

Allied Telesis

CentreCOM®

AR450S

Broadband Router

取扱説明書



CentreCOM AR450S

取扱説明書

アライドテレシス株式会社

安全のために

必ずお読みください



この取扱説明書には、お客様や他の人々への危害や財産への損害を未然に防ぎ、本製品を安全にお使いいただくために、守っていただきたい事項を記載しています。

その表示と図記号は次のようになっています。内容をよく理解してから、本文をお読みください。

本書を紛失または損傷したときは、当社のサポートセンターまたはお買い求めになった販売店でお求めください。

本書中で使用するマーク



警告

人命を失う、けがをするなど人身に対する危険性、本製品や他の機器の故障、データの破壊や消失などの可能性があることを示しています。



注意

本製品の動作に障害が発生する可能性があることを示しています。



ヒントマーク

知っていると便利な情報です。



参照

参照先を示しています。

ご使用にあたってのお願い

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

- ご使用の際は取扱説明書に従って正しい取り扱いをしてください。
- 本商品の故障、誤動作、不具合、あるいは停電等の外部要因によって、通信などの機会を逸したために生じた損害等の純粋経済損害につきましては、当社は一切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。
- 本商品を分解したり改造したりすることは絶対に行わないでください。
- 本商品および本書の一部または全部の無断改変、無断転載、無断複写を禁止いたします。
- この取扱説明書、ハードウェア、ソフトウェアおよび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。
- 本書は大切に保管してください。



警告

下記の注意事項を守らないと火災・感電により、死亡や大けがの原因となります。

分解や改造をしない

本製品は、取扱説明書に記載のない分解や改造はしないでください。火災や感電、けがの原因となります。



分解禁止

雷のときはケーブル類・機器類にさわらない

感電の原因となります。



雷のときはさわらない

異物はいれない 水は禁物

火災や感電の恐れがあります。水や異物を入れないように注意してください。万一水や異物が入った場合は、電源プラグをコンセントから抜いてください。(当社のサービス取扱所または販売店にご連絡ください。)



異物厳禁

表示以外の電圧では使用しない

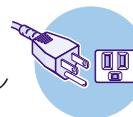
火災や感電の原因となります。
本製品は AC100 - 240V で動作します。
なお、本製品に付属の電源ケーブルは 100V 用ですのでご注意ください。



電圧注意

正しい電源ケーブル・コンセントを使用する

不適切な電源ケーブル・コンセントは火災や感電の原因となります。
接地端子付きの3ピン電源ケーブルを使用し、接地端子付きの3ピン電源コンセントに接続してください。



3ピン
コンセント

コンセントや配線器具の定格を超える使い方はしない

たこ足配線などで定格を超えると発熱による火災の原因となります。



たこ足禁止

設置・移動のときは電源プラグを抜く

感電の原因となります。



プラグを
抜け

電源ケーブルを傷つけない

火災や感電の原因となります。

電源ケーブルやプラグの取扱上の注意：

- ・加工しない、傷つけない。
- ・重いものを載せない。
- ・熱器具に近づけない、加熱しない。
- ・電源ケーブルをコンセントから抜くときは、必ずプラグを持って抜く。



傷つけない

ぬれた手で電源プラグを抜き差ししない

感電の原因となります。



ぬれた手で
さわらない

湿気やほこりの多いところ、油煙や湯気のあたる場所には置かない

内部回路のショートの原因になり、火災や感電の恐れがあります。



設置場所
注意

通風口はふさがらない

内部に熱がこもり、火災の原因となります。



ふさがらない



注意

下記の注意事項を守らないと、**データ**の損失や、**本製品の故障**などの原因になります。

次のような場所での使用や保管はしないでください。

- ・直射日光の当たる場所
- ・暖房器具の近くなどの高温になる場所
- ・急激な温度変化のある場所（結露するような場所）
- ・湿気が多い場所や、水などの液体がかかる場所（湿度80%以下の環境でご使用ください）
- ・振動の激しい場所
- ・ほこりの多い場所や、シュータンを敷いた場所（静電気障害の原因になります）
- ・腐食性ガスの発生する場所



静電気注意

本製品は、静電気に敏感な部品を使用しています。部品が静電破壊する恐れがありますので、コネクターの接点部分、ポート、部品などに素手で触れないでください。



取り扱いはていねいに

落としたり、ぶつけたり、強いショックを与えないでください。



お手入れについて

清掃するときは電源を切った状態で

誤動作の原因になります。



機器は、乾いた柔らかい布で拭く

汚れがひどい場合は、柔らかい布に薄めた台所用洗剤（中性）をしみこませ、強く絞ったものでふき、乾いた柔らかい布で仕上げてください。



ぬらすな



中性洗剤
使用



強く絞る

お手入れには次のものは使わないでください

・石油・みがき粉・シンナー・ベンジン・ワックス・熱湯・粉せっけん
(化学ぞうきんをご使用のときは、その注意書に従ってください。)



シンナー
類不可

0.1 本書について

この度は、AR450S をお買いあげいただき、誠にありがとうございます。
ます。

AR450S (以下本製品) は、企業拠点向けのインターネット接続に最適なブロードバンドルーターです。L2TP や IPsec による VPN で、インターネット経由の LAN 間接続が可能です。

本書は、はじめて本製品に触れるお客様が、本製品を使い始めるための情報が記載されています。また、章を読み進むごとに、段階を追って理解を深めていけるよう、ストーリーだてた構成となっています。

本書は、紙面の都合により、基本的な情報のみが記載されており
ます。より高度な設定のための情報は、CD-ROM の「コマンドリファ
レンス」、「設定例集」をご覧ください。

本製品を正しくお使いいただくため、ご使用になる前に本書をよくお
読みください。また、お読みになった後も大切に保管してください。

本書は、本製品のソフトウェアバージョン「2.5.2」をもとに記述さ
れていますが、「2.5.2」よりも新しいバージョンのソフトウェアが搭
載された製品に同梱されることがあります。その場合は、必ずリリ
ースノートや添付書類をお読みください。リリースノートや添付書類
には、重要な情報や、最新の情報が記載されています。

0.2 付属の CD-ROM について

付属の CD-ROM には、以下のマニュアルや情報が収録されていま
す。CD-ROM をコンピューターの CD-ROM ドライブに挿入すると、
自動的に HTML ファイルが表示されますので、表示内容に従って操
作してください。

・ソフトウェアリリースノート

今回のソフトウェア (ファームウェア) リリースで追加された機
能、変更点、注意点についてまとめたものです。過去の変更履歴
も記載されています。

・コマンドリファレンス

コマンドや、コマンドが取るパラメーターの詳細、機能の解説が
記載されています。本書の内容を含む、本製品の完全な情報が記
載されており、関連する設定例へのリンクがあります。

トップメニュー(機能)



サブメニュー(コマンド、機能の解説、設定例)

図 0.2.1 コマンドリファレンス

・設定例集

具体的な構成例を図解で示し、構成に関する設定の要点を簡潔に
説明したマニュアルです。構成例のリストは、番号順、回線別、
機能別にソートして、簡単に設定例を探しあてられるよう工夫さ
れています。

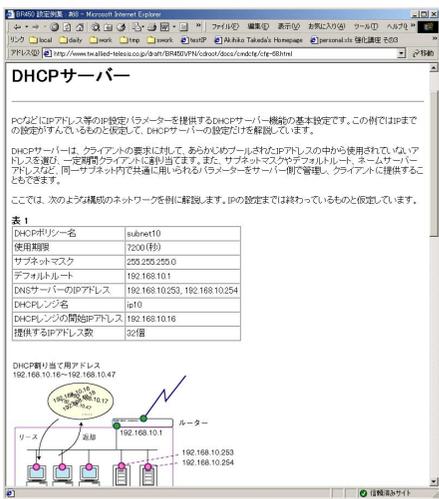


図 0.2.2 設定例集

0.3 表記について

画面表示

- コンソールターミナルに表示された内容や入力した文字を説明する場合、枠線で囲んでいます。
- 入力する文字を明示的に示す場合、**太文字**を使用します（下記の例では「HELP」）。
- 太文字以外の表示は、自動的に表示される文字です。
- コマンドを最後まで入力したら、**リターンキー**または**エンターキー**を 1 度押します（以後「リターンキーを押す」というように表現します）。

リターンキーは、「**↵**」マークで表します。下記では、「HELP」を入力し、リターンキーを押しています。

```
Manager > HELP ↵

AR450 オンラインヘルプ - V2.5 Rev.01 2003/05/06

This online help is written in Japanese (Shift-JIS).

入力は太文字の部分だけでかまいません（"HELP OPERATION" は "H O" と省略可）。

Help Operation      運用・管理（SNMP、ログ、トリガー、スクリプトなど）
Help Interface      インターフェース（スイッチ、ETHなど）
Help Ppp             PPP
Help Bridge         ブリッジング
Help IP              IP（RIP、OSPF、IPフィルターなど）
Help IPv6            IPv6
Help Firewall       ファイアウォール
Help Vrrp            VRRP
Help Dhcp            DHCP サーバー
Help Gre            GRE
Help L2tp            L2TP
Help IPsec           IPsec
Help Enco            番号

--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

図 0.3.1 表示画面の例

- 長いコマンドを紙面の都合で折り返す場合は、2 行目以降を**字下げ**して表します。実際にコマンドを入力する場合は、字下げされている行の前でスペース 1 つを入力してください（下記では、「SM=...」「DM=...」「AC=...」の前にスペースが 1 つ入っています）。すべての行を入力し、最後にリターンキーを押してください。

```
ADD IP FILT=1 SO=192.168.20.4
SM=255.255.255.255 DES=192.168.10.2
DM=255.255.255.255 DP=23 PROT=TCP SESS=ANY
AC=INCL ↵
```

図 0.3.2 紙面の都合でコマンドに折り返しがある例

キー入力における表記

- 「**Ctrl/△**」は、Ctrl キーを押しながら、△キーを押す操作を表します。
- 「**○,△**」は、○キーを押し、○キーを離してから、△キーを押す操作を表します。
 - 例 1 「**Break,T**」は、Break キーを押し、Break キーを離してから T キーを押します。
 - 例 2 「**Ctrl/K, Ctrl/X**」は、Ctrl キーを押しながら K キーを押し、Ctrl と K キーを離して、Ctrl キーを押しながら X キーを押します (Ctrl キーを押しながら K キーを押し、K キーのみを離して、X キーを押してもかまいません)。

製品名

本書では、「AR450S」を「本製品」と略します。

デフォルト

デフォルトは、何も指定しなかったときに採用されるもの、パラメーターなどを省略したときに採用される数値、またはご購入時の設定を意味します。

固有の文字列、グローバル IP アドレスについてのお断り

本書は、説明のために以下のような架空の文字列、グローバル IP アドレスを使用します。以下のグローバル IP アドレスは、お客様の環境でご使用いただくことはできません。実際の設定では、お客様の環境におけるものに適宜読み替えていただけますようお願い申し上げます。

- PPP 接続のためのログイン名として「site_a@example.co.jp」
- PPP 接続のためのパスワードとして「passwd_a」
- プロバイダーから与えられたコンピューター名として「zy1234567-a」
- プロバイダー側の DHCP サーバーとして「123.45.11.5」
- プロバイダー側の DNS サーバーのアドレスとして「87.65.43.21」「87.65.43.22」
- プロバイダー側のルーターとして「123.45.11.1」
- プロバイダーから取得したグローバル IP アドレスとして「123.45.67.80 ~ 123.45.67.87」「123.45.11.22」

安全のために	4	3.5 システム名の変更	29
本書中で使用するマーク	4	3.6 システム時間の設定	29
ご使用にあたってのお願い	4	3.7 設定の保存	30
0.1 本書について	8	3.8 起動スクリプトの指定	31
0.2 付属の CD-ROM について	8	3.9 再起動	31
0.3 表記について	9	RESTART ROUTER コマンドの入力	31
画面表示	9	RESTART REBOOT コマンドの入力	32
キー入力における表記	9	電源のオフ / オン	32
製品名	9	再起動時のご注意	32
デフォルト	9	3.10 ログアウト	32
固有の文字列、グローバル IP アドレスについてのお断り	9	3.11 停止	32
		3.12 ご購入時の状態に戻す	33
		3.13 ロックアウトされてしまったとき	33
		3.14 設定情報の表示	34

第 1 部 基本編

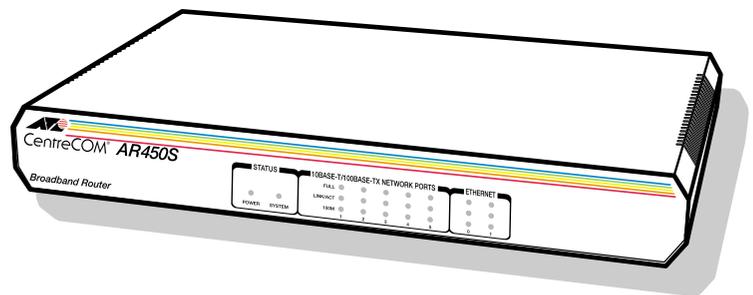
1 お使いになる前に	17	4 設定のための基礎知識	35
1.1 パッケージの確認	17	4.1 コマンドプロセッサ	35
1.2 特長	18	コマンド入力 の 注意 点	35
1.3 各部の名称と働き	20	キー操作 (ヒストリー機能)	36
2 設置・配線	23	次に選択可能なキーワードを表示する「?」	36
2.1 基本的なネットワーク構成	23	コマンドの分割入力	36
2.2 19 インチラックへの取り付け	24	IP フィルターコマンドの分割入力	37
設置における注意	24	4.2 コマンドの分類	38
取り付け手順	24	設定コマンド	38
2.3 配線する	24	実行コマンド	38
準備	24	4.3 オンラインヘルプ	39
❶ ONU / メディアコンバータを接続する	25	4.4 インターフェース	40
❷ コンピューターを接続する	25	インターフェースの階層構造	40
❸ コンソールターミナルを接続する	25	パラメーターにおけるインターフェースの表記	41
❹ 電源ケーブル抜け防止フックを取り付ける	25	物理インターフェース	41
❺ 電源ケーブルの接続	26	データリンク層インターフェース	43
2.4 HUB を接続する	26	ネットワーク層インターフェース	44
3 起動・設定の保存・再起動	27	4.5 ルーティング (スタティック)	45
3.1 コンソールターミナルの設定	27	2 つの LAN の接続	45
3.2 起動	27	3 つの LAN の接続	46
トラブルシューティング	27	デフォルトルート	48
3.3 ログイン (ご購入時)	28	インターネットからの戻りのルート	49
3.4 パスワードの変更	28	コンピューターにおけるデフォルトルート	49
		5 ユーザー管理とセキュリティー	51
		5.1 ユーザーレベル	51

5.2 ユーザー認証データベース.....	51	11 バージョンアップ.....	69
5.3 ユーザーの登録と情報の変更.....	52	11.1 必要なもの.....	69
新規ユーザー登録.....	52	11.2 セットアップツール.....	69
ユーザー情報変更.....	52	11.3 最新ソフトウェアセットの入手方法.....	69
パスワード変更.....	53	11.4 ファイルのバージョン表記.....	69
ユーザー情報表示.....	53	ファームウェアファイル.....	69
ユーザー削除.....	53	パッチファイル.....	69
ユーザー一括削除.....	53	ソフトウェアセット.....	70
5.4 ノーマルモード / セキュリティーモード.....	54	12 困ったときに.....	71
セキュリティモードへの移行.....	54	12.1 トラブルへの対処法.....	71
ノーマルモードへ戻る.....	55	LEDの観察.....	71
6 テキストエディター.....	57	本製品のログを見る.....	71
6.1 Editの実行.....	57	12.2 トラブル例.....	72
6.2 キー操作.....	57	コンソールターミナルに文字が入力できない.....	72
7 Telnetを使う.....	59	コンソールターミナルで文字化けする.....	72
7.1 本製品にTelnetでログインする.....	59	再起動したらプロバイダーに接続しない.....	72
7.2 フリッピングにおけるTelnet.....	59	パスワードを忘れた.....	72
7.3 TELNETコマンドの実行.....	60	ライセンスを削除した.....	73
IPアドレスのホスト名を設定する.....	60		
DNSサーバーを参照するように設定する.....	60		
8 Ping・Trace.....	61	第2部 設定例編	
8.1 Ping.....	61	13 構成例.....	77
8.2 Trace.....	61	13.1 設定をはじめの前に.....	77
9 ファイルシステム.....	63	コマンド入力における注意.....	77
9.1 フラッシュメモリー・ファイルシステム.....	63	コマンド入力の便宜のために.....	77
フラッシュメモリーのコンパクション.....	64	13.2 PPPoEによる端末型インターネット接続.....	78
9.2 ファイル名.....	64	プロバイダーから提供される情報.....	78
9.3 ワイルドカード.....	65	設定の方針.....	78
		設定.....	79
		まとめ.....	82
10 アップ/ダウンロード.....	67	13.3 PPPoEによるLAN型インターネット接続(アン ナンバード).....	83
10.1 TFTP.....	67	プロバイダーから提供される情報.....	84
ダウンロード.....	67	設定の方針.....	84
アップロード.....	67	設定.....	84
10.2 Zmodem.....	68	まとめ.....	87
ダウンロード.....	68	13.4 PPPoEによるLAN型インターネット接続(DMZ の設定).....	88
アップロード.....	68	プロバイダーから提供される情報.....	89
		設定の方針.....	89

設定	89	ハイパーターミナルの終了	145
まとめ	93	A.3 CONSOLE ポート	146
13.5 インターネット接続による 2 点間 IPsec VPN	94	A.4 10BASE-T/100BASE-TX ポート	147
プロバイダーから提供される情報	94	A.5 製品仕様	148
設定の方針	94	ハードウェア	148
拠点 A の設定	95	ソフトウェア	149
拠点 B の設定	100		
接続の確認	104	B ユーザーサポート	151
まとめ	105	B.1 保証について	151
13.6 インターネット接続による 3 点間 IPsec VPN	107	保証の制限	151
プロバイダーから提供される情報	107	B.2 ユーザーサポート	151
設定の方針	108	調査依頼書の内容について	151
拠点 A の設定	109	ご注意	153
拠点 B、拠点 C の設定	113	商標について	153
接続の確認	118	マニュアルバージョン	153
まとめ	119		
13.7 インターネットと CUG サービスの同時接続 (端 型)	121		
プロバイダーから提供される情報	122		
設定の方針	122		
設定	122		
まとめ	127		
13.8 インターネットと CUG サービスの同時接続 (LAN 型)	128		
プロバイダーから提供される情報	128		
設定の方針	128		
設定	129		
まとめ	133		
13.9 設定上の注意事項	135		
トリガーの動作	135		
設定の保存はリンクダウンの状態	135		
接続できないときは	136		
PPPoE セッションの手動による切断	136		
再接続	137		
PPPoE におけるアンナンバード	137		
A 付録	141		
A.1 コンピューターの設定	141		
Windows 2000	141		
Mac OS X	142		
A.2 ハイパーターミナルの設定	143		
ハイパーターミナルの設定の保存	145		

第 1 部 基本編

ここでは、本製品のパッケージを開けられた時点から、ご活用いただくまでのさまざまな場面で必要となる、基本的な情報について説明します。



1 お使いになる前に

1.1 パッケージの確認

パッケージを開いたら、これらがすべて揃っているかどうかを確認してください。万一、足りないものがありましたら、お買い上げになった販売店までお問い合わせください。

ルーター本体

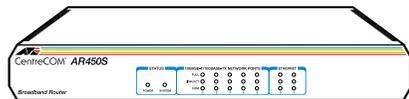


図 1.1.1 ルーター本体

電源ケーブル

本製品に電源を供給するための電源ケーブルです。必ず本製品に付属している電源ケーブルをご使用ください。不適切な AC アダプター、電源ケーブルをご使用になると、本製品の故障や火災の原因になり危険です。

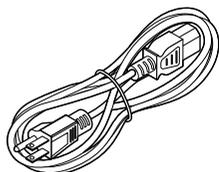


図 1.1.2 電源ケーブル

コンソールケーブル

本製品の CONSOLE ポート (RS-232) とコンソールターミナルを接続するためのストレートタイプの RS-232 ケーブルです。コネクタは、9 ピンオス (本製品側) - 9 ピンメスとなっています。

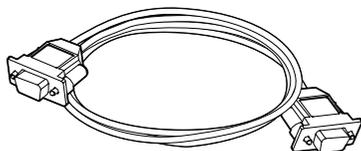


図 1.1.3 コンソールケーブル

電源ケーブル抜け防止フック

電源ケーブルの抜け落ちを防止するフックです。電源コネクターのフック取り付けプレートに取り付けて使用します。



図 1.1.4 電源ケーブル抜け防止フック

CD-ROM、マニュアルなど

基本的に下記の品が付属しています。これ以外に資料などが添付されることがあります。

- CD-ROM 1 枚
- 取扱説明書 1 冊
- 製品保証書 1 枚
- シリアル番号シール 2 枚



本製品を移送する場合は、ご購入時と同じ梱包箱で再梱包されることが望まれます。再梱包のために、本製品が納められていた梱包箱、緩衝材などは捨てずに保管してください。

1.2 特長

AR450S (以下本製品) は、企業向け高速ブロードバンドルーターです。本製品は、次のような特長を持っています。

インターネット接続と SOHO 環境の構築

WAN ポートを 2 つ、LAN 側として 5 ポートのスイッチを装備しています。他の HUB/ スイッチを用意せずに、5 台までのコンピューターを接続できます。各ポートは、10BASE-T、100BASE-TX に対応しています。また、WAN ポートの 1 つは DMZ ポートとしても使用することが可能になっており、LAN 内のセキュリティを保ったまま、WAN 側に各種サーバーを公開することができます。

さまざまな回線や接続サービスをサポート

xDSL、FTTH (10/100Mbps) などのブロードバンド系サービスに対応しています。

PPPoE (PPP over Ethernet) に対応した xDSL、FTTH 系のインターネット接続サービスが利用できます。PPPoE は、接続サービスが対応していれば、同時に 5 セッションまでの接続が可能です。アンナナンバーによる接続に対応しておりますので、複数グローバル IP 固定割り当てサービス (アンナナンバー接続) の利用も可能です。

DHCP クライアントも実装されているので、DHCP を利用したインターネット接続サービスも利用できます。

IP アドレスの有効利用

NAT/EnhancedNAT により、プロバイダーから取得したグローバルアドレスを共有し、LAN 側の複数のコンピューターでインターネットを利用できます。グローバル IP 固定型のサービスを利用すれば、Web サーバーの公開も可能です。

DHCP サーバー/リレーエージェント

IP アドレス、デフォルトルート、DNS アドレスといった、LAN 環境のコンピューターの設定情報を、DHCP サーバーによって一括管理することにより、管理の労力を削減できます。また、DHCP リレーエージェントにより、他のサブネットに存在する DHCP サーバーに対して、DHCP リクエストを中継することができます。

DNS リレー

LAN 環境のコンピューターからの DNS リクエストに対して、本製品が代理で DNS 問い合わせを行い、その結果をコンピューターに返す機能です。DHCP サーバーと併用する場合、コンピューターに通知する DNS アドレスとして、本製品の LAN 側 IP アドレスを設定しておきます。

ファイアウォールと IP フィルター

IP トラフィックフローの開始・終了を認識し、これに応じて動的なパケットフィルタリングを行うステートフル・インスペクション型のファイアウォールが搭載されています。

また、ヘッダー情報に基づき、受信 IP インターフェースにおける、パケットの破棄・通過を行う IP フィルター (トラフィックフィルター) も搭載されています。

汎用設計の IP フィルターに対して、ファイアウォールはインターネット接続を念頭に置いた設計になっており、最小限の設定で高い安全性を確保できるようになっています。ファイアウォールと IP フィルターは、運用上のニーズに応じて、使い分けたり、併用することができます。

セキュリティを保ちながら通信コストをカット (VPN)

L2TP により、インターネット経由の VPN が構築できます。IPsec を併用すればセキュリティも確保できます。インターネットの利用により、ローコストの LAN 間接続が可能です。

ルーティングプロトコル

RIP V1/V2、OSPF に対応しています。スタティックな経路情報も設定できます。

通信サービスの管理

受信パケットのヘッダー情報に基づき、パケットを送信するときに 8 段階の絶対優先度を設定できます (Priority-based Routing)。特定のトラフィックを最優先で送信できるよう設定できるので、例えば高トラフィック時における Telnet などのレスポンスの悪化を防ぐことができます。また、プリッジングではプロトコル別に 5 段階の優先度を設定できます。

受信パケットのヘッダー情報に基づき、パケットに経路選択ポリシー (サービスタイプ) を割り当て、サービスタイプに該当するパケットごとに異なる経路をとらせることが可能です (Policy-based Routing)。

高い信頼性を持つIP ネットワークの構築

VRRP (Virtual Router Redundancy Protocol) をサポートしています。VRRP は、複数のルーターをグループ化して (マスターと1台以上のバックアップ)、あたかも1台のルーターであるかのように見せかけるプロトコルです。マスタールーターの故障やリンクダウンなどの障害が発生した場合、バックアップルーターがマスタールーターに昇格し、障害が発生したルーターの動作を引き継ぎます。VRRP により、システムは冗長性を持ち、高い信頼性を持つIP ネットワークを構築できます。

同一LAN 上に複数のマスタールーターが存在する場合、複数のマスタールーターで1台のバックアップルーターを共有できます。

負荷分散機能により、機器や回線を有効利用することができます。

PPP認証とIPアドレスプール

PPP による接続における認証方法として、本製品のデータベースまたは認証サーバー (RADIUS) を使用できます。接続ユーザーに対してIP アドレスを与える場合、IP アドレスプールから動的にIP アドレスを割り当てることができます。

扱いやすいファイルシステム

コンフィグレーションは、設定スクリプトファイル (テキスト) として、フラッシュメモリー (ファイルシステム) に保存されます。ファイルシステムには、複数の設定スクリプトファイルを保存しておけます。トリガーと組み合わせることにより、環境の変化に合わせて、自動的に設定を切りかえるなど、柔軟な運用が可能です。

バッチファイルによるコマンドの実行ができます。バッチファイル (.SCP) には、設定スクリプトファイル (.CFG) に直接記述できないコマンドを記述することができ、実行結果のログも出力されます。この機能は、多くのルーターを管理する場合に、非常に便利です。

TFTP、Zmodem によるスクリプトファイルのアップ / ダウンロードができます。また、ファイルを編集するための、テキストエディターを搭載しています。

専用のセットアップツールによって、ファームウェアのバージョンアップが簡単にできます。最新ファームウェア、セットアップツールは、弊社のWeb ページからダウンロードできます。

システムの運用や管理

SSH (SecureShell)、Telnet による、本製品の遠隔管理ができます。

日時や曜日、特定インターフェースのリンクアップやダウンなど、様々なイベントによるトリガーを発生できます。例えば、ある時間内のみ通信を許可するといったことが可能です。

インターネットからのアタック、回線のリンク状態の変化、ログなどを、メールとして送信できます (SMTP)。

Syslog サーバーに対して、ログの出力ができます。ログは、コンソール、SSH、Telnet で確認することもできます。

NTP クライアントによる時間の同期が可能です。

SNMP をサポートしているので、インテリジェントHUB/ スイッチなどを含めた統合的なネットワーク管理が可能です。

機能は、本製品にロードされているファームウェアのバージョンに依存します。最新の機能は、リリースノートをご覧ください。

1.3 各部の名称と働き

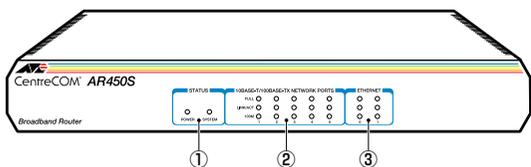


図 1.3.1 前面図

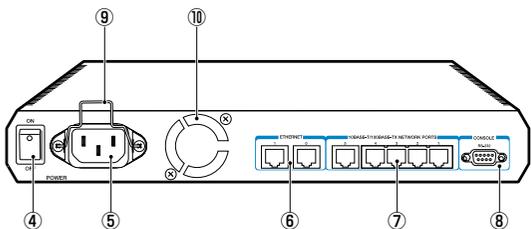


図 1.3.2 背面図

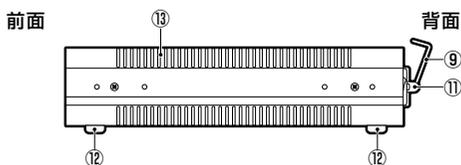


図 1.3.3 側面図

① STATUS LED

本製品の体系的な状態を表示するLEDです。

LED	色	状態	表示の内容
POWER	緑	点灯	本製品に電源が供給されています。
		消灯	本製品に電源が供給されていません。
SYSTEM	橙	点灯	本製品に異常が発生しています。
		消灯	本製品は正常に動作しています。

② 10BASE-T/100BASE-TX NETWORK PORTS LED

LAN 側の各ネットワークポートの接続状態や、ネットワークのアクティビティを表示するLEDです。LEDは各ポートごとに存在します (5 組み)。

LED	色	状態	表示の内容
FULL	緑	点灯	Full Duplex (全二重) でリンク ^a が確立しています。
		消灯	Half Duplex (半二重) でリンクが確立しています。
LINK/ACT	緑	点灯	Fullまたは Half Duplex でリンクが確立しています。
		点滅	パケットの送受信が行われています。
		消灯	リンクが確立していません。
100M	緑	点灯	100Mbps でリンクが確立しています。
		消灯	10Mbps でリンク ^a が確立しています。

a. FULL、100M LED における表示は、LINK/ACT LED が点灯 (リンクが確立) していることを前提としています。

③ ETHERNET LED

WAN 側ポート (ETH0、ETH1) の接続状態や、ネットワークのアクティビティを表示するLEDです。表示の意味は、10BASE-T/100BASE-TX NETWORK PORTS LED と同じです。

④ 電源スイッチ

本製品に供給される電源をオン、オフするためのスイッチです。

⑤ 電源コネクタ

電源ケーブルを接続するためのコネクタ (ソケット) です。本製品は、AC100-240V で動作しますが、付属のケーブルは AC100-120V 用ですのでご注意ください。

⑥ ETHERNET ポート

WAN 側の Ethernet ポートです (MDI)。2つのポート (ETH0、ETH1) があり 10BASE-T または 100BASE-TX に対応しています (オートネゴシエーション)。

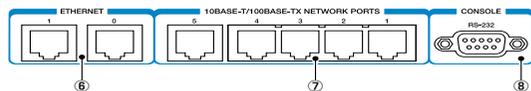


図 1.3.4 ポート

⑦ 10BASE-T/100BASE-TX ポート

LAN 側の Ethernet ポートです。5 つのポートがあり、各ポート間の通信はスイッチングにより行われます。10BASE-T または 100BASE-TX に対応しています（オートネゴシエーション）。すべてのポートは MDI/MDI-X の自動切り替えに対応していません。

⑧ CONSOLE ポート

本製品を設定するためのコンソールターミナルを接続する RS-232C ポートです。コンソールターミナルとの接続のために、コンソールケーブルが付属しています。

⑨ 電源ケーブル抜け防止フック

電源ケーブルの抜け落ちを防止する金具です（ご購入時は、フックは取り外された状態で、同梱されています）。

⑩ ファン

内部の熱を排出するためのファンです。この穴を塞がないように設置してください。

⑪ フック取り付けプレート

電源ケーブル抜け防止フックを取り付けるプレートです。

⑫ ゴム足

据え置き設置の際、本製品を固定し、衝撃を吸収するゴム足です。

⑬ 通気口

換気により、本体内部の熱を逃がすための通気口です。



本製品を設置する際は、この通気口をふさがないでください。通気口をふさいでしまうと、本製品の温度が上昇し、本製品の故障の原因になります。また、火災などの原因となることがあるため危険です。

2 設置・配線

本製品の設置時の注意点、電源ケーブル抜け防止フックの取り付け、配線の仕方について説明します。プロバイダーとの接続の方法は、

CATV、ADSL、FTTH、無線がありますが、以下ではFTTHの場合を例に挙げます。

2.1 基本的なネットワーク構成

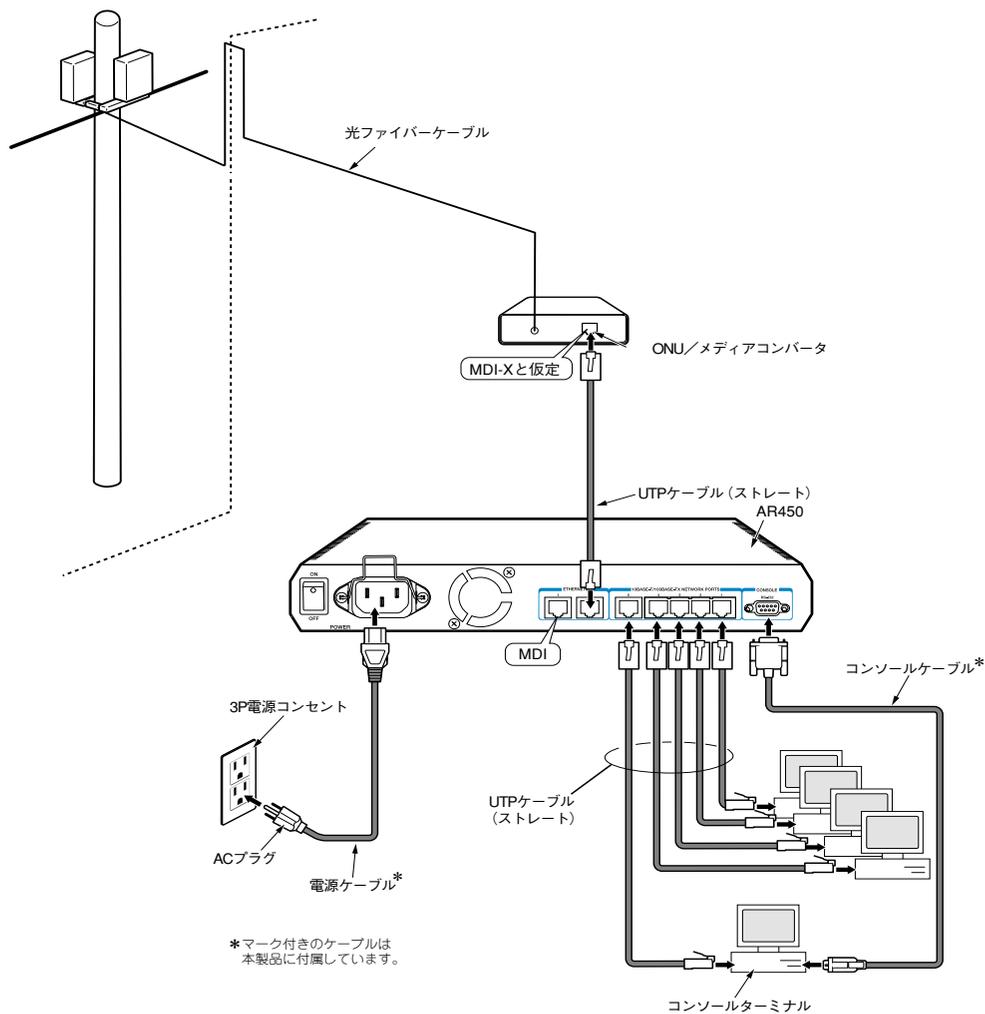


図 2.1.1 : FTTHを使用した基本的なネットワーク構成例

2.2 19 インチラックへの取り付け

本製品は卓上に設置するだけでなく、別売のラックマウントキット(AT-RKMT-J07)を使用して19インチラックに設置することができます。

設置における注意

本製品の設置や保守を始める前に、必ず「安全のために」(p.4)をよくお読みください。また、次の点に注意して設置してください。

- 接続されているケーブル類に無理な力が加わるような配置や敷設はさけてください。
- テレビ、ラジオ、無線機などのそばに設置しないでください。
- 傾いた場所や、不安定な場所に設置しないでください。
- 本製品の上にものを置かないでください。
- 直射日光のあたる場所、多湿な場所、ほこりの多い場所に設置しないでください。
- 19インチラックに設置する場合は、正しいラックマウントキットを使用してください。

取り付け手順

- 1 ブラケットは、本製品の前面側または背面側に取り付けることができます。ブラケットの取り付け側を決めてください。
- 2 ラックマウントキットに付属のネジを使用し、次図のようにブラケットと取っ手を本製品の両側面に取り付けてください。詳しくは、ラックマウントキットに付属のマニュアルをご覧ください。

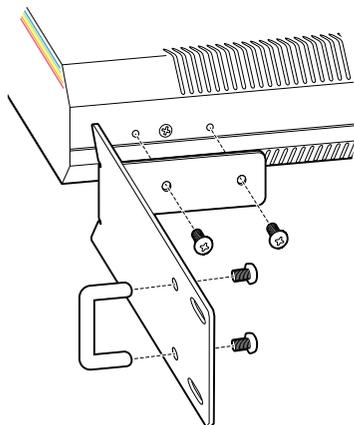


図2.2.1 ブラケットの取り付け

- 3 ラックに取り付けてください。ラックへの取り付けネジはラックマウントキットに付属しておりません。お客様でご用意ください。

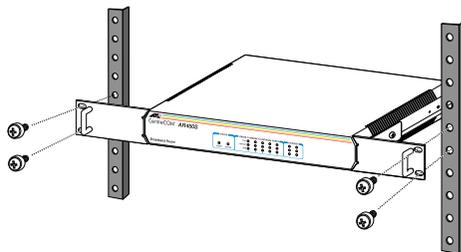


図2.2.2 ラックへの取り付け

2.3 配線する



稲妻が発生しているときは、本製品の設置や、ケーブルの配線などの作業を行わないでください。落雷により感電する恐れがあります。

準備

- 以下の手順は、回線からONUまでの工事（配線）が完了しているものとして説明します。
- 本製品に接続するコンピューターでTCP/IPプロトコルが使用できるように設定しておきます。
 本書「A.1 コンピューターの設定」(p.141)
- ストレートタイプのカテゴリー5のUTPケーブルを必要な本数だけご用意ください。^{*1}



^{*1} 10BASE-Tによる通信の場合は、カテゴリー3以上のUTPケーブルが使用可能ですが、カテゴリーの違いは外観では区別が付きにくく、不慮のトラブルをさけるためにもカテゴリー5で統一することをお勧めします。

1 ONU /メディアコンバータを接続する

- 1 ケーブル先端の爪部分を下側に持ち、ETHERNET0 ポートに挿入して、カチッと音がするまで、差し込んでください。

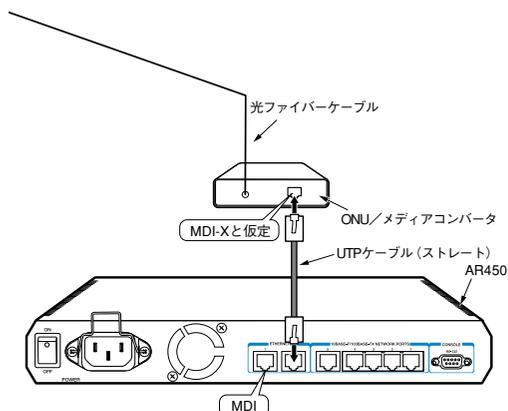


図 2.3.1 ONU/メディアコンバータの接続

- 2 UTP ケーブルのもう一端を、ONU /メディアコンバータに接続してください。

2 コンピューターを接続する

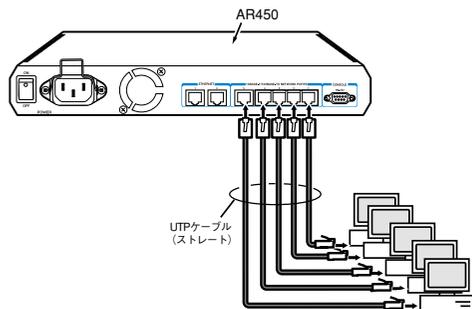


図 2.3.2 コンピューターの接続

- 1 UTP ケーブルの一端を本製品背面の 10BASE-T/100BASE-TX ポートに接続します。UTP ケーブル先端の爪部分を下側に持ち、カチッと音がするまで、しっかりと挿入してください。
- 2 手順 1 と同様にして、UTP ケーブルのもう一端を、コンピューターのネットワークポートに接続します。

- 3 手順 1、手順 2 を繰り返し、接続するコンピューターのすべてを本製品に接続してください。

3 コンソールターミナルを接続する*2

本製品の設定を行うためのコンソールターミナル（コンピューター）を接続します。コンソールターミナルは、「2 コンピューターを接続する」(p.25) のコンピューターを転用するのが便利です。

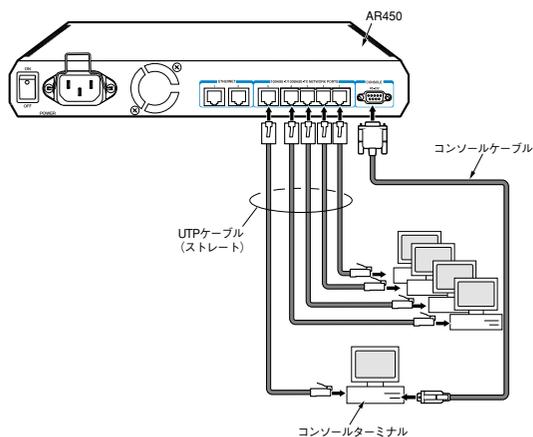


図 2.3.3 コンソールターミナルの接続

- 1 付属のコンソールケーブルのオス側を、本製品背面の CONSOLE ポートに接続し、ケーブルのネジを止めてください。
- 2 付属のコンソールケーブルのメス側を、コンソールターミナルの COM ポートに接続し、ケーブルのネジを止めてください。COM ポートは機種により、「SERIAL」、「|○|○|」などと表記されています。

4 電源ケーブル抜け防止フックを取り付ける

付属の電源ケーブル抜け防止フックを、下図のように取り付けてください。



*2 本製品の設定を終え、コンピューターとの通信ができるようになれば、Telnet による設定が可能となります。

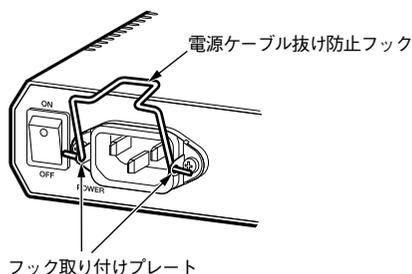


図 2.3.4 電源ケーブル抜け防止フックの取り付け

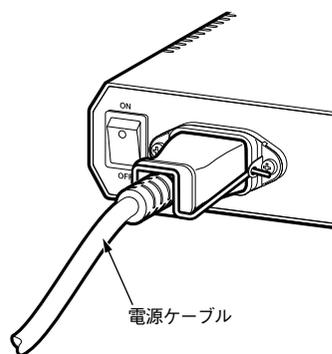


図 2.3.6 電源ケーブルのロック

5 電源ケーブルの接続

- 1 付属の電源ケーブルを本製品背面の電源コネクタに接続してください。

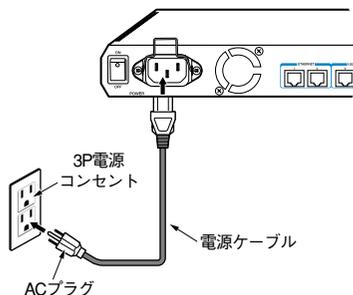


図 2.3.5 電源ケーブルの接続

- 2 電源ケーブルのプラグを電源コンセントに接続してください。電源プラグは3ピンになっています。接地付きの3ピンコンセントに接続してください。
- 3 電源ケーブル抜け防止フックで、電源ケーブルが抜け落ちないようにロックしてください。

2.4 HUB を接続する

本製品には、5 台までのコンピューターを接続できますが、更に多くのコンピューターを接続したい場合は、HUB やスイッチをカスケード接続することができます。

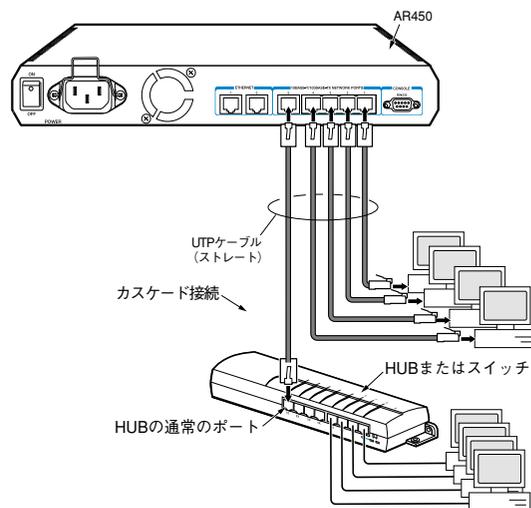


図 2.4.1 HUB の接続

- 1 UTP ケーブルの一端を、本製品背面の 10BASE-T/100BASE-TX ポートに接続します（上図ではポート5に接続しています）。UTP ケーブル先端の爪部分を下側に持ち、カチッと音がするまで、しっかりと挿入してください。
- 2 同様に、UTP ケーブルのもう一端を、HUB またはスイッチの通常のポートに接続します。

3 起動・設定の保存・再起動

本製品の起動や停止、ログインやログアウト、本製品に施した設定の保存など、本製品を運用管理するための基本的な操作について説明します。はじめて本製品をご使用になるお客様は、この章の各節を順にお読みになることにより、本製品の運用上の特徴的な部分を理解することができます。

3.1 コンソールターミナルの設定

本製品に対する設定や管理は、背面の CONSOLE ポートに接続したコンソールターミナル、または Telnet^{*1} を使用して行います。コンソールターミナルとして、下記を使用できます。

- Windows 95/98/Me/2000/XP、Windows NT に付属のハイパーターミナル
- Windows 95/98/Me/2000/XP、Windows NT で動作する VT100 をサポートした通信ソフトウェア
- 非同期のRS-232 インターフェースを持つ VT100 端末装置

通信ソフトウェアに設定するパラメーターは、下記の通りです。エミュレーション、「BackSpace」キーのコードは「EDIT」コマンドのための設定です。文字セットは、「HELP」コマンド（日本語オンラインヘルプ）のための設定です。

表3.1.1 コンソールターミナルの設定

項目	値
インターフェース速度	9,600bps
データビット	8
パリティ	なし
ストップビット	1
フロー制御	ハードウェア (RTS/CTS)
エミュレーション	VT100
BackSpace キーのコード	Delete
文字セット	SJIS

コンソールターミナルとして、ハイパーターミナルを使用するための設定手順は下記をご覧ください。

 本書「A.2 ハイパーターミナルの設定」(p.143)

 *1 Telnet を使って設定を行う場合、あらかじめコンソールターミナルで本製品に IP アドレスなどを割り当てておかなければなりません。Telnet は、本書「? Telnet を使う」(p.59) で説明しています。

3.2 起動

- 1 コンピューターの電源をオンにし、ハイパーターミナル（通信ソフトウェア）を起動してください。本書「3.1 コンソールターミナルの設定」(p.27) から引き続き実行している場合、そのままの手順にお進みください。
- 2 本製品の電源スイッチをオンにしてください。
- 3 自己診断テストが実行され、ファームウェアがロードされます。また、起動スクリプトが指定されていれば、実行します。

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 65536k bytes found.
INFO: Self tests complete.
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download successful.
INFO: Router startup complete

login:
```

図 3.2.1 ご購入時における起動メッセージ

- 4 login: と表示されたら、次の「3.3 ログイン（ご購入時）」にお進みください。

トラブルシューティング

うまくいかない場合は、下記をご確認ください。

「login:」と表示されない

- リターンキーを数回押してみる。
- 本製品の電源ケーブルが正しく接続されているか確認する。
- コンソールケーブルが正しく接続されているか確認する。

文字化けする

- ハイパーターミナル（通信ソフトウェア）の通信速度が9,600bps に設定されているか確認する。
- 別のフォントを選択してみる。

それでもうまくいかないときは、一旦本製品の電源スイッチをオフにし、3～5 秒待ってから、電源スイッチをオンにしてみます。まだうまくいかない場合には、ハイパーターミナルを一旦終了し、再起動してみます。また、Windows を再起動してみます。

3.3 ログイン (ご購入時)

設定や管理を行うためには、本製品にログインしなければなりません。ご購入時の状態では、Manager (管理者) レベルのユーザー「manager」のみが登録されています。初期パスワードは「friend」です。初期導入時の設定作業をはじめ、ほとんどの管理、設定作業は、ユーザー「manager」で行います。

表3.3.1 ご購入時のユーザー名とパスワード

ユーザー名	manager
パスワード	friend

- 1 login プロンプトが表示されたら、下記のように入力します。

```
login: manager ↵
```

- 2 Password プロンプトが表示されたら、下記のように入力します。実際の画面では入力したパスワードは表示されません。

```
Password: friend ↵ (表示されません)
```

- 3 コマンドプロンプト「Manager >」が表示されます。本製品に対する設定や管理は、このプロンプトに対してコマンドの文字列を入力することにより行います。

```
Manager >
```

 本書「4.1 コマンドプロセッサ」(p.35)

3.4 パスワードの変更

- 1 下記のように入力します。

```
Manager > SET PASSWORD ↵
```

- 2 現在のパスワードを入力します。ご購入時では初期パスワード「friend」なので、下記のように入力します。ここでは説明のためパスワードを記載しますが、実際の画面では入力したパスワードは表示されません。

```
Old password: friend ↵ (表示されません)
```

- 3 変更後に指定する新しいパスワードを入力します(6文字以上)。ここでは新パスワードを「rivADD」と仮定します。実際の画面では入力したパスワードは表示されません。

```
New password: rivADD ↵ (表示されません)
```

- 4 確認のために、再度新しいパスワードを入力します。ここでは説明のためパスワードを記載しますが、実際の画面では入力したパスワードは表示されません。Confirmを入力後、コマンドプロンプトが現れない場合、再度リターンキーを押してください。

```
Confirm: rivADD ↵ (表示されません)
```

```
Manager >
```

手順3と4で入力した「新しいパスワード」が同じものであれば、本製品はパスワードの変更を受け入れます。異なっている場合、次のメッセージが表示されますので、再度「SET PASSWORD」コマンドを実行してください。

```
Error (3045287): SET PASSWORD, confirm password incorrect.
```

```
Manager >
```

パスワードの変更が成功した場合、ユーザー「manager」の次からのパスワードは下記ようになります。

表3.4.1 次回のパスワード (本ページの例)

ユーザー名	manager
パスワード	rivADD



絶対にパスワードを忘れないでください。忘れてしまった場合、パスワードを初期状態に戻すためには、弊社持ち帰り修理を行うこととなります。弊社サポートセンターにご相談ください。



ユーザー「manager」のパスワードは、必ず変更してください。初期パスワードのままに運用した場合、重大なセキュリティホールとなります。

- 5 次の「3.7 設定の保存」(p.30) を実行してください。

ユーザー名、パスワードに使用可能な文字、ユーザーレベルなどの詳しい説明は、下記をご覧ください。



本書「5 ユーザー管理とセキュリティ」(p.51)

3.5 システム名の変更

システム名 (MIB II オブジェクト sysName) を設定すると、プロンプトにシステム名が表示されるようになります。複数のシステムを管理しているときは、各システムに異なる名前を設定しておく、どのシステムにログインしているのかがわかりやすくなり便利です。

- 1 下記のコマンドを実行します。下記では、システム名を「OSAKA」に設定しています。

```
Manager > SET SYSTEM NAME="OSAKA" ↓
```

- 2 プロンプトが「Manager OSAKA>」に変わります。

```
Info (1034003): Operation successful.  
Manager OSAKA>
```

また、login プロンプトにもシステム名が表示されるようになります。

```
OSAKA login:
```

- 3 次の「3.7 設定の保存」を実行してください。

3.6 システム時間の設定

本製品に内蔵の時計 (リアルタイムクロック) を現在の時間に合わせます。

- 1 現在の日時を入力します。例では、2002年4月11日の16時6分に合わせています。

```
Manager > SET TIME=16:06:00 DATE=11-APR-2002 ↓
```

- 2 下記のようなメッセージが表示されれば、時計合わせは完了です。

```
System time is 16:06:00 on Thursday 11-Apr-2002.
```

本製品の現在時刻は、「SHOW TIME」で確認することができます。

```
Manager > SHOW TIME ↓  
System time is 16:08:02 on Thursday 11-Apr-2002.
```

「SET TIME」コマンドは、電池によってバックアップされたリアルタイムクロックに対して実行され、効果は電源スイッチのオフ後も続きます。そのため「CREATE CONFIG」コマンドで作成される設定スクリプトに反映されません。

NTP プロトコルによって、NTP サーバーと時間を同期することもできます。詳しくは、下記をご覧ください。

 コマンドリファレンス「運用・管理」の「NTP」

3.7 設定の保存

入力したコマンドはただちに実行されますが、コマンドによって設定された内容はランタイムメモリー上にあるため、本製品の電源スイッチのオフや、再起動コマンドの実行で消失してしまいます。

現在の設定を、例えば先ほどのパスワードやシステム名を、次回の起動時に再現するために、設定スクリプトファイルを作成し、フラッシュメモリーに保存しておきます。

「CREATE CONFIG」コマンドは、ランタイムメモリー上に存在する現在の設定内容から、「その設定内容を作り出すために入力しなければならない一連のコマンド」(スクリプトファイル)を作成し、フラッシュメモリーに保存します。

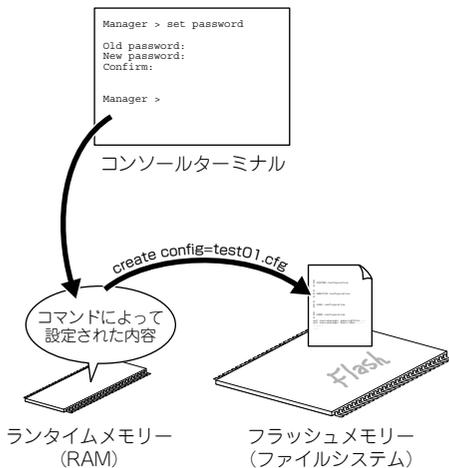


図3.7.1 スクリプトの作成と保存

- 1 プロンプトに対して、「CREATE CONFIG=filename.CFG」コマンドを入力します。この例では、設定スクリプトのファイル名を「test01.cfg」と仮定しています。

```
Manager > CREATE CONFIG=test01.cfg
```

設定スクリプトのファイル名には、通常「.cfg」という拡張子をつけます。ファイル名部分として、8文字以内の英数半角文字とハイフン「-」が使用できます。同じ名のファイルが既に存在する場合、上書きされます。存在しない場合は、新規に作成されます。

- 2 ファイルが正しく作成されたことを確認してみましょう。「SHOW FILE」コマンドで、ファイル名がリスト表示されます

(ファイルサイズと日付は一例です)。

```
Manager > SHOW FILE
```

Filename	Device	Size	Created	Locks
54-252.rez	flash	2333496	30-Apr-2003 21:29:01	0
ac100af0.dhc	flash	80	04-Apr-2003 15:11:56	0
ac1014f0.dhc	flash	80	04-Apr-2003 15:20:39	0
config.ins	flash	32	11-Apr-2003 20:46:20	0
feature.lic	flash	39	18-Feb-2003 15:38:26	0
help.hlp	flash	129254	30-Apr-2003 18:29:01	0
prefer.ins	flash	64	02-Apr-2003 15:40:40	0
release.lic	flash	32	18-Dec-2002 12:48:06	0
test01.cfg	flash	2290	11-Apr-2003 17:51:31	0

設定スクリプトは、テキストファイルです。「SHOW FILE」コマンドでファイル名を指定すると、内容を見ることができます。

```
Manager > SHOW FILE=test01.cfg
```

File : test01.cfg

```
1:
2:#
3:# SYSTEM configuration
4:#
5:
6:#
7:# SERVICE configuration
8:#
9:
10:#
11:# LOAD configuration
12:#
13:
14:#
15:# USER configuration
16:#
17:set user=manager pass=7c5ff696c5e944eb6f2a0d70a0a74354e2 priv=manager lo=yes
18:set user=manager desc="Manager Account" telnet=yes
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

「スペース」バーを押すと画面がスクロールします。「Q」キーを押すと表示を終了します。

既存の起動スクリプトで動作している本製品に対して、設定を追加したときには、手順 1 の「CREATE CONFIG」で既存の起動スクリプト名を指定します。例えば、今作った test01.cfg に、後で IP 情報などを追加した場合には、「create config=test01.cfg」で上書き保存します。

ファイル名に使用可能な文字、ファイルシステムなどの詳しい説明は、下記をご覧ください。

参照 本書「9 ファイルシステム」(p.63)

コマンドリファレンス「運用・管理」の「記憶装置とファイルシステム」

3.8 起動スクリプトの指定

本製品が起動するとき、作成した設定スクリプトが実行されるように設定します。起動時に実行される設定スクリプトのことを、「起動スクリプト」と呼びます。

- 1 「SET CONFIG=*filename.CFG*」コマンドで起動スクリプトを指定します。この例では、ファイル名を「test01.cfg」と仮定しています。

```
Manager > SET CONFIG=test01.cfg ↓
```

- 2 これで起動スクリプトを指定できました。現在指定されている起動スクリプトは、「SHOW CONFIG」コマンドで確認できます。

```
Manager > SHOW CONFIG ↓
```

```
Boot configuration file: test01.cfg (exists)
Current configuration: None
```

「Boot configuration file:」は現在指定されている起動スクリプトファイル、「Current configuration:」は起動したとき実行したスクリプトファイルです。上記の例で「Current configuration: None」となっているのは、起動スクリプトとして「test01.cfg」は指定されているが、指定直後であり、再起動されていないことを示しています。

3.9 再起動

本製品を再起動する方法は、次の3つがあります。

- RESTART ROUTER コマンドの入力
- RESTART REBOOT コマンドの入力
- 電源スイッチのオフ / オン

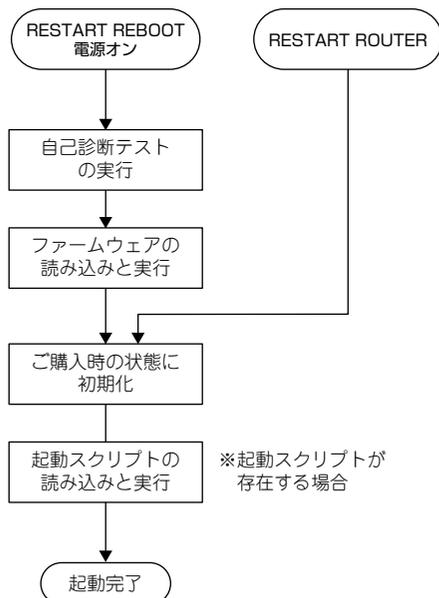


図 3.9.1 ブートシーケンス

RESTART ROUTER コマンドの入力

ソフトウェア的なりセットを行います（ウォームスタート）。起動スクリプトだけを読み直して設定を初期化します（起動スクリプトは「SET CONFIG」コマンドで指定します）。起動スクリプト（*filename.cfg*）だけを変更した場合に、このコマンドを使用します。

- 1 プロンプトが表示された状態で、下記のように入力します。

```
Manager > RESTART ROUTER ↓
```

- 2 login プロンプトが表示されたら、再起動は完了です。下記では、起動メッセージにより「test01.cfg」が読み込まれたことが表示

されています。

```
INFO: Executing configuration script <test01.cfg>
INFO: Router startup complete

login:
```

RESTART REBOOT コマンドの入力

次の「電源のオフ / オン」と同じ動作を行うコマンドです（**コールドスタート**）。ハードウェア的にリセットされ、自己診断テストの実行、ファームウェアをロードした後、起動スクリプトを読み込み、起動スクリプトの内容による動作を開始します。本製品のファームウェアをバージョンアップした場合は、この操作を実行しなければなりません。

- 1 プロンプトが表示された状態で、下記のように入力します。

```
Manager > RESTART REBOOT ↓
```

- 2 login プロンプトが表示されたら、再起動は完了です。下記では、起動メッセージにより「test01.cfg」が読み込まれたことが表示されています。

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 65536k bytes found.
INFO: Self tests complete.
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download successful.
INFO: Executing configuration script <test01.cfg>
INFO: Router startup complete

login:
```

電源のオフ / オン

本製品の電源スイッチをオフにした後、オンにします。ハードウェア的にリセットされ、自己診断テストの実行、ファームウェアをロードした後、起動スクリプトを読み込み、起動スクリプトの内容による動作を開始します。本製品のファームウェアをバージョンアップした場合は、この操作を実行しなければなりません。

- 1 本製品の電源スイッチをオフにします。
- 2 3～5 秒待ってから、電源スイッチをオンにします。
- 3 login プロンプトが表示されたら、再起動は完了です。

再起動時のご注意

PPPoE によってプロバイダーと接続している場合、本製品の再起動は、PPPoE の接続が確立していない状態で行なってください。接続が確立したままで再起動してしまうと、PPPoE の接続相手の装置で矛盾が生じてしまうため、プロバイダーによっては本製品の起動後、しばらくの間再接続ができなくなることがあります。

- 1 「DISABLE PPP」コマンドによって、接続を正しく切断します。詳しくは、下記をご覧ください。



本書「PPPoE セッションの手動による切断」(p.136)

- 2 電源スイッチのオフや、「RESTART」コマンドを実行してください。

3.10 ログアウト

本製品の設定が終了したら、本製品からログアウトして通信ソフトウェアを終了します。

- 1 次のプロンプトが表示された状態で、下記のように入力します。

```
Manager > LOGOFF ↓
```

- 2 これでログアウトが完了です。ログアウトコマンドは、「LOGOFF」の代わりに「LOGOUT」や「LO」でも可能です。



通信ソフトウェア（コンソールターミナル）を終了する前に、必ずログアウトしてください。ログアウトせず通信ソフトウェアを終了すると、コンソールターミナルを使用できる誰でも Manager レベル権限を得ることができます。セキュリティのために、必ずログアウトしてください。

3.11 停止

本製品は、下記の方法で停止します。

- 1 本製品にログインしている場合は、ログアウトしてください。
- 2 本製品の電源スイッチをオフにします。
- 3 これで本製品は停止しました。

3.12 ご購入時の状態に戻す

ご購入時の状態、すなわち本製品に対して設定がまったく施されていない状態に戻す手順を説明します。

- 1 Manager レベルでログインしてください。

```
login: manager 』  
Password:
```

- 2 「SET CONFIG=NONE」コマンドにより、起動時に設定スクリプトが読み込まれないようにします。詳細は、本書「3.8 起動スクリプトの指定」(p.31)をご覧ください。

```
Manager > SET CONFIG=NONE 』
```

- 3 「RESTART ROUTER」コマンドを実行してください。本製品は、起動スクリプトを読み込まない状態で初期化され、初期化のためにログアウトしてしまいます。ソフトウェア的にはご購入時の状態となりますが、まだお客様が保存した設定スクリプトは削除されていません。

```
Manager > RESTART ROUTER 』  
  
login:
```

「RESTART REBOOT」の実行や、電源スイッチのオフ/オンによる再起動を行ってもかまいません。

- 4 Manager レベルでログインしなおします (パスワードはデフォルトに戻っています)。

```
login: manager 』  
Password: friend 』 (表示されません)
```

- 5 設定スクリプトのすべてを削除すると、完全にご購入時の状態となります。ファイル名をひとつひとつ指定してもかまいませんが、ワイルドカード「*」を使用するのが便利です。

```
Manager > DELETE FILE=* .cfg 』
```



設定スクリプト (.CFG) を削除してしまうと、お客様が保存した設定は完全に失われます。

3.13 ロックアウトされてしまったとき

コンソールターミナルまたは Telnet によって本製品にログインするとき、同じユーザー名でパスワードを連続して5回間違えると、下記のメッセージが表示され、しばらくの間ログインできなくなります。

```
login: manager 』  
Password:  
  
Info. This device is locked out temporarily  
(login-lockout).
```

10分(デフォルト)が経過するとロックアウトは解除され、再びログインできるようになります(電源のオフ/オンを実行すれば、即時にロックアウトは解除されます)。

本製品に登録されているユーザーアカウントに対するアクセスは、「SHOW USER」コマンドによって表示することができます。下記では、「manager」によるアクセスのうち2回はログインに成功、5回失敗しています。

```
Manager > SHOW USER 』  
  
User Authentication Database  
-----  
Username: manager (Manager Account)  
Status: enabled Privilege: manager Telnet: yes  
Logins: 2 Fails: 5 Sent: 0 Rcvd: 0  
-----  
  
Active (logged in) Users  
-----  


| User    | Port/Device | Location | Login Time           |
|---------|-------------|----------|----------------------|
| manager | Asyn 0      | local    | 17:46:54 26-Feb-2001 |


```

3.14 設定情報の表示

よく使用する「SHOW」コマンドを示します。画面が広いスクリーンをご使用の場合、例えば66行に設定された通信ソフトウェアをお使いの場合、「SET ASYN=asyn0 PAGE=66」を実行しておくこと、最下行で「--MORE--」が表示されるようになります。

「SHOW SYSTEM」コマンドは、システムの全般的な情報を表示します。

```
Manager OSAKA> SHOW SYSTEM 』

Router System Status           Time 17:12:54 Date 04-May-2003.
Board   ID Bay Board Name      Rev   Serial number
-----
Base    195  AR450             M1-0  57004257
-----
Memory -  DRAM : 65536 kB   FLASH : 16384 kB
-----
SysDescription
CentreCOM AR450  version 2.5.2-00 27-Apr-2003
SysContact

SysLocation

SysName
OSAKA
SysDistName

SysUpTime
49540 ( 00:08:15 )
Boot Image      : 450_105.FBR size 872376 16-Apr-2003
Software Version: 2.5.2-00 27-Apr-2003
Release Version : 2.5.2-00 27-Apr-2003
Patch Installed : NONE
Territory       : japan
Help File       : help.hlp

Configuration
Boot configuration file: TEST01.cfg (exists)
Current configuration: test01.cfg

Security Mode   : Disabled

Warning (2048284): No patches found.

Manager OSAKA>
```

「SHOW CONFIG」コマンドは、現在指定されている起動スクリプトのファイル名を表示します。

```
Manager OSAKA> SHOW CONFIG 』

Boot configuration file: TEST01.CFG (exists)
Current configuration: TEST01.CFG
```

「SHOW FILE」コマンドは、ファイルをリスト表示します。

「SHOW FILE=*filename*.CFG」のようにファイル名を指定すると、ファイルの内容を表示します。

 本書「3.7 設定の保存」(p.30)

「SHOW CONFIG DYNAMIC」コマンドは、ランタイムメモリ（RAM）上の設定内容を表示します。設定をスクリプトファイルとして保存する前に、このコマンドで確認するのが便利です。

```
Manager OSAKA> SHOW CONFIG DYNAMIC 』

#
# SYSTEM configuration
#
set system name="OSAKA"

#
# SERVICE configuration
#

#
# LOAD configuration
#

#
# USER configuration
#
set user=manager pass=3af5001f767b64cadiceb3eff0c6ab5d4 priv=manager lo=yes
set user=manager desc="Manager Account" telnet=yes

#
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

「SHOW CONFIG DYNAMIC=*module-id*」のように機能モジュール名を指定すると、その部分だけが表示されます。機能は、SYSTEM、IP、PPP、DHCP、INT、SNMP、TELNET、USERなどが指定できます。

```
Manager OSAKA> SHOW CONFIG DYNAMIC=SYSTEM 』

#
# SYSTEM configuration
#
set system name="OSAKA"

#
# SERVICE configuration
#
```

4 設定のための基礎知識

コンソールターミナルまたは Telnet 経由で本製品にログインすることによって、本製品に対する設定を施すことができます。本章では、設定を施すためのコマンド入力に関する基本的操作方法、コマンドの分類、ソフトウェア的な内部構造、インターフェース名について説明します。

4.1 コマンドプロセッサ

コマンドプロセッサは、文字ベースの対話型ユーザーインターフェースです。

ユーザーが本製品にログインすると、コマンドプロセッサはコマンドの入力を促すためにコマンドプロンプトを表示します。コマンドプロンプトは、ログインしているユーザーの権限レベルと、システム名が設定されているか否かによって、次のように変化します。

表 4.1.1

権限レベル	システム名設定なし	システム名設定あり ^a
User	>	OSAKA>
Manager	Manager >	Manager OSAKA>
Security Officer	SecOff >	SecOff OSAKA>

a. システム名「OSAKA」の場合。

 本書「5 ユーザー管理とセキュリティ」(p.51)
本書「3.5 システム名の変更」(p.29)

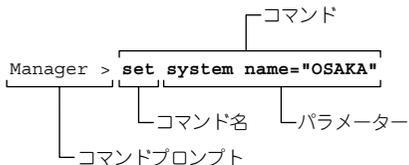


図 4.1.1 コマンドの構成

コマンドプロンプトに対してコマンドを入力すると、コマンドプロセッサは、コマンドを解析し実行します。コマンドは、コマンド名(行頭のキーワード)とパラメーター(先頭のキーワードに従属するキーワード)から構成され、スペースで区切って羅列します。

パラメーターは、上図の「SYSTEM」のように値を持たないものと、「NAME="OSAKA"」のように値(PARAMETER=value)を持つものがあります。

パラメーターが連続する場合、先行して入力したパラメーターによって、後続のパラメーターが限定されることがあります。

 本書「次に選択可能なキーワードを表示する「?」」(p.36)

コマンドを入力し、実行に成功すると、「... successful」というメッセージが表示されます。

```
Manager > SET SYSTEM NAME="OSAKA" ↵
Info (1034003): Operation successful.
```

図 4.1.2 成功メッセージ例

入力ミスなどにより、コマンドの実行に失敗すると、「Error」で始まるメッセージが表示されます。

```
Manager > SEG SYSTEM NAME="OSAKA" ↵
Error (335256): Unknown command "seg".
```

図 4.1.3 失敗メッセージ例

コマンド入力の注意点

コマンド入力における注意点をまとめます。

- 1行で入力できるコマンドの文字数は、スペースを含み121文字以下です^{*1}。1行が122文字以上になる場合には、コマンド名やパラメーターの省略形を使用したり、ADDとSETまたはCREATEとSETの組み合わせを使って、コマンドを分割します。

 本書「コマンドの分割入力」(p.36)

- コマンド名やパラメーターは、省略形が使用可能です。例えば、「SHOW PORT」は「SH PO」、「HELP SHOW PORT」は「H SH PO」のように省略できます。

 本書「次に選択可能なキーワードを表示する「?」」(p.36)

- コマンド名やパラメーターは、大文字、小文字を区別しませんが、値として文字列が与えられている場合、値は大文字、小文字を区別することがあります(例えば、パスワード、システム名など)。

- ログインユーザーの権限によって、実行できるコマンド名が異なります。通常の管理作業は、Managerレベルで行います。セキュリティモードでは、Security Officerレベルの権限が必要です。

 本書「5 ユーザー管理とセキュリティ」(p.51)

- コマンドの効果は、コマンドを入力するとただちに現れます(エラーがなければ)。再起動などを行う必要はありません。ただし、本製品を再起動すると設定内容は消失してしまうので、設



*1 システム名が設定されている場合 (SET SYSTEM NAME)、入力可能な文字数は、システム名の文字数だけ短くなります。

定をスクリプトとして保存し、起動時に読み込まれるように設定しておかなければなりません。

 本書「3.7 設定の保存」(p.30)

本書「3.8 起動スクリプトの指定」(p.31)

キー操作 (ヒストリー機能)

コマンドプロンプトに対してカーソルが表示されている行、すなわちコマンドを入力しようとしている行のことをコマンドラインと言います。コマンドラインでは、次のような編集機能を使用できます。下記の表において、「Ctrl/ □」は Ctrl キーを押しながら、「/」の後のキーを押すことを意味します。

表 4.1.2 コマンドラインにおける編集キー

機能	VT 端末のキー
コマンドライン内のカーソル移動	←、→
カーソル左の 1 文字削除	Delete、Backspace
挿入モード、上書きモードの切り替え	Ctrl/O
コマンドラインの消去	Ctrl/U
入力したコマンドの履歴をさかのぼる	↑、Ctrl/B
入力したコマンドの履歴を進める	↓、Ctrl/F
入力したコマンドの履歴のすべてを表示する	Ctrl/C 「SHOW ASYN HISTORY」の <input type="text"/>
コマンドの履歴のすべてを消去する	「RESET ASYN HISTORY」の <input type="text"/>
最後に入力した <i>string</i> で始まるコマンドを表示する	<i>string</i> + タブ (Ctrl/I)

次に選択可能なキーワードを表示する「？」

「？」は特別な意味を持つキーです。コマンドの入力途中で押すと、次に選択可能なキーワード(コマンド名、パラメーター)のリストを表示します。

コマンドプロンプトに対して、「？」キーを押してみてください。コマンドのトップレベルで使用可能なキーワード(コマンド名)が表示され、再びコマンドプロンプトが表示されます。

```
Manager > ? (?は表示されません)
```

```
Options : ACTivate ADD Connect CLear CREate DEACTivate DELete DESTroy  
DISable Disconnect DUMP Edit ENable FINGER FLUsh Help LOAD MAIL MODify  
PING PURge RENAME Reconnect RESET RESTART SET SHOW SSH START Stop TELnet  
TRAce UPLoad LOGIN LOGON LOfgoff LOfgout
```

```
Manager >
```

表示されるキーワードのリストで、大文字の部分は**省略形**で、キーワードとして一意に識別するために最低限入力しなければなりません。

「SHOW」+「半角スペース」を入力して、「？」キーを押すと、SHOW に続く選択可能なキーワードが表示され、プロンプトには「？」キーを押す寸前のコマンド (SHOW + 半角スペース) が再表示されます。「？」キーを押すとき、コマンドラインに何らかの文字列を入力している場合、文字列の後ろに半角スペースを入力し、「？」と区切らなければなりません。

```
Manager > SHOW ? (?は表示されません)
```

```
Options : ACC ALias APPLetalk BGP BOOTp BRIDge BRI BUFFER CLNS CONFig  
CPU DEcNet DEBug DHCP DTe DTESt1 DVMrp ENCo ETH EXception File FEature  
FIREwall FFile Flash FRamereley GRE GUI HTTP INSTall INTerface IP IPV6  
IPSec IPX ISAkmp ISDN L2TP LAPB LAPD LDAP LDecker LOG LPD MAnager MAIL  
MIOX NTP NVS OSFP PATCH PERM PIM PING PKT ASYN POrt PKI PPP PRI Q931  
RADIUS RELease RSPV SA SScript SERVICE SNImp SSH STAR STARTUp STReam STT  
SWitch SYN SYStem TELnet TPAD TRAce TRIGger SESSions TCP TEST Time TTY  
TAcacs USEr VLAN VRRP X25C X25T TDM
```

```
Manager > SHOW
```

更に、選択可能なキーワードを掘り下げていく場合、例えば上記の例で「PPP」を指定する場合、続けて「PPP」+「半角スペース」を入力し、「？」キーを押します。

```
Manager > SHOW PPP ? (?は表示されません)
```

```
Options : COUnter CONFig MULTILink IDLEtimer NAMEServers DEBUg TXStatus  
TEMPlate LIMits PPPOE
```

```
Manager > SHOW PPP
```

コマンドの分割入力

CREATE、ADD で始まる長いコマンドは、CREATE と SET、ADD と SET の組み合わせを使って分割することができます。例えば、CREATE で始まる下記の長いコマンドは、

```
Manager > CREATE PPP=0 OVER=eth0-any  
BAP=OFF IPREQUEST=ON  
USER="site_a@example.co.jp"  
PASSWORD="jK5H&2p"  
LQR=OFF ECHO=ON IDLE=ON ↵
```

図 4.1.4 CREATE で始まる長いコマンド

次のように、CREATE と SET で始まる行に分割して入力することができます。この場合、「SET」コマンドでは先行して入力した「CREATE」コマンドのパラメーターを指定しなければなりません(下記では「ppp=0」や「over=eth0-any」)。

```

Manager > CREATE PPP=0 OVER=eth0-any
      BAP=OFF IPREQUEST=ON ↓

Manager > SET PPP=0
      USER="site_a@example.co.jp"
      PASSWORD="jk5H&2p" ↓

Manager > SET PPP=0 OVER=eth0-any
      LQR=OFF ECHO=ON IDLE=ON ↓

```

図 4.1.5 CREATE、SET で分割

コマンドを分割して入力する際の各パラメータの指定等の詳細については、添付 CD-ROM 内の「コマンドリファレンス」にて参照できます。

IP フィルターコマンドの分割入力

コマンドが長くなりがちな IP フィルターコマンドについて、補足説明します。下記は、「ADD IP FILTER」コマンドがパラメーターとして取るおもなキーワードの省略形です。

ACTION: AC	DESTINATION: DES
DMASK: DM	DPORT: DP
ENTRY: ENT	EXCLUDE: EXCL
FILTER: FIL	INCLUDE: INCL
PROTOCOL: PROT	SESSION: SESS
SOURCE: SO	SMASK: SM
SPORT: SP	

また、SPORT、DPORT パラメーターには TELNET のようなプロトコル名を指定せずに、23 のようにポート番号を指定するとコマンド長が短縮できます。



コマンドリファレンス「IP」-「付録」-「おもな Well-known ポート」

下記の長いコマンドを入力しようとする、

```

ADD IP FILTER=1 SOURCE=192.168.20.4
SMASK=255.255.255.255
DESTINATION=192.168.10.2
DMASK=255.255.255.255 DPORT=TELNET
PROTOCOL=TCP SESSION=ANY
ACTION=INCLUDE

```

図 4.1.6 長すぎるコマンド

次のようにコマンドの途中までしか入力できませんが、

```

Manager > ADD IP FILTER=1 SOURCE=192.168.20.4
SMASK=255.255.255.255
DESTINATION=192.168.10.2
DMASK=255.255.255.255 DPORT=TELNET
PRO

```

図 4.1.7 途中でしか入力できない

コマンドの省略形を使用することにより入力可能となります。

```

Manager > ADD IP FILT=1 SO=192.168.20.4
SM=255.255.255.255 DES=192.168.10.2
DM=255.255.255.255 DP=23
PROT=TCP SESS=ANY AC=INCL ↓

```

図 4.1.8 省略形により入力できる

また、下記もコマンドが 122 文字以上のため入力できませんが、

```

ADD IP FILTER=1 SOURCE=192.168.20.4
SMASK=255.255.255.255
DESTINATION=192.168.10.2
DMASK=255.255.255.255 ACTION=INCLUDE
ENTRY=1 DPORT=TELNET PROTOCOL=TCP
SESSION=ANY

```

図 4.1.9 長すぎるコマンド

ADD と SET の組み合わせを使い、コマンドを分割することにより入力可能となります。「SET」コマンドでフィルター内容を追加する場合、必ず ENTRY パラメーターを指定してください。ENTRY はフィルタールール番号で、「SHOW IP FILTER」コマンドで確認できます。

```

Manager > ADD IP FILTER=1 SOURCE=192.168.20.4
SMASK=255.255.255.255
DESTINATION=192.168.10.2
DMASK=255.255.255.255 ACTION=INCLUDE ↓

```

```

Manager > SHOW IP FILTER ↓

```

```

IP Filters
-----
No. Ent. Source Port  Source Address  Source Mask  Session  Size
  Dest. Port  Dest. Address  Dest. Mask  Prot. (T/C)  Options
   Type      Act/Pol/Pri   Logging
-----
1   1   ---      192.168.20.4   255.255.255.255  ---      Any
   ---      192.168.10.2   255.255.255.255  Any      Any
   General  Include      Off
-----
Requests: 0          Passes: 0          Fails: 0
-----

```

```

Manager > SET IP FILTER=1 ENTRY=1
DPORT=TELNET PROTOCOL=TCP
SESSION=ANY ↓

```

図 4.1.10 分割により入力できる

4.2 コマンドの分類

本製品は、高度な機能を実現するために、多くのコマンド名やパラメーターをサポートしています。コマンドは、おおむね設定コマンドと、実行コマンドに分けることができます（コマンドによっては明確に分類できないものもあります）。

設定コマンド

設定コマンドは、「CREATE CONFIG」コマンドの実行により作成される設定スクリプトファイルの内容として保存されるか、または設定スクリプトファイルが保存されるとき、その内容に対して影響を与えます。^{*2}

設定コマンドの多くは、ランタイムメモリー上に展開されている、本製品の動作を制御するための各種のテーブルの内容を変更します。例えば、「ADD IP ROUTE」コマンドは、ルーティングテーブルを変更し、パケットの配送を制御します。また、「PURGE IP」コマンドは IP に関するすべての設定を削除します。

設定コマンドは、内容によってはいくつかの設定コマンドを組み合わせ、はじめて有効となることもあります。代表的な設定コマンドには、以下のようなものがあります。

ACTIVATE DEACTIVATE

「ACTIVATE」は、すでに存在しているものを実際に動作させるコマンドです。「DEACTIVATE」は、「ACTIVATE」コマンドで動作しているものを中止、または停止するコマンドです。例えば、設定済みの接続先に対する発呼や切断、スクリプトの実行や取りやめなどで使用します。

ADD DELETE

「ADD」は、既存のテーブルなどに情報を追加、または登録するコマンドです。「DELETE」は、「ADD」で追加した情報を削除するコマンドです。例えば、インターフェースの追加や削除、ルーティング情報の追加や削除に使用します。

CREATE DESTROY

「CREATE」は、存在していないものを作成するコマンドです^{*3}。「DESTROY」は、「CREATE」で作成したものを削除するコマ

ンドです。例えば、PPP インターフェースの作成や削除を行います。

ENABLE DISABLE

「ENABLE」は、既存のものを有効化するコマンドです。「DISABLE」は、「ENABLE」で有効化したものを無効にするコマンドです。例えば、モジュールやインターフェースなどの有効化、無効化を行います。

PURGE

「PURGE」は、指定した項目を全消去するコマンドです。例えば、「PURGE USER」は、「manager/friend（デフォルト）」以外の、登録したユーザー情報をすべて削除します。

SET

「SET」は、すでに存在するパラメーターの設定、追加、または変更を行うコマンドです。「SET」が取るパラメーターによっては、「ADD」や「CREATE」コマンドの実行後でなければ、実行できないことがあります。

実行コマンド

実行コマンドは、「CREATE CONFIG」コマンドの実行により作成される設定スクリプトファイルの内容として保存されません。

実行コマンドは、ログイン、ログアウト、TELNET、ヘルプの表示、ファイルに対する操作、通信のテストなどのようなコマンドです。

実行コマンドを使用する前に、設定コマンドによってあらかじめ設定しなくてはならないこともあります。代表的な実行コマンドには、以下のようなものがあります。

EDIT

テキストエディターを起動するコマンドです。このコマンドにより、「.cfg」（設定スクリプトファイル）、「.scp」（スクリプトファイル）を直接編集することができます。

 本書「6 テキストエディター」（p.57）

HELP

オンラインヘルプを表示するコマンドです。

 本書「4.3 オンラインヘルプ」（p.39）

LOAD

TFTP サーバーや Zmodem などにより、ファイルを本製品にダウンロードするコマンドです。

 本書「10 アップ / ダウンロード」（p.67）



^{*2} 「SHOW CONFIG DYNAMIC」コマンドに対しても同様です。

^{*3} ある機能に対する設定コマンドが、ADD であるか、それとも CREATE であるかは、本製品における機能の実装に依存しています。

LOGIN

ログインするコマンドです。別のユーザーでログインしなおすときなどに使用します。

LOGOFF、LOGOUT

ログアウトするコマンドです。

 本書「3.10 ログアウト」(p.32)

PING

指定した相手からの応答を確認するコマンドです。

 本書「8.1 Ping」(p.61)

RESET

「RESET」は、設定内容は変更せずに、実行中の動作を中止し、はじめからやり直す(リセットする)コマンドです。

RESTART

本製品を再起動するコマンドです。

 本書「3.9 再起動」(p.31)

SHOW

「SHOW」は、設定内容などの各種の情報を表示するコマンドです。

STOP PING

「PING」を中止するコマンドです。

 本書「8.1 Ping」(p.61)

TELNET

「Telnet」を実行するコマンドです。

 本書「7 Telnet を使う」(p.59)

TRACE

経路のトレースを実行するコマンドです。

 本書「8.2 Trace」(p.61)

UPLOAD

TFTP サーバーや Zmodem などにより、ファイルをサーバーやコンピューターへアップロードするコマンドです。

 本書「10 アップ / ダウンロード」(p.67)

4.3 オンラインヘルプ

本製品は、オンラインヘルプを搭載しています。コマンドの概要や、コマンドが取り得るパラメーターとその範囲を知りたいときにご利用ください。オンラインヘルプは、ログイン後のプロンプトに対して使用できます。Manager レベル、User レベルでは表示されるヘルプの内容が異なります。

プロンプトに対して、「HELP」を入力すると、ヘルプのトップ画面が表示されます。

表示画面が1画面(24行)におさまらない場合、「--MORE--」プロンプトが表示されます。「--MORE--」に対する操作キーは次の通りです。

- 「スペース」バーで、次の1ページを表示します。
- 「リターン」キーで、次の1行を表示します。
- 「C」キーで、該当項目の残りすべてを表示します。
- 「Q」キーで、表示を中止します。

```
Manager > HELP ↵

AR450 オンラインヘルプ - V2.5 Rev.01 2003/05/06

This online help is written in Japanese (Shift-JIS).

ヘルプは次のトピックを説明しています。
入力は大文字の部分だけでかまいません (*HELP OPERATION* は *H O* と省略可)。

Help Operation      運用・管理 (SNMP、ログ、トリガー、スクリプトなど)
Help Interface      インターフェース (スイッチ、ETH など)
Help Ppp            PPP
Help Bridge         ブリッジング
Help IP             IP (RIP、OSPF、IP フィルターなど)
Help IPv6           IPv6
Help Firewall       ファイアウォール
Help Vrrp           VRRP
Help Dhcp           DHCP サーバー
Help Gre            GRE
Help L2tp           L2TP
Help IPSec          IPSec
Help Bnco           番号

Help Keybind        キーバインド
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)
```

図 4.3.1 「HELP」の結果

トップ画面の内容から、さらに表示したい項目を指定します。ヘルプでも省略形が使用できます（大文字の部分が、最低限入力しなければならない文字列です）。例えば、「H O」を入力すると、運用・管理に関連するサブメニューが表示されます。

```

Manager > H O ↓

AR450 オンラインヘルプ - V2.5 Rev.01 2003/05/06

運用・管理

Help Operation SSystem          システム
Help Operation Filesystem        記憶装置とファイルシステム
Help Operation Configuration     コンフィグレーション
Help Operation SShell            コマンドプロセッサ
Help Operation User              ユーザー認証データベース
Help Operation Authserver        認証サーバー
Help Operation LOAder            アップロード・ダウンロード
Help Operation TRigger           ソフトウェア
Help Operation Mail              メール送信
Help Operation SSecurity         セキュリティ
Help Operation LOG              ログ
Help Operation SScript           スクリプト
Help Operation TRigger           トリガー
Help Operation SNImp            SNMP
Help Operation Ntp              NTP
Help Operation TTerminal        ターミナルサービス
Help Operation SSh              Secure Shell
-More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)

```

図 4.3.2 [HELP OPERATION] の結果

更に項目を選択すると、該当項目のヘルプが表示されます。

```

Manager > H O SY ↓

Manager > H O SY

AR450 オンラインヘルプ - V2.5 Rev.01 2003/05/06

運用・管理 / システム

EDIT [filename]
HELP [topic]
LOGIN [login-name]
LOGOFF
RESTART {REBOOT|ROUTER} [CONFIG={filename|NONE}]
SET HELP=filename
SET SYSTEM CONTACT=string
SET SYSTEM LOCATION=string
SET SYSTEM NAME=string
SET [TIME=time] [DATE=date]
SHOW BUFFER
SHOW CPU
SHOW DEBUG [STACK]
SHOW EXCEPTION
SHOW STARTUP
SHOW SYSTEM
SHOW TIME
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)

```

図 4.3.3 [HELP OPERATION SYSTEM] の結果

4.4 インターフェース

物理インターフェース、データリンク層インターフェース、ネットワーク層インターフェースに関する概要を説明します。インターフェースに関する、完全な説明は下記をご覧ください。

 コマンドリファレンス「インターフェース」-「概要」

インターフェースの階層構造

本製品の内部をソフトウェア的に見ると、下図のようになります。本製品に対する設定は、最下位に位置する物理インターフェースの上になんがさまざまな論理インターフェースを重ね、コマンドによって関連づけることによって行います。

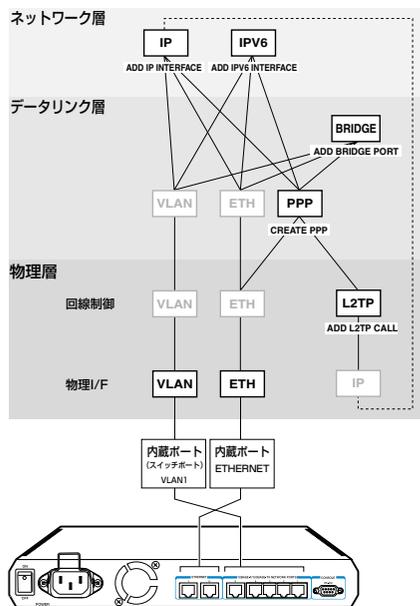


図 4.4.1 インターフェースの階層構造

最下層は物理インターフェースです（VLAN、ETH）。

その上は、物理インターフェースに接続されている回線を制御するソフトウェアモジュールです。VLAN、Ethernetの場合は特に設定の必要がないため、明確な形では存在しません。ここまでが OSI モデルでの物理層に相当します。

回線制御モジュールの上位になるのが、OSI 参照モデルの第 2 層にあたるデータリンク層インターフェースモジュールです。本製品では VLAN、Ethernet、PPP の 3 種類をサポートしています。この層で

は、単なるビット列をフレームと呼ばれる単位に組み立て、一回線（データリンク）上での通信を制御します。

VLAN、Ethernet インターフェースは物理層とデータリンク層が一体となっているため、特に設定の必要はありません。PPP の場合は、「CREATE PPP」コマンドで明示的にインターフェースを作成します。このとき、下位インターフェースとして、回線制御モジュールが物理インターフェースを指定します。

データリンク層の上には、第3層にあたるネットワーク層プロトコルのインターフェースモジュールが位置します。本製品ではIP(IPv4)とIPv6をサポートしています。ネットワーク層インターフェースは、「ADD IP INTERFACE」や「ADD IPV6 INTERFACE」コマンドを使って、データリンク層インターフェース上に追加（ADD）する形となります。

図には、示してありませんが、IP（IPv4）の上の仮想的なIPv6 インターフェイスとして、IPv6-over-IPv4 トンネルインターフェース（virtX）があります。



コマンドリファレンス「IPv6」

インターフェース名

「SHOW INTERFACE」コマンドを実行すると、システムによって認識されているインターフェースの名前、インディックス番号（ifIndex）を確認できます。

インターフェース名は、インターフェースの種類を示す略称（ETH、VLANなど）に、インターフェース番号（0、1）をつけたものです。

物理インターフェースの場合、インターフェース番号は同じ種類のインターフェースの間で重ならないよう、システムが0から順番に割り当てます。

表4.4.1 物理インターフェース名

物理インターフェース	名前
VLAN インターフェース（データリンク層と一体）	vlan1 ^a
Ethernet インターフェース（データリンク層と一体）	eth0およびeth1

- a. VLAN インターフェースの名前は、固定的に「vlan1」が割り当てられています。

データリンク層インターフェースの場合、インターフェースの番号は「CREATE PPP」コマンドで指定した番号になります。番号は有効範囲内で任意に選べますが、通例として0から順に割り当てます。

表4.4.2 データリンク層インターフェース名

インターフェース	名前
PPP インターフェース	ppp0 など

パラメーターにおけるインターフェースの表記

下記は、コマンドのパラメーターとして、インターフェースを指定するときの表記パターンです。

表4.4.3 パラメーターにおけるインターフェースの表記例

	名前
インターフェース番号だけを取るパラメーター	eth=0 または eth=eth0
インターフェース名を取るパラメーター	over=eth0
マルチホーミングしたIP インターフェースを指定するパラメーター	int=eth0-1
インターフェースのインディックス番号（ifIndex）を取るパラメーター	int=1 または int=eth0

物理インターフェース

本製品で使用可能な物理インターフェースは、以下の2種類です。^{*4}

- VLAN インターフェース（vlan）
- Ethernet インターフェース（eth）

物理インターフェースは、本製品と各種回線を接続するための接続口（ポート）です。ソフトウェア的に見ると、ポートを制御するドライバーなどを含んでおり、上位の回線制御モジュールやデータリンク層インターフェースにサービスを提供します。

VLAN（LAN側）インターフェース

VLAN（LAN側）インターフェースは、本製品をEthernet LAN（100BASE-TX、10BASE-T）に接続するためのインターフェースです。インターフェース名は「vlan1」（固定）です。

VLAN インターフェースは5ポートのEthernetスイッチになっており、複数のコンピューターを接続することができます。vlan1 インターフェースは、Ethernet と同じように物理層からデータリンク層までが一体となったインターフェースであり、上位層の設定においては、eth0、ppp0 などと同等のデータリンク層インターフェースとして扱うことができます。

VLAN（vlan1）インターフェースを使用するにあたって、特に設定しなくてはならない項目はありません。Ethernet インターフェースと同様、直接上位にレイヤー3 インターフェース（IP、IPv6）を作成することができます。たとえば、vlan1 上にIPイ



^{*4} 本製品は、このほかに非同期シリアルインターフェース（asyn）1ポートを装備していますが、同ポートはコンソール接続専用となっております。モデムなどを接続してのネットワーク接続はサポートしていません。

ンターフェースを作成するには、次のようにします。

```
Manager > ADD IP INTERFACE=vlan1
IP=192.168.1.10 MASK=255.255.255.0 ｡
```

VLAN インターフェースは、Ethernet インターフェースとほぼ同等ですが、以下の点は異なります。

- VLAN インターフェース上では、PPPoE を使用できません。
- VLAN インターフェース上では、トリガー機能を使用できません。

LAN 側スイッチポートのグループ構成を変更することはできません。常に全ポートがvlan1 所属になります。

Ethernet (ETH) インターフェース

Ethernet インターフェースは、本製品を Ethernet LAN (100BASE-TX、10BASE-T) に接続するためのインターフェースです。本製品では Ethernet インターフェースを 2 つ備えており、それぞれ「eth0」、 「eth1」と表します。

Ethernet インターフェースを使用するにあたって、設定しなくてはならない項目はありません。他の物理インターフェースと異なり、Ethernet は物理層からデータリンク層 (MAC 副層) までをカバーする規格であるため、直接上位にレイヤー 3 インターフェース (IP、IPv6) を作成することができます。例えば、eth0 上に IP インターフェースを作成するには、次のようにします。

```
Manager > ADD IP INTERFACE=eth0
IP=192.168.2.10 MASK=255.255.255.0 ｡
```

また、Ethernet インターフェースは、LAN との接続に使用するほか、PPPoE (PPP over Ethernet) による WAN 接続にも使用できます。PPPoE は Ethernet 上で PPP (Point-to-Point Protocol) を使用するためのプロトコルで、xDSL などのブロードバンドサービスで広く使用されています。

PPPoE インターフェースを作成する場合も、Ethernet インターフェースに対して特別な設定は必要ありません。「CREATE PPP」コマンドで PPP インターフェースを作成するときに、OVER パラメーターに「Ethernet インターフェース名」+ハイフン (-) +「PPPoE サービス名」を指定してください。プロバイダーから PPPoE サービス名が指定されていない場合は、キーワード any が任意の文字列を指定できます。例えば、eth0 上に PPPoE インターフェースを作成する場合、サービス名が「fuga」ならば「OVER=eth0-fuga」のように指定します。サービス名の指定がない場合は「OVER=eth0-any」とするか、任意の文字列を指定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ｡
```

Ethernet インターフェース上で動作しているソフトウェアモジュール、プロトコル、フレームタイプなどを確認するには、「SHOW ETH CONFIGURATION」コマンドを使います。

```
Manager > SHOW ETH=0 CONFIGURATION ｡
```

Configuration for ETH instance 0:

Module	Protocol	Format	Discrim	MAC address
-----	-----	-----	-----	-----
PPP	-	Ethernet	8864	0000cd0300b1
PPP	-	Ethernet	8863	0000cd0300b1
IP	IP	Ethernet	0800	0000cd0300b1
IP	ARP	Ethernet	0806	0000cd0300b1
-----	-----	-----	-----	-----

Ethernet インターフェースの MAC アドレスは、「SHOW ETH MACADDRESS」コマンドで確認できます。

```
Manager > SHOW ETH=0 MACADDRESS ｡
```

MAC address for ETH instance 0:

```
Address
-----
00-00-cd-03-00-b1
-----
```

Ethernet インターフェースで受信するよう設定されている MAC アドレスの一覧は、「SHOW ETH RECEIVE」コマンドで確認できます。

```
Manager > SHOW ETH=0 RECEIVE ｡
```

Receive addresses for ETH instance 0:

```
Address
-----
00-00-cd-03-00-b1
01-00-5e-00-00-05
01-00-5e-00-00-06
01-00-5e-00-00-09
ff-ff-ff-ff-ff-ff
all IP multicasts
-----
```

Ethernet インターフェースのリンクステータス、速度、デュプレックスモードは、「SHOW ETH STATE」コマンドで確認できます。

```
Manager > SHOW ETH=0 STATE ↵

State for ETH instance 0:

Link ..... up
Speed ..... 100 Mbps
Max BW Limit ..... None
Duplex mode ..... full
Auto-negotiation ..... complete

Link partner capabilities
Auto-negotiation ..... yes
100BASE-TX full duplex ..... yes
100BASE-TX ..... yes
10BASE-T full duplex ..... yes
10BASE-T ..... yes
```

Ethernet インターフェースをリセットするには、「RESET ETH」コマンドを使います。

```
Manager > RESET ETH=0 ↵
```

データリンク層インターフェース

本製品で使用できるデータリンク層インターフェースは以下の3種類です。

- VLAN インターフェース (vlan)
- Ethernet インターフェース (eth)
- PPP インターフェース (ppp)

データリンク層インターフェースは、物理インターフェースの上に直接作成する場合と、物理インターフェース上にセットアップした回線制御モジュール上に作成する場合があります。以下、それぞれのセットアップ方法について、例を挙げながら簡単に説明します。

VLAN インターフェース

VLAN インターフェースは、物理層とデータリンク層が一体になっています。VLAN インターフェースを使用するにあたって特別な設定は必要ありません。ネットワーク層インターフェースの設定時に、インターフェース名 (vlan1 で固定) を指定するだけで使用できます。

LAN 側スイッチポートのグループ構成を変更することはできません。常に全ポートが vlan1 所属になります。IP アドレスなど上位層の設定は、個々のスイッチポートではなく、vlan1 インターフェースに対して行います。

Ethernet インターフェース

Ethernet インターフェースは、物理層とデータリンク層が一体になっています。Ethernet インターフェースを使用するにあたって特別な設定は必要ありません。ネットワーク層インターフェースの設定時に、インターフェース名 (例: eth0) を指定するだけで使用できます。

PPP インターフェース

PPP インターフェースは、2 点間の WAN 接続に使用するデータリンク層インターフェースです。PPP インターフェースは、物理インターフェースである Ethernet インターフェース (eth) 上に作成することができます。

また、トンネリングプロトコル L2TP を使用すると、IP ネットワーク上に仮想的な回線 (L2TP コール) を構築し、その上に PPP インターフェースを作成することもできます。

PPP インターフェースは「CREATE PPP」コマンドで作成します。下位のインターフェースは、OVER パラメーターで指定します。

Ethernet 上で PPP を使用する (PPP over Ethernet。PPPoE) には、OVER パラメーターに「Ethernet インターフェース名」+ ハイフン (-) + 「PPPoE サービス名」を指定します。プロバイダーから PPPoE サービス名が指定されていない場合は、すべてのサービスを意味するキーワード「any」が任意の文字列を指定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵
```

ネットワーク層インターフェース

本製品で使用できるネットワーク層インターフェースは以下の2種類です。かつ内は設定コマンドにおける呼称です。

- IP インターフェース
- IPv6 インターフェース

ネットワーク層インターフェースは、本製品の基本機能であるルーティングのためのインターフェースです。本製品をルーターとして機能させるためには、使用するルーティングモジュール (IP、IPv6) を有効にし、ネットワーク層インターフェースを2つ以上作成する必要があります。

ネットワーク層インターフェースは、データリンク層インターフェースの上に作成します。

IP インターフェース

IP インターフェースは、IP パケットの送受信を行うためのインターフェースです。IP モジュールを有効にし、IP インターフェースを複数作成した時点で IP パケットの転送 (ルーティング) が行われるようになります。

IP インターフェースは、「ADD IP INTERFACE」コマンドでデータリンク層インターフェースに IP アドレス (とネットマスク) を割り当てることによって作成します。

作成した IP インターフェースは、データリンク層インターフェースと同じ名前でも参照できます。例えば、Ethernet インターフェース「0」上に作成した IP インターフェースを他の IP 関連コマンドで指定するときは「eth0」とします。

IP モジュールを有効化するには、「ENABLE IP」コマンドを実行します。

```
Manager > ENABLE IP ↓
```

VLAN インターフェースに IP アドレスを設定するには次のようになります。

```
Manager > ADD IP INT=VLAN1 IP=192.168.1.1  
MASK=255.255.255.0 ↓
```

Ethernet インターフェースに IP アドレスを設定するには次のようになります。

```
Manager > ADD IP INT=eth0 IP=192.168.10.1  
MASK=255.255.255.0 ↓
```

```
Manager > SHOW IP INTERFACE ↓
```

Interface	Type	IP Address	Bc Fr	PArp	Filt	RIP Met.	SA Mode	IP Sc
Pri. Filt	Pol. Filt	Network Mask	MTU	VJC	GRE	OSPF Met.	DBcast	Mul.
Local	---	Not set	-	-	---	---	Pass	---
---	---	Not set	1500	-	---	---	---	---
vlan1	Static	192.168.1.1	1	n	Off	---	01	Pass No
---	---	255.255.255.0	1500	-	---	0000000001	No	Rec
eth0	Static	192.168.10.1	1	n	On	---	01	Pass No
---	---	255.255.255.0	1500	-	---	0000000001	No	Rec

PPP インターフェースに IP アドレスを設定するには次のようになります。

```
Manager > ADD IP INT=PPP0 IP=192.168.100.1  
MASK=255.255.255.0 ↓
```

マルチホーミング

ひとつのデータリンク層インターフェースに対して、複数の IP インターフェース (IP アドレス) を与えることを「マルチホーミング」と言います。本製品では、データリンク層インターフェースに対して、最大 16 個までの IP インターフェースを持たせることができます。

マルチホーミングされたインターフェース名は、「eth0-1」のようにインターフェース名の後に、ハイフンで 0 ~ 15 番号の番号を付けて表します。マルチホーミングすると、例えば「eth0」は「eth0-0」と表示されます。

VLAN1 に 192.168.1.1 を割り当てるとします。

```
Manager > ENABLE IP ↓
```

```
Info (1005287): IP module has been enabled.
```

```
Manager > ADD IP INT=VLAN1 IP=192.168.1.1 ↓
```

```
Info (1005275): interface successfully added.
```

```
Manager > SHOW CONFIG DYN=IP ↓
```

```
#  
# IP configuration  
#  
enable ip  
add ip int=vlan1 ip=192.168.1.1
```

次に、VLAN1-1 に 192.168.2.1 を割り当てるとすると、VLAN1 はVLAN1-0 となります。

```
Manager > ADD IP INT=VLAN1-1 IP=192.168.2.1 ↵  
  
Info (1005275): interface successfully added.  
  
Manager > SHOW CONFIG DYN=IP ↵  
  
#  
# IP configuration  
#  
enable ip  
add ip int=vlan1-0 ip=192.168.1.1  
add ip int=vlan1-1 ip=192.168.2.1
```

4.5 ルーティング (スタティック)

2つのLANの接続

ネットワークXとYがあり、XとYをルーターで接続するには、以下のように設定します。

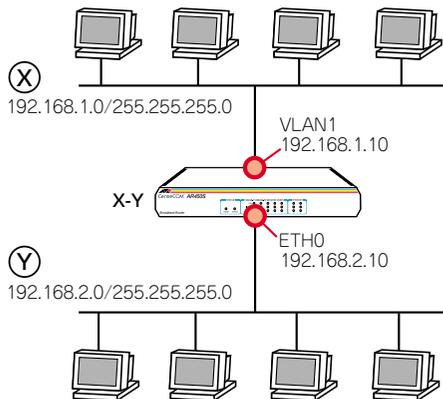


図 4.5.1 2つのLANの接続

- 1 ルーター X-Y に、Manager レベルでログインします。

```
login:manager ↵  
Password:friend ↵
```

- 2 わかりやすさのために、システム名を設定します。

```
Manager > SET SYSTEM NAME=X-Y ↵  
  
Info (134003): Operation successful.  
  
Manager X-Y>
```

- 3 IP モジュールを有効にします。

```
Manager X-Y> ENABLE IP ↵  
  
Info (1005287): IP module has been enabled.
```

- 4 物理インターフェースに IP アドレスを設定します。
VLAN1 に対して、下記を入力します。

```
Manager X-Y> ADD IP INTERFACE=vlan1  
IP=192.168.1.10 MASK=255.255.255.0 ↵  
  
Info (1005275): interface successfully added.
```

ETH0 に対して、下記を入力します。

```

Manager X-Y> ADD IP INTERFACE=eth0
IP=192.168.2.10 MASK=255.255.255.0 ↵

Info (1005275): interface successfully added.

Manager > SHOW IP INTERFACE ↵

```

Interface	Type	IP Address	Bc Pr PArp	Filt RIP Met.	SAMode	IPSc
Pri. Filt	Pol.Filt	Network Mask	MTU VJC	GRE OSPF Met.	DBcast	Mul.
Local	---	Not set	- - -	---	Pass	--
---	---	Not set	1500	---	---	---
vlan1	Static	192.168.1.10	1 n Off	---	01	Pass No
---	---	255.255.255.0	1500	---	0000000001	No Rec
eth0	Static	192.168.2.10	1 n On	---	01	Pass No
---	---	255.255.255.0	1500	---	0000000001	No Rec

5 物理インターフェイスに IP アドレスを割り当てると、それらのアドレスはルーティングテーブルに登録され、ネットワーク X と Y は通信可能となります。下記は、各ネットワークが物理インターフェイスに直接接続されていることを示しています。

```

Manager X-Y> SHOW IP ROUTE ↵

```

Destination	Mask	Type	Policy	NextHop Protocol	Interface Metrics	Age Preference
192.168.1.0	255.255.255.0	0.0.0.0	interface	vlan1	1	16
-	direct	0	0.0.0.0	eth0	1	0
192.168.2.0	255.255.255.0	0.0.0.0	interface	eth0	1	7
-	direct	0	0.0.0.0	interface	1	0

3 つの LAN の接続

図 4.5.1 (p.45) の例に、ネットワーク Z を追加する場合は、以下のように設定します。

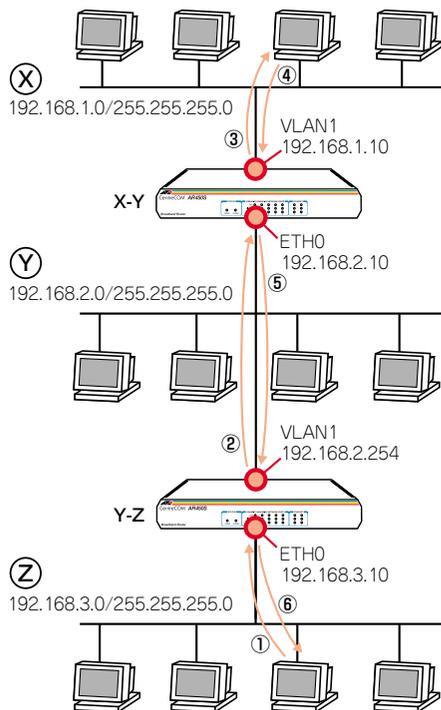


図 4.5.2 3 つの LAN の接続

1 ルーター Y-Z に、Manager レベルでログインします。

```

login:manager ↵
Password:friend ↵

```

2 わかりやすさのために、システム名を設定します。

```

Manager > SET SYSTEM NAME=Y-Z ↵

Info (134003): Operation successful.

Manager Y-Z>

```

3 IP モジュールを有効にします。

```
Manager Y-Z> ENABLE IP ↵
Info (1005287): IP module has been enabled.
```

4 物理インターフェースにIP アドレスを設定します。 VLAN1 に対して、下記を入力します。

```
Manager Y-Z> ADD IP INTERFACE=vlan1
IP=192.168.2.254 MASK=255.255.255.0 ↵
Info (1005275): interface successfully added.
```

ETH0 に対して、下記を入力します。

```
Manager Y-Z> ADD IP INTERFACE=eth0
IP=192.168.3.10 MASK=255.255.255.0 ↵
Info (1005275): interface successfully added.
```

5 物理インターフェースにIP アドレスを割り当てると、それらのアドレスはルーティング情報として、ルーティングテーブルに登録され、ネットワーク Y と Z は通信可能となります。下記は、各ネットワークが物理インターフェースに直接接続されていることを示しています。

```
Manager Y-Z> SHOW IP ROUTE ↵
IP Routes
-----
Destination      Mask      NextHop      Interface      Age
DLCI/Circ.      Type      Policy      Protocol      Metrics      Preference
-----
192.168.2.0      255.255.255.0  0.0.0.0      vlan1          15
-                direct  0            interface      1            0
192.168.3.0      255.255.255.0  0.0.0.0      eth0           6
-                direct  0            interface      1            0
```

6 しかしながら、X-Y はネットワーク Z の所在を知らないため、X から Z に向かうパケットを配送できません。また、Y-Z はネットワーク X の所在を知らないため、Z から X に向かうパケットを配送できません。X と Z 間の通信ができるようにするために、「ADD IP ROUTE」コマンドにより、ネットワークの所在（経路情報）をルーティングテーブルに登録します。

X-Y に対して、ネットワーク Z (192.168.3.0) は、ETH0 に接続されている側のネットワークの 192.168.2.254 にパケットを送ればよいことを教えてやります。METRIC は、経由するルー

ターの数+1を設定します。

```
Manager X-Y> ADD IP ROUTE=192.168.3.0
MASK=255.255.255.0 INTERFACE=eth0
NEXTHOP=192.168.2.254 METRIC=2 ↵
Info (1005275): IP route successfully added.
```

X-Y のルーティングテーブルは、次のようになります。

```
Manager X-Y> SHOW IP ROUTE ↵
IP Routes
-----
Destination      Mask      NextHop      Interface      Age
DLCI/Circ.      Type      Policy      Protocol      Metrics      Preference
-----
192.168.1.0      255.255.255.0  0.0.0.0      vlan1          107
-                direct  0            interface      1            0
192.168.2.0      255.255.255.0  0.0.0.0      eth0           97
-                direct  0            interface      1            0
192.168.3.0      255.255.255.0  192.168.2.254 eth0           5
-                remote  0            static         2            60
```

Y-Z に対して、ネットワーク X (192.168.1.0) は、VLAN1 に接続されている側のネットワークの 192.168.2.10 にパケットを送ればよいことを教えてやります。METRIC は、経由するルーターの数+1を設定します。

```
Manager Y-Z> ADD IP ROUTE=192.168.1.0
MASK=255.255.255.0 INTERFACE=vlan1
NEXTHOP=192.168.2.10 METRIC=2 ↵
Info (1005275): IP route successfully added.
```

Y-Z のルーティングテーブルは、次のようになります。

```
Manager Y-Z> SHOW IP ROUTE ↵
IP Routes
-----
Destination      Mask      NextHop      Interface      Age
DLCI/Circ.      Type      Policy      Protocol      Metrics      Preference
-----
192.168.1.0      255.255.255.0  192.168.2.10 vlan1          9
-                remote  0            static         2            60
192.168.2.0      255.255.255.0  0.0.0.0      vlan1          517
-                direct  0            interface      1            0
192.168.3.0      255.255.255.0  0.0.0.0      eth0           508
-                direct  0            interface      1            0
```

7 以上で、ネットワーク X、Y、Z は相互に通信できるようになります。

デフォルトルート

ネットワークX、Y、Zをインターネットに接続する場合は、デフォルトルートを設定します。デフォルトルートとは、最終到達点までの経路が不明なパケットを配送してくれるルーターまでの経路です。以下の例では、インターネットに向かうパケット、すなわちX、Y、Z以外のアドレスを持つパケットを配送してくれるルーターまでの経路です。

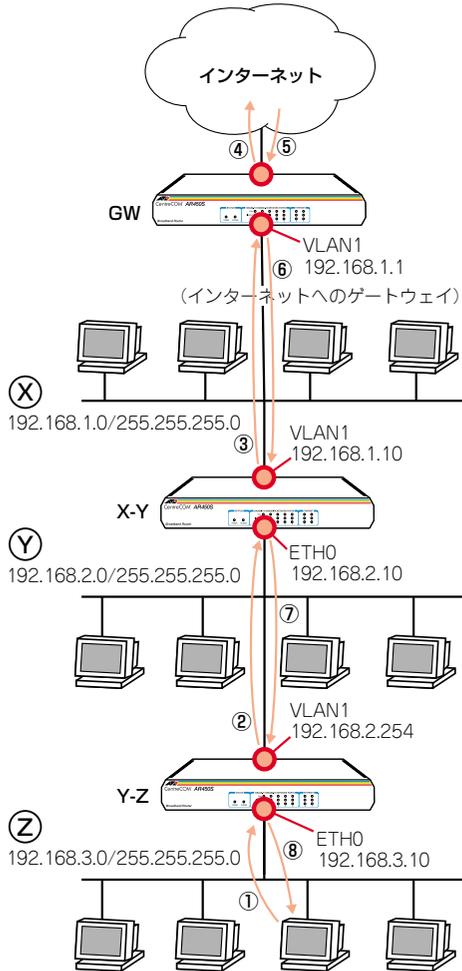


図4.5.3 インターネットにも接続

- 1 X-Yに対して、インターネットに向かう任意のパケットは、VLAN1に接続されている側のネットワークの192.168.1.1に送ればよいことを教えてやります。

```
Manager X-Y> ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0
INTERFACE=vlan1 NEXTHOP=192.168.1.1
METRIC=2 ↓
```

Info (1005275): IP route successfully added.

X-Yのルーティングテーブルは、次のようになります。

```
Manager X-Y> SHOW IP ROUTE ↓
```

IP Routes					
Destination DLCI/Circ.	Mask Type	Policy	NextHop Protocol	Interface Metrics	Age Preference
0.0.0.0	0.0.0.0		192.168.1.1	vlan1	6
-	remote	0	static	2	360
192.168.1.0	255.255.255.0		0.0.0.0	vlan1	3488
-	direct	0	interface	1	0
192.168.2.0	255.255.255.0		0.0.0.0	eth0	3478
-	direct	0	interface	1	0
192.168.3.0	255.255.255.0		192.168.2.254	eth0	3386
-	remote	0	static	2	60

- 2 Y-Zに対して、インターネットに向かう任意のパケットは、VLAN1が接続されている側のネットワークの192.168.2.10に送ればよいことを教えてやります。METRICは、経由するルーターの数+1を設定します。

```
Manager Y-Z> ADD IP ROUTE=0.0.0.0 MASK=0.0.0.0
INTERFACE=vlan1 NEXTHOP=192.168.2.10
METRIC=2 ↓
```

Info (1005275): IP route successfully added.

Y-Zのルーティングテーブルは、次のようになります。

```
Manager Y-Z> SHOW IP ROUTE ↓
```

IP Routes					
Destination DLCI/Circ.	Mask Type	Policy	NextHop Protocol	Interface Metrics	Age Preference
0.0.0.0	0.0.0.0		192.168.2.10	vlan1	3
-	remote	0	static	2	360
192.168.1.0	255.255.255.0		192.168.2.10	vlan1	151
-	remote	0	static	2	60
192.168.2.0	255.255.255.0		0.0.0.0	vlan1	181
-	direct	0	interface	1	0
192.168.3.0	255.255.255.0		0.0.0.0	eth0	172
-	direct	0	interface	1	0

この場合、宛先がネットワークXのパケットは、デフォルトルートによっても配送が可能なので、手順6 (p.47) の下記のコマンドは省略できます。

```
Manager Y-Z> ADD IP ROUTE=192.168.1.0
MASK=255.255.255.0 INTERFACE=vlan1
NEXTHOP=192.168.2.10 METRIC=2 』

Info (1005275): IP route successfully added.
```

インターネットからの戻りのルート

ゲートウェイ GW には、インターネットからの戻りのパケットが、ネットワークY、Z に配送されるよう、経路情報を追加する必要があります。

```
Manager GW> ADD IP ROUTE=192.168.2.0
MASK=255.255.255.0 INTERFACE=vlan1
NEXTHOP=192.168.1.10 METRIC=2 』

Manager GW> ADD IP ROUTE=192.168.3.0
MASK=255.255.255.0 INTERFACE=vlan1
NEXTHOP=192.168.1.10 METRIC=2 』
```

コンピューターにおけるデフォルトルート

ネットワークX、Y には、ルーターが2 つずつあります。各ネットワークのコンピューターに設定するデフォルトゲートウェイ^{*5}は、2つのルーターのどちらを指定してもかまいません。例えば、デフォルトゲートウェイとして192.168.2.10 が設定された、ネットワークYのコンピューターがネットワークZと通信する場合、コンピューターからのパケットはルーターX-Y に向かって送信されますが、そのパケットはX-Y によってY-Z に転送されます。



*5 コンピューターでは、直接接続されていないネットワーク宛のパケットのすべては、デフォルトゲートウェイ(デフォルトルート)に送ります。

5 ユーザー管理とセキュリティー

5.1 ユーザーレベル

権限によって、User（一般ユーザー）、Manager（管理者）、Security Officer（保安管理者）の3つのユーザーレベルが存在します。

表5.1.1：動作モードとユーザーレベルの権限

レベル	ノーマルモード	セキュリティーモード
User	<ul style="list-style-type: none">ユーザー自身に関する端末設定、パスワードのごく一部のコマンドのみ実行可能おもにWANを経由で接続してくるPPPユーザーの認証に使用	
Manager	<ul style="list-style-type: none">すべてのコマンドを実行可能	<ul style="list-style-type: none">ユーザーやIPsecなどセキュリティーに関するコマンドの実行不可第2位のユーザーレベル
Security Officer	<ul style="list-style-type: none">すべてのコマンドを実行可能Managerと同じユーザーレベル	<ul style="list-style-type: none">すべてのコマンドを実行可能第1位のユーザーレベル

Manager、Security Officer レベルの権限は、動作モードによって変わります。

 本書「5.4 ノーマルモード / セキュリティーモード」(p.54)

ユーザーレベルによって、コマンドプロンプトが変わります。

 本書「4.1 コマンドプロセッサ」(p.35)

5.2 ユーザー認証データベース

本製品は、ユーザー認証データベースを持っており、次のような状況が発生したとき、このデータベースを使用してユーザーの認証を行います。

- コンソールターミナルまたはTelnetによってユーザーが本製品にログインするとき
- PPPによって相手が接続してきたとき

関連する情報として、本書「3.4 パスワードの変更」(p.28)、「4.1 コマンドプロセッサ」(p.35)もご覧ください。

ユーザー認証データベースには、次のような情報を登録することができます。このデータベースへのアクセスは、ノーマルモードではManagerまたはSecurity Officerレベル、セキュリティーモードではSecurity Officerレベルの権限が必要です。

表5.2.1 ユーザー認証データベース

ユーザー名	USER <ul style="list-style-type: none">1～64文字の半角のアルファベットと数字を使用可スペース、「?」、ダブルクォーテーション「"」は使用不可。その他の半角記号は使用可大文字、小文字の区別なし
パスワード	PASSWORD <ul style="list-style-type: none">1～32文字までの半角のアルファベットと数字を使用可デフォルトでは6文字以上の長さが必要「?」、ダブルクォーテーション「"」は使用不可。その他の半角記号は使用可スペースが含まれる場合、ダブルクォーテーション「"」でくくる大文字、小文字の区別あり
ユーザーレベル	PRIVILEGE <ul style="list-style-type: none">USER、MANAGER、SECURITYOFFICERから選択デフォルトのユーザーレベルは「USER」
ログイン権	LOGIN <ul style="list-style-type: none">コンソールターミナルまたはTelnetによるログインを許可するか否かユーザーレベルが「USER」の場合は必須。USERレベルのユーザーは、おもにPPPの認証に使用されるものなので、通常は「LOGIN=NO」を指定
Telnet実行権	TELNET <ul style="list-style-type: none">ログインしたユーザーにTELNETコマンドの実行権を与えるか否かデフォルトは「与えない」
コメント	DESCRIPTION <ul style="list-style-type: none">ユーザーについての説明

ご購入時には、Managerレベルのユーザー「manager」のみが登録されています。初期パスワードは「friend」です。

 本書「3.3 ログイン（ご購入時）」(p.28)

ユーザー認証データベースだけでなく、RADIUS、TACACSサーバーによる認証も可能です。

 コマンドリファレンス「運用・管理」- 「ユーザー認証データベース」- 「ユーザー認証処理の順序」

コマンドリファレンス「運用・管理」- 「認証サーバー」

5.3 ユーザーの登録と情報の変更

ユーザー認証データベースへのアクセスは、ノーマルモードでは Manager レベル、セキュリティモードでは Security Officer レベルの権限が必要です。

新規ユーザー登録

- 1 Managerレベルでログインします。下記では、ユーザー「manager」ログインしています。

```
login: manager 』
Password: _____ (表示されません)
```

```
Manager > ADD USER=osaka-shisya
PASSWORD="okonomiyaki" LOGIN=NO 』
```

- 2 新規ユーザー登録は、「ADD USER」コマンドを使います。下記では、ユーザー名「osaka-shisya」、パスワード「okonomiyaki」を仮定しています。ユーザーレベルは User です (デフォルト)。ユーザーレベルが「User」であるため、LOGINパラメーターの指定が必要です。PPP 認証のためのユーザーなので「NO」を指定します。「TELNET」コマンドは使用できません (デフォルト)。

```
Manager > ADD USER=osaka-shisya
PASSWORD="okonomiyaki" LOGIN=NO 』
```

Manager レベルでログインすると、セキュリティタイマーがスタートします (デフォルトは 60 秒)。ログインして 60 秒以内にユーザー管理コマンドを実行した場合、パスワードは要求されませんが、60 秒以上経過すると Manager レベルのパスワードを要求されます。

```
This is a security command, enter your password at the prompt
Password: _____ (表示されません)
```

```
User Authentication Database
```

```
-----
Username: osaka-shisya ()
Status: enabled Privilege: user Telnet: no
Logins: 0 Fails: 0 Sent: 0 Rcvd: 0
Authentications: 0 Fails: 0
```

タイマーはユーザー管理コマンドを実行するたびにリセットされます。60 秒以内にユーザー管理コマンドを実行しないとタイマーがタイムアウトし、あらためて Manager レベルのパスワードを要求されます。

セキュリティタイマーの値は、次のコマンドで変更できます。下記は、90 秒に変更しています。値は 10 ~ 600 秒に設定できます。

```
Manager > SET USER SECUREDELAY=90 』
```

```
This is a security command, enter your password at the prompt
Password: _____ (表示されません)
```

```
User module configuration and counters
```

```
-----
Security parameters
login failures before lockout ..... 5 (LOGINFAIL)
lockout period ..... 600 seconds (LOCKOUTPD)
manager password failures before logoff .. 3 (MANPWDFAIL)
maximum security command interval ..... 90 seconds (SECUREDELAY)
minimum password length ..... 6 characters (MINPWLEN)
semi-permanent manager port ..... none
```

```
Security counters
```

```
logins 2 authentications 0
managerPwdChanges 0 defaultAcctRecoveries 1
unknownLoginNames 0 tacacsLoginReqs 0
totalPwdFails 0 tacacsLoginRejs 0
managerPwdFails 1 tacacsReqTimeouts 0
securityCmdLogoffs 0 tacacsReqFails 0
loginLockouts 0 databaseClearTotallys 0
-----
```

ユーザー情報変更

既に登録されているユーザーの情報を変更する場合、「SET USER」コマンドを使用します。下記では、「osaka-shisya」にログイン権限を与え、コメントを追加しています。

```
Manager > SET USER=osaka-shisya LOGIN=yes
DESC="osaka-shisya PPP account" 』
```

```
This is a security command, enter your password at the prompt
Password: _____ (表示されません)
```

```
User Authentication Database
```

```
-----
Username: osaka-shisya (osaka-shisya PPP account)
Status: enabled Privilege: user Telnet: no Login: yes
Logins: 0 Fails: 0 Sent: 0 Rcvd: 0
Authentications: 0 Fails: 0
```

パスワード変更

ユーザー本人がパスワードを変更する場合は、「SET PASSWORD」コマンドを使用します（この場合、パスワードにスペースを含んでもダブルクォートでくくる必要はありません）。

```
login: osaka-shisya 』
Password:

> SET PASSWORD 』

OLD passsword: _____ (表示されません)
New password: _____ (表示されません)
Confirm: _____ (表示されません)
```

 本書「3.4 パスワードの変更」(p.28)

ユーザー情報表示

ユーザー情報の表示は、「SHOW USER」コマンドを使用します。

```
Manager > SHOW USER 』

User Authentication Database
-----
Username: manager (Manager Account)
Status: enabled   Privilege: manager   Telnet: yes   Login: yes
Logins: 1         Fails: 0       Sent: 0       Rcvd: 0
Authentications: 0 Fails: 0
Username: osaka-shisya (osaka-shisya PPP account)
Status: enabled   Privilege: user       Telnet: no    Login: yes
Logins: 0         Fails: 0       Sent: 0       Rcvd: 0
Authentications: 0 Fails: 0
-----

Active (logged in) Users
-----
User      Port/Device  Location      Login Time
-----
manager   Asyn 0       local         20:47:50 17-Apr-2002
```

ユーザー削除

ユーザーの削除は、「DELETE USER」コマンドを使用します。

```
Manager > DELETE USER=osaka-shisya 』

This is a security command, enter your password at the prompt
Password: _____ (表示されません)

Info (145265): DELETE USER, user osaka-shisya has been deleted.
```

ユーザー一括削除

全ユーザーの一括削除は、「PURGE USER」コマンドを使用します。ご購入時における唯一のユーザー「manager」は削除されませんが、パスワードを変更している場合、ご購入時の「friend」に戻ります。

```
Manager > PURGE USER 』

This is a security command, enter your password at the prompt
Password: _____ (表示されません)

Info (145269): PURGE USER, user database has been purged.

Manager > SHOW USER 』

User Authentication Database
-----
Username: manager (Manager Account)
Status: enabled   Privilege: manager   Telnet: yes   Login: yes
Logins: 0         Fails: 0       Sent: 0       Rcvd: 0
Authentications: 0 Fails: 0
-----

Active (logged in) Users
-----
User      Port/Device  Location      Login Time
-----
manager   Asyn 0       local         20:47:50 17-Apr-2002
```

5.4 ノーマルモード / セキュリティーモード

本製品は、「ノーマルモード」「セキュリティーモード」の2つの動作モードを持っています。

ノーマルモード (Normal Mode)

デフォルトの動作モードです。ご購入時は、このモードとなっています。

セキュリティーモード (Security Mode)

より高いセキュリティーレベルを実現するためのモードです。ログインセキュリティーや管理コマンドの実行権が厳しく制限されます。

IPsecなどのセキュリティー機能を利用するときや、本製品の管理に関するセキュリティーを高めたい場合に使います。

セキュリティーモードへの移行

セキュリティーモードに移行するためには、あらかじめ Security Officer レベルのユーザーを作成しておく必要があります。セキュリティーモードに移行すると、Manager レベルは第2位の権限レベルに降格され、セキュリティーに関するコマンドを実行できなくなります。

- 1 Security Officer レベルのユーザーを作成します。

```
Manager > ADD USER=secoff
PRIVILEGE=SECURITYOFFICER
PASSWORD="top secret" ↓
```

- 2 セキュリティーモードに移行すると、Telnet 接続では Security Officer レベルでログインできなくなるので（他のレベルならログイン可）、必要に応じて RSO (Remote Security Officer) の設定をしておきます。

```
Manager > ENABLE USER RSO ↓

This is a security command, enter your password at the prompt
Password: _____ (表示されません)

Info (1045057): RSO has been enabled.

Manager > ADD USER RSO IP=192.168.10.5 ↓

Remote Security Officer Access is enabled

Remote Security Officer ... 192.168.10.5/255.255.255.255
```

RSO は、セキュリティーモードにおいて、指定したアドレスからの Security Officer レベルでのログインを許可する機能です。

- 3 Security Officer レベルのアカウントを設定スクリプトとして保存し、起動時に実行されるように指定しておきます。

```
Manager > CREATE CONFIG=TEST01.CFG ↓

Info (1034003): Operation successful.

Manager > SET CONFIG=TEST01.CFG ↓

Info (1034003): Operation successful.
```

- 4 セキュリティーモードに移行するには「ENABLE SYSTEM SECURITY_MODE」コマンドを実行します。

```
Manager > ENABLE SYSTEM SECURITY_MODE ↓

Info (1034003): Operation successful.
```

このコマンドを実行すると、フラッシュメモリーに「enabled.sec」ファイルが作成されます。システム起動時に本ファイルが存在すればセキュリティーモードとなります。このファイルを削除したり、修正、編集、コピー、リネームなどを行わないでください。

- 5 Security Officer レベルでログインしなおすと、コマンドプロンプトが「SecOff >」に変わります。

```
Manager > LOGIN secoff ↓

Password: _____ (表示されません)

SecOff >
```

- 6 Security Officer レベルでログインすると、セキュリティータイマーがスタートします（デフォルトは60秒）。ログインして60秒以内にセキュリティーに関連するコマンドを実行した場合、パスワードは要求されませんが、60秒以上経過すると、Security Officer レベルのパスワードを要求されます。

```
SecOff > add user=nagoya-sisya
password="misokatsu" login=no ↓

This is a security command, enter your password at the prompt
Password: _____ (表示されません)

Number of logged in Security Officers currently active.....1

User Authentication Database
-----
Username: nagoya-sisya ()
Status: enabled Privilege: user Telnet: no Login: no
Logins: 0 Fails: 0 Sent: 0 Rcvd: 0
Authentications: 0 Fails: 0
-----
```

タイマーはセキュリティー関連コマンドを実行するたびにリセットされます。60秒以内にセキュリティーコマンドを実行し

ないとタイマーがタイムアウトし、ログインユーザーの権限は Manager レベルに格下げされます。格下げされた状態でセキュリティーコマンドを実行しようとする、あらためて Security Officerレベルのパスワードを要求されます。

セキュリティータイマーの値は、次のコマンドで変更できます。下記は、90 秒に変更しています。値は 10 ~ 600 秒に設定できます。

```
SecOff > SET USER SECUREDELAY=90 』

This is a security command, enter your password at the prompt
Password: _____ (表示されません)

User module configuration and counters
-----
Security parameters
login failures before lockout ..... 5 (LOGINFAIL)
lockout period ..... 600 seconds (LOCKOUTPD)
manager password failures before logoff .. 3 (MANPWDFAIL)
maximum security command interval ..... 90 seconds (SECURELAY)
minimum password length ..... 6 characters (MINPWDLEN)
semi-permanent manager port ..... none

Security counters
logins 2 authentications 0
managerPwdChanges 0 defaultAcctRecoveries 1
unknownLoginNames 0 tacacsLoginReqs 0
totalPwdFails 0 tacacsLoginRejs 0
managerPwdFails 1 tacacsReqTimeouts 0
securityCmdLogoffs 0 tacacsReqFails 0
loginLockouts 0 databaseClearTotallys 0
-----
```

現在の動作モードを確認するには「SHOW SYSTEM」コマンドを実行します。「Security Mode」が Enabled ならセキュリティーモード、Disabled ならノーマルモードです。

セキュリティーモード時に「SET CONFIG」コマンドで起動スクリプトを変更するときは注意が必要です。例えば、SET CONFIG=NONE を実行すると、起動スクリプトが実行されずに、動作モードはセキュリティーモードのままになります。この状態でシステムを再起動すると、Security Officer レベルのユーザーが存在しないことになるため、多くのコマンドが実行できなくなります。このような状態になった場合は、「DISABLE SYSTEM SECURITY_MODE」コマンドを実行するしかありません。

ノーマルモードへ戻る

セキュリティーモードからノーマルモードに戻るには、次のコマンドを入力します。このコマンドを実行すると、「enabled.sec」が削除されます。また、ノーマルモードになった時点で、セキュリティーモードでのみ保存可能なファイル（暗号鍵ファイルなど）は自動的に削除されます。

```
Manager > DISABLE SYSTEM SECURITY_MODE 』

Warning: This command will disable security mode and
delete all security files.
Are you sure you wish to proceed?(Y/N) y
```



このコマンドをご使用になる場合は、充分にご注意ください。削除された機密ファイルは復活できません。

6 テキストエディター

本製品は、テキストエディター機能を内蔵しています。例えば「CREATE CONFIG=*filename*.CFG」によって保存された設定スクリプトファイルを開き、編集を施して、保存することができます。

 本書「9.2 ファイル名」(p.64)

6.1 Editの実行

エディターの起動は、「EDIT」に続けて、ファイル名を指定します。拡張子は、cfg、scp、txt が指定可能です。指定したファイルが存在しない場合は、内容が空のファイルが作成されます。例えば、既存のファイルROUTER.CFGを指定して、下記のコマンドを入力すると、

```
Manager > EDIT ROUTER.CFG ↓
```

次のようなエディター画面が表示されます。^{*1}

```

#
# SYSTEM configuration
#
#
# SERVICE configuration
#
#
# LOAD configuration
#
#
# USER configuration
#
set user=manager pass=3af116ce503efb5dbf7a00c6cad64467bf priv=manager lo=yes
set user=manager desc="Manager Account" telnet=yes
#
# TTY configuration
#

```

Ctrl+K+H = Help | File = ROUTER.CFG | Insert | 1:1

画面の最下行は、ステータス行です。左側から下記の項目を表示しています。

- ヘルプを表示するキー (Ctrl+K+H = Help)
- ファイル名 (File = ROUTER.CFG)
- Insert (挿入モード) または Overstrike (上書きモード)
- 内容が変更されているか否か (変更ありは Modified と表示)
- カーソル位置 (行番号 : 列番号)

 ^{*1} 入力されたコマンドは、本製品のルールにしたがった書式に変換されるため、実際に入力したコマンドと、「CREATE CONFIG=*filename*.CFG」で保存されたファイルのコマンドの見かけは異なったものとなります。しかしながら、保存されている設定情報は同じです。類似の概念として、「コマンドの分割入力」(p.36)をご覧ください。

カーソル移動キー (←↑↓→) を操作してみてください。カーソルが正しく移動しない場合は、通信ソフトウェアのエミュレーションを VT100 に設定してください。

 本書「3.1 コンソールターミナルの設定」(p.27)
本書「A.2 ハイパーターミナルの設定」(p.143)

「↓」キーを押し続け、カーソルが最下行まで移動すると、画面がスクロールします。ハイパーターミナルをご使用の場合、スクロールしたときに、長い行の右側が正しく表示されませんが、「Ctrl」キーを押しながら「W」キーを押すと、画面が再描画されます。

シャープ「#」で始まる行は、コメント行です。この行は、設定として解釈されません。カーソルをコメント行に移動して、「BackSpace」キーを押してみてください。文字を消去できない場合は、通信ソフトウェアの「BackSpace」キーのコードを「Delete」に設定してください。また、「Delete」キーでも文字を消去することができます。

内容を変更せずにエディターを終了する場合、「Ctrl」キーを押しながら「C」キーを押します。変更内容を破棄するか否かを問われますので、「Y」キー (はい) を押してください。「N」キーを押すと、エディター画面に戻ります。

```
Lose changes ( y/n ) ? Y
```

内容を保存する場合は、「Ctrl」キーを押しながら「K」キーを押し、続けて「Ctrl」キーを押したまま「X」キーを押します。保存するか否かを問われますので、「Y」キーを押してください。「N」キーを押すと、内容を保存せずにエディターが終了します。

```
Save file ( y/n ) ? Y
```

6.2 キー操作

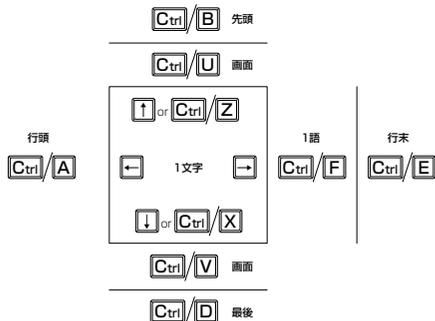


図 6.2.1 カーソル移動キー

キー操作は、以下の通りです。「Ctrl/△」は「Ctrl」キーを押しながら「△」キーを押す操作を意味します。

「Ctrl/△, Ctrl/○」は、「Ctrl」キーを押しながら「△」キーを押し、続けて「Ctrl」キーを押しながら「○」を押す操作を意味します。

表 6.2.1 : カーソル移動

キー	機能
↑ ^a または Ctrl/Z	1 行上に、移動する。
↓ または Ctrl/X	1 行下に、移動する。
→	1 桁右に、移動する。
←	1 桁左に、移動する。
Ctrl/B	ファイルの先頭に、移動する。
Ctrl/D ^b	ファイルの最後に、移動する。
Ctrl/A	行頭に、移動する。
Ctrl/E	行末に、移動する。
Ctrl/U	1 画面前に、移動する (スクロールダウン)。
Ctrl/V	1 画面後に、移動する (スクロールアップ)。
Ctrl/F	1 ワード右に移動する。

- ハイパーターミナルをご使用の場合、カーソル移動キー ↑ ↓ → ← は使用できません。
- Ctrl/D を入力すると Telnet セッションが切断されることがありますのでご注意ください。

表 6.2.2 : モードの切り替え

キー	機能
Ctrl/O	上書きモード
Ctrl/I	挿入モード

表 6.2.3 : 消去

キー	機能
Ctrl/T	カーソル右の 1 ワードを消去する。
Ctrl/Y	行全体を消去する。
BackSpace、Delete ^a	カーソル右の 1 文字を消去する。

- ハイパーターミナルをご使用の場合、「ファイル」→「プロパティ」→「設定」→「Backspace キーの送信方法」を「Delete」に設定してください。

表 6.2.4 : ブロック操作

キー	機能
Ctrl/K, Ctrl/B	ブロックマークを開始する。
Ctrl/K, Ctrl/C	ブロックでコピーする。
Ctrl/K, Ctrl/D	ブロックマークを終了する。
Ctrl/K, Ctrl/P	ブロックでペースト (貼りつけ) する。
Ctrl/K, Ctrl/U	ブロックでカットする。
Ctrl/K, Ctrl/Y	ブロックで消去する。
Ctrl/F	1 ワード右に移動する。

表 6.2.5 : 検索

キー	機能
Ctrl/K, Ctrl/F	文字列を検索する。
Ctrl/L	検索を再実行する。

表 6.2.6 : 終了・保存

キー	機能
Ctrl/K, Ctrl/X	上書き保存し、エディターを終了する。
Ctrl/C	変更を破棄するか問い合わせを表示してエディターを終了する。

表 6.2.7 : その他

キー	機能
Ctrl/W	画面をリフレッシュ (再表示) する。
Ctrl/K, Ctrl/O	別のファイルを開く。
Ctrl/K, Ctrl/H	エディターのオンラインヘルプを表示する。

7 Telnet を使う

本製品は、Telnet デーモン（サーバー）およびクライアントの機能を内蔵しています。この章では、Telnet を使用するための設定や、操作について説明します。

7.1 本製品に Telnet でログインする

本製品は、Telnet デーモンを内蔵しており、他の Telnet クライアントからネットワーク経由でログインすることができます。

Telnet クライアントは、次のように設定してください。エミュレーション、「BackSpace」キーのコードは EDIT コマンドのための設定です。文字セットは、HELP コマンド（日本語オンラインヘルプ）のための設定です。

表 7.1.1 Telnet クライアントの設定

項目	値
エミュレーション	VT100
「BackSpace」キーのコード	Delete
文字セット	SJIS

また、LAN 側 Ethernet インターフェース経由でログインするためには、本製品に次のような設定が施されている必要があります。

```
Manager > ENABLE IP ↓  
Manager > ADD IP INT=vlan1 IP=192.168.1.1 ↓
```

- 1 通信機能を利用できるコンピューターを使用し、本製品に対して Telnet を実行します。下記では、あらかじめ本製品の物理ポートに IP アドレス「192.168.1.1」が割り当てられていると仮定しています。実際には、お客様の環境におけるものをご使用ください。

```
TELNET 192.168.1.1 ↓
```

- 2 本製品に接続すると、ログインプロンプトが表示されますので、ユーザー名、パスワードを入力してください。下記では、デフォルトの Manager レベルのユーザー名、パスワード（入力は表示されません）を仮定しています。ログインに成功すると、コマンドプロンプトが表示されます。

```
TELNET session now in ESTABLISHED state  
  
login: manager ↓  
Password: friend ↓  
  
Manager >
```

セキュリティモードでは、Security Officer レベルのユーザーは Telnet でログインできなくなります（他のレベルなら可）。Security

Officer レベルでログインするためには、Remote Security Officer の設定が必要です。

 本書「セキュリティモードへの移行」(p.54)

7.2 ブリッジングにおける Telnet

リモートブリッジとして動作するように設定されている場合（IP がブリッジングされている）においても、Ethernet または WAN インターフェース経由の IP アクセスが可能です。これにより Ethernet 側や WAN 回線を経由して、Telnet クライアントによる本製品へのログイン、または本製品を Telnet クライアントとして動作させることができます。下記にローカルブリッジにおける設定例を示します（IP の機能モジュールを有効化し、Ethernet インターフェースに IP アドレスを割り付けています）。

```
ENABLE BRIDGE ↓  
ADD BRIDGE PROTOCOL="ALL ETHERNET II"  
TYPE=ALLETHII PRIO=1 ↓  
ADD BRIDGE PROTOCOL="IP" TYPE=IP PRIO=1 ↓  
ADD BRIDGE PROTOCOL="ARP" TYPE=ARP PRIO=1 ↓  
ADD BRID PO=1 INT=vlan1 ↓  
ADD BRID PO=2 INT=eth0 ↓  
ENABLE IP ↓  
ADD IP INT=eth0 IP=192.168.5.1 ↓
```

図 7.2.1 ブリッジングにおける IP アクセスのための設定

Telnet クライアントから 192.168.5.1 にアクセスすると、

```
TELNET 192.168.5.1 ↓
```

プロンプト「login:」が表示されます。

```
TELNET session now in ESTABLISHED state  
  
login:
```

7.3 TELNET コマンドの実行

本製品は、Telnet クライアントの機能を内蔵しているため、本製品から他の機器に対して Telnet を実行することができます。



コンピューターでマルチウインドウの Telnet が使える場合は、本製品にログインして「TELNET」コマンドを実行するよりは、コンピューターで複数の Telnet セッションを実行する方が便利です。

本製品に Manager レベルでログインし、「TELNET」コマンドを実行します。以下では、接続先の IP アドレスを「192.168.10.1」と仮定しています。実際には、お客様の環境におけるものをご使用ください。

```
Manager > TELNET 192.168.10.1 ↵
```

IP アドレスのホスト名を設定する

IP アドレスの代わりに分かりやすいホスト名を設定することができます。例えば、上記の例の IP アドレスのホスト名が「pearl」であると仮定すると、次のコマンドを入力します。

```
Manager > ADD IP HOST=pearl IP=192.168.10.1 ↵
```

ホスト名を使用して、Telnet を実行することができます。

```
Manager > TELNET pearl ↵
```

DNS サーバーを参照するように設定する

ホスト名から IP アドレスを得るために、DNS サーバーを参照するように設定することができます。DNS サーバーの IP アドレスが「192.168.10.200」とであると仮定すると、次のコマンドを入力します。

```
Manager > SET IP NAMESERVER=192.168.10.200 ↵

Info (133256): Attempting Telnet connection to
192.168.10.200, Please wait ....
TELNET session now in ESTABLISHED state

login:
```

ホスト名を使用して、Telnet を実行することができます。

```
Manager > TELNET spankfire.deilla.co.jp ↵
```

8.1 Ping

「PING」コマンドによって、指定した相手との通信が可能かどうかを確認することができます。PING は、指定した相手にエコーを要求するパケットを送信し、相手からの応答を表示します。

IP における例を下記に示します。PING に続けて IP アドレスを指定します。デフォルトの回数は5回です。

```
Manager > ping 192.168.10.32 ↓  
  
Echo reply 1 from 1192.168.10.32 time delay 1 ms  
  
Echo reply 2 from 1192.168.10.32 time delay 1 ms  
  
Echo reply 3 from 1192.168.10.32 time delay 1 ms  
  
Echo reply 4 from 1192.168.10.32 time delay 1 ms  
  
Echo reply 5 from 1192.168.10.32 time delay 1 ms
```

相手のみを指定して PING を打つと、発信元の IP アドレスとして送出インターフェースの IP アドレスが付加されます。これを防ぐためには明示的に発信元の IP を指定します。また、この明示的な IP はルーター内部に設定済みの IP でなければいけません。

```
Manager > ping 192.168.10.32  
sipa=192.168.1.1 ↓
```

PING に対する応答がある場合、「Echo reply 1 from xxxxxx time delay xx ms」のように表示されます。PING に対する応答がない場合、「Request 1 timed-out: No reply from xxxxxx」のように表示されます。「No route to specified destination」のように表示される場合、経路情報が未設定か、設定内容に誤りがあります。

「SET PING」コマンドにより、PING のオプションを設定することができます。「SHOW PING」コマンドにより、PING の設定情報を表示します。「STOP PING」コマンドにより、実行中の PING を中止します (PING はバックグラウンドで実行されます。PING の結果が次々に表示されている状態でも、コマンドの入力は可能です)。

8.2 Trace

「TRACE」コマンドによって、指定した相手までの実際の経路を表示することができます。

```
Manager > trace 192.168.80.121 ↓  
  
Trace from 192.168.28.128 to 192.168.80.121, 1-30 hops  
1. 192.168.48.32 0 13 20 (ms)  
2. 192.168.83.33 20 20 20 (ms)  
3. 192.168.80.121 ? 40 ? (ms)  
***  
Target reached
```

「SET TRACE」コマンドにより、TRACE のオプションを設定することができます。「SHOW TRACE」コマンドにより、TRACE の設定情報を表示します。「STOP TRACE」コマンドにより、実行中の TRACE を中止します (TRACE はバックグラウンドで実行されます。TRACE の結果が次々に表示されている状態でも、コマンドの入力は可能です)。

9 ファイルシステム

9.1 フラッシュメモリ・ファイルシステム

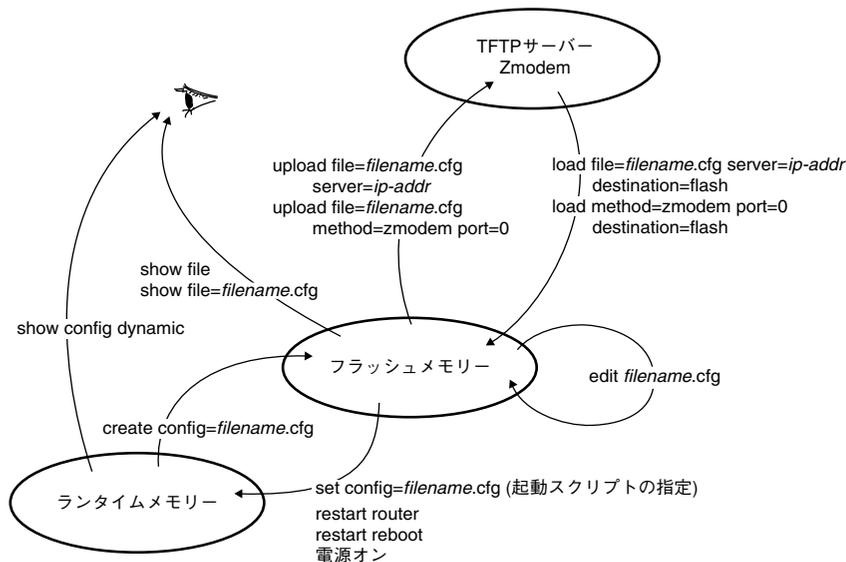


図9.1.1 設定ファイルに関するコマンド

本製品は、不揮発性メモリとして16MByteのフラッシュメモリ（FLASH）を内蔵しており、ファイルシステムとして15MByteが使用できます。フラッシュメモリは、コンピューターにおける起動ディスクのように振る舞います。電源をオンにすると、フラッシュメモリからファームウェアやパッチファイルをロードし、起動スクリプトファイル（.CFG）が指定されていれば、それもロードします。

「SHOW FILE」コマンドによって、フラッシュメモリに保存されているファイルの一覧を表示することができます。下記に例を示します（実際のファイル名は、お客様の環境、保存されているファームウェアなどのバージョンによって異なります）。

```
Manager > SHOW FILE ↓
```

Filename	Device	Size	Created	Locks
54-252.rez	flash	2394684	04-Mar-2003 14:23:25	0
c0a80164.dhc	flash	776	19-Apr-2002 19:58:46	0
config.ins	flash	32	26-Apr-2002 19:46:36	0
down.scp	flash	18	19-Apr-2002 19:59:32	0
feature.lic	flash	39	18-Feb-2002 15:38:26	0
fwmat.cfg	flash	3143	21-Apr-2002 11:20:54	0
help.hlp	flash	66957	11-Apr-2003 18:29:01	0
prefer.ins	flash	64	16-Apr-2002 08:14:18	0
release.lic	flash	32	18-Dec-2001 12:48:06	0
reset.scp	flash	13	19-Apr-2002 19:59:05	0
router.cfg	flash	3247	20-Apr-2002 19:14:05	0
up.scp	flash	19	19-Apr-2002 19:59:20	0

「SHOW FLASH」コマンドによって、フラッシュメモリの状態を表示することができます。

```
Manager > SHOW FLASH ↓
```

```
FFS info:
global operation ..... none
compaction count ..... 14
est compaction time ... 100 seconds
files ..... 2506692 bytes (15 files)
garbage ..... 47832 bytes
free ..... 13043044 bytes
required free block ... 131072 bytes
total ..... 15728640 bytes
```

```
diagnostic counters:
event      successes      failures
-----
get        0              0
open       0              0
read       9              0
close      7              0
complete   0              0
write      0              0
create     0              0
put        0              0
delete     0              0
check      1              0
erase      0              0
compact    0              0
verify     0              0
-----
```

フラッシュメモリーのコンパクション

「ACTIVATE FLASH COMPACTION」コマンドにより、フラッシュメモリーのコンパクション（ガベッジの除去）を行うことができます。

通常の運用であれば、このコマンドを使用する必要はほとんどありませんが、フラッシュメモリーは空いているはずなのに、ファイルがロードできないといった状況では、このコマンドを実行してみます。

```
Manager > ACTIVATE FLASH COMPACTION ↓  
Info (131260): Flash compacting...  
DO NOT restart the router until compaction is completed.
```

コンパクションは、バックグラウンドで実行されます。コンパクションが完了して、次のメッセージが表示されるまで、絶対に本製品の電源をオフにしたり、「RESTART」コマンドを実行しないでください（状況によっては、1～5分かかることがあります。）。

```
Manager >  
Info (131261): Flash compaction successfully completed.
```



コンパクション実行中に、絶対に本製品の電源をオフにしたり、「RESTART」コマンドを実行しないでください。リスタートや電源オフを行うと、ファイルシステムが破壊されます。

ファームウェアのバージョンアップなどで使用するセットアップツールは、ファームウェアなどの大きなファイルを削除したとき、自動的にこのコンパクションを実行します。

9.2 ファイル名

ファイル名は、次の形式で表されます。*filename* と *ext* はピリオドで結びます。ディレクトリー（フォルダー）の概念はありません。

```
filename.ext
```

filename

ファイル名（ベース名）。文字数は1～8文字。半角英数字とハイフン（-）が使えます。大文字・小文字の区別はありませんが、表示には大文字・小文字の区別が反映されます。

ext

拡張子。ファイル名には必ず拡張子をつけなければなりません。表9.2.1の拡張子が使用可能です。大文字・小文字の区別はありませんが、表示には大文字・小文字の区別が反映されます。

「UserDoc.CfG」のように大文字・小文字混ざりのファイルを作成することが可能です。しかしながら、大文字・小文字の属性は無視されるため、「UserDoc.CfG」が作成されていれば「userdoc.cfg」は作成できませんし、「userdoc.cfg」を指定すると「UserDoc.CfG」が対象となります。

EDIT コマンドは、CFG、SCP、TXT の拡張子を持つファイルを指定することができます。また、ファイルをロードする場合も、表9.2.1に挙げた拡張子のファイルのみが許されます。

表 9.2.1 使用可能な拡張子

拡張子	ファイルタイプ / 機能
REZ	本製品が起動するとき、ロードされるファームウェアの圧縮形式のファイル。
PAZ	ファームウェアに対するパッチの圧縮形式のファイル。ソフトウェアのバージョンによっては、インストールされていない場合もあります。
CFG	本製品の設定スクリプトファイル ^a 。「SCP」との間に明確な区別はありませんが、慣例として設定内容を保存するスクリプトには「CFG」を使います。
SCP	実行スクリプトファイル。「CFG」との間に明確な区別はありませんが、慣例としてトリガースクリプトやパッチファイル的なスクリプトには「SCP」を使います。
HLP	オンラインヘルプのファイルです。
LIC	ライセンスファイル。ファームウェア（リリース）や追加機能（フィーチャー）のライセンス情報を格納しているファイルです。絶対に削除しないでください。
INS	起動時に読み込むファームウェアや設定ファイルの情報を格納しているファイル。
DHC	DHCP サーバーの設定情報ファイル。DHCP サーバーに関する設定を行うと自動的に作成されます。
TXT	プレーンテキストファイル。

- a. CFG、SCP ファイルの内容において、「#」で始まる行は、コメントと見なされ無視されます。

表9.2.2 特別な役割を持つファイル

ファイル名	役割
boot.cfg	デフォルトの起動スクリプトファイル。「SET CONFIG」コマンドで起動スクリプトが設定されていない (none) 場合、本ファイルが存在していれば起動時に自動実行されます。起動スクリプトが設定されている場合は、設定されているファイルが実行されます。
config.ins	起動スクリプトファイルの情報を保存しているファイル。「SET CONFIG= <i>filename</i> .CFG」を実行すると作成 (上書き) されます。「SET CONFIG=NONE」を実行すると削除されます。
prefer.ins	起動時にロードするファームウェア、パッチファイルの情報を保存しています。
enabled.sec	セキュリティモードへ移行したときに自動的に作成されるファイル。システムに対し、起動時にセキュリティモードへ移行すべきことを示すファイルです。
random.rnd	IPsecなどの暗号化のためのテーブルとして自動的に作成されるファイル。内部処理のために使われるもので、ユーザーが意識する必要はありません。
release.lic	リリースライセンスファイル。ファームウェア (リリース) のライセンス情報を持つファイルです。削除しないでください。
feature.lic	フィーチャーライセンスファイル。追加機能 (フィーチャー) のライセンス情報を持つファイルです。削除しないでください。

9.3 ワイルドカード

ファイル进行操作する次のコマンドは、ワイルドカード (*) を使って複数のファイルを一度に指定できます。

- DELETE FILE コマンド
- SHOW FILE コマンド

ワイルドカード (*) は「任意の文字列」を示すもので、例えば下記はすべての設定スクリプトファイルを表示します。

```
Manager > SHOW FILE=*.*.cfg ↓
```

Filename	Device	Size	Created	Locks
52catv.cfg	flash	2199	08-May-2002 21:48:14	0
53perso.cfg	flash	3223	08-May-2002 22:00:07	0
55mulho.cfg	flash	3149	08-May-2002 22:36:19	0
telnet.cfg	flash	2324	26-Apr-2002 16:11:25	0
tokyo.cfg	flash	4511	09-May-2002 01:30:02	0
tokyo.scp	flash	2430	11-May-2002 21:45:06	0
x-y.cfg	flash	2276	11-May-2002 20:44:19	0
y-z.cfg	flash	2359	11-May-2002 21:46:33	0

filename 部分では「*string**」のような使い方ができます。ext 部分では、単独で適用します。例えば、下記は「t」で始まるファイルを表示します。ただし、*filename* 部分に対して「**string*」「*str*ing*」のような使い方はできません。

```
Manager > SHOW FILE=t*.* ↓
```

Filename	Device	Size	Created	Locks
test01.cfg	flash	2324	26-Apr-2002 16:11:25	0
tokyo.cfg	flash	4511	09-May-2002 01:30:02	0
tokyo.scp	flash	2430	11-May-2002 21:45:06	0

下記は、no で始まる scp ファイルのすべてを削除します。

```
Manager > DELETE FILE=no*.*.scp ↓
```



削除してしまったファイルの復旧はできません。「DELETE FILE=*.*」を使用してファイルを削除するとすべてのファイルが削除され、本体が起動できなくなります。ワイルドカードを使用したファイルの削除は、充分にご注意ください。

10 アップ/ダウンロード

本製品は、TFTP を使用して本製品のフラッシュメモリーと TFTP サーバー、または Zmodem を使用して本製品のフラッシュメモリーとコンソールターミナルの間で、設定スクリプトファイルなどの転送を行うことができます。



ファームウェア、パッチファイルなどは、アップロードできません。

本章では、TFTP、Zmodem を使用したファイル転送の方法について説明します。

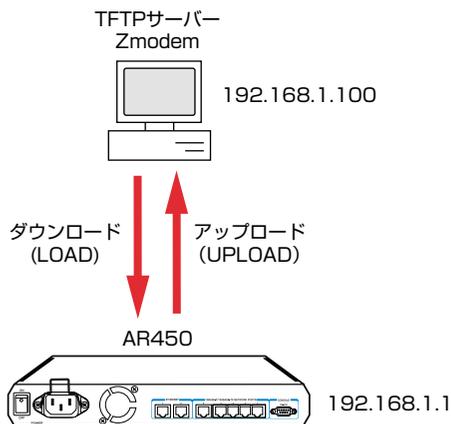


図 10.0.1 アップ/ダウンロード

10.1 TFTP

本製品は、TFTP クライアントの機能を内蔵しており、TFTP サーバーから本製品のフラッシュメモリーへのダウンロード、または本製品のフラッシュメモリーから TFTP サーバーへのアップロードが可能です。

本書「9 ファイルシステム」(p.63)

TFTP 機能を利用するためには、次のような設定が本製品に施されている必要があります。

```
Manager > ENABLE IP ↓  
Manager > ADD IP INT=vlan1 IP=192.168.1.1 ↓
```

以下の説明では、LAN 側インターフェース VLAN1 (192.168.1.1) に、TFTP サーバー (192.168.1.100) が直接接続されていると仮定します。

アップ/ダウンロードは、ノーマルモードの場合は Manager レベル、セキュリティーモードの場合は Security Officer レベルの権限が必要です。

ダウンロード

ダウンロードは、「LOAD」コマンドを使用します。次に、入力例を示します。ファイル名として「test01.cfg」を仮定しています。

```
Manager> LOAD FILE=test01.cfg  
SERVER=192.168.1.100  
DESTINATION=FLASH ↓  
  
Manager >  
Info (1048270): File transfer successfully completed.
```

きちんとダウンロードできたかは、「SHOW FILE」コマンドで確認できます。

TFTP サーバーによっては (UNIX 系 OS の tftpd など)、ファイルをダウンロードする際に、ファイル名の太文字・小文字を区別しますのでご注意ください。フラッシュメモリー上では太文字・小文字の区別はありませんが、表示には太文字・小文字の区別が反映されます。

TFTP では、ダウンロードするファイルと同名のファイルが、フラッシュメモリー上に存在する場合、ダウンロードできません。「DELETE FILE」コマンドでフラッシュメモリー上のファイルを削除してからダウンロードしてください。

アップロード

アップロードは、「UPLOAD」コマンドを使用します。次に、入力例を示します。ファイル名は、太文字・小文字を識別します。

```
Manager> UPLOAD FILE=test01.cfg  
SERVER=192.168.1.100 ↓  
  
Manager >  
Info (1048270): File transfer successfully completed.
```

TFTP サーバーによっては (UNIX 系 OS の tftpd など)、ファイルをアップロードする際に、TFTP サーバーでファイルのクリエイト (作成) ができないために、アップロードが失敗することがあります。そのような場合は、TFTP サーバーのディレクトリーに、あらかじめアップロードされるファイルと同じ名前のファイルを作成し、書き込める権限をあたえておいてください (UNIX 系 OS では、太文字・小文字を区別します)。

10.2 Zmodem

本製品は、Zmodem プロトコルを内蔵しており、コンソールポートに接続されているコンソールターミナルから本製品のフラッシュメモリーへのファイルのダウンロード、本製品のフラッシュメモリーからコンソールターミナルへのファイルのアップロードが可能です。

ここでは、通信ソフトウェアとして Windows 2000 のハイパーターミナルを使用する場合を説明します。

 本書「3.1 コンソールターミナルの設定」(p.27)

本書「9 ファイルシステム」(p.63)

ダウンロード

- 1 ハイパーターミナルを起動し、Manager レベルでログインしてください（セキュリティーモードの場合は、Security Officer レベルでログインしてください）。
- 2 ダウンロードは、「LOAD」コマンドを使用します。次に、入力例を示します。Zmodem によるダウンロードでは、フラッシュメモリー上に同名のファイルが存在する場合、上書きされずにコマンドはすぐに終了しますのでご注意ください。

```
Manager> LOAD METHOD=ZMODEM ASYN=0  
DESTINATION=FLASH _J
```

- 3 画面に「Router ready to begin ZMODEM file transfers ...」と表示されたら、ハイパーターミナルのメニューバーから「転送」→「ファイルの送信」を選択し、ファイルを指定します。
- 4 指定したファイルを再確認し、良ければ「送信」ボタンをクリックします。
- 5 画面に「Zmodem, session over.」と表示されたらダウンロードは完了です。
- 6 「SHOW FILE」コマンドで本製品にきちんとダウンロードできたことを確認してください。

アップロード

- 1 ハイパーターミナルを起動し、Manager モードでログインしてください（セキュリティーモードの場合は、Security Officer レベルでログインしてください）。
- 2 アップロードは、「UPLOAD」コマンドを使用します。次に、入力例を示します。

```
Manager> UPLOAD FILE=TOOS.cfg METHOD=ZMODEM  
ASYN=0 _J
```
- 3 ハイパーターミナルが自動的にファイル受信を開始します。
- 4 「File transfer successfully completed.」と表示されたら、アップロードは完了です。

11 バージョンアップ

弊社は、改良（機能拡張、バグフィクスなど）のために、予告なく本製品のソフトウェアのバージョンアップやパッチレベルアップを行うことがあります。この章では、最新ソフトウェアの入手方法について説明します。

11.1 必要なもの

本製品（AR450S）のバージョンアップには、次のものがが必要です。

- セットアップツール（ファームウェアインストーラー）
TFTPによりファームウェアなどのファイルを、本製品にダウンロードするツールです。付属CD-ROMに収録されています。
- 最新ファームウェアのソフトウェアセット
ファームウェア、パッチ、ヘルプファイルなどをまとめた圧縮ファイルで提供されます。弊社 Web ページからダウンロードできます。
- リリースノート
機能拡張、バグフィクス内容について説明した html ファイルです。重要な情報が記載されていますので、必ずご覧ください。
- バージョンアップ手順書
バージョンアップのしかたは、このファイルをご熟読ください。
- Windows 2000/Me/98/95、Windows NT が動作するコンピュータ
セットアップツールを実行します。

11.2 セットアップツール

セットアップツールは、本製品に対して以下の動作を自動的に行いません。

- 1 古いファイル（ファームウェア、パッチ、ヘルプ）の削除
- 2 ファイルのダウンロード（TFTP）
- 3 ファイルの有効化
ファームウェアは、本製品にダウンロードしただけでは動作しません。内部シリアル番号と認証キーにより、ライセンスを付与します。また、パッチ、ヘルプを有効化します。
- 4 本製品の再起動

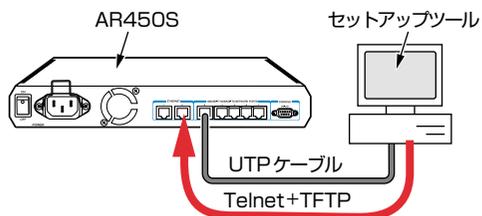


図 11.2.1 セットアップツール

11.3 最新ソフトウェアセットの入手方法

最新のソフトウェアセット（ファームウェアファイルやパッチファイル）は、弊社 Web ページから入手することができます。

<http://www.allied-telesis.co.jp/>

トップページから「サポート」へのリンクを選び、本製品のサポート情報を検索してください。

11.4 ファイルのバージョン表記

ファームウェアファイル

ファームウェアファイルのバージョンは、ピリオドで結んだ 3 桁の数字「*majer.minor.interim*」、例えば「2.5.3」のように表されます。「*majer*」はメジャーバージョン番号、「*minor*」はマイナーバージョン番号です。「*interim*」は、バグフィクスなどのために提供されていたパッチがファームウェアに反映された時点で加算されます。

ファームウェアは、「54-rrr.REL」または「54-rrr.REZ」というファイル名で提供されます。「54-」で始まり、「rrr」は「*majer.minor.interim*」からピリオドを取り除いた 3 桁の数値です。（例）

54-253.REZ

 本書「9 ファイルシステム」(p.63)

パッチファイル

ファームウェアに対する暫定的なバグフィクスのためにパッチファイルが使用されます。パッチファイルは、「54rrr-pp.PAT」または「54rrr-pp.PAZ」というファイル名で提供されます。「54-」で始まり、「rrr」はパッチの対象となるリリースのバージョン番号、「pp」はパッチ番号を示します。

パッチ番号は「01」から始まります。例えば「54-253.REZ」に対して、初めて提供されるパッチは下記ようになります。

(例)

```
54253-01.PAZ
```

最新のパッチファイルは、パッチ番号「01」からのバグフィクス内容のすべてを含む形式で提供されます(対象となるファームウェアに適用可能なパッチファイルはひとつだけです)。



本書「9 ファイルシステム」(p.63)

ソフトウェアセット

Web ページなどから提供される最新のソフトウェアセットは、自己解凍の圧縮ファイルとして提供されます。ソフトウェアセットに付与されるバージョン番号は、「*major.minor.interim PL pp*」のように表し、各数値は前述のファイルの項目に一致します。

(例)

```
Ver.2.5.3 PL 1
```

ソフトウェアセットにおける「*pp*」の10の桁の「0」は表記されません。「*pp*」が「0」である場合、キットにはファームウェアファイルだけが含まれており、パッチファイルは含まれていません。

ソフトウェアセットの圧縮ファイル名は、「ar54」で始まり、「*major.minor.interim*」「*pp*」を連結した exe 形式ファイルとなります。

(例)

```
ar542531.exe
```

12 困ったときに

本章では、本書内でご説明した内容に関するトラブル対策をご紹介します。うまく動かない、故障かな？困ったな、と思ったとき、サポートセンターへご連絡いただく前に、まず本章の内容をご確認ください。

12.1 トラブルへの対処法

お買い求め先、また弊社サポートセンターに連絡する前に、まず次のことをご確認ください。トラブル内容がどのようなことでも、以下は行っていただくようお願いいたします。

LEDの観察

本製品前面のLEDの状態を観察してください。LEDの状態は問題解決のため役立ちますので、問い合わせの前にLEDの状態（点灯、点滅、消灯など）を、ご確認していただきますようお願いいたします。LEDの状態については、下記に説明があります。

 本書「1.3 各部の名称と働き」(p.20)

●POWER LEDの観察

POWER LEDの消灯は、本製品に電源が供給されていないことを示しています。以下の点を確認してください。

- 電源スイッチは、オンになっているか
- 電源ケーブルは、本製品の電源コネクタに正しく接続されているか
- ACプラグは、電源コンセントに正しく接続されているか
- 電源コンセントには、電源が供給されているか

●SYSTEM LEDの観察

- 1 本製品の電源をオフにし、3～5秒ほど待ってオンにします。
- 2 コンソールターミナルが接続されていれば、起動が完了した時点で「login:」プロンプトが表示されます。

```
INFO: Self tests beginning.
INFO: RAM test beginning.
PASS: RAM test, 16384k bytes found.
INFO: Self tests complete.
INFO: Downloading router software.
Force EPROM download (Y) ?
INFO: Initial download successful.
INFO: Router startup complete

login:
```

- 3 SYSTEM LEDが赤く点灯し続けていたら、お買い求め先または弊社サポートセンターへご連絡ください。

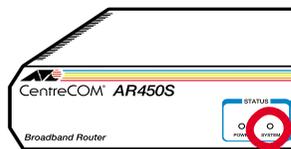


図 12.1.1 前面図

 本書「B.2 ユーザーサポート」(p.151)

●LINK LEDの観察

LINK LEDの消灯は、該当の10BASE-T/100BASE-TXポートに接続されている機器との通信ができないことを示しています。以下の点を確認してください。

- 接続先機器の電源は、オンになっているか
- UTPケーブルは、本製品と接続先機器に接続されているか
- 該当のポートに接続されているUTPケーブルを他のポートに接続してみる（他のポートでも消灯すれば、接続先機器側またはUTPケーブルの問題）
- 接続先機器側のLINK LEDは点灯しているか（LINK LEDは、本製品と接続先機器の両方にあり、両方が点灯していなければならない）
- UTPケーブルを接続先機器の他のポートに接続してみる（他のポートでも消灯すれば、本製品側またはUTPケーブルの問題）
- 正しいUTPケーブルを使用しているか（ストレートタイプのケーブルを使用し、100BASE-TXの場合はカテゴリ5以上、10BASE-Tの場合はカテゴリ3以上）
- 正常に接続できることが分かっている、他のUTPケーブルに交換してみる

本製品のログを見る

本製品が生成するログを見ることにより、原因を究明できることがあります。ログは、「SHOW LOG」コマンドで表示できます。

```

login: manager 
Password: _____ 

Manager > SHOW LOG 

Date/Time   S Mod Type  SType Message
-----
13 16:32:24 4 ENCO ENCO  PAC  1141 Encryption Processor Found.
13 16:32:24 4 ENCO ENCO  PAC  1141 Encryption Processor Initialised
13 16:32:24 4 ENCO ENCO  STAC  STAC SW Initialised
13 16:32:24 7 SYS  REST  NORM Router startup, ver 2.5.2-00, 17-Nov-2002, Clock
Log: 16:32:18 on 13-Apr-2003
13 16:32:24 6 FIRE FIRE  ENBLD 13-Apr-2003 16:32:24 Firewall enabled
13 16:32:25 3 LOG   FFSerr 20 opening file  \temp .ins
13 16:32:25 3 LOG   FFSerr 20 opening file  \default .ins
13 16:32:28 3 USER USER  LON   manager login on port0
13 16:34:32 5 PPP  INTER BDATT ppp0: PPPoE active discovery aborted.
13 16:35:04 3 TRG  BATCH ACT  Trigger 1 activated (Automatic)
13 16:37:12 5 PPP  INTER BDATT ppp0: PPPoE active discovery aborted.
13 16:38:04 3 TRG  BATCH ACT  Trigger 1 activated (Automatic)
13 16:38:05 3 PPP  VINT  UP    ppp0: Interface has come up and is able to send
and receive data
13 16:38:05 3 PPP  AUTH  OK    ppp0: CHAP authentication over eth0-any
succeeded
13 16:38:05 3 IPG  CIRC  CONF  Remote request to set ppp0 IP to 123.45.11.22
accepted
-----

```

図 12.1.2 ログの表示例

- 通信ソフトウェアのエンコードをシフトJIS (SJIS) に設定する (HELP コマンドは、シフトJIS で日本語を表示)



本書「3.1 コンソールターミナルの設定」(p.27)

本書「A.2 ハイパーターミナルの設定」(p.143)

- 入力モードは、英数半角モードになっているか (全角文字や半角カナは入力できない。Windows では、「Alt」キーを押しながら「半角/全角」キーを押して切り替える)

EDIT のトラブル

●「BackSpace」キーで文字が消せない

- 通信ソフトウェアの「BackSpace」キーのコードを Delete にする

- 「Delete」キーを使う



本書「3.1 コンソールターミナルの設定」(p.27)

本書「A.2 ハイパーターミナルの設定」(p.143)

本書「6 テキストエディター」(p.57)

●カーソルキーが利かない

- 通信ソフトウェアのエミュレーションをVT100 にする

●ハイパーターミナルで画面右の文字がスクロールしない

- 「Ctrl」キーを押しながら「W」キーを押して画面を再描画する

- Tera Term などの通信ソフトウェアを使用する

再起動したらプロバイダーに接続しない

- PPPoE による接続において、正しい手順による再起動、本製品の電源スイッチオフを行わなかった場合、しばらくの間プロバイダーとの接続ができなくなることがあります。数分～十数分待った後、接続状態を確認してみてください。



本書「再起動時のご注意」(p.32)

- PPPoE による接続において、PPP の接続が切断されていない状態で、設定スクリプトファイルを保存してしまった可能性があります。設定スクリプトファイルのトリガーの内容を確認してください。



本書「設定の保存はリンクダウンの状態」(p.135)

パスワードを忘れた

- パスワードを忘れてしまった場合、パスワードを初期状態に戻すために、センドバック修理を行うことになります。弊社サポート

12.2 トラブル例

コンソールターミナルに文字が入力できない

- コンソールケーブルは正しく接続されているか
- 本製品を再起動してみる
- 通信ソフトウェアを 2 つ以上同時に起動していないか (複数の通信ソフトウェアを同時に起動するとCOMポートで競合が発生し、通信できない、不安定になるなどの障害が発生)
- 通信ソフトウェアの設定内容は正しいか (特に、コンソールケーブルを接続しているCOMポート名と、通信ソフトウェアで設定しているCOMポート名は一致しているか)



本書「3.1 コンソールターミナルの設定」(p.27)

本書「A.2 ハイパーターミナルの設定」(p.143)

- 通信ソフトウェアのメニューなどで一度「切断」し、再度「接続」してみる
- 通信ソフトウェアを再起動してやってみる
- コンピューターの再起動からやってみる

コンソールターミナルで文字化けする

- 通信ソフトウェアの通信速度は9,600bps に設定してあるか (本製品のご購入時の設定は9,600bps)

センターにお問い合わせください。また、セキュリティーモードでご使用になっていた場合、修理により暗号鍵ファイルなどは削除されます。

 本書「B.2 ユーザーサポート」(p.151)

ライセンスを削除した

- RELEASE.LICはファームウェアに対して、FEATURE.LICはファィアウォールなどの拡張機能に対してライセンスを与えるファイルです。これらのファイルを削除してしまった場合、RELEASE.LICはバージョンアップツールでファームウェアをダウンロードすることにより復旧できますが、FEATURE.LICの復旧はセンドバックによる修理が必要です。詳細は、弊社サポートセンターにお問い合わせください。

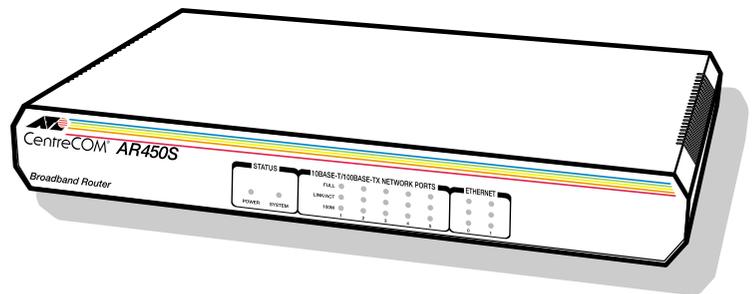
 本書「11 バージョンアップ」(p.69)

本書「9.2 ファイル名」(p.64)

本書「B.2 ユーザーサポート」(p.151)

第2部 設定例編

ここでは、本製品がよく使われる環境をいくつかとりあげ、その設定方法について解説します。



ここまでの章で、運用・管理に関することがらや、ソフトウェア的な内部構造について説明しました。本章では、よく使われまた便利な構成を挙げて、設定の要点を説明しつつ、必要なコマンド入力を示します。さらに高度な設定に進むための、はじめの一歩としてお読みください。

本章の構成は、下記のようになっています。まず、インターネット接続について、3例を説明します。

- 13.2 PPPoE による端末型インターネット接続 (p.78)
- 13.3 PPPoE による LAN 型インターネット接続 (アンナンバード) (p.83)
- 13.4 PPPoE による LAN 型インターネット接続 (DMZの設定) (p.88)

次に、IPsec を利用してセキュリティーを確保しながらインターネット経由で、複数の拠点における LAN を相互接続する方法を説明します。

- 13.5 インターネット接続による 2 点間 IPsec VPN (p.94)
- 13.6 インターネット接続による 3 点間 IPsec VPN (p.107)

そして、PPPoE のマルチセッションを用い、インターネット接続と、NTT 東日本のフレッツ・グループアクセスや NTT 西日本のフレッツ・グループなどの CUG サービスを同時に利用する方法を説明します。

- 13.7 インターネットと CUG サービスの同時接続 (端末型) (p.121)
- 13.8 インターネットと CUG サービスの同時接続 (LAN 型) (p.128)

最後に、PPPoE の自動接続を行うための設定の詳細と、注意事項など、知っておいていただきたい情報をまとめてあります。実際に設定を始める前にご覧ください。

- 13.9 設定上の注意事項 (p.135)
 - 「トリガーの動作」 (p.135)
 - 「設定の保存はリンクダウンの状態」 (p.135)
 - 「接続できないときは..」 (p.136)
 - 「PPPoEセッションの手動による切断」 (p.136)
 - 「再接続」 (p.137)
 - 「PPPoEにおけるアンナンバード」 (p.137)

13.1 設定をはじめの前に

コマンド入力における注意

下記にコマンドの入力例を示します。実際に入力する部分は、太文字で示します。「**J**」は、リターンキーまたはエンターキーです (本書では、リターンキーと表記します)。

紙面の都合により、コマンドを折り返す場合は、2 行目以降を字下げします。実際のコマンド入力では、字下げされている行の前にスペースひとつを入れ、「**J**」まで 1 行で入力してください。

(例)

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0  
NEXTHOP=0.0.0.0 J  
  
Info (1005275): IP route successfully added.
```

コマンド入力の便宜のために

入力の労力と間違いを減らすために、付属の CD-ROM にこの章で入力する全コマンドを収録したテキストファイルがあります。(¥SAMPLE¥450SAMP.TXT)

このファイルをご使用のコンピューターにコピーし、あらかじめテキストエディターでお客様固有の部分を修正した後、テキストエディターからコンソールターミナルに、コマンドをコピー&ペーストしてください。

一度に 1 行ずつコピー&ペーストし、表示されるメッセージを確認しながら進めるのが安全です。一度に全部の行をコピー&ペーストすると、バッファがあふれたり、メッセージが確認できないために、正常にコマンドが実行されたことが分かりません。

TFTP や Zmodem を使用して、直接本製品にダウンロードすることも可能ですが、実際に 1 行ずつコマンドを入力してみることをお勧めします。

13.2 PPPoE による端末型インターネット接続

続

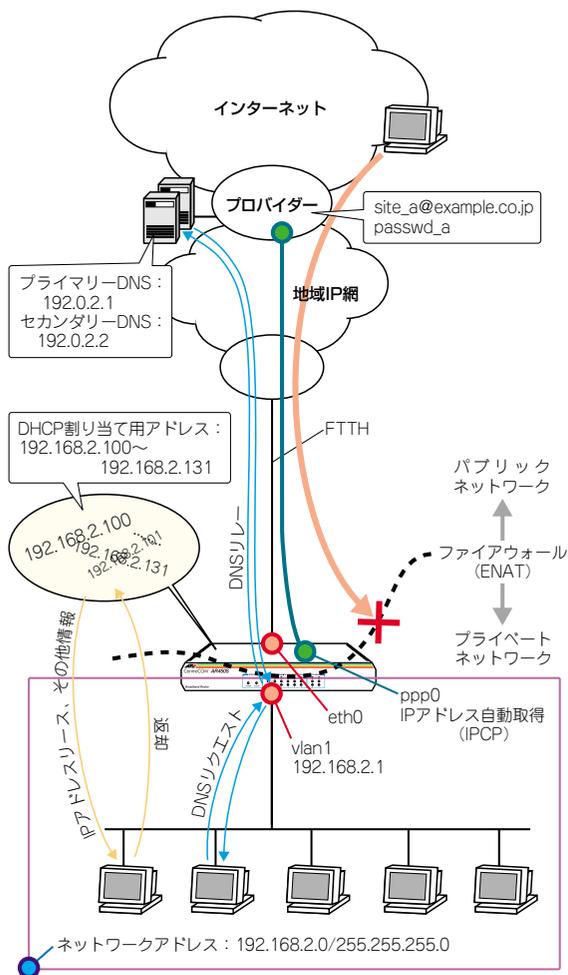


図 13.2.1 PPPoE による端末型の接続

PPPoE を使ってプロバイダーに接続します。PPPoE は、ADSL や FTTH などのいわゆる「ブロードバンド」系サービスで広く使用されているプロトコルです。この例は、接続するとき動的にアドレスを 1 つ割り当てられる端末型の基本設定です。

ダイナミック ENAT で 1 個のアドレスを共用し、ファイアウォールで外部からの不正アクセスを防止します。また、LAN 側クライアント

トの設定を簡単にするため、DNS リレーと DHCP サーバーも利用します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：1 個（動的割り当て）
- DNS サーバー：接続時に通知される

設定の方針

- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。
- ファイアウォールのダイナミック ENAT 機能を使用して、LAN 側ネットワークのプライベート IP アドレスを、プロバイダーから与えられたグローバル IP アドレスに変換します。これにより、LAN に接続された複数のコンピューターからインターネットへの同時アクセスが可能になります。
- トリガー機能を使って PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合に、自動的に再接続するよう設定します。
- 本製品の IP アドレスは、下記のように設定します。

表 13.2.1 本製品の基本設定

WAN 側物理インターフェース	eth0
WAN 側 (ppp0) IP アドレス	接続時にプロバイダーから取得する
LAN 側 (vlan1) IP アドレス	192.168.2.1/24
DHCP サーバー機能	有効

- 本製品を DHCP サーバーとして動作させ、LAN に接続されたコンピューターに IP アドレス、サブネットマスク、デフォルトゲートウェイ、DNS サーバーアドレスの情報を提供します。

表 13.2.2 本製品のDHCP サーバーの設定

DHCP ポリシー名	BASE
使用期限	7200 (秒)
サブネットマスク	255.255.255.0
デフォルトルート	192.168.2.1
DNS サーバー	192.168.2.1
DHCP レンジ名	LOCAL
提供する IP アドレスの範囲	192.168.2.100 ~ 192.168.2.131 (32 個)

- 本製品のDNS リレー機能をオンにして、LAN 側コンピューターからの DNS リクエストを、プロバイダーの DNS サーバーに転送します。上記 DHCP サーバーの設定により、LAN 側コンピューターに対しては、DNS サーバーアドレスとして本製品自身の IP アドレスを教えます。

設定

- 1 本製品の電源がオフの状態、本製品のWAN 側 (eth0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。
- 2 本製品の電源スイッチをオンにします。
- 3 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager ↵
Password: friend (表示されません)
```

● PPP の設定

- 4 WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵
Info (1003003): Operation successful.
```

- 5 プロバイダーから通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの

機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=site_a@example.co.jp
PASSWORD=passwd_a LQR=OFF ECHO=ON ↵
Info (1003003): Operation successful.
```

● IP、ルーティングの設定

- 6 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵
Info (1005287): IP module has been enabled.
```

- 7 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するよう設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵
Info (1005287): Remote IP assignment has been enabled.
```

- 8 LAN 側 (vlan1) インターフェースに IP アドレスを設定します。

```
Manager > ADD IP INT=vlan1 IP=192.168.2.1
MASK=255.255.255.0 ↵
Info (1005275): interface successfully added.
```

- 9 WAN 側 (ppp0) インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↵
Info (1005275): interface successfully added.
```

- 10 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
NEXTHop=0.0.0.0 ↵
Info (1005275): IP route successfully added.
```

● DNS リレーの設定

- 11 DNS リレー機能を有効にします。

```
Manager > ENABLE IP DNSRELAY ↵
Info (1005003): Operation successful.
```

- 12 DNSリレーの中継先を指定します。通常、中継先にはDNSサーバーのアドレスを指定しますが、IPCPによりアドレスを取得するまでは不明であるため、ここではインターフェース名を指定します。

```
Manager > SET IP DNSRELAY INT=ppp0 ↵  
Info (1005003): Operation successful.
```

●ファイアウォールの設定

- 13 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↵  
Info (1077257): 19-Apr-2002 19:55:22  
Firewall enabled.  
Info (1077003): Operation successful.
```

- 14 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↵  
Info (1077003): Operation successful.
```

- 15 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。^{*1}

```
Manager > ENABLE FIREWALL POLICY=net  
ICMP F=PING,UNREACH ↵  
Info (1077003): Operation successful.
```

- 16 本製品の ident プロキシ機能を無効にし、外部のメール (SMTP) サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager > DISABLE FIREWALL POLICY=net  
IDENTPROXY ↵  
Info (1077003): Operation successful.
```

 *1 デフォルト設定では、ICMPはファイアウォールを通過できません。

- 17 ファイアウォールポリシーの適用対象となるインターフェースを指定します。LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1  
TYPE=PRIVATE ↵  
Info (1077003): Operation successful.
```

WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0  
TYPE=PUBLIC ↵  
Info (1077003): Operation successful.
```

- 18 LAN 側ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるように設定します。グローバルアドレスには、ppp0 の IP アドレスを使用します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED  
INT=vlan1 GBLINT=ppp0 ↵  
Info (1077003): Operation successful.
```

●DHCP サーバーの設定

- 19 LAN 側コンピューター (DHCP クライアント) のために、DHCP サーバー機能を有効にします。

```
Manager > ENABLE DHCP ↵  
Info (1070003): Operation successful.
```

- 20 DHCP ポリシー「BASE」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。IP アドレスの使用期限は 7,200 秒 (2 時間) とします。

```
Manager > CREATE DHCP POLICY=BASE  
LEASETIME=7200 ↵  
Info (1070003): Operation successful.
```

- 21 DHCP クライアントに提供する情報を設定します。ここでは、DNS サーバーアドレスとして、本製品の LAN 側インターフェースの IP アドレスを指定しています。

```
Manager > ADD DHCP POLICY=BASE  
SUBNET=255.255.255.0 ROUTER=192.168.2.1  
DNSSERVER=192.168.2.1 ↵  
Info (1070003): Operation successful.
```

- 22 DHCPのレンジ「LOCAL」を作成し、DHCPクライアントに提供するIPアドレスの範囲を設定します。レンジの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE DHCP RANGE=LOCAL POLICY=BASE
IP=192.168.2.100 NUMBER=32 ↵

Info (1070003): Operation successful.
```

●トリガーの設定

- 23 PPPoEセッションを自動再接続するためのトリガースクリプトを作成します。
ppp0をリセットするスクリプトreset.scpを作成します。

```
Manager > ADD SCRIPT=reset.scp TEXT="RESET
PPP=0" ↵

File : reset.scp

1:RESET PPP=0
```

トリガー1を無効状態にするスクリプトup.scpを作成します。

```
Manager > ADD SCRIPT=up.scp TEXT="DISABLE
TRIGGER=1" ↵

File : up.scp

1:DISABLE TRIGGER=1
```

トリガー1を有効状態にするスクリプトdown.scpを作成します。

```
Manager > ADD SCRIPT=down.scp TEXT="ENABLE
TRIGGER=1" ↵

File : down.scp

1:ENABLE TRIGGER=1
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド（内蔵フルスクリーンエディター）などを使って設定スクリプトファイル（.CFG）にこのコマンドを記述しても意図した結果になりません。

- 24 トリガー機能を有効にします。

```
Manager > ENABLE TRIGGER ↵

Info (1053268): The trigger module has been enabled.
```

- 25 ppp0Eセッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順23で設定したそれぞれのトリガースクリプトを実行します。

reset.scpを実行する定期トリガー1を作成します。このトリガーは、ppp0インターフェースがダウンすると同時に有効になり、3分間隔で実行され、アップすると無効になります。

```
Manager > CREATE TRIGGER=1 PERIODIC=3
SCRIPT=reset.scp ↵

Info (1053262): Trigger successfully added.
```

ppp0のアップ時にup.scpを実行するインターフェーストリガー2を作成します。

```
Manager > CREATE TRIGGER=2 INTERFACE=ppp0
EVENT=UP CP=IPCP SCRIPT=up.scp ↵

Info (1053262): Trigger successfully added.
```

ppp0のダウン時にdown.scpを実行するインターフェーストリガー3を作成します。

```
Manager > CREATE TRIGGER=3 INTERFACE=ppp0
EVENT=DOWN CP=IPCP SCRIPT=down.scp ↵

Info (1053262): Trigger successfully added.
```

 参照 本書「トリガーの動作」(p.135)

●時刻、パスワード、設定保存

- 26 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=21-APR-2002 ↵

System time is 01:00:01 on Sunday 21-Apr-2002.
```

- 27 ユーザー「manager」のパスワードを変更します。Confirm:の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↵

Old password: friend ↵
New password: xxxxxxxx ↵
Confirm: xxxxxxxx ↵
```

28 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↓
Info (1049003): Operation successful.
```

29 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↓
Info (1049003): Operation successful.
```

30 WAN 側 (eth0) インターフェースに UTP ケーブルを接続してください。

●接続の確認

31 PPP の接続の確認は、「SHOW PPP」コマンドで確認できます。トリガー 1 は 3 分間隔で実行されるので、UTP ケーブルを接続してから、PPP の接続確立まで最長 3 分かかります（ご契約のプロバイダー側の機器によっては更に数分かかることがあります）。「SHOW PPP」コマンドを繰り返し入力しながら、State が「CLOSED」から「OPENED」に変わるまで待ってください。

```
Manager > SHOW PPP ↓

Name          Enabled ifIndex Over          CP          State
-----
ppp0          YES     04          eth0-any    IPCP        OPENED
              LCP        OPENED
```

また、「SHOW INT」コマンドでは、全インターフェースの状態を確認できます。

```
Manager > SHOW INT ↓

Interfaces                               sysUpTime:      01:26:55
DynamicLinkTraps.....Disabled
TrapLimit.....20

Number of unencrypted PPP/FR links.....1

ifIndex Interface  ifAdminStatus  ifOperStatus  ifLastChange
-----
1   eth0    Up             Up             01:17:13
3   vlan1  Up             Up             00:00:01
4   ppp0    Up             Up             01:17:35
.....
```

32 PPP 接続時にプロバイダーから取得した IP アドレスなどの情報は、「SHOW PPP CONFIG」コマンドによって確認できます。

```
Manager > SHOW PPP CONFIG ↓

Interface - description
Parameter          Configured          Negotiated
-----
ppp0 -
.....
.....
eth0-any
.....
.....
IP
IP Compression Protocol  NONE          NONE          WJC
IP Pool                  NOT SET
IP Address Request       ON
IP Address               123.45.11.22  123.45.11.22  123.45.67.1
Primary DNS Address      87.65.43.21   87.65.43.21   NONE
Secondary DNS Address    87.65.43.22   87.65.43.22   NONE
Primary WinS Address     NOT SET
Secondary WinS Address   NOT SET
PPPoE
Session ID              B1CC          B1CC
MAC Address of Peer     00-90-99-0a-0a-04
Service Name            any
Debug
Maximum packet bytes to display  32
-----
```

33 LAN 側のコンピューターで Web ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合（DHCP クライアントである場合）、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

まとめ

前述の設定手順を実行することによって、作成、保存されるスクリプトファイルを示します。

表 13.2.3 設定スクリプトファイル (ROUTER.CFG)

```
1 CREATE PPP=0 OVER=eth0-any
2 SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON
  USER=site_a@example.co.jp PASSWORD=passwd_a
  LQR=OFF ECHO=ON
3 ENABLE IP
4 ENABLE IP REMOTEASSIGN
5 ADD IP INT=vlan1 IP=192.168.2.1
  MASK=255.255.255.0
6 ADD IP INT=ppp0 IP=0.0.0.0
7 ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
8 ENABLE IP DNSRELAY
9 SET IP DNSRELAY INT=ppp0
```

表 13.2.3 設定スクリプトファイル (ROUTER.CFG)

```

10  ENABLE FIREWALL
11  CREATE FIREWALL POLICY=net
12  ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
13  DISABLE FIREWALL POLICY=net IDENTPROXY
14  ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
15  ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
16  ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1
    GBLINT=ppp0
17  ENABLE DHCP
18  CREATE DHCP POLICY=BASE LEASETIME=7200
19  ADD DHCP POLICY=BASE SUBNET=255.255.255.0
    ROUTER=192.168.2.1 DNSSERVER=192.168.2.1
20  CREATE DHCP RANGE=LOCAL POLICY=BASE
    IP=192.168.2.100 NUMBER=32
21  ENABLE TRIGGER
22  CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
23  CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP
    CP=IPCP SCRIPT=up.scp
24  CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN
    CP=IPCP SCRIPT=down.scp

```

「SET TIME」、 「ADD SCRIPT」 コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

表 13.2.4 スクリプト [reset.scp]

```

RESET PPP=0

```

表 13.2.5 スクリプト [up.scp]

```

DISABLE TRIGGER=1

```

表 13.2.6 スクリプト [down.scp]

```

ENABLE TRIGGER=1

```

13.3 PPPoE による LAN 型インターネット接続 (アンナンバード)

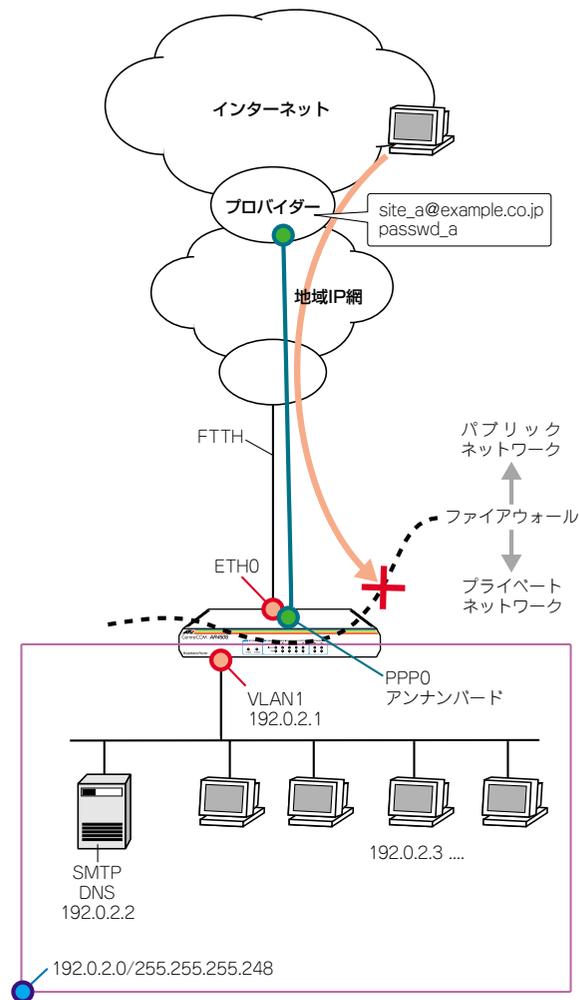


図 13.3.1 PPPoE による LAN 型の接続 (LAN 側グローバル)

PPPoE を使ってプロバイダーに接続します。グローバルアドレスを 8 個、16 個などのブロック単位で固定的に割り当てられる LAN 型接続の設定例です。

この例では、NAT を使用せず、LAN 側端末にグローバルアドレスを直接割り当てます。また、ファイアウォールを使って外部からのアクセスを原則拒否しつつ、特定のサーバーだけを外部に公開します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- 使用できる IP アドレス：192.0.2.0/29(192.0.2.0～192.0.2.7)

設定の方針

- LAN 側端末はすべてグローバルアドレスで運用します。NATは使用しません。プロバイダーから割り当てられているアドレスは 8 個ですが、ネットワークアドレス (192.0.2.0)、ブロードキャストアドレス(192.0.2.7)、ルーター自身のアドレス(192.0.2.1)にそれぞれ 1 個ずつ消費されるため、端末に設定できるアドレスは 192.0.2.2～192.0.2.6 の 5 個となります。
- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。
- 外部からのアクセスは基本的にすべて遮断しますが、次のサービスだけは特例として許可します。
 - SMTP サーバー：192.0.2.2：25/tcp
 - DNS サーバー：192.0.2.2：53/tcp、53/udp
- トリガー機能を使って PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合に、自動的に再接続するよう設定します。
- 本製品の基本設定は、次の通りです。

表 13.3.1 本製品の基本設定

WAN 側物理インターフェース	eth0
WAN 側 (ppp0) IP アドレス	アンナンバード
LAN 側 (VLAN1) IP アドレス	192.0.2.1/24
DHCP サーバー機能	使わない

設定

- 1 本製品の電源がオフの状態では、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。

- 2 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager ↵
Password: friend (表示されません)
```

● PPP の設定

- 3 WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵
Info (1003003): Operation successful.
```

- 4 プロバイダーから通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=site_a@example.co.jp
PASSWORD=passwd_a LQR=OFF ECHO=ON ↵
Info (1003003): Operation successful.
```

アンナンバードによる WAN 側インターフェースに関しては下記の項もご覧ください。



本書「PPPoE におけるアンナンバード」(p.137)

● IP、ルーティングの設定

- 5 IP モジュールを有効にします。

```
Manager > ENABLE IP ↵
Info (1005287): IP module has been enabled.
```

- 6 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するよう設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵
Info (1005287): Remote IP assignment has been enabled.
```

- 7 LAN 側 (vlan1) インターフェースに ISP から割り当てられたグローバルアドレスの先頭アドレス (192.0.2.1) を設定します。アドレスを 8 個や 16 個といった単位で割り当てられる場合は、ネットマスクが変則的になるので注意してください。

```
Manager > ADD IP INT=vlan1 IP=192.0.2.1  
MASK=255.255.255.248 ↓
```

```
Info (1005275): interface successfully added.
```

- 8 WAN 側 (ppp0) インターフェースをアンナンバードに設定します。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↓
```

```
Info (1005275): interface successfully added.
```

- 9 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0  
NEXTHop=0.0.0.0 ↓
```

```
Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

- 10 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↓
```

```
Info (1077257): 19-Apr-2002 19:55:22  
Firewall enabled.
```

```
Info (1077003): Operation successful.
```

- 11 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↓
```

```
Info (1077003): Operation successful.
```

- 12 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。^{*2}

```
Manager > ENABLE FIREWALL POLICY=net  
ICMP_F=PING,UNREACH ↓
```

```
Info (1077003): Operation successful.
```

- 13 外部のメール (SMTP) サーバーなどからの ident 要求に対して、本製品が内部のサーバーの代わりに応答する、ident プロキシ機能がデフォルトで有効になっています。そこで、内部のサーバー自身が応答できるように、ident プロキシ機能を無効にします。

```
Manager > DISABLE FIREWALL POLICY=net  
IDENTPROXY ↓
```

```
Info (1077003): Operation successful.
```

- 14 ファイアウォールポリシーの適用対象となる インターフェースを指定します。

LAN 側 (VLAN1) インターフェースを PRIVATE (内部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=VLAN1  
TYPE=PRIVATE ↓
```

```
Info (1077003): Operation successful.
```

WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0  
TYPE=PUBLIC ↓
```

```
Info (1077003): Operation successful.
```

- 15 外部からのパケットをすべて拒否するファイアウォールの基本ルールに対し、DMZ のサーバーへパケットを通すための設定を行います。

SMTP サーバー (192.0.2.2 の TCP25 番) へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=1  
AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.2  
PORT=25 ↓
```

```
Info (1077003): Operation successful.
```



*2 デフォルト設定では、ICMP はファイアウォールを通過できません。

DNS サーバー (192.0.2.2 の TCP*3 と UDP の 53 番) へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=2
AC=ALLOW INT=ppp0-0 PROTO=TCP IP=192.0.2.2
PORT=53 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager > ADD FIREWALL POLICY=net RULE=2
AC=ALLOW INT=ppp0-0 PROTO=UDP IP=192.0.2.2
PORT=53 ↓
```

```
Info (1077003): Operation successful.
```

●トリガーの設定

16 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。

ppp0 をリセットするスクリプト reset.scp を作成します。

```
Manager > ADD SCRIPT=reset.scp TEXT="RESET
PPP=0" ↓
```

```
File : reset.scp
```

```
1:RESET PPP=0
```

トリガー 1 を無効状態にするスクリプト up.scp を作成します。

```
Manager > ADD SCRIPT=up.scp TEXT="DISABLE
TRIGGER=1" ↓
```

```
File : up.scp
```

```
1:DISABLE TRIGGER=1
```

トリガー 1 を有効状態にするスクリプト down.scp を作成します。

```
Manager > ADD SCRIPT=down.scp TEXT="ENABLE
TRIGGER=1" ↓
```

```
File : down.scp
```

```
1:ENABLE TRIGGER=1
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド (内蔵フルスクリーンエディター) などを使って設定スクリプトファイル (.CFG) にこのコマンドを記述しても意図した結果になりません。

17 トリガー機能を有効にします。

```
Manager > ENABLE TRIGGER ↓
```

```
Info (1053268): The trigger module has been enabled.
```

18 ppp0E セッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順 16 で設定したそれぞれのトリガースクリプトを実行します。

reset.scp を実行する定期トリガー 1 を作成します。このトリガーは、ppp0 インターフェースがダウンすると同時に有効になり、3 分間隔で実行され、アップすると無効になります。

```
Manager > CREATE TRIGGER=1 PERIODIC=3
SCRIPT=reset.scp ↓
```

```
Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up.scp を実行するインターフェーストリガー 2 を作成します。

```
Manager > CREATE TRIGGER=2 INTERFACE=ppp0
EVENT=UP CP=IPCP SCRIPT=up.scp ↓
```

```
Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down.scp を実行するインターフェーストリガー 3 を作成します。

```
Manager > CREATE TRIGGER=3 INTERFACE=ppp0
EVENT=DOWN CP=IPCP SCRIPT=down.scp ↓
```

```
Info (1053262): Trigger successfully added.
```



本書「トリガーの動作」(p.135)

●時刻、パスワード、設定保存

19 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=21-APR-2002 ↓
```

```
System time is 01:00:01 on Sunday 21-Apr-2002.
```

20 ユーザー「manager」のパスワードを変更します。Confirm : の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↓
```

```
Old password: friend ↓
New password: xxxxxxxx ↓
Confirm: xxxxxxxx ↓
```



*3 セカンダリー DNS サーバーからのアクセスで TCP が使用されます。

- 21 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↓
Info (1049003): Operation successful.
```

- 22 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↓
Info (1049003): Operation successful.
```

- 23 WAN 側 (eth0) インターフェースに UTP ケーブルを接続してください。

●接続の確認

- 24 PPP の接続の確認は、「SHOW PPP」コマンドで確認できます。トリガー 1 は 3 分間隔で実行されるので、UTP ケーブルを接続してから、PPP の接続確立まで最長 3 分かかります（ご契約のプロバイダー側の機器によっては更に数分かかることがあります）。「SHOW PPP」コマンドを繰り返し入力しながら、State が「CLOSED」から「OPENED」に変わるまで待ってください。

```
Manager > SHOW PPP ↓

Name          Enabled ifIndex Over          CP          State
-----
ppp0          YES     04          eth0-any    IPCP        OPENED
              LCP        OPENED
```

また、「SHOW INT」コマンドでは、全インターフェースの状態を確認できます。

```
Manager > SHOW INT ↓

Interfaces          sysUpTime:      01:26:55
DynamicLinkTraps....Disabled
TrapLimit.....20

Number of unencrypted PPP/FR links.....1

ifIndex Interface  ifAdminStatus  ifOperStatus  ifLastChange
-----
1   eth0      Up             Up             01:17:13
3   vlan1    Up             Up             00:00:01
4   ppp0     Up             Up             01:17:35
.....
```

- 25 PPP 接続時にプロバイダーから取得した IP アドレスなどの情報は、「SHOW PPP CONFIG」コマンドによって確認できます。

```
Manager > SHOW PPP CONFIG ↓

Interface - description
Parameter          Configured          Negotiated
-----
ppp0 -
.....
.....
eth0-any
.....
.....
IP
IP Compression Protocol  NONE          NONE          VJC
IP Pool                  NOT SET
IP Address Request       ON
IP Address              123.45.11.22   123.45.11.22   123.45.67.1
Primary DNS Address      87.65.43.21    87.65.43.21    NONE
Secondary DNS Address    87.65.43.22    87.65.43.22    NONE
Primary WinS Address     NOT SET
Secondary WinS Address   NOT SET
PPPoE
Session ID              B1CC          B1CC
MAC Address of Peer      00-90-99-0a-0a-04
Service Name            any
Debug
Maximum packet bytes to display  32
```

- 26 LAN 側のコンピューターで Web ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合（DHCP クライアントである場合）、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 13.3.2 設定スクリプトファイル (ROUTER.CFG)

```
1 CREATE PPP=0 OVER=eth0-any
2 SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON
  USER=site_a@example.co.jp PASSWORD=passwd_a
  LQR=OFF ECHO=ON
3 ENABLE IP
4 ENABLE IP REMOTEASSIGN
5 ADD IP INT=VLAN1 IP=192.0.2.1
  MASK=255.255.255.248
6 ADD IP INT=ppp0 IP=0.0.0.0
7 ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
8 ENABLE FIREWALL
9 CREATE FIREWALL POLICY=net
```

表 13.3.2 設定スクリプトファイル (ROUTER.CFG)

```

10  ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
11  DISABLE FIREWALL POLICY=net IDENTPROXY
12  ADD FIREWALL POLICY=net INT=VLAN1 TYPE=PRIVATE
13  ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
14  ADD FIREWALL POLICY=net RULE=1 AC=ALLOW
    INT=ppp0 PROTO=TCP IP=192.0.2.2 PORT=25
15  ADD FIREWALL POLICY=net RULE=2 AC=ALLOW
    INT=ppp0 PROTO=TCP IP=192.0.2.2 PORT=53
16  ADD FIREWALL POLICY=net RULE=3 AC=ALLOW
    INT=ppp0 PROTO=UDP IP=192.0.2.2 PORT=53
17  ENABLE TRIGGER
18  CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
19  CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP
    CP=IPCP SCRIPT=up.scp
20  CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN
    CP=IPCP SCRIPT=down.scp

```

「SET TIME」、「ADD SCRIPT」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

表 13.3.3 スクリプト「reset.scp」

```

RESET PPP=0

```

表 13.3.4 スクリプト「up.scp」

```

DISABLE TRIGGER=1

```

表 13.3.5 スクリプト「down.scp」

```

ENABLE TRIGGER=1

```

13.4 PPPoE による LAN 型インターネット接続 (DMZ の設定)

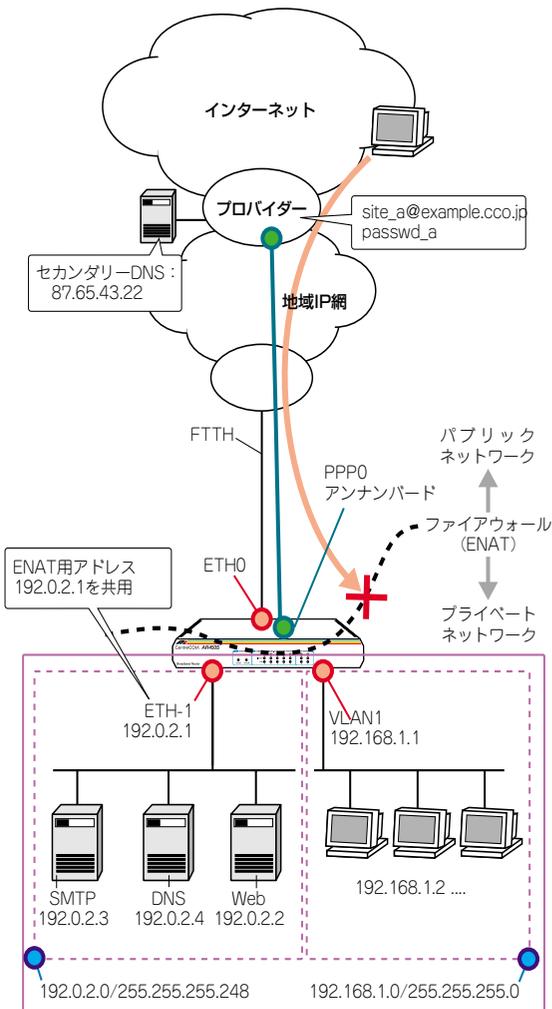


図 13.4.1 PPPoE による LAN 型の接続 (DMZ)

PPPoE を使ってプロバイダーに接続します。グローバルアドレスを 8 個、16 個などのブロック単位で固定的に割り当てられる LAN 型接続の設定例です。

この例では、LAN 側を 2 つのサブネットに分割し、一方をグローバルアドレスで運用するサーバー用 (DMZ)、もう一方をプライベートアドレスで運用するクライアント用とします。クライアントはダイナミック ENAT 経由でインターネットにアクセスします。また、ファ

ファイアウォールを使って外部からのアクセスを原則拒否しつつ、特定のサーバーだけを外部に公開します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

- 接続のユーザー名: site_a@example.co.jp
- 接続のパスワード: passwd_a
- PPPoE サービス名: 指定なし
- 使用できるIP アドレス: 192.0.2.0/29 (192.0.2.0 ~ 192.0.2.7)

設定の方針

- LAN 側を vlan1 と eth1 の 2 つのサブネットに分割し、eth1 にはプロバイダーから割り当てられたグローバルアドレスを、vlan1 にはプライベートアドレスを割り当てます。グローバルサブネットは DMZ としてサーバーを配置し、プライベートサブネットにはクライアントを配置します。
- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。
- 外部からのアクセスは基本的にすべて遮断しますが、次のサービスだけは特例として許可します。
 - Web サーバー: 192.0.2.2 : 80/tcp
 - SMTP サーバー: 192.0.2.3 : 25/tcp
 - DNS サーバー: 192.0.2.4 : 53/tcp, 53/udp
- プライベートサブネットのクライアントがインターネットにアクセスできるよう、ダイナミックENAT を使用します。グローバルアドレスには、eth1 に割り当てたアドレス (192.0.2.1) を共用します。
- トリガー機能を使って PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合に、自動的に再接続するよう設定します。

- 本製品の基本設定は、次の通りです。

表 13.4.1 本製品の基本設定

WAN 側物理インターフェース	eth0
WAN 側 (ppp0) IP アドレス	アンナンバード
DMZ 側 (eth1) IP アドレス	192.0.2.1/29
LAN 側 (vlan1) IP アドレス	192.168.1.1/24
DHCP サーバー機能	使わない

設定

- 1 本製品の電源がオフの状態で、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。
- 2 本製品の電源スイッチをオンにします。
- 3 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager ]
Password: friend (表示されません)
```

● PPP の設定

- 4 WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ]
Info (1003003): Operation successful.
```

- 5 プロバイダーから通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=site_a@example.co.jp
PASSWORD=passwd_a LQR=OFF ECHO=ON ]
Info (1003003): Operation successful.
```

アンナンバードによるWAN側インターフェースに関しては下記の項もご覧ください。

 本書「PPPoEにおけるアンナンバード」(p.137)

● IP、ルーティングの設定

6 IP モジュールを有効にします。

```
Manager > ENABLE IP ↓  
Info (1005287): IP module has been enabled.
```

7 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するよう設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↓  
Info (1005287): Remote IP assignment has been enabled.
```

8 DMZ 側 (eth1) インターフェースにプロバイダーから割り当てられたグローバルアドレスの先頭アドレス (192.0.2.1) を設定します。アドレスを 8 個や 16 個といった単位で割り当てられる場合は、ネットマスクが変則的になるので注意してください。

```
Manager > ADD IP INT=eth1 IP=192.0.2.1  
MASK=255.255.255.248 ↓  
Info (1005275): interface successfully added.
```

9 LAN 側 (vlan1) インターフェースにプライベート IP アドレスを割り当て、クライアント用のサブネットとします。

```
Manager > ADD IP INT=vlan1 IP=192.168.1.1  
MASK=255.255.255.0 ↓  
Info (1005275): interface successfully added.
```

10 WAN 側 (ppp0) インターフェースをアンナンバードに設定します。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↓  
Info (1005275): interface successfully added.
```

11 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0  
NEXTHOP=0.0.0.0 ↓  
Info (1005275): IP route successfully added.
```

●ファイアウォールの設定

12 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↓  
Info (1077257): 19-Apr-2002 19:55:22  
Firewall enabled.  
Info (1077003): Operation successful.
```

13 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↓  
Info (1077003): Operation successful.
```

14 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。^{*4}

```
Manager > ENABLE FIREWALL POLICY=net  
ICMP_F=PING,UNREACH ↓  
Info (1077003): Operation successful.
```

15 外部のメール(SMTP) サーバーなどからの ident 要求に対して、本製品が内部のサーバーの代わりに応答する、ident プロキシ機能がデフォルトで有効になっています。そこで、内部のサーバー自身が応答できるように、ident プロキシ機能を無効にします。

```
Manager > DISABLE FIREWALL POLICY=net  
IDENTPROXY ↓  
Info (1077003): Operation successful.
```

16 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

DMZ 側 (eth1) インターフェースを PRIVATE (内部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=eth1  
TYPE=PRIVATE ↓  
Info (1077003): Operation successful.
```



^{*4} デフォルト設定では、ICMP はファイアウォールを通過できません。

LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1
TYPE=PRIVATE ↵
Info (1077003): Operation successful.
```

WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0
TYPE=PUBLIC ↵
Info (1077003): Operation successful.
```

- 17 LAN 側 (vlan1) ネットワークに接続されているすべてのコンピュータが ENAT 機能を使用できるように設定します。グローバルアドレスには 192.0.2.1 を共用します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
INT=vlan1 GBLINT=ppp0 GBLIP=192.0.2.1 ↵
Info (1077003): Operation successful.
```

- 18 外部からのパケットをすべて拒否するファイアウォールの基本ルールに対し、DMZ のサーバーへパケットを通すための設定を行います。

Web サーバー (192.0.2.5 の TCP80 番) へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=1
AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.2
PORT=80 ↵
Info (1077003): Operation successful.
```

SMTP サーバー (192.0.2.4 の TCP25 番) へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=2
AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.3
PORT=25 ↵
Info (1077003): Operation successful.
```

DNS サーバー (192.0.2.4 の TCP*⁵ と UDP の 53 番) へのパケットは通過させます。

```
Manager > ADD FIREWALL POLICY=net RULE=3
AC=ALLOW INT=ppp0 PROTO=TCP IP=192.0.2.4
PORT=53 ↵
Info (1077003): Operation successful.

Manager > ADD FIREWALL POLICY=net RULE=4
AC=ALLOW INT=ppp0 PROTO=UDP IP=192.0.2.4
PORT=53 ↵
Info (1077003): Operation successful.
```

●トリガーの設定

- 19 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。
ppp0 をリセットするスクリプト reset.scp を作成します。

```
Manager > ADD SCRIPT=reset.scp TEXT="RESET
PPP=0" ↵
File : reset.scp
1:RESET PPP=0
```

トリガー 1 を無効状態にするスクリプト up.scp を作成します。

```
Manager > ADD SCRIPT=up.scp TEXT="DISABLE
TRIGGER=1" ↵
File : up.scp
1:DISABLE TRIGGER=1
```

トリガー 1 を有効状態にするスクリプト down.scp を作成します。

```
Manager > ADD SCRIPT=down.scp TEXT="ENABLE
TRIGGER=1" ↵
File : down.scp
1:ENABLE TRIGGER=1
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド (内蔵フルスクリーンエディター) などを使って設定スクリプトファイル (.CFG) にこのコマンドを記述しても意図した結果になりません。



*5 セカンダリー DNS サーバーからのアクセスで TCP が使用されます。

20 トリガー機能を有効にします。

```
Manager > ENABLE TRIGGER ↓  
Info (1053268): The trigger module has been enabled.
```

21 ppp0E セッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順 19 で設定したそれぞれのトリガースクリプトを実行します。

reset.scp を実行する定期トリガー 1 を作成します。このトリガーは、ppp0 インターフェースがダウンすると同時に有効になり、3分間隔で実行され、アップすると無効になります。

```
Manager > CREATE TRIGGER=1 PERIODIC=3  
SCRIPT=reset.scp ↓  
Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up.scp を実行するインターフェーストリガー 2 を作成します。

```
Manager > CREATE TRIGGER=2 INTERFACE=ppp0  
EVENT=UP CP=IPCP SCRIPT=up.scp ↓  
Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down.scp を実行するインターフェーストリガー 3 を作成します。

```
Manager > CREATE TRIGGER=3 INTERFACE=ppp0  
EVENT=DOWN CP=IPCP SCRIPT=down.scp ↓  
Info (1053262): Trigger successfully added.
```

 本書「トリガーの動作」(p.135)

●時刻、パスワード、設定保存

22 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=21-APR-2002 ↓  
System time is 01:00:01 on Sunday 21-Apr-2002.
```

23 ユーザー「manager」のパスワードを変更します。Confirm : の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↓  
Old password: friend ↓  
New password: xxxxxxxx ↓  
Confirm: xxxxxxxx ↓
```

24 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↓  
Info (1049003): Operation successful.
```

25 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↓  
Info (1049003): Operation successful.
```

26 WAN 側 (eth0) インターフェースに UTP ケーブルを接続してください。

●接続の確認

27 PPP の接続の確立は、「SHOW PPP」コマンドで確認できます。トリガー 1 は 3 分間隔で実行されるので、UTP ケーブルを接続してから、PPP の接続確立まで最長 3 分かかります（ご契約のプロバイダー側の機器によっては更に数分かかることがあります）。「SHOW PPP」コマンドを繰り返し入力しながら、State が「CLOSED」から「OPENED」に変わるまで待ってください。

```
Manager > SHOW PPP ↓  


| Name | Enabled | ifIndex | Over     | CP          | State            |
|------|---------|---------|----------|-------------|------------------|
| ppp0 | YES     | 04      | eth0-any | IPCP<br>LCP | OPENED<br>OPENED |


```

また、「SHOW INT」コマンドでは、全インターフェースの状態を確認できます。

```
Manager > SHOW INT ↓  


| ifIndex | Interface | ifAdminStatus | ifOperStatus | ifLastChange |
|---------|-----------|---------------|--------------|--------------|
| 1       | eth0      | Up            | Up           | 01:17:13     |
| 3       | vlan1     | Up            | Up           | 00:00:01     |
| 4       | ppp0      | Up            | Up           | 01:17:35     |


```

28 PPP接続時にプロバイダーから取得したIPアドレスなどの情報は、「SHOW PPP CONFIG」コマンドによって確認できます。

```

Manager > SHOW PPP CONFIG ↓

```

Interface - description Parameter	Configured	Negotiated	

ppp0 -		Local	Peer
.....		
.....		
eth0-any			
.....		
.....		
IP			
IP Compression Protocol	NONE	NONE	VJC
IP Pool	NOT SET		
IP Address Request	ON		
IP Address	123.45.11.22	123.45.11.22	123.45.67.1
Primary DNS Address	87.65.43.21	87.65.43.21	NONE
Secondary DNS Address	87.65.43.22	87.65.43.22	NONE
Primary WinS Address	NOT SET		NONE
Secondary WinS Address	NOT SET		NONE
PPPoE			
Session ID		B1CC	B1CC
MAC Address of Peer		00-90-99-0a-0a-04	
Service Name	any		
Debug			
Maximum packet bytes to display	32		

29 LAN側のコンピューターでWebブラウザなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN側のコンピューターがIPアドレスを自動取得するように設定されている場合（DHCPクライアントである場合）、本製品のDHCPサーバー機能を設定した後に、コンピューターを起動（または再起動）する必要があります。

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 13.4.2 設定スクリプトファイル (ROUTER.CFG)

```

1 CREATE PPP=0 OVER=eth0-any
2 SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON
  USER=site_a@example.co.jp PASSWORD=passwd_a
  LQR=OFF ECHO=ON
3 ENABLE IP
4 ENABLE IP REMOTEASSIGN
5 ADD IP INT=eth1 IP=192.0.2.1
  MASK=255.255.255.248
6 ADD IP INT=vlan1 IP=192.168.1.1
  MASK=255.255.255.0
7 ADD IP INT=ppp0 IP=0.0.0.0
8 ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0

```

表 13.4.3 設定スクリプトファイル (ROUTER.CFG)

```

9 ENABLE FIREWALL
10 CREATE FIREWALL POLICY=net
11 ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
12 DISABLE FIREWALL POLICY=net IDENTPROXY
13 ADD FIREWALL POLICY=net INT=eth1 TYPE=PRIVATE
14 ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
15 ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
16 ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1
  GBLINT=ppp0 GBLIP=192.0.2.1
17 ADD FIREWALL POLICY=net RULE=1 AC=ALLOW
  INT=ppp0 PROTO=TCP IP=192.0.2.2 PORT=80
18 ADD FIREWALL POLICY=net RULE=2 AC=ALLOW
  INT=ppp0 PROTO=TCP IP=192.0.2.3 PORT=25
19 ADD FIREWALL POLICY=net RULE=3 AC=ALLOW
  INT=ppp0 PROTO=TCP IP=192.0.2.4 PORT=53
20 ADD FIREWALL POLICY=net RULE=4 AC=ALLOW
  INT=ppp0 PROTO=UDP IP=192.0.2.4 PORT=53
21 ENABLE TRIGGER
22 CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
23 CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP
  CP=IPCP SCRIPT=up.scp
24 CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN
  CP=IPCP SCRIPT=down.scp

```

「SET TIME」、「ADD SCRIPT」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

表 13.4.4 スクリプト「reset.scp」

```
RESET PPP=0
```

表 13.4.5 スクリプト「up.scp」

```
DISABLE TRIGGER=1
```

表 13.4.6 スクリプト「down.scp」

```
ENABLE TRIGGER=1
```

13.5 インターネット接続による2点間IPsec VPN

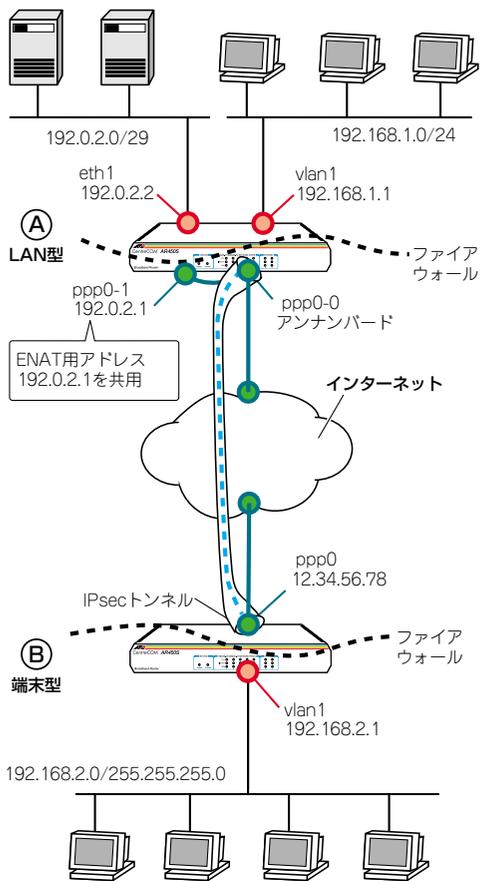


図 13.5.1 IPsec による接続

PPPoE でインターネットに接続している 2 つの拠点を、IPsec で接続しデータの安全性を確保します。

この例では、以下の 2 拠点間の接続を、トンネルモード (ESP) で暗号化します。

- グローバルアドレス 8 個を固定的に割り当てられている拠点 A
- グローバルアドレス 1 個を固定的に割り当てられている拠点 B

上記の組み合わせ以外に対しても、本設定例中の IPsec 部分の適用は可能ですが、最低限一方の IP アドレスが固定である必要があります。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●拠点 A

- 接続のユーザー名: site_a@example.co.jp
- 接続のパスワード: passwd_a
- PPPoE サービス名: 指定なし
- IP アドレス グローバルアドレス: 192.0.2.0/29 (8 個固定)
- DNS サーバー: 接続時に通知される

●拠点 B

- 接続のユーザー名: site_b@example.co.jp
- 接続のパスワード: passswd_b
- PPPoE サービス名: 指定なし
- IP アドレス グローバルアドレス: 12.34.56.78/32 (1 個固定)
- DNS サーバー: 接続時に通知される

設定の方針

●インターネット接続設定

- グローバルアドレス 8 個をもつ拠点 A のルーターでは、グローバルサブネット (eth1) にサーバーを、プライベートサブネット (vln1) にクライアントを配置します。また、WAN 側 (ppp0) インターフェースをマルチホーミングし、そのうちの一方 (ppp0-1) にグローバルアドレスの 1 つを設定します。拠点 A のルーターが送信する IPsec パケットの始点アドレスにはこのアドレスがセットされます。このような設定をするのは、PPPoE の LAN 型接続では WAN 側 (ppp0) インターフェースにネットワークアドレス (ホスト部が 0 のアドレスが始点アドレスとしては使用できないため事実上のアンナナバード) が割り当てられるためです

- グローバルアドレスが 1 個しかない拠点 B のルーターでは、WAN 側 (ppp0) インターフェースにグローバルアドレスを設定したダイナミック ENAT による、通常の端末型を使用します。このグローバルアドレスが IPsec パケットの始点アドレスとしてセットされます。

- トリガー機能を使って PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合に、自動的に再接続するよう設定します。

表 13.5.1 インターネット接続設定

	拠点 A	拠点 B
WAN 側物理インターフェース	eth0	eth0
WAN 側 IP アドレス (1)	Unnumbered (ppp0-0)	12.34.56.78/32 (ppp0)
WAN 側 IP アドレス (2)	192.0.2.1/32 (ppp0-1)	-
LAN 側 IP アドレス	192.168.1.1/24 (vlan1)	192.168.2.1/24 (vlan1)
DMZ 側 IP アドレス	192.0.2.2/29 (eth1)	-

● VPN 設定

- IPsec トンネルは、A の ppp0-1 と B の ppp0 の間に張られません。このトンネルはプライベートLAN 間を接続するためのもので、IP のパケットを暗号化して通します。
- ファイアウォールの設定においては、IPsec 関連のパケット (IKE、ESP) を除く外部からの不正アクセスを遮断し、内部からは自由にインターネットへのアクセスができるようにします。
- トンネリング対象のパケットに NAT が適用されないようルールを設定します。

表 13.5.2 IKE フェーズ 1 (ISAKMP SA のネゴシエーション)

本製品間の認証方式	事前共有鍵 (pre-shared key)
IKE 交換モード	Main モード
事前共有鍵	secret (文字列)
Oakley グループ	1 (デフォルト)
ISAKMP メッセージの暗号化方式	DES (デフォルト)
ISAKMP メッセージの認証方式	SHA1 (デフォルト)
ISAKMP SA の有効期限 (時間)	86400 秒 (24 時間) (デフォルト)
ISAKMP SA の有効期限 (Kbyte 数)	なし (デフォルト)
起動時の ISAKMP ネゴシエーション	行わない

表 13.5.1 IKE フェーズ 2 (IPsec SA のネゴシエーション)

SA モード	トンネルモード
セキュリティプロトコル	ESP (暗号 + 認証)
暗号化方式	DES
認証方式	SHA1

表 13.5.1 IKE フェーズ 2 (IPsec SA のネゴシエーション)

IPComp	使わない
IPsec SA の有効期限 (時間)	28800 秒 (8 時間) (デフォルト)
IPsec SA の有効期限 (Kbyte 数)	なし (デフォルト)
IPsec の適用対象 IP アドレス	192.168.10.0/24 ⇔ 192.168.20.0/24
トンネル終端アドレス	192.0.2.1 ⇔ 12.34.56.78
インターネットとの平文通信	行なう

拠点 A の設定

- 本製品の電源がオフの状態で、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。
- 本製品の電源スイッチをオンにします。
- ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager J
Password: friend (表示されません)
```

- 管理をしやすくするために、本製品にシステム名を設定します。サイト A には「A」を設定します。

```
Manager > SET SYSTEM NAME=A J
Info (1034003): Operation successful.
Manager A>
```

- IPsec はセキュリティモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officer レベルのユーザーを登録しておきます。Security Officer のパスワードは厳重に管理してください。ここでは、ユーザー名「secoff」、パスワード「passwdSA」を仮定します。

```
Manager A> ADD USER=secoff PASSWORD=passwdSA
PRIVILEGE=SECURITYOFFICER J
User Authentication Database
-----
Username: secoff ()
Status: enabled Privilege: Sec Off Telnet: no Login: yes
Logins: 0 Fails: 0 Sent: 0 Rcvd: 0
Authentications: 0 Fails: 0
-----
```

● PPP の設定

- 6 WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager A> CREATE PPP=0 OVER=eth0-any ↵  
Info (1003003): Operation successful.
```

- 7 プロバイダーから通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
Manager A> SET PPP=0 OVER=eth0-any BAP=OFF  
IPREQUEST=ON USER=site_a@example.co.jp  
PASSWORD=passwd_a LQR=OFF ECHO=ON ↵  
Info (1003003): Operation successful.
```

● IP、ルーティングの設定

- 8 IP モジュールを有効にします。

```
Manager A> ENABLE IP ↵  
Info (1005287): IP module has been enabled.
```

- 9 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するよう設定します。

```
Manager A> ENABLE IP REMOTEASSIGN ↵  
Info (1005287): Remote IP assignment has been enabled.
```

- 10 DMZ 側 (eth1) インターフェースにプロバイダーから割り当てられたグローバルアドレスのうちの 1 つ 192.0.2.2 を設定します。アドレスを 8 個や 16 個といった単位で割り当てられる場合は、ネットマスクが変則的になるので注意してください。

```
Manager A> ADD IP INT=eth1 IP=192.0.2.2  
MASK=255.255.255.248 ↵  
Info (1005275): interface successfully added.
```

- 11 LAN 側 (vlan1) インターフェースにプライベート IP アドレスを割り当て、クライアント用のサブネットとします。

```
Manager A> ADD IP INT=vlan1 IP=192.168.1.1  
MASK=255.255.255.0 ↵  
Info (1005275): interface successfully added.
```

- 12 WAN 側 (ppp0) インターフェースをマルチホーミングし、ppp0-0 をアンナナバードに設定します。

```
Manager A> ADD IP INT=ppp0-0 IP=0.0.0.0 ↵  
Info (1005275): interface successfully added.
```

- 13 WAN 側 (ppp0-1) インターフェースにプロバイダーから割り当てられたグローバルアドレスの先頭アドレス (192.0.2.1) を 32 ビットマスクで割り当てます。デフォルトルートがこのインターフェースに向けることで、IPsec パケットの始点アドレスとしてこのアドレスが使われるようにします

```
Manager A> ADD IP INT=ppp0-1 IP=192.0.2.1  
MASK=255.255.255.255 ↵  
Info (1005275): interface successfully added.
```

- 14 デフォルトルートを ppp0-1 に向けて設定します。これは、ルーター A が送信する IPsec パケットの始点アドレスとして、ppp0-1 のアドレスが使われるようにするためです (通常、本製品自身がパケットを送信するときは、送出インターフェースのアドレスを始点アドレスとして使います)。

```
Manager A> ADD IP ROUTE=0.0.0.0 INT=ppp0-1  
NEXTHOP=0.0.0.0 ↵  
Info (1005275): IP route successfully added.
```

- 15 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。
ppp0 をリセットするスクリプト reset.scp を作成します。

```
Manager A> ADD SCRIPT=reset.scp TEXT="RESET  
PPP=0" ↵  
File : reset.scp  
1:RESET PPP=0
```

トリガー 1 を無効状態にするスクリプト up.scp を作成します。

```
Manager A> ADD SCRIPT=up.scp TEXT="DISABLE TRIGGER=1" ↓  
  
File : up.scp  
1:DISABLE TRIGGER=1
```

トリガー 1 を有効状態にするスクリプト down.scp を作成します。

```
Manager A> ADD SCRIPT=down.scp TEXT="ENABLE TRIGGER=1" ↓  
  
File : down.scp  
1:ENABLE TRIGGER=1
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド（内蔵フルスクリーンエディター）などを使って設定スクリプトファイル（.CFG）にこのコマンドを記述しても意図した結果になりません。

16 トリガー機能を有効にします。

```
Manager A> ENABLE TRIGGER ↓  
  
Info (1053268): The trigger module has been enabled.
```

- 17 PPPoE セッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順 15 で設定したそれぞれのトリガースクリプトを実行します。reset.scp を実行する定期トリガー 1 を作成します。このトリガーは、ppp0 インターフェイスがダウンすると同時に有効になり、3 分間隔で実行され、アップすると無効になります。

```
Manager A> CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp ↓  
  
Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up.scp を実行するインターフェーストリガー 2 を作成します。

```
Manager A> CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp ↓  
  
Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down.scp を実行するインターフェーストリガー 3 を作成します。

```
Manager A> CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp ↓  
  
Info (1053262): Trigger successfully added.
```

 本書「トリガーの動作」(p.135)

●ファイアウォールの設定

- 18 ファイアウォール機能を有効にします。

```
Manager A> ENABLE FIREWALL ↓  
  
Info (1077257): 19-Apr-2002 19:55:22 Firewall enabled.  
Info (1077003): Operation successful.
```

- 19 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager A> CREATE FIREWALL POLICY=net ↓  
  
Info (1077003): Operation successful.
```

- 20 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。^{*6}

```
Manager A> ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH ↓  
  
Info (1077003): Operation successful.
```

- 21 外部のメール (SMTP) サーバーなどからの ident 要求に対して、本製品が内部のサーバーの代わりに応答する、ident プロキシ機能がデフォルトで有効になっています。そこで、内部のサーバー自身が応答できるように、ident プロキシ機能を無効にします。

```
Manager A> DISABLE FIREWALL POLICY=net IDENTPROXY ↓  
  
Info (1077003): Operation successful.
```

- 22 ファイアウォールポリシーの適用対象となるインターフェースを指定します。



^{*6} デフォルト設定では、ICMP はファイアウォールを通過できません。

DMZ 側 (eth1) インターフェースを PRIVATE (内部) に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=eth1
TYPE=PRIVATE ↓
```

```
Info (1077003): Operation successful.
```

LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=vlan1
TYPE=PRIVATE ↓
```

```
Info (1077003): Operation successful.
```

WAN 側 (ppp0-1) インターフェースを PUBLIC (外部) に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp0-1
TYPE=PUBLIC ↓
```

```
Info (1077003): Operation successful.
```

WAN 側 (ppp0-1) インターフェースを PUBLIC (外部) に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp0-1
TYPE=PUBLIC ↓
```

```
Info (1077003): Operation successful.
```

23 LAN 側 (vlan1) ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるように設定します。グローバルアドレスには ppp0-1 に割り当てた 192.0.2.1 を共用します。

```
Manager A> ADD FIREWALL POLICY=net
NAT=ENHANCED INT=vlan1 GBLINT=ppp0-1
GBLIP=192.0.2.1 ↓
```

```
Info (1077003): Operation successful.
```

24 外部からのパケットをすべて拒否するファイアウォールの基本ルールに対し、DMZ のサーバーへパケットを通すための設定を行います。

Web サーバー (192.0.2.3 の TCP80 番) へのパケットは通過させます。

```
Manager A> ADD FIREWALL POLICY=net RULE=1
AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.3
PORT=80 ↓
```

```
Info (1077003): Operation successful.
```

SMTTP サーバー (192.0.2.4 の TCP25 番) へのパケットは通過させます。

```
Manager A> ADD FIREWALL POLICY=net RULE=2
AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4
PORT=25 ↓
```

```
Info (1077003): Operation successful.
```

DNS サーバー (192.0.2.4 の TCP^{*7} と UDP の 53 番) へのパケットは通過させます。

```
Manager A> ADD FIREWALL POLICY=net RULE=3
AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4
PORT=53 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager A> ADD FIREWALL POLICY=net RULE=4
AC=ALLOW INT=ppp0-1 PROTO=UDP IP=192.0.2.4
PORT=53 ↓
```

```
Info (1077003): Operation successful.
```

25 接続相手からの IKE パケット (UDP500 番) がファイアウォールを通過できるように設定します。

```
Manager A> ADD FIREWALL POLICY=net RU=5
AC=ALLOW INT=ppp0-1 PROTO=UDP GBLPO=500
GBLIP=192.0.2.1 PO=500 IP=192.0.2.1 ↓
```

```
Info (1077003): Operation successful.
```

26 ローカル LAN からリモート LAN へのパケットには NAT をかけないように設定します。

```
Manager A> ADD FIREWALL POLICY=net RU=6
AC=NONAT INT=vlan1 PROT=ALL
IP=192.168.1.1-192.168.1.254 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager A> SET FIREWALL POLICY=net RU=6
REMOTEIP=192.168.2.1-192.168.2.254 ↓
```

```
Info (1077003): Operation successful.
```

27 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点 IP アドレス」



*7 セカンダリー DNS サーバーからのアクセスで TCP が使用されます。

スが 192.168.1.1 ~ 192.168.1.254、つまりローカル LAN 例ならば、NAT の対象外とする」の意味になります。

```
Manager A> ADD FIREWALL POLICY=net RU=7
AC=NONAT INT=ppp0-1 PROT=ALL
IP=192.168.1.1-192.168.1.254 ENCAP=IPSEC 』
Info (1077003): Operation successful.
```

● IPsec の設定

- 28 ここからが IPsec の設定になります。最初に ISAKMP 用の事前共有鍵 (pre-shared key) を作成します。ここでは鍵番号を 1 番とし、鍵の値は「secret」という文字列で指定します (拠点 B のルーターも同じ番号に設定)。

```
Manager A> CREATE ENCO KEY=1 TYPE=GENERAL
VALUE="secret" 』
Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル (.CFG) に、このコマンドを記述しても無効になります。

なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では、ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

- 29 接続相手との IKE ネゴシエーション要求を受け入れる ISAKMP ポリシー「i」を作成します。KEY には、前の手順で作成した事前共有鍵 (鍵番号 1) を、PEER には拠点 B のルーターの IP アドレスを指定します。

```
Manager A> CREATE ISAKMP POLICY="i"
PEER=192.0.2.1 KEY=1 SENDN=TRUE 』
Info (1082003): Operation successful.
```

- 30 IPsec 通信の仕様を定義する SA スペック 1 を作成します。トンネルモード (デフォルト)、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager A> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
PROTOCOL=ESP ENCALG=DES HASHALG=SHA 』
Info (1081003): Operation successful.
```

- 31 SA スペック 1 だけからなる SA バンドルスペック 1 を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager A> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
STRING="1" 』
Info (1081003): Operation successful.
```

- 32 ISAKMP メッセージを素通しさせる IPsec ポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの 500 番ポートからリモートの 500 番ポート宛の UDP パケット (ISAKMP) に設定します。

```
Manager A> CREATE IPSEC POLICY="isa"
INT=ppp0-1 ACTION=PERMIT LPORT=500
RPORT=500 TRANSPORT=UDP 』
Info (1081003): Operation successful.
```

ISAKMP を使用する場合は、必ず最初の IPsec ポリシーで ISAKMP メッセージが通過できるような設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドの POSITION パラメーターを使用します。

- 33 実際の IPsec 通信に使用する IPsec ポリシー「vpn」を PPP0-1 に対して作成します。鍵管理方式「ISAKMP」、PEER には拠点 B のルーターの IP アドレスを、BUNDLE には SA バンドルスペック「1」を指定します。

```
Manager A> CREATE IPSEC POLICY="vpn" INT=ppp0-1
ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
PEER=12.34.56.78 』
Info (1081003): Operation successful.
```

- 34 IPsec ポリシー「vpn」に対して実際に IPsec 通信を行なう IP アドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

```
Manager A> SET IPSEC POLICY="vpn"
LAD=192.168.1.0 LMA=255.255.255.0
RAD=192.168.2.0 RMA=255.255.255.0 』
Info (1081003): Operation successful.
```

- 35 インターネットへの平文通信を許可する IPsec ポリシー「inet」を PPP0-1 に対して作成します。

```
Manager A> CREATE IPSEC POLICY="inet"  
INT=ppp0-1 ACTION=PERMIT ↓
```

```
Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後の IPsec ポリシーで、すべてのパケットを通過させるための上記の設定を行ってください。どの IPsec ポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、設定がないと VPN 以外との通信ができなくなります。

- 36 IPsec モジュールを有効にします。

```
Manager A> ENABLE IPSEC ↓
```

```
Info (1081003): Operation successful.
```

- 37 ISAKMP モジュールを有効にします。

```
Manager A> ENABLE ISAKMP ↓
```

```
Info (1082057): ISAKMP has been enabled.
```

- 38 Security Officer レベルのユーザーでログインしなおします。

```
Manager A> LOGIN secoff ↓
```

```
Password: passwdSA
```

- 39 動作モードをセキュリティーモードに切り替えます。

```
SecOff A> ENABLE SYSTEM SECURITY_MODE ↓
```

```
Info (1034003): Operation successful.
```

セキュリティーモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO (Remote Security Officer) の設定を行っておいてください。



本書「5.4 ノーマルモード / セキュリティーモード」
(p.54)

●設定の保存

- 40 WAN 側インターフェースの UTP ケーブルが抜けているのを確認し、設定を保存します。

```
SecOff A> CREATE CONFIG=ROUTER.CFG ↓
```

```
Info (1049003): Operation successful.
```

もし、ケーブルが刺さっていた場合は、ケーブルを抜き「SHOW PPP」コマンドで、接続が切断されているのを確認してから保存します。

- 41 保存したファイルを起動時設定ファイルに指定します。

```
SecOff A> SET CONFIG=ROUTER.CFG ↓
```

```
Info (1049003): Operation successful.
```

拠点 B の設定

- 1 本製品の電源がオフの状態、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。

- 2 本製品の電源スイッチをオンにします。

- 3 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager ↓  
Password: friend (表示されません)
```

- 4 管理をしやすくするために、本製品にシステム名を設定します。サイト B には「B」を設定します。

```
Manager > SET SYSTEM NAME=B ↓
```

```
Info (1034003): Operation successful.
```

```
Manager B>
```

- 5 IPsecはセキュリティーモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officer レベルのユーザーを登録しておきます。Security Officer のパスワードは厳重に管理してください。

ここでは、ユーザー名「secoff」、パスワード「passwdSB」を仮定します。

```
Manager B> ADD USER=secoff PASSWORD=passwdSB
PRIVILEGE=SECURITYOFFICER ↓

User Authentication Database
-----
Username: secoff ()
Status: enabled   Privilege: Sec Off   Telnet: no   Login: yes
Logins: 0         Fails: 0         Sent: 0      Rcvd: 0
Authentications: 0 Fails: 0
```

● PPP の設定

- 6 WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager B> CREATE PPP=0 OVER=eth0-any ↓

Info (1003003): Operation successful.
```

- 7 プロバイダーから通知された PPP ユーザー名とパスワードを設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
Manager B> SET PPP=0 OVER=eth0-any BAP=OFF
USER=site_b@example.co.jp PASS-
WORD=passwd_b LQR=OFF ECHO=ON ↓

Info (1003003): Operation successful.
```

● IP、ルーティングの設定

- 8 IP モジュールを有効にします。

```
Manager B> ENABLE IP ↓

Info (1005287): IP module has been enabled.
```

- 9 LAN 側 (vlan1) インターフェースにプライベート IP アドレスを割り当て、クライアント用のサブネットとします。

```
Manager B> ADD IP INT=vlan1 IP=192.168.2.1
MASK=255.255.255.0 ↓

Info (1005275): interface successfully added.
```

- 10 WAN 側 (ppp0) インターフェースにプロバイダーから割り当てられた IP アドレスを設定します。

```
Manager B> ADD IP INT=ppp0 IP=12.34.56.78
MASK=255.255.255.255 ↓

Info (1005275): interface successfully added.
```

- 11 デフォルトルートを設定します。

```
Manager B> ADD IP ROUTE=0.0.0.0 INT=ppp0
NEXTHOP=0.0.0.0 ↓

Info (1005275): IP route successfully added.
```

- 12 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。ppp0 をリセットするスクリプト reset.scp を作成します。

```
Manager B> ADD SCRIPT=reset.scp TEXT="RESET
PPP=0" ↓

File : reset.scp
1:RESET PPP=0
```

トリガー 1 を無効状態にするスクリプト up.scp を作成します。

```
Manager B> ADD SCRIPT=up.scp TEXT="DISABLE
TRIGGER=1" ↓

File : up.scp
1:DISABLE TRIGGER=1
```

トリガー 1 を有効状態にするスクリプト down.scp を作成します。

```
Manager B> ADD SCRIPT=down.scp TEXT="ENABLE
TRIGGER=1" ↓

File : down.scp
1:ENABLE TRIGGER=1
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド (内蔵フルスクリーンエディター) などを使って設定スクリプトファイル (.CFG) にこのコマンドを記述しても意図した結果になりません。

13 トリガー機能を有効にします。

```
Manager B> ENABLE TRIGGER ↓  
Info (1053268): The trigger module has been enabled.
```

- 14 ppp0E セッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順 12 で設定したそれぞれのトリガースクリプトを実行します。
reset.scp を実行する定期トリガー 1 を作成します。このトリガーは、ppp0 インターフェースがダウンすると同時に有効になり、3 分間隔で実行され、アップすると無効になります。

```
Manager B> CREATE TRIGGER=1 PERIODIC=3  
SCRIPT=reset.scp ↓  
Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up.scp を実行するインターフェーストリガー 2 を作成します。

```
Manager B> CREATE TRIGGER=2 INTERFACE=ppp0  
EVENT=UP CP=IPCP SCRIPT=up.scp ↓  
Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down.scp を実行するインターフェーストリガー 3 を作成します。

```
Manager B> CREATE TRIGGER=3 INTERFACE=ppp0  
EVENT=DOWN CP=IPCP SCRIPT=down.scp ↓  
Info (1053262): Trigger successfully added.
```

 本書「トリガーの動作」(p.135)

●ファイアウォールの設定

- 15 ファイアウォール機能を有効にします。

```
Manager B> ENABLE FIREWALL ↓  
Info (1077257): 19-Apr-2002 19:55:22  
Firewall enabled.  
Info (1077003): Operation successful.
```

- 16 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager B> CREATE FIREWALL POLICY=net ↓  
Info (1077003): Operation successful.
```

- 17 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。*8

```
Manager B> ENABLE FIREWALL POLICY=net  
ICMP_F=PING,UNREACH ↓  
Info (1077003): Operation successful.
```

- 18 ident プロキシ機能を無効にし、外部のメール (SMTP) サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager B> DISABLE FIREWALL POLICY=net  
IDENTPROXY ↓  
Info (1077003): Operation successful.
```

- 19 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=vlan1  
TYPE=PRIVATE ↓  
Info (1077003): Operation successful.
```

WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=ppp0  
TYPE=PUBLIC ↓  
Info (1077003): Operation successful.
```

- 20 LAN 側 (vlan1) ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるように設定します。グローバルアドレスには ppp0 のアドレスを使用します。

```
Manager B> ADD FIREWALL POLICY=net  
NAT=ENHANCED INT=vlan1 GBLINT=ppp0  
Info (1077003): Operation successful.
```



*8 デフォルト設定では、ICMP はファイアウォールを通過できません。

- 21 接続相手からの IKE パケット (UDP500 番) がファイアウォールを通過できるように設定します。

```
Manager B> ADD FIREWALL POLICY=net RU=1
AC=ALLOW INT=ppp0 PROT=UDP GBLPO=500
GBLIP=12.34.56.78 PO=500 IP=12.34.56.78 ↓

Info (1077003): Operation successful.
```

- 22 ローカル LAN からリモート LAN へのパケットには NAT をかけないように設定します。

```
Manager B> ADD FIREWALL POLICY=net RU=2
AC=NONAT INT=vlan1 PROT=ALL
IP=192.168.2.1-192.168.2.254 ↓

Info (1077003): Operation successful.

Manager B> SET FIREWALL POLICY=net RU=2
REMOTEIP=192.168.1.1-192.168.1.254 ↓

Info (1077003): Operation successful.
```

- 23 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点 IP アドレスが 192.168.2.1 ~ 192.168.2.254、つまりローカル LAN 側ならば、NAT の対象外とする」の意味になります。

```
Manager B> ADD FIREWALL POLICY=net RU=3
AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-
192.168.2.254 ENCAP=IPSEC ↓

Info (1077003): Operation successful.
```

● IPsec の設定

- 24 ここから IPsec の設定になります。最初に ISAKMP 用の事前共有鍵 (pre-shared key) を作成します。拠点 A で指定した鍵番号を 1 番と、鍵の値「secret」を指定します。

```
Manager B> CREATE ENCO KEY=1 TYPE=GENERAL
VALUE="secret" ↓

Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル (.CFG) に、このコマンドを記述しても無効になります。

なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では、ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

- 25 接続相手との IKE ネゴシエーション要求を受け入れる ISAKMP ポリシー「I」を作成します。KEY には、前の手順で作成した事前共有鍵 (鍵番号 1) を、PEER には拠点 A のルーターの IP アドレスを指定します。

```
Manager B> CREATE ISAKMP POLICY="i"
PEER=12.34.56.78 KEY=1 SENDN=TRUE ↓
```

- 26 IPsec 通信の仕様を定義する SA スペック 1 を作成します。拠点 A 同様にトンネルモード (デフォルト)、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager B> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↓

Info (1081003): Operation successful.
```

- 27 SA スペック 1 だけからなる SA バンドルスペック 1 を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager B> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
STRING="1" ↓

Info (1081003): Operation successful.
```

- 28 ISAKMP メッセージを素通しさせる IPsec ポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの 500 番ポートからリモートの 500 番ポート宛の UDP パケット (ISAKMP) に設定します。

```
Manager B> CREATE IPSEC POLICY="isa"
INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
TRANSPORT=UDP ↓

Info (1081003): Operation successful.
```

ISAKMP を使用する場合は、必ず最初の IPsec ポリシーで ISAKMP メッセージが通過できるように設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドの POSITION パラメーターを使用します。

- 29 実際のIPsec通信に使用するIPsecポリシー「vpn」をPPP0に対して作成します。鍵管理方式「ISAKMP」、PEERには拠点AのルーターのIPアドレスを、BUNDLEにはSAバンドルスペース「1」を指定します。

```
Manager B> CREATE IPSEC POLICY="vpn" INT=ppp0
ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
PEER=192.0.2.1 ㊟

Info (1081003): Operation successful.
```

- 30 IPsecポリシー「vpn」に対して実際にIPsec通信を行なうIPアドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

```
Manager B> SET IPSEC POLICY="vpn"
LAD=192.168.2.0 LMA=255.255.255.0
RAD=192.168.1.0 RMA=255.255.255.0 ㊟

Info (1081003): Operation successful.
```

- 31 インターネットへの平文通信を許可するIPsecポリシー「inet」をPPPインターフェース0に対して作成します。

```
Manager B> CREATE IPSEC POLICY="inet"
INT=ppp0 ACTION=PERMIT ㊟

Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後のIPsecポリシーですべてのパケットを通過させる設定を行ってください。どのIPsecポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、上記の設定がないとVPN以外との通信ができなくなります。

- 32 IPsecモジュールを有効にします。

```
Manager B> ENABLE IPSEC ㊟

Info (1081003): Operation successful.
```

- 33 ISAKMPモジュールを有効にします。

```
Manager B> ENABLE ISAKMP ㊟

Info (1082057): ISAKMP has been enabled.
```

- 34 Security Officerレベルのユーザーでログインしなします。

```
Manager B> LOGIN secoff ㊟

Password: passwdSB
```

- 35 動作モードをセキュリティーモードに切り替えます。

```
SecOff B> ENABLE SYSTEM SECURITY_MODE ㊟

Info (1034003): Operation successful.
```

セキュリティーモードでは、Security OfficerレベルでのTelnetログインが原則として禁止されています。セキュリティーモードにおいて、Security OfficerレベルでTelnetログインしたい場合は、あらかじめRSO (Remote Security Officer) の設定を行っておいてください。



本書「5.4 ノーマルモード / セキュリティーモード」(p.54)

●設定の保存

- 36 WAN側インターフェースのUTPケーブルが抜けているのを確認し、設定を保存します。

```
SecOff A> CREATE CONFIG=ROUTER.CFG ㊟

Info (1049003): Operation successful.
```

もし、ケーブルが刺さっていた場合は、ケーブルを抜き「SHOW PPP」コマンドで、接続が切断されているのを確認してから保存します。

- 37 保存したファイルを起動時設定ファイルに指定します。

```
SecOff A> SET CONFIG=ROUTER.CFG ㊟

Info (1049003): Operation successful.
```

接続の確認

- 38 拠点A、BともにUTPケーブルを接続し、「SHOW PPP」コマンドでPPPの接続が確立 (OPENED) したことを確認してください。

- 39 LAN側のコンピューターから、相手側の社内サーバーなどが参照できることを確認してください。^{*9}



^{*9} サブネット間でWindowsのネットワークドライブを参照するためには、例えばWindows 2000/XPでは「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーのIPアドレスなどを指定します。
(例) \\192.168.1.10

まとめ

拠点A、Bそれぞれで、前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 1 3.5.2 設定スクリプトファイル 拠点 A

1	SET SYSTEM NAME=A
2	ADD USER=secoff PASSWORD=passwdSA PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=eth1 IP=192.0.0.2 MASK=255.255.255.248
8	ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0
9	ADD IP INT=ppp0-0 IP=0.0.0.0
10	ADD IP INT=ppp0-1 IP=192.0.2.1 MASK=255.255.255.255
11	ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXTHOP=0.0.0.0
12	ENABLE TRIGGER
13	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
14	CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp
15	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp
16	ENABLE FIREWALL
17	CREATE FIREWALL POLICY=net
18	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
19	DISABLE FIREWALL POLICY=net IDENTPROXY
20	ADD FIREWALL POLICY=net INT=eth1 TYPE=PRIVATE
21	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
22	ADD FIREWALL POLICY=net INT=ppp0-0 TYPE=PUBLIC
23	ADD FIREWALL POLICY=net INT=ppp0-1 TYPE=PUBLIC
24	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0-1 GBLIP=192.0.2.1
25	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.3 PORT=80
26	ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4 PORT=25

表 1 3.5.2 設定スクリプトファイル 拠点 A

27	ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0-1 PROTO=TCP IP=192.0.2.4 PORT=53
28	ADD FIREWALL POLICY=net RULE=4 AC=ALLOW INT=ppp0-1 PROTO=UDP IP=192.0.2.4 PORT=53
29	ADD FIREWALL POLICY=net RU=5 AC=ALLOW INT=ppp0-1 PROTO=UDP GBLPO=500 GBLIP=192.0.2.1 PO=500 IP=192.0.2.1
30	ADD FIREWALL POLICY=net RU=6 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1- 192.168.1.254
31	SET FIREWALL POLICY=net RU=6 REMOTEIP=192.168.2.1-192.168.2.254
32	ADD FIREWALL POLICY=net RU=7 AC=NONAT INT=ppp0-1 PROT=ALL IP=192.168.1.1- 192.168.1.254 ENCAP=IPSEC
33	CREATE ISAKMP POLICY="i" PEER=12.34.56.78 KEY=1 SENDN=TRUE
34	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=BSP ENCALG=DES HASHALG=SHA
35	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
36	CREATE IPSEC POLICY="isa" INT=ppp0-1 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
37	CREATE IPSEC POLICY="vpn" INT=ppp0-1 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=12.34.56.78
38	SET IPSEC POLICY="vpn" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.2.0 RMA=255.255.255.0
39	CREATE IPSEC POLICY="inet" INT=ppp0-1 ACTION=PERMIT
40	ENABLE IPSEC
41	ENABLE ISAKMP
15	SET IPSEC POLICY="vpn" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.2.0 RMA=255.255.255.0
16	CREATE IPSEC POLICY="inet" INT=ppp0-1 ACTION=PERMIT
17	ENABLE IPSEC
18	ENABLE ISAKMP

表 1 3.5.3 設定スクリプトファイル 拠点 B

1	SET SYSTEM NAME=B
2	ADD USER=secoff PASSWORD=passwdSB PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_b@example.co.jp PASSWORD=passwd_b LQR=OFF ECHO=ON

表 13.5.3 設定スクリプトファイル 拠点B

5	ENABLE IP
6	ADD IP INT=vlan1 IP=192.168.2.1 MASK=255.255.255.0
7	ADD IP INT=ppp0 IP=12.34.56.78 MASK=255.255.255.255
8	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
9	ENABLE TRIGGER
10	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
11	CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp
12	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp
13	ENABLE FIREWALL
14	CREATE FIREWALL POLICY=net
15	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
16	DISABLE FIREWALL POLICY=net IDENTPROXY
17	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
19	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
20	ADD FIREWALL POLICY=net RU=1 AC=ALLOW INT=ppp0 PROT=UDP GBLPO=500 GBLIP=12.34.56.78 PO=500 IP=12.34.56.78
21	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.2.1- 192.168.2.254
22	SET FIREWALL POLICY=net RU=2 REMOTEIP=192.168.1.1-192.168.1.254
23	ADD FIREWALL POLICY=net RU=3 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-192.168.2.254 ENCAP=IPSEC
24	CREATE ISAKMP POLICY="i" PEER=192.0.2.1 KEY=1 SENDN=TRUE
25	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
26	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
27	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
28	CREATE IPSEC POLICY="vpn" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=192.0.2.1
29	SET IPSEC POLICY="vpn" LAD=192.168.2.0 LMA=255.255.255.0 RAD=192.168.1.0 RMA=255.255.255.0
30	CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT

表 13.5.3 設定スクリプトファイル 拠点B

31	ENABLE IPSEC
32	ENABLE ISAKMP

「SET TIME」、「ADD SCRIPT」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

拠点 A、B ともに以下のスクリプトは共通です。

表 13.5.4 スクリプト「reset.scp」

RESET PPP=0

表 13.5.5 スクリプト「up.scp」

DISABLE TRIGGER=1

表 13.5.6 スクリプト「down.scp」

ENABLE TRIGGER=1

13.6 インターネット接続による3点間IPsec VPN

PPPoEでインターネットに接続している3つの拠点を、IPsecで接続しデータの安全性を確保します。

この例では、本社と各支社の接続を例にあげます。以下の3拠間の接続を、トンネルモード(ESP)で暗号化します。ただし、本社支社間の安全な通信経路を確保することを目的とし、各支社間の通信は行いません。

- グローバルアドレス1個を固定的に割り当てられている拠点A(本社)
- グローバルアドレス1個をに割り当てられている拠点B、C(支社)

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●拠点A

- 接続のユーザー名: site_a@example.co.jp
- 接続のパスワード: passwd_a
- PPPoE サービス名: 指定なし
- IP アドレス グローバルアドレス: 192.0.2.0/29 (8個固定)
- DNS サーバー: 接続時に通知される

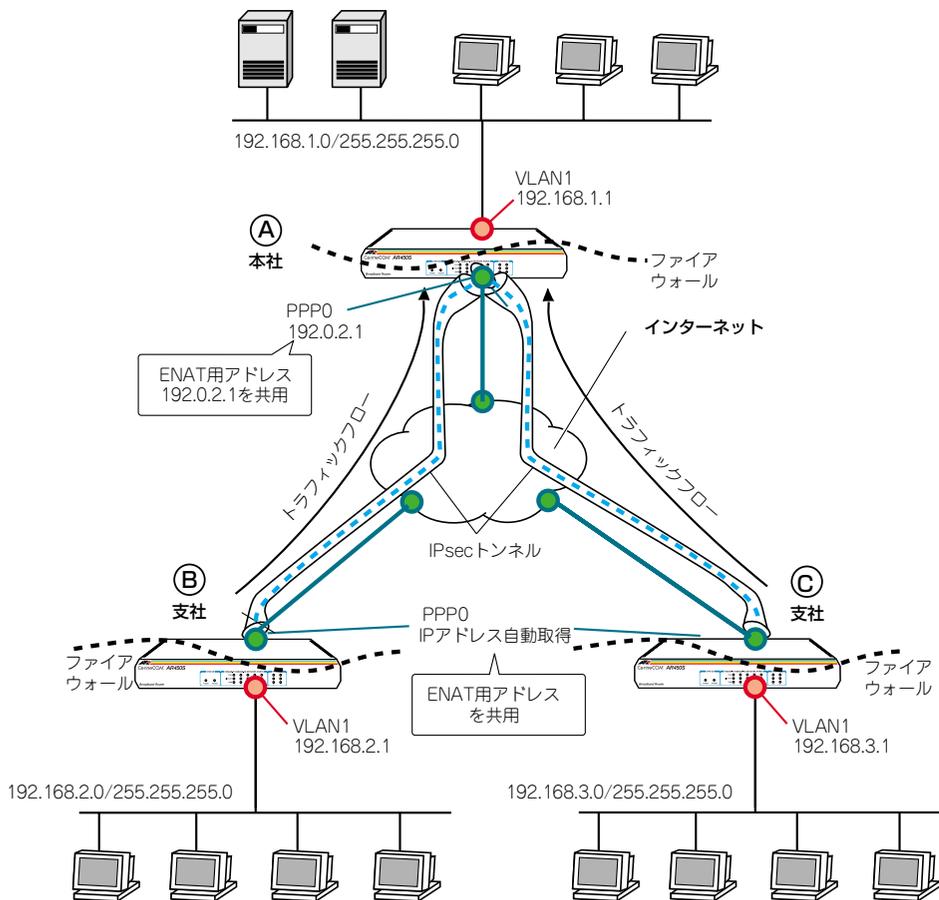


図 13.6.1 IPsec による接続

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●拠点 A

- 接続のユーザー名：site_a@example.co.jp
- 接続のパスワード：passwd_a
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：192.0.2.0/29（8 個固定）
- DNS サーバー：接続時に通知される

●拠点 B

- 接続のユーザー名：site_b@example.co.jp
- 接続のパスワード：passwd_b
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：1 個不定
- DNS サーバー：接続時に通知される

●拠点 C

- 接続のユーザー名：site_c@example.co.jp
- 接続のパスワード：passwd_c
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：1 個不定
- DNS サーバー：接続時に通知される

設定の方針

●インターネット接続設定

- すべての拠点においてグローバルアドレスの割り当ては 1 個しかないので、WAN 側 (ppp0) インターフェースにグローバルアドレスを設定したダイナミック ENAT による、通常の端末型を使用します。このグローバルアドレスが IPsec パケットの始点アドレスとしてセットされます。
- トリガー機能を使って PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合に、自動的に再接続するよう設定します。

表 13.6.1 インターネット接続設定

	拠点 A	拠点 B	拠点 B
WAN 側物理インターフェース	eth0	eth0	eth0
WAN 側 IP アドレス (ppp0)	192.0.2.1/32	動的割り当て	動的割り当て
LAN 側 IP アドレス (vlan1)	192.168.1.1/24 (vlan1)	192.168.2.1/24 (vlan1)	192.168.3.1/24 (vlan1)

●VPN 設定

- IPsec トンネルは、拠点 A の ppp0 と拠点 B の ppp0 の間、拠点 A の ppp0 と拠点 C の ppp0 の間にそれぞれ別個に張られます。このトンネルはプライベート LAN 間を接続するためのもので、IP のパケットを暗号化して通します。
- ファイアウォールの設定においては、IPsec 関連のパケット (IKE、ESP) を除く外部からの不正アクセスを遮断し、内部からは自由にインターネットへのアクセスができるようにします。
- トンネリング対象のパケットに NAT が適用されないようルールを設定します。

表 13.6.2 IKE フェーズ 1 (ISAKMP SA のネゴシエーション)

本製品間の認証方式	事前共有鍵 (pre-shared key)
IKE 交換モード	Aggressive モード
事前共有鍵 (A-B 間)	secret-ab (文字列)
事前共有鍵 (A-C 間)	secret-ab (文字列)
拠点 A のルーターの認証 ID	IP アドレス : 192.0.2.1 (デフォルト)
拠点 B のルーターの認証 ID	名前 : client_B
拠点 C のルーターの認証 ID	名前 : client_C
Oakley グループ	1 (デフォルト)
ISAKMP メッセージの暗号化方式	DES (デフォルト)
ISAKMP メッセージの認証方式	SHA1 (デフォルト)
ISAKMP SA の有効期限 (時間)	86400 秒 (24 時間) (デフォルト)
ISAKMP SA の有効期限 (Kbyte 数)	なし (デフォルト)
起動時の ISAKMP ネゴシエーション	行わない

表 13.6.3 IKE フェーズ 2 (IPsec SA のネゴシエーション)

SA モード	トンネルモード
セキュリティープロトコル	ESP (暗号 + 認証)
暗号化方式	DES
認証方式	SHA1
IPComp	使わない
IPsec SA の有効期限 (時間)	28800 秒 (8 時間) (デフォルト)
IPsec SA の有効期限 (Kbyte 数)	なし (デフォルト)
IPsec の適用対象 IP アドレス (A-B 間)	192.168.1.0/24 ⇔ 192.168.2.0/24
トンネル終端アドレス (A-B 間)	192.0.2.1 ⇔ 不定

表 1.3.6.3 IKE フェーズ2 (IPsec SAのネゴシエーション)

IPsecの適用対象 IP アドレス (A-C間)	192.168.1.0/24 ⇔ 192.168.3.0/24
トンネル端末アドレス (A-C間)	192.0.2.1 ⇔ 不定
インターネットとの平文通信	行なう

拠点 A の設定

1 本製品の電源がオフの状態、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。

2 本製品の電源スイッチをオンにします。

3 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager 』
Password: friend (表示されません)
```

4 管理をしやすいするために、本製品にシステム名を設定します。サイト A には「A」を設定します。

```
Manager > SET SYSTEM NAME=A 』
Info (1034003): Operation successful.
Manager A>
```

5 IPsec はセキュリティーモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officer レベルのユーザーを登録しておきます。Security Officer のパスワードは厳重に管理してください。

ここでは、ユーザー名「secoff」、パスワード「passwdSA」を仮定します。

```
Manager A> ADD USER=secoff PASSWORD=passwdSA
PRIVILEGE=SECURITYOFFICER 』

User Authentication Database
-----
Username: secoff ()
Status: enabled   Privilege: Sec Off   Telnet: no   Login: yes
Logins: 0         Fails: 0             Sent: 0     Rcvd: 0
Authentications: 0 Fails: 0
```

● PPP の設定

6 WAN 側 Ethernet インターフェース (eth0) 上に PPP インターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager A> CREATE PPP=0 OVER=eth0-any 』
Info (1003003): Operation successful.
```

7 プロバイダーから通知された PPP ユーザー名とパスワードを設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
Manager A> SET PPP=0 OVER=eth0-any BAP=OFF
USER=site_a@example.co.jp
PASSWORD=passwd_a LQR=OFF ECHO=ON 』
Info (1003003): Operation successful.
```

● IP、ルーティングの設定

8 IP モジュールを有効にします。

```
Manager A> ENABLE IP 』
Info (1005287): IP module has been enabled.
```

9 LAN 側 (vlan1) インターフェースにプライベート IP アドレスを割り当てます。

```
Manager A> ADD IP INT=vlan1 IP=192.168.1.1
MASK=255.255.255.0 』
Info (1005275): interface successfully added.
```

10 WAN 側 (ppp0) インターフェースにプロバイダーから割り当てられた IP アドレスを設定します。

```
Manager A> ADD IP INT=ppp0 IP=192.0.2.1
MASK=255.255.255.255 』
Info (1005275): interface successfully added.
```

11 デフォルトルートを設定します。

```
Manager A> ADD IP ROUTE=0.0.0.0 INT=ppp0
NEXTHOP=0.0.0.0 』
Info (1005275): IP route successfully added.
```

- 12 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。
ppp0 をリセットするスクリプト reset.scp を作成します。

```
Manager A> ADD SCRIPT=reset.scp TEXT="RESET
PPP=0" ↓

File : reset.scp

1:RESET PPP=0
```

トリガー 1 を無効状態にするスクリプト up.scp を作成します。

```
Manager A> ADD SCRIPT=up.scp TEXT="DISABLE
TRIGGER=1" ↓

File : up.scp

1:DISABLE TRIGGER=1
```

トリガー 1 を有効状態にするスクリプト down.scp を作成します。

```
Manager A> ADD SCRIPT=down.scp TEXT="ENABLE
TRIGGER=1" ↓

File : down.scp

1:ENABLE TRIGGER=1
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド（内蔵フルスクリーンエディター）などを使って設定スクリプトファイル（.CFG）にこのコマンドを記述しても意図した結果になりません。

- 13 トリガー機能を有効にします。

```
Manager A> ENABLE TRIGGER ↓

Info (1053268): The trigger module has been enabled.
```

- 14 PPPoE セッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順 12 で設定したそれぞれのトリガースクリプトを実行します。
reset.scp を実行する定期トリガー 1 を作成します。このトリガーは、ppp0 インターフェースがダウンすると同時に有効になり、3 分間隔で実行され、アップすると無効になります。

```
Manager A> CREATE TRIGGER=1 PERIODIC=3
SCRIPT=reset.scp ↓

Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up.scp を実行するインターフェーストリガー 2 を作成します。

```
Manager A> CREATE TRIGGER=2 INTERFACE=ppp0
EVENT=UP CP=IPCP SCRIPT=up.scp ↓

Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down.scp を実行するインターフェーストリガー 3 を作成します。

```
Manager A> CREATE TRIGGER=3 INTERFACE=ppp0
EVENT=DOWN CP=IPCP SCRIPT=down.scp ↓

Info (1053262): Trigger successfully added.
```

 本書「トリガーの動作」(p.135)

●ファイアウォールの設定

- 15 ファイアウォール機能を有効にします。

```
Manager A> ENABLE FIREWALL ↓

Info (1077257): 19-Apr-2002 19:55:22
Firewall enabled.

Info (1077003): Operation successful.
```

- 16 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager A> CREATE FIREWALL POLICY=net ↓

Info (1077003): Operation successful.
```

- 17 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。^{*10}

```
Manager A> ENABLE FIREWALL POLICY=net
ICMP_F=PING,UNREACHABLE ↓

Info (1077003): Operation successful.
```

- 18 ident プロキシ機能が無効にし、外部のメール (SMTP) サーバーなどからの ident 要求に対して、ただちに TCP RST を返



*10 デフォルト設定では、ICMP はファイアウォールを通過できません。

すよう設定します。

```
Manager A> DISABLE FIREWALL POLICY=net  
IDENTPROXY ↓
```

```
Info (1077003): Operation successful.
```

- 19 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=vlan1  
TYPE=PRIVATE ↓
```

```
Info (1077003): Operation successful.
```

WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp0  
TYPE=PUBLIC ↓
```

```
Info (1077003): Operation successful.
```

- 20 LAN 側 (vlan1) ネットワークに接続されているすべてのコンピュータが ENAT 機能を使用できるよう設定します。グローバルアドレスには ppp0 の IP アドレスを使用します。

```
Manager A> ADD FIREWALL POLICY=net  
NAT=ENHANCED INT=vlan1 GBLINT=ppp0 ↓
```

```
Info (1077003): Operation successful.
```

- 21 接続相手からの IKE パケット (UDP500 番) がファイアウォールを通過できるように設定します。

```
Manager A> ADD FIREWALL POLICY=net RU=1  
AC=ALLOW INT=ppp0 PROTO=UDP GBLPO=500  
GBLIP=192.0.2.1 PO=500 IP=192.0.2.1 ↓
```

```
Info (1077003): Operation successful.
```

- 22 各拠点向けのパケットには NAT の対象にしないように設定します。

拠点 B 向けのルールは以下のようになります。

```
Manager A> ADD FIREWALL POLICY=net RU=2  
AC=NONAT INT=vlan1 PROT=ALL  
IP=192.168.1.1-192.168.1.254 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager A> SET FIREWALL POLICY=net RU=2  
REMOTEIP=192.168.2.1-192.168.2.254 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager A> ADD FIREWALL POLICY=net RU=3  
AC=NONAT INT=vlan1 PROT=ALL  
IP=192.168.1.1-192.168.1.254 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager A> SET FIREWALL POLICY=net RU=3  
REMOTEIP=192.168.3.1-192.168.3.254 ↓
```

```
Info (1077003): Operation successful.
```

- 23 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点 IP アドレスが 192.168.1.1 ~ 192.168.1.254、つまり拠点 A 向けならば、NAT の対象外とする」の意味になります。

```
Manager A> ADD FIREWALL POLICY=net RU=4  
AC=NONAT INT=ppp0 PROT=ALL IP=192.168.1.1-  
192.168.1.254 ENCAP=IPSEC ↓
```

```
Info (1077003): Operation successful.
```

● IPsec の設定

24 ここからIPsec の設定になります。最初に ISAKMP 用の事前共有鍵 (pre-shared key) を作成します。ここでは拠点 B 向けは鍵番号を「1」番、鍵の値は「secret-ab」とし、拠点 C 向けは「2」番と「secret-ac」とします (拠点 B、C のルーターも同様に設定)。

```
Manager A> CREATE ENCO KEY=1 TYPE=GENERAL
VALUE="secret-ab" ↓

Info (1073003): Operation successful.

Manager A> CREATE ENCO KEY=2 TYPE=GENERAL
VALUE="secret-ac" ↓

Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル (.CFG) に、このコマンドを記述しても無効になります。

なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では、ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

25 接続相手との IKE ネゴシエーション要求を受け入れる ISAKMP ポリシーを作成します。この例では相手のアドレスが不定なため、拠点 B、C ともに PEER に「ANY」を、MODE に「AGGRESSIVE」を指定して Aggressive モードを使うよう設定します。拠点 B 向けには、KEY に前の手順で作成した鍵番号「1」を、REMOTEID で認証 ID 「client_B」を指定し、ポリシー 「i_B」として作成します。拠点 C 向けには、KEY に前の手順で作成した鍵番号「2」を、REMOTEID で認証 ID 「client_C」を指定しポリシー 「i_C」として作成します。

```
Manager A> CREATE ISAKMP POLICY="i_B" PEER=ANY
KEY=1 SENDN=TRUE REMOTEID="client_B"
MODE=AGGRESSIVE HEARTBEATMODE=BOTH ↓

Info (1082003): Operation successful.

Manager A> CREATE ISAKMP POLICY="i_C" PEER=ANY
KEY=2 SENDN=TRUE REMOTEID="client_C"
MODE=AGGRESSIVE HEARTBEATMODE=BOTH ↓

Info (1082003): Operation successful.
```

26 IPsec 通信の仕様を定義する SA スペック 1 を作成します。トンネルモード (デフォルト)、鍵管理方式「ISAKMP」、プロトコル

「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager A> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↓

Info (1081003): Operation successful.
```

27 SA スペック 1 だけからなる SA バンドルスペック 1 を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager A> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
STRING="1" ↓

Info (1081003): Operation successful.
```

28 ISAKMP メッセージを素通しさせる IPsec ポリシー 「isa」を作成します。ポリシーの適用対象を、ローカルの 500 番ポートからリモートの 500 番ポート宛の UDP パケット (ISAKMP) に設定します。

```
Manager A> CREATE IPSEC POLICY="isa" INT=ppp0
ACTION=PERMIT LPORT=500 RPORT=500
TRANSPORT=UDP ↓

Info (1081003): Operation successful.
```

ISAKMP を使用する場合は、必ず最初の IPsec ポリシーで ISAKMP メッセージが通過できるような設定を行ってください。「IPsec ポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドの POSITION パラメーターを使用します。

29 実際の IPsec 通信に使用する IPsec ポリシーを PPP0 に対して作成します。相手の IP アドレスが不定なので、PEER に「DYNAMIC」を指定します。鍵管理方式は「ISAKMP」、BUNDLE には SA バンドルスペック「1」を指定します。拠点 B と拠点 C 向けの違いはポリシー名のみです。

```
Manager A> CREATE IPSEC POLICY="vpn_B"
INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUN-
DLE=1 PEER=DYNAMIC ↓

Info (1081003): Operation successful.

Manager A> CREATE IPSEC POLICY="vpn_C"
INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUN-
DLE=1 PEER=DYNAMIC ↓

Info (1081003): Operation successful.
```

- 30 IPsec ポリシーに対して、それぞれの拠点向けに実際に IPsec 通信を行なう IP アドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

```
Manager A> SET IPSEC POLICY="vpn_B"
LAD=192.168.1.0 LMA=255.255.255.0
RAD=192.168.2.0 RMA=255.255.255.0 』

Info (1081003): Operation successful.

Manager A> SET IPSEC POLICY="vpn_C"
LAD=192.168.1.0 LMA=255.255.255.0
RAD=192.168.3.0 RMA=255.255.255.0 』

Info (1081003): Operation successful.
```

- 31 インターネットへの平文通信を許可する IPsec ポリシー「inet」を PPPoE に対して作成します。

```
Manager A> CREATE IPSEC POLICY="inet" INT=ppp0
ACTION=PERMIT 』

Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後の IPsec ポリシーで、すべてのパケットを通過させるための上記の設定を行ってください。どの IPsec ポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、設定がないと VPN 以外との通信ができなくなります。

- 32 IPsec モジュールを有効にします。

```
Manager A> ENABLE IPSEC 』

Info (1081003): Operation successful.
```

- 33 ISAKMP モジュールを有効にします。

```
Manager A> ENABLE ISAKMP 』

Info (1082057): ISAKMP has been enabled.
```

- 34 Security Officer レベルのユーザーでログインしなおします。

```
Manager A> LOGIN secoff 』

Password: passwdSA
```

- 35 動作モードをセキュリティーモードに切り替えます。

```
SecOff A> ENABLE SYSTEM SECURITY_MODE 』

Info (1034003): Operation successful.
```

セキュリティーモードでは、Security Officer レベルでの Telnet ログインが原則として禁止されています。セキュリティーモードにおいて、Security Officer レベルで Telnet ログインしたい場合は、あらかじめ RSO (Remote Security Officer) の設定を行っておいてください。

 本書「5.4 ノーマルモード / セキュリティーモード」(p.54)

●設定の保存

- 36 WAN 側インターフェースの UTP ケーブルが抜けているのを確認し、設定を保存します。

```
SecOff A> CREATE CONFIG=ROUTER.CFG 』

Info (1049003): Operation successful.
```

もし、ケーブルが刺さっていた場合は、ケーブルを抜き「SHOW PPP」コマンドで、接続が切断されているのを確認してから保存します。

- 37 保存したファイルを起動時設定ファイルに指定します。

```
SecOff A> SET CONFIG=ROUTER.CFG 』

Info (1049003): Operation successful.
```

拠点 B、拠点 C の設定

拠点 B と拠点 C では、それぞれの拠点ごとの設定値が異なるだけで、基本的な設定方法は同じです。

拠点 B と拠点 C で設定値が違う部分については、それぞれ向けの操作例などを明示します。それ以外の部分は両拠点について同様の設定を行ってください。

- 1 本製品の電源がオフの状態では、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。
- 2 本製品の電源スイッチをオンにします。
- 3 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager 』
Password: friend (表示されません)
```

- 4 管理をしやすくするために、本製品にシステム名を設定します。サイトBには「B」を設定します。

拠点B

```
Manager > SET SYSTEM NAME=B ↓  
  
Info (1034003): Operation successful.  
  
Manager B>
```

拠点Cには「C」を設定します。

拠点C

```
Manager > SET SYSTEM NAME=C ↓  
  
Info (1034003): Operation successful.  
  
Manager C>
```

- 5 IPsecはセキュリティーモードでなければ動作しません。あらかじめ、同モードで管理や設定を行うことのできる Security Officerレベルのユーザーを登録しておきます。Security Officerのパスワードは厳重に管理してください。

拠点Bでは、ユーザー名「secoff」、パスワード「passwdSB」を仮定します。

拠点B

```
Manager B> ADD USER=secoff PASSWORD=passwdSB  
PRIVILEGE=SECURITYOFFICER ↓  
  
User Authentication Database  
-----  
Username: secoff ()  
Status: enabled Privilege: Sec Off Telnet: no Login: yes  
Logins: 0 Fails: 0 Sent: 0 Rcvd: 0  
Authentications: 0 Fails: 0  
-----
```

拠点Cでは、ユーザー名「secoff」、パスワード「passwordSC」を仮定します。

拠点C

```
Manager C> ADD USER=secoff PASSWORD=passwordSC  
PRIVILEGE=SECURITYOFFICER ↓  
  
User Authentication Database  
-----  
Username: secoff ()  
Status: enabled Privilege: Sec Off Telnet: no Login: yes  
Logins: 0 Fails: 0 Sent: 0 Rcvd: 0  
Authentications: 0 Fails: 0  
-----
```

● PPPの設定

- 6 WAN側Ethernetインターフェース(eth0)上にPPPインターフェースを作成します。「OVER=eth0-XXXX」の「XXXX」の部

分には、通知されたPPPoEの「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager B> CREATE PPP=0 OVER=eth0-any ↓  
  
Info (1003003): Operation successful.
```

- 7 プロバイダーから通知されたPPPユーザー名とパスワードを各拠点ごとに指定し接続時にIPアドレス割り当てを行うように設定します。LQRはオフにし、代わりにLCP Echoパケットを使ってPPPリンクの状態を監視するようにします。また、ISDN向けの機能であるBAPはオフにします。

拠点B

```
Manager B> SET PPP=0 OVER=eth0-any BAP=OFF  
USER=site_b@example.co.jp PASS-  
WORD=passwd_b IPREQSERV=ON LQR=OFF  
ECHO=ON ↓  
  
Info (1003003): Operation successful.
```

拠点C

```
Manager C> SET PPP=0 OVER=eth0-any BAP=OFF  
USER=site_c@example.co.jp PASS-  
WORD=passwd_c IPREQSERV=ON LQR=OFF  
ECHO=ON ↓  
  
Info (1003003): Operation successful.
```

● IP、ルーティングの設定

- 8 IPモジュールを有効にします。

```
Manager B> ENABLE IP ↓  
  
Info (1005287): IP module has been enabled.
```

- 9 IPCPネゴシエーションで与えられたIPアドレスをPPPインターフェースで使用するよう設定します。

```
Manager B> ENABLE IP REMOTEASSIGN ↓  
  
Info (1005287): IP module has been enabled.
```

- 10 LAN側(vlan1)インターフェースに各拠点ごとのプライベートIPアドレスを割り当て、クライアント用のサブネットとします。

拠点B

```
Manager B> ADD IP INT=vlan1 IP=192.168.2.1  
MASK=255.255.255.0 ↓  
  
Info (1005275): interface successfully added.
```

拠点C

```
Manager C> ADD IP INT=vlan1 IP=192.168.3.1
MASK=255.255.255.0 ｡

Info (1005275): interface successfully added.
```

- 11 WAN 側 (ppp0) インターフェースにプロバイダーから割り当てられたIP アドレスを設定します。

```
Manager B> ADD IP INT=ppp0 IP=0.0.0.0 ｡

Info (1005275): interface successfully added.
```

- 12 デフォルトルートを設定します。

```
Manager B> ADD IP ROUTE=0.0.0.0 INT=ppp0
NEXTHop=0.0.0.0 ｡

Info (1005275): IP route successfully added.
```

- 13 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。
ppp0 をリセットするスクリプト reset.scp を作成します。

```
Manager B> ADD SCRIPT=reset.scp TEXT="RESET
PPP=0" ｡

File : reset.scp
1:RESET PPP=0
```

トリガー 1 を無効状態にするスクリプト up.scp を作成します。

```
Manager B> ADD SCRIPT=up.scp TEXT="DISABLE
TRIGGER=1" ｡

File : up.scp
1:DISABLE TRIGGER=1
```

トリガー 1 を有効状態にするスクリプト down.scp を作成します。

```
Manager B> ADD SCRIPT=down.scp TEXT="ENABLE
TRIGGER=1" ｡

File : down.scp
1:ENABLE TRIGGER=1
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド (内蔵フルスクリーンエディター) などを使って設定スクリプトファイル (.CFG) にこのコマンドを記述しても意図した結果になりません。

- 14 トリガー機能を有効にします。

```
Manager B> ENABLE TRIGGER ｡

Info (1053268): The trigger module has been enabled.
```

- 15 PPPoE セッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順 13 で設定したそれぞれのトリガースクリプトを実行します。

reset.scp を実行する定期トリガー 1 を作成します。このトリガーは、ppp0 インターフェースがダウンすると同時に有効になり、3分間隔で実行され、アップすると無効になります。

```
Manager B> CREATE TRIGGER=1 PERIODIC=3
SCRIPT=reset.scp ｡

Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up.scp を実行するインターフェーストリガー 2 を作成します。

```
Manager B> CREATE TRIGGER=2 INTERFACE=ppp0
EVENT=UP CP=IPCP SCRIPT=up.scp ｡

Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down.scp を実行するインターフェーストリガー 3 を作成します。

```
Manager B> CREATE TRIGGER=3 INTERFACE=ppp0
EVENT=DOWN CP=IPCP SCRIPT=down.scp ｡

Info (1053262): Trigger successfully added.
```

 参照 本書「トリガーの動作」(p.135)

●ファイアウォールの設定

- 16 ファイアウォール機能を有効にします。

```
Manager B> ENABLE FIREWALL ｡

Info (1077257): 19-Apr-2002 19:55:22
Firewall enabled.

Info (1077003): Operation successful.
```

- 17 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager B> CREATE FIREWALL POLICY=net ｡

Info (1077003): Operation successful.
```

- 18 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。*11

```
Manager B> ENABLE FIREWALL POLICY=net  
ICMP_F=PING,UNREACHABLE ↓
```

```
Info (1077003): Operation successful.
```

- 19 ident プロキシ機能を無効にし、外部のメール (SMTP) サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager B> DISABLE FIREWALL POLICY=net  
IDENTPROXY ↓
```

```
Info (1077003): Operation successful.
```

- 20 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=vlan1  
TYPE=PRIVATE ↓
```

```
Info (1077003): Operation successful.
```

WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager B> ADD FIREWALL POLICY=net INT=ppp0  
TYPE=PUBLIC ↓
```

```
Info (1077003): Operation successful.
```

- 21 LAN 側 (vlan1) ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるよう設定します。グローバルアドレスには ppp0 のアドレスを使用します。

```
Manager B> ADD FIREWALL POLICY=net  
NAT=ENHANCED INT=vlan1 GBLINT=ppp0
```

```
Info (1077003): Operation successful.
```

- 22 ローカル LAN からリモート LAN へのパケットには NAT をかけないように設定します。

拠点B

```
Manager B> ADD FIREWALL POLICY=net RU=1  
AC=NONAT INT=vlan1 PROT=ALL  
IP=192.168.2.1-192.168.2.254 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager B> SET FIREWALL POLICY=net RU=1  
REMOTEIP=192.168.1.1-192.168.1.254 ↓
```

```
Info (1077003): Operation successful.
```

拠点C

```
Manager C> ADD FIREWALL POLICY=net RU=1  
AC=NONAT INT=vlan1 PROT=ALL  
IP=192.168.3.1-192.168.3.254 ↓
```

```
Info (1077003): Operation successful.
```

```
Manager C> SET FIREWALL POLICY=net RU=1  
REMOTEIP=192.168.1.1-192.168.1.254 ↓
```

```
Info (1077003): Operation successful.
```

- 23 基本ルールのままでは IPsec パケットまで遮断されてしまうので、これらのパケットを通過させるためのルールを設定します。

「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケットを取り出したあとでこのルールを適用することを示します。よって、次のコマンドは、「取り出したパケットの終点 IP アドレスがローカル LAN 側ならば、NAT の対象外とする」の意味になります。IP にはそれぞれの拠点の LAN 側 IP アドレスの範囲を指定します。

拠点B

```
Manager B> ADD FIREWALL POLICY=net RU=2  
AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-  
192.168.2.254 ENCAP=IPSEC ↓
```

```
Info (1077003): Operation successful.
```

拠点C

```
Manager C> ADD FIREWALL POLICY=net RU=2  
AC=NONAT INT=ppp0 PROT=ALL IP=192.168.3.1-  
192.168.3.254 ENCAP=IPSEC ↓
```

```
Info (1077003): Operation successful.
```

● IPsec の設定

- 24 ここからが IPsec の設定になります。最初に ISAKMP 用の事前共有鍵 (pre-shared key) を作成します。鍵番号と、それぞれの拠点に対して拠点 A で指定した鍵の値を指定します。



*11 デフォルト設定では、ICMP はファイアウォールを通過できません。

```
Manager B> CREATE ENCO KEY=1 TYPE=GENERAL
VALUE="secret-ab" ↓
```

```
Info (1073003): Operation successful.
```

拠点C

```
Manager C> CREATE ENCO KEY=1 TYPE=GENERAL
VALUE="secret-ac" ↓
```

```
Info (1073003): Operation successful.
```

「CREATE ENCO KEY」コマンドは、コンソールからログインしている場合のみ有効なコマンドです。そのため、「EDIT」コマンドなどで設定スクリプトファイル (.CFG) に、このコマンドを記述しても無効になります。

なお、「CREATE ECHO KEY」コマンドで作成された鍵は、セキュリティモード以外では、ルーターの再起動によって消去されます。鍵を使用する場合は、必ず最後にセキュリティモードに移行して鍵が保存されるようにしてください。

- 25** 前手順で作成した鍵を使い、接続相手とのIKEネゴシエーション要求を受け入れるISAKMPポリシー「i_A」を作成します。PEERにはルーターAのIPアドレスを指定します。また、自分のアドレスが不定なため、LOCALIDで自分の認証IDを指定し、MODEは「AGGRESSIVE」でAggressiveモードを使うよう設定します。拠点BではLOCALIDは「client_B」を、拠点Cには「client_C」を指定します。

拠点B

```
Manager B> CREATE ISAKMP POLICY="i_A"
PEER=192.0.2.1 KEY=1 SENDN=TRUE
LOCALID="client_B" MODE=AGGRESSIVE HEART-
BEATMODE=BOTH ↓
```

拠点C

```
Manager C> CREATE ISAKMP POLICY="i_A"
PEER=192.0.2.1 KEY=1 SENDN=TRUE
LOCALID="client_C" MODE=AGGRESSIVE HEART-
BEATMODE=BOTH ↓
```

- 26** IPsec通信の仕様を定義するSAスペック1を作成します。拠点A同様にトンネルモード(デフォルト)、鍵管理方式「ISAKMP」、プロトコル「ESP」、暗号化方式「DES」、認証方式「SHA」に設定します。

```
Manager B> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
PROTOCOL=ESP ENCALG=DES HASHALG=SHA ↓
```

```
Info (1081003): Operation successful.
```

- 27** SAスペック1だけからなるSAバンドルスペック1を作成します。鍵管理方式は「ISAKMP」を指定します。

```
Manager B> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
STRING="1" ↓
```

```
Info (1081003): Operation successful.
```

- 28** ISAKMPメッセージを素通しさせるIPsecポリシー「isa」を作成します。ポリシーの適用対象を、ローカルの500番ポートからリモートの500番ポート宛のUDPパケット(ISAKMP)に設定します。

```
Manager B> CREATE IPSEC POLICY="isa"
INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500
TRANSPORT=UDP ↓
```

```
Info (1081003): Operation successful.
```

ISAKMPを使用する場合は、必ず最初のIPsecポリシーでISAKMPメッセージが通過できるような設定を行ってください。「IPsecポリシー」は設定順に検索され、最初にマッチしたものが適用されるため、設定順序には注意が必要です。検索順は「SHOW IPSEC POLICY」コマンドで確認できます。また、検索順を変更するには、「SET IPSEC POLICY」コマンドのPOSITIONパラメータを使用します。

- 29** 実際のIPsec通信に使用するIPsecポリシー「vpn_A」をPPPOに対して作成します。鍵管理方式「ISAKMP」、PEERには拠点AのルーターのIPアドレスを、BUNDLEにはSAバンドルスペック「1」を指定します。

```
Manager B> CREATE IPSEC POLICY="vpn_A"
INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUN-
DLE=1 PEER=192.0.2.1 ↓
```

```
Info (1081003): Operation successful.
```

- 30** IPsecポリシー「vpn_A」に対して実際にIPsec通信を行なうIPアドレスの範囲を指定します。コマンドが長くなるため、できるだけ省略形を用いてください。

拠点B

```
Manager B> SET IPSEC POLICY="vpn_A"
LAD=192.168.2.0 LMA=255.255.255.0
RAD=192.168.1.0 RMA=255.255.255.0 ↓
```

```
Info (1081003): Operation successful.
```

拠点C

```
Manager C> SET IPSEC POLICY="vpn_A"  
LAD=192.168.3.0 LMA=255.255.255.0  
RAD=192.168.1.0 RMA=255.255.255.0 ↓
```

```
Info (1081003): Operation successful.
```

- 31 インターネットへの平文通信を許可するIPsecポリシー「inet」をPPPインターフェース0に対して作成します。

```
Manager B> CREATE IPSEC POLICY="inet"  
INT=ppp0 ACTION=PERMIT ↓
```

```
Info (1081003): Operation successful.
```

インターネットにもアクセスしたい場合は、必ず最後のIPsecポリシーですべてのパケットを通過させる設定を行ってください。どのIPsecポリシーにもマッチしなかったトラフィックはデフォルトで破棄されてしまうため、上記の設定がないとVPN以外との通信ができなくなります。

- 32 IPsecモジュールを有効にします。

```
Manager B> ENABLE IPSEC ↓
```

```
Info (1081003): Operation successful.
```

- 33 ISAKMPモジュールを有効にします。

```
Manager B> ENABLE ISAKMP ↓
```

```
Info (1082057): ISAKMP has been enabled.
```

- 34 Security Officerレベルのユーザーでログインしなします。

拠点B

```
Manager B> LOGIN secoff ↓
```

```
Password: passwdsb
```

拠点C

```
Manager C> LOGIN secoff ↓
```

```
Password: passwdsc
```

- 35 動作モードをセキュリティモードに切り替えます。

```
SecOff B> ENABLE SYSTEM SECURITY_MODE ↓
```

```
Info (1034003): Operation successful.
```

セキュリティモードでは、Security OfficerレベルでのTelnetログインが原則として禁止されています。セキュリティモード

において、Security OfficerレベルでTelnetログインしたい場合は、あらかじめRSO (Remote Security Officer) の設定を行っておいてください。



本書「5.4 ノーマルモード / セキュリティモード」(p.54)

●設定の保存

- 36 WAN側インターフェースのUTPケーブルが抜けているのを確認し、設定を保存します。

```
SecOff B> CREATE CONFIG=ROUTER.CFG ↓
```

```
Info (1049003): Operation successful.
```

もし、ケーブルが刺さっていた場合は、ケーブルを抜き「SHOW PPP」コマンドで、接続が切断されているのを確認してから保存します。

- 37 保存したファイルを起動時設定ファイルに指定します。

```
SecOff B> SET CONFIG=ROUTER.CFG ↓
```

```
Info (1049003): Operation successful.
```

接続の確認

- 38 拠点A、B、CともにUTPケーブルを接続し、「SHOW PPP」コマンドでPPPの接続が確立 (OPENED) したことを確認してください。

- 39 LAN側のコンピューターから、相手側の社内サーバーなどが参照できることを確認してください。^{*12}



*12 サブネット間でWindowsのネットワークドライブを参照するためには、例えばWindows 2000/XPでは「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーのIPアドレスなどを指定します。
(例) \\192.168.1.10

まとめ

サイトA、B、Cそれぞれで、前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 13.6.4 設定スクリプトファイル 拠点 A

1	SET SYSTEM NAME=A
2	ADD USER=secoff PASSWORD=passwdSA PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_a@example.co.jp PASSWORD=passwd_a LQR=OFF ECHO=ON
5	ENABLE IP
6	ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0
7	ADD IP INT=ppp0 IP=192.0.2.1 MASK=255.255.255.255
8	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
9	ENABLE TRIGGER
10	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
11	CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp
12	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp
13	ENABLE FIREWALL
14	CREATE FIREWALL POLICY=net
15	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
16	DISABLE FIREWALL POLICY=net IDENTPROXY
17	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
19	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
20	ADD FIREWALL POLICY=net RU=1 AC=ALLOW INT=ppp0 PROTO=UDP GBLPO=500 GBLIP=192.0.2.1 PO=500 IP=192.0.2.1
21	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1- 192.168.1.254
22	SET FIREWALL POLICY=net RU=2 REMOTEIP=192.168.2.1-192.168.2.254
23	ADD FIREWALL POLICY=net RU=3 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.1.1- 192.168.1.254
24	SET FIREWALL POLICY=net RU=3 REMOTEIP=192.168.3.1-192.168.3.254

表 13.6.4 設定スクリプトファイル 拠点 A

25	ADD FIREWALL POLICY=net RU=4 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.1.1-192.168.1.254 ENCAP=IPSEC
26	CREATE ISAKMP POLICY="i_B" PEER=ANY KEY=1 SENDN=TRUE REMOTEID="client_B" MODE=AGGRESSIVE HEARTBEATMODE=BOTH
27	CREATE ISAKMP POLICY="i_C" PEER=ANY KEY=2 SENDN=TRUE REMOTEID="client_C" MODE=AGGRESSIVE HEARTBEATMODE=BOTH
28	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
29	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
30	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
31	CREATE IPSEC POLICY="vpn_B" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=DYNAMIC
32	CREATE IPSEC POLICY="vpn_C" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=DYNAMIC
33	SET IPSEC POLICY="vpn_B" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.2.0 RMA=255.255.255.0
34	SET IPSEC POLICY="vpn_C" LAD=192.168.1.0 LMA=255.255.255.0 RAD=192.168.3.0 RMA=255.255.255.0
35	CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT
36	ENABLE IPSEC
37	ENABLE ISAKMP

表 13.6.5 設定スクリプトファイル 拠点 B

1	SET SYSTEM NAME=B
2	ADD USER=secoff PASSWORD=passwdSB PRIVILEGE=SECURITYOFFICER
3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_b@example.co.jp PASSWORD=passwd_b LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.2.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0

表 13.6.5 設定スクリプトファイル 拠点B

10	ENABLE TRIGGER
11	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
12	CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp
13	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp
14	ENABLE FIREWALL
15	CREATE FIREWALL POLICY=net
16	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
17	DISABLE FIREWALL POLICY=net IDENTPROXY
18	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
19	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
20	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
21	ADD FIREWALL POLICY=net RU=1 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.2.1- 192.168.2.254
22	SET FIREWALL POLICY=net RU=1 REMOTEIP=192.168.1.1-192.168.1.254
23	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.2.1-192.168.2.254 ENCAP=IPSEC
24	CREATE ISAKMP POLICY="i_A" PEER=192.0.2.1 KEY=1 SENDN=TRUE LOCALID="client_B" MODE=AGGRESSIVE HEARTBEATMODE=BOTH
25	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
26	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
27	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
28	CREATE IPSEC POLICY="vpn_A" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=192.0.2.1
29	SET IPSEC POLICY="vpn_A" LAD=192.168.2.0 LMA=255.255.255.0 RAD=192.168.1.0 RMA=255.255.255.0
30	CREATE IPSEC POLICY="inet" INT=ppp0 ACTION=PERMIT
31	ENABLE IPSEC
32	ENABLE ISAKMP

表 13.6.6 設定スクリプトファイル 拠点C

1	SET SYSTEM NAME=C
2	ADD USER=secoff PASSWORD=passwdSC PRIVILEGE=SECURITYOFFICER

表 13.6.6 設定スクリプトファイル 拠点C

3	CREATE PPP=0 OVER=eth0-any
4	SET PPP=0 OVER=eth0-any BAP=OFF USER=site_c@example.co.jp PASSWORD=passwd_c IPREQUEST=ON LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.3.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
10	ENABLE TRIGGER
11	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
12	CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp
13	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp
14	ENABLE FIREWALL
15	CREATE FIREWALL POLICY=net
16	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
17	DISABLE FIREWALL POLICY=net IDENTPROXY
18	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
19	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
20	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
21	ADD FIREWALL POLICY=net RU=1 AC=NONAT INT=vlan1 PROT=ALL IP=192.168.3.1- 192.168.3.254
22	SET FIREWALL POLICY=net RU=1 REMOTEIP=192.168.1.1-192.168.1.254
23	ADD FIREWALL POLICY=net RU=2 AC=NONAT INT=ppp0 PROT=ALL IP=192.168.3.1-192.168.3.254 ENCAP=IPSEC
25	CREATE ISAKMP POLICY="i_A" PEER=192.0.2.1 KEY=1 SENDN=TRUE LOCALID="client_C" MODE=AGGRESSIVE HEARTBEATMODE=BOTH
26	CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP PROTOCOL=ESP ENCALG=DES HASHALG=SHA
27	CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP STRING="1"
28	CREATE IPSEC POLICY="isa" INT=ppp0 ACTION=PERMIT LPORT=500 RPORT=500 TRANSPORT=UDP
29	CREATE IPSEC POLICY="vpn_A" INT=ppp0 ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1 PEER=192.0.2.1

表 13.6.6 設定スクリプトファイル 拠点 C

```

30 SET IPSEC POLICY="vpn_A" LAD=192.168.3.0
   LMA=255.255.255.0 RAD=192.168.1.0
   RMA=255.255.255.0
31 CREATE IPSEC POLICY="inet" INT=ppp0
   ACTION=PERMIT
32 ENABLE IPSEC
33 ENABLE ISAKMP
  
```

「SET TIME」、「ADD SCRIPT」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

拠点A、B、Cともに以下のスクリプトは共通です。

表 13.6.7 スクリプト「reset.scp」

```
RESET PPP=0
```

表 13.6.8 スクリプト「up.scp」

```
DISABLE TRIGGER=1
```

表 13.6.9 スクリプト「down.scp」

```
ENABLE TRIGGER=1
```

13.7 インターネットと CUG サービスの同時接続 (端末型)

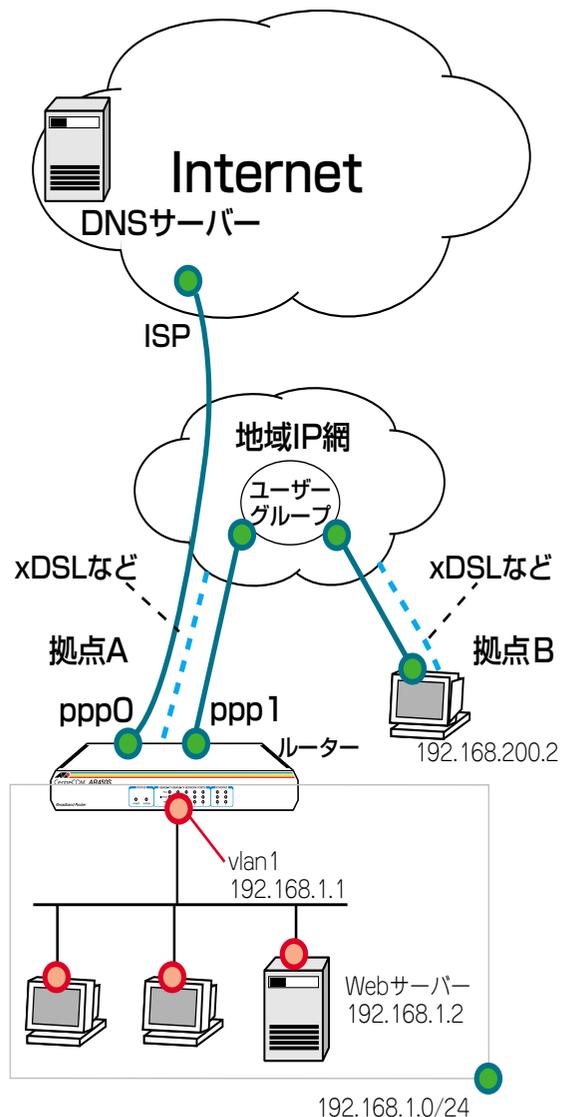


図13.7.1 インターネットとCUGサービスの同時接続(端末型)

PPPoE セッションを 2 本同時に使い、インターネット接続と、フレッツ・グループアクセス(ライト)およびフレッツ・グループ(ベー

シックメニュー)の CUG (Closed Users Group) サービス (端末型)を同時に利用します。

この例では、LAN 側はプライベートアドレスで運用し、相手先のアドレスによって、スタティックな経路制御を行いパケットを振り分けます。クライアントはダイナミック ENAT 経由でインターネットや CUG サービスにアクセスします。また、ファイアウォールを使って外部からのアクセスを拒否します。

プロバイダーから提供される情報

以下の説明では、プロバイダーもしくは CUG サービスの管理者から下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●インターネット接続

- 接続のユーザー名: site_a@example.co.jp
- 接続のパスワード: passwd_a
- PPPoE サービス名: 指定なし
- 使用できる IP アドレス: 動的割り当て (1 個不定)
- DNS サーバー: 接続時に通知される

●CUG サービス

- 接続のユーザー名: flets_a
- 接続のパスワード: fpasswd_a
- PPPoE サービス名: 指定なし
- 使用できる IP アドレス: 動的割り当て (1 個)
- 他のユーザーの IP アドレス: 192.168.200.2/32

設定の方針

- スタティックルーティングにより、CUG サービス内の他ユーザー宛のパケットと、それ以外のパケット (インターネット宛)の転送先を振り分けます。
- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようになります。
- ファイアウォールのダイナミック ENAT 機能を使用して、LAN 側ネットワークのプライベート IP アドレスを、WAN 側インターフェースに設定されたアドレスに変換します。インターネット宛のパケットはプロバイダーから与えられたグローバル IP アドレスに、CUG サービス宛のパケットは管理者から指定されたプライベート IP アドレスに変換します。これにより、LAN に接続された複数のコンピューターから、インターネット、CUG サービスへの同時アクセスが可能になります
- CUG サービスからのパケットは、ファイアウォールのルールを使用して、LAN 内の特定のサーバーに振り分けます。

- Web サーバー (ポート 80): 192.168.1.2

- ルーターの DNS リレー機能をオンにして、LAN 側コンピューターからの DNS リクエストを、プロバイダーの DNS サーバーに転送します。
- トリガー機能を使って PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合に、自動的に再接続するよう設定します。
- 本製品の基本設定は、次の通りです。

表 13.7.1 本製品の基本設定

WAN 側物理インターフェース	eth0
インターネット向け WAN 側 (ppp0) IP アドレス	不定
CUG サービス向け WAN 側 (ppp1) IP アドレス	不定
LAN 側 (vlan1) IP アドレス	192.168.1.1/32
DHCP サーバー機能	使わない

設定

- 1 本製品の電源がオフの状態、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。
- 2 本製品の電源スイッチをオンにします。
- 3 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager ↵  
Password: friend (表示されません)
```

●PPP の設定

- 4 WAN 側 Ethernet インターフェース (eth0) 上にインターネットと接続するための PPP インターフェース「0」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵  
Info (1003003): Operation successful.
```

- 5 プロバイダーから通知されたPPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=site_a@example.co.jp
PASSWORD=passwd_a LQR=OFF ECHO=ON ↓
```

```
Info (1003003): Operation successful.
```

- 6 WAN 側 Ethernet インターフェース (eth0) 上に CUG サービスと接続するための PPP インターフェース「1」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=1 OVER=eth0-any ↓
```

```
Info (1003003): Operation successful.
```

- 7 CUG サービス管理者から通知された PPP ユーザー名とパスワードを指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

```
Manager > SET PPP=1 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=flets_a
PASSWORD=fpasswd_a LQR=OFF ECHO=ON ↓
```

```
Info (1003003): Operation successful.
```

● IP、ルーティングの設定

- 8 IP モジュールを有効にします。

```
Manager > ENABLE IP ↓
```

```
Info (1005287): IP module has been enabled.
```

- 9 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェースで使用するよう設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↓
```

```
Info (1005287): Remote IP assignment has been enabled.
```

- 10 LAN 側 (vlan1) インターフェースにプライベート IP アドレスを割り当て、クライアント用のサブネットとします。CUG サービスのアドレス (ppp1) とは、重ならないものを指定してください。

```
Manager > ADD IP INT=vlan1 IP=192.168.1.1
MASK=255.255.255.0 ↓
```

```
Info (1005275): interface successfully added.
```

- 11 インターネット接続用の WAN 側 (ppp0) インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↓
```

```
Info (1005275): interface successfully added.
```

- 12 CUG サービス接続用の WAN 側 (ppp1) インターフェースに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp1 IP=0.0.0.0 ↓
```

```
Info (1005275): interface successfully added.
```

- 13 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0
NEXTHOP=0.0.0.0 ↓
```

```
Info (1005275): IP route successfully added.
```

- 14 CUG サービス向けの経路をスタティックに設定します。CUG サービス内に複数の拠点がある場合には、それぞれの拠点ごとに経路を設定します。

```
Manager > ADD IP ROUTE=192.168.200.2
MASK=255.255.255.255 INT=ppp1
NEXTHOP=0.0.0.0 ↓
```

```
Info (1005275): IP route successfully added.
```

- 15 DNS リレー機能を有効にします。

```
Manager > ENABLE IP DNSRELAY ↓
```

```
Info (1005003): Operation successful.
```

●ファイアウォールの設定

16 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↓  
  
Info (1077257): 19-Apr-2002 19:55:22  
Firewall enabled.  
  
Info (1077003): Operation successful.
```

17 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↓  
  
Info (1077003): Operation successful.
```

18 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。^{*13}

```
Manager > ENABLE FIREWALL POLICY=net  
ICMP_F=PING,UNREACH ↓  
  
Info (1077003): Operation successful.
```

19 ident プロキシ機能を無効にし、外部のメール (SMTP) サーバーなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager > DISABLE FIREWALL POLICY=net  
IDENTPROXY ↓  
  
Info (1077003): Operation successful.
```

20 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1  
TYPE=PRIVATE ↓  
  
Info (1077003): Operation successful.
```

インターネット接続用の WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0  
TYPE=PUBLIC ↓  
  
Info (1077003): Operation successful.
```

CUG サービス接続用の WAN 側 (ppp1) インターフェースを PUBLIC (外部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp1  
TYPE=PUBLIC ↓  
  
Info (1077003): Operation successful.
```

21 LAN 側ネットワークに接続されているすべてのコンピューターが ENAT 機能を使用できるように設定します。インターネット宛てパケットの場合は、NAT アドレスとして ppp0 の IP アドレスを使用します。CUG サービス宛てパケットの場合は、NAT アドレスとして ppp1 の IP アドレスを使用します。ファイアウォールのダイナミック ENAT では、パケットが INT から GBLINT に転送されたときに、パケットの始点アドレスを GBLINT のアドレスに書き換えます。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED  
INT=vlan1 GBLINT=ppp0 ↓  
  
Info (1077003): Operation successful.  
  
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED  
INT=vlan1 GBLINT=ppp1 ↓  
  
Info (1077003): Operation successful.
```

22 CUG サービス側からのルーターに向けた HTTP (ポート 80) パケットを、LAN 内の IP アドレス 192.168.1.2 のサーバーに転送するルールを設定します。他にも公開したいサーバーがあるときには、それぞれについて、ルールを設定します。逆にサーバーを公開しない場合には、このルール設定は不要です。

```
Manager > ADD FIREWALL POLICY=net RU=1  
AC=ALLOW INT=ppp1 PROT=tcp PORT=80  
IP=192.168.1.2 GBLINT=0.0.0.0 GBLP=80 ↓  
  
Info (1077003): Operation successful.
```



^{*13} デフォルト設定では、ICMP はファイアウォールを通過できません。

●トリガーの設定

- 23 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。
ppp0 をリセットするスクリプト reset0.scp を作成します。

```
Manager > ADD SCRIPT=reset0.scp TEXT="RESET  
PPP=0" ↓  
  
File : reset0.scp  
1:RESET PPP=0
```

ppp1 をリセットするスクリプト reset1.scp を作成します。

```
Manager > ADD SCRIPT=reset1.scp TEXT="RESET  
PPP=1" ↓  
  
File : reset1.scp  
1:RESET PPP=1
```

トリガー1 を無効状態にするスクリプト up0.scp を作成します。

```
Manager > ADD SCRIPT=up0.scp TEXT="DISABLE  
TRIGGER=1" ↓  
  
File : up0.scp  
1:DISABLE TRIGGER=1
```

トリガー2 を無効状態にするスクリプト up1.scp を作成します。

```
Manager > ADD SCRIPT=up1.scp TEXT="DISABLE  
TRIGGER=2" ↓  
  
File : up1.scp  
1:DISABLE TRIGGER=2
```

トリガー1 を有効状態にするスクリプト down0.scp を作成します。

```
Manager > ADD SCRIPT=down0.scp TEXT="ENABLE  
TRIGGER=1" ↓  
  
File : down0.scp  
1:ENABLE TRIGGER=1
```

トリガー2 を有効状態にするスクリプト down1.scp を作成します。

```
Manager > ADD SCRIPT=down1.scp TEXT="ENABLE  
TRIGGER=2" ↓  
  
File : down1.scp  
1:ENABLE TRIGGER=2
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド（内蔵フルスクリーンエディター）などを使って設定スクリプトファイル（CFG）にこのコマンドを記述しても意図した結果になりません。

- 24 トリガー機能を有効にします。

```
Manager > ENABLE TRIGGER ↓  
  
Info (1053268): The trigger module has been enabled.
```

- 25 PPPoE セッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順 23 で設定したそれぞれのトリガースクリプトを実行します。
reset0.scp を実行する定期トリガー 1 を作成します。このトリガーは、ppp0 インターフェースがダウンすると同時に有効になり、3分間隔で実行され、アップすると無効になります。

```
Manager > CREATE TRIGGER=1 PERIODIC=3  
SCRIPT=reset0.scp ↓  
  
Info (1053262): Trigger successfully added.
```

reset1.scp を実行する定期トリガー 2 を作成します。このトリガーは、ppp1 インターフェースがダウンすると同時に有効になり、3分間隔で実行され、アップすると無効になります。

```
Manager > CREATE TRIGGER=2 PERIODIC=3  
SCRIPT=reset1.scp ↓  
  
Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up0.scp を実行するインターフェーストリガー 3 を作成します。

```
Manager > CREATE TRIGGER=3 INTERFACE=ppp0  
EVENT=UP CP=IPCP SCRIPT=up0.scp ↓  
  
Info (1053262): Trigger successfully added.
```

ppp1 のアップ時に up1.scp を実行するインターフェーストリガー4を作成します。

```
Manager > CREATE TRIGGER=4 INTERFACE=ppp1
EVENT=UP CP=IPCP SCRIPT=up1.scp ↓
Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down0.scp を実行するインターフェーストリガー5を作成します。

```
Manager > CREATE TRIGGER=5 INTERFACE=ppp0
EVENT=DOWN CP=IPCP SCRIPT=down0.scp ↓
Info (1053262): Trigger successfully added.
```

ppp1 のダウン時に down1.scp を実行するインターフェーストリガー6を作成します。

```
Manager > CREATE TRIGGER=6 INTERFACE=ppp1
EVENT=DOWN CP=IPCP SCRIPT=down1.scp ↓
Info (1053262): Trigger successfully added.
```



本書「トリガーの動作」(p.135)

●時刻、パスワード、設定保存

26 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=21-APR-2002 ↓
System time is 01:00:01 on Sunday 21-Apr-2002.
```

27 ユーザー「manager」のパスワードを変更します。Confirm: の入力を終えたとき、コマンドプロンプトが表示されない場合は、リターンキーを押してください。

```
Manager > SET PASSWORD ↓
Old password: friend ↓
New password: xxxxxxxx ↓
Confirm: xxxxxxxx ↓
```

28 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↓
Info (1049003): Operation successful.
```

29 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↓
Info (1049003): Operation successful.
```

30 WAN 側 (eth0) インターフェースに UTP ケーブルを接続してください。

●接続の確認

31 PPP の接続の確立は、「SHOW PPP」コマンドで確認できます。トリガー1、トリガー2は3分間隔で実行されるので、UTP ケーブルを接続してから、PPP の接続確立まで最長3分かかります(ご契約のプロバイダー側の機器によっては更に数分かかることがあります)。「SHOW PPP」コマンドを繰り返し入力しながら、State が「CLOSED」から「OPENED」に変わるまで待ってください。

```
Manager > SHOW PPP ↓
```

Name	Enabled	ifIndex	Over	CP	State
ppp0	YES	04	eth0-any	IPCP	OPENED
				LCP	OPENED
ppp1	YES	04	eth0-any	IPCP	OPENED
				LCP	OPENED

32 LAN 側のコンピューターで Web ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合 (DHCP クライアントである場合)、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動 (または再起動) する必要があります。

33 LAN 側のコンピューターから、CUG サービスで接続しているサーバーなどが参照できることを確認してください。^{*14}



*14 サブネット間で Windows のネットワークドライブを参照するためには、例えば Windows 2000/XP では「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーの IP アドレスなどを指定します。
(例) \\192.168.1.10

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 13.7.2 設定スクリプトファイル (ROUTER.CFG)

```

1 CREATE PPP=0 OVER=eth0-any
2 SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON
  USER=site_a@example.co.jp PASSWORD=passwd_a
  LQR=OFF ECHO=ON
3 CREATE PPP=1 OVER=eth0-any
4 SET PPP=1 OVER=eth0-any BAP=OFF IPREQUEST=ON
  USER=flets_a PASSWORD=fpasswd_a LQR=OFF
  ECHO=ON
5 ENABLE IP
6 ENABLE IP REMOTEASSIGN
7 ADD IP INT=vlan1 IP=192.168.1.1
  MASK=255.255.255.0
8 ADD IP INT=ppp0 IP=0.0.0.0
9 ADD IP INT=ppp1 IP=0.0.0.0
10 ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
11 ADD IP ROUTE=192.168.200.2
  MASK=255.255.255.255 INT=ppp1 NEXTHOP=0.0.0.0
12 ENABLE IP DNSRELAY
13 ENABLE FIREWALL
14 CREATE FIREWALL POLICY=net
15 ENABLE FIREWALL POLICY=net
  ICMP_F=PING,UNREACHABLE
16 DISABLE FIREWALL POLICY=net IDENTPROXY
17 ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18 ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
19 ADD FIREWALL POLICY=net INT=ppp1 TYPE=PUBLIC
20 ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1
  GBLINT=ppp0
21 ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1
  GBLINT=ppp1
22 ADD FIREWALL POLICY=net RU= 1 AC=ALLOW
  INT=ppp1 PROT=tcp PORT=80 IP=192.168.1.2
  GBLIP=0.0.0.0 GBLP=80
23 ENABLE TRIGGER
24 CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset0.scp
25 CREATE TRIGGER=2 PERIODIC=3 SCRIPT=reset1.scp
26 CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=UP
  CP=IPCP SCRIPT=up0.scp
27 CREATE TRIGGER=4 INTERFACE=ppp1 EVENT=UP
  CP=IPCP SCRIPT=up1.scp

```

表 13.7.2 設定スクリプトファイル (ROUTER.CFG)

```

28 CREATE TRIGGER=5 INTERFACE=ppp0 EVENT=DOWN
  CP=IPCP SCRIPT=down0.scp
29 CREATE TRIGGER=6 INTERFACE=ppp1 EVENT=DOWN
  CP=IPCP SCRIPT=down1.scp

```

「SET TIME」、「ADD SCRIPT」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください。

表 13.7.3 スクリプト「reset0.scp」

```
RESET PPP=0
```

表 13.7.4 スクリプト「reset1.scp」

```
RESET PPP=1
```

表 13.7.5 スクリプト「up0.scp」

```
DISABLE TRIGGER=1
```

表 13.7.6 スクリプト「up1.scp」

```
DISABLE TRIGGER=2
```

表 13.7.7 スクリプト「down0.scp」

```
ENABLE TRIGGER=1
```

表 13.7.8 スクリプト「down1.scp」

```
ENABLE TRIGGER=2
```

13.8 インターネットと CUG サービスの同時接続 (LAN 型)

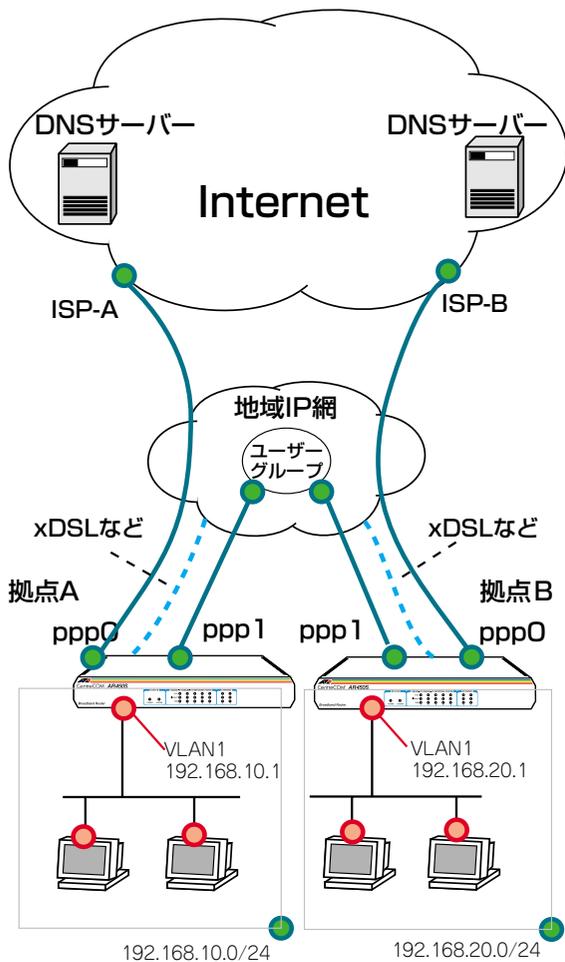


図 13.8.1 インターネットと CUG サービスの同時接続 (LAN 型)

PPPoE セッションを 2 本同時に使って、インターネット接続と、フレッツ・グループアクセス (プロ) およびフレッツ・グループ (ビジネスメニュー) の CUG (Closed Users Group) サービス (LAN 型) を同時に利用します。

この例では、各拠点の LAN 側はプライベートアドレスで運用し、相手先のアドレスによって、スタティックな経路制御を行いパケットを

振り分けます。クライアントはインターネットにはダイナミック ENAT 経由で、CUG サービスにはプライベートアドレスのままアクセスします。また、ファイアウォールを使って外部からのアクセスを拒否します。

プロバイダーから提供される情報

以下の説明では、プロバイダーから下記の契約情報が与えられていると仮定します。実際の設定には、お客様の契約情報をご使用ください。

●拠点 A のインターネット接続

- 接続のユーザー名: site_a@example.co.jp
- 接続のパスワード: passwd_a
- PPPoE サービス名: 指定なし
- 使用できる IP アドレス: 動的割り当て (1 個不定)
- DNS サーバー: 接続時に通知される

●拠点 B のインターネット接続

- 接続のユーザー名: site_b@example.co.jp
- 接続のパスワード: passwd_b
- PPPoE サービス名: 指定なし
- 使用できる IP アドレス: 動的割り当て (1 個不定)
- DNS サーバー: 接続時に通知される

●拠点 A の CUG サービス

- 接続のユーザー名: flets_a
- 接続のパスワード: fpasswd_a
- PPPoE サービス名: 指定なし
- CUG サービスのネットワークアドレス: 192.168.10.0/24

●拠点 B の CUG サービス

- 接続のユーザー名: flets_b
- 接続のパスワード: fpasswd_b
- PPPoE サービス名: 指定なし
- CUG サービスのネットワークアドレス: 192.168.20.0/24

設定の方針

- スタティックルーティングにより、CUG サービス内の他ユーザー宛のパケットと、それ以外のパケット (インターネット宛) の転送先を振り分けます。
- ファイアウォールを利用して、外部からの不正アクセスを遮断しつつ、内部からは自由にインターネットへのアクセスができるようにします。

- ファイアウォールのダイナミック ENAT 機能を使用して、インターネット宛てのパケットはLAN 側ネットワークのプライベート IP アドレスを、インターネット向け WAN 側インターフェースに設定されたアドレスに変換します。CUG サービス向け WAN 側インターフェースはアンナンバードとして、LAN 内のコンピュータは設定されたプライベートアドレスそのままでの拠点にアクセスします。
- ルーターの DNS リレー機能をオンにして、LAN 側コンピュータからの DNS リクエストを、プロバイダーの DNS サーバーに転送します。
- トリガー機能を使って PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合に、自動的に再接続するように設定します。
- 本製品の基本設定は、次の通りです。

表 13.8.1 本製品の基本設定

WAN 側物理インターフェース	eth0	eth0
インターネット向け WAN 側 (ppp0) IP アドレス	不定	不定
CUG サービス向け WAN 側 (ppp1) IP アドレス	不定	不定
LAN 側 (vlan1) IP アドレス	192.168.10.1 /24	192.168.20.1 /24
DHCP サーバー機能	使わない	使わない

設定

各拠点では、設定する IP アドレスなどの設定値が異なるだけで、基本的な設定方法は同じです。

各拠点で設定値が違う部分については、それぞれ向けの操作例などを明示します。それ以外の部分は両拠点について同様の設定を行ってください。

- 1 本製品の電源がオフの状態、本製品の WAN 側 (ETH0) の UTP ケーブルを外し、PPP インターフェースがリンクアップしないようにしておきます。これは、後述のトリガーの設定中にリンク状態 (アップ、ダウン) が変化しないようにするための措置です。
- 2 本製品の電源スイッチをオンにします。
- 3 ユーザー「manager」でログインします。デフォルトのパスワードは「friend」です。

```
login: manager ↵
Password: friend (表示されません)
```

● PPP の設定

- 4 WAN 側 Ethernet インターフェース (eth0) 上にインターネットと接続するための PPP インターフェース「0」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=0 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

- 5 プロバイダーから通知された PPP ユーザー名とパスワードをそれぞれの拠点ごとに指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

拠点 A

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=site_a@example.co.jp
PASSWORD=passwd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

拠点 B

```
Manager > SET PPP=0 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=site_b@example.co.jp
PASSWORD=passwd_b LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

- 6 WAN 側 Ethernet インターフェース (eth0) 上に CUG サービスと接続するための PPP インターフェース「1」を作成します。「OVER=eth0-XXXX」の「XXXX」の部分には、通知された PPPoE の「サービス名」を記述します。指定がない場合は、どのサービス名タグでも受け入れられるよう、「any」を設定します。

```
Manager > CREATE PPP=1 OVER=eth0-any ↵

Info (1003003): Operation successful.
```

- 7 CUG サービス管理者から通知された PPP ユーザー名とパスワードをそれぞれの拠点ごとに指定し、接続時に IP アドレス割り当ての要求を行うように設定します。LQR はオフにし、代わりに LCP Echo パケットを使って PPP リンクの状態を監視するようにします。また、ISDN 向けの機能である BAP はオフにします。

拠点 A

```
Manager > SET PPP=1 OVER=eth0-any BAP=OFF
IPREQUEST=ON USER=flets_a
PASSWORD=fpasswd_a LQR=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

拠点B

```
Manager > SET PPP=1 OVER=eth0-any BAP=OFF  
IPREQUEST=ON USER=flets_b  
PASSWORD=fpasswd_b LQR=OFF ECHO=ON ↓
```

```
Info (1003003): Operation successful.
```

● IP、ルーティングの設定

8 IP モジュールを有効にします。

```
Manager > ENABLE IP ↓
```

```
Info (1005287): IP module has been enabled.
```

9 IPCP ネゴシエーションで与えられた IP アドレスを PPP インターフェイスで使用するよう設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↓
```

```
Info (1005287): Remote IP assignment has been enabled.
```

10 LAN 側 (vlan1) インターフェイスに CUG サービス管理者から指定された IP アドレスをそれぞれの拠点ごとに指定します。

拠点A

```
Manager > ADD IP INT=vlan1 IP=192.168.10.1  
MASK=255.255.255.0 ↓
```

```
Info (1005275): interface successfully added.
```

拠点B

```
Manager > ADD IP INT=vlan1 IP=192.168.20.1  
MASK=255.255.255.0 ↓
```

```
Info (1005275): interface successfully added.
```

11 インターネット接続用の WAN 側 (ppp0) インターフェイスに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp0 IP=0.0.0.0 ↓
```

```
Info (1005275): interface successfully added.
```

12 CUG サービス接続用の WAN 側 (ppp1) インターフェイスに IP アドレス「0.0.0.0」を設定します。プロバイダーとの接続が確立するまで、IP アドレスは確定しません。

```
Manager > ADD IP INT=ppp1 IP=0.0.0.0 ↓
```

```
Info (1005275): interface successfully added.
```

13 デフォルトルートを設定します。

```
Manager > ADD IP ROUTE=0.0.0.0 INT=ppp0  
NEXTHOP=0.0.0.0 ↓
```

```
Info (1005275): IP route successfully added.
```

14 他の拠点向けの経路をスタティックに設定します。拠点が 3 つ以上ある場合には、それぞれの拠点向けに ROUTE、MASK の値を適切なものに変更して、複数登録してください。

拠点A

```
Manager > ADD IP ROUTE=192.168.20.0  
MASK=255.255.255.0 INT=ppp1  
NEXTHOP=0.0.0.0 ↓
```

```
Info (1005275): IP route successfully added.
```

拠点B

```
Manager > ADD IP ROUTE=192.168.10.0  
MASK=255.255.255.0 INT=ppp1  
NEXTHOP=0.0.0.0 ↓
```

```
Info (1005275): IP route successfully added.
```

15 DNS リレー機能を有効にします。

```
Manager > ENABLE IP DNSRELAY ↓
```

```
Info (1005003): Operation successful.
```

●ファイアウォールの設定

16 ファイアウォール機能を有効にします。

```
Manager > ENABLE FIREWALL ↓
```

```
Info (1077257): 19-Apr-2002 19:55:22  
Firewall enabled.
```

```
Info (1077003): Operation successful.
```

17 ファイアウォールの動作を規定するファイアウォールポリシー「net」を作成します。ポリシーの文字列は、お客様によって任意に設定できます。

```
Manager > CREATE FIREWALL POLICY=net ↓
```

```
Info (1077003): Operation successful.
```

- 18 ICMP パケットは Ping (Echo/Echo Reply) と到達不可能 (Unreachable) のみ双方向で許可します。*15

```
Manager > ENABLE FIREWALL POLICY=net
ICMP_F=PING,UNREACH ↓
Info (1077003): Operation successful.
```

- 19 ident プロキシ機能を無効にし、外部のメール (SMTP) サーバなどからの ident 要求に対して、ただちに TCP RST を返すよう設定します。

```
Manager > DISABLE FIREWALL POLICY=net
IDENTPROXY ↓
Info (1077003): Operation successful.
```

- 20 ファイアウォールポリシーの適用対象となるインターフェースを指定します。

LAN 側 (vlan1) インターフェースを PRIVATE (内部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=vlan1
TYPE=PRIVATE ↓
Info (1077003): Operation successful.
```

インターネット接続用の WAN 側 (ppp0) インターフェースを PUBLIC (外部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0
TYPE=PUBLIC ↓
Info (1077003): Operation successful.
```

CUG サービス接続用の WAN 側 (ppp1) インターフェースを PUBLIC (外部) に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp1
TYPE=PUBLIC ↓
Info (1077003): Operation successful.
```

- 21 LAN 側ネットワークに接続されているすべてのコンピュータがインターネットへの通信に ENAT 機能を使用できるように設定します。NAT アドレスとして ppp0 の IP アドレスを使用します。ファイアウォールのダイナミック ENAT では、パケットが INT から GBLINT に転送されたときに、パケットの始点アドレスを GBLINT のアドレスに書き換えます。



*15 デフォルト設定では、ICMP はファイアウォールを通過できません。

CUG サービス宛てパケットの場合は、NAT は使いません。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
INT=vlan1 GBLINT=ppp0 ↓
Info (1077003): Operation successful.
```

- 22 他の拠点からの通信をすべて許可するルールを設定します。拠点が 3 つ以上ある場合には、すべての拠点の IP アドレスごとの REMOTEIP を指定したルールを設定してください。

拠点 A

```
Manager > ADD FIREWALL POLICY=net RULE=1
AC=ALLOW INT=ppp1 PROT=ALL
REMOTEIP=192.168.20.1-192.168.20.254 ↓
Info (1077003): Operation successful.
```

拠点 B

```
Manager > ADD FIREWALL POLICY=net RULE=1
AC=ALLOW INT=ppp1 PROT=ALL
REMOTEIP=192.168.10.1-192.168.10.254 ↓
Info (1077003): Operation successful.
```

●トリガーの設定

- 23 PPPoE セッションを自動再接続するためのトリガースクリプトを作成します。ppp0 をリセットするスクリプト reset0.scp を作成します。

```
Manager > ADD SCRIPT=reset0.scp TEXT="RESET
PPP=0" ↓
File : reset0.scp
1:RESET PPP=0
```

ppp1 をリセットするスクリプト reset1.scp を作成します。

```
Manager > ADD SCRIPT=reset1.scp TEXT="RESET
PPP=1" ↓
File : reset1.scp
1:RESET PPP=1
```

トリガー 1 を無効状態にするスクリプト up0.scp を作成します。

```
Manager > ADD SCRIPT=up0.scp TEXT="DISABLE
TRIGGER=1" ↓
File : up0.scp
1:DISABLE TRIGGER=1
```

トリガー2を無効状態にするスクリプト up1.scp を作成します。

```
Manager > ADD SCRIPT=up1.scp TEXT="DISABLE
TRIGGER=2" ↓

File : up1.scp
1:DISABLE TRIGGER=2
```

トリガー1を有効状態にするスクリプト down0.scp を作成します。

```
Manager > ADD SCRIPT=down0.scp TEXT="ENABLE
TRIGGER=1" ↓

File : down0.scp
1:ENABLE TRIGGER=1
```

トリガー2を有効状態にするスクリプト down1.scp を作成します。

```
Manager > ADD SCRIPT=down1.scp TEXT="ENABLE
TRIGGER=2" ↓

File : down1.scp
1:ENABLE TRIGGER=2
```

「ADD SCRIPT」コマンドは、コンソールなどからログインした状態で、実行するためのコマンドです。そのため、「EDIT」コマンド（内蔵フルスクリーンエディター）などを使って設定スクリプトファイル（.CFG）にこのコマンドを記述しても意図した結果になりません。

24 トリガー機能を有効にします。

```
Manager > ENABLE TRIGGER ↓

Info (1053268): The trigger module has been enabled.
```

25 PPPoEセッションを自動再接続するためのトリガーを作成します。これらのトリガーは手順23で設定したそれぞれのトリガースクリプトを実行します。

reset0.scp を実行する定期トリガー1を作成します。このトリガーは、ppp0 インターフェイスがダウンすると同時に有効になり、3分間隔で実行され、アップすると無効になります。

```
Manager > CREATE TRIGGER=1 PERIODIC=3
SCRIPT=reset0.scp ↓

Info (1053262): Trigger successfully added.
```

reset1.scp を実行する定期トリガー2を作成します。このトリガーは、ppp1 インターフェイスがダウンすると同時に有効にな

り、3分間隔で実行され、アップすると無効になります。

```
Manager > CREATE TRIGGER=2 PERIODIC=3
SCRIPT=reset1.scp ↓

Info (1053262): Trigger successfully added.
```

ppp0 のアップ時に up0.scp を実行するインターフェーストリガー3を作成します。

```
Manager > CREATE TRIGGER=3 INTERFACE=ppp0
EVENT=UP CP=IPCP SCRIPT=up0.scp ↓

Info (1053262): Trigger successfully added.
```

ppp1 のアップ時に up1.scp を実行するインターフェーストリガー4を作成します。

```
Manager > CREATE TRIGGER=4 INTERFACE=ppp1
EVENT=UP CP=IPCP SCRIPT=up1.scp ↓

Info (1053262): Trigger successfully added.
```

ppp0 のダウン時に down0.scp を実行するインターフェーストリガー5を作成します。

```
Manager > CREATE TRIGGER=5 INTERFACE=ppp0
EVENT=DOWN CP=IPCP SCRIPT=down0.scp ↓

Info (1053262): Trigger successfully added.
```

ppp1 のダウン時に down1.scp を実行するインターフェーストリガー6を作成します。

```
Manager > CREATE TRIGGER=6 INTERFACE=ppp1
EVENT=DOWN CP=IPCP SCRIPT=down1.scp ↓

Info (1053262): Trigger successfully added.
```

 本書「トリガーの動作」(p.135)

●時刻、パスワード、設定保存

26 時刻を設定します。以前、時刻を設定したことがある場合、時刻の再設定は不要です。

```
Manager > SET TIME=01:00:01 DATE=21-APR-2002 ↓

System time is 01:00:01 on Sunday 21-Apr-2002.
```

27 ユーザー「manager」のパスワードを変更します。Confirm: の入力を終えたとき、コマンドプロンプトが表示されない場合は、

リターンキーを押してください。

```
Manager > SET PASSWORD ↓  
  
Old password: friend ↓  
New password: xxxxxxxx ↓  
Confirm: xxxxxxxx ↓
```

- 28 設定は以上です。設定内容を設定スクリプトファイルに保存します。

```
Manager > CREATE CONFIG=ROUTER.CFG ↓  
  
Info (1049003): Operation successful.
```

- 29 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↓  
  
Info (1049003): Operation successful.
```

- 30 WAN 側 (eth0) インターフェースに UTP ケーブルを接続してください。

●接続の確認

- 31 PPP の接続の確立は、「SHOW PPP」コマンドで確認できます。トリガー1、トリガー2は3分間隔で実行されるので、UTP ケーブルを接続してから、PPP の接続確立まで最長3分かかります(ご契約のプロバイダー側の機器によっては更に数分がかかることがあります)。「SHOW PPP」コマンドを繰り返し入力しながら、State が「CLOSED」から「OPENED」に変わるまで待ってください。

```
Manager > SHOW PPP ↓  
  
Name      Enabled ifIndex Over      CP      State  
-----  
ppp0      YES      04      eth0-any  IPCP    OPENED  
          YES      04      eth0-any  LCP     OPENED  
ppp1      YES      04      eth0-any  IPCP    OPENED  
          YES      04      eth0-any  LCP     OPENED  
-----
```

- 32 LAN 側のコンピューターで Web ブラウザーなどを実行し、インターネットにアクセスできることを確認してください。

なお、LAN 側のコンピューターが IP アドレスを自動取得するように設定されている場合 (DHCP クライアントである場合)、本製品の DHCP サーバー機能を設定した後に、コンピューターを起動 (または再起動) する必要があります。

- 33 LAN 側のコンピューターから、CUG サービスで接続しているサーバーなどが参照できることを確認してください。^{*16}

まとめ

前述の設定手順を実行することによって、作成、保存される設定スクリプトファイルを示します。

表 13.8.2 拠点 A の設定スクリプトファイル (ROUTER.A.CFG)

```
1 CREATE PPP=0 OVER=eth0-any  
2 SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON  
  USER=site_a@example.co.jp PASSWORD=passwd_a  
  LQR=OFF ECHO=ON  
3 CREATE PPP=1 OVER=eth0-any  
4 SET PPP=1 OVER=eth0-any BAP=OFF IPREQUEST=ON  
  USER=flets_a PASSWORD=fpasswd_a LQR=OFF  
  ECHO=ON  
5 ENABLE IP  
6 ENABLE IP REMOTEASSIGN  
7 ADD IP INT=vlan1 IP=192.168.10.1  
  MASK=255.255.255.0  
8 ADD IP INT=ppp0 IP=0.0.0.0  
9 ADD IP INT=ppp1 IP=0.0.0.0  
10 ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0  
11 ADD IP ROUTE=192.168.20.0 MASK=255.255.255.0  
  INT=ppp1 NEXTHOP=0.0.0.0  
12 ENABLE IP DNSRELAY  
13 ENABLE FIREWALL  
14 CREATE FIREWALL POLICY=net  
15 ENABLE FIREWALL POLICY=net  
  ICMP_F=PING, UNREACHABLE  
16 DISABLE FIREWALL POLICY=net IDENTPROXY  
17 ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE  
18 ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC  
19 ADD FIREWALL POLICY=net INT=ppp1 TYPE=PUBLIC  
20 ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1  
  GBLINT=ppp0  
21 ADD FIREWALL POLICY=net RULE=1 AC=ALLOW  
  INT=ppp1 PROT=ALL REMOTEIP=192.168.20.1-  
  192.168.20.254  
22 ENABLE TRIGGER  
23 CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset0.scp
```



*16 サブネット間で Windows のネットワークドライブを参照するためには、例えば Windows 2000/XP では「マイネットワーク」→「ネットワークプレースの追加」で現れるダイアログボックスで、サーバーの IP アドレスなどを指定します。

(例) ¥¥192.168.1.10

表 13.8.2 拠点 A の設定スクリプトファイル (ROUTERA.CFG)

24	CREATE TRIGGER=2 PERIODIC=3 SCRIPT=reset1.scp
25	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up0.scp
26	CREATE TRIGGER=4 INTERFACE=ppp1 EVENT=UP CP=IPCP SCRIPT=up1.scp
27	CREATE TRIGGER=5 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down0.scp
28	CREATE TRIGGER=6 INTERFACE=ppp1 EVENT=DOWN CP=IPCP SCRIPT=down1.scp

表 13.8.3 拠点 B の設定スクリプトファイル (ROUTERB.CFG)

1	CREATE PPP=0 OVER=eth0-any
2	SET PPP=0 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=site_b@example.co.jp PASSWORD=passwd_b LQR=OFF ECHO=ON
3	CREATE PPP=1 OVER=eth0-any
4	SET PPP=1 OVER=eth0-any BAP=OFF IPREQUEST=ON USER=flets_b PASSWORD=fpasswd_b LQR=OFF ECHO=ON
5	ENABLE IP
6	ENABLE IP REMOTEASSIGN
7	ADD IP INT=vlan1 IP=192.168.20.1 MASK=255.255.255.0
8	ADD IP INT=ppp0 IP=0.0.0.0
9	ADD IP INT=ppp1 IP=0.0.0.0
10	ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
11	ADD IP ROUTE=192.168.10.0 MASK=255.255.255.0 INT=ppp1 NEXTHOP=0.0.0.0
12	ENABLE IP DNSRELAY
13	ENABLE FIREWALL
14	CREATE FIREWALL POLICY=net
15	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACHABLE
16	DISABLE FIREWALL POLICY=net IDENTPROXY
17	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
18	ADD FIREWALL POLICY=net INT=ppp0 TYPE=PUBLIC
19	ADD FIREWALL POLICY=net INT=ppp1 TYPE=PUBLIC
20	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0
21	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp1 PROT=ALL REMOTEIP=192.168.10.1- 192.168.10.254
22	ENABLE TRIGGER
23	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset0.scp
24	CREATE TRIGGER=2 PERIODIC=3 SCRIPT=reset1.scp

表 13.8.3 拠点 B の設定スクリプトファイル (ROUTERB.CFG)

25	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up0.scp
26	CREATE TRIGGER=4 INTERFACE=ppp1 EVENT=UP CP=IPCP SCRIPT=up1.scp
27	CREATE TRIGGER=5 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down0.scp
28	CREATE TRIGGER=6 INTERFACE=ppp1 EVENT=DOWN CP=IPCP SCRIPT=down1.scp

「SET TIME」、「ADD SCRIPT」コマンドなど、コマンドプロンプトに対して入力したコマンドのすべてが、設定ファイルとして保存されるわけではないという点にご注意ください

拠点 A、B、C ともに以下のスクリプトは共通です

表 13.8.4 スクリプト「reset0.scp」

RESET PPP=0

表 13.8.5 スクリプト「reset1.scp」

RESET PPP=1

表 13.8.6 スクリプト「up0.scp」

DISABLE TRIGGER=1

表 13.8.7 スクリプト「up1.scp」

DISABLE TRIGGER=2

表 13.8.8 スクリプト「down0.scp」

ENABLE TRIGGER=1

表 13.8.9 スクリプト「down1.scp」

ENABLE TRIGGER=2

13.9 設定上の注意事項

トリガーの動作

この章で紹介した設定例では、PPP インターフェースを監視し、PPPoE のセッションが局側から切断されたような場合、トリガーにより自動的に再接続を行います。

以下にトリガーの動作のしくみについて説明します。

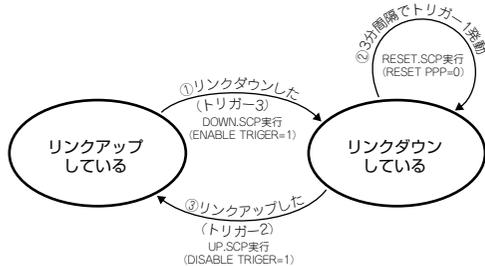


図 13.9.1 トリガーの動作

- 1 各設定でトリガー-1を作成した時点で、トリガー-1 (PPP0) をリセットするスクリプトが 3 分間隔で実行されます。しかしながら、WAN 側インターフェースに UTP ケーブルが接続されていないので、リンクはアップしません。
- 2 UTP ケーブルが接続されると、トリガー-1 が実行されたタイミングでリンクがアップします。
- 3 リンクがアップすると、トリガー-2 が実行され、トリガー-1 が無効になります。
- 4 何らかの要因で、例えば局側からの切断などにより、リンクがダウンすると、トリガー-3 が実行され、トリガー-1 が有効になります。

設定の保存はリンクダウンの状態です

PPP リンクのアップ、ダウンによって、ランタイムメモリー上に展開されているトリガー-1 の設定状態は動的に変化します。

何らかの設定を追加したり、変更などを行った後、フラッシュメモリーの設定スクリプトファイルを更新 (上書き保存) する場合は、必ず WAN 側インターフェースの UTP ケーブルを外し、PPP のリンク

ダウンを確認した上で行ってください

```
Manager > SHOW PPP ↓

Name          Enabled ifIndex Over          CP          State
-----
ppp0          YES     04          eth0-any    IPCP        CLOSED
              LCP        OPENED

Manager > SHOW CONFIG DYN=TRIG ↓
#
# TRIGGER Configuration
#
enable trigger
create trigger=1 periodic=3 script=reset.scp
create trigger=2 interface=ppp0 event=up cp=ipcp script=up.scp
create trigger=3 interface=ppp0 event=down cp=ipcp script=down.scp

Manager > CREATE CONFIG=ROUTER.CFG ↓

Info (1049003): Operation successful.
```

設定の保存が完了したら、WAN 側インターフェースの UTP ケーブルを接続し、PPP リンクのアップを確認してください。

リンクがアップしているときは、トリガー-2 の実行によって、ランタイムメモリー上のトリガー-1 の設定スクリプトに「state=disable」というパラメーターが付加されます。この状態で「CREATE CONFIG」コマンドを実行すると、「state=disable」は設定スクリプトファイルの内容として保存されてしまいます。そうすると、本製品を再起動したときトリガー-1 が実行されず、いつまで経っても PPP リンクが確立しません。

```
Manager > SHOW PPP ↓

Name          Enabled ifIndex Over          CP          State
-----
ppp0          YES     04          eth0-any    IPCP        OPENED
              LCP        OPENED

Manager > SHOW CONFIG DYN=TRIG ↓
#
# TRIGGER Configuration
#
enable trigger
create trigger=1 periodic=3 state=disabled script=reset.scp
create trigger=2 interface=ppp0 event=up cp=ipcp script=up.scp
create trigger=3 interface=ppp0 event=down cp=ipcp script=down.scp
```

また、次の方法を使用すれば、PPP リンクのアップ、ダウンの状態に依存せずに、フラッシュメモリー上の設定スクリプトファイルを変更することができます。

- コンピューター上で設定スクリプトファイルを作成し、Zmodem が TFTP で本製品に転送する。

- 本製品の「EDIT」コマンドで設定スクリプトファイルを作成する。

接続できないときは..

- 1 「SHOW FILE」コマンドを実行し、設定スクリプトファイルのトリガー 1 の設定を確認します。下記では、設定スクリプトのファイル名を「ROUTER.CFG」と仮定しています。

```

Manager > SHOW FILE=ROUTER.CFG ↓

File : ROUTER.CFG

1:
2: #
3: # SYSTEM configuration
4: #
5:
6: #
7: # SERVICE configuration
8: #
9:
10: #
11: # LOAD configuration
12: #
13:
14: #
15: # USER configuration
16: #
17: set user-manager pass=3f7a67b6c6cad1b5db4403ef6ce5af00f priv-manager lo=yes
18: set user-manager desc="Manager Account" telnet=yes
--More-- (<space> = next page, <CR> = one line, C = continuous, Q = quit)

```

- 2 トリガーの設定は、ファイルの最後にあります。最後の行が表示されるまで、繰り返しスペースバーを押してください。

トリガー 1 の設定内容を確認してください。正しく保存されている場合、トリガー 1 の設定は次のようになります。

```
create trigger=1 periodic=3 script=reset.scp
```

手順が正しくなかった場合は、次のように「state=disabled」というパラメーターが付きます。この設定では、本製品起動直後に再接続機能が動きません。

```
create trigger=1 periodic=3 state=disabled
script=reset.scp
```

- 3 「state=disabled」が付いている場合、「EDIT」コマンドで設定スクリプトファイルを開いてください。下記は、ファイル名として「ROUTER.CFG」を仮定しています。

```
Manager > EDIT ROUTER.CFG ↓
```

- 4 ファイルの内容が表示されます。↓キーを押し、ファイルの最後に移動してください。→キーで「state=disable」の後まで移動

し、DEL キーで「state=disable」を削除してください。

```

#
#
# HTTP configuration
#
#
# VRRP configuration
#
#
# GUI configuration
#
#
# BGP configuration
#
# TRIGGER Configuration
#
enable trigger
create trigger=1 periodic=3 state=disabled script=reset.scp
create trigger=2 interface=ppp0 event=up cp=ipcp script=up.scp
create trigger=3 interface=ppp0 event=down cp=ipcp script=down.scp
Ctrl+K+H = Help | File = ROUTER.CFG | Insert | Modified | 286/43

```

スクロールしたとき、画面右側の文字が正しく表示されない場合、Ctrl/W キーを押してください（画面が再描画されます）。どうしてもうまく行かない場合、ハイパーターミナル以外の通信ソフトウェアをご使用ください。また、文字を消去するコードは DELETE に設定してください。



本書「6.1 Edit の実行」(p.57)

本書「A.2 ハイパーターミナルの設定」(p.143)

- 5 CTRL キーを押しながら K キーを押し、続いて CTRL キーを押したまま X キーを押してください。保存するかどうか問われますので、Y キーを押してください。N キーを押すと、保存せずにエディターが終了します。

```
Save file ( y/n ) ? Y
```

- 6 本製品を再起動します。次のコマンドを入力してください。

```
Manager > RESTART ROUTER ↓
```

- 7 ログインし、PPP のリンクを確認してください。

PPPoE セッションの手動による切断

本設定では、本製品が起動すると同時に PPPoE セッションが確立され、以後常時接続された状態となります。PPPoE セッションの切断、再接続を行う場合は、手動で行います。

切断は、「DISABLE PPP」コマンドを実行します。

```
Manager > DISABLE PPP=0 ↓

Info (1003003): Operation successful.

Manager > SHOW PPP ↓

Name          Enabled ifIndex Over          CP          State
-----
ppp0          NO          04          eth0-any    LCP         CLOSED
              LCP         INITIAL
```

「DISABLE PPP」コマンドは、PPP リンクを切断しますが、トリガー1は実行されません。また、トリガー1のランタイムメモリー上の設定スクリプトも変更しません。

```
Manager > SHOW CONFIG DYN=TRIG ↓

#
# TRIGGER Configuration
#

enable trigger
create trigger=1 periodic=3 script=reset.scp
create trigger=2 interface=ppp0 event=up cp=ipcp script=up.scp
create trigger=3 interface=ppp0 event=down cp=ipcp script=down.scp
```

ただし、「DISABLE PPP」コマンドは、ランタイムメモリー上のPPPの設定スクリプトに追加されるので注意が必要です。この状態でCREATE CONFIG コマンドを実行すると、「disable ppp=0」は設定スクリプトファイルの内容として保存されます。本製品を再起動したとき、いつまで経ってもPPPリンクが確立しません。

```
Manager > SHOW CONFIG DYN=PPP ↓

#
# PPP configuration
#

create ppp=0 over=eth0-any
set ppp=0 bap=off iprequest=on username="user1@isp" password="ispaswd1"
set ppp=0 over=eth0-any lqr=off echo=10
disable ppp=0
```

再接続

「DISABLE PPP」コマンドによる切断を、再接続するには「RESTART ROUTER」コマンドを実行してください。

```
Manager > RESTART ROUTER ↓
```

PPPoE におけるアンナンバード

PPPoEのLAN型接続では、IPCP ネゴシエーションによって、WAN側（PPP）インターフェースにネットワークアドレス（ホスト部が0のアドレス）が割り当てられます。ネットワークアドレスは、ホストアドレスとしては使用できないため、事実上アンナンバードと同じですが、厳密に言うと専用線接続などで使用するアンナンバードとは異なります。

ルーター自身がWAN側インターフェースからIPパケットを送出する場合を考えてみましょう。純粋なアンナンバードでは、送出インターフェースにアドレスが設定されていないため、他のインターフェースのアドレスを使用します。しかしながら、PPPoE LAN型の場合は、まがりなりにもWAN側インターフェースにアドレスが設定されているため、パケットの始点アドレスとして本来使用できないネットワークアドレスが使用されてしまいます（相手からの応答のパケットが届きません）。

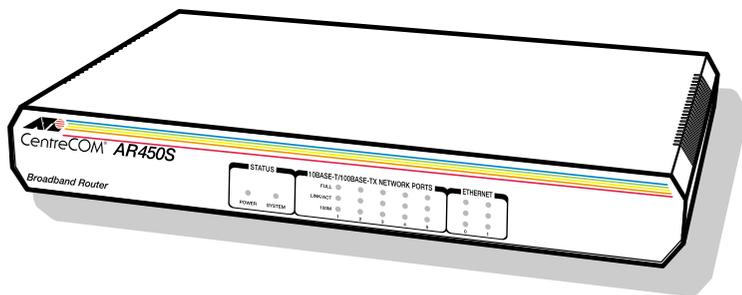
通常は、ルーター自身がパケットを送信することはないため、このことを意識する必要はありませんが、L2TP、IPsec では注意が必要です。これらでカプセル化されたパケットには、始点アドレスとしてルーターのWAN側インターフェースのアドレスが使用されるため、そのアドレスとして有効なものを使用しなければなりません。

有効なアドレスが使用されるようにするには、WAN側インターフェースをマルチホーミングし、一方に有効なアドレスを設定した上で、デフォルトルートを有効なアドレスのインターフェースに向けてやります。

例えば、プロバイダーから192.0.2.0/29のアドレスが割り当てられているとすると、次のように設定します。この例では、LAN側からWAN側へのパケットはppp0-1にルーティングされ、始点アドレスとして192.0.2.1が使用されるようになります。

```
ADD IP INT=ppp0-0 IP=0.0.0.0
ADD IP INT=ppp0-1 IP=192.0.2.1
    MASK=255.255.255.255
ADD IP INT=VLAN1 IP=192.0.2.2
    MASK=255.255.255.248
ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXT=0.0.0.0
```


付録



A.1 コンピューターの設定

第2部「13 構成例」(p.77)のLAN環境におけるコンピューター側の設定として、Windows 2000、Mac OS Xの例を挙げます。Windowsの他のバージョン、Mac OSの他のバージョンでは手順が異なりますが、以下の例を参考にして設定してください。

Windows 2000

- 1 「コントロールパネル」→「ネットワークとダイヤルアップ接続」→「ローカルエリア接続」をダブルクリックしてください。



図 A.1.1 「ローカルエリア接続」アイコン

- 2 「プロパティ」をクリックしてください。

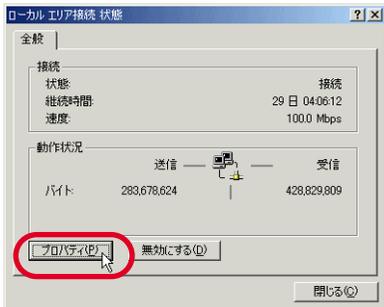


図 A.1.2 ローカルエリア接続状態

- 3 「インターネットプロトコル (TCP/IP)」を選択し、「プロパティ」をクリックしてください。

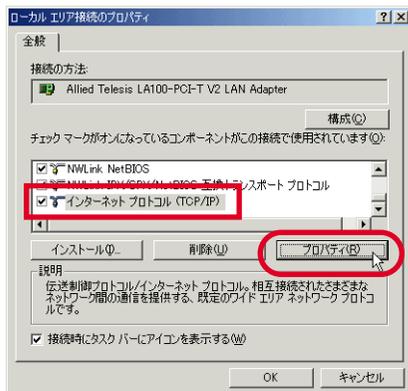


図 A.1.3 ローカルエリア接続のプロパティ

- 4 本製品 (DHCP サーバー) から IP アドレスを自動的に取得する場合は、次のように設定してください (この設定は、Windows 2000 におけるデフォルトです)。「IP アドレスを自動的に取得する」と「DNS サーバーの IP アドレスを自動的に取得する」をクリックし、「OK」をクリックしてください。

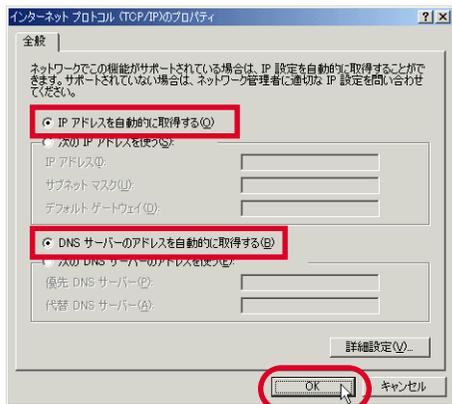


図 A.1.4 IP アドレス自動取得 (DHCP クライアント)

IP アドレスなどを固定的に設定する場合は、次のように設定してください。「次の IP アドレスを使う」をクリックし、「IP アドレス」「サブネットマスク」「デフォルトゲートウェイ」を入力します。「デフォルトゲートウェイ」は、本製品の LAN 側の IP アドレスを指定します。さらに、「次の DNS サーバーの IP アドレスを使う」をクリックし、「優先 DNS サーバー」に本製品の LAN 側の IP アドレスを入力します（本製品に DNS リレーの設定が必要です）。「代替 DNS サーバー」は空欄のままにしておきます。最後に、「OK」をクリックしてください。

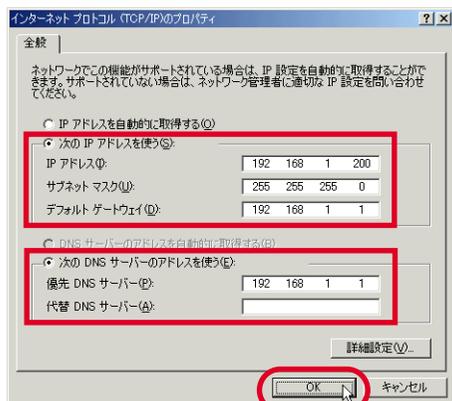


図 A.1.5 IP アドレス固定 (DNS リレー)

DNS リレーを使用しない場合は、プロバイダーの DNS サーバーを直接指定します。

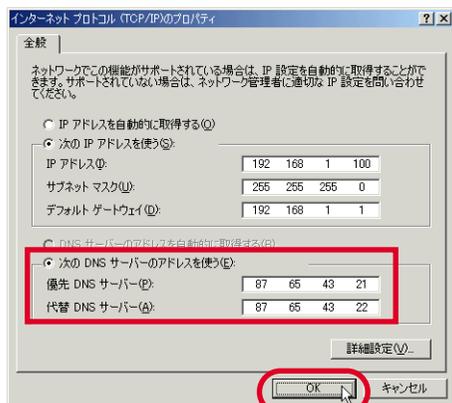


図 A.1.6 IP アドレス固定 (DNS ダイレクト)

Mac OS X

- 1 「アップルメニュー」→「システム環境設定」を開いてください。
- 2 「システム環境設定」ダイアログボックスの「ネットワーク」をクリックしてください。
- 3 本製品 (DHCP サーバー) から IP アドレスを自動的に取得する場合は、次のように設定してください (この設定は、Mac OS X におけるデフォルトです)。「表示」で「内蔵 Ethernet」を選択しておき、「TCP/IP」タブの「設定」で「DHCP サーバを参照」を選択します。最後に「今すぐ適用」をクリックしてください。本製品からの IP アドレス取得に成功すると、取得した IP アドレスなどの情報が表示されます (点線の囲み)。

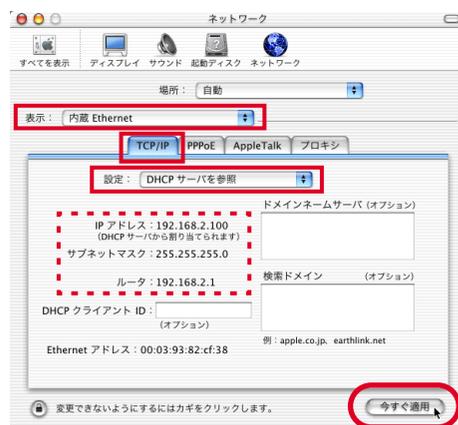


図 A.1.7 IP アドレス自動取得 (DHCP クライアント)

- 5 再起動を促すダイアログが現れたら、指示に従い再起動してください。

IP アドレスなどを固定的に設定する場合は、次のように設定してください。「表示」で「内蔵 Ethernet」を選択しておき、「TCP/IP」タブの「設定」で「手入力」を選択します。「IP アドレス」「サブネットマスク」「ルータ」を入力します。「ルータ」は、本製品のLAN側のIPアドレスを指定します。「ドメインネームサーバ」に本製品のLAN側のIPアドレスを入力します（本製品にDNSリレーの設定が必要です）。最後に、「今すぐ適用」をクリックしてください。

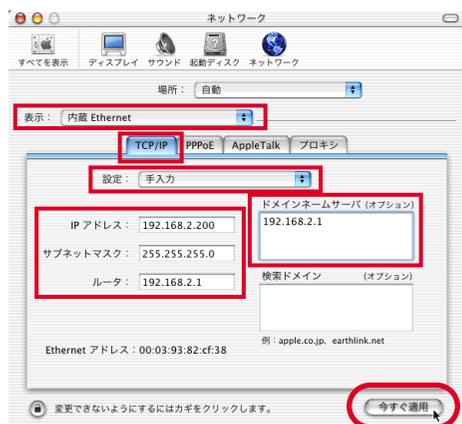


図 A.1.8 IP アドレス固定 (DNS リレー)

DNSリレーを使用しない場合は、プロバイダーのDNSサーバーを直接指定します。

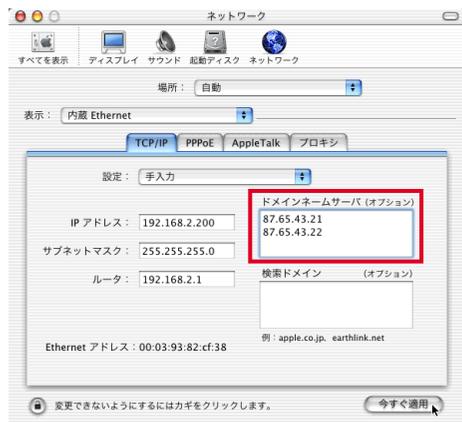


図 A.1.9 IP アドレス固定 (DNS ダイレクト)

4 「ネットワーク」ダイアログボックスを開いてください。

A.2 ハイパーターミナルの設定

コンソールターミナルとして、Windows 2000 のハイパーターミナルを使用する例を示します。Windows の他のバージョンのハイパーターミナルや、他の通信ソフトウェアをご使用の場合は、手順が若干異なりますが、以下の例を参考にして設定してください。

通信ソフトウェアに設定するパラメーターは、下記の通りです。エミュレーション、「BackSpace」キーのコードは「EDIT」コマンドのための設定です。文字セットは、「HELP」コマンド（日本語オンラインヘルプ）のための設定です。

表 A.2.1 コンソールターミナルの設定

項目	値
インターフェース速度	9,600bps
データビット	8
パリティ	なし
ストップビット	1
フロー制御	ハードウェア (RTS/CTS)
エミュレーション	VT100
BackSpace キーのコード	Delete
エンコード	SJIS

1 「**3** コンソールターミナルを接続する」(p.25) に従い、本製品背面の CONSOLE ポートとコンピューター (Windows 2000) を接続してください。

2 Windows 2000 を起動し、「スタート」→「プログラム」→「アクセサリ」→「通信」→「ハイパーターミナル」をクリックしてください。

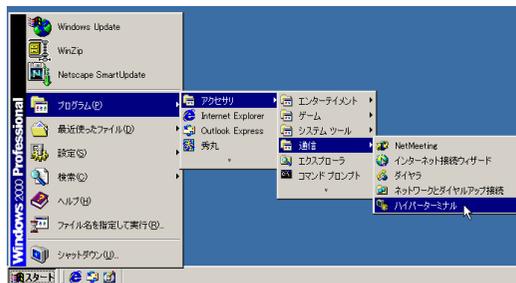


図 A.2.1 「ハイパーターミナル」フォルダ

- 3 次のダイアログボックスが現れたら*1、「国名 / 地域名」で「日本」を選択、「市外局番 / エリアコード」を入力して「OK」をクリックしてください。ここでは市外局番として「03」、外線発信番号は「無し」（0 発信しない）、ダイヤル方法は「トーン」を仮定しています。

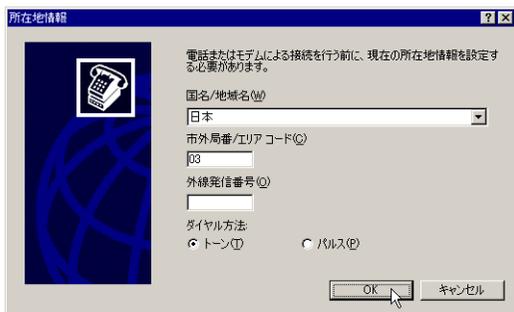


図 A.2.2 「所在地情報」の設定

- 4 次のダイアログボックスが現れたら、「OK」をクリックしてください。



図 A.2.3 「電話とモデムのオプション」の設定

- 5 接続の「名前」を入力、「アイコン」を選択して「OK」をクリックしてください。ここでは「名前」として「AR_ROUTER」を仮定しています。



図 A.2.4 接続の名前を入力

- 6 「接続の方法」を選択し、「OK」をクリックしてください。ここではコンピューターの COM1 ポートにコンソールケーブルを接続すると仮定し、「COM1」を選択しています。他のポートに接続している場合は、接続しているポートを指定してください。



図 A.2.5 接続方法で COM1 を指定

- 7 「ビット / 秒」で「9600」、「データビット」で「8」、「パリティ」で「なし」、「ストップビット」で「1」、「フロー制御」で「ハードウェア」を選択し、「OK」をクリックしてください（「ビット / 秒」以外はデフォルトです）。



図 A.2.6 「COM1」のプロパティの設定



*1 電話とモデムの設定が完了している場合、図 A.2.2、図 A.2.3 のダイアログボックスは表示されません。

- 8 ハイパーターミナルの画面が表示されます。

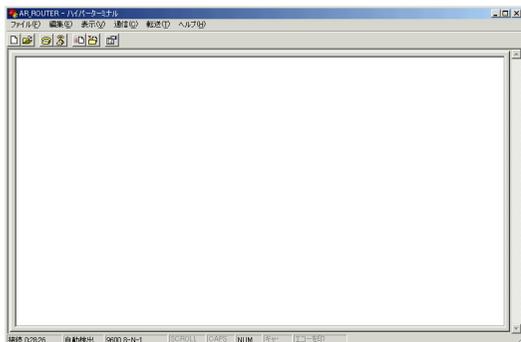


図 A.2.7 ターミナル画面

- 9 「ファイル」→「プロパティ」をクリックしてください。「AR_ROUTER のプロパティ」ダイアログボックスが現れます。「設定」ページを選択し、「エミュレーション」で「VT100J」、 「BackSpace キーの送信方法」で「Delete」を選択してください。「エンコード方法」をクリックしてください。

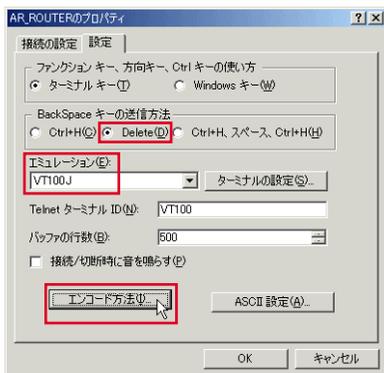


図 A.2.8 キーの設定

- 10 「Shift-JIS」を選択し、「OK」をクリックしてください。下記のダイアログボックスが閉じ、図 A.2.8 に戻りますので、「OK」をクリックしてください。

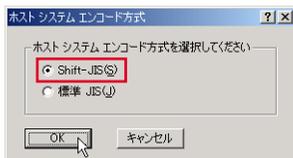


図 A.2.9 エンコード方式

- 11 以上で、ハイパーターミナルをコンソールターミナルとして使用するための設定は終了です。

ハイパーターミナルの設定の保存

次のハイパーターミナルの実行の便宜のために、前述の手順で施した内容を保存しておきます。

- 1 「ファイル」→「名前を付けて保存」をクリックしてください。



図 A.2.10 ハイパーターミナル設定の保存

- 2 「ファイル名」に「A.2 ハイパーターミナルの設定」の手順5で指定した名前のファイル（拡張子は ht）が表示されていることを確認し、「保存」をクリックしてください。



図 A.2.11 ハイパーターミナル設定ファイル名の入力

次のハイパーターミナルの起動は、「スタート」→「プログラム」→「アクセサリ」→「通信」→「ハイパーターミナル」フォルダー→「AR_ROUTER.ht」をクリックしてください。

ハイパーターミナルの終了

- 1 本製品にログインしている場合は、ログアウトしてください。
- 2 「ファイル」→「ハイパーターミナルの終了」をクリックしてください。

- 3 次のメッセージボックスが現れたら、「OK」をクリックしてください。

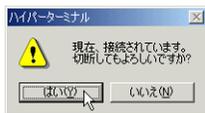


図 A.2.12 接続中の警告

A.3 CONSOLE ポート

本製品の CONSOLE ポート (DCE) は、RS-232 規格の D サブ 9 ピン (メス) コネクタが使用されています。ご使用のコンソールターミナル (DTE) との接続は、付属のコンソールケーブル (ストレートタイプ) をご使用ください。通信パラメーターは下記の通りです (本製品がブートモニターの状態におかれているとき、フロー制御は「Xon/Xoff」となります)。

表 A.3.1 通信パラメーター

項目	値
インターフェース速度	9,600bps
データビット	8
パリティ	なし
ストップビット	1
フロー制御	ハードウェア (RTS/CTS)

A.4 10BASE-T/100BASE-TX ポート

本製品は、LAN 側として 10BASE-T/100BASE-TX ポートを 5 つ持っています。各ポートは、RJ-45 型と呼ばれるモジュラージャックが使用されています。

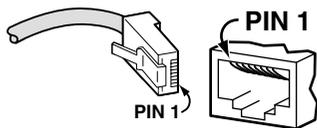


図 A.4.1 RJ-45モジュラープラグ (左)、ジャック (右)

LAN 側ポートはすべて「MDI/MDI-X自動切り替え」になっているため、どのポートもカスケードポートとして使用できます。また、ストレート、クロスケーブルのどちらを使用しても、正常に動作します。

ETHERNET (WAN) 側は「MDI固定」の 10BASE-T/100BASE-TX ポートを 2 つ持っています。ストレートタイプのケーブルを利用する場合、接続相手のポートはMDI-X でなければなりません。

表 A.4.1 MDI 仕様における信号線名

ピン番号	信号 (MDIポート)
1	送信データ (+)
2	送信データ (-)
3	受信データ (+)
4	未使用
5	未使用
6	受信データ (-)
7	未使用
8	未使用

A.5 製品仕様

ハードウェア

CPU	
PowerPC 400MHz	
メモリー容量	
メインメモリー	
64MByte	
フラッシュメモリー	
16MByte (ファイルシステムで 15MByte が使用可能)	
ポート	
WAN	
10BASE-T/100BASE-TX (MDI) × 2 (オートネゴシエーション)	
LAN	
10BASE-T/100BASE-TX × 5 (MDI/MDI-X 自動切替)	
コンソール	
RS-232 (DCE)、D サブ 9 ピン (メス) × 1	
スイッチ部 (LAN)	
スイッチング方式	
ストア&フォワード	
パケットバッファ	
120KByte	
MAC アドレス登録数	
1K (最大)	
エージングタイム (MAC アドレス保持時間)	
約 300 秒	
オプション (別売)	
ライセンス	
AR450S 用 3DES/AES ライセンス (AT-FL-12)	
電源部	
定格入力電圧	AC100-240V
入力電圧範囲	AC90-255V
	付属の電源ケーブルは、AC100V のみに対応して おります。他の電源電圧で使用しないで ください。
定格周波数	50/60Hz
定格入力電流	1.0A
最大入力電流 (実測値)	0.36A

平均消費電力	16W (最大 22W)
平均発熱量	57kJ/h (最大 80kJ/h)
環境条件	
動作時温度	0℃～40℃
動作時湿度	80%以下 (結露なきこと)
保管時温度	−20℃～60℃
保管時湿度	95%以下 (結露なきこと)
外形寸法	
	305 (W) × 182 (D) × 44 (H) mm (突起部含まず)
質量	
	1.7kg
適合規格	
	UL60950 CSA-C 22.2 No.60950
	JATE (D03-0222JP)
	VCCI クラス B

ソフトウェア

準拠規格
IEEE 802.3 10BASE-T
IEEE 802.3u 100BASE-TX
IEEE 802.1q VLAN tagging
IEEE 802.1p Class of Service
ルーティングプロトコル
IP、IPv6
ルーティング方式
スタティック、RIP/RIP2、OSPF
WAN サービス
ADSL、CATV、FTTH、インターネットVPN、IP-VPN、広域イーサネットなどの各種ブロードバンド回線／サービス
機能
PPP over Ethernet ^a
NAT/EnhancedNAT
DHCP (Server、Client、Relay Agent)、DNS Relay
Firewall (Stateful Inspection、攻撃検出・通知)
Packet Filtering
VPN (IPsec (IKE/ISAKMP)、L2TP (RFC2661 準拠)、GRE)
Bridging
UPnP
Multi Homing
サービス管理 (Priority-Based Routing、Policy-based Routing)
VRRP
PAP/CHAP、RADIUS、IP Address Pool
管理機能
Text Editor、Zmodem、TFTP Client、
Secure Shell、Telnet (Server、Client)、Trigger、メール送信 (SMTP)、Syslog、NTP Client、
SNMP (MIB II、Bridge MIB、Ethernet MIB、Private MIB)、

- a. サービスが対応していれば同時 5 セッション可

このソフトウェア仕様は、Ver.2.5.2 の機能をもとに記載されています。機能は、ソフトウェア（ファームウェア）のバージョンに依存します。ご使用になるソフトウェアの機能は、最新のカatalog、リリースノートをご覧ください。

B ユーザーサポート

B.1 保証について

本製品の保障内容は、製品に添付されている「製品保証書」の「製品保証規定」に記載されています。製品をご利用になる前にご確認ください。

保証の制限

本製品の使用または使用不能によって生じたいかなる損害（人の生命・身体に対する被害、事業の中断、事業情報の損失またはその他の金銭的損害を含み、またこれらに限定されない）については、当社は、その責を一切負わないこととします。

B.2 ユーザーサポート

障害回避などのユーザーサポートは、「製品保証書」をご確認のうえ、調査依頼書として弊社サポートセンターへご連絡ください。

アライドテレシス株式会社 サポートセンター

メールアドレス: support@allied-telesis.co.jp

Fax: ☎ 0120-860-662

年中無休24時間受付

Tel: ☎ 0120-860-772

月～金（祝・祭日を除く）9:00～12:00 13:00～18:00

（携帯電話／PHS をご使用のお客様は「045-476-6203」までおかけください）

調査依頼書の内容について

調査依頼書は、お客様の環境で発生した様々な障害の原因を突き止めるためのものです。ご提供いただく情報が不十分な場合には、障害の原因究明に時間がかかり、最悪の場合には障害の解消ができない場合もあります。迅速に障害の解消を行うためにも、弊社担当者が障害の発生した環境を理解できるように、以下の点についてご記載ください。なお、都合によりご連絡が遅れることもございますが、あらかじめご了承ください。

1 一般事項

- 送付日
- お客様の会社名、ご担当者
- ご連絡先
すでに「サポート ID 番号」を取得している場合、サポート ID 番号をご記載ください。サポート ID 番号をご記入いただいた場合

には、ご連絡住所などの詳細は省略していただいてもかまいません。

- ご購入先

2 使用しているハードウェア、ソフトウェアについて

製品名、製品のシリアル番号 (S/N)、製品リビジョンコード (Rev) などのハードウェア情報を調査依頼書に記入してください。製品のシリアル番号、製品リビジョンコードは、製品底面のバーコードシールに記入されています。

(例)



「Rev」、「Software Version」、「Release Version」などのソフトウェア情報をご記入ください。これらは、Manager または Security Officer レベルでログインし、「SHOW SYSTEM」コマンドで確認できます。図 B.2.1 (p.134) に例を示します（日付などは一例です）。

```
login: manager
Password: xxxxxxxx (お客様の環境におけるものを入力)

Manager >SHOW SYSTEM ↓

Router System Status                               Time 17:12:54 Date 04-Jun-2003.
Board      ID  Bay Board Name                       Rev      Serial number
-----
Base       190  AR450                               MI-0     57004257
-----
Memory -   DRAM : 65536 kB  FLASH : 16384 kB
-----
SysDescription
CentreCOM AR450 version 2.5.2-01 22-MAY-2003
SysContact

SysLocation

SysName
OSAKA
SysDistName

SysUpTime
49540 (00:08:15)
-----
Software Version: 2.5.2-01 22-May-2003
Release Version : 2.5.2-00 08-May-2003
Patch Installed : Release Patch
Territory       : japan
.....
```

図 B.2.1 サポートに必要なソフトウェア情報

3 回線について

プロバイダーとの接続方法、ご契約のプロバイダー名をご記入ください。

(例) フレッツ・ADSL で RIMNET に接続、専用線で IJ に接続

4 お問い合わせ内容について

どのような症状が発生するのか、それはどのような状況でまたどのような頻度で発生するのかをできる限り具体的に(再現できるように) 記入してください。

エラーメッセージやエラーコードが表示される場合には、表示されるメッセージの内容を添付してください。

可能であれば、設定スクリプトファイルをお送りください (パスワードや固有名など差し障りのある情報は、抹消してお送りくださいますようお願いいたします)。

5 ネットワーク構成について

ネットワークとの接続状況や、使用されているネットワーク機器がわかる簡単な図を添付してください。

他社の製品をご使用の場合は、メーカー名、機種名、バージョンなどをご記入ください。

ご注意

- 本マニュアルは、アライドテレスイス株式会社が作成したもので、すべての権利をアライドテレスイス株式会社が保有しています。本書の全部または一部を弊社の同意なしにコピーまたは転載することを固くお断りいたします。
- アライドテレスイス株式会社は、予告なく本マニュアルの一部または全体を修正、変更することがありますのでご了承ください。
- アライドテレスイス株式会社は、改良のため予告なく製品の仕様を変更することがありますのでご了承ください。
- 本マニュアルについて、万一記載漏れ、誤りやご不審な点等ございましたらご連絡ください。
- 本製品を運用して発生した結果については、上記の項にかかわらず、責任を負いかねますのでご了承ください。

©2003 アライドテレスイス株式会社

©2003 Allied Telesyn International Corporation

商標について

CentreCOMは、アライドテレスイス株式会社の登録商標です。
Apple、Mac OS、Macintoshは、米国その他の国で登録された米国アップルコンピュータ社の商標です。
Windows、MS-DOS、Windows NT は、米国Microsoft Corporationの米国およびその他の国における登録商標です。
その他、この文書に掲載しているソフトウェアおよび周辺機器の名称は各メーカーの商標または登録商標です。

マニュアルバージョン

2003年6月20日 Rev.A 初版 (Firmware Ver.2.5.2)

