EAP 対応 RADIUS サーバアプライアンス

FutureNet RA-630
RA-1100

ユーザーズガイド

Ver1.7.0

CENTURY SYSTEMS

目次

はじめに

◆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下さい。
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下さい。
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下さい。

◆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、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

ご使用にあたって

本製品を安全にお使いいただくために、まず以下の注意事項を必ずお読み下さい。

絵表示について	この取扱説明書では、製品を安全に正しくお使いいただき、あなたや他の人々への危害や財産への損害を未然に防止するために、いろいろな絵表示をしています。その表示と意味は次のようになっています。内容をよく理解してから本文をお読みください。

次の表示の区分は、表示内容を守らず、誤った使用をした場合に生じる「危害や損害の程度」を説明しています。

⚠ 危険	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う危険が差し迫って生じることが想定される内容を示しています。
⚠ 警告	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容を示しています。
⚠ 注意	この表示を無視して誤った取り扱いをすると、人が死亡または重傷を負う可能性が想定される内容および物的損害のみの発生が想定される内容を示しています。

次の絵表示の区分は、お守りいただく内容を説明しています。

	このような絵表示は、してはいけない「禁止」を意味するものです。それぞれに具体的な禁止内容が書かれています。
	このような絵表示は、必ず実行していただく「強制」を指示するものです。それぞれに具体的な指示内容が書かれています。

⚠ 危険

 必ず本体に付属している電源ケーブルをご使用ください。

 使用温度範囲は0℃～40℃です。この温度範囲以外では使用しないでください。

 ストーブのそばなど高温の場所で使用したり、放置しないでください。

 火の中に投入したり、加熱したりしないでください。

 製品の隙間から針金などの異物を挿入しないでください。

ご使用にあたって

⚠ 警告

万一、異物(金属片・水・液体)が製品の内部に入った場合は、まず電源を外し、お買い上げの販売店にご連絡下さい。そのまま使用すると火災の原因となります。

万一、発熱していたり、煙が出ている、変な臭いがするなどの異常状態のまま使用すると、火災の原因となります。すぐに電源を外し、お買い上げの販売店にご連絡下さい。

本体を分解、改造しないでください。けがや感電などの事故の原因となります。

本体または電源ケーブルを直射日光の当たる場所や 、調理場や風呂場など湿気の多い場所では絶対に使用しないでください。火災・感電・故障の原因となります。

電源ケーブルの電源プラグについたほこりはふき取ってください。
火災の原因になります。

濡れた手で電源ケーブル、コンセントに触れないでください。感電の原因となります。

電源ケーブルのプラグにドライバなどの金属が触れないようにしてください。
火災・感電・故障の原因となります。

AC100Vの家庭用電源以外では絶対に使用しないでください。
火災・感電・故障の原因となります。

ご使用にあたって

⚠ 注意

湿気やほこりの多いところ、または高温となるところには保管しないでください。
故障の原因となります。

乳幼児の手の届かないところに保管してください。けがなどの原因となります。

長期間使用しないときには、電源ケーブルをコンセントおよび本体から外してください。

電源ケーブルの上に重いものを乗せたり、ケーブルを改造したりしないで下さい。
また、電源ケーブルを無理に曲げたりしないでください。
火災・感電・故障の原因となることがあります。

電源ケーブルは必ず電源プラグを持って抜いてください。ケーブルを引っ張ると、ケーブルに傷が付き、火災・感電・故障の原因となることがあります。

近くに雷が発生したときには、AC アダプタをコンセントから抜いて、ご使用をお控え下さい。落雷が火災・感電・故障の原因となることがあります。

AC アダプタのプラグを本体に差し込んだ後に AC アダプタのケーブルを左右および上下に引っ張ったり、ねじったり、曲げたりしないでください。緩みがある状態にしてください。

本製品に乗らないでください。本体が壊れて、けがの原因となることがあります。

高出力のアンテナや高圧線などが近くにある環境下では、正常な通信ができない場合があります。

パッケージの内容物の確認

本製品のパッケージには以下のものが同梱されております。本製品をお使いいただく前に、内容物がすべて揃っているかご確認ください。

万が一不足がありましたら、お買いあげいただいた店舗または弊社サポートデスクまでご連絡ください。

品名	数量
本体	１台
マニュアル収録CD-R　（※RA-630のみ）	１枚
UTPケーブル(CAT5，ストレート，1m)	１本
電源コード	１本
はじめにお読みください	１枚
保証書	１枚
海外使用禁止シート	１枚
ラックマウント用レール　（※RA-1100のみ）	１式
ラック組み立てマニュアル　（※RA-1100のみ）	１部

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-630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-1100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

装置全体の設定を行える「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

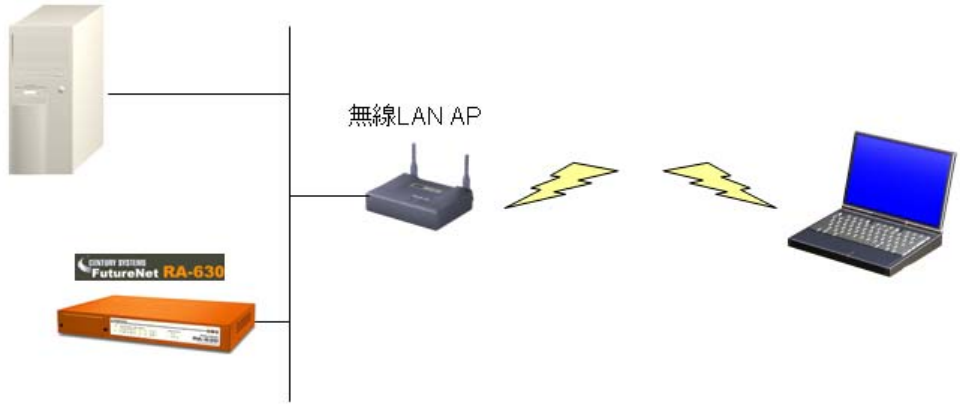
ログは、システムログ、認証ログ、アカウンティングログの３種類に分けて記録されます。ネットワーク経由で他のsyslogサーバに送ることもできます。

・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。

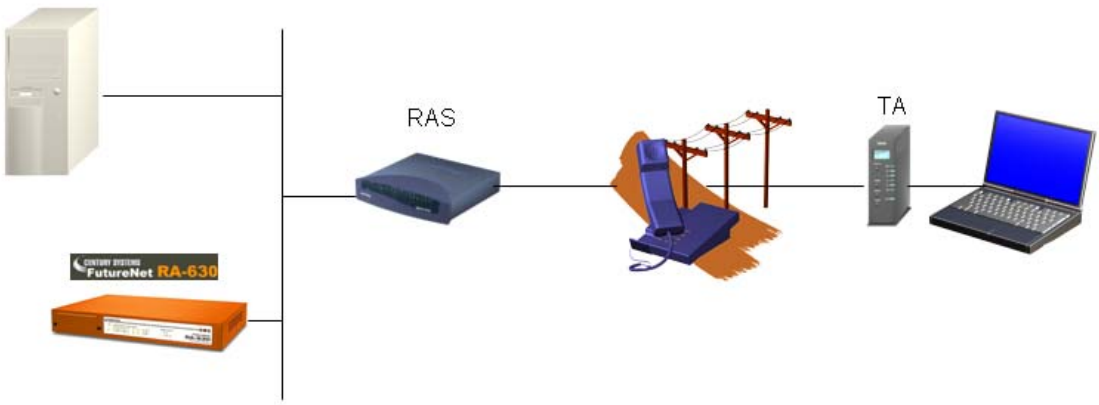
Ⅱ．利用例

◆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。

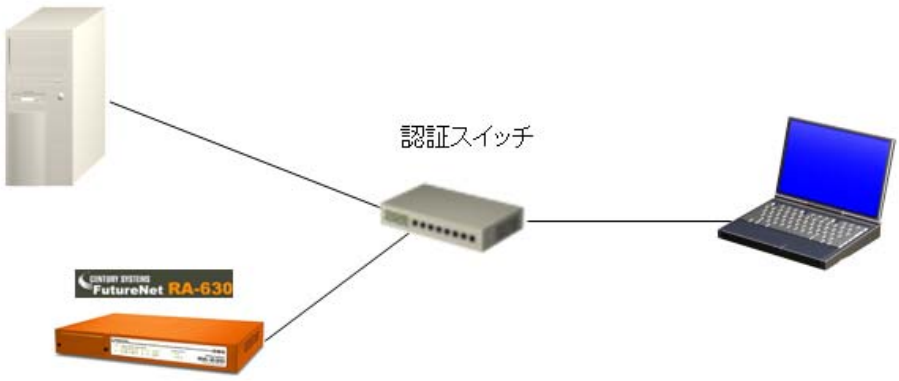
◆利用例２　リモートアクセス



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。

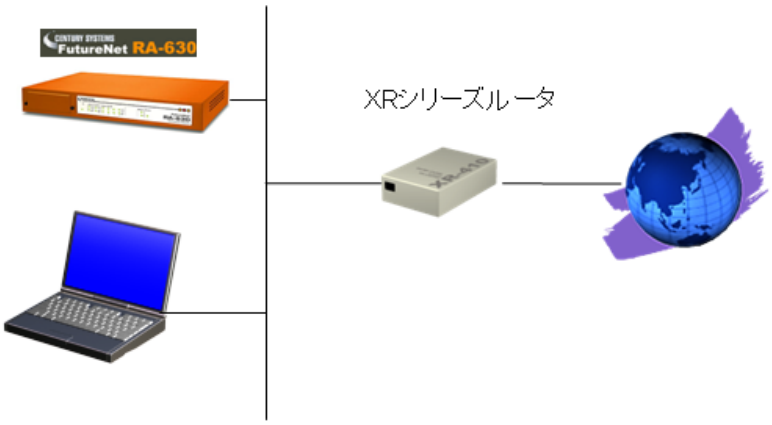
Ⅱ．利用例

◆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。

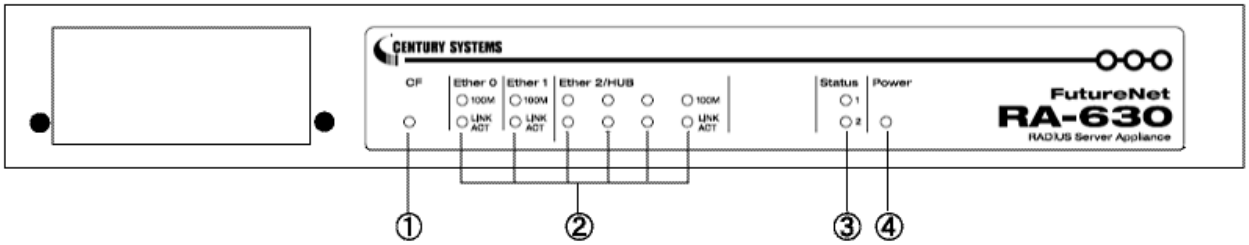
◆利用例４ GW 認証



当社 XR シリーズに搭載している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、XR 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

◆製品前面 （RA-630）



① CF LED

内臓されているCFカードが正常動作しているときに、CF(緑)が点灯します。

② Ethernetポート LED

各Ethernetポートの状態を表示します。
LANケーブルが正常に接続されているときに「LINK/ACT」(緑)ランプが点灯します。
「100M」(緑)ランプは、10Base-Tで接続した場合に消灯、100Base-TXで接続した場合点に点灯します。
データ通信時は「LINK/ACT」ランプが消灯します。

③ STATUS LED

本装置の全てのサービスが動作開始状態になっているときに、STATUS1(赤)は消灯します。

ファームウェアのアップデート作業中は、STATUS1(赤)が点滅します。

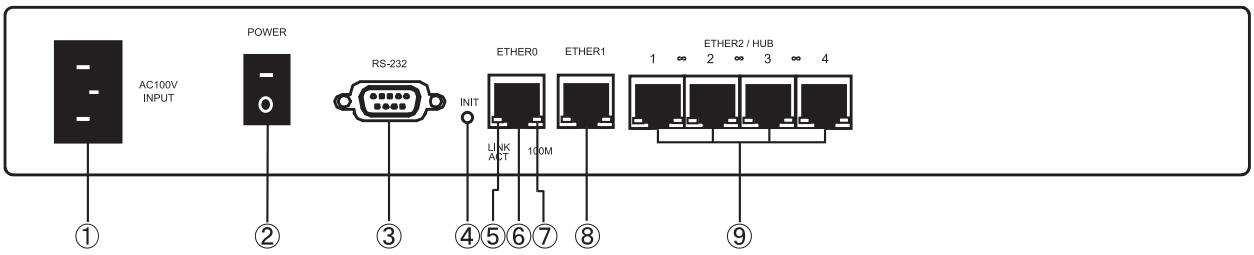
ファームウェアのアップデートに失敗した場合など、本装置が正常に起動できない状態になったときは、STATUS1(赤)とSTATUS2(緑)のどちらも点滅します。

④ POWER LED

本装置に電源が投入されているときに点灯(緑)します。

Ⅲ．各部の名称と機能

◆製品背面 （RA-630）



① 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。

② 電源スイッチ
電源をオン / オフするためのスイッチです。

③ RS-232 ポート
本装置では使用しません。

④ INIT ボタン
本装置を工場出荷時の設定に戻して起動するときに押します。

⑤ LINK/ACT LED（緑）
Ethernet ポートのリンク状態を示します。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

データ通信時は「LINK/ACT」ランプが消灯します。
本装置のすべての Ehternet ポートに実装されています。

⑥ Ether 0 ポート
主に LAN 側ネットワークとの接続に使用します。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。

⑦ 100M LED（橙）
Ethernet の接続速度を示します。以下のようなパターンで点灯 / 消灯します。

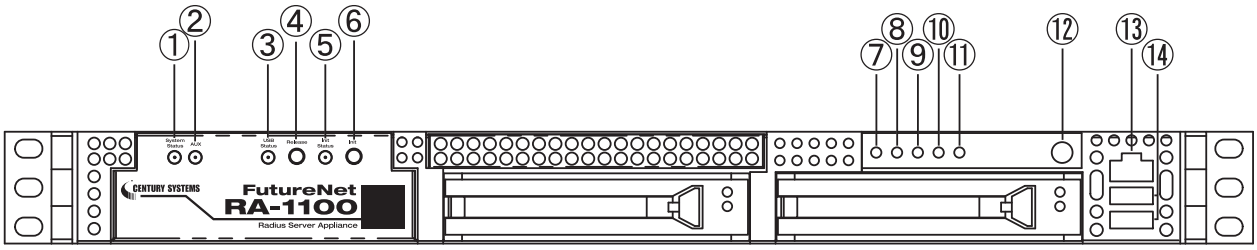
10Base-T ：消灯
100Base-TX ：点灯

⑧ Eehter1 ポート
Ether0 ポートとは別セグメントを接続するポートとして使います。RADIUS クライアントが LAN 側ネットワークと別のネットワークセグメントに接続する場合に利用する事をお勧めいたします。接続には、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。

⑨ Ether2 ポート
４ポートのスイッチング HUB です。
主に設定管理用に使用します。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。

Ⅲ．各部の名称と機能

◆製品前面 （RA-1100）



① System Status LED(緑)
本装置が動作状態にあるとき点灯します。

② AUX LED（緑）
本装置にAUXで接続しているときに点灯します。

③ USB STATUS LED
使用しません。

④ RELEASEスイッチ
使用しません。

⑤ INIT STATUS LED(橙)
INITスイッチにより本装置を初期化するときに、本装置の状態を示します。

⑥ INITスイッチ
このスイッチを押すことで、本装置を工場出荷状態に戻します。詳細は第13章「復旧操作」をご参照ください。

⑦ Temp LED（赤）
本装置の温度が一定以上になると点灯します。

⑧ Ether 1 LED（緑）
Ether1ポートの状態を示します。Link up時には点灯します。

⑨ Ether 0 LED（緑）
Ether0ポートの状態を示します。Link up時には点灯します。

⑩ CF LED（橙）
CFカードの状態を示します。

⑪ POWER LED（緑）
本装置に電源を投入しているときに点灯します。

⑫ 電源スイッチ
電源スイッチを押すと、動作が停止して待機状態になります。待機状態とは、電源オフ状態と同じですが、本装置には通電している状態です。

ただし、通常は設定画面の「システム設定」→「本体停止」画面で待機状態にしてください。
待機状態にするのは、本装置がハングアップしたときなどの非常時のみにしてください。

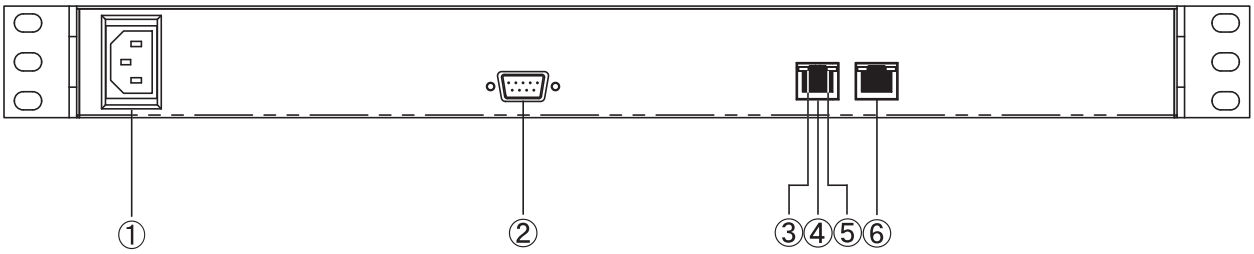
完全に電源をオフにする場合は、電源スイッチを4秒以上押してください。

⑬ RS-232 I/F(RJ-45)
使用しません。

⑭ USB I/F
使用しません。

Ⅲ．各部の名称と機能

◆製品背面 （RA-1100）



① 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。

③ RS-232 ポート
本装置では使用しません。

③ 速度表示ランプ
Ethernet の接続速度を示します。ランプは以下のようなパターンで点灯 / 消灯します。

10Base-T モード ： 消灯
100Base-TX モード ： 緑点灯
1000Base-T モード ： 橙点灯

④ Ether0 ポート(RJ-45)
主に LAN 側ネットワークとの接続に使用します。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。

⑤ LINK ランプ(橙)
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 ：橙点灯
Link Down：消灯

⑥ Ether1 ポート(RJ-45)
Ether0 ポートとは別セグメントを接続するポートとして使います。RADIUS クライアントが LAN 側ネットワークと別のネットワークセグメントに接続する場合に利用する事をお勧めいたします。接続には、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。

搭載されているインタフェース / ポートは、上記のもの以外は使用できません。

Ⅳ．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 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、InternetExplorer6.0 以降か Firefox1.0 以降がインストールされていること。

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、あらかじめご了承下さい。

第2章

コンピュータ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。

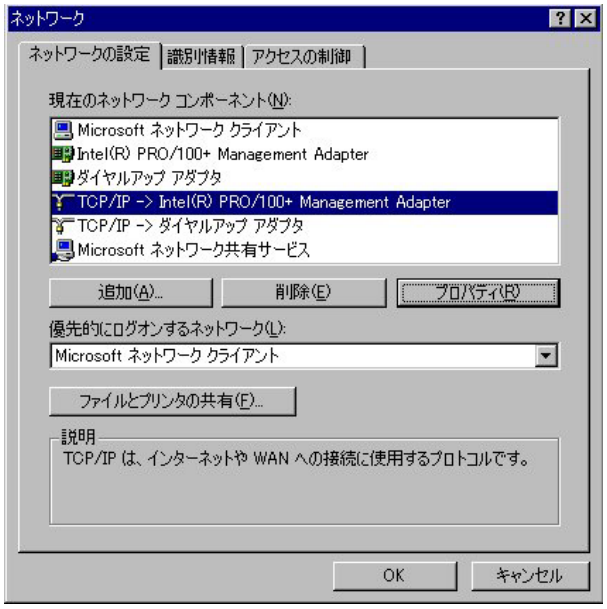
本章では、設定に使うパソコン側のネットワーク設定の方法について、OS毎に説明します。パソコンのOSに合わせてページを参照し、設定を行ってください。

第２章 コンピュータのネットワーク設定

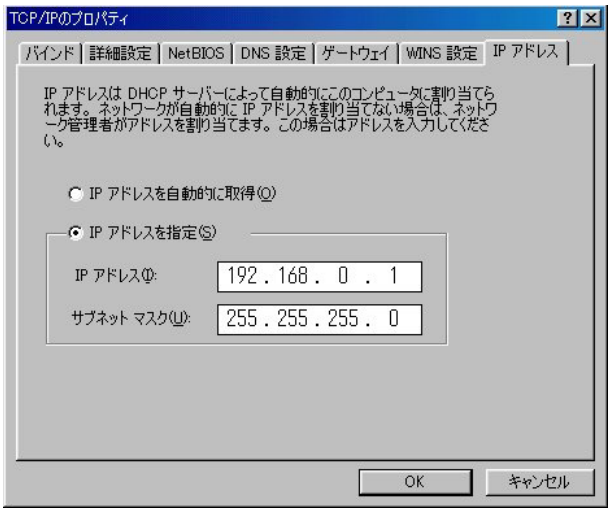
Ⅰ．Windows 95/98/Me のネットワーク設定

ここではWindows95/98/Me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。

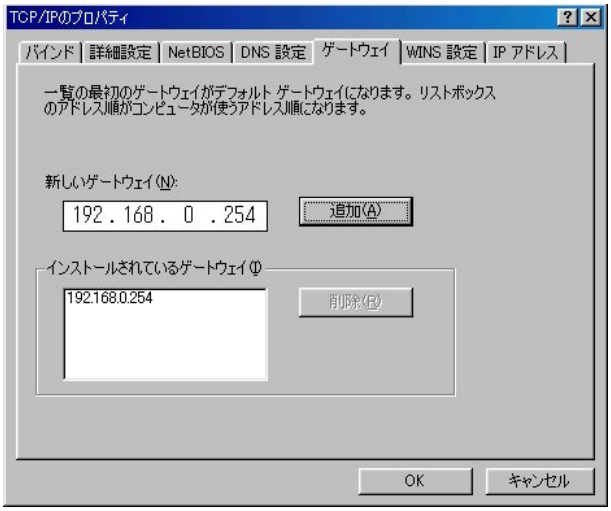
1 「コントロールパネル」→「ネットワーク」の順で開き、「ネットワークの設定」タブの「現在のネットワーク構成」から、コンピュータに装着されたLANボード(カード)のプロパティを開きます。



2 「TCP/IPのプロパティ」が開いたら、「IPアドレス」タブをクリックしてIP設定をおこないます。「IPアドレスを指定」にチェックを入れて、IPアドレスに「192.168.0.1」、サブネットマスクに「255.255.255.0」と入力します。



3 続いて「ゲートウェイ」タブをクリックして、新しいゲートウェイに「192.168.0.254」と入力して追加ボタンをクリックしてください。



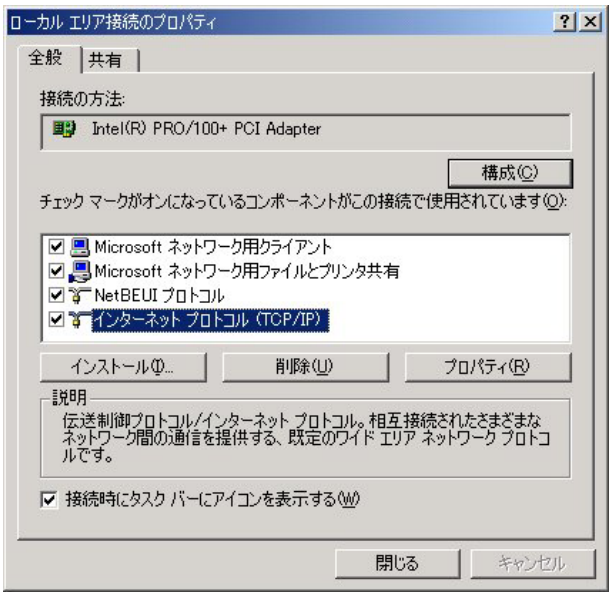
4 最後にOKボタンをクリックするとコンピュータが再起動します。再起動後に、本装置の設定画面へのログインが可能になります。

II．Windows 2000のネットワーク設定

ここではWindows2000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。

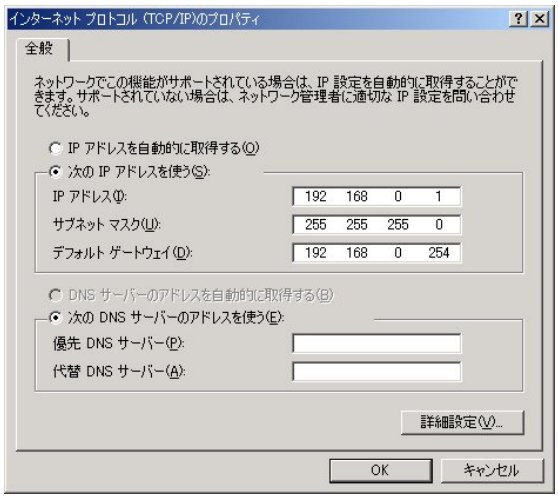
1 「コントロールパネル」→「ネットワークとダイヤルアップ接続」から、「ローカル接続」を開きます。

2 画面が開いたら、「インターネットプロトコル(TCP/IP)」のプロパティを開きます。



3 「全般」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」



4 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。

III. 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。

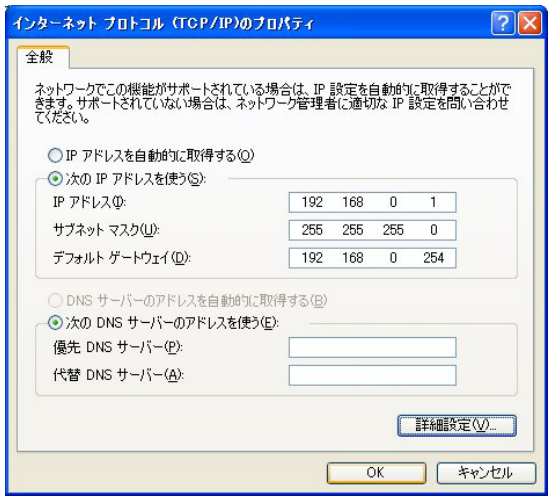
1 「コントロールパネル」→「ネットワーク接続」から、「ローカル接続」を開きます。

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」



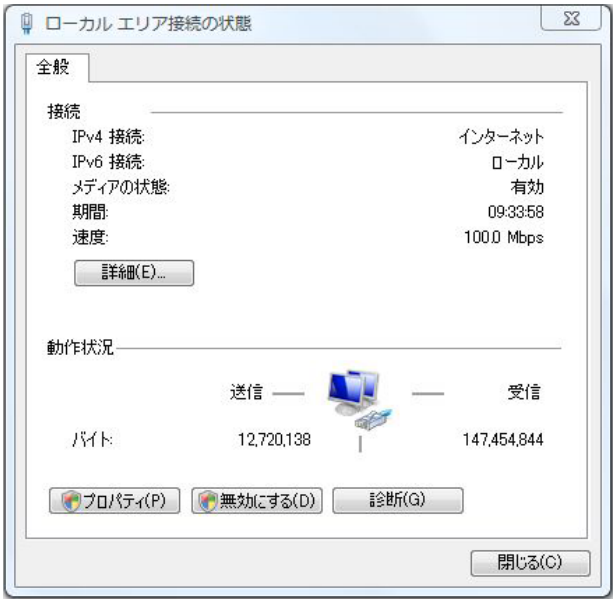
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

Ⅳ. Windows Vistaのネットワーク設定

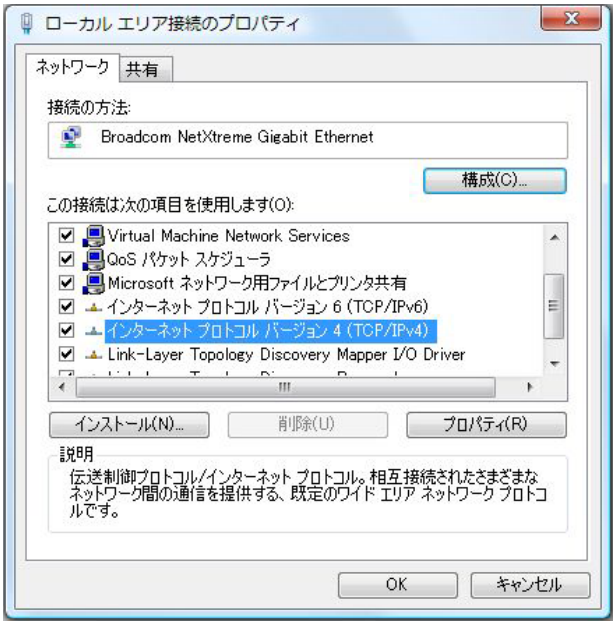
ここではWindows Vistaが搭載されたコンピュータのネットワーク設定について説明します。

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。

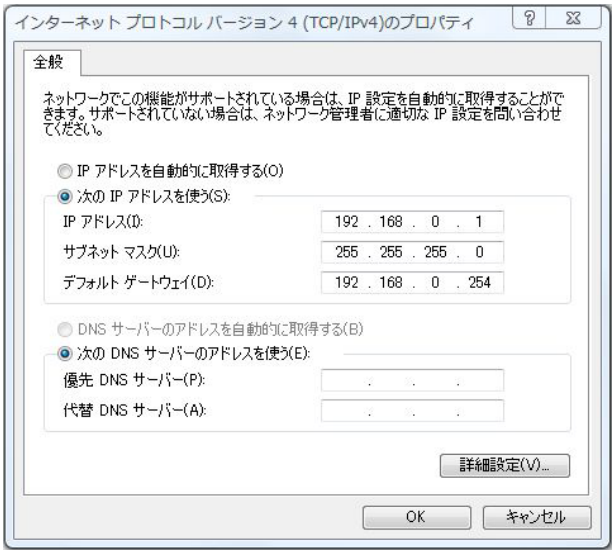


3 「ローカルエリア接続のプロパティ」画面が開いたら、「インターネットプロトコルバージョン4(TCP/IPv4)」を選択して「プロパティ」ボタンをクリックします。



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」



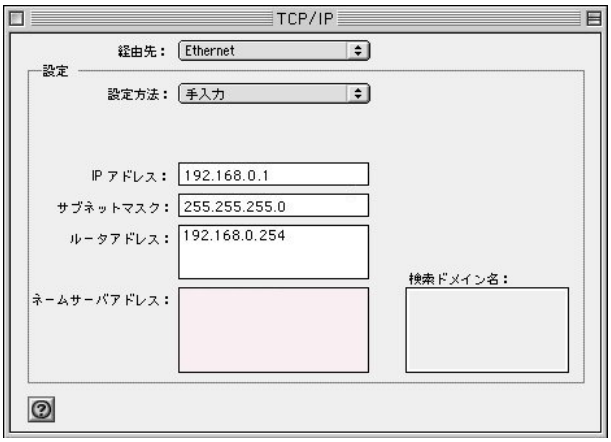
5 最後にOKボタンをクリックして設定完了です。これで本装置へのログインの準備が整いました。

Ｖ．Macintoshのネットワーク設定

ここではMacintoshのネットワーク設定について説明します。

1 「アップルメニュー」から「コントロールパネル」→「TCP/IP」を開きます。

2 経由先を「Ethernet」、設定方法を「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」
ルーターアドレス「192.168.0.254」

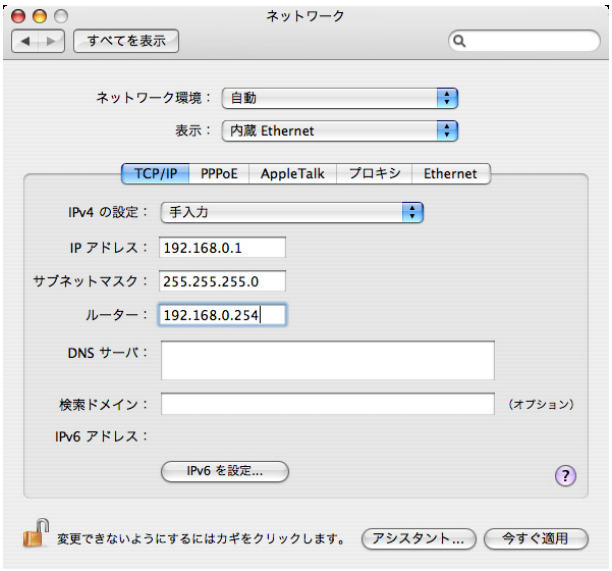


3 ウィンドウを閉じて設定を保存します。その後Macintosh本体を再起動してください。これで本装置へログインする準備が整いました。

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

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行ないます。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。
HTTP(ポート 80)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。

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。**設定画面のポート番号 80 は変更することができません。**

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/

「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。

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 Explorer6.0 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。

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。

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

[表示画面例]

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。

[入力画面例]

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項目毎に説明ページを参照してください。

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	説明ページ
1．管理者	○	○	○		P.29
2．ネットワーク基本情報	○	○	○		P.30
3．内蔵時計	○	○	○		P.31
4．ログ	○	○	○		P.32
5．スタティックルート	○	○	○		P.33
6．DNS	○	○	○		P.34
7．NTP	○	○	○		P.35
8．SNMP	○	○	○		P.36
9．CA- 基本情報	○				P.37
10．CA-RADIUS サーバ証明書	○				P.39
11．CA-HTTPS サーバ証明書	○				P.40
12．CA-LDAP クライアント証明書	○				P.40
13．CA-LDAP サーバ証明書	○				P.40
14．管理画面へのアクセス	○	○	○		P.41
15．RADIUS- 基本情報	○	○			P.42
16．RADIUS- 二重化	○	○			P.43
17．RADIUS- ログ	○	○			P.44
18．RADIUS- アドレスプール	○	○			P.45
19．RADIUS- クライアント	○	○			P.46
20．RADIUS- アトリビュート	○	○			P.47
21．RADIUS-ActiveDirectory	○				P.49
22．RADIUS-LDAP	○				P.50
23．RADIUS- ユーザ基本情報	○	○		○	P.52
24．RADIUS- 認証アトリビュート	○	○		○	P.54
25．RADIUS- 応答アトリビュート	○	○		○	P.56
26．RADIUS- グループ ID	○	○		○	P.57
27．RADIUS- ユーザ証明書	○			○	P.58
28．RADIUS- ユーザプロファイル	○	○		○	P.59
29．RADIUS- ユーザ作成	○	○		○	P.60
30．RADIUS-AD ユーザ	○				P.64
31．RADIUS-LDAP ユーザ	○				P.65
32．ユーザ管理者	○	○	○		P.66
33．フィルタ	○	○	○		P.67
34．RADIUS 起動	○	○			P.69
35．設定の保存	○	○	○	○	P.70
36．完了	○	○	○	○	P.71

表． 各設定ウィザード毎の設定内容一覧

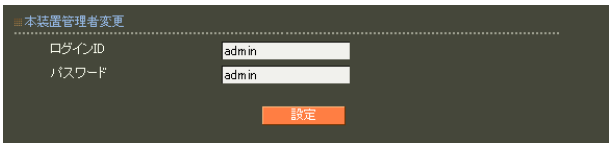
Ⅱ．設定内容の詳細

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。
入力後「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。

ログインIDに使用可能な文字は英数字および以下の記号になります。

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

パスワードに使用可能な文字は、ユーザIDの入力可能文字に加え空白文字と以下になります。

```
,:;\
```

Ⅱ．設定内容の詳細

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。

○インターフェイス
インターフェイスの設定を変更する場合は変更したいインターフェイス欄の「編集」ボタンを押します。次の入力画面が表示されます。

・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

・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 のままで利用して下さい。

・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。

(※ RA-630 のみ)
Ether2 ポートは自動設定のみとなります。

○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。

・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。

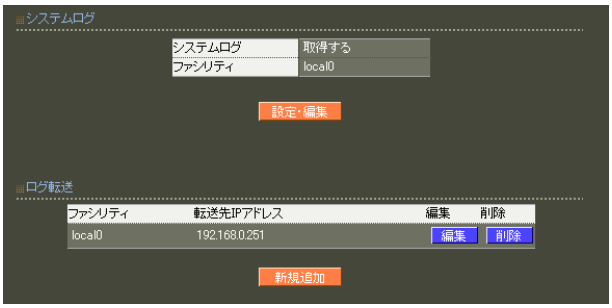
24時間単位で時刻を設定してください。

「設定」ボタンをクリックして設定完了です。

Ⅱ．設定内容の詳細

４．ログ

システム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。



○システムログ
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。

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。「取得する」にした場合、ファシリティをプルダウンから選択します。ログが指定されたファシリティで出力されます。

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。

○ログ転送一覧
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
「新規追加」をクリックすると入力画面が表示されます。

・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。

・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。

転送先は最大５個まで設定することができます。

○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。

本装置に記録しておけるログの容量には制限があります。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
「新規追加」をクリックすると入力画面が表示されます。

・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。

スタティックルートは最大 10 個まで設定することができます。

○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。

・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 サーバと通信を行い、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 一覧
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。

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

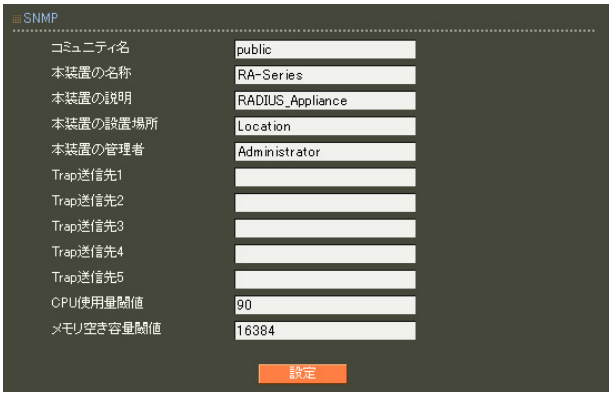
Ⅱ．設定内容の詳細

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。



・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 送信元 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。
推奨値は 90 です。

・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。
推奨値は 16384 (16 MB)です。

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。

◯ 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サービス起動時にCold Startを送信
・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。

(※RA-630のみ)
ただし、Ether 2 については 実際のlink up/downの状態によらず常にupとして扱われます。

設定情報の同期を行う設定の場合でも、本設定は対向装置へ同期されません。

なお、CPU 及びメモリの状況は、GetRequest 等で取得できます。
例:

```
$ snmpwalk -v2c -c public 192.168.0.254 enterprises
enterprises.20376.3.1.1.1.1.0 = 4
enterprises.20376.3.1.1.1.2.0 = 1
enterprises.20376.3.1.1.1.3.0 = 95
enterprises.20376.3.1.1.2.1.0 = 256608
enterprises.20376.3.1.1.2.2.0 = 194280

$ snmpwalk -v2c -c public 192.168.0.254 -M CS-Product-RA-MIB.txt enterprises
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemCPU.csRASystemCPUUser.0
= 4
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemCPU.csRASystemCPUSystem.0
= 1
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemCPU.csRASystemCPUIdle.0
= 95
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemMemory.csRASystemMemoryTotal.0
= 256608
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemMemory.csRASystemMemoryFree.0
= 194280
```

９.CA - 基本情報

本装置のCAの設定を行います。

「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。

・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。
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。

・Signature Algorithm
署名アルゴリズムを選択します。
署名アルゴリズムは「SHA-1」または「MD5」を選択することができます。

・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で設定します。

・パスフレーズ
パスフレーズを入力します。
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。

・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。
1-365日の間で指定します。

※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(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/
  0-9, a-z, A-Z, -, _
- 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。

II．設定内容の詳細

CA の設定を一度行うと、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/ 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。

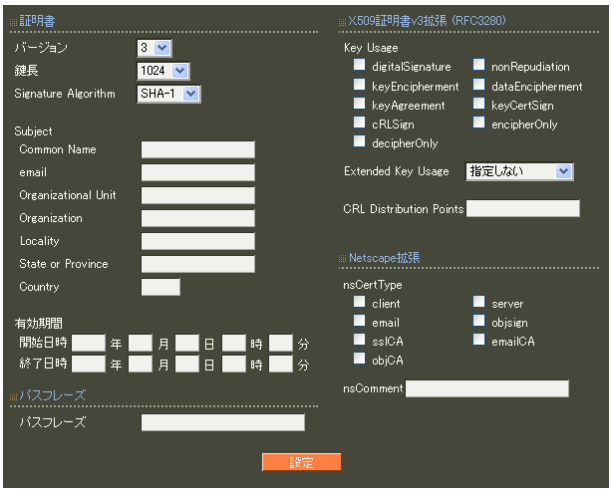
○失効リストの取得
失効リストの取得欄で「取り出し」ボタンをクリックすることにより CRL を取り出すことができます。
この際、取り出す形式を PEM または DER から選択することができます。

○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。

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行います。

「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」の117ページ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」を参照して下さい。

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行います。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

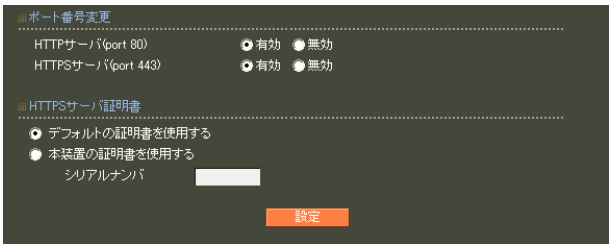
ユーザ認証時に LDAP サーバ連携をおこなう場合で、StartTLS または LDAPS プロトコルにより通信を保護したい場合に、LDAP サーバ側の証明書を作成します。このメニューの操作は「10.CA-RADIUS サーバ証明書」と同一になります。本証明書の作成後、この証明書を取り出して、LDAP サーバに設定をしてください。

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行います。

画面中の「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」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。



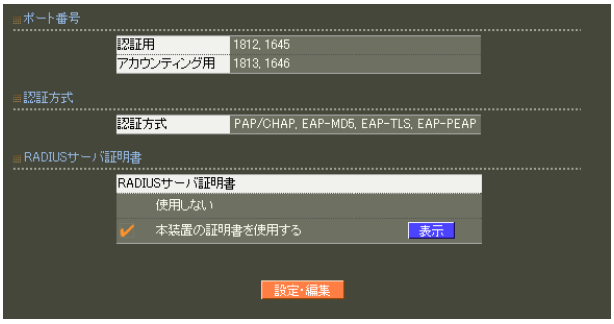
・ポート番号
HTTP/HTTPS によるアクセスを有効にするか無効にするかを選択します。必ずどちらかは有効にしておく必要があります。

・HTTPS サーバ証明書
デフォルトで設定されている証明書を使用するか、「CA」で設定したサーバ証明書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。

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。

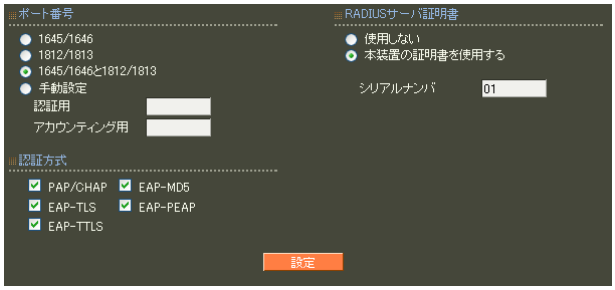
15.RADIUS - 基本情報

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行います。



画面中の「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」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行っていますが、そのポート番号の設定を行います。
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行います。
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

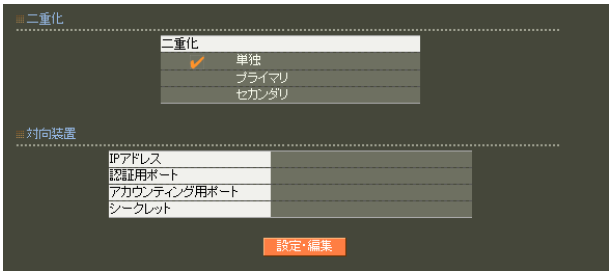
使用する認証方式のチェックボックスをチェックしてください。なお、「EAP-PEAP」または「EAP-TTLS」を選択する場合は、「EAP-TLS」も選択しておく必要があります。また、「EAP-TTLS」を選択する場合には TTLS 内部認証で使う認証方式も同時に選択してください。

◯ RADIUS サーバ証明書設定
認証で、「EAP-TLS」、「EAP-PEAP」まはた「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。

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

本装置を単独で利用する場合には「単独」を設定します。

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」に相手装置の IP アドレスを入力します。

また、「認証用ポート」、「アカウンティング用ポート」、「シークレット」の３項目を相手装置の設定内容と一致するように入力します。

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。

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
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。「取得する」にした場合、ファシリティをプルダウンから選択します。認証ログが指定されたファシリティで出力されます。

○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。「取得する」にした場合、ファシリティをプルダウンから選択します。アカウンティングログが指定されたファシリティで出力されます。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。
項目の詳細については「第６章　RADIUS 設定」の92ページ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
「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、下記のとおりです。

RA-630 ： 10 個
RA-1100: 100 個

◯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
「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。この設定内容は、RADIUSクライアントから送られてくるアトリビュート ”NAS-IP-Address” との比較に使われ、クライアントの識別に用いられます。

・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。

・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。

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。

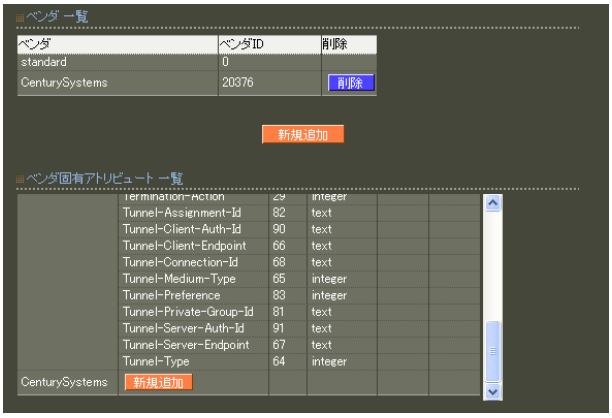
設定可能なクライアントの最大数は、下記のとおりです。

RA-630 ： 100個
RA-1100: 1,000個

○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。



上段の表に登録されているベンダの一覧が表示されます。また、下段の表に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。

◯ベンダ
ベンダ一覧から「新規追加」ボタンを押してベンダの追加を先におこないます。

・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。

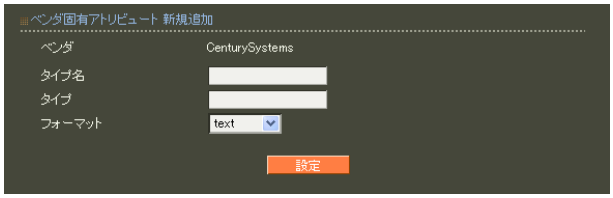
・ベンダ ID
ベンダ毎に割り当てられているベンダ ID を数値で入力します。

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。

ベンダは最大 10 個まで登録することができます。

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
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
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 4 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。

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。

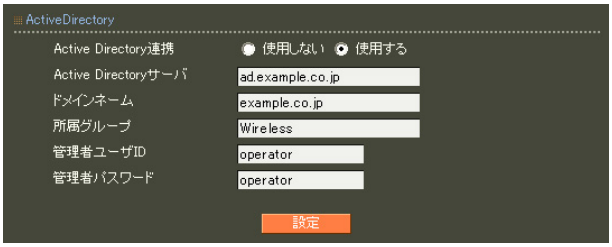
ベンダ固有アトリビュートはベンダ毎に最大 10 個まで設定することができます。

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。



・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
Active Directory が稼動しているドメインコントローラのホスト名を FQDN または IP アドレスで指定します。

・ドメインネーム
認証を受けるドメイン名を入力します。

・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行います。

・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。

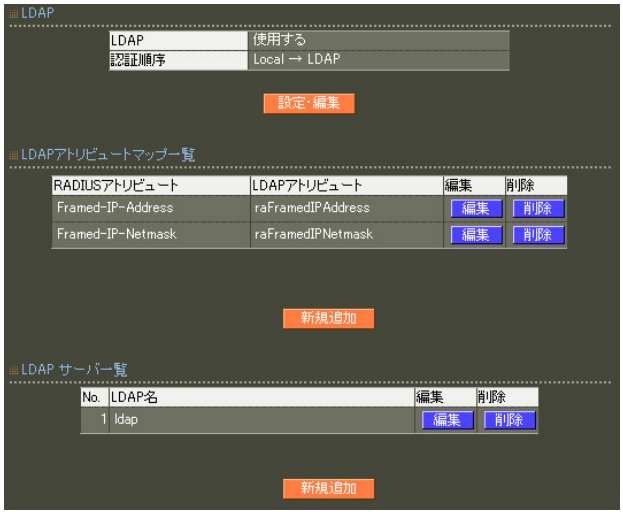
・管理者パスワード
管理者ユーザ ID に対応したパスワードを入力します。

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。

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。

22.RADIUS - LDAP

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



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。

◯ LDAPの設定・編集
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行われます。

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数は10です。

設定情報の同期を行う設定の場合、本設定は対向装置へ同期されます。

◯ LDAPアトリビュートマップの新規追加
「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。

・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行われます。

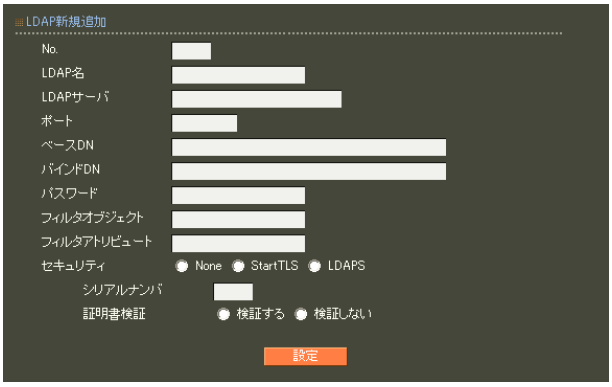
使用可能な文字は、下記の通りです。
0-9，a-z，A-z，-(0x2c)，_(0x5f)。
最大文字数は「20」で、デフォルト値はありません。

○ LDAP アトリビュートマップの編集
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。

○ LDAP アトリビュートマップの削除
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。

○ LDAP サーバの新規追加
「新規追加」ボタンを押すと入力画面が表示されます。

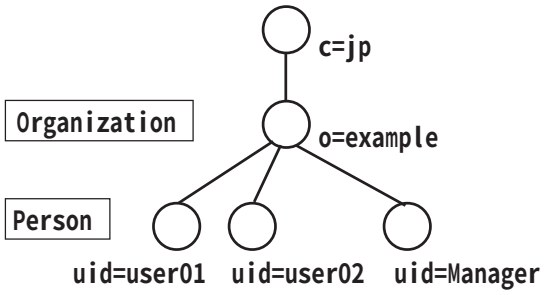


・No.
この LDAP サーバの認証の順番を指定します。
空欄にした場合には既存の LDAP サーバ設定の最後に追加されます。
既に LDAP サーバが登録されている番号を指定した場合には、今回作成する LDAP サーバがその番号で設定され、指定された番号から下の既存の LDAP サーバ設定が一つずつ後ろにずれて設定されます。

・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。



図：ディレクトリツリーの例

・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

・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。
＜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。

・フィルタオブジェクト
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、オブジェクトクラスを指定して検索をおこないたい場合に指定します。
＜入力例＞
person

・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」参照)。
使用する証明書のシリアルナンバを 1 6 進数で入力します。

・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。

LDAP サーバは最大 10 台まで設定することができます。

○ LDAP サーバの変更・削除
LDAP サーバ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。

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
「新規追加」をクリックすると入力画面が表示されます。

・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行います。
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」を選択して下さい。

（次ページへ続きます。）

・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、下記のとおりです。

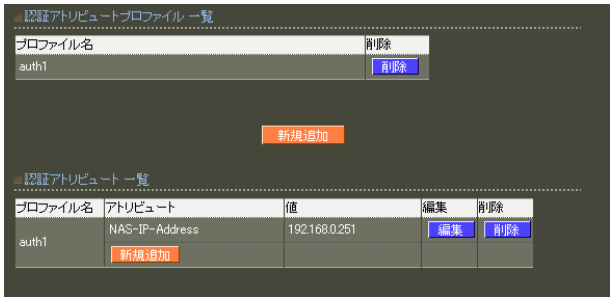
RA-630 ： 20 個
RA-1100：100 個

◯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。



上段の表に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。
下段の表に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
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。

「プロファイル名」に任意の名前を 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。

認証アトリビュートプロファイルは最大 20 個まで登録することができます。

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。

II．設定内容の詳細

○認証アトリビュート
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。

・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。但し、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

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。

アトリビュートは 1 プロファイルあたり最大 10 個まで設定することができます。

○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。

上段の表に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。
下段の表に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
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。

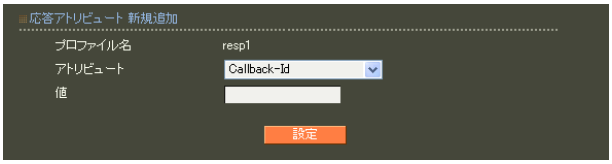
「プロファイル名」に任意の名前を20文字以内で入力します。「ユーザプロファイル」メニューで応答アトリビュートプロファイルを設定する際に、ここで設定されたプロファイル名が選択肢として表示されます。

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。

応答アトリビュートプロファイルは最大20個まで登録することができます。

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
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。



・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。

アトリビュートは1プロファイルあたり最大10個まで設定することができます。

○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
「新規追加」をクリックすると入力画面が表示されます。

・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。

グループ ID プロファイルは最大 50 個まで設定することができます。

○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
「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」の 103 ページを参照して入力してください。

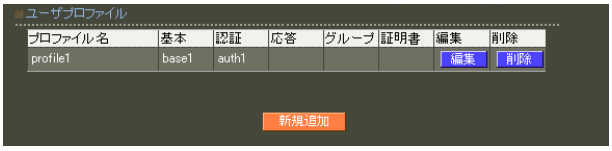
各項目に入力後、「設定」ボタンを押すと設定内容が保存され、一覧表示画面に戻ります。

証明書プロファイルは最大 20 個まで設定することができます。

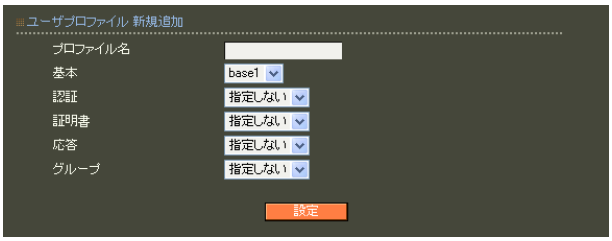
○変更・削除
証明書プロファイル一覧に登録されている設定を編集または削除したい場合には、そのプロファイルが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

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
「新規追加」をクリックすると入力画面が表示されます。



「プロファイル名」には任意の名前を 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行う際に、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。

「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」は、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、下記のとおりです。

RA-630 ： 20 個
RA-1100： 100 個

○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。

○ユーザの追加
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 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 の入力可能文字に加え空白文字と以下になります。
,:;\

・ユーザプロファイル
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。

・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。

・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、認証処理を行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。
設定情報の同期を行う設定の場合、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、下記のとおりです。
RA-630 ： 2,000個
RA-1100: 50,000個

※ 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。

II．設定内容の詳細

ユーザが登録されると、表示画面では次のようなユーザー一覧が表示されるようになります。

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 / 編集 / 削除

ユーザー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。

画面上部には現在設定されているユーザ設定情報が表示されます。
また下段には、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。
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ー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。

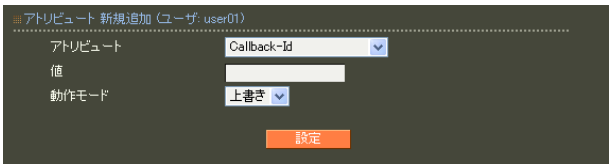
個別設定が可能なアトリビュート
ユーザ基本情報、認証、応答

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。

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。

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
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」を選択した場合、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」を選択した場合、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」を選択した場合には、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。

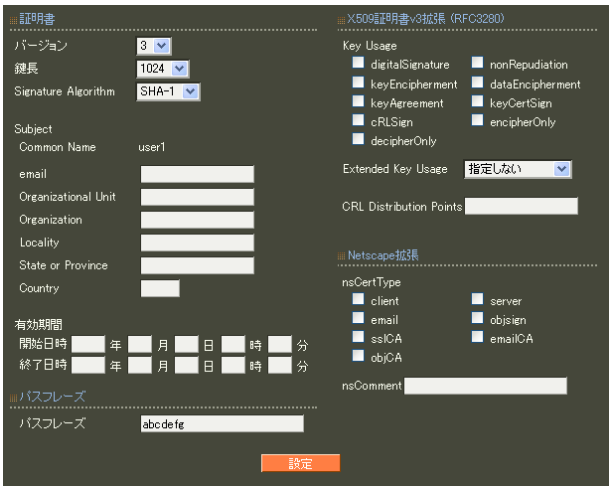
「設定」ボタンを押すと個別設定が適用されます。
個別設定ではユーザ毎に 5 つのプロファイルを追加または削除指定することができます。

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。)
このボタンを押すと、次のユーザ証明書の作成画面が表示されます。

Ⅱ．設定内容の詳細



Subject の Common Name にはユーザ 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。

・Subject
　・emailAddress
　　ユーザのメールアドレスを設定します。

・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。

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。形式は PKCS#12，PEM，DER から、一つ選択します。
内容は、「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下さい。

・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。

使用するプロファイルを選択して「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。

使用するプロファイルを選択して「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。

LDAP 連携は PAP および EAP-TTLS/PAP 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 PAP または EAP-TTLS/PAP 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。

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。

○ユーザ管理者新規追加
「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。「アカウントロック」は通常は「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。

ユーザ管理者は最大５人まで設定することができます。

ログイン ID に使用可能な文字は英数字および以下の記号になります。

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

パスワードに使用可能な文字は、ユーザ ID の入力可能文字に加え空白文字と以下になります。

```
,:;\
```

○ユーザ管理者変更・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、本装置が送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。

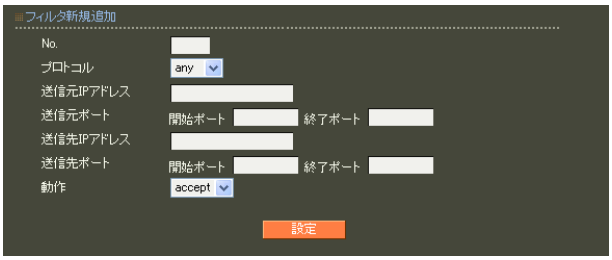
フィルタルールと一致しなかった場合にパケットを通過させる場合には「ACCEPT」を、破棄させる場合には「DROP」を選択します。選択後「設定」ボタンをクリックして設定完了です。設定はすぐに反映されます。

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	TCP/802 ～ 803
NTP	TCP/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)

○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。

○フィルタ新規追加
「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。



・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 又は 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。

フィルタルールは最大 20 個まで設定することができます。

○フィルタ変更・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。

よく使われるポートの番号については、下記の表を参考にしてください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

34.RADIUS 起動

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。

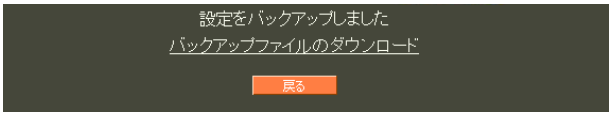
起動途中および再起動途中に他の操作を行なわないでください。

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行う事をお勧めします。

設定を保存するときは、文字コードを選択して保存ボタンを押します。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

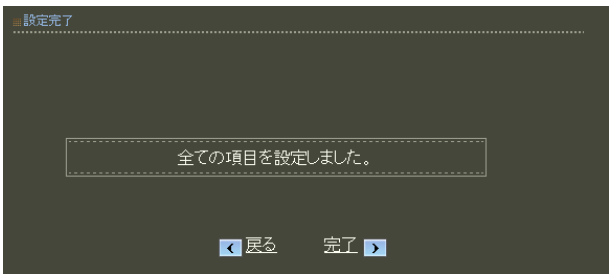
・User：
設定ファイルを取り出したユーザ名

・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。



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。

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。

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
    - 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

画面構成

- 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
  - 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
    - 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
    - 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
  - 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行なわないでください。

Ⅰ．サーバ設定

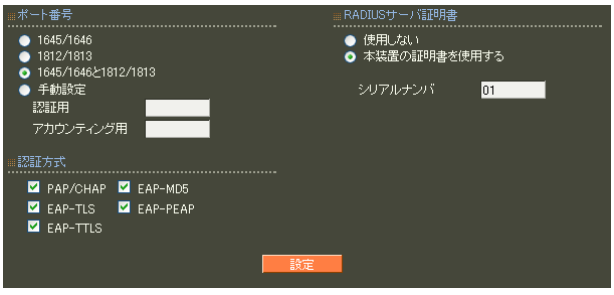
２．基本情報

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行います。

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。

画面中の「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」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行っていますが、そのポート番号の設定を行います。
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行います。
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」まはた「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。

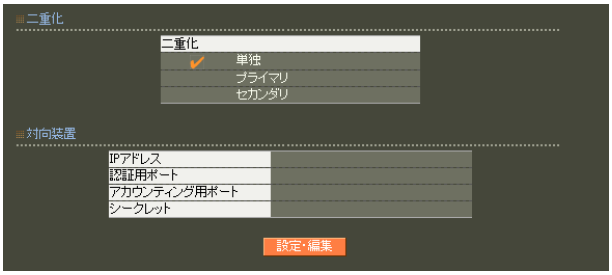
各項目に入力後、「設定」ボタンを押すと設定内容が保存されます。保存された設定内容を反映させるには、RADIUSサーバの再起動が必要になります。

Ⅰ．サーバ設定

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

本装置を単独で利用する場合には「単独」を設定します。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

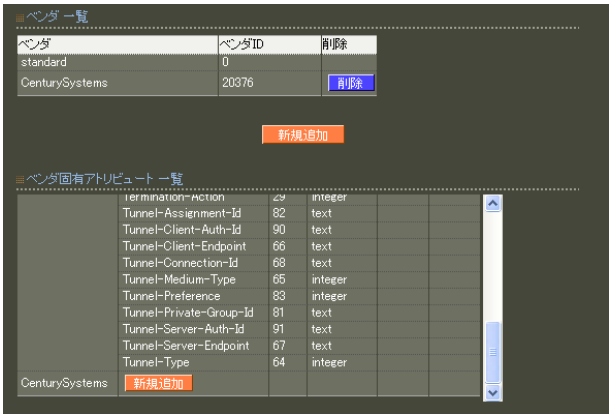
二重化構成で使用する場合の、相手装置に関する情報を入力します。「IPアドレス」に相手装置のIPアドレスを入力します。また、「認証用ポート」、「アカウンティング用ポート」、「シークレット」の３項目を相手装置の設定内容と一致するように入力します。

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。

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。



上段の表に登録されているベンダの一覧が表示されます。また、下段の表に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。

◯ベンダ
ベンダ一覧から「新規追加」ボタンを押してベンダの追加を先におこないます。

・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。

ベンダは最大 10 個まで登録することができます。

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
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。

・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 4 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。

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。

ベンダ固有アトリビュートはベンダ毎に最大 10 個まで設定することができます。

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。

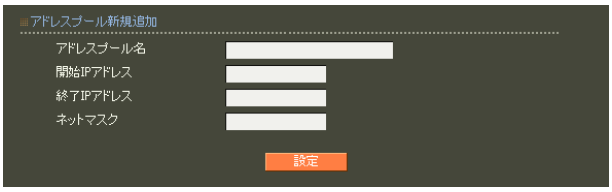
Ⅰ．サーバ設定

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
「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、下記のとおりです。

RA-630 ： 10 個
RA-1100: 100 個

◯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
「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。この設定内容は、RADIUS クライアントから送られてくるアトリビュート ”NAS-IP-Address ” との比較に使われ、クライアントの識別に用いられます。

・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。

・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。

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、下記のとおりです。

RA-630 ： 100個
RA-1100: 1,000個

○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。

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。

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。

・Active Directory 連携
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
Active Directory が稼動しているドメインコントローラのホスト名を FQDN または IP アドレスで指定します。

・ドメインネーム
認証を受けるドメイン名を入力します。

・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行います。

・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。

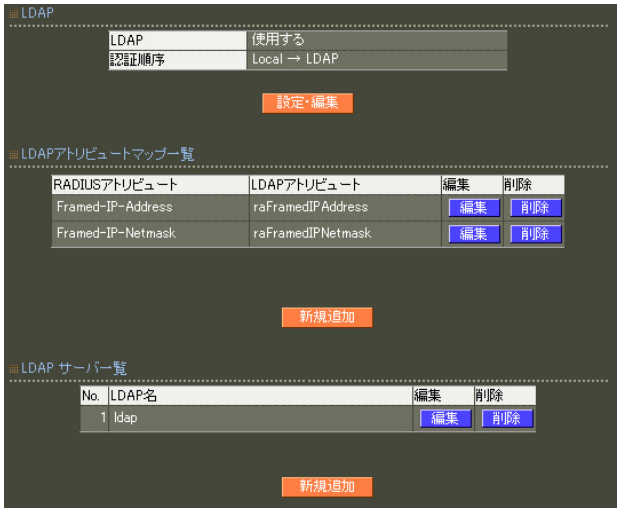
Active Directory 連携機能を利用するためには、DNS の設定(管理機能メニューの「ネットワーク」-「DNS」)で所属するドメインの DNS サーバが設定されている必要があります。

Ⅰ．サーバ設定

8 .LDAP

ユーザ認証を LDAP サーバでおこないたい場合に設定します。本設定をおこなうと PAP または EAP-TTLS/PAP による認証要求を受けた場合に、設定された LDAP 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「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。

◯ LDAP の設定・編集
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 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行われます。

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数は 10 です。

設定情報の同期を行う設定の場合、本設定は対向装置へ同期されます。

◯ LDAP アトリビュートマップの新規追加
「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。

・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。

Ⅰ．サーバ設定

・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行われます。

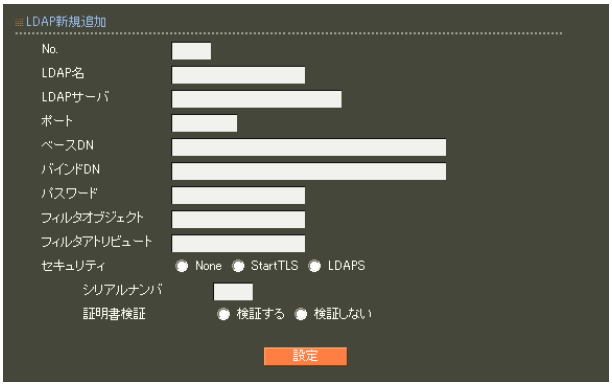
使用可能な文字は、下記の通りです。
0-9，a-z，A-z，-(0x2c)，_(0x5f)。
最大文字数は「20」で、デフォルト値はありません。

○ LDAP アトリビュートマップの編集
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。

○ LDAP アトリビュートマップの削除
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。

○ LDAP サーバの新規追加
「新規追加」ボタンを押すと入力画面が表示されます。

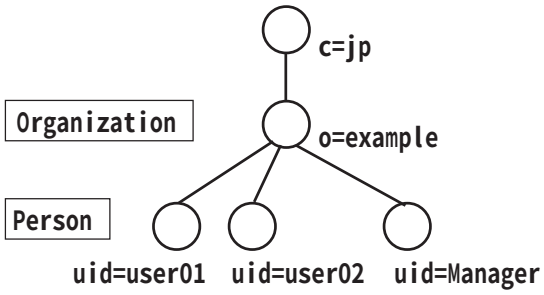


・No.
この LDAP サーバの認証の順番を指定します。空欄にした場合には既存の LDAP サーバ設定の最後に追加されます。既に LDAP サーバが登録されている番号を指定した場合には、今回作成する LDAP サーバがその番号で設定され、指定された番号から下の既存の LDAP サーバ設定が一つずつ後ろにずれて設定されます。

・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。



図：ディレクトリツリーの例

・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

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。

＜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。

・フィルタオブジェクト
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、オブジェクトクラスを指定して検索をおこないたい場合に指定します。

＜入力例＞
person

・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」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。

・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。

LDAPサーバは最大10台まで設定することができます。

○ LDAPサーバの変更・削除
LDAPサーバ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

９．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
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。「取得する」にした場合、ファシリティをプルダウンから選択します。認証ログが指定されたファシリティで出力されます。

○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。「取得する」にした場合、ファシリティをプルダウンから選択します。アカウンティングログが指定されたファシリティで出力されます。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。
- 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行う際には、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。

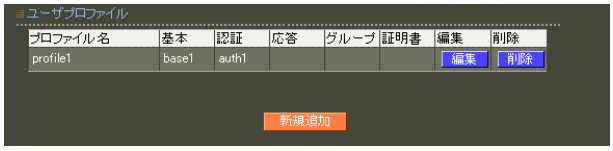
本メニューではこのプロファイルの設定をおこないます。

Ⅱ．プロファイル

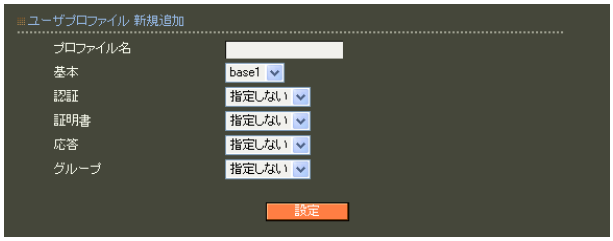
１．ユーザプロファイル

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
「新規追加」をクリックすると入力画面が表示されます。



「プロファイル名」には任意の名前を 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行う際に、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。）

「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」は、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、下記のとおりです。

RA-630 ： 20 個
RA-1100： 100 個

◯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
「新規追加」をクリックすると入力画面が表示されます。

・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行います。
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」を選択して下さい。

・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、下記のとおりです。

RA-630 ： 20 個
RA-1100: 100 個

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。

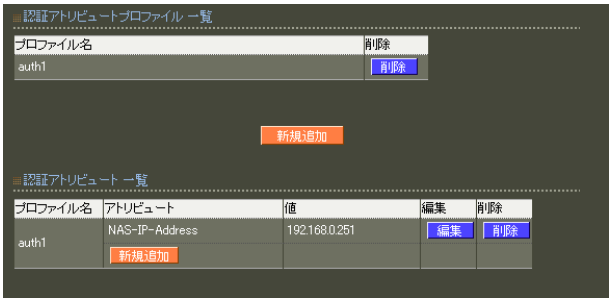
プロファイルの編集をおこなって設定を変更した場合、そのプロファイルを使って定義されているユーザにも変更された設定が反映されます。

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。



上段の表に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。下段の表に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
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。

「プロファイル名」に任意の名前を 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、下記のとおりです。

RA-630 ： 20 個
RA-1100: 100 個

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
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。

・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。但し、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

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。

アトリビュートは 1 プロファイルあたり最大 10 個まで設定することができます。

○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。

Ⅱ．プロファイル

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。

上段の表に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。下段の表に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
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。

「プロファイル名」に任意の名前を 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。

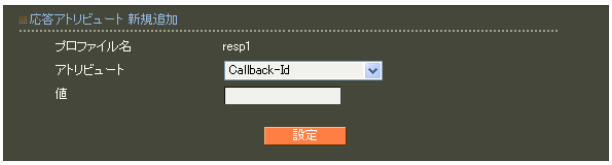
応答アトリビュートプロファイルは最大 20 個まで登録することができます。

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
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。



・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。但し、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

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。

アトリビュートは 1 プロファイルあたり最大 20 個まで設定することができます。

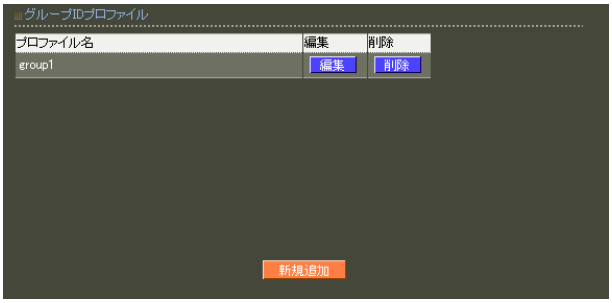
○変更・削除
応答アトリビュート一覧に登録されている設定を編集または削除したい場合には、そのアトリビュートが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

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
「新規追加」をクリックすると入力画面が表示されます。

・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。

グループ ID プロファイルは最大 50 個まで設定することができます。

◯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。

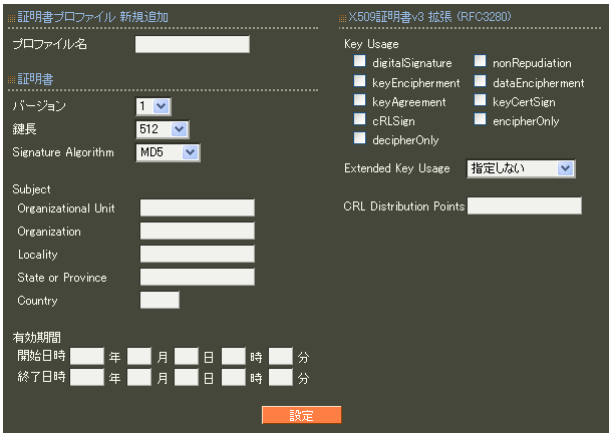
Ⅱ．プロファイル

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
「新規追加」をクリックすると入力画面が表示されます。



・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。
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。

・signature algorithm
署名アルゴリズムを選択します。署名アルゴリズムは「SHA-1」または「MD5」を選択することができます。

・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 Country を除き英数字およびハイフン(“ - ”)、アンダーバー(“ _ ”)になります。Country は英大文字で入力してください。

・有効期間
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、有効期間の終了日時

II．プロファイル

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、設定を行って下さい。

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。

証明書プロファイルは最大 20 個まで設定することができます。

◯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。

○ユーザの追加
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 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 の入力可能文字に加え空白文字と以下になります。

,:;\

・ユーザプロファイル
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。

・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。

・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、認証処理を行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。
設定情報の同期を行う設定の場合、本設定は対向装置へ同期されます。

III．ユーザ設定

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、下記のとおりです。

RA-630 ： 2,000 個
RA-1100: 50,000 個

※ 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。

○ユーザの詳細表示 / 編集 / 削除
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。

画面上部には現在設定されているユーザ設定情報が表示されます。
また下段には、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。

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。

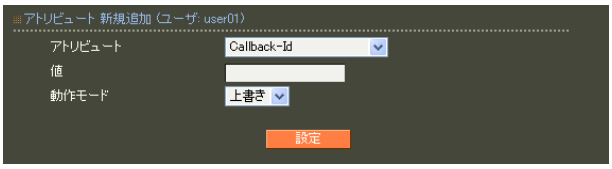
個別設定が可能なアトリビュート
ユーザ基本情報、認証、応答

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。

III．ユーザ設定

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。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
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。

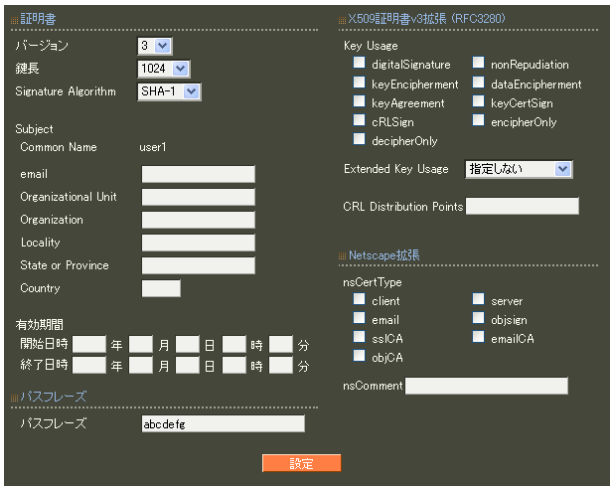
・動作モード
「上書き」、「追加」、「削除」の中から選択します。（認証アトリビュートの場合は「追加」は選択できません。）「上書き」を選択した場合、プロファイルで同じアトリビュートが存在していた場合、プロファイルで設定されたアトリビュート値はこのユーザには適用されず、個別設定されたアトリビュート値のみが使われるようになります。
「追加」を選択した場合、プロファイルで同じアトリビュートが存在していた場合、プロファイルで設定されたアトリビュート値と、個別設定されたアトリビュート値の両方がユーザに対して使われるようになります。指定したアトリビュートがプロファイルに存在しない場合には、「上書き」と「追加」で動作に違いは有りません。
「削除」を選択した場合には、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。個別設定ではユーザ毎に5つのプロファイルを追加または削除指定することができます。

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。)このボタンを押すと、次のユーザ証明書の作成画面が表示されます。



III．ユーザ設定

Subject の Common Name にはユーザ 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。

・Subject
　・emailAddress
　　ユーザのメールアドレスを設定します。

・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。

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行うことができます。

・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。形式は PKCS#12，PEM，DER から、一つ選択します。内容は、「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下さい。

・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。

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。

使用するプロファイルを選択して「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。

III．ユーザ設定

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。

使用するプロファイルを選択して「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。

LDAP 連携は PAP および EAP-TTLS/PAP 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 PAP またはEAP-TTLS/PAP 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。

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同時に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。

・リセット
既存の設定を消去してから読み込む場合にはリセットするを選択します。既存の設定に追加して読み込みたい場合にはリセットしないを選択してください。リセット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。

・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 B 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。

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。

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。

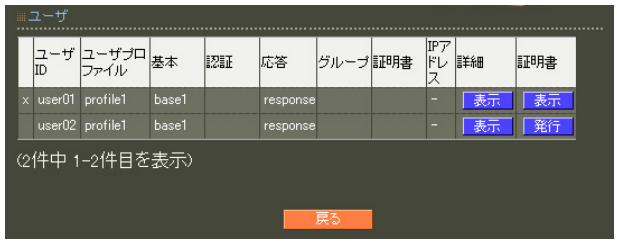
・基本条件
ユーザ基本情報プロファイルで設定されている内容に基づいて、詳細に検索条件を指定することができます。

・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。

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。

第7章

CA設定

第７章 CA設定

Ⅰ．CA/CRL設定

本装置のCAの設定を行います。

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。

◯CAの新規作成
「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。

・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。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。

・Signature Algorithm
署名アルゴリズムを選択します。署名アルゴリズムは「SHA-1」または「MD5」を選択することができます。

・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
証明書有効期間の終了日を設定します。

・パスフレーズ
パスフレーズを入力します。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。

・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。1-365日の間で指定します。

※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(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/
  0-9, a-z, A-Z, -, _
・Country
  A-Z

第7章 CA設定

Ⅰ．CA/CRL設定

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の設定を一度行うと、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/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。
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を再起動する必要があります。

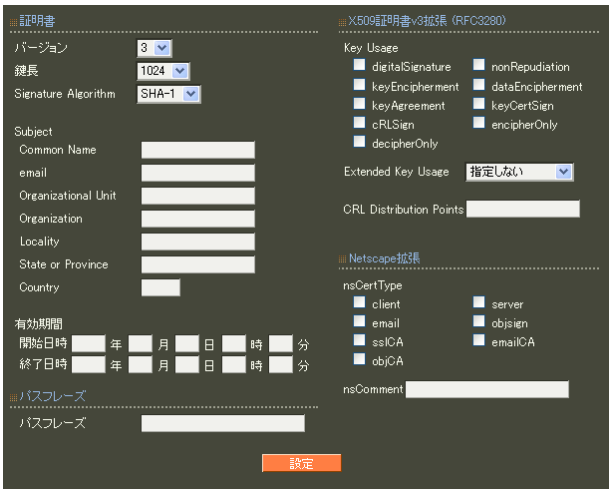
Ⅱ．証明書

ユーザ証明書、サーバ証明書の作成を行います。
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」を選択すると、現在作成されている証明書が一覧表示されます。

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。

○証明書の作成
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。



・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。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。

・Signature Algorithm
署名アルゴリズムを選択します。署名アルゴリズムは「SHA-1」または「MD5」を選択することができます。

・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/
　0-9, a-z, A-Z, -, _
・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
パスフレーズを入力します。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。

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、設定を行って下さい。

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

・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、通常最低限以下のKey Usage/Extended Key Usageを指定するようにします。
・Key Usage
  digitalSignature および 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、下記のとおりです。
RA-630 ： 2,000個
RA-1100: 10,000個

○証明書の表示
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。

・証明書の取り出し
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。形式はPKCS#12，PEM，DERから、一つ選択します。内容は、「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下さい。

・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を再起動する必要があります。

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。

○インターフェイス
インターフェイスの設定を変更する場合は変更したいインターフェイス欄の「編集」ボタンを押します。次の入力画面が表示されます。

・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

・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 のままで利用して下さい。

・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。

(※ RA-630 のみ)
Ether2 ポートは自動設定のみとなります。

○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。

・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。

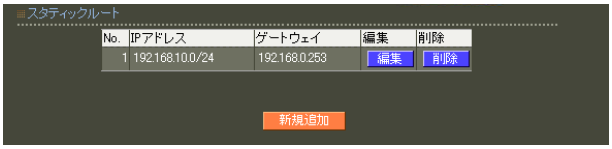
各項目に入力後、「設定」ボタンをクリックして設定完了です。設定はすぐに反映されます。

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。

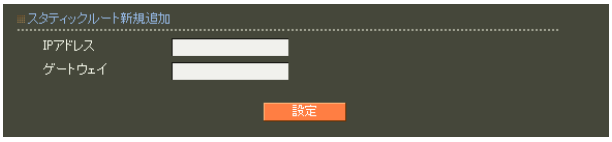
２．スタティックルート

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
「新規追加」をクリックすると入力画面が表示されます。



・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。

スタティックルートは最大 10 個まで設定することができます。

○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、本装置が送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。

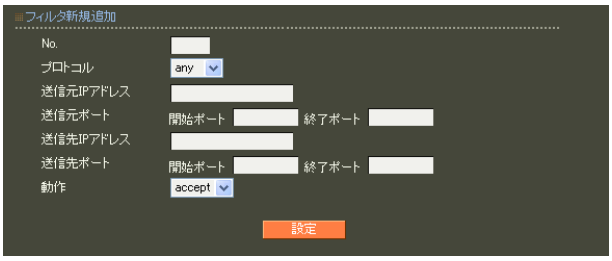
フィルタルールと一致しなかった場合にパケットを通過させる場合には「ACCEPT」を、破棄させる場合には「DROP」を選択します。選択後「設定」ボタンをクリックして設定完了です。
設定はすぐに反映されます。

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	TCP/802 ～ 803
NTP	TCP/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)

○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。

○フィルタ新規追加
「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。



・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。

Ⅰ．ネットワーク

・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 又は 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。

フィルタルールは最大 20 個まで設定することができます。

○フィルタ変更・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。

よく使われるポートの番号については、下記の表を参考にしてください。

ftp-data	20
ftp	21
telnet	23
smtp	25
dns	53
bootps	67
bootpc	68
tftp	69
finger	79
http	80
pop3	110
sunrpc	111
ident,auth	113
nntp	119
ntp	123
netBIOS	137～139
snmp	161
snmptrap	162
route	520

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。

・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。

Ⅰ．ネットワーク

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サーバと通信を行い、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 一覧
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。

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。

・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 送信元 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。推奨値は 90 です。

・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。
推奨値は 16384 (16 MB)です。

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。

◯ 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 サービス起動時に Cold Start を送信
・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。
ただし、Ether 2 については 実際の link up/down の状態によらず常に up として扱われます。

設定情報の同期を行う設定の場合でも、本設定は対向装置へ同期されません。

なお、CPU 及びメモリの状況は、GetRequest 等で取得できます。
例:

```
$ snmpwalk -v2c -c public 192.168.0.254 enterprises
enterprises.20376.3.1.1.1.1.0 = 4
enterprises.20376.3.1.1.1.2.0 = 1
enterprises.20376.3.1.1.1.3.0 = 95
enterprises.20376.3.1.1.2.1.0 = 256608
enterprises.20376.3.1.1.2.2.0 = 194280

$ snmpwalk -v2c -c public 192.168.0.254 -M CS-Product-RA-MIB.txt enterprises
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemCPU.csRASystemCPUUser.0
= 4
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemCPU.csRASystemCPUSystem.0
= 1
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemCPU.csRASystemCPUIdle.0
= 95
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemMemory.csRASystemMemoryTotal.0
= 256608
enterprises.centurysys.csMtRA.csRASystem.csRASystemObjects.csRASystemMemory.csRASystemMemoryFree.0
= 194280
```

Ⅱ．システム

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。

24時間単位で時刻を設定してください。

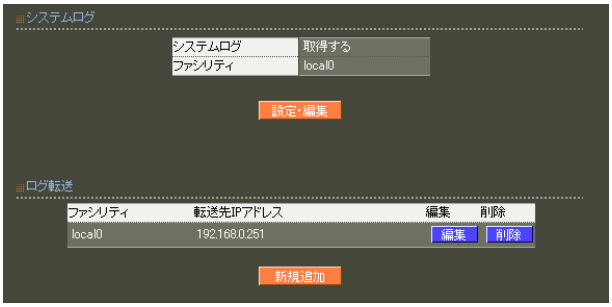
「設定」ボタンをクリックして設定完了です。

Ⅱ．システム

２．ログ

システム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。



◯システムログ
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。

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。「取得する」にした場合、ファシリティをプルダウンから選択します。ログが指定されたファシリティで出力されます。

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。

◯ログ転送一覧
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
「新規追加」をクリックすると入力画面が表示されます。

・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。

・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。

転送先は最大 5 個まで設定することができます。

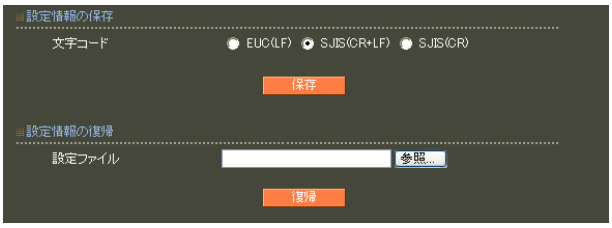
◯変更・削除
ログ転送一覧に登録されている設定を編集または削除したい場合には、そのエントリが表示されている行の「編集」ボタン、「削除」ボタンを押すことで実行できます。

本装置に記録しておけるログの容量には制限があります。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

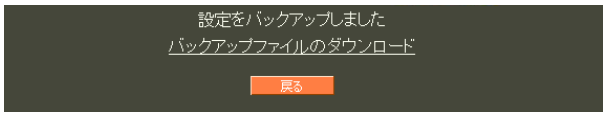
本装置の設定情報の保存、および保存した設定情報の復帰をおこないます。

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行う事をお勧めします。

○設定情報の保存
[設定の保存]
設定を保存するときは、文字コードを選択して保存ボタンを押します。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

・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
「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。

その後「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。

RADIUS サーバが起動している状態で設定の復帰をおこなった場合、正常に復帰しない場合があります。設定の復帰は RADIUS サーバが停止している状態でおこなってください。

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。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。

「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。

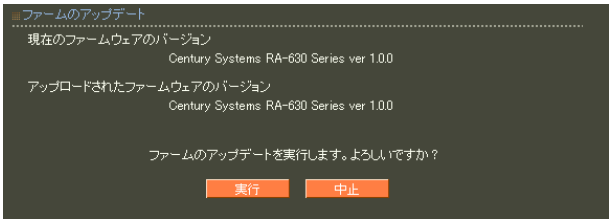
５．ファームのアップデート

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。

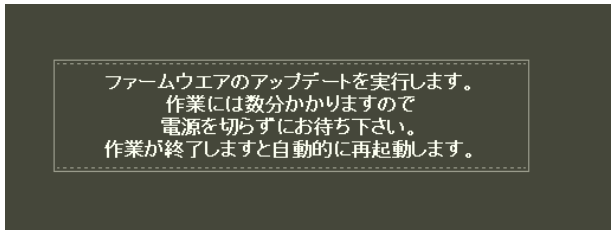
管理機能のメニュー「システム」から「ファームのアップデート」を選択します。

「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行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。

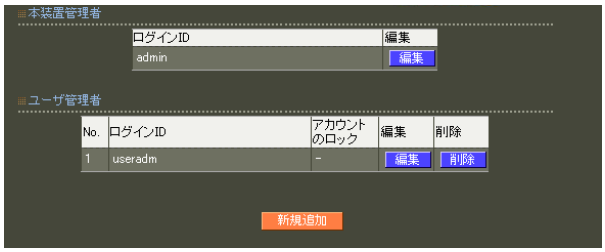
管理機能のメニュー「システム」から「再起動」を選択します。

「実行」ボタンをクリックすると、再起動します。

７．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。入力後「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。

○ユーザ管理者一覧
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。

○ユーザ管理者新規追加
「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。「アカウントのロック」は通常は「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。

ユーザ管理者は最大 5 人まで設定することができます。

ログイン ID に使用可能な文字は英数字および以下の記号になります。

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

パスワードに使用可能な文字は、ユーザ ID の入力可能文字に加え空白文字と以下になります。

```
,:;\
```

○ユーザ管理者変更・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。

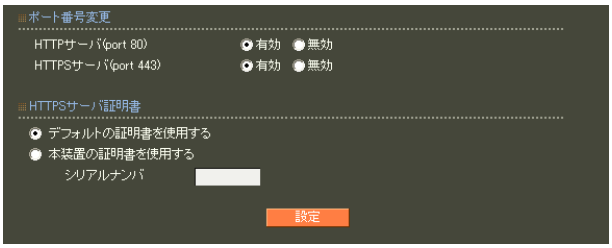
8．管理画面へのアクセス

本装置の管理画面へアクセスするために必要な設定を行います。

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。

画面中の「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」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
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を使用するか、「CA」で設定したサーバ証明書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。

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。

９．設定情報の同期

RA-630・RA-1100 は、元となる RA-630・RA-1100 に対して行った設定情報の変更を他の RA-630・RA-1100 に同期させることが出来ます。本機能による RA-630・RA-1100 間での通信は暗号化されます。

同期可能な設定情報・操作は次ページの表を参考にして下さい。

本機能により設定情報を共有する RA-630・RA-1100 間で設定可能な CA は一つのみです。

CA に関連する操作(証明書の発行、失効など)は基本的に MASTER で行います（※同期を行う本装置のうち、設定の元となる機器を MASTER、それ以外を SLAVE と呼びます)。MASTER が存在しない状態ではこれらの操作を行うことが出来ません。

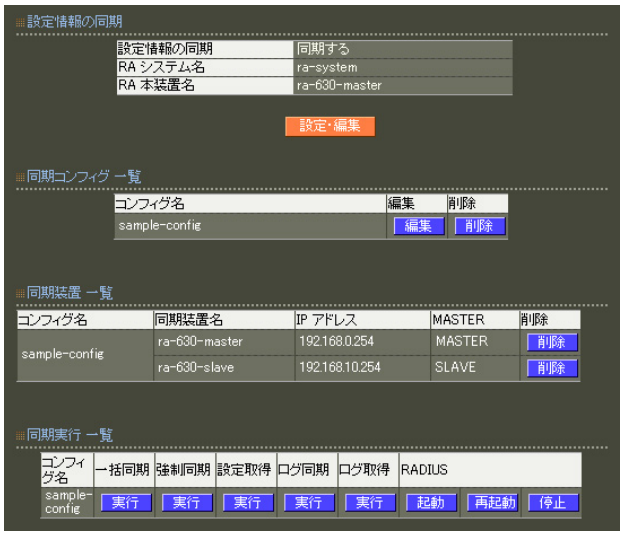
CA に関連しない操作（RADIUS ユーザの追加など）についても、基本的には MASTER で行います。しかし MASTER が存在しない状態、または、MASTER との通信が途切れていた場合でも、SLAVE で設定・変更など操作は可能です。ただし、その場合には、同期を行う RA-630・RA-1100 間での設定情報の同一性は保証されません。

同期処理			各設定項目
×	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
○			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
○			ユーザ(証明書の発行)
○			AD ユーザ
○			LDAP ユーザ
○			ファイル読み込み
○	CA	CA/CRL	新規作成
○			失効リストの更新
×			証明書の取得
×			失効リストの取得
○		証明書	発行
×			取得
×	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
×		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
×			管理者
×			管理画面へのアクセス
○	運用機能	ユーザ情報	ログイン情報

表．設定情報の同期機能により同期が行われる設定情報及び操作

「設定情報の同期」機能の設定を行います。

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
同期を行う RA-630・RA-1100 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
同期を行う RA-630・RA-1100 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。

○設定情報の同期機能の設定
「設定情報の同期」の「設定・編集」ボタンをクリックします。

・設定情報の同期
本機能を使用するか否かを選択します。
使用しない場合は「同期しない」を、使用する場合は「同期する」を選択して下さい。

・RA システム名
同期を行う RA-630・RA-1100 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
同期を行う RA-630・RA-1100 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。

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」の「新規追加」または「編集」ボタンをクリックします。

・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。

・設定情報の同期

作成する設定情報の同期を行うか否かを選択します。

「同期しない」「同期する」からひとつを選択します。

・処理タイミング

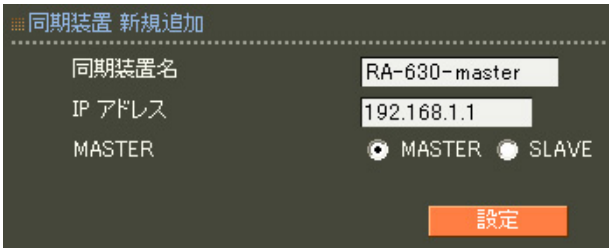
同期処理を行うタイミングを設定します。同期を設定操作ごとに行う場合は「即時実行」、同期を設定操作ごとに行わず、のちにまとめて行う場合は「一括処理」を選択します。

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。

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下さい。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下さい。

○同期装置の設定

「同期装置一覧」の「新規追加」ボタンをクリックします。



・同期装置名

同期を行う RA-630・RA-1100 の名前を設定します（最大 20 文字）。本装置の設定をする場合は、「設定情報の同期」で設定した「RA 本装置名」を設定して下さい。使用可能な文字は 0-9，a-z，A-Z，-(0x2c)，_(0x5f)です。

・IP アドレス

同期を行う RA-630・RA-1100 の IP アドレスを指定します（IPv4 形式）。

・MASTER

設定する RA-630・RA-1100 が、同期を行う RA-630・RA-1100 間で MASTER となるか SLAVE となるかを選択します。

「MASTER」「SLAVE」からひとつを選択します。

本装置と同期を行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。

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下さい。

○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・停止等が行えます。
本機能は、「設定情報の同期」を設定した 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。

・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 側で設定を行うと、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出来ます。
「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。
送信処理中は、両装置ともに認証処理を行う事ができません。

・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。
取得処理中は、両装置ともに認証処理を行う事ができません。

・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出来ます。
各ボタンをクリックして動作を実行して下さい。

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
同期が正常に行われているかは、「運用機能」メニュー「システム情報」の「システム情報」で確認して下さい。

第9章

運用機能

Ｉ．ユーザ情報

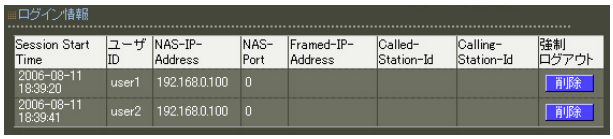
１．ログイン情報

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



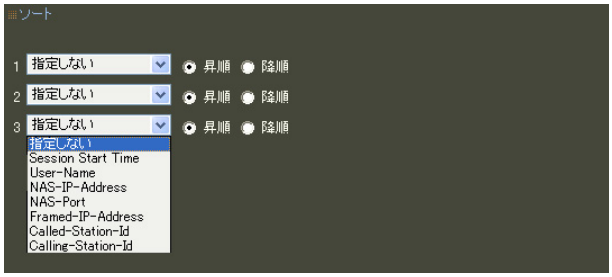
各項目はRADIUSクライアントからのアカウンティング要求の情報に基づいて表示されます。

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。
実際に接続を行っている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、一切の通知を行いません。

○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。



ソートの対象項目を選択します。

- 指定しない
- SessionStartTime
- User-Name
- NAS-IP-Address
- NAS-Port
- Framed-IP-Address
- Called-Station-Id
- Calling-Station-Id

ソートの順序を選択します。

- 昇順
- 降順

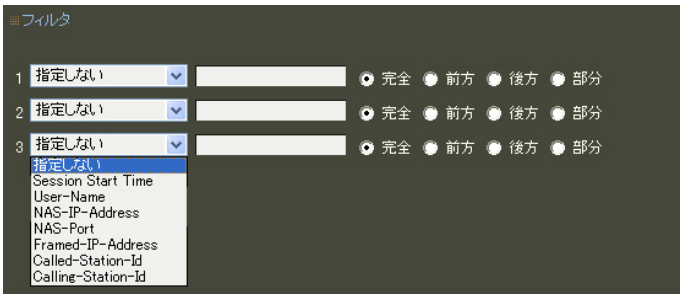
デフォルトは昇順です。

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
・User-Name
・NAS-IP-Address
・NAS-Port
・Framed-IP-Address
・Called-Station-Id
・Calling-Station-Id

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 （但し 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

○一括ログアウト機能
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。

設定情報の同期を行う設定の場合、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

RADIUS 設定で Active Directory を「使用する」に設定している場合に、ActiveDirectory に登録されたユーザの中で現在認証可能なユーザ名を表示します。

RADIUS サーバの Active Directory 設定でグループ情報が設定されている場合は、所属グループに属する認証可能なユーザ名をソートして表示します。

所属グループが設定されていない場合は、認証可能なユーザ名をソートして表示します。

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。

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。

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。

- “ System ”
  システムログであることを表します。
- 日付
- 時刻
- 分類
  “ RADIUS ”, “ NTP ” などのログの種別。
- ログ内容

Ⅱ．ログ情報

２．認証ログ

RADIUSサーバによる認証のログ情報を表示します。

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。
- 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
- 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。

○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。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。

Ⅱ．ログ情報

○表示出力先
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行うことができます。

３．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。

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。

・「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」の92ページ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。

○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。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。

○表示出力先
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行うことができます。

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。

・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 56 バイトです。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下さい。

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。

・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。

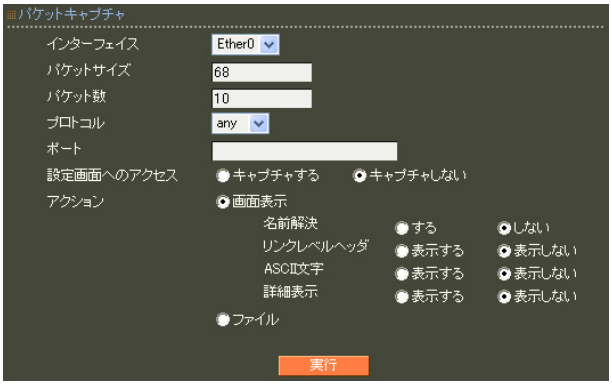
各項目を入力後「実行」ボタンを押すと結果が画面に表示されます。

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下さい。

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。指定したインターフェイスをモニタし、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。



・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ーフェイスを選択します。

・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 の場合はポートは指定できません。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。

出力結果を画面に表示する場合には、「画面表示」を選択します。

・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。

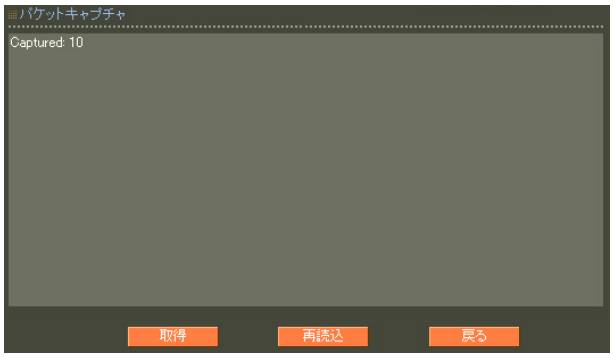
・ASCII 表示
16 進数表示に加え、ASCII 文字に変換した値も表示したい時には「表示する」を選択します。

・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。

III．ネットワークテスト

出力結果をファイルに保存したい場合には、「ファイル」を選択して「実行」ボタンを押します。



「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。

４．名前解決確認

ネットワークテストをおこないます。名前解決が正しく行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。

DNS の正引きを行いたい時には引き方で「正引き」を選択し、ホスト名(FQDN)を入力して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には引き方で「逆引き」を選択し、IP アドレスを入力して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

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。

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。

- **IP アドレス**
  各インターフェイスの IP アドレスや MAC アドレスなどです。

- **送受信カウンタ**
  各インターフェイスの通過パケット数等を表示します。

- **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。

- **二重化**
  二重化の状態を表示します。

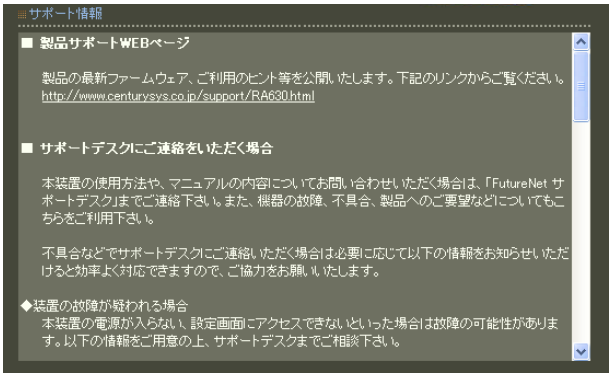
- **同期**
  設定情報の同期の状態を表示します。

再表示ボタンを押すと最新の情報に更新します。

Ⅴ. 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。



第 10 章

ユーザ管理者メニュー

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 の 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。

・管理機能の管理者メニュー
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。

・設定ウィザードの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。

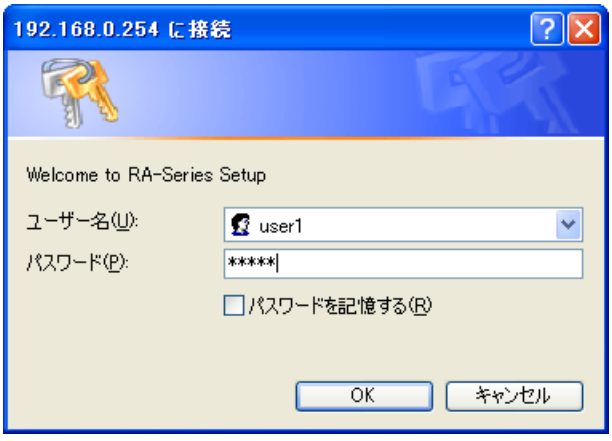
管理者としてログインする場合同様、ブラウザのアドレス欄に以下の URL を入力します。

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「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

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。

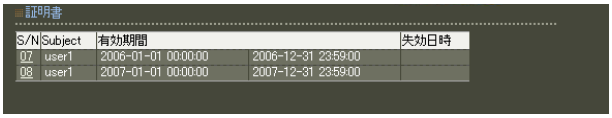
新しいパスワードを入力して「設定」ボタンを押すとパスワードが変更されます。次回のログインからは、新しく設定したパスワードを使ってログインしてください。

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。

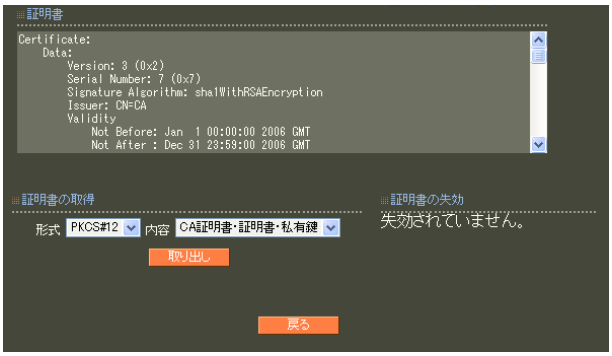
```
!"#$%&'()*+-./<=>?@[]^_`{|}~,:;\
```

III. 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。



「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。



上部の証明書欄には証明書の内容が表示されます。また右下の証明書の失効欄にはこの証明書が失効されているか否かが表示されます。

証明書の取得欄から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。形式は PKCS#12，PEM，DER から、一つ選択します。内容は、「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下さい。

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。

第 12 章

一般ユーザによる PC の設定

設定例

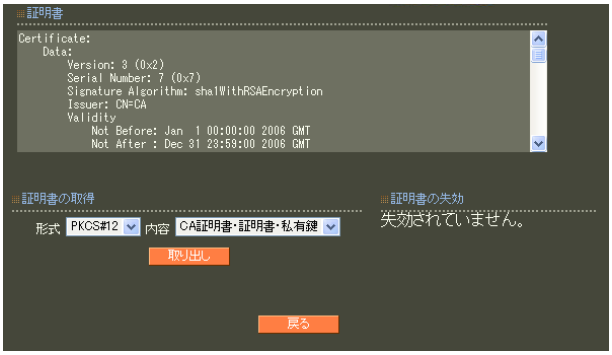
本装置を使って実際に認証処理をおこなう場合には、RADIUS クライアントである、NAS や無線 LAN アクセスポイントの設定および、認証を受ける PC の設定が必要になります。本章では EAP-TLS で認証をおこなう場合に必要な PC の設定について設定例を記述します。なお、実際の設定にあたっては各ハード、ソフトウェアに付属するマニュアルを参照してください。本設定例では、サプリカントとして WindowsXP に標準で含まれているサプリカントを使用します。

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。

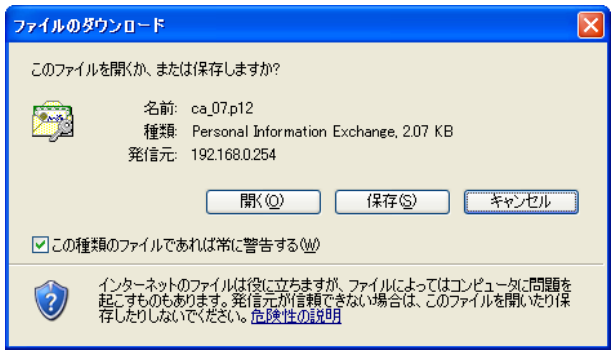
・与えられたユーザ ID とパスワードを用いて Web ブラウザから本装置にログインして、自分の証明書をダウンロードします。



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　ユーザーメニュー」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。

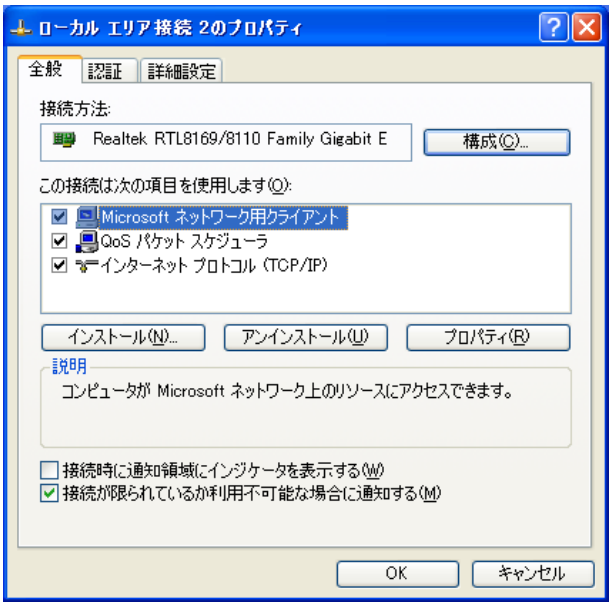
2 EAP-TLS の設定

EAP-TLS の設定をします。

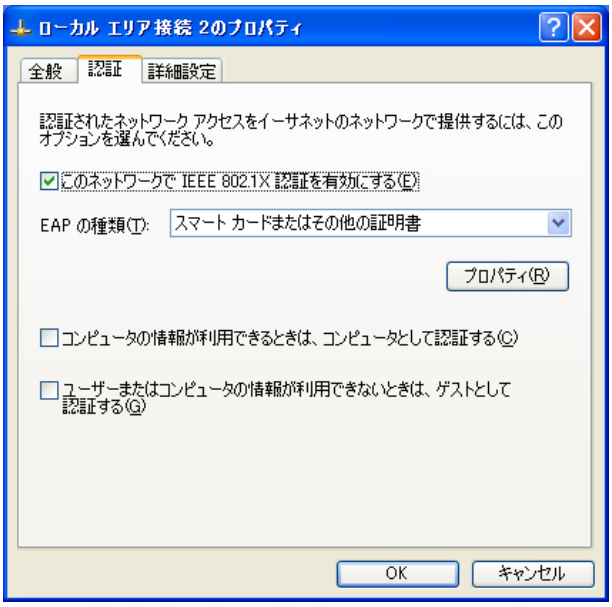
・コントロールパネルから「ネットワーク接続」をダブルクリックします。

・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。

設定例



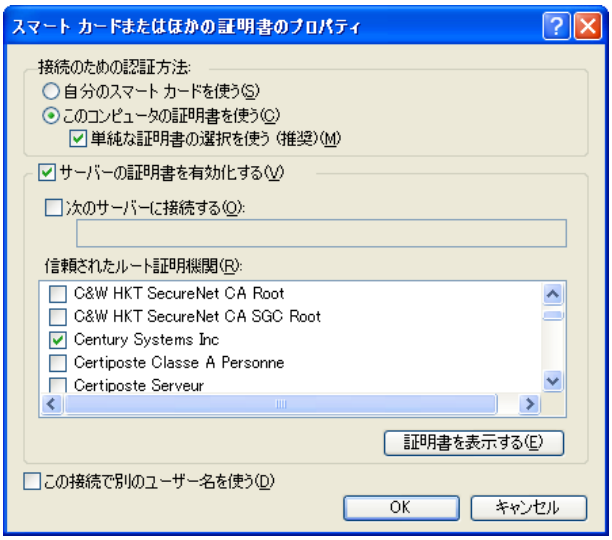
・認証タブを選択します。



・「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。



以上で設定が終わりです。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行われ、認証に成功すると通信がおこなえるようになります。

第 13 章

復旧操作

INIT ボタンの操作

RA-630 の背面、RA-1100 の前面にある「INIT ボタン」を使用して、**工場出荷設定に戻す**ことができます。

INITボタンを押したまま電源切断→電源投入し、電源投入後も 5 秒ほど INIT ボタンを押しつづけると、設定が消去され、工場出荷時設定に戻ります。

付録 A

最大数一覧

付録 A

最大数一覧

RA-630 と RA-1100 で最大数の異なる項目を下記の表に示します。

項目	RA-630	RA-1100
RADIUS - サーバ - アドレスプール	10	100
RADIUS - サーバ - クライアント	100	1,000
RADIUS - プロファイル - ユーザプロファイル	20	100
RADIUS - プロファイル - 基本プロファイル	20	100
RADIUS - ユーザ - ユーザ	2,000	50,000
CA - 証明書	2,000	10,000
アドレスプールあたりのアドレス数	2,000	2,000

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、下記へご連絡下さい。

・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　http://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下さい。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下さい。
・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下さい。
・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、是非ご覧下さい。

RA-630 製品サポートページ
　http://www.centurysys.co.jp/support/RA630.html
RA-1100 製品サポートページ
　http://www.centurysys.co.jp/support/RA1100.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下さい。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。

サンプル設定ファイル

```
[RADIUS| プロファイル | 基本]
create basic
profile_name=base01
auth_type=2
simul_conn_count=
ipaddress_allocate=0
addrpool=

[RADIUS| プロファイル | ユーザプロファイル]
create userprofile
profile_name=prof01
base=base01
auth=
cert=
resp=
group=

[RADIUS| ユーザ]
create user
user_id=user01
password=pass01
profile=prof01
ipaddress=
netmask=

create user
user_id=user02
password=pass02
profile=prof01
ipaddress=
netmask=
```

このサンプル設定ファイルでは、ユーザ基本情報プロファイル “ base01 ” とユーザプロファイル “ prof01 ”を作った上で、 “ prof01 ”をプロファイルに指定したユーザ “ user01 ”および “ user02 ”を作成する例になります。

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)

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 | 証明書発行]
　ユーザ証明書の設定

作成するデータが無いセクションについてはセクションのタイトルを記述する必要はありません。また、同じセクションで複数のデータを作成したい時には、先ほどのサンプルの“ user01 ”および“ user02 ”の様にセクションタイトルの下に空白行で区切った複数の作成データを書くようにします。ファイルの最後は改行コードで終わっている必要があります。

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。

○[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
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。

prfole_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
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。

prfole_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
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。

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
profile_name=resp01
```

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。

prfole_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
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。

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
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。

profile_name	プロファイル名
group_id	グループ ID

○[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
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=
```

ユーザ設定情報のファイルフォーマット

```
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。

profile_name	プロファイル名
version	バージョン: 1 または 3
key_length	鍵長:2048, 1024, 512
sign_algorithm	Signature Algorithm: SHA-1 または MD5
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

○[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
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。

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

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]
ユーザについて記述します。

設定例

```
[RADIUS| ユーザ]
create user
user_id=user01
password=pass01
profile=prof01
ipaddress=
netmask=
locked=on|off
```

※ locked ロック (on または off. 空文字列は off と同義)

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。

user_id	ユーザ ID
password	パスワード
profile	プロファイル名
ipaddress	IP アドレス
netmask	ネットマスク

○[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
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	個別設定を行うユーザ名。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。
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
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。

付録 C

ユーザ設定情報のファイルフォーマット

user	個別設定を行うユーザ名。 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。
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 remove 削除

○[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
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	個別設定を行うユーザ名。 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。
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
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...
...
...UB4OrpxTVdU7TdMsrzALK6+WxaLrWi
-----END CERTIFICATE REQUEST-----
--_____FILE--
```

付録 C

ユーザ設定情報のファイルフォーマット

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 ID
passphrase	パスフレーズ
version	バージョン: 1 または 3
key_length	鍵長:2048, 1024, 512
sign_algorithm	Signature Algorithm: SHA-1 または MD5
subject_email	email
subject_cn	Common Name: ユーザ ID を指定してください。(グループ ID がユーザに定義されている場合には、グループ ID 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。

証明書を発行するユーザに証明書プロファイルが指定されている場合には、証明書発行セクションでの指定を省略することができます。証明書発行セクションで空欄にした項目に対して、証明書プロファイル側でデータが定義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。

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 認証を行う認証方式。

[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行う認証方式。

[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。

[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。

[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。

付録 D

用語説明

[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行います。

[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。

[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 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。

[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。

付録 D

用語説明

[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。

[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。

[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。

付録 D

用語説明

[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。

[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 があります。

[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-630・RA-1100)の全ての設定を行う権限をもつ RA-630・RA-1100 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。

付録 D

用語説明

[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、失効のみを行う権限をもつ RA-630・RA-1100 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

RA-630 RA-1100 ユーザーズガイド ver1.7.0
2007 年 08 月版
発行 センチュリー・システムズ株式会社