

P3NK-3942-06Z0

# FUJITSU Network Si-R Si-Rシリーズ

トラブルシューティング V35

The logo consists of the word "FUJITSU" in a bold, red, sans-serif font. Above the letter "I" is a stylized red infinity symbol or a pair of interlocking circles.

# 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11月初版

2010年7月第2版

2012年11月第3版

2013年11月第4版

2014年6月第5版

2017年6月第6版

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。  
Copyright FUJITSU LIMITED 2009 - 2017

# 目次

はじめに .....	2
本書の使いかた .....	4
本書の読者と前提知識 .....	4
本書における商標の表記について .....	5
本装置のマニュアルの構成 .....	6
1 回線料金がおかしいと思ったら .....	7
1.1 超過課金の見分け方 .....	7
1.2 超過課金が発生した原因を調べる .....	7
2 通信ができない場合には .....	11
2.1 起動時の動作に関するトラブル .....	11
2.2 本装置設定時のトラブル .....	12
2.3 回線への接続に関するトラブル .....	16
2.4 データ通信に関するトラブル .....	20
2.5 導入に関するトラブル .....	22
2.6 IPsec/IKE に関するトラブル .....	25
2.7 MPLS に関するトラブル .....	43
2.8 VoIP NAT トラバースルに関するトラブル .....	43
2.9 SNMP に関するトラブル .....	45
2.10 VRRP に関するトラブル .....	46
2.11 外部メディアスタート機能に関するトラブル .....	50
2.12 その他のトラブル .....	50
3 コマンド入力为正しくできないときには .....	51
3.1 シェルに関するトラブル .....	51
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) .....	52
4.1 パソコン (FTP クライアント) を準備する .....	52
4.2 本装置を準備する .....	52
4.3 ファームウェアを更新する .....	54
5 ご購入時の状態に戻すには .....	55
5.1 LAN で接続する .....	55
5.2 コンソールポートに接続する .....	57
<b>索引</b> .....	<b>59</b>

# 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。  
ネットワーク設定を初めて行う方でも「機能説明書」に分かりやすく記載していますので、安心してお読みいただけます。

## 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。
-  **適用機種** 本装置の機能を使用する際に、対象となる機種名を示します。
-  **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。

Adobe および Reader は、Adobe Systems Incorporated (アドビシステムズ社) の米国ならびに他の国における商標または登録商標です。

UNIX は、米国およびその他の国におけるオープン・グループの登録商標です。

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-R180B ご利用にあたって	Si-R180B 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-R220C ご利用にあたって	Si-R220C 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-R220D ご利用にあたって	Si-R220D 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-R240B ご利用にあたって	Si-R240B 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-R260B ご利用にあたって	Si-R260B 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-R370 ご利用にあたって	Si-R370 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-R370B ご利用にあたって	Si-R370B 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-R570 ご利用にあたって	Si-R570 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-R570B ご利用にあたって	Si-R570B 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 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。

## 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】** 無通信監視時間設定を行っていても、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となります。
- 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】** 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を経過すると回線は自動的に切断されます。



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 running-config remote <number> ip rip
```

☛ 参照 Web 設定事例集 [「2.14 IPフィルタリング機能を使う」\(P392\)](#)、  
コマンド設定事例集 [「2.14 IPフィルタリング機能を使う」\(P174\)](#)

## 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2】**

**【対処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 Web 設定事例集 [「2.14 IPフィルタリング機能を使う」\(P392\)](#)、  
コマンド設定事例集 [「2.14 IPフィルタリング機能を使う」\(P174\)](#)

**【対処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 Web 設定事例集 [「2.26 特定のURLへのアクセスを禁止する（URLフィルタ機能）」\(P1019\)](#)、  
コマンド設定事例集 [「2.26 特定のURLへのアクセスを禁止する（URLフィルタ機能）」\(P421\)](#)

**【対処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。

```
[proxymdns:[<QTYPE>:<QNAME>]from<IPアドレス>to<ネットワーク名>]
```

☛ 参照 Web 設定事例集 [「2.25.5 DNS問い合わせタイプフィルタ機能を使う」\(P1015\)](#)、  
コマンド設定事例集 [「2.25.5 DNS問い合わせタイプフィルタ機能を使う」\(P419\)](#)



## デフォルトルートどうして接続している場合

【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】 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外してください。

☛ 参照 Web 設定事例集「[1.9 事業所 LAN を ISDN で接続する](#)」(P.100)、  
コマンド設定事例集「[1.10 事業所 LAN を ISDN で接続する](#)」(P.33)

## 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。
- さらに内部時刻の時刻設定も確認してください。

【対処】 上記スケジュール機能および内部時刻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 Web 設定事例集「[2.32 スケジュール機能を使う](#)」(P.1085)、  
Web ユーザーズガイド「[1.5 時刻を設定する](#)」(P.18)、  
コマンド設定事例集「[2.32 スケジュール機能を使う](#)」(P.443)、  
コマンドユーザーズガイド「[1.2 時刻を設定する](#)」(P.13)

## 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されているときとで、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】 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、スケジュール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。

## 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】 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」 \(P.55\)](#)

## 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ません。

【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ません。

【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】 本装置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。

#### ● CHECK ランプが橙色で点灯している

**接続したポートに該当する通信状態を示すランプが点灯していない**

**show system status 実行時の machine\_state が、“FALLBACK” となっている**

【原因】 ハード障害を検出したため、縮退モードに遷移しました。

【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。

#### ● CHECK ランプが橙色で点滅している

【原因】 USB ポートで過電流を検出しました。

【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。

#### ● 拡張モジュールの STS ランプが橙点灯または点灯していない

【原因】 本装置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 (SLOT) 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ません。

【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ます。

【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ます。

【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ます。

【対処】 Si-R220C、Si-R220Dでは、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 Si-R220C ご利用にあたって「ディップスイッチの設定」(P.24)

Si-R220D ご利用にあたって「ディップスイッチの設定」(P.21)

## 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ません。

【対処】 本装置の10／100／1000M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／1000M／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。なお、1000MはSi-R570、Si-R570Bのみサポートしていません。

☛ 参照 Si-R180B ご利用にあたって「100M/FULLランプの詳細」(P.21)、

Si-R220C ご利用にあたって「100M/FULLランプの詳細」(P.22)、

Si-R220D ご利用にあたって「100M/FULLランプの詳細」(P.19)、

Si-R240B ご利用にあたって「100M/FULLランプの詳細」(P.22)、

Si-R260B ご利用にあたって「100M/FULLランプの詳細」(P.22)、

Si-R370 ご利用にあたって「100M/FULLランプの詳細」(P.23)、

Si-R370B ご利用にあたって「100M/FULLランプの詳細」(P.19)、

Si-R570 ご利用にあたって「1000M/100M/FULLランプの詳細」(P.23)、

Si-R570B ご利用にあたって「1000M/100M/FULLランプの詳細」(P.19)

【原因】 LANケーブルのタイプが違います。

【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。



• Si-R180B

LAN0ポートは、構成定義でMDI/MDI-Xの設定を変更することができます。  
スイッチポート（SW1～4）は、AutoMDI/MDI-Xをサポートしています。

• Si-R260B

LAN0ポートは、to HUB to PCスイッチでMDI/MDI-Xを切り替えることができます。  
LAN0以外のポートは、構成定義でMDI/MDI-Xの設定を変更することができます。

• Si-R220C、Si-R220D、Si-R240B、Si-R370、Si-R370B、Si-R570、Si-R570B

基本ボード上のLANポートは、AutoMDI/MDI-Xをサポートしています。

【原因】 接続に誤りがあります。または、LANケーブルが断線しています。

【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。

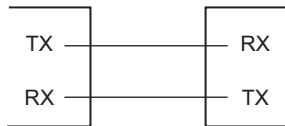
【原因】 LAN ポートの AutoMDI/MDI-X の設定が on の状態で、LAN ポートに接続しているパソコンまたは HUB の LAN ポートが AutoMDI/MDI-X となっている場合に、正常に接続できていません。

【対処】 本装置の LAN ポートの AutoMDI/MDI-X の設定を off にします。または、LAN ポートに接続しているパソコンまたは HUB の LAN ポートの設定を off にします。

● **接続した FX ポートに該当する SLOT ランプが橙色で点滅している、または接続相手のリンクランプが点灯してしない**

【原因】 光モジュールの接続が間違っています。

【対処】 光モジュールどうしは、TX / RX をそれぞれクロスして接続する必要があります。接続を確認してください。



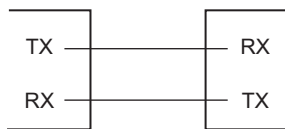
【原因】 接続相手の光モジュールやケーブルのタイプが違います。

【対処】 100BASE-FX (SIR37EF) 拡張モジュール L2 は、Single Mode Fiber (SMF) 用の光モジュール (1300nm) を使用しています。Multi Mode Fiber (MMF) 対応の機器やケーブルは使用できません。Single Mode Fiber (SMF) 対応の接続相手に Single Mode Fiber (SMF) ケーブルで接続してください。

● **接続した ATM155 ポートに該当する SLOT ランプが橙色で点滅している、または接続相手のリンクランプが点灯してしない**

【原因】 光モジュールの接続が間違っています。

【対処】 光モジュールどうしは、TX / RX をそれぞれクロスして接続する必要があります。接続を確認してください。



【原因】 接続相手の光モジュールやケーブルのタイプが違います。

【対処】 ATM155M (SIR37ATB) 拡張モジュール L2 は、Single Mode Fiber (SMF) 用の光モジュール (1300nm) を使用しています。Multi Mode Fiber (MMF) 対応の機器やケーブルは使用できません。Single Mode Fiber (SMF) 対応の接続相手に Single Mode Fiber (SMF) ケーブルで接続してください。

● **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ます。


【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。


 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ます。
- 【対処】 LAN インタフェースのIPアドレスを再割り当てるため、パソコンを再起動してください。
- 【原因】 LAN0ポート (Si-R180Bはスイッチポート) 以外に接続されています。
- 【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ます。
- 【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う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ます。
- 【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ます。
- 【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ません。
- 【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】 接続に誤りがあります。または、LANケーブルが断線しています。
- 【対処】 接続した10 / 100 / 1000BASE-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、Si-R260Bの場合はto HUB to PCスイッチが正しく設定されているか、Si-R180B、Si-R220C、Si-R220D、Si-R240B、Si-R370、Si-R370B、Si-R570、Si-R570Bの場合はAutoMDI/MDI-Xの設定が正しい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。なお、1000BASE-TポートはSi-R570、Si-R570Bのみサポートしています。
- 【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ます。
- 【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。

 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ます。
- 【対処】 LAN インタフェースのIPアドレスを再割り当てるため、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ます。

- 【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ます。

【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ます。

【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ます。

【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ません。

【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、ネットワー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】 コンソールでログインして、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」 (P55)

### ● 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ます。
  - 【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ます。
  - 【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ます。
  - 【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。

## 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ります。
  - 【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。
- **BRI 拡張モジュール L2 を使った通信で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ります。
  - 【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 (SLOT) ランプがまったく点灯しない)**
  - 【原因】 接続先が話し中です。
  - 【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ります。
  - 【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ます。
- 【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ます。
- 【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ません。
- 【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制します。
- 【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制しています。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、自動発信の抑制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ます。
- 【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 Si-R220C ご利用にあたって「[ディップスイッチの設定](#)」(P24)
- Si-R220D ご利用にあたって「[ディップスイッチの設定](#)」(P21)

### ● ISDN 公衆回線で相手先につながらない (B1/B2 (SLOT) 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】 認証に失敗しました。
- 【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ました。
- 【対処】 接続先に適合するように設定を変更してください。

 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 (SLOT) 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ります。
- 【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ります。
- 【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ません。
- 【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ます。
- 【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ります。

【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 Web ユーザーズガイド「[2.3.3 構成定義情報を退避する／復元する](#)」(P52)、  
コマンドユーザーズガイド「[2.4 構成定義情報を確認する](#)」(P43)

【原因】 パソコンの設定に誤りがあります。

【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ります。

【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ります。

【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ります。

【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ます。

【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ります。

【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 Web ユーザーズガイド「[2.3.3 構成定義情報を退避する／復元する](#)」(P52)、  
コマンドユーザーズガイド「[2.4 構成定義情報を確認する](#)」(P43)

【原因】 ネットワーク上のコンピュータが通信しています。

【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ました。

【対処】 本装置の電源を切って、回線を切断してください。

● **専用線論理リンク構成で通信ができない**

【原因】 PPP ネゴシエーションが失敗しました。

【対処】 本装置と相手装置の認証をオフに設定するか、両装置に正しい情報を設定してください。  
show access-pointなどで IPCP 状態が「negotiating」になっている場合、両装置での認証情報が一致していないことが考えられます。

【原因】 PPP ネゴシエーションが失敗しました。

【対処】 本装置と相手装置でマルチリンクが有効になっているか確認してください。  
show access-pointなどで IPCP 状態が「negotiating」になっている場合、両装置での認証情報が一致していないことが考えられます。

【原因】 論理速度が回線の総和になりません。

【対処】 本装置と相手装置でマルチリンクが有効になっているか確認してください。

● **専用線と ISDN 回線の論理リンク構成で ISDN 回線が接続されない**

【原因】 発信番号が正しく設定されていません。

【対処】 本装置と相手装置で、接続先電話番号が論理リンクのマスタ定義に設定されているか確認してください。

【原因】 両装置で着信番号認証が無効になっています。

【対処】 以下のどちらかの状態に設定してください。

- 両装置で着信番号認証を有効にします。
- 着信番号認証が無効の装置に answer accept enable を設定し、発信者番号 (CLID) が通知されない着信、または remote ap called number で設定したどの番号とも一致しない着信について、着信を許可する設定にします。

● **専用線と ISDN 回線の論理リンク構成で ISDN 回線が接続されたまま切断されない**

【原因】 本装置または相手装置で通信料によるチャンネル制御が設定されていません。

【対処】 本装置または相手装置のどちらか一方、または両方に通信料によるチャンネル制御を設定してください。

● **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 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**

【原因】 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。

【対処】 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ます。

【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ました。

【対処】 本装置の10 / 100 / 1000BASE-Tポート（LANランプ、100Mランプ、1000M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（1000Mbps-全二重、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。なお、1000MはSi-R570、Si-R570Bのみサポートしています。

- **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ます。

【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ます。

【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の設定が古いです。

【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の設定が古いです。

【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モデムとつな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ました。

【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ます。

【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ました。

【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ません。

【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モデムにリバーシ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ます。

【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ません。

【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。

● 複数の事業所 LAN を ATM で接続できない

【原因】 VP / VC 速度の設定に誤りがあります。

【対処】 使用する ATM 拡張モジュールによって設定条件が異なる点に注意して、正しく設定し直してください。  
Si-R260B の ATM25 インタフェースは ATM25 拡張モジュール L2 と同じです。

拡張モジュール	注意点
ATM25M / ATM155M 拡張モジュール L2	<ul style="list-style-type: none"> <li>• VP / VC 速度を設定する場合は、64Kbps ~ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。</li> <li>• VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。             <ul style="list-style-type: none"> <li>- VPC が 1VPC の場合にだけ、VP シェーピングと VC シェーピングを同時に利用することができます。</li> <li>- VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。</li> </ul> </li> <li>• 本装置で複数 VPC を使って ATM 網を利用する場合は、以下のように設定してください。             <ul style="list-style-type: none"> <li>- 複数 VPC で VP シェーピングが必要となる場合は、1VPC あたり 1VCC となるようにネットワークを設計してください。このとき、16VPC まで利用することができます。</li> <li>- VP 速度は設定しないでください。契約時の VP 速度は VC 速度として設定し、サービスタイプを CBR に設定してください。</li> </ul> </li> <li>• VP シェーピングを必要としない場合は、複数 VPC 上で複数 VC シェーピングを行うことができます。</li> <li>• VP シェーピング時は、VC 速度 (CBR、GFR+)、平均速度 (SCR) および最低速度 (UBR+) の総和が VP 速度を超えないようにように設定してください。</li> <li>• VC シェーピング時は、VC 速度 (CBR、GFR+)、平均速度 (SCR) および最低速度 (UBR+) の総和が 25Mbps を超えないようにように設定してください。</li> </ul>
ATM25M 拡張モジュール H1	<ul style="list-style-type: none"> <li>• VP / VC 速度を設定する場合は、以下の設定範囲で設定してください。             <ul style="list-style-type: none"> <li>- 64Kbps ~ 25Mbps の範囲で 8Kbps または 50Kbps 刻みで指定します。</li> </ul> </li> <li>• VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。             <ul style="list-style-type: none"> <li>- VP 速度の総和を 25Mbps 以下に設定してください。</li> <li>- 1-VPC での VP / VC シェーピング時以外で、サービスタイプ UBR+ は設定できません。複数 VPC での VP / VC シェーピング時は VBR を設定してください。</li> <li>- サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。</li> <li>- サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。</li> <li>- サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。</li> <li>- サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。</li> <li>- VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。</li> </ul> </li> </ul>

拡張モジュール	注意点
ATM155M 拡張モジュールH1	<ul style="list-style-type: none"> <li>• VP / VC 速度を設定する場合は、以下の設定範囲で設定してください。                         <ul style="list-style-type: none"> <li>- VP 速度は、200Kbps ~ 50Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。</li> <li>- VC 速度は、64Kbps ~ 100Mbps の範囲で 8Kbps または 50Kbps 刻みで指定できます。</li> </ul> </li> <li>• VP シェーピングを前提とした運用を本装置で行う場合は、以下のように設定してください。                         <ul style="list-style-type: none"> <li>- VP 速度の総和を 50Mbps 以下に設定してください。</li> <li>- 1-VPC での VP / VC シェーピング時以外ではサービスタイプ UBR+ は設定できません。複数 VPC での VP / VC シェーピング時は VBR を設定してください。</li> <li>- サービスタイプが VBR の場合は、平均速度の総和が VP 速度を超えないように設定してください。</li> <li>- サービスタイプが CBR の場合は、VC 速度の総和が VP 速度を超えないように設定してください。</li> <li>- サービスタイプが UBR+ の場合は、最低速度の総和が VP 速度を超えないように設定してください。</li> <li>- サービスタイプが GFR+ の場合は、VC 速度の総和が VP 速度を超えないように設定してください。</li> <li>- VPC 内の VC 速度の最高速度は 50Mbps になります。</li> <li>- VP シェーピングを行う VPC と VP シェーピングを行わない VPC は、同一拡張モジュール内で同時に利用することはできません。</li> </ul> </li> <li>• DSU 接続する場合は、atm send clock コマンドで送信クロックの設定を recovery にしてください。                         <div style="border: 1px solid black; padding: 5px; margin-top: 10px; width: fit-content;">                             atm &lt;slot&gt; send clock recovery                         </div> </li> </ul>

● **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) を送信しています。

【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ます。

【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ます。

【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。  
 特に Si-R180B では初期設定で 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ます。

【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ます。

【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ます。

【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ます。

【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ません。

【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ません。

【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ありません。

【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です。

【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ません。

【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ありません。

【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です。

【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ました。

【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ました。

【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。

● **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）時間が同じです。

【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 が残っています。

【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ません。

【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し、ATM の場合は VC 速度を設定すると、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ません。

【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 が一致していません。

【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ません。

【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ません。
  - 【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ません。
  - 【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ます。
  - 【対処】 IPsec トンネルパケットと手動鍵送信用 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ました。
    - 【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ます。
    - 【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ます。
    - 【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 認証で失敗しています。

【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なっている場合、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ていません。

【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ます。

【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 アドレスおよび宛先 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ります。または、スタティック経路情報がありません。

【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 になっています。

【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ません。

【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ります。

【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ません。
  - 【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ります。または、不足しています。
  - 【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ません。
  - 【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ません。
  - 【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ります。
  - 【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ません。
  - 【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します。
  - 【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ませんでした。
  - 【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 になっています。
  - 【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ません。
  - 【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装置が存在しません。

【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）を指定しています。

【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定義を設定しています。

【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が一致していません。

【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



## 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」\(P35\)](#) 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 mismatched、psk mismatched、certificate mismatched、signature mismatched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. sir370->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
#
```

- Main Mode Responderの場合、以下の太字行に相手装置証明書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
Jun 16 15:09:55 192.168.1.1 Si-R570: init: system startup now.
Jun 16 15:09:55 192.168.1.1 Si-R570: sshd: generating public/private host key pair.
Jun 16 15:09:55 192.168.1.1 Si-R570: protocol: [mb/0] lan port link up
Jun 16 15:09:55 192.168.1.1 Si-R570: protocol: [mb/1] lan port link up
Jun 16 15:10:03 192.168.1.1 Si-R570: sshd: generated public/private host key pair.
Jun 16 15:10:03 192.168.1.1 Si-R570: isakmp: signature mismatched.
Jun 16 15:10:13 192.168.1.1 Si-R570: isakmp: signature mismatched.
Jun 16 15:10:30 192.168.1.1 Si-R570: isakmp: signature mismatched.
Jun 16 15:11:23 192.168.1.1 Si-R570: 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 Initiator 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】 \(P37\)](#)
- MTU、MRU 長の設定間違い→ [【対処 B】 \(P38\)](#)
- IPsec 対象先の経路情報の設定間違い→ [【対処 C】 \(P39\)](#)
- Pre-Shared Key 不一致→ [【対処 D】 \(P39\)](#)
- IPsec 対象範囲にパケットが送信されていない→ [【対処 E】 \(P40\)](#)
- 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】 \(P40\)](#)
- remote ap tunnel remote [address] の設定間違い→ [【対処 G】 \(P41\)](#)
- remote ip address local が未設定→ [【対処 H】 \(P42\)](#)

### 【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るても 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 トンネルの途中で 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
```

## 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 アダプターを接続しても VoIP ランプが点灯せず通話できない**

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

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

【原因】 VoIP アダプターの設定内容に問題があります。

【対処】 VoIP アダプターに設定した、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】 Si-R 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ます。

【対処】 Si-R 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 アダプターを Si-R に接続するポートに問題があります。

【対処】 VoIP アダプターは、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 Si-R に接続するポートに問題があります。

【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 Si-R を接続すると Si-R 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 です。

【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 に接続するとマイネットワークやタスクトレイに Si-R のアイコンが表示され、ダブルクリックすると Si-R の Web 設定画面が表示されます。

● **パソコンに Si-R 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 以外です。

【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 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ません。

【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。

## 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ません。

【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ません。

【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ません (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ません (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ません (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ません (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。

## 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す。

【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ます。

【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アドレスではありません。

【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ます。

【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、またはNS (Neighbor Solicitation) メッセージに応答する装置が存在します。

【対処】 仮想IPアドレスを解決するARPリクエスト、またはNS (Neighbor Solicitation) メッセージに응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を指定しています。

【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) を指定しています。

【対処】 優先度に最優先 (master) 以外を指定してください。



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ません。

【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ます。

【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。



コマンドユーザズガイド「[2.1.8 VRRP手動切り戻し機能を使う](#)」(P36)

Webユーザズガイド「[2.1.10 VRRP手動切り戻し機能を使う](#)」(P34)

【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ルータより低いです。

【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を指定していません。

【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。

● **本来のマスター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に設定されています。

【対処】 プリエンプトモードをonに設定してください。

【原因】 本来のマスターでダウントリガが発動しています。

【対処】 本来のマスターで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ー状態である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が同一ではありません。

VRRP情報の「VRID illegal packets」がカウントされています。

【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ありません。

VRRP情報の「Authentication failed packets」または「Authentication type mismatch packets」がカウントされています。

【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ます。

VRRP-ADメッセージ：

あて先IPアドレス : 224.0.0.18  
ff02::12

プロトコル番号 : 112

IPv6 Next Header : 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ます。

【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ます。

【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ます。

【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の設定が誤っています。

【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が故障しています。

【対処】 VRRPルータを連結しているHUBを調べてください。

● **マスター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ます。

【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になっていません。

【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 が同一ではありません。  
VRRP 情報の「Virtual router IP address configuration mismatched packets」がカウントされています。
- 【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ません。
- 【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す。
- 【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 につながらない**

- 【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ます。
- 【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) を指定しています。
- 【対処】 優先度に最優先 (master) 以外を指定してください。



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 を指定しています。

【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ます。
- 【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ます。
- 【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) を指定しています。
- 【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。



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 以下にはなりません。
- 【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ません。
  - 【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ません。
  - 【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ます (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ます。
  - 【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ます。
  - 【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ます。
  - 【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) または着信抑止 (dialreject) が発動したのに発信抑止または着信抑止しない**
  - 【原因】 発信抑止または着信抑止するリモートが ISDN (回線交換) / PPPoE 接続以外です。
  - 【対処】 発信抑止または着信抑止の仕様です。
- **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 ISDN (回線交換) / PPPoE 接続またはテンプレート着信による接続となっています。
  - 【対処】 切断／閉塞コマンドの仕様です。

## 2.11 外部メディアスタート機能に関するトラブル

外部メディアスタート機能に関するトラブルには、以下のようなものがあります。

- **CHECK / LAN0 / 100M / FULL ランプが橙色で点滅している (Si-R180B)**
- **LAN0 ~ 3 ランプが橙色で点滅している (Si-R220C、Si-R220D)**
- **LAN0 ~ 1 ランプ、SLOT0 ~ SLOT1 ランプが橙色で点滅している (Si-R240B)**

【原因】 外部メディアスタート機能が異常終了しました。

【対処】 システムログメッセージまたは USB メモリ内に作成された「output.txt」の内容を参照し、エラー内容を確認してください。

【原因】 外部メディアスタート機能でパスワード認証エラーが発生しました。

【対処】 装置に管理者パスワードが設定されている場合は、パスワードファイルを USB メモリ上に用意する必要があります。

☞ 参照 コマンドユーザズガイド「[2.6.5 パスワードファイルの作り方](#)」(P53)

- **装置が起動できない**

【原因】 外部メディアスタート機能の動作中に USB メモリが抜けた、または本装置の電源ケーブルが抜かれたなどの理由で、ファームウェアのインストールに失敗した可能性があります。

【対処】 バックアップファームを起動し、ファームウェアをインストールしてください。

☞ 参照 Si-R180B ご利用にあたって  
[「3.2 ファームウェア更新に失敗したときには \(バックアップファーム機能\)」](#) (P60)、  
 Si-R220C ご利用にあたって  
[「3.2 ファームウェア更新に失敗したときには \(バックアップファーム機能\)」](#) (P76)、  
 Si-R220D ご利用にあたって  
[「3.2 ファームウェア更新に失敗したときには \(バックアップファーム機能\)」](#) (P73)、  
 Si-R240B ご利用にあたって  
[「3.2 ファームウェア更新に失敗したときには \(バックアップファーム機能\)」](#) (P74)

## 2.12 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ません。

【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ます。

【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] + [ ] キーを処理してしまうため入力できません。

【対処】 端末ソフトウェアの設定で、[CTRL] + [ ] 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] + [ ] 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）を使用しています。

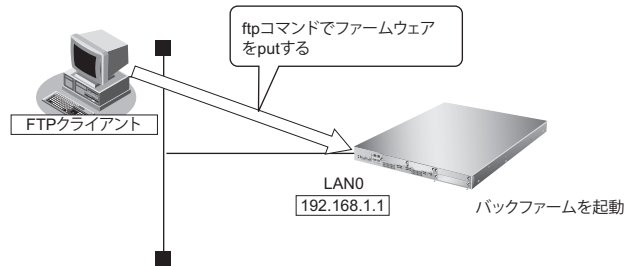
【対処】 矢印キーの代わりに [Ctrl] + [B] キーおよび [Ctrl] + [F] キーでカーソル移動、[Ctrl] + [P] キーおよび [Ctrl] + [N] キーでコマンド履歴移動を行ってください。

## 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。

ここでは、Si-R570 を例に説明します。



### 4.1 パソコン (FTP クライアント) を準備する

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 本装置を準備する

#### 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クライアントだけを接続してください。

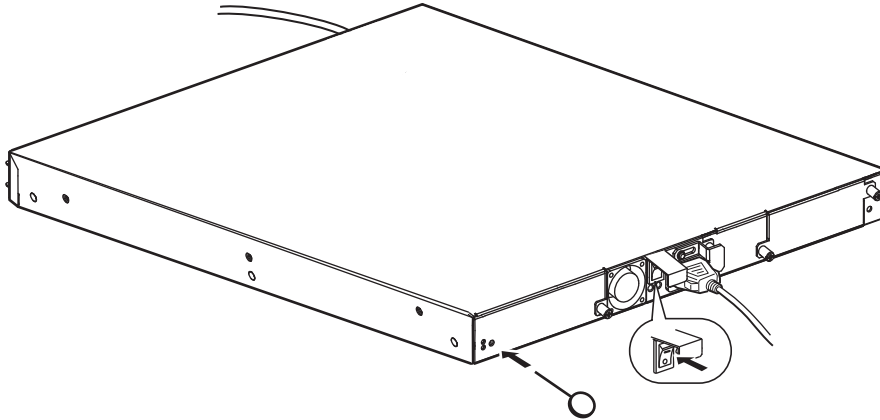
お使いになっている装置がSi-R180Bの場合は、インタフェースが逆であるため、LAN1 (Si-R180Bの場合はスイッチポート (SW1~4)) のIPアドレスが192.168.1.1になっています。LAN0は使用できません。

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 (Si-R180B、Si-R220C、Si-R220D、Si-R240B、Si-R260B、Si-R370、Si-R370B) または10/100/1000BASE-Tポート (Si-R570、Si-R570B) にケーブルを接続します。ただし、Si-R260BだけはAutoMDI/MDI-X機能をサポートしていないため、本装置のLAN0側のto HUB to PCスイッチをto PCにしてから、10/100BASE-TXポートにケーブルを接続します。

お使いになっている装置がSi-R180Bの場合は、初期設定ではスイッチポートが有効となっています。

3. 先の細いものでリセットスイッチを押しながら電源を投入します。



4. 以下の表に示すランプが緑色で点滅することを確認して、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。

装置名	緑色点滅するランプ
Si-R180B	CHECK / LAN0 / 100M / FULL / SW / SW1 ~ 4
Si-R220C、Si-R220D	CHECK / LAN0 ~ 3 / COM / B1 / B2
Si-R240B	CHECK / LAN0 ~ 1 / SLOT0 ~ 1
Si-R260B	CHECK / ATM25 / LAN0 ~ 3
Si-R370、Si-R370B	CHECK / SLOT0 / SLOT1 / LAN0 ~ 3
Si-R570、Si-R570B	CHECK / LAN0、1/Fiber / SLOT0 ~ 3 / LAN0 ~ 3



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転送します。

 参照 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](#)」(P62)、  
コマンドユーザーズガイド「[2.5.2 FTP サーバ機能によるファームウェアの更新](#)」(P47)

### 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。

 正常に更新が行われた場合、以下の表のランプが緑色と橙色で交互に点滅します。

装置名	緑色と橙色で交互に点滅するランプ
Si-R180B	CHECK / LAN0 / 100M / FULL
Si-R220C、Si-R220D	LAN0 ~ 3
Si-R240B	LAN0 ~ 1 / SLOT0 ~ 1
Si-R260B	LAN0 ~ 3
Si-R370、Si-R370B	LAN0 ~ 3
Si-R570、Si-R570B	LAN0 ~ 3

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。ここでは、Si-R570 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（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）またはLANケーブル



Si-R220D、Si-R370B、Si-R570Bの場合は、コンソールケーブルは同梱されていません。

「5.2 コンソールポートに接続する」(P57)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://fenics.fujitsu.com/products/manual/cable3/>

- 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）

### 5.1 LANで接続する

#### 本装置を準備する

### こんな事に気をつけて

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、パソコンだけを接続してください。

お使いになっている装置がSi-R180Bの場合は、インタフェースが逆であるため、LAN1（Si-R180Bの場合はスイッチポート（SW1～4））のIPアドレスが192.168.1.1になっています。LAN0は使用できません。

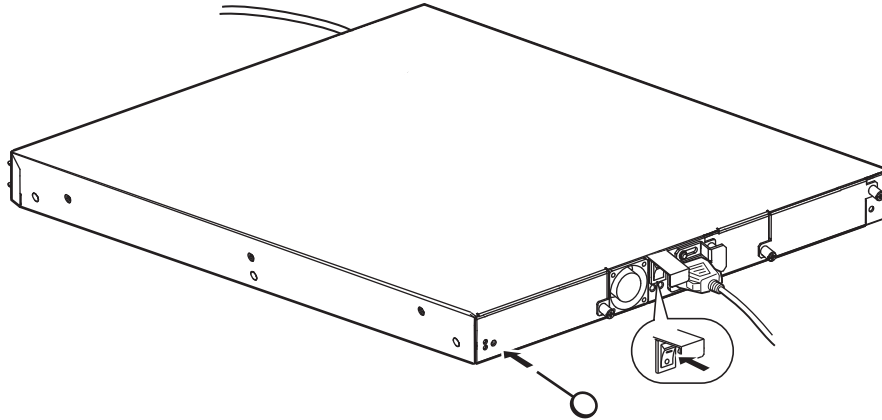
1. 本装置の電源が切れていることを確認します。
2. 本装置とパソコンをLAN接続します。



本装置とパソコンをHUBを介さず、直接、10/100BASE-TXポート（Si-R180B、Si-R220C、Si-R220D、Si-R240B、Si-R260B、Si-R370、Si-R370B）または10/100/1000BASE-Tポート（Si-R570、Si-R570B）にケーブルを接続します。ただし、Si-R260BだけはAutoMDI/MDI-X機能をサポートしていないため、本装置のLAN0側のto HUB to PCスイッチをto PCにしてから、10/100BASE-TXポートにケーブルを接続します。


お使いになっている装置がSi-R180Bの場合は、初期設定ではスイッチポートが有効となっています。

3. 先の細いものでリセットスイッチを押しながら電源を投入します。



4. 以下の表に示す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。

装置名	緑色点滅するランプ
Si-R180B	CHECK / LAN0 / 100M / FULL / SW / SW1 ~ 4
Si-R220C、Si-R220D	CHECK / LAN0 ~ 3 / COM / B1 / B2
Si-R240B	CHECK / LAN0 ~ 1 / SLOT0 ~ 1
Si-R260B	CHECK / ATM25 / LAN0 ~ 3
Si-R370、Si-R370B	CHECK / SLOT0 / SLOT1 / LAN0 ~ 3
Si-R570、Si-R570B	CHECK / LAN0、1/Fiber / SLOT0 ~ 3 / LAN0 ~ 3

 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

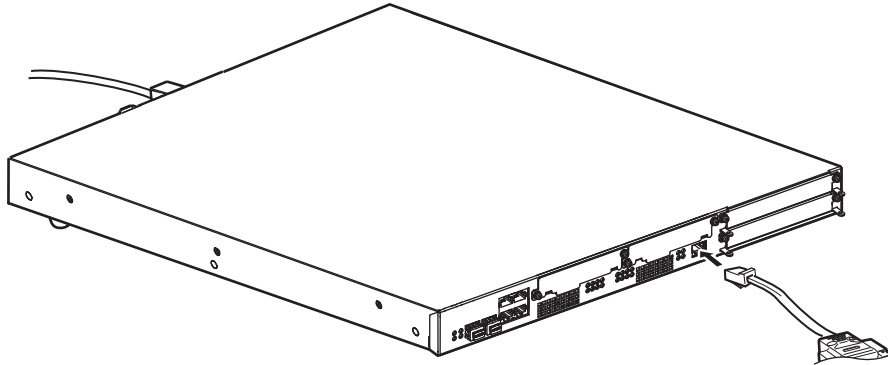
- telnet でログインします。  
パソコンには、本装置と同じネットワークの IP アドレスを設定してください。本装置のご購入時の IP アドレスは「192.168.1.1」、サブネットマスクは「255.255.255.0」です。
  - [Return] キーまたは [Enter] キーを押します。
  - 画面に「backup#」と表示されたことを確認します。
  - reset clear と入力して、[Return] キーまたは [Enter] キーを押します。  
本装置の構成定義情報が初期化されます。
- backup# reset clear (下線部入力)
- telnet 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。



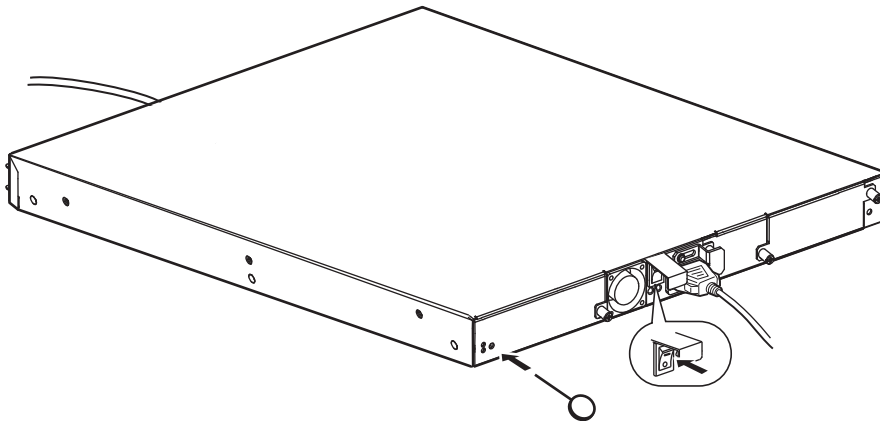
## 5.2 コンソールポートに接続する

### 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. RS232C ケーブルと同梱の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. 先の細いものでリセットスイッチを押しながら電源を投入します。



5. 以下の表に示す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。

装置名	緑色点滅するランプ
Si-R180B	CHECK / LAN0 / 100M / FULL / SW / SW1 ~ 4
Si-R220C、Si-R220D	CHECK / LAN0 ~ 3 / COM / B1 / B2
Si-R240B	CHECK / LAN0 ~ 1 / SLOT0 ~ 1
Si-R260B	CHECK / ATM25 / LAN0 ~ 3
Si-R370、Si-R370B	CHECK / SLOT0 / SLOT1 / LAN0 ~ 3
Si-R570、Si-R570B	CHECK / LAN0、1/Fiber / SLOT0 ~ 3 / LAN0 ~ 3



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. 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



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。

本装置をご購入時の状態で起動します。

# 索引

## A

ATM155 ポート ..... 13

## B

B1/B2 ランプ ..... 11, 16

## C

CHECK ランプ ..... 11

## F

FTP クライアント ..... 52

FX ポート ..... 13

## H

HyperTerminal ..... 55

## I

ipconfig ..... 13, 14

## N

NetBIOS ..... 50

## P

POWER ランプ ..... 11

PPPoE 接続 ..... 21

## R

RIP パケット ..... 7

RS232C ケーブル ..... 55

## S

SLOT ランプ ..... 11

## T

telnet ..... 13

## W

Windows NT 4.0 ..... 19

WWW ブラウザ ..... 14, 15

## え

エラーログ情報 ..... 11

## か

回線料金 ..... 7

## こ

ご購入時の状態に戻す ..... 55

コンソールケーブル ..... 55

## し

自動送信パケット ..... 8

## す

スケジュール機能 ..... 9

## た

ターミナルソフトウェア ..... 55

## ち

超過課金 ..... 7

## つ

通信料金 ..... 50

## て

データ通信 ..... 20

デフォルトルート ..... 9

## は

パスワード ..... 15

バックアップファーム機能 ..... 52

## ふ

ファームウェア更新 ..... 54

## ほ

本装置 IP アドレス ..... 15

**ま**

---

マニュアル構成 .....6

**り**

---

リセットスイッチ .....57

履歴 .....16

---

## Si-R シリーズ トラブルシューティング

P3NK-3942-06Z0

発行日 2017年6月

発行責任 富士通株式会社

---

- 本書の一部または全部を無断で他に転載しないよう、お願いいたします。
- 本書は、改善のために予告なしに変更することがあります。
- 本書に記載されたデータの使用に起因する第三者の特許権、その他の権利、損害については、弊社はその責を負いません。