cost	1 Filler	2
0x4	2	Maximize Reliability	0 Best Effort	1
0x6	3	mmc+mr	0 Best Effort	1
0x8	4	Maximize Throughput	2 Bulk	2
0xa	5	mmc+mt	2 Bulk	2
0xc	6	mr+mt	2 Bulk	2
0xe	7	mmc+mr+mt	2 Bulk	2
0x10	8	Minimize Delay	6 Interactive	0
0x12	9	mmc+md	6 Interactive	0
0x14	10	mr+md	6 Interactive	0
0x16	11	mmc+mr+md	6 Interactive	0
0x18	12	mt+md	4 Int. Bulk	1
0x1a	13	mmc+mt+md	4 Int. Bulk	1
0x1c	14	mr+mt+md	4 Int. Bulk	1
0x1e	15	mmc+mr+mt+md	4 Int. Bulk	1

バンドは優先度です。0が最も優先度が高いものです。初期値ではバンド数は3(優先度は3段階)です。本装置では、PQ Paramater設定の「最大Band数設定」でバンド数を変更できます(0~4)。

Linuxでの扱いの数値は、LinuxでのTOSビット列の解釈です。これはPQ Paramater設定の「Priority-map設定」の箱にリンクしており、対応するPriority-mapの箱に送られます。

## 第30章 パケット分類設定

### . TOSについて

またアプリケーションごとのパケットの取り扱い方法も定義されています(RFC1349)。

アプリケーションのTOS値は以下のようになっています。<表3>

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

表中のTOSビット値(2進数表記)が、<表2>のビットに対応しています。

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

## 第30章 パケット分類設定

### . 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DSCH値だけを参照してQoS制御をおこなうことができます。

#### TOS と DS フィールドのビット定義

## 【TOS フィールド構造】

0 1 2 3 4 5 6 7

+---+---+---+---+---+---+---+

|Precedence |Type of Service|CU|

+---+---+---+---+---+---+---+

## 【DSCP フィールド構造】

Detailed description: The diagram illustrates the 8-bit DSCP field. It consists of two main sections separated by a vertical line. The left section, from bit 0 to bit 3, is labeled 'DSCP'. The right section, from bit 5 to bit 7, is labeled 'CU'. Each section is represented by a row of eight '+' characters, with the labels positioned above them.

0	1	2	3	4	5	6	7
+	+	+	+	+	+	+	+
	DSCP				CU		
+	+	+	+	+	+	+	+

DSCP: differentiated services code point  
CU: currently unused (現在未使用)

DSCPビットのとりうる値とその制御方法の定義は以下のようになっています。

定義名	DSCP 値	制御方法
EF(Expedited Forwarding)	0x2e	パケットを最優先で転送(RFC3246)
AF(Assured Forwarding) AF11/AF12/AF13 AF21/AF22/AF23 AF31/AF32/AF33 AF41/AF42/AF43	0x0a / 0x0c / 0x0e 0x12 / 0x14 / 0x16 0x1a / 0x1c / 0x1e 0x22 / 0x24 / 0x26	4つの送出優先度と3つの廃棄優先度を持ち、数字の上位桁は送出優先度(クラス)、下位桁は廃棄優先度を表します。(RFC2597) <ul style="list-style-type: none"> <li>・送出優先度 (高) 1 &gt; 2 &gt; 3 &gt; 4 (低)</li> <li>・廃棄優先度 (高) 1 &gt; 2 &gt; 3 (低)</li> </ul>
CS(Class Selector) CS1 CS2 CS3 CS4 CS5 CS6 CS7	0x08 0x10 0x18 0x20 0x28 0x30 0x38	既存のTOS互換による優先制御をおこないます。 <ul style="list-style-type: none"> <li>Precedence1(Priority)</li> <li>Precedence2(Immediate)</li> <li>Precedence3(Flash)</li> <li>Precedence4(Flash Override)</li> <li>Precedence5(Critic/ESP)</li> <li>Precedence6(Internetwork Control)</li> <li>Precedence7(Network Control)</li> </ul>
BE (Best Effort)	0x00	ベストエフォート(優先制御なし)

# 第 31 章

---

---

Web 認証機能

## . Web 認証機能の設定

「Web 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。

**実行方法**

Web 設定画面で「Web 認証設定」をクリックして、各設定をおこないます。

**基本設定**

Web 認証設定 (基本設定)		
基本設定	ユーザ設定	RADIUS設定
<b>MACアドレスフィルタ</b>	フィルタ設定	ログ設定
<b>基本設定</b>		
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
MACアドレスフィルタ	<input checked="" type="radio"/> 使用しない	<input type="radio"/> 使用する
<b>URL転送</b>		
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
<b>認証方法</b>		
<input checked="" type="radio"/> ローカル	<input type="radio"/> RADIUSサーバ	
<b>接続許可時間</b>		
<input checked="" type="radio"/> アイドルタイムアウト <input type="text" value="30"/> 分 (1~43200)		
<input type="radio"/> セッションタイムアウト <input type="text"/> 分 (1~43200)		
<input type="radio"/> 認証を受けたWebブラウザのウィンドウを閉じるまで		
<b>設定変更</b>		

**[基本設定]****本機能**

Web 認証機能を使う場合は「使用する」を選択します。

**認証**

当機能を使用していて、かつ認証をおこなうときは「する」を選択します(初期設定)。認証をおこなわないときは「しない(URL転送のみ)」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つたときに、強制的にWeb 認証をおこないます。

初期設定は監視を「行わない」設定となります。

**MAC アドレスフィルタ**

MAC アドレスフィルタを有効にする場合は「使用する」を選択します。

**[URL 転送]****URL**

転送先の URL を設定します。

**通常認証後**

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

**強制認証後**

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

**[認証方法]****ローカル**

本装置でアカウントを管理 / 認証します。

**RADIUS サーバ**

外部の RADIUS サーバでアカウントを管理 / 認証します。

## . Web 認証機能の設定

## [接続許可時間]

## 接続許可時間

認証したからの、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 Web 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。

Web 認証機能を「**使用する**」にした場合はただちに機能が有効となりますので、[ユーザー設定等から設定をおこなってください。](#)

## ユーザー設定

設定可能なユーザの最大数は 64 です。

画面最下部にある「[ユーザ設定画面インデックス](#)」のリンクをクリックしてください。

Web 認証設定 (ユーザ設定)		
基本設定	ユーザ設定	RADIUS設定
MACアドレスフィルタ	フィルタ設定	ログ設定
No.1~16まで		

No.	ユーザID	パスワード	削除
1			<input type="checkbox"/>
2			<input type="checkbox"/>
3			<input type="checkbox"/>
4			<input type="checkbox"/>
5			<input type="checkbox"/>
6			<input type="checkbox"/>
7			<input type="checkbox"/>
8			<input type="checkbox"/>
9			<input type="checkbox"/>
10			<input type="checkbox"/>
11			<input type="checkbox"/>
12			<input type="checkbox"/>
13			<input type="checkbox"/>
14			<input type="checkbox"/>
15			<input type="checkbox"/>
16			<input type="checkbox"/>

**設定/削除の実行**

[ユーザ設定画面インデックス](#)  
001- 017- 033- 049-

## ユーザ ID

## パスワード

ユーザアカウントを登録します。

ユーザ ID・パスワードには半角英数字で設定してください。空白やコロン(:)は含めることができます。

## 削除

チェックすると、その設定が削除対象となります。

最後に「**設定 / 削除の実行**」をクリックしてください。

## . Web 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」に設定した場合にのみ設定します。

Web 認証設定 (RADIUS 設定)			
基本設定	ユーザ認定	RADIUS 設定	
MACアドレスフィルタ	フィルタ設定	ログ設定	
<b>プライマリサーバ設定</b>			
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"/>		
<b>セカンダリサーバ設定</b>			
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"/>		
<b>サーバ共通設定</b>			
NAS-IP-Address	<input type="text"/>		
NAS-Identifier	<input type="text"/>		
<b>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)</b>			
アイドルタイムアウト	指定しない <input type="button" value="▼"/>		
セッションタイムアウト	指定しない <input type="button" value="▼"/>		
<input type="button" value="設定変更"/>			

## [プライマリサーバ設定]

プライマリサーバ項目の設定は必須です。

IP アドレス

ポート番号

secret

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

## [セカンダリサーバ設定]

セカンダリ項目の設定はなくてもかまいません。

IP アドレス

ポート番号

secret

設定はプライマリサーバ設定と同様です。

## [サーバ共通設定]

RADIUS サーバへ問い合わせをする際に送信する NAS の情報を設定します。RADUIS サーバが、どの NAS かを識別するために使います。どちらかの設定が必須です。

NAS-IP-Address

通常は本装置の IP アドレスを設定します。

NAS-Identifier

任意の文字列を設定します。  
半角英数字が使用できます。

## [接続許可時間 (RADIUS サーバから送信されるアトリビュートの指定)]

それぞれ、基本設定で選択されているものが有効となります。

アイドルタイムアウト

プルダウンの以下の項目から選択してください。

## ・ 指定しない

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

## ・ Idle-Timeout\_28

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

## ・ Ascend-Idle-Limit\_244/529

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

## ・ Ascend-Idle-Limit\_244

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

## . Web 認証機能の設定

## セッションタイムアウト

プルダウンの以下の項目から選択してください。

## ・指定しない

RADIUSサーバからの認証応答に該当のアトリビュートがあればその値を使います。

該当のアトリビュートがなければ「基本設定」で設定した値を使用します。

## ・Session-Timeout\_27

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

## ・Ascend-Maximum-Time\_194/529

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

## ・Ascend-Maximum-Time\_194

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

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。

## MAC アドレスフィルタ

Web 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。MAC アドレスフィルタを設定することによって認証を必要とせずに通信が可能になります。

本機能で設定した MAC アドレスを送信元 MAC アドレスとする IP パケットの転送がおこなわれると、それ以降はその IP アドレスを送信元 / 送信先とする IP パケットの転送を許可します。

ここで設定する MAC アドレスは、転送許可を最初に決定する場合に用いられます。

Web 認証設定 (MACアドレスフィルタ)		
基本設定	ユーザ設定	RADIUS設定
<b>MACアドレスフィルタ</b>	フィルタ設定	ログ設定
MACアドレス インタフェース 動作 設定変更 MACアドレスフィルタは未設定です		

[MACアドレスフィルタの新規追加](#)

「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 <b>追加</b>	
MACアドレス	<input type="text"/>
インターフェース	<input type="text"/>
動作	<b>許可</b> <input checked="" type="checkbox"/>

**追加** **実行**

## [MACアドレスフィルタの 追加]

MAC アドレス

フィルタリング対象とする、送信元 MAC アドレスを入力します。

インターフェース

フィルタリングをおこなうインターフェース名を入力します(任意で指定)。

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

## . Web 認証機能の設定

### 動作

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

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	インターフェース	動作	設定変更
00:01:02:03:04:05	eth0	許可	<a href="#">編集</a> <a href="#">削除</a>

一覧表示からは、設定の編集・削除をおこなう事ができます。

### 編集

編集したい設定の行にある「編集」ボタンをクリックしてください。

「インターフェース」と「動作」の設定が変更できます。

### 削除

削除したい設定の行にある「削除」ボタンをクリックしてください。

削除確認画面が表示されます。「実行」ボタンをクリックすると設定の削除がおこなわれます。

### フィルタ設定

Web 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。フィルタ設定によって認証を必要とせずに通信可能にできます。

「特定のポートだけは常に通信できるようにしたい」といった場合に設定します。

設定画面「フィルタ設定」をクリックします。

Web 認証設定（フィルタ設定）		
基本設定	ユーザ設定	RADIUS設定
<a href="#">MACアドレスフィルタ</a>	<a href="#">フィルタ設定</a>	<a href="#">ログ設定</a>

[「フィルタ設定」のWeb 認証設定フィルタ設定画面](#)にて設定して下さい。

上記のメッセージが表示されたらリンクをクリックしてください。

「Web 認証フィルタ」設定画面に移ります。

No.	インターフェース	方向	動作	プロトコル	No.1~16まで			
					入力フィルタ	転送フィルタ	出力フィルタ	Web 認証フィルタ
1		パケット受信時	許可	全て				<a href="#">情報表示</a>
2		パケット受信時	許可	全て				<a href="#">LOG</a>

ここで設定したIPアドレスやポートについては、Web 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26章 パケットフィルタリング機能」をご参照ください。

## . Web 認証機能の設定

**ログ設定**

Web 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。

Web 認証設定 (ログ設定)		
基本設定	ユーザ設定	RADIUS設定
MACアドレスフィルタ	フィルタ設定	ログ設定
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	

**設定変更**

ログを取得するかどうかを選択します。

**エラーログ**

Web 認証時のログインエラーを出力します。

<エラーログの表示例>

```
Apr 7 17:04:45 localhost httpd[21529]:  
[error] [client 192.168.0.1] user abc: authentication failure for "/": password mismatch
```

**アクセスログ**

Web 認証時のアクセスログを出力します。

<アクセスログの表示例>

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

### . Web 認証下のアクセス方法

#### ホストからのアクセス方法

1 ホストから本装置にアクセスします。  
以下の形式でアドレスを指定してアクセスします。

**http://<本装置の IP アドレス>/login.cgi**

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

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

<認証成功時の表示例>

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

Date: Mon Apr 7 10:06:51 2003

#### 設定画面へのアクセスについて

Web 認証機能を使用していて認証をおこなっていなくても、本装置の設定画面にはアクセスすることができます。

アクセス方法は、通常と同じです。

#### RADIUS 設定について

認証方法を「RADIUS サーバ」に選択した場合、XR-430 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、セカンドリサーバに要求を送信します。

#### 認証について

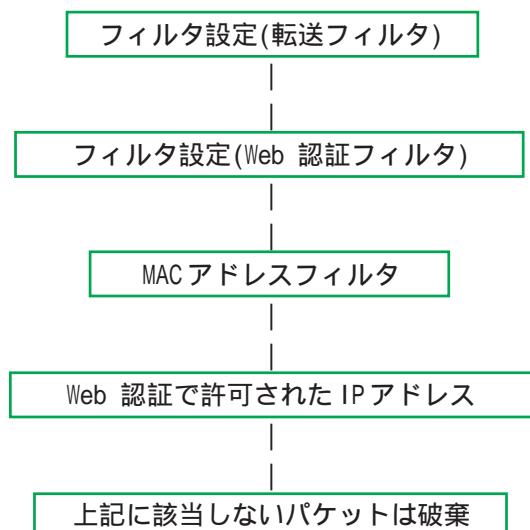
認証方法が「ローカル」、「RADIUS サーバ」のどちらの場合でも、クライアント - 本装置間の認証には、HTTP Basic 認証が用いられます。また、「RADIUS サーバ」を使用する場合、本装置 - RADIUS サーバ間は User-Password を用いた認証 (PAP) がおこなわれます。

## . Web 認証の制御方法について

Web 認証機能はパケットフィルタの一種で、認証で許可されたユーザー（ホスト）の IP アドレスを送信元 / あて先に持つ転送パケットのみを通過させます。

制御は、転送フィルタ設定の最後でおこなわれます。

フィルタリング制御の順番は以下の通りです。



Web 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、Web 認証よりも優先してそのフィルタが参照されてしまい、Web 認証が有効に機能しなくなる恐れがあります。

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

# 第32章

---

---

ネットワークテスト

## ネットワークテスト

XR-430の運用時において、ネットワークテストをおこなうことができます。ネットワークのトラブルシューティングに有効です。

以下の3つのテストができます。

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

### 実行方法

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

ネットワーク・テスト	
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  <input type="radio"/> Ether0 <input type="radio"/> Ether1  <input checked="" type="radio"/> その他 <input type="text"/></p> <p>オプション</p> <p>count <input type="text" value="10"/> size <input type="text" value="56"/> timeout <input type="text" value="30"/></p> <p style="text-align: center;"><b>実行</b></p>
Trace Route	<p>FQDNまたはIPアドレス</p> <input type="text"/> <p>オプション</p> <p><input type="radio"/> UDP <input checked="" type="radio"/> ICMP</p> <p style="text-align: center;"><b>実行</b></p>
パケットダンプ	<p><input type="radio"/> 主回線 <input type="radio"/> マルチ#2 <input type="radio"/> マルチ#3 <input type="radio"/> マルチ#4  <input type="radio"/> Ether0 <input type="radio"/> Ether1  <input type="radio"/> その他 <input type="text"/></p> <p style="text-align: center;"><b>実行</b> <b>結果表示</b></p>
PacketDump TypePcap	<p>Device <input type="text"/> CapCount <input type="text"/> CapSize <input type="text"/>          Dump Filter</p> <p style="font-size: small;">生成ファイルの最大サイズは圧縮後で約4Mbyteです 高帯域下での使用はパケットロスを生じる場合があります</p> <p style="text-align: center;"><b>実行</b> <b>結果表示</b></p>

### [Ping テスト]

指定した相手に本装置から Ping を発信します。

FQDN または IP アドレス

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

インターフェースの指定(省略可)

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

#### オプション

##### ・ count

送信する ping パケット数を指定します。

入力可能な範囲 : 1-10 です。初期値は 10 です。

##### ・ size

送信するデータサイズ(byte)を指定します。

入力可能な範囲 : 56-1500 です。初期値は 56 です(8 バイトの ICMP ヘッダが追加されるため、64 バイトの ICMP データが送信されます)。

##### ・ timeout

ping コマンドの起動時間を指定します。

入力可能な範囲 : 1-30 です。初期値は 30 です。

入力が終わりましたら「実行」をクリックします。

### 実行結果例

実行結果
<pre>PING 211.14.13.66 (211.14.13.66): 56 data bytes 64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=49.5 ms 64 bytes from 211.14.13.66: icmp_seq=1 ttl=52 time=65.7 ms 64 bytes from 211.14.13.66: icmp_seq=2 ttl=52 time=11.7 ms 64 bytes from 211.14.13.66: icmp_seq=3 ttl=52 time=12.0 ms 64 bytes from 211.14.13.66: icmp_seq=4 ttl=52 time=69.0 ms 64 bytes from 211.14.13.66: icmp_seq=5 ttl=52 time=58.3 ms 64 bytes from 211.14.13.66: icmp_seq=6 ttl=52 time=12.0 ms 64 bytes from 211.14.13.66: icmp_seq=7 ttl=52 time=71.4 ms 64 bytes from 211.14.13.66: icmp_seq=8 ttl=52 time=12.0 ms 64 bytes from 211.14.13.66: icmp_seq=9 ttl=52 time=11.8 ms  --- 211.14.13.66 ping statistics --- 10 packets transmitted, 10 packets received, 0% packet loss round-trip min/avg/max = 11.7/37.3/71.4 ms</pre>

第32章 ネットワークテスト

## ネットワークテスト

## [Trace Route テスト]

指定した宛先までに経由するルータの情報を表示します。

FQDN または IP アドレス

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

## オプション

- UDP

UDPパケットを使用する場合に指定します。  
初期設定は UDP です。

- ICMP

ICMPパケットを使用する場合に指定します。

入力が終わったら「実行」をクリックします。

## 実行結果例

実行結果

```
PING 211.14.13.66 (211.14.13.66): 56 data bytes  
64 bytes from 211.14.13.66: icmp_seq=0 ttl=52 time=12.4 ms
```

```

--- 211.14.13.66 ping statistics ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 12.4/12.4/12.4 ms
transcoute 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  1.807 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  21.183 ms  13.946 ms
  4 210.185.192.108 (210.185.192.108), 9.205 ms  8.953 ms  9.310 ms
  5 210.185.206.34 (210.185.206.34), 38.598 ms  19.923 ms  14.744 ms
  6 210.185.208.10 (210.185.208.10), 41.841 ms  40.476 ms  63.293 ms
  7 210.171.224.1105 (210.171.224.1105), 49.348 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), 53.578 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 ! 15.213 ms !

```

## [パケットダンプテスト]

パケットのダンプを取得できます。

ダンプを取得したいインターフェースを選択して「実行」をクリックします。

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

その後、「結果表示」をクリックすると、ダンプ内容が表示されます。

実行結果例

「結果表示」をクリックするたびに、表示結果が更新されます。

パケットダンプの表示は、最大で 100 パケット分までです。100 パケット分を超えると、古いものから順に表示されなくなります。

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

### ネットワークテスト

#### [PacketDump TypePcap テスト]

拡張版パケットダンプ取得機能です。

指定したインターフェースで、指定した数のパケットダンプを取得できます。

##### Device

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

##### CapCount

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

##### CapSize

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

##### Dump Filter

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

入力後、「実行」ボタンでパケットダンプを開始します。

#### パケットダンプを開始したときの画面表示

実行結果は即時出力できない場合があります。  
[再表示]で確認して下さい

[再表示] [実行中断]

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

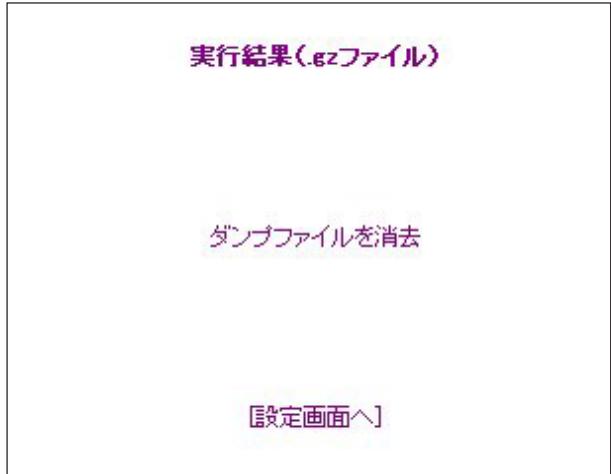
ダンプ実行結果はありません。

まだ指定パケット数を記録していません  
記録用ストレージ使用率 約3%

[再表示] [実行中断]

### ネットワークテスト

パケットダンプが実行終了したときの画面



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

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

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

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

#### PacketDump TypePcap の注意点

- 取得したパケットダンプ結果は、libpcap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書の「**付録A インタフェース名一覧**」をご参照ください。

# 第 33 章

---

---

各種システム設定

## 各種システム設定

「システム設定」ページでは、XR-430 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。

システム設定								
時計の設定	ログの表示 ログの削除	パスワードの設定	ファームのアップデート	設定の保存・復帰	設定のリセット	再起動		
セッションライフ タイムの設定	設定画面の設定	ARP filter設定	メール送信機能の設定	モバイル通信インターフェース一覧	外部ストレージ管理			

- ・時計の設定
- ・ログの表示 / 削除
- ・パスワード設定
- ・ファームウェアアップデート
- ・設定の保存・復帰
- ・設定のリセット
- ・本体の再起動
- ・セッションライフタイムの設定
- ・設定画面の設定
- ・ARP filter 設定
- ・メール送信機能の設定
- ・モバイル通信インターフェース一覧
- ・外部ストレージ管理

## 時計の設定

本装置内蔵時計の設定をおこないます。

## 設定方法

「時計の設定」をクリックして設定画面を開きます。

## 内蔵時計の設定

2008 年 08 月 26 日 火曜日
12 時 00 分 00 秒
※時刻は24時間形式で入力してください。

24時間単位で時刻を設定してください。

## 設定方法

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。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。

設定はすぐに反映されます。

## 各種システム設定

## ログの表示

「ログの表示」をクリックして表示画面を開きます。

```

Apr 26 00:00:11 localhost -- MARK --
Apr 26 00:00:25:11 localhost -- MARK --
Apr 26 00:00:37:59 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 00:00:37:59 localhost named[436]: USAGE 1019749079 1019556843
CPU=2.58u/2.34s CHILDCPU=0/u/0s
Apr 26 00:00:37:59 localhost named[436]: XSTATS 1019749079 1019556843 RR=0 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RErr=0 RA邢R=0 RLame=0 RPorts=0 SSys=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RD=3 RIO=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SAns=0 SNKD=0
Apr 26 01:06:08 localhost -- MARK --
Apr 26 01:26:08 localhost -- MARK --
Apr 26 01:30:57 localhost named[436]: Cleaned cache of 0 RRsets
Apr 26 01:30:57 localhost named[436]: USAGE 1019752737 1019556843
CPU=2.58u/2.34s CHILDCPU=0/u/0s
Apr 26 01:30:57 localhost named[436]: XSTATS 1019752737 1019556843 RR=0 RNKD=0
RFwdR=0 RDupR=0 RFail=0 RErr=0 RA邢R=0 RLame=0 RPorts=0 SSys=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RD=3 RIO=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SAns=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=0/u/0s
Apr 26 02:39:54 localhost named[436]: XSTATS 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 RErr=0 RA邢R=0 RLame=0 RPorts=0 SSys=1 SAns=0
SFwdQ=3 SDupQ=19233 SErr=4 RD=3 RIO=0 RDupQ=0 RTCP=0 SFwdR=0 SFail=0
SFErr=0 SAns=0 SNKD=0

```

最大1000行まで表示できます

[表示の更新](#)

[ログファイルの取得](#)

ブラウザの“リンクを保存する”を使用して取得して下さい  
[最新ログ](#)

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。

保存されるログファイルは最大で6つです。  
ログファイルが作成されたときは画面上にリンクが生成されます。  
古いログファイルから順に削除されていきます。

[ログファイルの取得](#)

ブラウザの“リンクを保存する”を使用して取得して下さい

[最新ログ](#)  
[バックアップログ1](#)  
[バックアップログ2](#)  
[バックアップログ3](#)  
[バックアップログ4](#)  
[バックアップログ5](#)  
[バックアップログ6](#)

「攻撃検出機能」を使用している場合は、そのログも併せてここで表示されます。

設定方法は「第18章 攻撃検出機能」をご参照ください。

本体の再起動をおこなった場合、それまでのログは全てクリアされます。

## ログの削除

ログ情報は最大2MBまでのサイズで保存されます。また再起動時にログ情報は削除されます。手動で削除する場合は次のようにしてください。

## 実行方法

「ログの削除」をクリックして画面を開きます。

[ログの削除](#)

すべてのログメッセージを削除します。

[実行する](#)

「実行する」ボタンをクリックすると、保存されているログが全て削除されます。

## 各種システム設定

**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名、  
パスワードを変更します。  
ルータ自身のセキュリティのためにパスワードを  
変更されることを推奨します。

**設定方法**

「パスワードの設定」をクリックして設定画面を開きます。

**パスワード設定**

---

新しいユーザ名	<input type="text"/>
新しいパスワード	<input type="password"/>
もう一度入力してください	<input type="password"/>

[入力のやり直し](#) [設定の保存](#)

ユーザー名とパスワードの設定ができます。

**新しいユーザ名**  
半角英数字で1から15文字まで設定可能です。

**新しいパスワード**  
半角英数字で1から8文字まで設定可能です。  
大文字・小文字も判別しますのでご注意ください。

**もう一度入力してください**  
確認のため再度「新しいパスワード」を入力してください。

入力が終わりましたら「設定の保存」ボタンをクリックして設定完了です。

次回のログインからは、新しく設定したユーザー名とパスワードを使います。

## 各種システム設定

## ファームウェアのアップデート

本装置は、ブラウザ上からファームウェアのアップデートをおこないます。

ファームウェアは弊社ホームページよりダウンロードできます。

弊社サポートサイト

<http://www.centurysys.co.jp/support/xr430.html>

実行方法

- 「ファームウェアのアップデート」をクリックして画面を開きます。

## ファームウェアのアップデート

ここではファームウェアのアップデートをおこなうことができます。

ファイルの指定	<input type="text"/>	<a href="#">参照...</a>
<a href="#">アップデート実行</a>		

- 「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、右上のようなアップデートの確認画面が表示されます。  
バージョン等が正しければ「実行する」をクリックしてください。

## ファームウェアのアップデート

ファームウェアのダウンロードが完了しました

現在のファームウェアのバージョン

Century Systems XR-430 Series ver 1.0.0

ダウンロードされたファームウェアのバージョン

Century Systems XR-430 Series 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**

[実行する](#)

[中止する](#)

上記画面が表示されたままで3分間以上経過してから、「実行する」ボタンをクリックすると、以下の画面が表示され、アップデートは実行されません。

## ファームウェアのアップデート

アップロード完了から3分以上経過したため  
ファームウェアは破棄されました

[\[設定画面へ\]](#)

アップデートを実行するには再度、2の操作からおこなってください。

- アップデートを実行した場合は以下の画面が表示され、ファームウェアの書き換えが始まります。

## ファームウェアのアップデート

ファームウェアのアップデートを実行します。  
作業には数分かかりますので電源を切らずにお待ち下さい。  
作業が終了しますと自動的に再起動します。

[引き続き、次ページもご覧ください。](#)

### 各種システム設定

#### ファームウェアアップデート実行時のLED

アップデート中は、本装置前面のLEDが以下のように動作します。

- Status :  (同時に点滅)
- Power : 

LEDが動作中は、アクセスをおこなわずに、そのままお待ちください。

ファームウェアの書き換えが終了すると、本装置は自動的に再起動して、アップデートの完了となります。

アップデート完了後のLEDは、通常動作時と同じ状態です。

- Power : 

本装置の設定により、Main LED(緑)、Backup LED(緑)も点灯している場合があります。

各LEDの状態は『第1章 XR-430 の概要 . 各部の名称と機能』をご参照ください。

#### ファームウェアアップデート実行時の禁止

##### 事項

本装置のファームウェアのアップデートは、10分程度かかります。

アップデート実行中に、以下の操作はおこなわないでください。

##### 本装置へのアクセス

アップデート失敗の原因となることがあります。

##### 本装置の電源を切る

アップデート実行中は、絶対に電源を切らないでください。

更新中に電源が切れると、故障原因となります。もしもこのような状態になった場合は、弊社サポートデスク(support@centurysys.co.jp)へご相談ください。

## 各種システム設定

## 設定の保存と復帰

本装置の設定の保存および、保存した設定の復帰をおこないます。

クリックすると以下のメッセージが表示されます。

**設定の保存・復帰**

## 実行方法

「設定の保存・復帰」をクリックして画面を開きます。

**設定の保存・復帰(確認)**

設定の保存作業を行っています。

設定をバックアップしました  
バックアップファイルのダウンロード

ブラウザのリンクを保存する等で保存して下さい。

## -- 注意 --

「設定の保存復帰画面」にて設定情報を表示・更新する際、ご利用のプロバイダ登録情報や本装置のRSAの秘密鍵を含む設定情報等がネットワーク上に平文で流れます。設定の保存・復帰は、ローカル環境もしくはVPN環境等、セキュリティが確保された環境下で行う事をおすすめします。

**[設定の保存・復帰]**

上記のような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方式と保存形式を選択します。

**設定の保存・復帰**

**[設定画面へ]**

「バックアップファイルのダウンロード」リンクから、設定をテキストファイルで保存しておきます。

## [設定の復帰]

上記項目から「参照」をクリックして、保存しておいた設定ファイルを選択します。全設定の保存ファイルはgzip圧縮形式のまま、復帰させることができます。

ここでは設定を復帰させることができます。

ファイルの指定  [参照...]

[設定の復帰]

設定の復帰が正しく行われると本機器は自動的に再起動します。その後「設定の復帰」をクリックすると、設定の復帰がおこなわれます。

設定が正常に復帰できたときは、本装置が自動的に再起動されます。

**設定ファイルの作成**

## 全設定

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

初期値と異なる設定のみを抽出して、テキスト形式で保存します。このテキストファイルの内容を直接書き換えて設定を変更することもできます。

選択したら「設定ファイルの作成」をクリックします。

## -- 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おこなう事をおすすめします。

### 各種システム設定

#### 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。

設定のリセット

現在の本体設定内容を全てクリアして工場出荷設定に戻します。

実行する

「実行する」ボタンをクリックするとリセットが実行され、本体の全設定が工場出荷設定に戻ります。

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

#### 再起動

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。

本体の再起動

本体を再起動します。

実行する

「実行する」ボタンをクリックすると、リセットが実行されます。

本体の再起動をおこなった場合、それまでのログは全てクリアされます。

## 各種システム設定

## セッションライフタイムの設定

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

## 設定方法

「セッションライフタイムの設定」をクリックして画面を開きます。

## セッションライフタイムの設定

UDP	30	秒 (0 - 8640000)
UDP stream	180	秒 (0 - 8640000)
TCP	3600	秒 (0 - 8640000)
セッション最大数	4096	セッション (0, 4096 - 16384)
0を入力した場合、デフォルト値を設定します。		

## 設定の保存

## UDP

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

## UDP stream

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

## TCP

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

## セッション最大数

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

なお、本装置内部で保持しているセッション数は、  
周期的にsyslogに表示することができます。  
詳しくは「第17章 SYSLOG機能」のシステムメッセージの項を参照してください。

それぞれの項目で“0”を設定すると、初期値で動作します。

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

## 各種システム設定

**設定画面の設定**

WEB設定画面へのアクセスログについての設定をします。

**設定方法**

「設定画面の設定」をクリックして画面を開きます。

**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
<b>設定の保存</b>	

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

「設定の保存」をクリックします。

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

**ARP filter設定**

ARP filter設定をおこないます。

**設定方法**

「ARP filter設定」をクリックして画面を開きます。

**ARP filter設定**

ARP filter	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
<b>設定の保存</b>	

「有効」を選択して保存すると、ARP filterが動作します。

ARP filterを有効にすることで、同一IPアドレスのARPを複数のインター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ーフェースからARP応答を出さないようにできます。

選択したら「設定の保存」をクリックしてください。設定が完了します。  
設定はすぐに反映されます。

## 各種システム設定

## メール送信機能の設定

各種メール送信機能の設定をおこないます。  
ここでは以下の場合にメール送信を設定出来ます。

- ・SYSLOG サービスのログメール送信
- ・PPP/PPPoE 接続設定の主回線 接続 IP 変更  
お知らせメール
- ・PPP/PPPoE 接続設定のバックアップ回線 接続  
お知らせメール

## 設定方法

「メール送信機能の設定」をクリックして画面を開きます。

**メール送信機能の設定**

基本設定	
メール認証	<input checked="" type="radio"/> 認証しない <input type="radio"/> POP before SMTP <input type="radio"/> SMTP-AUTH(login) <input type="radio"/> SMTP-AUTH(plain)
SMTPサーバアドレス	<input type="text"/>
SMTPサーバポート	25
POP3サーバアドレス	<input type="text"/>
ユーザID	<input type="text"/>
パスワード	<input type="password"/>
<b>シリログのメール送信</b>	
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	admin@localhost
件名	Log keyword detection
文字列は1行(255文字まで、最大32個(行)までです。 <div style="border: 1px solid #ccc; height: 100px; width: 100%;"></div>	
<b>検出文字列の指定</b>	
<b>PPPoEお知らせメール送信</b>	
お知らせメール送信	<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	admin@localhost
件名	Changed IP / PPPoE
<b>PPPoE Backup回線のお知らせメール送信</b>	
お知らせメール送信	<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	admin@localhost
件名	Started Backup connection

## &lt;基本設定&gt;

## メール認証

下記よりいずれかを選択します。

## 「認証しない」

メールサーバとの認証をおこなわずに、本装置が自律的にメールを送信します。

## 「POP before SMTP」

指定したPOP3サーバにあらかじめアクセスさせることによって、SMTPによるメールの送信を許可する方式です。

## 「SMTP-AUTH(login)」

メール送信時にユーザ認証をおこない、メールの送信を許可する方法です。平文によるユーザ認証方式です。

## 「SMTP-AUTH(plain)」

メール送信時にユーザ認証をおこない、メールの送信を許可する方法です。LOGINも PLAIN同様、平文を用いた認証形式です。

## SMTPサーバアドレス

SMTPサーバアドレスは3箇所まで設定できます。それぞれの設定箇所において1つのIPv4アドレス、またはFQDNが設定可能です。FQDNは最大64文字で、ドメイン形式とホスト形式のどちらでも設定できます。

## ドメイン形式で指定する場合

<入力例> @centurysys.co.jp

## ホスト形式で指定する場合

<入力例> smtp.centurysys.co.jp

**本設定は、メール認証設定で「認証しない」場合は任意ですが、認証ありの場合は必ず設定してください。**

## SMTPサーバポート

設定されたポートを使用してメールを送信します。  
設定可能な範囲：1-65535です。

初期設定は“25”です。

### 各種システム設定

#### POP3 サーバアドレス

IPv4 アドレス、または FQDN で設定します。  
FQDN は最大 64 文字で、ホスト形式のみ設定できます。  
認証方式で「POP before SMTP」を指定した場合は必ず設定してください。

#### ユーザ ID

ユーザ ID を設定します。  
最大文字数は 64 文字です。  
認証方式を「認証しない」以外で選択した場合は必ず設定してください。

#### パスワード

パスワードを設定します。  
半角英数字で 64 文字まで設定可能です。大文字・小文字も判別しますのでご注意ください。  
認証方式を「認証しない」以外で選択した場合は必ず設定してください。

#### <シスログのメール送信>

ログの内容を電子メールで送信したいときの設定です。

##### ログのメール送信

ログメール機能を使用する場合は「送信する」を選択します。

##### 送信先メールアドレス

ログメッセージの送信先メールアドレスを指定します。  
最大文字数は 64 文字です。

##### 送信元メールアドレス

送信元のメールアドレスは任意で指定できます。  
最大文字数は 64 文字です。  
初期設定は「admin@localhost」です。

##### 件名

任意で指定できます。  
使用可能な文字は半角英数字で、最大 64 文字です。  
初期設定は「Log Keyword detection」です。

##### 検出文字列の指定

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

文字列の指定は、半角英数字で一行につき 255 文字まで、かつ最大 32 行までです。

空白・大小文字も判別します。

一行中に複数の文字(文字列)を指定すると、その文字(文字列)に完全一致したログのみ抽出して送信します。

なお「検出文字列の指定」項目は、「シスログのメール送信」機能のみ有効です。

### 各種システム設定

#### < PPPoE お知らせメール送信 >

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

##### お知らせメール送信

お知らせメール機能を使用する場合は「送信する」を選択します。

##### 送信先メールアドレス

お知らせメールの送り先メールアドレスを 1 箇所入力します。

最大文字数は 64 文字です。

##### 送信元メールアドレス

お知らせメールの送り元メールアドレスを 1 箇所入力します。

最大文字数は 64 文字です。

初期設定は「admin@localhost」です。

##### 件名

送信されるメールの件名を任意で設定できます。  
使用可能な文字は半角英数字で、最大 64 文字です。

初期設定は「Changed IP/PPP(oE)」です。

#### < PPPoE Backup 回線のお知らせメール送信 >

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

設定内容は < PPPoE お知らせメール送信 > と同様です。

##### お知らせメール送信

##### 送信先メールアドレス

##### 送信元メールアドレス

##### 件名

初期設定は「Started Backup connection」です。

必要項目への入力が終わりましたら「設定の保存」をクリックしてください。

##### 情報表示

リンクをクリックすると、メール送信の成功 / 失敗に関する情報が表示されます。

## 各種システム設定

## モバイル通信インターフェース一覧

本装置に装着されているデータ通信モジュールの状態を一覧で確認できます。

モバイル通信インターフェース一覧

インターフェースタイプ	インターフェース識別名	電波状態	取出
USB0	e-mobile D02HW	強	取り出せます
USB1		未装着	未装着
CF		未装着	ストレージ利用中

(画面は表示例です)

## インターフェースタイプ

CFカード、USB0、USB1の分類を表示します。

## インターフェース識別名

モバイル通信インターフェースに装着されているデータ通信カードを識別して、名称を表示します。

## 電波状態

モバイル通信インターフェースの状態を表示します。各状態についての表示内容は以下のとおりです。  
文字はすべて赤で表示されます。

## [未装着]

以下の状態に表示されます。

- データ通信モジュールが装着されていない状態
- CFタイプのデータ通信モジュールにて取り出し操作をおこなった場合

## [強 / 中 / 弱]

電波状態は、モバイル通信インターフェースが動作中である場合に表示されます。

各インターフェースの電波状態は「強」「中」「弱」の3段階で表示します。

## [未サポート]

NTT DoCoMoのデータ通信モジュール(A2502, P2403, N2502)を装着した場合に表示されます。  
電波状態は表示されませんが、モバイル通信は通常通り使用できます。

## [圏外]

データ通信モジュールを装着していても、圏外の場合に表示されます。

## インターフェースの取り出し実行方法

## 取出

モバイル通信インターフェースの取り出し操作に関する状態を表示します。

表示内容は以下のとおりです。

## [未装着]

以下の状態に表示されます。

- インターフェースタイプに関わらず、データ通信モジュールが装着されていない状態
- 装着中のCFタイプのデータ通信モジュールにて取り出し操作をおこない、取り出し可能状態である場合

## [取り出せます]

USBタイプのデータ通信モジュールが装着されている状態に表示されます。

装着中のUSBタイプのデータ通信モジュールを取り外す際は、そのまま抜き取ってください。

## [「実行」ボタン]

CFタイプのデータ通信モジュールが装着されている状態に表示されます。

装着中のCFタイプのデータ通信モジュールを取り出す際、「実行」ボタンをクリックすることにより無効化され、抜き出し可能な状態になります。

インターフェースタイプ:CF  
モバイル通信インターフェースを無効にしています

モバイル通信インターフェースを取り出せます

操作状況は順に表示されます。最後に、以下の表示が現れるまではそのままお待ちください。

## [設定画面へ]

表示がない状態で本装置へアクセスすると、操作処理に失敗することがあります。

本装置に装着したCFタイプのデータ通信モジュールを取り外すときは、必ず設定画面にて取り外しの操作をおこなってください。

本操作をおこなわずに取り外した場合、本装置が故障する場合があります。

## 各種システム設定

### [取り出せません]

PPP/PPPoE接続が動作開始状態である場合に表示されます。

「PPP/PPPoE接続設定」の「接続ポート」に指定されているデータ通信カードは取り出せません。

PPP/PPPoE接続設定画面で接続「切断」することで、「実行」ボタンが表示されます。

### [アクセスサーバ機能動作中]

アクセスサーバ機能が動作状態である場合に表示されます。

「アクセスサーバ設定」の「着信するモバイル通信インターフェース」に指定されているデータ通信カードは取り出せません。

アクセスサーバ設定を「使用しない」状態にすることで、「実行」ボタンが表示されます。

### [ストレージ利用中]

「外部ストレージ」にて、記録用途でインターフェースが装着されている場合に表示されます。

この状態の時は、データ通信モジュールはご利用なれません。

[ストレージ利用中]表示は、「外部ストレージ管理」において、装着された外部ストレージが初期化済状態で表示されます。

外部ストレージにつきましては、次ページ「外部ストレージ管理」をご参照ください。

## 各種システム設定

## 外部ストレージ管理

本装置では、CF、USB0、USB1 の各インターフェースをデータ（本体設定、シリログ情報）保存用としても利用することができます。  
利用できるストレージは、CF、USB0、USB1 のいずれか1つのインターフェースのみです。

## 外部ストレージ管理

ストレージタイプ	状態	操作
USB0	オプションUSBフラッシュディスクは、 通信用として利用中です	操作できません
USB1	オプションUSBフラッシュディスクは、 現在使用できません	初期化 有効 無効
CF	オプションCFカードの状況 総容量[62436 kbyte] 空容量[59428 kbyte] 使用率[5%]  機器設定のバックアップはありません	初期化 設定コピー 有効 無効

(画面は表示例です)

## ストレージタイプ

CFカード、USB0、USB1 の分類を表示します。

## 状態

外部ストレージの状態を表示します。

ストレージタイプは下記のように表示されます。

USB0, USB1 : オプション USB フラッシュディスク

CF : オプション CF カード

各状態についての表示内容は以下のとおりです。

文字はすべての状態が赤で表示されます。

## ・認識不可状態

外部ストレージが未装着のため認識されていない場合に表示されます。

[ オプション USB フラッシュディスクは、/  
オプション CF カードは、  
認識できません ]

## ・使用不可状態

初期化されていないため使用できない、または外部ストレージとして指定されていない場合に表示されます。

[ このオプションUSBフラッシュディスクは、/  
このオプションCFカードは、  
現在使用できません ]

## ・初期化前、有効実行状態

本装置にて初期化を実行する前に有効化させた場合に表示されます。

使用するには、初期化を実行してください。

[ このオプション USB フラッシュディスクは、/  
このオプション CF カードは、  
初期化しないと使用できません ]

## ・初期化済状態

初期化が実行済みにより本装置にて利用可能な場合に表示されます。

[ オプション USB フラッシュディスクの /  
オプション CF カードの  
状況 ]

総容量 [124906kbyte]

空容量 [121894kbyte]

使用率 [3%]

機器設定のバックアップはありません ]

## ・設定コピー状態

初期化が実行済みにより本装置にて利用可能な状態でいて、かつ既に設定情報が保存されている場合に設定をコピーした日時と合わせて表示されます。

[ オプション USB フラッシュディスクの /  
オプション CF カードの  
状況 ]

総容量 [124906kbyte]

空容量 [121826kbyte]

使用率 [3%]

機器設定のバックアップ日時

Aug 6 19:25 ]

## ・他機種において設定コピー済状態

既に本装置以外の機種の設定情報が保存されている外部ストレージを装着した場合に表示されます。

本装置で使用するには、初期化を実行してください。

[ このオプション USB フラッシュディスクには /  
このオプション CF カードには  
他機種のバックアップデータが含まれています ]

本装置に装着した外部ストレージの初期化を実行すると、外部ストレージに事前に保存されていたすべてのデータが削除されますのでご注意ください。

### 各種システム設定

#### ・通信利用状態

「モバイル通信インターフェース」にて、通信用途でインターフェースが装着されている場合に表示されます。  
この状態の時は、外部ストレージはご利用なれません。

[オプションUSBフラッシュディスクは、/  
オプションCFカードは、  
通信用として利用中です]

[通信用として利用中です]表示は、「モバイル通信インターフェース一覧」において、データ通信モジュールが装着状態で表示されます。  
モバイル通信インターフェースにつきましては、前ページ「モバイル通信インターフェース一覧」をご参照ください。

#### 外部ストレージの操作実行方法

##### 操作

装着した外部ストレージの中身を読み込んで、操作に関する項目を表示します。

各操作項目をクリックすると、該当の処理実行中画面が表示されますが、以下の表示が現れるまではそのままお待ちください。

[\[設定画面へ\]](#)

表示がない状態で本装置へアクセスすると、操作処理に失敗することがあります。

各操作についての操作内容は以下のとおりです。

##### [操作できません]

認識不可状態と、通信用途でインターフェースが装着されている場合に表示されます。

##### [初期化]

クリックすると、指定した外部ストレージを本装置で利用できるよう初期化をおこないます。  
実行すると、外部ストレージの現在の状況が「状態」欄に表示されます。

[ストレージ操作中]  
ストレージ(CF)を初期化しています

(設定状況は設定画面に戻り、確認して下さい)

#### [有効]

指定した外部ストレージを有効にします。  
ただし、初期化されていない場合は使用できませんので、初期化操作をおこなってください。

[ストレージ操作中]  
ストレージ(CF)を有効にしています

(設定状況は設定画面に戻り、確認して下さい)

#### [設定コピー]

現在設定されている設定内容を外部ストレージへコピーします。  
実行すると、設定コピー後の外部ストレージの使用状況が「状態」欄に表示されます。

[ストレージ操作中]  
ストレージ(CF)に設定をコピーしています

(設定状況は設定画面に戻り、確認して下さい)

#### [無効]

指定した外部ストレージを無効にします。  
本装置に装着した外部ストレージを取り外すときは、必ず設定画面にて[無効]化処理をおこなってください。  
本操作をおこなわずに取り外した場合、本装置が故障する場合があります。

実行すると、「状態」欄の表示が「認識不可状態」となり、外部ストレージを本装置から取り出し可能状態となります。

[ストレージ操作中]  
ストレージ(CF)を無効にしています

(設定状況は設定画面に戻り、確認して下さい)

[無効]化の実行後、本装置から外部ストレージを抜き取るタイミングは、画面に[\[設定画面へ\]](#)が表示された状態で抜き取ってください。

[無効]処理をした外部ストレージを装着したまま[\[設定画面へ\]](#)をクリックすると、新たに装着されたものとして読み込みをおこない、一覧表示には装着状態で表示されます。

# 第34章

---

---

情報表示

## 本体情報の表示

本体の機器情報を表示します。

以下の項目を表示します。

### ・ファームウェアバージョン情報

現在のファームウェアバージョンを確認できます。

### ・インターフェース情報

各インターフェースのIPアドレスやMACアドレスなどです。

PPP/PPPoEやIPsec論理インターフェースもここに表示されます。

### ・リンク情報

本装置の各Ethernetポートのリンク状態およびリンク速度が表示されます。

### ・ルーティング情報

直接接続、静态ルート、ダイナミックルートに関するルーティング情報です。

### ・Default Gateway情報

デフォルトルート情報です。

### ・DHCPクライアント情報

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

### 実行方法

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



画面中の「更新」をクリックすると、表示内容が更新されます。

# 第 35 章

---

---

テクニカルサポート

## 第35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。

Web設定画面の「テクニカルサポート」をクリックすると以下の画面が表示されます。

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。

情報の取得を行っています

情報の取得が終了しました

[download](#)

ブラウザのリンクを保存する等で保存して下さい

**remove**

「remove」をクリックすると、ファイルは消去されます。

ここでは、下記の3つの情報を一括して取得することができます。

ログ

詳細は、「第33章 各種システム設定 ログの表示 / 削除」をご覧ください。

設定ファイル

詳細は、「第33章 各種システム設定 設定の保存・復帰」をご覧ください。

本体の機器情報

詳細は、「第34章 情報表示」をご覧ください。

# 第 36 章

---

---

運用管理設定

### INITボタンの操作

本装置の前面にある「Init」ボタンを使用して、XR-430の設定を一時的に工場出荷設定に戻すことができます。

設定を完全にリセットする場合は、「システム設定」「設定のリセット」でリセットを実行してください。

#### 実行方法

- 1 電源OFFの状態にします。
- 2 本体前面にある「Init」ボタンを押します。
- 3 「Init」ボタンを押したままの状態で電源を投入し、電源投入後も5秒ほど「Init」ボタンを押しつづけます。

以上の動作で本装置は工場出荷時の設定で再起動します。

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

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

# 付録 A

---

---

インターフェース名一覧

## 付録A

### インターフェース名一覧

本装置は、以下の設定においてインターフェース名を直接指定する必要があります。

- ・OSPF機能
- ・スタティックルート設定
- ・ソースルート設定
- ・NAT機能
- ・パケットフィルタリング機能
- ・仮想インターフェース機能
- ・ネットワークテスト

本装置のインターフェース名と実際の接続インター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
ppp0	PPP/PPPoE主回線
ppp2	PPP/PPPoEマルチ接続 2
ppp3	PPP/PPPoEマルチ接続 3
ppp4	PPP/PPPoEマルチ接続 4
ppp5	バックアップ回線
ppp6	リモートアクセス回線
ipsec0	ppp0上のipsec
ipsec1	ppp2上のipsec
ipsec2	ppp3上のipsec
ipsec3	ppp4上のipsec
ipsec4	ppp5上のipsec
ipsec5	eth0上のipsec
ipsec6	eth1上のipsec
gre<n>	gre (<n>は設定番号)
eth0.<n>	eth0上のVLANインターフェース (<n>はVLAN ID)
eth1.<n>	eth1上のVLANインターフェース

表左：インターフェース名

表右：実際の接続デバイス

# 付録 B

---

---

工場出荷設定一覧

## 付録B

### 工場出荷設定一覧

IPアドレス設定	IPアドレス/サブネットマスク値
Ether0ポート	192.168.0.254/255.255.255.0
Ether1ポート	192.168.1.254/255.255.255.0
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
ダイヤルアップ接続	無効
DNSリレー/キャッシュ機能	有効
DHCPサーバ/リレー機能	有効
IPsec機能	無効
UPnP機能	無効
ダイナミックルーティング機能	無効
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
VRP機能	無効
アクセスサーバ機能	無効
スタティックルート設定	設定なし
ソースルーティング設定	設定なし
NAT機能	設定なし
パケットフィルタリング機能	NetBIOSからの漏洩を防止するフィルタ設定 (入力・転送フィルタ設定)  外部からのUPnPパケットを遮断する設定 (入力・転送フィルタ設定)
ネットワークイベント機能	無効
仮想インターフェース機能	設定なし
GRE機能	無効
パケット分類機能	設定なし
Web認証機能	無効
設定画面ログインID	admin
設定画面ログインパスワード	admin

# 付録 C

---

---

サポートについて

## サポートについて

本製品に関するサポートは、ユーザ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、お願いいいたします。

サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。

・サポートデスク

e-mail : support@centurysys.co.jp

電話 : 0422-37-8926

FAX : 0422-55-3373

受付時間 : 10:00 ~ 17:00 (土日祝祭日、および弊社の定める休日を除きます)

・ホームページ <http://www.centurysys.co.jp/>

故障と思われる場合は

製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。

事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

ご連絡をいただく前に

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

- ・ファームウェアのバージョンと MAC アドレス  
(バージョンの確認方法は「第 34 章 情報表示」をご覧ください)
- ・ネットワークの構成(図)  
どのようなネットワークで運用されているかを、差し支えのない範囲でお知らせください。
- ・不具合の内容または、不具合の再現手順  
何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせください。
- ・エラーメッセージ  
エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
- ・XR-430 の設定内容、およびコンピュータの IP 設定
- ・可能であれば、「**設定のバックアップファイル**」をお送りください。

サポート情報

弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。  
また製品の FAQ も掲載しておりますので、是非ご覧ください。

FutureNet XR シリーズ 製品サポートページ

<http://www.centurysys.co.jp/support/>

インデックスページから本装置の製品名「> XR-430」をクリックしてください。

製品の保証について

本製品の保証期間は、お買い上げ日より 1 年間です。

保証期間をすぎたもの、保証書に販売店印のないもの(弊社より直接販売したもののは除く)、また保証の範囲外の故障については有償修理となりますのでご了承ください。

保証規定については、同梱の保証書をご覧ください。

---

XR-430 ユーザーズガイド v1.1.0 対応版

2008 年 08 月 版

発行 センチュリー・システムズ株式会社

Copyright (c) 2008 Century Systems Co., Ltd. All rights reserved.

---