BR500Sトラブルシューティング

はじめに

このたびは、本装置をお買い上げいただき、まことにありがとうございます。
インターネットやLANをさらに活用するために、本装置をご利用ください。

2008年9月

本装置の外観・仕様は、予告なしに変更することがあります。

本装置は日本国内用に設計されています。海外では使用できません。
This equipment is designed for use in Japan only and cannnot be used in any other country.

本ドキュメントには「外国為替及び外国貿易管理法」に基づく特定技術が含まれています。

従って本ドキュメントを輸出または非居住者に提供するとき、同法に基づく許可が必要となります。

Microsoft Corporationのガイドラインに従って画面写真を使用しています。

本書の内容につきましては万全を期しておりますが、お気づきの点がございましたら、当社のサービス取扱所へお申しつけください。

目次

本書の使いかた

本書では、困ったときの原因・対処方法やご購入時の状態に戻す方法について説明しています。
また、CD-ROMの中のREADMEファイルには大切な情報が記載されていますので、併せてお読みください。

本書の読者と前提知識

本書は、ネットワーク管理を行っている方を対象に記述しています。
本書を利用するにあたって、ネットワークおよびインターネットに関する基本的な知識が必要です。

マークについて

本書で使用しているマーク類は、以下のような内容を表しています。

ヒント	**本装置をお使いになる際に、役に立つ知識をコラム形式で説明しています。**
こんな事に気をつけて	**本装置をご使用になる際に、注意していただきたいことを説明しています。**
補足	**操作手順で説明しているものの他に、補足情報を説明しています。**
参照	**操作方法など関連事項を説明している箇所を示します。**
警告	**製造物責任法（PL）関連の警告事項をあらわしています。本装置をお使いの際は必ず守ってください。**
注意	**製造物責任法（PL）関連の注意事項をあらわしています。本装置をお使いの際は必ず守ってください。**

本書における商標の表記について

Microsoft、Windowsおよび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。

Windows® XPの正式名称は、Microsoft® Windows® XP Professional operating system、または Microsoft® Windows® XP Home Edition operating systemです。

Windows® Meの正式名称は、Microsoft® Windows® Millennium Edition operating systemです。

Windows® 98の正式名称は、Microsoft® Windows® 98 operating system です。

Windows® 95の正式名称は、Microsoft® Windows® 95 operating system です。

Windows® 2000の正式名称は、Microsoft® Windows® 2000 Server Network operating system、または Microsoft® Windows® 2000 Professional operating system です。

Windows NT® 4.0の正式名称は、Microsoft® Windows NT® Server network operating system Version 4.0、または Microsoft® Windows NT® Workstation operating system Version 4.0です。

フレッツは、NTT東日本・NTT西日本のサービス名であり、登録商標です。

フレッツ・ADSLは、NTT東日本・NTT西日本の登録商標です。

Linuxは、Linus Torvalds氏の米国およびその他の国における登録商標または商標です。

本書に記載されているその他の会社名および製品名は、各社の商標または登録商標です。

1　回線料金がおかしいと思ったら

超過課金とは、利用者が意図しない回線接続や回線使用が長期的に続き、その結果として必要以上の回線料金が課金されることがあります。

以下に超過課金の見分け方と調査方法などについて説明します。

1.1　超過課金の見分け方

超過課金が発生する原因は 2 つあります。

（1）　回線未接続状態で LAN に接続したパソコンなどから利用者の意図しないデータが回線に流れ、その結果、回線が接続することが頻発する場合。

（2）　回線を接続したあとに、LAN に接続されたパソコンなどから利用者の意図しないデータが定期的に発信され、回線が長時間接続されたままの状態になる場合。

これらは課金情報を確認し、利用状況と照らし合わせることで超過課金が発生していることがわかります。課金情報で表示されている回線接続していた時間が利用時間よりも極端に長い場合は、超過課金が発生している可能性があります。

参照　BR500S Web ユーザーズガイド「2.2.4 課金情報で運用状況を確認する」（P.33）
BR500S コマンドユーザーズガイド「2.1.8 課金情報で運用状況を確認する」（P.34）

1.2　超過課金が発生した原因を調べる

ここでは、超過課金が発生する代表的な事例をあげ、それぞれの調査方法と対処方法について説明します。

WAN 側に RIP パケットが流れている場合

【現象】

LAN 側のパソコンの通信が終了したが、長時間回線が自動切断されない。

【原因】

WAN 側接続相手（たとえばプロバイダのルータ）がダイナミックルーティングを使用し、本装置に経路情報（RIP パケット）を送信してくる場合に、通信がないにもかかわらず回線が接続されたままになることがあります。

【調査方法】

- まず LAN 側端末が回線を使用した通信を行っていないことを確認します。
- もし、パソコンが通信をしているかが判断できない場合は、それらのパソコンの電源を切断します。
- この状態で本装置の表示ランプを監視します。ここで B1 または B2 ランプが一定間隔（15～45 秒間隔）で点滅していた場合は、経路情報などのなんらかのデータが接続相手から送られてきていることになります。
- さらに上記ランプが点滅するたびに IP 統計情報を確認します。表示された IP 統計情報の中の udp XXX datagrams received の部分の数字が確認するたびに増加していれば、原因は経路情報（RIP）受信によるものと考えられます。

【対処方法】

IP フィルタリング機能を使って経路情報（RIP）を破棄するように以下の設定をしてください。

```
remote <number> ip filter <count> reject any any any any 520 17 yes any any
```

これにより、接続相手から経路情報（RIP）が送出されてきても無通信監視時間（初期設定値は 60 秒）を経過すると回線は自動的に切断されます。

補足 上記以外にも本装置の設定でWAN側にダイナミックルーティング機能を使用する設定になっていることが原因の場合もあります。この場合は、以下のコマンドでRIP送信をしない設定であることを確認してください。

```
# show remote <number> ip rip
```

参照 BR500S Web設定事例集「2.12 IPフィルタリング機能を使う」（P.308）、
BR500S Webユーザーズガイド「2.2.8 IP統計情報を確認する」（P.40）、
BR500S コマンド設定事例集「2.12 IPフィルタリング機能を使う」（P.132）、
BR500S コマンドユーザーズガイド「2.1.13 IP統計情報を確認する」（P.42）

パソコンからの自動送信パケット

【現象】

LAN側のパソコンなどからの通信がないにもかかわらず、いつのまにか本装置からの発信により回線接続してしまう。

【原因】

Windows®のパソコンは、利用者の意図とは無関係に（利用者が通信している意識がないにもかかわらず）自動的にパケットを回線側に送出してしまう場合があります。

【調査方法】

- 利用者が通信していないこと（WWWブラウザや電子メールなど使用していないこと）を確認してください。
- この状態で回線の発信が起きている場合は、システムログ（メッセージ集）を参照して発信の契機となった事象を確認してください。
- 発信ログの意味が「パケット送信による発信処理」の場合は、パソコンが回線側にパケットを送信しています。→【対処方法1】
- 発信ログの意味が「上記以外の理由による発信処理」の場合で、発信理由がProxyDNSの場合は、パソコンが本装置のProxyDNS機能を利用しようとしてDNS要求を送信しています。→【対処方法2】

【対処方法1】

IPフィルタリング機能を使ってNetBIOS over TCPの情報を回線側に流さないように設定してください。

参照 BR500S Web設定事例集「2.12 IPフィルタリング機能を使う」（P.308）、
BR500S コマンド設定事例集「2.12 IPフィルタリング機能を使う」（P.132）

【対処方法2】

URLフィルタ機能を使ってWindowsのワークグループ名のアクセスを禁止してください。この場合はアクセスを禁止するドメイン名に「<ワークグループ名>＊」を指定してください。

参照 BR500S Web設定事例集「2.24 特定のURLへのアクセスを禁止する（URLフィルタ機能）」（P.528）、
BR500S コマンド設定事例集「2.24 特定のURLへのアクセスを禁止する（URLフィルタ機能）」（P.234）

【対処方法3】

パソコンが送信するDNSパケットの問い合わせタイプ（QTYPE）がA（1）、PTR（12）以外の場合、DNS問い合わせタイプフィルタ機能を使って、特定の問い合わせタイプのパケットを破棄することができます。DNSパケットの問い合わせタイプ（QTYPE）は、本装置のシステムログ情報に以下の情報が記録されていることから確認してください。「proxydns:[<QTYPE>:<QNAME>]from<IPアドレス>to<ネットワーク名>」

参照 BR500S Web設定事例集「2.23.4 DNS問い合わせタイプフィルタ機能を使う」（P.524）、
BR500S コマンド設定事例集「2.23.4 DNS問い合わせタイプフィルタ機能を使う」（P.232）

デフォルトルートどうしで接続している場合

【現象】

パソコン上のアプリケーション（WWW ブラウザや電子メールなど）が異常終了し、数分から数十分間回線が接続されたままになる。

【原因】

自側および相手側本装置の両方でデフォルトルートの設定がされていることが原因です。

【調査方法】

両者のデフォルトルートの設定内容を確認してください。

【対処方法】

どちらかの本装置の設定からデフォルトルートの設定をはずしてください。

参照 BR500S Web 設定事例集「1.7 事業所 LAN を ISDN で接続する」（P.72）、
BR500S コマンド設定事例集「1.7 事業所 LAN を ISDN で接続する」（P.19）

スケジュール機能の設定を誤った場合

【現象】

スケジュール機能で夜間は発信抑止しているにもかかわらず、発信してしまう。

【原因】

スケジュール機能の設定が誤っていることが原因です。

【調査方法】

- スケジュール機能の設定を確認してください。ここで予約時刻、終了時刻が正しく設定されているかを確認してください。
- さらに内部時計の時刻設定も確認してください。

【対処方法】

上記スケジュール機能および内部時計の時刻設定をそれぞれ正しく設定し直してください。

参照 BR500S Web 設定事例集「2.30 スケジュール機能を使う」（P.586）、
BR500S Web ユーザーズガイド「1.3 時計を設定する」（P.10）、「2.1.5 時計を設定する」（P.20）、
BR500S コマンド設定事例集「2.30 スケジュール機能を使う」（P.253）、
BR500S コマンドユーザーズガイド「1.1 時計を設定する」（P.7）

LAN 側のパソコンを移設した場合

【現象】

ほかの LAN に接続してあったパソコンなどを本装置の LAN に移設したら、頻繁に回線発信が行われるようになった。または回線が切断されなくなった。

【原因】

そのパソコンが以前接続していた LAN 環境で運用されていたサービスやアプリケーションが WAN 環境にはふさわしくないことが原因です。

【調査方法】

問題のパソコンが立ち上がっているときと電源が切断れているときとで、上記現象の発生の有無が変わることを確認してください。

【対処方法】

詳細な原因は、問題となるサービスやアプリケーションに依存するため対応方法はさまざまです。特定のサーバや特定のサービスへのアクセスが原因の場合、IP フィルタリング機能を使用して無意味な発信を抑止します。また、スケジューリング機能を使用することで防止できる場合もあります。どの場合にもシステムログ情報を確認して発信の契機となったサービスやアプリケーションを特定するか、またはそのパソコンの以前の利用者にサービス内容やアプリケーションの設定内容を確認してください。

参照 BR500S Web ユーザーズガイド「2.2.7 システムログを確認する」（P.39）、
BR500S コマンドユーザーズガイド「2.1.12 システムログを確認する」（P.41）

本装置を移設した場合

【現象】

ほかの環境に接続していた本装置を移設した、本装置が関係するネットワークの一部または全部が変更になったところ、回線発信が頻発するようになった。または回線が切断されなくなった。

【原因】

本装置の設定が新たな環境にふさわしくないものであることが原因です。

【調査方法】

特に必要ありません。

【対処方法】

本装置の設定を一度ご購入時の状態に戻したあと、最初から設定し直してください。

参照 「5 ご購入時の状態に戻すには」（P.42）

2　通信ができない場合には

通信ができない場合、さまざまな原因が考えられます。まず、以下を参考に本装置の動作状況を確認してみてください。

ヒント

◆ **エラー番号からトラブルの原因を探る**

エラーログ情報に表示されたエラー番号から、エラーの原因をある程度特定できます。

エラーログ情報をプリントアウトして保管しておくことをお勧めします。

警告

- **決してご自身では修理を行わないでください。**
- **本装置が故障した場合は、弊社の技術者または弊社が認定した技術員によるメンテナンスを受けてください。**

2.1　起動時の動作に関するトラブル

本装置起動時のトラブルには、以下のようなものがあります。

● **POWER ランプがつかない**

【原因】 電源ケーブルが、電源コネクタまたはコンセントに正しく接続されていない。

【対処】 電源ケーブルを、電源コネクタまたはコンセントに正しく接続してください。

【原因】 本装置の電源スイッチが入っていない。

【対処】 本装置の電源スイッチが「｜」側へ押されているか確認してください。

● **CHECK ランプが橙色で点灯している**

【原因】 本体に異常が発生しました。

【対処】 弊社の技術員または弊社が認定した技術員へ連絡してください。

● **回線（ISDN 公衆回線／専用線／フレームリレー）につないで電源を入れたら、B1/B2 ランプが橙色で点滅している**

【原因】 回線ケーブルがきちんと差し込まれていない。

【対処】 回線ケーブルをきちんと差し込んでください。

【原因】 回線で同期はずれが発生している。

【対処】 通信事業者に調査を依頼してください。

【原因】 回線契約（フレームリレー）と本装置の設定が間違っている。

【対処】 本装置の設定を回線契約に合わせて正しく行ってください。

【原因】 ISDN 回線の極性が反転している。

【対処】 ディップスイッチで回線極性を変更することができます。本装置の電源を切断後、回線極性を変更して、再度電源を投入してください。

参照 BR500S ご利用にあたって「ディップスイッチの設定」（P.18）

2.2 本装置設定時のトラブル

本装置設定時のトラブルには、以下のようなものがあります。

● 接続したLANポートに該当するLANランプが橙色で点滅している、または、パソコンまたはHUBのリンクランプが点灯していない

【原因】 スピード／全二重・半二重のモード設定が接続相手と合っていない。

【対処】 本装置の10／100MおよびFULL／HALFの設定とパソコンまたはHUBの接続状態が合っているか確認してください。本装置は100M／FULLランプまたはステータスコマンド（stlan）で接続状態が確認できます。

参照 BR500Sご利用にあたって「100M/FULLランプの詳細」（P.16）

【原因】 LANケーブルのタイプが違う。

【対処】 LAN機器と接続する場合、パソコンにはストレートケーブル、HUBにはクロスケーブルで接続する必要があります。ケーブルのタイプを確認して、必要なLANケーブルを用意してください。
LAN0ポートではto HUB to PCスイッチを備えているため、接続対象に合わせてスイッチを切り替えることができます。また、LAN1～3ポートはMDI/MDI-Xをサポートしているため、構成定義で状況に合わせて設定を変更することができ、ストレートおよびクロスの両方のケーブルを使用することができます。

【原因】 接続に誤りがある。または、LANケーブルが断線している。

【対処】 点灯していない場合は、LANケーブルが正しく接続されていないか、または断線している可能性があります。LANケーブルがパソコンまたはHUBと本装置に正しく差し込んであるか、to HUB to PCスイッチ（LAN0ポートのみ）の設定が正しく設定されているかを確認し、それでも点灯しない場合は、別のLANケーブルに交換してください。

● telnetで本装置のIPアドレスを指定したがうまくつながらない

【原因】 パソコンのIPアドレスやネットマスクが間違っている。

【対処】
- パソコンの設定でIPアドレスやネットマスクを設定している場合は、本装置と通信できるIPアドレスが設定されているかどうかを確認してください。
  本装置のIPアドレスやネットマスクを変更していない場合は、パソコンには以下の範囲で設定する必要があります。
  IPアドレス　：192.168.1.2～192.168.1.254
  ネットマスク　：255.255.255.0
- 本装置のDHCPサーバ機能を利用している場合は、パソコンを再起動してください。

補足 パソコン側のIP設定は、winipcfgコマンド（Windows® 95／98／Meの場合）やipconfigコマンド（Windows® 2000／XP／Windows NT®の場合）で確認できます。

【原因】 パソコンとTAでインターネットに接続したときの設定が残っている。

【対処】 LANインタフェースのIPアドレスを再割り当てするため、パソコンを再起動してください。

【原因】 LAN0ポート以外に接続されている。

【対処】 本装置の設定を変更していない場合は、LAN0ポートだけが接続できる設定となっています。LANケーブルが本装置のLAN0ポートに正しく差し込んであることを確認してください。

【原因】 パソコンのARPエントリの値がおかしくなっている。

【対処】 本装置と同じIPアドレスを持つ機器と通信した直後に、パソコンの電源を落とさないまま本装置へ接続を変更した場合は通信できません。しばらく待つか、パソコンを再起動してください。

【原因】 本装置と同じ IP アドレスを持つ機器が接続されている。

【対処】 IP アドレスが重複している機器が LAN 上に存在すると、正しく通信できません。
本装置から設定を行うパソコン以外を接続している LAN ケーブルをはずし、パソコンを再起動してください。

【原因】 本装置の IP アドレスが変更されている。

【対処】 変更後の本装置の IP アドレスを指定してください。

【原因】 パソコンの IP アドレスを変更していない。

【対処】 本装置の IP アドレスを変更した場合、必ずパソコン側の IP アドレスもそれに合わせて変更します。
パソコンの IP アドレスを本装置と直接通信可能なアドレスに変更してください。また、ネットマスクを本装置に設定した値と同じ値に設定してください。このとき、DNS サーバの IP アドレスも忘れずに入力してください。

● WWW ブラウザでマニュアルどおりの URL を指定したが本装置のトップページが表示されない

【原因】 接続に誤りがある。または、LAN ケーブルが断線している。

【対処】 接続した 10／100BASE-TX ポートに該当する LAN ランプが緑点灯しているかを確認してください。緑点灯していない場合は正しく接続されていないか、ケーブルが断線している可能性があります。LAN ケーブルがパソコンまたは HUB と本装置にきちんと差し込んであるか、to HUB to PC スイッチが正しく設定されているかを確認してください。それでも LAN ランプが緑点灯しない場合は、別の LAN ケーブルに交換してください。

【原因】 パソコンの IP アドレスやネットマスクが間違っている。

【対処】
- パソコンの設定で IP アドレスやネットマスクを設定している場合は、本装置と通信できる IP アドレスが設定されているかどうかを確認してください。
  本装置の IP アドレスやネットマスクを変更していない場合は、パソコンには以下の範囲で設定を行う必要があります。

  IP アドレス　：192.168.1.2 ～ 192.168.1.254

  ネットマスク　：255.255.255.0
- 本装置の DHCP サーバ機能を利用している場合は、パソコンを再起動してください。
- Windows® 98 の場合は、「プライベート IP アドレス自動割り当て」機構により、DHCP サーバから自動取得する設定にしていても、169.254.XX.XX という IP アドレスが設定される場合があります。
  この場合は IP アドレスを固定で割り当てても通信できないことが多いため、ネットワークドライバと TCP/IP を入れ直してください。

補足 パソコン側の IP 設定は、winipcfg コマンド（Windows® 95／98／Me の場合）や ipconfig コマンド（Windows® 2000／XP／Windows NT® の場合）で確認できます。

【原因】 パソコンと TA でインターネットに接続したときの設定が残っている。

【対処】 LAN インタフェースの IP アドレスを再割り当てするため、パソコンを再起動してください。

【原因】 WWWブラウザの設定が間違っている。

【対処】
- WWWブラウザ（Microsoft® Internet Explorer 5.5）の場合、［ツール］－［インターネットオプション］－［接続］で、インターネットオプション画面のダイヤルアップの設定で「ダイヤルしない」が選択されていることを確認してください。「通常の接続でダイヤルする」が選択されているとWWWブラウザを起動するたびにモデムやTAからインターネットへ接続しようとして本装置と通信できない可能性があります。
- WWWブラウザの設定でProxyサーバの設定が有効になっている可能性があります。［ツール］－［インターネットオプション］－［接続］－［LANの設定］で、プロキシサーバの欄で「プロキシサーバを使用する」のチェックを外して、Proxyサーバを使用しない状態にしてください。また、Proxyサーバを使用する場合は、［プロキシの設定］で例外の欄に本装置のIPアドレス（本装置のIPアドレスを変更していない場合は192.168.1.1）を追加してください。

【原因】 パソコンのARPエントリの値がおかしくなっている。

【対処】 本装置と同じIPアドレスを持つ機器と通信した直後に、パソコンの電源を落とさないまま本装置へ接続変更を行った場合は通信できません。しばらく待つか、パソコンを再起動してください。

【原因】 本装置と同じIPアドレスを持つ機器が接続されている。

【対処】 IPアドレスが重複している機器がLAN上に存在すると、正しく通信できません。
本装置から設定を行うパソコン以外を接続しているLANケーブルをはずし、パソコンを再起動してください。

【原因】 本装置のIPアドレスが変更されている。

【対処】 変更後の本装置のIPアドレスを指定してください。

【原因】 パソコンのIPアドレスを変更していない。

【対処】 本装置のIPアドレスを変更した場合、必ずパソコン側のIPアドレスもそれに合わせて変更します。
- 本装置のDHCPサーバ機能を利用している場合
  パソコンを再起動してください。
- 本装置のDHCPサーバ機能を利用していない場合
  パソコンのIPアドレスを本装置と直接通信可能なアドレスに変更してください。また、ネットマスクを本装置に設定した値と同じ値に設定してください。このとき、DNSサーバのIPアドレスも忘れずに入力してください。

● 変更した本装置のIPアドレスがわからなくなった

【対処】 コンソールでログオンして、構成定義を確認してください。

● 本装置に設定したパスワードがわからなくなった

【対処】 本装置をご購入時の状態に戻してください。こうすることでパスワードを削除し、IPアドレスを「192.168.1.1」に戻すことができます。それまでに設定した内容はすべて消えてしまいますので、最初から設定し直してください。

☛ 参照 「5 ご購入時の状態に戻すには」（P.42）

● WWWブラウザの［戻る］ボタンまたはエラー画面の［1つ前に戻る］ボタンで戻ったあと、［更新］ボタンをクリックすると入力したパスワードが削除された。

【原因】 WWWブラウザの仕様です。

【対処】 ご使用のWWWブラウザによっては、画面を移動するとパスワード情報（入力データが「＊」で表示されるテキストボックス）が削除されます。この場合、パスワード情報を再入力してください。

● **WWW ブラウザの［戻る］ボタンまたはエラー画面の［1 つ前に戻る］ボタンをクリックしても反応がなく、1 つ前の設定画面を表示することができない。**

【原因】 ブラウザによっては、履歴を正しくたどることができない場合があります。

【対処】 再度、目的の操作を実施して、再設定してください（エラーの場合は、正しい情報を再入力してください）。

2.3 回線への接続に関するトラブル

本装置で回線に接続する際のトラブルには、以下のようなものがあります。

● **通信エラーが発生する、または回線が切断される**

【原因】 回線ケーブルおよび終端抵抗の配線に誤りがある。

【対処】 モジュラコネクタまでの回線ケーブルは 10m 以内で最終端のモジュラコネクタに終端抵抗を備えてください。

● **ISDN 公衆回線で相手先につながらない（B1/B2 ランプがまったく点灯しない）**

【原因】 接続先が話し中である。

【対処】 時間をおいてから接続し直してください。

【原因】 接続先の電話番号、サブアドレスの設定に誤りがある。

【対処】 接続先の電話番号、サブアドレスを正しく設定し直してください。

【原因】 接続先から拒否されている。

【対処】 接続先の管理者に問い合わせてください。

【原因】 課金制限値または接続時間制限値を超えている。

【対処】 課金情報を確認し、設定した制限値を超えていないかどうかを確認してください。

【原因】 スケジュール機能で発信抑止を設定している場合、開始時刻／終了時刻、または本装置の時刻が正しく設定されていない。

【対処】 発信抑止の開始時刻／終了時刻、または本装置の時刻を正しく設定し直してください。

【原因】 発信が連続して失敗した場合、3 分間に 2 回を超える再発信を行おうとすると、本装置が自動発信を抑止する。

【対処】 システムログの情報から発信失敗の原因を確認してください。また、接続先情報の設定内容を確認し、誤りがあった場合は正しく設定し直してください。

【原因】 認証エラーなどの発信失敗が 30 回連続して発生したため、本装置が自動発信を抑止している。このとき、以下のシステムログが出力されます。

```
protocol: continuous PPP negotiation error ～: call stop
```

【対処】 接続先情報の設定内容に誤りがある場合は、対象となる接続先の情報を変更してから接続を行ってください。また、接続先の（一時的な）不具合による場合は、不具合が解消されたあと、手動接続を行ってください。接続先情報の設定内容を変更して設定反映するか、手動接続で正常に接続できると、自動発信の抑止状態は解除されます。

【原因】 モジュラジャックの極性が反転している。

【対処】 モジュラジャックの極性が逆転している可能性があります。ディップスイッチの回線極性の設定を切り替えてください。

参照 BR500S ご利用にあたって「ディップスイッチの設定」（P.18）

● ISDN 公衆回線で相手先につながらない（B1/B2 ランプは一時は点灯するが、すぐ消灯する）

PPP ネゴシエーションで切断されている可能性があります。PPP フレームトレースで原因を特定できます。

【原因】 認証に失敗した。

【対処】 送信する認証 ID、認証パスワードを正しく設定し直してください。

【原因】 PPP ネゴシエーションに失敗した。

【対処】 接続先に適合するように設定を変更してください。

補足 PPP ネゴシエーションの動作に関する情報は「PPP フレームトレース情報」に記録されます。

● ISDN 公衆回線で相手先につながらない（B1/B2 ランプは点灯しているが、通信ができない）

【原因】 パソコンの設定に誤りがある。

【対処】 パソコンの経路情報や DNS サーバ IP アドレスに誤りがないか確認してください。

【原因】 本装置の経路情報の設定に誤りがある。

【対処】 本装置のダイナミックルーティングの経路情報、スタティックルーティングの経路情報を正しく設定し直してください。

【原因】 接続先が DNS サーバアドレスの通知機能を持っていない。

【対処】 接続先情報として、プロバイダから通知された DNS サーバアドレスを指定してください。

【原因】 IP フィルタによって遮断されている。

【対処】 IP フィルタの設定をやり直してください。

● フレームリレーで相手先につながらない

【原因】 本装置の設定に誤りがある。

【対処】 構成定義情報で以下の項目に誤りがないか確認してください。

- 回線の種別と速度
- IP アドレス
- 経路情報
- DNS サーバ
- DLCI

参照 BR500S Web ユーザーズガイド「2.3.10 構成定義情報を退避する／復元する」（P.113）、
BR500S コマンドユーザーズガイド「2.2.9 構成定義情報を確認する」（P.118）

【原因】 パソコンの設定に誤りがある。

【対処】 「ISDN 公衆回線で相手先につながらない（B1/B2 ランプは点灯しているが、通信ができない）」場合を参考にして、正しく設定し直してください。

【原因】 フレームリレー自体に異常がある。

【対処】 通信事業者に調査を依頼してください。

● 専用線で相手先につながらない

【原因】 パソコンの設定に誤りがある。

【対処】 「ISDN 公衆回線で相手先につながらない（B1/B2 ランプは点灯しているが、通信ができない）」場合を参考にして、正しく設定し直してください。

【原因】 専用線の回線自体に異常がある。

【対処】 通信事業者に調査を依頼してください。

● ISDN公衆回線がつながったままになっている

【原因】 接続先から定期的にデータを受信している。

【対処】 接続先からRIP、ICMP、Keep Aliveなどのパケットが送信されていないか確認してください。

【原因】 本装置の設定に誤りがある。

【対処】 構成定義情報で以下の項目に誤りがないか確認してください。

- IPアドレス
- 経路情報
- RIP送信しない／RIP受信しない

参照 BR500S Webユーザーズガイド「2.3.10 構成定義情報を退避する／復元する」（P.113）、
BR500S コマンドユーザーズガイド「2.2.9 構成定義情報を確認する」（P.118）

【原因】 ネットワーク上のコンピュータが通信している。

【対処】 コンピュータが通信していないかどうか、またアプリケーションが定期的に通信する設定になっていないかどうかを確認してください。

【原因】 回線接続中にパソコンやワークステーションが誤動作した。

【対処】 本装置の電源を切って、回線を切断してください。

● Windows NT® 4.0でネットワークにログインするたびに回線が勝手につながってしまう

【原因】 Remote Access Service（RAS）機能の設定が原因です。

【対処】 以下の手順で設定を変更してください。

1. ［スタート］－［コントロールパネル］をクリックします。
2. ［サービス］アイコンをダブルクリックして開きます。
3. 一覧から「Remote Access Autodial Manager」を選択し、［停止］ボタンをクリックします。
4. ［スタートアップ］をクリックし、「手動」か「無効」を選択します。

● Windows® 95／98で15分に1回ずつ回線が勝手につながってしまう

【原因】 Windows® 95／98が使用している通信プロトコル「NetBIOS over TCP/IP」が原因の場合があります。

【対処】 IPフィルタリング機能を使って、ポート番号137～139でのデータ通信を遮断するか、以下の手順でWindows® 95／98の設定を変更してください。

1. ［スタート］－［コントロールパネル］をクリックします。
2. ［ネットワーク］アイコンをダブルクリックして開きます。
3. TCP/IPのプロパティ画面で［バインド］タブをクリックします。
4. 「Microsoftネットワーク...」をクリックして、チェックを外します。
5. ［OK］ボタンをクリックして、ウィンドウを閉じます。
6. 画面の指示に従って、パソコンを再起動します。

● Windows® 95 からWindows® 98 にOS をアップグレードしたら、Internet Explorer でWWW ページが閲覧できなくなった

Internet Explorer の設定が「モデムを使用してインターネットに接続」になっている可能性があります。以下の手順で設定を変更してください。

1. Internet Explorer を起動します。
2. メニューバーの［ツール］をクリックします。
3. ［インターネットオプション］をクリックします。
4. ［接続］タグをクリックします。
5. 接続の設定を「LAN を使用してインターネットに接続」に変更し、［OK］ボタンをクリックして、ウィンドウを閉じます。

● Windows® のアクティブデスクトップを使用すると、ときどき回線が自動的につながってしまう

アクティブデスクトップの Internet Explorer チャンネルバーの中のサイトを「購読」する設定になっているなどの原因が考えられます。この場合は、以下の手順で設定を変更してください。

1. Internet Explorer を起動します。
2. メニューバーの［お気に入り］をクリックします。
3. ［購読の管理］をクリックします。
4. 選択されているチャンネルを削除します。

2.4 データ通信に関するトラブル

本装置でデータ通信を行う際のトラブルには、以下のようなものがあります。

● 回線はつながるが、データ通信ができない

【原因】 IP フィルタリング、NAT または経路情報（本装置／相手）の設定が間違っている。

【対処】 IP フィルタリングの設定やNAT の設定を、ご利用のネットワーク環境や目的に合わせて正しく設定し直してください。

【原因】 LAN の転送レートの自動認識に失敗した。

【対処】 本装置の 10／100BASE-TX ポート（LAN ランプ、100M ランプ、FULL ランプ）の状態と接続しているHUB 装置の LINK 状態を確認します。両者の表示が異なっている場合は自動認識に失敗しています。本装置の転送レートを HUB 装置の仕様に合わせた転送レート（100Mbps- 全二重、10Mbps- 全二重、100Mbps- 半二重、10Mbps- 半二重）に変更し、再接続してください。

● 回線は接続されて Ping の応答は正常だが、WWW ブラウザや電子メールは通信できない

【原因】 DNS の設定が間違っている。

【対処】 本装置の DHCP サーバおよび ProxyDNS を使用するか、パソコン側で DNS サーバのアドレスを正しく設定し直してください。

● ブラウザを立ち上げると勝手に回線が接続されてしまう

【原因】 ブラウザ起動時にインターネット上のページを表示するよう指定している。

【対処】 ブラウザ起動時に表示されるページに何も指定しないか、ローカルディスク上のファイルを指定してください。

● 回線は接続されるが「このサーバに対するDNS項目がありません」などメッセージが表示されてブラウザの表示が止まってしまう

【原因】 DHCPサーバ機能を利用している場合、本装置の設定終了直後はパソコン側にDNSアドレス情報が含まれていないため、WWWブラウザでURL「http://www.ntt.co.jp」を入力したときに「www.ntt.co.jp」のIPアドレスを取り出せず、このようなメッセージが表示されます。

【対処】 パソコンを再起動して、DHCP（DNSサーバのIPアドレス）の最新情報をパソコン側に確実に反映させてください。

【原因】 DHCPサーバ機能を利用していない場合、DNSサーバのIPアドレスを手入力する必要があります。

【対処】 マニュアルに記載されている情報（IPアドレス、ネットマスク、ゲートウェイ）に加え、DNSサーバのIPアドレスを設定してください。

● 本装置のIPアドレスを変更し、再起動したら、まったくつながらなくなった

【原因】 DHCPの設定が古い。

【対処】 IPアドレスを変更すると、DHCPの割り当て先頭IPアドレスが書き換わらないため、個別に設定を変更する必要があります。

● ルータ設定でIPアドレスを変更し、再起動したら、まったくつながらなくなった

【原因】 DHCPの設定が古い。

【対処】 かんたん設定の場合、IPアドレスを変更すると、連動してDHCPの割り当て先頭IPアドレスが書き換わりますが、ルータ設定の場合、連動しないため、個別に設定を変更する必要があります。以下に例を示します。

例）本装置のIPアドレスを「192.168.1.1」から「172.32.100.1」に変更した場合

	［変更前］		［変更後］	
	IPアドレス	DHCP先頭IPアドレス	IPアドレス	DHCP先頭IPアドレス
かんたん設定	192.168.1.1	192.168.1.2	172.32.100.1	172.32.100.2
ルータ設定	192.168.1.1	192.168.1.2	172.32.100.1	192.168.1.2

● PPPoEで接続できない

【原因】 前回の接続中にルータの電源を切断したり、ADSLモデムと繋がっているケーブルを抜くなどして、正常な切断処理を行わずにPPPoEセッションが切断された。

【対処】 通信事業者側のPPPoEサーバが、まだ前回の接続が切断したことを認識していない場合があります。しばらく待ってから、再度、接続してください。

【原因】 アクセスコンセントレータ名やサービス名を入力している。

【対処】 通信事業者からの指示がない限り、アクセスコンセントレータ名やサービス名を入力しないでください。

【原因】 フレッツ・ADSLの場合、ユーザ認証IDに＠以下を入力し忘れている。

【対処】 フレッツ・ADSLのユーザ認証IDは「xxx@xxx.ne.jp」や「xxx@xxx.com」のような形式を使用しています。契約しているプロバイダの指示にあわせて＠以下も入力してください。

【原因】 ADSLモデムと本装置との接続のしかたがおかしいためリンクが確立していない。

【対処】 ADSLモデムと本装置との間でリンクが確立していることを確認してください。ADSLモデムにリバーススイッチがついている場合、スイッチの設定が間違っている可能性があります。ADSLモデムの説明書に従ってスイッチを設定してください。

● ISDN接続の「かんたん設定」のあと、疎通確認のためにpingを実行したが相手からの応答がない（発信もされない）

【原因】 「かんたん設定」で設定した際、「かんたんフィルタ」がかけられたためです。「かんたんフィルタ」では、「回線が切断されているときはICMP（ping）を通さない」設定になっています。

【対処】 pingを利用する場合は、IPフィルタリングの設定で、ICMPをフィルタリング対象から外してください。

● フレッツ・ISDNを使用している環境で、回線はつながるが、一部のホームページが表示できない

【原因】 フレッツ・ISDNを使用している場合、接続地域やプロバイダによってはフレッツ・ADSLと同じ設備を経由している可能性があります。その場合、フラグメントを禁止してICMPを遮断している一部のWebサイトを表示できないことがあります。

【対処】 本装置のMSS書き換え機能を使用し、Webサーバとの間でパケット分割が起きないようにすることによって、解決する場合があります。書き換えサイズを1414バイトに設定してください。

2.5 導入に関するトラブル

ネットワークに本装置を導入する際のトラブルには、以下のようなものがあります。

● プライベートLANを構築できない

【原因】 プライベートLAN側に接続されたパソコンに固定IPアドレスが設定されている。

【対処】 本装置のDHCPサーバ機能を利用するLAN側のパソコンは、IPアドレスを自動的に取得する設定にしてください。固定のIPアドレスを設定していると、本装置が配布するIPアドレスと重なり、矛盾が生じる場合があります。
本装置のIPアドレスを変更した場合、以下の2つの操作を行ってください。

- 本装置に接続しているパソコンのIPアドレスも本装置のIPアドレスに合わせて変更する必要があります。DHCPサーバ機能を使用して、再度IPアドレスを割り当ててください。
- 再起動後に本装置にアクセスするために、telnetで指定するIPアドレスに変更後のIPアドレスを指定してください。

● インターネットへPPPoEで接続できない

【原因】 物理LANインタフェースの転送レートを含むLAN情報が保存されていない。

【対処】 PPPoEを利用する物理インタフェースのLAN情報設定で、転送レートを必ず設定してください。
転送レートが設定されずに、その他のLAN情報で設定する値もすべて初期値の場合、そのLAN情報は保存されないため、通信できません。

● IPv6の事業所LANをISDNで接続する場合に思わぬ課金が発生する

【原因】 RIP（IPv6）を送信している。

【対処】 ISDNまたはフレームリレーの場合、RIP（IPv6）を送信しないでください。
RIP（IPv6）を送信すると、思わぬ課金（定期発信または長時間接続）が発生します。

● IPv6の事業所LANをIPv6 over IPv4トンネルで接続できない

【原因】 相手情報のMTUが不適切でカプセル化されたIPv4パケットのフラグメントが発生している。

【対処】 利用する相手情報のMTUを1280に設定してください。

● 複数の事業所LANをIP-VPN網を利用して接続できない

【原因】 BGP機能とNAT機能を併用する設定になっている。

【対処】 BGP機能とNAT機能は併用できません。NAT機能の設定を変更してください。
初期設定で、NAT機能を使用する設定になっています。

2.6 IPsec/IKE に関するトラブル

IPsec/IKE 通信を行う際のトラブルには、以下のようなものがあります。

● IPsec/IKE 定義を複数行うと接続できない拠点がある

【原因】 各拠点の装置または相手情報のネットワーク情報（接続先情報）が複数定義されている装置の IPsec 情報の対象パケットが他拠点と重なっている。

【対処】 相手情報のネットワーク情報（接続先情報）で自側／相手側エンドポイントが各拠点で誤りがないか確認してください。また、相手情報のネットワーク情報（接続先情報）が複数定義されている装置の IPsec 情報の対象パケットが重ならないようにしてください。

【原因】 可変 IP アドレスの VPN 接続で、Responder（相手装置が可変 IP アドレス）の定義をしている装置の各拠点の相手情報のネットワーク情報（接続先情報）の相手装置識別情報が重複している。

【対処】 相手情報のネットワーク情報（接続先情報）の相手装置識別情報が異なるように設定してください。

● IKE ネゴシエーションの LifeTime が互いに異なる

【原因】 相手情報のネットワーク情報（接続先情報）の IKE 情報または IPsec 情報の SA 有効時間が装置間で異なっている。

【対処】 互いの装置の定義を確認して相手情報のネットワーク情報（接続先情報）の IKE 情報または IPsec 情報の SA 有効時間を合わせてください。

● Aggressive Mode 設定を行っても IKE ネゴシエーションが開始されない

【原因】 可変 IP アドレスの VPN 接続で Responder（相手装置が可変 IP アドレス）の定義をしている装置から IKE ネゴシエーションを開始しようとしている。

【対処】 Initiator（自装置が可変 IP アドレス）の定義をしている装置から IPsec 対象となる装置に対し ping などの疎通確認により、IKE ネゴシエーションを開始するように設定してください。

● IPsec SA が存在するのに IKE セッション監視パケットが暗号化されない

【原因】 相手情報のネットワーク情報（接続先情報）の IPsec 情報の対象パケットに LAN 情報（IP 関連）の IP アドレスが含まれていない。

【対処】 相手情報のネットワーク情報（接続先情報）の IPsec 情報の対象パケットに LAN 情報（IP 関連）の IP アドレスが含まれるように設定してください。

● IPsec SA が存在するのに IKE セッション監視がダウンした

【原因】 監視先装置がネットワークに接続されていない。

【対処】 監視先装置をネットワークに接続するか、すでに接続されている装置を指定してください。

【原因】 IKE セッション監視パケットの応答経路が監視先装置にない。

【対処】 経路を設定してください。

【原因】 通信負荷が高い、または回線品質が悪い。

【対処】 IKE セッション監視パケットが最優先されるように、相手情報のネットワーク情報（接続先情報）の帯域制御情報（IP 関連）を設定してください。

● IPsec SA が存在するのに接続先セッション監視がダウンした

【原因】 監視先装置がネットワークに接続されていない。

【対処】 監視先装置をネットワークに接続するか、すでに接続されている装置を指定してください。

【原因】 接続先セッション監視パケットの応答経路が監視先装置にない。

【対処】 経路を設定してください。

【原因】 通信負荷が高い、または回線品質が悪い。

【対処】 接続先セッション監視パケットが最優先されるように、相手情報のネットワーク情報（接続先情報）の帯域制御情報（IP 関連）を設定してください。

● IPsec SAは存在するが、IKE SAが存在しない

【原因】 相手IKEセッションから削除ペイロードを受信した。

【対処】 対処の必要はありません。次回のIPsec SAの更新（Rekey）時にIKE SAが作成されます。

【原因】 IPsec SAが存在するときにIKE SAがSA有効時間を満了して解放された。

【対処】 対処の必要はありません。次回のIPsec SAの更新（Rekey）時にIKE SAが作成されます。

● IKEネゴシエーション後に同一相手にもかかわらず複数のIPsec SAおよびIKE SAが作成される

【原因】 相手IKEセッションとIPsec SAの更新（Rekey開始）時間が同じ。

【対処】 相手情報のネットワーク情報（接続先情報）のIPsec情報のSA更新（Initiator時／Responder時）を装置間で異なるように設定してください。

● IPsec化される前の帯域制御が行われない

【原因】 IPsec/IKE接続定義をしている相手情報のネットワーク情報（共通情報）でシェーピングが設定されていない。

【対処】 IPsec/IKE接続定義をしている相手情報のネットワーク情報（共通情報）でシェーピングを設定してください。
使用する回線がLANの場合はシェーピングを使用すると帯域制御機能が有効に動作します。

【原因】 相手情報のネットワーク情報（接続先情報）の帯域制御情報（IP関連）の対象範囲が相手情報のネットワーク情報（接続先情報）のIPsec情報の対象パケットに含まれていない。

【対処】 相手情報のネットワーク情報（接続先情報）の帯域制御情報（IP関連）の対象範囲が相手情報のネットワーク情報（接続先情報）のIPsec情報の対象パケットに含まれるように設定してください。

● 手動鍵設定でIPsec通信ができない

【原因】 自装置の手動鍵送信用IPsec情報のセキュリティパラメタインデックスのSPIと相手装置の手動鍵受信用IPsec情報のSPI、または自装置の手動鍵受信用IPsec情報のSPIと相手装置の手動鍵送信用IPsec情報のSPIが一致していない。

【対処】 自装置の手動鍵送信用IPsec情報のSPIと相手装置の手動鍵受信用IPsec情報のSPI、または自装置の手動鍵受信用IPsec情報のSPIと相手装置の手動鍵送信用IPsec情報のSPIを合わせてください。

【原因】 自装置の手動鍵送信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵受信用IPsec情報のセキュリティプロトコル、または自装置の手動鍵受信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵送信用IPsec情報のセキュリティプロトコルが一致していない。

【対処】 自装置の手動鍵送信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵受信用IPsec情報のセキュリティプロトコル、または自装置の手動鍵受信用IPsec情報のセキュリティプロトコルと相手装置の手動鍵送信用IPsec情報のセキュリティプロトコルを合わせてください。

【原因】 自装置の手動鍵送信用IPsec情報の対象範囲と相手装置の手動鍵受信用IPsec情報の対象範囲、または自装置の手動鍵受信用IPsec情報の対象範囲と相手装置の手動鍵送信用IPsec情報の対象範囲が一致していない。

【対処】 自装置の手動鍵送信用IPsec情報の対象範囲と相手装置の手動鍵受信用IPsec情報の対象範囲、または自装置の手動鍵受信用IPsec情報の対象範囲と相手装置の手動鍵送信用IPsec情報の対象範囲を合わせてください。

【原因】 自装置の手動鍵送信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵受信用IPsec情報の暗号情報／認証情報、または自装置の手動鍵受信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵送信用IPsec情報の暗号情報／認証情報が一致していない。

【対処】 自装置の手動鍵送信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵受信用IPsec情報の暗号情報／認証情報、または自装置の手動鍵受信用IPsec情報の暗号情報／認証情報と相手装置の手動鍵送信用IPsec情報の暗号情報／認証情報を合わせてください。鍵には、文字列鍵と16進数鍵があるので注意してください。

【原因】 トンネル利用時の自側／相手側のトンネルエンドポイントアドレス（IPsec トンネル）パケットが手動鍵送受信用 IPsec 情報の対象範囲パケットと同じインタフェースから送受信するようになっている。

【対処】 IPsec トンネルパケットと手動鍵送受信用 IPsec 情報の対象範囲パケットが別のインタフェースから送受信するように設定してください。

● IKE ネゴシエーション後に同一相手にかかわらず複数の IPsec SA および IKE SA が作成される

【原因】 互いの装置から同時に IKE ネゴシエーションが行われた。

【対処】 対処の必要はありません。次回の IPsec SA の更新（Rekey）および IPsec 通信に影響はありません。

● 手動鍵設定の暗号アルゴリズムが互いの装置で des-cbc と 3des-cbc の場合にもかかわらず IPsec 通信できた

【原因】 3des-cbc の暗号鍵を 16 桁ごとに 3 つに分割した鍵が、des-cbc の暗号鍵と同じ鍵になっている。

【対処】 アルゴリズムは、トンネルの往路または復路で同じものを設定してください。また、暗号アルゴリズムに 3des を選択する場合は、以下のように鍵を 16 桁ごとに 3 つに分割し、鍵 1 ≠鍵 2 ≠鍵 3 となるように鍵を設定してください。

鍵 :1122334455667788　9900aabbccddeeff　1122334455667788

鍵 1（16 桁）　鍵 2（16 桁）　鍵 3（16 桁）

鍵 1 ＝鍵 3 のように鍵を設定すると、16 バイトの鍵で暗号化するのと同じ結果になります。また、鍵 1 ＝鍵 2、鍵 2 ＝鍵 3 のように鍵を設定すると、それぞれ鍵 3、鍵 1 の des-cbc 暗号と同じ結果になります（鍵 1 ＝鍵 2 ＝鍵 3 の場合も同様です）。

IPsec 設定ミス　トラブルシュート方法

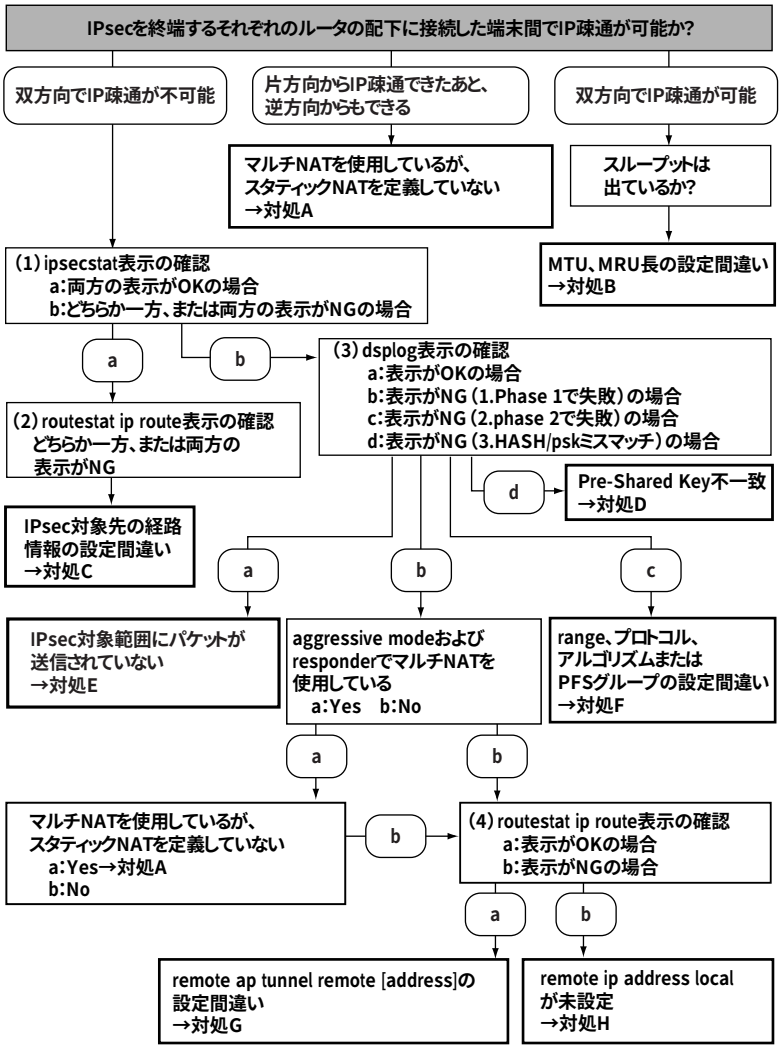
IPsecの設定ミスの原因と対処を、以下のフローチャートで特定してください。

フローチャート内の（1）～（4）は「ログ表示の確認」（P.23）の（1）～（4）に対応しています。各項目のOK表示例およびNG表示例を確認し、a～dのあてはまる項目へ進みます。

また、対処A～Hは「対処方法」（P.28）の対処A～Hに対応しています。

こんな事に気をつけて

ここで解説しているトラブルシュート方法は、IPsec接続に限定した記述であり、PPPoE接続などの下位レイヤ接続はすでに確立していることを前提としています。また、接続携帯や構成により接続できない原因は多様であるため、設定ミスの特定もあくまでミスの可能性を示すものであり、必ずしも断定的なものではありません。



ログ表示の確認

ログのOK表示例とNG表示例を、フローチャート内の（1）～（4）の順に説明します。

IPsecを終端しているそれぞれのルータで確認してください。

（1）ipsecstat表示を確認

OKの場合の表示例

IPsec SAがIN、OUTそれぞれ1つ以上、IKE SAが1つ以上表示される。

```
# ipsecstat
[IPsec SA Information]
[1]     Destination(192.168.2.1/24), Source(192.168.1.1/24), rmt1, ap0
        Side(Initiator), Gateway(10.1.1.1,10.1.2.1), OUT
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=6446374488(0x03d7a380)
        Created(Jan  1 08:47:17 GMT), NewSA(28710secs, 0Kbyte)
        Lifetime(28800secs), Current(242secs), Remain(28558secs)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[2]     Destination(192.168.1.1/24), Source(192.168.2.1/24), rmt1, ap0
        Side(Initiator), Gateway(10.1.2.1, 10.1.1.1), IN
        Protocol(ESP), Enctype(des-cbc), Authtype(hmac-md5), PFS(modp768)
        Status(mature), Spi=176237763(0x0a812cc3)
        Created(Jan  1 08:47:17 GMT), NewSA(28710secs, 0Kbyte)
        Lifetime(28800secs), Current(242secs), Remain(28558secs)
        Lifebyte(0Kbyte), Current(1Kbyte), Remain(0Kbyte)

[IKE SA Information]
[1]     Destination(10.1.1.1.500), Source(10.1.2.1.500), rmt1
        Cookies(b9d8faf6fd0f3432:0f04db45d410b1b3)
        Side(Initiator), Status(ESTABLISHED), Exchangetype(MAIN)
        Enctype(des-cbc), Hashtype(hmac-md5), PFS(modp768)
        Created(Jan  1 08:47:15 GMT)
        Lifetime(86400secs), Current(244secs), Remain(86156secs)

#
```

NGの場合の表示例

- IPsec SAが表示されない、およびIKE SAが1つだけ表示され、Cookiesの後半がすべて0となっている。

```
# ipsecstat
[IKE SA Information]
[1]     Destination(10.1.2.1.500), Source(10.1.1.1.500), rmt1
        Cookies(bd86fa3dfcb1a389:0000000000000000)
        Side(Initiator), Status(MSG1SENT), Exchangetype(MAIN)
        Enctype( ), Hashtype( ), PFS( )
        Created( )
        Lifetime(0secs), Current(0secs), Remain(0secs)

#
#ipsecstat
#
```

- IPsecSA、IKE SAともに何も表示されない。

(2)routestat ip route 表示の確認

OKの場合の表示例

IPsec通信対象のあて先ネットワークアドレスが、IPsecインタフェースに向いている。

以下の例では、IPsecインタフェースはremote 1であり、IPsec対象である対向ルータLAN側ネットワークアドレス192.168.2.0/24がスタティックで有効になっている。

```
# routestat ip route
Codes: C - connected, S - static, R - RIP, B - BGP, O - OSPF,
           > - selected route, * - FIB route

S> * default [0/1] is directly connected, rmt0
C> * unnumbered is directly connected, rmt0
    *                  is directly connected, rmt1
C> * 10.1.1.1/32 is directly connected, rmt0
C> * 192.168.1.0/24 is directly connected, lan1
S> * 192.168.2.0/24 [0/1] via rmt1
Total Routing Tables   2
#
```

NGの場合の表示例

IPsec通信対象のあて先ネットワークアドレスが、IPsecインタフェースに向いていない。

以下の例では、IPsecインタフェースはremote 1であり、IPsec対象のあて先は対向ルータLAN側ネットワークアドレス192.168.2.0/24であるが、デフォルトルートに一致するためremote 0のPPPoEインタフェースにルーティングされる（IPsec暗号化されない）。

```
# routestat ip route
Codes: C - connected, S - static, R - RIP, B - BGP, O - OSPF,
           > - selected route, * - FIB route

S>*default[0/1]is directly connected, rmt0
C>*unnumbered is directly connected, rmt0
  *         is directly connected, rmt1
C>*10.1.1.1/32 is directly connected, rmt0
C>*192.168.1.0/24 is directly connected, lan1
Total Routing Tables  2
#
```

(3)dsplog 表示の確認

OKの場合の表示例

以下のようにIPsec/IKE関連のメッセージが表示されない。

```
# dsplog
Mar 08 06:59:52 init: system startup now.
Mar 08 06:59:52 protocol: [mb/0] lan port link down
Mar 08 06:59:52 protocol: [mb/1] lan port link down
Mar 08 06:59:52 protocol: [mb/0] lan port link up
Mar 08 06:59:52 protocol: [lan0] connected to PPPoE.pppoe() by keep connection
#
```

NGの場合の表示例

1.phase 1 で失敗

表示内に“**isakmp:give up phase1 negotiation.**”が表示されている。

ただし、“isakmp:HASH mismatched”または“isakmp:psk mismatched”が表示されている場合は「3.HASH/pskミスマッチ」（P.26）を参照してください。

```
# dsplog
Jan 01 09:23:53 init: system startup now.
Jan 01 09:23:53 protocol: [mb/0] lan port link down
Jan 01 09:23:53 protocol: [mb/1] lan port link down
Jan 01 09:23:53 protocol: [mb/0] lan port link up
Jan 01 09:23:53 protocol: [mb/1] lan port link up
Jan 01 09:23:53 protocol: [lan0] connected to PPPoE.pppoe() by keep connection
Jan 01 09:25:04 isakmp: give up phase1 negotiation. 10.1.2.1->10.1.1.1
#
```

2.phase 2 で失敗

表示内に“**isakmp: give up phase2 negotiation.**”が表示されている。

Initiator

```
# dsplog
Apr 28 14:31:29 init: system startup now.
Apr 28 14:31:29 protocol: [mb/0] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link up
Apr 28 14:32:24 isakmp: give up phase2 negotiation. 1.1.1.1 -> 1.1.1.2
#
```

Responder

- range間違いは、syslogの出力はない

```
# dsplog
Apr 28 14:31:29 init: system startup now.
Apr 28 14:31:29 protocol: [mb/0] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link up
#
```

- プロトコル間違いは、syslogの出力はない

```
# dsplog
Apr 28 14:31:29 init: system startup now.
Apr 28 14:31:29 protocol: [mb/0] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link up
#
```

- 暗号アルゴリズム間違い

```
# dsplog
Apr 28 14:31:29 init: system startup now.
Apr 28 14:31:29 protocol: [mb/0] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link up
Apr 28 14:34:04 isakmp: IPsec SA encryption algorithm mismatched.
Apr 28 14:34:14 isakmp: IPsec SA encryption algorithm mismatched.
#
```

- 認証アルゴリズム間違い

```
# dsplog
Apr 28 14:31:29 init: system startup now.
Apr 28 14:31:29 protocol: [mb/0] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link up
Apr 28 14:35:32 isakmp: IPsec SA authentication algorithm mismatched.
Apr 28 14:35:42 isakmp: IPsec SA authentication algorithm mismatched.
#
```

- PFS グループ間違い

```
# dsplog
Apr 28 14:31:29 init: system startup now.
Apr 28 14:31:29 protocol: [mb/0] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link down
Apr 28 14:31:29 protocol: [mb/1] lan port link up
Apr 28 14:32:00 isakmp: IPsec SA pfs group mismatched.
Apr 28 14:32:10 isakmp: IPsec SA pfs group mismatched.
#
```

3.HASH/psk ミスマッチ

HASH mismatch、psk mismatch は、Aggressive Mode の場合 Initiator で、Main Mode の場合 Responder で確認する。どちらも結果的には Phase 1 で失敗となる。

- Aggressive Mode Initiator の場合、以下の太字行に、受信した HASH 値と受信パケットから生成した HASH 値が一致しないことを示すメッセージが表示されている。

```
# dsplog
Jan 01 04:35:36 init: system startup now.
Jan 01 04:35:36 protocol: [mb/0] lan port link down
Jan 01 04:35:36 protocol: [mb/1] lan port link down
Jan 01 04:35:36 protocol: [mb/0] lan port link up
Jan 01 04:35:36 protocol: [mb/1] lan port link up
Jan 01 04:35:36 logon: logon console
Jan 01 04:35:36 protocol: [lan0] connected to PPPoE.pppoe() by keep connection
Jan 01 04:35:37 isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:35:46 isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:36:01 isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:36:21 isakmp: HASH mismatched side=0 exchange type=4 status=3.
Jan 01 04:36:30 isakmp: give up phase1 negotiation.BR500S->10.1.1.2
#
```

- Main Mode Responder の場合、以下の太字行に共有鍵が一致していない可能性があることを示すメッセージが表示されている。

```
# dsplog
Apr 20 17:29:59 init: system startup now.
Apr 20 17:29:59 protocol: [mb/0] lan port link down
Apr 20 17:29:59 protocol: [mb/1] lan port link down
Apr 20 17:29:59 protocol: [mb/0] lan port link up
Apr 20 17:29:59 protocol: [lan0] connected to PPPoE.pppoe() by keep connection
Apr 20 17:50:14 isakmp: psk mismatched.
Apr 20 17:50:24 isakmp: psk mismatched.
Apr 20 17:50:42 isakmp: psk mismatched.
Apr 20 17:51:03 isakmp: psk mismatched.
Apr 20 17:51:09 isakmp: give up phase1 negotiation. 10.1.2.1->10.1.1.1
#
```

(4)routestat ip route 表示の確認

OK の場合の表示例

自側 IPsec トンネルエンドポイントのアドレス（ホストアドレス）が該当インタフェースに向いている。

以下の例では、10.1.1.1/32 が PPPoE インタフェース remote 0 で有効になっている。

```
# routestat ip route
Codes: C - connected, S - static, R - RIP, B - BGP, O - OSPF,
           > - selected route, * - FIB route

S> * default [0/1] is directly connected, rmt0
C> * unnumbered is directly connected, rmt0
    *       is directly connected, rmt1
C> * 10.1.1.1/32 is directly connected, rmt0
C> * 192.168.1.0/24 is directly connected, lan1
S> * 192.168.2.0/24 [0/1] via rmt1
Total Routing Tables 2
#
```

NG の場合の表示例

自側 IPsec トンネルエンドポイントのアドレス（ホストアドレス）が該当インタフェースに向いていない。

以下の例では、自側エンドポイントアドレスは 10.1.1.1 であるが、表示されていない。

ただし、可変 IP アドレスでの Aggressive Mode の Initiatior の場合は、以下の表示でも問題ない。

```
# routestat ip route
Codes: C - connected, S - static, R - RIP, B - BGP, O - OSPF,
           > - selected route, * - FIB route

S> * default [0/1] is directly connected, rmt0
C> * unnumbered is directly connected, rmt0
    *       is directly connected, rmt1
C> * 192.168.1.0/24 is directly connected, lan1
S> * 192.168.2.0/24 [0/1] via rmt1
Total Routing Tables 2
#
```

対処方法

フローチャート内の対処 A～H について、以下に説明します。

対処に合わせて設定を変更してください。なお、コマンド内の（本文）は表示されません。

- マルチ NAT を使用しているが、スタティック NAT を定義していない→【対処 A】（P.28）
- MTU、MRU 長の設定間違い→【対処 B】（P.29）
- IPsec 対象先の経路情報の設定間違い→【対処 C】（P.30）
- Pre-Shared Key 不一致→【対処 D】（P.30）
- IPsec 対象範囲にパケットが送信されていない→【対処 E】（P.31）
- range、プロトコル、アルゴリズムまたは PFS グループの設定間違い→【対処 F】（P.31）
- remote ap tunnel remote [address] の設定間違い→【対処 G】（P.31）
- remote ip address local が未設定→【対処 H】（P.32）

【対処 A】

インターネット VPN などで、IPsec 通信のほかにインターネット上のサーバなどと通信する場合、マルチ NAT 機能を使用する必要があります。マルチ NAT 機能を使用して、VPN で使用するアドレスが NAT のアドレスプールに含まれる場合は、スタティック NAT を指定してください。これは IPsec 通信に用いられるアドレスが変換されてしまうのを防ぐためです。

設定例

Aggressive Mode Initiator PPPoE で割り当てられる可変アドレスでの VPN の場合

```
# lan 0 mode auto
# lan 1 ip address 192.168.2.1/24 3
# remote 0 name ISP
# remote 0 mtu 1454
# remote 0 ap 0 name isp
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send BR2 BR2
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
（NAT を使用する場合は以下のスタティック NAT が設定されているか確認する）
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17 ESP(IP:50)
# remote 0 ip nat static 1 192.168.2.1 any any any 50 IKE(UDP:500)
# remote 0 ip msschange 1414
# remote 1 name BR
# remote 1 ap 0 name BR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local BR500S
# remote 1 ap 0 ike shared key text BR500S
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
# remote 1 ap 0 ike initial connect
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch 192.168.2.1 192.168.1.1 10s 1m 5s 1s 255
# remote 1 ip route 0 192.168.1.0/24 1 1
```

Aggressive Mode では Initiator だけがマルチ NAT 機能だけを使用しているのであれば、IPsec SA 自体は確立できますが、その後 Responder から IPsec パケットを送信しなければ NAT テーブルが作成されず、通信できません。Responder でマルチ NAT 機能だけを使用していると IPsec SA も確立されません。

Main Modeでは IKE のネゴシエーションを双方から開始するので、マルチ NAT 機能だけを使用していても IPsec SA は確立されます。ただし、IPsec 通信は NAT テーブルが双方に作成されるまで不可能となります。

【対処 B】

フレッツ ADSL をアクセス回線としてインターネットに接続する場合、PPPoE ヘッダと PPP ヘッダが付加されるため、それを見積もった MTU/MSS を設定してください。PPPoE を設定しているインタフェースで、MTU=1454、MSS=1414 に設定していないと、通信がうまくいかなかったり、パケット分割して送信するため通常よりスループットが出ない場合があります。

設定例

```
# lan 0 mode auto
# lan 1 ip address 192.168.2.1/24 3
# remote 0 name ISP
（以下の設定がされているか確認する）
# remote 0 mtu 1454
# remote 0 ap 0 name isp
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send BR2 BR2
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
（以下の設定がされているか確認する）
# remote 0 ip msschange 1414
# remote 1 name BR
# remote 1 ap 0 name BR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local BR500S
# remote 1 ap 0 ike shared key text BR500S
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
# remote 1 ap 0 ike initial connect
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch 192.168.2.1 192.168.1.1 10s 1m 5s 1s 255
# remote 1 ip route 0 192.168.1.0/24 1 1
```

【対処 C】

IPsec対象先のネットワークアドレスが、IPsecインタフェースに向いていないため、IPsec 対象先の経路情報を設定してください。

設定例

```
# routestat ip route
Codes: C - connected, S - static, R - RIP, B - BGP, O - OSPF,
           > - selected route, * - FIB route

S> * default [0/1] is directly connected, rmt0
C> * unnumbered is directly connected, rmt0
    *                   is directly connected, rmt1
C> * 10.1.1.1/32 is directly connected, rmt0
C> * 192.168.1.0/24 is directly connected, lan1
S> * 192.168.2.0/24 [0/1] via rmt1
Total Routing Tables   2
#
```

【対処 D】

Pre-Shared Key認証はIKEの認証方式で、IKEの相手と同じ秘密鍵を生成し、それを元にHASH計算した値を交換することにより、認証を行います。これはPhase 1で行われるので、本装置に設定したPre-Shared Keyが異なればPhase 1のIKEネゴシエーションで失敗します。必ずそれぞれのIPsec終端ルータで同じ鍵を設定してください。

設定例

```
# lan 0 mode auto
# lan 1 ip address 192.168.2.1/24 3
# remote 0 name ISP
# remote 0 mtu 1454
# remote 0 ap 0 name isp
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send BR2 BR2
# remote 0 ip route 0 default 1 0
# remote 0 ip nat mode multi any 1 5m
# remote 0 ip nat static 0 192.168.2.1 500 any 500 17
# remote 0 ip nat static 1 192.168.2.1 any any any 50
# remote 0 ip msschange 1414
# remote 1 name BR
# remote 1 ap 0 name BR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local BR500S
（以下の設定が対向ルータと合っているか確認する）
# remote 1 ap 0 ike shared key text BR500S
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
# remote 1 ap 0 ike initial connect
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch 192.168.2.1 192.168.1.1 10s 1m 5s 1s 255
# remote 1 ip route 0 192.168.1.0/24 1 1
```

【対処 E】

IPsec/IKE 関連のメッセージが表示されない場合、IKE ネゴシエーションの送受信が行われていません。IPsec 対象範囲にパケットが送信されているか確認してください。

設定例

送信元アドレスが 192.168.1.0/24 のネットワーク内である場合

```
# remote 0 ap 0 ipsec ike range 192.168.1.0/24 any4
```

【対処 F】

IKE ネゴシエーションでは phase 2 で互いの IPsec 暗号化対象ネットワークアドレス（range）の交換を行います。それぞれの IPsec 終端ルータで送信元、あて先を逆に設定してください。

以下の設定では IPsec SA が確立できません。

```
ルータ A
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
ルータ B
# remote 1 ap 0 ipsec ike range 192.168.2.0/24 any4
```

以下の設定のように変更してください。

```
ルータ A
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 192.168.2.0/24
ルータ B
# remote 1 ap 0 ipsec ike range 192.168.2.0/24 192.168.1.0/24
```

```
ルータ A
# remote 1 ap 0 ipsec ike range 192.168.1.0/24 any4
ルータ B
# remote 1 ap 0 ipsec ike range any4 192.168.1.0/24
```

```
ルータ A
# remote 1 ap 0 ipsec ike range any4 any4
ルータ B
# remote 1 ap 0 ipsec ike range any4 any4
```

設定例

```
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec ike protocol esp
（以下の部分の設定が IPsec 対象先と矛盾していないか確認する）
# remote 1 ap 0 ipsec ike range 192.168.2.0/24 any4
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ipsec type ike
```

【対処 G】

IPsec を終端する対向ルータの IP アドレス（トンネルエンドポイント）を設定してください。以下のように、モードによって必要な設定が異なる場合があります。

- Aggressive Mode の場合

  Initiator remote ap tunnel remote の設定

  Responder remote ap tunnel local の設定

- Main Modeの場合

  両方にremote ap tunnel local、remote ap tunnel remoteの設定

設定例

```
# remote 1 name BR
# remote 1 ap 0 name BR
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt 3des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ipsec ike pfs modp768
# remote 1 ap 0 ike name local BR500S
# remote 1 ap 0 ike shared key text BR500S
# remote 1 ap 0 ike proposal 0 encrypt 3des-cbc
# remote 1 ap 0 ike initial connect
（以下の設定がきちんとされているか確認する）
# remote 1 ap 0 tunnel remote 10.1.1.1
# remote 1 ap 0 sessionwatch 192.168.2.1 192.168.1.1 10s 1m 5s 1s 255
# remote 1 ip route 0 192.168.1.0/24 1 1
```

【対処 H】

Main Modeの双方とAggressive ModeのResponderで、必ずPPPoEインタフェースなどの、IPsecで暗号化されたパケットが送出されるように、インタフェースを設定してください。これはほとんどの場合（IPsecトンネルの途中にNAT変換機器などが存在する場合を除く）、自側トンネルエンドポイントと同じアドレスが設定されます。

設定例

```
# lan 0 mode auto
# lan 1 mode auto
# lan 1 ip address 192.168.1.1/24 3
# remote 0 name ISP-1
# remote 0 mtu 1454
# remote 0 ap 0 name ISP-1
# remote 0 ap 0 datalink bind lan 0
# remote 0 ap 0 ppp auth send nttA nttA
# remote 0 ap 0 keep connect
（Main Modeの場合、remote 1 ap 0 tunnel local で設定するアドレスが自インタフェースに設定されているか確認する）
# remote 0 ip address local 10.1.1.1
# remote 0 ip route 0 192.168.2.1/32 1 0
# remote 0 ip msschange 1414
# remote 1 name A-10
# remote 1 ap 0 name VPN-10
# remote 1 ap 0 datalink type ipsec
# remote 1 ap 0 ipsec type ike
# remote 1 ap 0 ipsec ike protocol esp
# remote 1 ap 0 ipsec ike encrypt des-cbc
# remote 1 ap 0 ipsec ike auth hmac-md5
# remote 1 ap 0 ike mode main
# remote 1 ap 0 ike shared key text vpn10
# remote 1 ap 0 ike proposal 0 encrypt des-cbc
# remote 1 ap 0 ike initial connect
# remote 1 ap 0 tunnel local 10.1.1.1
# remote 1 ap 0 tunnel remote 10.1.1.2
# remote 1 ap 0 sessionwatch 192.168.1.1 192.168.2.1 10s 3m 5s 1s 255
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ip msschange 1414
```

2.7 MPLS に関するトラブル

MPLS 通信を行う際のトラブルには、以下のようなものがあります。

● 隣接 LSR と LDP のセッションが確立できない

【原因】 IPv4 Transport Address に対応する経路が存在しない可能性があります。

【対処】 IPv4 Transport Address の設定を行った場合は、隣接 LSR となる装置にそのアドレスに対する経路情報が必要です。経路情報の設定を見直してください。

2.8 VoIP NAT トラバーサルに関するトラブル

VoIP NAT トラバーサル機能を使用して通信を行う際のトラブルには、以下のようなものがあります。

● VoIP アダプタを接続しても VoIP ランプが点灯せず通話できない

【原因】 VoIP アダプタの設定で、UPnP 機能を使用しないようになっている。

【対処】 VoIP アダプタの設定で、UPnP 機能を使用するようにしてください。

【原因】 VoIP アダプタの設定内容に問題がある。

【対処】 VoIP アダプタに設定した、ユーザ認証情報、VoIP サーバアドレス、電話番号などの設定内容が正しいか確認してください。

【原因】 本装置の設定で、VoIP NAT トラバーサル機能（UPnP 機能）を使用しないようになっている。

【対処】 本装置の設定で、VoIP NAT トラバーサル機能（UPnP 機能）を使用するようにしてください。

【原因】 VoIP アダプタを本装置に接続するポートに問題がある。

【対処】 VoIP アダプタは、NAT 機能を使用しない LAN のポートに接続してください。

【原因】 VoIP サーバ（インターネット回線）を本装置に接続するポートに問題がある。

【対処】 VoIP サーバ（インターネット回線）は、NAT 機能を使用する一番小さな定義番号の lan ポートに接続してください。該当ポートがない場合は、一番小さな定義番号の remote ポートに接続してください。

● パソコンに本装置を接続すると本装置のアイコンが自動的に表示されてしまう

【原因】 パソコンの OS が Microsoft® Windows® Me または Microsoft® Windows® XP である。

【対処】 Microsoft® Windows® Me と Microsoft® Windows® XP は、標準で UPnP 機能をサポートしています。このため、本装置に接続するとマイネットワークやタスクトレイに本装置のアイコンが表示され、ダブルクリックすると本装置の Web 設定画面が表示されます。

● パソコンに本装置のアイコンが自動的に表示されない

【原因】 パソコンの OS が Microsoft® Windows® Me または Windows® XP 以外である。

【対処】 Windows® 95、WIndows® 98/SE、Linux、FreeBSD などの OS では、UPnP 機能をサポートしていないため、パソコンの画面上に本装置のアイコンは表示されません。

【原因】 パソコンのOSがMicrosoft® Windows® XPで、UPnP機能が有効になっていない。

【対処】 以下の手順で、Microsoft® Windows® XPのUPnP機能を有効にしてください。

1.［スタート］－［コントロールパネル］をクリックします。
2.「ネットワークとインターネット接続」をクリックします。
3.「ネットワーク接続」をクリックします。
4. メニューバーの「詳細設定」をクリックし、「オプションネットワークコンポーネント」をクリックします。
5.「コンポーネント」－「ネットワークサービス」を選択し、［詳細］ボタンをクリックします。
6.「ネットワークサービスのサブコンポーネント」－「ユニバーサルプラグアンドプレイ」をチェックし、［OK］ボタンをクリックします。

以降の操作は、画面の指示に従ってください。なお、Windows® XPのインストールCD-ROMをセットするよう指示される場合があります。

【原因】 パソコンのOSがMicrosoft® Windows® Meで、UPnP機能が有効になっていない。

【対処】 以下の手順で、Microsoft® Windows® MeのUPnP機能を有効にしてください。

1.［スタート］－［設定］－［コントロールパネル］をクリックします。
2.「アプリケーションの追加と削除」アイコンをダブルクリックして開きます。
3.「Windowsファイル」タブをクリックします。
4.「通信」を選択し、［詳細］ボタンをクリックします。
5.「コンポーネントの種類」－「ユニバーサルプラグアンドプレイ」をチェックし、［OK］ボタンをクリックします。

以降の操作は、画面の指示に従ってください。なお、Windows® MeのインストールCD-ROMをセットするよう指示される場合があります。

2.9 SNMPに関するトラブル

SNMP機能でネットワークの管理を行う際のトラブルには、以下のようなものがあります。

● SNMPマネージャと通信ができない

【原因】 エージェントアドレスが正しく設定されていない。

【対処】 エージェントアドレスに本装置のインタフェースのアドレスのどれかを設定してください。

2.10 VRRPに関するトラブル

VRRP機能を利用する際のトラブルには、以下のようなものがあります。

● VRRPグループが開始しない

【原因】 仮想IPが、装置に設定されたIPアドレスのどれかと同一である。

【対処】 仮想IPは、端末のIPアドレスのサブネットに一致し、装置に設定されたIPアドレスとは異なるアドレスを指定してください。

【原因】 装置内にVRIDが重複して設定されている。

【対処】 装置内でVRIDは一意である必要があります。異なるVRIDを設定してください。

● VRRPルータがマスタ状態となったのに通信不能となる

【原因】 仮想IPが、端末のIPアドレスのサブネットに一致するIPアドレスではない。

【対処】 仮想IPを端末のIPアドレスのサブネットに一致するよう変更してください。

【原因】 仮想IPと同一のIPアドレスである装置が接続されている。

【対処】 仮想IPと同一のIPアドレスである装置のIPアドレスを変更してください。

【原因】 マスタ以外で、仮想IPを解決するARPリクエストに応答する装置が存在する。

【対処】 仮想IPを解決するARPリクエストに応答する装置の設定を応答しないように変更してください。

● プリエンプトモードoffに設定しても自動で切り戻る

【原因】 優先度が低い設定のVRRPルータにプリエンプトモードoffを指定している。

【対処】 優先度が高い設定のVRRPルータにプリエンプトモードoffを指定してください。

【原因】 優先度にマスタを指定している。

【対処】 優先度にマスタ以外を指定してください。

補足 Web設定では「プライオリティ」設定項目のマスタ（255）選択が該当します。
バックアップを選択して、優先度に値を指定してください（例:254）。

【原因】 VRRPグループが開始してからプリエンプトモード移行禁止時間が経過していない。

【対処】 プリエンプトモード移行禁止時間中はプリエンプトモードonが指定されている場合と同じ動作となり、対処の必要はありません。

● 手動切り戻しできない

【原因】 マスタ状態のVRRPルータで手動切り戻しを実行している。

【対処】 バックアップ状態（本来のマスタ）のVRRPルータで手動切り戻しを実行してください。

参照 BR500S コマンドユーザーズガイド「2.1.5 VRRP手動切り戻し機能を使う」（P.24）
BR500S Webユーザーズガイド「2.1.7 VRRP手動切り戻し機能を使う」（P.22）

【原因】 バックアップ状態ではあるが、現在の優先度が現在のマスタ状態のVRRPルータより低い。

【対処】 バックアップ状態であるにもかかわらず切り戻らない場合は、VRRP情報を表示して現在の優先度、およびダウントリガ発動状態を確認してください。
ダウントリガが発動している場合は、ダウントリガが発動している原因を除去してください。

参照 BR500S コマンドユーザーズガイド「2.1.29 VRRP情報を確認する」（P.87）
BR500S Webユーザーズガイド「2.2.24 VRRP情報を確認する」（P.79）

【原因】 優先度が高い設定のVRRPルータにプリエンプトモードoffを指定していない。

【対処】 優先度が高い設定のVRRPルータにプリエンプトモードoffを指定してください。

● 本来のマスタが復旧したのに自動で切り戻らない

【原因】 プリエンプトモードがoffに設定されている。

【対処】 プリエンプトモードをonに設定してください。

【原因】 本来のマスタでダウントリガが発動している。

【対処】 本来のマスタでVRRP情報を表示してダウントリガ発動状態を確認してください。
ダウントリガが発動している場合は、ダウントリガが発動している原因を除去してください。

参照 BR500S コマンドユーザーズガイド「2.1.29 VRRP情報を確認する」（P.87）
BR500S Webユーザーズガイド「2.2.24 VRRP情報を確認する」（P.79）

● 単一 VRRP グループに複数のマスタ状態である VRRP ルータが存在する

【原因】 VRRP グループである各 VRRP ルータの VRID が同一ではない。
VRRP 情報の「VRID illegal packets」がカウントされている。

【対処】 VRID を同一の値に設定してください。

参照 BR500S コマンドユーザーズガイド「2.1.29 VRRP 情報を確認する」（P.87）
BR500S Web ユーザーズガイド「2.2.24 VRRP 情報を確認する」（P.79）

【原因】 VRRP グループである各 VRRP ルータの VRRP パスワード設定が同一ではない。
VRRP 情報の「Authentication failed packets」、または「Authentication type mismatch packets」がカウントされている。

【対処】 VRRP パスワード設定を同一にしてください。

参照 BR500S コマンドユーザーズガイド「2.1.29 VRRP 情報を確認する」（P.87）
BR500S Web ユーザーズガイド「2.2.24 VRRP 情報を確認する」（P.79）

【原因】 IP フィルタで VRRP-AD メッセージが遮断されている。
VRRP-AD メッセージ：
あて先 IP アドレス　：224.0.0.18
プロトコル番号　　：112

【対処】 VRRP ルータの IP フィルタ設定で VRRP-AD メッセージが遮断される設定を削除してください。

【原因】 VRRP ルータの接続方法が誤っている。

【対処】 VRRP ルータを同一リンクに接続してください。

【原因】 VRRP 情報の「TTL/HopLimit illegal packets」がカウントされている。

【対処】 VRRP ルータを同一リンクに接続してください。

参照 BR500S コマンドユーザーズガイド「2.1.29 VRRP 情報を確認する」（P.87）
BR500S Web ユーザーズガイド「2.2.24 VRRP 情報を確認する」（P.79）

【原因】 VRRP ルータを連結している HUB で STP 機能を有効にしている。

【対処】 VRRP ルータを連結している HUB の STP 機能を無効に設定してください。

【原因】 VRRP ルータを連結している HUB の設定が誤っている。

【対処】 VRRP ルータを連結している HUB の設定を確認して、正しく設定し直してください。
VRRP ルータどうしは同一リンクで接続される必要があります。
VRRP ルータどうしは VRRP-AD メッセージを送受信可能である必要があります。

【原因】 VRRP ルータを連結している HUB が故障している。

【対処】 VRRP ルータを連結している HUB を調べてください。

● マスタが正常に切り替わったのに通信不能となる

【原因】 VRRP 機能が有効である lan 設定でダイナミックルーティングを有効に設定している。

【対処】 ダイナミックルーティングを無効に設定してください。

【原因】 端末のデフォルトルートが仮想 IP になっていない。

【対処】 端末のデフォルトルートを仮想 IP に設定してください。

【原因】 VRRPグループである各VRRPルータの仮想IPが同一ではない。
VRRP情報の「Virtual router IP address configuration mismatched packets」がカウントされている。

【対処】 仮想IPを同一に設定してください。

参照 BR500S コマンドユーザーズガイド「2.1.29 VRRP情報を確認する」（P.87）
BR500S Webユーザーズガイド「2.2.24 VRRP情報を確認する」（P.79）

● 仮想IPあてのpingに応答しない

● 仮想IPあてのtelnetが本装置に繋がらない

【原因】 VRRPが仮想IPあてのパケットを破棄するため。

【対処】 VRRPの仕様です。実IPをあて先に指定してください。

● マスタがバックアップになると実IPあての通信が不能となる

【原因】 優先度にマスタを指定している。

【対処】 優先度にマスタ以外を指定してください。

補足 Web設定では「プライオリティ」設定項目のマスタ（255）選択が該当します。
バックアップを選択して、優先度に値を指定してください（例:254）。

● ダウントリガが発動したのにマスタが切り替わらない

【原因】 優先度が低い設定のVRRPルータにプリエンプトモードoffを指定している。

【対処】 プリエンプトモードをonに設定してください。
手動切り戻しとしたい場合は優先度が高い設定のVRRPルータにプリエンプトモードoffを指定してください。

【原因】 発動したダウントリガの優先度（優先度減算値）設定が小さい値を指定している。

【対処】 （マスタの優先度値 - バックアップの優先度値）+1よりダウントリガの優先度を大きい値に設定してください。

【原因】 バックアップ側でダウントリガが発動している。

【対処】 バックアップ側でVRRP情報を表示して現在の優先度、およびダウントリガ発動状態を確認してください。ダウントリガが発動している場合は、ダウントリガが発動している原因を除去してください。
必要に応じてマスタ側が発動したダウントリガの優先度設定を大きい値に変更してください。

参照 BR500S コマンドユーザーズガイド「2.1.29 VRRP情報を確認する」（P.87）
BR500S Webユーザーズガイド「2.2.24 VRRP情報を確認する」（P.79）

● ノードダウントリガが一度発動すると復旧しない

【原因】 優先度にマスタを指定している。

【対処】 ダウントリガを使用する場合は優先度にマスタを指定しないでください。

補足 Web設定では「プライオリティ」設定項目のマスタ（255）選択が該当します。
バックアップを選択して、優先度に値を指定してください（例:254）。

● ダウントリガの減算優先度の合計が255以上であるのにVRRP状態がInitial状態とならない

【原因】 ダウントリガが発動した場合、優先度の最低値は1以下にはならない。

【対処】 本装置のVRRPの仕様です。VRRPの設定されたLANインタフェースに異常が発生しなければInisial状態とはなりません。

- **インタフェースダウントリガで PPPoE インタフェースを指定したが、異常が発生してもダウントリガが発動しない**

【原因】 回線接続保持機能の設定が常時接続機能を使用するに指定されていない。

【対処】 回線接続保持機能の設定を常時接続機能を使用するに指定してください。

- **リモート側も VRRP を構成して、ローカル側でマスタ切り替わりが発生すると通信不能となる**

【原因】 ローカル側と対になるリモート側 VRRP ルータが同期して切り替わっていない。

【対処】 同期して切り替わるようにダウントリガを設定してください。

2.11 その他のトラブル

その他、以下のようなトラブルがあります。

- **データ通信はほとんどしていないはずなのに、通信料金が高い**

【対処】
- システムログを確認してください。
- Windows®（TCP 上の NetBIOS）環境のネットワークでは、セキュリティ上の問題と、超過課金を抑えるために、ポート番号137～139の外向きの転送経路をふさいでおく必要があります。必要に応じて IP フィルタリングを正しく設定してください。

3　コマンド入力が正しくできないときには

コマンドで設定や操作を行ったときに正しくコマンドが入力できない場合は、まず、以下を参考に本装置の動作状況を確認してみてください。

3.1　シェルに関するトラブル

シェルで入力編集を行う際のトラブルには、以下のようなものがあります。

- **シェルでの入力編集や more コマンド実行時に表示がおかしくなる**

【原因】 端末ソフトウェアが VT100 端末エミュレーション機能をサポートしていない。

【対処】 VT100 端末エミュレーション機能をサポートしている端末ソフトウェアを使用してください。

- **シェルでの入力編集や more コマンド実行時に、カーソルが変な位置に移動してしまう**

【原因】 端末の画面サイズが正しく設定されていない。

【対処】 env コマンドで環境変数 LINES および COLUMNS を正しい値に設定し直してください。

【原因】 画面サイズを通知しない telnet クライアントを使用している。

【対処】 画面サイズを通知する telnet クライアントを使用してください。または、env コマンドで環境変数 LINES および COLUMNS を正しい値に設定し直してください。

- **特定の［CTRL］+［α］キーが動作しない（［α］キー：任意のキー）**

【原因】 端末ソフトウェアが［CTRL］+［α］キーを処理してしまうため入力できない。

【対処】 端末ソフトウェアの設定で、［CTRL］+［α］キーを使用できるよう設定してください。
端末ソフトウェアに［ESC］キー（次に入力したキーをそのまま入力するキー）が用意されているのであれば、［ESC］キーを入力したあと［CTRL］+［α］キーを入力してください。

- **矢印キー（↑、↓、←、→）が動作しない**

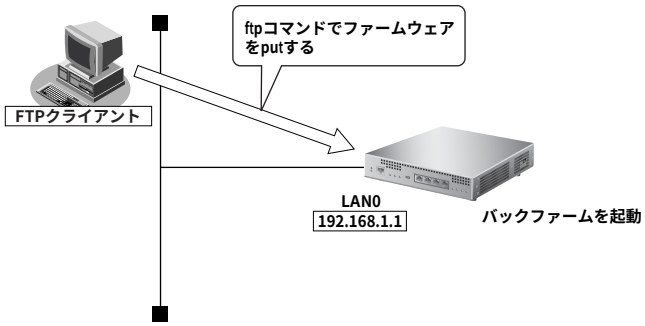
【原因】 矢印キーをサポートしていない端末ソフトウェア（Microsoft® Windows® OS 標準のハイパーターミナルなど）を使用している。

【対処】 矢印キーの代わりに［Ctrl］+［B］キーおよび［Ctrl］+［F］キーでカーソル移動、［Ctrl］+［P］キーおよび［Ctrl］+［N］キーでコマンド履歴移動を行ってください。

4 ファームウェア更新に失敗したときには（バックアップファーム機能）

停電などでファームウェアの更新に失敗し、本装置を起動できなくなった場合、バックアップ用のファームを起動し、ネットワーク上のFTPクライアントからファームウェアを転送することにより、正常な状態に復旧することができます。

補足 リセットスイッチを押しながら電源を投入するとバックアップファームが起動されます。



4.1 パソコン（FTPクライアント）の準備をする

1. 更新するためのファームウェアをFTPクライアントに保存します。

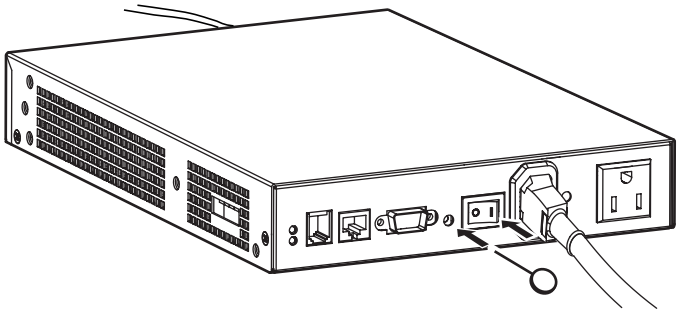
4.2 本装置の準備をする

こんな事に気をつけて

本装置がバックアップファームで起動された場合、LAN0のIPアドレスは192.168.1.1になっています。運用中のLANで、このアドレスに問題がある場合は、FTPクライアントと2台だけ接続してください。

1. 本装置とパソコン（FTPクライアント）をLAN接続します。

2. 先の細いものでリセットスイッチを押しながら電源を投入します。



3. **CHECK／B1／B2／COM／LAN0～3ランプが緑色で点滅するのを確認して、リセットスイッチをはなします。**

バックアップファームが起動します。

補足 バックアップファームが動作しているときは、CHECKランプが緑色で点灯します。

4.3 ファームウェアを更新する

1. **パソコン（FTPクライアント）から本装置にファームウェアを書き込みます。**

参照 BR500S Webユーザーズガイド「FTPサーバ機能によるファームウェアの更新」（P.120）、
BR500S コマンドユーザーズガイド「FTPサーバ機能によるファームウェアの更新」（P.123）

こんな事に気をつけて

- **ファームウェアの転送（put）中は、本装置の電源を切断しないでください。**
- **転送中に電源を切断すると、本装置が使用できなくなる場合があります。**

2. **ファームウェアの更新が正常に行われたことをランプで確認し、電源を切断します。**

補足 正常に更新が行われた場合、LAN0～3ランプが緑色と橙色で交互に点滅します。

3. **電源を投入すると、更新したファームウェアで本装置が起動します。**

5　ご購入時の状態に戻すには

本装置を誤って設定した場合やトラブルが発生した場合は、本装置をご購入時の状態に戻すことができます。

こんな事に気をつけて

ご購入時の状態に戻すと、それまでの設定内容がすべて失われます。構成定義情報の退避、または設定内容をメモしておきましょう。

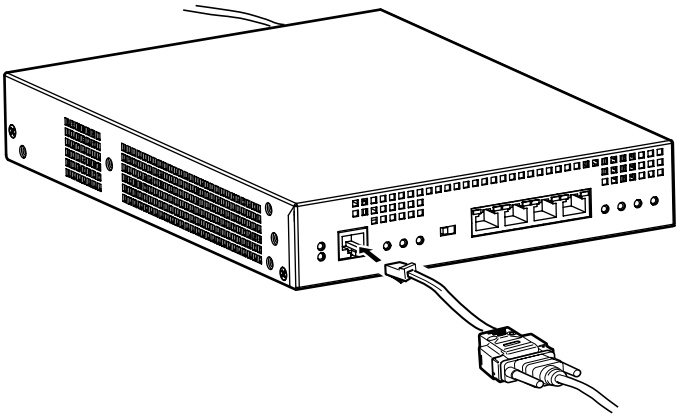
用意するもの

- コンソールケーブル（本製品に同梱のRJ45をD-SUB9ピンに変換するストレートケーブル）
- RS232Cケーブル（クロス、本装置に接続する側がメス型9ピンのD-SUBコネクタ）
- ターミナルソフトウェア（Windows® に標準で装備されている「HyperTerminal」など）

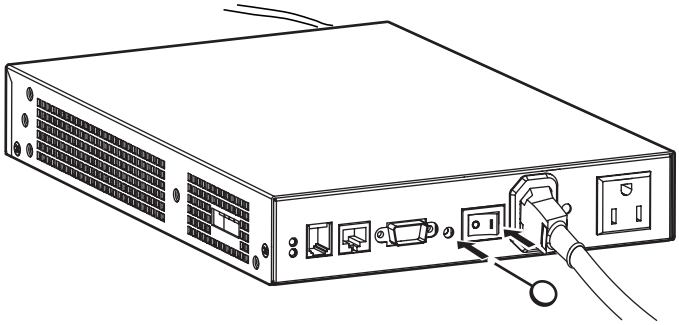
5.1　本装置を準備する

1.　RS232Cケーブルと同梱のコンソールケーブルを接続します。

2.　本装置のコンソールポートにコンソールケーブルのRJ45プラグを差し込みます。



3.　先の細いものでリセットスイッチを押しながら電源を投入します。



5.2 本装置をご購入時の状態に戻す

1. パソコンでターミナルソフトウェアを起動します。

2. 設定条件を以下のように設定します。

スタートBit	データ Bit	パリティ Bit	ストップ Bit	同期方式	通信速度	フロー制御
1	8	なし	1	非同期	9600	なし

補足 設定条件の設定方法については、ターミナルソフトウェアのマニュアルを参照してください。

3. ［Return］キーまたは［Enter］キーを押します。

4. 画面に「>」と表示されたことを確認します。

5. logonと入力して、［Return］キーまたは［Enter］キーを押します。

6. 画面に「backup#」と表示されたことを確認します。

7. reset clearと入力して、［Return］キーまたは［Enter］キーを押します。

本装置の構成定義情報が初期化されます。

```
>logon
backup# reset clear（下線部入力）
>
```

8. 電源を再投入します。

本装置がご購入時の状態で起動します。

索引