P3NK-4012-05Z0

FUJITSU Network Si-R
Si-Rシリーズ

Webユーザーズガイド V35

FUJITSU

はじめに

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

2009年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

目次

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

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

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

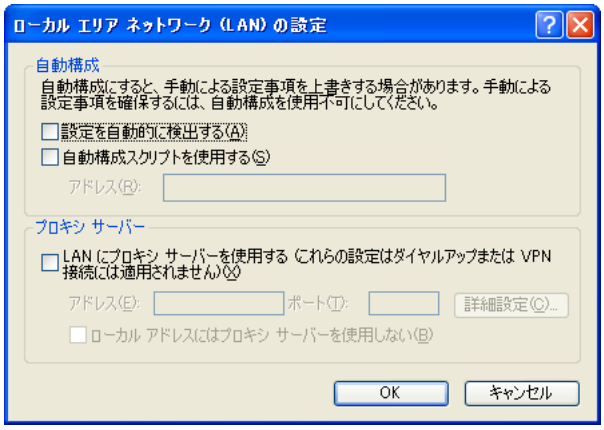
ブラウザの設定が、「Proxy（プロキシ）サーバ機能」を利用しないようになっていることを確認してください。以下のように確認します。

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。



補足

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。

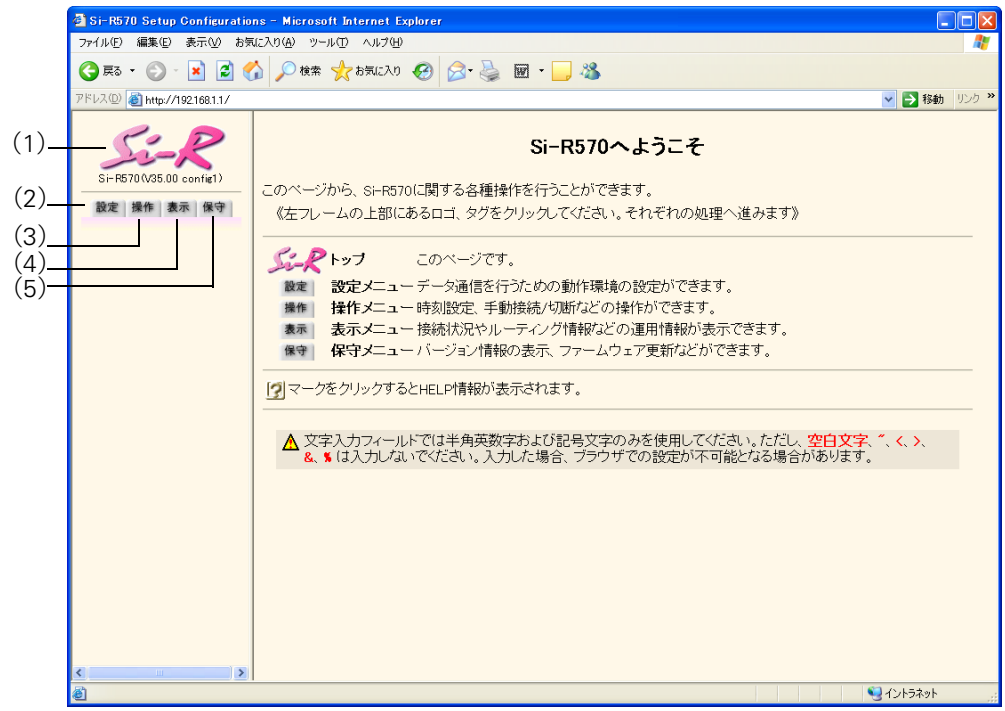
ここでは、Si-R570 の場合を例に説明します。

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.　トップページの画面左側の［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

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」（P.55）

- **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。

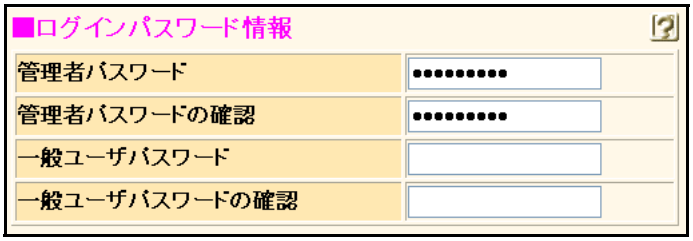
「パスワード情報」ページが表示されます。

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。

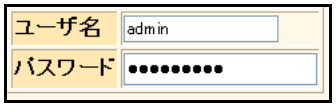
「パスワードを更新しました。更新した情報は、即時有効になります。」というメッセージが表示されます。

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止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」（P.55）

- **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」（P.12）

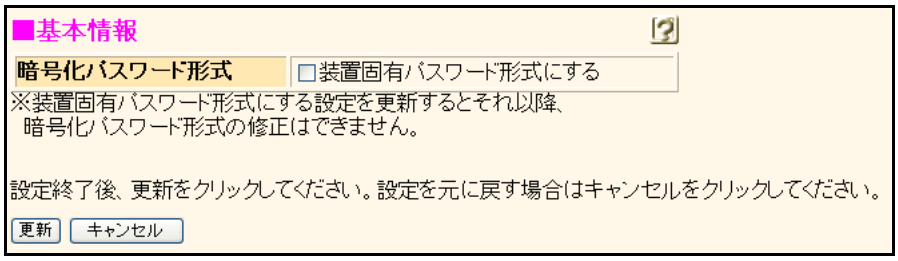
暗号化パスワード形式を装置固有パスワード形式に設定する手順を示します。

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。

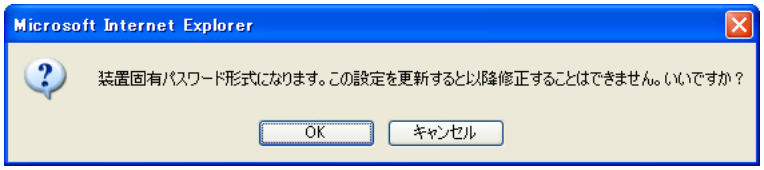
2.　「基本情報」をクリックします。

「基本情報」が表示されます。



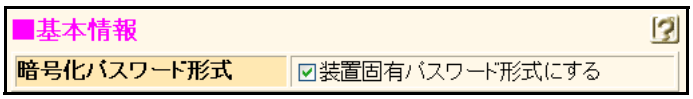
3.　暗号化パスワード形式の装置固有パスワード形式にするにチェックします。

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。



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。

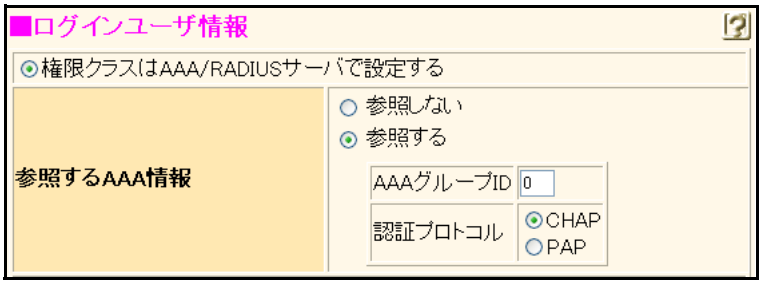
「パスワード情報」ページが表示されます。

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



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。

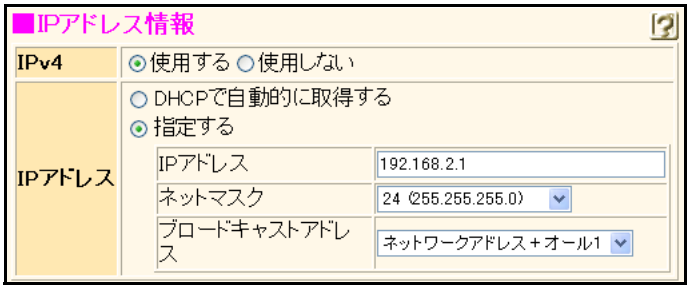
「LAN1 情報（物理 LAN）」ページが表示されます。Si-R180B でスイッチポートを利用している場合は、「LAN1 情報（VLAN）」ページが表示されます。

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



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。

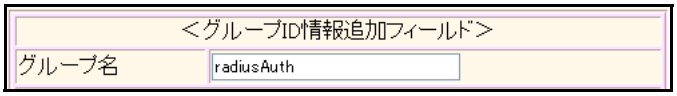
「AAA 情報」ページが表示されます。

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



13.　［追加］ボタンをクリックします。

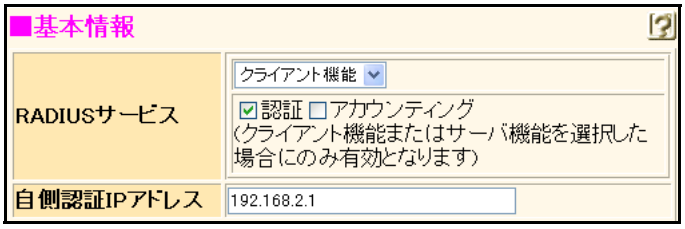
「グループ ID 情報（0）」と設定項目が表示されます。

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　→クライアント機能
  認証　→チェックする
  アカウンティング　→チェックしない
- 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。

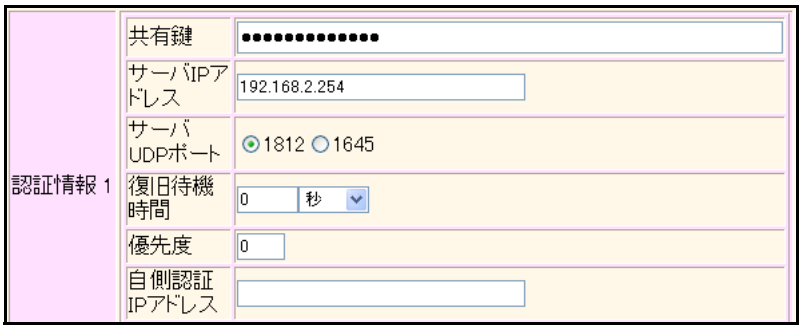
17.　RADIUS 関連の設定項目の「サーバ情報」をクリックします。

「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



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

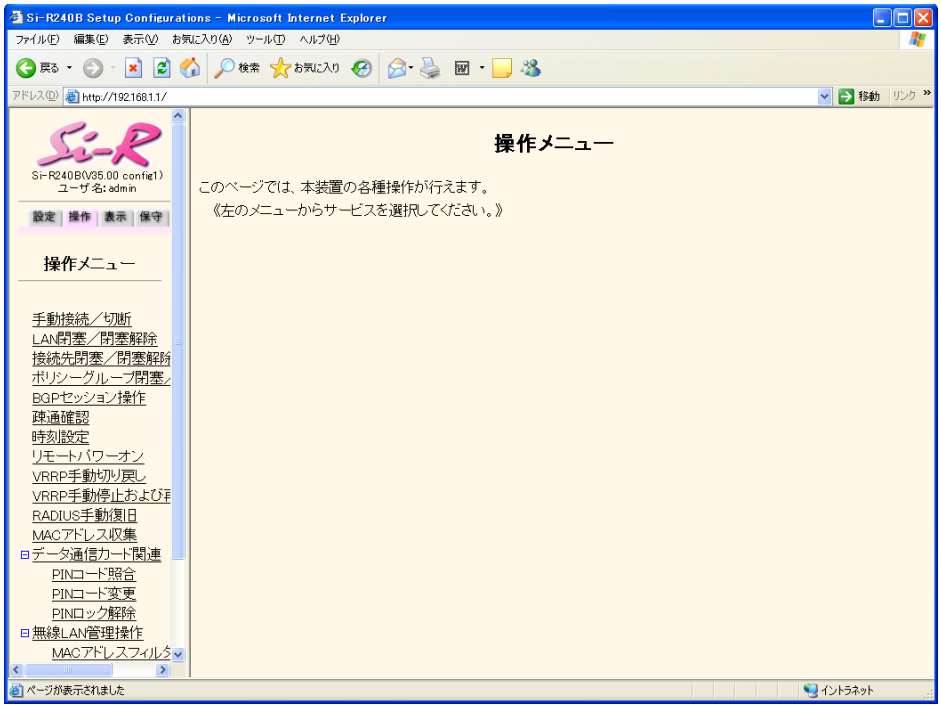
こんな事に気をつけて

- **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」（P.11）

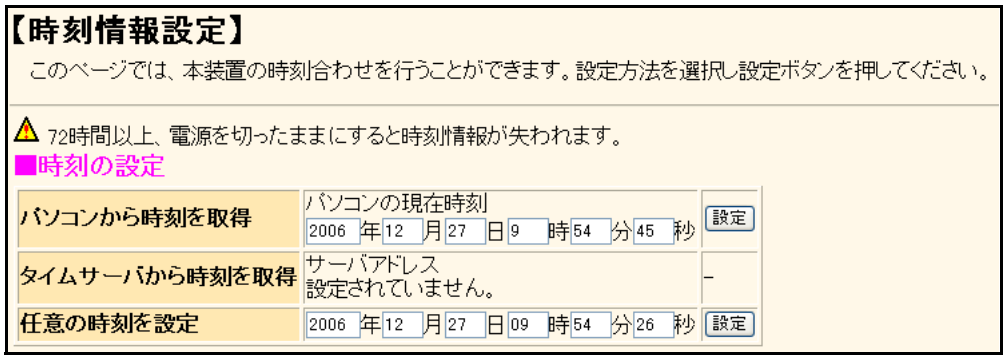
1.　本装置のトップページで、画面左側の［操作］タブをクリックします。

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。



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○○○○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

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

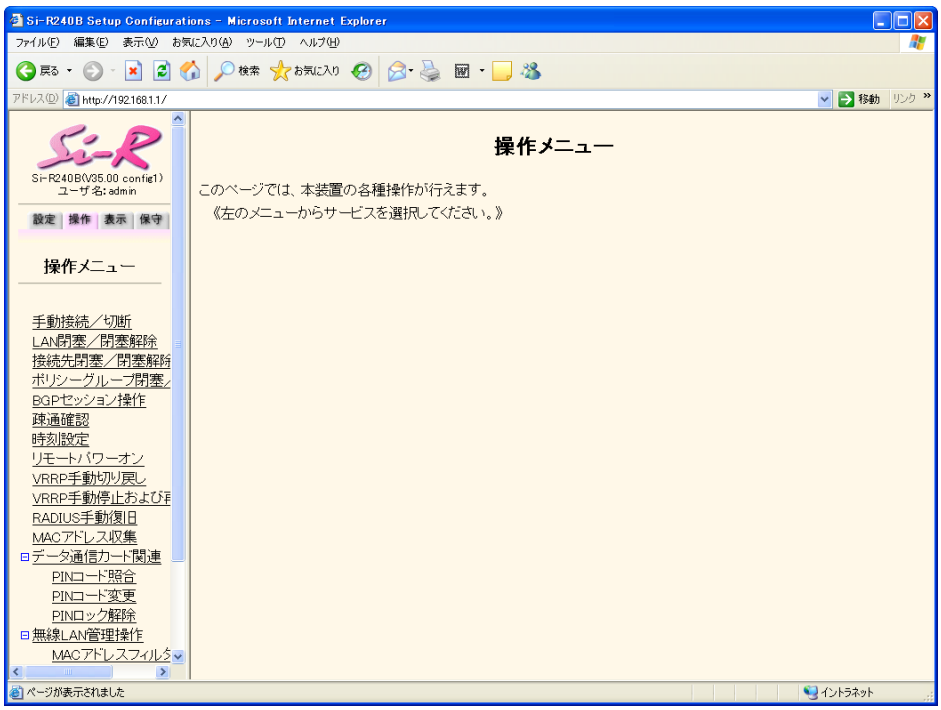
一般ユーザ（user）でログインしている場合は、「疎通確認」情報のみが表示され、操作することができます。その他の操作を使用する場合は、管理者（admin）に移行してください。

☛ 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。

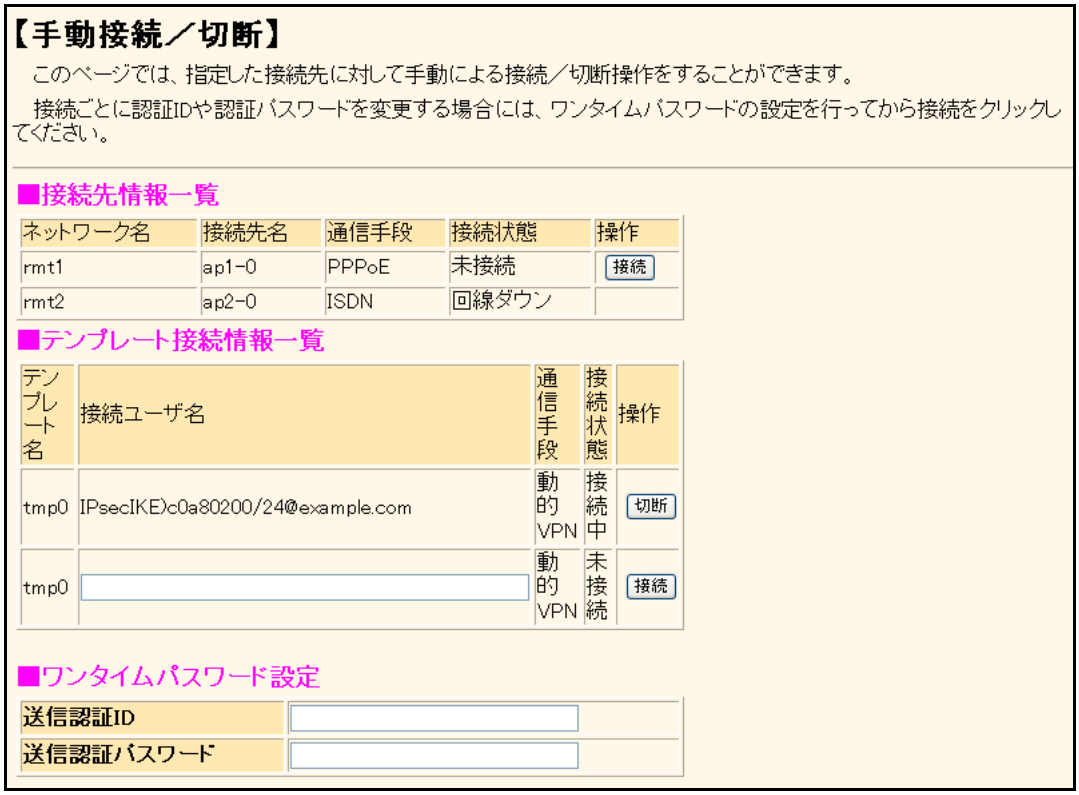
データ通信カード関連は、Si-R240B で表示されます。

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。



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。

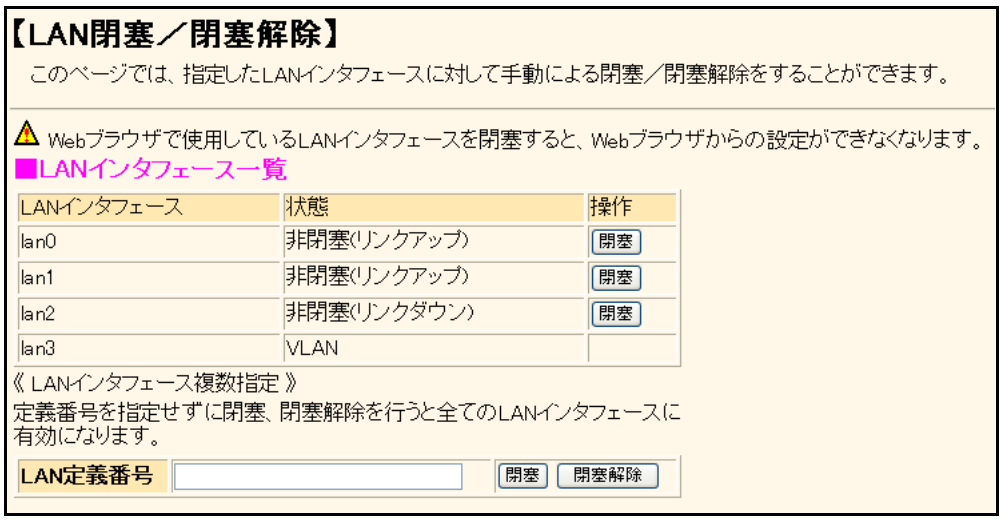
2.1.3　手動で LAN を有効化／無効化する

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。



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。

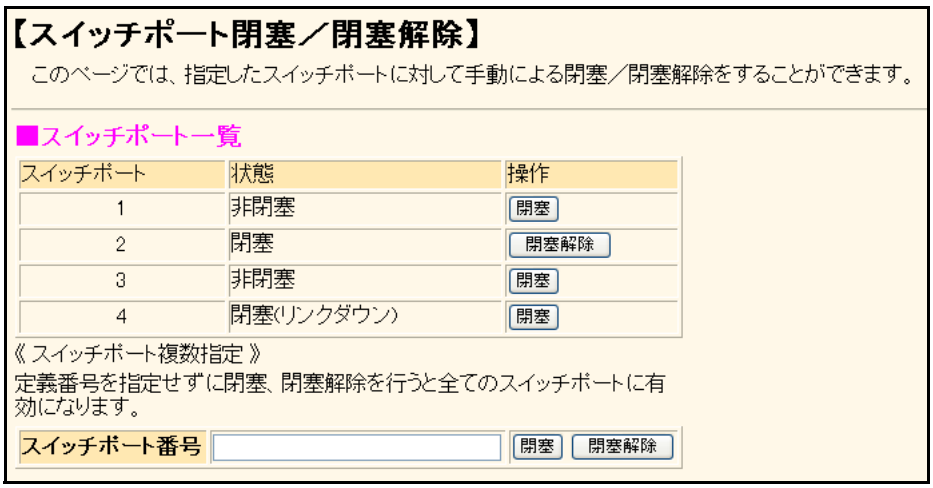
2.1.4　手動でスイッチポートを有効化／無効化する

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。



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。

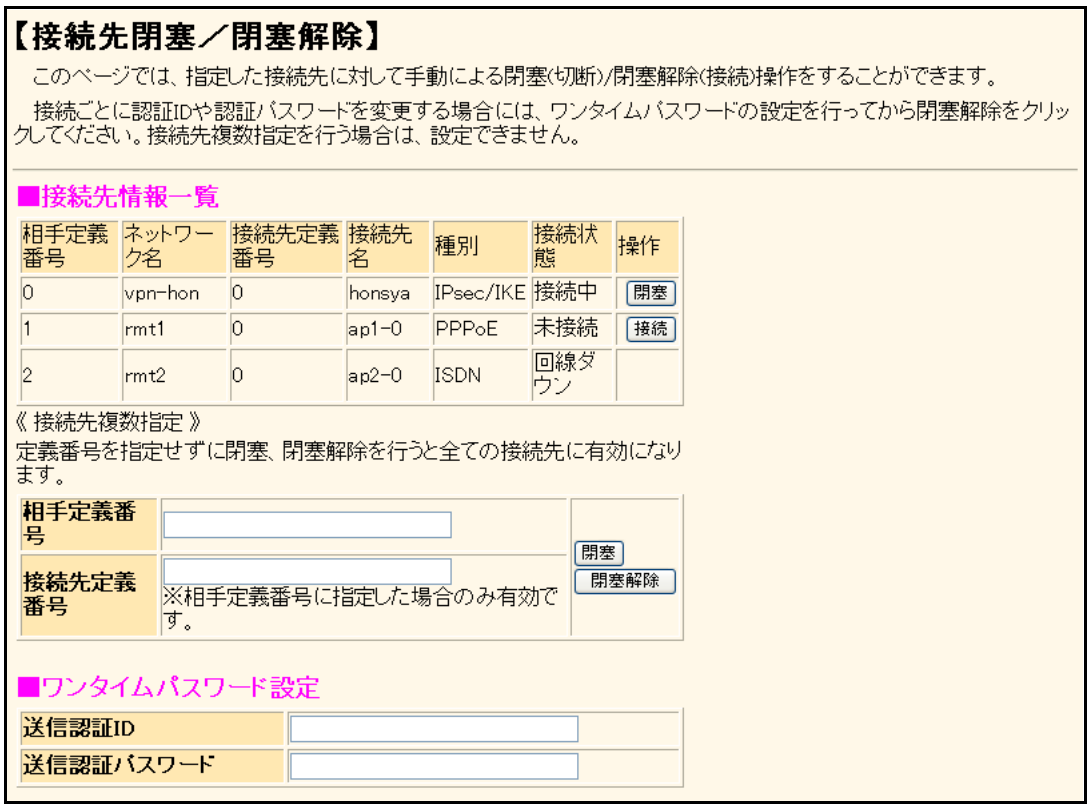
2.1.5　手動で接続先を有効化／無効化する

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。



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。

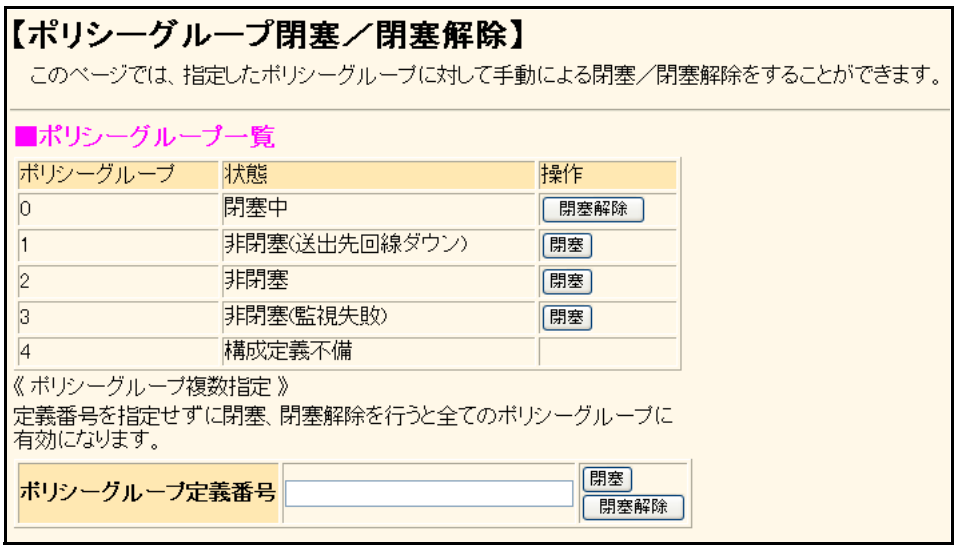
2.1.6　手動でポリシーグループを有効化／無効化する

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。



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

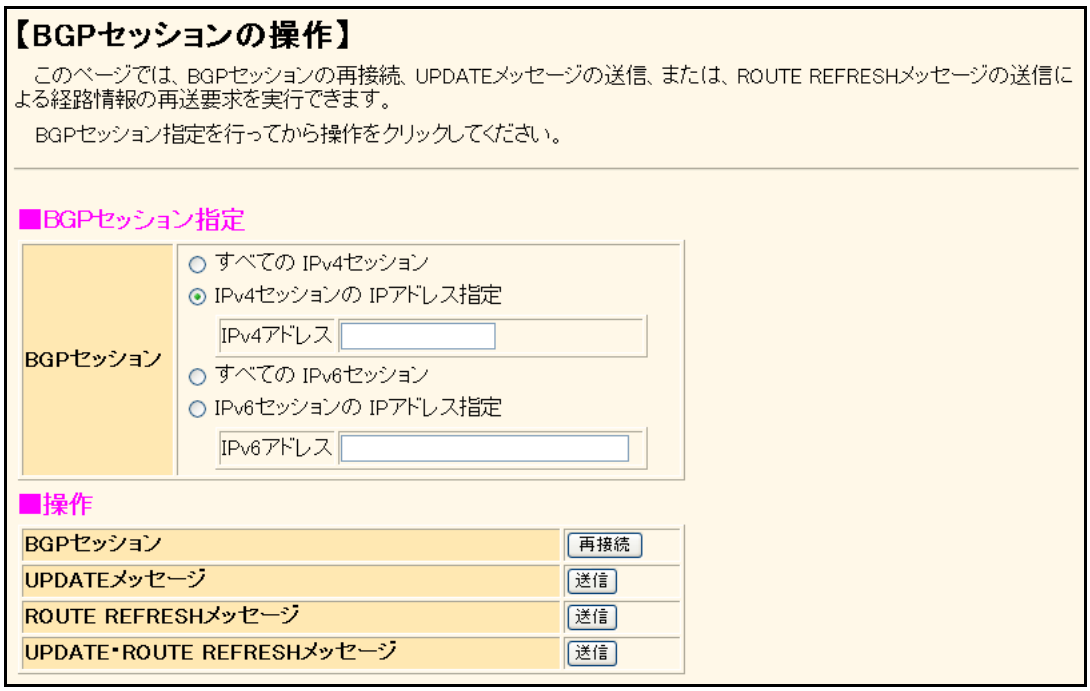
BGP セッションの再接続や経路情報の再交換を行う機能です。属性変更やフィルタ設定を変更した場合、その設定は設定変更前に送受信された経路情報には反映されませんが、この機能を使用することで反映させることができます。

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。



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。

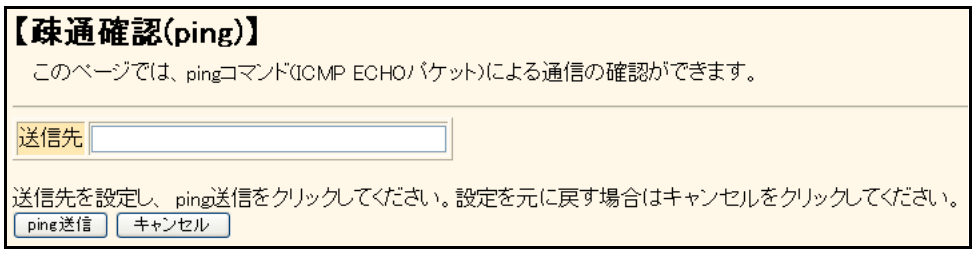
2.1.8　ネットワークの接続を確認する

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。



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。

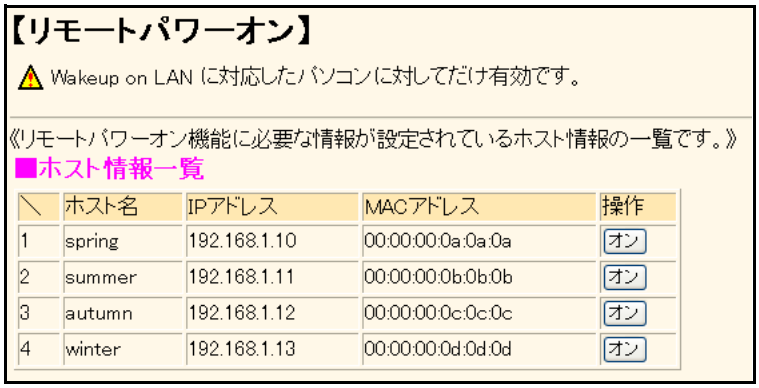
2.1.9　リモートパワーオン機能を使う

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」ー「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。



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。

補足　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。

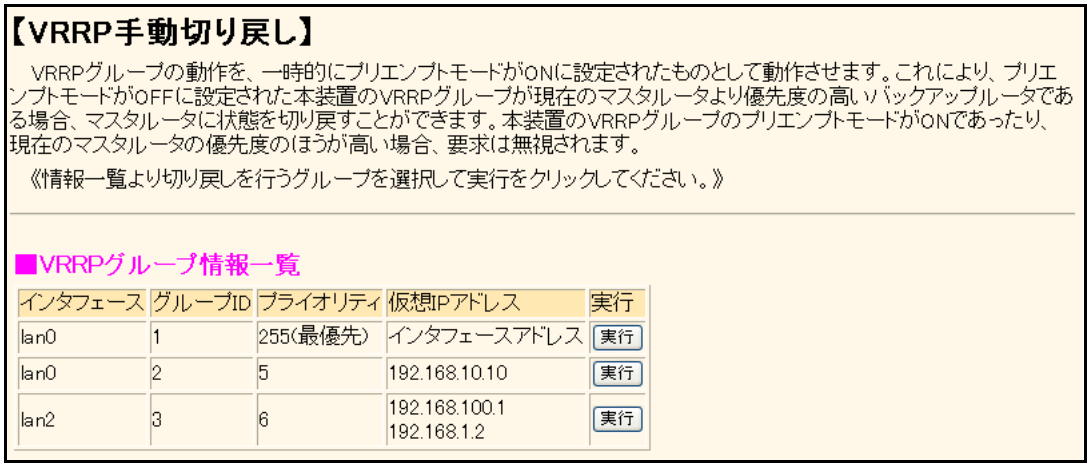
2.1.10　VRRP 手動切り戻し機能を使う

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。



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／再開始機能を使う

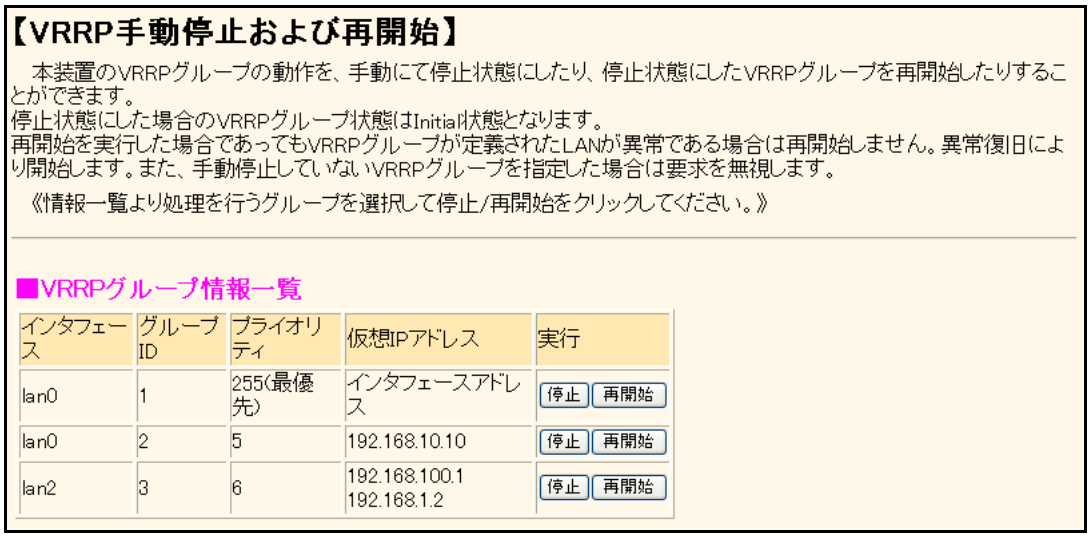
適用機種　全機種

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始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。

再開始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始できません。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／再開始」をクリックします。

「VRRP 手動停止／再開始」ページが表示されます。



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。
- 再開始する場合
  ［VRRP グループ情報一覧］で再開始するグループの欄の［再開始］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	復旧
	認証	1	192.168.2.6	1812	100	alive	-	
	アカウンティング	0	192.168.2.5	1813	0	alive	-	
	アカウンティング	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 コードによる照合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。

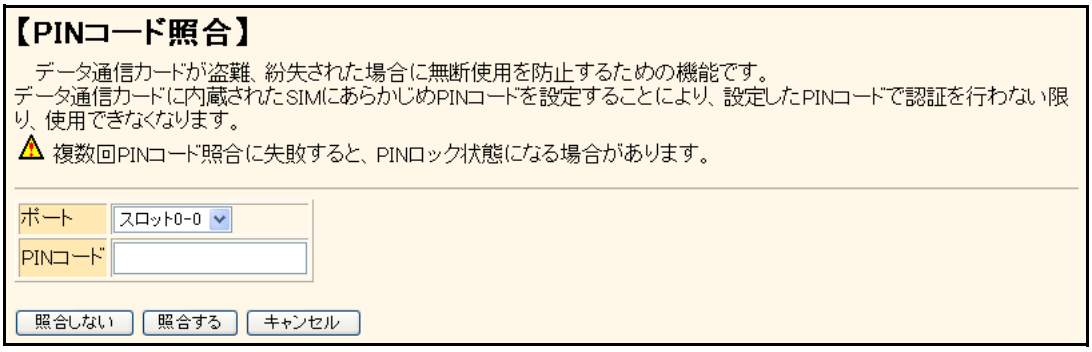
データ通信カードに内蔵された SIM にあらかじめ PIN コードを設定することにより、設定した PIN コードで認証を行わない限り、使用できなくなります。

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。



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。

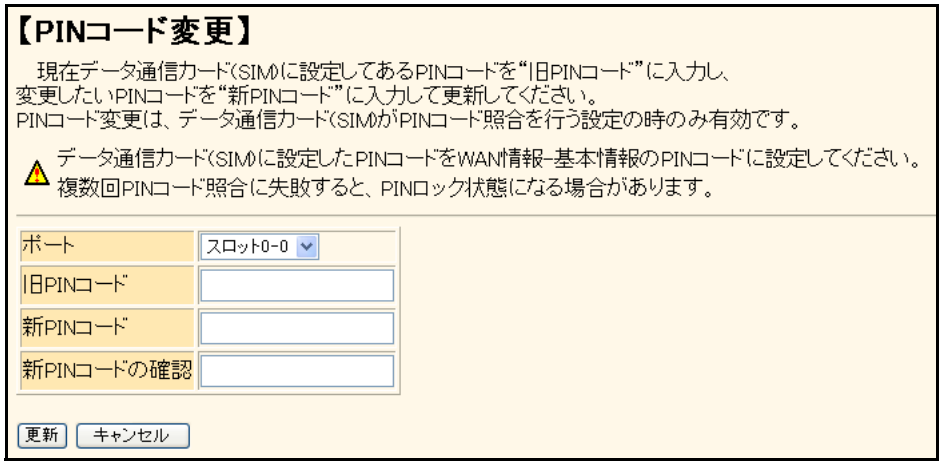
PIN コード変更は、データ通信カード（SIM）が PIN コード照合を行う設定のときだけ有効です。

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。



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。

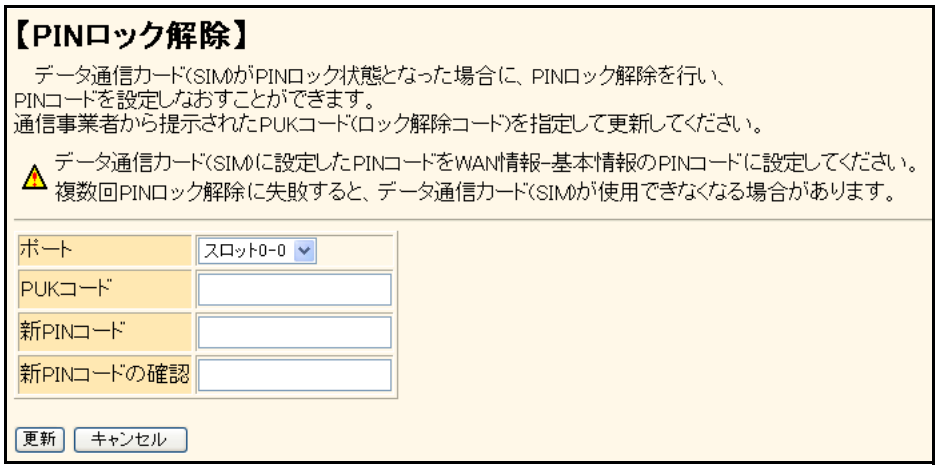
通信事業者から提示された PUK コード（ロック解除コード）を指定して更新してください。

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。



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。

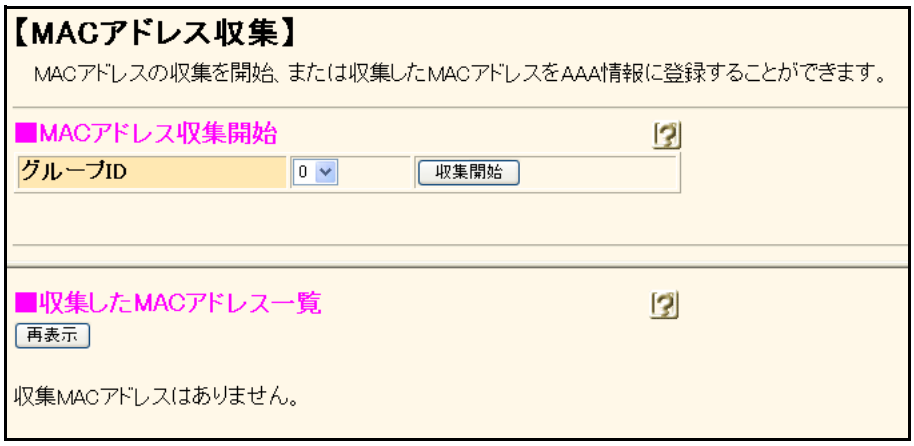
2.1.14　MAC アドレスの収集を行う

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。



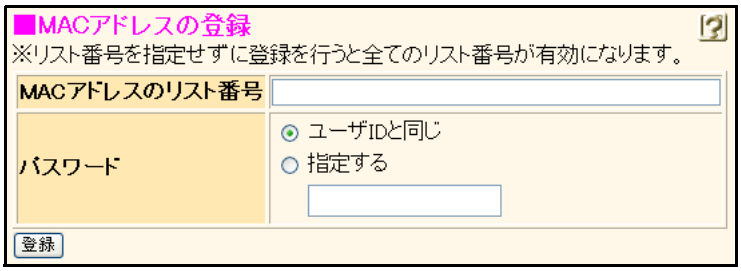
2.　「MAC アドレス収集開始」のグループ ID を指定して、［収集開始］ボタンをクリックします。

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

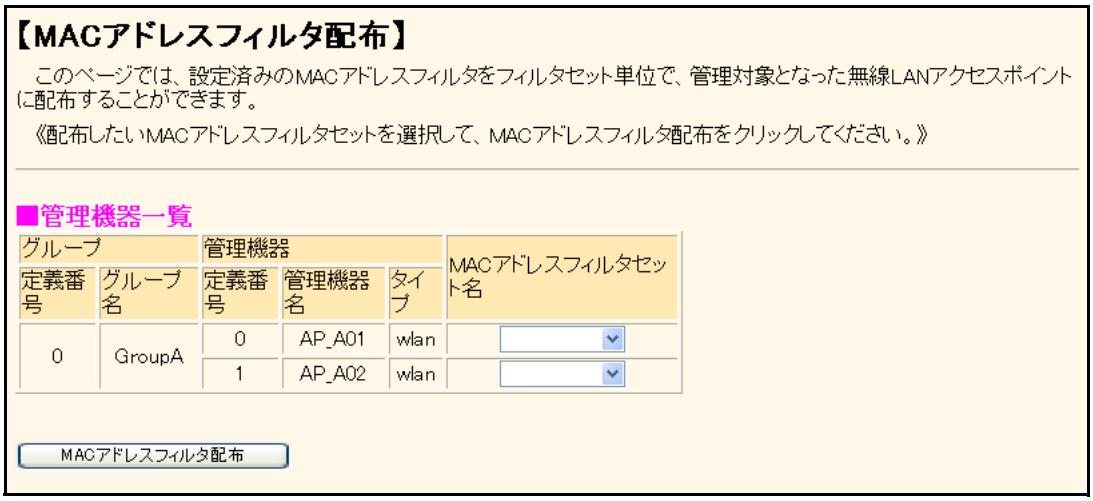
設定済みの MAC アドレスフィルタをフィルタセット単位で管理対象となった無線 LAN アクセスポイントに配布することができます。

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。



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。

補足
- 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

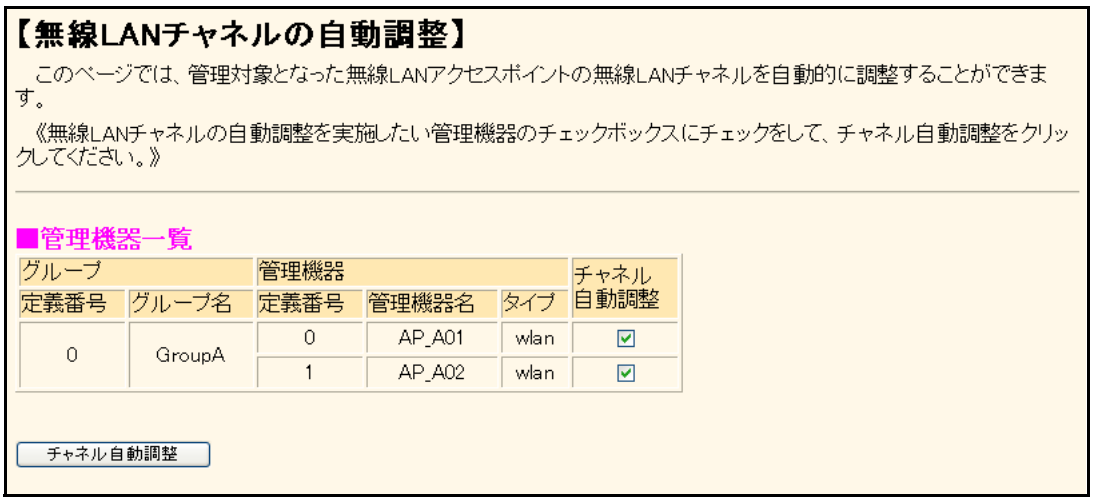
管理対象となった無線 LAN アクセスポイントの無線 LAN チャネルを自動的に調整することができます。

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 チャネルの自動調整」をクリックします。

「無線 LAN チャネルの自動調整」ページが表示されます。



2.　無線 LAN チャ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.　［チャネル自動調整］ボタンをクリックします。

無線 LAN チャ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 チャネル自動調整を行うようにしてください。

補足　無線 LAN チャ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

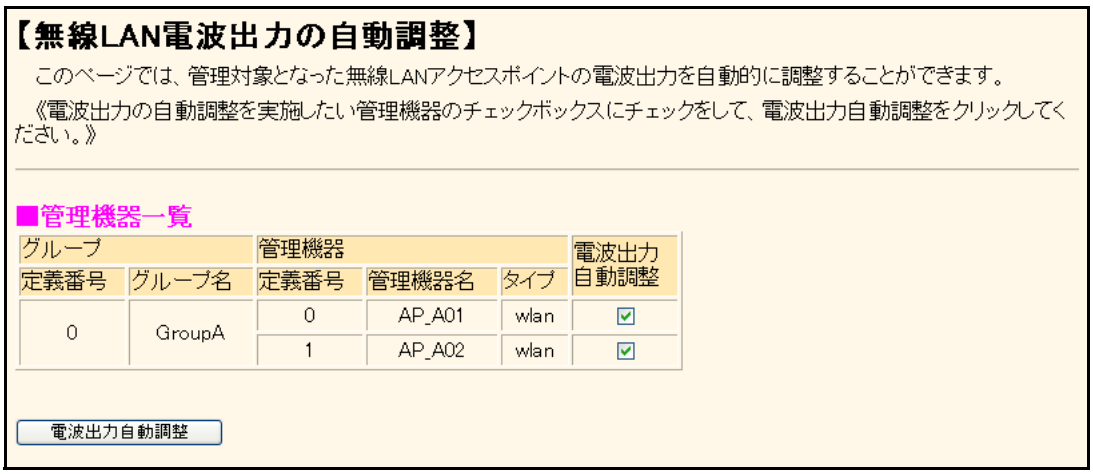
管理対象となった無線 LAN アクセスポイントの電波出力を自動的に調整することができます。

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。



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。

補足
- 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

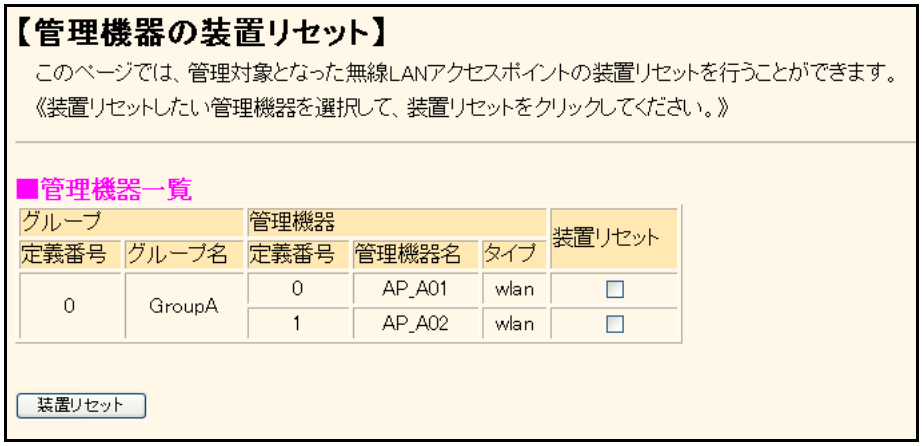
管理対象となった無線 LAN アクセスポイントの装置リセットを行うことができます。

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。



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

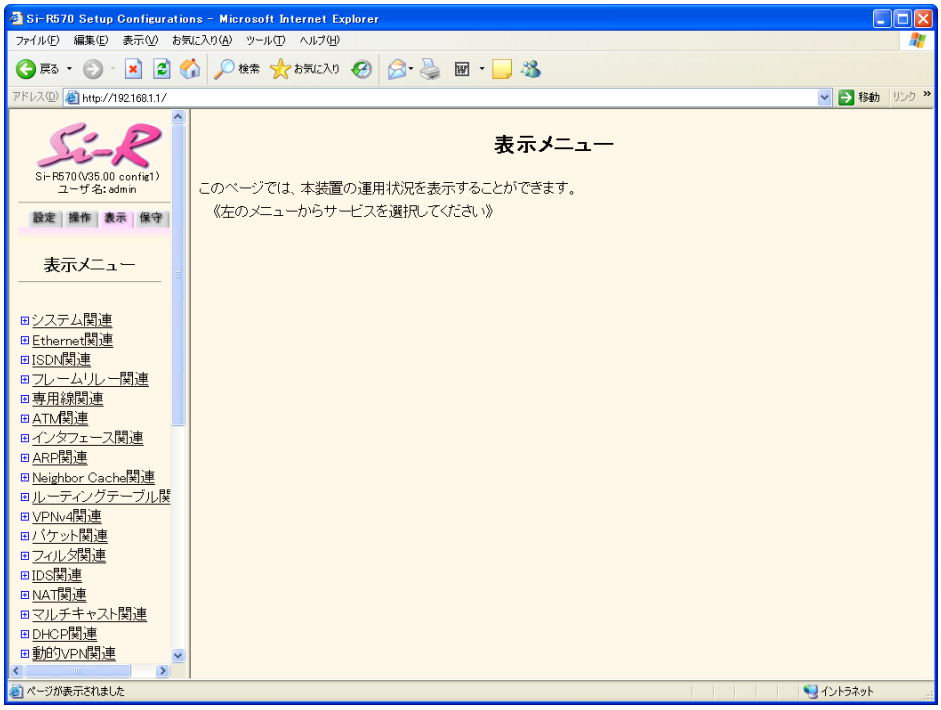
一般ユーザ（user）でログインしている場合は、「統計情報」をクリアすることができません。クリアする場合は、管理者（admin）に移行してください。

☛ 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
	WPA 統計情報	show wlan wpa statistics
インタフェース関連	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
	テンプレート統計情報	show template statistics
ARP 関連	ARP エントリ情報	show arp
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	show ip dhcp
	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
	スパニングツリー情報	show spanning-tree
MPLS 関連	FTN テーブル情報	show mpls ftn 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 sipgw
	統計情報	show sipgw 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

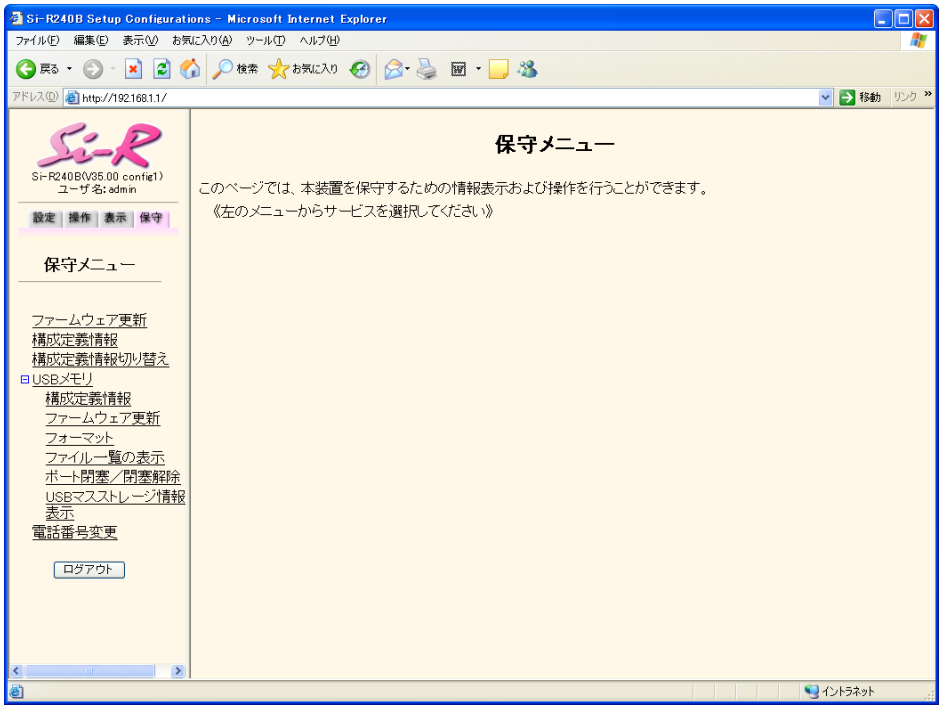
一般ユーザ（user）でログインしている場合は、「保守メニュー」が表示されません。「保守メニュー」を使用する場合は、管理者（admin）に移行してください。

☛ 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。

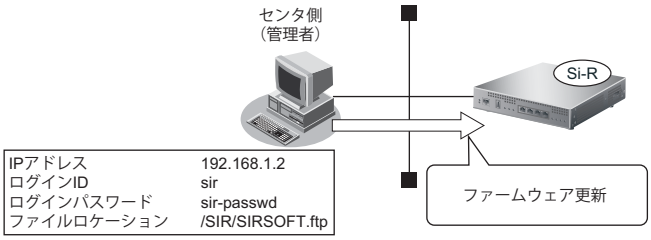
FTP サーバ（FTP サーバ機能を持つパソコンや UNIX システム）にファームウェアファイルを配置し、WWW ブラウザ（本装置の設定メニュー）を使ってネットワークに接続した本装置のファームウェアを更新できます。

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。

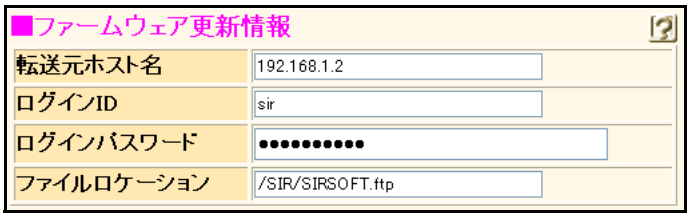
こんな事に気をつけて

- **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。



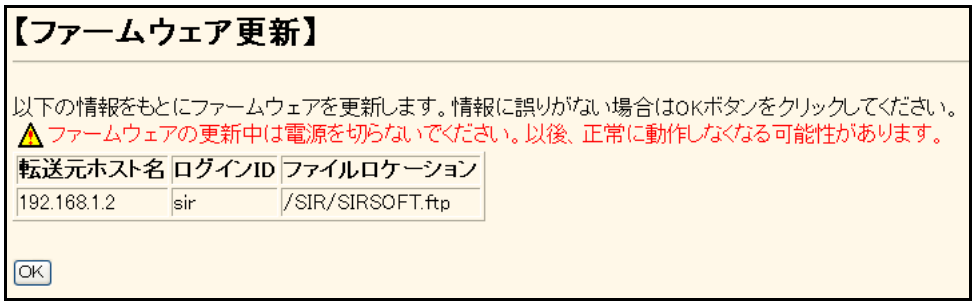
1. **設定メニューの基本設定で「装置情報」をクリックします。**
   「装置情報」ページが表示されます。
2. **「ファームウェア更新情報」をクリックします。**
   ［ファームウェア更新情報］が表示されます。
3. **以下の項目を指定します。**
   - 転送元ホスト名　→ 192.168.1.2
   - ログイン ID　→ sir
   - ログインパスワード　→ sir-passwd
   - ファイルロケーション　→ /SIR/SIRSOFT.ftp



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。



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

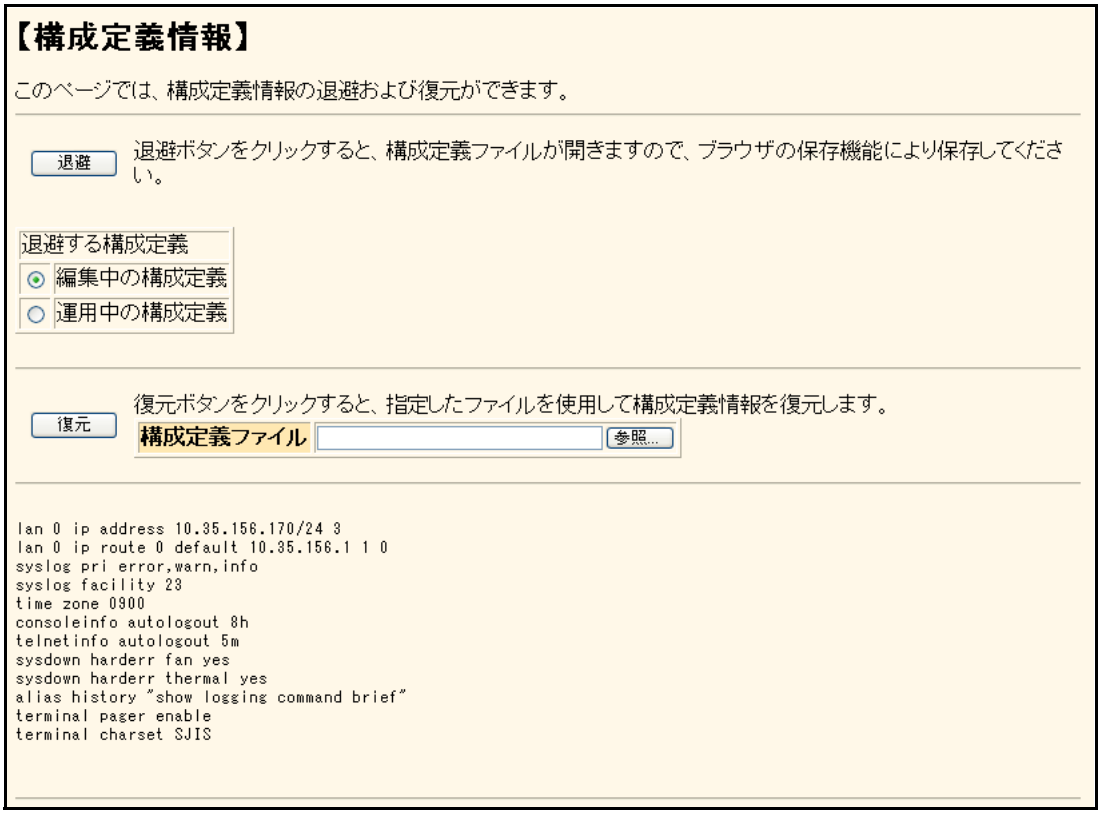
現在の本装置の構成定義情報をファイルに保存し、退避しておきます。必要になったときに保存しておいた構成定義情報を復元できます。

● 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。



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

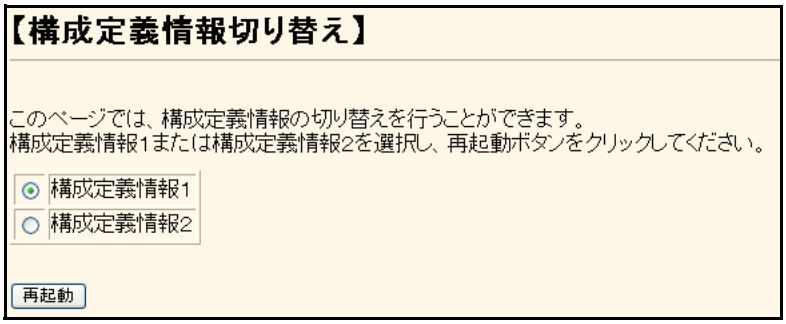
適用機種　全機種

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。



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。

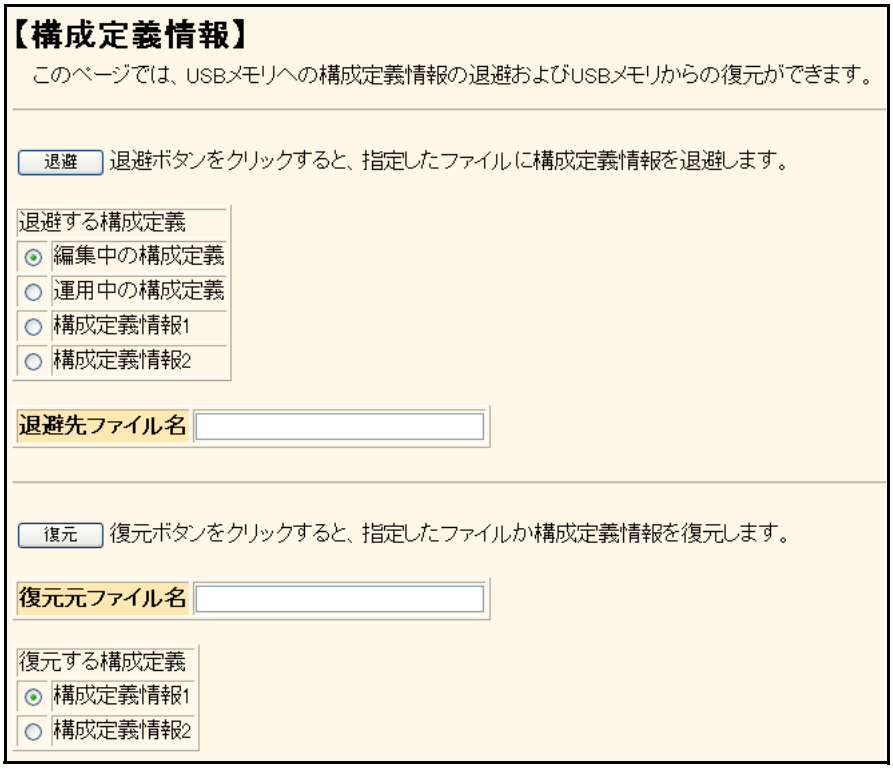
● 退避できる構成定義情報

- 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。



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。

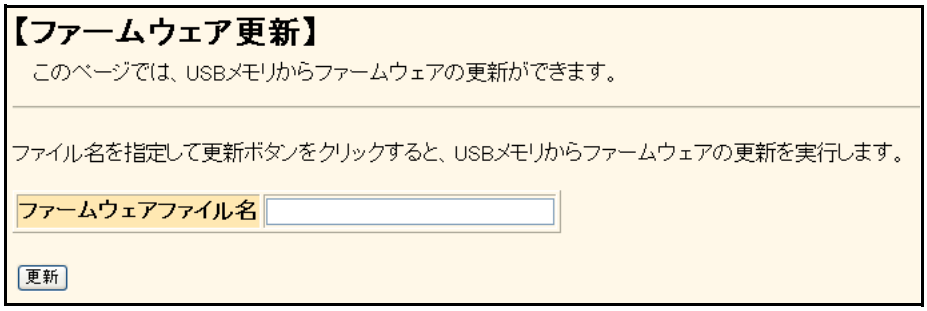
USB メモリに保存しておいた構成定義情報が復元されます。

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。



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。

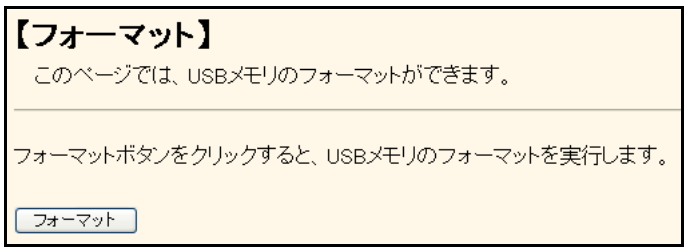
ファームウェアが更新されます。

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。



2.　［フォーマット］ボタンをクリックします。

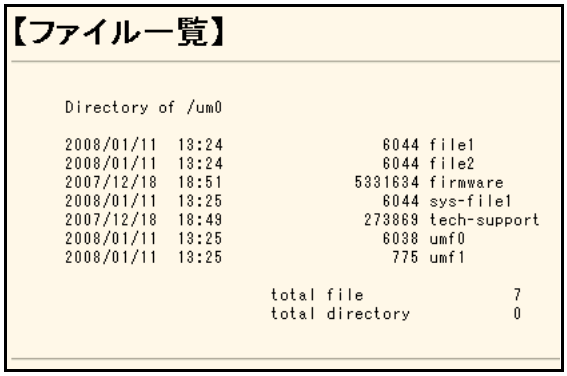
USB メモリがフォーマットされます。

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。

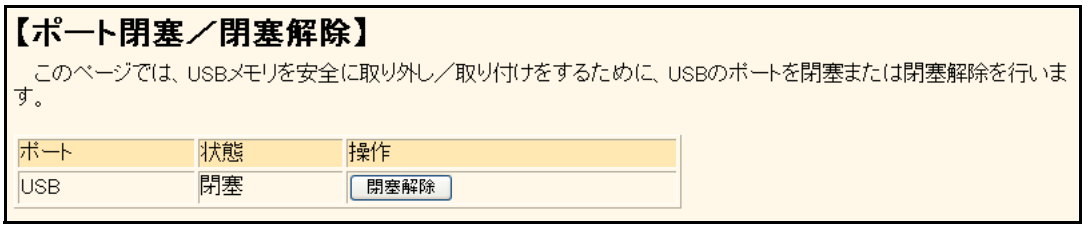


ポート閉塞／閉塞解除

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。



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

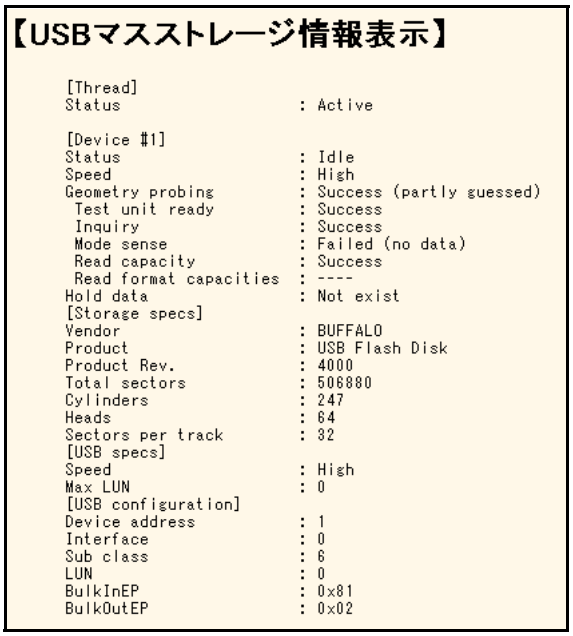
- **USB ポート閉塞実行後に USB メモリを取り外す場合は、保守メニューの「USB メモリ」-「ポート閉塞／閉塞解除」をクリックし、状態が「閉塞」となっていることを確認してから取り外してください。**
- **USB ポート閉塞解除実行後は、状態が「閉塞解除」になるまでは USB メモリを使用することができません。保守メニューの「USB メモリ」-「ポート閉塞／閉塞解除」をクリックし、状態を確認してください。**

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。



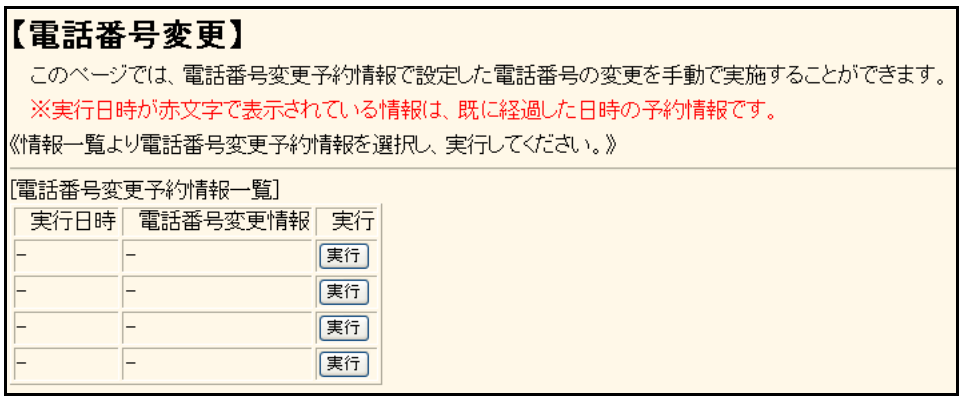
2.3.6　電話番号を変更する

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。



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。

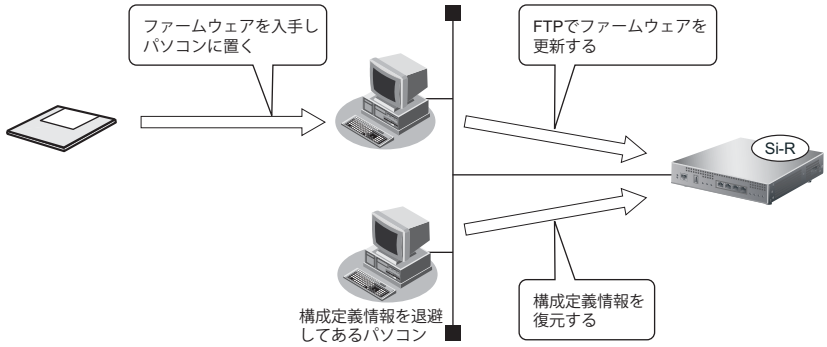
設定した内容が有効になります。

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。

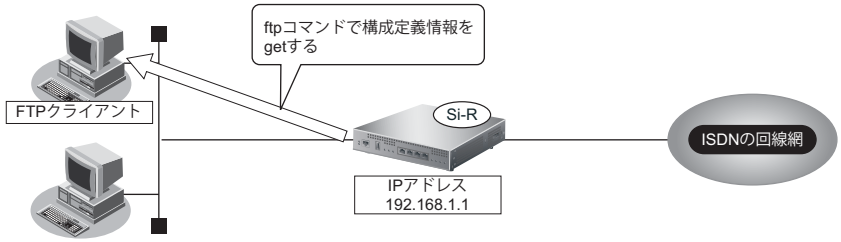
こんな事に気をつけて

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

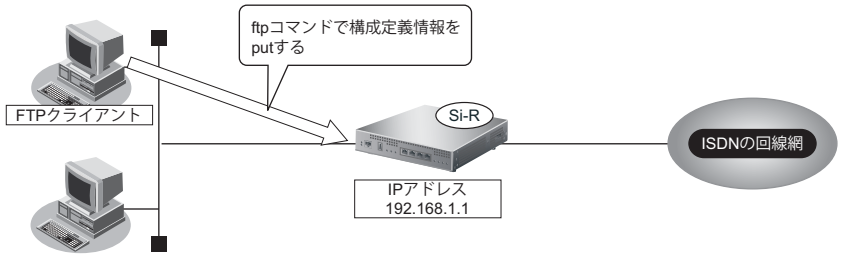
構成定義情報 1 をパソコン上の config1-1 ファイルに退避する場合の例を示します。

```
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>
```

補足 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。

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。

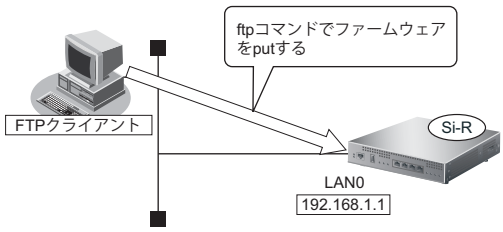
```
C:¥>cd 構成定義情報格納ディレクトリ
C:¥tmp>ftp 192.168.1.1                    ：本装置に接続する
Connected to 192.168.1.1.
220 Si-R370 V35.00 FTP server (config1) ready.
Name(192.168.1.1:root): ftp-admin         ：ユーザ名を入力する
331 Password required for ftp-admin.
Password:                                 ：パスワードを入力する
230 User 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>
```

補足　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>
```

補足

- 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

ね

は

ひ

ふ

ほ

ま

む

ゆ

り

ろ

Si-R シリーズ　Web ユーザーズガイド

P3NK-4012-05Z0

発行日　　2014 年 6 月

発行責任　　富士通株式会社