P3NK-3312-03Z0

FUJITSU Network Si-R
Si-R brinシリーズ

トラブルシューティング V2

FUJITSU

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。

2009 年 2月初版
2014 年 3月第2版
2016 年12月第3版

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ほかに、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）関連の警告事項を表しています。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）関連の注意事項を表しています。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、Windows NT、Windows ServerおよびWindows Vista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。

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。

製品名の略称について

本書で使用している製品名は、以下のように略して表記します。

なお、本文中では®を省略しています。

製品名称	本文中の表記
Microsoft® Windows® XP Professional operating system	Windows XP
Microsoft® Windows® XP Home Edition operating system	
Microsoft® Windows® 2000 Server Network operating system	Windows 2000
Microsoft® Windows® 2000 Professional operating system	
Microsoft® Windows NT® Server network operating system Version 4.0	Windows NT 4.0
Microsoft® Windows NT® Workstation operating system Version 4.0	
Microsoft® Windows Server® 2003, Standard Edition	Windows Server 2003
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise Edition	
Microsoft® Windows Server® 2003 R2, Enterprise Edition	
Microsoft® Windows Server® 2003, Datacenter Edition	
Microsoft® Windows Server® 2003 R2, Datacenter Edition	
Microsoft® Windows Server® 2003, Web Edition	
Microsoft® Windows Server® 2003, Standard x64 Edition	
Microsoft® Windows Server® 2003 R2, Standard Edition	
Microsoft® Windows Server® 2003, Enterprise x64 Edition	
Microsoft® Windows Server® 2003 R2, Enterprise x64 Edition	
Microsoft® Windows Server® 2003, Enterprise Edition for Itanium-based systems	
Microsoft® Windows Server® 2003, Datacenter x64 Edition	
Microsoft® Windows Server® 2003 R2, Datacenter x64 Edition	
Microsoft® Windows Vista® Ultimate operating system	Windows Vista
Microsoft® Windows Vista® Business operating system	
Microsoft® Windows Vista® Home Premium operating system	
Microsoft® Windows Vista® Home Basic operating system	
Microsoft® Windows Vista® Enterprise operating system	
Microsoft® Windows® 7 64bit Home Premium	Windows 7
Microsoft® Windows® 7 32bit Professional	

本装置のマニュアルの構成

本装置の取扱説明書は、以下のとおり構成されています。使用する目的に応じて、お使いください。

マニュアル名称	内容
Si-R 効率化運用ツール使用手引書	Si-R 効率化運用ツールを使用する方法を説明しています。
Si-R80brin　ご利用にあたって	Si-R80brin の設置方法やソフトウェアのインストール方法を説明しています。
Si-R90brin　ご利用にあたって	Si-R90brin の設置方法やソフトウェアのインストール方法を説明しています。
機能説明書	本装置の便利な機能について説明しています。
トラブルシューティング（本書）	トラブルが起きたときの原因と対処方法を説明しています。
メッセージ集	システムログ情報などのメッセージの詳細な情報を説明しています。
仕様一覧	本装置のハード／ソフトウェア仕様と MIB/Trap 一覧を説明しています。
コマンドユーザーズガイド	コマンドを使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
コマンド設定事例集	コマンドを使用した、基本的な接続形態または機能の活用方法を説明しています。
コマンドリファレンス - 構成定義編 -	構成定義コマンドの項目やパラメタの詳細な情報を説明しています。
コマンドリファレンス - 運用管理編 -	運用管理コマンド、その他のコマンドの項目やパラメタの詳細な情報を説明しています。
Web ユーザーズガイド	Web 画面を使用して、時刻などの基本的な設定またはメンテナンスについて説明しています。
Web 設定事例集	Web 画面を使用した、基本的な接続形態または機能の活用方法を説明しています。
Web リファレンス	Web 画面の項目の詳細な情報を説明しています。

1 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、同梱の保証書に記載の弊社窓口または富士通認定の技術員までご連絡ください。**

1.1 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】 AC アダプターが、DC-IN 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】 AC アダプターを、DC-IN コネクタまたはコンセントに正しく接続してください。

- **CHECK ランプが橙色で点灯している**

【原因】 本装置に異常が発生しました。

【対処】 同梱の保証書に記載の弊社窓口または富士通認定の技術員までご連絡ください。

1.2 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（show ether）で接続状態が確認できます。

参照 マニュアル「Si-R80brin　ご利用にあたって」
マニュアル「Si-R90brin　ご利用にあたって」

【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。

補足 LAN0 ポート、スイッチポート（SW1 ～ 4）は、AutoMDI/MDI-X をサポートしています。

【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。

【原因】 LANポートに接続しているパソコンまたはHUBのLANポートがAutoMDI/MDI-Xとなっている場合に、正常に接続できていない。

【対処】 LANポートに接続しているパソコンまたはHUBのLANポートのAutoMDI/MDI-Xの設定をoffにしてください。

● 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、ipconfigコマンド（Windows 2000／Windows XP／Windows Vista／Windows 7／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ポートに接続されている。

【対処】 本装置の設定をご購入時から変更していない場合は、SW1～SW4ポートが接続できる設定となっています。LANケーブルは、本装置のSW1～SW4ポートのどれかに正しく接続してください。

【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ケーブルを外し、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-T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、LANポートに接続しているパソコンまたはHUBのLANポートのAutoMDI/MDI-X設定がoffになっ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。

補足 パソコン側のIP設定は、ipconfigコマンド（Windows 2000／Windows XP／Windows Vista／Windows 7／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ケーブルを外し、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 「4 ご購入時の状態に戻すには」（P.40）

● **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、1つ前の設定画面を正しく表示することができない（反応がない、1つ前の設定画面と異なる画面が表示されるなど）**

【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）。

● **他装置で使用している構成定義を設定しようとしても、暗号化パスワード文字列がエラーになって設定できない**

【原因】 他装置の構成定義にpassword format uniqueが設定されており、暗号化パスワード文字列が装置固有パスワード形式になっている。

【対処】 暗号化パスワード文字列を平文パスワード文字列に置き換え、続くencryptedの文字列を除いて設定してください。

● **装置を交換したあと、以前設定していた構成定義を再設定しようとしても、暗号化パスワード文字列がエラーになって設定できない**

【原因】 以前の構成定義にpassword format uniqueが設定されており、暗号化パスワード文字列が装置固有パスワード形式になっている。

【対処】 暗号化パスワード文字列を平文パスワード文字列に置き換え、続くencryptedの文字列を除いて設定してください。

● **WWWブラウザで保存しておいた構成定義情報を新たな装置に復元しようとしても、暗号化パスワード文字列を含む構成定義がエラーになって復元できない**

【原因】 保存しておいた構成定義情報にpassword format uniqueが設定されており、暗号化パスワード文字列が装置固有パスワード形式になっている。

【対処】 WWWブラウザですべて設定し直してください。または、保存しておいた構成定義情報のファイルをテキストエディタで開き、装置固有パスワード文字列を平文パスワード文字列に置き換え、続くencryptedの文字列を削除して保存し、保存した構成定義ファイルを指定して構成定義情報を復元してください。

1.3 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-T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.fujitsu.com」を入力したときに「www.fujitsu.com」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合わせて＠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。

1.4 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。
初期設定ではNAT機能を使用する設定になっています。

1.5 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）時間が同じである。

【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。

● 互いの装置から最初のIKEネゴシエーションを同時に行うとIKEネゴシエーションに失敗する

【原因】 互いの装置から送信したInitial-Contactメッセージにより互い違いのIKE SAが残っている。

【対処】 接続優先制御の設定を一方の装置で「Initiatorを優先」、一方の装置で「Responderを優先」のように互いの装置で異なる設定にしてください。

● 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。

【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:11223344556677889900aabbccddeeff1122334455667788

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）。

● テンプレート着信機能（AAA認証またはRADIUS認証）を使用したIPsec/IKE定義を行うとIKEネゴシエーションが開始されない

【原因】 テンプレート着信機能（AAA認証またはRADIUS認証）を使用したIPsec/IKE定義を行っている装置からIKEネゴシエーションを開始しようとしている。

【対処】 テンプレート着信機能（AAA認証またはRADIUS認証）を使用してVPN接続を行う相手装置から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してください。

● テンプレート着信機能（AAA認証またはRADIUS認証）を使用したIPsec/IKE定義を行うと接続できない

【原因】 AAA認証またはRADIUS認証で失敗している。

【対処】 以下のどれかに該当していないか確認してください。

- AAAの設定またはRADIUS認証サーバへ認証IDおよび認証パスワードを設定していない場合は、認証IDおよび認証パスワードを設定してください。
- AAAの設定またはRADIUS認証サーバへ登録している認証IDと認証パスワードが異なっている可能性があります。認証IDと認証パスワードは同じものを設定してください。
- 相手装置の認証ID（Aggressive Modeの場合は装置識別情報、Main Modeの場合はIPsecトンネルアドレスを示す）とAAAまたはRADIUS認証サーバの設定が異っている場合、どちらも同じ認証IDを設定してください。

- IPv6トンネルの構成でIPv6トンネルアドレスを認証IDおよび認証パスワードとした場合、IPv6アドレスを省略して記述しないでください。省略なしのIPv6アドレスを認証IDおよび認証パスワードとして設定してください。
- RADIUS認証を設定している場合、RADIUS認証サーバへ通信が行えていることを確認してください。

【原因】 AAA設定またはRADIUS認証サーバへ登録しているIKE情報の共有鍵と接続相手のIKE情報の共有鍵が一致しない。

【対処】 AAA設定またはRADIUS認証サーバへ接続相手と同じ共有鍵を設定してください。

【原因】 AAA設定またはRADIUS認証サーバへ登録している情報が不足している。

【対処】 AAA設定またはRADIUS認証サーバへ必要な以下の情報を設定してください。

- 認証ID
- 認証パスワード
- 共有鍵
- IPsec対象範囲
  ただしAAAの設定に限り、送信元IPアドレスおよびあて先IPアドレスは、すべてのIPv4アドレスをIPsec対象に含める場合、初期設定のため設定する必要はありません。
- スタティック経路情報

● テンプレート着信機能（AAA認証またはRADIUS認証）を使用したIPsec/IKE定義を行うとIPsec SAが存在するのに暗号化されない

【原因】 AAA設定またはRADIUS認証サーバへ登録しているスタティック経路情報に誤りがある。または、スタティック経路情報がない。

【対処】 AAA設定またはRADIUS認証サーバへ登録しているスタティック経路情報に誤りがないことを確認して設定してください。

【原因】 IPsec対象パケットがIPv6アドレスでテンプレート情報のIPv6機能の設定がoffになっている。

【対処】 テンプレート情報のIPv6機能をonに設定してください。

【原因】 AAA設定のスタティック経路情報がアクセスインタフェースに存在しない。

【対処】 AAA設定のスタティック経路情報をほかのインタフェースと重複しないように設定してください。

● テンプレート着信機能（AAA認証またはRADIUS認証）を使用したIPsec/IKE定義を行うとIPsec SAが存在するのに通信できない

【原因】 AAA設定またはRADIUS認証サーバへ登録しているIPsec対象範囲に誤りがある。

【対処】 AAA設定またはRADIUS認証サーバへ登録しているIPsec対象範囲に誤りがないことを確認して設定してください。

● テンプレート着信機能（AAA認証またはRADIUS認証）を使用したIPsec/IKE定義を行うとテンプレートの接続先監視機能が動作しない

【原因】 AAA設定またはRADIUS認証サーバへ登録している接続先監視アドレス、および、テンプレートに設定している接続先監視アドレスのどちらか一方しか設定していない。

【対処】 AAA設定またはRADIUS認証サーバへ登録している接続先監視アドレス、および、テンプレート定義に設定している接続先監視アドレスの両方を設定してください。

● テンプレート着信機能（動的VPN）を使用したIPsec/IKE定義を行うと接続できない

【原因】 テンプレート着信機能（動的VPN）を使用したIPsec/IKE定義を行うための情報に誤りがある。または、不足している。

【対処】 テンプレート着信機能（動的VPN）を使用したIPsec/IKE定義情報を確認して正しく設定してください。

【原因】 自側ユーザIDが動的VPNサーバに登録されていない。

【対処】 動的VPNサーバへの通信が行えることを確認してください。

【原因】 接続相手のユーザIDが動的VPNサーバに登録されていない。

【対処】 接続相手のユーザIDが動的VPNサーバに登録してください。登録されるまで動的VPNで接続することができません。

【原因】 動的VPN接続契機パケットの検出条件が設定されていない、または設定に誤りがある。

【対処】 動的VPN接続契機パケットの検出条件を確認し、正しく設定してください。

【原因】 IPsecまたはIKE情報のどちらかが接続相手と一致していない。

【対処】 以下の設定が接続相手と同じになるように設定してください。

- 自動鍵交換用IPsec情報のセキュリティプロトコルの設定
- 自動鍵交換用IPsec情報の暗号情報の設定
- 自動鍵交換用IPsec情報の認証情報の設定
- 自動鍵交換用IPsec情報のPFS使用時のDH（Diffie-Hellman）グループの設定
- IKEセッション確立時の共有鍵（Pre-shared key）の設定
- IKEセッション用暗号情報の設定

【原因】 動的VPN情報交換で取得した相手IPsecトンネルアドレスに対し、優先度の高い経路がすでに存在する。

【対処】 対象となる既存経路の優先度を下げてください。

【原因】 静的経路数が最大数を超えたため、動的VPN情報交換で取得した相手IPsecトンネルアドレスに対する経路が追加できなかった。

【対処】 静的経路を確認してください。

● テンプレート着信機能（動的VPN）を使用したIPsec/IKE定義を行うとIPsec SAが存在していても拠点間通信ができない

【原因】 IPsec対象パケットがIPv6アドレスでテンプレート情報のIPv6機能の設定がoffになっている。

【対処】 テンプレート情報のIPv6機能をonに設定してください。

● テンプレート着信機能（動的VPN）を使用して接続先監視ができない

【原因】 本装置または相手装置のどちらかに接続先監視の定義がされていない。

【対処】 接続先監視を行う場合は、両方の装置で設定してください。

● NATトラバーサルを使用したIPsec/IKE機能が動作しない

【原因】 IKE区間にNAT装置が存在しない。

【対処】 NATトラバーサルは、IKE区間にNAT装置を検出したときだけ動作します。

【原因】 セキュリティプロトコルに認証（AH）を指定している。

【対処】 NATトラバーサルでは、セキュリティプロトコルは暗号（ESP）しかサポートしていません。セキュリティプロトコルを暗号（ESP）で指定するように定義を変更してください。

● NATトラバーサルを使用したIKEネゴシエーションに失敗する

【原因】 動的VPN機能を使用したIPsec/IKE定義を設定している。

【対処】 動的VPNは未サポートのため使用できません。

【原因】 両装置でサポートするベンダIDが一致しない。

【対処】 以下のベンダIDだけをサポートしています。対抗装置が以下をサポートしていない場合は、NATトラバーサルは使用できません。

- RFC 3947
- draft-ietf-ipsec-nat-t-ike-03
- draft-ietf-ipsec-nat-t-ike-02\n
- draft-ietf-ipsec-nat-t-ike-02

IPsec設定ミス　トラブルシュート方法

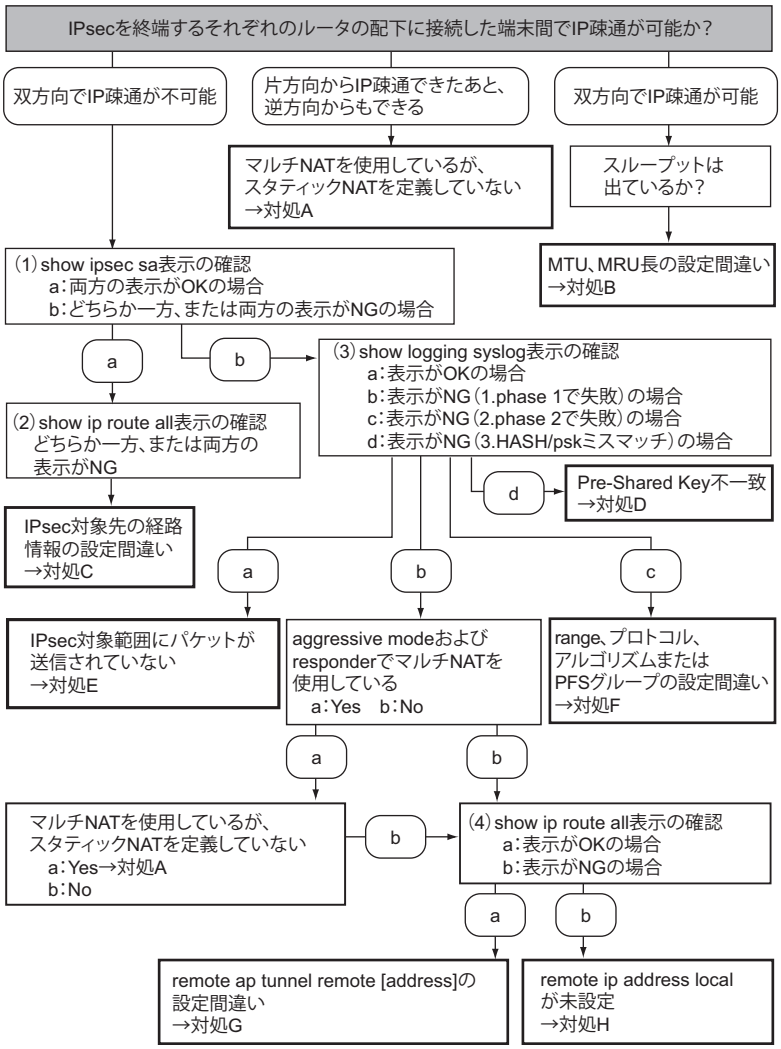
IPsecの設定ミスの原因と対処を、以下のフローチャートで特定してください。

フローチャート内の（1）～（4）は「 ログ表示の確認」（P.20）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.25）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、接続形態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）show ipsec sa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。

```
# show ipsec sa
[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。

```
# show ipsec sa
[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)

#
#show ipsec sa
#
```

- IPsecSA、IKE SAともに何も表示されない。

(2)show ip route all 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。

```
# show ip route all
FP    Destination/Mask    Gateway      Distance    UpTime      Interface
*S    0.0.0.0/0           rmt0                0    00:01:03    rmt0
*L    10.1.1.1/32         10.1.1.1            0    00:03:49    rmt0
*C    192.168.1.0/24      192.168.1.1         0    00:03:49    lan1
*S    192.168.2.0/24      rmt1                0    00:01:03    rmt1
#
```

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）。

```
# show ip route all
FP    Destination/Mask    Gateway      Distance    UpTime      Interface
*S    0.0.0.0/0           rmt0                0    00:01:03    rmt0
*L    10.1.1.1/32         10.1.1.1            0    00:03:49    rmt0
*C    192.168.1.0/24      192.168.1.1         0    00:03:49    lan1
#
```

(3)show logging syslog 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。

```
# show logging syslog
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/certificate ミスマッチ」（P.23）を参照してください。

```
# show logging syslog
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

```
# show logging syslog
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

```
# show logging syslog
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

```
# show logging syslog
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

```
# show logging syslog
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

```
# show logging syslog
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

```
# show logging syslog
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/certificate ミスマッチ

HASH mismatchd、psk mismatchd は、Aggressive Mode の場合 Initiator で、Main Mode の場合 Responder で確認する。

- 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。

```
# show logging syslog
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. sir80brin->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。

```
# show logging syslog
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)show ip route all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。

```
# show ip route all
FP    Destination/Mask    Gateway      Distance      UpTime      Interface
*S    0.0.0.0/0           rmt0                0      00:01:03    rmt0
*L    10.1.1.1/32         10.1.1.1            0      00:03:49    rmt0
*C    192.168.1.0/24      192.168.1.1         0      00:03:49    lan1
*S    192.168.2.0/24      rmt1                0      00:01:03    rmt1
#
```

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。

```
# show ip route all
FP    Destination/Mask    Gateway      Distance      UpTime      Interface
*S    0.0.0.0/0           rmt0                0      00:01:03    rmt0
*C    192.168.1.0/24      192.168.1.1         0      00:03:49    lan1
*S    192.168.2.0/24      rmt1                0      00:01:03    rmt1
#
```

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.25）
- MTU、MRU長の設定間違い→【対処B】（P.26）
- IPsec対象先の経路情報の設定間違い→【対処C】（P.27）
- Pre-Shared Key不一致→【対処D】（P.27）
- IPsec対象範囲にパケットが送信されていない→【対処E】（P.28）
- 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.28）
- remote ap tunnel remote [address]の設定間違い→【対処G】（P.29）
- remote ip address local が未設定→【対処H】（P.30）

【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 sir2 sir2
# 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 IKE(UDP:500)
# remote 0 ip nat static 1 192.168.2.1 any any any 50 ESP(IP:50)
# remote 0 ip msschange 1414
# remote 1 name SIR
# remote 1 ap 0 name sir
# 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 sir370
# remote 1 ap 0 ike shared key text sir370
# 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 address 192.168.2.1 192.168.1.1
# 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 sir2 sir2
# 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 SIR
# remote 1 ap 0 name sir
# 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 sir370
# remote 1 ap 0 ike shared key text sir370
# 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 address 192.168.2.1 192.168.1.1
# 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

```
# show ip route all
FP    Destination/Mask    Gateway      Distance      UpTime      Interface
*S    0.0.0.0/0           rmt0                0      00:01:03    rmt0
*L    10.1.1.1/32         10.1.1.1            0      00:03:49    rmt0
*C    192.168.1.0/24      192.168.1.1         0      00:03:49    lan1
*S    192.168.2.0/24      rmt1                0      00:01:03    rmt1
#
```

【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 sir2 sir2
# 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 SIR
# remote 1 ap 0 name sir
# 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 sir370
（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 sir370
# 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 address 192.168.2.1 192.168.1.1
# 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 SIR
# remote 1 ap 0 name sir
# 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 sir370
# remote 1 ap 0 ike shared key text sir370
# 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 address 192.168.2.1 192.168.1.1
# 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 fujitsuA fujitsuA
# 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 address 192.168.1.1 192.168.2.1
# remote 1 ap 0 sessionwatch interval 10s 3m 5s
# remote 1 ip route 0 192.168.2.0/24 1 0
# remote 1 ip msschange 1414
```

1.6 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。

● パソコンに Si-R brin を接続すると Si-R brin 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 Windows XP または Windows Vista である。

【対処】 Windows XP および Windows Vista は、標準で UPnP 機能をサポートしています。このため、Si-R brin に接続するとマイネットワークやタスクトレイに Si-R brin のアイコンが表示され、ダブルクリックすると Si-R brin の Web 設定画面が表示されます。

● パソコンに Si-R brin 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 Windows XP または Windows Vista 以外である。

【対処】 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 Si-R brin のアイコンは表示されません。

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

【対処】 以下の手順で、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。

1.7 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ホストと通信ができない

【原因】 SNMPエージェントアドレスが正しく設定されていない。

【対処】 本装置のインタフェースに割り当てられているIPアドレスのどれかをSNMPエージェントアドレスとして設定してください。

【原因】 SNMPホストのIPアドレスが正しく設定されていない。

【対処】 本装置にアクセスするSNMPホストのIPアドレスを確認し、正しいIPアドレスを設定してください。

【原因】 コミュニティ名が正しく設定されていない（SNMPv1またはSNMPv2c使用時）。

【対処】 本装置にアクセスするSNMPホストのコミュニティ名を確認し、正しいコミュニティ名を設定してください。

【原因】 SNMPユーザ名が正しく設定されていない（SNMPv3使用時）。

【対処】 本装置にアクセスするSNMPホストのSNMPユーザ名を確認し、正しいSNMPユーザ名を設定してください。

【原因】 認証プロトコルまたは認証パスワードが正しく設定されていない（SNMPv3使用時）。

【対処】 本装置にアクセスするSNMPホストの認証プロトコルまたは認証パスワードを確認し、正しい認証プロトコルまたは認証パスワードを設定してください。

【原因】 暗号プロトコルまたは暗号パスワードが正しく設定されていない（SNMPv3使用時）。

【対処】 本装置にアクセスするSNMPホストの暗号プロトコルまたは暗号パスワードを確認し、正しい暗号プロトコルまたは暗号パスワードを設定してください。

1.8 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アドレスが、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アドレスは、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IP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アドレスが、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アドレスを端末の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アドレスと同一のIPアドレスである装置が接続されている。

【対処】 仮想IPアドレスと同一の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アドレスを解決するARPリクエストに応答する装置が存在する。

【対処】 仮想IPアドレスを解決する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】 優先度に最優先（master）を指定している。

【対処】 優先度に最優先（master）以外を指定してください。

補足 Web設定では、「LAN情報」-［共通情報］-［VRRPグループ情報］のプライオリティで“優先度固定（最優先）”を選択して、優先度に値（例:254）を指定してください。

【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 マニュアル「コマンドユーザーズガイド」
マニュアル「Webユーザーズガイド」

【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。
イニシャル状態である場合は、以降の「イニシャル状態から、バックアップ状態またはマスタ状態に遷移しない」を参照してください。

【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。

● 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。

【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。

【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。

【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アドレスを同一に設定してください。

● **仮想IPアドレスあてのpingに応答しない**

【原因】 仮想IPアドレスあてのicmp受信設定がされていない。

【対処】 仮想IPアドレスあてのicmp受信を有効に設定してください（lan vrrp group vaddr icmp accept）。

【原因】 仮想IPアドレスのVRRPグループがマスタ状態以外である。

【対処】 仮想IPアドレスあてのpingに応答するのは、マスタ状態のVRRPルータだけです。

● **仮想IPアドレスあてのtelnetがSi-R brinに繋がらない**

【原因】 VRRPが仮想IPアドレスあてのパケットが破棄されている。

【対処】 VRRPの仕様です。実IPアドレス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アドレスあての通信が不能となる**

【原因】 優先度に最優先（master）を指定している。

【対処】 優先度に最優先（master）以外を指定してください。

補足 Web設定では、「LAN情報」-［共通情報］-［VRRPグループ情報］のプライオリティで“優先度固定（最優先）”を選択して、優先度に値（例:254）を指定してください。

● **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。

【調査方法】

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。

● **ノードダウントリガが一度発動すると復旧しない**

【原因】 優先度に最優先（master）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最優先（master）を指定しないでください。

補足 Web設定では、「LAN情報」-［共通情報］-［VRRPグループ情報］のプライオリティで“優先度固定（最優先）”を選択して、優先度に値（例:254）を指定してください。

● **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状態がイニシャル状態とならない**

【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するか、手動停止コマンドを実行しなければイニシャル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。

● **イニシャル状態から、バックアップ状態またはマスタ状態に遷移しない**

【原因】 VRRPグループ手動停止コマンドが実行されている（vrrp action disable）。

【対処】 VRRPグループ手動再開始コマンドを実行してください（vrrp action enable）。
手動停止コマンドが実行されているかは、VRRP情報を表示して確認することができます。現在のVRRPグループの状態が Initialize:Disabled の場合は手動停止コマンドが実行されています。

【原因】 VRRPグループが設定されたLANで異常が発生している。

【対処】 LANケーブルの抜けや、接続されたHUBの異常などを確認してください。また、LANに対して切断／閉塞コマンド（offline）が実行されていないかも確認してください。

● **VRRPアクションが一度発動すると復旧しない**

【原因】 VRRPアクションでVRRPが設定されたLANに対して切断／閉塞コマンドが指定されている。

【対処】 VRRPアクションでVRRPが設定されたLANに対して切断／閉塞コマンドが実行されないように設定してください。たとえば、切断／閉塞コマンドを実行する必要があるLANを個別に指定します。

● **VRRPアクションの発動する状態にバックアップを指定したにもかかわらず、VRRPルータ開始時に発動しない**

【原因】 VRRPアクションに切断／閉塞コマンドまたは接続／閉塞解除コマンドを指定している。

【対処】 VRRPアクションの切断／閉塞コマンドまたは接続／閉塞解除コマンドは発動する状態にバックアップを指定した場合、マスタ状態からマスタ状態以外に遷移しなければ発動しない仕様です。

● **VRRPアクションの発信抑止（diallock）が発動したのに発信抑止しない**

【原因】 発信抑止するリモートがPPPoE接続以外である。

【対処】 発信抑止の仕様です。

● **VRRPアクションの切断／閉塞コマンド（offline）が発動したのに対象が閉塞状態とならない**

【原因】 切断／閉塞する対象がPPPoE接続またはテンプレート着信による接続となっている。

【対処】 切断／閉塞コマンドの仕様です。

2 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。

2.1 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ページャ表示時に、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】 terminal window コマンドで正しい画面サイズを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、terminal windowコマンドで正しい画面サイズを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（HyperTerminalなど）を使用している。

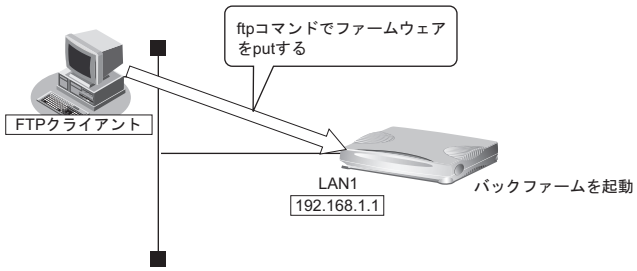
【対処】 矢印キーの代わりに［Ctrl］+［B］キーおよび［Ctrl］+［F］キーでカーソル移動、［Ctrl］+［P］キーおよび［Ctrl］+［N］キーでコマンド履歴移動を行ってください。

3 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。

ここでは、Si-R90brinを例に説明します。



3.1 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。

3.2 本装置の準備をする

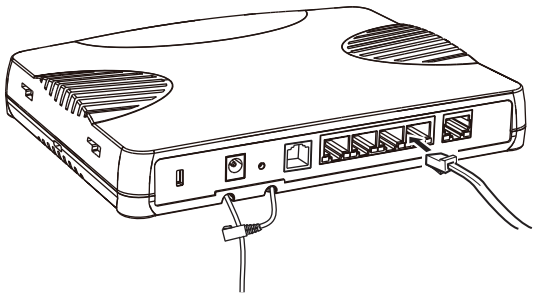
こんな事に気をつけて

本装置がバックアップファームで起動された場合、SW1ポートの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。LAN0は使用できません。

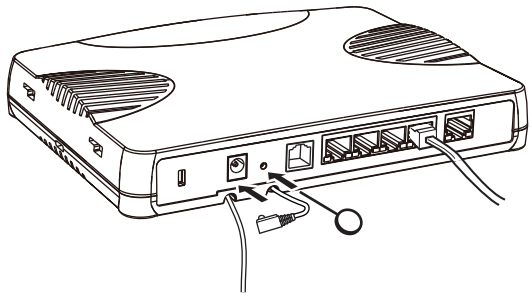
1. 本装置の電源が切れていることを確認します。

2. 本装置とパソコン（FTPクライアント）をLAN接続します。

補足 本装置とパソコンをHUBを介さず、直接10/100BASE-TXポートにケーブルを接続します。
初期設定ではスイッチポートが有効となっています。



3.　先の細いもので本装置背面のリセットスイッチを押しながら、DC-IN コネクタに AC アダプターを差し込みます。



4.　CHECK ／ FUNC ／ LAN0 ／ PPPoE ／ VPN 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。

3.3　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転送します。

参照　マニュアル「Web ユーザーズガイド」
マニュアル「コマンドユーザーズガイド」

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、CHECK ／ FUNC ／ LAN0 ランプのみ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。

4 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。
ここでは、Si-R90brin を例に説明します。

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またはLANケーブル

補足 Si-R90brin には、コンソールケーブルは同梱されていません。
「4.2 コンソールポートに接続する」（P.42）の方法でご購入時の状態に戻す場合は、コンソールケーブルを用意してください。
ケーブルについては、以下の富士通ホームページをご覧ください。
URL : http://www.fujitsu.com/jp/products/network/router/manual/cable3.html

- 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）
  コンソールケーブルを使用する場合に必要です。
- ターミナルソフトウェア（HyperTerminal など）

4.1 LANで接続する

本装置を準備する

こんな事に気をつけて

バックアップファームが起動した場合、本装置の SW1 ポートの 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 クライアントだけを接続してください。

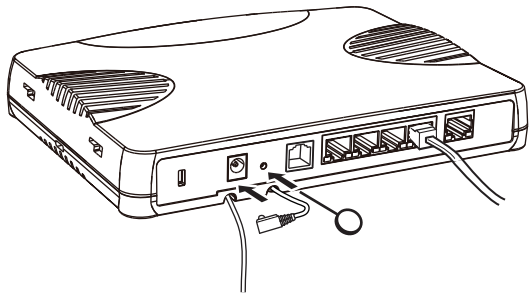
1. 本装置の電源が切れていることを確認します。

2. 本装置とパソコン（FTP クライアント）を LAN 接続します。

本装置とパソコンを HUB を介さず、直接、10/100BASE-TX ポートにケーブルを接続します。

補足
- ツイストペアケーブルを機器に接続する直前に、静電気除去ツールなどを使用してケーブルに帯電している静電気を除電してください。除電については、以下を参照してください。
  マニュアル「Si-R80brin　ご利用にあたって」
  マニュアル「Si-R90brin　ご利用にあたって」
- LANケーブルの接続方法およびパソコンの準備については、以下を参照してください。
  マニュアル「Si-R80brin　ご利用にあたって」
  マニュアル「Si-R90brin　ご利用にあたって」
- 本装置は、AutoMDI/MDI-X 機能をサポートしているため、パソコンと HUB を意識しないで、10/100BASE-TX ポートにケーブルを接続することができます。

3. **先の細いもので本装置背面のリセットスイッチを押しながら、DC-IN コネクタに AC アダプターを差し込みます。**



4. **CHECK ／ FUNC ／ LAN0 ／ PPPoE ／ VPN 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。

本装置をご購入時の状態に戻す

1. **telnet でログインします。**

パソコンには、本装置と同じネットワークの IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」、サブネットマスクは「255.255.255.0」です。

2. **[Return] キーまたは [Enter] キーを押します。**

3. **画面に「backup#」と表示されたことを確認します。**

4. **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。

```
backup# reset clear（下線部入力）
```

5. **telnet で再度ログインできる状態になったあとに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。

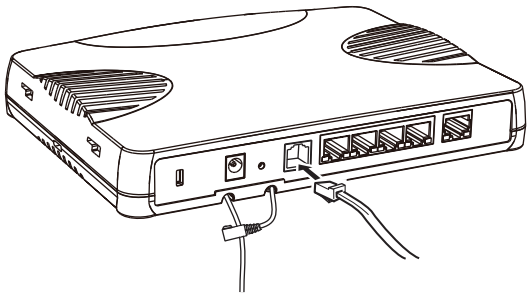
4.2　コンソールポートに接続する

本装置を準備する

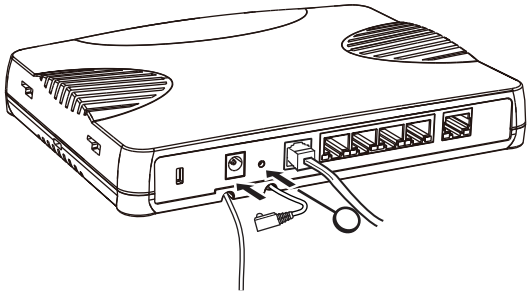
1.　本装置の電源が切れていることを確認します。

2.　パソコンとコンソールケーブルを接続します。

3.　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。



4.　先の細いもので本装置背面のリセットスイッチを押しながら、DC-INコネクタにACアダプターを差し込みます。



5.　CHECK／FUNC／LAN0／PPPoE／VPN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の起動には、1分程度かかります。
バックアップファームが起動すると、CHECKランプが緑色で点灯します。

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. **画面に「>」と表示されたことを確認したあとに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

Si-R brin シリーズ　トラブルシューティング

P3NK-3312-03Z0

発行日　　2016年12月

発行責任　　富士通株式会社