EAP 対応 RADIUS サーバアプライアンス

FutureNet RAシリーズ
ユーザーズガイド

Ver.1.12.0 対応版

CENTURY SYSTEMS

目次

はじめに

本書は、FutureNet RA-1200 および RA-730 のユーザーズガイドです。

◆ご注意

1 本装置の故障、誤動作、不具合、あるいは停電などの外部要因によって、通信の機会を逸したために生じた損害などの純粋経済損失につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。

2 通信情報が漏洩した事による経済的、精神的損害につきましては、当社はいっさいその責任を負いかねますのであらかじめご了承ください。

3 本書の内容の一部または全部を無断で転載、複写することを禁じます。

4 本書およびソフトウェア、ハードウェア、外観の内容について、将来予告なしに変更することがあります。

5 本書の内容については万全を期しておりますが、万一ご不審な点や誤り、記載漏れなどお気づきの点がありましたらご連絡ください。

◆商標の表示

□「FutureNet」はセンチュリー・システムズ株式会社の登録商標です。

□下記製品名等は米国 Microsoft Corporation の登録商標です。

Microsoft、Windows、Windows 95、Windows 98、Windows 2000、Windows Me、Windows XP、Windows Vista、Windows 7、Windows 8、ActiveDirectory

□ Macintosh、Mac OS X は、アップル社の登録商標です。

その他、本書で使用する各会社名、製品名は各社の商標または登録商標です。

◆本ユーザーズガイドを読む前に

□参考文献は以下のとおりです。

RFC 2865 Remote Authentication Dial In User Service (RADIUS).
RFC 2866 RADIUS Accounting.
RFC 2867 RADIUS Accounting Modifications for Tunnel Protocol Support.
RFC 2868 RADIUS Attributes for Tunnel Protocol Support.
RFC 2869 RADIUS Extensions.
RFC 3162 RADIUS and IPv6
RFC 3575 IANA Considerations for RADIUS (Remote Authentication Dial In User Service).
RFC 3579 RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP).
RFC 3580 IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines.
RFC 3748 Extensible Authentication Protocol (EAP).
RFC 4590 RADIUS Extension for Digest Authentication.
RFC 4675 RADIUS Attributes for Virtual LAN and Priority Support

第1章

本装置の概要

第１章 本装置の概要

Ⅰ．機能概要

FutureNet RA-730は、小型のRADIUSサーバアプライアンスです。IP-VPNサービスのRADIUS認証サーバとして利用できるだけでなく、有線/無線LANのセキュリティ確保のためIEEE802.1Xにも対応しており、ユーザ認証やアクセス履歴管理をおこなえます。

FutureNet RA-1200は、大規模ネットワーク向けのRADIUSサーバアプライアンスです。ギガビットに対応したイーサネットインタフェースを2ポート備え、大規模なIP-VPNサービスのRADIUS認証サーバとして利用できます。

◆主な機能

・EAPのサポート

PAP,CHAP認証の他に、EAP-MD5、EAP-TLS、EAP-PEAP、EAP-TTLSの各認証方式をサポートしています。

・ActiveDirectory，LDAPサーバとの連携

ユーザ情報を本装置上で管理するだけでなく、外部ActiveDirectoryまたはLDAPサーバ上のユーザ情報を利用してユーザ認証をおこなうことができます。
ActiveDirectory連携をおこなう場合、NT Domain名付きユーザの認証やコンピュータ認証も利用できます。

・柔軟なアトリビュート設定

認証に使用するアトリビュートや、認証成功時にレスポンス情報に付加するアトリビュートを任意に設定することができます。ベンダ固有アトリビュートも任意に指定できます。例えば、VLAN IDなどを認証結果情報に含めてRADIUSクライアントに通知することができます。

・プライベートCA

CAとして、クライアント証明書、サーバ証明書を発行する機能を有しており、EAP-TLS認証に必要な証明書を発行できます。

・各種ネットワークサービスへの対応

NTPに対応しており、外部NTPサーバと時刻同期がおこなえます。また、パケットフィルタ機能により、本装置への不要なトラフィックの流入や外部からの攻撃を防ぎます。

・Webブラウザからの設定とファームウェア更新

全ての設定はWebブラウザを用いたGUI画面でおこなえます。設定画面への通信はSSLで暗号化できます。また、Webブラウザの画面上から簡単にファームウェアの更新ができます。

・設定ウィザードによる容易な設定

管理者による設定をサポートするウィザード設定を用意しており、RADIUSの設定に不慣れな管理者でも、相互依存性のある設定項目を漏れなく順番に設定していくことができます。

・管理者権限の分割

装置全体の設定をおこなえる「本装置管理者」の他に、ユーザの追加削除等のユーザ管理作業のみをおこなえる「ユーザ管理者」を設定できます。

・ユーザプロファイル

同じ内容の設定を複数ユーザに対して容易に設定できるようにするために、共通の設定内容をあらかじめプロファイルとして設定しておくことが可能です。管理者は新規にユーザ登録する際には、このプロファイルの選択をおこなうことで、ユーザ毎の入力を省略することができます。プロファイルは、「ユーザ基本情報」、「認証アトリビュート」「応答アトリビュート」、「証明書」、「グループID」に分かれており、このプロファイルを組み合わせることでユーザ情報を素早く登録していくことができます。

・利用状況の把握

各ユーザの現在のログイン情報を管理画面上で確認することができます。管理者の操作により、ログイン中のユーザを強制的にログアウトさせることができます。

・充実したログ

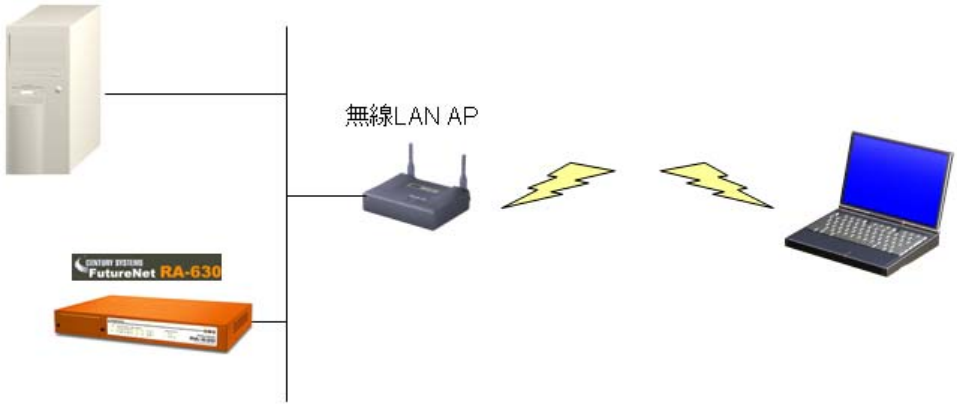
ログは、システムログ、認証ログ、アカウンティングログの３種類に分けて記録されます。ネットワーク経由で他のsyslogサーバに送ることもできます。

・ネットワークテスト

設定時、運用時のネットワークトラブルの解決のため、管理画面上から到達性確認、ルート確認、名前解決確認のテストをおこなうことができます。条件を指定してパケットキャプチャを実行し、画面上にダンプ情報を表示します。

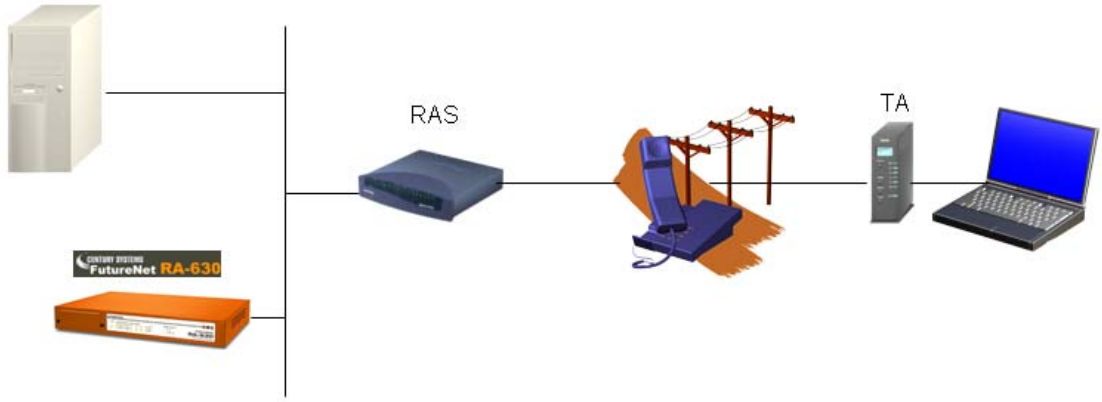
Ⅱ．利用例

◆利用例１　無線 LAN



本装置を 802.1X 対応無線 LAN の認証サーバとして利用します。
ワイヤレス LAN クライアントである PC が無線 LAN アクセスポイントに接続した際に、無線 LAN アクセスポイントが認証処理を本装置に問い合わせるように設定することで、多数のアクセスポイントにおける認証を本装置で一元的に管理できます。認証には、EAP-MD5、EAP-TLS、EAP-PEAP、EAP-TTLS の各認証方式を利用できます。

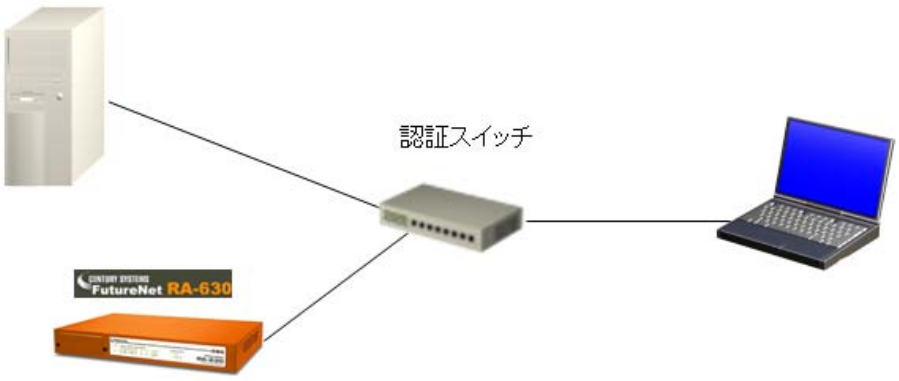
◆利用例２　リモートアクセス



本装置を ISDN 等によるリモート接続の認証サーバとして利用します。
リモート PC からの接続に対し、リモートアクセスサーバ(RAS)が、認証処理を本装置に問い合わせるように設定することで、リモートアクセスの認証処理を本装置で一元的に管理できます。認証には、PAP/CHAP 認証方式を利用します。また、着信した電話番号に応じた認証可否の判断等も RAS と連携しておこなうことができます。

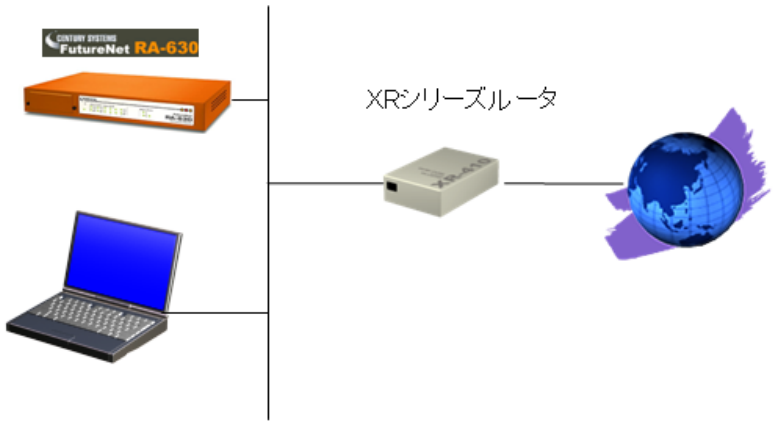
Ⅱ．利用例

◆利用例３ 認証スイッチ



本装置を 802.1X 対応認証スイッチの認証サーバとして利用します。
PC を認証スイッチに接続した際の認証処理を本装置に問い合わせるように設定することで、各認証スイッチにおける認証を本装置で一元的に管理できます。認証には、EAP-MD5、EAP-TLS、EAP-PEAP、EAP-TTLS の各認証方式を利用できます。認証スイッチ側に MAC アドレス認証や VLAN 設定の機能があれば、本装置側でこれらの情報を用いた認証や設定管理をおこなうことで、不正な持込み PC の排除や、ユーザに応じた VLAN の切り替えなどをおこなうことができます。

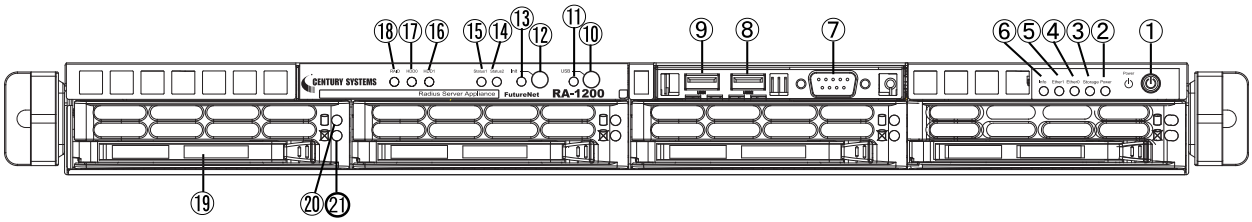
◆利用例４ Web 認証（ゲートウェイ認証）



当社 NXR シリーズに搭載している Web 認証（ゲートウェイ認証)機能の利用時に、認証情報を本装置に問い合わせるように設定することができます。認証には、PAP を利用します。これにより、NXR を超えた通信の可否の判断を、本装置上でおこなうことができます。

III．各部の名称と機能（RA-1200）

◆製品前面 （RA-1200）



① Power スイッチ
停止中(スタンバイ状態）に Power スイッチを押すと、システムが起動します。ただし、通電開始直後は、Power スイッチを押すまで 30 秒以上待つ必要があります。
起動中に Power スイッチを押すと、終了処理を行いスタンバイ状態に移行します。

通電を開始した場合の動作は、以前の停止状態に依存します。
正常に停止していれば、通電を開始してもスタンバイ状態のままです（起動しません)。
正常に停止していなければ、通電開始とともにシステムが起動します。

② Power LED（●）
本装置の起動中は点灯（●）します。
停止中(スタンバイ状態）は消灯（●）します。

③ Storage LED(●)
内蔵ディスク(RAIDを除く)へのアクセス時に点滅します（＊)。

④ Ether0 LED（●）
⑤ Ether1 LED（●）
対応する Ethernet ポートの状態を表示します。
接続（Link up）時は、点灯します（●)。
未接続（Link down）時は、消灯します（●)。
通信中は、点滅します（＊)。

⑥ Information LED（●）
電源ユニットの異常時や、温度やファン異常時に、点滅（＊）または点灯（●）します。
点滅または点灯によって、ハードウェアに何らかの異常が発生したことを知らせますが、どのような異常かを特定することはできません。

⑦ RS-232 ポート
本装置では使用しません。

⑧ USB2 ポート
⑨ USB1 ポート
本バージョンでは使用しません。

⑩ USB スイッチ
本バージョンでは使用しません。

⑪ USB LED(●)
本バージョンでは使用しません。

⑫ Init スイッチ
システム起動時(通電開始時、または Power スイッチ押下時）に本スイッチが押されている場合、システムは工場出荷状態で起動します。

約 3 秒間押し続けると、スイッチの押下が確定し、Init LED が点灯します。この後、システムは工場出荷状態で起動します。

⑬ Init LED(●)
機器の起動・停止、設定の復帰、初期化などの状態を表します。

工場出荷状態での起動処理中、および初期化処理中に点灯(●)します。
通常の起動処理中、停止処理中、設定の復帰処理中は消灯(●)します。
詳細については、p.12 の表を参照してください。

III．各部の名称と機能（RA-1200）

⑭ **Status2 LED**(●)
⑮ **Status1 LED**(●)
機器の状態を表示します。
詳細については、p.13 の表を参照してください。

⑯ **HDD1 LED**(●)
⑰ **HDD0 LED**(●)
本バージョンでは使用しません。

⑱ **RAID LED**(●)
本バージョンでは使用しません。

⑲ **RAID(HDD ベイ)**
前面に 4 個の HDD ベイを配置しています。向かって左から 0，1，2，3 とします。

0，1 に HDD を実装しています。2，3 は使用しません。RAID1 に対応しています。

RA-1200 が故障した場合、2 台の HDD を同時に別の RA-1200 に移設することが出来ます。

⑳ **Activity LED**(●)
㉑ **Fail LED**（●）
HDD ベイ毎に、Activity LED と Fail LED を装備しています。

Activity LED は、アクセス時に点灯（●）します。

異常が発生した場合は、該当する HDD ベイの Fail LED が点滅（＊）または点灯（●）します。
正常時は、消灯（●）しています。
故障時は、点灯（●）します。
リビルド中は、1Hz（on:50msec，off:500msec）で点滅（＊）します。

III．各部の名称と機能（RA-1200）

RA-1200 の Status1 LED、Status2 LED および Init LED の表示状態と、本装置の動作内容の関係を下表に記します。

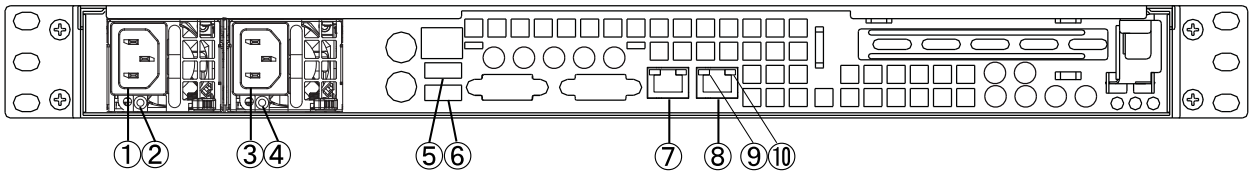
本装置の動作	LEDの表示状態			備考
	Status1	Status2	Init	
停止中(スタンバイ状態)	●	●	●	—
機器起動	●	●	●	約1秒間
	●	●	●	約80秒間
	＊	●	●	40秒以上(設定に依存)
機器再起動	＊	●	●	約20秒間
	●	●	●	約1秒間
	●	●	●	約70秒間
	＊	●	●	40秒以上(設定に依存)
機器停止	＊	●	●	約20秒間
工場出荷状態での起動 (Initスイッチ押下)	●	●	●	約1秒間
	●	●	●	約3秒間
	●	●	●	約80秒間
	＊	●	●	40秒以上(設定に依存)
起動処理完了	●	●	●	—
設定復帰 (強制同期を含む) (設定取得の設定更新時を含む)	＊	●	●	40秒以上(設定に依存)
設定初期化	＊	●	●	40秒以上(設定に依存)
設定復帰・設定初期化完了	●	●	●	—
RADIUSサービス起動中	●	●	●	—
ファームウェア更新 (再起動完了まで)	＊	＊	●	約30秒間
	＊	●	●	約10秒間
	●	●	●	約1秒間
	●	●	●	約70秒間
	＊	●	●	40秒以上(設定に依存)
ハードウェア異常	＊＊	＊＊	＊＊	早い点滅(3～4Hz)

●： LED が消灯している状態です。
●： LED が点灯(緑色)している状態です。
●： LED が点灯(橙色)している状態です。

＊ ： LED が点滅(緑色)している状態です。
1Hz(on:500msec，off:500msec)
＊＊： LED が高速点滅(緑色)している状態です。
＊＊： LED が高速点滅(橙色)している状態です。
3～4Hz

Ⅲ．各部の名称と機能（RA-1200）

◆製品背面 （RA-1200）



①　電源ケーブル差込口
③　電源ケーブル差込口
製品付属の電源ケーブルを接続するコネクターです。ケーブルは必ず付属のものをご使用ください。

本装置は、電源ユニット(400W)を２個搭載しています。

②　電源ユニット LED(● / ●)
④　電源ユニット LED(● / ●)
各電源ユニットに、LED が１つあります。
機器起動時は緑色点灯（●）します。
停止中（スタンバイ状態）は橙色点灯（●）します。

⑤　USB0 ポート
⑥　USB3 ポート
本バージョンでは使用しません。

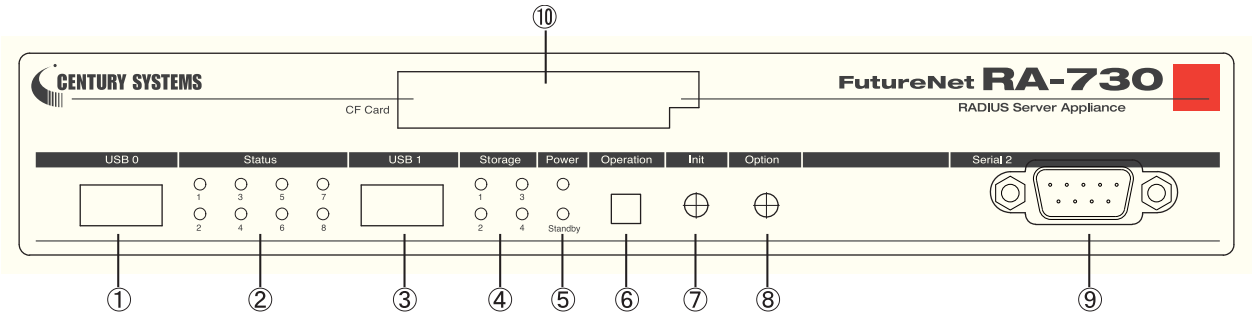
⑦　Ether0 ポート
⑧　Ether1 ポート
イーサネット規格の UTP ケーブル(LAN ケーブル)を接続する Ethernet ポートです。
Auto MDI/MDI-X に対応しています。ただし、Auto negotiation を OFF にした場合は、Auto MDI/MDI-X も OFF になります。

⑨　Speed LED(■ / ■)
Ethernet の接続速度を示します。LED は以下のようなパターンで点灯 / 消灯します。
未接続　　：消灯(■)
10Base-T モード　：消灯(■)
100Base-TX モード ：緑点灯(■)
1000Base-T モード ：橙点灯(■)

⑩　Activity LED(■)
Ethernet ケーブルのリンク状態を示します。ランプは以下のようなパターンで点灯 / 消灯します。
Link Up　　：点灯(■)
Link Down　：消灯(■)
通信中　　：点滅（＊）

Ⅳ．各部の名称と機能（RA-730）

◆製品前面 （RA-730）



① USB 0 ポート
使用しません。

② Status LED
Status LED の概要は、下記のとおりです。
1(●): ファームウェア更新ステータスを示します。
2(●): システムステータスを示します。
3(●): 初期化処理ステータスを示します。
4(●): RADIUSサービスステータスを示します。
5(●): 使用しません。
6(●): 使用しません。
7(●): 使用しません。
8(●): 使用しません。

なお、Status LED の詳細については、次ページを参照してください。

③ USB 1 ポート
使用しません。

④ Storage LED
1(●): 使用しません。
2(●): 使用しません。
3(●): 内蔵ストレージまたはCFカードへのアクセス時に点滅(＊)します。
4(●): 使用しません。

⑤ Power LED ・ Standby LED
本装置の起動・停止の状態を示します。
Power LED(●) ： 起動中に点灯(●)します。
Standby LED(●): 停止中(スタンバイ状態)に点灯(●)します。

⑥ Operation スイッチ
・起動中に押すと、終了処理を行いスタンバイ状態に移行します。**ただし、通常は設定画面の管理機能のメニュー「システム」から「停止」画面でシステム停止状態にしてください。**
・起動中に 4 秒以上押すと、強制終了処理を行いスタンバイ状態に移行します。**ただし、本装置が破損する可能性があるので、非常時のみに使用して下さい。**
・停止中(スタンバイ状態) に押すと、システムが起動します。
・なお、電源を投入すると、本スイッチを押さなくても起動処理が開始されます。

⑦ Init スイッチ
本装置を初期化するときに使用します。本装置の起動処理時に本スイッチが押された場合、工場出荷状態で起動します。
初期化が行われる場合、Status LED 3 が点灯(●)します。

⑧ Option スイッチ
使用しません。

⑨ Serial 2 ポート
使用しません。

⑩ CF カードスロット
使用しません。

Ⅳ．各部の名称と機能（RA-730）

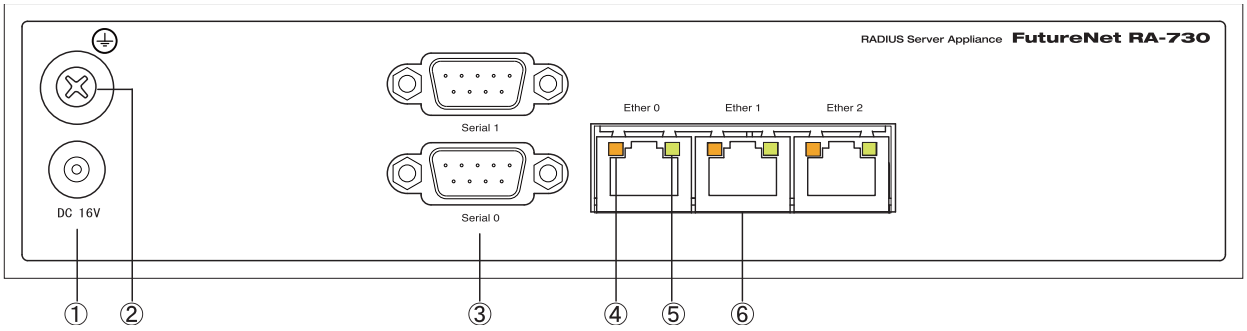
RA-730 の Status LED および Power LED、Standby LED の表示状態と、本装置の動作内容の関係を下表に記します。

LEDの表示		本装置の動作内容
Status ①　③　⑤　⑦ ②　④　⑥　⑧	Power ○ ○ Standby	
●　●　●　● ●　●　●　●	● ●	- 停止中(スタンバイ状態)
●　●　●　● ●　●　●　●	● ●	- 起動処理開始 (20～25秒程度)
●　●　●　● ＊　●　●　●	● ●	- 起動処理中 - 設定復帰中(強制同期、設定取得の設定更新時も含む) - 停止処理中
●　●　●　● ＊　●　●　●	● ●	- 工場出荷状態での起動処理中(Initスイッチ押下) - 設定初期化中
●　●　●　● ●　●　●　●	● ●	- 起動処理完了 - 設定復帰完了
●　●　●　● ●　●　●　●	● ●	- RADIUS サービス起動中(RADIUS 認証可能状態)
●　●　●　● ＊　●　●　●	● ●	- ファームウェア更新中
＊　＊　●　● ＊　＊　●　●	● ●	- 起動処理失敗(再起動は行わない) - ファームウェア更新失敗 (再起動は行わない)
＊　＊　＊　＊ ＊　＊　＊　＊	● ●	- 重大なエラー (10秒後に再起動を開始)

●：　LED が点灯(橙色)している状態です。
＊：　LED が点滅(橙色)している状態です。
●：　LED が点灯(緑色)している状態です。
＊：　LED が点滅(緑色)している状態です。
●：　LED が消灯している状態です。

Ⅳ．各部の名称と機能（RA-730）

◆製品背面 （RA-730）



① DC 16V 電源コネクタ
製品付属のAC アダプタを接続します。

② FG(アース）端子
保安用接続端子です。必ずアース線を接続してください。

③ Serial 0 ポート・Serial 1 ポート
使用しません。

④ SPEED LED
Ethernet ポートの接続速度を表示します。
10Base-T モード（■）
100Base-TX モード(■)
1000Base-T モード（■）

⑤ LINK/ACT LED
Ethernet ポートの接続状態を示します。
Link Up(■)
Link Down(■)
データ通信時(＊(点滅))

⑥ Ether 0・Ether 1・Ether 2
それぞれ、独立したセグメントとして動作します。
全てのEthernetポートは、Gigabit Ethernet (1000BASE-T)に対応しています。
イーサネット規格のUTP ケーブル(LAN ケーブル)を接続します。極性は自動判別します。

Ｖ．動作環境

本製品をお使いいただくには、以下の環境を満たしている必要があります。

◆ハードウェア環境

・本製品に接続するコンピュータの全てに、10Base-T または 100Base-TX、1000Base-T の LAN ボード / カードがインストールされていること。

・本製品と全てのコンピュータを接続するためのハブやスイッチングハブが用意されていること。

・本製品と全てのコンピュータを接続するために必要な種類のネットワークケーブルが用意されていること。

◆ソフトウェア環境

・TCP/IP を利用できる OS がインストールされていること。

・接続されている全てのコンピュータの中で少なくとも１台に、ブラウザがインストールされていること。弊社では Internet Explorer で動作確認を行っています。

なおサポートにつきましては、本製品固有の設定項目と本製品の設定に関係する OS 上の設定に限らせていただきます。OS 上の一般的な設定やパソコンにインストールされた LAN ボード / カードの設定、各種アプリケーションの固有の設定等のお問い合わせについてはサポート対象外とさせていただきますので、あらかじめご了承ください。

第2章

コンピュータのネットワーク設定

第2章 コンピューターのネットワーク設定

ネットワーク設定について

本製品の設定は、Webブラウザが動くパソコンから本製品の設定画面へアクセスしておこないます。
工場出荷時には、**本製品のIPアドレスは「192.168.0.254」に初期設定**されているため、設定に使うパソコンのネットワーク設定を、事前にこのIPアドレスと通信できるように設定しておく必要があります。

本章では、設定に使うパソコン側のネットワーク設定の方法について、OS毎に説明します。
ご使用のパソコンのOSに合わせて参照し、設定をおこなってください。

第2章 コンピューターのネットワーク設定

Ⅰ．Windows XPのネットワーク設定

ここではWindowsXPが搭載されたコンピュータのネットワーク設定について説明します。

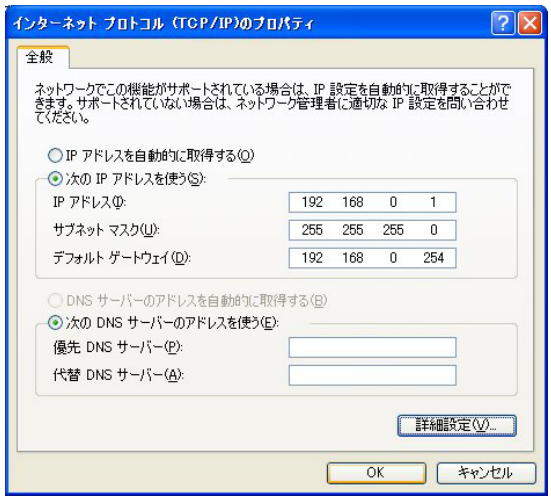
1 「コントロールパネル」→「ネットワーク接続」から、「ローカル接続」を開きます。

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコル(TCP/IP)」を選択して「プロパティ」ボタンをクリックします。

4 「インターネットプロトコル(TCP/IP)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



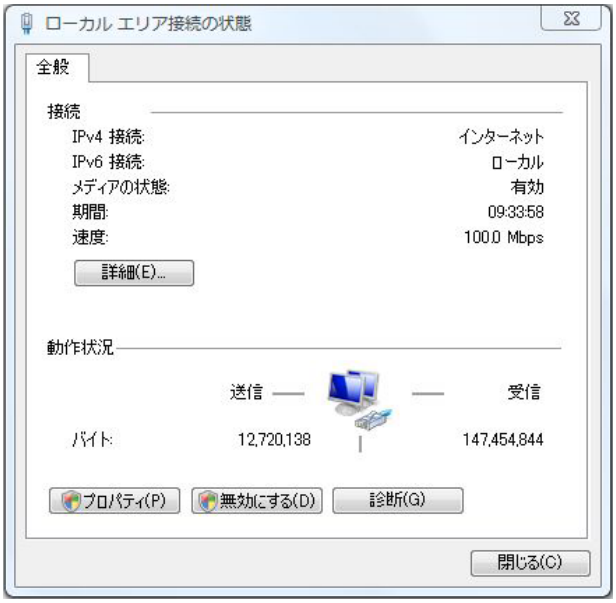
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

Ⅱ．Windows Vistaのネットワーク設定

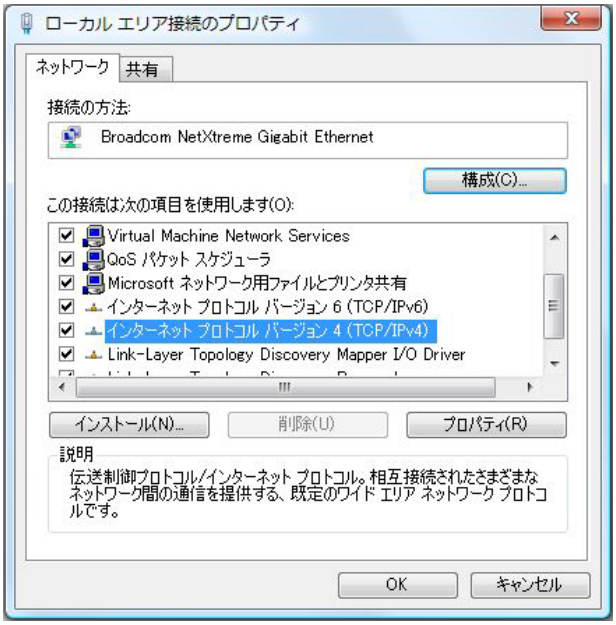
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

1 「コントロールパネル」→「ネットワークと共有センター」→「ネットワーク接続の管理」から、「ローカル接続」を開きます。

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

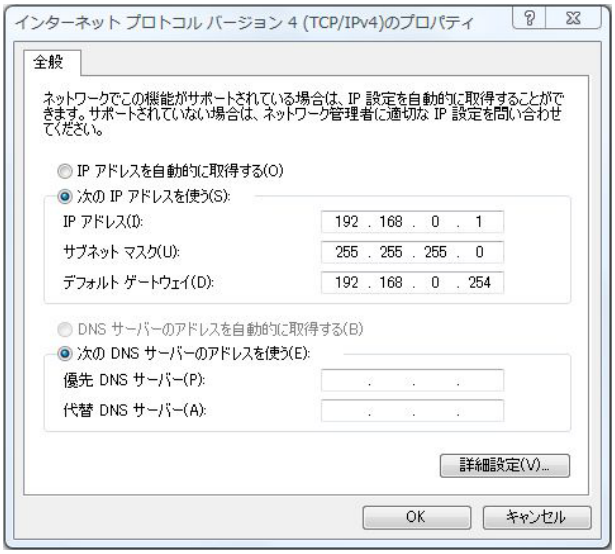


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



4 「インターネットプロトコルバージョン4(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

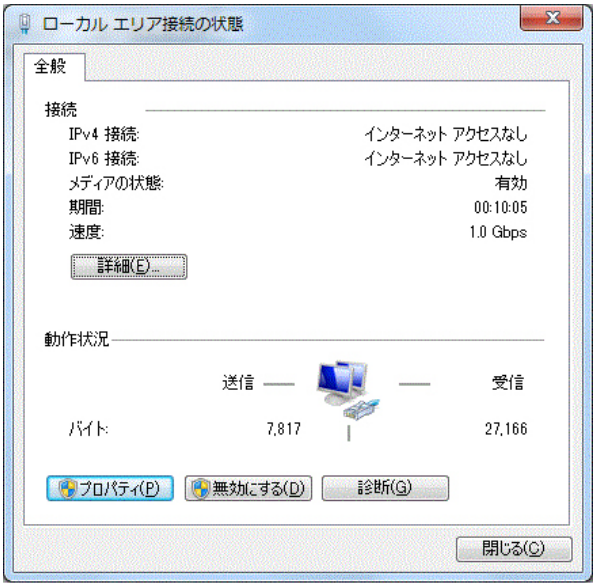
第2章 コンピューターのネットワーク設定

III. Windows 7のネットワーク設定

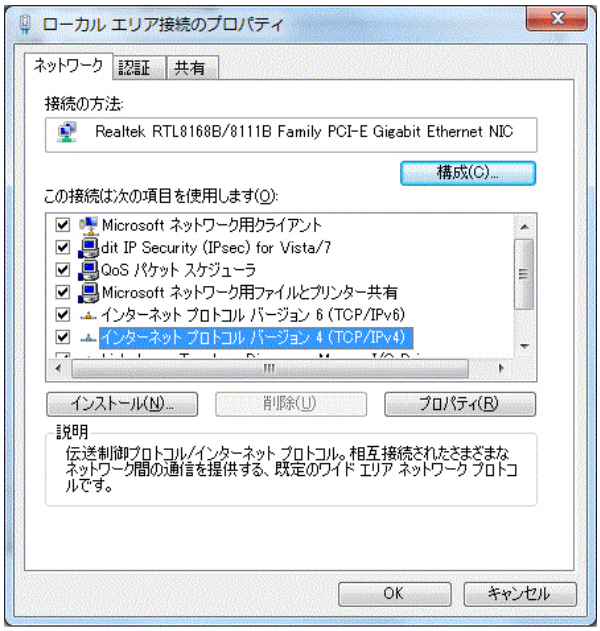
ここではWindows 7が搭載されたコンピュータのネットワーク設定について説明します。

1 「コントロールパネル」→「ネットワークとインターネット」→「ネットワークと共有センター」から、「ローカル接続」を開きます。

2 「ローカルエリア接続の状態」画面が開いたらプロパティをクリックします。

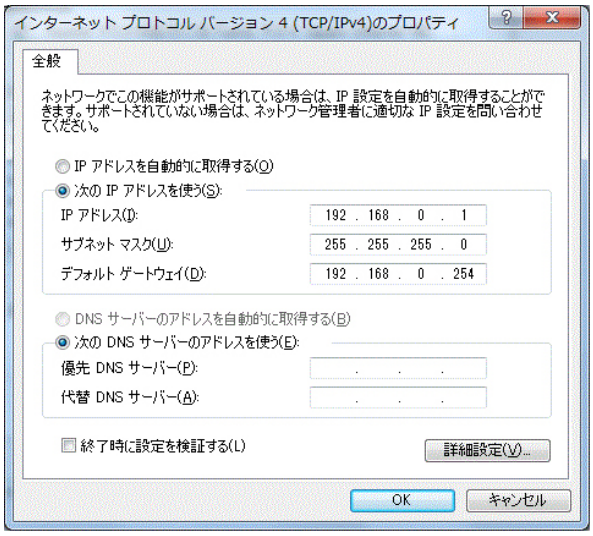


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



4 「インターネットプロトコルバージョン4(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」

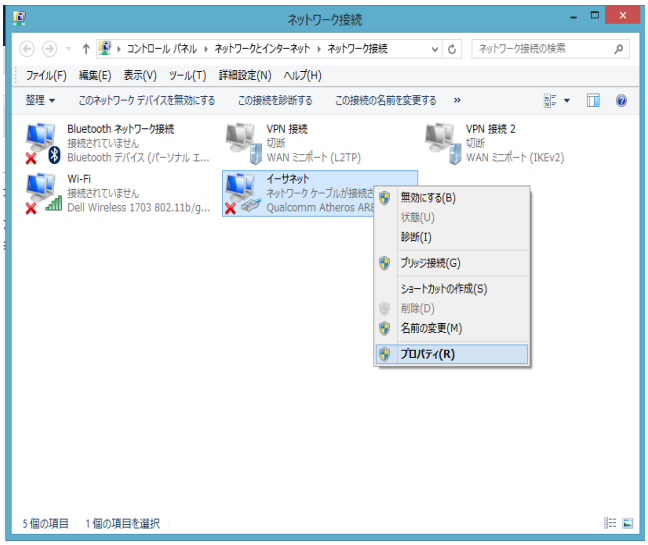


5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

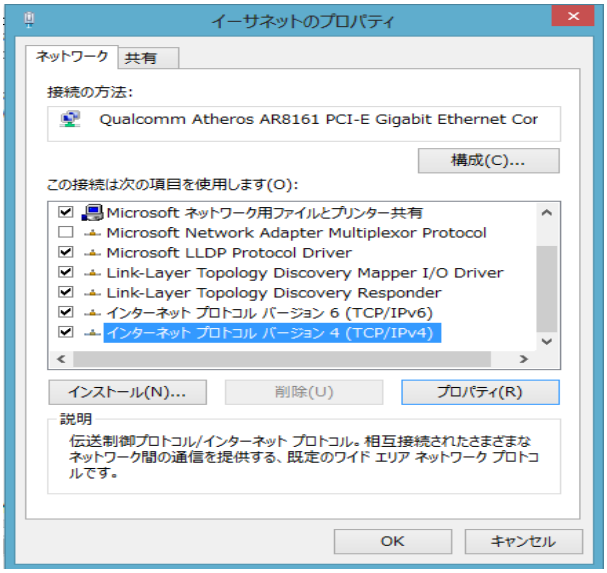
Ⅳ. Windows 8のネットワーク設定

1 「コントロールパネル」→「ネットワークとインターネット」→「ネットワークと共有センター」から、「アダプターの設定変更」を開きます。

2 「ネットワーク接続」の画面が開いたら「イーサネット」のアイコンを右クリックしてプロパティを選択します。

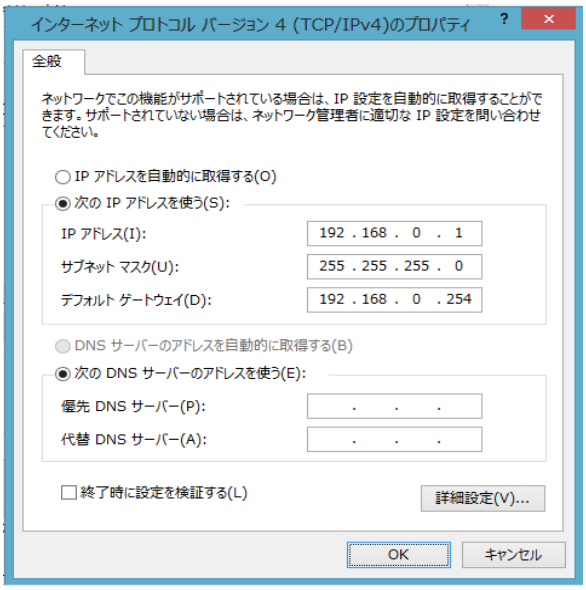


3 「イーサネットのプロパティ」の「ネットワークタブ」で、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



4 「インターネットプロトコルバージョン4(TCP/IPv4)」の画面では、「次のIPアドレスを使う」にチェックを入れて以下のように入力します。

IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
デフォルトゲートウェイ「192.168.0.254」



5 最後にOKボタンをクリックして設定完了です。

これで本装置へのログインの準備が整いました。

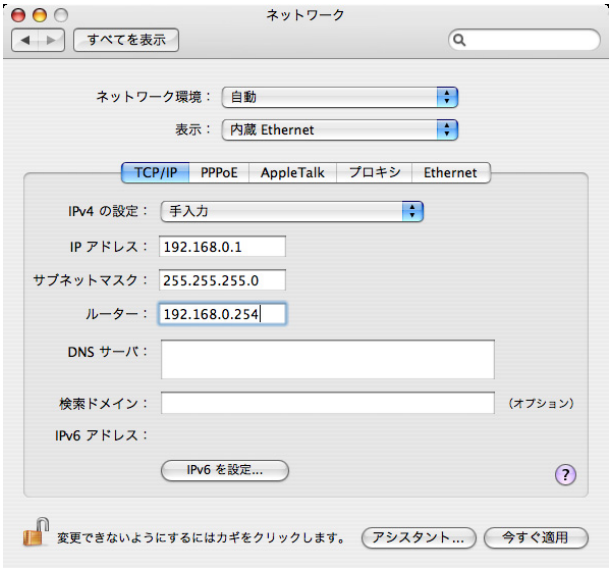
Ｖ．Mac OS Xのネットワーク設定

ここでは、Mac OS Xのネットワーク設定について説明します。

1 「システム環境設定」から「ネットワーク」を開きます。

2 ネットワーク環境を「自動」、表示を「内蔵Ethernet」、IPv4の設定を「手入力」にして、以下のように入力してください。

IPアドレス「192.168.0.1」
サブネットマスク「255.255.255.0」
ルーター「192.168.0.254」



3 ウィンドウを閉じて設定の変更を適用します。

これで、本装置へログインする準備が整いました。

第3章

設定画面へのログイン方法

Ⅰ．設定画面へのログイン方法

本装置はWebブラウザ上から設定をおこないます。この章ではWebブラウザでの設定画面へのログイン方法について説明します。

1 各種ブラウザを開きます。

2 ブラウザから設定画面にアクセスします。

本装置ではHTTP(ポート80)，HTTPS(ポート443)でのアクセスが可能です。
設定画面へのポート番号（HTTP(80)，HTTPS(443)）を変更することはできません。

HTTP(ポート80)でアクセスする場合

ブラウザのアドレス欄に以下のURLを入力してください。

http://192.168.0.254/

「192.168.0.254」は、Ether0ポートの工場出荷時のアドレスです。アドレスを変更した場合は、そのアドレスを指定してください。

HTTPS(ポート443)でアクセスする場合

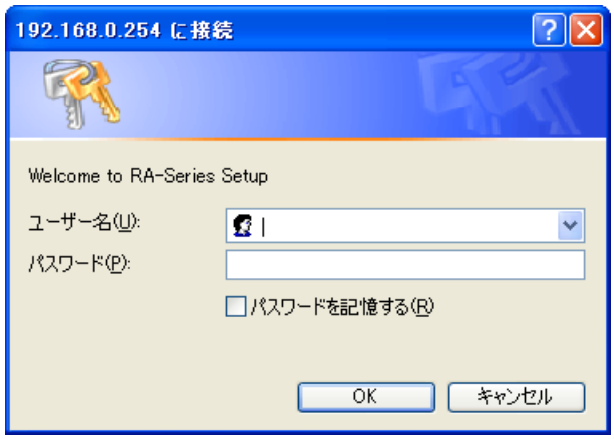
ブラウザのアドレス欄に以下のURLを入力してください。

https://192.168.0.254/

「192.168.0.254」は、Ether0ポートの工場出荷時のアドレスです。アドレスを変更した場合は、そのアドレスを指定してください。

HTTPSアクセスについては「第３章 設定画面へのアクセス ⅠⅠ.HTTPSアクセス時のCA証明書のインポート方法」を参照してください。

3 次のような認証ダイアログが表示されます。



4 ダイアログ画面にパスワードを入力します。

工場出荷設定のユーザー名とパスワードはともに「admin」です。ユーザー名・パスワードを変更している場合は、それにあわせてユーザー名・パスワードを入力します。

5 本装置の設定画面が表示されます。

設定画面はブラウザとしてInternet Explorerを使用した場合にレイアウトが最適に表示されるように作られています。他のブラウザをご利用の場合で画面レイアウトが崩れる場合は、フォントの文字サイズを小さめに指定してください。

II ． HTTPS アクセス時の CA 証明書のインポート方法

クライアント PC に CA 証明書がインポートされていない状態で本装置へ HTTPS（ポート 443）アクセスすると、「セキュリティの警告」画面が表示されます。HTTPS アクセス時の警告メッセージの対応として、CA 証明書をクライアント PC にインポートすることをお薦めします。

クライアントPCへのCA証明書のインポート手順は、OS、バージョン等により設定手順が異なります。

◆Windows XP Professional SP2
＋
Internet Explorer 6

と

◆Windows Vista
＋
Internet Explorer 7

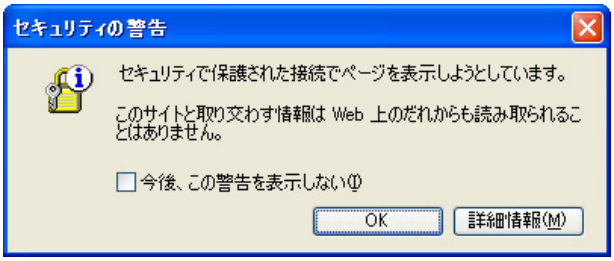
の場合の設定手順を例示します。ご使用の環境に合わせてご参照ください。

◆Windows XP Professional SP2 ＋ Internet Explorer 6

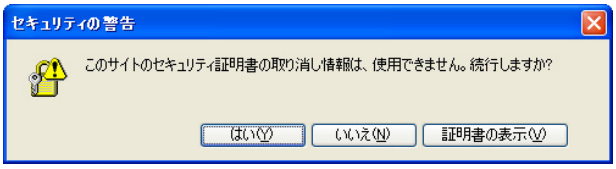
Windows XP Professional SP2＋Internet Explorer 6を使用したクライアントPCにおけるCA証明書のインポート手順です。

CA証明書がインポートされていない状態でのHTTPSアクセス

CA 証明書がクライアント PC にインポートされていない状態で本装置へHTTPSアクセスするとインターネットオプションの設定によって、以下のような警告画面が現れます。

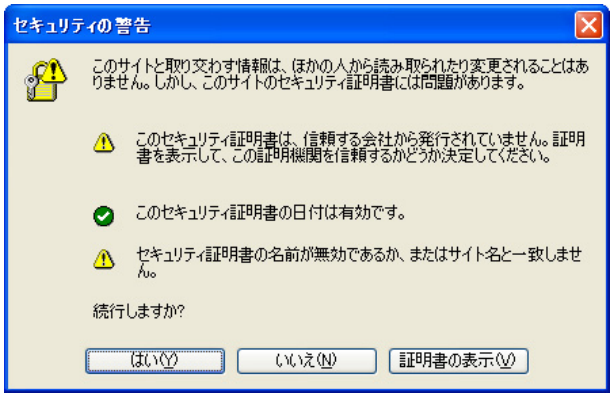


または、



※ インターネットオプション等の設定によってはこれらの警告画面が表示されないこともあります。

警告画面の「OK」（または「はい(Y)」）を選択すると、さらに次のような警告画面が現れます。



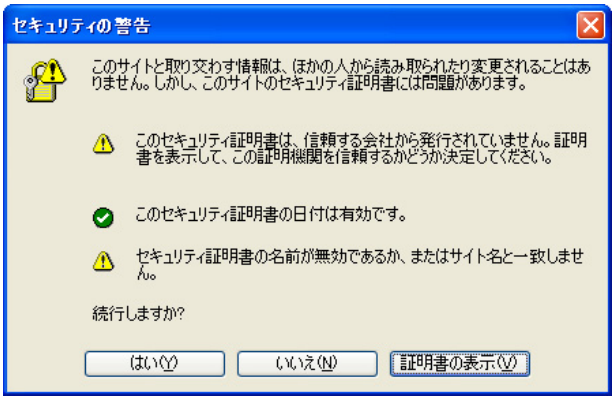
「はい(Y)」をクリックするとログイン用の認証ダイアログが現れますので、HTTP アクセスと同様にユーザー名とパスワードを入力してください。

II ． HTTPS アクセス時の CA 証明書のインポート方法

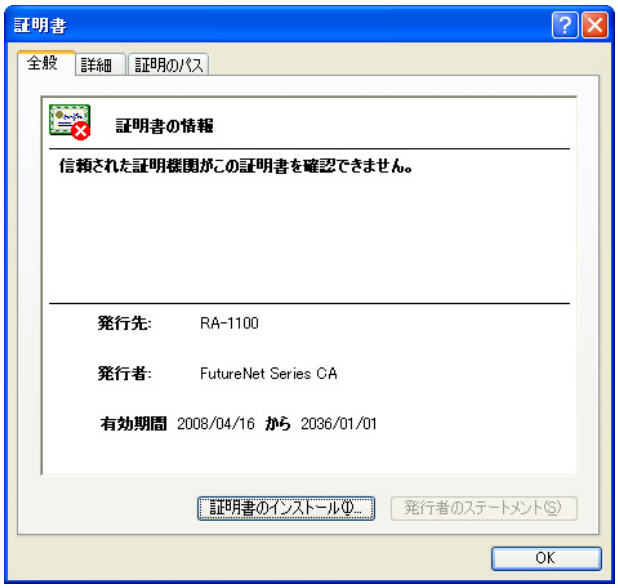
CA 証明書のインポート

あらかじめ取得しておいたCA証明書を実行すると証明書のインポートウィザードが開始されます。

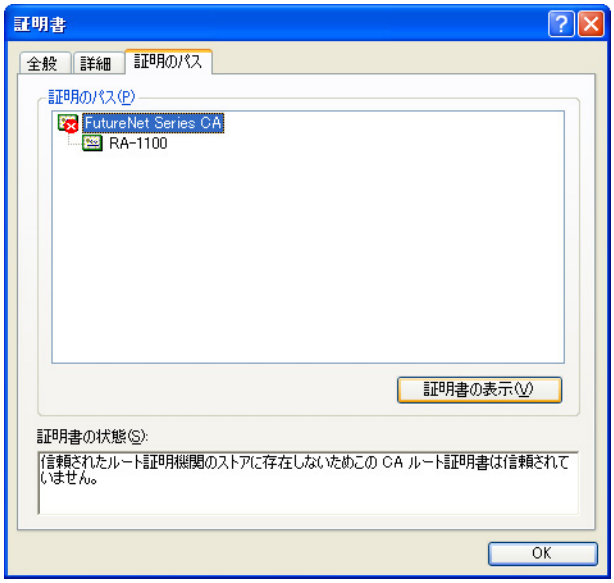
CA 証明書を取得しておくのが難しい場合には、「セキュリティの警告」画面の「証明書の表示(V)」をクリックしてください。



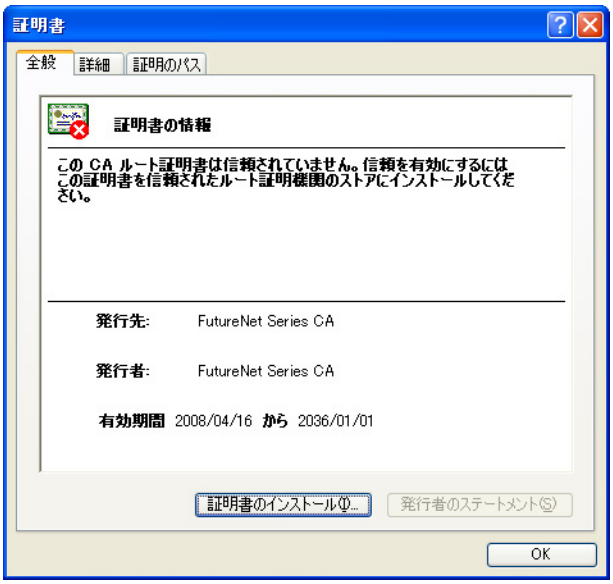
以下の画面が表示されます。



「証明のパス」タブを開き、「証明のパス(P)」に表示されている最上位証明書を選択して「証明書の表示(V)」をクリックします。

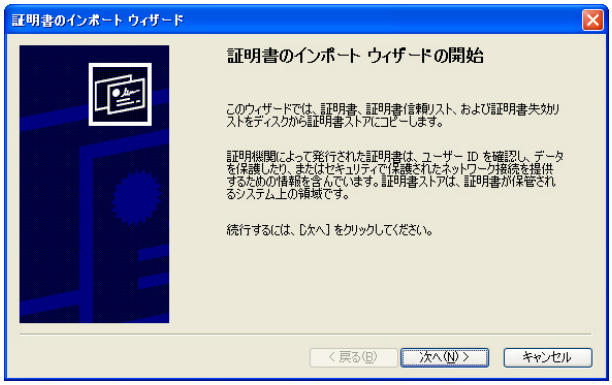


「全般」タブにある「証明書のインストール(I)」を開くと、CA証明書のインポートを開始することができます。

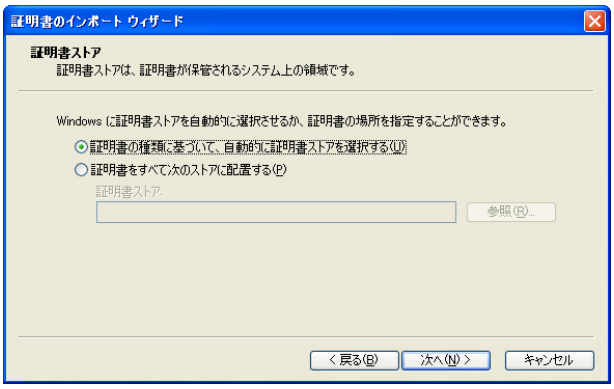


II ． HTTPS アクセス時の CA 証明書のインポート方法

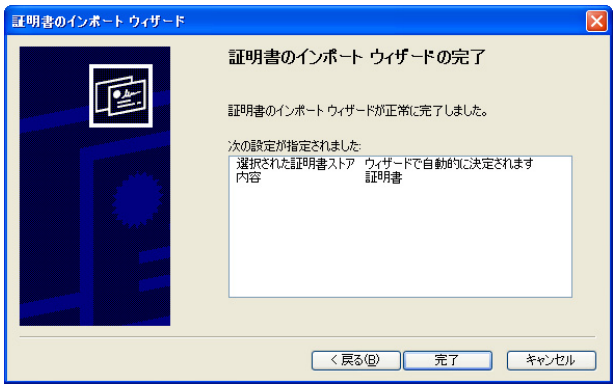
「証明書のインポートウィザード」が開始されたら「次へ(N)」をクリックしてください。



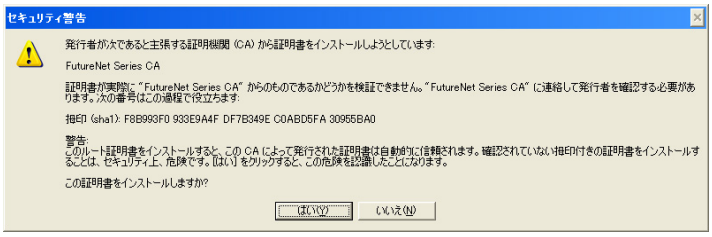
「証明書ストア」での証明書が保管される場所は「証明書の種類に基づいて、自動的に証明書ストアを選択する(U)」のままで次へ進みます。



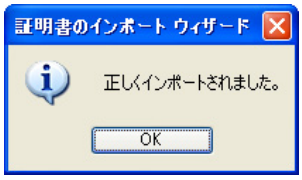
「完了」をクリックします。



ルート証明書のインストール確認メッセージが表示されますので、証明書の拇印が正しいことを確認し「はい(Y)」を選択してください。

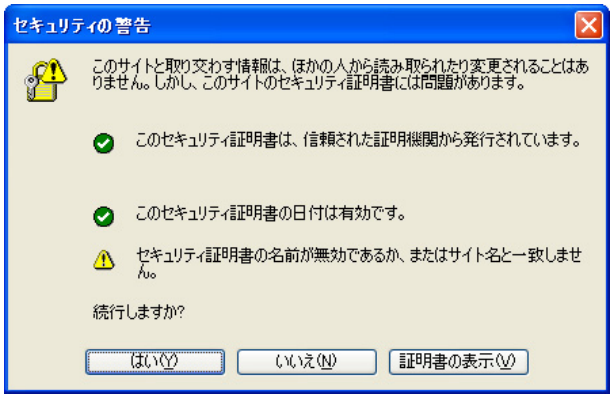


証明書のインポートが完了します。



CA証明書がインポートされた状態でのHTTPSアクセス

CA 証明書をクライアント PC にインポートした後に本装置へ HTTPS アクセスすると、以下のような警告画面が現れます。



これは、ホスト名(または IP アドレス)と証明書の CommonName が一致していないために発生します。

ログインするには「はい(Y)」を選択すると認証ダイアログが表示されます。

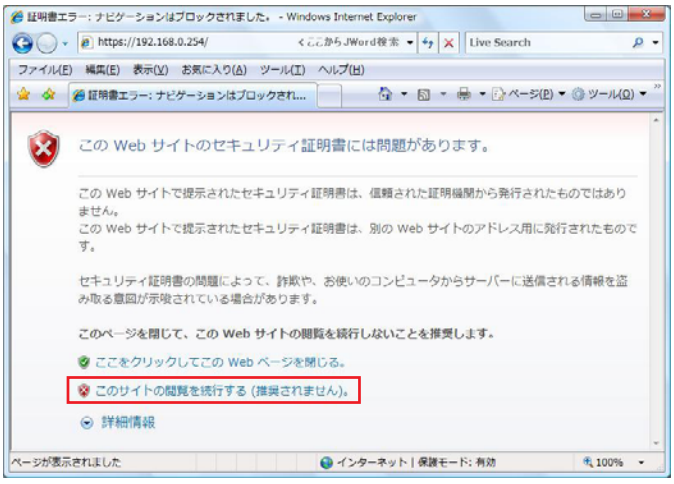
II ． HTTPS アクセス時の CA 証明書のインポート方法

◆Windows Vista＋Internet Explorer 7

Windows Vista＋Internet Explorer 7を使用したクライアントPCにおけるCA証明書のインポート手順です。

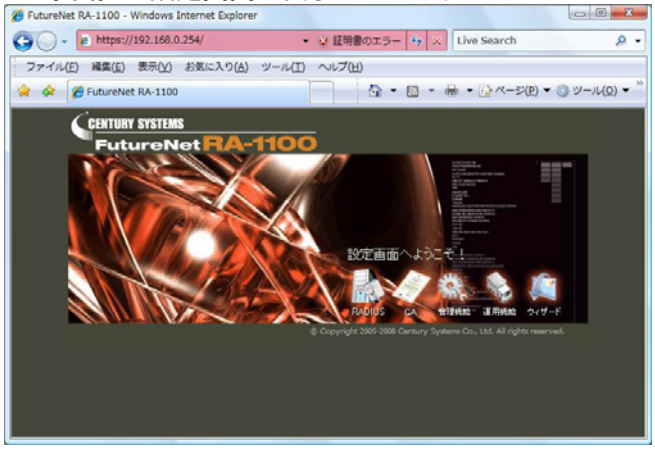
CA証明書がインポートされていない状態でのHTTPSアクセス

CA証明書がクライアントPCにインポートされていない状態で本装置へHTTPSアクセスすると以下のような画面が表示されます。



「このサイトの閲覧を続行する（推奨されません）。」をクリックするとログイン用の認証ダイアログが現れますので、ユーザー名とパスワードを入力してください。

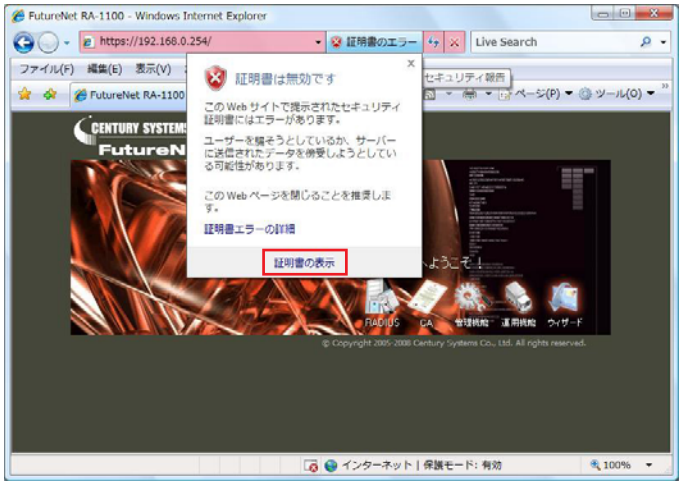
本装置の設定画面が表示されます。



CA証明書のインポート

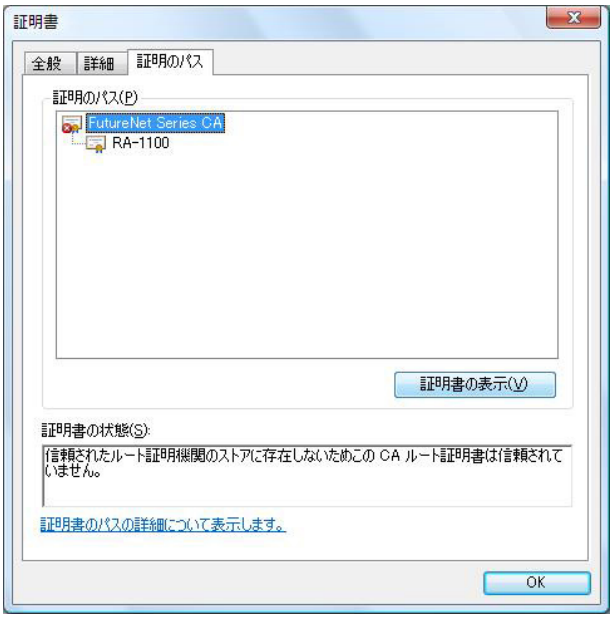
あらかじめ取得しておいたCA証明書を実行すると証明書のインポートウィザードが開始されます。

CA証明書を取得しておくのが難しい場合には、アドレスバーの隣に表示されている「証明書のエラー」をクリックして、最下部の「証明書の表示」を開きます。



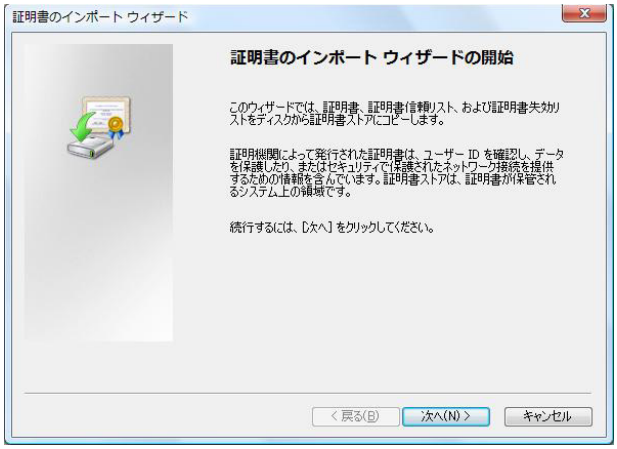
II ． HTTPS アクセス時の CA 証明書のインポート方法

「証明のパス」タブを開き、「証明のパス(P)」に表示されている最上位証明書を選択して「証明書の表示(V)」をクリックします。

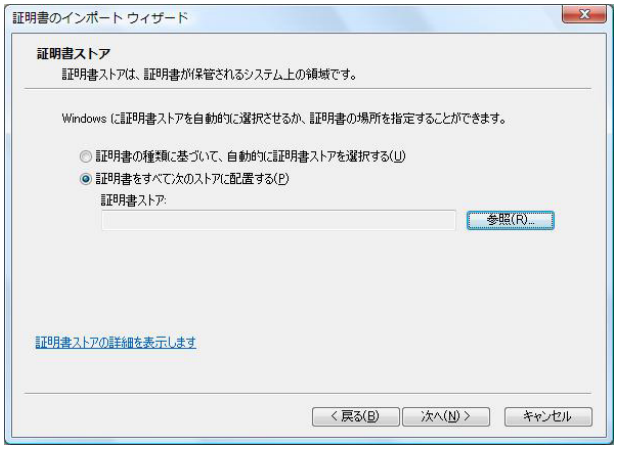


「全般」タブにある「証明書のインストール(I)」を開くと、CA証明書のインポートを開始することができます。

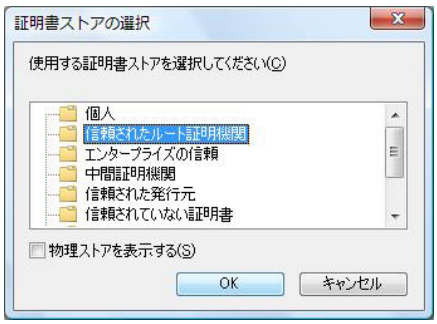
「証明書インポートウィザード」が開始されたら「次へ(N)」をクリックしてください。



「証明書ストア」で証明書が保管される場所を指定することができます。
「証明書をすべて次のストアに配置する(P)」を選択して、「参照(R)」ボタンをクリックします。

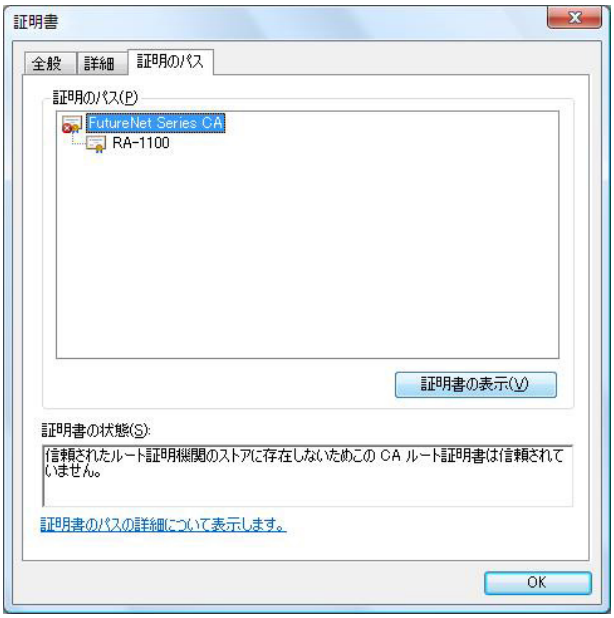


証明書ストアは「信頼されたルート証明機関」としてください。



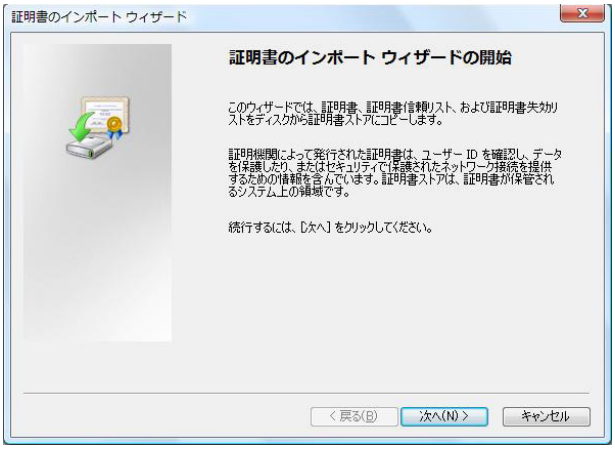
II ． HTTPS アクセス時の CA 証明書のインポート方法

「証明のパス」タブを開き、「証明のパス(P)」に表示されている最上位証明書を選択して「証明書の表示(V)」をクリックします。

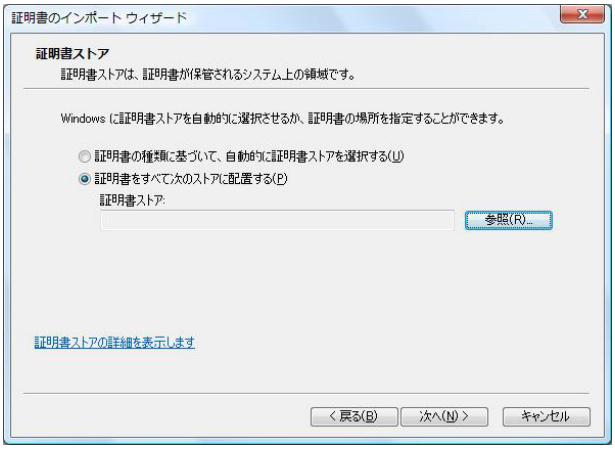


「全般」タブにある「証明書のインストール(I)」を開くと、CA証明書のインポートを開始することができます。

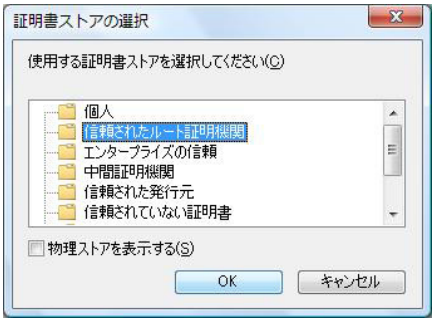
「証明書インポートウィザード」が開始されたら「次へ(N)」をクリックしてください。



「証明書ストア」で証明書が保管される場所を指定することができます。
「証明書をすべて次のストアに配置する(P)」を選択して、「参照(R)」ボタンをクリックします。



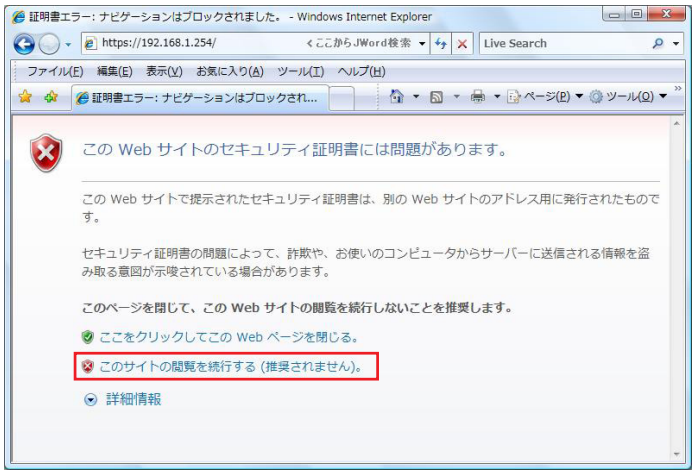
証明書ストアは「信頼されたルート証明機関」としてください。



II ． HTTPS アクセス時の CA 証明書のインポート方法

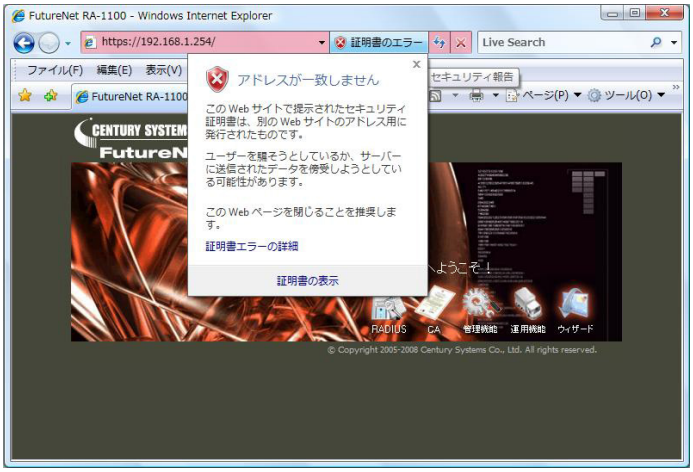
CA 証明書がインポートされた状態での HTTPS アクセス

CA 証明書をクライアント PC にインポートした後にも本装置へ HTTPS アクセスすると、以下のような警告画面が現れます。



「このサイトの閲覧を続行する（推奨されません）。」をクリックしてログインしてください。

CA証明書をインポート後でも、HTTPSアクセスでログインすると、アドレスバーの隣の「証明書エラー」が表示されますが、これは、ホスト名(または IP アドレス)と証明書の CommonName が一致していないために発生します。



第4章

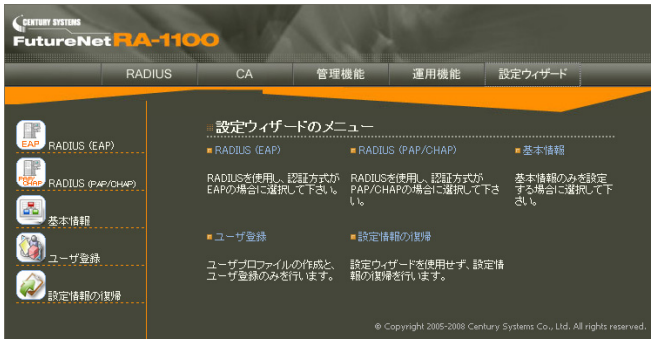
設定ウィザードによる設定

第４章 設定ウィザードによる設定

Ｉ．設定を始める前に

設定ウィザードを使うと、画面に表示される順番に設定をおこなうことで、本装置に必要な設定を一通りおこなうことができます。初めて本装置にログインし、設定をおこなう場合には、設定ウィザードによる設定が適しています。
ただし、設定ウィザードを用いて親子連携機能の設定を行うことは出来ません。

ウィザードのアイコンをクリックすると次の画面が表示されます。



◆各ウィザードの設定内容

設定ウィザードは目的に応じて以下の５つの中から一つを選んで実行するようにします。

- RADIUS(EAP)
  本装置を EAP 認証で使う場合に最適のウィザードです。本装置のほぼ全ての設定項目を設定することができます。

- RADIUS(PAP/CHAP)
  本装置を PAP/CHAP 認証で使う場合に最適のウィザードです。RADIUS サーバの設定、ユーザ登録等をおこないます。証明書関連の設定は不必要なためおこないません。

- 基本情報
  本装置の IP アドレスの設定など、ターゲットのネットワークに設置するための最低限の設定のみをおこないます。RADIUS サーバの設定やユーザ登録はおこないません。RADIUS の設定は後回しにして、装置の設置のみをおこないたい場合に適しています。

- ユーザ登録
  ネットワーク設定や、RADIUS サーバの設定が既に終わっている状態の時に、ユーザ情報の追加だけをおこないたい時に使用します。

- 設定情報の復帰
  別途用意した設定ファイルを読み込むだけのウィザードです。装置の設定を初期化した後、以前バックアップしてあった設定内容を読み込む時などに使います。

◆設定ウィザード画面の説明

設定ウィザードを選択すると、以降以下のような画面が表示されます。

左下のフレームには必要な設定項目がリスト表示されます。現在設定をおこなっている項目が青色で、未設定の項目は灰色で、既に設定が終わった項目は白色で表示されます。

右下のフレームが設定情報を入力する画面になります。各設定項目に移動した直後にはその項目の現在の設定内容を表示する画面（以降表示画面と呼びます）が表示されます。表示画面には設定項目を前後に移動するための「次へ」ボタンと「戻る」ボタンがあります。

Ⅰ．設定を始める前に

設定を追加変更する場合には画面に応じて「設定・編集」ボタン、または「新規追加」ボタン、「編集」ボタンなどを押します。すると入力画面が表示されます。

設定内容を入力後「設定」ボタンまたは「実行」ボタンを押すと表示画面にもどります。設定された内容は直ちに保存され装置に反映されます。

次の設定項目へ進む場合には表示画面から「次へ」ボタンを押します。以前の設定をやり直す場合には「戻る」ボタンを押して戻ることができます。

次節ではRADIUS(EAP)のウィザードを例に各設定項目毎の設定内容を説明します。
RADIUS(PAP/CHAP)、基本情報、ユーザ登録の各ウィザードについては、次ページの表を参照して、該当する項目の説明をご覧ください。

設定を始める前に本装置の IP アドレスや、RADIUS クライアントの情報、設定するユーザ情報など、設定に必要なデータを事前に準備した上で設定を開始することをお勧めします。

Ⅰ．設定を始める前に

	RADIUS (EAP)	RADIUS (PAP/CHAP)	基本設定	ユーザ登録
1. 管理者	○	○	○	
2. ネットワーク基本情報	○	○	○	
3. 内蔵時計	○	○	○	
4. ログ	○	○	○	
5. スタティックルート	○	○	○	
6. DNS	○	○	○	
7. NTP	○	○	○	
8. SNMP	○	○	○	
9. CA-基本情報	○			
10. CA-RADIUSサーバ証明書	○			
11. CA-HTTPSサーバ証明書	○			
12. CA-LDAPクライアント証明書	○			
13. CA-LDAPサーバ証明書	○			
14. 管理画面へのアクセス	○	○	○	
15. RADIUS-基本情報	○	○		
16. RADIUS-二重化	○	○		
17. RADIUS-ログ	○	○		
18. RADIUS-アドレスプール	○	○		
19. RADIUS-クライアント	○	○		
20. RADIUS-アトリビュート	○	○		
21. RADIUS-ActiveDirectory	○			
22. RADISU-LDAP	○			
23. RADIUS-ユーザ基本情報	○	○		○
24. RADIUS-認証アトリビュート	○	○		○
25. RADIUS-応答アトリビュート	○	○		○
26. RADIUS-グループID	○	○		○
27. RADIUS-ユーザ証明書	○			○
28. RADIUS-ユーザプロファイル	○	○		○
29. RADIUS-ユーザ作成	○	○		○
30. RADIUS-ADユーザ	○			
31. RADIUS-LDAPユーザ	○			
32. ユーザ管理者	○	○	○	
33. フィルタ	○	○	○	
34. RADIUS起動	○	○		
35. 設定の保存	○	○	○	○
36. 完了	○	○	○	○

表． 各設定ウィザード毎の設定内容一覧

Ⅱ．設定内容の詳細

1. 管理者

本装置ではログインするユーザの権限によって「本装置管理者」、「ユーザ管理者」、「ユーザ」の３種類のアカウントが用意されています。ここでは最も権限の強い本装置管理者のログインIDとパスワードを設定します。装置のセキュリティ確保のために推測されにくいパスワードを設定してください。
工場出荷設定のユーザー名とパスワードはともに「admin」です。

表示画面では本装置管理者のログインIDが表示されています。

設定を変更する場合は「編集」ボタンを押すと、次の入力画面が表示されます。
新しいログインIDとパスワードを入力してください。

■本装置管理者変更

○ログインID
使用可能な文字は英数字および以下の記号と空白文字になります。

```
!"#$%&'()*+-./<=>?@[]^_`{|}~
```

○パスワード
使用可能な文字は、ログインID の入力可能文字と以下の記号になります。

```
,:;\
```

「設定」ボタンをクリックして設定完了です。

次回のログインからは、新しく設定したユーザー名とパスワードを使ってログインしてください。

2. ネットワーク基本情報

本装置の IP アドレスおよびデフォルトゲートウェイの設定をおこないます。

（RA-730 の設定画面です。）

Ether0，Ether1，Ether2
(※ RA-1200 は、Ether0 と Ether1 のみです。)
設定を変更する場合は、変更したいインタフェース欄の「編集」ボタンを押します。
次の入力画面が表示されます。

■基本情報

（RA-730 の設定画面です。）

○ IP アドレス
Ether ポートの IP アドレスとネットマスクを入力します。
ネットマスクは IP アドレスの後、’ / ’(スラッシュ)に続けてビット数表記で入力します。例えば、IP アドレスが 192.168.1.10 で、ネットマスクがドット区切り表記で 255.255.255.0 であれば以下のように入力します。
　入力例）192.168.1.10/24

複数の Ethernet ポートに同一ネットワークに属するアドレスを 設定しないで下さい。正常に動作しないことがあります。

○ MTU
「Path-MTU-Black-HOLE」現象が発生した場合等は、ここの値を変更することで回避できます。
通常は初期設定の 1500Bytes のままで利用してください。

○通信モード
Ether ポートの通信速度・方式を選択します。
工場出荷設定では「自動」(オートネゴシエーション)となっていますが、必要に応じて通信速度・方式を選択してください。

デフォルトゲートウェイ
デフォルトゲートウェイ欄の「編集」ボタンを押すと次の入力画面が表示されます。

■基本情報

○デフォルトゲートウェイ
本装置のデフォルトゲートウェイとなる IP アドレスを入力してください。

各項目に入力後、「設定」ボタンをクリックして設定完了です。

本装置のインタフェースのアドレスを変更した後は、設定画面にアクセスしているコンピュータの IP 設定もそれにあわせて変更し、変更した IP アドレスの設定画面に再ログインしてください。

3. 内蔵時計

本装置の時刻を合わせます。

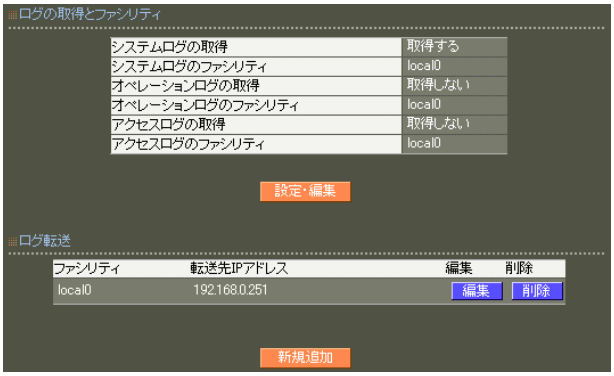
時刻を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■内蔵時計
24時間単位で時刻を設定してください。

「実行」ボタンをクリックして設定完了です。

4. ログ

ログに関する設定をします。
また、取得した各ログの転送先を設定します。



■ログの取得とファシリティ

現在の設定内容が表示されています。
設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ログの取得とファシリティ変更

○システムログの取得
システムログについて記録に残すかどうかを設定します。

○システムログのファシリティ
システムログを「取得する」にした場合、システムログが出力されるファシリティを指定します。
プルダウンから選択してください。

○オペレーションログの取得
オペレーションログについて記録に残すかどうかを設定します。

○オペレーションログのファシリティ
オペレーションログを「取得する」にした場合、オペレーションログが出力されるファシリティを指定します。
プルダウンから選択してください。

○アクセスログの取得
アクセスログについて記録に残すかどうかを設定します。

○アクセスログのファシリティ
アクセスログを「取得する」にした場合、アクセスログが出力されるファシリティを指定します。
プルダウンから選択してください。

各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

■ログ転送

各ファシリティ毎のログの転送先が一覧表示されています。
この画面で設定をおこなうシステムログ・オペレーションログ・アクセスログに加え、後で設定をおこなう認証ログ、アカウンティングログも転送先の指定に従って転送されます。

「新規追加」をクリックすると入力画面が表示されます。

■ログ転送新規追加

○ファシリティ

転送したいログのファシリティを指定します。
プルダウンから選択してください。

○転送先 IP アドレス

ログを転送するサーバを指定します。
指定したマシン上で syslog サーバを動かす必要があります。

各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

設定可能な転送先 IP アドレスの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除

ログ転送一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

本装置に記録できるログの数には上限があります（「付録 A 最大数一覧」を参照してください）。継続的にログを取得される場合は外部の syslog サーバにログを送信するようにしてください。

5. スタティックルート

本装置のスタティックルートの設定をおこないます。

「新規追加」をクリックすると入力画面が表示されます。

■スタティックルート新規追加

○ IP アドレス
あて先ホストまたはネットワークの IP アドレスを入力します。
あて先の範囲をネットマスクで指定します。
ネットマスクは IP アドレスの後、’ / ’(スラッシュ) に続けてビット数表記で入力します。例えば、IP アドレスが 192.168.1.0 で、ネットマスクがドット区切り表記で255.255.255.0の範囲 であれば以下のように入力します。

入力例）192.168.1.0/24

ホストを指定する場合は ’ /32 ’ は付けずに IP アドレスで指定します。

入力例）192.168.1.1

○ゲートウェイ
IPアドレス欄で指定したアドレスへ送信するパケットを中継する、ルータのアドレスを入力します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
設定はすぐに反映されます。

設定可能なスタティックルートの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
スタティックルート一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

6.DNS

本装置が使用するDNSの設定をおこないます。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ DNS

○プライマリサーバ
プライマリDNSサーバのIPアドレスを入力します。

○セカンダリサーバ
セカンダリDNSサーバのIPアドレスを入力します。

各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

7.NTP

本装置は、NTPクライアント/サーバ機能を持っています。インターネットを使った時刻同期の手法の一つであるNTP(Network Time Protocol)を用いてNTPサーバと通信をおこない、時刻を同期させることができます。

■起動・停止
現在NTPサーバが停止している場合には、「停止中」と表示されます。「起動」ボタンをクリックする事でNTPサーバが起動します。

NTPサーバが起動している場合には、「動作中」と表示されます。
「停止」ボタンをクリックする事でNTPサーバは停止します。また、「再起動」ボタンをクリックするとNTPプロセスが再起動します。

■NTPサーバ
設定されているNTPサーバが表示されています。設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ NTP

○プライマリサーバ
プライマリNTPサーバのIPアドレスもしくはFQDNを入力します。

○セカンダリサーバ
セカンダリNTPサーバのIPアドレスもしくはFQDNを入力します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

保存された設定内容を反映させるには、NTPサーバの再起動が必要になります。
「再起動」ボタンを押してください。

基準NTPサーバについて
基準となるNTPサーバには以下のようなものがあります。

- ntp1.jst.mfeed.ad.jp
- ntp2.jst.mfeed.ad.jp
- ntp3.jst.mfeed.ad.jp

8.SNMP

SNMP エージェントを起動すると、SNMP マネージャから本装置の MIB-II（RFC1213)の情報を取得することができます。

■起動・停止
現在 SNMP が停止している場合には、「停止中」と表示されます。「起動」ボタンをクリックする事で SNMP が起動します。

SNMP が起動している場合には、「動作中」と表示されます。「停止」ボタンをクリックする事で SNMP サーバは停止します。また、「再起動」ボタンをクリックすると SNMP プロセスが再起動します。

■ SNMP サーバ
管理者が設定変更できる項目について、現在の設定内容が表示されています。
設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ SNMP

○コミュニティ名
任意のコミュニティ名を指定します。
ご使用の SNMP マネージャの設定に合わせて入力してください。

○本装置の名称
本装置の管理上の名前を入力します。通常 FQDN などを指定します。

○本装置の説明
本装置についての説明を入力します。

○本装置の設置場所
本装置の物理的な設置場所を指定します。

○本装置の管理者
本装置管理者への連絡先などを指定します。

○ Trap 送信先 1 ～ 5
Trap の送信先（SNMP マネージャ）の IP アドレスを設定します。
デフォルト値はありません。
未設定の場合は trap の送信はしません。
最大 5 個まで設定可能です。

○ CPU 使用率閾値
CPU 使用率の閾値を設定します。
単位は %で、有効な値は 10 以上 100 未満の整数となります。
デフォルト値はありません。
設定されない場合は、対応する trap は送信されません。
CPU 使用率は、設定内容及びご利用状況によって変わります。
運用中の実際の使用率を元に、適当と思われる閾値を設定してください。

○メモリ空き容量閾値
メモリ 空き容量の閾値を設定します。
単位は kB で、有効な値は 1 以上の整数となります。
デフォルト値はありません。
設定されない場合は、対応する trap は送信されません。
メモリ空き容量については別項(後述)を参照して下さい。

メモリ空き容量は設定及びご利用状況によって変わります。
運用中の実際の空き容量を元に、適当と思われる閾値を 設定してください。

各項目に使用可能な文字は以下となります。
・コミュニティ名、本装置の説明、本装置の設置場所
　0-9，a-z，A-Z，-，_
・本装置の名称
　0-9，a-z，A-Z，-，_，.
・本装置の管理者
　0-9，a-z，A-Z，-，_，@，<，>，.

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

保存された設定内容を反映させるには、SNMP サーバの再起動が必要になります。
「再起動」ボタンを押してください。

メモリ空き容量
RA では、データの読み出し / 書き込み時にメモリをキャッシュという形で確保します。
一度キャッシュとして確保したデータは、メモリを介して処理が行われるため高速に動作します。
新たなデータの読み出し / 書き込み要求によりメモリ領域が必要とならない限り、キャッシュは解放されません。

(※ 1.8.12 以降)
メモリ空き容量(csRASystemMemoryFree)には、このキャッシュが含まれます。
(※ 1.8.11 以前)
メモリ空き容量(csRASystemMemoryFree)には、このキャッシュは含まれません。
したがって、連続して運用を続けると、メモリ空き容量(csRASystemMemoryFree)は逓減します。

SNMP trap

ユーザが設定したSNMPマネージャにSNMP trapを送信します。
送信されるtrapは以下の通りです。

・SNMPサービスを起動した時

Cold Start trapを送信します。

・CPU使用率がユーザ定義の閾値を超えた時
・CPU使用率がユーザ定義の閾値以下になった時

CPU使用率を一定時間毎(1秒)に測定します。
前回の測定値が閾値以下で、今回の測定値が閾値より大きい場合にtrapを送信します。
測定値が閾値より大きくなったことがあり、その後の測定値が一定回数(10回)だけ連続して閾値以下の場合にtrapを送信します。
SNMPサービス起動直後に閾値より大きい場合はtrapを送信します。
閾値以下の場合は送信しません。

・メモリ空き容量がユーザが定義した閾値より小さくなった時
・メモリ空き容量がユーザが定義した閾値以上になった時

メモリ空き容量を一定時間毎(1秒)に測定します。
前回の測定値が閾値以上で、今回の測定値が閾値より小さい場合にtrapを送信します。
測定値が閾値より小さくなったことがあり、その後の測定値が一定回数(10回)だけ連続して閾値以上の場合にtrapを送信します。
SNMPサービス起動直後に閾値より小さい場合はtrapを送信します。
閾値以上の場合は送信しません。

・Ethernetインタフェースがlink downした時
・Ethernetインタフェースがlink upした時

Ethernetインタフェースのlink up/down に応じてtrapを送信します。
SNMPサービス起動直後にlink down ならばtrapを送信します。
link up ならば送信しません。

・電源の状態が変わった時 （※RA-1200のみ）

電源ユニットへの通電がなくなったり、電源ユニット自体が故障したりなど、注意が必要な状態になった場合に trap を送信します。
また、注意が必要な状態から正常な状態に戻った場合にもtrap を送信します。

・RAIDの状態が変わった時 （※RA-1200のみ）

RAIDで障害が発生した場合、リビルドが始まった場合、リビルドが終了した場合にtrap を送信します。

CPU やメモリ、電源、RAID の状況は、GetRequest などで取得できます。

例:

```
$ snmpwalk -v2c -c public 192.168.0.254 centurysys
   CS-RA-PRODUCT-MIB::csRASystemCPUUser.0 = INTEGER: 0
   CS-RA-PRODUCT-MIB::csRASystemCPUSystem.0 = INTEGER: 1
   CS-RA-PRODUCT-MIB::csRASystemCPUIdle.0 = INTEGER: 99
   CS-RA-PRODUCT-MIB::csRASystemMemoryTotal.0 = INTEGER: 4123252
   CS-RA-PRODUCT-MIB::csRASystemMemoryFree.0 = INTEGER: 4009080
   CS-RA-PRODUCT-MIB::csRAPowerStatus.0 = INTEGER: ok(1)
   CS-RA-PRODUCT-MIB::csRARaidLdLevel.1 = INTEGER: raid1(2)
   CS-RA-PRODUCT-MIB::csRARaidLdStatus.1 = INTEGER: ok(1)
```

9.CA - 基本情報

本装置のCAの設定をおこないます。

「新規追加」をクリックすると次の入力画面が表示されます。

■CA

○バージョン

証明書のバージョンを示します。V3固定です。

○鍵長

RSAの鍵の長さを選択します。

・～ ver1.11.0

鍵の長さは「512」、「1024」、「2048」のいずれかを選択することができます。

・ver1.12.0 ～

鍵の長さは「1024」、「2048」のいずれかを選択することができます。

「512」、「1024」は十分安全とは言えません。

「2048」を推奨します。

○Signature Algorithm

署名アルゴリズムを選択します。

・ver1.8.4以前

「SHA-1」または「MD5」を選択することができます。

・ver1.8.5 ～ ver1.11.0

「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれかを選択することができます。

・ver1.12.0 ～

「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれかを選択することができます。

「SHA-1」、「MD5」は十分安全とは言えません。

「SHA-256」を推奨します。

○Subject

Subjectには以下の項目があります。

・Common Name

CA Nameとして、認証局名称を設定します。

・email

認証局管理者のメールアドレス

・Organizational Unit

一般には部署名を設定します。

・Organization

一般には企業名、組織名を設定します。

・Locality

市町村名を設定します。

・State or Province

都道府県名を設定します。

・Country

国名を設定します。

日本国内の場合は、「JP」とします。

○有効期間

証明書有効期間を日数（終了日時）で設定します。

■パスフレーズ

○パスフレーズ

パスフレーズは5文字以上30文字以下で入力してください。

■失効リスト更新間隔
○失効リスト更新間隔
失効リストの更新間隔日数を設定します。
0-4000日の間で指定します。

・ver1.9.2以降
0 を指定した場合、次の更新（Next Update）は、CA 証明書の有効期間の終了日時になります。

※この設定では、以下の項目が必須の設定項目になります。
- ○バージョン(固定)
- ○鍵長
- ○Signature Algorithm
- ○subject
  - ・Common Name
- ○有効期間
- ○パスフレーズ
- ○失効リスト更新間隔

また、各項目に使用可能な文字は以下となります。
- ・E-mailAddress
  0-9，a-z，A-Z，-.@_
- ・Common Name
  制御コードを除く任意の半角文字
- ・Organizational Unit/Organization/Locality/ State or Province/
  ver1.8.4以前: 0-9，a-z，A-Z，-_
  ver1.8.5以降: 0-9，a-z，A-Z，-_',.SPACE
- ・Country
  A-Z

各項目に入力後、「設定」ボタンを押してCA証明書を発行します。

CAの設定を一度おこなうと、以降、「CA/CRL」メニューを選択した場合、次の画面が表示されるようになります。

この画面では以下の操作をおこなえます。

■CA証明書
○CA/失効リストの表示
画面上部にある「CA」/「失効リスト」の選択ボタンを選んで「表示」ボタンを押すと、CAの内容または失効リストの内容が表示されます。

○CAの削除
「削除」ボタンを押すと本装置で設定したCA証明書，CRL，各証明書を全て削除します。

■CA証明書の取得
CA証明書欄で「取り出し」ボタンをクリックすることによりCA証明書を取り出すことができます。この際、取り出す形式を PEM または DER から選択することができます。

■失効リストの取得
失効リストの取得欄で「取り出し」ボタンをクリックすることによりCRLを取り出すことができます。
この際、取り出す形式を PEM または DER から選択することができます。

■失効リストの更新
失効リストの更新欄で「更新」ボタンをクリックするとCRLが最新のものに置き換えられます。

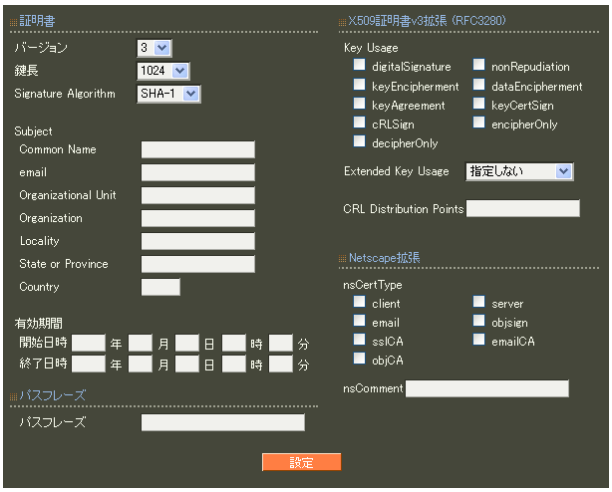
・ver1.10.0 以降
失効リスト更新間隔を、0-4000日の間で指定することができます。
デフォルト値は、CA証明書を発行した時に指定した値です。
0を指定した場合、次の更新（Next Update）は、CA証明書の有効期間の終了日時になります。

失効リストが、失効リストの更新間隔で決められた日時よりも古い場合には、証明書自体が有効であっても証明書の認証は拒否されます。
失効リスト更新間隔で決められた期間中に一度以上、失効リストの更新をおこなうようにしてください。
また、RADIUSサーバに新しい失効リストを認識させるには、RADIUS(サービス)を再起動する必要があります。

10.CA - RADIUS サーバ証明書

EAPによる認証に用いるサーバ証明書の作成をおこないます。

「新規追加」をクリックすると入力画面が表示されます。

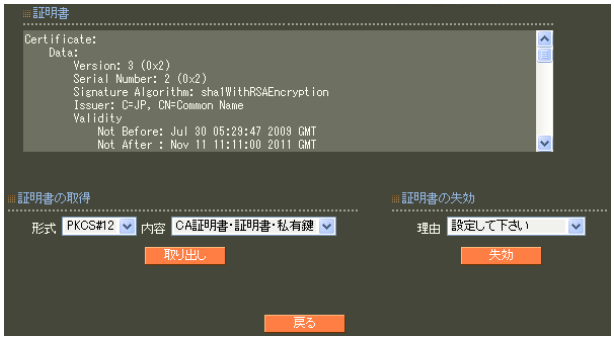


入力項目の詳細については、**「第７章 CA設定 Ⅱ．証明書 ○証明書の作成」**を参照してください。

各項目に入力後、「実行」ボタンを押して証明書を発行します。

証明書発行後は次の画面が表示されるようになります。

「S/N」（シリアルナンバ）を押すと、次の証明書表示画面が表示され、発行内容を確認することができます。



証明書の操作の詳細については
「第７章 CA設定 Ⅱ．証明書 ○証明書の表示」を参照してください。

11.CA - HTTPS サーバ証明書

本装置の管理画面アクセスに SSL を用いる場合の、サーバ証明書の作成をおこないます。
このメニューの操作は前の「10.CA-RADIUS サーバ証明書」と同一になります。

12.CA - LDAP クライアント証明書

ユーザ認証時に LDAP サーバ連携をおこなう場合で、StartTLS または LDAPS プロトコルにより通信を保護したい場合に、本装置側の証明書を作成します。
このメニューの操作は「10.CA-RADIUS サーバ証明書」と同一になります。

13.CA - LDAP サーバ証明書

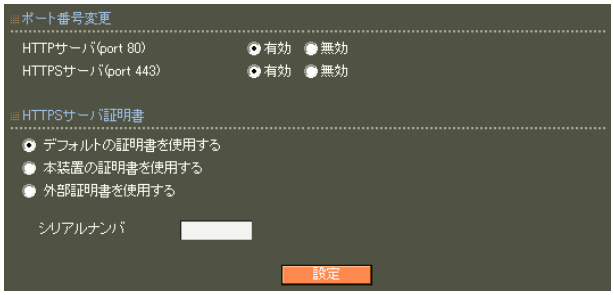
ユーザ認証時に LDAP サーバ連携をおこなう場合で、StartTLS または LDAPS プロトコルにより通信を保護したい場合に、LDAP サーバ側の証明書を作成します。
このメニューの操作は「10.CA-RADIUS サーバ証明書」と同一になります。本証明書の作成後、この証明書を取り出して、LDAP サーバに設定をしてください。

14. 管理画面へのアクセス

本装置の管理画面へアクセスするために必要な設定をおこないます。

■ HTTPS サーバ証明書
「本装置の証明書を使用する」欄の「表示」ボタンは、HTTPS サーバ証明書で、「本装置の証明書を使用する」が設定されている場合にのみ表示されます。
このボタンを押すと証明書の内容が表示され、証明書の取得等ができます。
証明書の詳細については**「第7章 CA設定 II. 証明書」**を参照してください。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。



■ポート番号変更
HTTP サーバ(port 80)/HTTPS サーバ(port 443)によるアクセスを有効にするか無効にするかを選択します。
必ずどちらかは有効にしておく必要があります。

■ HTTPS サーバ証明書
デフォルトで設定されている証明書、本装置の CA で発行したサーバ証明書、外部の CA で発行されたサーバ証明書のいずれを使用するか選択します。

「本装置の証明書を使用する」を選択した場合には、証明書のシリアルナンバを入力して証明書を指定してください。シリアルナンバは、16 進数で入力します。

「外部証明書を使用する」を選択する場合は、事前に証明書をインポートしておく必要があります。

「デフォルトの証明書を使用する」は、 初期設定のための一時的な利用を想定しています。
できるだけ本装置で発行した証明書または外部証明書を使用してください。

証明書の鍵長・Signature Algorithm は、
それぞれ 2048・SHA-256 を推奨します。

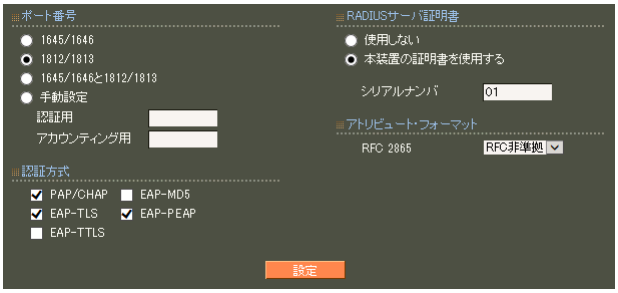
各項目に入力後、「設定」ボタンをクリックして設定完了です。設定はすぐに反映されます。

15.RADIUS - 基本情報

ポート番号、認証方式、RADIUS サーバの証明書の指定など、RADIUS の基本的な情報の設定をおこないます。

■ RADIUS サーバ証明書
「本装置の証明書を使用する」欄にある「表示」ボタンは RADIUS サーバ証明書が設定されている場合にのみ表示されます。
このボタンを押すと証明書の内容が表示され、証明書の取得等ができます。
証明書の詳細については**「第７章 CA 設定 II. 証明書」**を参照してください。

基本情報の設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。



■ポート番号
RADIUS では、認証（Authentication）とアカウンティング（Accounting）の２つのポートを利用して、RADIUS クライアントとの通信をおこなっていますが、そのポート番号の設定をおこないます。
以下の４種類から選択します。

- 1645/1646
- 1812/1813
- 1645/1646、1812/1813 の双方
- 手動設定

手動設定の場合は、さらに使用したいポート番号を指定します。
指定できるポート範囲は、1024 以上 60000 以下で、認証用とアカウンティング用で異なるポート番号を指定してください。

■認証方式
利用するユーザ認証方式の選択をおこないます。
本装置では、以下の５つの認証方式をサポートしています。

- PAP/CHAP
- EAP-MD5
- EAP-TLS
- EAP-PEAP
- EAP-TTLS

使用する認証方式のチェックボックスをチェックしてください。なお、「EAP-PEAP」または「EAP-TTLS」を選択する場合は、「EAP-TLS」も選択しておく必要があります。
また、「EAP-TTLS」を選択する場合には TTLS 内部認証で使う認証方式も同時に選択してください。

■ RADIUS サーバ証明書
認証で、「EAP-TLS」、「EAP-PEAP」または「EAP-TTLS」を選択した場合には、RADIUS サーバ証明書が必要となります。
証明書は事前に CA のメニューにて生成しておく必要があります（**「第７章 CA 設定」**参照）。
証明書を作成した後、設定画面から「本装置の証明書を使用する」を選択して、作成した証明書のシリアルナンバを指定します。シリアルナンバは、16 進数で入力します。
有効期間内の証明書を設定して下さい。有効期間外の場合は認証に成功しないことがあります(サプリカントに依存します)。

■ アトリビュート・フォーマット
認証アトリビュートや応答アトリビュートなどに使用する際のアトリビュート・フォーマットを設定します。

「RFC 2865」の値を変更することで、
Callback-Number
Callback-Id
Called-Station-Id
Calling-Station-Id
NAS-Identifier
の各アトリビュートのフォーマットを変更できます。

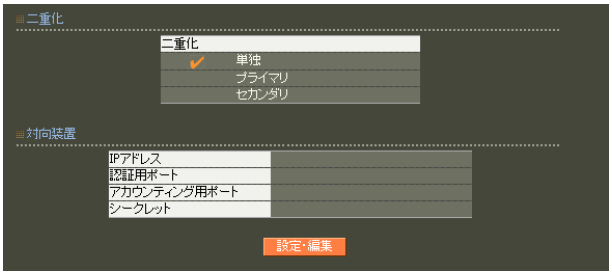
「RFC非準拠」にした場合、これらのフォーマットは、text（ASCII文字列)として扱われます。
「RFC準拠」にした場合は、これらのフォーマットは、string（バイナリデータ）になります。

これらが
認証プロファイル
応答プロファイル
ユーザ個別設定（認証アトリビュート）
ユーザ個別設定（応答アトリビュート）
LDAP アトリビュートマップ
に使用されている場合、本設定値を変更することはできません。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

16.RADIUS - 二重化

本装置は、２台構成にて、冗長化機能を持たせる事ができます。



設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■二重化
○単独
本装置を単独で利用する場合に設定します。

○プライマリ
○セカンダリ
本装置を二重化構成で使用する場合に「プライマリ」または「セカンダリ」を指定します。
二重化構成を取る装置の片方を「プライマリ」に、もう一方を「セカンダリ」に設定してください。

■対向装置
二重化構成で使用する場合の、相手装置に関する情報を入力します。

○ IP アドレス
相手装置の IP アドレスを入力します。

○認証用ポート
○アカウンティング用ポート
○シークレット
相手装置の設定内容と一致するように入力します。
最大 30 文字まで入力することが可能で、使用可能な文字は英数字と空白文字および以下の記号です。

!#$%&'()*+,-./:;<=>?@[]^_`{|}~

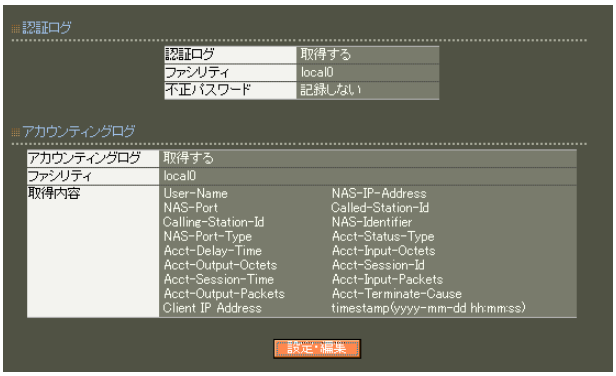
各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

二重化構成では、2 台の RA の時刻同期を行ってください。
時刻同期には、NTP 機能を利用することが可能です。

二重化構成におけるファームウェア更新については、「付録 F 同期・二重化構成におけるファームウェア更新手順」を参照してください。

17.RADIUS - ログ

RADIUS関連のログについて、記録に残すログの種類を設定します。



設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■認証ログ

○認証ログ

RADIUSによるユーザ認証に関する記録を残すかどうかを選択します。

○ファシリティ

認証ログを「取得する」にした場合、認証ログが出力されるファシリティを指定します。
プルダウンから選択してください。

○不正パスワード

「記録する」を選んだ場合、パスワードが正しくないことが原因で認証失敗した時に、認証要求に含まれるパスワードが認証ログに記録されます。
パスワードが記録されるのは、PAP または EAP-TTLS/PAPの場合に限られます。

■アカウンティングログ

○アカウンティングログ

RADIUSのアカウンティング記録を残すかどうかを選択します。

○ファシリティ

アカウンティングログを「取得する」にした場合、アカウンティングログが出力されるファシリティを指定します。
プルダウンから選択してください。

○取得項目

記録に残したい項目を選んで、チェックボックスをチェックします。
項目の詳細については「**第6章 RADIUS設定 I. サーバ設定 10. ログ**」を参照してください。

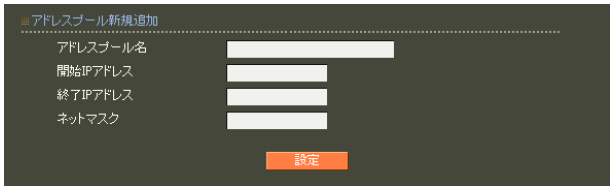
各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

18.RADIUS - アドレスプール

端末に IP アドレスを割当てる場合に貸与する IP アドレスの領域を設定します。

「新規追加」をクリックすると入力画面が表示されます。

■アドレスプール新規追加



○アドレスプール名
任意の名前を 20 文字以内で入力します。後に他のメニューでアドレスプールを割り当てる時に、ここで設定された名前が選択肢として表示されます。使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。

○開始 IP アドレス
端末に貸与する IP アドレスの最初の IP アドレスを指定します。

○終了 IP アドレス
端末に貸与する IP アドレスの最後の IP アドレスを指定します。開始 IP アドレスから終了 IP アドレスまでの間の IP アドレスがクライアントに貸与されます。ここで設定された値は、RADIUS アトリビュートの「Framed-IP-Address」の値となり、RADIUS クライアントに返信されます。

○ネットマスク
サブネットマスクの値を登録します。
ここで設定された値は、RADIUS アトリビュートの「Framed-IP-Netmask」の値となり、RADIUS クライアントに返信されます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なアドレスプールの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
アドレスプール一覧に登録されている設定を編集または削除したい場合には、そのアドレスプールが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

19.RADIUS - クライアント

本装置にアクセス可能なRADIUSクライアントを設定します。

「新規追加」をクリックすると入力画面が表示されます。

■クライアント新規追加

○クライアント名
任意の名前を20文字以内で入力します。使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。

○ IPアドレス
RADIUSクライアントのIPアドレスを入力します。

○シークレット
RADIUSクライアントとの認証や暗号処理に用いる文字列を入力します。RADIUSクライアント側でも同じ値が設定されている必要があります。
最大30文字まで入力することが可能で、使用可能な文字は英数字と空白文字および以下の記号です。

!#$%&'()*+,-./:;<=>?@[]^_`{|}~

○アドレスプール
端末にIPアドレスを割当てる場合に、アドレスプール名を選択します。アドレスプールの選択肢には、前項の「アドレスプール」メニューで設定した名前が表示されます。IPアドレスを本装置から割り当てない場合には「指定しない」を選択します。

アドレスプールは後のメニュー「RADIUS-ユーザ基本情報」の中で割り当てることもできます。
ユーザ基本情報プロファイルのIPアドレス割り当てが指定されている場合、そのプロファイルを使用しているユーザへのIPアドレス割り当ては、プロファイル中の設定が優先して使われます。
本メニューのアドレスプールは、ユーザ基本情報プロファイルのIPアドレス割り当てが「未使用」のユーザ、または、「固定」で設定されているユーザの内、固定IPアドレスが指定されていないユーザにのみ適用されます。

本項のアドレスプールを設定してIPアドレスを割当てるためには、本装置でRADIUSクライアントとして設定したアドレスがNAS-IP-Addressとして Access-Requestに含まれている必要があります。

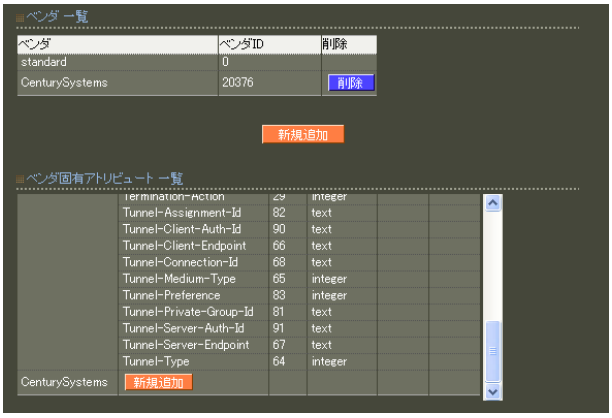
各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なクライアントの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
クライアント一覧に登録されている設定を編集または削除したい場合には、そのアドレスプールが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

20.RADIUS - アトリビュート

RADIUS標準アトリビュート以外に、ベンダ固有アトリビュート(VSA)を使用したい場合に設定します。
本メニューにて設定されたベンダ固有アトリビュートは、後のメニューにて、認証に使用するアトリビュートとして指定したり、認証応答に付加されるVSA設定値の指定に使えるようになります。



■ベンダー一覧
登録されているベンダの一覧が表示されます。

■ベンダ固有アトリビュートー一覧
登録されているアトリビュートの一覧がベンダ毎に表示されます。
良く使われる標準のアトリビュートについてはベンダ「standard」として定義されています。「standard」として定義されているアトリビュートについては新規作成や、編集、削除はできません。

先にベンダの追加をおこないます。
ベンダー一覧の「新規追加」ボタンを押します。

■ベンダ新規追加

◯ベンダ
追加したいベンダ名を入力します。最大20文字まで入力可能です。使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。

◯ベンダ ID
ベンダ毎に割り当てられているベンダ IDを数値で入力します。

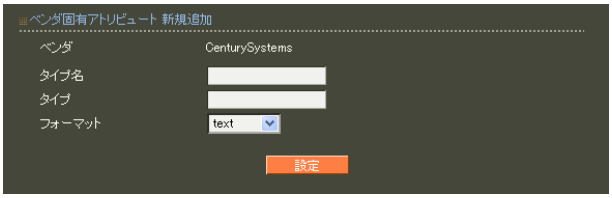
各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

設定可能なベンダの最大数は
「付録 A 最大数一覧」を参照してください。

削除
登録されているベンダを削除したい場合には「削除」ボタンを押すと削除されます。
ベンダ固有アトリビュートで使われているベンダは削除できません。

続いて、ベンダ固有アトリビュート一覧から「新規追加」ボタンを押すと入力画面が表示されます。

■ベンダ固有アトリビュート新規追加



○ベンダ
選択されたベンダ名が表示されます。

○タイプ名
ベンダ固有アトリビュート用にベンダから指定されているタイプ名を指定します。最大 20 文字まで入力可能です。使用可能な文字は英数字およびハイフン(‘ - ’)、アンダーバー(‘ _ ’)になります。

○タイプ
アトリビュート番号を指定します。1 ～ 255 の整数値を入力してください。

○フォーマット
アトリビュートのデータ型をプルダウンから選択してください。以下の 5 種類から選択できます。

- text
  対象アトリビュートのデータ型が ASCII 文字列の場合に選択します。

- string
  対象アトリビュートのデータ型がバイナリデータの場合に選択します。

- address
  対象アトリビュートのデータ型が IP アドレス形式の場合に選択します。

- integer
  対象アトリビュートのデータ型が整数の場合に選択します。

- ipv6address
  対象アトリビュートのデータ型が IPv6 アドレス形式の場合に選択します

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なベンダ固有アトリビュートの最大数は「付録 A 最大数一覧」を参照してください。

変更・削除
ベンダ固有アトリビュート一覧に登録されているアトリビュートを編集または削除したい場合にはアトリビュートが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

21.RADIUS - ActiveDirectory

ユーザ認証を Active Directory でおこないたい場合に設定します。
本設定をおこなうと、EAP-PEAP による認証要求を受けた場合に、設定された Active Directory サーバに問い合わせることで認証の可否を判断します。

「設定・編集」ボタンを押すと入力画面が表示されます。

■ ActiveDirectory

○Active Directory 連携
ActiveDirectory 連携機能を使用する場合に「使用する」を選択します。

○Active Directory サーバ
・1.8.13 以降
　使用しません。
　DNS を使用してドメインコントローラを自動的に検索します。
・1.8.12 以前
　ドメインコントローラを FQDN または IP アドレスで指定します。

○ドメイン名
認証を受けるドメイン名を入力します。

○ドメイン名(Windows2000 より前)
ドメインに設定された NetBIOS名を設定します。
Windows サーバ上で「ドメイン名(Windows2000 より前)」や「ドメイン名(Windows2000 以前)」などの名前で参照できます。
「ドメイン名」の先頭パートと同一の場合は省略可能です。
最大 15 バイトまで入力可能です。
使用可能な文字は、英数字およびハイフン(-)、アンダーバー(_)です。

○所属グループ
認証を受ける所属グループ名を入力します。
空欄にするとグループ情報を用いずに認証をおこないます。

○管理者ユーザ ID
認証情報の確認をおこなうための ActiveDirectory のユーザアカウントを指定します。
このユーザは Administrators グループまたは AccountOperators グループに所属しているか、または同等の権利が与えられている必要があります。

○管理者パスワード
管理者ユーザ ID に対応したパスワードを入力します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。
保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。
RADIUS サーバの起動時に、RA はドメインに参加します。管理者ユーザ ID の権限で、Active Directory サーバにコンピュータアカウントを作成します。

Active Directory 連携機能を利用する際の注意

・Active Directory 連携機能を利用するためには、DNSの設定(管理機能メニューの「ネットワーク」-「DNS」)で所属するドメインのDNSサーバが設定されている必要があります。

・Active Directory サーバと本装置の時刻がずれている場合、Active Directory サーバとの連携ができないことがあります。

・ Active Directory サーバへの認証情報の問い合わせは、以下の手順で行われます。

(1) 認証要求に含まれるユーザ名 (User-Name) から最初の \ 以前を取り除く。
(2) (1) の結果に @ が含まれる場合、最後の @ より後ろの文字列がドメイン名(設定値)に一致していなければ問い合わせしない。(1.9.0 以降のみ)
(3) (1) の結果から最後の @ 以降を取り除く。(1.9.0 以降のみ)
(4) (3) の結果が空文字列であれば、問い合わせしない。(1.9.0 以降のみ)
(5) (3) の結果に \ が含まれていれば、問い合わせしない。(1.9.0 以降のみ)
(6) (3) の結果をユーザ名として Active Directory サーバへ問い合わせを行う。

・Active Directory 連携機能を有効にした場合、EAP-PEAP 認証では常に Active Directory サーバのユーザ情報が使用されます。LDAP 連携機能や本装置内に設定されたユーザ情報などは使われません。

・LDAP 連携機能において EAP-PEAP 認証を行う場合、Active Directory 連携機能と同時に使用することはできません。

Active Directory サーバへの対応状況

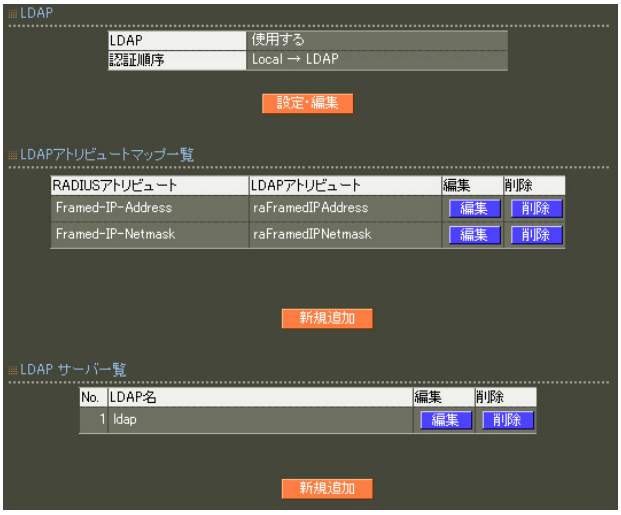
Active Directory サーバの各バージョンに対するRAの対応状況は以下の通りです。

Active Directoryサーバの version	対応しているRAの version	
	RA-1200	RA-730
Windows Server 2012 R2	1.10.0	1.10.0
Windows Server 2012	1.10.0	1.10.0
Windows Server 2008 R2	1.8.9	1.8.3
Windows Server 2008	1.8.9	1.8.3

但し、全ての環境において Active Directory サーバとの連携を保証するものではありません。

22.RADIUS - LDAP

LDAPサーバと連携してユーザ認証をおこないたい場合に設定します。
PAP/CHAP、EAP-MD5、EAP-PEAP、EAP-TTLS/PAP、CHAP、EAP-TTLS/EAP-MD5による認証要求を受けた場合に、設定されたLDAP サーバを利用して認証の可否を判断することができます。



これより、各設定について説明します。

■ LDAP

LDAPサーバ連携使用の有無と、使用する場合の認証順序が表示されています。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ LDAP

○ LDAP

LDAPサーバ連携機能を使用する場合に「使用する」を選択します。

○認証順序

LDAPサーバ上のユーザ情報に基づく認証と、本装置上に登録されたユーザ情報に基づく認証のどちらを優先しておこなうかを指定します。
「Local → LDAP」を指定した場合、最初に本装置上で認証を試みます。そして認証要求されたユーザが本装置上に登録されていなかった場合にLDAPサーバ連携による認証をおこないます。
「LDAP → Local」の場合は逆に、LDAP上のユーザ認証が最初におこなわれます。

選択後「設定」ボタンを押してください。
LDAPサーバを使用する選択にした場合には続いてLDAPサーバの登録をおこなってください。

■LDAPアトリビュートマップ一覧

LDAPアトリビュートマップ機能を用いることで、LDAPサーバから応答アトリビュートを取得し、RADIUSクライアントに返すことが可能となります。応答アトリビュートはLDAPサーバでユーザ毎に設定します。
LDAPアトリビュートマップは、LDAPサーバ毎ではなく全体で共有されます。

設定可能なLDAPアトリビュートマップの最大数は「付録 A 最大数一覧」を参照してください。

設定情報の同期をおこなう設定の場合、本設定は対向装置へ同期されます。

「新規追加」ボタンを押すと入力画面が表示され、LDAPアトリビュートマップをひとつ作成することができます。
ここでは、LDAPサーバ上のアトリビュートからRADIUS応答アトリビュートへの変換ルールの組を設定します。

■LDAPアトリビュートマップ新規追加

○RADIUSアトリビュート
RADIUSアトリビュートを選択します。任意のアトリビュートを選択することができます。

○LDAPアトリビュート
LDAPサーバへ問い合わせる際の検索フィルタアトリビュートを設定します。
各LDAPサーバで設定された「ベースDN」や「フィルタアトリビュート」などと複合してLDAPサーバに問い合わせがおこなわれます。LDAPアトリビュートは「管理者ユーザID」の権限で読み出せる必要があります。

使用可能な文字は、下記の通りです。
0-9，a-z，A-z，-(0x2c)，_(0x5f)。
最大文字数は「40（ver1.8.3以前は20）」で、デフォルト値はありません。

入力後に「設定」ボタンを押してください。

変更

既に設定されているLDAPアトリビュートマップのひとつを変更することができます。
RADIUSアトリビュートは編集することはできませんが、LDAPアトリビュートは変更可能です。

削除

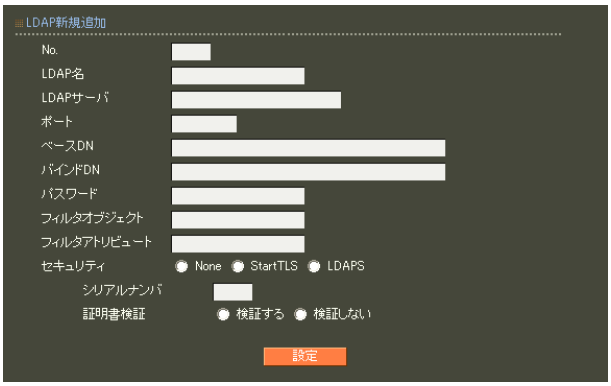
既に設定されているLDAPアトリビュートマップのひとつを削除することができます。

■ LDAP サーバ一覧

表示画面の下段には設定済みの LDAP サーバが一覧表示されています。1 番のサーバから順に LDAP による認証が試みられます。

「新規追加」ボタンを押すと入力画面が表示されます。

■ LDAP 新規追加



○ No.

この LDAP サーバの認証の順番を指定します。
空欄にした場合には既存の LDAP サーバ設定の最後に追加されます。
既に LDAP サーバが登録されている番号を指定した場合には、今回作成する LDAP サーバがその番号で設定され、指定された番号から下の既存の LDAP サーバ設定が一つずつ後ろにずれて設定されます。

○ LDAP 名

識別用に任意の名前を 20 文字以内で入力します。

○ LDAP サーバ

LDAP サーバ名を FQDN または IP アドレスで指定します。

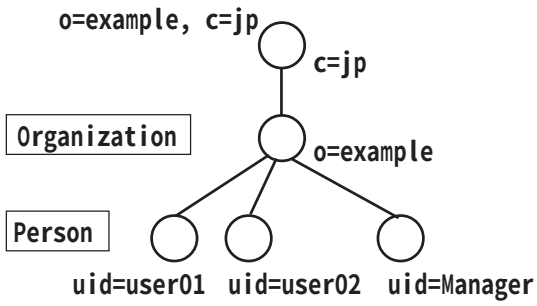
○ポート

LDAP サーバのポート番号を指定します。
指定できるポート範囲は、80，443，802 番を除く 1 ～ 1023 の範囲になります。
一般的には LDAP(StartTLS 含む)の場合には 389、LDAPS の場合には 636 が使われます。

○ベース DN

認証要求で送られたユーザ名を LDAP サーバに問い合わせる際の基点となるエントリの Distinguished Name を指定します。

＜入力例＞



図：ディレクトリツリーの例

○バインドDN
認証要求で送られたユーザ名をLDAPサーバに問い合わせる際に用いるユーザのDistinguished Nameを指定します。
ユーザの検索に必要なアクセス権が与えられている必要があります。
バインドDNが未設定の場合は、LDAPサーバに匿名アクセスを行います。

<入力例>
uid=Manager，o=example，c=jp

○パスワード
上記「バインドDN」に対応したパスワードを指定します。
バインドDNが未設定の場合(LDAPサーバに匿名アクセスを行う場合)は、設定しないで下さい。

○フィルタオブジェクト
使用しません。

○フィルタアトリビュート
認証要求で送られたユーザ名をLDAPサーバに問い合わせる際に、指定されたユーザ名に対応させる属性を指定します。

<入力例>
uid

LDAPサーバとしてActive Directoryを使用する場合には以下を指定するようにします。

sAMAccountName

○セキュリティ
LDAPサーバと通信をおこなう場合のセキュリティプロトコルを指定します。
「None」を指定した場合には通信がLDAPでおこなわれ、暗号化等はされません。
「StartTLS」「LDAPS」が指定された場合にはそれぞれのプロトコルに従って通信がおこなわれます。

○シリアルナンバ
セキュリティで「StartTLS」または「LDAPS」を選択した場合に、本装置が用いるクライアント証明書を指定します。
証明書はあらかじめCAメニューの「証明書」で生成しておく必要があります(「**第7章 CA設定 II．証明書**」参照)。
使用する証明書のシリアルナンバを16進数で入力します。
有効期間内の証明書を設定して下さい。有効期間外の場合は認証に成功しないことがあります(LDAPサーバに依存します)。

○証明書検証
「StartTLS」または「LDAPS」使用時にLDAPサーバの証明書を検証するか否かを指定します。
検証するにした場合、LDAPサーバの証明書が不正であった場合にはそのLDAPサーバは認証に使用しなくなります。
LDAPサーバ証明書のCNの値がサーバ名と異なっていた場合には不正な証明書とみなされます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

設定可能なLDAPサーバの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
LDAPサーバー一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

LDAP連携機能における認証について

LDAPサーバと連携してユーザ認証をおこなう方法は3種類あります(ver1.8.3以前は1種類)。

(1) バインド(接続)

認証させたいユーザの権限でLDAPサーバにバインド(接続)できる場合に、PAPまたはEAP-TTLS/PAPで認証可能となります。

認証の可否はLDAPサーバが決定します。LDAPサーバでユーザにアクセス制限等が掛けられていれば認証に成功しません。

(2) 平文パスワード(ver1.8.4以降のみ)

LDAPサーバのuserPasswordアトリビュートに、平文のパスワードが設定されていて、かつRAに設定した管理者ユーザIDの権限でその値が読み出せる場合に、CHAP、EAP-MD5、EAP-PEAP、EAP-TTLS/CHAP、EAP-TTLS/EAP-MD5で認証可能となります。

LDAPサーバから読み出したパスワードの先頭に{CLEAR}または{CLEARTEXT}が付加されている場合、それらを無視します。
また、それらの大文字小文字は区別しません。{CLEAR}、{clear}、{Clear}などいずれの場合も無視します。

認証の可否はRAが決定します。LDAPサーバでユーザにアクセス制限等が掛けられていても、管理者ユーザIDの権限でパスワードの読み出しが可能であれば認証に成功します。

(3) NTLMハッシュ(ver1.8.4以降のみ)

LDAPサーバにNTLMハッシュが設定されていて、かつRAに設定した管理者ユーザIDの権限でその値が読み出せる場合に、EAP-PEAPで認証可能となります。

NTLMハッシュとは、UTF-16LEでエンコードされたパスワードをMD4を用いてハッシュした16バイトの値です。

LDAPサーバをRAと連携させるためには、sambaNTPasswordアトリビュート、またはcsRANTLMHashアトリビュートのいずれかに各ユーザのNTLMハッシュが設定されている必要があります。
また、その値は16バイトのハッシュ値を16進数表記で表した32バイトの文字列でなければなりません。(例：00112233445566778899AABBCCDDEEFF)。大文字小文字どちらも使用可能です。

認証の可否はRAが決定します。LDAPサーバでユーザにアクセス制限等が掛けられていても、管理者ユーザIDの権限でNTLM ハッシュの読み出しが可能であれば認証に成功します。

NTLMハッシュが部外者に漏洩しないように注意して下さい。NTLMハッシュを用いることで、ユーザ認証を不正に成功させることが可能です。

なお、EAP-PEAP認証においては、NTLMハッシュと平文パスワードの両方が設定されている場合には、NTLM ハッシュを使用します。

LDAP連携機能を利用する際の注意

LDAP連携機能においてEAP-PEAP認証を行う場合、Active Directory連携機能と同時に使用することはできません。

Active Directory を LDAP サーバとして使用する場合、利用できる認証方式は PAP または EAP-TTLS/PAP のみです。

23.RADIUS - ユーザ基本情報

本装置では、同じ内容の設定を複数ユーザに対して容易に設定できるようにするために、共通の設定内容をあらかじめプロファイルとして定義しておくことができます。
プロファイルは、「ユーザ基本情報」、「認証アトリビュート」「応答アトリビュート」、「証明書」、「グループ ID」に分けて設定することができ、このプロファイルを組み合わせて「ユーザプロファイル」とします。このユーザプロファイルを各ユーザの設定時に選択することで、ユーザ情報を素早く入力していくことができます。

ユーザ基本情報プロファイルは、認証方式や IP アドレスの割り当て方式などを指定するプロファイルです。ユーザ基本情報プロファイルは必ず一つ以上作成する必要があります。

「新規追加」をクリックすると入力画面が表示されます。

■ユーザ基本情報プロファイル新規追加

○プロファイル名
任意の名前を 20 文字以内で入力します。
「ユーザプロファイル」メニューでユーザ基本情報プロファイルを設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。
(他のプロファイルも同様です。)

○認証方式
ユーザ認証方式の選択をおこないます。
本装置では、以下の 7 つの認証方式をサポートしています。

- PAP/CHAP
- EAP-MD5
- EAP-TLS
- EAP-PEAP
- EAP-TTLS/PAP,CHAP
- EAP-TTLS/EAP-MD5
- EAP-TTLS/EAP-PEAP

選択した認証方式については、「RADIUS- 基本情報」でも選択されていることを確認してください。「RADIUS- 基本情報」で選択されていない認証方式については、本メニューで選択しても認証はおこなわれません。

○同時接続数
一人のユーザが同時に RADIUS サーバの認証を受けられる数を指定します。一人のユーザが同時に多数の接続をおこなうことを制限したい場合に用います。
設定可能な同時接続数は、「1」～「9」になります。また、空欄にした場合、同時接続数は無制限になります。

○ IP アドレス割り当て
ユーザ認証に成功した端末に対する IP アドレスの割り当て方法の設定です。
IP アドレス割り当てをおこなわない場合には「未使用」を選択します。
RADIUS クライアント装置が割り当てをおこなう場合には「RADIUS クライアント」を選択します。
本装置のアドレスプールを利用して割り当てる場合には、「アドレスプール」を選択します。
固定 IP アドレスをユーザ毎に割り当てる場合には、「固定」を選択してください。

○アドレスプール
IPアドレス割り当てで「アドレスプール」を選択した場合に、設定をおこないます。
「アドレスプール」の項目で設定した内容が選択肢に表示されますので、設定したいアドレスプールを選択します。

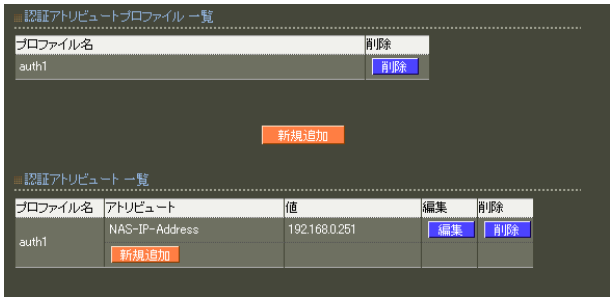
各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なユーザ基本情報プロファイルの最大数は「付録 A 最大数一覧」を参照してください。

変更・削除
ユーザ基本情報プロファイル一覧に登録されている設定を編集または削除したい場合には、そのプロファイルが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

24.RADIUS - 認証アトリビュート

認証時に認証方式に応じて送られるパスワードなどの情報に加え、RADIUSクライアントから送られてくるアトリビュートを認証に用いる場合に使用するプロファイルです。
このような認証をおこなわない場合には認証アトリビュートプロファイルを作成する必要はありません。
このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ作成」メニューでユーザに適用されます。



■認証アトリビュートプロファイル一覧
登録されている認証アトリビュートプロファイルの一覧が表示されます。

■認証アトリビュート一覧
各認証アトリビュートプロファイルで定義されているアトリビュートの一覧が表示されます。

■認証アトリビュートプロファイル一覧
新たに認証アトリビュートプロファイルを追加する場合には、一覧から「新規追加」ボタンを押してプロファイルの追加をおこないます。

■認証アトリビュートプロファイル新規追加

○プロファイル名
任意の名前を20文字以内で入力します。
「ユーザプロファイル」メニューで認証アトリビュートプロファイルを設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

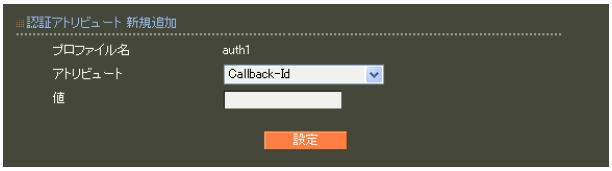
設定可能な認証アトリビュートプロファイルの最大数は「付録 A 最大数一覧」を参照してください。

削除
登録されているプロファイルを削除したい場合には一覧から「削除」ボタンを押すと削除されます。

■認証アトリビュート一覧

認証アトリビュートプロファイルに対してアトリビュートの追加・編集・削除をおこないます。
アトリビュートを追加する場合には、追加したい認証アトリビュートプロファイルの表中に表示されている「新規追加」ボタンを押します。
以下の入力画面が表示されます。

■認証アトリビュート新規追加



○プロファイル名

選択したプロファイル名が表示されています。

○アトリビュート

ユーザ認証に使用するアトリビュートをプルダウンから選択します。
選択できるアトリビュートは、あらかじめ本製品で定義されてあるものの他、「RADIUS- アトリビュート」で追加したベンダ固有アトリビュートも使用できます。

○値

認証に使用するアトリビュートの値を定義します。
選択したアトリビュートのフォーマットに応じて次のように入力します。

・text(ASCII 文字列)
ASCII 形式の文字列を入力してください。
設定可能な長さは、定義済みの standard のアトリビュートで最大 253 文字、追加したベンダ固有アトリビュートで最大 247 文字です。
入力例：century

・string(バイナリデータ)
16 進表記で入力してください。ただし、行頭に 0x は不要です。
設定可能な長さは定義済みの standard のアトリビュートで最大 253 オクテット(2～506 文字)、追加したベンダ固有アトリビュートで最大 247 オクテット(2～494 文字)です。
入力例：63656e74757279
(“century”の文字コードデータ)

・address(IP アドレス)
IPv4 アドレス表記で入力してください。
入力例：192.168.0.1

・integer(整数)
負ではない整数値を入力してください。
設定可能な範囲は 0～4294967295 です。
入力例：65536

・ ipv6address(IPv6 アドレス)
IPv6 アドレス表記で入力してください。
入力例：fe80::1111

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能な認証アトリビュートの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除

認証アトリビュート一覧に登録されている設定を編集または削除したい場合には、そのアトリビュートが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

25.RADIUS - 応答アトリビュート

認証成功時にRADIUSクライアントに送るアトリビュートを指定するためのプロファイルです。
指定するアトリビュートが無い場合には作成する必要はありません。このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ作成」メニューでユーザに適用されます。

■応答アトリビュートプロファイル一覧
登録されている応答アトリビュートプロファイル名の一覧が表示されています。

■応答アトリビュート一覧
各応答アトリビュートプロファイルで定義されているアトリビュートの一覧が表示されています。

■応答アトリビュートプロファイル一覧
新たに応答アトリビュートプロファイルを追加する場合には、一覧から「新規追加」ボタンを押してプロファイルの追加をおこないます。

■応答アトリビュートプロファイル新規追加

◯プロファイル名
任意の名前を20文字以内で入力します。
「ユーザプロファイル」メニューで応答アトリビュートプロファイルを設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

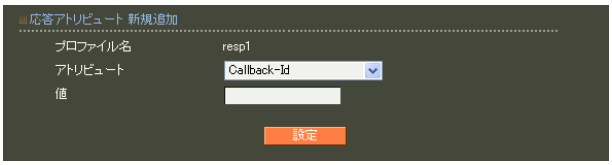
設定可能な応答アトリビュートプロファイルの最大数は「付録 A 最大数一覧」を参照してください。

削除
登録されているプロファイルを削除したい場合には一覧から「削除」ボタンを押すと削除されます。

■応答アトリビュート一覧

応答アトリビュートプロファイルに対してアトリビュートの追加・編集・削除をおこないます。
アトリビュートを追加する場合には、追加したい応答アトリビュートプロファイルの表中に表示されている「新規追加」ボタンを押します。
以下の入力画面が表示されます。

■応答アトリビュート新規追加



選択したプロファイル名が表示されています。

○アトリビュート
RADIUSクライアントに送付するアトリビュートをプルダウンから選択します。
選択できるアトリビュートは、あらかじめ本製品で定義されてあるものの他、RADIUSの「サーバ」メニューのアトリビュートで追加したベンダ固有アトリビュートも使用できます。

○値
送付するアトリビュートの値を定義します。
選択したアトリビュートのフォーマットに応じて入力します。入力の仕方は認証アトリビュートと同じです。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能な応答アトリビュートの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除

応答アトリビュート一覧に登録されている設定を編集または削除したい場合には、そのアトリビュートが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

26. グループ ID

ユーザ ID を "user@centurysys.co.jp" または ”CENTURYSYS\user ” のように、所属グループを表わす文字列を付加して指定するためのプロファイルです。
このようなユーザ ID を利用しない場合には作成する必要はありません。このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ」メニューでユーザに適用されます。ユーザに適用した場合、そのユーザは、グループ ID も付加したユーザ名の形でのみ認証され、ユーザ ID 単独での認証には失敗するようになります。

「新規追加」をクリックすると入力画面が表示されます。

■グループ ID プロファイル新規追加

○プロファイル名
任意の名前を 20 文字以内で入力します。
「ユーザプロファイル」メニューでグループ ID を設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

○グループ ID
ユーザ名に付加する文字列を指定します。
最大 40 文字まで指定できます。使用可能な文字は英数字およびハイフン(“ - ”)、ピリオド(“ . ”)になります。

○形式
グループ ID、ユーザ ID および区切り文字の結合の仕方を指定します。
UserID@GroupID または GroupID\UserID から選択します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なグループ ID プロファイルの最大数は「付録 A 最大数一覧」を参照してください。

変更・削除
グループ ID プロファイル一覧に登録されている設定を編集または削除したい場合には、そのプロファイルが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

27.RADIUS - ユーザ証明書

ユーザ証明書を発行する際の共通項目をあらかじめ指定するためのプロファイルです。
このプロファイルの作成は任意です。このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ作成」メニューでユーザに適用されます。

「新規追加」をクリックすると入力画面が表示されます。

各設定内容の詳細については、**「第６章 RADIUS設定 II.プロファイル** 6.証明書」を参照して入力してください。

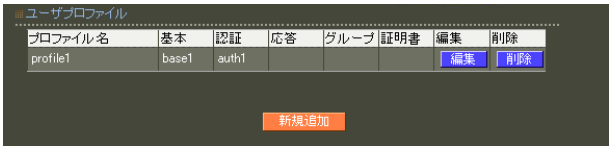
各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能な証明書プロファイルの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
証明書プロファイル一覧に登録されている設定を編集または削除したい場合には、そのプロファイルが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

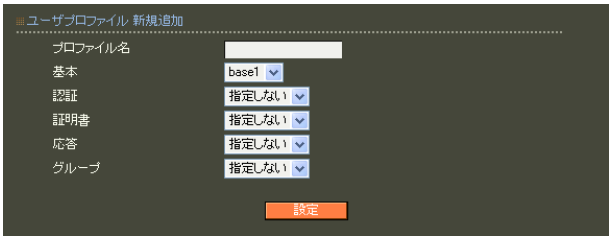
28.RADIUS - ユーザプロファイル

最終的にRADIUSの「ユーザ作成」メニューでユーザに適用することになる、大元のプロファイルです。このプロファイルは「ユーザ基本情報」、「認証アトリビュート」「応答アトリビュート」、「証明書」、「グループ ID」の各プロファイルを選択することで生成します。



「新規追加」をクリックすると入力画面が表示されます。

■ユーザプロファイル新規追加



○プロファイル名
任意の名前を20文字以内で入力します。
後に「ユーザ」メニューでユーザの追加や編集をおこなう際に、ここで設定されたプロファイル名が選択肢として表示されます。
使用可能な文字は英数字およびハイフン(" - ")、アンダーバー(" _ ")になります。

○基本 （ユーザ基本情報）
○認証 （認証アトリビュート）
○証明書
○応答 （応答アトリビュート）
○グループ （グループ ID）
既に設定されている各プロファイルの名前が選択肢に表示されますので、割り当てたいプロファイルをそれぞれ選択します。
「ユーザ基本情報」以外のプロファイルについては、プロファイルを使用しない場合、「指定しない」を選択することもできます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なユーザプロファイルの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
アドレスプール一覧に登録されている設定を編集または削除したい場合には、そのアドレスプールが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

29.RADIUS - ユーザ作成

ユーザの登録やユーザへのプロファイルの割り当てをおこないます。

ユーザ一覧表示画面から「新規追加」をクリックすると入力画面が表示されます。

■ユーザ新規追加
○ユーザ ID
登録するユーザ名を入力します。
ユーザ ID は、最大 20 文字まで入力する事が可能です。
使用可能な文字は英数字および以下の記号と空白文字になります。

```
!"#$%&'()*+-./<=>?@[]^_`{|}~
```

○パスワード
認証用パスワードを入力します。
パスワードは、最大 20 文字まで入力する事が可能です。
使用可能な文字は、ユーザ ID の入力可能文字と以下の記号になります。

```
,:;\
```

○プロファイル
このユーザに適用したいユーザプロファイルを選択します。「プロファイル」メニューで設定済みのユーザプロファイルが選択肢に表示されます。

■固定 IP アドレス払い出し
○ IP アドレス
固定の IP アドレスをユーザに払い出す場合に、端末に割り当てる IP アドレスを登録します。
ここで設定された値は、RADIUS アトリビュートの「Framed-IP-Address」の値となり、RADIUS クライアントに返信されます。
この設定を有効にするためにはユーザに割り当てられたユーザ基本情報プロファイルの IP アドレス割り当てが「固定」に設定されている必要があります。

○ネットマスク
サブネットマスクの値を登録します。
ここで設定された値は、RADIUS アトリビュートの「Framed-IP-Netmask」の値となり、RADIUS クライアントに返信されます。
この設定を有効にするためにはユーザに割り当てられたユーザ基本情報プロファイルの IP アドレス割り当てが「固定」に設定されている必要があります。

■備考
○備考
備考を設定することが出来ます。

備考は、最大 40 文字まで(日本語は 20 文字まで)入力することができます。
使用可能な文字は次の通りです。

0 ～ 9、A ～ Z、a ～ z、空白文字、
-(マイナス・ハイフン)、.(ピリオド・ドット)、@、
日本語（JIS X 0208:1997 に収録された 6879 文字)

※いわゆる半角カナ(1バイトの片仮名)やいわゆる機種依存文字(例えば Shift_JIS の『丸付き数字』など)は使用できません。

■アカウントのロック
○ロック
ユーザ毎に「ロックしない」「ロックする」のいずれかを選択します。
デフォルト値は「ロックしない」です。
それぞれの動作は下記の通りになります。

・「ロックしない」
・RADIUS 認証要求には、認証処理をおこなった結果を応答する
・GUI へのアクセスを許可する

・「ロックする」
・RADIUS 認証要求には、常に Reject を応答する
・GUI へのアクセスを許可しない

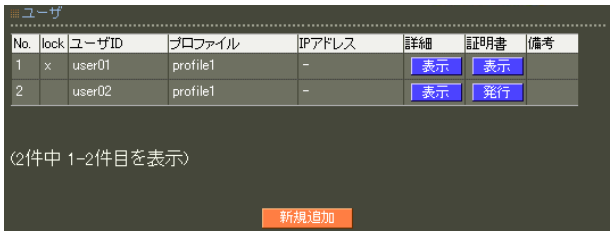
「ロックする」を選択している場合はユーザ一覧の「lock」欄に『 x 』が表示されます。
設定情報の同期をおこなう設定の場合、本設定は対向装置へ同期されます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なユーザの最大数は
「付録 A 最大数一覧」を参照してください。

※ 認証方式が EAP-TLS の場合にはユーザ証明書のみを使って認証処理をおこないます。ユーザ ID およびパスワードは認証に使用しません。
また、認証時にはユーザ証明書の Subject の Common Name を使ってユーザ ID との対応を取り、参照するプロファイルを決定します。

ユーザが登録されると、表示画面では次のようなユーザ一覧が表示されるようになります。
■ユーザ



ユーザの編集削除や、証明書発行などの操作をこの画面からおこなうことができます。

◆ユーザの詳細表示

ユーザ一覧表示画面において、詳細欄の「表示」ボタンを押すとユーザの現在の設定内容が表示されます。

■ユーザ設定

現在設定されているユーザ設定情報が表示されます。

■ユーザ設定（詳細）

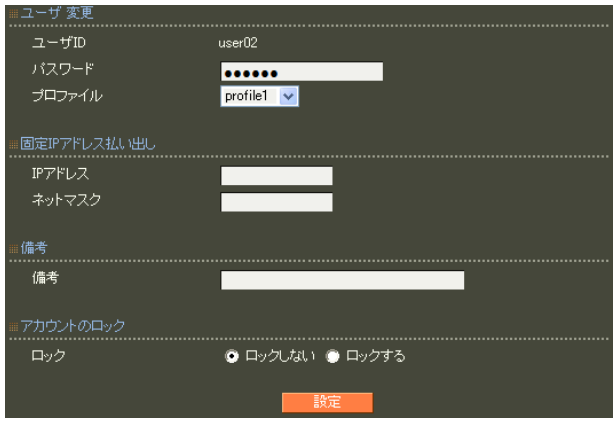
プロファイルの選択によって適用されている設定内容が表示されます。

■ユーザ設定

この画面からユーザの設定内容の編集、削除、およびユーザ個別設定をおこなうことができます。

編集

「編集」ボタンを押すとユーザ情報の編集画面が表示されます。



変更したい内容を入力して「設定」ボタンを押すと変更内容が反映されます。

削除

「削除」ボタンを押すと表示されているユーザが削除されます。

◆ユーザの個別設定

■ユーザ設定（詳細）

ユーザの詳細表示画面の下段に表示されている認証方式や応答アトリビュートなどは、本来ユーザに適用されているユーザプロファイルに従って設定され、ユーザに適用されます。
しかしプロファイルから外れた形でユーザ一人一人に対して個別に設定したい場合には、この詳細表示画面から個別に設定をおこなうことができます。
個別設定は以下の各プロファイルで設定されている内容を上書きまたは追加する形でおこなわれます。

個別設定が可能なアトリビュート
・基本
・認証
・応答

ユーザに個別設定がされている場合には、ユーザの詳細表示画面で各項目について左右に二つの設定値が表示されるようになります。
左側の値はプロファイルによって本来設定される筈の値が表示されます。
また右側の値は個別設定によって設定されている値が表示されます。

・基本

変更

ユーザ基本情報プロファイルで設定される項目について個別設定をおこないたい場合にはユーザ基本情報プロファイルの行にある「編集」ボタンを押します。
編集画面が現れるので、個別設定したい内容を設定し、「設定」ボタンを押してください。

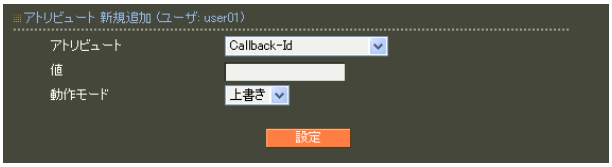
削除

個別設定を削除し、ユーザ基本情報プロファイルで設定された値に戻したいときには「削除」ボタンを押してください。

・認証
・応答

変更

認証アトリビュート、応答アトリビュートの個別設定は各アトリビュートの「新規追加」ボタン、または既存設定に対する「編集」ボタンでおこないます。
次のような設定画面が表示されます。



■アトリビュート新規追加（ユーザ :“ ユーザ ID ”）

○アトリビュート
個別に設定したいアトリビュートを選択します。
「編集」ボタンで設定画面を表示した場合には既に選択された状態で表示されます。

○値
アトリビュートの値を設定します。
選択したアトリビュートのフォーマットに合わせて入力してください。

○動作モード
「上書き」、「追加」、「削除」の中から選択します。
（※ 認証アトリビュートの場合は「追加」は選択できません。）

・上書き
プロファイルで同じアトリビュートが存在していた場合、プロファイルで設定されたアトリビュート値はこのユーザには適用されず、個別設定されたアトリビュート値のみが使われるようになります。

・追加
プロファイルで同じアトリビュートが存在していた場合、プロファイルで設定されたアトリビュート値と、個別設定されたアトリビュート値の両方がユーザに対して使われるようになります。
指定したアトリビュートがプロファイルに存在しない場合には、「上書き」と「追加」で動作に違いは有りません。

・削除
プロファイルで設定されたアトリビュートは本ユーザに対して適用されなくなります。「削除」を選択する場合には値は指定しないでください。

「設定」ボタンを押すと個別設定が適用されます。
個別設定で登録可能なアトリビュートの最大数は「付録 A 最大数一覧」を参照してください。

削除
個別設定したアトリビュートを削除する場合は削除したいアトリビュートの右側の「削除」ボタンを押してください。

ユーザが削除された場合、またはユーザに適用されるユーザプロファイルが変更された場合、そのユーザの個別設定は全て削除されます。
ユーザプロファイルでユーザ基本情報が変更された場合、そのユーザプロファイルが適用されているユーザのユーザ基本情報個別設定は削除されます。認証アトリビュート個別設定、応答アトリビュート個別設定についても同様です。

◆ユーザ証明書の発行

EAP-TLS 認証を使用する場合には、ユーザ毎に証明書を発行する必要があります。
証明書が未発行のユーザは、ユーザ一覧表示画面の証明書欄に「発行」ボタンが表示されます。
(※ CA が作成されていない場合には「発行」ボタンは表示されません。先に CA メニューで CA を設定してください。)

「発行」ボタンを押すと、次のユーザ証明書の作成画面が表示されます。

■証明書

○バージョン

X.509 のどのバージョンの証明書を発行するかを選択します。
バージョンは「１」または「３」を選択することができます。

○鍵長

RSA の鍵の長さを選択します。

・～ ver1.11.0
鍵の長さは「512」、「1024」、「2048」のいずれかを選択することができます。

・ver1.12.0 ～
鍵の長さは「1024」、「2048」のいずれかを選択することができます。
「512」、「1024」は十分安全とは言えません。
「2048」を推奨します。

○ Signature Algorithm

署名アルゴリズムを選択します。

・ver1.8.4 以前
「SHA-1」または「MD5」を選択することができます。

・ver1.8.5 ～ ver1.11.0
「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれかを選択することができます。

・ver1.12.0 ～
「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれかを選択することができます。
「SHA-1」、「MD5」は十分安全とは言えません。
「SHA-256」を推奨します。

○ Subject

・Common Name
ユーザ ID が自動的に設定されます。（ユーザプロファイルでグループ ID が指定されている場合にはグループ ID も付加されます。）
Common Name を変更することはできません。

入力欄には証明書プロファイルで設定されている内容が初期値として表示される他、パスフレーズにはユーザのパスワードが表示されます。以下の項目に入力をおこないます。

・email
ユーザのメールアドレスを設定します。

・Organizational Unit
一般には部署名を設定します。

・Organization
一般には企業名、組織名を設定します。

・Locality
市町村名を設定します。

・State or Province
都道府県名を設定します。

・Country
国名を設定します。
日本国内の場合は、「JP」とします。

各項目に使用可能な文字は以下となります。

・emai
0-9, a-z, A-Z, -.@_

・Organizational Unit/Organization/Locality/
State or Province/
ver1.8.4 以前: 0-9, a-z, A-Z, -_
ver1.8.5 以降: 0-9, a-z, A-Z, -_',.SPACE

・Country
A-Z

○有効期間
証明書有効期間の開始日時と終了日時を設定します。日時は GMT(グリニッジ標準時)で指定します。たとえば日本時間で 2006/12/31 23:59 まで有効にしたい場合には、”2006 年 12 月 31 日 14 時 59 分 ”と入力します。

■パスフレーズ
○パスフレーズ
パスフレーズを入力します。ユーザのパスワードが初期値として入力されています。パスフレーズは 5 文字以上 30 文字以下で入力してください。

パスフレーズにはユーザのパスワードが●●●●で表示されます。

■ X.509 証明書 v3 拡張（RFC3280）
下記設定項目は、X.509v3 がサポートしている拡張機能になりますが、認証アプリケーションに依存した項目となりますので、本設定に関しては認証されるアプリケーションの仕様を確認の上、設定をおこなってください。

以下に、それぞれのパラメータの説明を記します。

○ Key Usage
証明書に含まれている公開鍵の使用目的を示します。KeyUsage には以下の項目があります。

- digitalSignature
  デジタル署名の検証に利用できることを表しています。
- nonRepudiation
  否認防止を目的としたデジタル署名の検証に利用できることを表しています。
- keyEncipherment
  鍵を送信する場合に、鍵を暗号化して利用できることを表しています。
- dataEncipherment
  データの暗号化に利用できることを表しています。
- keyAgreement
  鍵交換で利用できることを表しています。
- keyCertSign
  証明書の署名の検証に利用できることを表しています。
- cRLSign
  失効リストの署名の検証に利用できることを表しています。
- encipherOnly
  keyAgreement が指定されている場合のみ有効で、鍵交換をデータの暗号化でのみ利用できることを表しています。
- decipherOnly
  keyAgreement が指定されている場合のみ有効で、鍵交換をデータの復号化でのみ利用できることを表しています。

○ Extended Key Usage
Key Usage より詳細に、証明書に含まれている公開鍵の使用目的を示します。
Extended Key Usage には以下の項目があります。

- serverAuth
  TLS サーバ認証に利用できることを表しています。
- clientAuth
  TLS クライアント認証に利用できることを表しています。
- codeSigning
  コード署名のために利用できることを表しています。
- emailProtection
  電子メールの保護のために利用できることを表しています。

○ CRL Distribution Points
失効リストの配布点を入力します。本装置から失効リストを配布することもできます。その場合は以下の URL を入力します。
http://(本装置のホスト名)/crl/crl.crl

■Netscape拡張

○nsCertType

Netscapeで使用される証明書のタイプを指定します。nsCertTypeには以下の項目があります。

- client
  クライアント認証に利用できることを表しています。
- server
  サーバ認証に利用できることを表しています。
- email
  S/MIMEのクライアント認証で利用できることを表しています。
- objsign
  Java等のオブジェクトサインで利用できることを表しています。
- sslCA
  SSL認証局で利用できることを表しています。
- emailCA
  S/MINE認証局で利用できることを表しています。
- objCA
  オブジェクトサイン認証局で利用できることを表しています。

○nsComment

Netscapeのコメントを示します。使用可能な文字は英数字およびハイフン(“-”)、アンダーバー(“_”)になります。

※この設定では、以下の項目が必須の設定項目になります。

- ○バージョン
- ○鍵長
- ○Signature Algorithm
- ○有効期間
  - ・終了日時
- ○パスフレーズ

※バージョン3のサーバ証明書を作成する場合には、通常最低限以下を指定するようにします。実際にどのKey Usage/Extended Key Usageが必須であるかは通信相手のソフトウェアに依存します。

- ○Key Usage
  - ・digitalSignature
  - ・keyEncipherment
- ○Extended Key Usage
  - ・serverAuth

既にプロファイルで設定されている項目についても修正を加えることができます。

各項目に入力後、「実行」ボタンを押すと証明書が発行されます。

◆ユーザ証明書の表示

既にユーザ証明書が発行されているユーザは、ユーザ一覧表示画面の証明書欄に「表示」ボタンが表示されます。
このボタンを押すと、そのユーザに対して発行されている全ての証明書が一覧表示されます。

この画面では次の操作がおこなえます。

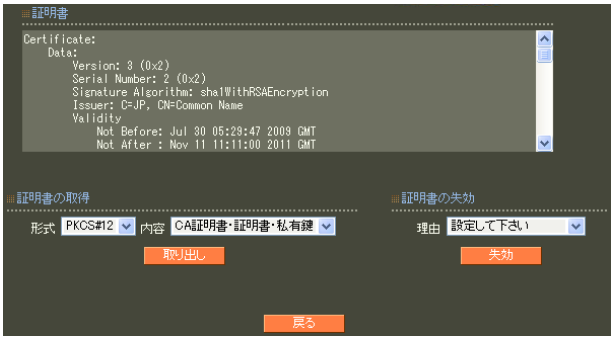
証明書の追加発行

このユーザに対して新しい証明書を発行します。
この後の操作は最初に証明書を発行する時と同じになります。

証明書の確認

「S/N」（シリアルナンバ）をクリックすることでその証明書の詳細内容を表示します。また、証明書の取得や失効などの操作をおこなうことができます。

「S/N」（シリアルナンバ）をクリックすると次の画面が表示されます。



この画面では次の操作がおこなえます。

■証明書の取得

ユーザ証明書を本装置からダウンロードします。
取り出す形式と内容を指定して「取り出し」ボタンを押します。

○形式

「PKCS#12」、「PEM」、「DER」から一つ選択します。

○内容

「CA 証明書・証明書・私有鍵」、「証明書・私有鍵」、「証明書」、「私有鍵」から一つ選択します。

※ PKCS#12 を選択した場合
　証明書と私有鍵のどちらか一方のみは選択できません。
※ PEM，DER を選択した場合
　証明書と私有鍵を同時に取り出すことはできません。それぞれ別々に取り出してください。

■証明書の失効

プルダウンメニューで失効理由を選択して、「失効」ボタンを押すと、証明書が失効します。
失効理由は以下の中から選択します。

- unspecified
  理由を指定しません。
- keyCompromise
  秘密鍵の漏洩などにより、証明書の信頼性がなくなったことを表します。
- CACompromise
  CAの信頼性がなくなったことを表します。
- affiliation Changed
  証明書の内容が変更されたことを表します。
- superseded
  証明書が取り替えられたことを表します。
- cessationOfOperation
  証明書がその目的では必要なくなったことを表します。
- removeFromCRL
  失効リストから削除されたことを表します。

30.AD ユーザ

Active Directory 連携を使用する場合にユーザプロファイルを指定します。
Active Directory 連携機能によって認証されたユーザは全て、ここで指定されたプロファイルが使われます。なお、プロファイルで記述された情報の中で、有効となるのは応答アトリビュート設定のみで、他の設定内容は使用されません。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ AD ユーザ

○ユーザプロファイル
使用するプロファイルを選択してください。

「設定」ボタンを押して設定完了です。設定はすぐに反映されます。

Active Directory 連携は EAP-PEAP 認証のみをサポートしているため、プロファイルでは認証方式が EAP-PEAP であるものを選択してください。
応答アトリビュートを使用しない場合には、「指定しない」を選択することもできます。

31.LDAP ユーザ

LDAP連携を使用する場合にユーザプロファイルを指定します。
LDAP連携機能によって認証されたユーザは全て、ここで指定されたプロファイルが使われます。
なお、プロファイルで記述された情報の中で、現バージョンで有効となるのは応答アトリビュート設定のみで、他の設定内容は使用されません。

プロファイルを設定したいLDAPサーバの「編集」ボタンを押すと、次の入力画面が表示されます。

■ LDAP ユーザ変更

◯ユーザプロファイル
使用するプロファイルを選択してください。
認証方式が PAP/CHAP、EAP-MD5、EAP-PEAP、EAP-TTLS/PAP,CHAP、EAP-TTLS/EAP-MD5 のいずれか(ver1.8.3 以前は、PAP/CHAP、EAP-TTLS/PAP,CHAP のいずれか)であるプロファイルを設定することが出来ます。

応答アトリビュートを使用しない場合には、「指定しない」を選択することもできます。

「設定」ボタンを押して設定完了です。設定はすぐに反映されます。

32. ユーザ管理者

本装置の全ての設定をおこなうことができる本装置管理者の他に、RADIUS のユーザ情報の設定管理のみをおこなえるユーザ管理者を設定することができます。

「新規追加」をクリックすると入力画面が表示されます。
ユーザ管理者のログイン ID とパスワードを入力します。

■ユーザ管理者新規追加

○ログイン ID
使用可能な文字は英数字および以下の記号と空白文字になります。

```
!"#$%&'()*+-./<=>?@[]^_`{|}~
```

○パスワード
使用可能な文字は、ログイン ID の入力可能文字と以下の記号になります。

```
,:;\
```

○ロック
通常は「ロックしない」を選択します。
一時的にユーザ管理者がログインできないように設定したい場合に、「ロックする」を選択するようにします。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
設定はすぐに反映されます。

設定可能なユーザ管理者の最大数は「付録 A 最大数一覧」を参照してください。

変更・削除
ユーザ管理者一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

33. フィルタ

本装置はパケットフィルタリング機能を搭載しています。フィルタ機能を使うと、本装置が受信するパケットに制限を加えることができます。

フィルタは以下の情報に基づいて条件を設定することができます。

- プロトコル(TCP/UDP/ICMP)
- 送信元 / 送信先 IP アドレス
- 送信元 / 送信先ポート番号

■デフォルト動作

送受信されるパケットが、下のフィルター覧のルールと全て一致しなかった場合のフィルタ動作が表示されています。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■デフォルト動作

○ accept
フィルタルールと一致しなかった時にパケットを通過させる場合に選択します。

○ drop
フィルタルールと一致しなかった時にパケットを破棄させる場合に選択します。

選択後「設定」ボタンをクリックして設定完了です。設定はすぐに反映されます。

デフォルトを「drop」に変更する場合には、フィルター覧で必要な通信が許可されていることを事前にご確認ください。特に本装置の設定画面へのアクセスがフィルタルールで許可されるように忘れずに設定してください。本装置が使用するポートには次のものがあります。

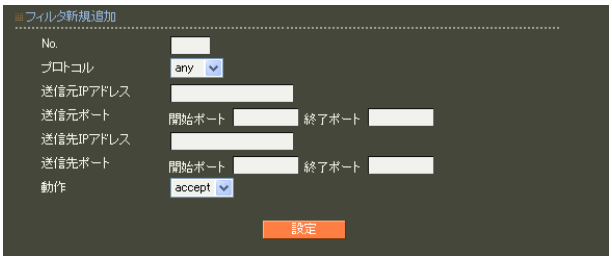
RADIUS認証ポート	UDP/(可変)
RADIUSアカウンティングポート	UDP/(可変)
二重化・設定情報の同期	TCP/802～809
NTP	UDP/123
管理画面へのアクセス(HTTP)	TCP/80
管理画面へのアクセス(HTTPS)	TCP/443
ルート確認	UDP/33435 ～33435+(ttl*3)
SNMP	UDP/161
SNMP trap	UDP/162
DNS	UDP/53
LDAP	TCP/(可変)
SYSLOG	UDP/514
DHCP	UDP/67

■フィルター覧

フィルタルールが一行ずつ表示されています。本装置に送受信されるパケットはこの一覧の各行と上から順に比較され、最初に一致した行の動作がパケットに対して適用されます。どの行とも一致しなかった場合にはデフォルト動作が適用されます。

「新規追加」ボタンを押すと入力画面が表示されます。

■フィルタ新規追加



○No.
この入力内容を登録する場所を指定します。
既に設定されているルールの最後にこのルールを追加する場合には、現在設定されているルールの数に１を加えた数を入力します。
既にルールが登録されている番号を指定した場合には、今回作成するルールがその番号で設定され、既存のルールの指定された番号から下のルールは番号が一つずつ後ろにずれます。

○プロトコル
フィルタリング対象とするプロトコルを「any」、「tcp」、「udp」、「icmp」の中から選択します。
「any」を選択した場合は任意のプロトコルとマッチします。

○送信元 IP アドレス
フィルタリング対象とする、送信元の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。

＜入力例＞
単一の IP アドレスを指定する：
192.168.253.19 （”/32”は付けない）
ネットワーク単位で指定する：
192.168.253.0/24

○送信元ポート
フィルタリング対象とする、送信元のポート番号を入力します。
開始ポートと終了ポートを指定することで、その間のポート番号範囲が指定されます。

特定のポート番号のみを指定する場合は開始ポートと終了ポートに同じポート番号を入力するか、開始ポートのみを指定して終了ポートを空欄にしてください。
ポート番号を指定するときは、プロトコルもあわせて選択する必要があります。
「icmp」または「any」のプロトコルを選択して、ポート番号を指定することはできません。

○送信先アドレス
フィルタリング対象とする、送信先の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。
入力方法は、送信元 IP アドレスと同様です。

○送信先ポート
フィルタリング対象とする、送信先のポート番号を入力します。
開始ポートと終了ポートで範囲を指定します。指定方法は送信元ポート同様です。

○動作
フィルタリング設定にマッチしたときにパケットを破棄するか通過させるかを選択します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
設定はすぐに反映されます。

設定可能なフィルタルールの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
フィルター覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

34.RADIUS 起動

■起動・停止
現在 RADIUS サーバが停止している場合には次の画面が表示されます。

RADIUS サーバが起動している場合には次の画面が表示されます。

RADIUS サーバの起動
RADIUS サーバが停止状態の時に、「起動する」ボタンをクリックする事で、RADIUS サーバは起動します。

メニュー「15.RADIUS- 基本情報」で、一つ以上の認証方式が選択されていない場合には、RADIUS サーバは起動しません。
また、メニュー「19.RADIUS- クライアント」でクライアントが一つも定義されていない場合には、RADIUS サーバは起動しません。

RADIUS サーバの停止
RADIUS サーバが起動状態の時に、「停止する」ボタンをクリックする事で、RADIUS サーバは停止します。

RADIUS サーバの再起動
RADIUS サーバの各種設定を変更した場合には再起動が必要です。RADIUS サーバが起動状態の時に、「再起動」ボタンをクリックする事で、RADIUS サーバのプロセスが再起動します。

起動途中および再起動途中に他の操作をおこなわないでください。

35. 設定の保存

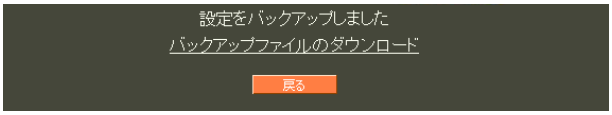
本装置の設定情報の保存をおこないます。

「設定の保存画面」にて設定情報を表示・更新する際、本装置のRSAの秘密鍵を含む設定情報等がHTTPSを使用しない場合ネットワーク上に平文で流れます。
設定の保存は、ローカル環境もしくはVPN環境等、セキュリティが確保された環境下でおこなう事をお勧めします。

■設定情報の保存

○文字コード
設定を保存するときは、文字コードを「EUC(LF)」「SJIS(CR+LF)」「SJIS(CR)」の中から選択してください。

「保存」ボタンを押すと、以下の画面が表示されます。



「バックアップファイルのダウンロード」のリンクから、設定をテキストファイルで保存してください。

保存したテキストファイルには、本装置の設定がすべて記述されています。
このテキストファイルの内容を直接書き換えて設定を変更することもできます。

また、設定ファイルの一番上には以下の情報が表示されますので、サポートへのお問い合わせの際にお伝えください。

・Version：
RAを表す文字列・バージョン番号・ビルド番号・ファームの作成日付

・Serial Number：
本装置のシリアル番号

・User：
設定ファイルを取り出したユーザ名

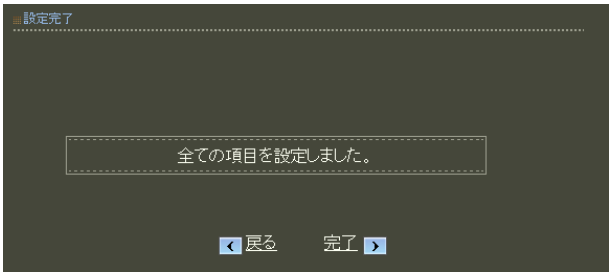
・Address：
設定ファイルを取り出したクライアントのIPアドレス

・Date：
設定ファイルを取り出した日時

36. 完了

ウィザード設定完了のメッセージが表示されます。
「完了」ボタンを押すとウィザードが終了し、通常のメニュー画面に移ります。

■設定完了



第5章

本装置管理者メニュー

画面構成

各設定項目毎に個別に設定をおこなう場合には
ウィザード以外のメニューを選択するようにします。

ウィザード以外のメニューアイコンをクリックすると以下のような画面が表示されます。

画面の上部には常に「RADIUS」「CA」「管理機能」「運用機能」「設定ウィザード」の５つのボタンが表示されています。上部のボタンをクリックすると、選択されたボタンに合わせたメニュー項目が画面左側に表示されます。この画面左側のメニューが表示される部分をメニューフレームと呼びます。メニューフレーム上のアイコンをクリックするとより詳細なメニュー項目が表示されます。

この最下層のメニューを選択することで、その項目の現在の設定内容が画面右側に表示されます。

次の章からは全メニュー項目について、この表示画面を基点として、設定方法と設定内容について説明します。なお、設定ウィザードについては４章で説明済みのため省略します。

画面構成

本装置管理者でログインした場合のメニュー階層は次のようになります。

RADIUS	サーバ	起動・停止
		基本情報
		二重化
		アトリビュート
		アドレスプール
		クライアント
		ActiveDirectory
		LDAP
		レルム(Ver 1.9.0以降のみ)
		ログ
	プロファイル	ユーザプロファイル
		ユーザ基本情報
		認証アトリビュート
		応答アトリビュート
		グループID
		証明書
	ユーザ	ユーザ
		AD ユーザ
		LDAP ユーザ
		ファイル読み込み
		ユーザ検索

CA	CA/CRL	
	証明書	

管理機能	ネットワーク	基本情報
		スタティックルート
		フィルタ
		DNS
		NTP
		SNMP
		DHCP(Ver 1.10.0以降のみ)
	システム	内蔵時計
		ログ
		設定情報の保存・復帰
		設定情報の初期化
		ファームのアップデート
		再起動
		停止
		管理者
		管理画面へのアクセス
		設定情報の同期

運用機能	ユーザ情報	ログイン情報
		ADユーザ情報
	ログ情報	システムログ
		オペレーションログ
		アクセスログ
		認証ログ
		アカウンティングログ
	ネットワークテスト	到達性確認
		ルート確認
		パケットキャプチャ
		名前解決確認
	システム情報	システム情報
		DHCPリース情報 (Ver 1.10.0以降のみ)
	サポート情報	サポート情報

設定ウィザード	RADIUS(EAP)	
	RADIUS(PAP/CHAP)	
	基本情報	
	ユーザ登録	
	設定情報の復帰	

第6章

RADIUS設定

Ⅰ．サーバ設定

1. 起動・停止

RADIUS のメニュー「サーバ」から「起動・停止」を選択します。

現在 RADIUS サーバが停止している場合には次の画面が表示されます。

RADIUS サーバが起動している場合には次の画面が表示されます。

RADIUS サーバの起動
RADIUS サーバが停止状態の時に、「起動する」ボタンをクリックする事で、RADIUS サーバは起動します。

メニュー「サーバ」の「基本情報」で、一つ以上の認証方式が選択されていない場合には、RADIUS サーバは起動しません。また、メニュー「サーバ」の「クライアント」でクライアントが一つも定義されていない場合には、RADIUS サーバは起動しません。

RADIUS サーバの停止
RADIUS サーバが起動状態の時に、「停止する」ボタンをクリックする事で、RADIUS サーバは停止します。

RADIUS サーバの再起動
RADIUS サーバの各種設定を変更した場合には再起動が必要です。RADIUS サーバが起動状態の時に、「再起動」ボタンをクリックする事で、RADIUS サーバのプロセスが再起動します。

起動途中および再起動途中に他の操作をおこなわないでください。

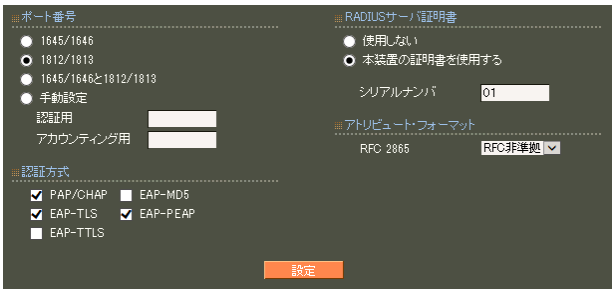
2. 基本情報

このメニューでは、ポート番号、認証方式、RADIUS サーバの証明書の指定など、RADIUS の基本的な情報の設定をおこないます。

RADIUS のメニュー「サーバ」から「基本情報」を選択すると、現在設定されている内容が表示されます。

「本装置の証明書を使用する」欄の「表示」ボタンは RADIUS サーバ証明書が設定されている場合にのみ表示されます。
このボタンを押すと証明書の内容が表示され、証明書の取得等ができます。
証明書の詳細については**「第 7 章 CA 設定 II. 証明書」**を参照してください。

基本情報の設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。



■ポート番号
RADIUS では、認証（Authentication）とアカウンティング（Accounting）の２つのポートを利用して、RADIUS クライアントとの通信をおこなっていますが、そのポート番号の設定をおこないます。
以下の４種類から選択します。

- 1645/1646
- 1812/1813
- 1645/1646、1812/1813 の双方
- 手動設定

手動設定の場合は、さらに使用したいポート番号を指定します。指定できるポート範囲は、1024 以上 60000 以下で、認証用とアカウンティング用で異なるポート番号を指定してください。

■認証方式
利用するユーザ認証方式の選択をおこないます。
本装置では、以下の５つの認証方式をサポートしています。

- PAP/CHAP
- EAP-MD5
- EAP-TLS
- EAP-PEAP
- EAP-TTLS

使用する認証方式のチェックボックスをチェックしてください。なお、「EAP-PEAP」または「EAP-TTLS」を選択する場合は、「EAP-TLS」も選択しておく必要があります。
また、「EAP-TTLS」を選択する場合には TTLS 内部認証で使う認証方式も同時に選択してください。

■ RADIUS サーバ証明書設定
認証で、「EAP-TLS」、「EAP-PEAP」または「EAP-TTLS」を選択した場合には、RADIUS サーバ証明書が必要となります。
証明書は事前に CA のメニューにて生成しておく必要があります（**「第 7 章 CA 設定 II. 証明書」**参照）。
証明書を作成した後、設定画面から「本装置の証明書を使用する」を選択して、作成した証明書のシリアルナンバを指定します。シリアルナンバは、16 進数で入力します。
有効期間内の証明書を設定して下さい。有効期間外の場合は認証に成功しないことがあります(サプリカントに依存します)。

Ⅰ．サーバ設定

■ アトリビュート・フォーマット
認証アトリビュートや応答アトリビュートなどに使用する際のアトリビュート・フォーマットを設定します。

「RFC 2865」の値を変更することで、
Callback-Number
Callback-Id
Called-Station-Id
Calling-Station-Id
NAS-Identifier
の各アトリビュートのフォーマットを変更できます。

「RFC 非準拠」にした場合、これらのフォーマットは、text（ASCII 文字列)として扱われます。
「RFC 準拠」にした場合は、これらのフォーマットは、string（バイナリデータ）になります。

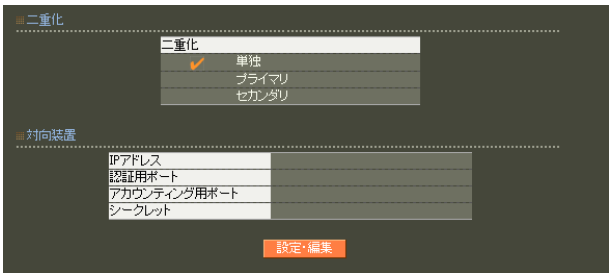
これらが
認証プロファイル
応答プロファイル
ユーザ個別設定（認証アトリビュート）
ユーザ個別設定（応答アトリビュート）
LDAP アトリビュートマップ
に使用されている場合、本設定値を変更することはできません。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。
保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。

3. 二重化

本装置は、２台構成にて、冗長化機能を持たせる事ができます。

RADIUS のメニュー「サーバ」から「二重化」を選択すると、現在設定されている内容が表示されます。



設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■二重化

○単独

本装置を単独で利用する場合に設定します。

○プライマリ

○セカンダリ

本装置を二重化構成で使用する場合には「プライマリ」または「セカンダリ」を指定します。

二重化構成を取る装置の片方を「プライマリ」に、もう一方を「セカンダリ」に設定してください。

■対向装置

二重化構成で使用する場合の、相手装置に関する情報を入力します。

○ IP アドレス

相手装置の IP アドレスを入力します。

○認証用ポート

○アカウンティング用ポート

○シークレット

相手装置の設定内容と一致するように入力します。

最大 30 文字まで入力することが可能で、使用可能な文字は英数字と空白文字および以下の記号です。

```
!#$%&'()*+,-./:;<=>?@[]^_`{|}~
```

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。

二重化構成では、2 台の RA の時刻同期を行ってください。

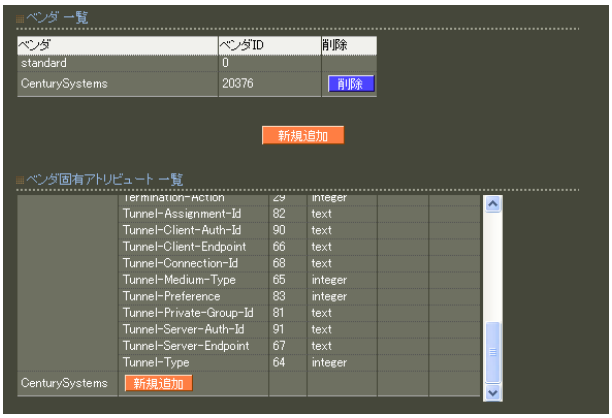
時刻同期には、NTP 機能を利用することが可能です。

二重化構成におけるファームウェア更新については、「付録 F 同期・二重化構成におけるファームウェア更新手順」を参照してください。

4. アトリビュート

RADIUS標準アトリビュート以外に、ベンダ固有アトリビュート(VSA)を使用したい場合に設定します。本メニューにて設定されたベンダ固有アトリビュートは、「プロファイル」メニューにて、認証に使用するアトリビュートとして指定したり、認証応答に付加されるVSA設定値の指定に使えるようになります。

RADIUS のメニュー「サーバ」から「アトリビュート」を選択すると、現在設定されている内容が表示されます。



■ベンダー覧
登録されているベンダの一覧が表示されます。

■ベンダ固有アトリビュート一覧
登録されているアトリビュートの一覧がベンダ毎に表示されます。良く使われる標準のアトリビュートについてはベンダ「standard」として定義されています。「standard」として定義されているアトリビュートについては新規作成や、編集、削除はできません。

先にベンダの追加をおこないます。
ベンダー覧の「新規追加」ボタンを押します。

■ベンダ新規追加

○ベンダ
追加したいベンダ名を入力します。最大 20 文字まで入力可能です。使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。

○ベンダ ID
ベンダ毎に割り当てられているベンダ ID を数値で入力します。

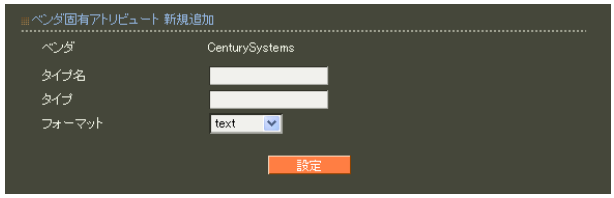
各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

設定可能なベンダの最大数は
「付録 A 最大数一覧」を参照してください。

削除
登録されているベンダを削除したい場合には「削除」ボタンを押すと削除されます。

ベンダ固有アトリビュートで使われているベンダは削除できません。

ベンダ固有アトリビュート一覧の中で、追加したいベンダの欄の「新規追加」ボタンを押すと入力画面が表示されます。



○ベンダ
選択されたベンダ名が表示されます。

○タイプ名
ベンダ固有アトリビュート用にベンダから指定されているタイプ名を指定します。最大 20 文字まで入力可能です。使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。

Ⅰ．サーバ設定

○タイプ
アトリビュート番号を指定します。
1～255 の整数値を入力してください。

○フォーマット
アトリビュートのデータ型をプルダウンから選択してください。以下の 5 種類から選択できます。

- text
  対象アトリビュートのデータ型が ASCII 文字列の場合に選択します。
- string
  対象アトリビュートのデータ型がバイナリデータの場合に選択します。
- address
  対象アトリビュートのデータ型が IP アドレス形式の場合に選択します。
- integer
  対象アトリビュートのデータ型が整数の場合に選択します。
- ipv6address
  対象アトリビュートのデータ型が IPv6 アドレス形式の場合に選択します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なベンダ固有アトリビュートの最大数は「付録 A 最大数一覧」を参照してください。

変更・削除
ベンダ固有アトリビュート一覧に登録されているアトリビュートを編集または削除したい場合にはアトリビュートが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

「プロファイル」メニューで使われているアトリビュートは削除できません。

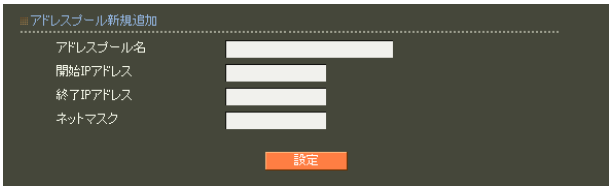
5. アドレスプール

端末に IP アドレスを割当てる場合に貸与する IP アドレスの領域を設定します。
本メニューにて設定されたアドレスプールを、次節の「クライアント」メニューまたは「プロファイル」メニューにて選択することで、実際の運用が可能になります。

RADIUS のメニュー「サーバ」から「アドレスプール」を選択すると、現在設定されている内容が表示されます。

「新規追加」をクリックすると入力画面が表示されます。

■アドレスプール新規追加



○アドレスプール名
任意の名前を 20 文字以内で入力します。
後に他のメニューでアドレスプールを割り当てる時に、ここで設定された名前が選択肢として表示されます。
使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。

○開始 IP アドレス
端末に貸与する IP アドレスの最初の IP アドレスを指定します。

○終了 IP アドレス
端末に貸与する IP アドレスの最後の IP アドレスを指定します。
開始 IP アドレスから終了 IP アドレスまでの間の IP アドレスがクライアントに貸与されます。

○ネットマスク
サブネットマスクの値を登録します。
ここで設定された値は、RADIUS アトリビュートの「Framed-IP-Netmask」の値となり、RADIUS クライアントに返信されます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なアドレスプールの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
アドレスプール一覧に登録されている設定を編集または削除したい場合には、そのアドレスプールが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

「クライアント」メニューまたは「プロファイル」メニューで使われているアドレスプールは削除できません。

6. クライアント

本装置にアクセス可能な RADIUS クライアントを設定します。

RADIUS のメニュー「サーバ」から「クライアント」を選択すると、現在設定されている内容が表示されます。

「新規追加」をクリックすると入力画面が表示されます。

■クライアント新規追加

○クライアント名
任意の名前を 20 文字以内で入力します。使用可能な文字は英数字およびハイフン(‘ - ’)、アンダーバー(‘ _ ’)になります。

○ IP アドレス
RADIUS クライアントの IP アドレスを入力します。

○シークレット
RADIUS クライアントとの認証や暗号処理に用いる文字列を入力します。RADIUS クライアント側でも同じ値が設定されている必要があります。
最大 30 文字まで入力することが可能で、使用可能な文字は英数字と空白文字および以下の記号です。

```
!#$%&'()*+,-./:;<=>?@[]^_`{|}~
```

○アドレスプール
端末に IP アドレスを割当てる場合に、アドレスプール名を選択します。
アドレスプールの選択肢には、前項の「アドレスプール」メニューで設定した名前が表示されます。
IP アドレスを本装置から割り当てない場合には「指定しない」を選択します。

アドレスプールは次節「プロファイル」の中で割り当てることもできます。ユーザ基本情報プロファイルの IP アドレス割り当てが指定されている場合、そのプロファイルを使用しているユーザへの IP アドレス割り当ては、プロファイル中の設定が優先して使われます。本メニューのアドレスプールは、ユーザ基本情報プロファイルの IP アドレス割り当てが「未使用」のユーザ、または、「固定」で設定されているユーザの内、固定 IP アドレスが指定されていないユーザにのみ適用されます。

本項のアドレスプールを設定して IP アドレスを割当てるためには、本装置で RADIUS クライアントとして設定したアドレスが NAS-IP-Address として Access-Request に含まれている必要があります。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。

設定可能なクライアントの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
クライアント一覧に登録されている設定を編集または削除したい場合には、そのアドレスプールが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

7.ActiveDirectory

ユーザ認証を Active Directory でおこないたい場合に設定します。
本設定をおこなうと、EAP-PEAP による認証要求を受けた場合に、設定された Active Directory サーバに問い合わせることで認証の可否を判断します。

RADIUS のメニュー「サーバ」から「Active Directory」を選択すると、現在設定されている内容が表示されます。

「設定・編集」ボタンを押すと入力画面が表示されます。

■ ActiveDirectory

Active Directory 連携機能を使用する場合に「使用する」を選択します。

○Active Directory サーバ
・1.8.13 以降
使用しません。
DNS を使用してドメインコントローラを自動的に検索します。
・1.8.12 以前
ドメインコントローラを FQDN または IP アドレスで指定します。

○ドメイン名
認証を受けるドメイン名を入力します。

○ドメイン名(Windows2000 より前)
ドメインに設定された NetBIOS名を設定します。
Windows サーバ上で「ドメイン名(Windows2000 より前)」や「ドメイン名(Windows2000 以前)」などの名前で参照できます。
「ドメイン名」の先頭パートと同一の場合は省略可能です。
最大 15 バイトまで入力可能です。
使用可能な文字は、英数字およびハイフン(-)、アンダーバー(_)です。

○所属グループ
認証を受ける所属グループ名を入力します。
空欄にするとグループ情報を用いずに認証をおこないます。

○管理者ユーザ ID
認証情報の確認をおこなうための ActiveDirectory のユーザアカウントを指定します。
このユーザは Administrators グループまたは AccountOperators グループに所属しているか、または同等の権利が与えられている必要があります。

○管理者パスワード
管理者ユーザ ID に対応したパスワードを入力します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。
保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。
RADIUS サーバの起動時に、RA はドメインに参加します。管理者ユーザ ID の権限で、Active Directory サーバにコンピュータアカウントを作成します。

Ⅰ．サーバ設定

Active Directory 連携機能を利用する際の注意

・Active Directory 連携機能を利用するためには、DNSの設定(管理機能メニューの「ネットワーク」-「DNS」)で所属するドメインのDNSサーバが設定されている必要があります。

・Active Directory サーバと本装置の時刻がずれている場合、Active Directory サーバとの連携ができないことがあります。

・ Active Directory サーバへの認証情報の問い合わせは、以下の手順で行われます。

(1) 認証要求に含まれるユーザ名 (User-Name) から最初の \ 以前を取り除く。
(2) (1) の結果に @ が含まれる場合、最後の @ より後ろの文字列がドメイン名(設定値)に一致していなければ問い合わせしない。(1.9.0 以降のみ)
(3) (1) の結果から最後の @ 以降を取り除く。(1.9.0 以降のみ)
(4) (3) の結果が空文字列であれば、問い合わせしない。(1.9.0 以降のみ)
(5) (3) の結果に \ が含まれていれば、問い合わせしない。(1.9.0 以降のみ)
(6) (3) の結果をユーザ名として Active Directory サーバへ問い合わせを行う。

・Active Directory 連携機能を有効にした場合、EAP-PEAP 認証では常に Active Directory サーバのユーザ情報が使用されます。LDAP 連携機能や本装置内に設定されたユーザ情報などは使われません。

・LDAP 連携機能において EAP-PEAP 認証を行う場合、Active Directory 連携機能と同時に使用することはできません。

Active Directoryサーバへの対応状況

Active Directoryサーバの各バージョンに対するRAの対応状況は以下の通りです。

Active Directoryサーバのversion	対応しているRAの version	
	RA-1200	RA-730
Windows Server 2012 R2	1.10.0	1.10.0
Windows Server 2012	1.10.0	1.10.0
Windows Server 2008 R2	1.8.9	1.8.3
Windows Server 2008	1.8.9	1.8.3

但し、全ての環境において Active Directory サーバとの連携を保証するものではありません。

Ⅰ．サーバ設定

8.LDAP

LDAP サーバと連携してユーザ認証をおこないたい場合に設定します。
PAP/CHAP、EAP-MD5、EAP-PEAP、EAP-TTLS/PAP、CHAP、EAP-TTLS/EAP-MD5 による認証要求を受けた場合に、設定された LDAP サーバを利用して認証の可否を判断することができます。

RADIUS のメニュー「サーバ」から「LDAP」を選択すると、現在設定されている内容が表示されます。

■ LDAP
LDAP サーバ連携使用の有無と、使用する場合の認証順序が表示されています。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ LDAP

○ LDAP
LDAP サーバ連携機能を使用する場合に「使用する」を選択します。

○認証順序
LDAP サーバ上のユーザ情報に基づく認証と、本装置上に登録されたユーザ情報に基づく認証のどちらを優先しておこなうかを指定します。
「Local → LDAP」を指定した場合、最初に本装置上で認証を試みます。そして認証要求されたユーザが本装置上に登録されていなかった場合に LDAP サーバ連携による認証をおこないます。
「LDAP → Local」の場合は逆に、LDAP 上のユーザ認証が最初におこなわれます。

選択後「設定」ボタンを押してください。LDAP サーバを使用する選択にした場合には続いて LDAP サーバの登録をおこなってください。

Ⅰ．サーバ設定

■LDAP アトリビュートマップ一覧

LDAP アトリビュートマップ機能を用いることで、LDAP サーバから応答アトリビュートを取得し、RADIUS クライアントに返すことが可能となります。応答アトリビュートはLDAPサーバでユーザ毎に設定します。
LDAPアトリビュートマップは、LDAPサーバ毎ではなく全体で共有されます。

設定可能な LDAP アトリビュートマップの最大数は「付録 A 最大数一覧」を参照してください。

設定情報の同期をおこなう設定の場合、本設定は対向装置へ同期されます。

「新規追加」ボタンを押すと入力画面が表示され、LDAP アトリビュートマップをひとつ作成することができます。
ここでは、LDAP サーバ上のアトリビュートから RADIUS 応答アトリビュートへの変換ルールの組を設定します。

■LDAP アトリビュートマップ新規追加

○ RADIUS アトリビュート
RADIUS アトリビュートを選択します。任意のアトリビュートを選択することができます。

○ LDAP アトリビュート
LDAP サーバへ問い合わせる際の検索フィルタアトリビュートを設定します。
各 LDAP サーバで設定された「ベース DN」や「フィルタアトリビュート」などと複合して LDAP サーバに問い合わせがおこなわれます。LDAP アトリビュートは「管理者ユーザ ID」の権限で読み出せる必要があります。

使用可能な文字は、下記の通りです。
0-9，a-z，A-z，-(0x2c)，_(0x5f)。
最大文字数は「40 (ver1.8.3以前は20)」で、デフォルト値はありません。

入力後に「設定」ボタンを押してください。

変更
既に設定されている LDAP アトリビュートマップのひとつを変更することができます。
RADIUS アトリビュートは編集することはできませんが、LDAP アトリビュートは変更可能です。

削除
既に設定されている LDAP アトリビュートマップのひとつを削除することができます。

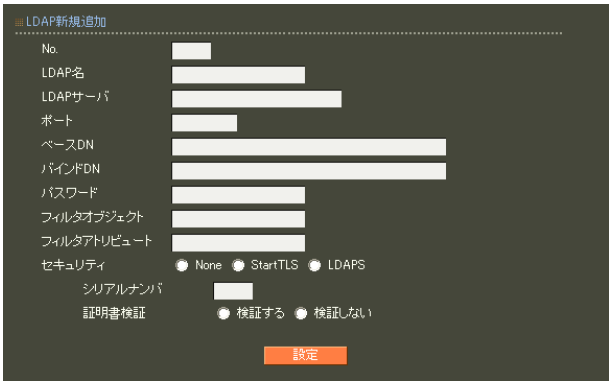
Ⅰ．サーバ設定

■ LDAP サーバー一覧

表示画面の下段には設定済みの LDAP サーバが一覧表示されています。1 番のサーバから順に LDAP による認証が試みられます。

「新規追加」ボタンを押すと入力画面が表示されます。

■ LDAP 新規追加



○ No.

この LDAP サーバの認証の順番を指定します。
空欄にした場合には既存の LDAP サーバ設定の最後に追加されます。既に LDAP サーバが登録されている番号を指定した場合には、今回作成する LDAP サーバがその番号で設定され、指定された番号から下の既存の LDAP サーバ設定が一つずつ後ろにずれて設定されます。

○ LDAP 名

識別用に任意の名前を 20 文字以内で入力します。

○ LDAP サーバ

LDAP サーバ名を FQDN または IP アドレスで指定します。

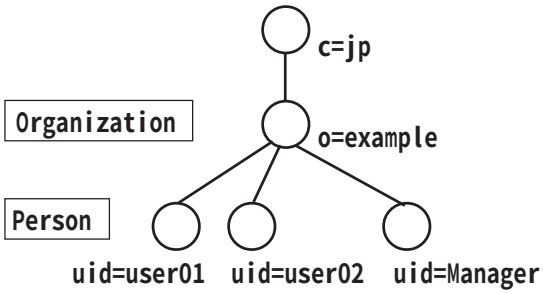
○ポート

LDAP サーバのポート番号を指定します。
指定できるポート範囲は、80，443，802 番を除く 1 ～ 1023 の範囲になります。
一般的には LDAP(StartTLS 含む)の場合には 389、LDAPS の場合には 636 が使われます。

○ベース DN

認証要求で送られたユーザ名を LDAP サーバに問い合わせる際の基点となるエントリの Distinguished Name を指定します。

＜入力例＞
o=example，c=jp



図：ディレクトリツリーの例

Ⅰ．サーバ設定

○バインド DN
認証要求で送られたユーザ名を LDAP サーバに問い合わせる際に用いるユーザの Distinguished Name を指定します。
ユーザの検索に必要なアクセス権が与えられている必要があります。
バインド DN が未設定の場合は、LDAP サーバに匿名アクセスを行います。

＜入力例＞
uid=Manager, o=example, c=jp

○パスワード
上記「バインド DN」に対応したパスワードを指定します。
バインド DN が未設定の場合(LDAP サーバに匿名アクセスを行う場合)は、設定しないで下さい。

○フィルタオブジェクト
使用しません。

○フィルタアトリビュート
認証要求で送られたユーザ名を LDAP サーバに問い合わせる際に、指定されたユーザ名に対応させる属性を指定します。

＜入力例＞
uid

LDAP サーバとして Active Directory を使用する場合には以下を指定するようにします。

sAMAccountName

○セキュリティ
LDAP サーバと通信をおこなう場合のセキュリティプロトコルを指定します。
「None」を指定した場合には通信が LDAP でおこなわれ、暗号化等はされません。
「StartTLS」「LDAPS」が指定された場合にはそれぞれのプロトコルに従って通信がおこなわれます。

○シリアルナンバ
セキュリティで「StartTLS」または「LDAPS」を選択した場合に、本装置が用いるクライアント証明書を指定します。
証明書はあらかじめ CA メニューの「証明書」で生成しておく必要があります(「第 7 章 CA 設定 II. 証明書」参照)。
使用する証明書のシリアルナンバを 16 進数で入力します。
有効期間内の証明書を設定して下さい。有効期間外の場合は認証に成功しないことがあります(LDAP サーバに依存します)。

○証明書検証
「StartTLS」または「LDAPS」使用時に LDAP サーバの証明書を検証するか否かを指定します。
検証するにした場合、LDAP サーバの証明書が不正であった場合にはその LDAP サーバは認証に使用しなくなります。
LDAP サーバ証明書の CN の値がサーバ名と異なっていた場合には不正な証明書とみなされます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。
保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。

設定可能な LDAP サーバの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
LDAP サーバー一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

Ⅰ．サーバ設定

LDAP 連携機能における認証について

LDAP サーバと連携してユーザ認証をおこなう方法は 3 種類あります(ver1.8.3 以前は 1 種類)。

(1) バインド(接続)
認証させたいユーザの権限で LDAP サーバにバインド(接続)できる場合に、PAP または EAP-TTLS/PAP で認証可能となります。

認証の可否は LDAP サーバが決定します。LDAP サーバでユーザにアクセス制限等が掛けられていれば認証に成功しません。

(2) 平文パスワード(ver1.8.4 以降のみ)
LDAP サーバの userPassword アトリビュートに、平文のパスワードが設定されていて、かつ RA に設定した管理者ユーザ ID の権限でその値が読み出せる場合に、CHAP、EAP-MD5、EAP-PEAP、EAP-TTLS/CHAP、EAP-TTLS/EAP-MD5 で認証可能となります。

LDAP サーバから読み出したパスワードの先頭に{CLEAR}または{CLEARTEXT}が付加されている場合、それらを無視します。
また、それらの大文字小文字は区別しません。{CLEAR}、{clear}、{Clear}などいずれの場合も無視します。

認証の可否は RA が決定します。LDAP サーバでユーザにアクセス制限等が掛けられていても、管理者ユーザ ID の権限でパスワードの読み出しが可能であれば認証に成功します。

(3) NTLM ハッシュ(ver1.8.4 以降のみ)
LDAP サーバに NTLM ハッシュが設定されていて、かつ RA に設定した管理者ユーザ ID の権限でその値が読み出せる場合に、EAP-PEAP で認証可能となります。

NTLM ハッシュとは、UTF-16LE でエンコードされたパスワードを MD4 を用いてハッシュした 16 バイトの値です。

LDAP サーバを RA と連携させるためには、sambaNTPassword アトリビュート、または csRANTLMHash アトリビュートのいずれかに、各ユーザの NTLM ハッシュが設定されている必要があります。
また、その値は 16 バイトのハッシュ値を 16 進数表記で表した 32 バイトの文字列でなければなりません。(例：00112233445566778899AABBCCDDEEFF)。大文字小文字どちらも使用可能です。

認証の可否は RA が決定します。LDAP サーバでユーザにアクセス制限等が掛けられていても、管理者ユーザ ID の権限で NTLM ハッシュの読み出しが可能であれば認証に成功します。

NTLM ハッシュが部外者に漏洩しないように注意して下さい。NTLM ハッシュを用いることで、ユーザ認証を不正に成功させることが可能です。

なお、EAP-PEAP 認証においては、NTLM ハッシュと平文パスワードの両方が設定されている場合には、NTLM ハッシュを使用します。

LDAP 連携機能を利用する際の注意

LDAP 連携機能において EAP-PEAP 認証を行う場合、Active Directory 連携機能と同時に使用することはできません。

Active Directory を LDAP サーバとして使用する場合、利用できる認証方式は PAP または EAP-TTLS/PAP のみです。

9. レルム(Ver 1.9.0 以降のみ)

RADIUS Proxy 機能（認証要求やアカウンティング要求を他のサーバに転送する機能）を使用したい場合に設定します。

本装置では、認証要求やアカウンティング要求に含まれるユーザ名（User-Name)の最後に現れる @ より後ろの文字列をレルムとして扱います。

受信した要求に含まれるレルムの値によって、要求を本装置で処理するか、他サーバへ転送するか(RADIUS Proxy)を選択することができます。

RADIUS のサーバメニューから「レルム」を選択すると、現在設定されている内容が表示されます。

「新規追加」をクリックすると、入力画面が表示されます。

■レルム新規追加

○レルム名
設定したいレルムを表す任意の名前を入力します。最大 20 文字まで入力可能です。使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。

○種別
設定するレルムの種別を「指定文字列」、「デフォルト」、「レルムなし」から選択します。
※「デフォルト」は任意のレルムを表します。いずれの「指定文字列」にも一致しなかった場合に適用されます。

○優先度
設定するレルムの適用順序を決めるための優先度を「1～9999」の整数で入力します。優先度の値が小さいレルム設定から順番に一致判定が行われます。
「種別」が「指定文字列」の場合のみ入力します。

※「種別」が「デフォルト」の場合は「64000」が、「レルムなし」の場合は「65000」が自動的に反映されます（変更不可）。

○指定文字列
設定するレルムの内容を表す文字列を入力します。最大 40 文字まで入力することが可能で、使用可能な文字は英数字およびハイフン(“ - ”)、ドット(“ . ”)になります。大文字・小文字の区別はしません。
※「指定文字列」選択時のみ入力必須

○一致条件
設定するレルムに一致するか判定するための条件を「完全一致」、「後方一致」から選択します。
※「指定文字列」選択時のみ入力必須

○動作
設定するレルムに一致した場合に行われる動作を選択します。要求を他サーバへ転送したい場合は「forward」を、本装置で処理する場合は「local」を選択します。

Ⅰ．サーバ設定

○転送先サーバ 1
転送先プライマリサーバを IP アドレス形式で入力します。
※「forward」選択時のみ入力必須

○認証ポート 1
転送先プライマリサーバの認証ポートを入力します。指定可能なポート番号は「1024 ～ 60000」の整数です。
※「forward」選択時のみ入力必須

○アカウンティングポート 1
転送先プライマリサーバのアカウンティングポートを入力します。指定可能なポート番号は「1024 ～ 60000」の整数です。
※「forward」選択時のみ入力必須

○シークレット 1
転送先プライマリサーバとの認証や暗号処理に用いる文字列を入力します。最大 30 文字まで入力することが可能で、使用可能な文字は英数字と空白文字および以下の記号です。

```
!#$%&'()*+,-./:;<=>?@[]^_`{|}~
```

※「forward」選択時のみ入力必須
転送先プライマリサーバ側でも同じ値が設定されている必要があります。

○転送先サーバ 2
転送先のセカンダリサーバを IP アドレス形式で入力します。※省略可

○認証ポート 2
転送先のセカンダリサーバの認証ポートを入力します。指定可能なポート番号は「1024 ～ 60000」の整数です。※省略可

○アカウンティングポート 2
転送先セカンダリサーバのアカウンティングポートを入力します。指定可能なポート番号は「1024 ～ 60000」の整数です。※省略可

○シークレット 2
転送先セカンダリサーバとの認証や暗号処理に用いる文字列を入力します。※省略可
最大 30 文字まで入力することが可能で、使用可能な文字は英数字と空白文字および以下の記号です。

```
!#$%&'()*+,-./:;<=>?@[]^_`{|}~
```

転送先セカンダリサーバ側でも同じ値が設定されている必要があります。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。

設定可能なレルムの最大数は
「付録 A 最大数一覧」を参照してください。

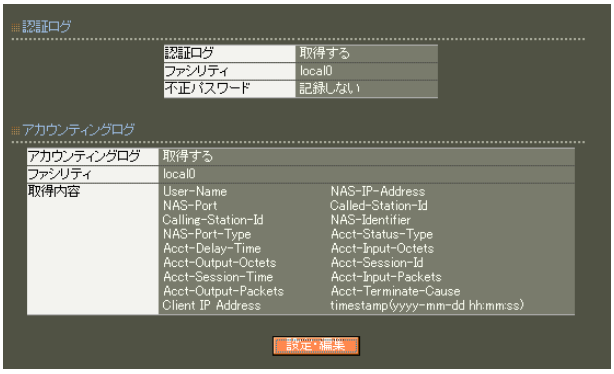
レルム設定は「設定情報の同期」の対象となります。親子連携との併用はできません。
※付録 G 親子連携参照

変更・削除
レルム一覧に登録されている設定を編集または削除したい場合には、そのレルムが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

10. ログ

RADIUS 関連のログについて、記録に残すログの種類を設定します。
なお、RADIUS 以外のログについては、管理機能のメニュー「システム」「ログ」の中で設定します。

RADIUS のサーバメニューから「ログ」を選択すると、現在設定されている内容が表示されます。



設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■認証ログ
○認証ログ
RADIUS によるユーザ認証に関する記録を残すかどうかを選択します。

○ファシリティ
認証ログを「取得する」にした場合、認証ログが出力されるファシリティを指定します。
プルダウンから選択してください。

○不正パスワード
「記録する」を選んだ場合、パスワードが正しくないことが原因で認証失敗した時に、認証要求に含まれるパスワードが認証ログに記録されます。
パスワードが記録されるのは、PAP または EAP-TTLS/PAP の場合に限られます。

■アカウンティングログ
○アカウンティングログ
RADIUS のアカウンティング記録を残すかどうかを選択します。

○ファシリティ
アカウンティングログを「取得する」にした場合、アカウンティングログが出力されるファシリティを指定します。
プルダウンから選択してください。

○取得項目
また、記録に残したい項目を選んで、チェックボックスをチェックします。
各項目は以下の内容となります。

- User-Name
  認証するユーザ名です。
- NAS-IP-Address
  アクセスサーバの IP アドレスです。
- NAS-Port
  アクセスサーバのポート番号です。
- Service-Type
  サービスの種類を表しています。
- Framed-Protocol
  PPP 等のプロトコルの種類を表しています。
- Framed-IP-Address
  ユーザに割り当てる IP アドレスです。
- Called-Station-Id
  NAS の電話番号、着信番号です。

Ⅰ．サーバ設定

・Calling-Station-Id
ユーザの電話番号、発信者番号です。

・NAS-Identifier
NAS の識別子です。RADIUS サーバが NAS を識別する為の文字列です。

・NAS-Port-Type
接続時のポートの種類を表しています。

・Acct-Status-Type
Start(接続開始)，Stop(接続終了)などのアカウンティングの種類を表しています。

・Acct-Delay-Time
遅延時間を表します。

・Acct-Input-Octets
受信したバイト数を表しています。

・Acct-Output-Octets
送信したバイト数を表しています。

・Acct-Session-Id
セッション ID を表しています。

・Acct-Authentic
RADIUS クライアントの認証方法を表しています。

・Acct-Session-Time
接続時間を表しています。

・Acct-Input-Packets
受信したパケット数を表しています。

・Acct-Output-Packets
送信したパケット数を表しています。

・Acct-Terminate-Cause
切断理由を表しています。

・client IP address
NAS のアドレスです。実際の送信元 IP アドレスです。
似た項目に、NAS-IP-Address がありますが、NAS-IP-Address は RADIUS サーバで NAS を一意に特定できればいいので、実際の送信元アドレスとは異なっている場合があります。

・timestamp(yyyy-mm-dd hh:mm:ss)
パケットを受信した時刻です。
「2004-10-31 19:05:20」のフォーマット
(2004 年 10 月 31 日 19 時 05 分 20 秒)です。

・timestamp(epoc time)
パケットを受信した時刻です。
1970-01-01 00:00:00 からの経過秒数です。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。
保存された設定内容を反映させるには、RADIUS サーバの再起動が必要になります。

「取得する」に設定したログは、管理機能のメニュー「システム」「ログ」の中で、本装置に記録するか、他の装置の syslog デーモンに転送するかを設定することができます。

II．プロファイル

本装置では、同じ内容の設定を複数ユーザに対して容易に設定できるようにするために、共通の設定内容をあらかじめプロファイルとして定義しておくことができます。

ユーザの追加変更をおこなう際には、このプロファイルを選択することで、ユーザ毎の入力を省略することができます。

プロファイルは、「ユーザ基本情報」、「認証アトリビュート」「応答アトリビュート」、「証明書」、「グループ ID」に分けて設定することができ、このプロファイルを組み合わせて「ユーザプロファイル」とします。
このユーザプロファイルを各ユーザの設定時に選択することで、ユーザ情報を素早く入力していくことができます。

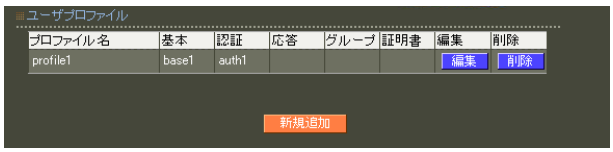
本メニューではこのプロファイルの設定をおこないます。

Ⅱ．プロファイル

1. ユーザプロファイル

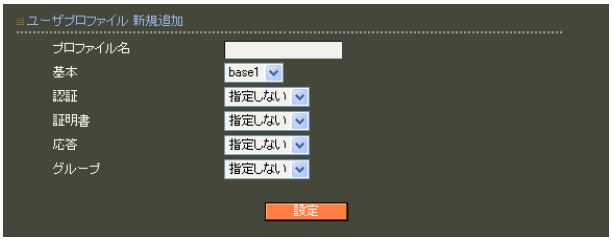
最終的にRADIUSの「ユーザ」メニューでユーザに適用することになる、大元のプロファイルです。このプロファイルは次節以降の「ユーザ基本情報」、「認証アトリビュート」「応答アトリビュート」、「証明書」、「グループ ID」の各プロファイルを選択することで生成します。
先に上記５つのプロファイルを作成した上で設定をおこなうようにしてください。

RADIUS のメニュー「プロファイル」から「ユーザプロファイル」を選択すると、現在設定されている内容が表示されます。



「新規追加」をクリックすると入力画面が表示されます。

■ユーザプロファイル新規追加



○プロファイル名
任意の名前を 20 文字以内で入力します。
後に「ユーザ」メニューでユーザの追加や編集をおこなう際に、ここで設定されたプロファイル名が選択肢として表示されます。
使用可能な文字は英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。(他のプロファイルも同様です。)

○基本　(ユーザ基本情報)
○認証　(認証アトリビュート)
○証明書
○応答　(応答アトリビュート)
○グループ　(グループ ID)
既に設定されている各プロファイルの名前が選択肢に表示されますので、割り当てたいプロファイルをそれぞれ選択します。
「ユーザ基本情報」以外のプロファイルについては、プロファイルを使用しない場合、「指定しない」を選択することもできます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なユーザプロファイルの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
アドレスプール一覧に登録されている設定を編集または削除したい場合には、そのアドレスプールが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

ユーザプロファイルの編集をおこなって設定を変更した場合、そのユーザプロファイルを使って定義されているユーザにも変更された設定が反映されます。

ユーザの設定に使われているユーザプロファイルは削除できません。
「ユーザ」メニューで設定を変更して、削除したいユーザプロファイルがどのユーザでも使われていないようにした後で、削除するようにしてください。

2. ユーザ基本情報

認証方式や IP アドレスの割り当て方式などを指定するプロファイルです。
ユーザ基本情報プロファイルは必ず一つ以上作成する必要があります。
このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ」メニューでユーザに適用されます。

RADIUS のメニュー「プロファイル」から「ユーザ基本情報」を選択すると、現在設定されている内容が表示されます。

「新規追加」をクリックすると入力画面が表示されます。

■ユーザ基本情報プロファイル新規追加

○プロファイル名
任意の名前を 20 文字以内で入力します。
「ユーザプロファイル」メニューでユーザ基本情報プロファイルを設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

○認証方式
ユーザ認証方式の選択をおこないます。
本装置では、以下の 7 つの認証方式をサポートしています。

- PAP/CHAP
- EAP-MD5
- EAP-TLS
- EAP-PEAP
- EAP-TTLS/PAP,CHAP
- EAP-TTLS/EAP-MD5
- EAP-TTLS/EAP-PEAP

選択した認証方式については、RADIUS のサーバメニューの「基本情報」でも選択されていることを確認してください。サーバメニューの「基本情報」で選択されていない認証方式については、本メニューで選択しても認証はおこなわれません。

○同時接続数
一人のユーザが同時に RADIUS サーバの認証を受けられる数を指定します。一人のユーザが同時に多数の接続をおこなうことを制限したい場合に用います。
設定可能な同時接続数は、「1」～「9」になります。また、空欄にした場合、同時接続数は無制限になります。

○ IP アドレス割り当て
ユーザ認証に成功した端末に対する IP アドレスの割り当て方法の設定です。
IP アドレス割り当てをおこなわない場合には「未使用」を選択します。
RADIUS クライアント装置が割り当てをおこなう場合には「RADIUS クライアント」を選択します。本装置のアドレスプールを利用して割り当てる場合には、「アドレスプール」を選択します。固定 IP アドレスをユーザ毎に割り当てる場合には、「固定」を選択してください。

○アドレスプール
IP アドレス割り当てで「アドレスプール」を選択した場合に、設定をおこないます。
サーバメニューの「アドレスプール」で設定した内容が選択肢に表示されますので、設定したいアドレスプールを選択します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なユーザ基本情報プロファイルの最大数は「付録 A 最大数一覧」を参照してください。

II．プロファイル

変更・削除

ユーザ基本情報プロファイル一覧に登録されている設定を編集または削除したい場合には、そのプロファイルが表示されている行の「編集」ボタン、「削除」ボタンを押すと実行できます。

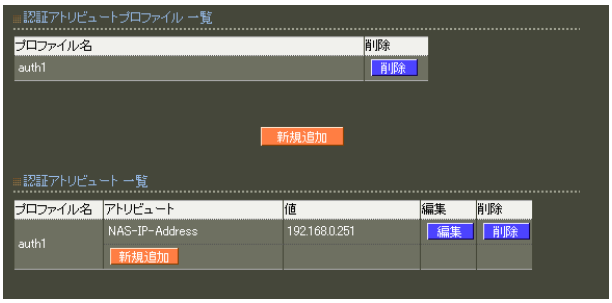
プロファイルの編集をおこなって設定を変更した場合、そのプロファイルを使って定義されているユーザにも変更された設定が反映されます。

ユーザプロファイルの設定に使われているユーザ基本情報プロファイルは削除できません。
「ユーザプロファイル」メニューで設定を変更してから削除するようにしてください。

3. 認証アトリビュート

認証時に認証方式に応じて送られるパスワードなどの情報に加え、RADIUS クライアントから送られてくるアトリビュートを認証に用いる場合に使用するプロファイルです。
このような認証をおこなわない場合には認証アトリビュートプロファイルを作成する必要はありません。
このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ」メニューでユーザに適用されます。

RADIUS のメニュー「プロファイル」から「認証アトリビュート」を選択すると、現在設定されている内容が表示されます。



■認証アトリビュートプロファイル一覧
登録されている認証アトリビュートプロファイルの一覧が表示されます。

■認証アトリビュート一覧
各認証アトリビュートプロファイルで定義されているアトリビュートの一覧が表示されます。

■認証アトリビュートプロファイル一覧
新たに認証アトリビュートプロファイルを追加する場合には、一覧から「新規追加」ボタンを押してプロファイルの追加をおこないます。

■認証アトリビュートプロファイル新規追加

○プロファイル名
任意の名前を 20 文字以内で入力します。
「ユーザプロファイル」メニューで認証アトリビュートプロファイルを設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

登録可能な認証アトリビュートプロファイルの最大数は「付録 A 最大数一覧」を参照してください。

削除
登録されているプロファイルを削除したい場合には一覧から「削除」ボタンを押すと削除されます。

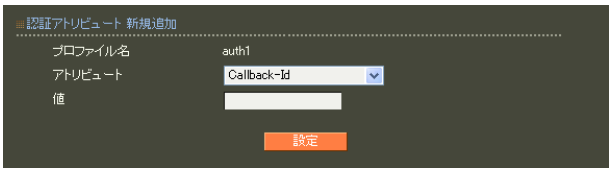
ユーザプロファイルの設定に使われている認証アトリビュートプロファイルは削除できません。
「ユーザプロファイル」メニューで設定を変更してから削除するようにしてください。

II．プロファイル

■認証アトリビュート一覧

認証アトリビュートプロファイルに対してアトリビュートの追加・編集・削除をおこないます。
アトリビュートを追加する場合には、追加したい認証アトリビュートプロファイルの表中に表示されている「新規追加」ボタンを押します。
以下の入力画面が表示されます。

■認証アトリビュート新規追加



○プロファイル名

選択したプロファイル名が表示されています。

○アトリビュート

ユーザ認証に使用するアトリビュートをプルダウンから選択します。
選択できるアトリビュートは、あらかじめ本製品で定義されてあるものの他、RADIUS の「サーバ」メニューのアトリビュートで追加したベンダ固有アトリビュートも使用できます。

○値

認証に使用するアトリビュートの値を定義します。
選択したアトリビュートのフォーマットに応じて次のように入力します。

・text(ASCII 文字列)
ASCII 形式の文字列を入力してください。設定可能な長さは、定義済みの standard のアトリビュートで最大 253 文字、追加したベンダ固有アトリビュートで最大 247 文字です。
入力例：century

・string(バイナリデータ)
16 進表記で入力してください。ただし、行頭に 0x は不要です。
設定可能な長さは定義済みの standard のアトリビュートで最大 253 オクテット(2 ～ 506 文字)、追加したベンダ固有アトリビュートで最大 247 オクテット(2 ～ 494 文字)です。
入力例：63656e74757279
(“ century ” の文字コードデータ)

・address(IP アドレス)
IPv4 アドレス表記で入力してください。
入力例：192.168.0.1

・integer(整数)
負ではない整数値を入力してください。
設定可能な範囲は 0 ～ 4294967295 です。
入力例：65536

・ ipv6address(IPv6 アドレス)
IPv6 アドレス表記で入力してください。
入力例：fe80::1111

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能な認証アトリビュートの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除

認証アトリビュート一覧に登録されている設定を編集または削除したい場合には、そのアトリビュートが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

プロファイルの編集をおこなって設定を変更した場合、そのプロファイルを使って定義されているユーザにも変更された設定が反映されます。

4. 応答アトリビュート

認証成功時に RADIUS クライアントに送るアトリビュートを指定するためのプロファイルです。指定するアトリビュートが無い場合には作成する必要はありません。このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ」メニューでユーザに適用されます。

RADIUS のメニュー「プロファイル」から「応答アトリビュート」を選択すると、現在設定されている内容が表示されます。

■応答アトリビュートプロファイル一覧
登録されている応答アトリビュートプロファイル名の一覧が表示されています。

■応答アトリビュート一覧
各応答アトリビュートプロファイルで定義されているアトリビュートの一覧が表示されています。

■応答アトリビュートプロファイル一覧
新たに応答アトリビュートプロファイルを追加する場合には、一覧から「新規追加」ボタンを押してプロファイルの追加をおこないます。

■応答アトリビュートプロファイル新規追加

○プロファイル名
任意の名前を 20 文字以内で入力します。
「ユーザプロファイル」メニューで応答アトリビュートプロファイルを設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

登録可能な応答アトリビュートプロファイルの最大数は「付録 A 最大数一覧」を参照してください。

削除
登録されているプロファイルを削除したい場合には一覧から「削除」ボタンを押すと削除されます。

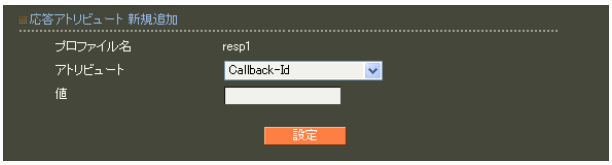
ユーザプロファイルの設定に使われている応答アトリビュートプロファイルは削除できません。
「ユーザプロファイル」メニューで設定を変更してから削除するようにしてください。

II．プロファイル

■応答アトリビュート一覧

応答アトリビュートプロファイルに対してアトリビュートの追加・編集・削除をおこないます。
アトリビュートを追加する場合には、追加したい応答アトリビュートプロファイルの表中に表示されている「新規追加」ボタンを押します。
以下の入力画面が表示されます。

■応答アトリビュート新規追加



○プロファイル名

選択したプロファイル名が表示されています。

○アトリビュート

RADIUS クライアントに送付するアトリビュートをプルダウンから選択します。
選択できるアトリビュートは、あらかじめ本製品で定義されてあるものの他、RADIUS の「サーバ」メニューのアトリビュートで追加したベンダ固有アトリビュートも使用できます。

○値

送付するアトリビュートの値を定義します。
選択したアトリビュートのフォーマットに応じて次のように入力します。

・text(ASCII 文字列)
ASCII 形式の文字列を入力してください。設定可能な長さは、定義済みの standard のアトリビュートで最大 253 文字、追加したベンダ固有アトリビュートで最大 247 文字です。
入力例：century

・string(バイナリデータ)
16 進表記で入力してください。ただし、行頭に 0x は不要です。
設定可能な長さは定義済みの standard のアトリビュートで最大 253 オクテット(2 ～ 506 文字)、追加したベンダ固有アトリビュートで最大 247 オクテット(2 ～ 494 文字)です。
入力例：63656e74757279
(“century”の文字コードデータ)

・address(IP アドレス)
IPv4 アドレス表記で入力してください。
入力例：192.168.0.1

・integer(整数)
負ではない整数値を入力してください。
設定可能な範囲は 0 ～ 4294967295 です。
入力例：65536

・ ipv6address(IPv6 アドレス)
IPv6 アドレス表記で入力してください。
入力例：fe80::1111

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能な応答アトリビュートの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除

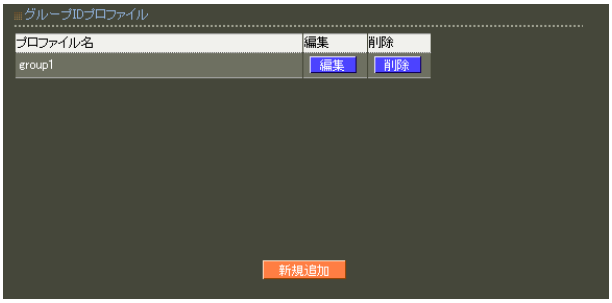
応答アトリビュート一覧に登録されている設定を編集または削除したい場合には、そのアトリビュートが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

プロファイルの編集をおこなって設定を変更した場合、そのプロファイルを使って定義されているユーザにも変更された設定が反映されます。

5. グループ ID

ユーザ ID を "user@centurysys.co.jp" または ”CENTURYSYS\user ”のように、所属グループを表わす文字列を付加して指定するためのプロファイルです。このようなユーザIDを利用しない場合には作成する必要はありません。このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ」メニューでユーザに適用されます。ユーザに適用した場合、そのユーザは、グループ IDも付加したユーザ名の形でのみ認証され、ユーザ ID単独での認証には失敗するようになります。

RADIUS のメニュー「プロファイル」から「グループ ID」を選択すると、現在設定されている内容が表示されます。



「新規追加」をクリックすると入力画面が表示されます。

■グループ ID プロファイル新規追加

○プロファイル名
任意の名前を 20 文字以内で入力します。
「ユーザプロファイル」メニューでグループ ID を設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

○グループ ID
ユーザ名に付加する文字列を指定します。
最大 40 文字まで指定できます。使用可能な文字は英数字およびハイフン(“ - ”)、ピリオド(“ . ”)になります。

○形式
グループ ID、ユーザ ID および区切り文字の結合の仕方を指定します。
UserID@GroupID または GroupID\UserID から選択します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なグループ ID プロファイルの最大数は「付録 A 最大数一覧」を参照してください。

変更・削除
グループ ID プロファイル一覧に登録されている設定を編集または削除したい場合には、そのプロファイルが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

プロファイルの編集をおこなって設定を変更した場合、そのプロファイルを使って定義されているユーザにも変更された設定が反映されます。

ユーザプロファイルの設定に使われているグループ ID プロファイルは削除できません。
「ユーザプロファイル」メニューで設定を変更してから削除するようにしてください。

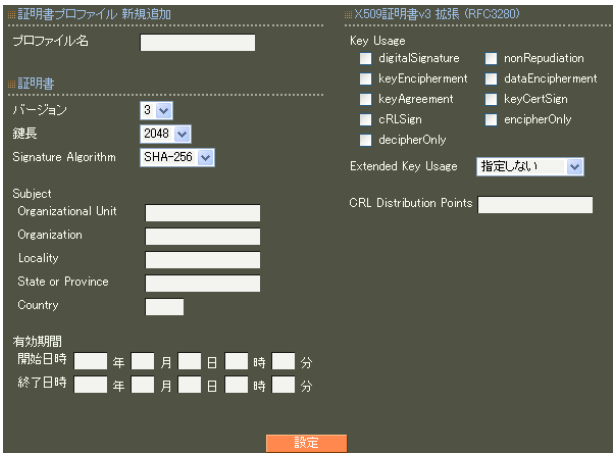
Ⅱ．プロファイル

6. 証明書

ユーザ証明書を発行する際の共通項目をあらかじめ指定するためのプロファイルです。
このプロファイルの作成は任意です。
このプロファイルはユーザプロファイルで他のプロファイルとまとめられた上で、「ユーザ」メニューでユーザに適用されます。

RADIUS のメニュー「プロファイル」から「証明書」を選択すると、現在設定されている内容が表示されます。

「新規追加」をクリックすると入力画面が表示されます。



■証明書プロファイル新規追加
○プロファイル名
任意の名前を 20 文字以内で入力します。

■証明書
○バージョン
X.509 のどのバージョンの証明書を発行するかを選択します。
バージョンは「1」または「3」を選択することができます。

○鍵長
RSA の鍵の長さを選択します。
・～ ver1.11.0
鍵の長さは「512」、「1024」、「2048」のいずれかを選択することができます。
・ver1.12.0 ～
鍵の長さは「1024」、「2048」のいずれかを選択することができます。
「512」、「1024」は十分安全とは言えません。
「2048」を推奨します。

○Signature Algorithm
署名アルゴリズムを選択します。
・ver1.8.4 以前
「SHA-1」または「MD5」を選択することができます。
・ver1.8.5 ～ ver1.11.0
「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれかを選択することができます。
・ver1.12.0 ～
「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれかを選択することができます。
「SHA-1」、「MD5」は十分安全とは言えません。
「SHA-256」を推奨します。

II．プロファイル

○ Subject
Subject には以下の項目があります。
- Organizational Unit
  一般には部署名を設定します。
- Organization
  一般には企業名、組織名を設定します。
- Locality
  市町村名を設定します。
- State or Province
  都道府県名を設定します。
- Country
  国名を設定します。
  日本国内の場合は、「JP」とします。

各項目に使用可能な文字は以下となります。
- Organizational Unit/Organization/Locality/ State or Province/
  ver1.8.4 以前: 0-9, a-z, A-Z, -_
  ver1.8.5 以降: 0-9, a-z, A-Z, -_',.SPACE
- Country
  A-Z

■有効期間
○開始日時
○終了日時
証明書有効期間の開始日時および終了日時を設定します。
設定できるのは 2005 年 - 2035 年の間になります。
日時は GMT(グリニッジ標準時)で指定します。
たとえば日本時間で 2006/12/31 23:59 まで有効にしたい場合には、”2006 年 12 月 31 日 14 時 59 分 ” と入力します。

※ この設定では、以下の項目が必須の設定項目になります。
○バージョン
○鍵長
○ Signature Algorithm

■ X.509 証明書 v3 拡張（RFC3280）
下記設定項目は、X.509v3 がサポートしている拡張機能になりますが、認証アプリケーションに依存した項目となりますので、本設定に関しては認証されるアプリケーションの仕様を確認の上、設定をおこなってください。

以下に、それぞれのパラメータの説明を記します。

○ Key Usage
証明書に含まれている公開鍵の使用目的を示します。
KeyUsage には以下の項目があります。
- digitalSignature
  デジタル署名の検証に利用できることを表しています。
- nonRepudiation
  否認防止を目的としたデジタル署名の検証に利用できることを表しています。
- keyEncipherment
  鍵を送信する場合に、鍵を暗号化して利用できることを表しています。
- dataEncipherment
  データの暗号化に利用できることを表しています。
- keyAgreement
  鍵交換で利用できることを表しています。
- keyCertSign
  証明書の署名の検証に利用できることを表しています。
- cRLSign
  失効リストの署名の検証に利用できることを表しています。
- encipherOnly
  keyAgreement が指定されている場合のみ有効で、鍵交換をデータの暗号化でのみ利用できることを表しています。
- decipherOnly
  keyAgreement が指定されている場合のみ有効で、鍵交換をデータの復号化でのみ利用できることを表しています。

○ Extended Key Usage
Key Usage より詳細に、証明書に含まれている公開鍵の使用目的を示します。Extended Key Usage には以下の項目があります。

- serverAuth
  TLS サーバ認証に利用できることを表しています。
- clientAuth
  TLS クライアント認証に利用できることを表しています。
- codeSigning
  コード署名のために利用できることを表しています。
- emailProtection
  電子メールの保護のために利用できることを表しています。

○ CRL Distribution Points
失効リストの配布点を入力します。本装置から失効リストを配布することもできます。その場合は以下の URL を入力します。

http://(本装置のホスト名)/crl/crl.crl

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能な証明書プロファイルの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
証明書プロファイル一覧に登録されている設定を編集または削除したい場合には、そのプロファイルが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

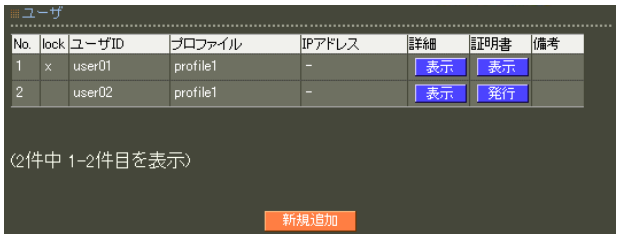
ユーザプロファイルの設定に使われている証明書プロファイルは削除できません。
「ユーザプロファイル」メニューで設定を変更してから削除するようにしてください。

III．ユーザ設定

1. ユーザ

ユーザの登録やユーザへのプロファイルの割り当てをおこないます。
ユーザ登録をおこなう場合には、先にメニュー「プロファイル」で、登録するユーザに合わせたユーザプロファイルを作成しておく必要があります。

RADIUS のメニュー「ユーザ」から「ユーザ」を選択すると、現在設定されているユーザー一覧が表示されます。



ユーザに関する各種設定やユーザ証明書に関する操作をこの画面からおこなうことができます。

ユーザー一覧表示画面から「新規追加」をクリックすると入力画面が表示されます。

■ユーザ新規追加
○ユーザ ID
登録するユーザ名を入力します。
ユーザ ID は、最大 20 文字まで入力する事が可能です。
使用可能な文字は英数字および以下の記号と空白文字になります。

```
!"#$%&'()*+-./<=>?@[]^_`{|}~
```

○パスワード
認証用パスワードを入力します。
パスワードは、最大 20 文字まで入力する事が可能です。
使用可能な文字は、ユーザ ID の入力可能文字と以下の記号になります。

```
,:;\
```

○プロファイル
このユーザに適用したいユーザプロファイルを選択します。「プロファイル」メニューで設定済みのユーザプロファイルが選択肢に表示されます。

■固定 IP アドレス払い出し
○ IP アドレス
固定のIPアドレスをユーザに払い出す場合に、端末に割り当てる IP アドレスを登録します。
ここで設定された値は、RADIUS アトリビュートの「Framed-IP-Address」の値となり、RADIUS クライアントに返信されます。
この設定を有効にするためにはユーザに割り当てられたユーザ基本情報プロファイルのIPアドレス割り当てが「固定」に設定されている必要があります。

○ネットマスク
払い出すサブネットマスクの値を登録します。
ここで設定された値は、RADIUS アトリビュートの「Framed-IP-Netmask」の値となり、RADIUS クライアントに返信されます。
この設定を有効にするためにはユーザに割り当てられたユーザ基本情報プロファイルのIPアドレス割り当てが「固定」に設定されている必要があります。

■備考
○備考
備考を設定することが出来ます。

備考は、最大 40 文字まで(日本語は 20 文字まで)
入力することができます。
使用可能な文字は次の通りです。

0 ～ 9、A ～ Z、a ～ z、空白文字、
-(マイナス・ハイフン)、.(ピリオド・ドット)、@、
日本語(JIS X 0208:1997 に収録された 6879 文字)

※いわゆる半角カナ(1バイトの片仮名)やいわゆる機種依存文字(例えば Shift_JIS の『丸付き数字』など)は使用できません。

■アカウントのロック
○ロック
ユーザ毎に「ロックしない」「ロックする」のいずれかを選択します。
デフォルト値は「ロックしない」です。
それぞれの動作は下記の通りになります。

- ロックしない
  - RADIUS 認証要求には、認証処理をおこなった結果を応答する
  - GUI へのアクセスを許可する
- ロックする
  - RADIUS 認証要求には、常に Reject を応答する
  - GUI へのアクセスを許可しない

「ロックする」を選択している場合はユーザー一覧の「lock」欄に『 x 』が表示されます。
設定情報の同期をおこなう設定の場合、本設定は対向装置へ同期されます。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

設定可能なユーザの最大数は
「付録 A 最大数一覧」を参照してください。

※ 認証方式がEAP-TLSの場合にはユーザ証明書のみを使って認証処理をおこないます。
ユーザ IDおよびパスワードは認証に使用しません。
また、認証時にはユーザ証明書の Subject の Common Name を使ってユーザ ID との対応を取り、参照するプロファイルを決定します。

III．ユーザ設定

◆ユーザの詳細表示

ユーザ一覧表示画面において、詳細欄の「表示」のボタンを押すとユーザの現在の設定内容が表示されます。

■ユーザ設定

現在設定されているユーザ設定情報が表示されます。

■ユーザ設定(詳細)

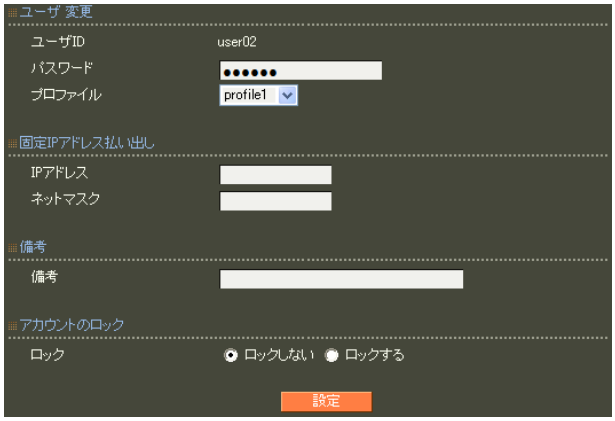
プロファイルの選択によって適用されている設定内容が表示されます。

■ユーザ設定

この画面からユーザの設定内容の編集、削除、およびユーザ個別設定をおこなうことができます。

編集

「編集」ボタンを押すとユーザ情報の編集画面が表示されます。



変更したい内容を入力して「設定」ボタンを押すと変更内容が反映されます。

削除

「削除」ボタンを押すと表示されているユーザが削除されます。

◆ユーザ個別設定

■ユーザ設定(詳細)

ユーザの詳細表示画面の下段に表示されている認証方式や応答アトリビュートなどは、本来ユーザに適用されているユーザプロファイルに従って設定され、ユーザに適用されます。
しかしプロファイルから外れた形でユーザ一人一人に対して個別に設定したい場合には、この詳細表示画面から個別に設定をおこなうことができます。個別設定は以下の各プロファイルで設定されている内容を上書きまたは追加する形でおこなわれます。

個別設定が可能なアトリビュート

- 基本
- 認証
- 応答

III．ユーザ設定

ユーザに個別設定がされている場合には、ユーザの詳細表示画面で各項目について左右に二つの設定値が表示されるようになります。
左側の値はプロファイルによって本来設定される筈の値が表示されます。また右側の値は個別設定によって設定されている値が表示されます。

・基本

変更

ユーザ基本情報プロファイルで設定される項目について個別設定をおこないたい場合にはユーザ基本情報プロファイルの行にある「編集」ボタンを押します。編集画面が現れるので、個別設定したい内容を設定し、「設定」ボタンを押してください。

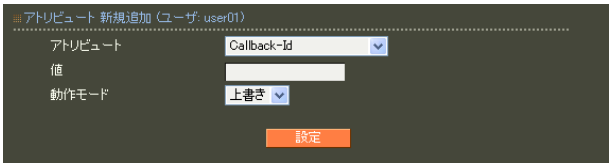
削除

個別設定を削除し、ユーザ基本情報プロファイルで設定された値に戻したいときには「削除」ボタンを押してください。

・認証
・応答

変更

認証アトリビュート、応答アトリビュートの個別設定は各アトリビュートの「新規追加」ボタン、または既存設定に対する「編集」ボタンでおこないます。次のような設定画面が表示されます。



■アトリビュート新規追加（ユーザ：“ユーザ ID”）

○アトリビュート

個別に設定したいアトリビュートを選択します。
「編集」ボタンで設定画面を表示した場合には既に選択された状態で表示されます。

○値

アトリビュートの値を設定します。選択したアトリビュートのフォーマットに合わせて入力してください。

○動作モード

「上書き」、「追加」、「削除」の中から選択します。（認証アトリビュートの場合は「追加」は選択できません。）

・上書き

選択した場合、プロファイルで同じアトリビュートが存在していた場合、プロファイルで設定されたアトリビュート値はこのユーザには適用されず、個別設定されたアトリビュート値のみが使われるようになります。

・追加

選択した場合、プロファイルで同じアトリビュートが存在していた場合、プロファイルで設定されたアトリビュート値と、個別設定されたアトリビュート値の両方がユーザに対して使われるようになります。指定したアトリビュートがプロファイルに存在しない場合には、「上書き」と「追加」で動作に違いは有りません。

・削除

選択した場合には、プロファイルで設定されたアトリビュートは本ユーザに対して適用されなくなります。「削除」を選択する場合には値は指定しないでください。

「設定」ボタンを押すと個別設定が適用されます。
個別設定で登録可能なアトリビュートの最大数は「付録 A 最大数一覧」を参照してください。

削除

個別設定したアトリビュートを削除する場合は削除したいアトリビュートの右側の「削除」ボタンを押してください。

ユーザが削除された場合、またはユーザに適用されるユーザプロファイルが変更された場合、そのユーザの個別設定は全て削除されます。
ユーザプロファイルでユーザ基本情報が変更された場合、そのユーザプロファイルが適用されているユーザのユーザ基本情報個別設定は削除されます。
認証アトリビュート個別設定、応答アトリビュート個別設定についても同様です。

III．ユーザ設定

◆ユーザ証明書の発行

EAP-TLS 認証を使用する場合には、ユーザ毎に証明書を発行する必要があります。
証明書が未発行のユーザは、ユーザ一覧表示画面の証明書欄に「発行」ボタンが表示されます。
(※ CA が作成されていない場合には「発行」ボタンは表示されません。先に CA メニューで CA を設定してください。)

「発行」ボタンを押すと、次のユーザ証明書の作成画面が表示されます。

■証明書

○バージョン

X.509 のどのバージョンの証明書を発行するかを選択します。
バージョンは「１」または「３」を選択することができます。

○鍵長

RSA の鍵の長さを選択します。

- ～ ver1.11.0
  鍵の長さは「512」、「1024」、「2048」のいずれかを選択することができます。
- ver1.12.0 ～
  鍵の長さは「1024」、「2048」のいずれかを選択することができます。
  「512」、「1024」は十分安全とは言えません。
  「2048」を推奨します。

○ Signature Algorithm

署名アルゴリズムを選択します。

- ver1.8.4 以前
  「SHA-1」または「MD5」を選択することができます。
- ver1.8.5 ～ ver1.11.0
  「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれかを選択することができます。
- ver1.12.0 ～
  「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれかを選択することができます。
  「SHA-1」、「MD5」は十分安全とは言えません。
  「SHA-256」を推奨します。

III．ユーザ設定

○ Subject

- Common Name
  ユーザ ID が自動的に設定されます。（ユーザプロファイルでグループ ID が指定されている場合にはグループ ID も付加されます。）
  Common Name を変更することはできません。

入力欄には証明書プロファイルで設定されている内容が初期値として表示される他、パスフレーズにはユーザのパスワードが表示されます。以下の項目に入力をおこないます。

- email
  ユーザのメールアドレスを設定します。
- Organizational Unit
  一般には部署名を設定します。
- Organization
  一般には企業名、組織名を設定します。
- Locality
  市町村名を設定します。
- State or Province
  都道府県名を設定します。
- Country
  国名を設定します。
  日本国内の場合は、「JP」とします。

各項目に使用可能な文字は以下となります。

- emai
  0-9, a-z, A-Z, -.@_
- Organizational Unit/Organization/Locality/ State or Province/
  ver1.8.4 以前: 0-9, a-z, A-Z, -_
  ver1.8.5 以降: 0-9, a-z, A-Z, -_',.SPACE
- Country
  A-Z

○有効期間

証明書有効期間の開始日時と終了日時を設定します。日時は GMT(グリニッジ標準時)で指定します。たとえば日本時間で 2006/12/31 23:59 まで有効にしたい場合には、”2006 年 12 月 31 日 14 時 59 分 ” と入力します。

■パスフレーズ

○パスフレーズ

パスフレーズを入力します。ユーザのパスワードが初期値として入力されています。パスフレーズは 5 文字以上 30 文字以下で入力してください。

パスフレーズにはユーザのパスワードが●●●●で表示されます。

■ X.509 証明書 v3 拡張（RFC3280）
下記設定項目は、X.509v3 がサポートしている拡張機能になりますが、認証アプリケーションに依存した項目となりますので、本設定に関しては認証されるアプリケーションの仕様を確認の上、設定をおこなってください。

以下に、それぞれのパラメータの説明を記します。

○ Key Usage
証明書に含まれている公開鍵の使用目的を示します。KeyUsage には以下の項目があります。

- digitalSignature
  デジタル署名の検証に利用できることを表しています。
- nonRepudiation
  否認防止を目的としたデジタル署名の検証に利用できることを表しています。
- keyEncipherment
  鍵を送信する場合に、鍵を暗号化して利用できることを表しています。
- dataEncipherment
  データの暗号化に利用できることを表しています。
- keyAgreement
  鍵交換で利用できることを表しています。
- keyCertSign
  証明書の署名の検証に利用できることを表しています。
- cRLSign
  失効リストの署名の検証に利用できることを表しています。
- encipherOnly
  keyAgreement が指定されている場合のみ有効で、鍵交換をデータの暗号化でのみ利用できることを表しています。
- decipherOnly
  keyAgreement が指定されている場合のみ有効で、鍵交換をデータの復号化でのみ利用できることを表しています。

○ Extended Key Usage
Key Usage より詳細に、証明書に含まれている公開鍵の使用目的を示します。
Extended Key Usage には以下の項目があります。

- serverAuth
  TLS サーバ認証に利用できることを表しています。
- clientAuth
  TLS クライアント認証に利用できることを表しています。
- codeSigning
  コード署名のために利用できることを表しています。
- emailProtection
  電子メールの保護のために利用できることを表しています。

○ CRL Distribution Points
失効リストの配布点を入力します。本装置から失効リストを配布することもできます。その場合は以下の URL を入力します。
http://(本装置のホスト名)/crl/crl.crl

■ Netscape拡張
○ nsCertType
Netscapeで使用される証明書のタイプを指定します。nsCertTypeには以下の項目があります。

- client
  クライアント認証に利用できることを表しています。
- server
  サーバ認証に利用できることを表しています。
- email
  S/MIMEのクライアント認証で利用できることを表しています。
- objsign
  Java等のオブジェクトサインで利用できることを表しています。
- sslCA
  SSL認証局で利用できることを表しています。
- emailCA
  S/MINE認証局で利用できることを表しています。
- objCA
  オブジェクトサイン認証局で利用できることを表しています。

○ nsComment
Netscapeのコメントを示します。使用可能な文字は英数字およびハイフン(‘ - ’)、アンダーバー(‘ _ ’)になります。

※この設定では、以下の項目が必須の設定項目になります。
- ○バージョン
- ○鍵長
- ○ Signature Algorithm
- ○有効期間
  - ・終了日時
- ○パスフレーズ

※バージョン3のサーバ証明書を作成する場合には、通常最低限以下を指定するようにします。実際にどのKey Usage/Extended Key Usageが必須であるかは通信相手のソフトウェアに依存します。
- ○ Key Usage
  - ・digitalSignature
  - ・keyEncipherment
- ○ Extended Key Usage
  - ・serverAuth

既にプロファイルで設定されている項目についても修正を加えることができます。

各項目に入力後、「実行」ボタンを押すと証明書が発行されます。

◆ユーザ証明書の表示

既にユーザ証明書が発行されているユーザは、ユーザ一覧表示画面の証明書欄に「表示」ボタンが表示されます。このボタンを押すと、そのユーザに対して発行されている全ての証明書が一覧表示されます。

この画面では次の操作がおこなえます。

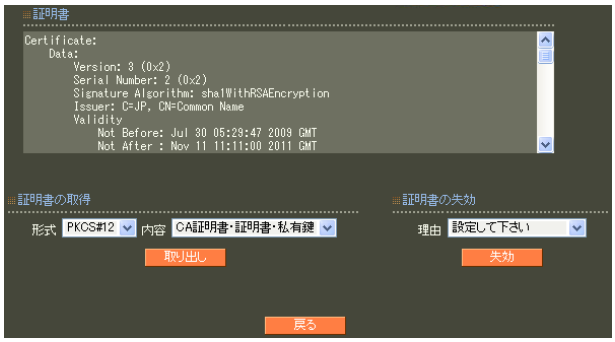
証明書の追加発行

このユーザに対して新しい証明書を発行します。
この後の操作は最初の証明書を発行する時と同じになります。

証明書の確認

「S/N」（シリアルナンバ）をクリックすることでその証明書の詳細内容を表示します。また、証明書の取得や失効などの操作をおこなうことができます。

「S/N」（シリアルナンバ）をクリックすると次の画面が表示されます。



この画面では次の操作をおこなうことができます。

■証明書の取得

ユーザ証明書を本装置からダウンロードします。
取り出す形式と内容を指定して「取り出し」ボタンを押します。

○形式

「PKCS#12」、「PEM」、「DER」から一つ選択します。

○内容

「CA 証明書・証明書・私有鍵」、「証明書・私有鍵」、「証明書」、「私有鍵」から一つ選択します。

※ PKCS#12 を選択した場合
　証明書と私有鍵のどちらか一方のみは選択できません。
※ PEM，DER を選択した場合
　証明書と私有鍵を同時に取り出すことはできません。それぞれ別々に取り出してください。

■証明書の失効

プルダウンメニューで失効理由を選択して、「失効」ボタンを押すと、証明書が失効します。
失効理由は以下の中から選択します。

- unspecified
  理由を指定しません。
- keyCompromise
  秘密鍵の漏洩などにより、証明書の信頼性がなくなったことを表します。
- CACompromise
  CAの信頼性がなくなったことを表します。
- affiliation Changed
  証明書の内容が変更されたことを表します。
- superseded
  証明書が取り替えられたことを表します。
- cessationOfOperation
  証明書がその目的では必要なくなったことを表します。
- removeFromCRL
  失効リストから削除されたことを表します。

失効した証明書は取得できません。

III．ユーザ設定

2.AD ユーザ

Active Directory 連携を使用する場合にユーザプロファイルを指定します。
Active Directory 連携機能によって認証されたユーザは全て、ここで指定されたプロファイルが使われます。なお、プロファイルで記述された情報の中で、現バージョンで有効となるのは応答アトリビュート設定のみで、他の設定内容は使用されません。

RADIUS のメニュー「ユーザ」から「AD ユーザ」を選択すると、現在設定されている内容が表示されます。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ AD ユーザ

○ユーザプロファイル
使用するプロファイルを選択してください。

「設定」ボタンを押して設定完了です。
設定はすぐに反映されます。

Active Directory 連携は EAP-PEAP 認証のみをサポートしているため、プロファイルでは認証方式が EAP-PEAP であるものを選択してください。
応答アトリビュートを使用しない場合には、「指定しない」を選択することもできます。

3.LDAP ユーザ

LDAP連携を使用する場合にユーザプロファイルを指定します。
LDAP連携機能によって認証されたユーザは全て、ここで指定されたプロファイルが使われます。なお、プロファイルで記述された情報の中で、現バージョンで有効となるのは応答アトリビュート設定のみで、他の設定内容は使用されません。

RADIUS のメニュー「ユーザ」から「LDAP ユーザ」を選択すると、現在設定されている内容が表示されます。

プロファイルを設定したい LDAP サーバの「編集」ボタンを押すと、次の入力画面が表示されます。

■ユーザ変更

◯ユーザプロファイル
使用するプロファイルを選択してください。
認証方式が PAP/CHAP、EAP-MD5、EAP-PEAP、EAP-TTLS/PAP,CHAP、EAP-TTLS/EAP-MD5 のいずれか(ver1.8.3 以前は、PAP/CHAP、EAP-TTLS/PAP,CHAP のいずれか)であるプロファイルを設定することが出来ます。
応答アトリビュートを使用しない場合には、「指定しない」を選択することもできます。

「設定」ボタンを押して設定完了です。設定はすぐに反映されます。

4. ファイル読み込み

ユーザをまとめて作成したい場合に使用します。
あらかじめユーザ作成に必要な情報をテキストファイルで用意しておき、本メニューで読み込ませることでユーザを一括作成します。
プロファイルやユーザ証明書も作ることができます。

RADIUS のメニュー「ユーザ」から「ファイル読み込み」を選択すると次の画面が表示されます。

■ RADIUS ユーザファイル読み込み

◯リセット
・する
既存の設定を消去してから読み込む場合に選択します。
「する」を選択した場合、設定済みの全プロファイルおよびユーザデータは削除されます。
またユーザ証明書は全て失効されます。

・しない
既存の設定に追加して読み込みたい場合に選択してください。

◯設定ファイル
作成したいユーザ情報が書かれているファイル名を指定します。
設定ファイルの書き方の詳細については「付録 C ユーザ設定情報のファイルフォーマット」を参照してください。
利用可能な文字コードは、「EUC-JP」または「Shift_JIS」です。

念のため、管理機能メニューの「システム」-「設定情報の保存・復帰」で現在の設定を保存してからファイル読み込みをおこなうことをお勧めします。

**設定ファイルの読み込み時には画面入力の場合と同様に入力チェックがおこなわれます。
例えば証明書のパスフレーズが 4 文字以下の場合にはエラーとなります。設定ファイルにエラーとなる情報が含まれていた場合、その行以降の内容は設定に反映されません。**

**RA 間で同期を行っている環境において、設定ファイルにエラーとなる情報が含まれていた場合、MASTER ではエラー以降の設定は反映されません(エラー以前の設定は反映されます)。
SLAVE ではエラー以前・以降全ての設定が反映されません。**

エラーが発生し、同期している RA 間の設定に差分が生じた場合は、強制同期などを使用して全ての RA の設定が同じになるようにして下さい。

詳細は『第 8 章 管理機能「10. 設定情報の同期」』や『付録 G 親子連携』を参照してください。

**一度に設定するユーザ数が多い場合やユーザ証明書を作成する場合には処理に時間がかかります。
途中で他のメニューを操作しないようにしてください。**

III．ユーザ設定

5. ユーザ検索

登録済みのユーザから条件に合うユーザを検索表示します。

RADIUS のメニュー「ユーザ」から「ユーザ検索」を選択すると検索画面が表示されます。

各検索条件を指定します。

■ユーザ条件

ユーザ ID、グループ ID、備考、およびロックを指定します。
ユーザ ID は、部分的な文字列を指定することでその文字列を含むユーザ ID を検索することができます。
ロックは、「指定しない」、「ロックされていない」、「ロックされている」を選択できます。
デフォルト値は「指定しない」です。

■プロファイル条件

検索に使用する「プロファイル名」を選択します。

■基本条件

ユーザ基本情報プロファイルで設定されている内容に基づいて、詳細に検索条件を指定することができます。

■アトリビュート条件

アトリビュート条件を指定する場合、認証アトリビュートで検索をするか応答アトリビュートで検索をするかを「種別」で指定します。
次に検索するアトリビュート名およびそのアトリビュートの値を指定します。値には部分的な文字列を指定することでその文字列を含むアトリビュートを検索することができます。
値を指定しなかった場合は選択したアトリビュート名が使われていれば値に関係なく検索されます。

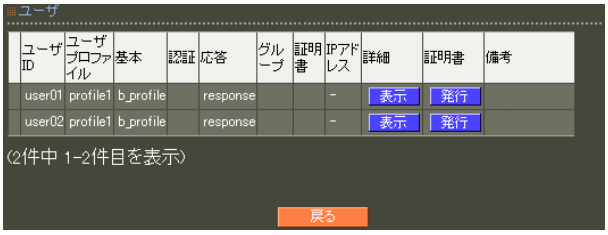
■証明書条件

ユーザ証明書に基づいた検索条件を指定します。
以下の選択肢の中から選択します。

- 指定しない
  証明書に基づいた検索条件を指定しません。
- 未発行
  証明書が発行されていないユーザを検索します。
- 無効
  証明書が発行されているが、失効または期限切れにより現在有効な証明書が無いユーザを検索します。
- 有効
  使用可能な証明書が発行されているユーザを検索します。
- 期限切れ間近
  1ヶ月以内に証明書の有効期限が切れるユーザを検索します。

III．ユーザ設定

検索条件を指定して「検索」ボタンを押すと、全ての条件と一致するユーザが一覧表示されます。1 ページあたり、100 件まで表示されます。



この画面から「ユーザ」メニュー同様、ユーザの編集、削除、および証明書の発行操作をおこなうことができます。

ユーザに個別設定がされていた場合には、個別設定された値に従って検索されます。

ユーザ条件の備考に日本語を使用した場合、検索にマッチしないはずのユーザが検索結果に表示されることがあります。

第7章

CA設定

Ⅰ．CA/CRL設定

CA/CRL

本装置のCAの設定をおこないます。
CAのメニュー「CA/CRL」を選択します。初期状態ではCAは設定されていません。
「新規追加」をクリックすると次の入力画面が表示されます。

■CA
○バージョン
証明書のバージョンを示します。V3固定です。

○鍵長
RSAの鍵の長さを選択します。
・～ ver1.11.0
鍵の長さは「512」、「1024」、「2048」のいずれかを選択することができます。
・ver1.12.0 ～
鍵の長さは「1024」、「2048」のいずれかを選択することができます。
「512」、「1024」は十分安全とは言えません。
「2048」を推奨します。

○Signature Algorithm
署名アルゴリズムを選択します。
・ver1.8.4以前
「SHA-1」または「MD5」を選択することができます。
・ver1.8.5 ～ ver1.11.0
「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれかを選択することができます。
・ver1.12.0 ～
「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれかを選択することができます。
「SHA-1」、「MD5」は十分安全とは言えません。
「SHA-256」を推奨します。

○Subject
Subjectには以下の項目があります。

・Common Name
CA Nameとして、認証局名称を設定します。

・email
認証局管理者のメールアドレス

・Organizational Unit
一般には部署名を設定します。

・Organization
一般には企業名、組織名を設定します。

・Locality
市町村名を設定します。

・State or Province
都道府県名を設定します。

・Country
国名を設定します。
日本国内の場合は、「JP」とします。

○有効期間
証明書有効期間（終了日時）を設定します。

■パスフレーズ
○パスフレーズ
パスフレーズは5文字以上30文字以下で入力してください。

Ⅰ．CA/CRL設定

■失効リスト更新間隔
○失効リスト更新間隔
失効リストの更新間隔日数を設定します。
0-4000日の間で指定します。

・ver1.9.2以降
0 を指定した場合、次の更新（Next Update）は、
CA 証明書の有効期間の終了日時になります。

第 7 章 CA 設定

Ⅰ．CA/CRL 設定

※ この設定では、以下の項目が必須の設定項目になります。

○バージョン(固定)
○鍵長
○ Signature Algorithm
○ subject
・Common Name
○有効期間
○パスフレーズ
○失効リスト更新間隔

また、各項目に使用可能な文字は以下となります。

・email
0-9，a-z，A-Z，-.@_

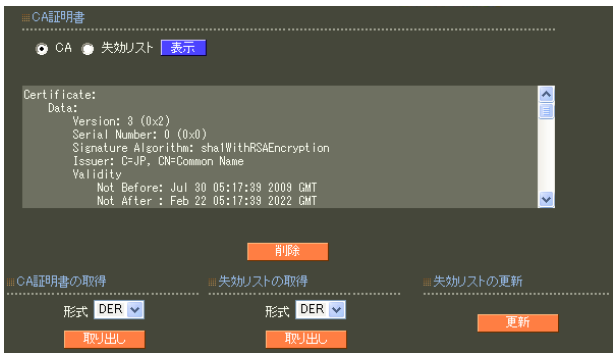
・Common Name
制御コードを除く任意の半角文字

・Organizational Unit/Organization/Locality/ State or Province/
ver1.8.4 以前: 0-9，a-z，A-Z，-_
ver1.8.5 以降: 0-9，a-z，A-Z，-_',.SPACE

・Country
A-Z

各項目に入力後、「設定」ボタンを押して CA 証明書を発行します。

CA の設定を一度おこなうと、以降、「CA/CRL」メニューを選択した場合、次の画面が表示されるようになります。



この画面では以下の操作をおこなえます。

■ CA 証明書

○ CA/ 失効リストの表示

画面上部にある「CA」/「失効リスト」の選択ボタンを選んで「表示」ボタンを押すと、CA の内容または失効リストの内容が表示されます。

○ CA の削除

「削除」ボタンを押すと本装置で設定した CA 証明書，CRL，各証明書を全て削除します。

※　設定情報の同期を設定している場合の注意

SLAVE で HTTPS サーバ証明書に「本装置の証明書」を設定している場合、SLAVE の CA の削除に失敗します。

CA の削除前に SLAVE の HTTPS サーバ証明書を変更して下さい。詳細については、「第 8 章 II. システム 9. 管理画面へのアクセス」を参照して下さい。

■ CA 証明書の取得

CA 証明書欄で「取り出し」ボタンをクリックすることにより CA 証明書を取り出すことができます。この際、取り出す形式を PEM または DER から選択することができます。

■失効リストの取得

失効リストの取得欄で「取り出し」ボタンをクリックすることにより CRL を取り出すことができます。

この際、取り出す形式を PEM または DER から選択することができます。

■失効リストの更新

失効リストの更新欄で「更新」ボタンをクリックすると CRL が最新のものに置き換えられます。

・ver1.10.0 以降

失効リスト更新間隔を、0-4000日の間で指定することができます。

デフォルト値は、CA証明書を発行した時に指定した値です。

0を指定した場合、次の更新（Next Update）は、CA証明書の有効期間の終了日時になります。

Ⅰ．CA/CRL設定

失効リストが、失効リストの更新間隔で決められた日時よりも古い場合には、証明書自体が有効であっても証明書の認証は拒否されます。
失効リスト更新間隔で決められた期間中に一度以上、失効リストの更新をおこなうようにしてください。
また、RADIUSサーバに新しい失効リストを認識させるには、RADIUS（サービス）を再起動する必要があります。

Ⅱ．証明書

証明書

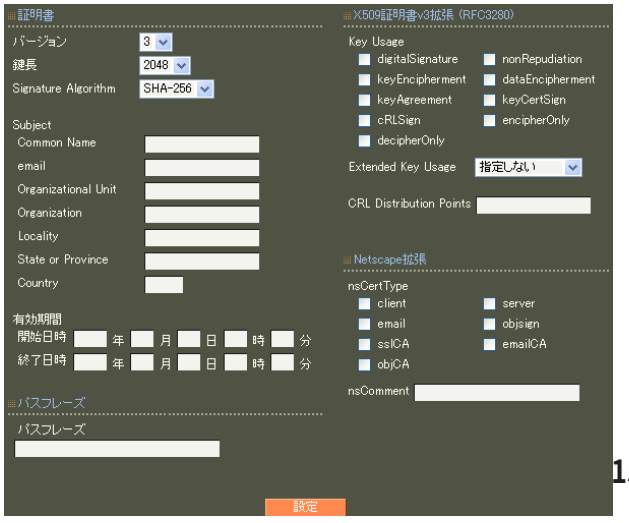
ユーザ証明書、サーバ証明書の作成をおこないます。
先に「CA/CRL」メニューでCAが設定されている必要があります。

CAのメニュー「証明書」をクリックすると、現在作成されている証明書が一覧表示されます。

表示条件を選択することができます。「全て」を選択した場合は、全ての証明書が表示されます。「未失効」を選択した場合は、未失効の証明書のみが表示されます。

証明書の作成や失効などの操作をこの画面からおこなうことができます。

証明書一覧表示画面から「新規追加」をクリックすると入力画面が表示されます。



■証明書

○バージョン

X.509のどのバージョンの証明書を発行するかを選択します。
バージョンは「１」または「３」を選択することができます。

○鍵長

RSAの鍵の長さを選択します。

・～ ver1.11.0
　鍵の長さは「512」、「1024」、「2048」のいずれかを選択することができます。
・ver1.12.0 ～
　鍵の長さは「1024」、「2048」のいずれかを選択することができます。
　「512」、「1024」は十分安全とは言えません。
　「2048」を推奨します。

○ Signature Algorithm

署名アルゴリズムを選択します。

・ver1.8.4以前
　「SHA-1」または「MD5」を選択することができます。
・ver1.8.5 ～ ver1.11.0
　「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれかを選択することができます。
・ver1.12.0 ～
　「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれかを選択することができます。
　「SHA-1」、「MD5」は十分安全とは言えません。
　「SHA-256」を推奨します。

○ Subject
Subjectには以下の項目があります。

- Common Name
  CA Nameとして、認証局名称を設定します。
- email
  認証局管理者のメールアドレス
- Organizational Unit
  一般には部署名を設定します。
- Organization
  一般には企業名、組織名を設定します。
- Locality
  市町村名を設定します。
- State or Province
  都道府県名を設定します。
- Country
  国名を設定します。
  日本国内の場合は、「JP」とします。

各項目に使用可能な文字は以下となります。

- E-mailAddress
  0-9, a-z, A-Z, -.@_
- Common Name
  制御コードを除く任意の半角文字
- Organizational Unit/Organization/Locality/
  State or Province/
  ver1.8.4以前: 0-9, a-z, A-Z, -_
  ver1.8.5以降: 0-9, a-z, A-Z, -_',.SPACE
- Country
  A-Z

○有効期間
証明書有効期間の開始日時と終了日時を設定します。日時はGMT(グリニッジ標準時)で指定します。たとえば日本時間で 2006/12/31 23:59 まで有効にしたい場合には、”2006年12月31日14時59分”と入力します。

■パスフレーズ
○パスフレーズ
パスフレーズは5文字以上30文字以下で入力してください。

■ X.509証明書v3拡張（RFC3280）
下記設定項目は、X.509v3がサポートしている拡張機能になりますが、認証アプリケーションに依存した項目となりますので、本設定に関しては認証されるアプリケーションの仕様を確認の上、設定をおこなってください。

以下に、それぞれのパラメータの説明を記します。

○ Key Usage
証明書に含まれている公開鍵の使用目的を示します。KeyUsageには以下の項目があります。

- digitalSignature
  デジタル署名の検証に利用できることを表しています。
- nonRepudiation
  否認防止を目的としたデジタル署名の検証に利用できることを表しています。
- keyEncipherment
  鍵を送信する場合に、鍵を暗号化して利用できることを表しています。
- dataEncipherment
  データの暗号化に利用できることを表しています。
- keyAgreement
  鍵交換で利用できることを表しています。
- keyCertSign
  証明書の署名の検証に利用できることを表しています。
- cRLSign
  失効リストの署名の検証に利用できることを表しています。
- encipherOnly
  keyAgreementが指定されている場合のみ有効で、鍵交換をデータの暗号化でのみ利用できることを表しています。
- decipherOnly
  keyAgreementが指定されている場合のみ有効で、鍵交換をデータの復号化でのみ利用できることを表しています。

○ Extended Key Usage
Key Usageより詳細に、証明書に含まれている公開鍵の使用目的を示します。
Extended Key Usageには以下の項目があります。

- serverAuth
  TLSサーバ認証に利用できることを表しています。
- clientAuth
  TLSクライアント認証に利用できることを表しています。
- codeSigning
  コード署名のために利用できることを表しています。
- emailProtection
  電子メールの保護のために利用できることを表しています。

○ CRL Distribution Points
失効リストの配布点を入力します。本装置から失効リストを配布することもできます。その場合は以下のURLを入力します。
http://(本装置のホスト名)/crl/crl.crl

■ Netscape拡張
○ nsCertType
Netscapeで使用される証明書のタイプを指定します。nsCertTypeには以下の項目があります。

- client
  クライアント認証に利用できることを表しています。
- server
  サーバ認証に利用できることを表しています。
- email
  S/MIMEのクライアント認証で利用できることを表しています。
- objsign
  Java等のオブジェクトサインで利用できることを表しています。
- sslCA
  SSL認証局で利用できることを表しています。
- emailCA
  S/MINE認証局で利用できることを表しています。
- objCA
  オブジェクトサイン認証局で利用できることを表しています。

○ nsComment
Netscapeのコメントを示します。使用可能な文字は英数字およびハイフン(" - ")、アンダーバー(" _ ")になります。

※ この設定では、以下の項目が必須の設定項目になります。
○バージョン
○鍵長
○ Signature Algorithm
○ Subject
- Common Name

○有効期間
○パスフレーズ

※ バージョン3のサーバ証明書を作成する場合には、通常最低限以下を指定するようにします。

○ Key Usage
- digitalSignature
- keyEncipherment

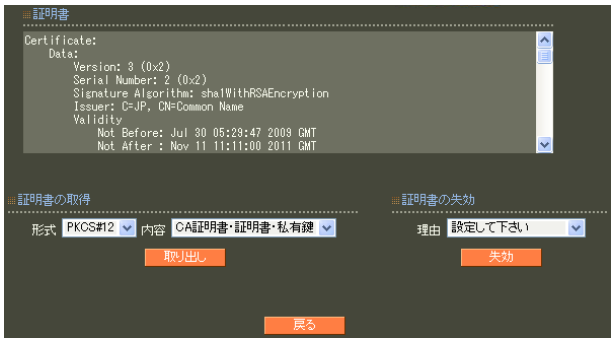
○ Extended Key Usage
- serverAuth

実際にどのKey Usage/Extended Key Usageが必須であるかは通信相手のソフトウェアに依存します。

各項目に入力後、「実行」ボタンを押して証明書を発行します。

発行可能な証明書の最大数は
「付録 A 最大数一覧」を参照してください。

証明書一覧表示画面において、「S/N」（シリアルナンバ）を押すと、次の証明書表示画面が表示されます。



この画面では次の操作がおこなえます。

■証明書の取得
証明書を本装置からダウンロードします。
取り出す形式と内容を指定して「取り出し」ボタンを押します。

○形式
「PKCS#12」、「PEM」、「DER」から一つ選択します。

○内容
「CA 証明書・証明書・私有鍵」、「証明書・私有鍵」、「証明書」、「私有鍵」から一つ選択します。

※ PKCS#12 を選択した場合
証明書と私有鍵のどちらか一方のみは選択できません。
※ PEM，DER を選択した場合
証明書と私有鍵を同時に取り出すことはできません。それぞれ別々に取り出してください。

■証明書の失効
プルダウンメニューで失効理由を選択して、「失効」ボタンを押すと、証明書が失効します。
失効理由は以下の中から選択します。

- unspecified
  理由を指定しません。
- keyCompromise
  秘密鍵の漏洩などにより、証明書の信頼性がなくなったことを表します。
- CACompromise
  CA の信頼性がなくなったことを表します。
- affiliation Changed
  証明書の内容が変更されたことを表します。
- superseded
  証明書が取り替えられたことを表します。
- cessationOfOperation
  証明書がその目的では必要なくなったことを表します。
- removeFromCRL
  失効リストから削除されたことを表します。

EAP-TLS 認証使用時に、失効させたクライアント証明書を RADIUS サーバに認識させるには、メニュー「CA/CRL」で失効リストの更新をおこなった上で RADIUS（サービス）を再起動する必要があります。

失効した証明書は取得できません。

第8章

管理機能

Ⅰ．ネットワーク

1. 基本情報

本装置の IP アドレスおよびデフォルトゲートウェイの設定をおこないます。

管理機能のメニュー「ネットワーク」から「基本情報」を選択すると、現在設定されている内容が表示されます。

（RA-730 の設定画面です。）

Ether0，Ether1，Ether2
(※ RA-1200 は、Ether0 と Ether1 のみです。)
インタフェースの設定を変更する場合は変更したいインタフェース欄の「編集」ボタンを押します。
次の入力画面が表示されます。

■基本情報

（RA-730 の設定画面です。）

○ IP アドレス
Ether ポートの IP アドレスとネットマスクを入力します。
ネットマスクは IP アドレスの後、’ / ’(スラッシュ)に続けてビット数表記で入力します。例えば、IP アドレスが 192.168.1.10 で、ネットマスクがドット区切り表記で 255.255.255.0 であれば以下のように入力します。

入力例）192.168.1.10/24

複数の Ethernet ポートに同一ネットワークに属するアドレスを 設定しないで下さい。正常に動作しないことがあります。

○ MTU
「Path-MTU-Black-HOLE」現象が発生した場合等は、ここの値を変更することで回避できます。
通常は初期設定の 1500Bytes のままで利用してください。

○通信モード
Ether ポートの通信速度・方式を選択します。
工場出荷設定では「自動」(オートネゴシエーション)となっていますが、必要に応じて通信速度・方式を選択してください。

デフォルトゲートウェイ
デフォルトゲートウェイ欄の「編集」ボタンを押すと次の入力画面が表示されます。

■基本情報

○デフォルトゲートウェイ
本装置のデフォルトゲートウェイとなる IP アドレスを入力してください。

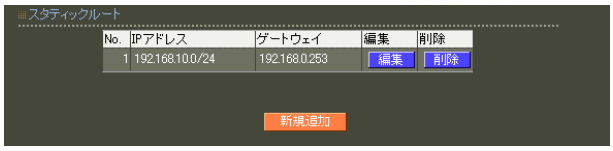
各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

本装置のインタフェースのアドレスを変更した後は、設定画面にアクセスしているコンピュータの IP 設定もそれにあわせて変更し、変更した IP アドレスの設定画面に再ログインしてください。

2. スタティックルート

本装置のスタティックルートの設定をおこないます。

管理機能のメニュー「ネットワーク」から「スタティックルート」を選択すると、現在設定されている内容が表示されます。



「新規追加」をクリックすると入力画面が表示されます。

■スタティックルート新規追加

○ IP アドレス
あて先ホストまたはネットワークの IP アドレスを入力します。
あて先の範囲をネットマスクで指定します。
ネットマスクは IP アドレスの後、’ / ’(スラッシュ)に続けてビット数表記で入力します。例えば、IP アドレスが 192.168.1.0 で、ネットマスクがドット区切り表記で255.255.255.0の範囲 であれば以下のように入力します。

入力例）192.168.1.0/24

ホストを指定する場合は ’ /32 ’ は付けずに IP アドレスで指定します。

入力例）192.168.1.1

○ゲートウェイ
IPアドレス欄で指定したアドレスへ送信するパケットを中継する、ルータのアドレスを入力します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
設定はすぐに反映されます。

設定可能なスタティックルートの最大数は「付録 A 最大数一覧」を参照してください。

変更・削除
スタティックルート一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

3. フィルタ

本装置はパケットフィルタリング機能を搭載しています。フィルタ機能を使うと、本装置が受信するパケットに制限を加えることができます。

フィルタは以下の情報に基づいて条件を設定することができます。

- プロトコル(TCP/UDP/ICMP)
- 送信元 / 送信先 IP アドレス
- 送信元 / 送信先ポート番号

管理機能のメニュー「ネットワーク」から「フィルタ」を選択すると、現在設定されている内容が表示されます。

■デフォルト動作

送受信されるパケットが、下のフィルター覧のルールと全て一致しなかった場合のフィルタ動作が表示されています。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■デフォルト動作

◯ accept

フィルタルールと一致しなかった時にパケットを通過させる場合に選択します。

◯ drop

フィルタルールと一致しなかった時にパケットを破棄させる場合に選択します。

選択後「設定」ボタンをクリックして設定完了です。

設定はすぐに反映されます。

デフォルトを「drop」に変更する場合には、フィルター覧で必要な通信が許可されていることを事前にご確認ください。特に本装置の設定画面へのアクセスがフィルタルールで許可されるように忘れずに設定してください。本装置が使用するポートには次のものがあります。

RADIUS認証ポート	UDP/(可変)
RADIUSアカウンティングポート	UDP/(可変)
二重化・設定情報の同期	TCP/802～809
NTP	UDP/123
管理画面へのアクセス(HTTP)	TCP/80
管理画面へのアクセス(HTTPS)	TCP/443
ルート確認	UDP/33435 ～33435+(ttl*3)
SNMP	UDP/161
SNMP trap	UDP/162
DNS	UDP/53
LDAP	TCP/(可変)
SYSLOG	UDP/514
DHCP	UDP/67

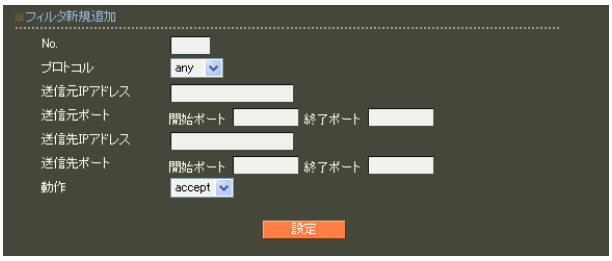
Ⅰ．ネットワーク

■フィルター一覧

フィルタルールが一行ずつ表示されています。
本装置に送受信されるパケットはこの一覧の各行と上から順に比較され、最初に一致した行の動作がパケットに対して適用されます。どの行とも一致しなかった場合にはデフォルト動作が適用されます。

「新規追加」ボタンをクリックすると入力画面が表示されます。

■フィルタ新規追加



○ No.
この入力内容を登録する場所を指定します。
既に設定されているルールの最後にこのルールを追加する場合には、現在設定されているルールの数に 1 を加えた数を入力します。
既にルールが登録されている番号を指定した場合には、今回作成するルールがその番号で設定され、既存のルールの指定された番号から下のルールは番号が一つずつ後ろにずれます。

○プロトコル
フィルタリング対象とするプロトコルを any、tcp、udp、icmp の中から選択します。any を選択した場合は任意のプロトコルとマッチします。

○送信元 IP アドレス
フィルタリング対象とする、送信元の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。
＜入力例＞
単一の IP アドレスを指定する：
192.168.253.19 （”/32”は付けない）
ネットワーク単位で指定する：
192.168.253.0/24

○送信元ポート
フィルタリング対象とする、送信元のポート番号を入力します。
開始ポートと終了ポートを指定することで、その間のポート番号範囲が指定されます。

特定のポート番号のみを指定する場合は開始ポートと終了ポートに同じポート番号を入力するか、開始ポートのみを指定して終了ポートを空欄にしてください。
ポート番号を指定するときは、プロトコルもあわせて選択する必要があります。
「icmp」または「any」のプロトコルを選択して、ポート番号を指定することはできません。

○送信先アドレス
フィルタリング対象とする、送信先の IP アドレスを入力します。ホストアドレスのほか、ネットワークアドレスでの指定が可能です。
入力方法は、送信元 IP アドレスと同様です。

○送信先ポート
フィルタリング対象とする、送信先のポート番号を入力します。
開始ポートと終了ポートで範囲を指定します。指定方法は送信元ポート同様です。

○動作
フィルタリング設定にマッチしたときにパケットを破棄するか通過させるかを選択します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
設定はすぐに反映されます。

設定可能なフィルタルールの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除
フィルター一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

4.DNS

本装置が使用する DNS の設定をおこないます。

管理機能のメニュー「ネットワーク」から「DNS」を選択すると、現在設定されている内容が表示されます。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ DNS

○プライマリサーバ
プライマリ DNS サーバの IP アドレスを入力します。

○セカンダリサーバ
セカンダリ DNS サーバの IP アドレスを入力します。

各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

5.NTP

本装置は、NTPクライアント/サーバ機能を持っています。
インターネットを使った時刻同期の手法の一つであるNTP(Network Time Protocol)を用いてNTPサーバと通信をおこない、時刻を同期させることができます。

管理機能のメニュー「ネットワーク」から「NTP」を選択すると、現在のサーバの状態と設定されている内容が表示されます。

■起動・停止
現在 NTP サーバが停止している場合には、「停止中」と表示されます。「起動」ボタンをクリックする事で NTP サーバが起動します。

NTP サーバが起動している場合には、「動作中」と表示されます。「停止」ボタンをクリックする事で NTP サーバは停止します。また、「再起動」ボタンをクリックすると NTP プロセスが再起動します。

■ NTP サーバ
設定されている NTP サーバが表示されています。
設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

○プライマリサーバ
プライマリ NTP サーバの IP アドレスもしくは FQDN を入力します。

○セカンダリサーバ
セカンダリ NTP サーバの IP アドレスもしくは FQDN を入力します。

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

保存された設定内容を反映させるには、NTP サーバの再起動が必要になります。
「再起動」ボタンを押してください。

基準 NTP サーバについて

基準となる NTP サーバには以下のようなものがあります。

- ntp1.jst.mfeed.ad.jp
- ntp2.jst.mfeed.ad.jp
- ntp3.jst.mfeed.ad.jp

6.SNMP

SNMP エージェントを起動すると、SNMP マネージャから本装置の MIB-II（RFC1213)の情報を取得することができます。

管理機能のメニュー「ネットワーク」から「SNMP」を選択すると、現在のサーバの状態と設定されている内容が表示されます。

■起動・停止
現在 SNMP が停止している場合には、「停止中」と表示されます。「起動」ボタンをクリックする事で SNMP が起動します。

SNMP が起動している場合には、「動作中」と表示されます。「停止」ボタンをクリックする事で SNMP サーバは停止します。また、「再起動」ボタンをクリックすると SNMP プロセスが再起動します。

■ SNMP サーバ
管理者が設定変更できる項目について、現在の設定内容が表示されています。
設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ SNMP

○コミュニティ名
任意のコミュニティ名を指定します。
ご使用の SNMP マネージャの設定に合わせて入力してください。

○本装置の名称
本装置の管理上の名前を入力します。通常 FQDN などを指定します。

○本装置の説明
本装置についての説明を入力します。

○本装置の設置場所
本装置の物理的な設置場所を指定します。

○本装置の管理者
本装置管理者への連絡先などを指定します。

○ Trap 送信先 1 ～ 5
Trap の送信先（SNMP マネージャ）の IP アドレスを設定します。
デフォルト値はありません。
未設定の場合は trap の送信はしません。
最大 5 個まで設定可能です。

○ CPU 使用率閾値
CPU 使用率の閾値を設定します。
単位は%で、有効な値は 10 以上 100 未満の整数となります。
デフォルト値はありません。
設定されない場合は、対応する trap は送信されません。
CPU 使用率は、設定内容及びご利用状況によって変わります。
運用中の実際の使用率を元に、適当と思われる閾値を設定してください。

○メモリ空き容量閾値
メモリ 空き容量の閾値を設定します。
単位は kB で、有効な値は 1 以上の整数となります。
デフォルト値はありません。
設定されない場合は、対応する trap は送信されません。
メモリ空き容量については別項(後述)を参照して下さい。

メモリ空き容量は設定及びご利用状況によって変わります。
運用中の実際の空き容量を元に、適当と思われる閾値を設定してください。

各項目に使用可能な文字は以下となります。
・コミュニティ名、本装置の説明、本装置の設置場所
　0-9, a-z, A-Z, -, _
・本装置の名称
　0-9, a-z, A-Z, -, _, .
・本装置の管理者
　0-9, a-z, A-Z, -, _, @, <, >, .

各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。

保存された設定内容を反映させるには、SNMP サーバの再起動が必要になります。
「再起動」ボタンを押してください。

メモリ空き容量
RA では、データの読み出し / 書き込み時にメモリをキャッシュという形で確保します。
一度キャッシュとして確保したデータは、メモリを介して処理が行われるため高速に動作します。
新たなデータの読み出し / 書き込み要求によりメモリ領域が必要とならない限り、キャッシュは解放されません。
(※ 1.8.12 以降)
メモリ空き容量(csRASystemMemoryFree)には、このキャッシュが含まれます。
(※ 1.8.11 以前)
メモリ空き容量(csRASystemMemoryFree)には、このキャッシュは含まれません。
したがって、連続して運用を続けると、メモリ空き容量(csRASystemMemoryFree)は逓減します。

Ⅰ．ネットワーク

SNMP trap

ユーザが設定した SNMP マネージャに SNMP trap を送信します。
送信される trap は以下の通りです。

・SNMP サービスを起動した時

Cold Start trap を送信します。

・CPU 使用率がユーザ定義の閾値を超えた時
・CPU 使用率がユーザ定義の閾値以下になった時

CPU 使用率を一定時間毎(1 秒)に測定します。
前回の測定値が閾値以下で、今回の測定値が閾値より大きい場合に trap を送信します。
測定値が閾値より大きくなったことがあり、その後の測定値が一定回数(10 回)だけ連続して閾値以下の場合に trap を送信します。
SNMP サービス起動直後に閾値より大きい場合は trap を送信します。
閾値以下の場合は送信しません。

・メモリ空き容量がユーザが定義した閾値より小さくなった時
・メモリ空き容量がユーザが定義した閾値以上になった時

メモリ空き容量を一定時間毎(1 秒)に測定します。
前回の測定値が閾値以上で、今回の測定値が閾値より小さい場合に trap を送信します。
測定値が閾値より小さくなったことがあり、その後の測定値が一定回数(10 回)だけ連続して閾値以上の場合に trap を送信します。
SNMP サービス起動直後に閾値より小さい場合は trap を送信します。
閾値以上の場合は送信しません。

・Ethernet インタフェースが link down した時
・Ethernet インタフェースが link up した時

Ethernet インタフェースの link up/down に応じて trap を送信します。
SNMP サービス起動直後に link down ならば trap を送信します。
link up ならば送信しません。

・電源の状態が変わった時 （※ RA-1200 のみ）

電源ユニットへの通電がなくなったり、電源ユニット自体が故障したりなど、注意が必要な状態になった場合に trap を送信します。
また、注意が必要な状態から正常な状態に戻った場合にも trap を送信します。

・RAID の状態が変わった時 （※ RA-1200 のみ）

RAID で障害が発生した場合、リビルドが始まった場合、リビルドが終了した場合に trap を送信します。

Ⅰ．ネットワーク

CPU やメモリ、電源、RAID の状況は、GetRequest などで取得できます。

例:

```
$ snmpwalk -v2c -c public 192.168.0.254 centurysys
   CS-RA-PRODUCT-MIB::csRASystemCPUUser.0 = INTEGER: 0
   CS-RA-PRODUCT-MIB::csRASystemCPUSystem.0 = INTEGER: 1
   CS-RA-PRODUCT-MIB::csRASystemCPUIdle.0 = INTEGER: 99
   CS-RA-PRODUCT-MIB::csRASystemMemoryTotal.0 = INTEGER: 4123252
   CS-RA-PRODUCT-MIB::csRASystemMemoryFree.0 = INTEGER: 4009080
   CS-RA-PRODUCT-MIB::csRAPowerStatus.0 = INTEGER: ok(1)
   CS-RA-PRODUCT-MIB::csRARaidLdLevel.1 = INTEGER: raid1(2)
   CS-RA-PRODUCT-MIB::csRARaidLdStatus.1 = INTEGER: ok(1)
```

Ⅰ．ネットワーク

7.DHCP(Ver 1.10.0 以降のみ)

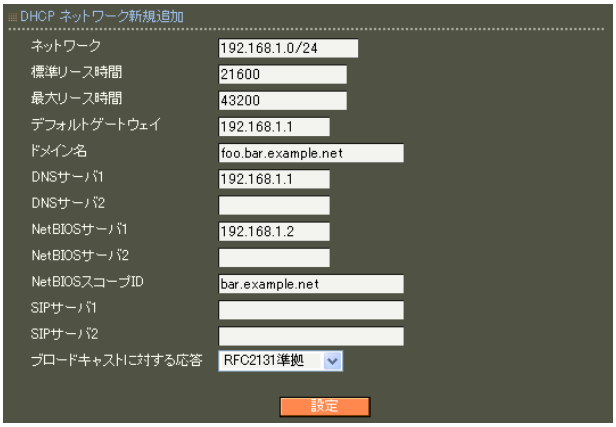
ネットワークに接続するための情報（IP アドレスなど）を、DHCP を用いてクライアントに割り当てる（提供する）ことができます。

管理機能のメニュー「ネットワーク」から「DHCP」を選択すると、現在の DHCP サービスの状態、DHCP ネットワークの設定、および DHCP 固定割り当ての設定が表示されます。

■起動・停止
DHCP サービスの起動・停止・再起動を実行することが出来ます。
DHCP ネットワークが、どの Ethernet インタフェースのネットワークとも一致しない場合、DHCP サービスは起動しません。

■ DHCP ネットワーク
クライアントに割り当てるネットワークを定義します。　設定可能なネットワークの最大数は「付録 A 最大数一覧」を参照してください。

「新規追加」をクリックすると、次の画面が表示されます。



○ネットワーク（入力必須）
クライアントに割り当てるネットワーク・アドレスをプレフィックス表記(A.B.C.D/M）で指定します。

「ネットワーク」のプレフィックス長は、「8」以上を設定してください。
「ネットワーク」は、他の「ネットワーク」と重複しないように設定してください。

○標準リース時間（入力必須）
IP アドレスの標準リース時間（秒）を指定します。
デフォルト値は、21600（秒）です。
600-15552000（秒）の間の整数値を指定します。
最大リース時間以下の値を指定します。

○最大リース時間（入力必須）
IP アドレスの最大リース時間（秒）を指定します。
デフォルト値は、43200（秒）です。
600-15552000（秒）の間の整数値を指定します。
標準リース時間以上の値を指定します。

○デフォルトゲートウェイ（省略可能）
デフォルトゲートウェイを、IP アドレスで指定します。
「ネットワーク」に属する IP アドレスを入力します。

○ドメイン名（省略可能）
ドメイン名を FQDN で指定します。
最大長は、64 文字です。

○ DNS サーバ 1（省略可能）
○ DNS サーバ 2（省略可能）
DNS サーバを、最大 2 個まで、IP アドレスで指定します。
DNS サーバ 2 だけを指定することはできません。

○ NetBIOS サーバ 1（省略可能）
○ NetBIOS サーバ 2（省略可能）
NetBIOS ネームサーバ(WINS サーバ)を、最大 2 個まで、IP アドレスで指定します。
NetBIOS サーバ 2 だけを指定することはできません。

Ⅰ．ネットワーク

○ NetBIOS スコープ ID（省略可能）
NetBIOS スコープ ID を、FQDN 形式で指定します。
最大長は、64 文字です。

○ SIP サーバ 1（省略可能）
○ SIP サーバ 2（省略可能）
SIP サーバを、最大 2 個まで、IP アドレスまたは FQDN で指定します。
SIP サーバ 2 だけを、指定することはできません。
SIP サーバ 1 と SIP サーバ 2 は、同じ形式(IP アドレスまたは FQDN)で入力します。
FQDN の場合、最大長は 64 文字です。

○ブロードキャストに対する応答（省略可能）
broadcast bit が「1」である DHCP パケットを受信した場合の動作を切り替えるために指定します。
「RFC2131 準拠」または「RFC2131 非準拠」を指定します。
省略した場合は「RFC2131 準拠」が指定されたものとします。

「RFC2131 準拠」を指定した場合、broadcast bit が「1」である DHCP パケットを受信した時の動作は RFC 2131 に準拠します。
応答 Ethernet フレームの宛先 MAC アドレスは、ブロードキャスト(FF:FF:FF:FF:FF:FF) です。

「RFC2131 非準拠」を指定した場合、broadcast bit が「1」である DHCP パケットを受信した時の動作は RFC 2131 に準拠しません。
応答 Ethernet フレームの宛先 MAC アドレスはユニキャストです。

なお、宛先 IP アドレスは、常にリミテッド・ブロードキャスト(255.255.255.255) です。

■ DHCP リースアドレス

DHCP クライアントに割り当てる IP アドレス(リースアドレス)の範囲を、開始アドレスと終了アドレスの組で指定します。
アドレス範囲は、「DHCP ネットワーク」の設定に付与されます。
設定可能なリースアドレスの最大数は
「付録 A 最大数一覧」を参照してください。

○開始アドレス（入力必須）
○終了アドレス（入力必須）
DHCP クライアントに割り当てる IP アドレス(リースアドレス）の範囲を、開始アドレスと終了アドレスの組で指定します。
設定の変更は出来ません。変更する場合は、削除・追加を順次行ってください。

開始アドレスは、終了アドレス以下となるように指定します。
開始アドレス・終了アドレス共に、ネットワークに属するアドレスを指定します。
開始アドレス～終了アドレスの間に「デフォルトゲートウェイ」を含まないように設定します。
開始アドレス～終了アドレスで指定される IP アドレス範囲は、他の IP アドレス範囲と重複しないように設定します。

開始アドレス～終了アドレスで指定される IP アドレス範囲に「DHCP 固定割り当て」で定義された IP アドレスを含んでいても問題ありません。
「固定割り当て」で定義された IP アドレスは「固定割り当て」で定義された MAC アドレス以外のクライアントには割り当てられません。

■ DHCP 固定割り当て

DHCP クライアントの MAC アドレスに対して、特定の IP アドレスを割り当てることができます。
特定の MAC アドレスに割り当てた IP アドレスが、別の DHCP クライアントに割り当てられることはありません。
設定可能な DHCP 固定割り当ての最大数は
「付録 A 最大数一覧」を参照してください。

○ MAC アドレス（入力必須）
DHCP クライアントの MAC アドレスを指定します。
英数字（A ～ F、a ～ f、0 ～ 9）とコロン(:)のみ入力することができます。
　入力例）　01:23:45:67:89:AB

○ IP アドレス（入力必須）
固定的に割り当てる IP アドレスを指定します。
「DHCP リースアドレス」に、含まれない IP アドレスでも問題ありません。
「DHCP ネットワーク」に含まれない IP アドレスを指定した場合、当該 IP アドレスがクライアントに割り当てられることはありません。

1. 内蔵時計

本装置の時刻を合わせます。

管理機能のメニュー「システム」から「内蔵時計」を選択すると、現在時刻が表示されます。

時刻を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

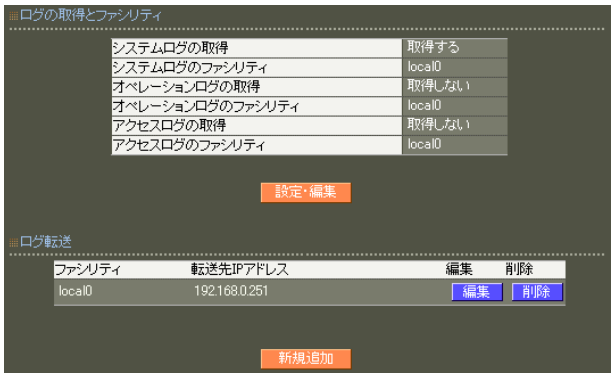
■内蔵時計
24時間単位で時刻を設定してください。

「実行」ボタンをクリックして設定完了です。

2. ログ

ログに関する設定をします。
また、取得した各ログの転送先を設定します。

管理機能のメニュー「システム」から「ログ」を選択すると、現在設定されている内容が表示されます。



■ログの取得とファシリティ
現在の設定内容が表示されています。
設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。

■ログの取得とファシリティ変更

○システムログの取得
システムログについて記録に残すかどうかを設定します。

○システムログのファシリティ
システムログを「取得する」にした場合、システムログが出力されるファシリティを指定します。
プルダウンから選択してください。

○オペレーションログの取得
オペレーションログについて記録に残すかどうかを設定します。

○オペレーションログのファシリティ
オペレーションログを「取得する」にした場合、オペレーションログが出力されるファシリティを指定します。
プルダウンから選択してください。

○アクセスログの取得
アクセスログについて記録に残すかどうかを設定します。

○アクセスログのファシリティ
アクセスログを「取得する」にした場合、アクセスログが出力されるファシリティを指定します。
プルダウンから選択してください。

各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

■ログ転送

各ファシリティ毎のログの転送先が一覧表示されています。
この画面で設定をおこなうシステムログ・オペレーションログ・アクセスログに加え、RADIUS サーバのメニューで設定した認証ログ、アカウンティングログも転送先の指定に従って転送されます。

「新規追加」をクリックすると入力画面が表示されます。

■ログ転送新規追加

○ファシリティ

転送したいログのファシリティを指定します。
プルダウンから選択してください。

○転送先 IP アドレス

ログを転送するサーバを指定します。
指定したマシン上で syslog サーバを動かす必要があります。

各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

設定可能な転送先 IP アドレスの最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除

ログ転送一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

**本装置に記録できるログの数には上限があります（「付録 A 最大数一覧」を参照してください）。
継続的にログを取得される場合は外部の syslog サーバにログを送信するようにしてください。**

3. 設定情報の保存・復帰

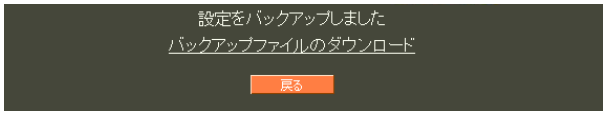
本装置の設定情報の保存、および保存した設定情報の復帰をおこないます。

管理機能のメニュー「システム」から「設定情報の保存・復帰」を選択します。

「設定の保存・復帰画面」にて設定情報を表示・更新する際、本装置のRSAの秘密鍵を含む設定情報等がHTTPSを使用しない場合ネットワーク上に平文で流れます。
設定の保存・復帰は、ローカル環境もしくはVPN環境等、セキュリティが確保された環境下でおこなう事をお勧めします。

■設定情報の保存
○文字コード
設定を保存するときは、文字コードを選択してください。

「保存」ボタンを押すと以下の画面が表示されます。



「バックアップファイルのダウンロード」のリンクから、設定をテキストファイルで保存してください。

保存したテキストファイルには、本装置の設定がすべて記述されています。
このテキストファイルの内容を直接書き換えて設定を変更することもできます。

また、設定ファイルの一番上には次の情報が表示されますので、サポートへのお問い合わせの際にお伝えください。

・Version：
RA を表す文字列・バージョン番号・ビルド番号・ファームの作成日付

・Serial Number：
本装置のシリアル番号

・User：
設定ファイルを取り出したユーザ名

・Address：
設定ファイルを取り出したクライアントの IP アドレス

・Date：
設定ファイルを取り出した日時

■設定情報の復帰
○設定ファイル
「参照」をクリックして、保存しておいた設定情報ファイルを選択します。
利用可能な文字コードは、「EUC-JP」または「Shift_JIS」です。

「復帰」ボタンをクリックすると、設定の復帰がおこなわれます。

設定の復帰を実施した直後に本装置にアクセスした場合に、Web の認証画面が繰り返し表示される場合があります。
このような場合にはまだ設定の復帰が完了しておりません。しばらく待ってから再度アクセスするようにしてください。

復帰した時点で設定情報ファイルの内容が不正であった場合には復帰されません。

(RA ver1.8.5 以前のみ該当)
例えばRADIUSサーバ証明書の有効期限が切れているような場合には、不正な設定情報ファイルと見なされます。

4. 設定情報の初期化

本装置の設定を全てリセットし、工場出荷時の設定に戻します。

管理機能のメニュー「システム」から「設定情報の初期化」を選択します。

■初期化
「実行」ボタンを押すと初期化が実行され、本体の全設定が工場出荷設定に戻ります。

設定の初期により全ての設定が失われますので、念のために設定情報の保存を実行しておくようにしてください。

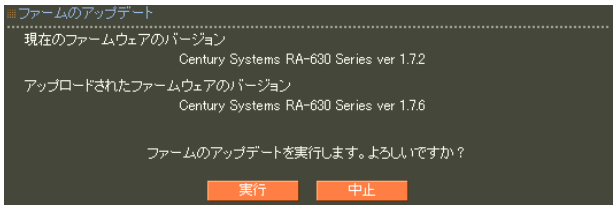
5. ファームのアップデート

本装置のファームウェアのアップデートをおこないます。

管理機能のメニュー「システム」から「ファームのアップデート」を選択します。

■ファームのアップデート
「参照」ボタンを押して、弊社ホームページからダウンロードしてきたファームウェアファイルを選択し、「実行」ボタンを押してください。

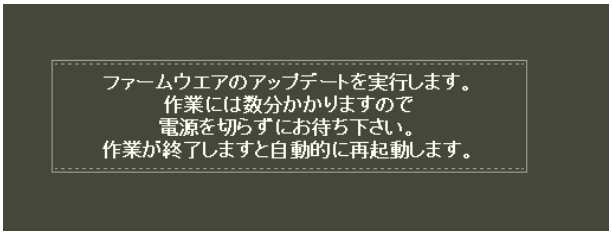
その後、ファームウェアを本装置に転送します(転送が終わるまではしばらく時間がかかります)。
転送完了後に、次のアップデートの確認画面が表示されます。



バージョンが正しければ「実行」ボタンを押してください。

３分以内に「実行」ボタンが押されなかった場合、ファームは破棄されます。

「実行」ボタンを押した場合は次の画面が表示され、ファームウェアの書き換えが始まります。



ファームウェアの書き換え後に本装置が自動的に再起動されて、アップデートが完了します。

アップデート実行中は、本装置へのアクセスはおこなわないでください。アップデート失敗の原因となることがあります。

6. 再起動

本装置を再起動します。

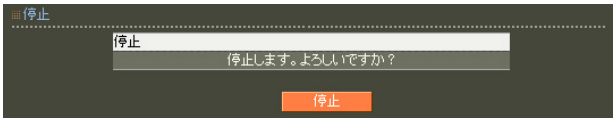
管理機能のメニュー「システム」から「再起動」
を選択します。

■再起動
「実行」ボタンをクリックすると、再起動します。

7. 停止

本装置を停止状態にします。

管理機能のメニュー「システム」から「停止」を選択します。



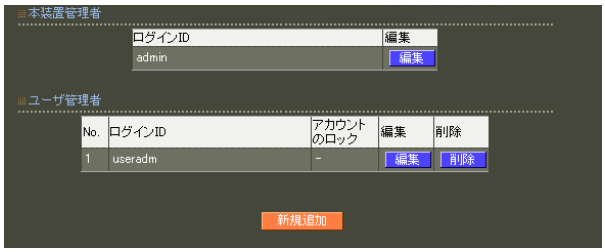
■停止

「停止」ボタンをクリックすると、本装置は停止状態になります。

8. 管理者

管理者がログインする際のユーザー名、パスワードを設定します。装置のセキュリティ確保のために推測されにくいパスワードを設定してください。

管理機能のメニュー「システム」から「管理者」を選択すると、現在設定されている内容が表示されます。



■本装置管理者

本装置管理者のログイン ID が表示されています。

設定を変更する場合は「編集」ボタンを押すと、次の入力画面が表示されます。
新しいログイン ID とパスワードを入力してください。

■本装置管理者変更

○ログイン ID

使用可能な文字は英数字および以下の記号と空白文字になります。

```
!"#$%&'()*+-./<=>?@[]^_`{|}~
```

○パスワード

使用可能な文字は、ログイン ID の入力可能文字と以下の記号になります。

```
,:;\
```

「設定」ボタンをクリックして設定完了です。
次回のログインからは、新しく設定したユーザー名とパスワードを使います。

■ユーザ管理者

本装置管理者の他に、RADIUS のユーザ情報の設定管理のみをおこなえるユーザ管理者を設定することができます。

「新規追加」をクリックすると入力画面が表示されます。
ユーザ管理者のログイン ID とパスワードを入力します。

■ユーザ管理者新規追加

○ログイン ID

使用可能な文字は英数字および以下の記号と空白文字になります。

```
!"#$%&'()*+-./<=>?@[]^_`{|}~
```

○パスワード

使用可能な文字は、ログイン ID の入力可能文字と以下の記号になります。

```
,:;\
```

○ロック

通常は「ロックしない」を選択します。
一時的にユーザ管理者がログインできないように設定したい場合に、「ロックする」を選択するようにします。

各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。
設定はすぐに反映されます。

設定可能なユーザ管理者の最大数は
「付録 A 最大数一覧」を参照してください。

変更・削除

ユーザ管理者一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

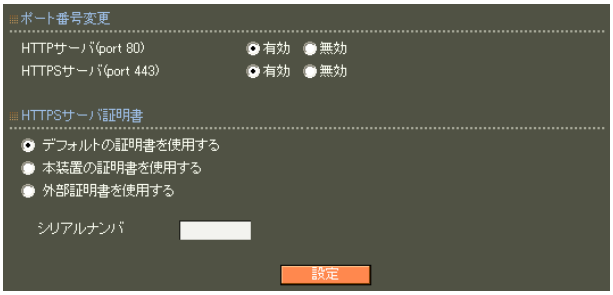
9. 管理画面へのアクセス

本装置の管理画面へアクセスするために必要な設定をおこないます。

管理機能のメニュー「システム」から「管理画面へのアクセス」を選択すると、現在設定されている内容が表示されます。

■ HTTPS サーバ証明書
「本装置の証明書を使用する」欄の「表示」ボタンは HTTPS サーバ証明書で、「本装置の証明書を使用する」が設定されている場合にのみ表示されます。このボタンを押すと証明書の内容が表示され、証明書の取得等ができます。
証明書の詳細については「**第 7 章 CA 設定 II. 証明書**」を参照してください。

設定を変更する場合は「設定・編集」ボタンを押すと、次の入力画面が表示されます。



■ポート番号変更
HTTP/HTTPS によるアクセスを有効にするか無効にするかを選択します。
必ずどちらかは有効にしておく必要があります。

■ HTTPS サーバ証明書
デフォルトで設定されている証明書、本装置の CA で発行したサーバ証明書、外部の CA で発行されたサーバ証明書のいずれを使用するか選択します。

「本装置の証明書を使用する」を選択した場合には、証明書のシリアルナンバを入力して証明書を指定してください。シリアルナンバは、16 進数で入力します。

「外部証明書を使用する」を選択する場合は、事前に証明書をインポートしておく必要があります。

「デフォルトの証明書を使用する」は、 初期設定のための一時的な利用を想定しています。
 できるだけ本装置で発行した証明書または外部証明書を使用してください。

証明書の鍵長・Signature Algorithm は、
それぞれ 2048・SHA-256 を推奨します。

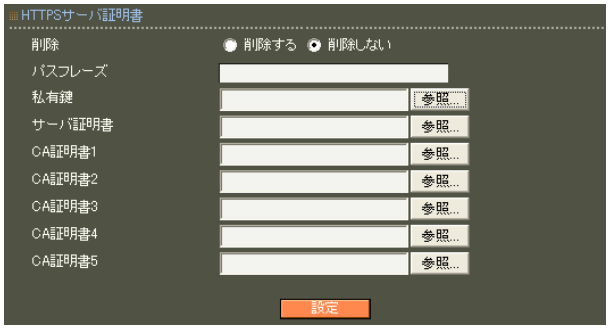
各項目に入力後、「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

10.HTTPS サーバ証明書

外部の CA で発行された証明書を、 HTTPS サーバ証明書として使用するために必要な設定をおこないます。

管理機能のメニュー「システム」から「HTTPS サーバ証明書」を選択すると、現在設定されている内容が表示されます。

■ HTTPS サーバ証明書
「設定」ボタンを押すと入力画面が表示されます。
証明書・私有鍵などを入力します。



○削除
インポートした証明書・私有鍵を削除したい場合に「削除する」を選択します。

○パスフレーズ
私有鍵が暗号化されている場合にそのパスフレーズを入力します。

○私有鍵
サーバ証明書に対応する私有鍵を入力します。必須です。

○サーバ証明書
HTTPS サーバ証明書として使用したい証明書を入力します。
私有鍵に対応している必要があります。必須です。

○ CA 証明書 1 ～ CA 証明書 5
サーバ証明書を発行した CA の証明書を CA 証明書 1 に入力します。
CA 証明書 1 を発行した CA の証明書を CA 証明書 2 に入力します。
以下同様です。

証明書・私有鍵は PEM ファイルのみが入力可能です。

Ver1.11.0 時点では、
公開鍵暗号方式として RSA（鍵長 2048 bit または 4096 bit）のみがサポートされています。
署名方式は SHA-256，SHA-384，SHA-512 のみがサポートされています(CA 証明書は SHA-1 も可)。

サーバ証明書・CA 証明書 1 ～ CA 証明書 5 のいずれかは、自己署名証明書(ルート CA)でなければなりません。

11. 設定情報の同期

■ 概要

RAでは、元となるRAに対しておこなった設定情報の変更を、他のRAに同期させることができます。本機能による RA 間での通信は暗号化されます。

■ 用語の解説

本機能では、以下の用語を使用します。

同期装置
設定情報の同期機能を用いて設定情報を共有する本装置を同期装置と呼びます。

同期コンフィグ
同期装置間で共有される設定情報です。1 つの同期コンフィグは、1 台の MASTER と 1 台の SLAVE で共有されます。

同期システム
同期コンフィグおよび同期装置によって構成される系です。各同期装置は、ただ 1 つの同期システムに属することができます。

親子連携機能
1 つの同期システムに、複数の同期コンフィグを含む機能です。

装置種別
同期をおこなう本装置のうち、設定の元となる機器を MASTER、それ以外を SLAVE と呼びます。

親、子
親子連携機能における、MASTER を親、SLAVE を子と呼びます。

親子連携機能が「有効」「無効」の場合の、構成の違いおよび操作上の注意点は下記のとおりです。

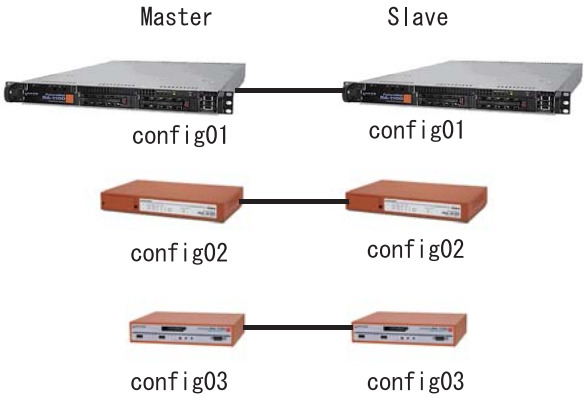
■ 親子連携機能が無効

・1 つの同期コンフィグ
・1 台の MASTER、1 台の SLAVE
・CA は 1 つ

CA に関連する操作(ユーザ証明書を含む証明書の発行・失効や RADIUS ユーザファイル読み込みなど)は基本的に MASTER で行います。
MASTER が存在しない状態ではこれらの操作をおこなうことができません。

CA に関連しない操作（RADIUS ユーザの追加など）についても、基本的には MASTER でおこないます。しかし MASTER が存在しない状態、または、MASTER との通信が途切れていた場合でも、SLAVE で設定・変更など操作は可能です。
ただし、その場合には、同期をおこなう RA 間での設定情報の同一性は保証されません。

下記は、親子連携機能が無効な状態の同期システムの構成例です。



RA-1200 と RA-1100 の二重化・同期はサポートしていません。但し、RA-1100 から RA-1200 へのリプレース等の一時的な同期処理は可能です。

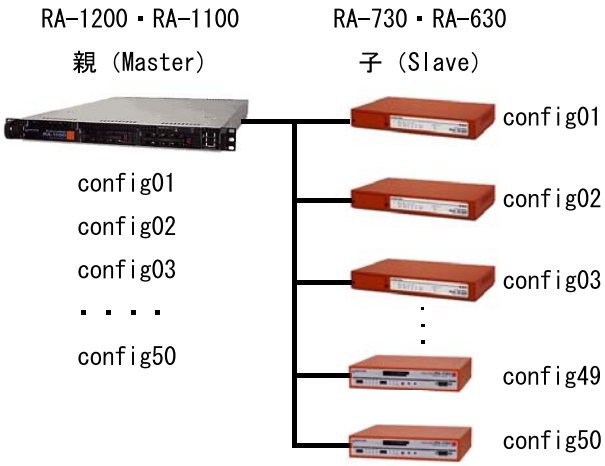
RA-730 と RA-630 の二重化・同期はサポートしていません。但し、RA-630 から RA-730 へのリプレース等の一時的な同期処理は可能です。

■ 親子連携機能が有効

・複数の同期コンフィグ（最大 50 まで）
・1 台の親、複数台の子
・CA は 1 つ（同期システム全体）
・1 つの同期コンフィグを 2 台の同期装置で使用（1 台の親と 1 台の子）
・親は複数の同期コンフィグ、子は 1 つの同期コンフィグを保有

親子連携機能が有効の場合の操作上の注意点は、「付録 G 親子連携」を参照してください。

下記は、親子連携機能が有効な状態の同期システムの構成例です。



■ 同期構成におけるファームウェア更新

同期構成におけるファームウェア更新については、「付録 F 同期・二重化構成におけるファームウェア更新手順」を参照してください。

■ 同期構成における時刻同期

同期構成における各装置の時刻同期を行ってください。
時刻同期には NTP 機能を利用することが可能です。

Ⅱ．システム

同期可能な設定情報・操作は下記の表のとおりです。
同期する場合でも、各設定項目によって動作条件が異なります。表中の印の意味を次に示します。

○印：同期する。
●印：同期する。親のみで実行可能。
＊印：同期する。Master 動作時のみ実行可能。
★印：同期する。Master のみ実行可能。
▲印：二重化の設定に従う。

表．設定項目一覧 (1/3)　（次ページへ続く）

同期処理			階層1	階層2	階層3（各設定項目）
親子連携無効（同期する）	親子連携有効	親子連携有効範囲			
同期しない	同期しない		RADIUS	サーバ	起動・停止
○	●	同期システムで共有			基本情報
同期しない	使用不可				二重化
○	●	同期システムで共有			アトリビュート
○	●	同期コンフィグ毎			アドレスプール
○	●	同期コンフィグ毎			クライアント
○	使用不可				ActiveDirectory
○	使用不可				LDAP
○	使用不可				レルム
○	●	同期システムで共有			ログ
○	●	同期コンフィグ毎		プロファイル	ユーザプロファイル
○	●	同期コンフィグ毎			ユーザ基本情報
○	●	同期コンフィグ毎			認証アトリビュート
○	●	同期コンフィグ毎			応答アトリビュート
○	●	同期コンフィグ毎			グループID
○	●	同期コンフィグ毎			証明書
○	●	同期コンフィグ毎		ユーザ	ユーザ
＊	●	同期コンフィグ毎			ユーザ(証明書の発行)
○	●	同期コンフィグ毎			ユーザ(個別設定)
○	使用不可				AD ユーザ
○	使用不可				LDAP ユーザ
＊	●	同期コンフィグ毎			ファイル読み込み（証明書の発行以外）
＊	●	同期コンフィグ毎			ファイル読み込み（証明書の発行）
同期しない	同期しない				ユーザ検索

表．設定項目一覧 (2/3)　　（次ページへ続く）

同期処理			階層1	階層2	階層3（各設定項目）
親子連携無効（同期する）	親子連携有効	親子連携有効範囲			
＊	●	同期システムで共有	CA	CA/CRL	新規作成
＊	●	同期システムで共有			削除 (※)
＊	●	同期システムで共有			失効リストの更新
同期しない	同期しない				証明書の取得
同期しない	同期しない				失効リストの取得
＊	●	同期システムで共有 同期コンフィグ毎		証明書	発行
同期しない	同期しない				取得
＊	●	同期システムで共有			失効
同期しない	同期しない		管理機能	ネットワーク	基本情報
同期しない	同期しない				スタティックルート
同期しない	同期しない				フィルタ
同期しない	同期しない				DNS
同期しない	同期しない				NTP
同期しない	同期しない				SNMP
同期しない	同期しない				DHCP
同期しない	同期しない			システム	内蔵時計
同期しない	同期しない				ログ
同期しない	同期しない				設定情報の保存・復帰
同期しない	同期しない				設定情報の初期化
同期しない	同期しない				ファームのアップデート
同期しない	同期しない				再起動
同期しない	同期しない				停止
同期しない	同期しない				管理者（本装置管理者）
同期しない	使用不可				管理者（ユーザ管理者）
同期しない	同期しない				管理画面へのアクセス
同期しない	同期しない				設定情報の同期（システム）
同期しない	同期しない				設定情報の同期 （同期コンフィグ）
同期しない	同期しない				設定情報の同期（同期装置）
★	使用不可				設定情報の同期（一括同期）
★	●	同期コンフィグ毎			設定情報の同期（強制同期）
★	使用不可				設定情報の同期（設定取得）
★	●	同期コンフィグ毎			設定情報の同期（ログ同期）
★	●	同期コンフィグ毎			設定情報の同期（ログ取得）
★	●	同期コンフィグ毎			設定情報の同期 （RADIUSサーバ起動・停止）

※「CA CA/CRL 削除」
SLAVE(または子)で HTTPS サーバ証明書に「本装置の証明書」を設定している場合、SLAVE(または子)の CA の削除に失敗します。CA の削除前に SLAVE(または子)の HTTPS サーバ証明書を変更して下さい。詳細については「第 8 章 II. システム 9. 管理画面へのアクセス」を参照して下さい。

表．設定項目一覧 (3/3)

同期処理			階層1	階層2	階層3（各設定項目）
親子連携無効（同期する）	親子連携有効	親子連携有効範囲			
▲	○	同期コンフィグ毎	運用機能	ユーザ情報	ログイン情報
○	○	同期コンフィグ毎			強制ログアウト
○	○	同期コンフィグ毎			一括ログアウト
同期しない	使用不可				ADユーザ情報
同期しない	同期しない			ログ情報	システムログ
同期しない	同期しない				オペレーションログ
同期しない	同期しない				アクセスログ
▲	○	同期コンフィグ毎			認証ログ
▲	○	同期コンフィグ毎			アカウンティングログ
同期しない	同期しない			ネットワークテスト	到達性確認
同期しない	同期しない				ルート確認
同期しない	同期しない				パケットキャプチャ
同期しない	同期しない				名前解決確認
同期しない	同期しない			システム情報	システム情報
同期しない	同期しない				DHCPリース情報
同期しない	同期しない			サポート情報	サポート情報

「設定情報の同期」機能の設定をおこないます。

管理機能メニュー「システム」から「設定情報の同期」を選択すると、現在の設定内容が表示されます。

■設定情報の同期

同期をおこなうRA間でのシステム名・本装置名が表示されます。

■同期コンフィグ一覧

設定を共有するためのコンフィグファイルの一覧が表示されます。

■同期装置一覧

同期をおこなう RA の一覧が表示されます。

■同期実行一覧

必要に応じて実行します。

本機能は、「設定情報の同期」を「同期する」または「親子連携」に設定したMasterにのみ表示されます。

◆設定情報の同期機能の設定

■設定情報の同期

「設定・編集」ボタンをクリックします。

■設定情報の同期

○設定情報の同期

・同期しない
　設定情報の同期を行わない場合に選択します。
・同期する
　設定情報の同期を行う場合に選択します。
・親子連携
　親子連携を使用する場合に選択します。

○ RA システム名

同期をおこなう RA 間でのシステム名を設定します(最大 20 文字)。
使用可能な文字は 0-9，a-z，A-Z，-(0x2c)，_(0x5f)です。

○ RA 本装置名

同期をおこなう RA 間での本装置名を設定します(最大 20 文字)。
使用可能な文字は 0-9，a-z，A-Z，-(0x2c)，_(0x5f)です。

○装置種別

本装置が、同期をおこなう RA 間で MASTER となるか SLAVE となるかを選択します。
親子連携機能を使用する場合、RA-1200 を MASTER、RA-730 を SLAVE に設定してください。RA-1200 を SLAVE、RA-730 を MASTER に設定することはできません。

各項目に入力後、「設定」ボタンを押して本機能の設定を完了します。

◆同期コンフィグの設定

■同期コンフィグ一覧

「新規追加」ボタンをクリックします。既に作成されている設定を編集する場合は、「編集」ボタンをクリックします。「設定情報の同期」で「親子連携」を選択した場合には、「編集」ボタンは表示されません。

■同期コンフィグ新規追加

「設定情報の同期」で、「同期しない」または「同期する」を選択した場合は、下記の画面が表示されます。

「設定情報の同期」で、「親子連携」を選択した場合は、下記の画面が表示されます。

○コンフィグ名

共有する設定情報の名前を設定します（最大 20 文字)。編集の場合は変更できません。
使用可能な文字は 0-9，a-z，A-Z，-(0x2c)，_(0x5f)です。

○処理タイミング

同期処理をおこなうタイミングを設定します。
同期を設定操作ごとにおこなう場合は「即時実行」、同期を設定操作ごとにおこなわず、後にまとめておこなう場合は「一括処理」を選択します。

各項目に入力後、「設定」ボタンを押して同期コンフィグの設定を完了します。

削除

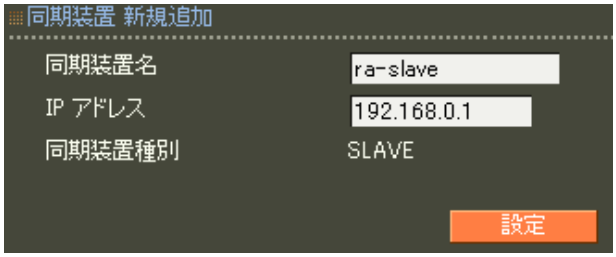
同期コンフィグを削除する場合は、「削除」ボタンをクリックして削除してください。
削除する同期コンフィグに同期装置が設定してある場合は、先に同期装置一覧を削除してください。

◆同期装置の設定

■同期装置一覧

「新規追加」ボタンをクリックします。

■同期装置新規追加



本装置の装置種別を選択しなかった場合は、同期装置種別も選択可能になります。

○同期装置名
同期をおこなう RA の名前を設定します（最大 20 文字)。
使用可能な文字は 0-9，a-z，A-Z，-(0x2c)，_ (0x5f)です。

○ IP アドレス
同期をおこなう RA の IP アドレスを指定します（IPv4 形式)。

○同期装置種別
本装置が、同期をおこなう RA 間で MASTER となるか SLAVE となるかを選択します。

本装置と同期をおこなう対向装置の両方の入力が済みましたら、「設定」ボタンを押して設定を完了します。

削除
同期装置を削除する場合は、「削除」ボタンをクリックして削除してください。

◆同期実行の設定

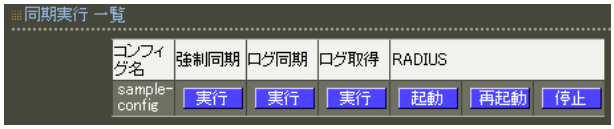
■同期実行一覧

ここでは一括同期の実行や、対向装置の起動・停止等がおこなえます。

下記画面は、「設定情報の同期」を「同期する」に設定した Master にのみ表示されます。

「RADIUS サーバの二重化」「設定情報の同期」の両方が設定されている場合は、[ログ同期]と[ログ取得]が追加表示され、有効になります。

下記画面は、「設定情報の同期」を「親子連携」に設定した Master にのみ表示されます。



○コンフィグ名

「同期コンフィグ一覧」で作成したコンフィグ名が表示されます。

○一括同期

同期コンフィグの設定で処理タイミングに「一括処理」を選択している場合、クリックすると同期を終えていない情報の同期を実行します。

「実行」ボタンをクリックして同期を実行します。

○強制同期

MASTERとSLAVEが異なる設定をしている場合、MASTER の設定情報を SLAVE の設定情報に上書きし、強制同期させます。

「実行」ボタンをクリックして同期を実行します。

○設定取得

MASTER-SLAVE 間で通信ができない状態のまま SLAVE 側で設定をおこなうと、MASTER-SLAVE 間で設定の不一致が発生します。このような場合に MASTER は SLAVE の設定情報を取得し反映させることができます。

「実行」ボタンをクリックして設定情報を取得します。

「設定取得」で「RADIUS」メニュー「サーバ」に関する設定（基本情報、二重化、アトリビュート、アドレスプール、クライアント、ActiveDirectory、LDAP、ログ）を変更した場合、設定内容を有効にするためには MASTER 側 RADIUS の再起動が必要です。

○ログ同期

本ボタンが実行されると、対向の RA へログイン情報、認証ログ、アカウンティングログが送信されます。

ログイン情報にはアドレスプールの情報も含まれます。

送信した場合には、対向の RA が持つログイン情報、認証ログ、アカウンティングログはそれぞれ破棄されます。

○ログ取得

本ボタンが実行されると、対向のRAからログイン情報、認証ログ、アカウンティングログが取得されます。

ログイン情報にはアドレスプールの情報も含まれます。

取得した場合には、自分自身が持つログイン情報、認証ログ、アカウンティングログはそれぞれ破棄されます。

○ RADIUS

本装置が MASTER である場合、SLAVE の RADIUS の起動・停止・再起動をMASTER側から指示することができます。

各ボタンをクリックして動作を実行してください。

本機能により「RADIUS」メニュー「サーバ」に関する設定（基本情報、二重化、アトリビュート、アドレスプール、クライアント、ActiveDirectory、LDAP、ログ）を変更した場合、設定内容を有効にするためにはSLAVE 側 RADIUS の再起動が必要です。

◆同期の確認

同期が正常におこなわれているかは、「運用機能」メニュー「システム情報」の「システム情報」で確認してください。

第9章

運用機能

Ⅰ．ユーザ情報

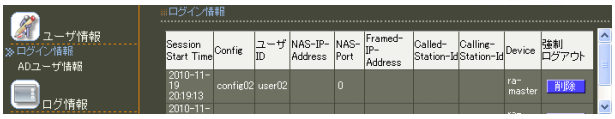
1. ログイン情報

現在ログインしているユーザ名を表示します。

運用機能のメニュー「ユーザ情報」から「ログイン情報」を選択します。

※以下より説明する、**各設定画面は、全て同画面で表示されます。**

■ログイン情報
各項目はRADIUSクライアントからのアカウンティング要求の情報に基づいて表示されます。
親子連携機能が有効の場合に限り、同期コンフィグ及び同期装置も記録されます。



削除
接続されているユーザの「強制ログアウト」欄の「削除」ボタンを押すことで、その接続を削除する事が可能です。

ここでの強制ログアウトとは、RADIUSサーバ内のログイン情報を強制的にログアウト状態に変更することを表します。
実際に接続をおこなっているRADIUSクライアント(無線LANアクセスポイント、認証スイッチ、NAS、RAS等)には、一切の通知をおこないません。

■ソート
ログイン情報をソートさせて表示することができます。
ソート項目は、3 個まで設定可能です。
それぞれ昇順、降順の指定が可能ですが、大文字、小文字の区別はしません。
複数のソート項目が指定された場合は、順にソートされます。

プルダウンからソートの対象項目を選択します。
◯指定しない
◯ SessionStartTime
◯ Config
◯ User-Name
◯ NAS-IP-Address
◯ NAS-Port
◯ Framed-IP-Address
◯ Called-Station-Id
◯ Calling-Station-Id
◯ Device

ソートの順序を選択します。
◯昇順
◯降順
デフォルトは昇順です。

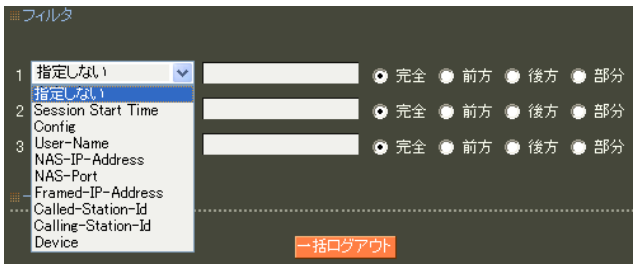
Ｉ．ユーザ情報

■フィルタ

フィルタによる検索を実施することができます。
それぞれ、下記の指定が可能です。

・完全一致
(設定された文字列と完全に一致した場合のみ表示)
・前方一致
(設定された文字列が先頭に持つもののみ表示)
・後方一致
(設定された文字列が末尾に持つもののみ表示)
・部分一致
(設定された文字列を含むもののみ表示)

複数のフィルタが指定された場合は、それらの AND 結果を表示します。



フィルタの対象項目を選択します。
◯指定しない
◯ SessionStartTime
◯ Config
◯ User-Name
◯ NAS-IP-Address
◯ NAS-Port
◯ Framed-IP-Address
◯ Called-Station-Id
◯ Calling-Station-Id
◯ Device

フィルタさせる文字列を設定します。
入力可能な文字列は、ASCII コードの 0x21-0x7e（ただし 0x22(")，0x25(%)，0x5c(\) は含みません)です。
最大文字長は「20」で、デフォルト値はありません。

フィルタ条件を選択します。
◯完全
◯前方
◯後方
◯部分

■一括ログアウト

ログイン中のユーザを全てログアウトしたものとして扱います。
画面表示されたユーザだけでなく、全てのユーザが対象です。
二重化している場合は、もう一方も全てログアウトしたものとします。

設定情報の同期をおこなう設定の場合、本設定は対向装置へ同期されます。

Ⅰ．ユーザ情報

2.AD ユーザ情報

Active Directory サーバに登録されたユーザを表示します。

認証に使用しているサーバの情報も併せて表示します(Ver 1.10.0 以降のみ)。

運用機能のメニュー「ユーザ情報」から「AD ユーザ情報」を選択します。

■ AD ユーザ情報

RADIUS 設定で「Active Directory」を「使用する」に設定している場合に、Active Directory サーバに登録されたユーザのうち、設定された「ドメインネーム」・「所属グループ」に所属するユーザ名が表示されます。「所属グループ」が設定されていない場合は、「ドメインネーム」に所属する全ユーザ名が表示されます。

Active Directory サーバでアカウントが無効に設定されているユーザは、lock 欄に x が表示されます (ver 1.8.3 以降のみ)。

ユーザ名に日本語などが含まれる場合、正しく表示されないことがあります。

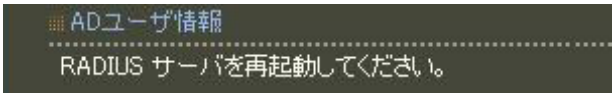
表示されるユーザが全て認証可能とは限りません。Active Directory サーバの設定により認証できない場合もあります。また、日本語などがユーザ名に含まれるユーザも認証できません。

エラーメッセージ

○Active Directory 連携は未使用です。

「Active Directory」が「使用しない」に設定されている場合、または「Active Directory」が「使用する」に設定されているが RADIUS サーバが停止している場合に表示されます。
「Active Directory」を「使用する」に設定した上、RADIUS サーバを起動して下さい。

○RADIUS サーバを再起動してください。

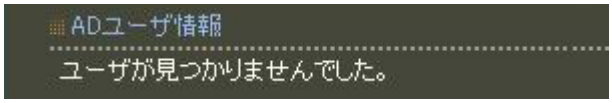


Active Directory の設定を変更したが、設定変更が反映されていない場合に表示されます。RADIUS サーバを再起動して設定を反映させてください。

○サーバと通信できませんでした。

Active Directory サーバと正常に通信ができない場合に表示されます。設定内容、Active Directory サーバへのネットワーク到達性、Active Directory サーバの設定などを確認して下さい。

○ユーザが見つかりませんでした。



該当するユーザが存在しない場合に表示されます。

Ⅱ．ログ情報

1. システムログ

本装置の稼働状況について記録されているログ情報を表示します。

本装置に記録できるログの数には上限があります(「付録 A 最大数一覧」を参照してください)。

運用機能のメニュー「ログ情報」から「システムログ」を選択します。

■システムログ

表示順を指定して「実行」ボタンを押すと最新のログが時刻順でソートされて表示されます。

システムログの表示内容
システムログには以下の項目がカンマ区切りで表示されます。

・日時
・分類
　“ RADIUS ”, “ NTP ” などのログの種別。
・ログ内容

システムログの表示内容の詳細については、「付録 E システムログ一覧」を参照して下さい。

II．ログ情報

2. オペレーションログ

本装置の GUI で行った設定変更操作についてのログ情報を表示します。

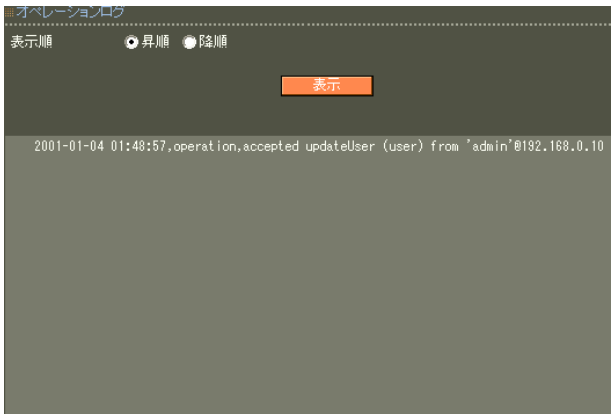
対象は RADIUSユーザのパスワード変更のみです。

設定情報の同期を使用している場合、最初に設定変更処理が実行される装置（通常は MASTER)で記録されます。

本装置に記録できるログの数には上限があります（「付録 A 最大数一覧」を参照してください）。

運用機能のメニュー「ログ情報」から「オペレーションログ」を選択します。

■オペレーションログ



表示順を指定して「実行」ボタンを押すと最新のログが時刻順でソートされて表示されます。

オペレーションログの表示内容

オペレーションログには以下の項目がカンマ区切りで表示されます。

・日時
・"operation"
　オペレーションログであることを表します。
・ログ内容

result-string cmd (*target-user*)
　　from '*username*'@*ipaddress*
　　[via *slave-ipaddress*] [(*aux-string*)]

ここでそれぞれの意味は以下の通りです。

result-stirng:
　認証結果です。
　設定変更成功時は accepted、
　失敗時は rejected です。

cmd:
　変更内容です。
　例えば、管理者によるユーザ設定変更時は
　updateUser になります。
　RADIUSユーザ自身によるパスワード変更時は、
　updatePassword です。

target-user:
　変更対象のユーザ名です。

username:
　操作を行ったユーザ名です。

ipaddress:
　接続元 IP アドレスです。

設定情報の同期を使用している状態で、
SLAVE で、GUI 操作を行った場合、
メッセージに via *slave-ipaddress*が付加されます。
*slave-ipaddress*は、SLAVE の IP アドレスです。

補足メッセージとして、*aux-string*が付加されることがあります。
例えば、パスワードが変更されていない場合は、
password not changed というメッセージが付加されます。

II．ログ情報

3. アクセスログ

本装置のGUIアクセスにおけるユーザ認証結果についてのログ情報を表示します。

GUI アクセスにおいて、ユーザ認証が成功した場合は、成功したことを表すログを記録します。

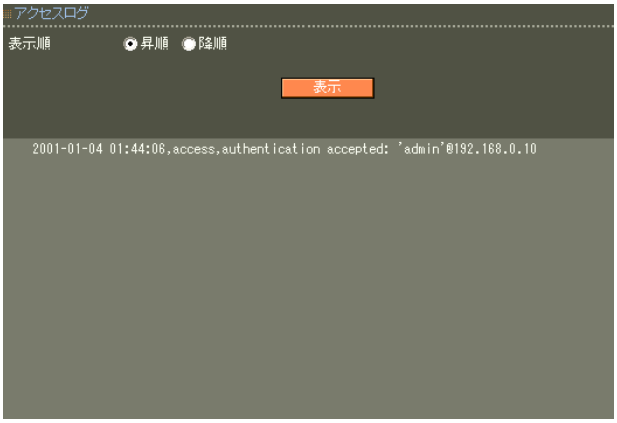
アクセスが継続している間は、15分に1回程度の割合で記録します。

ユーザ認証に失敗した場合は、失敗したことを表すログを記録します。
アクセスの度に記録します。

本装置に記録できるログの数には上限があります(「付録 A 最大数一覧」を参照してください)。

運用機能のメニュー「ログ情報」から「アクセスログ」を選択します。

■アクセスログ



表示順を指定して「実行」ボタンを押すと最新のログが時刻順でソートされて表示されます。

アクセスログの表示内容
アクセスログには以下の項目がカンマ区切りで表示されます。

・日時
・"access"
　アクセスログであることを表します。
・ログ内容

ユーザ認証成功時:
authentication accepted: '*username*'@*ipaddress*

ユーザ認証失敗時:
authentication rejected: '*username*'@*ipaddress*

ここで、username、ipaddress は、それぞれ、ユーザ名、接続元 IP アドレスを表します。

4. 認証ログ

RADIUS サーバによる認証のログ情報を表示します。

本装置に記録できるログの数には上限があります（「付録 A 最大数一覧」を参照してください）。

認証ログの reason メッセージについては、「付録 H 認証ログの reason メッセージ一覧」を参照してください。

運用機能のメニュー「ログ情報」から「認証ログ」を選択します。

■認証ログ

認証ログの表示内容

認証ログには以下の項目がカンマ区切りで表示されます。

- “Auth”
  認証ログであることを表します。
- 同期コンフィグ
  親子連携機能が有効の場合のみ表示されます。
- 認証要求で送られたユーザ ID
- 認証方式が EAP-TLS/EAP-PEAP/EAP-TTLS
  であった時に、phase 2 で送られたユーザ ID
- 認証結果
- 認証に失敗した場合の理由
- RADIUS クライアントの IP アドレス
- 認証要求で送られたアトリビュート
  NAS-IP-Address の値
- 認証要求で送られたアトリビュート
  NAS-Identifier の値
- 認証要求で送られたアトリビュート
  Called-Station-Id の値
- 認証要求で送られたアトリビュート
  Calling-Station-Id の値
- 同期装置
  親子連携機能が有効の場合のみ表示されます。
- 日時

RADIUS クライアントに設定されていない IP アドレスを持つマシンからの認証要求を拒絶したログについては、認証ログではなく、システムログの方に記録されます。

■ソート

認証ログを表示する順序を指定します。
プルダウンメニューで、ソートしたい項目を指定し、「昇順」または「降順」でその項目の並び順を指定します。
1 から 3 番のソート項目を指定することにより、1 番の項目でソートされた中をさらに 2 番の項目、3 番の項目でソートするという並び順になります。

設定後「表示」ボタンを押すことで最新のログが指定された順序で表示されます。

Ⅱ．ログ情報

■フィルタ
認証ログが表示する内容を絞りたい場合に指定します。
プルダウンメニューで絞り込みの条件に使用したい項目を指定します。
隣の入力欄にその項目の検索対象文字列を指定します。
最後にその文字列で検索をおこなう条件を指定します。

- 完全
  指定された項目が、検索対象文字列と完全に一致するログが表示されます。
- 前方
  指定された項目の最初の部分が、検索対象文字列と一致するログが表示されます。
- 後方
  指定された項目の最後の部分が、検索対象文字列と一致するログが表示されます。
- 部分
  指定された項目が、検索対象文字列を含んでいるログが表示されます。

1から3番に複数のフィルタ項目を指定することができます。複数のフィルタ項目を指定した場合には、全ての条件と一致するログのみが表示されます。

設定後「表示」ボタンを押すことで最新のログが指定されたフィルタ条件で表示されます。
一致するログが無かった場合には何も表示されません。

解除
フィルタを解除する時には全てのフィルタ項目で「指定しない」を選択して「表示」ボタンを押してください。

■出力先
表示出力先を「画面」「画面（table)」「ファイル(text)」「ファイル(csv)」の中から選択してください。
ファイルを選択した場合にはブラウザの指示に従ってファイルを保存してください。

ソート、フィルタ、表示出力先の指定は同時におこなうことができます。

5. アカウンティングログ

RADIUSサーバによるアカウンティングのログ情報を表示します。

本装置に記録できるログの数には上限があります(「付録 A 最大数一覧」を参照してください)。

運用機能のメニュー「ログ情報」から「アカウンティングログ」を選択します。

■アカウンティングログ

アカウンティングログの表示内容
アカウンティングログには以下の項目がカンマ区切りで表示されます。

- “Acct”
  アカウンティングログであることを表します。
- 同期コンフィグ
  親子連携機能が有効の場合のみ表示されます。
- 同期装置
  親子連携機能が有効の場合のみ表示されます。

「RADIUS」のメニュー「サーバ」の「ログ」中のアカウンティングログの各項目。
具体的な内容は**「第6章 RADIUS設定 I. サーバ設定 10. ログ」**を参照してください。

■ソート
アカウンティングログを表示する順序を指定します。プルダウンメニューで、ソートしたい項目を指定し、「昇順」または「降順」でその項目の並び順を指定します。
1から3番のソート項目を指定することにより、1番の項目でソートされた中をさらに2番の項目、3番の項目でソートするという並び順になります。

設定後「表示」ボタンを押すことで最新のログが指定された順序で表示されます。

II．ログ情報

■フィルタ
アカウンティングログが表示する内容を絞りたい場合に指定します。
プルダウンメニューで絞り込みの条件に使用したい項目を指定します。
隣の入力欄にその項目の検索対象文字列を指定します。
最後にその文字列で検索をおこなう条件を指定します。

- 完全
  指定された項目が、検索対象文字列と完全に一致するログが表示されます。
- 前方
  指定された項目の最初の部分が、検索対象文字列と一致するログが表示されます。
- 後方
  指定された項目の最後の部分が、検索対象文字列と一致するログが表示されます。
- 部分
  指定された項目が、検索対象文字列を含んでいるログが表示されます。

1 から 3 番に複数のフィルタ項目を指定することができます。複数のフィルタ項目を指定した場合には、全ての条件と一致するログのみが表示されます。

設定後「表示」ボタンを押すことで最新のログが指定されたフィルタ条件で表示されます。
一致するログが無かった場合には何も表示されません。

解除
フィルタを解除する時には全てのフィルタ項目で「指定しない」を選択して「表示」ボタンを押してください。

■出力先
表示出力先を「画面」「画面（table)」「ファイル(text)」「ファイル(csv)」の中から選択してください。
ファイルを選択した場合にはブラウザの指示に従ってファイルを保存してください。

ソート、フィルタ、表示出力先の指定は同時におこなうことができます。

III. ネットワークテスト

本装置の運用時において、ネットワークテストをおこなうことができます。
ネットワークのトラブルシューティングに有効です。
以下の 4 つのテストができます。

- 到達性確認
- ルート確認
- パケットキャプチャ
- 名前解決確認

III. ネットワークテスト

1. 到達性確認

ネットワークテストをおこないます。
指定した相手に ICMP echo パケットを送信し、相手装置から返信されたパケットを表示します。

運用機能のメニュー「ネットワークテスト」の「到達性確認」を選択すると次の画面が表示されます。

■到達性確認

○送信先
到達性を確認したい相手装置の FQDN (www.example.co.jp などのホスト名)、もしくは IP アドレスを入力します。

○サイズ
送信するパケットのバイト数を指定します。
デフォルトは 56byte です。0-65507 の間で指定します。

○ DF フラグ
パケットの分割を許可したくない場合に「あり」を指定します。

各項目を入力後「実行」ボタンを押すと結果が画面に表示されます。

応答メッセージが表示されない場合は、DNS で名前解決ができていない可能性があります。その場合はまず、IP アドレスを直接指定してご確認ください。

III. ネットワークテスト

2. ルート確認

ネットワークテストをおこないます。
指定した相手に TTL を順に増やしながらパケットを送信することでパケットの送信経路を確認します。

運用機能のメニュー「ネットワークテスト」の「ルート確認」を選択すると次の画面が表示されます。

■ルート確認

○送信先
ルート確認をおこないたい相手装置の FQDN (www.example.co.jp などのホスト名)、もしくは IP アドレスを入力します。

○最大 TTL
送信するパケットの TTL を最大いくつまで設定して送信するかをホップ数で指定します。
1-60 の範囲で指定します。

○名前解決
結果表示をおこなう際に IP アドレスをホスト名に変換して表示する場合には「する」を選択します。
ネットワーク障害等により DNS の名前解決ができない状況の時は「しない」を選択してください。

各項目を入力後「実行」ボタンを押すと結果が画面に表示されます。

応答メッセージが表示されない場合は、DNS で名前解決ができていない可能性があります。その場合はまず、IP アドレスを直接指定してご確認ください。

Ⅲ．ネットワークテスト

3. パケットキャプチャ

ネットワークテストをおこないます。
指定したインタフェースをモニタし、送受信されたパケットの情報を記録します。

運用機能のメニュー「ネットワークテスト」の「パケットキャプチャ」を選択すると次の画面が表示されます。

■パケットキャプチャ

○インターフェイス
パケットキャプチャを実施するインタフェースを選択します。

○パケットサイズ
キャプチャするパケットサイズを入力します。
デフォルトは68byteです。68-1514の範囲で指定します。

○パケット数
キャプチャするパケット数を入力します。
キャプチャできるのは最大1000パケットまでです。

○プロトコル
キャプチャするプロトコルを選択します。
「ANY」、「TCP」、「UDP」、「ICMP」の中から選択します。

○ポート
キャプチャするポートを指定します。
プロトコルが「ICMP」の場合はポートの指定はできません。
複数ポートを指定したい場合には空白文字で区切って複数の数字を入力します。
空欄にした場合には全てのポートが対象となります。

○設定画面へのアクセス
設定画面を表示するのに使用しているパケットがキャプチャされるのを防ぎたい場合に「キャプチャしない」を選択します。

○アクション
「画面表示」「ファイル」のどちらかひとつを選択します。

・画面表示
出力結果を画面に表示する場合に選択します。

・名前解決
結果表示をおこなう際にIPアドレスをホスト名に変換して表示する場合には「する」を選択します。
ネットワーク障害等によりDNSの名前解決ができない状況の時は「しない」を選択してください。

・リンクレベルヘッダ
リンクレベルヘッダの表示を省略したい時には「表示しない」を選択します。

・ASCII表示
16進数表示に加え、ASCII文字に変換した値も表示したい時には「表示する」を選択します。

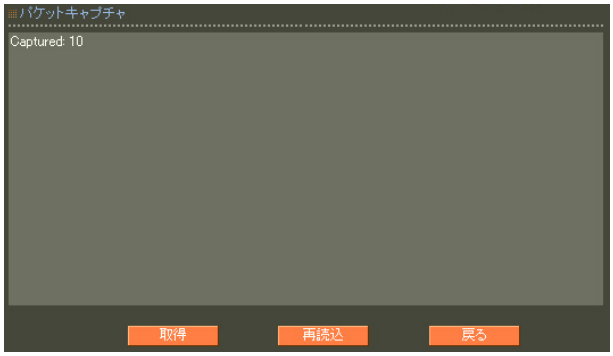
・詳細表示
パケットの内容をより詳細に表示したい場合に「する」を選択します。TTLやサービスの種類などが出力されるようになります。

各項目を入力後「実行」ボタンを押すと、キャプチャを開始します。

・ファイル
出力結果をファイルに保存したい場合に選択して「実行」ボタンを押します。

III. ネットワークテスト

■パケットキャプチャ



「取得」をクリックすると出力結果を pcap 形式で保存することができます。取得後のファイルは、「ethereal」などのアプリケーションで表示させることができます。

「再読込」をクリックするとキャプチャ数を更新することができます。

III. ネットワークテスト

4. 名前解決確認

ネットワークテストをおこないます。
名前解決が正しくおこなわれるかを確認します。

運用機能のメニュー「ネットワークテスト」の「名前解決確認」を選択すると次の画面が表示されます。

■名前解決確認

DNS の正引きをおこないたい時
○引き方
正引きを選択します。

○ホスト
ホスト名(FQDN)を入力します。

入力後に「実行」ボタンを押します。

名前解決に成功すれば、入力された FQDN に一致する IP アドレスが表示されます。

DNS の逆引きをおこないたい時
○引き方
逆引きを選択します。

○ホスト
IP アドレスを入力します。

入力後に「実行」ボタンを押します。

名前解決に成功すれば、入力された IP アドレスに一致するホスト名が表示されます。

Ⅳ. システム情報

1. システム情報

本装置の機器情報を表示します。

運用機能のメニュー「システム情報」の「システム情報」を選択すると次の画面が表示されます。

■情報表示

＜親子連携無効時＞

＜親子連携有効時＞

表示欄に以下の内容について表示されます。

○ファームウェアバージョン
本装置の現在のファームウェアバージョンを表示します。

○シリアル番号
本装置のシリアル番号を表示します。

○ IP アドレス
各インタフェースの IP アドレスや MAC アドレスなどです。

○送受信カウンタ
各インタフェースの通過パケット数等を表示します。

○リンク
各インタフェースのリンク状態を表示します。

○デフォルトゲートウェイ
デフォルトルート情報です。

○スタティックルート
直接接続、スタティックルートに関するルーティング情報です。

○ネイバー
ARP テーブルの情報です。

○フィルタ
パケットフィルタに関する情報です。

○電源（※ RA-1200 のみ）
電源の状態を表示します。

OK	電源が正しい状態
Warning	電源が正しくない状態

○ RAID（※ RA-1200 のみ）
RAID の状態を表示します。

OK	正常な状態
Degraded/Rebuilding	リビルド中
Degraded/Fault	障害状態

Ⅳ．システム情報

＜親子連携無効時＞
○二重化
二重化の状態を表示します。
　Unsetting　二重化設定をしていない
　OK　　二重化に成功している
　NG　　二重化に失敗している

○設定情報の同期
設定情報の同期の状態を表示します。
　Unsetting　設定情報の同期設定をしていない
　OK　　設定情報の同期に成功している
　NG　　設定情報の同期に失敗している

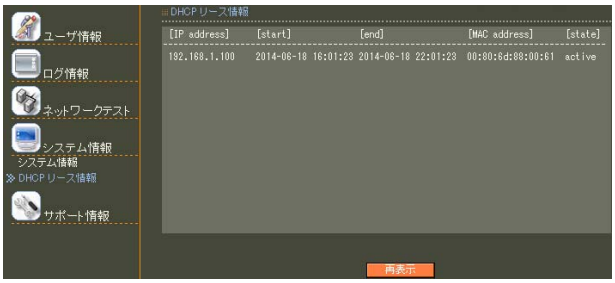
＜親子連携有効時＞
○二重化・設定情報の同期
同期コンフィグ、同期装置毎に、二重化・設定情報の同期の状態を表示します。
　Unsetting　コンフィグが未設定
　　or 対向装置の設定が１件もない
　OK　　二重化に成功している
　　OK　設定情報の同期に成功している
　NG　　二重化に失敗している
　　NG　設定情報の同期に失敗している

「再表示」ボタンを押すと最新の情報に更新します。

2.DHCP リース情報

IPアドレスのリースに関する情報を表示します。

運用機能のメニュー「システム情報」の「DHCP リース情報」を選択すると次の画面が表示されます。



IPアドレスのリースに関する以下の情報を表示します。
- IP address（IP アドレス）
- start（リース開始時刻）
- end（リース終了予定時刻）
- MAC address（クライアント MAC アドレス）
- state（状態）

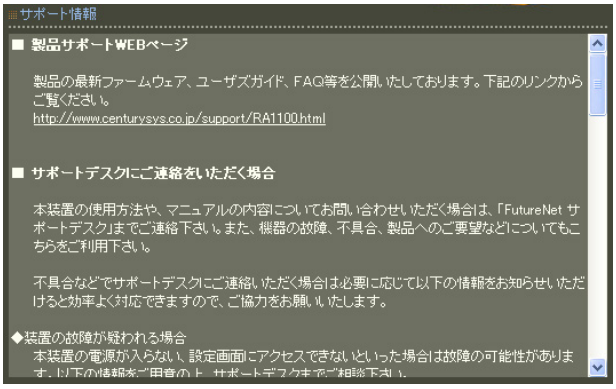
Ⅴ．サポート情報

サポート情報

本装置のサポート情報を表示します。

運用機能のメニュー「サポート情報」の「サポート情報」を選択すると製品サポートに関する情報が表示されます。

■サポート情報



第 10 章

ユーザ管理者メニュー

画面構成

ユーザ管理者 のユーザ名とパスワードを用いてログインした場合、以下に示す初期画面が最初に表示されます。

本装置管理者のユーザ名でログインした場合には全ての設定メニュー項目が利用できますが、ユーザ管理者のユーザ名でログインした場合には、使えるメニューはユーザ設定に必要なメニューのみとなります。

ユーザ管理者でログインした場合のメニュー階層を以下に示します。

- RADIUS
  - プロファイル
    - ユーザプロファイル
    - ユーザ基本情報
    - 認証アトリビュート
    - 応答アトリビュート
    - グループ ID
    - 証明書
  - ユーザ
    - ユーザ
    - AD ユーザ
    - LDAP ユーザ
    - ファイル読み込み
    - ユーザ検索
- CA
  - CA/CRL
- 管理機能
  - システム
    - 管理者
- 運用機能
  - ユーザ情報
    - ログイン情報
    - ＡＤユーザ情報
  - ログ情報
    - 認証ログ
    - アカウンティングログ
  - ネットワークテスト
    - 到達性確認
    - ルート確認
    - パケットキャプチャ
    - 名前解決確認
  - システム情報
    - システム情報
  - サポート情報
    - サポート情報
- 設定ウィザード
  - ユーザ登録

各メニュー項目の設定方法、設定内容については第 5 章～第 9 章を参照してください。

なお、同じメニュー項目でも以下のメニューについては本装置管理者とは利用できる操作が異なります。

◆「CA」-「CA/CRL」メニュー
CA 証明書の参照はできますが、作成、削除はできません。

◆「管理機能」-「システム」-「管理者」メニュー
ユーザ管理者自身のパスワードの変更のみおこなえます。

◆「設定ウィザード」-「ユーザ登録」ウィザード
設定の保存はおこなえません。

第11章

ユーザメニュー

第 11 章 ユーザメニュー

Ⅰ．ログイン

RADIUS メニュー「ユーザ」で設定されたユーザは、Web ブラウザから本装置にアクセスして、自身のパスワード変更、および自分に対して発行された証明書の取得をすることができます。

管理者としてログインする場合同様、ブラウザのアドレス欄に以下の URL を入力します。

http://192.168.0.254/

上記 URL は HTTP(ポート 80)でアクセスする場合の Ether0 ポートの工場出荷時のアドレスを使う場合の例です。
アドレスを変更した場合は、そのアドレスを指定してください。

HTTPS(ポート 443)でアクセスする場合は、ブラウザのアドレス欄に以下の URL を入力してください。

https://192.168.0.254/

認証ダイアログ画面が表示されますので、RADIUS メニュー「ユーザ」で設定されたユーザ ID とパスワードを指定します。

一度管理者でログイン済みの場合などで、ユーザを切り替えたい場合は、一度ブラウザを終了させてから、再度ブラウザを起動してください。

ユーザ ID、パスワードが正しければ次の画面が表示されます。

メニュー「CA/CRL」は CA が設定されている場合に表示されます。
メニュー「証明書」はユーザに対して証明書が発行されている場合にのみ表示されます。

次節からは各メニューについて説明します。

Ⅱ．パスワード

パスワード

メニュー「パスワード」を選択すると、次の画面が表示されます。

■ユーザ変更

○パスワード
新しいパスワードを入力します。
パスワードは最大20文字まで入力する事が可能です。
使用可能な文字は、英数字および以下の記号と空白文字になります。

```
!"#$%&'()*+-./<=>?@[]^_`{|}~,:;\
```

「設定」ボタンを押すとパスワードが変更されます。
次回のログインからは、新しく設定したパスワードを使ってログインしてください。

III. CA/CRL

CA/CRL

メニュー「CA/CRL」を選択すると、次の画面が表示されます。

■ CA 証明書

○ CA/ 失効リストの表示

画面上部にある「CA」/「失効リスト」の選択ボタンを選んで「表示」ボタンを押すと、CA の内容または失効リストの内容が表示されます。

■ CA 証明書の取得

CA 証明書欄で「取り出し」ボタンをクリックすることにより CA 証明書を取り出すことができます。この際、取り出す形式を PEM または DER から選択することができます。

■ 失効リストの取得

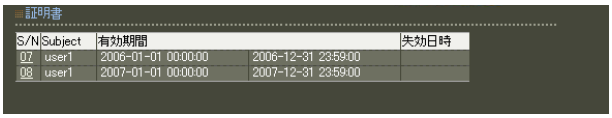
失効リストの取得欄で「取り出し」ボタンをクリックすることにより CRL を取り出すことができます。この際、取り出す形式を PEM または DER から選択することができます。

Ⅳ．証明書

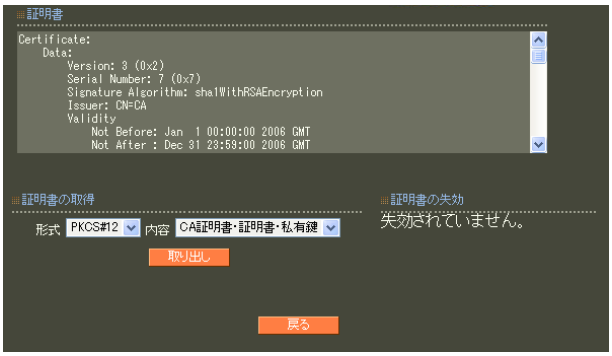
証明書

ユーザに対して証明書が発行されている場合に表示されるメニュー「証明書」を選択すると、ユーザの全ての証明書が一覧表示されます。

■証明書



「S/N」（シリアルナンバ）をクリックすることでその証明書の詳細内容が表示されます。



■証明書
欄には証明書の内容が表示されます。

■証明書の取得
ユーザ証明書をダウンロードすることができます。取り出す形式と内容を指定して「取り出し」ボタンを押します。

○形式
「PKCS#12」、「PEM」、「DER」から一つ選択します。

○内容
「CA 証明書・証明書・私有鍵」、「証明書・私有鍵」、「証明書」、「私有鍵」から一つ選択します。

※ PKCS#12 を選択した場合
　証明書と私有鍵のどちらか一方のみは選択できません。
※ PEM，DER を選択した場合
　証明書と私有鍵を同時に取り出すことはできません。それぞれ別々に取り出してください。

取り出した証明書はユーザの PC に保存して、RADIUS による認証時に利用するようにします。

■証明書の失効
この証明書が失効されているか否かが表示されます。

失効した証明書は取得できません。

Ⅴ．同期可能な設定情報・操作

同期可能な設定情報・操作

同期構成時に、同期可能な設定情報・操作は下記の表のとおりです。

同期処理	設定項目
同期する	パスワード変更
同期しない	証明書の取得

第 12 章

一般ユーザによる PC の設定

第 12 章　一般ユーザによる PC の設定

Ⅰ．設定例(EAP-TLS)

本装置を使って実際に認証処理をおこなう場合には、RADIUS クライアントである、NAS や無線 LAN アクセスポイントの設定および、認証を受ける PC の設定が必要になります。

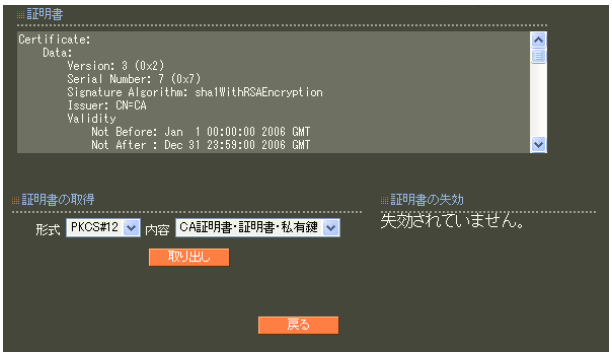
ここでは EAP-TLS で認証をおこなう場合に必要な PC の設定について設定例を記述します。
なお、実際の設定にあたっては各ハードウェア、ソフトウェアに付属するマニュアルを参照してください。
本設定例では、サプリカントとして WindowsXP に標準で含まれているサプリカントを使用します。

1 証明書のインポート

EAP-TLS 認証で必要となる、ユーザの証明書をインポートします。

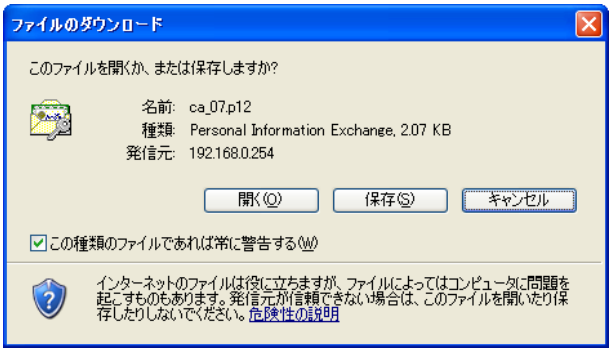
本装置管理者またはユーザ管理者から自分のユーザ ID、パスワード、証明書のパスフレーズを入手します。
本装置管理者またはユーザ管理者であれば RADIUS のメニュー「ユーザ」でこれらの情報を確認できます。安全な手段でユーザに伝えるようにしてください。

与えられたユーザ ID とパスワードを用いて Web ブラウザから本装置にログインして、自分の証明書をダウンロードします。



証明書表示画面へのアクセスの仕方についての詳細は「**第 11 章 ユーザメニュー**」を参照してください。
各証明書と秘密鍵が必要になるため、ここでは PKCS#12 形式で内容に「CA 証明書・証明書・私有鍵」を選択した場合で説明します。
「取り出し」ボタンをクリックすると、証明書のダウンロードが開始されます。

ダウンロードしたファイルをアプリケーションで開くか保存するかを確認する画面が表示されるので、「開く」をクリックします。



上記確認画面はブラウザによって異なります。

証明書のインポートウィザードが起動します。
画面の指示に従って証明書をインポートします。
途中パスワードの入力を求められるので管理者から入手したパスフレーズを入力するようにします。

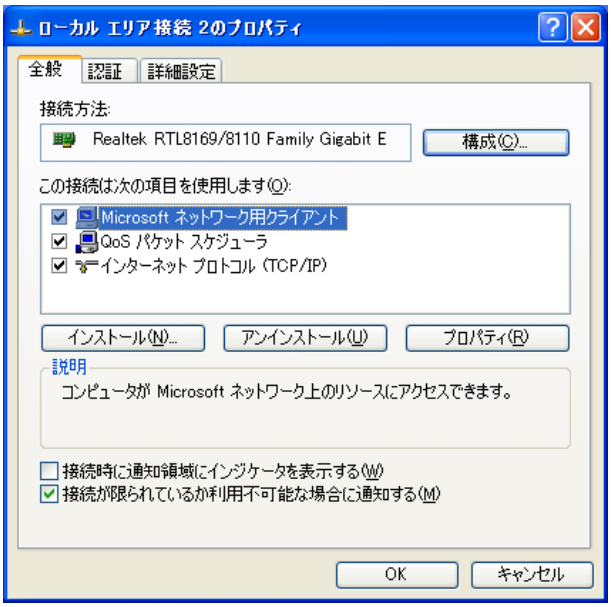
以上でユーザの証明書がインポートされます。

2 EAP-TLS の設定

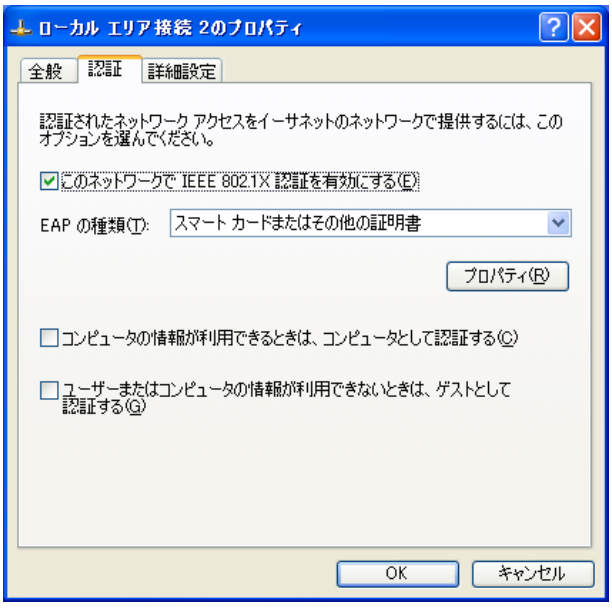
EAP-TLS の設定をします。

コントロールパネルから「ネットワーク接続」をダブルクリックします。

EAP-TLS接続を設定したいインタフェースを右クリックして「プロパティ」を選択します。次の画面が表示されます。



認証タブを選択します。

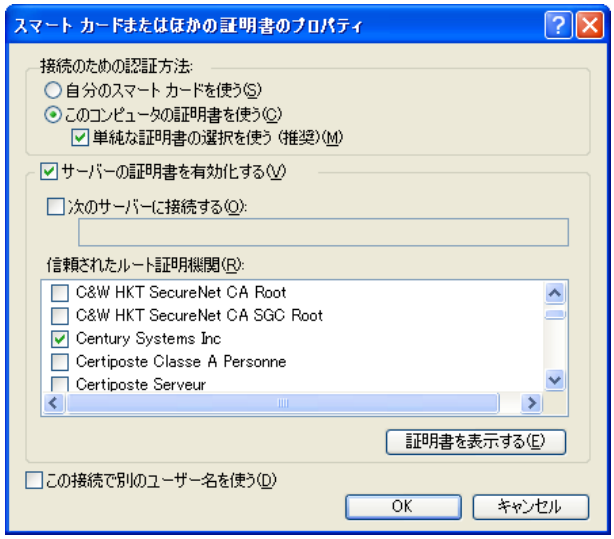


「このネットワークで IEEE 802.1X を有効にする」をチェックします。
「EAP の種類」で「スマートカードまたはその他の証明書」を選択します。
(EAP-MD5 認証の場合は「MD5-Challenge」を、EAP-PEAP の場合は「保護された EAP(PEAP)」を選択するようにします。なお、サービスパックの適用状況によっては「MD5-Challenge」は選択できない場合があります。)

「プロパティ」ボタンをクリックして、保護された EAP のプロパティを表示します。
以下の項目がチェックされていることを確認します。

- このコンピュータの証明書を使う
- 単純な証明書の選択を使う
- サーバーの証明書を有効化する

「信頼されたルート証明機関」で、インポートした証明書を発行した CA の名前を選択します。



以上で設定は終了です。
EAP-TLS認証を必要とするネットワークにつなぐことで認証がおこなわれ、認証に成功すると通信がおこなえるようになります。

II．設定例(EAP-PEAP)

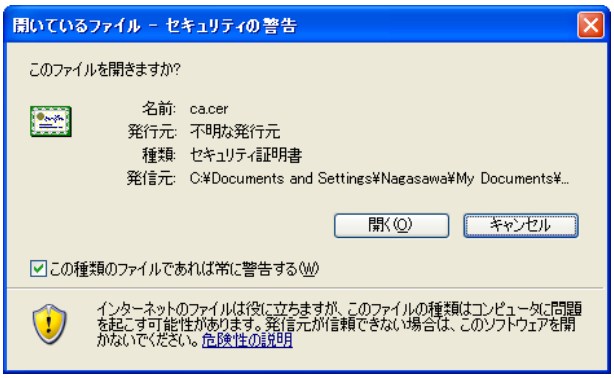
ここでは、EAP-PEAP で認証をおこなう場合に必要な PC の設定について設定例を記述します。

1 CA 証明書のインポート

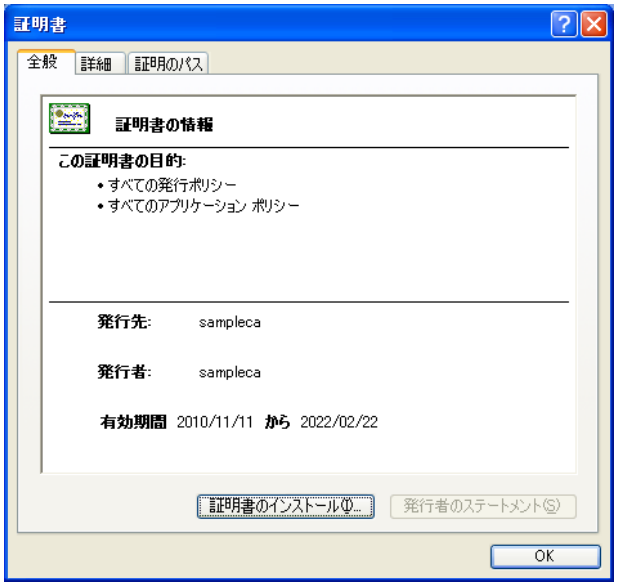
EAP-PEAP 認証で必要となる、CA 証明書をインポートします。

あらかじめ取得しておいた CA 証明書をクリックします。

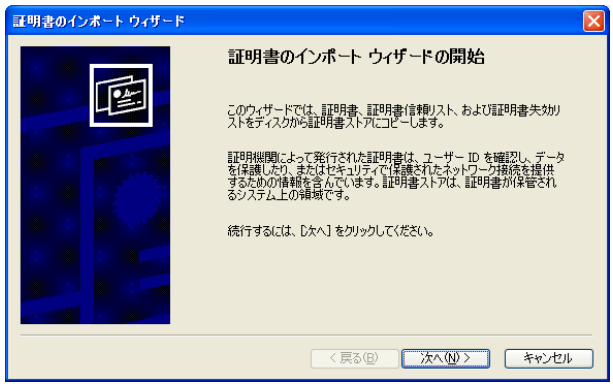
次の画面が表示されるので「開く」をクリックします。



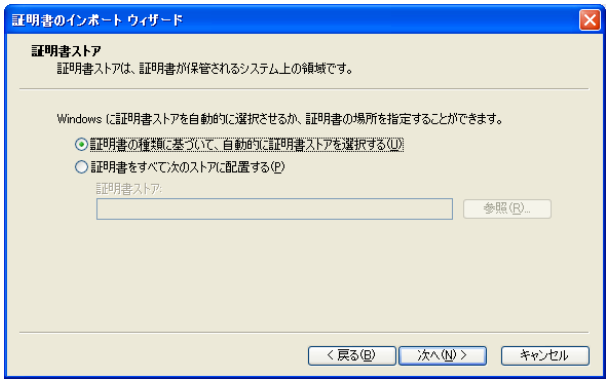
「証明書」の画面が表示されます。「証明書のインストール」をクリックします。



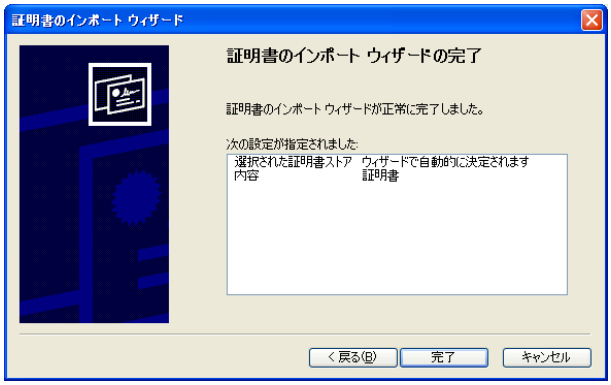
証明書のインポートウィザードが開始されます。下の画面で「次へ」をクリックします。



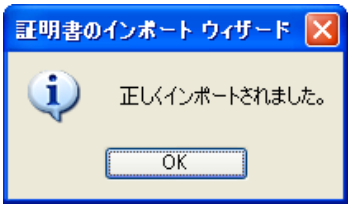
証明書ストアの画面が表示されます。「証明書の種類に基づいて、自動的に証明書ストアを選択する(U)」を ON にして、「次へ」をクリックします。



次の画面で「完了」をクリックします。



証明書が正しくインポートされると、次の画面が表示されます。

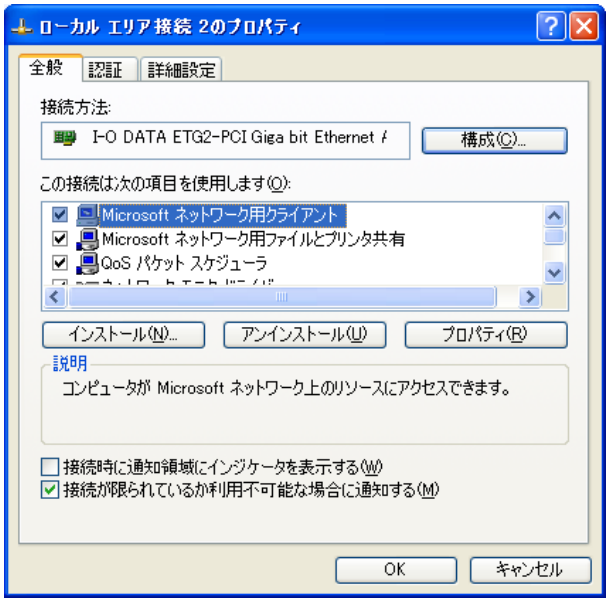


2 EAP-PEAP の設定

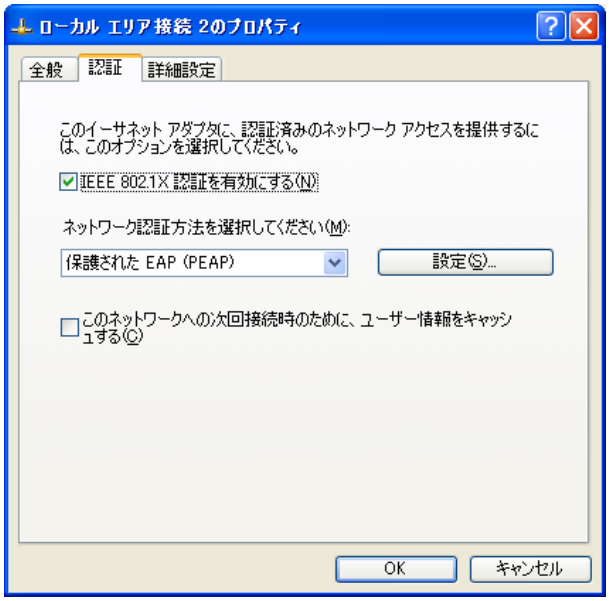
WindowsXP に標準で含まれているサプリカントを使用して、EAP-PEAP の設定を行います。

コントロールパネルから「ネットワーク接続」をクリックします。

EAP-PEAP 接続を設定したいインタフェースを右クリックして「プロパティ」を選択します。次の画面が表示されます。

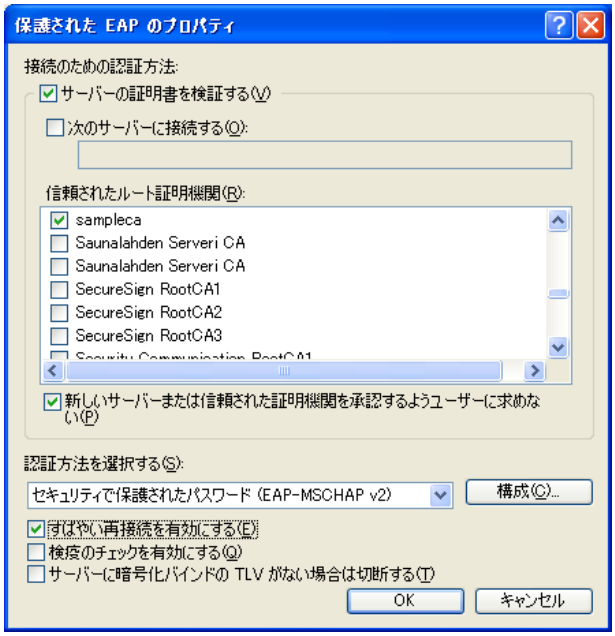


認証タブを選択すると、下記の画面が表示されます。



「IEEE 802.1X を有効にする」をチェックします。ネットワーク認証方法として「保護された EAP (PEAP)」を選択します。

「設定」ボタンをクリックします。「保護された EAP のプロパティ」が表示されます。



「サーバーの証明書を検証する」がチェックされていることを確認します。

「信頼されたルート証明機関」で、インポートした証明書を発行した CA の名前を選択します。

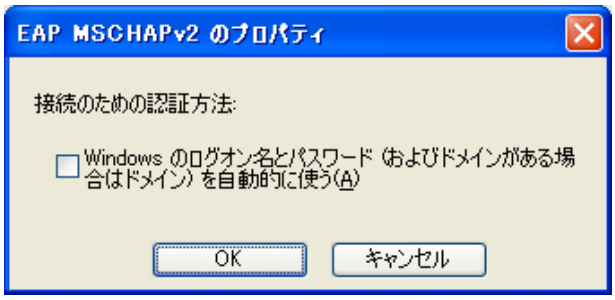
「認証方法を選択する」で「セキュリティで保護されたパスワード(EAP-MSCHAP v2)」を選択します。

「すばやい再接続を有効にする」は、使用する環境に合わせて、ON/OFF を選択してください。
(この例では、ON にしています。)

＜次ページに続く＞

II．設定例(EAP-PEAP)

「構成」をクリックすると、EAP MSCHAPv2 のプロパティが表示されます。



Windowsのログオン名とパスワードを自動的に使う場合は、チェックボックスを ON にします。
（この例では、OFF にしています。）

以上で設定は終了です。

EAP-PEAP 認証を必要とするネットワークに接続すると、下記のポップアップ画面が表示されます。

ユーザ名とパスワードを入力して、OK をクリックすると認証が行われます。
(ログオンドメインが必要な場合は、ログオンドメインも入力します。)

認証に成功すると通信が行えるようになります。

III . 設定例(EAP-TTLS)

ここでは、EAP-TTLS で認証をおこなう場合に必要な PC の設定について設定例を記述します。

1 CA 証明書のインポート

EAP-TTLS 認証で必要となる、CA 証明書をインポートします。

CA 証明書のインポートについては、「第 12 章 一般ユーザによる PC の設定」の「II . 設定例(EAP-PEAP)」を参照してください。

2 EAP-TTLS の設定

Windows 標準のサプリカントは、EAP-TTLS に対応していないため、設定例は記載しません。

第 13 章

復旧操作

Init(INIT)スイッチの操作

RA-1200・RA-730 の前面にある「Init スイッチ」を使用して、**工場出荷設定に戻す**ことができます。

RA-1200

1 本装置が停止状態になっていることを確認します。
2 本体前面にある「Init スイッチ」を押します。
3 「Init スイッチ」を押したままの状態で、「Power スイッチ」をオンにします。
4 「Init スイッチ」を約 3 秒間押し続けると「Init LED」が点灯します。
5 「Init スイッチ」を放します。
6 本装置が工場出荷設定で起動します。
起動が完了すると、「Status1 LED」が点灯(●)し、「Init LED」は消灯(●)します。

RA-730

「Init スイッチ」を押したまま電源切断→電源投入し、
電源投入後 20 秒ほど「Init スイッチ」を押し続けると、設定が消去され、工場出荷時設定に戻ります。
「Status LED 3」が点灯(●)していることを確認してください。

付録 A

最大数一覧

付録 A

最大数一覧

RAの最大設定数を下記の表に示します。

階層1	階層2	項目	RA-1200	RA-730
RADIUS	サーバ	ベンダ	10	10
		アトリビュート(ベンダあたり)	10	10
		アドレスプール	100	10
		アドレス（アドレスプールあたり)	2,000	2,000
		クライアント	1,000	250
		LDAPアトリビュートマップ	10	10
		LDAPサーバ	10	10
		レルム	10	10
	プロファイル	ユーザプロファイル	100	20
		ユーザ基本情報プロファイル	100	20
		認証プロファイル	20	20
		認証アトリビュート(プロファイルあたり)	10	10
		応答プロファイル	20	20
		応答アトリビュート(プロファイルあたり)	10	10
		グループIDプロファイル	50	50
		証明書プロファイル	20	20
	ユーザ	ユーザ(1.10.2以降)	100,000	2,000
		ユーザ(1.10.1以前)	50,000	2,000
		ユーザ個別設定(認証) (ユーザあたり)	5	5
		ユーザ個別設定(応答) (ユーザあたり)	5	5
		ユーザ証明書 (ユーザあたり)	10,000	2,000
CA	証明書	証明書(ユーザ証明書を含む)	10,000	2,000
管理機能	ネットワーク	スタティックルート	10	10
		フィルタ	20	20
		DHCPネットワーク	5	5
		DHCPリースアドレス範囲（ネットワークあたり）	16	16
		DHCPリースアドレス範囲（全体）	64	64
		DHCPリースアドレス	8,192	1,024
		DHCP固定割り当て	256	256
	システム	ログ転送　転送先IPアドレス	5	5
		ユーザ管理者	5	5
		同期コンフィグ（親子連携有効時）	50	1
		同期コンフィグ（親子連携無効時）	1	1

■ 備考

全ての設定項目を同時に最大数まで設定することはできません。

データ数が大量となる可能性のあるユーザやアトリビュートに関しては、以下のような内容を想定しています。

付録 A

最大数一覧

(RA-1200)

- ユーザ:
  - 100,000個程度まで（証明書総数が10個程度を超えない場合)
  - 10,000 個程度まで（証明書総数が10個程度を超える場合)
- アトリビュート:

  ユーザを100,000個設定するとして、
  - 認証・応答プロファイルおよび個別設定(認証・応答)全てを合計してユーザあたり5～6個まで
  - アトリビュートの値の長さは50文字（25～50オクテットに相当)まで

(RA-730)

- ユーザ:
  - 2,000個程度まで（証明書総数に関わらず)
- アトリビュート:

  ユーザを2,000個設定するとして、
  - 認証・応答プロファイルおよび個別設定(認証・応答)全てを合計してユーザあたり5～6個まで
  - アトリビュートの値の長さは50文字（25～50オクテットに相当)まで

これらを超えて設定した場合、正しく動作しない可能性があります。但し、あるユーザ群には10個以上アトリビュートを指定する代わりに別のユーザ群にはアトリビュートを指定しない、のような運用は可能です。

付録 A

最大数一覧

また、大量のデータがある場合、想定内の設定数であっても操作内容によっては比較的時間が掛かることがあります（数分以上)。　設定データによっては正常に操作を行うことができないこともあります。

- ユーザプロファイルに割り当てられたユーザ基本情報プロファイルを 別の基本情報プロファイルに変更する
- ユーザプロファイルに割り当てた認証・応答・グループ ID プロファイルを別の認証・応答・グループ ID プロファイルに変更する(認証・応答・グループ ID プロファイルの新規割り当てや割り当ての解除も含む)
- ユーザ基本情報プロファイル内の情報を変更する(値の変更)
- 認証・応答プロファイル内の情報を変更する(アトリビュートの追加・削除や値の変更)
- グループ ID プロファイル内の情報を変更する(値の変更)
- ユーザ個別設定（基本）の情報を変更する(値の変更)
- ユーザ個別設定（認証・応答）の情報を変更する(アトリビュートの追加・削除や値の変更)
- ユーザ設定情報をリセットする

などの操作が該当します。 これらの操作中は RADIUS 認証は行われません。

RAで記録できるログの数の上限を下記の表に示します。

	RA-1200	RA-730
認証ログ	100,000	40,000
オペレーションログ	10,000	10,000
アクセスログ	10,000	10,000
アカウンティングログ	100,000	40,000
システムログ	10,000	10,000

付録 B

サポートについて

付録 B

サポートについて

◆本製品に関してのサポートは、ユーザー登録をされたお客様に限らせていただきます。必ずユーザー登録していただきますよう、お願いいたします。

◆サポートに関する技術的なお問い合わせやご質問は、下記へご連絡ください。
- サポートデスク
  電話 0422-37-8926
  受付時間　10:00～17:00　(土日祝祭日、及び弊社の定める休日を除きます)
- FAX　0422-55-3373
- e-mail　support@centurysys.co.jp
- ホームページ　https://www.centurysys.co.jp/

◆故障と思われる場合は
製品の不良や故障と思われる場合でも、必ず事前に弊社までご連絡ください。事前のご連絡なしに弊社までご送付いただきましてもサポートをお受けすることはできません。

◆ご連絡をいただく前に
スムーズなユーザーサポートをご提供するために、サポートデスクにご連絡いただく場合は以下の内容をお知らせいただきますよう、お願いいたします。
- ファームウェアのバージョンと MAC アドレス
  (バージョンは運用機能の「システム情報」メニューで確認できます。)
- ネットワークの構成(図)
  どのようなネットワークで運用されているか、差し支えのない範囲でお知らせください。
- 不具合の内容または、不具合の再現手順
  何をしたときにどういう問題が発生するのか、できるだけ具体的にお知らせください。
- エラーメッセージ
  エラーメッセージが表示されている場合は、できるだけ正確にお知らせください。
- 本装置の設定内容
- **可能であれば、「設定のバックアップファイル」をお送りください。**

◆サポート情報
弊社ホームページにて、製品の最新ファームウェア、マニュアル、製品情報を掲載しています。また製品の FAQ も掲載しておりますので、是非ご覧ください。
RA-1200 製品サポートページ
https://www.centurysys.co.jp/support/RA1200.html
RA-730 製品サポートページ
https://www.centurysys.co.jp/support/RA730.html

◆製品の保証について
本製品の保証期間は、お買い上げ日より 1 年間です。保証期間をすぎたもの、保証書に販売店印のないもの(弊社より直接販売したものは除く)、また保証の範囲外の故障については有償修理となりますのでご了承ください。保証規定については、同梱の保証書をご覧ください。

付録 C

ユーザ設定情報のファイルフォーマット

付録 C

ユーザ設定情報のファイルフォーマット

RADIUS メニューの「ユーザ」-「ファイル読み込み」では、あらかじめ設定ファイルを用意して読み込ませることで大量のユーザをまとめて設定することができます。ここではこの機能を使ってユーザを作成するためのユーザ設定情報のファイルの形式について説明します。

ユーザ設定情報のファイルの形式は、管理機能メニューの[システム]-[設定の保存・復帰」で作成される設定保存ファイルに準じたファイルフォーマットになっています。

利用可能な文字コードは、「EUC-JP」または「Shift_JIS」です。

ユーザ設定情報は以下のセクションに分けて定義します。

・[RADIUS| プロファイル | 基本]
　ユーザ基本情報プロファイルの設定

・[RADIUS| プロファイル | 認証プロファイル]
　認証アトリビュートプロファイルの設定

・[RADIUS| プロファイル | 認証アトリビュート]
　認証アトリビュートの設定

・[RADIUS| プロファイル | 応答プロファイル]
　応答アトリビュートプロファイルの設定

・[RADIUS| プロファイル | 応答アトリビュート]
　応答アトリビュートの設定

・[RADIUS| プロファイル | グループ ID]
　グループ ID プロファイルの設定

・[RADIUS| プロファイル | 証明書]
　証明書プロファイルの設定

・[RADIUS| プロファイル | ユーザプロファイル]
　ユーザプロファイルの設定

・[RADIUS| ユーザ]
　ユーザの設定

・[RADIUS| ユーザ | 基本]
　ユーザ個別設定(基本情報)

・[RADIUS| ユーザ | 認証アトリビュート]
　ユーザ個別設定(認証アトリビュート)

・[RADIUS| ユーザ | 応答アトリビュート]
　ユーザ個別設定(応答アトリビュート)

・[RADIUS| ユーザ | 証明書発行]
　ユーザ証明書の設定

各セクション毎にファイル読み込みを実行する必要があります 。

作成するデータが無いセクションについてはファイル読み込みを実行する必要はありません。

複数のデータを記述する場合、各データを空白行で区切る必要があります。

(RA-1200)
1回のファイル読み込みで設定できるデータは10,000 件です。

(RA-730)
1回のファイル読み込みで設定できるデータは2,000 件です。

ファイルの末尾には改行コードが必要です。

各セクション内の記述の仕方について、以下順に説明します。

付録 C

ユーザ設定情報のファイルフォーマット

○[RADIUS| プロファイル | 基本]
ユーザ基本情報プロファイルについて記述します。

設定例

```
[RADIUS| プロファイル | 基本]
create basic
  config_id=config01
  profile_name=base01
  auth_type=2
  simul_conn_count=3
  ipaddress_allocate=2
  addrpool=pool01
```

データの先頭は create basic という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
profile_name	プロファイル名
auth_type	認証方式
0	PAP/CHAP
1	EAP-MD5
2	EAP-TLS
3	EAP-PEAP
4	EAP-TTLS/PAP,CHAP
7	EAP-TTLS/EAP-MD5
8	EAP-TTLS/EAP-PEAP
simul_conn_count	同時接続数
ipaddress_allocate	IP アドレス割り当て
0	未使用
1	RADIUS クライアント
2	アドレスプール
3	固定
addrpool	アドレスプール

○[RADIUS| プロファイル | 認証プロファイル]
認証アトリビュートプロファイルについて記述します。
設定例

```
[RADIUS| プロファイル | 認証プロファイル]
create profile
  config_id=config01
  profile_name=auth01
```

データの先頭は create profile という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
profile_name	プロファイル名

プロファイル中のアトリビュートは次のセクションで記述します。

○[RADIUS| プロファイル | 認証アトリビュート]
認証アトリビュートについて記述します。

設定例

```
[RADIUS| プロファイル | 認証アトリビュート]
create attribute
  config_id=config01
  auth=auth01
  attribute=Called-Station-Id
  value=000000000000
```

データの先頭は create attribute という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
auth	認証プロファイル名
attribute	アトリビュート
value	値

付録 C

ユーザ設定情報のファイルフォーマット

○[RADIUS| プロファイル | 応答プロファイル]
応答アトリビュートプロファイルについて記述します。

設定例

```
[RADIUS| プロファイル | 応答プロファイル]
create profile
  config_id=config01
  profile_name=resp01
```

データの先頭は create profile という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
profile_name	プロファイル名

プロファイル中のアトリビュートは次のセクションで記述します。

○[RADIUS| プロファイル | 応答アトリビュート]
応答アトリビュートについて記述します。

設定例

```
[RADIUS| プロファイル | 応答アトリビュート]
create attribute
  config_id=config01
  resp=resp01
  attribute=Reply-Message
  value=aaaaaa
```

データの先頭は create attribute という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
resp	応答プロファイル名
attribute	アトリビュート
value	値

○[RADIUS| プロファイル | グループ ID]
グループ ID プロファイルについて記述します。

設定例

```
[RADIUS| プロファイル | グループ ID]
create group
  config_id=config01
  profile_name=group01
  group_id=ggg
```

データの先頭は create group という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
profile_name	プロファイル名
group_id	グループ ID

付録 C

ユーザ設定情報のファイルフォーマット

○[RADIUS| プロファイル | 証明書]
証明書プロファイルについて記述します。
設定例

```
[RADIUS| プロファイル | 証明書]
create cert
  config_id=config01
  profile_name=cert01
  version=3
  key_length=1024
  sign_algorithm=SHA-1
  subject_ou=
  subject_o=
  subject_l=
  subject_s=
  subject_c=JP
  not_before_year=2006
  not_before_month=5
  not_before_day=1
  not_before_hour=0
  not_before_min=0
  not_after_year=2006
  not_after_month=12
  not_after_day=31
  not_after_hour=23
  not_after_min=59
  digitalSignature=on
  nonRepudiation=
  keyEncipherment=on
  dataEncipherment=
  keyAgreement=
  keyCertSign=
  cRLSign=
  enciperOnly=
  decipherOnly=
  ExtendedKeyUsage=clientAuth
  CRLDistributionPoints=
```

データの先頭は create cert という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
profile_name	プロファイル名
version	バージョン: 1 または 3
key_length	鍵長: (～ ver1.11.0) 2048, 1024, 512 (ver1.12.0 ～) 2048, 1024
sign_algorithm	Signature Algorithm: (～ ver1.8.4) 「SHA-1」または「MD5」 (ver1.8.5 ～ 1.11.0) 「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれか (ver1.12.0 ～) 「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれか
subject_ou	Organizational Unit
subject_o	Organization
subject_l	Locality
subject_s	State or Province
subject_c	Country
not_before_year	開始日時 年
not_before_month	開始日時 月
not_before_day	開始日時 日
not_before_hour	開始日時 時
not_before_min	開始日時 分
not_after_year	終了日時 年
not_after_month	終了日時 月
not_after_day	終了日時 日
not_after_hour	終了日時 時
not_after_min	終了日時 分
digitalSignature	digitalSignature: on または 空文字列
nonRepudiation	nonRepudiation: on または 空文字列
keyEnciphermen	keyEncipherment: on または 空文字列
dataEncipherment	dataEncipherment: on または 空文字列
keyAgreement	keyAgreement: on または 空文字列
keyCertSign	keyCertSign: on または 空文字列
cRLSign	cRLSign: on または 空文字列
enciperOnly	enciperOnly: on または 空文字列
decipherOnly	decipherOnly: on または 空文字列
ExtendedKeyUsage	ExtendedKeyUsage: serverAuth, clientAuth, codeSigning, emailProtection
CRLDistributionPoints	CRL Distribution Points

付録 C

ユーザ設定情報のファイルフォーマット

○[RADIUS| プロファイル | ユーザプロファイル]
ユーザプロファイルについて記述します。

設定例

```
[RADIUS| プロファイル | ユーザプロファイル]
create userprofile
  config_id=config01
  profile_name=profile01
  base=base01
  auth=auth01
  cert=cert01
  resp=
  group=
```

データの先頭は create userprofile という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
profile_name	プロファイル名
base	基本情報プロファイル名
auth	認証プロファイル名
resp	応答プロファイル名
group	グループプロファイル名
cert	証明書プロファイル名

○[RADIUS| ユーザ]
ユーザについて記述します。

設定例

```
[RADIUS| ユーザ]
create user
  config_id=config01
  user_id=user01
  password=pass01
  profile=prof01
  locked=on|off
  ipaddress=
  netmask=
  notes=
```

データの先頭は create user という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
user_id	ユーザ ID
password	パスワード
profile	プロファイル名
locked	ロック: on または off (空文字列は off と同義)
ipaddress	IP アドレス
netmask	ネットマスク
notes	備考 入力できない文字がある場合、それらの文字は削除されます。または〓に変換されます。

付録 C

ユーザ設定情報のファイルフォーマット

○[RADIUS| ユーザ | 基本]
ユーザ基本情報の個別設定について記述します。

設定例

```
[RADIUS| ユーザ | 基本]
create base
  user=user01
  config_id=config01
  user_profile=profile01
  auth_type=2
  simul_conn_count=3
  ipaddress_allocate=2
  addrpool=pool01
```

データの先頭は create base という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

user	個別設定をおこなうユーザ名。グループ ID が指定されている場合、グループ名も含めて指定してください。
config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
user_profile	ユーザプロファイル名 このユーザに割り当てられているユーザプロファイルを指定してください。
auth_type	認証方式 0 PAP/CHAP 1 EAP-MD5 2 EAP-TLS 3 EAP-PEAP 4 EAP-TTLS/PAP,CHAP 7 EAP-TTLS/EAP-MD5 8 EAP-TTLS/EAP-PEAP
simul_conn_count	同時接続数
ipaddress_allocate	IP アドレス割り当て 0 未使用 1 RADIUS クライアント 2 アドレスプール 3 固定
addrpool	アドレスプール

○[RADIUS| ユーザ | 認証アトリビュート]
認証アトリビュートの個別設定について記述します。

設定例

```
[RADIUS| ユーザ | 認証アトリビュート]
create auth
  user=user01
  config_id=config01
  user_profile=profile01
  attribute=Calling-Station-Id
  value=000000000000
  mode=override
```

データの先頭は create auth という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

user	個別設定をおこなうユーザ名。グループ ID が指定されている場合、グループ名も含めて指定してください。
config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
user_profile	ユーザプロファイル名 このユーザに割り当てられいるユーザプロファイルを指定してください。
attribute	アトリビュート
value	値
mode	動作モード
override	上書き
remove	削除

付録 C

ユーザ設定情報のファイルフォーマット

○[RADIUS| ユーザ | 応答アトリビュート]
応答アトリビュートについて記述します。

設定例

```
[RADIUS| ユーザ | 応答アトリビュート]
create resp
  user=user01
  config_id=config01
  user_profile=profile01
  attribute=Session-Timeout
  value=100
  mode=append
```

データの先頭は create resp という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

user	個別設定をおこなうユーザ名。グループ ID が指定されている場合、グループ名も含めて指定してください。
config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
user_profile	ユーザプロファイル名 このユーザに割り当てられているユーザプロファイルを指定してください。
attribute	アトリビュート
value	値
mode	動作モード override 上書き append 追加 remove 削除

○[RADIUS| ユーザ | 証明書発行]
ユーザ証明書を新規発行するための情報を記述します。

設定例

```
[RADIUS| ユーザ | 証明書発行]
create cert
  user=user01
  config_id=config01
  passphrase=password
  version=3
  key_length=1024
  sign_algorithm=SHA-1
  subject_email=
  subject_cn=user01
  subject_ou=
  subject_o=
  subject_l=
  subject_s=
  subject_c=JP
  not_before_year=2006
  not_before_month=5
  not_before_day=1
  not_before_hour=0
  not_before_min=0
  not_after_year=2006
  not_after_month=12
  not_after_day=31
  not_after_hour=23
  not_after_min=59
  digitalSignature=on
  nonRepudiation=
  keyEncipherment=on
  dataEncipherment=
  keyAgreement=
  keyCertSign=
  cRLSign=
  enciperOnly=
  decipherOnly=
  ExtendedKeyUsage=clientAuth
  CRLDistributionPoints=
  csr=--_____FILE
  -----BEGIN CERTIFICATE REQUEST-----
  MIIBEzCBvgIBADBZMQswCQYDVQQGE...
```

付録 C

ユーザ設定情報のファイルフォーマット

```
...
...UB4OrpxTVdU7TdMsrzALK6+WxaLrWi
-----END CERTIFICATE REQUEST-----
--_____________________________FILE--
```

データの先頭は create cert という行になります。以降の設定行と設定画面上の項目との対応は以下となります。

user	ユーザ名。グループ ID が指定されている場合、グループ名も含めて指定してください。
config_id	同期コンフィグ名 親子連携無効時は空文字列を指定してください。省略も可能です。
passphrase	パスフレーズ
version	バージョン: 1 または 3
key_length	鍵長: (〜 ver1.11.0) 2048, 1024, 512 (ver1.12.0 〜) 2048, 1024
sign_algorithm	Signature Algorithm: (〜 ver1.8.4) 「SHA-1」または「MD5」 (ver1.8.5 〜 1.11.0) 「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」、「MD5」のいずれか (ver1.12.0 〜) 「SHA-512」、「SHA-384」、「SHA-256」、「SHA-1」のいずれか
subject_email	email
subject_cn	Common Name。ユーザ名を指定して下さい。 グループ ID が指定されている場合、グループ名も含めて指定してください。
subject_ou	Organizational Unit
subject_o	Organization
subject_l	Locality
subject_s	State or Province
subject_c	Country
not_before_year	開始日時 年
not_before_month	開始日時 月
not_before_day	開始日時 日
not_before_hour	開始日時 時
not_before_min	開始日時 分
not_after_year	終了日時 年
not_after_month	終了日時 月
not_after_day	終了日時 日
not_after_hour	終了日時 時
not_after_min	終了日時 分
digitalSignature	digitalSignature: on または 空文字列
nonRepudiation	nonRepudiation: on または 空文字列
keyEnciphermen	keyEncipherment: on または 空文字列
dataEncipherment	dataEncipherment: on または 空文字列
keyAgreement	keyAgreement: on または 空文字列
keyCertSign	keyCertSign: on または 空文字列
cRLSign	cRLSign: on または 空文字列
enciperOnly	enciperOnly: on または 空文字列
decipherOnly	decipherOnly: on または 空文字列
ExtendedKeyUsage	ExtendedKeyUsage: serverAuth, clientAuth, codeSigning, emailProtection
CRLDistributionPoints	CRL Distribution Points
csr	証明書署名要求(※)

※ユーザファイル読み込み機能の独自機能として、証明書署名要求(Certificate Signing Request)を使った証明書発行ができます。証明書署名要求を使う場合には csr 行に PKCS#10 (BASE64 encoded) 形式の証明書署名要求データを指定するようにします。設定画面から証明書を発行する場合と同様に、本装置上で鍵生成をおこなう場合には csr 行は空文字列にします。

付録 C

ユーザ設定情報のファイルフォーマット

証明書発行セクションのユーザ ID、バージョン、鍵長、Signature Algorithm、Common Name、終了日時の各項目は空欄には出来ません。空欄にした項目に対して証明書プロファイルでデータが設定されている場合には、証明書プロファイルのデータを使って証明書を作成します。パスフレーズを空欄にした場合は、ユーザに設定されているパスワードが使用されます。

付録 C

ユーザ設定情報のファイルフォーマット

ファイル読み込みの実行例

■ファイル 1

```
[RADIUS| プロファイル | 基本]
create basic
  config_id=config01
  profile_name=base01
  auth_type=2
  simul_conn_count=
  ipaddress_allocate=0
  addrpool=
```

■ファイル 2

```
[RADIUS| プロファイル | ユーザプロファイル]
create userprofile
  config_id=config01
  profile_name=prof01
  base=base01
  auth=
  cert=
  resp=
  group=
```

■ファイル 3

```
[RADIUS| ユーザ]
create user
  config_id=config01
  user_id=user01
  password=pass01
  profile=prof01
  ipaddress=
  netmask=
  notes=

create user
  config_id=config01
  user_id=user02
  password=pass02
  profile=prof01
  ipaddress=
  netmask=
  notes=
```

ファイル 1 ～ファイル 3 を順次読み込ませることで、ユーザ基本情報プロファイル “ base01 ” の作成、ユーザプロファイル “ prof01 ” の作成、“ prof01 ” をプロファイルに指定したユーザ “ user01 ” および “ user02 ” の作成を行うことができます。

この例では親子連携が有効になっています (config_id=config01)。
親子連携が無効の場合は、同期コンフィグ名 config_id に空文字列を指定してください。
省略も可能です。

付録 D

用語説明

付録 D

用語説明

[Acct-Authentic]
アカウンティング記録用の RADIUS のアトリビュート。ユーザーがどのように認証されたか、Radius によるのか、NAS 自身でか、他の認証プロトコルでかを示すためにアカウンティング要求に含められます。

[Acct-Delay-Time]
アカウンティング記録用の RADIUS のアトリビュート。RADIUS クライアントが今まで何秒間このレコードを送ろうとしていたか示します。サーバへの到着時刻から引くことでこのアカウンティング要求が生成されたおよその時間がわかります。

[Acct-Input-Octets]
アカウンティング記録用の RADIUS のアトリビュート。このサービスが提供されているポートで何オクテット受信したかを示すもので、Acct- Status-Type が Stop のアカウンティング要求レコードでだけ存在しています。

[Acct-Input-Packets]
アカウンティング記録用の RADIUS のアトリビュート。このサービスが提供されているポートで何パケット受信したかを示すもので、Acct- Status-Type が Stop のアカウンティング要求レコードでだけ存在しています。

[Acct-Output-Octets]
アカウンティング記録用の RADIUS のアトリビュート。このサービスが提供されているポートで何オクテット送信したかを示すもので、Acct-Status-Type が Stop のアカウンティング要求レコードでだけ存在しています。

[Acct-Output-Packets]
アカウンティング記録用の RADIUS のアトリビュート。このサービスが提供されているポートで何パケット送信したかを示すもので、Acct-Status-Type が Stop のアカウンティング要求レコードでだけ存在しています。

[Acct-Session-Id]
アカウンティング記録用の RADIUS のアトリビュート。ユニークなアカウンティング ID で、ログファイル中のスタートとストップの対応をとる事を容易にします。あるセッションの開始レコードと停止レコードは同じ Acct-Session-Id で記録されます。

[Acct-Session-Time]
アカウンティング記録用の RADIUS のアトリビュート。ユーザーが何秒間サービスを受けたか示します。Acct-Status-Type が Stop に設定されているアカウンティング要求レコードにだけ存在します。

[Acct-Status-Type]
アカウンティング記録用の RADIUS のアトリビュート。アカウンティング要求がユーザサービスの開始または終了のどちらによるものかを示します。

[Acct-Terminate-Cause]
アカウンティング記録用の RADIUS のアトリビュート。どのようにセッションが終了したかを示すもので、Acct-Status-Type が Stop のアカウンティング要求レコードにだけ存在します。

[CA]
電子的な身分証明書を発行し、管理する機関。
証明書所有者の鍵ペア（私有鍵と公開鍵）に対して公開鍵証明書を発行します。

[Called-Station-Id]
認証要求時に NAS から RADIUS サーバに送られるアトリビュートの一つで、ユーザがダイアルした電話番号などが入れられます。802.1X 使用時には MAC アドレスが通常入れられます。

[Calling-Station-Id]
認証要求時に NAS から RADIUS サーバに送られるアトリビュートの一つで、電話をかけた側の電話番号などが入れられます。802.1X 使用時には MAC アドレスが通常入れられます。

[CA 証明書]
CA 自身の公開鍵証明書。CA 証明書に含まれる CA の公開鍵を使って、他の証明書の電子署名を検証することで、その証明書が正当なものであるかを検証することができます。

[CHAP]
PPP などにおけるチャレンジ・レスポンス方式を利用したユーザー認証方法。PAP に比べて、ユーザー名やパスワード情報をそのまま流さないので、安全性が高くなります。

[client IP address]
アカウンティングログに記録する項目。
RADIUS クライアントの IP アドレスが記録されます。

[clientAuth]
X.509 v3 証明書の拡張情報に含まれ、本証明書がクライアント認証（SSL/TLS による認証時にサーバ側がクライアントを認証する）に利用できることを表しています。

付録 D

用語説明

[codeSigning]
X.509 v3 証明書の拡張情報に含まれ、本証明書がコード署名に利用できることを表しています。

[Common Name]
X.509 証明書が証明する対象である Subject の一部。ユーザ名、サーバ名等を記述します。

[Country]
X.509 証明書が証明する対象である Subject の一部。国名を記述します。日本であれば "JP" になります。

[CRL]
さまざまな理由により有効期間内に失効した証明書のリスト。
→ 証明書、失効

[CRL Distribution Points]
CRL を配布する場所。URI(http://... 等)で指定します。
→ CRL

[cRLSign]
X.509 v3 証明書の拡張情報に含まれ、本証明書が失効リストの署名の検証に利用できることを表しています。

[CSR]
→ 証明書署名要求

[dataEncipherment]
X.509 v3 証明書の拡張情報に含まれ、本証明書がデータの暗号化に利用できることを表しています。

[decipherOnly]
X.509 v3 証明書の拡張情報に含まれ、鍵交換をデータの復号化でのみ利用できることを表しています。
keyAgreement が指定されている場合のみ有効です。

[DER 形式]
もともとバイナリ形式である証明書をファイル化するためのエンコード形式の一種。
Netscape 等で使用されています。

[DF フラグ]
このフラグを立てると IP パケットが配送途中で分割されないことを要求します。

[digitalSignature]
X.509 v3 証明書の拡張情報に含まれ、デジタル署名の検証に利用できることを表しています。

[Distinguished Name]
ITU-T X.500 で定義されている、オブジェクトを一意に表現する識別子。

[EAP]
リモートアクセスによるユーザー認証の際に用いられるプロトコルで、PPP を拡張し、追加的な認証方法をサポートします。
EAP-TLS、EAP-TTLS、EAP-PEAP など、さまざまな方式があります。

[EAP-MD5]
EAP フレームワーク上で CHAP 認証をおこなう認証方式。

[EAP-PEAP]
EAP-TTLS のコアアーキテクチャをベースにしてシスコシステムズ、マイクロソフト、RSA セキュリティの 3 社により作成された認証方式。

[EAP-TLS]
TLS（Transport Layer Security）を用いて、電子証明書による相互認証をおこなう認証方式。

[EAP-TTLS]
サーバ側は証明書、クライアント側はユーザ名とパスワードを用いる認証方式。
IETF の Proposed Standard。

[emailProtection]
X.509 v3 証明書の拡張情報に含まれ、電子メールの保護のために利用できることを表しています。

[encipherOnly]
X.509 v3 証明書の拡張情報に含まれ、鍵交換をデータの暗号化でのみ利用できることを表しています。
keyAgreement が指定されている場合のみ有効です。

[Extended Key Usage]
KeyUsage より詳細に、証明書に含まれている公開鍵の使用目的を示します。

[FQDN]
ホスト名等を指定するときに、ドメイン名を省略せずに、トップレベルからのすべての情報を持つドメイン名を表記したもの。

[Framed-IP-Address]
RADIUS のアトリビュートの一つで、ユーザに設定されるべき IP アドレスを表します。

付録 D

用語説明

[Framed-Protocol]
RADIUS のアトリビュートの一つで、PPP のようなフレーム構造を持つプロトコルを表します。

[HTTPS サーバ証明書]
本装置の管理画面に HTTPS で接続する際に使われるサーバ証明書。

[Key Usage]
X.509 v3 証明書の拡張情報に含まれるフィールドで、公開鍵の使用目的を示します。

[keyAgreement]
X.509 v3 証明書の拡張情報に含まれ、鍵交換で利用できることを表しています。

[keyCertSign]
X.509 v3 証明書の拡張情報に含まれ、証明書の署名の検証に利用できることを表しています。

[keyEncipherment]
X.509 v3 証明書の拡張情報に含まれ、鍵を送信する場合に、鍵を暗号化して利用できることを表しています。

[LDAP]
ディレクトリサービスに接続するために使用される通信プロトコルの一種。

[LDAP サーバ]
ディレクトリサービスを提供するサーバソフトウェア。

[LDAPS]
TLS（Transport Layer Security）のコネクション上でディレクトリサービスとの通信をおこなうプロトコル。

[Locality]
X.509 証明書が証明する対象である Subject の一部。市町村名を記述します。

[MIB]
SNMP で管理される機器が保持する自機の状態についての情報。MIB-II が RFC 1213 で規定されています。

[NAS]
ネットワークアクセスサーバ。RADIUSサーバに対してリモートユーザの認証やアカウンティングを依頼する装置。
→ RADIUS クライアント

[NAS-Identifier]
RADIUS のアトリビュートの一つで、Access-Request を送信した NAS を識別するための文字列（FQDN など）が入れられます。

[NAS-IP-Address]
RADIUS のアトリビュートの一つで、ユーザー認証を要求する NAS の IP アドレスを表します。Access-Request パケットでのみ使用されます。

[NAS-Port]
RADIUS のアトリビュートの一つで、NAS の物理ポート番号を表します。Access-Request パケットでのみ使用されます。

[NAS-Port-Type]
RADIUS のアトリビュートの一つで、NAS の物理ポート種別を表します。Access-Request パケットでのみ使用されます。

[Netscape 拡張]
ブラウザの一種である Netscape で使用される証明書のタイプを指定します。

[nonRepudiation]
X.509 v3 証明書の拡張情報に含まれ、否認防止を目的としたデジタル署名の検証に利用できることを表しています。

[NTLM ハッシュ]
UTF-16LE でエンコードされたパスワードを、MD4 を用いてハッシュした 16 バイトの値です。

[OCSP]
証明書の有効性を確認するために、CRL を用いる代わりに、OCSP サーバ宛に証明書の状態を問い合わせるプロトコル。

[OCSPSigning]
X.509 v3 証明書の拡張情報に含まれ、CA が発行した証明書の状態を OCSP レスポンダが返答することを CA 自身が委譲したことを示すために、OCSP レスポンダの証明書の使用目的に含めます。

[Organization]
X.509 証明書が証明する対象である Subject の一部。企業名、組織名などを記述します。

付録 D

用語説明

[Organizational Unit]
X.509 証明書が証明する対象である Subject の一部。部署名を記述します。

[PAP]
PPP で採用されている認証方式の一種。ユーザ ID/ パスワードの送信を平文でおこないます。

[PEM 形式]
もともとバイナリ形式である証明書をファイル化するためのエンコード形式の一種。

[RA]
RA-1200・RA-730 のいずれか、または全てを表す。RA-1200・RA-730 に共通する機能等を説明する時に使用する。

[RADIUS]
ダイヤルアップユーザの認証システム。現在はダイヤルアップ以外の認証やアカウンティングにも広く利用されています。詳細は RFC2865、RFC2866 等を参照してください。

[RADIUS Proxy]
RADIUS サーバが受信した認証要求やアカウンティング要求を他の RADIUS サーバへ転送する機能。
RADIUS Proxy 機能を持った RADIUS サーバ（RADIUS Proxy サーバ）は、RADIUS サーバであるとともに RADIUS クライアントでもあります。

[RADIUS クライアント]
RADIUS サーバに対してリモートユーザの認証やアカウンティングを依頼する機器。
無線 LAN アクセスポイント、認証スイッチ、NAS (Network Access Server)などがあります。

[RADIUS サーバ証明書]
本装置のサーバ証明書。EAP-TLS 認証等で本装置の正当性を示すために用いられます。

[RADIUS 私有鍵]
RADIUS サーバ証明書の公開鍵に対応した秘密鍵。

[serverAuth]
X.509 v3 証明書の拡張情報に含まれ、本証明書がサーバ認証（SSL/TLS による認証時にクライアントがサーバを認証する）に使われることを示します。

[Service-Type]
RADIUS のアトリビュートの一つで、ユーザが要求する、またはユーザに提供されるサービスの種類が指定されます。

[Session-Start-Time]
ユーザが RADIUS プロトコルによる認証を受けた時刻。

[Signature algorithm]
証明書への署名に使うアルゴリズム。

[SNMP]
TCP/IP ネットワークにおいて、ルータやコンピュータ、端末など、ネットワークに接続された通信機器をネットワーク経由で監視・制御するためのプロトコル。

[StartTLS]
LDAP 内で TLS（Transport Layer Security）による認証および暗号化をおこなう通信方式。

[State or Province]
X.509 証明書が証明する対象である Subject の一部。都道府県名などを記述します。

[Subject]
X.509 証明書が証明する対象の情報。

[timestamp(epoc time)]
アカウンティングログに記録する項目。
パケットを受信した時刻を表します。1970/01/01 00:00:00 からの経過秒数です。

[timestamp(yyyy-mm-dd hh:mm:ss)]
アカウンティングログに記録する項目。
パケットを受信した時刻を表します。「2004 年 10 月 31 日 19 時 05 分 20 秒」であれば、"2004-10-31 19:05:20" のフォーマットで記録します。

[timeStamping]
X.509 v3 証明書の拡張情報に含まれ、タイムスタンプサービスが時刻証明に用いる公開鍵を証明するために使用してよい証明書であることを表します。

[User-Name]
RADIUS のアトリビュートの一つで、認証に用いられたユーザ名を表します。

付録 D

用語説明

[VSA]
→ ベンダ固有アトリビュート

[X.509 証明書 v3 拡張]
X.509 証明書のバージョン３で新規に定義された拡張フィールド。
証明書の鍵ペアの使用方法等を定義可能になっています。
RFC 3280。

[アカウンティング]
RADIUS の機能の一つで、ログイン時刻や通過パケット数など、ユーザのサービス利用の事実を記録すること。

[アカウンティングログ]
RADIUS のアカウンティングに関する情報を記録するログファイル。

[アトリビュート]
RADIUS サーバと RADIUS クライアント間で送受信される情報。属性とその値のペアで構成されます。

[アドレスプール]
リモートコンピュータに割り当てる IP アドレスの範囲。

[応答アトリビュート]
認証成功時に RADIUS サーバが RADIUS クライアントに返すアトリビュート。

[応答アトリビュートプロファイル]
本装置が使用するプロファイルの一つ。認証後に NAS へ返すアトリビュートに関する設定をあらかじめプロファイルに設定しておくことで、ユーザ登録時の入力を省力化するために用います。

[オブジェクトクラス(LDAP)]
ディレクトリのエントリを定義するための型。

[親、子]
親子連携機能における、MASTER を親、SLAVE を子と呼びます。

[親子連携機能]
1 つの同期システムに、複数の同期コンフィグを含む機能です。

[鍵長]
暗号に用いる鍵の長さ。一般に長い方が安全ですが、その分処理に時間がかかります。

[クライアント]
→ RADIUS クライアント

[グループ ID]
ユーザ ID を "user@centurysys.co.jp" または ”CENTURYSYS\user ” のように、所属グループを表わす文字列を付加して指定する場合の、追加文字列。

[グループ ID プロファイル]
本装置が使用するプロファイルの一つ。グループ ID に関する設定をあらかじめプロファイルに設定しておくことで、ユーザ登録時の入力を省力化するために用います。

[コミュニティ名]
SNMP エージェントと通信するために SNMP マネージャがパスワードとして使用する名前。SNMP マネージャの設定に合わせて設定します。

[サーバ証明書]
サーバマシンに割り当てられる証明書。接続した相手が正しいサーバであるかをユーザが確認するために用いる。
→ 証明書

[最大 TTL]
ルート確認の実行時に指定する、TTL（目的のホストまでのホップ数）の上限値。

[サプリカント]
IEEE802.1X に準拠した認証を実現するために、ユーザーの PC 上で認証機能を提供するソフトウェア。

[シークレット]
RADIUS サーバと RADIUS クライアント間で共通で設定される文字列。RADIUS サーバクライアント間の認証や、ユーザパスワードの一時的な暗号化に用いられる。

[システムログ]
本装置の起動 / 停止など、システム運用に関連したログ

[失効]
まだ証明書の有効期間内であるが、私有鍵が他のユーザに漏れたなどの理由により証明書を無効化すること。

[失効日]
証明書が失効した日。

付録 D

用語説明

[失効リスト更新間隔]
CRL を更新する間隔。
→ CRL

[失効理由]
証明書が失効した理由。
→ 失効

[証明書]
公開鍵が本当に持ち主のものだということを証明するためのもの。電子的な身分証明書に相当します。

[証明書署名要求]
Certificate Signing Request (CSR).
公開鍵に対する証明書を受けるために送られる、電子的な申請書。申請者の公開鍵など証明書発行に必要な情報が含まれており、CA による証明書発行に用いることができます。

[証明書プロファイル]
本装置が使用するプロファイルの一つ。ユーザ証明書に関する設定をあらかじめプロファイルに設定しておくことで、ユーザ登録時の入力を省力化するために用います。

[設定ウィザード]
本装置に必要な設定をまとめておこなうための設定ツール。本装置購入後最初に立ち上げた場合に起動する他、メニューから選択することもできる。

[装置種別]
同期をおこなう本装置のうち、設定の元となる機器を MASTER、それ以外を SLAVE と呼びます。

[対向装置]
本装置を二重化して使用する際のもう一台のサーバ。

[タイプ名 (RADIUS VSA)]
RADIUS のベンダ固有アトリビュートを定義する場合のアトリビュート名。

[同期コンフィグ]
同期装置間で共有される設定情報です。1 つの同期コンフィグは、1 台の MASTER と 1 台の SLAVE で共有されます。

[同期システム]
同期コンフィグおよび同期装置によって構成される系です。各同期装置は、ただ 1 つの同期システムに属することができます。

[同期装置]
設定情報の同期機能を用いて設定情報を共有する本装置を同期装置と呼びます。

[同時接続数]
RADIUS サーバで同時ログインを許可する数の上限。

[二重化]
RADIUS サーバを 2 台設置することで、障害対策をおこなう構成を取る事。

[認証アトリビュート]
認証時に、パスワードなどの情報の他に認証の可否に利用するアトリビュートを指定します。

[認証アトリビュートプロファイル]
本装置が使用するプロファイルの一つ。認証時に確認するアトリビュートに関する設定をあらかじめプロファイルに設定しておくことで、ユーザ登録時の入力を省力化するために用います。

[認証方式]
ユーザ認証の方式。
→ PAP, CHAP, EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS

[認証ログ]
ユーザの認証結果を記録するログファイル。

[バインド(LDAP)]
LDAP プロトコルにおいて、認証をおこなう行為。

[パスフレーズ]
私有鍵を使用する場合に必要となる秘密の文字列。

[ファシリティ]
採取するログの分類。

[フォーマット (RADIUS VSA)]
RADIUS のベンダ固有アトリビュートを定義する場合のデータ型を指定します。text, string, address, integer, ipv6address があります。

付録 D

用語説明

[プロファイル]
同じ属性の設定内容をグループ化して設定するためのもの。テンプレート。
→ ユーザプロファイル、ユーザ基本情報プロファイル、認証アトリビュートプロファイル、証明書プロファイル、応答アトリビュートプロファイル、グループ ID プロファイル

[ベンダ (RADIUS VSA)]
RADIUS のベンダ固有アトリビュートを定義する場合のベンダ情報。

[ベンダ ID (RADIUS VSA)]
RADIUS のベンダ固有アトリビュートを定義する場合のベンダ ID。

[ベンダ固有アトリビュート]
RADIUS プロトコルでアトリビュート番号 26 の値として定義されるアトリビュート。各ベンダにより独自に規定されており、動作はベンダによって異なります。

[ベンダ名 (RADIUS VSA)]
RADIUS のベンダ固有アトリビュートを定義する場合のベンダ名。

[本装置管理者]
本装置(RA-1200・RA-730)の全ての設定をおこなう権限をもつ RA-1200・RA-730 のアカウント。
→ ユーザ管理者

[本装置の管理者(SNMP)]
本装置管理者への連絡先。SNMP の管理情報の一つ。

[本装置の設置場所(SNMP)]
本装置の物理的な設置場所。SNMP の管理情報の一つ。

[本装置の説明(SNMP)]
本装置についての説明。ハードウェアの名称、バージョン、OS の情報などを指定する。SNMP の管理情報の一つ。

[本装置の名称(SNMP)]
本装置の管理上の名前。通常 FQDN を指定する。SNMP の管理情報の一つ。

[有効期間]
証明書の有効期間。

[ユーザ]
RADIUS ユーザ。

[ユーザ ID]
RADIUS ユーザに対して一意に付けられる識別名。

[ユーザ管理者]
RADIUS ユーザの追加、編集、削除やユーザ証明書の発行、失効のみをおこなう権限をもつ RA-1200・RA-730 のアカウント。本装置管理者によって作られる。
→ 本装置管理者

[ユーザ基本情報]
認証方式、同時接続数、IP アドレスの割り当て方法、アドレスプールなど RADIUS ユーザに関する属性。

[ユーザ基本情報プロファイル]
本装置が使用するプロファイルの一つ。認証方式など、基本的な情報の設定をあらかじめプロファイルに設定しておくことで、ユーザ登録時の入力を省力化するために用います。

[ユーザ証明書]
ユーザが本人であることを証明する証明書。

[ユーザプロファイル]
ユーザに関する共通の設定情報をあらかじめ定義しておくことで、ユーザ登録時の入力を省力化するためのもの。ユーザ基本情報、認証アトリビュート、証明書、応答アトリビュート、グループ ID の各プロファイルからなります。
→ ユーザ基本情報プロファイル、認証アトリビュートプロファイル、証明書プロファイル、応答アトリビュート、グループ ID プロファイル

[レルム (realm)]
受信した要求の処理方法を決定するために RADIUS サーバが使用する領域。
本装置では、認証要求やアカウンティング要求に含まれるユーザ名 (User-Name) の最後に現れる @ より後ろの文字列をレルムとして扱います。
受信した要求に含まれるレルムの値によって、要求を本装置で処理するか、他サーバへ転送するか (RADIUS Proxy) を選択することができます。

付録 E

システムログ一覧

付録 E

システムログ一覧

■ログ

(1) YYYY-MM-DD hh:mm:ss,RADIUS,RADIUS start
(2) YYYY-MM-DD hh:mm:ss,RADIUS,RADIUS stop
(3) YYYY-MM-DD hh:mm:ss,RADIUS,RADIUS restart
(4) YYYY-MM-DD hh:mm:ss,system,peer up: PEER_DEVICE (A.B.C.D)
(5) YYYY-MM-DD hh:mm:ss,system,peer down: PEER_DEVICE (A.B.C.D)
(6) YYYY-MM-DD hh:mm:ss,system,peer up: A.B.C.D
(7) YYYY-MM-DD hh:mm:ss,system,peer down: A.B.C.D
(8) YYYY-MM-DD hh:mm:ss,system,[CFG_ID:PEER_DEVICE] invalid request found.
(9) YYYY-MM-DD hh:mm:ss,NTP,NTP start
(10) YYYY-MM-DD hh:mm:ss,NTP,NTP stop
(11) YYYY-MM-DD hh:mm:ss,NTP,NTP restart
(12) YYYY-MM-DD hh:mm:ss,SNMP,SNMP start
(13) YYYY-MM-DD hh:mm:ss,SNMP,SNMP stop
(14) YYYY-MM-DD hh:mm:ss,SNMP,SNMP restart
(15) YYYY-MM-DD hh:mm:ss,RADIUS,Unknown client A.B.C.D:E
(16) YYYY-MM-DD hh:mm:ss,AD Interaction,AD Interaction restart
ver1.8.3以降は出力されません。
(17) YYYY-MM-DD hh:mm:ss,DHCP,DHCP start
(18) YYYY-MM-DD hh:mm:ss,DHCP,DHCP stop
(19) YYYY-MM-DD hh:mm:ss,DHCP,DHCP restart

■ログ内容

(1) GUIを用いてRADIUSサーバが起動された時に出力されます。
(2) GUIを用いてRADIUSサーバが停止された時に出力されます。
(3) GUIを用いてRADIUSサーバが再起動された時、またはシステム起動によりRADIUSサーバが起動された時に出力されます。
(4) 設定情報の同期に関して対向装置との接続性が確認された時に出力されます。
(5) 設定情報の同期に関して対向装置との接続性が失われた時に出力されます。
(6) 二重化に関して対向装置との接続性が確認された時に出力されます。
(7) 二重化に関して対向装置との接続性が失われた時に出力されます。
(8) 設定変更の要求がMASTERからSLAVEへ転送された場合に、SLAVEで要求が処理されなかった時にMASTERで出力されます。設定情報の不整合などが原因として考えられます。
(9) GUIを用いてNTPサーバが起動された時に出力されます。
(10) GUIを用いてNTPサーバが停止された時に出力されます。
(11) GUIを用いてNTPサーバが再起動された時に出力されます。
(12) GUIを用いてSNMPサーバが起動された時に出力されます。
(13) GUIを用いてSNMPサーバが停止された時に出力されます。
(14) GUIを用いてSNMPサーバが再起動された時に出力されます。
(15) 未登録のRADIUSクライアントより認証要求があった時に出力されます。
(16) AD連携機能を利用し、RADIUSサーバが(再)起動された時に出力されます。
ver1.8.3以降は出力されません。
(17) GUIを用いて、DHCPサーバが起動された時に出力されます。
(18) GUIを用いて、DHCPサーバが停止された時に出力されます。
(19) GUIを用いて、DHCPサーバが再起動された時に出力されます。

付録 E

システムログ一覧

■ログ項目説明

以下の番号は、ログ項番に該当します。

YYYY-MM-DD hh:mm:ss ：日時

(4)(5)
PEER_DEVICE：対向の同期装置名
A.B.C.D：対向の同期装置の IP アドレス

(6)(7)
A.B.C.D：対向の装置の IP アドレス

(8)
CFG_ID：設定情報の同期の CONFIG_ID
PEER_DEVICE：対向の同期装置名

(15)
A.B.C.D：RADIUS クライアントの IP アドレス
E：RADIUS クライアントの送信元ポート番号

付録 F

同期・二重化構成におけるファームウェア更新手順

付録 F

同期・二重化構成におけるファームウェア更新手順

二重化構成におけるファームウェアの更新手順を図に示します。この手順はいずれも両機器で同時にサービスが停止しないことを重視しています。まれにログの欠落・重複が発生する可能性があります。

図: 二重化構成におけるファームウェア更新手順

Secondary、Primaryの順にファームウェアを更新	
Primary / Master	Secondary / Slave
↓	(1) RADIUSサービス停止
↓	↓
↓	(2) ファームウェア更新 (自動再起動)
↓	↓
(3) ログ同期	↓
↓	↓
↓	(4) RADIUSサービス開始
↓	↓
(5) RADIUSサービス停止	↓
↓	↓
(6) ファームウェア更新 (自動再起動)	↓
↓	↓
(7) ログ取得	↓
↓	↓
(8) RADIUSサービス開始	↓

Primary、Secondaryの順にファームウェアを更新	
Primary / Master	Secondary / Slave
(1) RADIUSサービス停止	↓
↓	↓
(2) ファームウェア更新 (自動再起動)	↓
↓	↓
(3') ログ取得	↓
↓	↓
(4) RADIUSサービス開始	↓
↓	↓
↓	(5) RADIUSサービス停止
↓	↓
↓	(6) ファームウェア更新 (自動再起動)
↓	↓
(7') ログ同期	↓
↓	↓
↓	(8) RADIUSサービス開始

(1)[RADIUS]－[サーバ]－[起動・停止]より「停止」ボタンを押下し、GUI 画面でサービスが「停止中」になっている事を確認します。
(2) [管理機能]－[システム]－[ファームのアップデート]よりファームウェアを指定して、「実行」ボタンを押下します。
(3)(3') 情報表示（[運用機能]－[システム情報]－[システム情報]）の［二重化 / 設定の同期状態］が「ＯＫ」となっている事を確認します。
(3) 「ログ同期」([管理機能]－[システム]－[設定情報の同期])ボタンを押下します。
(3') [ログ取得]([管理機能]－[システム]－[設定情報の同期])ボタンを押下します。
(4) [RADIUS]－[サーバ]－[起動・停止]より「開始」ボタンを押下し、GUI 画面でサービスが「動作中」になっている事を確認します。
(5) [RADIUS]－[サーバ]－[起動・停止]より「停止」ボタンを押下し、GUI 画面でサービスが「停止中」になっている事を確認します。
(6) [管理機能]－[システム]－[ファームのアップデート]よりファームウェアを指定して、「実行」ボタンを押下します。
(7)(7') 情報表示（[運用機能]－[システム情報]－[システム情報]）の［二重化 / 設定の同期状態］が「ＯＫ」となっている事を確認します。
(7) [ログ取得]([管理機能]－[システム]－[設定情報の同期])ボタンを押下します。
(7') 「ログ同期」([管理機能]－[システム]－[設定情報の同期])ボタンを押下します。
(8)[RADIUS]－[サーバ]－[起動・停止]より「開始」ボタンを押下し、GUI 画面でサービスが「動作中」になっている事を確認します。

付録 F

同期・二重化構成におけるファームウェア更新手順

■ Ver1.8.3以降のバージョンへのファームウェア更新

Ver1.8.2 以前のバージョンから Ver1.8.3 以降のバージョンへのファームウェア更新において、ログ同期・ログ取得を用いたログ等の引き継ぎに一部制限があります。

グループ ID(GroupID\UserID)を使用するユーザが存在する環境下などでログ等を引き継いだ場合、下記のような不都合が生じることがあります。

・アカウンティング要求(Stop)を受信しても、ファームウェア更新前にログインしたユーザのログイン情報が削除されない。

このような環境では、ファームウェア更新時にログの引き継ぎを行わないでください。RADIUS クライアントでも、リセット(再起動等)などの操作を行なってください。

ログイン情報が削除されないことがあれば、必要に応じて強制ログアウトなどを行って下さい。

付録 G

親子連携

付録 G

親子連携

親子連携機能を設定、使用する上での注意事項をまとめています。

■ 親子連携機能の有効化

親子連携機能の有効・無効は、ユーザが明示的に設定します。親子連携機能を有効にする場合は、「設定情報の同期」を「親子連携」に設定します。

親に設定する場合の例

子に設定する場合の例

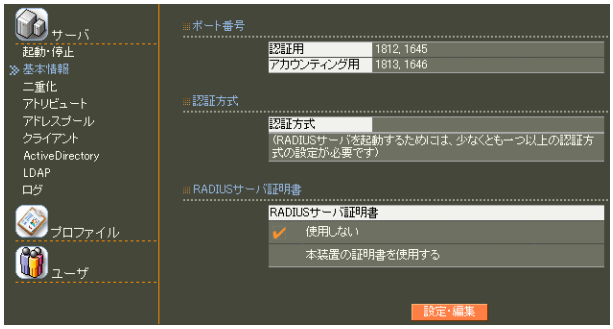
親子連携機能の有効・無効を切り替えるためには、以下の条件を満たすことが必要です。

- RADIUS サーバが停止していること。
- 同期コンフィグが存在しないこと。
- 同期コンフィグ毎の設定が存在しないこと。
  (「第 8 章 管理機能 II. システム」の「表 . 設定項目一覧」を参照してください。)
- CA・証明書が存在しないこと。
- Active Directory を使用していないこと。
- LDAP を使用していないこと。

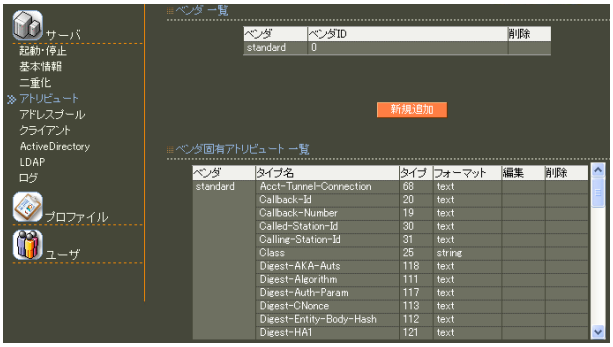
■ 全ての同期コンフィグで共有する設定

次の項目に関しては、同期コンフィグ毎には設定できません。全ての同期コンフィグで設定を共有します。

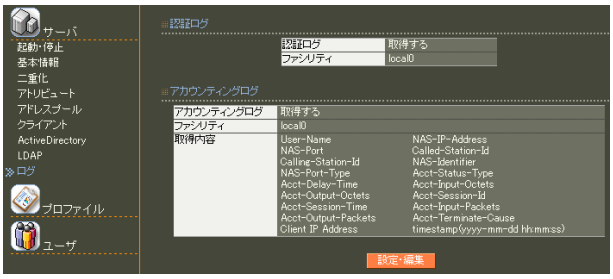
・[RADIUS]-[サーバ]-[基本情報]



・[RADIUS]-[サーバ]-[アトリビュート]



・[RADIUS]-[サーバ]-[ログ]



・[CA]-[CA/CRL]

・[CA]-[証明書](ユーザ証明書は除く)

但し、証明書については同期コンフィグ毎の設定も可能です。

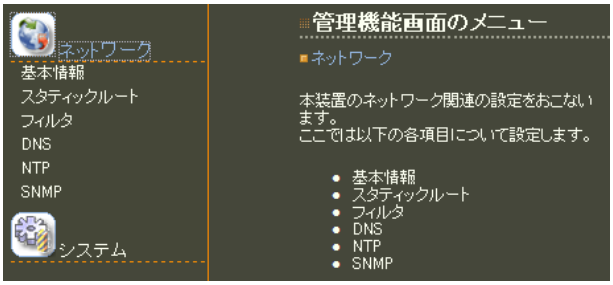
付録 G

親子連携

■ 子での設定

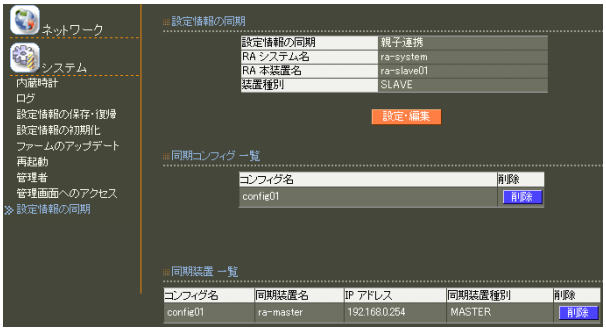
親子連携機能が有効の場合、子で設定できるのは、以下の管理機能だけです。

・[管理機能]-[ネットワーク]

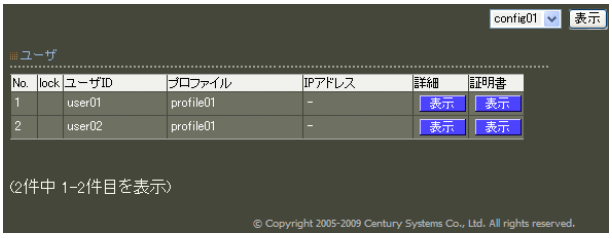


・[管理機能]-[システム]-[管理者]

・[管理機能]-[システム]-[設定情報の同期]



「第 8 章 管理機能 II. システム」の 「表 . 設定項目一覧」で、「親子連携有効」が●の項目については、子では設定変更ボタン（「新規追加」「編集」「削除」等のボタン）が表示されません。



「新規追加」ボタンが表示されない例

■ 親での設定

親子連携機能が有効の場合、設定（「新規追加」「編集」「削除」等は、全て親で行います。

「第 8 章 管理機能 II. システム」の 「表 . 設定項目一覧」で、「親子連携有効範囲」が「同期コンフィグ毎」の項目については、GUI 画面右上のプルダウンから、同期コンフィグを選択してから設定します。

右上プルダウンから同期コンフィグを選択

親から子（の一部）への reachability がない時でも、親での設定は可能です。「強制同期」するまで子には反映されません。

付録 G

親子連携

■ 「設定情報の同期」による冗長化

親子連携機能が有効の場合、[RADIUS]-[サーバ]-[二重化]の設定は無視され、常に同期処理・冗長化(二重化) 処理を実行します。同期したくない時は同期装置を削除して下さい。

親子連携機能が有効の場合、[RADIUS]-[サーバ]-[二重化]の設定変更は出来ません。設定画面を表示することも出来ません。

■ 設定可能な値

各設定項目について設定可能な値は、同期コンフィグ毎に独立していません。例えば、ユーザ名は同期システム全体で一意とします。

RADIUS クライアントの IP アドレスは、同期コンフィグ間での重複は許されません。

■ 設定可能な数

各設定項目について同期コンフィグ毎に設定可能な数は、全て RA-730 最大設定数と同じです。ただし、同期システム全体で RA-1200 の最大設定数を超えることは出来ません。

たとえば、RADIUS クライアントは同期コンフィグ毎に最大 250 まで作成可能ですが、同期システム全体では 1000 を超えることは出来ません。そのため、同期コンフィグの数を 5 とした場合、コンフィグあたりの最大クライアント数は、250 ではなくて 200 に制限されます。

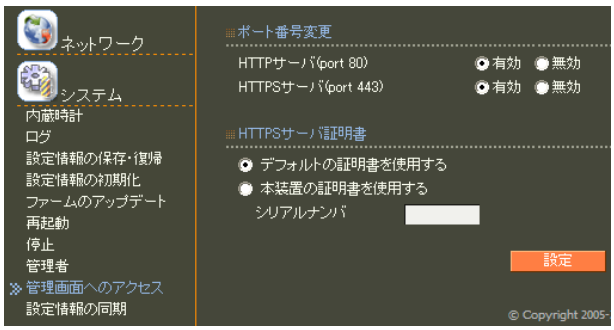
設定可能な数は「付録 A 最大数一覧」を参照してください。

■ CA の数

同期システム全体で CA の数は 1 つです。

■ CA の削除

CA の削除を行う際は、全ての同期装置の HTTPS サーバ証明書の設定を「本装置の証明書を使用する」以外の設定に変更してください。
「本装置の証明書を使用する」の状態で CA の削除を行った場合の動作は保証しません。



■ 証明書

同期コンフィグ毎の証明書(ユーザ証明書以外)を失効した場合は、全同期コンフィグで共有の証明書に変更されます。

ユーザ証明書を失効した場合は、同期コンフィグ毎のままで変更はされません。但し、該当ユーザを削除した場合に、全同期コンフィグで共有の証明書に変更されます。

■ ActiveDirectory

親子連携機能が有効の時に、ActiveDirecotry 連携機能は使用できません。また、ActiveDirecotry 連携機能を使用中は、親子連携機能を有効にすることは出来ません。

■ LDAP

親子連携機能が有効の状態で、LDAP は使用できません。また、LDAP を使用中は、親子連携機能を有効にすることは出来ません。

■レルム

親子連携機能が有効の状態で、レルム設定を追加することはできません。また、レルム設定が存在する場合、親子連携機能を有効にすることは出来ません。

付録 G

親子連携

■設定情報の同期

「同期しない」「同期する」から「親子連携」に変更する場合、または「親子連携」から「同期しない」「同期する」に変更する場合は、RADIUS サーバが停止している状態で行ってください。

■ 同期コンフィグ

親子連携機能が有効の状態で、同期コンフィグを追加・削除すると、その設定変更は RADIUS サーバに即時反映されます。

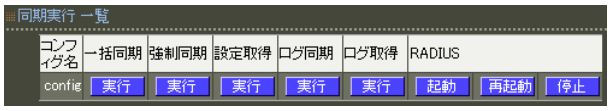
■ 同期装置

親子連携機能が有効の状態では、同期装置を追加・削除すると、その設定変更は RADIUS サーバに即時反映されます。

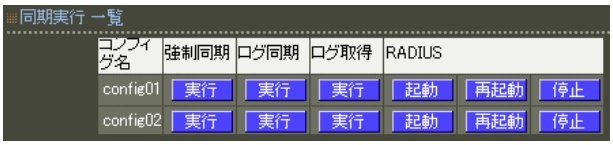
同期装置を削除した場合、未転送のメッセージ(ログ、設定情報など) があれば、転送されずに破棄されます。

■ 強制同期、設定取得、一括同期

親子連携が有効の状態では、設定情報の同期は「強制同期」のみ使用することができます。通常の自動的な同期処理は「即時実行」・「一括処理」ともに行いません。



設定情報の同期： 同期する



設定情報の同期： 親子連携

○一括同期

親子連携が有効の状態では、使用することはできません。

○強制同期

同期コンフィグ毎に行います。強制同期を行った場合、指定された同期コンフィグのみ初期化・設定を実施します。各種ログは削除されます。

○設定取得

親子連携が有効の状態では、使用することはできません。

○ログ同期

同期コンフィグ毎に行います。

○ログ取得

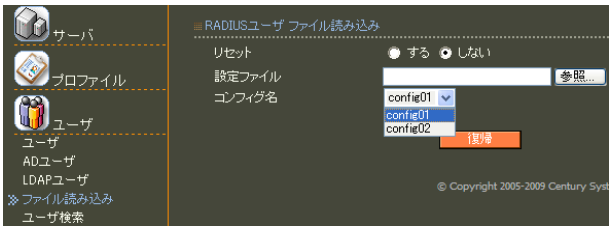
同期コンフィグ毎に行います。

付録 G

親子連携

■ ユーザファイル読み込み

親子連携機能が有効の状態では、ファイル読み込みは同期コンフィグ毎に行います。子では、設定画面の表示は出来ません。



■ ユーザ検索

親で検索を実行する場合

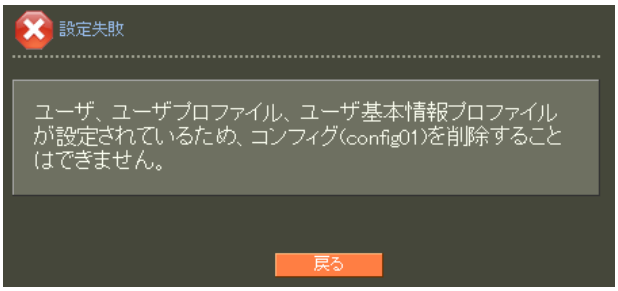
「指定しない」を選択すると、全ての同期コンフィグが検索対象となります。
同期コンフィグを選択すると、選択した同期コンフィグが検索対象となります。

子で検索を実行する場合

そのRAが属する同期コンフィグのみが検索対象となります。

■ 同期コンフィグの削除

同期コンフィグに属する設定がある場合、同期コンフィグ自体の削除は出来ません。



■ RADIUSサービスの起動・再起動・停止

親と子のRADIUS サービスの起動・再起動・停止は独立して動作します。一方を再起動しても他方は再起動しません。

■ 一括ログアウト

一括ログアウトは、同期コンフィグ毎に行います。

付録 H

認証ログの reason メッセージ一覧

付録 H

認証ログの reason メッセージ一覧

認証ログに記録する reason メッセージ、および当該 reason メッセージを記録する条件を以下に示します。

(1) Incorrect password (*password*) [*type*] または Incorrect password [*type*]
ユーザが入力したパスワードが正しくない時に記録されます。
(*password*)が記録されるのは、認証失敗時のパスワードを記録するように選んだ場合、かつ PAP または EAP-TTLS/PAP の場合に限ります。
パスワードは最大 30 バイトまで記録されます。31 バイト目以降は省略されます。30 バイトを超えた場合は、(looooooooooooooooooong passwo ...)のようになります。
type は、認証方式またはそれに準じる文字列です（以下同じ）。

(2) Empty password [*type*]
認証要求に含まれているパスワードの長さが 0 の時に記録されます。

(3) No username in request [*type*]
認証要求にユーザ名が含まれていない時、または認証要求に含まれているユーザ名の長さが 0 の時に記録されます。

(4) Too many sessions (*number*) [*type*]
ユーザ毎に設定された同時接続数を超えて認証要求があった時に記録されます。
number は同時接続数の設定値です。

(5) User not found [*type*]
ユーザが RA や LDAP サーバ上に存在しない時、または RA 上に存在するがロックされている時に記録されます。LDAP サーバに正常に接続できなかった時も含まれます。

(6) Type not permitted [*type*]
認証方式がユーザの設定値と異なる時に記録されます。
例えば、EAP-PEAP に設定されているユーザが、PAP を使用した場合などが該当します。

(7) Attributes unmatched [*type*]
指定した認証アトリビュートが認証要求に含まれていない時に記録されます。

(8) No address [*type*]
払い出すアドレスがない時(アドレスプール)に記録されます。

(9) No address (cannot connect) [*type*]
払い出すアドレスがない時(アドレスプール)に記録されます。
二重化構成時に、対向装置との接続に失敗した場合に記録されます。

付録 H

認証ログの reason メッセージ一覧

(10) No address (response timed out) [*type*]
払い出すアドレスがない時(アドレスプール)に記録されます。
二重化構成時に、対向装置からの応答が一定時間内になかった場合に記録されます。

(11) TLS verification error (*string*) [*type*]
TLSクライアント証明書の検証で失敗した時に記録されます。
*string*はその詳細な内容を示す文字列です。以下に例を示します。
(a) unable to get local issuer certificate
・クライアント証明書がRA で作成したCA で発行されたものでない時に記録されます。
(b) certificate revoked
・クライアント証明書が失効済みの時に記録されます。
(c) certificate is not yet valid
・クライアント証明書の有効期限の開始日時よりRAの時刻が前の時に記録されます。
(d) certificate has expired
・クライアント証明書の有効期限の終了日時よりRA の時刻が後の時に記録されます。
(e) CRL is not yet valid
・クライアント証明書用の失効リストの最後の更新(last Update) よりRAの時刻が前の時に記録されます。
(f) CRL has expired
・クライアント証明書用の失効リストの次の更新(next Update) よりRAの時刻が後の時に記録されます。

(12) TLS alert sent (*level description*) [*type*]
クライアントにTLS alertを送った時に記録されます。
*level*および*description*は、alertの内容を表します。
詳細は、RFC 5246などを参照してください。
例えばクライアントから提示された暗号スイート(cipher suite) の中に、本装置で利用可能なものがなければ(fatal handshake_failure)となります。

(13) TLS alert received (*level description*) [*type*]
クライアントからTLS alert を受け取った時に記録されます。
*level*および*description*は、alertの内容を表します。詳細は、RFC 5246などを参照してください。

(14) Unexpected EAP-Message [*type*]
予期しないEAP-Messageを受信した時に記録されます。
例えば、RAを二重化構成で使用している状態で、EAP-TLSセッション途中でプライマリからセカンダリに切り替えが発生した場合などに記録されます。

認証ログの reason メッセージ一覧

(15) Type not supported [*type*] または *Type* not supported [*type*]

サポートしていない EAP type を受信した時、RADIUS サーバ設定で有効にされていない認証方式を受信した時、受信した認証要求にパスワードが含まれていない時などに記録されます。

例:

Type not supported [PAP]

RADIUS サーバ設定で PAP/CHAP を無効にしている状態で、PAP を受信した時に記録されます。

Type not supported [???]

認証要求にパスワードが含まれていない時に記録されます。

Type not supported [EAP-TTLS/PAP]

RADIUS サーバ設定で PAP/CHAP を無効にしている状態で EAP-TTLS/PAP を受信した時に記録されます。

EAP-TTLS not supported [EAP]

RADIUS サーバ設定で EAP-TTLS を無効にしている状態で、EAP-TTLS を希望する Nak を受信した時に記録されます。

EAP-SIM not supported [EAP]

EAP-SIM を希望する Nak を受信した時に記録されます。

EAP-GTC not supported [EAP-TTLS/EAP]

EAP-TTLS/EAP-GTC を希望する Nak を受信した時に記録されます。

Type-41 not supported [EAP]

EAP-SPEKE を希望する Nak を受信した時に記録されます。

Type-0 not supported [EAP]

使用可能な type がないことを通知する Nak を受信した時に記録されます。

EAP-MD5 not supported [EAP-TTLS/EAP]

RADIUS サーバ設定で EAP-MD5 を無効にしている状態で、EAP-TTLS/EAP-*** を希望する Nak を受信した時に記録されます。

Type not supported [EAP-SIM]

クライアントが Identity などを省略して、EAP-SIM を突然送信してきた時に記録されます。

Type not supported [EAP-MSCHAPv2]

EAP-MSCHAPv2 を受信した時に記録されます。

Type not supported [Notification]

Notification を受信した時に記録されます。

(16) LDAP (*ldap-name*): Password not configured [*type*]

パスワードが LDAP サーバなどで設定されていない時、または LDAP サーバから取得できない時に記録されます。

例えば、認証方式が EAP-TTLS/CHAP、かつ管理者権限で平文パスワードが LDAP サーバから取得できない場合などに記録されます。

ldap-name は、本装置で設定した LDAP サーバの名前です(以下同じ)。

(17) LDAP (*ldap-name*): Incorrect password (*password*) [*type*] または
LDAP (*ldap-name*): Incorrect password [*type*]

LDAP サーバを使用、かつユーザが入力したパスワードが正しくない時に記録されます。

(*password*)については、Incorrect password (*password*) [*type*]についての記載を参照してください。

付録 H

認証ログの reason メッセージ一覧

(18) LDAP (*ldap-name*): TLS error (*number*) [*type*]
LDAP サーバとの接続に、TLS が理由で失敗した時に記録されます。
*number*は理由の詳細を表す数です。

(19) LDAP (*ldap-name*): Connection failed (*number*) [*type*]
LDAPサーバと接続できなかった場合に記録されます。。
TCP 接続後、上位レイヤーで reject された場合（アクセス禁止など。パスワード不一致以外）に記録されます。

(20) Remote server
RADIUS Proxy 使用時、転送先サーバからの応答を受信した時に記録されます。

(21) Remote server: No response (*number*)
RADIUS Proxy 使用時、転送先サーバから時間内に応答がなかった時に記録されます。
*number*は待ち時間（単位：秒）です。

(22) Active Directory [*type*]
Active Directory 連携時に記録されます。

(23) Protocol error *number* または Protocol error *number* [*type*]
クライアントがプロトコルとして正しくないメッセージを送信してきた時に記録されます。
*number*は理由の詳細を表す数です。

(24) Fatal error *number*
RADIUS サーバ内部で、致命的なエラーが発生した時に記録されます。例えば、メモリが確保出来なかった、などの場合に記録されます。*number*は理由の詳細を表す数です。

FutureNet RAシリーズ　ユーザーズガイド　Ver1.12.0対応版
2016年3月版
発行 センチュリー・システムズ株式会社