CentreCOM® AR410 V2 取扱説明書

Allied Telesis

CentreCOM®

AR410 V2

Broadband Router

取扱説明書

CentreCOM AR410 V2

取扱説明書

アライドテレシス株式会社

安全のために

必ずお守りください

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。

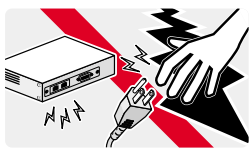
分解や改造をしない

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

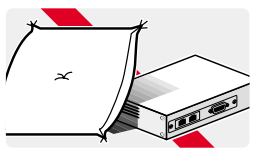
異物は入れない　水は禁物

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。(当社のサポートセンターまたは販売店にご連絡ください。)

異物厳禁

通風口はふさがない

内部に熱がこもり、火災の原因となります。



ふさがない

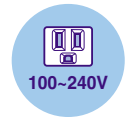
湿気やほこりの多いところ、油煙や湯気のあたる場所には置かない

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

表示以外の電圧では使用しない

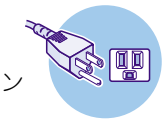
火災や感電の原因となります。
本製品は AC100 - 240V で動作します。
なお、本製品に付属の電源ケーブルは 100V 用ですのでご注意ください。



電圧注意

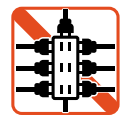
正しい電源ケーブル・コンセントを使用する

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

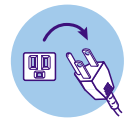
コンセントや配線器具の定格を超える使い方はしない

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

ご使用にあたってのお願い

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）
・湿気の多い場所や、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、ジ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、堅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　堅く絞る

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、CentreCOM AR410 V2 をお買いあげいただき、誠にありがとうございます。

CentreCOM AR410 V2（以下本製品または AR410V2）は、SOHOから中規模オフィス向けの、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。また、ブリッジングや、IPX、AppleTalkのルーティングもサポートしておりますので、IP をはじめとしたさまざまなネットワーク環境でご利用いただけます。

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「2.3.3」をもとに記述されていますが、「2.3.3」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。

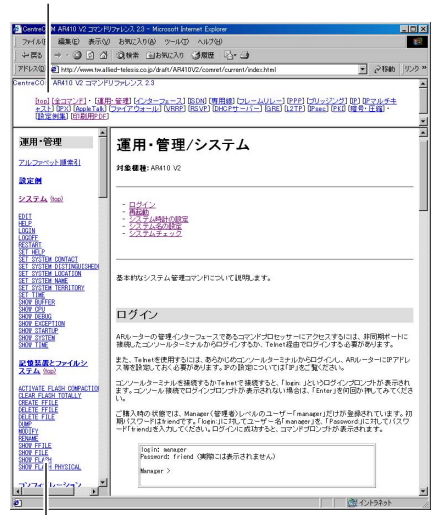
0.2 付属の CD-ROM について

付属のCD-ROM には、以下のマニュアルや情報が収録されております。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。

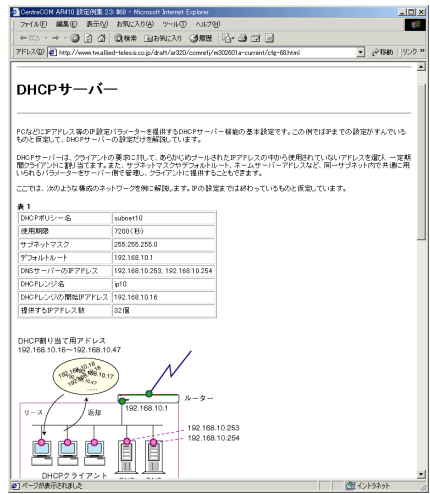


図 0.2.2 設定例集

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 ↵

        CentreCOM AR410 V2 オンラインヘルプ - V2.3 Rev.01 2002/09/04


  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）。
  (* マーク付きの機能は 2002/09 現在サポートしていません)
  (# マーク付きの機能は追加ライセンスが必要です )

    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、BRI、PRI など）
    Help ISdn               ISDN
    Help Tdm                専用線
    Help FRamerelay         フレームリレー
    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 IPMulticast      * IP マルチキャスト
    Help IPX                IPX
--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）。

マークについて

説明内容により、以下のマークをつけています。

危険
人命を失う、けがをするなど人身に対する危険性があることを示しています。

警告
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
なんらかの問題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。

製品名

本書は、「CentreCOM AR410 V2」を「本製品」または単に「AR410V2」と略します。また、PIC など本製品に装着可能なオプション製品は、「AR020」などのように「CentreCOM」を省略します。

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「hanako@my.isp.ne.jp」
- PPP 接続のためのパスワードとして「jK5H&i2p」
- 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」

目次

1.1 パッケージの確認

パッケージを開けたら、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

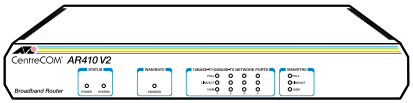


図 1.1.1 ルーター本体

電源ケーブル

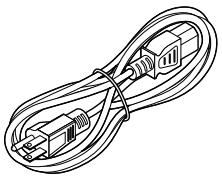


図 1.1.2 電源ケーブル

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。

コンソールケーブル

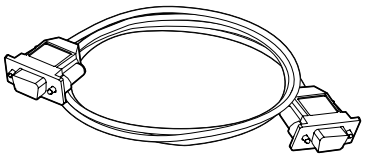


図 1.1.3 コンソールケーブル

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。コネクターは、9 ピンオス（本製品側）ー9 ピンメスとなっています。

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

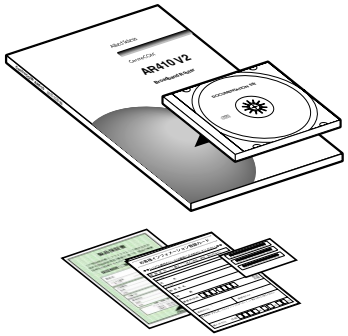


図 1.1.5 CD-ROM、マニュアルなど

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
- お客様インフォメーション登録カード 1 枚
- シリアル番号シール 3 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

CentreCOM AR410 V2（以下本製品またはAR410V2）は、SOHOから中規模オフィス向けの､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。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 1 つ、LAN 側として 4 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、4 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。

さまざまな回線や接続サービスをサポート

xDSL、CATV、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 4 セッションまでの接続が可能です。アンナンバード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（アンナンバード接続）の利用も可能です。

DHCP クライアントが実装されていますので、CATV 系のインターネット接続サービスが利用できます。

拡張スロット（PIC ベイ）を装備しておりますので、別売の PIC（Port Interface Card）カードを装着すれば、ISDN、専用線、フレームリレーへの接続も可能です。

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。

セキュリティー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[*1] を併用すればセキュリティーも確保できます。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。IP、IPX、AppleTalk のルーティングだけでなく、ブリッジングもサポートしていますので､さまざまなネットワーク環境でご利用いただけます。

マルチプロトコル・ルーティングとブリッジング

IP､IPX、AppleTalk のルーティングが可能です。IPX（NetWare）の SAP、WatchDog パケットの代理応答もできます。ルーティングを適用していないプロトコルのパケットは､ブリッジングを適用できます。例えば、NetBEUI のみを指定してフォワードすることができます。

マルチホーミング

物理インターフェースに、複数の IP アドレスを持たせることができます。

ルーティングプロトコル

RIP V1/V2、OSPF、RIP/IPX 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。

データ圧縮

限られた通信帯域をより有効に利用するためのデータ圧縮が可能です。Predictor、VJ Compression、STAC LZS[*2]、FRF.9（フレームリレー）、IPsec のための IP comp[*3] をサポートしており、異機種ルーター間の圧縮通信も可能です。

*1 暗号カード AR010、暗号・圧縮カード AR011 が必要。
*2 INS1500 などの回線で同時に 5 つ以上のセッションを張る場合、AR011 または圧縮カード AR012 が必要。
AR010、AR011、AR012 はご購入時オプションです（カード単体のご購入はできません）。

通信サービスの管理

音楽や映像などのように、継続的な情報の配信が必要なサービスのために、RSVP（Resource reSerVation Protocol）による通信帯域の確保ができます。

RSVP プロキシーエージェントにより、特定のヘッダー情報を持つトラフィックフローを検出すると、センダーやレシーバーに代わって RSVP メッセージを送信し帯域を確保します。該当のフローが無くなると自動的に帯域を開放します。

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す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、ブ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、TACACS）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るます。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 をサポートしています。弊社CentreNET SwimView、Swim Manager をご利用になれば、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。

19 インチラックへの取り付けが可能です（別売の AT-RKMT-J07 が必要）。

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、カタログ、リリースノートをご覧ください。

*3 IP compの利用は AR010、AR011 が必要。IP comp は STAC LZS アルゴリズムをサポート。

1.3 各部の名称と働き

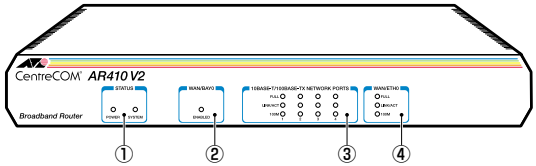


図 1.3.1 前面図

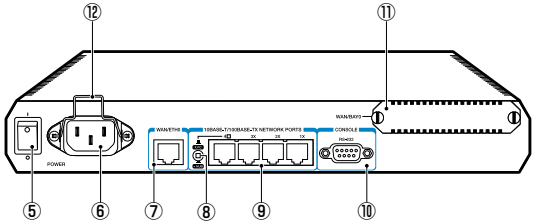


図 1.3.2 背面図

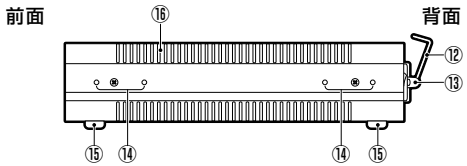


図 1.3.3 側面図

① STATUS LED

本製品のシステム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 WAN/BAYO LED

PIC ベイに装着された PIC の状態を表示する LED です。

LED	色	状態	表示の内容
ENABLE	緑	点灯	PIC（Port Interface Card）ベイに PIC が装着されており、本製品によって PIC が認識されています。
		消灯	PIC ベイに PIC が装着されていません。または、本製品によって PIC が認識されていません。

③ 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ーを表示するLED です。LEDは各ポートごとに存在します（4 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にしています。

④ WAN/ETH0 LED

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

⑤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。「I」がオン、「O」がオフとなります。

⑥電源コネクター

電源ケーブルを接続するためのコネクター（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。

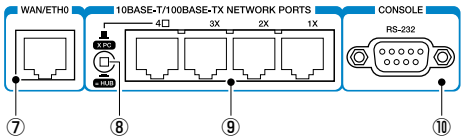


図 1.3.4 ポート

⑦WAN/ETH0 ポート

WAN 側の Ethernet ポートです（MDI）。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）。

⑧MDI/MDI-X 切替スイッチ

10BASE-T/100BASE-TX ポート 4 の用途を切り替えるスイッチです。

スイッチ位置	用途
X PC	ポート 4 を通常の HUB のポートに設定します（MDI-X）。コンピューターを接続する場合は、この位置に設定してください。
= HUB	ポート 4 を他の HUB/ スイッチと接続するためのカスケードポートに設定します（MDI）。

⑨10BASE-T/100BASE-TX ポート

LAN 側の Ethernet ポートです（MDI-X）。4 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）。
特に、ポート 4 は MDI/MDI-X 切替スイッチを装備しており、カスケードポートとして使用するのに便利です。

⑩CONSOLE 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-232 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。

⑪WAN/BAY0

PIC（Port Interface Card）を装着するためのベイ（スロット）です。使用しない場合は、ブランクパネルを取り付けておきます。

参照 本書「A.5 PIC（Port Interface Card）」（p.119）

⑫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）。

⑬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。

⑭ブラケット用ネジ穴

19 インチ・ラックマウントキット（別売）を取り付けるためのネジ穴です。ラックマウントキットは、前面側または背面側に取り付けることができます。

⑮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。

⑯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。

警告 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、ラックへの取り付け、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、ADSL、CATV、FTTH、無線がありますが、以下ではADSL、CATVの場合を例に挙げます。これらは、WAN側の構成が異なるだけで、本製品以下の構成は同じです。

2.1 基本的なネットワーク構成

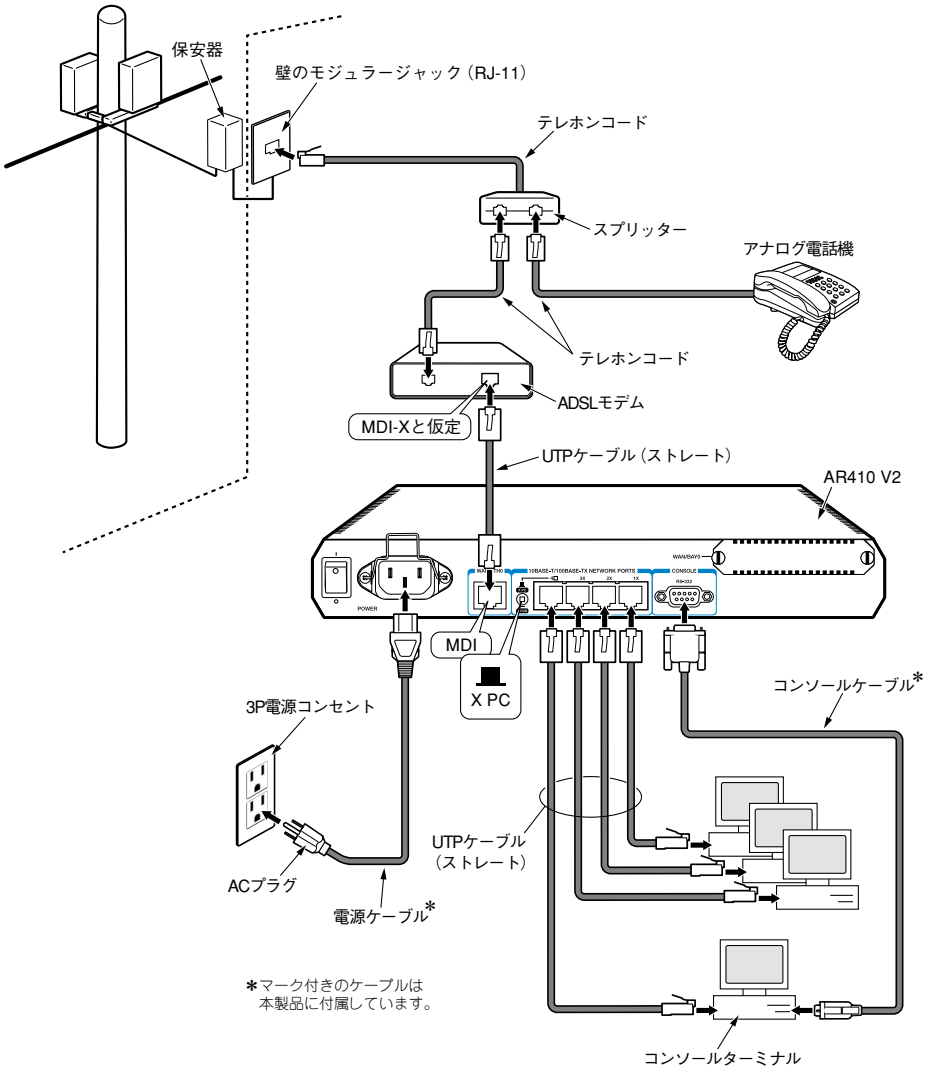


図 2.1.1：ADSLモデムを使用した基本的なネットワーク構成例

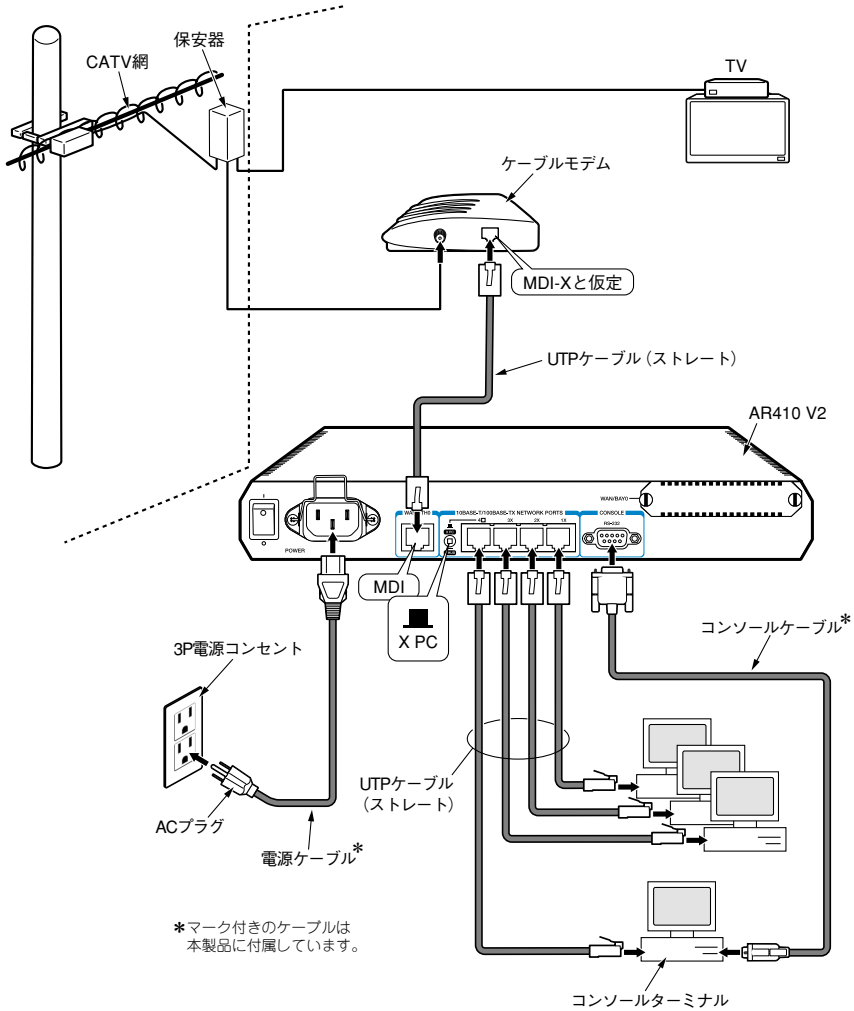


図 2.1.2 ケーブルモデムを使用した基本的なネットワーク構成例

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。

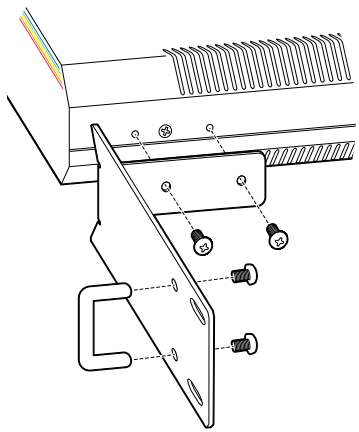


図 2.2.1 ブラケットの取り付け

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。

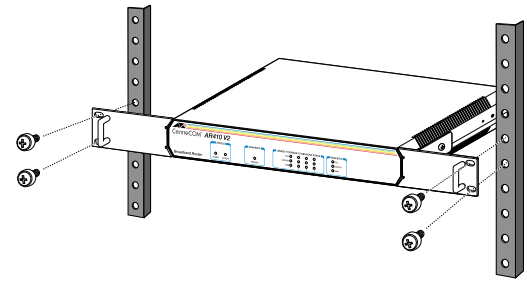


図 2.2.2 ラックへの取り付け

2.3 配線する

危 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 ADSL モデムまたはケーブルモデムまでの工事（配線）が完了しているものとして説明します。
- 19 インチラックに取り付ける場合、あらかじめ「2.2 19 インチラックへの取り付け」（p.23）に従って、設置を完了しておきます。
- 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。

  参照 本書「A.1 コンピューターの設定」（p.113）

- 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 *2

*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。

*2 弊社販売品のシールド付きカテゴリー 5（ストレート）ケーブルにも対応しています。

1 ADSL モデム / ケーブルモデムを接続する

1 ケーブル先端の爪部分を下側に持ち、WAN/ETH0 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。

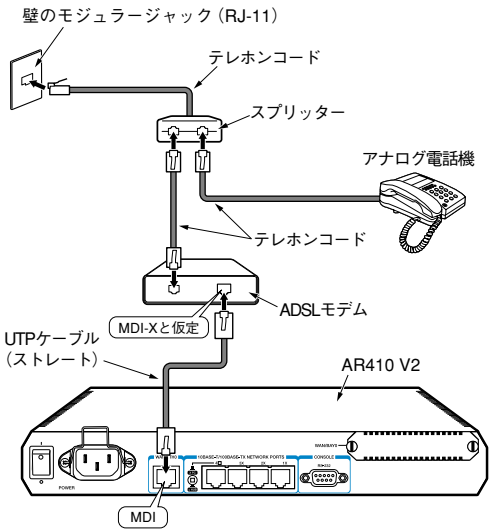


図2.3.1 ADSL モデムの接続

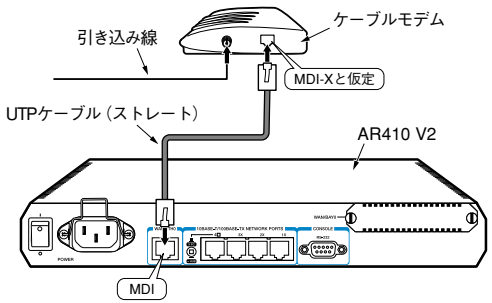


図2.3.2 ケーブルモデムの接続

2 UTP ケーブルのもう一端を、ADSL モデムまたはケーブルモデムに接続してください。

2 コンピューターを接続する

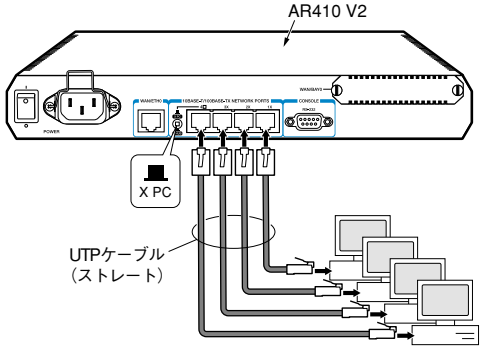


図2.3.3 コンピューターの接続

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。

4 コンピューターを 10BASE-T/100BASE-TX ポート 4 に接続した場合は、MDI/MDI-X 切替スイッチを「X PC」（飛び出した位置）に設定してください。

3 コンソールターミナルを接続する*3

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.24）のコンピューターを転用するのが便利です。

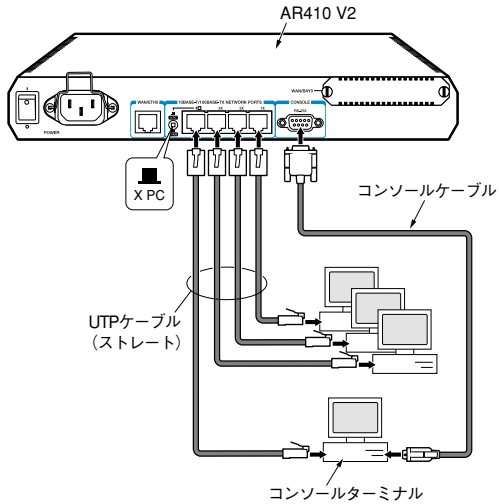


図2.3.4 コンソールターミナルの接続

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。

*3 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。

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。

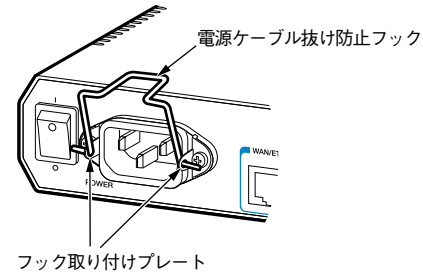


図 2.3.5 電源ケーブル抜け防止フックの取り付け

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ーに接続してください。

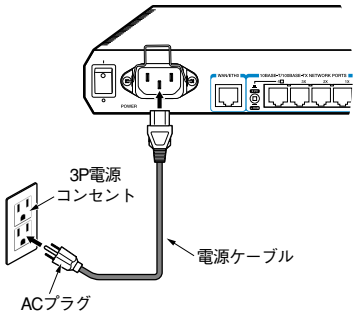


図2.3.6 電源ケーブルの接続

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。

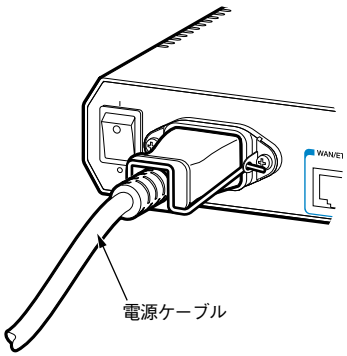


図2.3.7 電源ケーブルのロック

2.4 HUBを接続する

本製品には、4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。

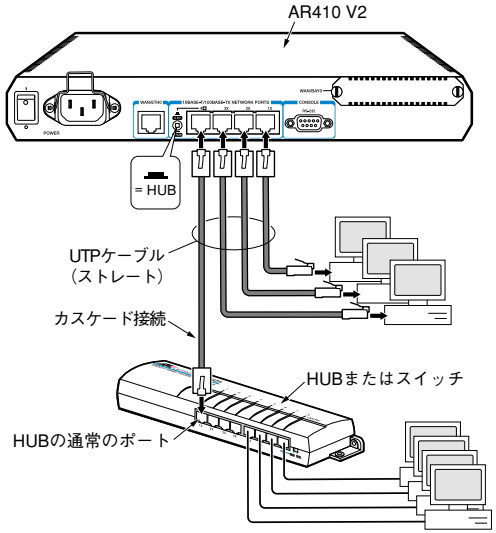


図2.4.1 HUBの接続

1 MDI/MDI-X 切替スイッチを「= HUB」（押し込まれた位置）に設定してください。

2 UTP ケーブルの一端を、本製品背面の 10BASE-T/100BASE-TX ポート 4 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。

3 手順2と同様にして、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。

参照 本書「A.2 ハイパーターミナルの設定」（p.115）

*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「8 Telnet を使う」（p.97）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、そのまま次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、AR ルーターの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, 16384k 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 >
```

参照 本書「4.1 コマンドプロセッサー」（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のようになります。

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

警告 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、センドバック修理を行うことになります。

警告 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で運用した場合、重大なセキュリティーホールとなります。

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。

参照 本書「6 ユーザー管理とセキュリティー」（p.89）

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と、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持続します。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。

参照 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。

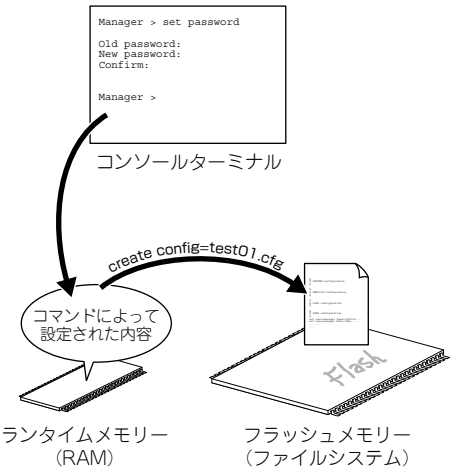


図3.7.1 スクリプトの作成と保存

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
-------------------------------------------------------------
52-233.rez     flash    2394684  04-Sep-2002 14:23:25    0
ac100af0.dhc   flash    80       04-Apr-2002 15:11:56    0
ac1014f0.dhc   flash    80       04-Apr-2002 15:20:39    0
config.ins     flash    32       11-Apr-2002 20:46:20    0
feature.lic    flash    39       18-Feb-2002 15:38:26    0
HELP.HLP       flash    129254   11-Apr-2002 18:29:01    0
prefer.ins     flash    64       02-Apr-2002 15:40:40    0
release.lic    flash    32       18-Dec-2001 12:48:06    0
test01.cfg     flash    2290     11-Apr-2002 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=7c6ff696c5e944eb6f2a0d70a0a74354e2 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「10 ファイルシステム」（p.101）

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

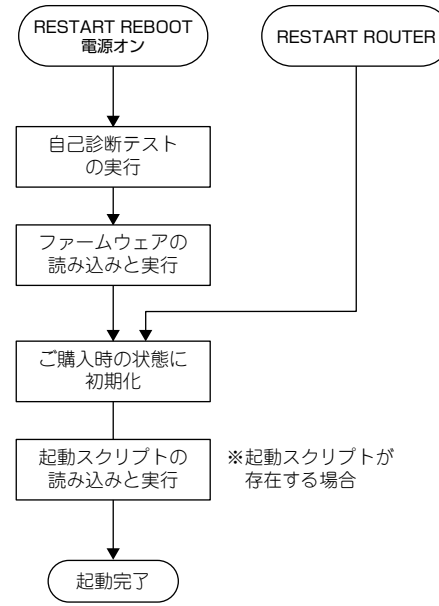


図 3.9.1 ブートシーケンス

RESTART ROUTER コマンドの入力

ソフトウェア的なリセットを行います（**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, 16384k 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。

参照 本書「PPPoE セッションの手動による切断」（p.62）

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。

注 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。セキュリティーのために、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な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-Sep-2002.
Board      ID  Bay Board Name                    Rev   Serial number
-------------------------------------------------------------------------------
Base      195      AR410 V2                      M1-0  57004257
-------------------------------------------------------------------------------
Memory -   DRAM : 16384 kB    FLASH :  7168 kB
-------------------------------------------------------------------------------
SysDescription
CentreCOM AR410 V2 version 2.3.3-00 27-Aug-2002
SysContact

SysLocation

SysName
OSAKA
SysDistName

SysUpTime
49540 ( 00:08:15 )
Software Version: 2.3.3-00 27-Aug-2002
Release Version : 2.3.3-00 27-Aug-2002
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。

参照 本書「3.7 設定の保存」（p.30）

「SHOW CONFIG DYNAMIC」コマンドは、ランタイムメモリー（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=3af5001f767b664cad1ceb3eff0c6ab5d4 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、APPLETALK、IPX 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ー

コマンドプロセッサーは、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ー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。

参照 本書「6 ユーザー管理とセキュリティー」(p.89)
本書「3.5 システム名の変更」(p.29)

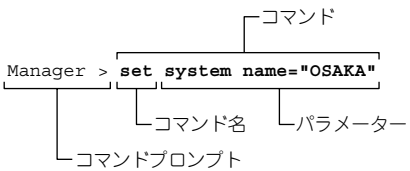


図4.1.1 コマンドの構成

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ーは、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。

参照 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。

  参照 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。

  参照 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。セキュリティーモードでは、Security Officer レベルの権限が必要です。

  参照 本書「6 ユーザー管理とセキュリティー」(p.89)

- 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。

参照 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」の入力
コマンドの履歴のすべてを消去する	「RESET ASYN HISTORY」の入力
最後に入力した *string* で始まるコマンドを表示する	*string*＋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 LOgoff LOgout

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。「?」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 FRamerelay GRE GUI HTTP INSTall INTerface IP IPV6
    IPSec IPX ISAkmp ISDN L2TP LAPB LAPD LDAP LOAder LOG LPD MAnager MAIL
    MIOX NTP NVS OSPF PATch PERM PIM PING PKT ASYn POrt PKI PPP PRI Q931
    RADius RELease RSVP SA SCript SERvice SNmp 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="hanako@myisp.ne.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="hanako@myisp.ne.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

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。

参照 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と、

```
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 途中ま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                         Matches
-------------------------------------------------------------------------------
1    1   ---            192.168.20.4       255.255.255.255  ---              Any
         ---            192.168.10.2       255.255.255.255  Any              Any
         General        Include            Off                               0

     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て、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。

参照 本書「7 テキストエディター」（p.95）

HELP
オンラインヘルプを表示するコマンドです。

参照 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。

参照 本書「11 アップ / ダウンロード」（p.105）

*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。

参照 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。

参照 本書「9.1 Ping」（p.99）

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。

参照 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。

参照 本書「9.1 Ping」（p.99）

TELNET

「Telnet」を実行するコマンドです。

参照 本書「8 Telnet を使う」（p.97）

TRACE

経路のトレースを実行するコマンドです。

参照 本書「9.2 Trace」（p.99）

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。

参照 本書「11 アップ / ダウンロード」（p.105）

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 ↵

        CentreCOM AR410 V2 オンラインヘルプ - V2.3 Rev.01 2002/09/04

  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）。
  (* マーク付きの機能は 2002/09 現在サポートしていません)
  (# マーク付きの機能は追加ライセンスが必要です )

    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、BRI、PRI など）
    Help ISdn               ISDN
    Help Tdm                専用線
    Help FRamerelay         フレームリレー
    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 IPMulticast      * IP マルチキャスト
    Help IPX                IPX
--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 ↵

        CentreCOM AR410 V2 オンラインヘルプ - V2.3 Rev.01 2002/09/04

運用・管理

    Help Operation SYstem                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 SHell                 コマンドプロセッサー
    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 Release               ソフトウェア
    Help Operation Mail                  メール送信
    Help Operation SEcurity              セキュリティー
    Help Operation LOG                   ログ
    Help Operation SCript                スクリプト
    Help Operation TRigger               トリガー
    Help Operation SNmp                  SNMP
    Help Operation Ntp                   NTP
--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

        CentreCOM AR410 V2 オンラインヘルプ - V2.3 Rev.01 2002/09/04

運用・管理 / システム

    EDIT [filename]
    HELP [topic]
    LOGIN [login-name]
    LOGOFF
    RESTART {REBOOT|ROUTER} [CONFIG={filename|NONE}]
    SET HELP=helpfile
    SET SYSTEM CONTACT=contact-name
    SET SYSTEM DISTINGUISHEDNAME={dist-name|NONE}
    SET SYSTEM LOCATION=location
    SET SYSTEM NAME=name
    SET SYSTEM TERRITORY={AUSTRALIA|CHINA|EUROPE|JAPAN|KOREA|NEWZEALAND|
       USA}
    SET [TIME=time] [DATE=date]
    SHOW BUFFER
    SHOW CPU
--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。紙面の都合により、IPX、AppleTalk、ISDN、専用線、フレームリレーには詳しく触れません。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。

参照 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（IPv6は2002年9月現在において未サポートです）。

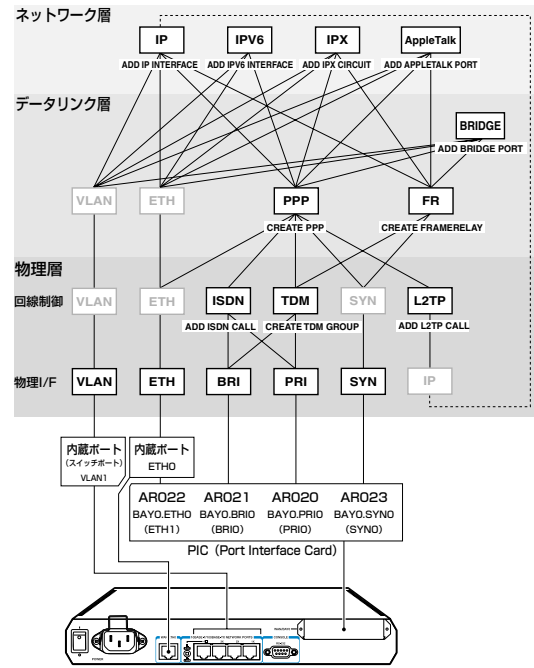


図4.4.1 インターフェースの階層構造

最下層は**物理インターフェース**（ポート）で、本製品に内蔵、またはPIC ベイに装着するPIC（Port Interface Card）モジュールとして提供されます。

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。BRI、PRI インターフェースで ISDN 網に接続するときは発信接続などを担当する ISDN モジュールを、専用線やフレームリレー網に接続するときはタイムスロットの処理を行う TDM モジュールを使います。同期シリアルインターフェースの場合は、回線制御が外付けの TA などによって行われるため、この層を担当するモジュールはありません。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くるのが、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、フレームリレー（FR）の 4 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、同一回線（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、フレームリレーの場合は、「CREATE PPP」「CREATE FRAMERELAY」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か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、IPX、AppleTalk 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」「ADD IPX CIRCUIT」「ADD APPLETALK PORT」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。

短いインターフェース名

インターフェース名には、通常使用する「短いインターフェース名」（短い名前）と、「長いインターフェース名」（長い名前、フルパス名）があります。

「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、短い名前、長い名前（full name）、インディックス番号（ifIndex）を確認できます。

短いインターフェース名（短い名前）は、インターフェースの種類を示す略称（ETH、PRI 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。割り当て順序は、内蔵、PIC ベイの順です。

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		短い名前	長い名前
VLAN インターフェース（データリンク層と一体）	内蔵	vlan1[a]	vlan1
Ethernet インターフェース（データリンク層と一体）	内蔵	eth0	eth0
Ethernet インターフェース（AR022）（データリンク層と一体）	PIC ベイ	eth1	bay0.eth0
BRI インターフェース（AR021）	PIC ベイ	bri0	bay0.bri0
PRI インターフェース（AR020）	PIC ベイ	pri0	bay0.pri0
SYN インターフェース（AR023）	PIC ベイ	syn0	bay0.syn0

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 FRAMERELAY」や「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
フレームリレーインターフェース	fr0 など
PPP インターフェース	ppp0 など

論理インターフェースは、長い名前を持ちません。

長いインターフェース名

物理インターフェースは、PIC ベイの位置情報を含む長い名前で指定することもできます（フルパス名）。PIC ベイは「BAYn」の形式で表します。n はベイの番号です。本製品の場合「0」となります。フルパス名は、PIC ベイ、インターフェースをピリオドで区切って表現します。例えば、PIC ベイに装着した AR022 は、「bay0.eth0」となります（ピリオドの後にくるインターフェースの番号は常に 0 となります）。

内蔵の物理インターフェースでは、短い名前と長い名前は同じになります（eth0）。

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

	短い名前	長い名前
インターフェース番号だけを取るパラメーター	eth=0	eth=eth0
	eth=1	eth=bay0.eth0
インターフェース名を取るパラメーター	over=eth0	over=eth0
	over=eth1	over=bay0.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	int=eth0-1
	int=eth1-1	int=bay0.eth0-1
インターフェースのインデックス番号（ifIndex）を取るパラメーター	int=1	int=eth0
	int=2	int=bay0.eth0

「CREATE CONFIG」コマンドを実行すると、長いインターフェース名で設定が保存されます。

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 5 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）
- BRI インターフェース（bri）
- PRI インターフェース（pri）
- 同期シリアルインターフェース（syn）

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。

*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おりません。

VLAN（LAN 側）インターフェース[*5]

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 4 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、fr0 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、IPX、AppleTalk）を作成することができます。たとえば、vlan1 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=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、AUI[*6]）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「ETHn」の形式で表します。

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、IPX、AppleTalk）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

*5 名前から想像できるとおり、「vlan1」はバーチャル LAN に由来しますが、本製品はユーザーによる VLAN 設定をサポートしておりません。LAN 側は、単なるスイッチ付きの Ethernet ポートと考えてください。

*6 AUI は AR022 によって提供されます。

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 か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 4 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）
- フレームリレーインターフェース（fr）

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、以下のインターフェース（物理インターフェースか回線制御モジュール）上に作成することができます。

- ISDN コール（ISDN 接続）
- TDM グループ（専用線接続）
- 同期シリアルインターフェース（syn）
- Ethernet インターフェース（eth）

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」か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 3 種類です。かっこ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
- IPX インターフェース（IPX サーキット）
- AppleTalk インターフェース（AppleTalk ポート）

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、IPX、AppleTalk）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します。

```
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します。

```
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.   SAMode  IPSc
Pri. Filt     Pol.Filt Network Mask     MTU   VJC   GRE  OSPF Met.  DBcast  Mul.
-------------------------------------------------------------------------------
Local         ---      Not set          -  -  -     ---  --         Pass    --
---           ---      Not set          1500  -     ---  --         ---     ---
vlan1         Static   192.168.1.1      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します。

```
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。

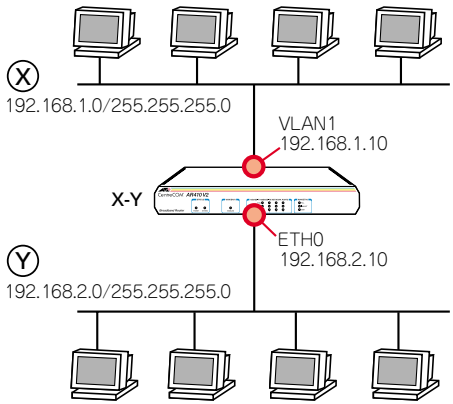


図 4.5.1 2 つの LAN の接続

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 Fr 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ー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 ↵

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              16
-                 direct   0        interface         1                   0
192.168.2.0       255.255.255.0     0.0.0.0           eth0                7
-                 direct   0        interface         1                   0
-------------------------------------------------------------------------------
```

3 つの LAN の接続

図 4.5.1（p.46）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。

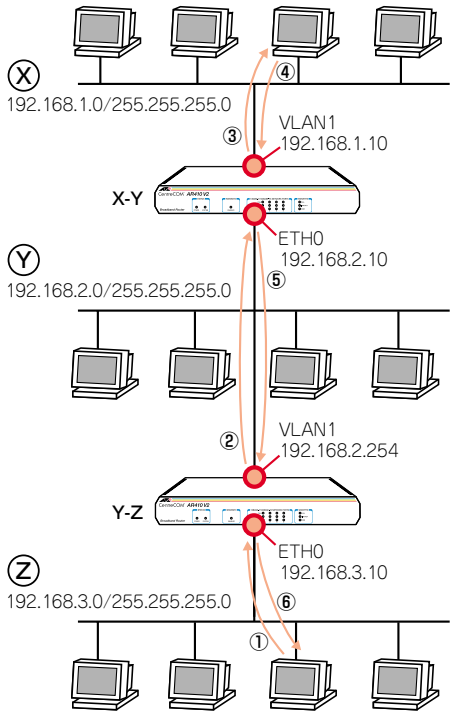


図 4.5.2 3 つの LAN の接続

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。

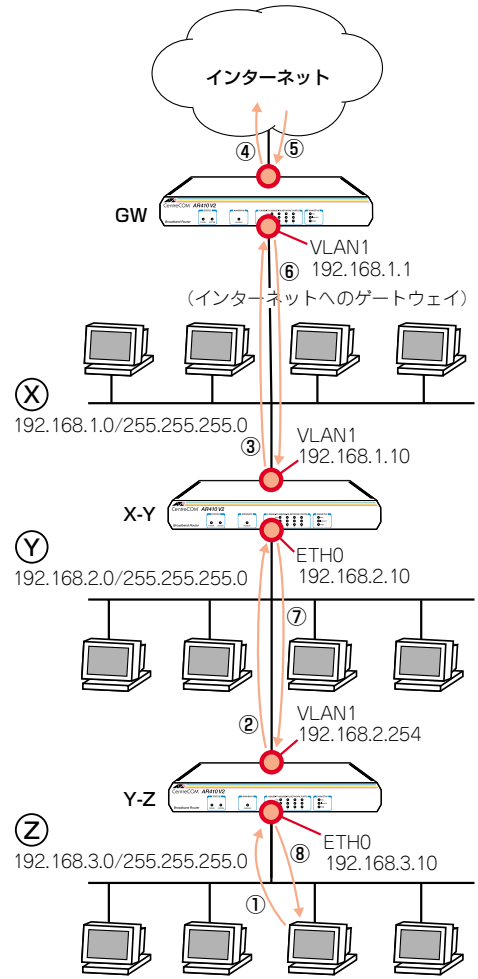


図4.5.3 インターネットにも接続

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       Mask             NextHop          Interface          Age
DLCI/Circ.        Type     Policy  Protocol         Metrics      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       Mask             NextHop          Interface          Age
DLCI/Circ.        Type     Policy  Protocol         Metrics      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[*7]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。

*7 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 構成例

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、5 例を説明します。

- 5.2 Ethernet による端末型インターネット接続（CATV）（p.52）
- 5.3 PPPoE による端末型インターネット接続（p.56）
- 5.4 PPPoE による端末型インターネット接続（固定 IP アドレス 1）（p.64）
- 5.5 PPPoE による LAN 型インターネット接続（マルチホーミング）（p.66）
- 5.6 PPPoE による LAN 型インターネット接続（スタティック NAT）（p.71）

次に、上記5 例で挙げた例同士を、L2TP によって LAN 間接続する方法を説明します。

- 5.7 L2TP による LAN 間接続（p.76）

最後に、IPsec を使用し L2TP にセキュリティーを与える方法を説明します。

- 5.7 L2TP による LAN 間接続（p.76）

5.1 設定をはじめる前に

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。「↵」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、「↵」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 ↵

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

また、複数サイトに対して設定を施す場合、両者を併記し、コマンド実行で表示されるメッセージは一方（A）のみを示します。

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¥410SAMP.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、バッファーがあふれたり、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。

5.2 Ethernet による端末型インターネット接続

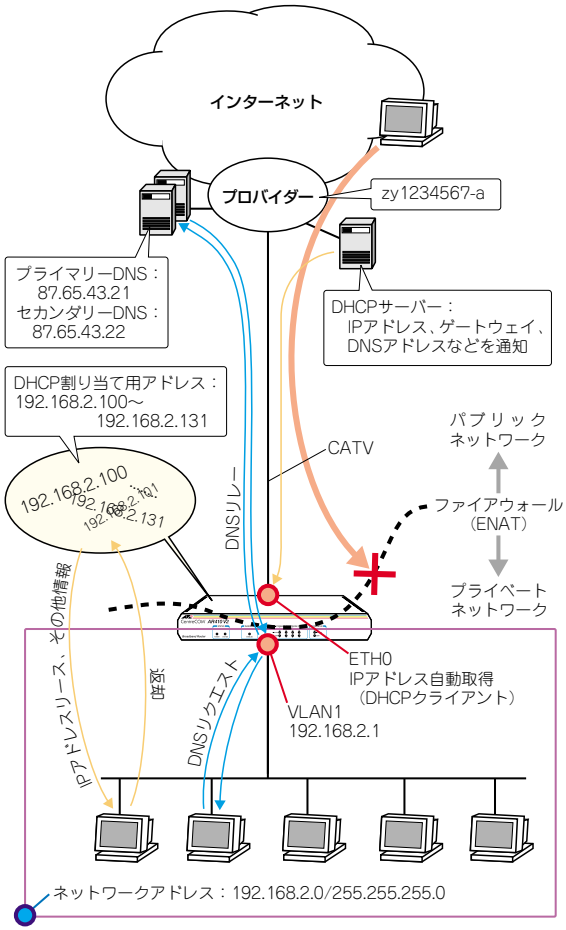


図5.2.1 CATVによる端末型の接続

CATV 系でよく見られる接続形態です。ケーブルモデムを介して、Ethernet でプロバイダーに接続します。この例は、DHCP によりグローバル IP アドレスを動的に割り当てられる端末型接続の基本設定です。

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。「コンピューター名」は、接続の際の認証に使用される文字列です（コンピューター名が提供されないプロバイダーもあります。その場合、設定は不要です）。

- コンピューター名：zy1234567-a
- IP アドレス グローバルアドレス：1 個（動的割り当て）
- ゲートウェイアドレス：接続時に通知される
- DNS サーバー：接続時に通知される

設定の方針

- WAN 側 Ethernet インターフェースの IP アドレスとネットマスクは、プロバイダーの DHCP サーバーから取得します。また、ゲートウェイアドレスと DNS サーバーアドレスも、DHCP サーバーから入手し自動的に設定します。
- 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。
- 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。
- 本製品の IP アドレスは、下記のように設定します。

表5.2.1 本製品の基本設定

WAN 側（eth0）IP アドレス	接続時にプロバイダーの DHCP サーバーから取得する
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5.2.2 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 設置、配線が完了したら、本製品の電源スイッチをオンにします。

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）
```

●IP、ルーティングの設定

3 IPモジュールを有効にします。

```
Manager > ENABLE IP ↵

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

4 プロバイダーのDHCPサーバーから取得したIPアドレスを、WAN側（eth0）インターフェースに割り当てるよう設定します。また、デフォルトルート、DNSサーバーアドレスの設定も、DHCPサーバーからの情報に基づいて自動的に行われます。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.

Manager > ADD IP INT=eth0 IP=DHCP ↵

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

5 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.
```

●DNSリレーの設定

6 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

7 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.
```

8 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.
```

9 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.
```

10 本製品のidentプロキシー機能を無効にし、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。

11 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（eth0）インターフェースをPUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=eth0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

12 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設定します。グローバルアドレスには、WAN 側（eth0）インターフェースの IP アドレスを使用します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=eth0 ↵

Info (1077003): Operation successful.
```

● DHCP サーバーの設定

13 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.
```

14 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.
```

15 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.
```

16 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.
```

●接続認証の設定

17 プロバイダーからコンピューター名が指示されている場合、そのコンピュータ名を本製品のシステム名に設定します（大文字・小文字を判別しますので、正確に入力してください）。システム名に設定された文字列は、本製品がプロバイダーの DHCP サーバーに対して、IP アドレスを要求する際の認証の文字列として使用されます。

```
Manager > SET SYSTEM NAME=zy1234567-a ↵
```

●時刻、パスワード、設定保存

18 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 zy1234567-a> SET TIME=01:00:01
    DATE=21-APR-2002 ↵

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

19 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 zy1234567-a> SET PASSWORD ↵

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

20 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 zy1234567-a> CREATE CONF=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

21 起動スクリプトとして指定します。

```
Manager zy1234567-a> SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

●接続の確認

22 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 DHCP」コマンドによって確認できます。

```
Manager zy1234567-a> SHOW DHCP ↵

DHCP Server

  State .................. enabled
  BOOTP Status ........... disabled
  Debug Status ........... disabled
  Policies ............... BASE
  Ranges ................. LOCAL ( 192.168.2.100 - 192.168.2.131 )
  In Messages ............ 6
  Out Messages ........... 10
  In DHCP Messages ....... 6
  Out DHCP Messages ...... 10
  In BOOTP Messages ...... 0
  Out BOOTP Messages ..... 0

DHCP Client

  Interface .............. eth0
  State .................. bound
  Server ................. 123.45.11.5
  Assigned Domain ........ myisp.ne.jp
  Assigned IP ............ 123.45.11.22
  Assigned Mask .......... 255.255.255.0
  Assigned Gateway ....... 123.45.11.1
  Assigned DNS ........... 87.65.43.21 87.65.43.22
  Assigned Lease ......... 259200
```

23 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。

L2TP、IPsec 使用時の注意

後述の「5.7 L2TP によるLAN 間接続」(p.76)、「5.8 L2TP ＋IPsec によるLAN 間接続」（p.80）の設定の際に、手順 17（p.54）で設定したシステム名を変更しないでください。変更してしまうと、認証に失敗しプロバイダーとの接続ができなくなります。

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5.2.3 設定スクリプトファイル（ROUTER.CFG）

1	ENABLE IP
2	ENABLE IP REMOTEASSIGN
3	ADD IP INT=eth0 IP=DHCP
4	ADD IP INT=vlan1 IP=192.168.2.1 MASK=255.255.255.0
5	ENABLE IP DNSRELAY
6	ENABLE FIREWALL
7	CREATE FIREWALL POLICY=net
8	ENABLE FIREWALL POLICY=net ICMP_F=PING,UNREACH
9	DISABLE FIREWALL POLICY=net IDENTPROXY
10	ADD FIREWALL POLICY=net INT=vlan1 TYPE=PRIVATE
11	ADD FIREWALL POLICY=net INT=eth0 TYPE=PUBLIC
12	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=eth0
13	ENABLE DHCP
14	CREATE DHCP POLICY=BASE LEASETIME=7200
15	ADD DHCP POLICY=BASE SUBNET=255.255.255.0 ROUTER=192.168.2.1 DNSSERVER=192.168.2.1
16	CREATE DHCP RANGE=LOCAL POLICY=BASE IP=192.168.2.100 NUMBER=32
17	SET SYSTEM NAME=zy1234567-a

「SET TIME」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。

5.3 PPPoE による端末型インターネット接続

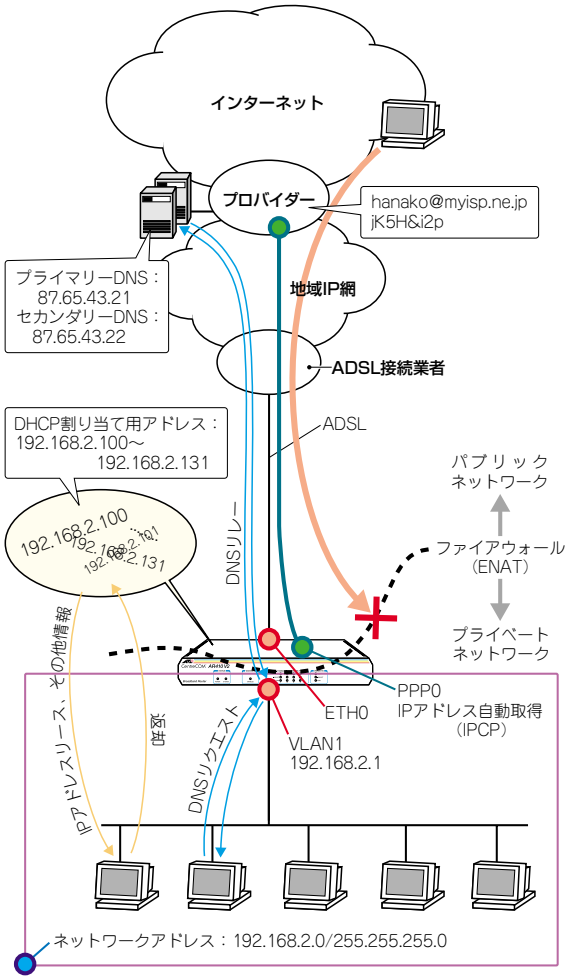


図5.3.1 PPPoEによる端末型の接続

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：hanako@myisp.ne.jp
- 接続のパスワード：jK5H&i2p
- 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5.3.1 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	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5.3.2 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、ADSL接続業者から通知されたPPPoEの「サービス名」を記述します。ADSL接続業者から指定がない場合は、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=hanako@myisp.ne.jp
    PASSWORD=jK5H&i2p 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に設定します。

```
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。*2

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

Info (1077003): Operation successful.
```

16 本製品の ident プロキシー機能を無効にし、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.
```

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.
```

*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。

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 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.
```

26 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.
```

27 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.
```

●時刻、パスワード、設定保存

28 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.
```

29 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: xxxxxxx ↵
Confirm: xxxxxxx ↵
```

30 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.
```

31 起動スクリプトとして指定します。

```
Manager > SET CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

32 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

33 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                          IPCP        OPENED
                                     eth0-any            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
  ------------------------------------------------------------------------

.........
```

34 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
  ------------------------------------------------------------------------
```

35 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。

トリガーの動作

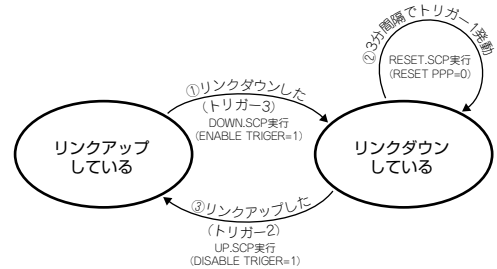


図5.3.2 トリガーの動作

1 手順 25（p.59）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

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（CREATE TFIGGER=1 のパラメーターが手順25（p.59）のコマンドと同じである必要があるため）。

```
Manager > SHOW PPP ↵

  Name           Enabled  ifIndex  Over                CP          State
  ---------------------------------------------------------------------------
  ppp0             YES      04                        IPCP        CLOSED
                                    eth0-any           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ます。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                        IPCP        OPENED
                                    eth0-any           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 か 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=3f7a67b6c6cad11b5db4403ef6ce5af00f 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働きません。

```
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。

参照 本書「7.1 Edit の実行」（p.95）
本書「A.2 ハイパーターミナルの設定」（p.115）

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。保存するか否か問われますので、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                        IPCP        CLOSED
                                    eth0-any           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="isppasswd1"
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 ↵
```

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5.3.3 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=hanako@myisp.ne.jp PASSWORD=jK5H&i2p 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
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5.3.4 スクリプト「reset.scp」

RESET PPP=0

表5.3.5 スクリプト「up.scp」

DISABLE TRIGGER=1

表5.3.6 スクリプト「down.scp」

ENABLE TRIGGER=1

5.4 PPPoE による端末型インターネット接続（固定 IP アドレス 1）

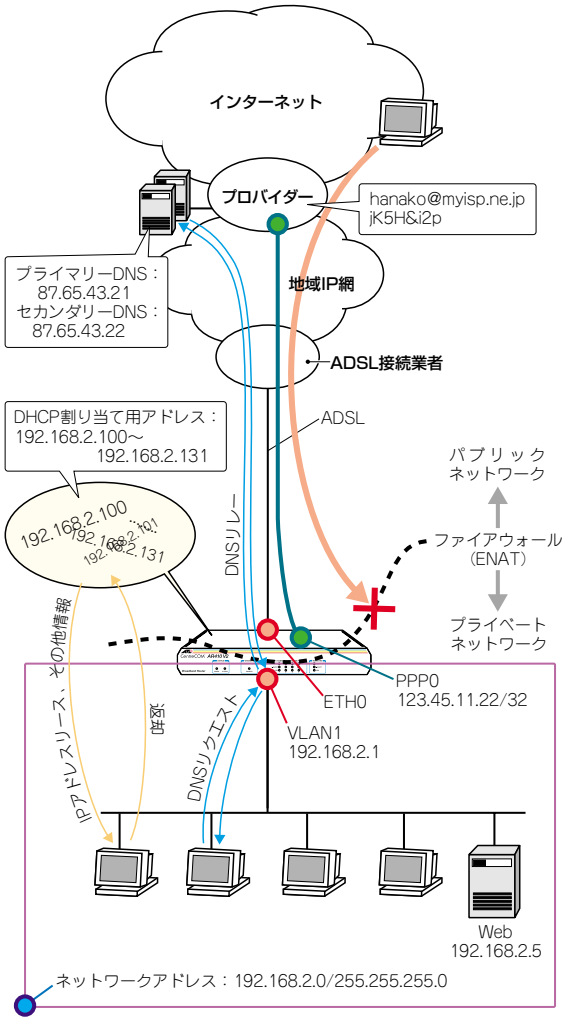


図 5.4.1 PPPoE による端末型の接続（IP1）

PPPoE を使ってプロバイダーに接続します。「ブロードバンド」系サービスプロバイダーの中には、ベストエフォート型ながらも、常時接続の性質を活かして IP アドレスを 1 個固定的に割り当てるサービスが見られます。このようなサービスを利用すると、接続形態は端末型でも、固定アドレスの利点を活かしてサーバーの公開や VPN の構築が容易になります。

この例では、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つつ、スタティック NAT を利用して Web サーバーを外部に公開します。また、LAN 側クライアン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：hanako@myisp.ne.jp
- 接続のパスワード：jK5H&i2p
- PPPoE サービス名：指定なし
- IP アドレス グローバルアドレス：123.45.11.22/32（固定）
- DNS サーバー：87.65.43.21、87.65.43.22

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。
- ファイアウォールのスタティック NAT 機能を利用して、本製品の 80 番ポートに送られてきた TCP パケットを LAN 側の Web サーバー（192.168.2.5）に転送します（ポート転送）。これにより、IP アドレスが 1 個であっても、サーバーを外部に公開することができます。
- 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 5.4.1 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	123.45.11.22/32（固定）
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5.4.2 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

IPアドレスがあらかじめ固定で与えられている点、スタティックNATを使用して Web サーバーをインターネットに公開する点を除いて、「5.3 PPPoE による端末型インターネット接続」（p.56）とほぼ同じです。

以下に、「5.3 PPPoE による端末型インターネット接続」（p.56）との相違点のみを挙げます。

●IP の設定

手順5（p.57）のコマンドの代わりに、下記を入力してください。IP アドレスは固定で入力するため、「IPREQUEST=ON」パラメーターは不要です。

```
Manager > SET PPP=0 OVER=eth0-any
    USER=hanako@myisp.ne.jp PASSWORD=jK5H&i2p
    LQR=OFF BAP=OFF ECHO=ON ↵

Info (1003003): Operation successful.
```

手順7（p.57）の「ENABLE IP REMOTEASSIGN」コマンドは入力しません。

手順 9（p.57）のコマンドの代わりに、下記を入力してください。WAN 側（ppp0）インターフェースには、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 > ADD IP INT=ppp0 IP=123.45.11.22
    MASK=255.255.255.255 ↵

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

●DNS リレーの設定

手順11（p.57）のコマンドでDNS 機能を有効化する前に、DNS サーバーアドレスを設定します。

```
Manager > SET IP NAMESERVER=87.65.43.21 ↵

Info (1005282): Name server successfully updated.

Manager > SET IP
    SECONDARYNAMESERVER=87.65.43.22 ↵

Info (1005282): Secondary name server successfully updated.

Manager > ENABLE IP DNSRELAY ↵

Info (1005003): Operation successful.
```

手順12（p.58）の「SET IP DNSRELAY INT=ppp0」コマンドは入力しません。DNS サーバーアドレスを設定しているので不要です。

●ファイアウォールの設定

手順18（p.58）のコマンドの入力の次に、下記を入力してください。これは、Web サーバー（192.168.2.5）をインターネットに公開する設定です。スタティックNAT により、本製品のWAN 側のインターフェース（ppp0）の80 番ポート宛てに送られた TCP パケットを、LAN 側のWeb サーバーに転送します。

```
Manager > ADD FIREWALL POLICY=net RULE=1
    AC=ALLOW INT=ppp0 PROTO=TCP
    GBLIP=123.45.11.22 GBLPORT=80
    IP=192.168.2.5 PORT=80 ↵

Info (1077003): Operation successful.
```

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。トリガー関連のスクリプトは、「5.3 PPPoE による端末型インターネット接続」におけるものと同じです（p.63）。

表 5.4.3 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 USER=hanako@myisp.ne.jp
        PASSWORD=jK5H&i2p LQR=OFF BAP=OFF ECHO=ON
3   ENABLE IP
4   ADD IP INT=vlan1 IP=192.168.2.1
        MASK=255.255.255.0
5   ADD IP INT=ppp0 IP=123.45.11.22
        MASK=255.255.255.255
6   ADD IP ROUTE=0.0.0.0 INT=ppp0 NEXTHOP=0.0.0.0
7   SET IP NAMESERVER=87.65.43.21
8   SET IP SECONDARYNAMESERVER=87.65.43.22
9   ENABLE IP DNSRELAY
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  ADD FIREWALL POLICY=net RULE=1 AC=ALLOW
        INT=ppp0 PROTO=TCP GBLIP=123.45.11.22
        GBLPORT=80 IP=192.168.2.5 PORT=80
18  ENABLE DHCP
19  CREATE DHCP POLICY=BASE LEASETIME=7200
20  ADD DHCP POLICY=BASE SUBNET=255.255.255.0
        ROUTER=192.168.2.1 DNSSERVER=192.168.2.1
21  CREATE DHCP RANGE=LOCAL POLICY=BASE
        IP=192.168.2.100 NUMBER=32
22  ENABLE TRIGGER
23  CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
24  CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP
        CP=IPCP SCRIPT=up.scp
25  CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN
        CP=IPCP SCRIPT=down.scp
```

5.5 PPPoE による LAN 型インターネット接続（マルチホーミング）

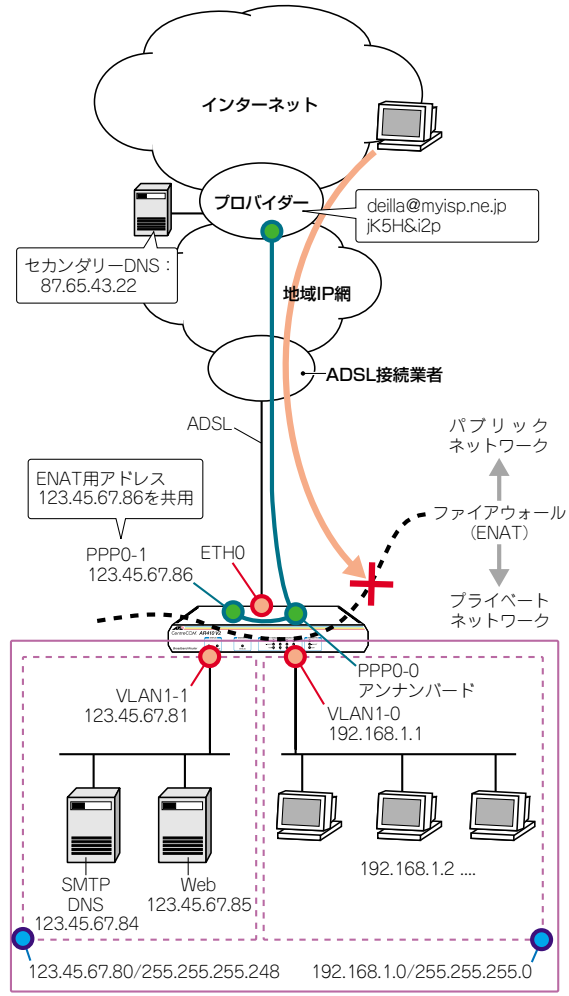


図 5.5.1 PPPoE による LAN 型の接続（マルチホーミング）

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、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：hanako@myisp.ne.jp
- 接続のパスワード：jK5H&i2p
- PPPoE サービス名：指定なし
- 使用できる IP アドレス：123.45.67.80/29（123.45.67.80 ～ 123.45.67.87）

設定の方針

- LAN 側インターフェースをマルチホーミングし、一方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、もう一方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擬似的な 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：123.45.67.85：80/tcp
  - SMTP サーバー：123.45.67.84：25/tcp
  - DNS サーバー：123.45.67.84：53/tcp、53/udp

- L2TP、IPsec を使用することを考慮し、PPP0 をマルチホーミングします。PPP0-0 をアンナンバードに、PPP0-1 に 123.45.67.86 を割り当て、デフォルトルートを PPP0-1 に向けます。

  参照 本書「PPPoE におけるアンナンバード」（p.70）

- 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、PPP0-1 に割り当てたアドレス（123.45.67.86）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 5.5.1 本製品の基本設定

WAN 側物理インターフェース	eth0
WAN 側（ppp0-0）IP アドレス	アンナンバード
WAN 側（ppp0-1）IP アドレス	123.45.67.86/32
DMZ 側（VLAN1-1）IP アドレス	123.45.67.81/29
LAN 側（VLAN1-0）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、ADSL 接続業者から通知された PPPoE の「サービス名」を記述します。ADSL 接続業者から指定がない場合は、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=deilla@myisp.ne.jp
    PASSWORD=jK5H&i2p 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に設定します。

```
Manager > ENABLE IP REMOTEASSIGN ↵

Info (1005287): Remote IP assignment has been enabled.
```

8 LAN 側（VLAN1-1）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（123.45.67.81）を設定し、擬似的な DMZ として使用します。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=VLAN1-1 IP=123.45.67.81
    MASK=255.255.255.248 ↵

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

9 LAN 側（VLAN1-0）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=VLAN1-0 IP=192.168.1.1
    MASK=255.255.255.0 ↵

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

10 WAN 側（ppp0-0）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=ppp0-0 IP=0.0.0.0 ↵

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

マルチホーミングしたインターフェース ppp0-1 に 123.45.67.86 を割り当てます。

```
Manager > ADD IP INT=ppp0-1 IP=123.45.67.86
    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 > ADD IP ROUTE=0.0.0.0 INT=ppp0-1
    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。[*3]

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

Info (1077003): Operation successful.
```

15 本製品の ident プロキシー機能を無効にし、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.
```

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。

*3 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（VLAN1-1）インターフェースをPRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=VLAN1-1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

LAN 側（VLAN1-0）インターフェースを PRIVATE（内部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=VLAN1-0
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

WAN 側（ppp0-0）インターフェースを PUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0-0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

マルチホーミングしたインターフェース（PPP0-1）を PUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0-1
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

17 LAN 側（VLAN1-0）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 123.45.67.86 を共用します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=VLAN1-0 GBLINT=ppp0-1
    GBLIP=123.45.67.86 ↵

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（123.45.67.85 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=ppp0-0 PROTO=TCP
    IP=123.45.67.85 PORT=80 ↵

Info (1077003): Operation successful.
```

SMTP サーバー（123.45.67.84 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=ppp0-0 PROTO=TCP
    IP=123.45.67.84 PORT=25 ↵

Info (1077003): Operation successful.
```

DNS サーバー（123.45.67.84 の TCP[*4] 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=ppp0-0 PROTO=TCP
    IP=123.45.67.84 PORT=53 ↵

Info (1077003): Operation successful.

Manager > ADD FIREWALL POLICY=net RULE=4
    AC=ALLOW INT=ppp0-0 PROTO=UDP
    IP=123.45.67.84 PORT=53 ↵

Info (1077003): Operation successful.
```

●トリガー、時刻、パスワード、設定保存、動作の確認

19「5.3 PPPoE による端末型インターネット接続」（p.56）の手順 23～ 35 を実行してください。

下記の項もご覧ください。

参照 本書「トリガーの動作」（p.60）
本書「設定の保存はリンクダウンの状態で」（p.61）
本書「接続できないときは ..」（p.61）
本書「PPPoE セッションの手動による切断」（p.62）
本書「再接続」（p.63）

*4 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。

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 123.45.67.80/29 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 123.45.67.86 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=123.45.67.86
    MASK=255.255.255.255
ADD IP INT=VLAN1-1 IP=123.45.67.81
    MASK=255.255.255.248
ADD IP INT=VLAN1-0 IP=192.168.1.1
    MASK=255.255.255.0
ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXT=0.0.0.0
```

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。トリガー関連のスクリプトは、「5.3 PPPoE による端末型インターネット接続」におけるものと同じです（p.63）。

表 5.5.2 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=deilla@myisp.ne.jp PASSWORD=jK5H&i2p LQR=OFF ECHO=ON
3	ENABLE IP
4	ENABLE IP REMOTEASSIGN
5	ADD IP INT=VLAN1-1 IP=123.45.67.81 MASK=255.255.255.248
6	ADD IP INT=VLAN1-0 IP=192.168.1.1 MASK=255.255.255.0
7	ADD IP INT=ppp0-0 IP=0.0.0.0
8	ADD IP INT=ppp0-1 IP=123.45.67.86 MASK=255.255.255.255
9	ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXTHOP=0.0.0.0
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=VLAN1-1 TYPE=PRIVATE
15	ADD FIREWALL POLICY=net INT=VLAN1-0 TYPE=PRIVATE
16	ADD FIREWALL POLICY=net INT=ppp0-0 TYPE=PUBLIC
17	ADD FIREWALL POLICY=net INT=ppp0-1 TYPE=PUBLIC
18	ADD FIREWALL POLICY=net NAT=ENHANCED INT=VLAN1-0 GBLINT=ppp0-1 GBLIP=123.45.67.86
19	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0-0 PROTO=TCP IP=123.45.67.85 PORT=80
20	ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0-0 PROTO=TCP IP=123.45.67.84 PORT=25
21	ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0-0 PROTO=TCP IP=123.45.67.84 PORT=53
22	ADD FIREWALL POLICY=net RULE=4 AC=ALLOW INT=ppp0-0 PROTO=UDP IP=123.45.67.84 PORT=53
23	ENABLE TRIGGER
24	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
25	CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp
26	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp

5.6 PPPoEによるLAN型インターネット接続（スタティックNAT）

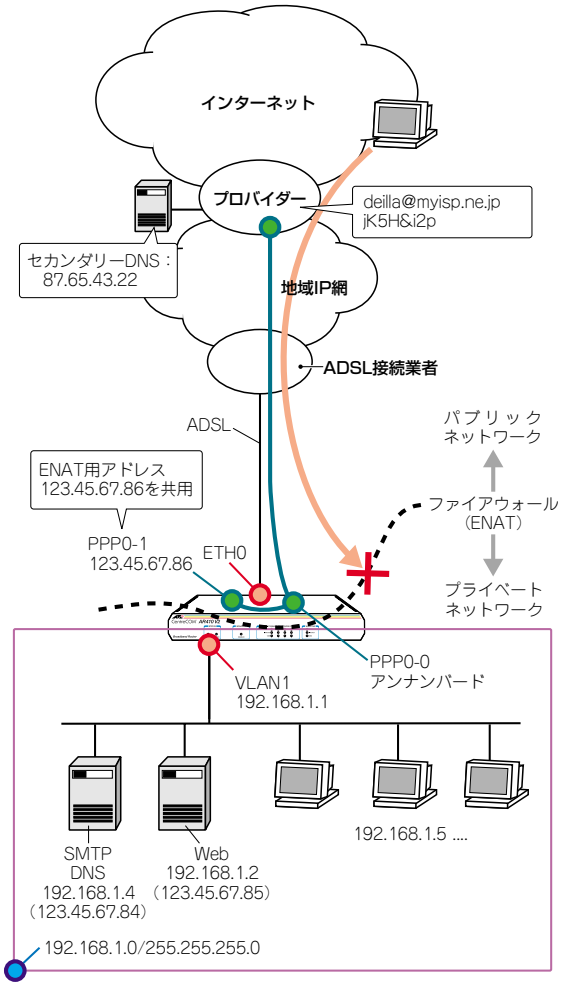


図5.6.1 PPPoEによるLAN型の接続（スタティックNAT）

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、プロバイダーから割り当てられたアドレスを本製品やホストに直接割り当てず、LAN 側コンピューターはプライベートアドレスで運用します。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させます。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、スタティック NAT を使って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：hanako@myisp.ne.jp
- 接続のパスワード：jK5H&i2p
- PPPoE サービス名：指定なし
- 使用できる IP アドレス：123.45.67.80/29（123.45.67.80 ～ 123.45.67.87）

設定の方針

- L2TP、IPsec を使用することを考慮し、PPP0 をマルチホーミングします。PPP0-0 をアンナンバードに、PPP0-1 に 123.45.67.86 を割り当て、デフォルトルートを PPP0-1 に向けます。

  参照 本書「PPPoE におけるアンナンバード」（p.70）

- LAN 側はすべてプライベートアドレスで運用します。LAN 側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、PPP0-1 に割り当てた 123.45.67.86 を使います。

- 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。

- LAN 側のサーバーにもプライベートアドレスを割り当てますが、外部からアクセスさせるため、スタティック NAT を使って外からはグローバルアドレスを持っているように見せかけます。変換ルールは次のとおりとします。

  - Web サーバー：192.168.1.2 → 123.45.67.85
  - SMTP/DNS サーバー：192.168.1.4 → 123.45.67.84

- 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：123.45.67.85：80/tcp
  - SMTP サーバー：123.45.67.84：25/tcp
  - DNS サーバー：123.45.67.84：53/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、下記の通りです。

表5.6.1 本製品の基本設定

WAN側物理インターフェース	eth0
WAN側（ppp0-0）IP アドレス	アンナンバード
WAN側（ppp0-1）IP アドレス	123.45.67.86/32
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、ADSL 接続業者から通知された PPPoE の「サービス名」を記述します。ADSL 接続業者から指定がない場合は、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=deilla@myisp.ne.jp
    PASSWORD=jK5H&i2p 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に設定します。

```
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.
```

9 WAN 側（ppp0-0）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=ppp0-0 IP=0.0.0.0 ↵

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

マルチホーミングしたインターフェースppp0-1 に123.45.67.86 を割り当てます。

```
Manager > ADD IP INT=ppp0-1 IP=123.45.67.86
    MASK=255.255.255.255 ↵

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=ppp0-1
    NEXTHOP=0.0.0.0 ↵

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

●ファイアウォールの設定

11 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.
```

12 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.
```

13 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。[*5]

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

Info (1077003): Operation successful.
```

14 本製品の ident プロキシー機能を無効にし、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.
```

15 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（ppp0-0）インターフェースを PUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0-0
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

マルチホーミングしたインターフェース（PPP0-1）を PUBLIC（外部）に設定します。

```
Manager > ADD FIREWALL POLICY=net INT=ppp0-1
    TYPE=PUBLIC ↵

Info (1077003): Operation successful.
```

16 スタティック NAT によるサーバー公開設定を行います。

Web サーバー（192.168.1.2）を、外部からは 123.45.67.85 であるかのように見せかけます。

```
Manager > ADD FIREWALL POLICY=net NAT=STANDARD
    INT=vlan1 IP=192.168.1.2 GBLINT=ppp0-0
    GBLIP=123.45.67.85 ↵

Info (1077003): Operation successful.
```

SMTP サーバー、DNS サーバー（192.168.1.4）を、外部からは 123.45.67.84 であるかのように見せかけます。

```
Manager > ADD FIREWALL POLICY=net NAT=STANDARD
    INT=vlan1 IP=192.168.1.4 GBLINT=ppp0-0
    GBLIP=123.45.67.84 ↵

Info (1077003): Operation successful.
```

17 ダイナミック ENAT の設定を行います。LAN 側のプライベート 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 123.45.67.86 に変換するよう設定します。

```
Manager > ADD FIREWALL POLICY=net NAT=ENHANCED
    INT=vlan1 GBLINT=ppp0-1
    GBLIP=123.45.67.86 ↵

Info (1077003): Operation successful.
```

*5 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。

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､サーバーへのパケットを通すための設定を行います。

Web サーバー（123.45.67.85 の TCP80 番）へのパケットは通過させます。スタティック NAT を使用しているため、NAT 後のグローバルアドレス（GBLIP、GBLPORT）と NAT 前のプライベートアドレス（IP、PORT）の両方を指定します。

```
Manager > ADD FIREWALL POLICY=net RULE=1
    AC=ALLOW INT=ppp0-0 PROTO=TCP
    GBLIP=123.45.67.85 GBLPORT=80
    IP=192.168.1.2 PORT=80 ↵

Info (1077003): Operation successful.
```

SMTP サーバー（123.45.67.84 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=ppp0-0 PROTO=TCP
    GBLIP=123.45.67.84 GBLPORT=25
    IP=192.168.1.4 PORT=25 ↵

Info (1077003): Operation successful.
```

DNS サーバー（123.45.67.84 の TCP[*6] 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=ppp0-0 PROTO=TCP
    GBLIP=123.45.67.84 GBLPORT=53
    IP=192.168.1.4 PORT=53 ↵

Info (1077003): Operation successful.

Manager > ADD FIREWALL POLICY=net RULE=4
    AC=ALLOW INT=ppp0-0 PROTO=UDP
    GBLIP=123.45.67.84 GBLPORT=53
    IP=192.168.1.4 PORT=53 ↵

Info (1077003): Operation successful.
```

●トリガー、時刻、パスワード、設定保存、動作の確認

19「5.3 PPPoE による端末型インターネット接続」（p.56）の手順 23～ 35 を実行してください。

下記の項もご覧ください。

参照 本書「トリガーの動作」（p.60）
本書「設定の保存はリンクダウンの状態で」（p.61）
本書「接続できないときは ..」（p.61）
本書「PPPoE セッションの手動による切断」（p.62）
本書「再接続」（p.63）

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。トリガー関連のスクリプトは、「5.3 PPPoE による端末型インターネット接続」におけるものと同じです（p.63）。

*6 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。

表5.6.2 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=deilla@myisp.ne.jp PASSWORD=jK5H&i2p LQR=OFF ECHO=ON
3	ENABLE IP
4	ENABLE IP REMOTEASSIGN
5	ADD IP INT=vlan1 IP=192.168.1.1 MASK=255.255.255.0
6	ADD IP INT=ppp0-0 IP=0.0.0.0
7	ADD IP INT=ppp0-1 IP=123.45.67.86 MASK=255.255.255.255
8	ADD IP ROUTE=0.0.0.0 INT=ppp0-1 NEXTHOP=0.0.0.0
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=vlan1 TYPE=PRIVATE
14	ADD FIREWALL POLICY=net INT=ppp0-0 TYPE=PUBLIC
15	ADD FIREWALL POLICY=net INT=ppp0-1 TYPE=PUBLIC
16	ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan1 IP=192.168.1.2 GBLINT=ppp0-0 GBLIP=123.45.67.85
17	ADD FIREWALL POLICY=net NAT=STANDARD INT=vlan1 IP=192.168.1.4 GBLINT=ppp0-0 GBLIP=123.45.67.84
18	ADD FIREWALL POLICY=net NAT=ENHANCED INT=vlan1 GBLINT=ppp0-1 GBLIP=123.45.67.86
19	ADD FIREWALL POLICY=net RULE=1 AC=ALLOW INT=ppp0-0 PROTO=TCP GBLIP=123.45.67.85 GBLPORT=80 IP=192.168.1.2 PORT=80
20	ADD FIREWALL POLICY=net RULE=2 AC=ALLOW INT=ppp0-0 PROTO=TCP GBLIP=123.45.67.84 GBLPORT=25 IP=192.168.1.4 PORT=25
21	ADD FIREWALL POLICY=net RULE=3 AC=ALLOW INT=ppp0-0 PROTO=TCP GBLIP=123.45.67.84 GBLPORT=53 IP=192.168.1.4 PORT=53
22	ADD FIREWALL POLICY=net RULE=4 AC=ALLOW INT=ppp0-0 PROTO=UDP GBLIP=123.45.67.84 GBLPORT=53 IP=192.168.1.4 PORT=53
23	ENABLE TRIGGER
24	CREATE TRIGGER=1 PERIODIC=3 SCRIPT=reset.scp
25	CREATE TRIGGER=2 INTERFACE=ppp0 EVENT=UP CP=IPCP SCRIPT=up.scp
26	CREATE TRIGGER=3 INTERFACE=ppp0 EVENT=DOWN CP=IPCP SCRIPT=down.scp

5.7 L2TP による LAN 間接続

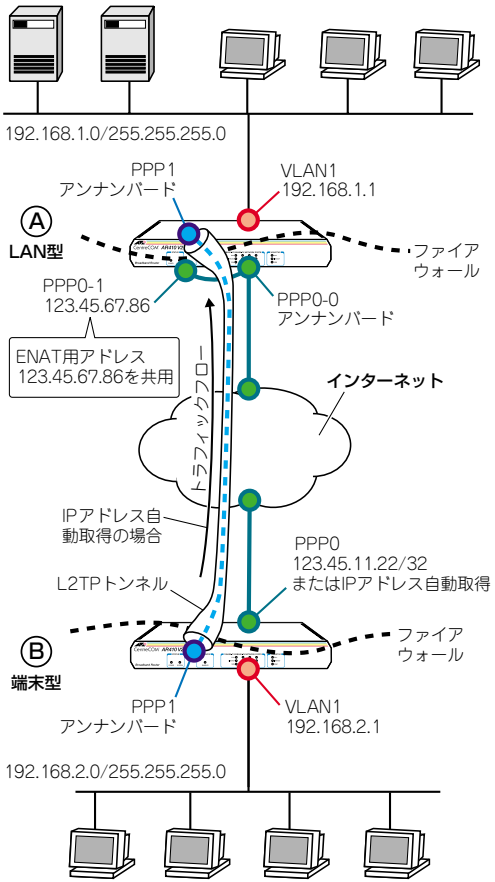


図5.7.1 L2TP による接続

L2TP（Layer 2 Tunneling Protocol）を使い、インターネット経由でプライベート LAN 同士を接続します。LAN 間接続は、IP だけでなく IPX、AppleTalk のルーティングや、ブリッジングも可能です。

本設定は、前述の 5 例の任意の組み合わせに対して適用が可能です。同じ例同士の組み合わせも可能ですが、端末型で IP アドレスが自動取得のもの同士の組み合わせはできません。

WAN/LAN 側で同一の IP アドレスを使用している例を組み合わせる場合は、IP アドレスを別のものに読み替えてください。

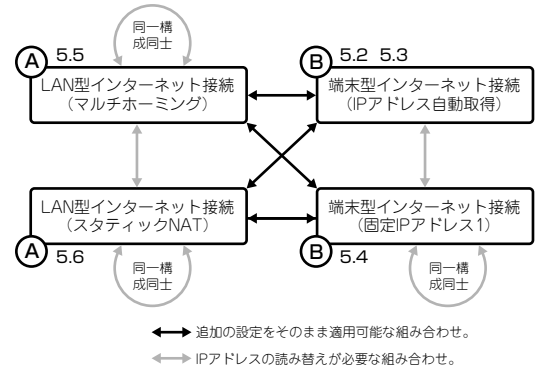


図5.7.2 接続の組み合わせ

設定の方針

- 各サイトは、あらかじめインターネットへの接続が確認できているものとします。ここでは、端末型（固定または不定のグローバルアドレス）とLAN 型（スタティックNAT）の組み合わせを使用すると仮定します（図5.7.2）。

- サイトB が IP アドレス自動取得の場合、グローバルアドレスが不定なので、常にサイトB から A に発呼します。
そのため、B のクライアントが A のサーバーを参照するような運用形態になります。

- L2TP トンネルは、A の PPP0-1 に割り当てたグローバルアドレス（123.45.67.86）と B のグローバルアドレス（123.45.11.22 または不定）の間に張られます。トンネル上に張った仮想 PPP コネクション（ppp1 ー ppp1）はプライベートLAN 間を接続するためのもので、IP のパケットを通します。

表5.7.1 L2TP・IPの設定

	A（LAN 型）	B（端末型）
L2TP コール名	remote	remote
L2TP 終端アドレス	123.45.67.86	123.45.11.22 B がアドレス自動取得の場合は不定
L2TP 発着優先	着呼優先 B がアドレス自動取得の場合は着信専用	発呼優先
L2TP サーバーモード	BOTH （LAC/LNS 兼用）	BOTH （LAC/LNS 兼用）
L2TP サーバーパスワード	L2tpA	L2tpB B がアドレス自動取得の場合は不要
WAN 側 IP アドレス（ppp1）	アンナンバード	アンナンバード

- L2TP とファイアウォールを併用する場合、L2TP パケット（始点・終点 UDP ポート 1701）が、ファイアウォールで遮断されないようにルールを設定します。

- L2TP はトンネリングの機能を提供するだけであり、セキュリティーは持っていません（盗聴が可能です）。セキュリティーが必要な場合は、IPsec などと併用してください。

設定

1 管理のしやすさのために、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>
```

サイト B には「B」を設定します。

```
Manager > SET SYSTEM NAME=B ↵

Info (1034003): Operation successful.

Manager B>
```

●L2TP の設定

2 サイト A の L2TP モジュールを有効にします。

```
Manager A> ENABLE L2TP ↵
```

サイト B でも同じコマンドを入力します。

3 サイト A の L2TP サーバーの動作モードを BOTH にします（SERVER=BOTH を設定するためには、コマンドを分ける必要があります）。

```
Manager A> ENABLE L2TP SERVER=BOTH ↵
```

サイト B でも同じコマンドを入力します。

4 相手の L2TP サーバーから接続要求を受けた際の認証用パスワードを設定します。

サイト A では次のように入力します。

```
Manager A> SET L2TP PASSWORD=L2tpA ↵
```

サイト B では次のように入力します。ただし、B がアドレス自動取得の場合、B は接続要求を受けることがないため（発呼専用）、このコマンドは入力しません。

```
Manager B> SET L2TP PASSWORD=L2tpB ↵
```

（B がアドレス自動取得の場合は不要）

5 サイト A、B 間に張られる呼（コール）を作成し、呼を張るための情報を設定します。
L2TP コール名は「remote」とします。
IP には相手側の本製品の IP アドレスを指定します。
TYPE は呼の種類を示すもので、LAN 間接続の場合は VIRTUAL を指定します。
REMOTE には、この L2TP コールに応じて相手側が起動する L2TP コール名を指定します。
PRECEDENCE は L2TP の通信が同時に開始されたとき、発呼・着呼のどちらを優先するかを指定します[*7]。
PASSWORD には、接続先で認証を受けるためのパスワードを指定します。

サイト A では次のように入力します。

```
Manager A> ADD L2TP CALL=remote
    IP=123.45.11.22 TYPE=VIRTUAL REMOTE=remote
    PRECEDENCE=IN PASSWORD=L2tpB ↵
```

ただし、サイト B がアドレス自動取得の場合、サイト A は次のように入力します。サイト A からは B に接続しにいかないため IP アドレスは「0.0.0.0」を設定しておきます。また、パスワードも不要です。

```
Manager A> ADD L2TP CALL=remote IP=0.0.0.0
    TYPE=VIRTUAL REMOTE=remote PRECEDENCE=IN ↵
```

（B がアドレス自動取得の場合）

サイト B では次のように入力します。

```
Manager B> ADD L2TP CALL=remote
    IP=123.45.67.86 TYPE=VIRTUAL REMOTE=remote
    PRECEDENCE=OUT PASSWORD=L2tpA ↵
```

*7 両サイトのグローバルアドレスが固定の場合、接続要求に応じてお互いに接続し合うため、発呼が同時に発生することがあります。一方を発呼優先にした場合、もう一方は着呼優先にします。

● PPP の設定

6 L2TP コールを仮想的な物理回線と見なし、その上に PPP インターフェースを作成します。OVER パラメーターに L2TP コールを指定するときは、コール名の前に「TNL-」を付けます。また、ここでは「IDLE=ON」を指定して、必要なときだけ接続するよう設定します。ISDN のための機能である BAP は OFF にします。

サイト A では次のように入力します。

```
Manager A> CREATE PPP=1 OVER=TNL-remote
    IDLE=ON BAP=OFF LQR=OFF ↵

Info (1003003): Operation successful.
```

サイト B でも同じコマンドを入力します。

7 L2TP 仮想回線上の PPP インターフェース 1 をアンナンバードに設定します。このインターフェースは、両拠点のプライベート LAN 同士を接続する仮想インターフェースです。

サイト A では次のように入力します（マルチホーミングされた環境では、int=ppp1 は int=ppp1-0 に展開されます）。

```
Manager A> ADD IP INT=ppp1 IP=0.0.0.0 ↵

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

サイト B でも同じコマンドを入力します。

● IP ルーティングの設定

8 経路情報を設定します。

サイト A では次のように入力します。サイト B の LAN 側（192.168.2.0/24）宛のパケットは、L2TP 上の PPP インターフェース 1 を通じて送り出します。

```
Manager A> ADD IP ROUTE=192.168.2.0
    MASK=255.255.255.0 INT=ppp1 NEXT=0.0.0.0 ↵

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

サイト B では次のように入力します。サイト A の LAN 側（192.168.1.0/24）宛のパケットは、L2TP 上の PPP インターフェース 1 を通じて送り出します。

```
Manager B> ADD IP ROUTE=192.168.1.0
    MASK=255.255.255.0 INT=ppp1 NEXT=0.0.0.0 ↵
```

●ファイアウォールの設定

9 L2TP トンネル上の PPP インターフェース（ppp1）を PRIVATE（内部）に設定します。

サイト A では次のように入力します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

サイト B でも同じコマンドを入力します。

10 接続相手からの L2TP パケット（UDP1701番）がファイアウォールを通過できるように設定します。

サイト A では次のように入力します。INT=ppp0-1 を指定すること、また RULE 番号は、すでに使用されている番号と重複しないよう注意してください。ここでは 5 としています。

```
Manager A> ADD FIREWALL POLICY=net RU=5
    AC=ALLOW INT=ppp0-1 PROT=UDP GBLPO=1701
    GBLIP=123.45.67.86 PO=1701
    IP=123.45.67.86 ↵

Info (1077003): Operation successful.
```

サイト B では次のように入力します。RULE 番号は、すでに使用されている番号と重複しないよう注意してください。ここでは 2 としています。
ただし、B がアドレス自動取得の場合、このコマンドは入力しません。L2TP の通信は常に B を起点として開始されるため、A から B に向かうトラフィックフローが存在しないからです。

```
Manager B> ADD FIREWALL POLICY=net RU=2
    AC=ALLOW INT=ppp0 PROT=UDP GBLPO=1701
    GBLIP=123.45.11.22 PO=1701
    IP=123.45.11.22 ↵
```

（B がアドレス自動取得の場合は不要）

●接続の確認

11 L2TP 上の PPP 接続の確立は、「SHOW PPP」コマンドで確認できます。

```
Manager A> SHOW PPP=1 ↵

  Name          Enabled  ifIndex  Over              CP          State
  ------------------------------------------------------------------------
  ppp1          YES      05                         IPCP        OPENED
                                  TNL-remote        LCP         OPENED
  ------------------------------------------------------------------------
```

12 LAN 側のコンピューターから、相手サイト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。[*8]

●設定の保存

13 WAN 側インターフェースの UTP ケーブルを抜き、PPP0 の接続が切断（CLOSED）されるまで待ちます。

```
Manager A> SHOW PPP=0 ↵

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

Manager A> 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
```

参照 本書「設定の保存はリンクダウンの状態で」（p.61）

14 サイトA、Bとも設定を保存します。

```
Manager A> CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

15 UTP ケーブルを接続し、PPP0 の接続が確立（OPENED）したことを確認してください。

```
Manager A> SHOW PPP ↵

  Name           Enabled  ifIndex  Over                CP          State
  ------------------------------------------------------------------------
  ppp0             YES      04                        IPCP        OPENED
                                    eth0-any           LCP         OPENED
  ppp1             YES      05                        IPCP        OPENED
                                    TNL-remote         LCP         OPENED
  ------------------------------------------------------------------------
```

*8 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

LAN 間をブリッジング

サイト A、B 間の NetBEUI もブリッジングする場合、サイト A、B とも下記のコマンドを追加実行してください。プライベート IP のルーティングをせずに、ブリッジングだけを行う場合、サイト A、B とも手順7～8（p.78）の代わりに、以下のコマンドを入力します。

1 ブリッジモジュールを有効にします。

```
Manager A> ENABLE BRIDGE ↵

Info (1027052): The Bridge module has been enabled.
```

2 ブリッジするプロトコルを指定します（指定しない場合、なにもブリッジされません）。ここでは NetBEUI を指定します。

```
Manager A> ADD BRIDGE PROTOCOL TYPE=netbeui ↵
```

参照 コマンドリファレンス「ADD BRIDGE PROTOCOL」（ブリッジング対象のプロトコルのリスト）

3 LAN 側（vlan1）インターフェースにブリッジポートを作成します。

```
Manager A> ADD BRIDGE PORT=1 INT=vlan1 ↵
```

4 WAN 側（ppp1）インターフェースにブリッジポートを作成します。ppp1 は、L2TP トンネル上に作成した仮想的な PPP インターフェースです。

```
Manager A> ADD BRIDGE PORT=2 INT=ppp1 ↵
```

AppleTalk ネットワークを接続

サイトA、B 間のAppleTalk もルーティングする場合、サイト A、B とも下記のコマンドを追加実行してください。プライベートIPのルーティングをせずに、AppleTalk ルーティングだけを行う場合、サイトA,Bとも手順7～8（p.78）の代わりに,以下のコマンドを入力します。

1 AppleTalk モジュールを有効にします（A、B 同じ）。

```
Manager A> ENABLE APPLETALK ↵

Info (1004003): Operation successful.
```

2 LAN 側（vlan1）インターフェースに AppleTalk ポートを作成します。A は次のように入力します。「SEED=10」はシードルーターとして機能させるためのパラメーターです。ここでは LAN

側のAppleTalk ネットワーク番号を 10 と仮定しています。

```
Manager A> ADD APPLETALK PORT INT=vlan1
    SEED=10 ↵

Info (1004003): Operation successful.
```

B は次のように入力します。LAN 側の AppleTalk ネットワーク番号を20 と仮定しています。

```
Manager B> ADD APPLETALK PORT INT=vlan1
    SEED=20 ↵
```

3 LAN 側ネットワークのデフォルトゾーン名を設定します（ゾーン名はセレクタに表示されます）。A は次のように入力します。ここではNetA という名前にしています。

```
Manager A> ADD APPLETALK ZONE=NetA PORT=1
    DEFAULT ↵

Info (1004003): Operation successful.
```

Bは次のように入力します。ここでは NetB という名前にしています。

```
Manager B> ADD APPLETALK ZONE=NetB PORT=1
    DEFAULT ↵
```

4 WAN側（PPP1）インターフェースに AppleTalk ポートを作成します（A、B 同じ）。「DEMAND=ON」はルーティング情報（RTMP）の交換を行わないようにするための指定です。PPP1 は、L2TP トンネル上に作成した仮想的な PPP インターフェースです。

```
Manager A> ADD APPLETALK PORT INT=PPP1
    DEMAND=ON ↵

Info (1004003): Operation successful.
```

5 スタティックルートを設定します。この例ではRTMP を使っていないため必須です。Aは次のように入力します。

```
Manager A> ADD APPLETALK ROUTE=20 PORT=2
    HOPS=2 ↵

Info (1004003): Operation successful.
```

Bは次のように入力します。

```
Manager B> ADD APPLETALK ROUTE=10 PORT=2
    HOPS=2 ↵
```

5.8 L2TP + IPsec による LAN 間接続

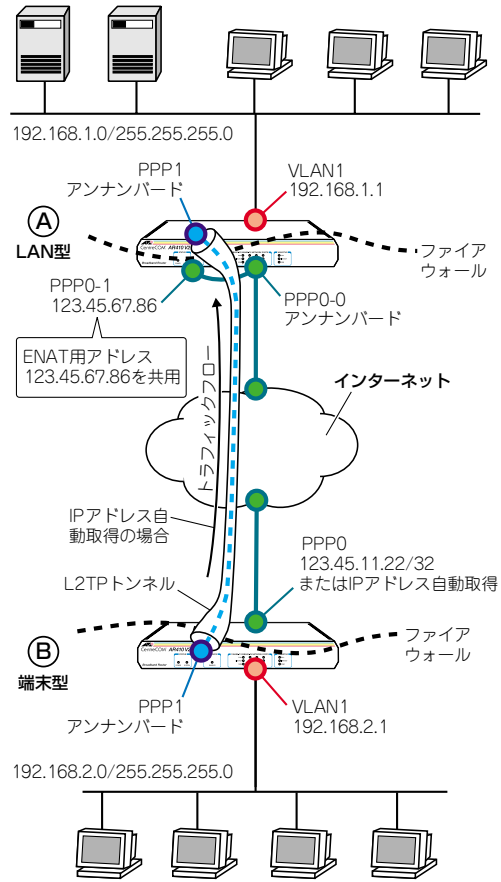


図5.8.1 L2TP による接続

L2TP（Layer 2 Tunneling Protocol）を使って、インターネット経由でプライベート LAN 同士を接続します。さらに、L2TP トンネルをトランスポートモード IPsec[*9]（ESP）で暗号化し、インターネット上を通るデータの安全性を確保します。

本設定は、前述の 5 例の任意の組み合わせに対して適用が可能です。同じ例同士の組み合わせも可能ですが、端末型で IP アドレスが自動取得のもの同士の組み合わせはできません。

WAN/LAN 側で同一の IP アドレスを使用している例を組み合わせる場合は、IP アドレスを別のものに読み替えてください。

*9 別売の暗号カード AR010、または暗号圧縮カード AR011 が必要です。

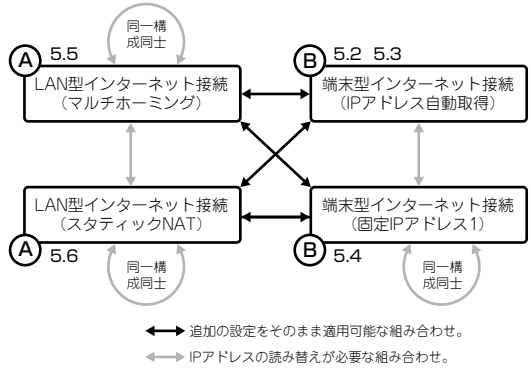


図5.8.2 接続の組み合わせ

設定の方針

- 各サイトは、あらかじめインターネットへの接続が確認できているものとします。ここでは、端末型（固定または不定のグローバルアドレス）とLAN型（スタティックNAT）の組み合わせを使用すると仮定します（図5.8.2）。

- サイトBがIPアドレス自動取得の場合、グローバルアドレスが不定なので、常にサイトBからAに発呼します。そのため、Bのクライアントが Aのサーバーを参照するような運用形態になります。

- L2TPトンネルは、Aの PPP0-1 に割り当てたグローバルアドレス（123.45.67.86）とBのグローバルアドレス（123.45.11.22または不定）の間に張られます。トンネル上に張った仮想 PPPコネクション（ppp1 ー ppp1）はプライベートLAN 間を接続するためのもので、IPのパケットを通します。

表5.8.1 L2TP・IPの設定

	A（LAN型）	B（端末型）
L2TP コール名	remote	remote
L2TP 終端アドレス	123.45.67.86	123.45.11.22 Bがアドレス自動取得の場合は不定
L2TP 発着優先	着呼優先 Bがアドレス自動取得の場合は着信専用	発呼優先
L2TP サーバーモード	BOTH （LAC/LNS 兼用）	BOTH （LAC/LNS兼用）
L2TP サーバーパスワード	なし（不要）	なし（不要）
WAN側IPアドレス（ppp1）	アンナンバード	アンナンバード

表5.8.2 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 サイトBがアドレス自動取得の場合は Aggressive モード
AのID（Bがアドレス自動取得の場合のみ必要）	IPアドレス：123.45.67.86 （デフォルト）
BのID（Bがアドレス自動取得の場合のみ必要）	名前：routerb
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5.8.3 IKEフェーズ2（IPsec SAのネゴシエーション）

SA モード	トランスポートモード
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	123.45.67.86:1701/udp ⇔ 123.45.11.22:1701/udp サイトBがアドレス自動取得の場合は 123.45.67.86:1701/udp ⇔不定:1701/udp
インターネットとの平文通信	行なう

設定

1 管理のしやすさのために、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>
```

サイトB には「B」を設定します。

```
Manager > SET SYSTEM NAME=B ↵

Info (1034003): Operation successful.

Manager B>
```

2 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。

サイト A では次のように入力します。ここでは、ユーザー名「secoff」、パスワード「gokuhi_A」を仮定します。

```
Manager A> ADD USER=secoff PASSWORD=gokuhi_A
    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
-------------------------------------------------------------------------------
```

サイト B では次のように入力します。ここでは、ユーザー名はAと同じ「secoff」、パスワード「gokuhi_B」を仮定します。

```
Manager B> ADD USER=secoff PASSWORD=gokuhi_B
    PRIVILEGE=SECURITYOFFICER ↵
```

● L2TP の設定

3 サイトA の L2TP モジュールを有効にします。

```
Manager A> ENABLE L2TP ↵
```

サイトB でも同じコマンドを入力します。

4 サイト A の L2TP サーバーの動作モードを BOTH にします（SERVER=BOTH を設定するためには、コマンドを分ける必要があります）。

```
Manager A> ENABLE L2TP SERVER=BOTH ↵
```

サイトB でも同じコマンドを入力します。

5 サイトA、B 間に張られる呼（コール）を作成し、呼を張るための情報を設定します。
L2TP コール名は「remote」とします。
IP には相手側の本製品の IP アドレスを指定します。
TYPE は呼の種類を示すもので、LAN 間接続の場合は VIRTUAL を指定します。
REMOTE には、この L2TP コールに応じて相手側が起動する L2TP コール名を指定します。
PRECEDENCE は L2TP の通信が同時に開始されたとき、発呼・着呼のどちらを優先するかを指定します[*10]。

サイトA では次のように入力します。

```
Manager A> ADD L2TP CALL=remote
    IP=123.45.11.22 TYPE=VIRTUAL REMOTE=remote
    PRECEDENCE=IN ↵
```

ただし、サイト B が IP アドレス自動取得の場合、サイト A は次のように入力します。サイト A からはB に接続しに行かないため、IP アドレスは「0.0.0.0」を設定しておきます。

```
Manager A> ADD L2TP CALL=remote IP=0.0.0.0
    TYPE=VIRTUAL REMOTE=remote PRECEDENCE=IN ↵
```

（B がアドレス自動取得の場合）

サイトB では次のように入力します。

```
Manager B> ADD L2TP CALL=remote
    IP=123.45.67.86 TYPE=VIRTUAL REMOTE=remote
    PRECEDENCE=OUT ↵
```

● PPP の設定

6 L2TP コールを仮想的な物理回線と見なし、その上に PPP インターフェースを作成します。OVER パラメーターに L2TP コールを指定するときは、コール名の前に「TNL-」を付けます。また、ここでは「IDLE=ON」を指定して、必要なときだけ接続するよう設定します。ISDN のための機能である BAP は OFF にします。

サイトA では次のように入力します。

```
Manager A> CREATE PPP=1 OVER=TNL-remote
    IDLE=ON BAP=OFF LQR=OFF ↵

Info (1003003): Operation successful.
```

*10 接続要求に応じてお互いに発呼し合うため、発呼が同時に発生し、競合することがあります。一方を発呼優先にした場合、もう一方は着呼優先にします。

サイトB でも同じコマンドを入力します。

7 L2TP 仮想回線上の PPP インターフェース 1 をアンナンバードに設定します。このインターフェースは、両拠点のプライベート LAN 同士を接続する仮想インターフェースです。

サイト A では次のように入力します（マルチホーミングされた環境では、int=ppp1 は int=ppp1-0 に展開されます）。

```
Manager A> ADD IP INT=ppp1 IP=0.0.0.0 ↵

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

サイトB でも同じコマンドを入力します。

●IP ルーティングの設定

8 経路情報を設定します。

サイト A では次のように入力します。サイト B の LAN 側（192.168.2.0/24）宛のパケットは、L2TP 上の PPP インターフェース 1 を通じて送り出します。

```
Manager A> ADD IP ROUTE=192.168.2.0
    MASK=255.255.255.0 INT=ppp1 NEXT=0.0.0.0 ↵

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

サイト B では次のように入力します。サイト A の LAN 側（192.168.1.0/24）宛のパケットは、L2TP 上の PPP インターフェース 1 を通じて送り出します。

```
Manager B> ADD IP ROUTE=192.168.1.0
    MASK=255.255.255.0 INT=ppp1 NEXT=0.0.0.0 ↵
```

●ファイアウォールの設定

9 L2TP トンネル上の PPP インターフェース（ppp1）を PRIVATE（内部）に設定します。

サイトA では次のように入力します。

```
Manager A> ADD FIREWALL POLICY=net INT=ppp1
    TYPE=PRIVATE ↵

Info (1077003): Operation successful.
```

サイトB でも同じコマンドを入力します。

10 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。

サイト A では次のように入力します。INT=ppp0-1 を指定すること、また RULE 番号は、すでに使用されている番号と重複しないよう注意してください。ここでは 5 としています。

```
Manager A> ADD FIREWALL POLICY=net RU=5
    AC=ALLOW INT=ppp0-1 PROT=UDP GBLPO=500
    GBLIP=123.45.67.86 PO=500
    IP=123.45.67.86 ↵

Info (1077003): Operation successful.
```

サイト B では次のように入力します。RULE 番号は、すでに使用されている番号と重複しないよう注意してください。ここでは 2 としています。
ただし、B がアドレス自動取得の場合、このコマンドは入力しません。L2TP の通信は常に B を起点として開始されるため、A から B に向かうトラフィックフローが存在しないからです。

```
Manager B> ADD FIREWALL POLICY=net RU=2
    AC=ALLOW INT=ppp0 PROT=UDP GBLPO=500
    GBLIP=123.45.11.22 PO=500
    IP=123.45.11.22 ↵
```

（B がアドレス自動取得の場合は不要）

11 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。

サイト A では次のように入力します（マルチホーミングされた環境では、int=vlan1 はint=vlan1-0 に展開されます）。

```
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.
```

サイト B では次のように入力します。

```
Manager B> ADD FIREWALL POLICY=net RU=3
    AC=NONAT INT=vlan1 PROT=ALL
    IP=192.168.2.1-192.168.2.254 ↵

Manager B> SET FIREWALL POLICY=net RU=3
    REMOTEIP=192.168.1.1-192.168.1.254 ↵
```

12 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。

サイト A では次のように入力します。「ENCAP=IPSEC」は、IPsec パケットからオリジナルのパケット（L2TP 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がUDPで終点IPアドレスが123.45.67.86、終点ポートが1701番ならば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=UDP PORT=1701
    IP=123.45.67.86 ENCAP=IPSEC ↵

Info (1077003): Operation successful.
```

サイトBでは次のように入力します。次のコマンドは、「取り出したパケットがUDPで終点IPアドレスが123.45.11.22、終点ポートが1701番ならばNATの対象外とする」の意味になります。

```
Manager B> ADD FIREWALL POLICY=net RU=4
    AC=NONAT INT=ppp0 PROT=UDP PORT=1701
    IP=123.45.11.22 ENCAP=IPSEC ↵
```

ただし、サイトBがアドレス自動取得の場合、IPアドレスが決まらないので、Bは次のように入力します。

```
Manager B> ADD FIREWALL POLICY=net RU=4
    AC=NONAT INT=ppp0 PROT=UDP PORT=1701
    ENCAP=IPSEC ↵
```

(Bがアドレス自動取得の場合)

● **IPsecの設定**

13 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。

サイトAでは次のように入力します。

```
Manager A> CREATE ENCO KEY=1 TYPE=GENERAL
    VALUE="secret" ↵

Info (1073003): Operation successful.
```

サイトBでも同じように入力します。

「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。

14 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には対向本製品のIPアドレスを指定します。

サイトAでは次のように入力します。

```
Manager A> CREATE ISAKMP POLICY="i"
    PEER=123.45.11.22 KEY=1 SENDN=TRUE ↵

Info (1082003): Operation successful.
```

ただし、サイトBがアドレス自動取得の場合、サイトAは次のように入力します。相手のIPアドレスが不定なので、PEERはANYを指定し、REMOTEIDで相手のIDを指定します。また、Aggressiveモードを使うよう設定します。

```
Manager A> CREATE ISAKMP POLICY="i" PEER=ANY
    KEY=1 SENDN=TRUE MODE=AGGRESSIVE
    REMOTEID="routerb" ↵
```

(Bがアドレス自動取得の場合)

サイトBでは次のように入力します。

```
Manager B> CREATE ISAKMP POLICY="i"
    PEER=123.45.67.86 KEY=1 SENDN=TRUE ↵
```

ただし、サイトBがアドレス自動取得の場合、サイトBは次のように入力します。自分のIPアドレスが不定なので、LOCALIDで自分のIDを指定します。また、Aggressiveモードを使うよう指定します。

```
Manager B> CREATE ISAKMP POLICY="i"
    PEER=123.45.67.86 KEY=1 SENDN=TRUE
    MODE=AGGRESSIVE LOCALID="routerb" ↵
```

(Bがアドレス自動取得の場合)

15 IPsec通信の仕様を定義するSAスペック1を作成します。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。この例ではすでにL2TPのトンネルが存在するため、デフォルトのトンネルモードは使用せずに、トランスポートモードを使用します。相手のUDP1701番ポート宛てに送受信されるL2TPパケットだけを暗号化する形になります。サイトAでは次のように入力します。

```
Manager A> CREATE IPSEC SASPEC=1 KEYMAN=ISAKMP
    PROTOCOL=ESP ENCALG=DES HASHALG=SHA
    MODE=TRANSPORT ↵

Info (1081003): Operation successful.
```

サイトBでも同じように入力します。

16 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。

サイトA では次のように入力します。

```
Manager A> CREATE IPSEC BUNDLE=1 KEYMAN=ISAKMP
    STRING="1" ↵

Info (1081003): Operation successful.
```

サイトB でも同じように入力します。

17 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。

サイトA では次のように入力します。

```
Manager A> CREATE IPSEC POLICY="isa"
    INT=ppp0-1 ACTION=PERMIT LPORT=500
    RPORT=500 TRANSPORT=UDP ↵

Info (1081003): Operation successful.
```

サイトB では次のように入力します。

```
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パラメーターを使用します。

18 L2TP パケットを暗号化する IPsecポリシー「L2」をPPP インターフェース0 に対して作成します。鍵管理方式には「ISAKMP」を、PEER には相手の IP アドレスを、BUNDLE には前の手順で作成した SA バンドルスペック 1 を指定します。また、LAD、LPORT、RAD、LPORT で対象となるパケットの条件を指定します。

サイト A では次のように入力します。

```
Manager A> CREATE IPSEC POLICY="L2" INT=ppp0-1
    ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=123.45.11.22 ↵

Info (1081003): Operation successful.

Manager A> SET IPSEC POLICY="L2"
    LAD=123.45.67.86 LPORT=1701
    RAD=123.45.11.22 RPORT=1701
    TRANSPORT=UDP ↵

Info (1081003): Operation successful.
```

ただし、サイト B がアドレス自動取得の場合、サイト A は次のように入力します。B の IP アドレスが不定なため、PEER には ISAKMP の認証をパスした相手という意味の「DYNAMIC」を指定します。RNAME は相手のアドレスが不定なため RAD の代わりに名前を指定するものです。

```
Manager A> CREATE IPSEC POLICY="L2" INT=ppp0-1
    ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=DYNAMIC ↵

Manager A> SET IPSEC POLICY="L2"
    LAD=123.45.67.86 LPORT=1701
    RNAME="routerb" RPORT=1701 TRANSPORT=UDP ↵
```

（B がアドレス自動取得の場合）

サイト B では次のように入力します。

```
Manager B> CREATE IPSEC POLICY="L2" INT=ppp0
    ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=123.45.67.86 ↵

Manager B> SET IPSEC POLICY="L2"
    LAD=123.45.11.22 LPORT=1701
    RAD=123.45.67.86 RPORT=1701
    TRANSPORT=UDP ↵
```

ただし、サイト B がアドレス自動取得の場合、サイト B は次のように入力します。1 行目のコマンドは、アドレス固定の場合と同じです。2 行目のコマンドで、自分の IP アドレスが不定なので、LAD の代わりに LNAME パラメーターで名前を指定しています。

```
Manager B> CREATE IPSEC POLICY="L2" INT=ppp0
    ACTION=IPSEC KEYMAN=ISAKMP BUNDLE=1
    PEER=123.45.67.86 ↵

Manager B> SET IPSEC POLICY="L2"
    LNAME="routerb" LPORT=1701
    RAD=123.45.67.86 RPORT=1701
    TRANSPORT=UDP ↵
```

（B がアドレス自動取得の場合）

19 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。

サイトA では次のように入力します。

```
Manager A> CREATE IPSEC POLICY="inet"
    INT=ppp0-1 ACTION=PERMIT ↵

Info (1081003): Operation successful.
```

サイトB では次のように入力します。

```
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。

20 IPsecモジュールを有効にします。

サイトA では次のように入力します。

```
Manager A> ENABLE IPSEC ↵

Info (1081003): Operation successful.
```

サイトB でも同じように入力します。

21 ISAKMP モジュールを有効にします。

サイトA では次のように入力します。

```
Manager A> ENABLE ISAKMP ↵

Info (1082057): ISAKMP has been enabled.
```

サイトB でも同じように入力します。

22 Security Officerレベルのユーザーでログインしなおします。

サイトA では次のように入力します。

```
Manager A> LOGIN secoff ↵

Password: gokuhi_A
```

サイトB でも同じように入力します。

23 動作モードをセキュリティーモードに切り替えます。

サイトA では次のように入力します。

```
SecOff A> ENABLE SYSTEM SECURITY_MODE ↵

Info (1034003): Operation successful.
```

サイトB でも同じように入力します。

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。

参照 本書「6.4 ノーマルモード / セキュリティーモード」（p.92）

本書「設定の保存はリンクダウンの状態で」（p.61）

●接続の確認

24 L2TP 上の PPP 接続の確立は、「SHOW PPP」コマンドで確認できます。

```
SecOff A> SHOW PPP=1 ↵

 Name          Enabled  ifIndex  Over              CP          State
 ------------------------------------------------------------------------
 ppp1           YES      05                       IPCP        OPENED
                                  TNL-remote       LCP         OPENED
 ------------------------------------------------------------------------
```

25 LAN 側のコンピューターから、相手サイト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。[*11]

*11 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

●設定の保存

26 WAN 側インターフェースの UTP ケーブルを抜き、PPP0 の接続が切断（CLOSED）されるまで待ちます。

```
SecOff A> SHOW PPP=0 ↵

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

Manager A> 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
```

参照 本書「設定の保存はリンクダウンの状態で」（p.61）

27 サイトA、Bとも設定を保存します。

```
SecOff A> CREATE CONFIG=ROUTER.CFG ↵

Info (1049003): Operation successful.
```

28 UTP ケーブルを接続し、PPP0 の接続が確立（OPENED）したことを確認してください。

```
SecOff A> SHOW PPP ↵

  Name           Enabled  ifIndex  Over                CP          State
  ------------------------------------------------------------------------
  ppp0             YES      04                        IPCP        OPENED
                                    eth0-any           LCP         OPENED
  ppp1             YES      05                        IPCP        OPENED
                                    TNL-remote         LCP         OPENED
  ------------------------------------------------------------------------
```

L2TP+IPsec の場合も、L2TP の下記がそのまま適用可能です。

参照 本書「LAN 間をブリッジング」（p.79）
本書「AppleTalk ネットワークを接続」（p.79）

5.9 他の構成例

端末型や LAN 型によるインターネットへの接続、L2TP によるインターネットを経由した LAN 間接続、L2TP 接続にセキュリティーを付加する方法、と順を追って説明してまいりましたが、本製品にはまだまだ多くの機能や使用方法があります。

紙面が限られているためご紹介しきれなかった数多くの構成例が、回線や機能ごとに分類され、下記の設定例集（CD-ROM）に収録されておりますので、ぜひご覧ください。

参照「設定例集」

また、機能に関する一般的かつ完全な説明、機能を利用するためのコマンドやパラメーターの詳細は、コマンドリファレンス（CD-ROM）をご覧ください。

参照「コマンドリファレンス」

6.1 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6.1.1：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	• ユーザー自身に関する端末設定、パスワードのような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	• すべてのコマンドを実行可能	• 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	• すべてのコマンドを実行可能 • Manager と同じユーザーレベル	• 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。

参照 本書「6.4 ノーマル モード / セキュリティー モード」（p.92）

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。

参照 本書「4.1 コマンドプロセッサー」（p.35）

6.2 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ー」（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6.2.1 ユーザー認証データベース

ユーザー名	USER • 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 • 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 • 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 • 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 • 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 • 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。

参照 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。

参照 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」

6.3 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、セキュリティーモードでは 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
-------------------------------------------------------------------------------
```

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。

```
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    (SECURDELAY)
  minimum password length ...................    6 characters (MINPWDLEN)
  TACACS retries ............................    3            (TACRETRIES)
  TACACS timeout period .....................    5 seconds    (TACTIMEOUT)
  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オートでくくる必要はありません）。

```
 login: osaka-shisya ↵
Password:

> SET PASSWORD ↵

OLD passsowd: _________  （表示されません）
New password: _________  （表示されません）
Confirm: _________  （表示されません）
```

参照 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」コマンドを使います。

```
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」コマンドを使います。

```
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」コマンドを使います。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
   Logins: 0          Fails: 0        Sent: 0           Rcvd: 0
---------------------------------------------------------------------------
```

6.4 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（IPsecを使用するためには、本製品に「暗号カード」が取り付けられていなければなりません）。

参照 本書「A.6 暗号 / 圧縮カードの取り付け」（p.127）

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と、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    (SECURDELAY)
  minimum password length ...................    6 characters (MINPWDLEN)
  TACACS retries ............................    3            (TACRETRIES)
  TACACS timeout period .....................    5 seconds    (TACTIMBOUT)
  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。

7 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。

参照 本書「10.2 ファイル名」(p.102)

7.1 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。

参照 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.115)

「↓」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
```

7.2 キー操作

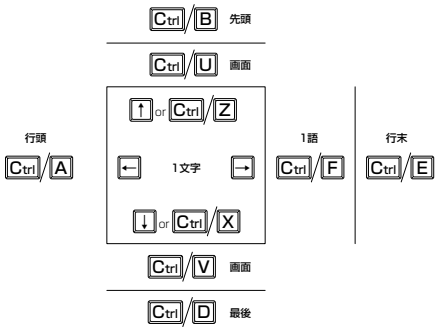


図 7.2.1 カーソル移動キー

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 7.2.1：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。

a. 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。
b. 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 7.2.2：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 7.2.3：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。

a. 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 7.2.4：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 7.2.5：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 7.2.6：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 7.2.7：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。

8 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。

8.1 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8.1.1 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 >
```

セキュリティーモードでは、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。

参照 本書「セキュリティーモードへの移行」(p.92)

8.2 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=vlan1 IP=192.168.5.1 ↵
```

図 8.2.1 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:
```

8.3 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」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 ↵
```

9.1 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。本製品に実装されている PING は、IP、IPX、AppleTalk に対応しています。

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 ↵
```

IPX における例を下記に示します。PING に続けて相手の「ネットワーク番号：ステーション番号」を入力します。

```
Manager > ping 401:00000001 ↵
```

AppleTalk における例を下記に示します。PING に続けて相手の「ネットワーク番号：ノード」を入力します。

```
Manager > ping 28:128 ↵
```

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）。

9.2 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）。

10.1 フラッシュメモリー・ファイルシステム

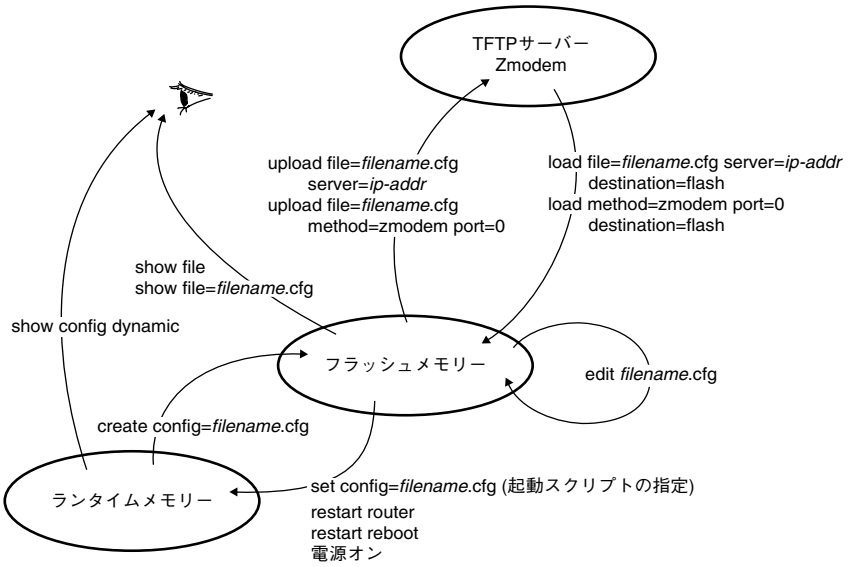


図 10.1.1 設定ファイルに関するコマンド

本製品は、不揮発性メモリーとして 8MByte のフラッシュメモリー（FLASH）を内蔵しており、ファイルシステムとして 7MByte が使用できます。フラッシュメモリーは、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、フラッシュメモリー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、フラッシュメモリー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
-------------------------------------------------------------------------
52-233.rez          flash         2394684  04-Sep-2002 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
fwnat.cfg           flash         3143     21-Apr-2002 11:20:54    0
help.hlp            flash         129254   11-Apr-2002 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、フラッシュメモリー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 ..... 6
est compaction time ... 190 seconds
files .................   4853060 bytes  (15 files)
garbage ...............        96 bytes
free ..................   2355804 bytes
required free block ...    131072 bytes
total .................   7340032 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、1～2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。

10.2 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 10.2.1 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 10.2.1 に挙げた拡張子のファイルのみが許されます。

表 10.2.1 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 10.2.2 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=*filename*.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	セキュリティー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ーモードへ移行すべきことを示すファイルです。
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。

10.3 ワイルドカード

ファイルを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。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。

11 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。

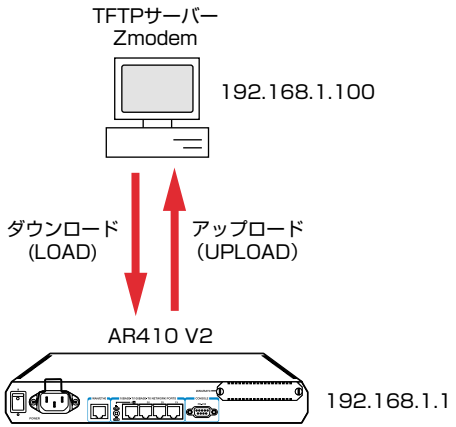


図 11.0.1 アップ / ダウンロード

11.1 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。

参照 本書「10 ファイルシステム」(p.101)

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、ファイル名の大文字・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。

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、大文字・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、大文字・小文字を区別します）。

11.2 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。

参照 本書「3.1 コンソールターミナルの設定」(p.27)
本書「10 ファイルシステム」(p.101)

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､上書きされますのでご注意ください。

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

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 ↵
```

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。

12 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、本製品へのダウンロードのしかたについて説明します。

12.1 必要なもの

本製品（AR410V2）のバージョンアップには、次のものが必要です。

- 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。弊社 Web ページからダウンロードできます。
- 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。
- バージョンアップの手順書
  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ー
  セットアップツールを実行します。

12.2 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す。

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

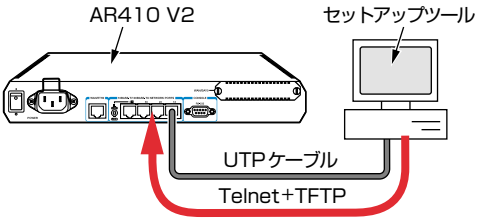


図 12.2.1 セットアップツール

12.3 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。

Web ページからソフトウェアのダウンロードを行う際に、お客様を認証するために、本製品の「**シリアル番号**」の入力を要求されます。ダウンロードを行う前に、あらかじめ本製品のシリアル番号を調べておいてください。シリアル番号は、製品底面に貼付されているバーコードシールに記入されています。

（例）S/N 000770000002346 Rev 1A

1. Microsoft Internet Explorer、Netscape Navigator などの Web ブラウザーを使用して、弊社の Web ページにアクセスします。

   ```
   http://www.allied-telesis.co.jp/
   ```

2. 「**サポート**」をクリックしてください。
3. 「**Bridge/Router**」を選択し、「**GO**」をクリックしてください。
4. 本製品の「**Download**」の項目を選択してください。
5. シリアル番号を入力し、「**GET!!**」をクリックしてください。
   （このページの「サービス内容のご案内」に「**リリースノート**」へのリンクがあります）
6. 最新ファームウェアのソフトウェアセット、またはセットアップツールをダウンロードしてください。

12.4 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「2.3.3」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、「**52-*rrr*.REL**」または「**52-*rrr*.REZ**」というファイル名で提供されます。「52-」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）

```
52-233.REZ
```

参照 本書「10 ファイルシステム」（p.101）

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、「**52*rrr-pp*.PAT**」または「**52*rrr-pp*.PAZ**」というファイル名で提供されます。「52」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「52-233.REZ」に対して、初めて提供されるパッチは下記のようになります。
（例）

```
52233-01.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）。

参照 本書「10 ファイルシステム」（p.101）

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、「***majer.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.2.3.3 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、「ar52」で始まり、「*majer.minor.interim*」「*pp*」を連結した exe 形式ファイルとなります。
（例）

```
ar522331.exe
```

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ています。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。

13.1 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、以下は行ってみ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。

参照 本書「1.3 各部の名称と働き」(p.18)

●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ー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。

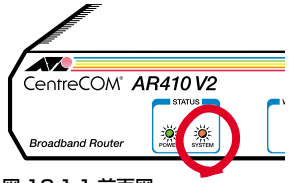


図 13.1.1 前面図

参照 本書「B.2 ユーザーサポート」(p.131)

●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）
- 該当のポートがポート 4 の場合、MDI/MDI-X 切替スイッチの設定は正しいか（接続先機器がコンピューターの場合は X PC、HUB やスイッチの場合は= HUB）
- 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 の場合はカテゴリー 5 以上、10BASE-T の場合はカテゴリー 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  STAC  STAC SW Initialised
13 16:32:24 7 SYS  REST  NORM  Router startup, ver 2.3.3-00, 27-Aug-2002, Clock
                               Log: 16:32:18 on 13-Sep-2002
13 16:32:24 6 FIRE FIRE  ENBLD 13-Sep-2002 16:32:24    Firewall enabled
13 16:32:25 3 LOG              FFSerror 20 opening file     \temp    .ins
13 16:32:25 3 LOG              FFSerror 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
13 16:38:05 3 TRG  BATCH ACT   Trigger 2 activated (Automatic)
-------------------------------------------------------------------------------
```

図 13.1.2 ログの表示例

13.2 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）

参照 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.115）

- 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）
- 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）

参照 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.115）

- 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

参照 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.115）
本書「7 テキストエディター」（p.95）

●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。

参照 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。

参照 本書「設定の保存はリンクダウンの状態で」（p.61）

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

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。

参照 本書「B.2 ユーザーサポート」（p.131）

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はファイ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。

参照 本書「12 バージョンアップ」（p.107）
本書「10.2 ファイル名」（p.102）
本書「B.2 ユーザーサポート」（p.131）

A.1 コンピューターの設定

「5 構成例」（p.51）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。

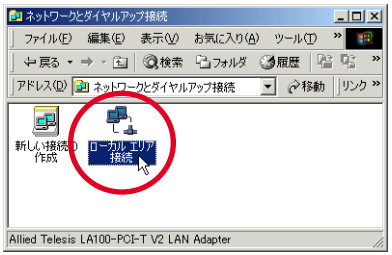


図 A.1.1 「ローカルエリア接続」アイコン

2「プロパティ」をクリックしてください。

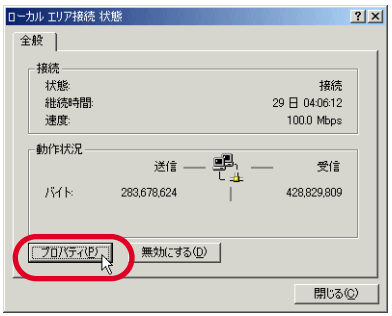


図 A.1.2 ローカルエリア接続状態

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。

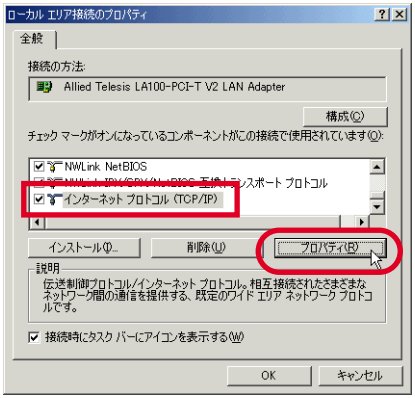


図 A.1.3 ローカルエリア接続のプロパティ

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。

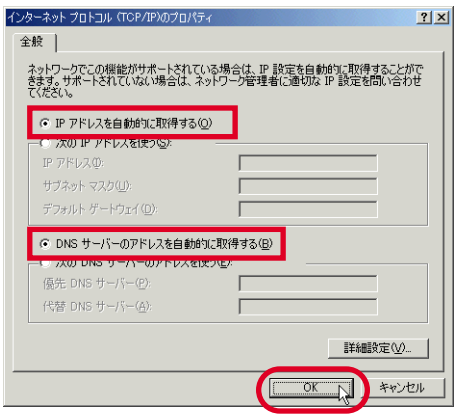


図 A.1.4 IP アドレス自動取得（DHCP クライアント）

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。

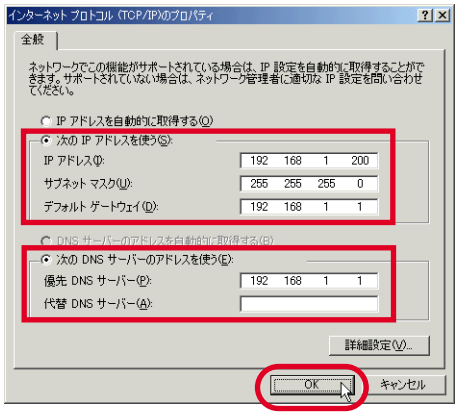


図 A.1.5 IP アドレス固定（DNS リレー）

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。

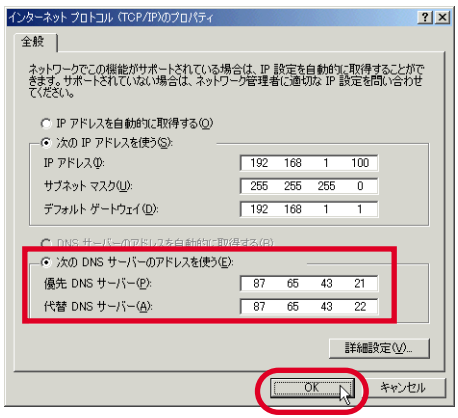


図 A.1.6 IP アドレス固定（DNS ダイレクト）

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。

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）。

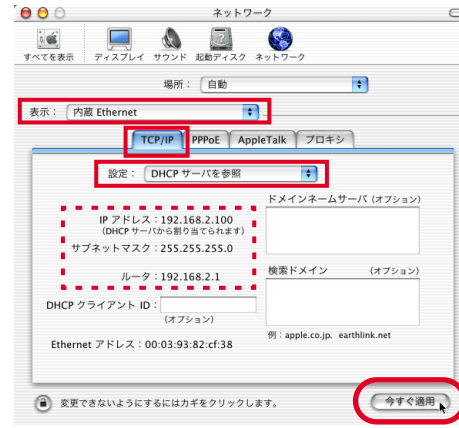
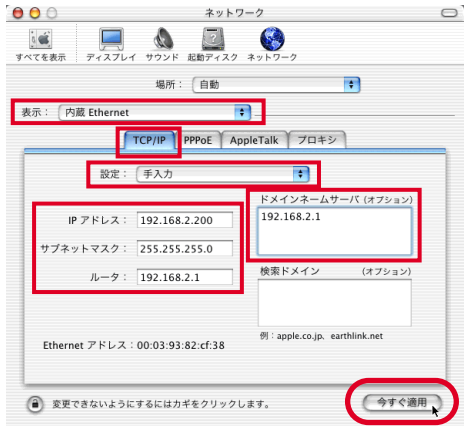


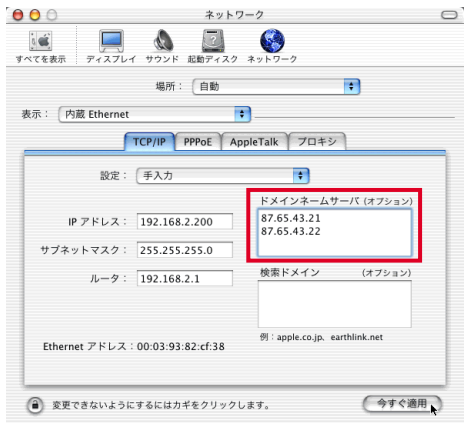
図 A.1.7 IP アドレス自動取得（DHCP クライアント）

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閉じてください。

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。

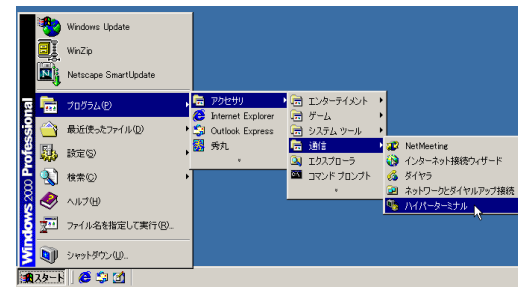


図 A.2.1 「ハイパーターミナル」フォルダ

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。

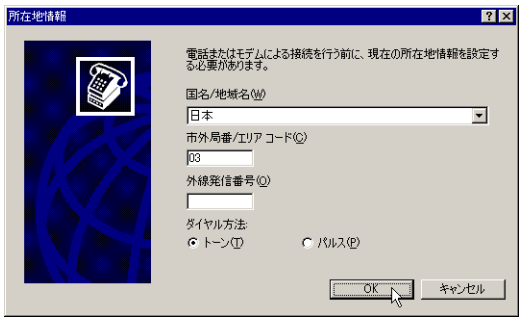


図 A.2.2 「所在地情報」の設定

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。

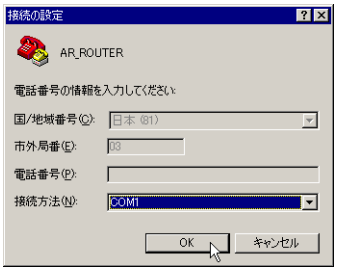


図 A.2.5 接続方法で COM1 を指定

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。

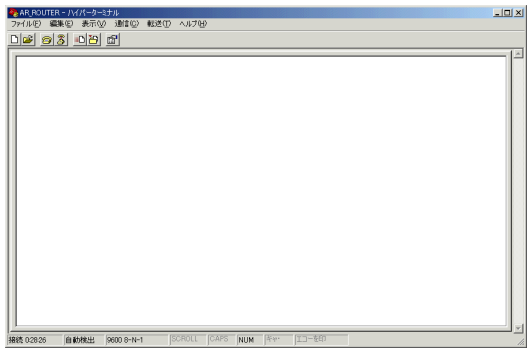


図 A.2.7 ターミナル画面

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。

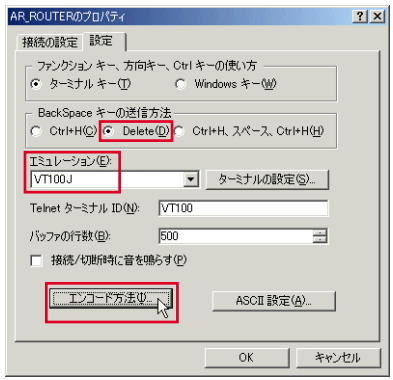


図 A.2.8 キーの設定

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。

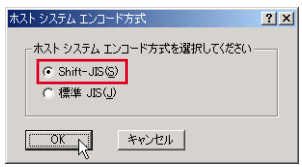


図 A.2.9 エンコード方式

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

次回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。

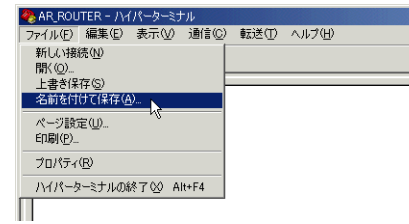


図 A.2.10 ハイパーターミナル設定の保存

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。

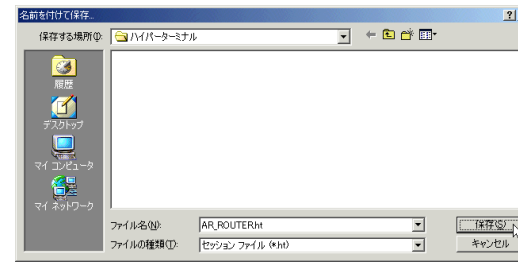


図 A.2.11 ハイパーターミナル設定ファイル名の入力

次回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。

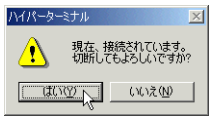


図 A.2.12 接続中の警告

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）コネクター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 4 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。

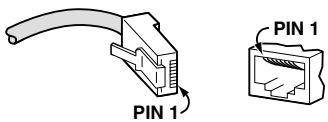


図 A.4.1 RJ-45 モジュラープラグ（左）、ジャック（右）

LAN 側ポートの 1 ～ 3 は、通常のポートです（MDI-X）。ポート 4 は「MDI/MDI-X 切替スイッチ」を装備しており、カスケードポートとして使用するのに便利です。

コンピューターをポート 4 に接続する場合、ストレートタイプの UTP ケーブルを使用し、スイッチを「X PC」に設定してください（図 A.4.2）。HUB やスイッチの通常のポート（MDI-X）をポート 4 に接続する場合、ストレートタイプの UTP ケーブルを使用し、スイッチを「= HUB」に設定してください（図 A.4.3）。

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

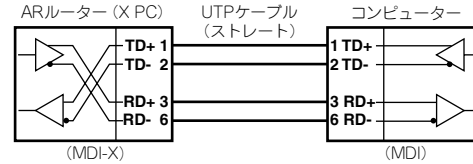


図 A.4.2 「X PC」に設定したとき

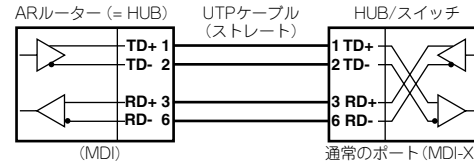


図 A.4.3 「= HUB」に設定したとき

A.5 PIC（Port Interface Card）

PIC（Port Interface Card）は、弊社 AR シリーズルーターのPIC ベイに装着して使用する拡張カードです。WAN ポートの違いにより、次の4 種類の PIC があります。

- AR020（PRI）
- AR021（BRI）
- AR022（10BASE-T、AUI）
- AR023（同期シリアル：V24、X21、V35）

PIC の取り付け

稲妻が発生しているときは、本製品（AR410V2）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。

1 電源スイッチをオフにしてください。安全のために、コンセントから電源ケーブルを抜いてください。

PIC を本製品に取り付けるときは、必ず本製品の電源スイッチをオフにし、コンセントから電源ケーブルを抜いてください。電源が供給されたまま、この作業を行うと本製品や PIC の故障の原因となります。

2 PIC ブランクパネルを取り外してください。

3 PIC が AR021（BRI）である場合は、必要に応じて基板上のジャンパーを設定してください。

PIC 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、PIC の接点、部品などに素手で触れないでください。確実のためには、リストストラップなどの静電気防止用具の着用をお勧めします。

4 PIC を本製品の PIC ベイに取り付けます。PIC ベイのレールに PIC を沿わせ、カチンとショックがあるまで押し込んでください。

5 PIC の固定ネジ（2 本）を締めてください。

6 PIC のポートにケーブルを接続してください。

7 本製品の電源スイッチをオンにし、「SHOW SYSTEM」コマンドを入力してPIC が認識されていることを確認してください。下記に、AR020 の表示例を示します。

```
Manager > SHOW SYSTEM ↵

Router System Status                              Time 17:12:54 Date 04-Sep-2002.
Board      ID  Bay Board Name                        Rev   Serial number
-------------------------------------------------------------------------------
Base      195      AR410 V2                         M1-0  57004257
PIC        75   0  AR020 PIC T1/E1 PRI              M1-1  39592696
-------------------------------------------------------------------------------
Memory -   DRAM : 16384 kB    FLASH :  7168 kB
-------------------------------------------------------------------------------
......
```

PIC の取り外し

稲妻が発生しているときは、本製品（AR410V2）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。

1 電源スイッチをオフにしてください。安全のために、コンセントから電源ケーブルを抜いてください。

PIC を本製品から取り外すときは、必ず本製品の電源スイッチをオフにし、コンセントから電源ケーブルを抜いてください。電源が供給されたまま、この作業を行うと本製品や PIC の故障の原因となります。

2 PIC のポートに接続されているケーブルを外してください。

3 PIC の固定ネジ（2 本）を締め、固定ネジを両手で持ちながら、手前に引き抜いてください。

PIC 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、PIC の接点、部品などに素手で触れないでください。確実のためには、リストストラップなどの静電気防止用具の着用をお勧めします。

4 PIC ブランクパネルを取り付けてください。

AR020（PRI）

AR020 カードは、PRI ポート（G.703/Primary Rate ISDN WAN ポート）を 1 つ持つPIC です。ISDN（23B+D）、192K ～ 1.5Mbps のデジタル専用線やフレームリレー網といったより高速なWAN回線への接続に使用します。

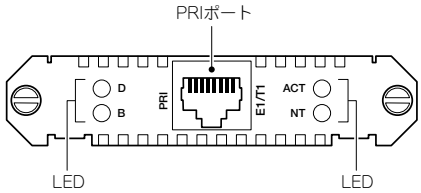


図 A.5.1 AR020 背面パネル

PRI ポート

ISDN 回線またはデジタル専用線に接続するためのポートです。コネクターはRJ-45ジャックが使用されており、結線はIS10173に準拠しています。

LED

LED	色	状態	表示の内容
D	緑	点滅	本製品と ISDN 交換機の間で、D チャネルを経由してパケットが交換されています。ISDN においてのみ意味を持ちます。
		消灯	本製品と ISDN 交換機の間で、D チャネルを経由してパケットが交換されていません。
B	緑	点滅	本製品ともう一方の接続端の機器（通常はルーター）間で、任意の B チャネルを経由してパケットが交換されています。
		消灯	本製品ともう一方の接続端の機器（通常はルーター）間で、任意の B チャネルを経由してパケットが交換されていません。
ACT	緑	点灯	レイヤ 1 のリンクが確立しています（本製品と交換機との間における通信が可能です）。
		消灯	レイヤ 1 のリンクが確立していません（本製品と交換機との間における通信ができません）。
NT	緑	点灯	PRI が ISDN NT モードで動作しています。ISDN においてのみ意味を持ちます。
		消灯	PRI が ISDN TE モード（通常の動作モード）で動作しています。ISDN においてのみ意味を持ちます。

ジャンパー

ハードウェア Rev. の違いにより、3 ジャンパー型、2 ジャンパー型の 2 種類が存在します。ジャンパーは、ISDN、デジタル専用線、フレームリレー網の如何に関わらず、日本国内では常にデフォルト設定でご使用ください（3 ジャンパー型では J3：あり、J2：あり、J1：なし。2 ジャンパー型では J2：あり、J1：なし）。

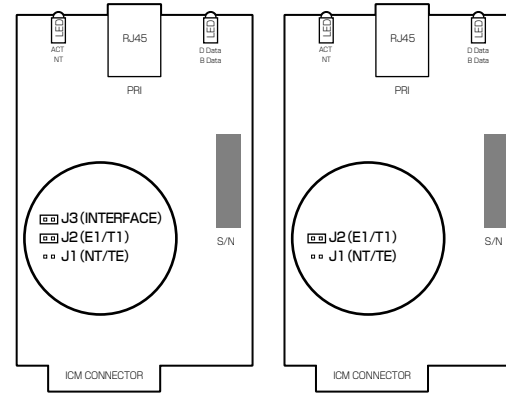


図 A.5.2 デフォルトのジャンパー設定

J1

ISDN の NT モード（本製品を交換機として網に接続）、または TE モード（本製品を端末として網に接続）を選択します。常に TE モードに設定してください（本製品は NT モードをサポートしておりません）。

J2

E1（Euro ISDN）または T1 を選択します。日本国内では T1 のみが使用可能です。

J3

E1 または T1（J2）に応じて、終端抵抗の値を選択します。日本国内では「あり」のみが可能です。2 ジャンパー型では、常に「J3：あり」となっています。

表 1.5.1 モードの設定

	あり	なし
J1	ISDN NT モード	**ISDN TE モード**
J2	**T1 モード**	E1 モード
J3	終端抵抗値を選択	

表 1.5.2 終端抵抗値の設定

J2	**あり（T1）**		なし（E1）	
J3	なし	**あり**	なし	あり
終端抵抗値	組み合わせ不可	**100Ω**	75Ω	120Ω

接続ケーブル

AR020 のコネクターは RJ-45 ジャックが使用されており、結線は IS10173 に準拠しています。また、DSU は IS10173 準拠、IS8877 準拠の 2 種類が存在します。IS10173 は PRI のための規格として最近規定されたもので、IS10173 が規定される前は、PRI においても BRI の規格である IS8877 が使用されていました。IS10173 準拠の DSU は RJ-48 ジャック（図 A.5.3）を装備し、IS8877 準拠の DSU は RJ-45 ジャック（図 A.4.1）を装備しています。IS10173 規格と IS8877 規格は、コネクター形状だけでなく結線も異なっています。

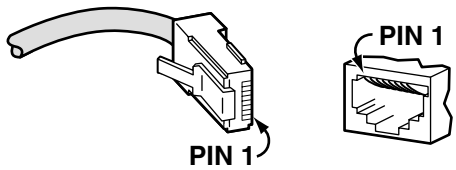


図 A.5.3 RJ-48 モジュラープラグ（左）、ジャック（右）

AR020 には、DSU に接続するための、次の 2 種類のケーブルが付属しています。各ケーブルは、DSU の仕様に合わせてご使用ください（各ケーブルは、AR020 専用です。他の用途に転用しないでください）。

- ARCBL-PRIRJ48
- ARCBL-PRIRJ45（IS10173-IS8877 変換ケーブル）

ARCBL-PRIRJ48

AR020 を IS10173 に準拠した DSU（RJ-48 ジャック）に接続する場合は、「ARCBL-PRIRJ48」をご使用ください。ARCBL-PRIRJ48 は、一方が RJ-48、もう一方が RJ-45 となっています。RJ-48 のジャックとプラグには、誤挿入防止の凹凸があり、RJ-48 のジャックとプラグ同士だけが嵌合可能です。

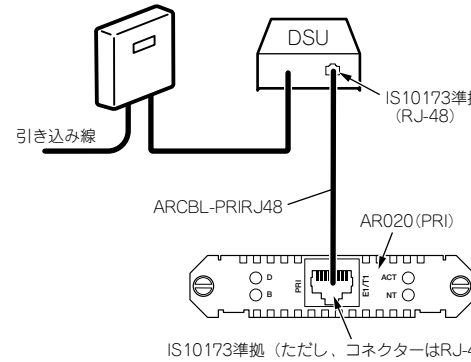


図 A.5.4 IS10173 準拠の DSU を使う場合

AR020（TE側、IS10173）			DSU（NT側、IS10173）	
機能	**ピン番号**		**ピン番号**	**機能 (注1)**
受信＋	1	←	1	送信＋（RA）
受信－	2	←	2	送信－（RB）
---	3		3	---
送信＋	4	→	4	受信＋（TA）
送信－	5	→	5	受信－（TB）
---	6		6	---
---	7		7	---
---	8		8	---

注1 RA、RB、TA、TBは、DSUのネジ止め端子台の信号線名です。

図 A.5.5 ARCBL-PRIRJ48 による接続

ARCBL-PRIRJ45

AR020 を IS8877 に準拠した DSU（RJ-45 ジャック）に接続する場合は、「ARCBL-PRIRJ45」をご使用ください。ARCBL-PRIRJ45 の両端には、接続されるべき機器の種類が明記されており、RJ-45 プラグの接続機器を入れ替えてご使用になることはできません。

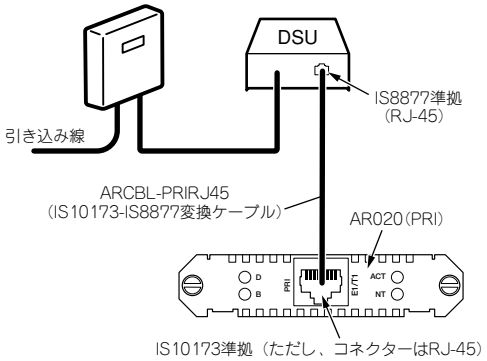


図 A.5.6 IS8877 準拠の DSU を使う場合

AR020 (TE側、IS10173)		DSU (NT側、IS8877)	
機能	ピン番号	ピン番号	機能 (注1)
受信＋	1	1	---
受信－	2	2	---
---	3	3	受信＋(TA)
送信＋	4	4	送信＋(RA)
送信－	5	5	送信－(RB)
---	6	6	受信－(TB)
---	7	7	---
---	8	8	---

注1 RA、RB、TA、TBは、DSUのネジ止め端子台の信号線名です。

図 A.5.7 ARCBL-PRIRJ45 による接続

AR021（BRI）

AR021 カードは、BRI ポート（Basic Rate ISDN S/T WAN ポート、RJ-45）を 1 つ持つ PIC です。本製品を ISDN（2B+D）、64K ～ 128Kbps のデジタル専用線やフレームリレー網への接続に使用します。

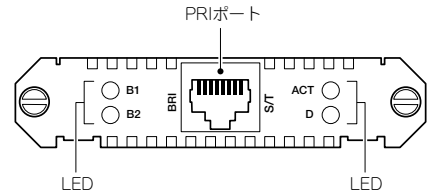


図 A.5.8 AR021 背面パネル

BRI ポート

ISDN 回線またはデジタル専用線に接続するためのポートです。BRI ポートは、RJ-45 モジュラージャックが使用されており、結線は IS8877 に準拠しています。接続用ケーブルは別途ご用意ください。

表 1.5.3 BRI ポート結線

ピン番号	機能
1	---
2	---
3	送信 +
4	受信 +
5	受信 -
6	送信 -
7	---
8	---

LED

LED	色	状態	表示の内容
B1	緑	点灯	ISDN の B1 チャネルがもう一方の接続端の機器と接続しています。
		点滅	データの送受信が行われています。
		消灯	ISDN の B1 チャネルがもう一方の接続端の機器と接続していません。64Kbps または 128Kbps 専用線の場合は、通常消灯しています。

B2	緑	点灯	ISDN のB2 チャネルがもう一方の接続端の機器と接続しています。
		点滅	データの送受信が行われています。ただし、64Kbps 専用線の場合は点滅しません。
		消灯	ISDN のB2 チャネルがもう一方の接続端の機器と接続していません。64Kbps または 128Kbps 専用線の場合は、通常消灯しています。
ACT	緑	点灯	レイヤ 1 のリンクが確立しています（本製品と交換機間の通信が可能です）。
		消灯	レイヤ 1 のリンクが確立していません（本製品と交換機間の通信ができません）。
D	緑	点滅	本製品と ISDN 交換機の間で、D チャネルを経由してパケットが交換されています。ISDN においてのみ意味を持ちます。
		消灯	本製品と ISDN 交換機の間で、D チャネルを経由してパケットが交換されていません。

ジャンパー

ジャンパー J1、J2 によって、終端抵抗（100Ω）のオン/ オフを設定します。J1 は TX 線の終端、J2 は RX 線の終端です。終端抵抗は、2 つを揃えてオンまたはオフに設定しなければなりません（一方がオン、もう一方がオフは許されません）。デフォルトは「オン」です。

終端抵抗をオフにする場合、ジャンパープラグをジャンパーピンの一方にだけ挿してください（ジャンパープラグの紛失を防ぐことができます）。

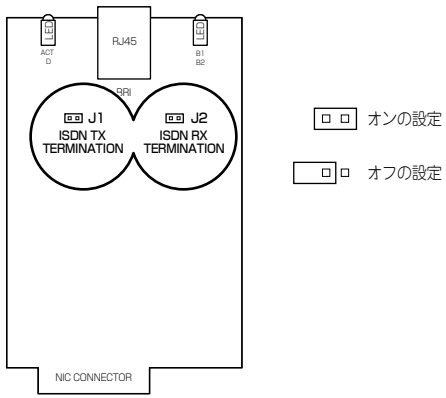


図 A.5.9 デフォルトのジャンパー設定

配線

回線 への接続にローゼット[*2] が介在する場合、AR021 の終端抵抗はオフ[*3]に設定してください（J1 :オフ、J2: オフ）。AR021 を DSU に直結する場合、終端抵抗はオンに設定してください（J1 :オン、J2 :オン）。接続用ケーブルは、別途ご用意ください。

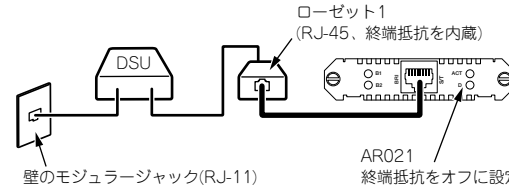


図 A.5.10 ローゼット 1 つの場合

図 A.5.11 DSU に直結の場合

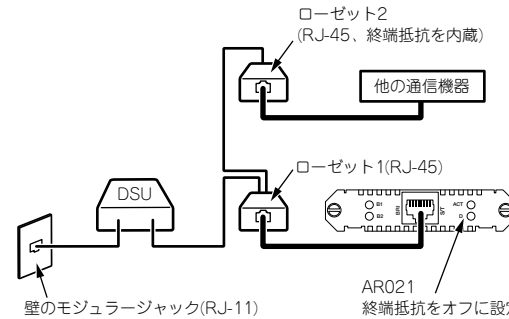


図 A.5.12 ローゼット 2 つの場合

*2 INS64の場合、複数のローゼットの接続が可能です。デジタル専用線の場合、ローゼット 1 個の接続、または直結が可能です。回線のお申し込みの際にご確認ください。

*3 DSU から見て一番遠いローゼットには、終端抵抗が内蔵されているため、AR021 の終端抵抗はオフに設定する必要があります。

AR022（10BASE-T、AUI）

AR022 カード（ETH）は、10BASE-T ポート、AUI ポートを 1 つずつ持つ PIC です。本製品に標準装備されている 10BASE-T/100BASE-TX ポート以外に、Ethernet ポートが必要なとき使用します。ジャンパーなど、設定が必要なか所はありません。

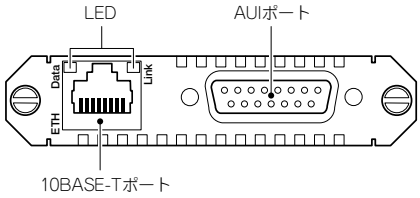


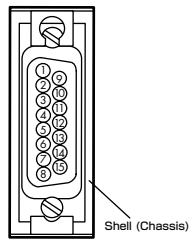
図 A.5.13 AR022 背面パネル

10BASE-T ポート

10BASE-T で Ethernet に接続するコネクターです（MDI）。Half Duplex のみをサポートしています。ストレートの UTP ケーブルを使用して、HUB やスイッチの通常のポート（MDI-X）に接続してください。AUI ポートを使用しているときに、このポートは使用できません。

AUI ポート

AUI ケーブルでトランシーバー（Ethernet）に接続するコネクターです。UTP ポートを使用しているときに、このポートは使用できません。



シールド	CI Shield (1)	(9) CI-	衝突検出(-)
衝突検出 (+)	CI+ (2)	(10) DO-	送信データ(-)
送信データ(+)	DO+ (3)	(11) DO Shield	シールド
シールド	DI Shield (4)	(12) DI-	受信データ(-)
受信データ(+)	DI+ (5)	(13) PWR+	電源供給線(+12V)
電源リターン	PWR RTN (6)	(14) PWR Shield	シールド
未使用	Not Used (7)	(15) Not Used	未使用
シールド	Shield (8)		

Shell (Protective GND)

図 A.5.14 AUI コネクター結線図

LED

LED は、10BASE-T ポートの状態を表示します。

LED	色	状態	表示の内容
Data	緑	点滅	データの送受信が行われています。
		消灯	データの送受信が行われていません。
LINK	緑	点灯	リンクが確立しています。
		消灯	リンクが確立していません。

AR023（SYN）

AR023 カードは、同期シリアルポート（SYN）を 1 つ持つ PIC です。専用ケーブル（別売）により、V.24、V.35、X.21 インターフェースを持つ DCE[*4] と接続できます。DCE から供給される ST2 クロック（外部クロック）に従い動作します。V.24、V.35 インターフェースにおける ST1 クロック信号の供給（DTE → DCE）はサポートしておりません。専用線、フレームリレーに対応しています。ISDN 回線モードの TA には対応していません。ジャンパーなど、設定が必要なか所はありません。

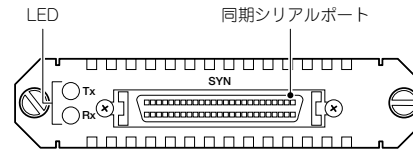


図 A.5.15 AR023 背面パネル

同期シリアルポート

DCE と接続するコネクターです。AMPLIMITE 50 ピンコネクターが使用されており、専用ケーブルを接続します。

LED

LED	色	状態	表示の内容
Tx	緑	点滅	データの送信が行われています。
		消灯	データの送信が行われていません。
Rx	緑	点滅	データの受信が行われています。
		消灯	データの受信が行われていません。

*4 Data Communication Equipment。ユーザー機器をネットワークに接続するための接続点を提供する、DSU、モデム、TA などの機器。

配線（専用ケーブル）

DCE への接続は、専用ケーブル（別売）で行います。ケーブルは、次の 3 種類があります。DCE が持つコネクタータイプに応じてご使用ください。

ケーブル名称	長さ	DCE 側ネジ仕様
ARCBL-V24DTE（RS-232）	2m	ISO 標準IS2110 準拠（固定ネジ：M2.6）
ARCBL-V35DTE	2m	ISO 標準IS2593 準拠（固定ネジ：2.99mm ピッチ 0.7938mm）
ARCBL-X21DTE	2m	ISO 標準IS4903 準拠（固定ネジ：M3）

電源スイッチをオンにしたとき、本製品はケーブルの種類を認識し、ケーブルに合わせて初期化されます。どのように認識しているかは、「SHOW SYN」コマンドで確認できます。下記に、V.35 の表示例を示します。

```
Manager > SHOW SYN ↵

SYN instance 0:        371 seconds   Last change at:          0 seconds

Module ..................... none
State ...................... enabled
Active ..................... no
Interface type ............. V.35 DTE
Clocks ..................... inactive
Actual baud rate ........... none
Configured baud rate ...... 48000
Max output queue length ... 100
Min interframe delay ...... no delay
Data sense ................. normal
Tx clock edge .............. rising
Hardware type .............. 68360
Debug ...................... off
```

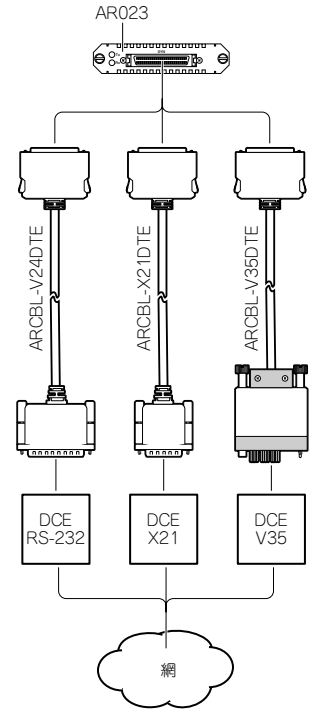


図 A.5.16 AR023 と各専用ケーブルの接続

ARCBL-V24DTE（V.24 ケーブル）

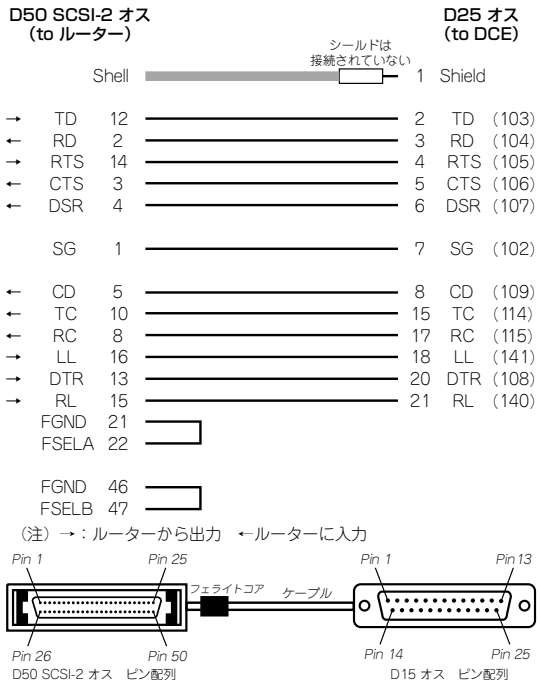


図 A.5.17 V.24（RS-232）ケーブル

ARCBL-V35（DTE V.35 ケーブル）

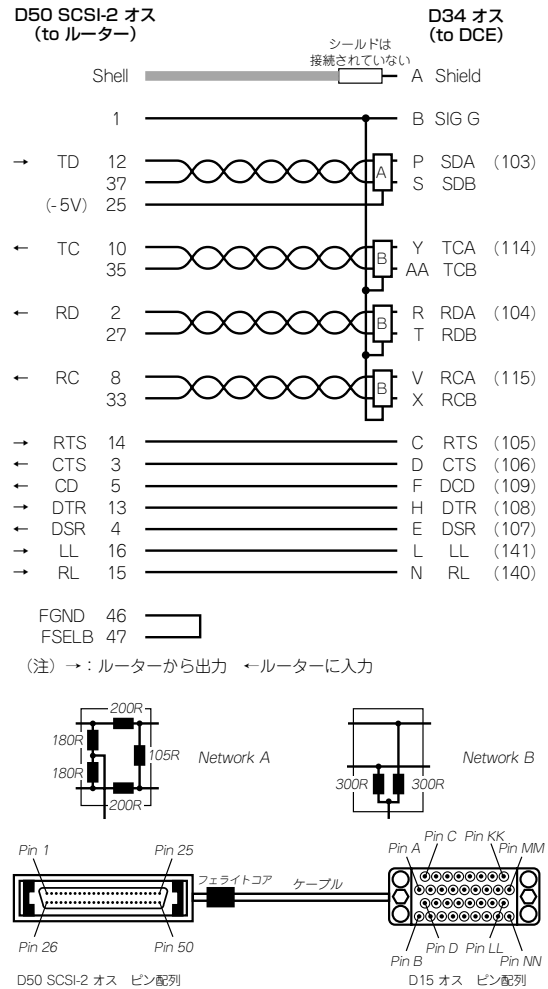


図 A.5.18 V.35 ケーブル結線図

ARCBL-X21DTE（X.21 ケーブル）

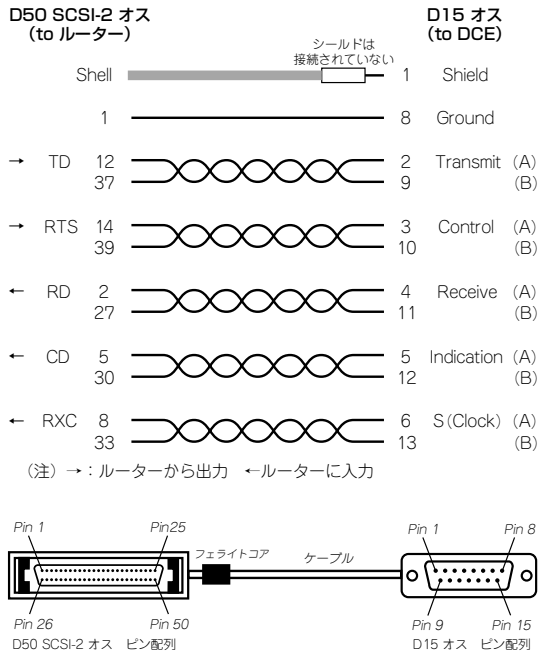


図 A.5.19 X.21 ケーブル

A.6 暗号 / 圧縮カードの取り付け

暗号 / 圧縮カード（オプションカード）は、本製品に装着した状態でのみ販売しております。オプションカードを単体で購入し、お客様によるオプションカードの装着はできません。

暗号 / 圧縮カード「AR010」または「AR011」は、「外国為替および外国貿易管理法」に基づいて規制される戦略物資（または役務）に該当します。このため、日本国外への持ち出しには、日本国政府の事前の許可などが必要です。

取り付け手順

1 プラスのドライバー（小）をご用意ください。

2 本製品の電源スイッチをオフにし、コンセントから電源ケーブルを抜いてください。

暗号 / 圧縮カードを本製品に取り付けるときは、必ず本製品の電源スイッチをオフにし、コンセントから電源ケーブルを抜いてください。電源が供給されたまま、この作業を行うと本製品や暗号 / 圧縮カードの故障の原因となります。

3 本製品に接続しているケーブル類があればすべて取り外してください。

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。

4 本製品側面のネジ（左右 2 個ずつ）、上面パネルのネジ（1 個）をプラスのドライバーで外してください。ネジを外すか所は合計 5 か所あります。後で、このネジは利用するため、紛失しないようにしてください。

5 上面パネルを外します。前面パネルを手前側にして、両手を使用し、前面に向かって約 2 センチずらします（前面パネルは上面パネルに固定されています）。上面パネルを真上に持ち上げてください。

次図のようにマザーボードが見えます（図は前面パネル側を手前に見ています）。点線で囲んだ部分が暗号 / 圧縮カード装着コネクターと固定用のつなぎナット（2 か所）です。

マザーボード右側にある「電源部」には手を触れないでください。高電圧がチャージしている可能性があり危険です。

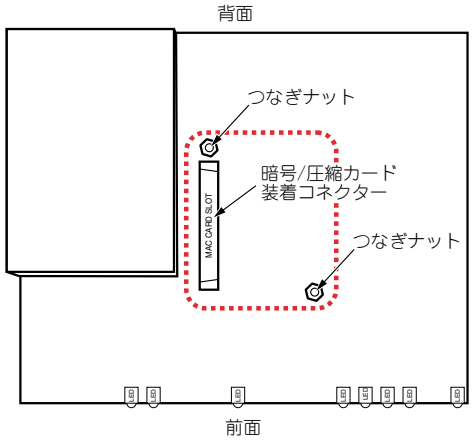


図 1.6.1 暗号 / 圧縮カード装着コネクターの位置

6 オプションカードの部品面を下に、切り欠きがある側を手前にして、オプションカードを暗号 / 圧縮カード装着コネクターに取り付けます。

オプションカードのコネクターをマザーボードのコネクターに差し込み、押し込んでください。コネクター同士が正しく嵌合していることを確認してください。オプションカードが外れないように、オプションカードに付属している固定ネジ（2 個）を使い、つなぎナットに固定してください。

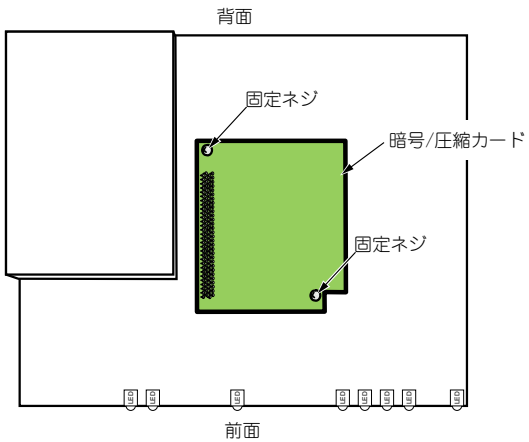


図 1.6.2 オプションカードの取り付け

暗号 / 圧縮カード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、カードの接点、部品などに素手で触れないでください。確実のためには、リストストラップなどの静電気防止用具の着用をお勧めします。

7 上面パネルを元通りにかぶせ、手順 4 で外したネジで止めてください。

8 ケーブル類をつないでください。

9 本製品の電源スイッチをオンにしてください。

オプションカードが認識されたことの確認

1 本製品の電源スイッチをオンにし、コンソールターミナルにログインプロンプトが現れたら、Manager レベルでログインしてください。

2「SHOW SYSTEM」コマンドを実行すると、オプションカードは「AR010 EMAC」として認識されていることを確認できます（下記は AR010 の例です）。

```
Manager > SHOW SYSTEM ↵

Router System Status                              Time 17:12:54 Date 04-Sep-2002.
Board      ID  Bay Board Name                        Rev   Serial number
------------------------------------------------------------------------------
Base      195      AR410 V2                          M1-0  57004257
PIC        75   0  AR020 PIC T1/E1 PRI               M1-1  39592696
MAC        66      AR010 EMAC                        M1-0  11750009
------------------------------------------------------------------------------
Memory -   DRAM : 16384 kB    FLASH :  7168 kB
------------------------------------------------------------------------------
......
```

図 1.6.3 オプションカードの認識

また、「SHOW ENCO」コマンドにより、オプションカードの状態を表示することができます。

```
Manager > SHOW ENCO ↵

ENCO Module Configuration

  MAC card present ....................... TRUE
  Lowest valid channel ................... 1
  Highest valid channel .................. 127
  Compression Statistics Enabled ......... FALSE
  Diffie Hellman Priority ................ HIGH

  SW Processes available
    RSA  - RSA Encryption
    DH   - Diffie Hellman
    HMAC - Message Digest

  MAC Processes available
    DES  - DES Encryption
```

A.7 回線申し込みにおける注意点

INS ネット 64/1500 お申し込み時の注意

基本的には、他の接続機器の状況も含め、ご自身の通信環境にあわせてお申し込みください。本製品の持つ機能を最大限に利用するための推奨値（**下線**）は以下のとおりです。各項目がどのような内容かは、NTT へご確認ください。

- 本製品の認定番号
  製品本体裏面のシールをご覧ください。

- インタフェース形態及びレイヤ 1 起動種別
  INS64 の場合「**P-MP 呼毎**」または「P-MP 常時」
  INS1500 の場合、通常はインターフェース形態として「**23B+D**」を選択してください。呼制御を行う D チャネルが必要なため「**24B**」の選択はできません。**呼番号長**は「1 オクテット」または「2 オクテット」のどちらでもかまいません。

- 発信者番号通知サービス
  プロバイダーへの接続のみの場合はいずれでもかまいません。拠点間の接続、例えば事業所と事業所を結ぶ通信を行う場合は、「**呼毎通知許可**」か「呼毎通知拒否」を推奨いたします。

- ユーザー周情報通知サービス
  「**着信許可**」または「着信拒否」

専用線お申し込み時の注意

特にありません。

A.8 製品仕様

ハードウェア

CPU	
	PowerPC 66MHz
メモリー容量	
	メインメモリー
	16MByte
	フラッシュメモリー
	8MByte（ファイルシステムで 7MByte が使用可能）
ポート	
	WAN
	10BASE-T/100BASE-TX（MDI）× 1
	LAN
	10BASE-T/100BASE-TX（MDI-X）× 4
	（ただし、ポート 4 は MDI/MDI-X 切替可能）
	コンソール
	RS-232（DCE）、D サブ 9 ピン（メス）× 1
拡張ベイ	
	Port Interface Card（PIC）× 1
スイッチ部（LAN）	
	スイッチング方式
	ストア＆フォワード
	パケットバッファー
	128KByte
	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）	
	拡張ボード
	AR010（暗号）、AR011（圧縮）、AR012（暗号 & 圧縮）
	PIC
	AR020（PRI）、AR021（BRI）、AR022（10BASE-T、AUI）、AR023（同期シリアル：V.24/V.35/X.21）
	ラックマウントキット
	AT-RKMT-J07
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）	0.13A（90VAC）
平均消費電力	6.1W（最大 9.2W）
平均発熱量	5.2kcal/h（最大 7.9kcal/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）	
重量	
1.6kg	
適合規格	
UL60950 CSA-C 22.2 No.60950	
JATE（CD02-0259JP）	
VCCI クラス A	

VCCI クラス A
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 A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずる よう要求されることがあります。

ソフトウェア

準拠規格
IEEE 802.3 10BASE-T
IEEE 802.3u 100BASE-TX
IEEE 802.1D Spanning Tree
ルーティングプロトコル
IP、IPX、AppleTalk phase I & II
ルーティング方式
スタティック、RIP/RIP2、OSPF、RIP（IPX）
WAN サービス
xDSL、CATV、FTTH
ISDN、専用線、フレームリレー、同期（V.24/V.35/X.21）
機能
PPP over Ethernet[a]、PPP/MP
NAT/EnhancedNAT
DHCP（Server、Client、Relay Agent）、DNS Relay
Firewall（Stateful Inspection、攻撃検出・通知）
Packet Filtering
VPN（IPsec[b]（IKE/ISAKMP）、L2TP（RFC2661 準拠）、GRE）
Bridging、IPX 代理応答
Multi Homing
データ圧縮（STAC LZS、VJ Compression、Predictor、FRF.9、IP comp[c]）
サービス管理（RSVP、RSVP Proxy Agent、Priority-Based Routing、Policy-based Routing）
VRRP
PAP/CHAP、RADIUS、TACACS、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、Frame Relay MIB、Ethernet MIB、Private MIB）、

a. サービスが対応していれば同時 4 セッション可
b. 暗号カード AR010 または AR011 が必要
c. 同上

このソフトウェア仕様は、Ver.2.3.3 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、最新のカタログ、リリースノートをご覧ください。

B 保証とユーザサポート

B.1 保証

製品に添付している「製品保証書」の「製品保証規定」をお読みになり、「お客さまインフォメーション登録カード」に必要事項を記入して、弊社「お客さまインフォメーション登録係」までご返送ください。「お客さまインフォメーション登録カード」が返送されていない場合、保証期間内の無償での修理や、障害発生時のユーザーサポートなどが受けられないことがあります。

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、この取扱説明書の巻末の調査依頼書をコピーしたものに必要事項を記入し、下記のサポート先にFAXしてください。記入内容の詳細は、『調査依頼書のご記入にあたって』をご覧ください。

アライドテレシス株式会社　サポートセンター

Tel: 0120-860-772
月～金（祝・祭日を除く）9:00～12:00 13:00～18:00

Fax: 0120-860-662
年中無休 24 時間受付

調査依頼書のご記入にあたって

本依頼書は、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にご記入いただくものです。ご提供いただく情報が不充分な場合には、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、以下の点にそってご記入ください。記入用紙で書き切れない場合には、プリントアウトなどを別途添付してください。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 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）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**」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）。

2 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 IIJ に接続

3 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のプリントアウトなど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のプリントアウトをお送りください（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）。

4 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。

調査依頼書（CentreCOM AR410 V2）

年　月　日

一般事項

1. 御社名：
   部署名：　　ご担当：
   ご連絡先住所：〒

   TEL：　（　）　　FAX：　（　）
2. ご購入先：　　ご購入年月日：

   ご購入先担当者：　　ご連絡先（TEL）：　（　）

ハードウェアとソフトウェア

1. ご使用のハードウェア機種（製品名）、シリアル番号、リビジョン

   CentreCOM AR410 V2　S/N＿＿＿＿＿＿＿＿ Rev＿＿

2. 本製品のファームウェア（ソフトウェア）のバージョン
   Rev（本体）：M　-＿＿＿＿＿＿
   SoftwareVersion：＿＿＿＿＿＿＿＿
   ReleaseVersion：＿＿＿＿＿＿＿＿

3. 回線
   □ ADSL：＿＿＿＿＿＿＿＿で＿＿＿＿＿＿＿＿と接続
   □ FTTH：＿＿＿＿＿＿＿＿で＿＿＿＿＿＿＿＿と接続
   □ CATV：＿＿＿＿＿＿＿＿で＿＿＿＿＿＿＿＿と接続
   □無線：＿＿＿＿＿＿＿＿で＿＿＿＿＿＿＿＿と接続
   □ ISDN：＿＿＿＿＿＿＿＿
   □専用線：＿＿＿＿＿＿＿＿
   □フレームリレー：＿＿＿＿＿＿＿＿

調査依頼書（CentreCOM AR410 V2）

年　月　日

お問い合わせ内容

□別紙あり　□別紙なし
□設置中に起こっている障害　□設置後、運用中に起こっている障害

ネットワーク構成図

□別紙あり　□別紙なし
簡単なもので結構ですからご記入をお願いします。

```
 login: manager
Password: xxxxxxx (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-Sep-2002.
Board      ID  Bay Board Name                        Rev    Serial number
-------------------------------------------------------------------------------
Base      195      AR410 V2                         M1-0   57004257
MAC        66      AR010 EMAC                       M1-0   11750009
-------------------------------------------------------------------------------
Memory -   DRAM : 16384 kB    FLASH :  7168 kB
-------------------------------------------------------------------------------
SysDescription
CentreCOM AR410 V2 version 2.3.3-00 27-Aug-2002
SysContact

SysLocation

SysName
OSAKA
SysDistName

SysUpTime
49540 ( 00:08:15 )
Software Version: 2.3.3-00 27-Aug-2002
Release Version : 2.3.3-00 27-Aug-2002
Patch Installed : NONE
Territory       : japan
.....
```

図B.2.1 サポートに必要なソフトウェア情報

ご注意

- 本マニュアルは、アライドテレシ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シ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。
- アライドテレシス株式会社は、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。
- アライドテレシス株式会社は、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。

商標について

CentreCOMは、アライドテレシ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

2002年9月4日　　Rev.A　　初版（Firmware Ver.2.3.3）

本製品のIPsec機能は、米国のセキュリティー認定機関TruSecure社（旧ICSA社）の認定を取得しており、IPsec通信の安全性および他社IPsec対応機器との相互接続性が確認されています。

本製品の Firewall機能は、米国のセキュリティー認定機関 TruSecure 社（旧 ICSA 社）の認定を取得してます。

CentreCOM® AR410 V2 取扱説明書

アライドテレシス株式会社
PN J613-M3048-00 Rev.A 020904