

P3NK-4012-05Z0

FUJITSU Network Si-R Si-Rシリーズ

Webユーザーズガイド V35

The logo consists of the word "FUJITSU" in a bold, red, sans-serif font. Above the letter "I", there are two small, red, interlocking circles that form a stylized infinity symbol or a network node.

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

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 - 2014

目次

はじめに	2
本書の構成と使いかた	5
本書の読者と前提知識	5
本書の構成	5
本書における商標の表記について	6
本装置のマニュアルの構成	7
第 1 章 設定.....	8
1.1 WWW ブラウザを準備する	9
1.2 本装置のトップページを表示させる	10
1.3 本装置にログインする	11
1.4 パスワード情報を設定する	13
1.4.1 ログインパスワード情報を設定する	13
1.4.2 暗号化パスワード形式を設定する	14
1.4.3 ログインユーザ情報を設定する	15
1.5 時刻を設定する	18
1.6 設定方法を選ぶ	20
1.6.1 本装置を購入時の状態で使用する場合	20
1.6.2 「かんたん設定メニュー」で本装置を設定する場合	21
1.6.3 「基本設定」と「ルータ設定」で設定する場合	22
1.7 文字入力フィールドで入力できる文字一覧	23
第 2 章 運用管理とメンテナンス	24
2.1 操作メニューを使う	25
2.1.1 操作メニューを表示する	25
2.1.2 手動で回線を接続する／切断する	26
2.1.3 手動で LAN を有効化／無効化する	27
2.1.4 手動でスイッチポートを有効化／無効化する	28
2.1.5 手動で接続先を有効化／無効化する	29
2.1.6 手動でポリシーグループを有効化／無効化する	30
2.1.7 BGP セッションを操作する	31
2.1.8 ネットワークの接続を確認する	32
2.1.9 リモートパワーオン機能を使う	33
2.1.10 VRRP 手動切り戻し機能を使う	34
2.1.11 VRRP 手動停止／再開機能を使う	35
2.1.12 RADIUS サーバを手動で復旧する	36
2.1.13 データ通信カード (SIM) を設定する	37
2.1.14 MAC アドレスの収集を行う	40
2.1.15 無線 LAN アクセスポイントに MAC アドレスフィルタを配布する	41
2.1.16 無線 LAN アクセスポイントの無線 LAN チャンネルを調整する	42
2.1.17 無線 LAN アクセスポイントの電波出力を調整する	43
2.1.18 無線 LAN アクセスポイントの装置リセットを行う	44
2.2 表示メニューを使う	45
2.2.1 表示メニューを表示する	45
2.3 保守メニューを使う	49
2.3.1 保守メニューを表示する	49
2.3.2 本装置のファームウェアを更新する	50
2.3.3 構成定義情報を退避する／復元する	52

2.3.4	構成定義情報を切り替える	53
2.3.5	USB メモリを使う	54
2.3.6	電話番号を変更する	58
2.3.7	FTP/SFTP サーバ機能を使ってメンテナンスする	59

索引	63
-----------------	-----------

本書の構成と使いかた

本書では、本装置の基本的な設定方法とメンテナンス情報など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。
機器の設置および設定用パソコンの接続方法などは、対象装置の「ご利用にあたって」で説明しています。

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。

本書の構成

以下に、本書の構成と各章の内容を示します。

章タイトル	内容
第1章 設定	この章では、本装置の基本的な設定方法を説明します。
第2章 運用管理とメンテナンス	この章では、本装置の運用状況を管理または確認する方法、およびメンテナンスする方法を説明します。

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	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 (本書)	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。

第1章 設定



この章では、本装置の基本的な設定方法を説明します。

1.1	WWWブラウザを準備する	9
1.2	本装置のトップページを表示させる	10
1.3	本装置にログインする	11
1.4	パスワード情報を設定する	13
1.4.1	ログインパスワード情報を設定する	13
1.4.2	暗号化パスワード形式を設定する	14
1.4.3	ログインユーザ情報を設定する	15
1.5	時刻を設定する	18
1.6	設定方法を選ぶ	20
1.6.1	本装置を購入時の状態で使用する場合	20
1.6.2	「かんたん設定メニュー」で本装置を設定する場合	21
1.6.3	「基本設定」と「ルータ設定」で設定する場合	22
1.7	文字入力フィールドで入力できる文字一覧	23

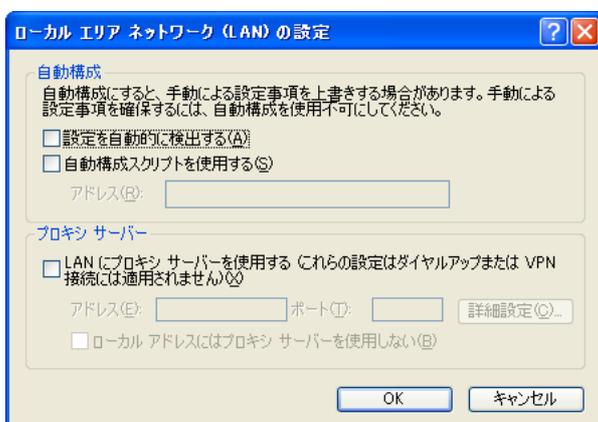
1.1 WWW ブラウザを準備する

本装置を利用するには、以下の WWW ブラウザを使用してください。

- Microsoft Internet Explorer Version 7.0
- Microsoft Internet Explorer Version 8.0

ブラウザの設定が、「Proxy (プロキシ) サーバ機能」を利用しないようになっていることを確認してください。以下のように確認します。

1. Microsoft Internet Explorer を起動します。
2. ツールバーまたはメニューバーの [ツール] をクリックし、「インターネットオプション」をクリックします。
3. インターネットオプション画面の「接続」タブで、「LAN の設定」 ボタンをクリックします。
4. プロキシサーバーの「LAN にプロキシサーバーを使用する」が選択されていないことを確認します。



Proxy サーバを使用する場合は、以下を参考にして本装置だけを Proxy の対象外にしてください。

1. Microsoft Internet Explorer を起動します。
2. ツールバーまたはメニューバーの [ツール] をクリックし、「インターネットオプション」をクリックします。
3. インターネットオプション画面の「接続」タブで、「LAN の設定」 ボタンをクリックします。
4. プロキシサーバーの「LAN にプロキシサーバーを使用する」が選択されていることを確認し、「詳細設定」 ボタンをクリックします。
5. 「HTTP」 にプロバイダの Proxy サーバを指定します。
6. 例外の「次で始まるアドレスにはプロキシを使用しない」に本装置の IP アドレス (192.168.1.1) を指定します。

1.2 本装置のトップページを表示させる

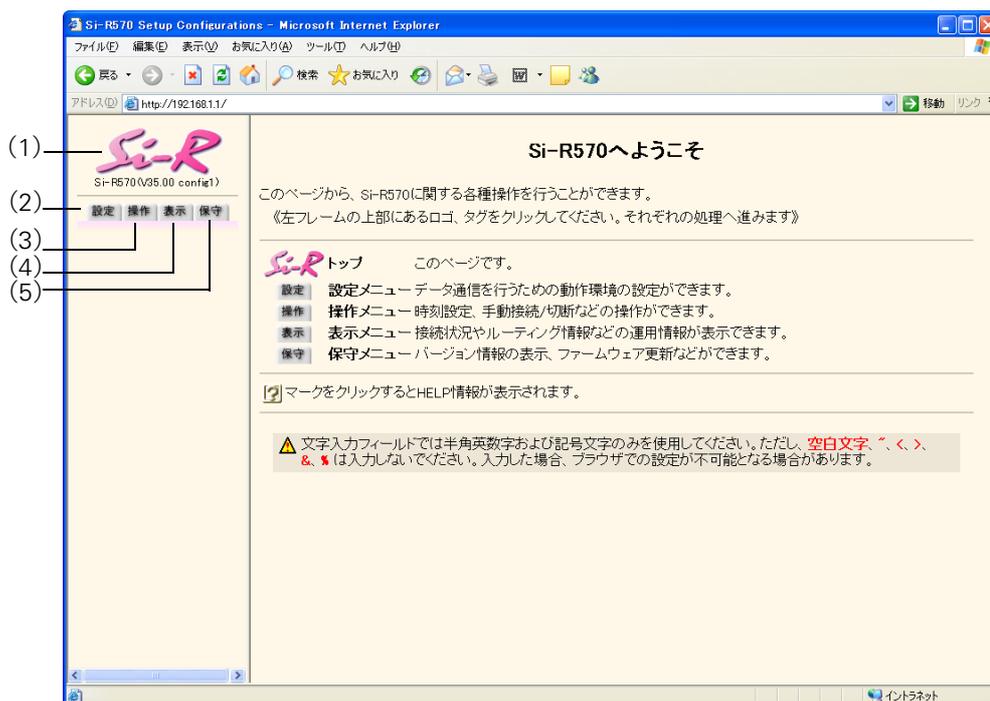
WWW ブラウザを使用して、本装置のトップページを表示します。

ここでは、Si-R570 の場合を例に説明します。

☛ 参照 「1.1 WWW ブラウザを準備する」 (P.9)

1. WWW ブラウザを起動します。
2. 本装置の URL 「http://192.168.1.1/」 を指定します。

本装置のトップページが表示されます。



画面左側に表示されるタブについて、以下に説明します。

- (1) 本装置ロゴ : クリックすると、トップページが表示されます。
- (2) [設定] タブ : Si-R180B、220C、220D の場合
 クリックすると、[かんたん設定メニュー] ボタンと [詳細設定メニュー] ボタンが表示されます。[詳細設定メニュー] ボタンをクリックすると、「基本設定」と「ルータ設定」が表示されます。
 Si-R240B、260B、370、370B、570、570B の場合
 クリックすると、設定メニューが表示されます。設定メニューには「基本設定」、「ルータ設定」があります。
- (3) [操作] タブ : クリックすると、操作メニューが表示されます。
- (4) [表示] タブ : クリックすると、表示メニューが表示されます。
- (5) [保守] タブ : クリックすると、保守メニューが表示されます。

☛ 参照 「2.1 操作メニューを使う」 (P.25)、 「2.2 表示メニューを使う」 (P.45)、 「2.3 保守メニューを使う」 (P.49)

1.3 本装置にログインする

ユーザ名とパスワードを入力することによって、本装置にログインすることができます。
ご購入時の状態では、管理者のみログインすることができます。

1. トップページ画面左側の【設定】タブをクリックします。

ログイン画面が表示されます。

2. 以下の項目を指定します。

- ユーザ名 : admin
- パスワード : 指定しない

ユーザ名	<input type="text" value="admin"/>
パスワード	<input type="password"/>

3. 【ログイン】ボタンをクリックします。

本装置のトップページ（ユーザ名：admin）が表示されます。

こんな事に気をつけて

一般ユーザでログインする場合は、一度管理者でログインしたあと、「パスワード情報」で一般ユーザのパスワードを設定し、再度一般ユーザでログインしてください。

☛ 参照 [「1.4 パスワード情報を設定する」\(P.13\)](#)

ユーザ名とパスワード

ユーザ名とパスワードは、管理者と一般ユーザによって異なります。

- ユーザ名
管理者は「admin」、一般ユーザは「user」です（固定ユーザ名）。
パスワード情報のログインユーザ情報で、AAA ユーザ情報または RADIUS サーバのユーザ情報を利用する設定とした場合、管理者および一般ユーザとして任意のユーザ名で追加設定することができます。
- パスワード
ご購入時は設定されていません。最初にログインしたときに必ずパスワード情報を設定してください。

☛ 参照 [「1.4 パスワード情報を設定する」\(P.13\)](#)

権限クラス（管理者クラスと一般ユーザクラス）

権限クラスには、管理者クラス（admin でログイン）と一般ユーザクラス（user でログイン）があります。

権限クラスによって実行できる画面が異なります。

権限クラスを移行する場合は、画面左側に表示される [ログアウト] ボタンをクリックしてください。本装置トップページが表示され、それ以降の処理でログイン画面が表示されます。

ログインしている権限クラスは、本装置ロゴの下に表示されるユーザ名で確認することができます。

以下に、管理者クラスと一般ユーザクラスで実行できる画面について示します。

○：実行できる、×：実行できない

権限クラス	画面名			
	設定メニュー	操作メニュー	表示メニュー	保守メニュー
管理者クラス	○	○	○	○
一般ユーザクラス	×	○（「疎通確認」画面のみ）	○（※）	×

※） 「統計情報」画面では、情報をクリアすることができません。クリアする場合は、管理者クラスに移行してください。

パスワード情報のログインユーザ情報で、AAA ユーザ情報または RADIUS サーバのユーザ情報を利用する設定とした場合の任意ユーザ名の権限クラスは、以下のとおり決定します。

- RADIUS サーバを使用する場合
RADIUS サーバに設定された Filter-ID アトリビュート情報により決定します。

RADIUS アトリビュート (番号)	設定
Filter-ID (11)	管理者クラスの場合 : "administrator" 一般ユーザクラスの場合 : "user"

- 本装置内のユーザ情報を使用する場合
「AAA 情報」 - 「AAA ユーザ情報」 - 「認証情報」の権限クラスの設定により決定します。

1.4 パスワード情報を設定する

1.4.1 ログインパスワード情報を設定する

パスワードを設定すると、WWW ブラウザ画面からの設定/コンソール、telnet からのログイン/FTP サーバ機能使用時に、パスワード入力によってログインを制限することができます。

こんな事に気をつけて

- 設定したパスワードを忘れた場合、ご購入時の状態に戻すことによって、パスワードを消すことができます。ただし、それまでの設定内容はすべて失われます。
 - 参照 [トラブルシューティング「5 ご購入時の状態に戻すには」\(P55\)](#)
- 一般ユーザでログインする場合は、一般ユーザのパスワードを設定してください。
- パスワードには8文字以上で、英字、数字、記号を混ぜた文字列を設定してください。7文字以下、英字のみ、数字のみのパスワードを設定した場合、および、設定を削除した場合は、脆弱である旨の警告が表示されます。

パスワード情報を設定する場合の例を示します。

1. 設定メニューの基本設定で「パスワード情報」をクリックします。

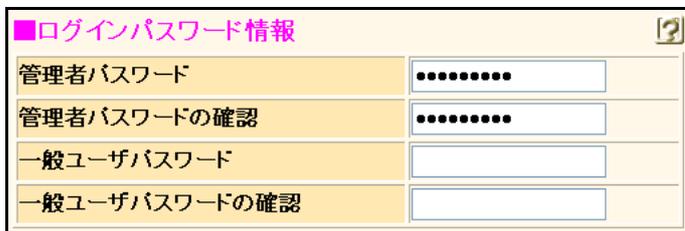
「パスワード情報」ページが表示されます。

2. 「ログインパスワード情報」をクリックします。

「ログインパスワード情報」が表示されます。

3. 以下の項目を指定します。

- 管理者パスワード → himitu132
- 管理者パスワードの確認 → himitu132



4. [更新] ボタンをクリックします。

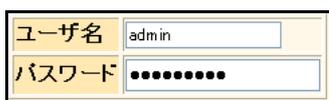
「パスワードを更新しました。更新した情報は、即時有効になります。」というメッセージが表示されます。

5. 画面左側の【設定】タブをクリックします。

ログイン画面が表示されます。

6. 以下の項目を指定します。

- ユーザ名 → admin
- パスワード → himitu132



7. [ログイン] ボタンをクリックします。

本装置のトップページ（ユーザ名：admin）が表示されます。

1.4.2 暗号化パスワード形式を設定する

本装置に設定した各種パスワード情報は、暗号化されて表示および保存されます。これにより、構成定義情報を見ただけでは平文パスワード文字列が分からず、不正ログインや不正アクセスを抑制する効果があります。

標準の暗号化パスワード文字列は共通パスワード形式で、装置故障などにより装置を交換した場合でも、保存しておいた各種暗号化パスワード文字列をそのまま復元することができます。しかし、暗号化パスワード文字列を含む構成定義情報をそのまま他装置に復元できるのはセキュリティ的に問題となる場合が考えられます。そのような場合は、暗号化パスワード文字列を装置固有パスワード形式に変更し、他装置には復元できなくすることで、セキュリティを強化することができます。装置固有パスワード形式に変更すると、設定済みの各種パスワード情報は自動的に装置固有パスワード形式で表示および保存されます。

本装置では、TCG (Trusted Computing Group) で策定された仕様に準拠したセキュリティチップ TPM (Trusted Platform Module) を内蔵しており、特定の装置上で設定された構成定義情報は、その装置だけでしか使えなくなるため、セキュリティを高めることができます。

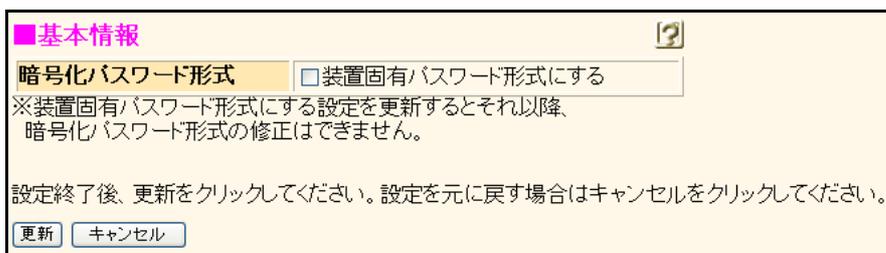
こんな事に気をつけて

- 装置固有パスワード形式に設定すると、共通パスワード形式に戻したり設定を削除することはできません。構成定義情報をご購入時の状態に戻すことによって、暗号化パスワード形式を共通パスワード形式に戻すことができます。
 参照 [トラブルシューティング \[5 ご購入時の状態に戻すには\] \(P55\)](#)
- 装置固有パスワード形式に設定すると、本装置が故障するなどして代替装置に交換した場合は、保存しておいた構成定義をそのまま復元できなくなります。装置に保存した構成定義を代替装置に復元する必要がある場合は、共通パスワード形式で作成した構成定義ファイルを別の場所に保管しておいてください。
 参照 [トラブルシューティング \[2.2 本装置設定時のトラブル\] \(P12\)](#)

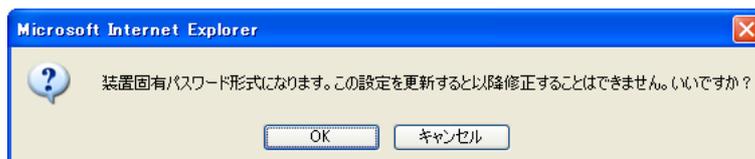
暗号化パスワード形式を装置固有パスワード形式に設定する手順を示します。

- 設定メニューの基本設定で「パスワード情報」をクリックします。
「パスワード情報」ページが表示されます。

- 「基本情報」をクリックします。
「基本情報」が表示されます。



- 暗号化パスワード形式の装置固有パスワード形式にするにチェックします。
装置固有パスワード形式への変更を確認する画面が表示されます。



4. [OK] ボタンをクリックします。

確認画面が閉じて、暗号化パスワード形式の装置固有パスワード形式にチェックがつきます。

■基本情報

暗号化パスワード形式 装置固有パスワード形式にする

5. [更新] ボタンをクリックします。

「基本情報を更新しました。更新した情報は、即時有効になります。」というメッセージが表示されます。

1.4.3 ログインユーザ情報を設定する

ログインユーザ情報を設定すると、個別のログインユーザ名でログインすることができるようになります。ログイン履歴はシステムログ情報で参照することができます。

こんな事に気をつけて

- ログインユーザ情報によるユーザ認証を行うには、ログインパスワード情報の管理者パスワードが設定されている必要があります。「1.4.1 ログインパスワード情報を設定する」(P.13) の内容に従って、必ず設定してください。
- ユーザ認証で参照する AAA 情報には、ユーザ ID とユーザ認証パスワードが設定されているか、ユーザ ID とユーザ認証パスワードが設定されている RADIUS 認証サーバが指定されている必要があります。ユーザ ID およびユーザ認証パスワードは、64 文字以内の ASCII 文字で設定してください。
- 本装置の固定ユーザ名である「admin」と「user」はログインユーザ情報によるユーザ認証を行いません。
- RADIUS サーバまたは本装置内のユーザ情報に権限クラスの設定がない場合は、正しい ID とパスワードが入力された場合でもログインできません。

ログインユーザ情報を設定する場合の例を示します。

● 設定条件

- RADIUS サーバの IP アドレス : 192.168.2.254
- RADIUS サーバのシークレット : radius-secret

ユーザ認証で参照する AAA 情報を設定する

1. 設定メニューの基本設定で「パスワード情報」をクリックします。

「パスワード情報」ページが表示されます。

2. 「ログインユーザ情報」をクリックします。

「ログインユーザ情報」が表示されます。

3. 以下の項目を指定します。

- 権限クラスは AAA/RADIUS サーバで設定する
- 参照する AAA 情報 → 参照する
AAA グループ ID → 0

■ログインユーザ情報

権限クラスはAAA/RADIUSサーバで設定する

参照するAAA情報

参照しない
 参照する

AAAグループID 0

認証プロトコル CHAP
 PAP

4. [保存] ボタンをクリックします。

RADIUS サーバ利用側の LAN 情報を設定する

5. 設定メニューのルータ設定で「LAN 情報」をクリックします。

「LAN 情報」ページが表示されます。

6. 「LAN 情報」でインタフェースが LAN1 の [修正] ボタンをクリックします。

「LAN1 情報 (物理 LAN)」ページが表示されます。Si-R180B でスイッチポートを利用している場合は、「LAN1 情報 (VLAN)」ページが表示されます。

7. 「IP 関連」をクリックします。

IP 関連の設定項目と「IP アドレス情報」が表示されます。

8. 以下の項目を指定します。

- IPv4 →使用する
- IP アドレス →指定する
 - IP アドレス →192.168.2.1
 - ネットマスク →24 (255.255.255.0)
 - ブロードキャストアドレス →ネットワークアドレス+オール1

IPv4	
	<input checked="" type="radio"/> 使用する <input type="radio"/> 使用しない
	<input type="radio"/> DHCPで自動的に取得する
	<input checked="" type="radio"/> 指定する
IPアドレス	IPアドレス: 192.168.2.1
	ネットマスク: 24 (255.255.255.0)
	ブロードキャストアドレス: ネットワークアドレス+オール1

9. [保存] ボタンをクリックします。

RADIUS サーバを利用する AAA グループ情報を設定する

10. 設定メニューのルータ設定で「AAA 情報」をクリックします。

「AAA 情報」ページが表示されます。

11. 「グループID 情報」をクリックします。

「グループID 情報」が表示されます。

12. 以下の項目を指定します。

- グループ名 →radiusAuth

<グループID情報追加フィールド>	
グループ名	radiusAuth

13. [追加] ボタンをクリックします。

「グループID 情報 (0)」と設定項目が表示されます。

14. 「RADIUS 関連」をクリックします。

RADIUS 関連の設定項目と「基本情報」が表示されます。

15. 以下の項目を指定します。

- RADIUS サービス
 - 認証 → クライアント機能
 - アカウントティング → チェックする
 - チェックしない
- 自側認証 IP アドレス → 192.168.2.1

■基本情報	
RADIUSサービス	クライアント機能 ▼ <input checked="" type="checkbox"/> 認証 <input type="checkbox"/> アカウントティング <small>(クライアント機能またはサーバ機能を選択した場合にのみ有効となります)</small>
自側認証IPアドレス	192.168.2.1

16. [保存] ボタンをクリックします。

17. RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「サーバ情報 (クライアント機能)」ページが表示されます。

18. 認証情報 1 の [修正] ボタンをクリックします。

19. 以下の項目を指定します。

- 認証情報 1
 - 共有鍵 → radius-secret
 - サーバ IP アドレス → 192.168.2.254

認証情報 1	共有鍵	●●●●●●●●
	サーバ IP アドレス	192.168.2.254
	サーバ UDPポート	<input checked="" type="radio"/> 1812 <input type="radio"/> 1645
	復旧待機時間	0 秒 ▼
	優先度	0
	自側認証 IP アドレス	

20. 認証情報 1 の [保存] ボタンをクリックします。

「サーバ情報 (クライアント機能)」に戻ります。

21. 画面左側の [設定反映] ボタンをクリックします。

設定した内容が有効になります。

1.5 時刻を設定する

本装置を運用開始する前に、必ず時刻を設定してください。

時刻を設定する方法は以下の3つがあります。

- ブラウザを利用しているパソコンの時刻を取得する方法
- ネットワーク上のTIME サーバまたはSNTP サーバから時刻を取得する方法
- 任意の時刻を設定する方法

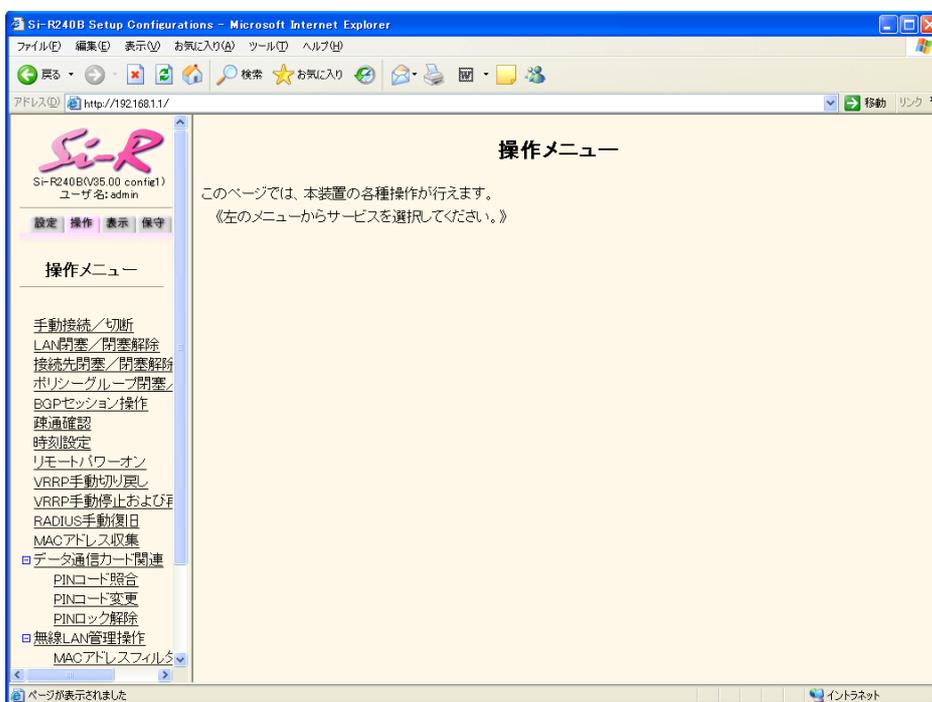
こんな事に気をつけて

- 72時間以上電源を切ったままにしておくと、時刻情報が失われます。
- 時刻を設定する場合は、管理者 (admin) でログインしてください。

☛ 参照 「1.3 本装置にログインする」 (R11)

1. 本装置のトップページで、画面左側の [操作] タブをクリックします。

操作メニューが表示されます。



2. 操作メニューで「時刻設定」をクリックします。

「時刻情報設定」ページが表示されます。

【時刻情報設定】

このページでは、本装置の時刻合わせを行うことができます。設定方法を選択し設定ボタンを押してください。

⚠ 72時間以上、電源を切ったままにすると時刻情報が失われます。

■時刻の設定

パソコンから時刻を取得	パソコンの現在時刻 2006年12月27日9時54分45秒	設定
タイムサーバから時刻を取得	サーバアドレス 設定されていません。	-
任意の時刻を設定	2006年12月27日09時54分26秒	設定

3. 時刻を設定する方法を以下の3つから選択します。

- パソコンから時刻を取得 → WWW ブラウザを利用しているパソコンの時刻を取得する
- タイムサーバから時刻を取得 → ネットワーク上の TIME サーバまたは SNTP サーバから時刻を取得する
- 任意の時刻を設定 → 現在の日時を入力する

4. 指定する時刻の設定方法の【設定】ボタンをクリックします。

「時刻を〇〇〇〇に設定しました。」というメッセージが表示されます。

1.6 設定方法を選ぶ

[設定] タブをクリックすると、設定用のメニューが表示されます。

設定用のメニューは、「かんたん設定」をサポートしているかどうかで表示される画面が異なります。

ここでは、以下の3つの設定方法について説明します。

- 「1.6.1 本装置を購入時の状態で使用する場合」(P.20) (Si-R180B)
本装置のIPアドレスを変更しない場合は、本装置の電源を投入するだけで通信することができます。
- 「1.6.2 「かんたん設定メニュー」で本装置を設定する場合」(P.21) (Si-R180B、220C、220D)
プライベートLAN構築、インターネットへISDN接続などを行う際に、1つの画面で最小限の項目を指定するだけで特定の接続構成を簡単に構築することができます。
- 「1.6.3 「基本設定」と「ルータ設定」で設定する場合」(P.22)
本装置のすべての構成定義情報について詳細に設定することができます。「かんたん設定」とは異なり、それぞれの画面で個別に項目を設定し、設定した情報を組み合わせて構築します。

1.6.1 本装置を購入時の状態で使用する場合

適用機種 Si-R180B

本装置は、購入時の状態ですぐにプライベートLANが使えるように設定されています。既存のLANにDHCPサーバがある場合は、パソコンに本装置を接続して、電源を投入するだけで使用することができます。

IPアドレスを変更する場合は、「かんたん設定」で設定する必要があります。

☛ 参照 Web 設定事例集 「1.4 プライベートLANを構築する」(P.57)

1.6.2 「かんたん設定メニュー」で本装置を設定する場合

適用機種 Si-R180B,220C,220D

[設定] タブをクリックすると、「かんたん設定メニュー」と「詳細設定メニュー」が表示されます。

通常設定する場合は、「かんたん設定メニュー」で十分に設定することができます。

「かんたん設定メニュー」の設定項目以外で設定が必要な場合は、「かんたん設定メニュー」で設定したあとに、「基本設定」と「ルータ設定」で設定を追加してください。

こんな事に気をつけて

- 「かんたん設定メニュー」で設定したあとに「詳細設定メニュー」で設定すると「かんたん設定メニュー」で設定した内容が変更されます。
- 「詳細設定メニュー」で設定したあとに「かんたん設定メニュー」で設定すると、「詳細設定メニュー」で設定した内容が無効となります。ただし、「パスワード情報」、「ファームウェア更新情報」は有効です。
- 「詳細設定メニュー」で設定した内容は、「かんたん設定メニュー」で確認できません。
- 本装置の IP アドレスを変更した場合は、パソコン側の設定も合わせて変更してください。
- 本装置の IP アドレスを変更した場合は、WWW ブラウザ上で新しい本装置の IP アドレスを URL に指定してください。

☛ 参照 「1.6.3 「基本設定」と「ルータ設定」で設定する場合」(P.22)

「かんたん設定メニュー」で設定した場合は、設定終了時に [設定終了] ボタンをクリックしてください。本装置が再起動され、設定が有効になります。ただし、データ通信が切断される場合があります。

以下に、かんたん設定で対応している接続形態と参照する設定方法箇所を示します。

機種名	接続形態	参照
Si-R180B	新規に LAN を構築し、CATV インターネット接続や既存のネットワークに一時的に LAN をつなぐときに使います。	Web 設定事例集 [1.1.1 プライベート LAN を構築する] (P.12)
	ネットワークに接続できるパソコン台数を超えたり、通信トラフィックが増加した場合など、ネットワークを分割するときに使います。	Web 設定事例集 [1.1.2 セグメント接続/分割する] (P.16)
	PPPoE プロトコルを利用したインターネット接続サービスをプライベート LAN 上の複数のパソコンから利用するときに使います。	Web 設定事例集 [1.1.3 PPPoE 接続する] (P.20)
Si-R220C、 Si-R220D	端末型ダイヤルアップ接続を行って、インターネットへ ISDN 接続するときに使います。	Web 設定事例集 [1.1.5 インターネットへ ISDN 接続する] (P.26)
	インターネットへ OCN エコノミーなどの専用線接続するときに使います。	Web 設定事例集 [1.1.6 インターネットへ専用線接続する] (P.31)
	PPPoE プロトコルを利用したインターネット接続サービスをプライベート LAN 上の複数のパソコンから利用するときに使います。	Web 設定事例集 [1.1.3 PPPoE 接続する] (P.20)
	事業所 LAN のネットワークどうしを ISDN 接続するときに使います。	Web 設定事例集 [1.1.7 オフィスへ ISDN 接続する] (P.35)
	事業所 LAN のネットワークどうしを専用線接続するときに使います。	Web 設定事例集 [1.1.8 オフィスへ専用線接続する] (P.40)
	新規に LAN を構築し、CATV インターネット接続や既存のネットワークに一時的に LAN をつなぐときに使います。	Web 設定事例集 [1.1.1 プライベート LAN を構築する] (P.12)
	ネットワークに接続できるパソコン台数を超えたり、通信トラフィックが増加した場合など、ネットワークを分割するときに使います。	Web 設定事例集 [1.1.2 セグメント接続/分割する] (P.16)

1.6.3 「基本設定」と「ルータ設定」で設定する場合

適用機種 全機種

Si-R180B、220C、220D では、[設定] タブをクリックすると、「かんたん設定メニュー」と「詳細設定メニュー」が表示されます。[詳細設定メニュー] ボタンをクリックすると、「基本設定」と「ルータ設定」が表示されます。その他の機種では、[設定] タブをクリックすると、「基本設定」と「ルータ設定」が表示されます。

「基本設定」と「ルータ設定」で設定した場合は、設定終了時に [設定反映] ボタンをクリックしてください。本装置が再起動され、設定が有効になります。ただし、データ通信が切断される場合があります。

こんな事に気をつけて

- 「かんたん設定メニュー」で設定したあとに「詳細設定メニュー」で設定すると「かんたん設定メニュー」で設定した内容が変更されます。
- 「詳細設定メニュー」で設定したあとに「かんたん設定メニュー」で設定すると、「詳細設定メニュー」で設定した内容が無効となります。ただし、「パスワード情報」、「ファームウェア更新情報」は有効です。
- 「詳細設定メニュー」で設定した内容は、「かんたん設定メニュー」で確認できません。
- 本装置の IP アドレスを変更した場合は、パソコン側の設定も合わせて変更してください。
- 本装置の IP アドレスを変更した場合は、WWW ブラウザ上で新しい本装置の IP アドレスを URL に指定してください。

参照 Web リファレンス 「1 「設定メニュー」を表示する」(P.11)

代表的な接続構成について：Web 設定事例集 「第 1 章 導入例」(P.11～)

詳細な設定（必要に応じて）：Web 設定事例集 「第 2 章 活用例」(P.205～)

1.7 文字入力フィールドで入力できる文字一覧

	+0	+1	+2	+3	+4	+5	+6	+7	+8	+9	+A	+B	+C	+D	+E	+F
20		!		#	\$	%(注)	&(注)	'	()	*	+	,	-	.	/
30	0	1	2	3	4	5	6	7	8	9	:	;	<(注)	=	>(注)	?
40	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
50	P	Q	R	S	T	U	V	W	X	Y	Z	[¥(注)]	^	_
60	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
70	p	q	r	s	t	u	v	w	x	y	z	{		}	_(注)	

注) ご使用のキーボードによって、「¥」の代わりに「\」、「」の代わりに「~」を入力してください。ご使用のターミナルソフトウェアやWWWブラウザによって、「¥」の代わりに「\」、「」の代わりに「~」が表示される場合があります。

WWWブラウザでの設定時に、文字入力フィールドに空白文字、「|」、「<」、「>」、「&」、「%」の文字を入力しないでください。これらの文字を入力した場合、WWWブラウザで設定できなくなります。

コマンドでの設定時には、「<」、「>」、「&」、「%」の文字は入力できますが、WWWブラウザでの設定ができなくなります。WWWブラウザで設定を行う場合は、これらの文字を使用しないようにコマンドで設定を変更してください。また、WWWブラウザで設定を行う場合は、空白文字を使用しないようにコマンドで設定を変更してください。

第2章 運用管理と メンテナンス



この章では、本装置の運用状況を管理または確認する方法、およびメンテナンスする方法を説明します。

2.1	操作メニューを使う.....	25
2.1.1	操作メニューを表示する.....	25
2.1.2	手動で回線を接続する／切断する.....	26
2.1.3	手動でLANを有効化／無効化する.....	27
2.1.4	手動でスイッチポートを有効化／無効化する.....	28
2.1.5	手動で接続先を有効化／無効化する.....	29
2.1.6	手動でポリシーグループを有効化／無効化する.....	30
2.1.7	BGPセッションを操作する.....	31
2.1.8	ネットワークの接続を確認する.....	32
2.1.9	リモートパワーオン機能を使う.....	33
2.1.10	VRRP手動切り戻し機能を使う.....	34
2.1.11	VRRP手動停止／再開機能を使う.....	35
2.1.12	RADIUSサーバを手動で復旧する.....	36
2.1.13	データ通信カード（SIM）を設定する.....	37
2.1.14	MACアドレスの収集を行う.....	40
2.1.15	無線LANアクセスポイントにMACアドレスフィルタを配布する.....	41
2.1.16	無線LANアクセスポイントの無線LANチャンネルを調整する.....	42
2.1.17	無線LANアクセスポイントの電波出力を調整する.....	43
2.1.18	無線LANアクセスポイントの装置リセットを行う.....	44
2.2	表示メニューを使う.....	45
2.2.1	表示メニューを表示する.....	45
2.3	保守メニューを使う.....	49
2.3.1	保守メニューを表示する.....	49
2.3.2	本装置のファームウェアを更新する.....	50
2.3.3	構成定義情報を退避する／復元する.....	52
2.3.4	構成定義情報を切り替える.....	53
2.3.5	USBメモリを使う.....	54
2.3.6	電話番号を変更する.....	58
2.3.7	FTP/SFTPサーバ機能を使ってメンテナンスする.....	59

2.1 操作メニューを使う

操作メニューでは、時刻設定、手動接続／切断、LAN 閉塞／閉塞解除、疎通確認、MAC アドレス収集、無線 LAN 管理操作などができます。

こんな事に気をつけて

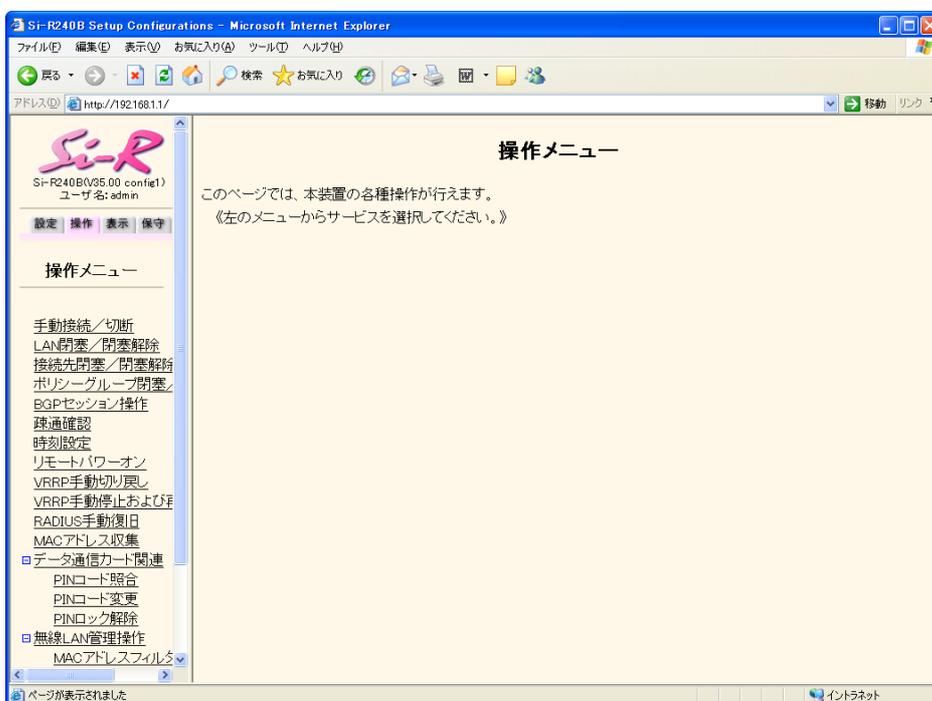
一般ユーザ (user) でログインしている場合は、「疎通確認」情報のみが表示され、操作することができます。その他の操作を使用する場合は、管理者 (admin) に移行してください。

☛ 参照 「1.3 本装置にログインする」(P.11)

2.1.1 操作メニューを表示する

適用機種 全機種

本装置のトップページで、画面左側の [操作] タブをクリックすると、操作メニューが表示されます。



スイッチポート閉塞／閉塞解除は、Si-R180B で表示されます。

データ通信カード関連は、Si-R240B で表示されます。

2.1.2 手動で回線を接続する／切断する

適用機種 全機種

接続先、または接続ユーザを指定して、手動で回線を接続／切断することができます。

接続する際、認証 ID および認証パスワードをワンタイムパスワードで設定することができます。

1. 操作メニューで「手動接続／切断」をクリックします。

「手動接続／切断」ページが表示されます。

【手動接続／切断】

このページでは、指定した接続先に対して手動による接続／切断操作をすることができます。

接続ごとに認証IDや認証パスワードを変更する場合には、ワンタイムパスワードの設定を行ってから接続をクリックしてください。

■接続先情報一覧

ネットワーク名	接続先名	通信手段	接続状態	操作
rmt1	ap1-0	PPPoE	未接続	<input type="button" value="接続"/>
rmt2	ap2-0	ISDN	回線ダウン	

■テンプレート接続情報一覧

テンプレート名	接続ユーザ名	通信手段	接続状態	操作
tmp0	IPsecIKE)c0a80200/24@example.com	動的VPN	接続中	<input type="button" value="切断"/>
tmp0	<input type="text"/>	動的VPN	未接続	<input type="button" value="接続"/>

■ワンタイムパスワード設定

送信認証ID	<input type="text"/>
送信認証パスワード	<input type="text"/>

2. 以下のどちらかの手順で設定します。

- 回線を接続する場合
「接続先情報一覧」または「テンプレート接続情報一覧」で [接続] ボタンをクリックします。
「接続先情報一覧」で接続する場合で、接続ごとに認証 ID や認証パスワードを変更するときは、「ワンタイムパスワード設定」で送信認証 ID と送信認証パスワードを設定してから、[接続] ボタンをクリックします。
「テンプレート接続情報一覧」で接続する場合は、接続ユーザ名を設定してから [接続] ボタンをクリックします。
- 回線を切断する場合
「接続先情報一覧」または「テンプレート接続情報一覧」で接続先または接続ユーザの欄の [切断] ボタンをクリックします。

2.1.3 手動で LAN を有効化／無効化する

適用機種 全機種

LAN を有効化／無効化することができます。

1. 操作メニューで「LAN 閉塞／閉塞解除」をクリックします。

「LAN 閉塞／閉塞解除」ページが表示されます。

【LAN閉塞／閉塞解除】

このページでは、指定したLANインタフェースに対して手動による閉塞／閉塞解除をすることができます。

▲ Webブラウザで使用しているLANインタフェースを閉塞すると、Webブラウザからの設定ができなくなります。

■ LANインタフェース一覧

LANインタフェース	状態	操作
lan0	非閉塞(リンクアップ)	閉塞
lan1	非閉塞(リンクアップ)	閉塞
lan2	非閉塞(リンクダウン)	閉塞
lan3	VLAN	

《 LANインタフェース複数指定 》
定義番号を指定せずに閉塞、閉塞解除を行うと全てのLANインタフェースに有効になります。

LAN定義番号

2. 以下のどちらかの手順で設定します。

- LAN を有効化する場合
LAN インタフェース一覧で LAN インタフェースの [閉塞解除] ボタンをクリックします。
または、「LAN 定義番号」に LAN 定義番号を入力して [閉塞解除] ボタンをクリックします。
- LAN を無効化する場合
LAN インタフェース一覧で LAN インタフェースの [閉塞] ボタンをクリックします。
または、「LAN 定義番号」に LAN 定義番号を入力して [閉塞] ボタンをクリックします。

2.1.4 手動でスイッチポートを有効化／無効化する

適用機種 Si-R180B

スイッチポートを有効化／無効化することができます。

1. 操作メニューで「スイッチポート閉塞／閉塞解除」をクリックします。

「スイッチポート閉塞／閉塞解除」ページが表示されます。

【スイッチポート閉塞／閉塞解除】

このページでは、指定したスイッチポートに対して手動による閉塞／閉塞解除をすることができます。

■スイッチポート一覧

スイッチポート	状態	操作
1	非閉塞	<input type="button" value="閉塞"/>
2	閉塞	<input type="button" value="閉塞解除"/>
3	非閉塞	<input type="button" value="閉塞"/>
4	閉塞(リンクダウン)	<input type="button" value="閉塞"/>

《スイッチポート複数指定》
定義番号を指定せずに閉塞、閉塞解除を行うと全てのスイッチポートに有効になります。

スイッチポート番号

2. 以下のどちらかの手順で設定します。

- スイッチポートを有効化する場合
スイッチポート一覧でスイッチポート（SW1～4）の [閉塞解除] ボタンをクリックします。
または、「スイッチポート番号」にスイッチポート番号を入力して [閉塞解除] ボタンをクリックします。
- スイッチポートを無効化する場合
スイッチポート一覧でスイッチポートの [閉塞] ボタンをクリックします。
または、「スイッチポート番号」にスイッチポート番号を入力して [閉塞] ボタンをクリックします。

2.1.5 手動で接続先を有効化／無効化する

適用機種 全機種

接続先を有効化／無効化することができます。

1. 操作メニューで「接続先閉塞／閉塞解除」をクリックします。

「接続先閉塞／閉塞解除」ページが表示されます。

【接続先閉塞／閉塞解除】

このページでは、指定した接続先に対して手動による閉塞(切断)/閉塞解除(接続)操作をすることができます。

接続ごとに認証IDや認証パスワードを変更する場合には、ワンタイムパスワードの設定を行ってから閉塞解除をクリックしてください。接続先複数指定を行う場合は、設定できません。

■接続先情報一覧

相手定義番号	ネットワーク名	接続先定義番号	接続先名	種別	接続状態	操作
0	vpn-hon	0	honsya	IPsec/IKE	接続中	閉塞
1	rmt1	0	ap1-0	PPPoE	未接続	接続
2	rmt2	0	ap2-0	ISDN	回線ダウン	

《 接続先複数指定 》
定義番号を指定せずに閉塞、閉塞解除を行うと全ての接続先に有効になります。

相手定義番号	<input type="text"/>	閉塞 閉塞解除
接続先定義番号	<input type="text"/> ※相手定義番号に指定した場合のみ有効です。	

■ワンタイムパスワード設定

送信認証ID	<input type="text"/>
送信認証パスワード	<input type="text"/>

2. 以下のどちらかの手順で設定します。

- 接続先を有効化する場合
接続先情報一覧で接続先の [閉塞解除] ボタンをクリックします。
または、「相手定義番号」と「接続先定義番号」を入力して [閉塞解除] ボタンをクリックします。
すべての接続先を一括で有効化するには、「相手定義番号」と「接続先定義番号」に何も入力しないで [閉塞解除] ボタンをクリックします。
- 接続先を無効化する場合
接続先情報一覧で接続先の [閉塞] ボタンをクリックします。
または、「相手定義番号」と「接続先定義番号」を入力して [閉塞] ボタンをクリックします。
すべての接続先を一括で無効化するには、「相手定義番号」と「接続先定義番号」に何も入力しないで [閉塞] ボタンをクリックします。

こんな事に気をつけて

接続ごとに認証IDや認証パスワードを変更する場合は、ワンタイムパスワードの設定を行ってから [閉塞解除] ボタンをクリックしてください。接続先複数指定を行う場合は、設定できません。

2.1.6 手動でポリシーグループを有効化／無効化する

適用機種 全機種

ポリシーグループを有効化／無効化することができます。

1. 操作メニューで「ポリシーグループ閉塞／閉塞解除」をクリックします。

「ポリシーグループ閉塞／閉塞解除」ページが表示されます。

【ポリシーグループ閉塞／閉塞解除】

このページでは、指定したポリシーグループに対して手動による閉塞／閉塞解除をすることができます。

■ポリシーグループ一覧

ポリシーグループ	状態	操作
0	閉塞中	<input type="button" value="閉塞解除"/>
1	非閉塞(送出先回線ダウン)	<input type="button" value="閉塞"/>
2	非閉塞	<input type="button" value="閉塞"/>
3	非閉塞(監視失敗)	<input type="button" value="閉塞"/>
4	構成定義不備	

《 ポリシーグループ複数指定 》
定義番号を指定せずに閉塞、閉塞解除を行うと全てのポリシーグループに有効になります。

ポリシーグループ定義番号

2. 以下のどちらかの手順で設定します。

- ポリシーグループを有効化する場合
ポリシーグループ一覧でポリシーグループの「閉塞解除」ボタンをクリックします。
または、「ポリシーグループ定義番号」にポリシーグループ定義番号を入力して「閉塞解除」ボタンをクリックします。
- ポリシーグループを無効化する場合
ポリシーグループ一覧でポリシーグループの「閉塞」ボタンをクリックします。
または、「ポリシーグループ定義番号」にポリシーグループ定義番号を入力して「閉塞」ボタンをクリックします。

2.1.7 BGP セッションを操作する

適用機種 全機種

BGP セッションの再接続や経路情報の再交換を行う機能です。属性変更やフィルタ設定を変更した場合、その設定は設定変更前に送受信された経路情報には反映されませんが、この機能を使用することで反映させることができます。

こんな事に気をつけて

IPv6 セッションは Si-R180B、220C、220D、240B、570、570B だけで使用できます。

IPv6 セッションを Si-R570、570B で使用する場合は、拡張用 512M メモリモジュールが必要です。

1. 操作メニューで「BGP セッション操作」をクリックします。

「BGP セッションの操作」ページが表示されます。

【BGPセッションの操作】

このページでは、BGPセッションの再接続、UPDATEメッセージの送信、または、ROUTE REFRESHメッセージの送信による経路情報の再送要求を実行できます。
BGPセッション指定を行ってから操作をクリックしてください。

■BGPセッション指定

BGPセッション	<input type="radio"/> すべての IPv4セッション
	<input checked="" type="radio"/> IPv4セッションの IPアドレス指定
	<input type="radio"/> すべての IPv6セッション
	<input type="radio"/> IPv6セッションの IPアドレス指定

IPv4アドレス

IPv6アドレス

■操作

BGPセッション	再接続
UPDATEメッセージ	送信
ROUTE REFRESHメッセージ	送信
UPDATE*ROUTE REFRESHメッセージ	送信

2. 「BGP セッション指定」で、操作するセッションを指定します。

3. 「操作」で、操作するボタンをクリックします。

2.1.8 ネットワークの接続を確認する

適用機種 全機種

ping コマンドを使って、IP 接続が成立しているかどうか確認することができます。

1. 操作メニューで「疎通確認」をクリックします。

「疎通確認 (ping)」ページが表示されます。

【疎通確認(ping)】

このページでは、pingコマンド(ICMP ECHOパケット)による通信の確認ができます。

送信先

送信先を設定し、ping送信をクリックしてください。設定を元に戻す場合はキャンセルをクリックしてください。

2. 「送信先」に送信先の IP アドレスを指定します。

3. 【ping送信】 ボタンをクリックします。

「ping実行中」というメッセージが表示されたあと、ブラウザ画面に ping 送信結果が表示されます。

2.1.9 リモートパワーオン機能を使う

適用機種 全機種

遠隔地にあるパソコンの電源投入を行う機能です。電源を投入するパソコンは、あらかじめ「ホストデータベース情報」－「リモート電源制御」で「対象」として登録しておく必要があります。

1. 操作メニューで「リモートパワーオン」をクリックします。

「リモートパワーオン」ページが表示されます。

【リモートパワーオン】

 Wakeup on LAN に対応したパソコンに対してだけ有効です。

《リモートパワーオン機能に必要な情報が設定されているホスト情報の一覧です。》

■ホスト情報一覧

	ホスト名	IPアドレス	MACアドレス	操作
1	spring	192.168.1.10	00:00:00:0a:0a:0a	<input type="button" value="オン"/>
2	summer	192.168.1.11	00:00:00:0b:0b:0b	<input type="button" value="オン"/>
3	autumn	192.168.1.12	00:00:00:0c:0c:0c	<input type="button" value="オン"/>
4	winter	192.168.1.13	00:00:00:0d:0d:0d	<input type="button" value="オン"/>

2. 起動するパソコンの [オン] ボタンをクリックします。

本装置が該当するパソコンに対して「Magic Packet」を送信し、パソコンが起動します。



パソコンが Magic Packet を受信してから起動が完了するまで、数十秒から数分かかります（お使いの機種や OS によって異なります）。

こんな事に気をつけて

本機能は、Wake up on LAN に対応したパソコンだけ利用できます。Wake up on LAN 対応機種については、パソコンのメーカーにお問い合わせください。

2.1.10 VRRP 手動切り戻し機能を使う

適用機種 全機種

VRRP グループの動作を、一時的にプリエンプトモードが ON に設定されたものとして動作させます。これにより、プリエンプトモードが OFF に設定された本装置の VRRP グループが、現在のマスタールータより優先度の高いバックアップルータである場合、マスタールータに状態を切り戻すことができます。本装置の VRRP グループのプリエンプトモードが ON に設定されていたり、現在のマスタールータの優先度のほうが高い場合、要求は無視されます。

1. 操作メニューで「VRRP 手動切り戻し」をクリックします。

「VRRP 手動切り戻し」ページが表示されます。

【VRRP 手動切り戻し】

VRRP グループの動作を、一時的にプリエンプトモードが ON に設定されたものとして動作させます。これにより、プリエンプトモードが OFF に設定された本装置の VRRP グループが現在のマスタールータより優先度の高いバックアップルータである場合、マスタールータに状態を切り戻すことができます。本装置の VRRP グループのプリエンプトモードが ON であったり、現在のマスタールータの優先度のほうが高い場合、要求は無視されます。

《情報一覧より切り戻しを行うグループを選択して実行をクリックしてください。》

■VRRP グループ情報一覧

インターフェース	グループID	プライオリティ	仮想IPアドレス	実行
lan0	1	255(最優先)	インターフェースアドレス	実行
lan0	2	5	192.168.10.10	実行
lan2	3	6	192.168.100.1 192.168.1.2	実行

2. 切り戻しを行うグループの [実行] ボタンをクリックします。

切り戻しが行われます。

2.1.11 VRRP 手動停止／再開機能を使う

適用機種 全機種

VRRP グループの動作を手動で停止状態にしたり、停止状態にした VRRP グループの動作を再開させることができます。停止状態にした場合の VRRP グループ状態はイニシャル状態となります。

再開を実行した場合でも、VRRP グループが定義された LAN が異常であるときは再開できません。異常復旧により開始します。また、手動停止していない VRRP グループを指定した場合、要求は無視されます。

1. 操作メニューで「VRRP 手動停止／再開」をクリックします。

「VRRP 手動停止／再開」ページが表示されます。

【VRRP 手動停止および再開】

本装置の VRRP グループの動作を、手動にて停止状態にしたり、停止状態にした VRRP グループを再開したりすることができます。

停止状態にした場合の VRRP グループ状態は Initial 状態となります。

再開を実行した場合であっても VRRP グループが定義された LAN が異常である場合は再開しません。異常復旧により開始します。また、手動停止していない VRRP グループを指定した場合は要求を無視します。

《情報一覧より処理を行うグループを選択して停止/再開をクリックしてください。》

■VRRP グループ情報一覧

インターフェース	グループ ID	プライオリティ	仮想 IP アドレス	実行
lan0	1	255(最優先)	インターフェースアドレス	<input type="button" value="停止"/> <input type="button" value="再開"/>
lan0	2	5	192.168.10.10	<input type="button" value="停止"/> <input type="button" value="再開"/>
lan2	3	6	192.168.100.1 192.168.1.2	<input type="button" value="停止"/> <input type="button" value="再開"/>

2. 以下のどちらかの手順で設定します。

- 手動停止する場合
[VRRP グループ情報一覧] で停止するグループの欄の [停止] ボタンをクリックします。
- 再開する場合
[VRRP グループ情報一覧] で再開するグループの欄の [再開] ボタンをクリックします。

2.1.12 RADIUS サーバを手動で復旧する

適用機種 全機種

dead 状態になった RADIUS サーバとの接続状態を手動で alive 状態に復旧させることができます。

1. 操作メニューで「RADIUS 手動復旧」をクリックします。

「RADIUS 手動復旧」ページが表示されます。

【RADIUS 手動復旧】

dead 状態になった RADIUS サーバとの接続状態を手動で alive 状態に復旧させることができます。
《情報一覧より復旧を行うサーバの復旧ボタンをクリックしてください。》

■サーバ情報一覧

AAAグループID	種別	定義番号	IPアドレス	ポート番号	優先度	状態	復旧残り時間(秒)	操作
0	認証	0	192.168.2.5	1812	255	dead	0/1800	<input type="button" value="復旧"/>
	認証	1	192.168.2.6	1812	100	alive	-	
	アカウントティング	0	192.168.2.5	1813	0	alive	-	
	アカウントティング	1	192.168.2.6	1813	100	alive	-	

2. 「サーバ情報一覧」で復旧するサーバの欄の「復旧」ボタンをクリックします。

2.1.13 データ通信カード (SIM) を設定する

適用機種 Si-R240B

PINコードによる照会をサポートしているデータ通信カードを使用するときに有効です。

こんな事に気をつけて

本操作は、WAN 情報にデータ通信カードを定義したときだけ有効です。

PINコード照合

データ通信カードが盗難、紛失された場合に無断使用を防止するための機能です。

データ通信カードに内蔵されたSIMにあらかじめPINコードを設定することにより、設定したPINコードで認証を行わない限り、使用できなくなります。

こんな事に気をつけて

原則としてPINコード認証に連続して3回失敗すると、PINロック状態になります。

ただし、前回認証に失敗したPINコードを再度入力した場合は、SIMに対して認証を行いません。

結果として、PINコード認証に連続して3回以上失敗した場合でもPINロック状態にならない場合があります。

1. 操作メニューで「データ通信カード関連」の「PINコード照合」をクリックします。

「PINコード照合」ページが表示されます。

【PINコード照合】

データ通信カードが盗難、紛失された場合に無断使用を防止するための機能です。
データ通信カードに内蔵されたSIMにあらかじめPINコードを設定することにより、設定したPINコードで認証を行わない限り、使用できなくなります。

⚠ 複数回PINコード照合に失敗すると、PINロック状態になる場合があります。

ポート

PINコード

2. 「ポート」でデータ通信カードを装着したスロットを選択します。

3. 以下のどちらかの手順で設定します。

- PINコード照合をしない場合
「PINコード」を入力し、[照合しない] ボタンをクリックします。
- PINコード照合をする場合
「PINコード」を入力し、[照合する] ボタンをクリックします。

PINコード変更

現在データ通信カード（SIM）に設定してあるPINコードを「旧PINコード」に入力し、変更したいPINコードを「新PINコード」に入力して更新します。

PINコード変更は、データ通信カード（SIM）がPINコード照合を行う設定のときだけ有効です。

こんな事に気をつけて

- PINコードは、4～8文字以内の数字で指定してください。
- データ通信カード（SIM）に設定したPINコードを「WAN情報」-「基本情報」のPINコードに設定してください。
- 原則としてPINコード認証に連続して3回失敗すると、PINロック状態になります。
ただし、前回認証に失敗したPINコードを再度入力した場合は、SIMに対して認証を行いません。
結果として、PINコード認証に連続して3回以上失敗した場合でもPINロック状態にならない場合があります。

1. 操作メニューで「データ通信カード関連」の「PINコード変更」をクリックします。

「PINコード変更」ページが表示されます。

【PINコード変更】

現在データ通信カード（SIM）に設定してあるPINコードを「旧PINコード」に入力し、変更したいPINコードを「新PINコード」に入力して更新してください。
PINコード変更は、データ通信カード（SIM）がPINコード照合を行う設定の時のみ有効です。

 データ通信カード（SIM）に設定したPINコードをWAN情報-基本情報のPINコードに設定してください。
複数回PINコード照合に失敗すると、PINロック状態になる場合があります。

ポート	スロット0-0 
旧PINコード	<input type="text"/>
新PINコード	<input type="text"/>
新PINコードの確認	<input type="text"/>

2. 「ポート」でデータ通信カードを装着したスロットを選択します。

3. 「旧PINコード」、「新PINコード」、「新PINコードの確認」に値を入力し、「更新」ボタンをクリックします。

PIN ロック解除

データ通信カード (SIM) が PIN ロック状態となった場合に、PIN ロック解除を行い、PIN コードを設定し直すことができます。

通信事業者から提示された PUK コード (ロック解除コード) を指定して更新してください。

こんな事に気をつけて

- PIN/PUK コードは、4～8 文字以内の数字で指定してください。
- データ通信カード (SIM) に設定した PIN コードを「WAN 情報」-「基本情報」の PIN コードに設定してください。
- 原則として PUK コード認証に連続して 10 回失敗すると、ロック状態を解除できなくなります。
ただし、前回認証に失敗した PUK コードを再度入力した場合は、SIM に対して認証を行いません。
結果として、PUK コード認証に連続して 10 回以上失敗した場合でもロック状態を解除できる場合があります。

1. 操作メニューで「データ通信カード関連」の「PIN ロック解除」をクリックします。

「PIN ロック解除」ページが表示されます。

【PINロック解除】

データ通信カード (SIM) が PIN ロック状態となった場合に、PIN ロック解除を行い、PIN コードを設定しなおすことができます。
通信事業者から提示された PUK コード (ロック解除コード) を指定して更新してください。

▲ データ通信カード (SIM) に設定した PIN コードを WAN 情報-基本情報の PIN コードに設定してください。
複数回 PIN ロック解除に失敗すると、データ通信カード (SIM) が使用できなくなる場合があります。

ポート	スロット0-0
PUKコード	<input type="text"/>
新PINコード	<input type="text"/>
新PINコードの確認	<input type="text"/>

2. 「ポート」でデータ通信カードを装着したスロットを選択します。

3. 「PUKコード」、「新PINコード」、「新PINコードの確認」に値を入力し、[更新] ボタンをクリックします。

2.1.14 MACアドレスの収集を行う

適用機種 全機種

MACアドレスの収集を行ったり、収集したMACアドレスをAAA情報に登録することができます。
ここでは、MACアドレスを収集して、それをAAA情報に登録する方法について説明します。

1. 操作メニューで「MACアドレス収集」をクリックします。

「MACアドレス収集」ページが表示されます。

2. 「MACアドレス収集開始」のグループIDを指定して、「収集開始」ボタンをクリックします。

MACアドレス収集機能が動作を開始します。

3. 「MACアドレス収集停止」の「収集停止」ボタンをクリックします。

MACアドレス収集機能が停止します。

「収集したMACアドレス一覧」に収集したMACアドレスの一覧が表示されます。

4. 「MACアドレスの登録」から登録するMACアドレスのリスト番号とパスワードを指定します。

5. 「登録」ボタンをクリックします。

2.1.15 無線 LAN アクセスポイントに MAC アドレスフィルタを配布する

適用機種 全機種

設定済みの MAC アドレスフィルタをフィルタセット単位で管理対象となった無線 LAN アクセスポイントに配布することができます。

こんな事に気をつけて

管理対象機器は、弊社製の無線 LAN アクセスポイント (SR-M20AP1) のみとなります。

1. 操作メニューで「無線 LAN 管理操作」の「MAC アドレスフィルタ配布」をクリックします。「MAC アドレスフィルタ配布」ページが表示されます。

【MAC アドレスフィルタ配布】

このページでは、設定済みの MAC アドレスフィルタをフィルタセット単位で、管理対象となった無線 LAN アクセスポイントに配布することができます。

《配布したい MAC アドレスフィルタセットを選択して、MAC アドレスフィルタ配布をクリックしてください。》

■管理機器一覧

グループ		管理機器			MAC アドレスフィルタセット名
定義番号	グループ名	定義番号	管理機器名	タイプ	
0	GroupA	0	AP_A01	wlan	<input type="text"/>
		1	AP_A02	wlan	<input type="text"/>

2. MAC アドレスフィルタを配布する管理機器に、MAC アドレスフィルタセット名を指定します。



- MAC アドレスフィルタを配布しない管理機器の MAC アドレスフィルタセット名は、空欄のままとしてください。
- 管理機器の MAC アドレスフィルタをクリアしたい場合は、MAC アドレスフィルタが設定されていない MAC アドレスフィルタセットを選択して、配布してください。

3. 【MAC アドレスフィルタ配布】 ボタンをクリックします。

MAC アドレスフィルタ配布の実行結果が表示され、管理対象となった無線 LAN アクセスポイントに MAC アドレスフィルタの配布が行われます。

2.1.16 無線 LAN アクセスポイントの無線 LAN チャンネルを調整する

適用機種 全機種

管理対象となった無線 LAN アクセスポイントの無線 LAN チャンネルを自動的に調整することができます。

こんな事に気をつけて

管理対象機器は、弊社製の無線 LAN アクセスポイント (SR-M20AP1) のみとなります。

1. 操作メニューで「無線 LAN 管理操作」の「無線 LAN チャンネルの自動調整」をクリックします。「無線 LAN チャンネルの自動調整」ページが表示されます。

【無線 LAN チャンネルの自動調整】

このページでは、管理対象となった無線 LAN アクセスポイントの無線 LAN チャンネルを自動的に調整することができます。

《無線 LAN チャンネルの自動調整を実施したい管理機器のチェックボックスにチェックをして、チャンネル自動調整をクリックしてください。》

■管理機器一覧

グループ		管理機器			チャンネル 自動調整
定義番号	グループ名	定義番号	管理機器名	タイプ	
0	GroupA	0	AP_A01	wlan	<input checked="" type="checkbox"/>
		1	AP_A02	wlan	<input checked="" type="checkbox"/>

2. 無線 LAN チャンネルの自動調整を実施する管理機器のチェックボックスにチェックします。
3. **【チャンネル自動調整】** ボタンをクリックします。

無線 LAN チャンネル自動調整の実行結果が表示され、管理対象となった無線 LAN アクセスポイントの無線 LAN チャンネルが自動的に調整されます。

こんな事に気をつけて

無線 LAN チャンネル自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で無線 LAN チャンネル自動調整を行うようにしてください。



無線 LAN チャンネルの自動調整を開始したあとにキャンセルした場合、現在処理中の無線 LAN アクセスポイントの無線 LAN チャンネルの調整が完了するまでバックグラウンドで処理を行います。この間、無線 LAN 管理機能のほかの操作はできません。

2.1.17 無線 LAN アクセスポイントの電波出力を調整する

適用機種 全機種

管理対象となった無線 LAN アクセスポイントの電波出力を自動的に調整することができます。

こんな事に気をつけて

管理対象機器は、弊社製の無線 LAN アクセスポイント (SR-M20AP1) のみとなります。

1. 操作メニューで「無線 LAN 管理操作」の「無線 LAN 電波出力の自動調整」をクリックします。
「無線 LAN 電波出力の自動調整」ページが表示されます。

【無線 LAN 電波出力の自動調整】

このページでは、管理対象となった無線 LAN アクセスポイントの電波出力を自動的に調整することができます。
《電波出力の自動調整を実施したい管理機器のチェックボックスにチェックをして、電波出力自動調整をクリックしてください。》

■管理機器一覧

グループ		管理機器			電波出力自動調整
定義番号	グループ名	定義番号	管理機器名	タイプ	
0	GroupA	0	AP_A01	wlan	<input checked="" type="checkbox"/>
		1	AP_A02	wlan	<input checked="" type="checkbox"/>

2. 電波出力の自動調整を実施する管理機器のチェックボックスにチェックします。
3. **【電波出力自動調整】** ボタンをクリックします。

電波出力自動調整の実行結果が表示され、管理対象となった無線 LAN アクセスポイントの電波出力が自動的に調整されます。

こんな事に気をつけて

電波出力自動調整の実施中は、無線の状態が不安定になる可能性があります。よって、メンテナンスなどの通常運用時以外で電波出力自動調整を行うようにしてください。



- 1 管理機器の電波出力を自動調整するには、かなりの時間が必要となりますので、電波出力の調整が必要な管理機器以外は設定しないようにしてください。
- 電波出力の自動調整を開始したあとにキャンセルした場合、現在処理中の無線 LAN アクセスポイントの電波出力の調整が完了するまでバックグラウンドで処理を行います。この間、無線 LAN 管理機能のほかの操作はできません。

2.1.18 無線 LAN アクセスポイントの装置リセットを行う

適用機種 全機種

管理対象となった無線 LAN アクセスポイントの装置リセットを行うことができます。

こんな事に気をつけて

管理対象機器は、弊社製の無線 LAN アクセスポイント (SR-M20AP1) のみとなります。

1. 操作メニューで「無線 LAN 管理操作」の「管理機器の装置リセット」をクリックします。
「管理機器の装置リセット」ページが表示されます。

【管理機器の装置リセット】

このページでは、管理対象となった無線 LAN アクセスポイントの装置リセットを行うことができます。
《装置リセットしたい管理機器を選択して、装置リセットをクリックしてください。》

■管理機器一覧

グループ		管理機器			装置リセット
定義番号	グループ名	定義番号	管理機器名	タイプ	
0	GroupA	0	AP_A01	wlan	<input type="checkbox"/>
		1	AP_A02	wlan	<input type="checkbox"/>

2. 装置リセットする管理機器のチェックボックスにチェックします。
3. **【装置リセット】** ボタンをクリックします。
管理対象となった無線 LAN アクセスポイントの装置リセットが実行されます。

2.2 表示メニューを使う

表示メニューでは、回線や機能の使用状況、現在時刻および経過時間情報などについて確認することができます。

こんな事に気をつけて

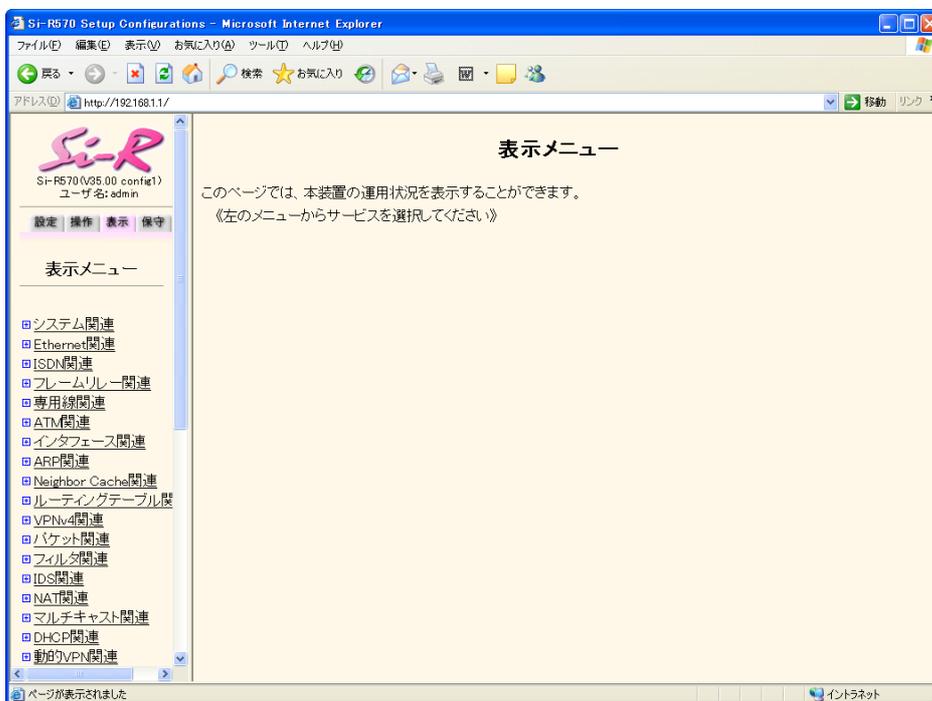
一般ユーザ (user) でログインしている場合は、「統計情報」をクリアすることができません。クリアする場合は、管理者 (admin) に移行してください。

☛ 参照 「1.3 本装置にログインする」(P.11)

2.2.1 表示メニューを表示する

適用機種 全機種

本装置のトップページで、画面左側の [表示] タブをクリックすると、表示メニューが表示されます。



各表示内容については、「コマンドリファレンス-運用管理編-」に記載されています。併せてご覧ください。

以下に、表示される各種情報および状態と表示するコマンドを示します。

機能分類	表示内容	コマンド
システム関連	静的システム情報	show system information
	動的システム情報	show system status
	エラーログ情報	show logging error
	システムログ情報	show logging syslog
	現在時刻情報	show date
Ethernet 関連	物理ポート情報	show ether
	物理ポート統計情報	show ether statistics
ISDN 関連	回線情報	show isdn
	統計情報	show isdn statistics circuit
	アカウント情報	show isdn account
	PIAFS 統計情報	show isdn statistics piafs
フレームリレー関連	回線情報	show fr
	統計情報	show fr statistics circuit
	PVC 統計情報	show fr statistics vc
専用線関連	回線情報	show hsd
	統計情報	show hsd statistics circuit
ATM 関連	回線情報	show atm
	統計情報	show atm statistics circuit
	PVC 統計情報	show atm statistics vc
	LLC / SNAP 統計情報	show atm statistics llc-snap
モデム関連	回線情報	show modem
	アカウント情報	show modem account
データ通信カード関連	回線情報	show cardmodem
	アカウント情報	show cardmodem account
無線 LAN 関連	状態情報	show wlan status
	接続端末情報	show wlan sta
	統計情報	show wlan statistics
	WPA 情報	show wlan wpa status
インタフェース関連	WPA 統計情報	show wlan wpa statistics
	インタフェース情報	show interface
	インタフェース統計情報	show interface statistics
	接続先情報	show access-point
	テンプレート状態情報	show template
ARP 関連	ARP エントリ情報	show arp
	テンプレート統計情報	show template statistics
Neighbor Cache 関連	テーブルエントリ情報	show ndp
ルーティングテーブル関連	IP カーネル情報	show ip route kernel
	ECMP 統計情報	show ip route kernel ecmp statistics
	IPv6 カーネル情報	show ipv6 route kernel
VPNv4 関連	ルーティングテーブル情報	show ip vpnv4 route
パケット関連	統計情報	show ip traffic
	IPv6 統計情報	show ipv6 traffic

機能分類	表示内容	コマンド
フィルタ関連	テーブル情報	show ip filter
	統計情報	show ip filter statistics
	IPv6 テーブル情報	show ipv6 filter
	IPv6 統計情報	show ipv6 filter statistics
IDS 関連	統計情報	show ip ids statistics
NAT 関連	テーブル情報	show ip nat
	統計情報	show ip nat statistics
マルチキャスト関連	グループ情報	show ip multicast group
	インタフェース情報	show ip multicast interface
	インタフェース統計情報	show ip multicast interface statistics
	PIM-SM ランデブーポイント情報	show ip multicast pimsm rp
	プロトコル情報	show ip multicast protocol
	ルーティングテーブル情報	show ip multicast route
	カーネルルーティングテーブル情報	show ip multicast route kernel
	カーネル統計情報	show ip multicast statistics
	カーネルルーティングテーブル統計情報	show ip multicast route kernel statistics
	DHCP 関連	IPv4 運用情報
IPv6 運用情報		show ipv6 dhcp
動的 VPN 関連	クライアントユーザ情報	show dvpn client user
	クライアントセッション情報	show dvpn client session
	サーバ情報	show dvpn server
	サーバユーザ情報	show dvpn server user
	サーバセッション情報	show dvpn server session
IPsec/IKE 関連	IPsec SA 情報	show ipsec sa
	IKE 統計情報	show ike statistics
		show ike statistics interface
VRRP 関連	VRRP 情報	show vrrp
ブリッジ関連	状態と統計情報	show bridge status
	学習テーブルの内容	show bridge
	スパンニングツリー情報	show spanning-tree
MPLS 関連	FTN テーブル情報	show mpls ftm detail
	ILM テーブル情報	show mpls ilm detail
	LDP インタフェース情報	show mpls ldp detail
	LDP 近隣情報	show mpls ldp adjacency
	LDP FEC テーブル情報	show mpls ldp fec
	LDP セッション情報	show mpls ldp session detail
	LDP 状態情報	show mpls ldp summary
	LDP VC 情報	show mpls ldp vc
	インタフェース統計情報	show mpls statistics
	VC テーブル情報	show mpls vc detail
	VRF テーブル情報	show mpls vrf detail

機能分類	表示内容	コマンド
LLDP 関連	設定情報	show lldp
	自装置情報	show lldp summary
	隣接情報	show lldp neighbors detail
	統計情報	show lldp statistics detail
MAC アドレス認証関連	状態と統計情報	show macauth
IEEE802.1X 認証関連	認証情報	show dot1x lan
	認証統計情報	show dot1x statistics
ARP 認証関連	認証状態	show arpauth lan
	統計情報	show arpauth statistics
SNMP 関連	統計情報	show snmp statistics
NETTIME 関連	統計情報	show nettime statistics
UPnP 関連	状態情報	show upnp
	統計情報	show upnp statistic
	ポートマッピング情報	show upnp portmapping
SSH 関連	DSA 公開鍵情報	show ssh server key dsa
	RSA 公開鍵情報	show ssh server key rsa
SIP-SIP ゲートウェイ関連	状態情報	show siggw
	統計情報	show siggw statistics
AAA 関連	RADIUS サーバ情報	show aaa radius client server-info
トレース関連	PPP 情報	show trace ppp
	PPPoE 情報	show trace pppoe
	IKE 情報	show trace ike
	SSH 情報	show trace ssh
	モデム情報	show trace modem
	データ通信カード関連	show trace cardmodem
ポリシーグループ関連	ポリシーグループ情報	show policy-group
証明書関連	証明書関連情報	show crypto certificate
	証明書関連情報 (Base64)	show crypto certificate base64
無線 LAN 管理関連	管理機器の一覧表示	show nodemanager node brief
	管理機器の詳細情報表示	show nodemanager node
	管理無線 LAN アクセスポイントの監視状況の一覧表示	show nodemanager logging wlan scan managed brief
	管理無線 LAN アクセスポイントの監視状況の表示	show nodemanager logging wlan scan managed
	管理外無線 LAN アクセスポイントの監視状況の表示	show nodemanager logging wlan scan unmanaged
	不明無線 LAN アクセスポイントの監視状況の表示	show nodemanager logging wlan scan unknown
	無線 LAN 端末の RSSI 最大値/最小値の一覧表示	show nodemanager logging wlan sta rssi
	無線 LAN インタフェースの無線 LAN 端末情報の表示	show nodemanager logging wlan sta
	無線 LAN 通信のトレース情報の表示	show nodemanager logging wlan trace
接続拒否の無線 LAN 端末情報の表示	show nodemanager logging wlan reject	

2.3 保守メニューを使う

保守メニューでは、ファームウェア更新、構成定義情報の退避／復元、構成定義情報切り替えなどができます。

こんな事に気をつけて

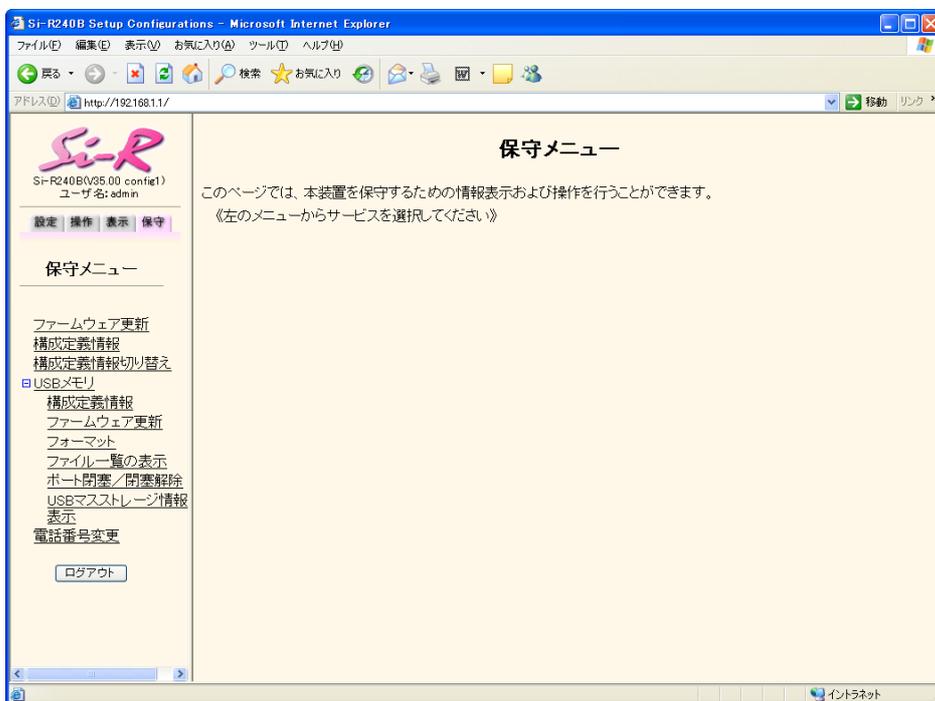
一般ユーザ (user) でログインしている場合は、「保守メニュー」が表示されません。「保守メニュー」を使用する場合は、管理者 (admin) に移行してください。

☛ 参照 「1.3 本装置にログインする」(P.11)

2.3.1 保守メニューを表示する

適用機種 全機種

本装置のトップページで、画面左側の「保守」タブをクリックすると、保守メニューが表示されます。



電話番号変更は、Si-R220C、220D、240B、370、370B、570、570B で表示されます。

USB メモリは、Si-R180B、220C、220D、240B で表示されます。

2.3.2 本装置のファームウェアを更新する

適用機種 全機種

ファームウェアを更新すると、本装置に新しい機能を追加できます。

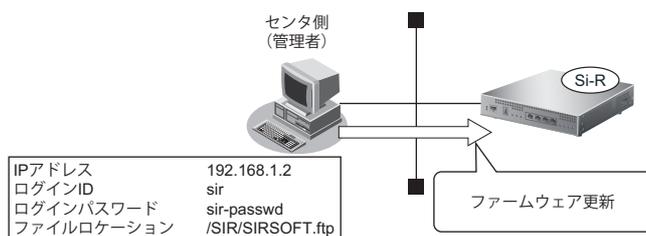
FTPサーバ（FTPサーバ機能を持つパソコンやUNIXシステム）にファームウェアファイルを配置し、WWWブラウザ（本装置の設定メニュー）を使ってネットワークに接続した本装置のファームウェアを更新できます。

ただし、初期状態ではファームウェア更新情報が設定されていないため、設定が必要です。

こんな事に気をつけて

- ・ ファームウェア更新中は、本装置の電源を切断しないでください。
- ・ ファームウェアを更新する前に、構成定義情報を退避しておいてください。

ここでは、ファームウェア更新情報の設定方法について例をあげて説明します。



1. 設定メニューの基本設定で「装置情報」をクリックします。

「装置情報」ページが表示されます。

2. 「ファームウェア更新情報」をクリックします。

「ファームウェア更新情報」が表示されます。

3. 以下の項目を指定します。

- ・ 転送元ホスト名 → 192.168.1.2
- ・ ログインID → sir
- ・ ログインパスワード → sir-passwd
- ・ ファイルロケーション → /SIR/SIRSOFT.ftp

■ファームウェア更新情報	
転送元ホスト名	<input type="text" value="192.168.1.2"/>
ログインID	<input type="text" value="sir"/>
ログインパスワード	<input type="password" value="....."/>
ファイルロケーション	<input type="text" value="/SIR/SIRSOFT.ftp"/>

4. 【保存】 ボタンをクリックします。

5. 画面左側の【再起動】 ボタンをクリックします。

設定した内容が有効になります。

6. 保守メニューで「ファームウェア更新」をクリックします。

「ファームウェア更新」ページが表示されます。

【ファームウェア更新】

以下の情報をもとにファームウェアを更新します。情報に誤りがない場合はOKボタンをクリックしてください。
▲ファームウェアの更新中は電源を切らないでください。以後、正常に動作しなくなる可能性があります。

転送元ホスト名	ログインID	ファイルロケーション
192.168.1.2	sir	/SIR/SIRSOFT.ftp

7. 表示されている内容を確認し、正しければ [OK] ボタンをクリックします。

ファームウェアの更新を開始します。

8. 「正常終了」のメッセージが表示されたら、[OK] ボタンをクリックします。**9. 【トップページに戻る】 ボタンをクリックします。**

トップページに戻ります。

2.3.3 構成定義情報を退避する／復元する

適用機種 全機種

現在の本装置の構成定義情報をファイルに保存し、退避しておきます。必要になったときに保存しておいた構成定義情報を復元できます。

● 退避できる構成定義情報

- 編集中の構成定義 : 本装置で設定を変更している構成定義情報
- 運用中の構成定義 : 現在、本装置で運用中の構成定義情報

1. 保守メニューで「構成定義情報」をクリックします。

「構成定義情報」ページが表示されます。

【構成定義情報】

このページでは、構成定義情報の退避および復元ができます。

退避 退避ボタンをクリックすると、構成定義ファイルが開きますので、ブラウザの保存機能により保存してください。

退避する構成定義

編集中の構成定義

運用中の構成定義

復元 復元ボタンをクリックすると、指定したファイルを使用して構成定義情報を復元します。

構成定義ファイル 参照...

```
lan 0 ip address 10.35.156.170/24 3
lan 0 ip route 0 default 10.35.156.1 1 0
syslog pri error,warn,info
syslog facility 23
time zone 0900
consoleinfo autologout 8h
telnetinfo autologout 5m
sysdown harderr fan yes
sysdown harderr thermal yes
alias history "show logging command brief"
terminal pager enable
terminal charset SJIS
```

2. 以下の手順で退避／復元します。

- 退避する場合
退避する構成定義を選択し、[退避] ボタンをクリックします。
構成定義ファイルが開きます。WWW ブラウザの保存機能によって保存します。
- 復元する場合
復元する構成定義ファイルを指定し、[復元] ボタンをクリックします。

こんな事に気をつけて

現在の本装置の IP アドレスと保存時の IP アドレスが異なると復元できません。

2.3.4 構成定義情報を切り替える

適用機種 全機種

本装置は構成定義情報を内部に2つ持つことができます。「スケジュール機能」または手動で切り替えることができます。

1. 保守メニューで「構成定義情報切り替え」をクリックします。

「構成定義情報切り替え」ページが表示されます。

補足 ページが表示されたときに、選択されている方が現在の構成定義情報です。

【構成定義情報切り替え】

このページでは、構成定義情報の切り替えを行うことができます。
構成定義情報1または構成定義情報2を選択し、再起動ボタンをクリックしてください。

構成定義情報1
 構成定義情報2

2. 再立ち上げ時に使用する構成定義情報をチェックし、[再起動] ボタンをクリックします。

再起動が行われ、選択した構成定義情報での立ち上げが行われます。

こんな事に気をつけて

- 電源投入時は、直前に動作していた側の構成定義情報で立ち上がります。
- データ通信中に再起動すると、通信が切断されます。
- 本装置のIPアドレスが変更となった場合、再起動後に本装置にアクセスするためには、パソコンの再起動およびURLを変更する必要があります。

2.3.5 USB メモリを使う

適用機種 Si-R180B,220C,220D,240B

USB メモリを使用して、構成定義情報の退避／復元、ファームウェアの更新などを行うことができます。

構成定義情報の退避／復元

本装置の構成定義情報を USB メモリに保存し、退避しておきます。必要になったときに USB メモリに保存しておいた構成定義情報を復元できます。

● 退避できる構成定義情報

- 編集中の構成定義 : 本装置で設定を変更している構成定義情報
- 運用中の構成定義 : 現在、本装置で運用中の構成定義情報
- 構成定義情報 1 : 本装置に保存されている構成定義情報 1
- 構成定義情報 2 : 本装置に保存されている構成定義情報 2

ここでは、構成定義情報 1 を退避／復元する方法について説明します。

1. 保守メニューで「USB メモリ」の「構成定義情報」をクリックします。

「構成定義情報」ページが表示されます。

【構成定義情報】

このページでは、USBメモリへの構成定義情報の退避およびUSBメモリからの復元ができます。

退避ボタンをクリックすると、指定したファイルに構成定義情報を退避します。

退避する構成定義

- 編集中の構成定義
- 運用中の構成定義
- 構成定義情報1
- 構成定義情報2

退避先ファイル名

復元ボタンをクリックすると、指定したファイルが構成定義情報を復元します。

復元元ファイル名

復元する構成定義

- 構成定義情報1
- 構成定義情報2

2. 以下の手順で退避／復元します。

- 退避する場合
 - (1) 退避する構成定義から「構成定義情報 1」を選択します。
 - (2) 退避先ファイル名 (例: config_save) を指定して [退避] ボタンをクリックします。
構成定義情報が USB メモリに退避されます。
- 復元する場合
 - (1) 復元する構成定義から「構成定義情報 1」を選択します。
 - (2) 復元元ファイル名 (例: config_save) を指定して [復元] ボタンをクリックします。
USB メモリに保存しておいた構成定義情報が復元されます。

ファームウェアの更新

ここでは、USB メモリを使用したファームウェアの更新方法について説明します。

1. 保守メニューで「USB メモリ」の「ファームウェア更新」をクリックします。
「ファームウェア更新」ページが表示されます。

【ファームウェア更新】
このページでは、USBメモリからファームウェアの更新ができます。

ファイル名を指定して更新ボタンをクリックすると、USBメモリからファームウェアの更新を実行します。

ファームウェアファイル名

2. ファームウェアファイル名を指定して [更新] ボタンをクリックします。
ファームウェアが更新されます。

フォーマット

ここでは、USB メモリのフォーマット方法について説明します。

1. 保守メニューで「USB メモリ」の「フォーマット」をクリックします。
「フォーマット」ページが表示されます。

【フォーマット】
このページでは、USBメモリのフォーマットができます。

フォーマットボタンをクリックすると、USBメモリのフォーマットを実行します。

2. 【フォーマット】 ボタンをクリックします。
USB メモリがフォーマットされます。

ファイル一覧の表示

ここでは、USB メモリのファイル一覧を表示する方法について説明します。

1. 保守メニューで「USB メモリ」の「ファイル一覧の表示」をクリックします。
「ファイル一覧」ページが表示されます。

【ファイル一覧】			
Directory of /um0			
2008/01/11	13:24	6044	file1
2008/01/11	13:24	6044	file2
2007/12/18	18:51	5331634	firmware
2008/01/11	13:25	6044	sys-file1
2007/12/18	18:49	273869	tech-support
2008/01/11	13:25	6038	umf0
2008/01/11	13:25	775	umf1
total file			7
total directory			0

ポート閉塞／閉塞解除

ここでは、USB メモリの安全な取り外し／取り付けを行うために、ポート閉塞およびポート閉塞解除をする方法について説明します。

1. 保守メニューで「USB メモリ」の「ポート閉塞／閉塞解除」をクリックします。
「ポート閉塞／閉塞解除」ページが表示されます。

【ポート閉塞／閉塞解除】		
このページでは、USBメモリを安全に取り外し／取り付けをするために、USBのポートを閉塞または閉塞解除を行います。		
ポート	状態	操作
USB	閉塞	<input type="button" value="閉塞解除"/>

2. 以下のどちらかの手順で設定します。
 - USB ポートを閉塞する場合
操作の [閉塞] ボタンをクリックします。
 - USB ポートを閉塞解除する場合
操作の [閉塞解除] ボタンをクリックします。

こんな事に気をつけて

- USB ポート閉塞実行後に USB メモリを取り外す場合は、保守メニューの「USB メモリ」-「ポート閉塞／閉塞解除」をクリックし、状態が「閉塞」となっていることを確認してから取り外してください。
- USB ポート閉塞解除実行後は、状態が「閉塞解除」になるまでは USB メモリを使用することができません。保守メニューの「USB メモリ」-「ポート閉塞／閉塞解除」をクリックし、状態を確認してください。

USB マスストレージ情報の表示

ここでは、USB メモリのマスストレージ情報を表示する方法について説明します。

1. 保守メニューで「USB メモリ」の「USB マスストレージ情報表示」をクリックします。
「USB マスストレージ情報表示」ページが表示されます。

【USB マスストレージ情報表示】

```
[Thread]
Status           : Active

[Device #1]
Status           : Idle
Speed            : High
Geometry probing : Success (partly guessed)
Test unit ready  : Success
Inquiry          : Success
Mode sense       : Failed (no data)
Read capacity    : Success
Read format capacities : ---
Hold data        : Not exist
[Storage specs]
Vendor           : BUFFALO
Product          : USB Flash Disk
Product Rev.     : 4000
Total sectors    : 506880
Cylinders        : 247
Heads            : 64
Sectors per track : 32
[USB specs]
Speed            : High
Max LUN          : 0
[USB configuration]
Device address   : 1
Interface        : 0
Sub class        : 6
LUN              : 0
BulkInEP         : 0x81
BulkOutEP        : 0x02
```

2.3.6 電話番号を変更する

適用機種 Si-R220C,220D,240B,370,370B,5570,570B

「スケジュール情報」の「電話番号変更予約情報」で設定した電話番号の変更を手動で行うことができます。

1. 保守メニューで「電話番号変更」をクリックします。

「電話番号変更」ページが表示されます。

【電話番号変更】

このページでは、電話番号変更予約情報で設定した電話番号の変更を手動で実施することができます。
※実行日時が赤文字で表示されている情報は、既に経過した日時の子約情報です。
《情報一覧より電話番号変更予約情報を選択し、実行してください。》

[電話番号変更予約情報一覧]

実行日時	電話番号変更情報	実行
-	-	実行

2. 変更する電話番号変更予約情報の【実行】ボタンをクリックします。

電話番号が変更されます。

3. 画面左側の【設定反映】ボタンをクリックします。

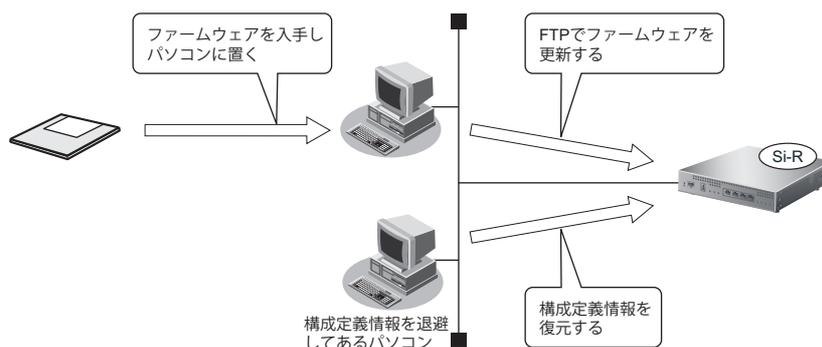
設定した内容が有効になります。

2.3.7 FTP/SFTP サーバ機能を使ってメンテナンスする

適用機種 全機種

本装置はFTPサーバ機能およびSFTPサーバ機能を持っており、パソコンやUNIXシステムのftpコマンドおよびsftpコマンドを使って構成定義情報の退避/復元およびファームウェアを更新することができます。ここでは、Si-R370のFTPサーバ機能をftpコマンドで使用する場合を例に説明します。

なお、SFTPサーバ機能を使用する場合は、別途SSHプロトコルバージョン2をサポートしているsftpクライアントソフトウェアを用意する必要があります。それにより、ftpコマンドと同様にsftpコマンドを使用することができます。



FTPサーバ機能を利用するときのユーザ名、パスワードは以下のとおりです。

- ユーザ名 : ftp-admin
- パスワード : 設定メニューの基本設定で設定したパスワードを指定します。

補足 パスワードを設定していない場合は、FTPサーバ機能もパスワードがないものとして動作します。

● メンテナンス対象のファイル

FTPサーバ機能でメンテナンス対象となるファイル名は以下のとおりです。

- 構成定義情報1 : config1
- 構成定義情報2 : config2
- ファームウェア : firmware

● 再起動方法

ftpコマンドのサブコマンドとして「get reset」を入力すると、本装置を再起動できます。

構成定義情報を切り替える場合は、「get reset1」または「get reset2」を入力して本装置を再起動します。

- 「get reset」を入力した場合 : 再起動後も現状の構成定義情報が有効です。
- 「get reset1」を入力した場合 : 再起動後は「構成定義情報1」が有効になります。
- 「get reset2」を入力した場合 : 再起動後は「構成定義情報2」が有効になります。

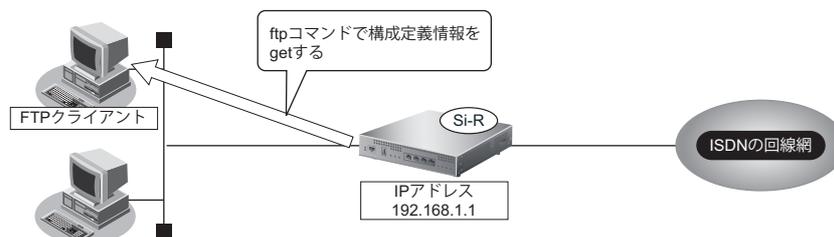
こんな事に気をつけて

セキュリティ確保のためパスワードを設定することを強くお勧めします。
設定しない場合、ネットワーク上のだれからでもアクセスできるため、非常に危険です。

☛ 参照 「1.4 パスワード情報を設定する」 (P.13)

FTP サーバ機能による構成定義情報の退避

パソコン上の ftp コマンドを使って構成定義情報を退避する方法を説明します。



こんな事に気をつけて

メンテナンス作業時は、以下のことを必ず守ってください。

- 本装置の電源を切断しないでください。
- 本装置上でデータ通信を行っている場合、データ通信が遅延することがあります。
- WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。

● ftp コマンドの使用例

構成定義情報 1 をパソコン上の config1-1 ファイルに退避する場合の例を示します。

```

C:¥>cd 構成定義情報格納ディレクトリ
C:¥tmp>ftp 192.168.1.1          : 本装置に接続する

Connected to 192.168.1.1.
220 Si-R370 V35.00 FTP server (config1) ready.
Name(192.168.1.1:root): ftp-admin  : ユーザ名を入力する

331 Password required for ftp-admin.
Password:                          : パスワードを入力する

230 User ftp-admin logged in.
ftp>bin                             : バイナリモードにする

200 Type set to I.
ftp>get config1 config1-1          : 構成定義情報 1 (config1) を config1-1 ファイルに格納する

local: config1 remote: config1-1
200 PORT command successful.
150 Opening BINARY mode data connection for 'config1'(2753 bytes).
226- Transfer complete.
2857 bytes received in 1.10 seconds (2.44 Kbytes/s)
ftp>bye                             : 処理を終了する

221 Goodbye.
C:¥tmp>

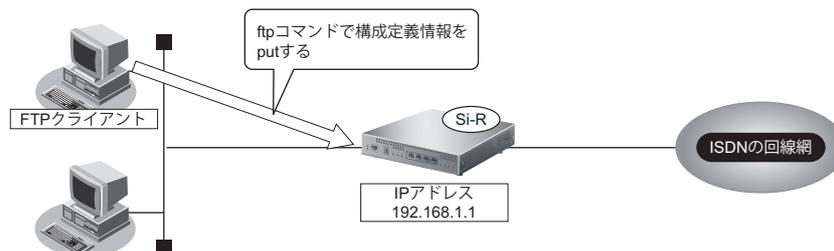
```



パスワードは、「1.4 パスワード情報を設定する」(P13) で設定したパスワードを指定してください。

FTP サーバ機能による構成定義情報の復元

パソコン上の ftp コマンドを使って構成定義情報を復元する方法を説明します。



こんな事に気をつけて

メンテナンス作業時は、以下のことを必ず守ってください。

- 本装置の電源を切断しないでください。
- 本装置上でデータ通信を行っている場合、データ通信が遅延することがあります。
- WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。

● ftp コマンドの使用例

構成定義情報 1 をパソコン上の config1-1 ファイルから復元する場合の例を示します。

```

C:¥>cd 構成定義情報格納ディレクトリ
C:¥tmp>ftp 192.168.1.1           : 本装置に接続する
Connected to 192.168.1.1.
220 Si-R370 V35.00 FTP server (config1) ready.
Name(192.168.1.1:root): ftp-admin : ユーザ名を入力する
331 Password required for ftp-admin.
Password:                       : パスワードを入力する
230 User ftp-admin logged in.
ftp>bin                          : バイナリモードにする
200 Type set to I.
ftp>put config1-1 config1        : config1-1 ファイルを構成定義情報 1 (config1) として書き込む
local: config1-1 remote: config1
200 PORT command successful.
150 Opening BINARY mode data connection for 'config1'.
226- Transfer complete.
update : File information check now!
update : File information check ok.
.
.
226 Write complete.
2856 bytes sent in 1.10 seconds (2.44 Kbytes/s)
ftp>get reset                    : 本装置を再起動する
local: reset remote: reset
200 PORT command successful.
421 Reset request ok. bye.
ftp>bye                          : 処理を終了する
C:¥tmp>

```



復元した構成定義情報を有効にするために、本装置を再起動してください。

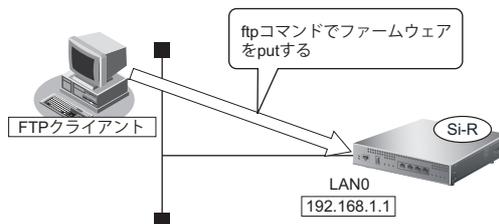
ftp コマンドのサブコマンドとして「get reset」を入力すると、再起動できます。

構成定義情報を切り替える場合は、「get reset1」または「get reset2」を入力して本装置を再起動します。

- 「get reset」を入力した場合 : 再起動後も現状の構成定義情報が有効です。
- 「get reset1」を入力した場合 : 再起動後は「構成定義情報 1」が有効になります。
- 「get reset2」を入力した場合 : 再起動後は「構成定義情報 2」が有効になります。

FTP サーバ機能によるファームウェアの更新

パソコン上の ftp コマンドを使ってファームウェアを更新する方法を説明します。



こんな事に気をつけて

ファームウェア更新時は、以下のことを必ず守ってください。

- 本装置の電源を切断しないでください。
- 本装置上でデータ通信を行っている場合、データ通信が遅延することがあります。
- WWW ブラウザ、コンソールによる設定作業を一切していない状態で行ってください。
- ファームウェアを更新する前に、構成定義情報を退避しておいてください。

● ftp コマンドの使用例

ファームウェアをパソコン上から更新する場合の例を示します。

```

C:¥> cd ファームウェアディレクトリ
C:¥tmp> ftp 192.168.1.1          : 本装置に接続する
Connected to 192.168.1.1.
220 Si-R370 V35.00 FTP server (config1) ready.
Name(192.168.1.1:root): ftp-admin : ユーザ名を入力する
331 Password required for ftp-admin.
Password:                          : パスワードを入力する
230 User ftp-admin logged in.
ftp>bin                             : バイナリモードにする
200 Type set to I.
ftp>put Si-R370SOFT.ftp firmware    : ファームウェアを書き込む
local: Si-R370SOFT.ftp remote: firmware
200 PORT command successful.
150 Opening BINARY mode data connection for 'firmware'.
226- Transfer complete.
update : Transfer file check now!
update : Transfer file check ok.
.
.
226 Write complete.
1966 bytes sent in 97.80 seconds (6.31 Kbytes/s)
ftp>get reset                       : 本装置を再起動する
local: reset remote: reset
200 PORT command successful.
421 Reset request ok. bye.
ftp>bye                             : 処理を終了する
C:¥tmp>

```



- 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「255.255.255.0」です。
- パスワードは、「1.4 パスワード情報を設定する」(P.13) で設定したパスワードを指定してください。ご購入時は、パスワードは設定されていません。
- ftp コマンドのサブコマンドとして「get reset」を入力すると、本装置を再起動することができます。

索引

B

BGP セッションの操作 31

F

ftp コマンド 59

FTP サーバ機能 59

M

MAC アドレスの収集 40

MAC アドレスフィルタ配布 41

Microsoft Internet Explorer 9

P

ping コマンド 32

PIN コード照合 37

PIN コード変更 38

PIN ロック解除 39

Proxy サーバ 9

R

RADIUS 手動復旧 36

S

sftp コマンド 59

SFTP サーバ機能 59

SNTP サーバ 18

T

TIME サーバ 18

U

USB メモリ 54

V

VRRP 手動切り戻し機能 34

VRRP 手動停止/再開機能 35

W

WWW ブラウザ 9

あ

暗号化パスワード 14

い

一般ユーザクラス 12

か

かんたん設定メニュー 10, 21

管理者クラス 12

け

権限クラス 12

こ

構成定義情報切り替え 53

構成定義情報の退避/復元 52

構成定義情報の退避/復元 (FTP サーバ機能)
..... 60, 61

購入時の状態 20

し

時刻の設定 18

手動 LAN 有効化/無効化 27

手動回線接続/切断 26

手動スイッチポート有効化/無効化 28

手動接続先有効化/無効化 29

手動ポリシーグループ有効化/無効化 30

詳細設定メニュー 10

せ

設定メニュー 10

そ

操作メニュー 10, 25

装置リセット 44

て

電波出力の自動調整 43

電話番号の変更 58

と

トップページ 10

に

入力文字一覧 23

ね

ネットワーク接続の確認 32

は

パスワード 11

パスワード情報の設定 13

ひ

表示メニュー 10, 45

ふ

ファームウェアの更新 50

ファームウェアの更新 (FTP サーバ機能) 62

プリエンプトモード 34

ほ

保守メニュー 10, 49

ホストデータベース情報 33

ま

マニュアル構成 7

む

無線 LAN チャンネルの自動調整 42

ゆ

ユーザ名 11

り

リモートパワーオン機能 33

ろ

ログイン 11

ログインパスワード情報 13

ログインユーザ情報 15

Si-Rシリーズ Webユーザズガイド

P3NK-4012-05Z0

発行日 2014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。