

---

EAP 対応 RADIUS サーバアプライアンス

# **FutureNet RA シリーズ**

設定例集

Ver 1.9.0

センチュリー・システムズ 株式会社

---

## はじめに

本書はRA シリーズをお使いいただくために、いくつかの具体的な設定例を示して解説しています。本書では、それぞれの構成に於いて、設定が必要な項目のみ記述しています。その他の項目についてはデフォルト値のままで使用可能です。

本書で紹介している設定例は動作を保証するものではありません。設定例通りに設定を行ってもお使いの環境によっては、正しく動作しない場合があります。

本マニュアルは、ファームウェア Ver1.9.0 に対応しております。それ以前のファームウェアでは、画面や設定内容が異なる場合がございますので、Ver1.8.13 以前の設定例集をご利用ください。

## 商標の表示

- 「FutureNet」はセンチュリー・システムズ株式会社の登録商標です。
- 下記製品名等は米国 Microsoft Corporation の登録商標です。  
Microsoft、Windows、Windows 95、Windows 98、Windows 2000、Windows Me、Windows XP、Windows Vista、Windows7、Windows8、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。

## - 目次 -

1.	各種認証方式を利用する.....	4
1.1.	PAP/CHAP 認証を利用する (フレッツ網の認証サーバとして利用する) .....	4
1.2.	PAP/CHAP 認証を利用する (MAC アドレスの認証サーバとして利用する) .....	8
1.3.	EAP-TTLS 認証を利用する .....	12
1.4.	EAP-PEAP 認証を利用する .....	19
1.5.	EAP-TLS 認証を利用する .....	26
1.6.	EAP-MD5 認証を利用する .....	34
2.	冗長化機能を利用する .....	38
2.1.	設定情報の同期機能を利用する .....	38
2.2.	二重化機能を利用する .....	41
2.3.	親子連携機能を利用する .....	43
3.	連携機能を利用する .....	60
3.1.	ActiveDirectory 連携機能を利用する .....	60
3.2.	LDAP 連携を利用する .....	67
3.3.	LDAP 連携で EAP-PEAP 認証を利用する .....	77
3.4.	ActiveDirectory を LDAP として利用する .....	84
3.5.	LDAP サーバから応答アトリビュートを取得する .....	92
4.	ファイル読み込み機能を利用する.....	99
4.1.	既存プロファイルに新規でユーザを追加する .....	99
4.2.	新規でユーザプロファイルとユーザを登録する .....	101
4.3.	証明書を発行する .....	104
5.	認証プロファイル/応答プロファイルを利用する.....	111
5.1.	フレッツナンバーアシストを利用する .....	111
5.2.	認証スイッチ毎に接続可能なユーザを限定する .....	114
5.3.	ユーザ毎に VLAN ID を設定する .....	118
6.	I P アドレスの払い出しを設定する.....	125
6.1.	アドレスプール機能を利用する .....	125
6.2.	ユーザ毎に固定 I P アドレスを設定する .....	127
7.	ユーザの個別設定機能を利用する.....	129
7.1.	ユーザ毎に VLAN ID を設定する .....	129
7.2.	無線アクセスポイント (SSID) 毎に接続可能なユーザを限定する.....	133
8.	RADIUS Proxy 機能を利用する .....	136
8.1.	全ての認証要求を転送する設定を行う .....	136
8.2.	特定のレルムに属するユーザをローカルで認証する設定を行う.....	147

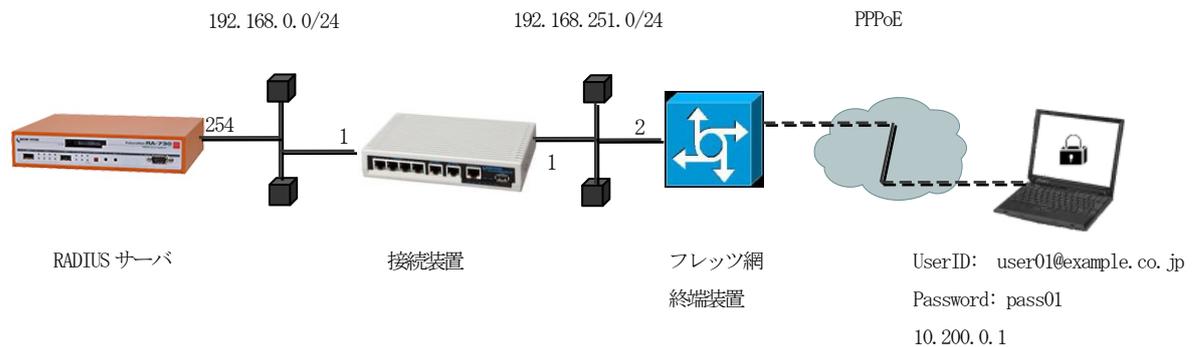
## 1. 各種認証方式を利用する

### 1.1. PAP/CHAP 認証を利用する（フレッツ網の認証サーバとして利用する）

#### ■ 概要

ここではNTT 地域会社により提供されている、フレッツ・オフィス/フレッツ・オフィスワイドサービス環境の認証サーバとして使用する例を紹介します。

#### ■ 構成



フレッツ環境における認証サーバとして使用するには以下の設定を行います。

- ・認証方式や使用ポートなどの基本設定
- ・RADIUS クライアント（網終端装置）の登録
- ・応答アトリビュートの登録
- ・ユーザの登録
- ・網終端装置へのルート設定

#### ■ 設定例

ここでは下記の内容で設定を行います。

設定条件：

ユーザ ID	user01
パスワード	pass01
グループ ID	example.co.jp
認証方式	PAP/CHAP
認証/アカウントングポート	1812/1813
IP アドレス割り当て	10.200.0.1（固定）
網への接続装置 IP アドレス	192.168.0.1
網終端装置の IP アドレス	192.168.251.2
網終端装置のシークレット	secret

## ネットワークの設定 (管理機能/ネットワーク/基本設定)

RA と網終端装置間の通信を行うためにルートを設定します。ここではデフォルトゲートウェイとして網への接続装置を指定します。インターフェイスの IP アドレスを **192.168.0.254/24**、デフォルトゲートウェイを **192.168.0.1** に設定します。

基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
デフォルトゲートウェイ		192.168.0.1	<input type="button" value="編集"/>

## 認証方式の設定 (RADIUS/サーバ/基本設定)

基本情報画面を開き以下設定を行います。

- ・ 認証/アカウントングに使用するポート番号を選択します。
- ・ 認証方式として **PAP/CHAP** を選択します。

ポート番号	RADIUSサーバ証明書
<input type="radio"/> 1645/1646 <input checked="" type="radio"/> 1812/1813 <input type="radio"/> 1645/1646と1812/1813 <input type="radio"/> 手動設定	<input checked="" type="radio"/> 使用しない <input type="radio"/> 本装置の証明書を使用する
認証用 <input type="text"/> アカウントング用 <input type="text"/>	シリアルナンバー <input type="text"/>
<b>認証方式</b> <input checked="" type="checkbox"/> PAP/CHAP <input type="checkbox"/> EAP-MD5 <input type="checkbox"/> EAP-TLS <input type="checkbox"/> EAP-PEAP <input type="checkbox"/> EAP-TTLS	
<input type="button" value="設定"/>	

## RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

網終端装置を RADIUS クライアントとして登録します。

IP アドレスは、網終端装置の IP アドレス、シークレットは網終端装置と共通のものを設定します。

クライアント新規追加	
クライアント名	<input type="text" value="client"/>
IPアドレス	<input type="text" value="192.168.251.2"/>
シークレット	<input type="text" value="secret"/>
アドレスグループ	<input type="text" value="指定しない"/>

ユーザはプロフィールという概念により、設定単位にグループ化を行うことができます。このプロフィールにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロフィール、ユーザプロフィールの作成が必要です。

#### ユーザ基本プロフィールの登録 (RADIUS/プロフィール/ユーザ基本情報)

ユーザを作成するにはユーザ基本情報プロフィールを作成します。  
設定条件に従い認証方式に **PAP/CHAP**、IP アドレス割り当てを **固定** に設定します。  
プロフィール名は **base\_user** とします。

ユーザ基本情報プロフィール 新規追加

プロフィール名: base\_user

認証方式: PAP/CHAP

同時接続数:

IPアドレス割り当て:  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール: 指定しない

設定

#### 応答アトリビュートプロフィールの登録 (RADIUS/プロフィール/応答アトリビュート)

ここでフレッツ網に返すための応答アトリビュートを登録します。まず画面上段の **新規追加** を押下して応答アトリビュートプロフィールを作成します。ここではファイル名を **reply** として作成します。続いて下段の表中の **新規追加** を押下してアトリビュートを追加します。応答アトリビュート新規追加画面では Service-Type, Framed-Protocol の各アトリビュートを追加します。アトリビュート **Service-Type** の値は **2**、**Framed-Protocol** の値は **1** を設定します。

応答アトリビュートプロフィール 一覧

プロフィール名	削除
reply	削除

新規追加

応答アトリビュート 一覧

プロフィール名	アトリビュート	値	編集	削除
reply	Service-Type	2	編集	削除
	Framed-Protocol	1	編集	削除

新規追加

#### グループ ID の設定 (RADIUS/プロフィール/グループ ID)

グループ ID として **example.co.jp** を設定します。プロフィール名は **group** とします。

グループIDプロフィール 新規追加

プロフィール名: group

グループID: example.co.jp

形式:  UserID@GroupID  GroupID#UserID

設定

### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

作成したユーザ基本情報プロフィール **base\_user** とグループプロフィール **group** を選択してユーザプロフィールを作成します。プロフィール名は **user** とします。

ユーザプロフィール 新規追加

プロフィール名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	reply
グループ	group

設定

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **user01**、パスワードに **pass01** を入力します。プロフィールは先ほど作成したユーザプロフィール **user** を指定します。固定 IP 払い出しの IP アドレスは **10.200.0.1**、ネットマスクに **255.255.255.0** を入力します。内容入力後 **設定** ボタンを押下してユーザを作成します。

ユーザ 変更

ユーザID	user01
パスワード	●●●●●●
プロフィール	user

固定IPアドレス払い出し

IPアドレス	10.200.0.1
ネットマスク	255.255.255.0

備考

備考

アカウントのロック

ロック  ロックしない  ロックする

設定

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

起動・停止

現在の状態

停止中

起動

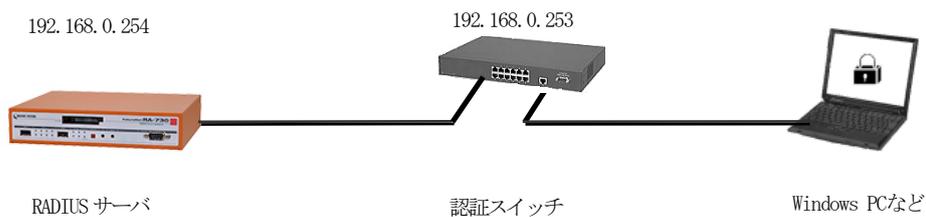
以上で設定は終了です。

## 1.2. PAP/CHAP 認証を利用する (MACアドレスの認証サーバとして利用する)

## ■ 概要

ここでは、認証方式はPAP/CHAPを使用し、MACアドレス認証に対応したスイッチ(以下認証スイッチ)の認証サーバとして使用する例を紹介します。

## ■ 構成



## ■ 設定例

設定条件：

RADIUS サーバの IP アドレス	192.168.0.254 (Ether0)
認証スイッチの IP アドレス	192.168.0.253
認証スイッチのシークレット	secret
ユーザ ID	00806d000000 ※1
パスワード	macpass ※2
認証方式	PAP/CHAP
認証/アカウントングポート	1812/1813

## ※1 MAC アドレス

認証スイッチより送信される MAC アドレスの形式で設定ください。

## ※2 認証スイッチで指定したパスワード

RA シリーズは、ユーザ ID とパスワードを指定する必要があります。

(パスワードを未指定とする事はできません)

認証スイッチでは、認証サーバの IP アドレス、RADIUS サーバに設定する共通のシークレット、その他 MAC アドレス認証に必要となる設定を行います。

ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS や NTP サーバを使用しないのであれば特に設定する必要はありません。

基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
デフォルトゲートウェイ			<input type="button" value="編集"/>

認証方式の設定 (RADIUS/サーバ/基本設定)

基本情報画面を開き以下設定を行います。

- ・ 認証/アカウントingに使用するポート番号を選択します。
- ・ 認証方式として **PAP/CHAP** を選択します。

ポート番号

1645/1646  
 1812/1813  
 1645/1646と1812/1813  
 手動設定

認証用

アカウントing用

RADIUSサーバ証明書

使用しない  
 本装置の証明書を使用する

シリアルナンバ

認証方式

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

RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして認証スイッチの情報を設定します。

クライアント新規追加画面の全ての項目を設定します。

IP アドレスは認証スイッチの IP アドレス、シークレットは認証スイッチに設定したものと同一ものを設定します。

クライアント新規追加

クライアント名

IPアドレス

シークレット

アドレスグループ

ユーザはプロフィールという概念により、設定単位にグループ化を行うことができます。このプロフィールにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロフィール、ユーザプロフィールの作成が必要です。

#### ユーザ基本情報プロフィールの作成 (RADIUS/プロフィール/ユーザ基本情報)

ユーザを作成するにはユーザ基本情報プロフィールを作成します。  
設定条件に従い 認証方式に **PAP/CHAP** に設定します。  
プロフィール名は **base\_user** とします。

ユーザ基本情報プロフィール 新規追加

プロフィール名	base_user
認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	<input checked="" type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input type="radio"/> アドレスプール <input type="radio"/> 固定
アドレスプール	指定しない

設定

#### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

作成したユーザ基本情報プロフィール **base\_user** を指定してユーザプロフィール **user** を作成します。

ユーザプロフィール 新規追加

プロフィール名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	指定しない

設定

ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **00806d000000**、パスワードに **macpass** を入力します。  
プロファイルは先ほど作成したユーザプロファイルを指定します。  
以上を設定して **設定** ボタンを押下してユーザを追加します。

The screenshot shows a configuration interface for adding a new user. It is divided into several sections:

- ユーザ 新規追加**:
  - ユーザID: 00806d000000
  - パスワード: 7 dots
  - プロファイル: user (dropdown menu)
- 固定IPアドレス払い出し**:
  - IPアドレス: [empty field]
  - ネットマスク: [empty field]
- 備考**:
  - 備考: [empty text area]
- アカウントのロック**:
  - ロック:  ロックしない  ロックする

A **設定** button is located at the bottom center of the form.

RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

The screenshot shows the status configuration for the RADIUS server. It includes:

- 起動・停止**:
  - 現在の状態: 停止中

A **起動** button is located at the bottom center of the form.

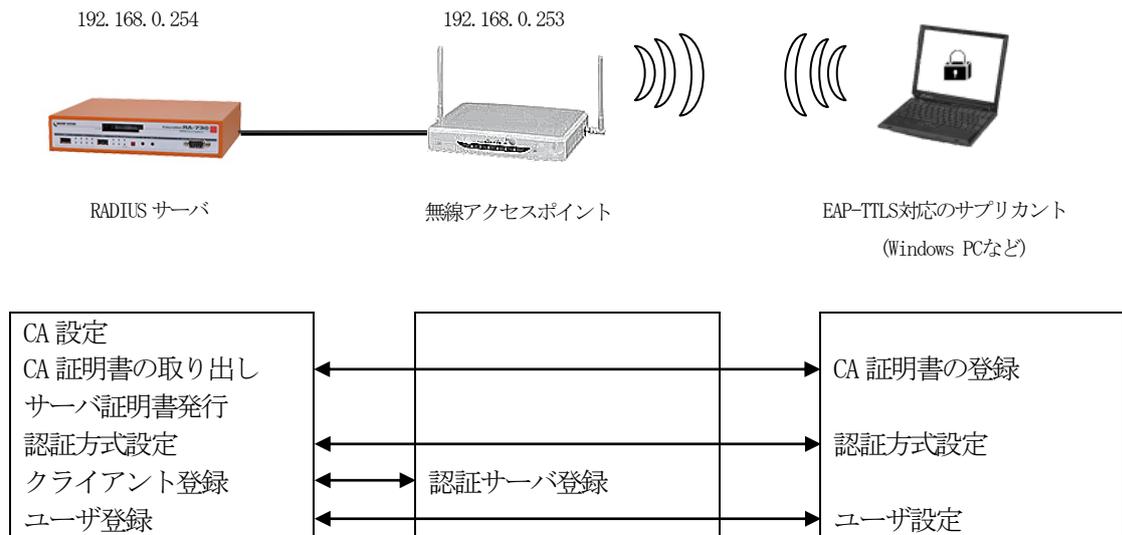
以上で設定は終了です。

### 1.3. EAP-TTLS 認証を利用する

#### ■ 概要

ここでは、認証方式は EAP-TTLS を使用し、802.1X に対応した無線アクセスポイントの認証サーバとして使用する例を紹介します。

#### ■ 構成



無線アクセスポイント接続の認証に EAP-TTLS 認証を使用するには以下の設定を行います。

- CA の設定
- RADIUS サーバ用のサーバ証明書の発行
- 認証方式や使用ポートなどの基本設定
- RADIUS クライアント（無線アクセスポイント）の登録
- ユーザの登録

※無線アクセスポイントでは、認証サーバの IP アドレスと RADIUS サーバに設定する共通のシークレットを指定します。  
 またサブクライアントでは、ユーザ ID/パスワードの設定の他、RADIUS サーバで発行した CA 証明書の登録を行います。

## ■ 設定例

ここでは下記の内容で設定を行います。設定ウィザードを使って設定する場合は、「RADIUS (EAP)」を選択します。

設定条件：

RADIUS サーバの IP アドレス	192.168.0.254 (Ether0)
無線アクセスポイントの IP アドレス	192.168.0.253
無線アクセスポイントのシークレット	secret
ユーザ ID	user01
パスワード	pass01
認証方式	EAP-TTLS/CHAP
認証/アカウンティングポート	1812/1813

### ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS や NTP サーバを使用しないのであれば特に設定する必要はありません。



基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	編集
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	
	MTU	1500	編集
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	
	MTU	1500	編集
	通信モード	Auto	
デフォルトゲートウェイ			編集

### CA の設定 (CA/CA/CRL)

EAP-TTLS 認証を使用する場合は CA の設定が必要になります。

CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているかご確認ください。

CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要です。

ここでは以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample

失効リスト更新間隔

365

※CAの再編集はできませんので設定の際は内容を十分確認してください。  
また、CAを削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name sample\_ca

email samp@example.co.jp

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035 年 12 月 31 日

パスフレーズ

パスフレーズ

失効リスト更新間隔

失効リスト更新間隔 365

設定

CA作成後はCA証明書画面より **取り出し** ボタンを押下してCA証明書を取得し、サブリカントへインストールします。

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

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 KeyUsage** を指定するようにします。

但し、実際にどの **Key Usage/Extended Key Usage** を必要とするかは通信相手のソフトウェアに依存します。

- **Key Usage** : digitalSignature および keyEncipherment
- **Extended Key Usage** : serverAuth

証明書

バージョン 3  
鍵長 1024  
Signature Algorithm SHA-256

Subject  
Common Name RA\_Server  
email  
Organizational Unit  
Organization  
Locality  
State or Province  
Country JP

有効期間  
開始日時 年 月 日 時 分  
終了日時 2025 年 12 月 31 日 14 時 59 分

パスフレーズ  
パスフレーズ

X.509証明書v3拡張 (RFC3280)

Key Usage  
 digitalSignature  
 keyEncipherment  
 keyAgreement  
 cRLSign  
 decipherOnly  
 nonRepudiation  
 dataEncipherment  
 keyCertSign  
 encipherOnly

Extended Key Usage serverAuth

CRL Distribution Points

Netscape拡張

nsCertType  
 client  
 email  
 sslCA  
 objCA  
 server  
 objsign  
 emailCA

nsComment

設定

### 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**, **EAP-TTLS** , 内部認証で使用するプロトコルを選択します。

RADIUS サーバ証明書は**本装置の証明書を使用する**を選択し、シリアルナンバーで前項にて発行した RADIUS サーバ証明書を指定します。

なおポート番号は、RADIUS クライアント(無線アクセスポイント)の設定と同一になるよう指定します。

ポート番号

1645/1646  
 1812/1813  
 1645/1646と1812/1813  
 手動設定

認証用   
アカウント用

RADIUSサーバ証明書

使用しない  
 本装置の証明書を使用する

シリアルナンバー

認証方式

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

設定

※EAP-TTLS を使用するにはEAP-TLS も選択されている必要があります。

### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの情報を設定します。

クライアント新規追加画面の全ての項目を設定します。

IP アドレスは、無線アクセスポイントの IP アドレス、シークレットは無線アクセスポイントに設定したものと同一ものを設定します。

クライアント新規追加

クライアント名   
IPアドレス   
シークレット   
アドレスグループ

設定

ユーザはプロフィールという概念により、設定単位にグループ化を行うことができます。このプロフィールにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロフィール、ユーザプロフィールの作成が必要です。

#### ユーザ基本情報プロフィールの作成 (RADIUS/プロフィール/ユーザ基本情報)

設定条件に従い 認証方式に **EAP-TTLS/PAP, CHAP** を設定します。プロフィール名は **base\_user** とします。

ユーザ基本情報プロフィール 新規追加

プロフィール名	base_user
認証方式	EAP-TTLS/PAP, CHAP
同時接続数	
IPアドレス割り当て	<input checked="" type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input type="radio"/> アドレスプール <input type="radio"/> 固定
アドレスプール	指定しない

設定

#### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

これまでに作成したユーザ基本プロフィール **base\_user** を指定してユーザプロフィール **user** を作成します。

ユーザプロフィール 新規追加

プロフィール名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	指定しない

設定

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **user01**、パスワードに **pass01** を入力します。  
プロファイルは先ほど作成したユーザプロファイルを指定します。

ユーザ 新規追加

ユーザID user01

パスワード pass01

プロファイル user

固定IPアドレス払い出し

IPアドレス

ネットマスク

備考

備考

アカウントのロック

ロック  ロックしない  ロックする

設定

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

起動・停止

現在の状態 停止中

起動

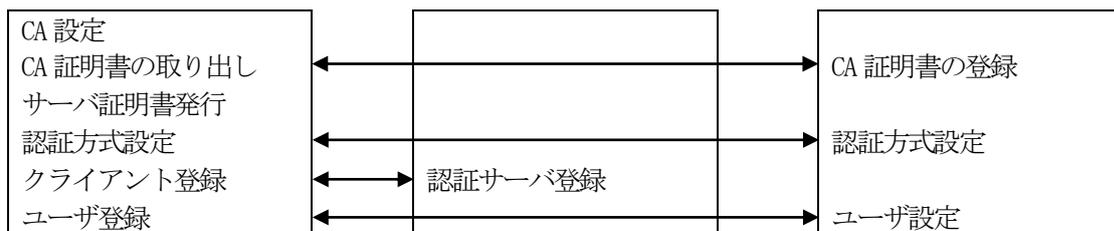
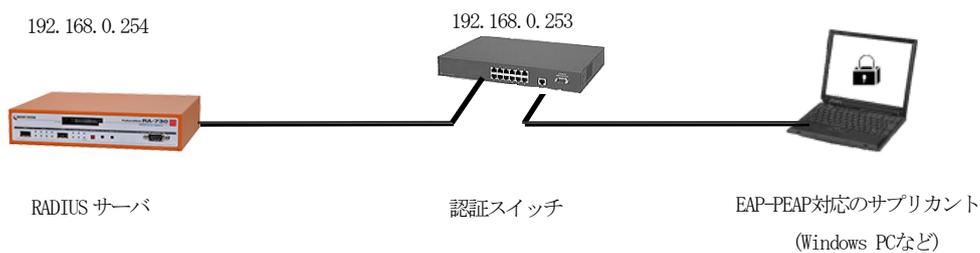
以上で設定は終了です。

## 1. 4. EAP-PEAP 認証を利用する

## ■ 概要

ここでは、認証方式は EAP-PEAP を使用し、802.1X に対応したスイッチ(以下認証スイッチ)の認証サーバとして使用する例を紹介します。

## ■ 構成



認証スイッチを使って EAP-PEAP 認証を使用するには以下の設定を行います。

- CA の設定
- RADIUS サーバ用のサーバ証明書の発行
- 認証方式や使用ポートなどの基本設定
- RADIUS クライアント (認証スイッチ) の登録
- ユーザの登録

※認証スイッチでは、認証サーバの IP アドレスと RADIUS サーバに設定する共通のシークレットを指定します。

またサブリクライアントでは、ユーザ ID/パスワードの設定の他、RADIUS サーバで発行した CA 証明書の登録を行います。

## ■ 設定例

ここでは下記の内容で設定を行います。設定ウィザードを使って設定する場合は「RADIUS (EAP)」を選択します。

設定条件：

RADIUS サーバの IP アドレス	192.168.0.254 (Ether0)
認証スイッチの IP アドレス	192.168.0.253
認証スイッチのシークレット	secret
ユーザ ID	user01
パスワード	pass01
認証方式	EAP-PEAP
認証/アカウンティングポート	1812/1813

### ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS や NTP サーバを使用しないのであれば特に設定する必要はありません。

基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	編集
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	
	MTU	1500	編集
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	
	MTU	1500	編集
	通信モード	Auto	
デフォルトゲートウェイ			編集

### CA の設定 (CA/CA/CRL)

EAP-PEAP 認証を使用する場合は CA の設定が必要になります。

CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているかご確認ください。

CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要で、

ここでは以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
Email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※CA の再編集はできませんので設定の際は内容を十分確認してください。  
また、CA を削除した場合は発行済みの全ての証明書も削除されます。

The screenshot shows a configuration window for a Certificate Authority (CA). The fields are as follows:

- バージョン**: 3
- 鍵長**: 1024
- Signature Algorithm**: SHA-256
- Subject**
  - Common Name**: sample\_ca
  - email**: samp@example.co.jp
  - Organizational Unit**: (empty)
  - Organization**: (empty)
  - Locality**: (empty)
  - State or Province**: (empty)
  - Country**: JP
- 有効期間**
  - 終了日時**: 2035 年 12 月 31 日
- パスフレーズ**
  - パスフレーズ**: (masked with 10 dots)
- 失効リスト更新間隔**
  - 失効リスト更新間隔**: 365

An orange button labeled **設定** (Settings) is located at the bottom right of the form.

CA 作成後は、CA 証明書画面より **取り出し** ボタンを押下して CA 証明書を取得し、サブリカントへインストールします。

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

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 KeyUsage** を指定するようにします。

但し、実際にどの **Key Usage/Extended Key Usage** を必要とするかは通信相手のソフトウェアに依存します。

- **Key Usage** : digitalSignature および keyEncipherment
- **Extended Key Usage** : serverAuth

The screenshot shows the configuration page for a certificate. The '証明書' (Certificate) section includes fields for Version (3), Key Length (1024), Signature Algorithm (SHA-256), and Subject information (Common Name: RA\_Server, Country: JP). The validity period is set to start at 00:00 and end at 2025-12-31 14:59. The 'X.509証明書v3拡張 (RFC3280)' section has 'Key Usage' with 'digitalSignature' and 'keyEncipherment' checked, and 'Extended Key Usage' set to 'serverAuth'. The 'Netscape拡張' section has 'nsCertType' with 'server' checked. A '設定' (Settings) button is at the bottom.

### 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**、**EAP-PEAP**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。EAP-PEAP を使用するには EAP-TLS も選択する必要があります。

シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバは CA の証明書一覧で確認することができます。また、設定ウィザードを使った場合は自動的に入力されます。なおポート番号は、RADIUS クライアント (認証スイッチ) の設定と同一になるよう指定します。

The screenshot shows a configuration interface for RADIUS server certificates. It is divided into three main sections:

- ポート番号 (Port Number):** Radio buttons for 1645/1646, 1812/1813, 1645/1646と1812/1813, and 手動設定 (Manual Setting). Below are input fields for 認証用 (Authentication) and アカウンティング用 (Accounting).
- RADIUSサーバ証明書 (RADIUS Server Certificate):** Radio buttons for 使用しない (Do not use) and 本装置の証明書を使用する (Use device certificate). A text field for シリアルナンバ (Serial Number) contains '01'.
- 認証方式 (Authentication Method):** Checkboxes for PAP/CHAP, EAP-MD5, EAP-TLS (checked), EAP-PEAP (checked), and EAP-TTLS.

An orange 設定 (Settings) button is located at the bottom right.

### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして認証スイッチの情報を設定します。

クライアント新規追加画面の全ての項目を設定します。

IP アドレスは認証スイッチの IP アドレス、シークレットは認証スイッチに設定したものと同一ものを設定します。

The screenshot shows the 'クライアント新規追加' (Add New Client) configuration screen. It contains the following fields:

- クライアント名 (Client Name): SW-01
- IPアドレス (IP Address): 192.168.0.253
- シークレット (Secret): secret
- アドレスプール (Address Pool): 指定しない (None) (dropdown menu)

An orange 設定 (Settings) button is located at the bottom right.

ユーザはプロフィールという概念により、設定単位にグループ化を行うことができます。このプロフィールにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロフィール、ユーザプロフィールの作成が必要です。

#### ユーザ基本情報プロフィールの作成 (RADIUS/プロフィール/ユーザ基本情報)

設定条件に従い認証方式に **EAP-PEAP** を設定します。プロフィール名は **base\_user** とします。



ユーザ基本情報プロフィール 新規追加

プロフィール名	base_user
認証方式	EAP-PEAP
同時接続数	
IPアドレス割り当て	<input checked="" type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input type="radio"/> アドレスプール <input type="radio"/> 固定
アドレスプール	指定しない

設定

#### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

作成したユーザ基本プロフィール **base\_user** を指定してユーザプロフィール **user** を作成します。



ユーザプロフィール 新規追加

プロフィール名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	指定しない

設定

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **user01**、パスワードに **pass01** を入力します。  
プロファイルは先ほど作成したユーザプロファイルを指定します。  
以上を設定して **設定** ボタンを押下します。

ユーザ 新規追加

ユーザID user01

パスワード ●●●●●●

プロファイル user

固定IPアドレス払い出し

IPアドレス

ネットマスク

備考

備考

アカウントのロック

ロック  ロックしない  ロックする

設定

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

起動・停止

現在の状態 停止中

起動

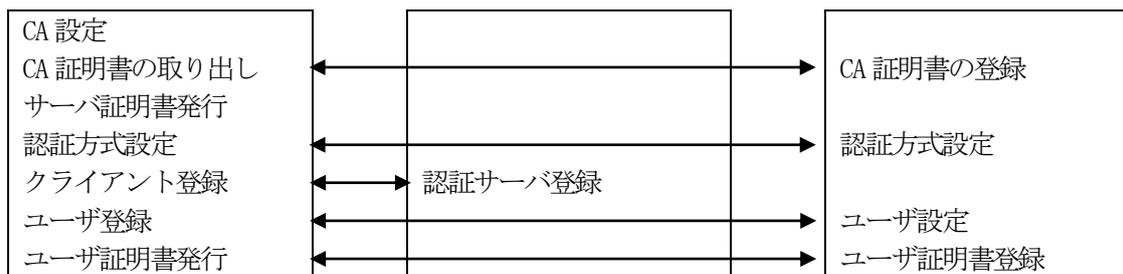
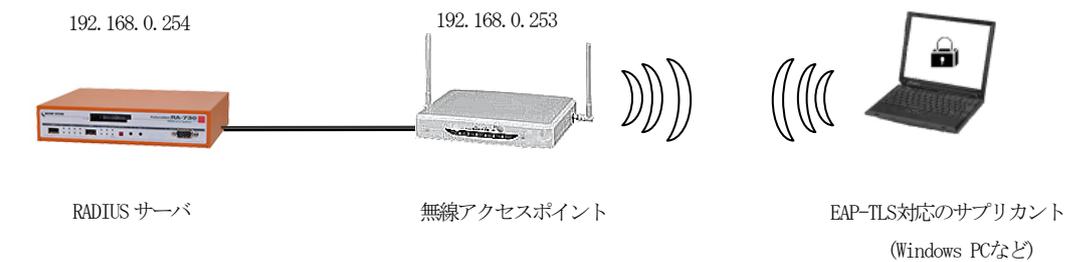
以上で設定は終了です。

## 1.5. EAP-TLS 認証を利用する

### ■ 概要

ここでは、認証方式はEAP-TLSを使用し、802.1Xに対応した無線アクセスポイントの認証サーバとして使用する例を紹介します。

### ■ 構成



無線アクセスポイント接続の認証に EAP-TLS 認証を使用するには以下の設定を行います。

- CA の設定
- RADIUS サーバ用のサーバ証明書の発行
- 認証方式や使用ポートなどの基本設定
- RADIUS クライアント（無線アクセスポイント）の登録
- ユーザの登録
- EAP-TLS 認証用にユーザ証明書の発行

※無線アクセスポイントでは、RADIUS サーバの IP アドレスと RADIUS サーバに設定する共通のシークレットを指定します。

またサブリカントでは、RADIUS サーバで発行した CA 証明書、ユーザ証明書の登録を行います。

## ■ 設定例

ここでは下記の内容で設定を行います。  
設定ウィザードを使って設定する場合は、「RADIUS (EAP)」を選択します。

設定条件：

RADIUS サーバの IP アドレス	192.168.0.254 (Ether0)
無線アクセスポイントの IP アドレス	192.168.0.253
無線アクセスポイントのシークレット	secret
ユーザ ID	user01
パスワード	pass01
認証方式	EAP-TLS
認証/アカウンティングポート	1812/1813

### ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。  
MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。  
ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS や NTP サーバを使用しないのであれば特に設定する必要はありません。



基本情報			
Ether0	IPアドレス	192.168.0.254/24	編集
	MTU	1500	
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	編集
	MTU	1500	
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	編集
	MTU	1500	
	通信モード	Auto	
デフォルトゲートウェイ			編集

### CA の設定 (CA/CA/CRL)

EAP-TLS 認証を使用する場合は CA の設定が必要になります。  
CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているかご確認ください。  
CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要で、ここでは以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name sample\_ca

email

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035 年 12 月 31 日

パスフレーズ

パスフレーズ

失効リスト更新間隔

失効リスト更新間隔 365

※[失効リスト更新間隔]で指定した間隔で失効リストの更新を行わなかった場合、証明書が有効な場合でも認証ができなくなります。必ず失効リストの更新処理を設定した間隔で行ってください。  
また更新した失効リストを有効にするには、RADIUS サービスの再起動が必要になります。  
CA の再編集はできませんので設定の際は内容を十分確認してください。  
また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

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 KeyUsage** を指定するようにします。

但し、実際にどの **Key Usage/Extended Key Usage** を必要とするかは通信相手のソフトウェアに依存します。

- **Key Usage** : digitalSignature および keyEncipherment
- **Extended Key Usage** : serverAuth

証明書

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name RA\_Server

email

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

開始日時 年 月 日 時 分

終了日時 2025 年 12 月 31 日 14 時 59 分

パスフレーズ

パスフレーズ

.....

設定

X.509証明書v3拡張 (RFC3280)

Key Usage

digitalSignature

keyEncipherment

keyAgreement

cRLSign

decipherOnly

nonRepudiation

dataEncipherment

keyCertSign

encipherOnly

Extended Key Usage serverAuth

CRL Distribution Points

Netscape拡張

nsCertType

client

email

sslCA

objCA

server

objsign

emailCA

nsComment

### 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。  
シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバは CA  
の証明書一覧で確認することができます。また、設定ウィザードを使った場合は自動的に入力されます。  
なおポート番号は、RADIUS クライアント(無線アクセスポイント)の設定と同一になるよう指定します。

ポート番号

- 1645/1646
- 1812/1813
- 1645/1646と1812/1813
- 手動設定

認証用

アカウント用

RADIUSサーバ証明書

- 使用しない
- 本装置の証明書を使用する

シリアルナンバ

認証方式

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

設定

### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの情報を設定します。  
クライアント新規追加画面の全ての項目を設定します。  
IP アドレスは、無線アクセスポイントの IP アドレス、シークレットは無線アクセスポイントに設定した  
ものと同じものを設定します。

クライアント新規追加

クライアント名

IPアドレス

シークレット

アドレスグループ

設定

ユーザはプロフィールという概念により、設定単位にグループ化を行うことができます。このプロフィールにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロフィール、ユーザプロフィールの作成が必要です。

### ユーザ基本情報プロフィールの作成 (RADIUS/プロフィール/ユーザ基本情報)

設定条件に従い認証方式に **EAP-TLS** に設定します。プロフィール名は **base\_user** とします。

ユーザ基本情報プロフィール 新規追加

プロフィール名: base\_user

認証方式: EAP-TLS

同時接続数: [ ]

IPアドレス割当て:  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール: 指定しない

設定

### 証明書プロフィールの作成 (RADIUS/プロフィール/証明書)

証明書プロフィールを作成しておくことで EAP-TLS 認証に必要なユーザ証明書の発行が簡単にできるようになります。

Key Usage/Extended KeyUsage の指定は必須ではありませんが、この証明書を HTTPS のクライアント認証など、他の認証にも使用する場合に備え、最低限以下の項目を指定しておくとい良いでしょう。

- Key Usage : digitalSignature
- Extended Key Usage : clientAuth

証明書プロフィール 新規追加

プロフィール名: cert

証明書

バージョン: 3

鍵長: 1024

Signature Algorithm: SHA-256

Subject

Organizational Unit: [ ]

Organization: [ ]

Locality: [ ]

State or Province: [ ]

Country: JP

有効期間

開始日時: [ ]年 [ ]月 [ ]日 [ ]時 [ ]分

終了日時: 2020年 12月 31日 14時 59分

Key Usage

digitalSignature  nonRepudiation

keyEncipherment  dataEncipherment

keyAgreement  keyCertSign

cRLSign  encipherOnly

decipherOnly

Extended Key Usage: clientAuth

CRL Distribution Points: [ ]

設定

## ユーザプロファイルの作成 (RADIUS/プロファイル/ユーザプロファイル)

これまでに作成したユーザ基本プロファイル **base\_user**、証明書プロファイル **cert** を指定してユーザプロファイル **user** を作成します。

ユーザプロファイル 新規追加	
プロファイル名	user
基本	base_user
認証	指定しない
証明書	cert
応答	指定しない
グループ	指定しない

**設定**

## ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **user01**、パスワードに **pass01** を入力します。プロファイルは先ほど作成したユーザプロファイルを指定します。以上を入力して **設定** を押下します。この作業を繰り返すことにより同じ設定（ここでは同じ証明書発行条件）のユーザを簡単に作成することができます。

ユーザ 新規追加	
ユーザID	user01
パスワード	●●●●●●
プロファイル	user

固定IPアドレス払い出し

IPアドレス	
ネットマスク	

備考

備考	
----	--

アカウントのロック

ロック	<input checked="" type="radio"/> ロックしない <input type="radio"/> ロックする
-----	---

**設定**

### ユーザ証明書の発行 (RADIUS/ユーザ/ユーザ)

ユーザ証明書はCAではなく、ユーザ一覧画面から行います。  
証明書の発行されていないユーザは証明書の欄のボタンが「発行」になっています。このボタンを押下することによりユーザ証明書を作成します。証明書作成画面では証明書プロファイルを設定してある場合はその内容が自動的に入力されます。証明書の有効期限を入力し、他に内容に変更がなければ設定ボタンを押下して証明書を発行してください。発行後は一覧のボタンは「表示」に変わります。

ユーザ							
No.	lock	ユーザID	プロファイル	IPアドレス	詳細	証明書	備考
1		user01	user	-	表示	発行	

ユーザ							
No.	lock	ユーザID	プロファイル	IPアドレス	詳細	証明書	備考
1		user01	user	-	表示	表示	

この「表示」ボタンを押下して表示される証明書画面からユーザ証明書の取り出しが行えます。証明書の取り出しは証明書画面から形式:「PKCS#12」、内容:「CA 証明書・証明書・私有鍵」を選択して

「取り出し」ボタンを押下します。

この取り出した証明書およびパスフレーズを使用してサブリカントへ設定します。

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に「起動」ボタンを押下してRADIUSサーバを起動します。

起動・停止	
現在の状態	停止中
起動	

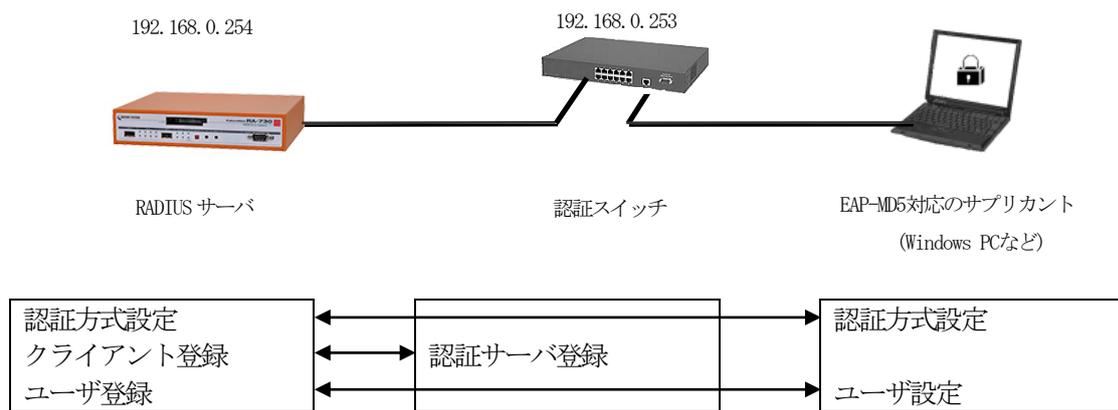
以上で設定は終了です。

## 1.6. EAP-MD5 認証を利用する

### ■ 概要

ここでは、認証方式はEAP-MD5を使用し、802.1Xに対応したスイッチ(以下認証スイッチ)の認証サーバとして使用する例を紹介します。

### ■ 構成



認証スイッチを使用し EAP-MD5 認証を使用するには以下の設定を行います。

- ・ 認証方式や使用ポートなどの基本設定
- ・ RADIUS クライアント (認証スイッチ) の登録
- ・ ユーザの登録

※認証スイッチでは、RADIUS サーバの IP アドレスと RADIUS サーバに設定する共通のシークレットを指定します。

またサブリカントでは、ユーザ ID/パスワードの設定を行います。

## ■ 設定例

ここでは下記の内容で設定を行います。認証方式は EAP-MD5 となっていますが、EAP-MD5 では証明書を必要としないので設定ウィザードを使って設定する場合は「RADIUS (PAP/CHAP)」を選択します。

設定条件：

RADIUS サーバの IP アドレス	192.168.0.254 (Ether0)
認証スイッチの IP アドレス	192.168.0.253
認証スイッチのシークレット	Secret
ユーザ ID	user01
パスワード	pass01
認証方式	EAP-MD5
認証/アカウントングポート	1812/1813

### ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS や NTP サーバを使用しないのであれば特に設定する必要はありません。

The screenshot shows the '基本情報' (Basic Information) section of the network configuration. It lists the following settings:

Interface	IP Address	MTU	Communication Mode	Action
Ether0	192.168.0.254/24	1500	Auto	編集
Ether1	192.168.1.254/24	1500	Auto	編集
Ether2	192.168.2.254/24	1500	Auto	編集
デフォルトゲートウェイ				編集

### 認証方式の設定 (RADIUS/サーバ/基本情報)

認証方式に **EAP-MD5**、RADIUS サーバ証明書に **使用しない** を選択します。

なおポート番号は、RADIUS クライアント(認証スイッチ)の設定と同一になるよう指定します。

The screenshot shows the 'RADIUSサーバ証明書' (RADIUS Server Certificate) and 'ポート番号' (Port Number) configuration sections. The 'ポート番号' section has radio buttons for '1645/1646', '1812/1813', '1645/1646と1812/1813', and '手動設定'. The 'RADIUSサーバ証明書' section has radio buttons for '使用しない' (selected) and '本装置の証明書を使用する'. Below these are input fields for 'シリアルナンバ'. The '認証方式' (Authentication Method) section has checkboxes for 'PAP/CHAP', 'EAP-TLS', 'EAP-TTLS', 'EAP-MD5' (checked), and 'EAP-PEAP'. A '設定' (Apply) button is at the bottom.

## RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

クライアント新規追加画面の全ての項目を設定します。IP アドレスは認証スイッチの IP アドレス、シークレットは認証スイッチへ設定したものと同一ものを設定します。

クライアント名	SW-01
IPアドレス	192.168.0.253
シークレット	secret
アドレスグループ	指定しない

設定

ユーザはプロファイルという概念により、設定単位にグループ化を行うことができます。このプロファイルにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロファイル、ユーザプロファイルの作成が必要です。

## ユーザ基本情報プロファイルの作成 (RADIUS/プロファイル/ユーザ基本情報)

設定条件に従い認証方式に **EAP-MD5** を設定します。プロファイル名は **base\_user** とします。

プロファイル名	base_user
認証方式	EAP-MD5
同時接続数	
IPアドレス割り当て	<input checked="" type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input type="radio"/> アドレスグループ <input type="radio"/> 固定
アドレスグループ	指定しない

設定

## ユーザプロファイルの作成 (RADIUS/プロファイル/ユーザプロファイル)

作成したユーザ基本プロファイル **base\_user** を指定してユーザプロファイル **user** を作成します。

プロファイル名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	指定しない

設定

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **user01**、パスワードに **pass01** を入力します。  
プロファイルは先ほど作成したユーザプロファイルを指定します。  
以上を入力して **設定** を押下します。

The screenshot shows a configuration interface for adding a new user. It is divided into several sections:

- ユーザ 新規追加**:
  - ユーザID: user01
  - パスワード: pass01 (masked with dots)
  - プロファイル: user (dropdown menu)
- 固定IPアドレス払い出し**:
  - IPアドレス: (empty field)
  - ネットマスク: (empty field)
- 備考**:
  - 備考: (empty text area)
- アカウントのロック**:
  - ロック:  ロックしない  ロックする

At the bottom right, there is an orange button labeled **設定**.

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

The screenshot shows the status configuration for the RADIUS server. It includes:

- 起動・停止**:
  - 現在の状態: 停止中

At the bottom center, there is an orange button labeled **起動**.

以上で設定は終了です。

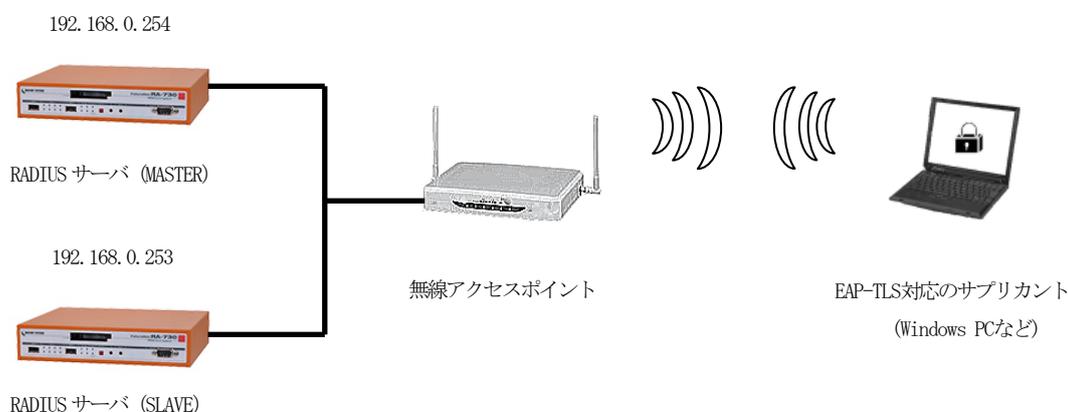
## 2. 冗長化機能を利用する

### 2.1. 設定情報の同期機能を利用する

#### ■ 概要

ここでは、設定情報の同期について紹介します。  
この設定を行う事により、二重化構成時に利用される各種設定情報を MASTER(マスタ)、SLAVE(スレーブ)間で同期させる事ができます。なお同期可能な項目の詳細については、ユーザズガイドを参照ください。

#### ■ 構成



#### ■ 設定例

「設定情報の同期」設定を行うには、事前にそれぞれの機器で IP アドレスの設定（「管理機能」-「ネットワーク」-「基本情報」）を行ってください。  
ここでは、「設定情報の同期」設定に関する内容のみ記載しておりますので、その他の設定については、ご利用される認証方式の設定例を参考に設定ください。

※ 設定情報の同期機能を使用する場合、必ず NTP サーバを設定の上ご利用ください。

ここでは下記の条件で設定を行います。

設定条件：

	MASTER	SLAVE
IP アドレス	192.168.0.254	192.168.0.253
RA システム名	RA-system	RA-system
RA 本装置名	RA-master	RA-slave
コンフィグ名	RA-config	RA-config

【設定情報の同期設定】（管理機能／システム／設定情報の同期）

MASTER 側

設定情報の同期設定

設定情報の同期

設定情報の同期  同期しない  同期する  親子連携

RA システム名 RA-system

RA 本装置名 RA-master

装置種別  MASTER  SLAVE

設定

同期コンフィグ一覧

同期コンフィグ 新規追加

コンフィグ名 RA-config

処理タイミング  即時実行  一括処理

設定

© Copyright 2005-2009 Century Systems Co., Ltd. All rights reserved

同期装置一覧

同期装置 新規追加

同期装置名 RA-slave

IP アドレス 192.168.0.253

同期装置種別 SLAVE

設定

上記設定後は、下記画面の様になります。

設定情報の同期

設定情報の同期	同期する
RA システム名	RA-system
RA 本装置名	RA-config
装置種別	MASTER

設定・編集

同期コンフィグ一覧

コンフィグ名	編集	削除
RA-config	編集	削除

同期装置一覧

コンフィグ名	同期装置名	IP アドレス	同期装置種別	削除
RA-config	RA-slave	192.168.0.253	SLAVE	削除

SLAVE 側

設定情報の同期

設定情報の同期  同期しない  同期する  親子連携

RA システム名 RA-system

RA 本装置名 RA-slave

装置種別  MASTER  SLAVE

設定

同期コンフィグ 新規追加

コンフィグ名 RA-config

処理タイミング  即時実行  一括処理

設定

© Copyright 2005-2009 Century Systems Co., Ltd. All rights reserved

同期装置 新規追加

同期装置名 RA-master

IP アドレス 192.168.0.254

同期装置種別 MASTER

設定

設定情報の同期

設定情報の同期	同期する
RA システム名	RA-system
RA 本装置名	RA-config
装置種別	SLAVE

設定・編集

同期コンフィグ一覧

コンフィグ名	編集	削除
RA-config	編集	削除

同期装置一覧

コンフィグ名	同期装置名	IP アドレス	同期装置種別	削除
RA-config	RA-master	192.168.0.254	MASTER	削除

- RA システム名は、MASTER、SLAVE 共、共通な名称を設定します。
- RA 本装置名は、MASTER、SLAVE それぞれ一意の名称を設定します。
- コンフィグ名は、MASTER、SLAVE 共、共通な名称を設定します。
- 処理のタイミングは、状況に応じて選択ください。  
**即時実行** を選択すると、MASTER 側で設定した内容が即時 SLAVE 側へ同期されます。  
**一括処理** を選択しますと MASTER 側の同期実行一覧で表示される一括同期の実行ボタンを押下するまで内容は同期されません。
- 同期装置の追加では、対向の同期装置情報（同期装置名/IP アドレス）を追加します。

既に二重化の設定が行われている場合は、下記の画面が MASTER に表示されます。

コ ン フ ィ グ 名	一括同期	強制同期	設定取得	ログ同期	ログ取得	RADIUS		
RA- config	実行	実行	実行	実行	実行	起動	再起動	停止

以上で設定は終了です。

## 2.2. 二重化機能を利用する

### ■ 概要

ここでは、二重化の設定について紹介します。  
この設定を行う事により認証/アカウントングログ及びログイン情報がプライマリ、セカンダリ間で同期されます。

### ■ 構成



### ■ 設定例

「二重化」設定を行うには、事前にそれぞれの機器でIPアドレスの設定（「管理機能」-「ネットワーク」-「基本情報」）を行ってください。

ここでは、「二重化」設定に関する内容のみ記載しておりますので、その他の設定については、ご利用される認証方式の設定例を参考に設定ください。

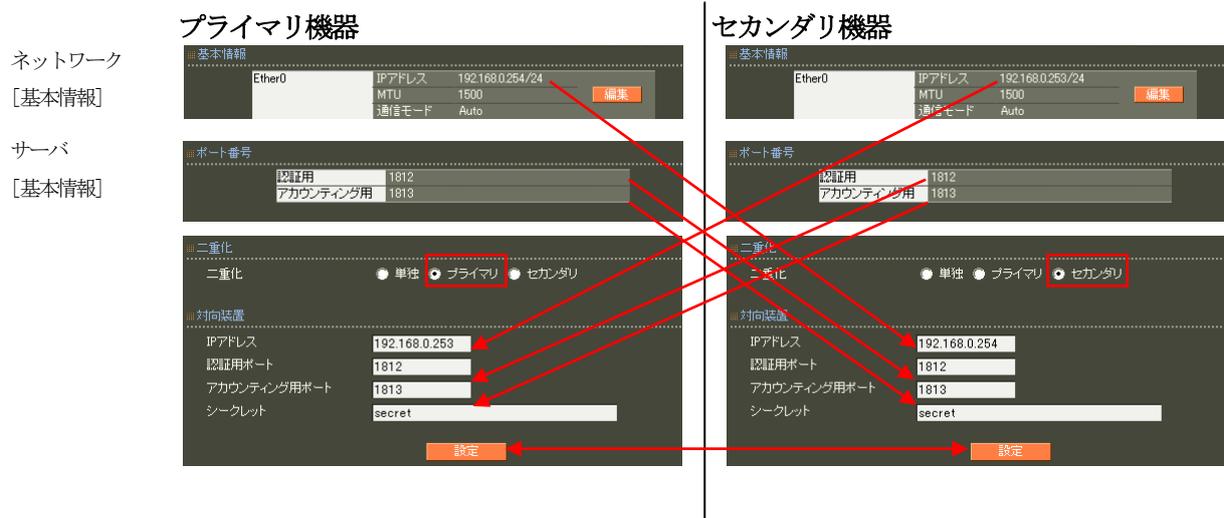
**※二重化機能を使用する場合、必ずNTPサーバを設定の上ご利用ください。**

ここでは下記の条件で二重化の設定を行います。

設定条件：

	プライマリ	セカンダリ
IP アドレス	192.168.0.254	192.168.0.253
認証用ポート	1812	1812
アカウントング用ポート	1813	1813
シークレット	secret	secret

二重化設定 (RADIUS/サーバ/二重化)



- ・ 対向装置の設定欄に相手装置の IP アドレス、認証用ポート、アカウント用ポートを設定します。シークレットは双方で同じものを設定してください。
- ・ 設定 or 設定変更後は、双方の機器で RADIUS サーバの再起動が必要となります。(RADIUS/サーバ/起動・停止)

※サーバの起動(再起動)はプライマリ、セカンダリ共にネットワークに接続された状態で行ってください。

RAIDUS サーバは、プライマリ機器に障害が発生した場合、自身でセカンダリ機器へ切り替えを行うような動作は行いません。  
通常 RADIUS クライアントに登録されているセカンダリ RADIUS サーバ設定により通信先を切替えるような動作となりますのでこの設定を行った後に RADIUS クライアントに双方の RADIUS サーバが正しく登録されているか確認ください。

以上で設定は終了です。

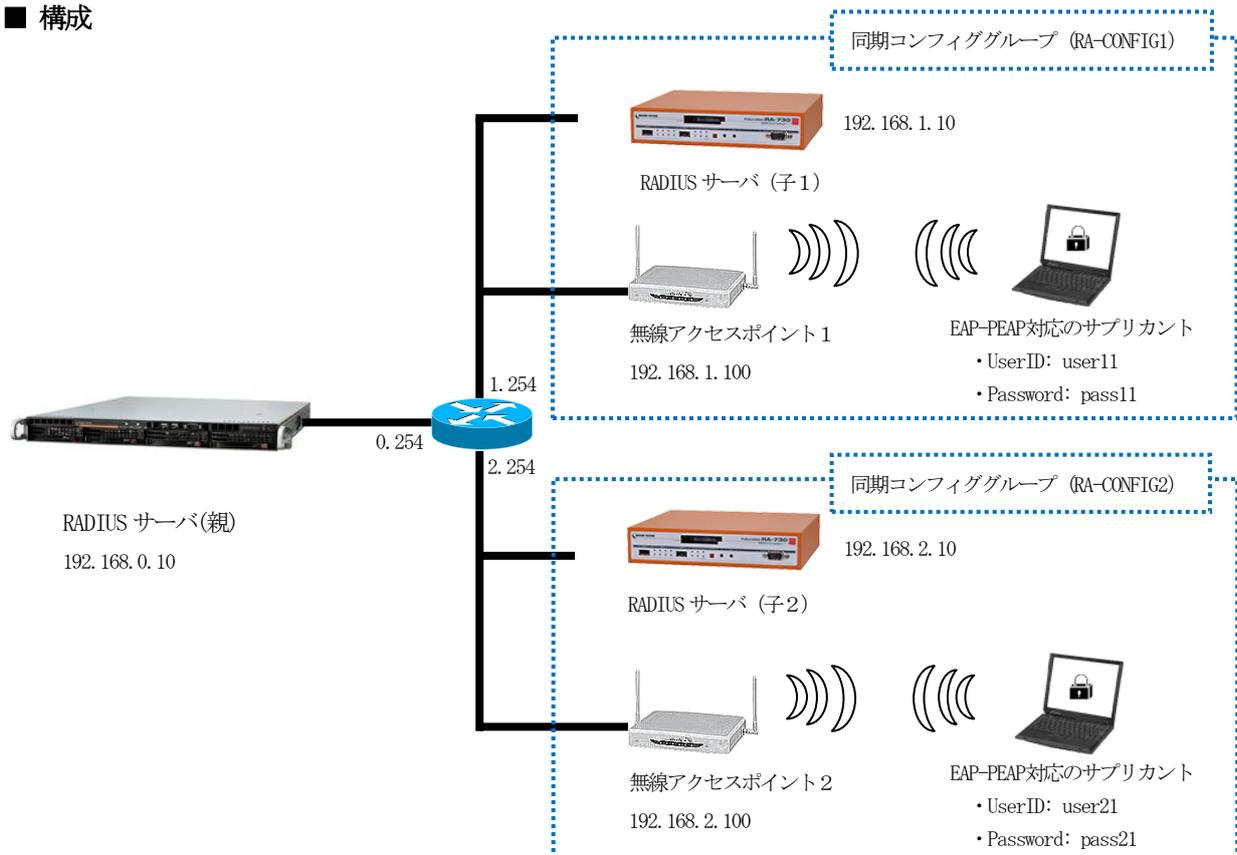
## 2.3. 親子連携機能を利用する

## ■ 概要

ここでは、親子連携機能について紹介します。

この設定を行う事により認証/アカウントングログ及びログイン情報が親子間で同期され子側の機器で障害が発生しても親側の機器で継続して認証/アカウントング処理を行う事ができます。  
また RADIUS 認証に関する設定は、親で管理する事ができます。

## ■ 構成



親子連携を利用し、無線アクセスポイント接続の認証に EAP-PEAP 認証を使用するには親機に対して下記設定を行います。

- ・ネットワークの設定
- ・設定情報の同期
- ・CA の設定
- ・RADIUS サーバ用のサーバ証明書の発行
- ・認証方式や使用ポートなどの基本設定
- ・RADIUS クライアント（無線アクセスポイント）の登録
- ・各プロファイルの登録（子1、子2用）
- ・ユーザの登録（子1、子2用）

※ 親子連携機能を使用する場合、必ず NTP サーバを設定の上ご利用ください

子機に対して、下記設定を行います。

- ・ネットワークの設定
- ・設定情報の同期

無線アクセスポイント1には、プライマリのRADIUSサーバとしてRADIUSサーバ(子1)のIPアドレスを、無線アクセスポイント2に対しては、プライマリのRADIUSサーバとしてRADIUSサーバ(子2)のIPアドレスを、セカンダリの認証サーバとしてRADIUSサーバ(親)のIPアドレスをそれぞれに設定し、認証及びアカウントングに使用するポート、シークレットの設定を行います。

サブリカントでは、親機または子機から取得したCA証明書の登録を行います。

## ■ 設定例

下記の条件で親子連携の設定を行います。

設定条件：

	親	子1	子2
IPアドレス	192.168.0.10	192.168.1.10	192.168.2.10
デフォルトゲートウェイ	192.168.0.254	192.168.1.254	192.168.2.254
認証用ポート	1812	1812	1812
アカウントング用ポート	1813	1813	1813
認証方式	EAP-PEAP	EAP-PEAP	EAP-PEAP
無線アクセスポイントのクライアント名	AP1 AP2	AP1	AP2
無線アクセスポイントのIPアドレス	192.168.1.100 192.168.2.100	192.168.1.100	192.168.2.100
無線アクセスポイントのシークレット	secret	secret	secret
ユーザID	user11 user21	user11	user21
パスワード	pass11 pass21	pass11	pass21

初めに親となる RADIUS サーバを動作させる環境、本体の設定を行います。

## ■ 親の環境設定

### ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.10/24** に設定します。  
 MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。  
 ここでは初期値のままとします。  
 デフォルトゲートウェイを 192.168.0.254 に設定します。  
 外部の DNS や NTP サーバを使用する場合も設定する必要があります。

基本情報			
Ether0	IPアドレス	192.168.0.10/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
デフォルトゲートウェイ		192.168.0.254	<input type="button" value="編集"/>

### 設定情報の同期の設定 (管理機能/システム/設定情報の同期)

ここでは、下記条件で設定を行います。

RA システム名	RA-SYSTEM
RA 本装置名 (親)	RA-OYA
コンフィグ名 (子1)	RA-CONFIG1
コンフィグ名 (子2)	RA-CONFIG2
同期装置名 (子1)	RA-K01
同期装置名 (子2)	RA-K02

設定情報の同期で  ボタンを押して、親の情報を設定します。

設定情報の同期	
設定情報の同期	<input type="radio"/> 同期しない <input type="radio"/> 同期する <input checked="" type="radio"/> 親子連携
RA システム名	<input type="text" value="RA-SYSTEM"/>
RA 本装置名	<input type="text" value="RA-OYA"/>
装置種別	<input checked="" type="radio"/> MASTER <input type="radio"/> SLAVE
<input type="button" value="設定"/>	

次に同期コンフィグ一覧で子1、子2で使用するコンフィグをそれぞれ作成します。

同期コンフィグ一覧で **新規追加** ボタンで設定します。

子1設定例：

同期コンフィグ 新規追加

---

コンフィグ名

**設定**

子2設定例：

同期コンフィグ 新規追加

---

コンフィグ名

**設定**

同期装置一覧で、各コンフィグに所属する装置を追加します。

同期装置 一覧

コンフィグ名	同期装置名	IP アドレス	同期装置種別	削除
RA-CONFIG1	<b>新規追加</b>			
RA-CONFIG2	<b>新規追加</b>			

各コンフィグ項目にある **新規追加** ボタンを押して子1、子2の装置情報を設定します。

子1設定例：

同期装置 新規追加

---

同期装置名

IP アドレス

同期装置種別

**設定**

子2設定例：

同期装置 新規追加

---

同期装置名

IP アドレス

同期装置種別

**設定**

上記設定完了後、以下の画面が表示されます。

The screenshot displays a web-based configuration interface for RA synchronization. It is divided into four main sections:

- 設定情報の同期 (Sync Settings):** A table showing synchronization information.
 

設定情報の同期	親子連携
RA システム名	RA-SYSTEM
RA 本装置名	RA-OYA
装置種別	MASTER

 Below the table is an orange button labeled "設定・編集".
- 同期コンフィグ一覧 (Sync Config List):** A table listing synchronization configurations.
 

コンフィグ名	削除
RA-CONFIG1	削除
RA-CONFIG2	削除

 Below the table is an orange button labeled "新規追加".
- 同期装置一覧 (Sync Device List):** A table listing synchronized devices.
 

コンフィグ名	同期装置名	IP アドレス	同期装置種別	削除
RA-CONFIG1	RA-KO1	192.168.1.10	SLAVE	削除
RA-CONFIG2	RA-KO2	192.168.2.10	SLAVE	削除
- 同期実行一覧 (Sync Execution List):** A table showing execution options for configurations.
 

コンフィグ名	強制同期	ログ同期	ログ取得	RADIUS
RA-CONFIG1	実行	実行	実行	起動 再起動 停止
RA-				

## CA の設定 (CA/CA/CRL)

EAP-PEAP 認証を使用する場合は CA の設定が必要です。  
 また、CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているか確認することをお奨めします。  
 CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要です。  
 ここでは以下の設定で CA を作成します。

CA にて CA 証明書の設定を行います。  
 CA 証明書画面から **新規追加** ボタンを押下します。

ここでは、下記条件で設定を行います。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample

失効リスト更新間隔	365
-----------	-----

設定例：

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name sample\_ca

email samp@example.co.jp

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035 年 12 月 31 日

パスフレーズ

パスフレーズ

失効リスト更新間隔

失効リスト更新間隔 365

設定

※CAの再編集はできませんので設定の際は内容を十分確認してください。  
また、CAを削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

RADIUS サーバ証明書の発行 (CA/証明書)

CA にて RADIUS サーバの証明に使用するサーバ証明書を発行します。

ここでは、下記条件で設定を行います。

バージョン	3
鍵長	1024
Signature Algorithm	SHA-256
Common Name	RA_Server
Country	JP
有効期間(終了日時)	2025/12/31 14: 59
パスフレーズ	RA_Serverpass
Key Usage	DigitalSignature KeyEncipherment
Extended Key Usage	serverAuth

証明書画面から **新規追加** ボタンを押下します。



親設定例：

※ 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 KeyUsage 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 を必要とするかは通信相手のソフトウェアに依存します。

#### 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

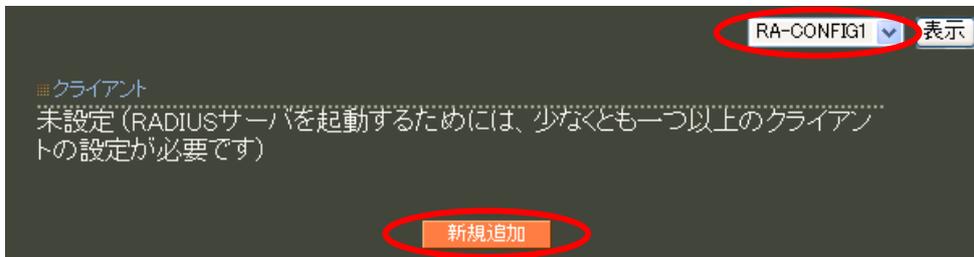
認証方式に **EAP-PEAP**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバはCAの証明書一覧で確認することができます。

設定例：

## RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

クライアント新規追加画面の全ての項目を設定します。IPアドレスは無線アクセスポイントのIPアドレス、シークレットは無線アクセスポイントへ設定したものと同一ものを設定します。

ここでも、子1、子2のコンフィグを指定して **新規追加** ボタンを押下します。



子1 設定例:

クライアント新規追加

コンフィグ名	RA-CONFIG1
クライアント名	AP1
IPアドレス	192.168.1.100
シークレット	secret
アドレスプール	指定しない

設定

子2 設定例:

クライアント新規追加

コンフィグ名	RA-CONFIG2
クライアント名	AP2
IPアドレス	192.168.2.100
シークレット	secret
アドレスプール	指定しない

設定

以上でRADIUSサーバの設定は終了です。次に認証するユーザの作成です。

## ユーザ基本情報プロファイルの作成 (RADIUS/プロフィール/ユーザ基本情報)

子1、子2のコンフィグを指定して **新規追加** ボタンを押下します。



子1、子2のプロファイル名は、それぞれ `user_base_config1`、`user_base_config2` とします。

設定条件に従い認証方式に **EAP-PEAP** を選択し、その他はデフォルト値とします。

子1設定例：

19

ユーザ基本情報プロフィール 新規追加

-----

コンフィグ名 RA-CONFIG1

プロフィール名 user\_base\_config1

認証方式 EAP-PEAP

同時接続数

IPアドレス割り当て  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール 指定しない

設定

子2設定例：

ユーザ基本情報プロフィール 新規追加

-----

コンフィグ名 RA-CONFIG2

プロフィール名 user\_base\_config2

認証方式 EAP-PEAP

同時接続数

IPアドレス割り当て  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール 指定しない

設定

### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

子1、子2のコンフィグを指定して **新規追加** ボタンを押下します。

RA-CONFIG1 表示

ユーザプロフィール

未設定

新規追加

子1、子2のプロファイル名を、それぞれ `user_config1`、`user_config2` とし、先ほど作成したユーザ基本情報プロファイルを選択します。

子1 設定例：

ユーザプロファイル 新規追加

コンフィグ名	RA-CONFIG1
プロファイル名	user_config1
基本	user_base_config1
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	指定しない

設定

子2 設定例：

ユーザプロファイル 新規追加

コンフィグ名	RA-CONFIG2
プロファイル名	user_config2
基本	user_base_config2
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	指定しない

設定

以上でユーザを作成する準備が整いました。

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

子1、子2のコンフィグを指定して **新規追加** ボタンを押下します。

ユーザ 新規追加

RA-CONFIG1 表示

ユーザ 未設定

新規追加

設定条件に従いユーザ ID に **user11**、パスワードに **pass11** を入力します。  
プロフィールは先ほど作成したユーザプロフィールを指定します。  
以上を入力して **設定** を押下します。  
この作業を繰り返すことにより同じ設定のユーザを作成することができます。

## 子1 設定例：



■ **コンフィグ名**

コンフィグ名 RA-CONFIG1

■ **ユーザ 新規追加**

ユーザID user11

パスワード ●●●●●●

プロフィール user\_config1

■ **固定IPアドレス払い出し**

IPアドレス

ネットマスク

■ **アカウントのロック**

ロック  ロックしない  ロックする

**設定**

## 子2 設定例：



■ **コンフィグ名**

コンフィグ名 RA-CONFIG2

■ **ユーザ 新規追加**

ユーザID user21

パスワード ●●●●●●

プロフィール user\_config2

■ **固定IPアドレス払い出し**

IPアドレス

ネットマスク

■ **アカウントのロック**

ロック  ロックしない  ロックする

**設定**

次に子となる RADIUS サーバを動作させる環境の設定を行います。

## ■子の環境設定

### ネットワークの設定 (管理機能/ネットワーク/基本情報)

子1、子2のそれぞれのEther0のIPアドレスに **192.168.1.10/24**、**192.168.2.10/24** に設定します。MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。ここでは初期値のままとします。  
デフォルトゲートウェイをそれぞれ 192.168.1.254、192.168.2.254 に設定します。

#### 子1の場合

基本情報			
Ether0	IPアドレス	192.168.1.10/24	
	MTU	1500	<a href="#">編集</a>
	通信モード	Auto	
Ether1	IPアドレス	192.168.10.254/24	
	MTU	1500	<a href="#">編集</a>
	通信モード	Auto	
Ether2	IPアドレス	192.168.20.254/24	
	MTU	1500	<a href="#">編集</a>
	通信モード	Auto	
デフォルトゲートウェイ		192.168.1.254	<a href="#">編集</a>

#### 子2の場合

基本情報			
Ether0	IPアドレス	192.168.2.10/24	
	MTU	1500	<a href="#">編集</a>
	通信モード	Auto	
Ether1	IPアドレス	192.168.10.254/24	
	MTU	1500	<a href="#">編集</a>
	通信モード	Auto	
Ether2	IPアドレス	192.168.20.254/24	
	MTU	1500	<a href="#">編集</a>
	通信モード	Auto	
デフォルトゲートウェイ		192.168.2.254	<a href="#">編集</a>

設定情報の同期の設定（管理機能/システム/設定情報の同期）

設定情報の同期画面で **設定・編集** ボタンで設定します。

ここでは、親で設定した内容に基づき下記設定を行います。

	子1	子2
RA システム名	RA-SYSTEM	RA-SYSTEM
RA 本装置名	RA-KO1	RA-KO2
コンフィグ名	RA-CONFIG1	RA-CONFIG2
同期装置名	RA-OYA	RA-OYA

子1の場合

同期コンフィグ一覧で **新規追加** ボタンで設定します。

子2の場合

同期コンフィグ一覧で **新規追加** ボタンで設定します。

同期コンフィグ 新規追加

コンフィグ名

**設定**

同期装置一覧で、各コンフィグに所属する装置（親）を追加します。

子1、子2共

同期装置 新規追加

同期装置名

IP アドレス

同期装置種別

**設定**

以上で子1、子2の設定情報の同期設定は完了です。  
設定後以下の画面が表示されます。

子1の場合

設定情報の同期

設定情報の同期	親子連携
RA システム名	RA-SYSTEM
RA 本装置名	RA-K01
装置種別	SLAVE

**設定・編集**

同期コンフィグ 一覧

コンフィグ名	削除
RA-CONFIG1	<b>削除</b>

同期装置 一覧

コンフィグ名	同期装置名	IP アドレス	同期装置種別	削除
RA-CONFIG1	RA-OYA	192.168.0.10	MASTER	<b>削除</b>

子2の場合

The screenshot displays the configuration interface for a child device. It is divided into three sections:

- 設定情報の同期 (Sync Settings):** A table showing synchronization details.
 

設定情報の同期	親子連携
RA システム名	RA-SYSTEM
RA 本装置名	RA-K02
装置種別	SLAVE
- 同期コンフィグ 一覧 (Sync Config List):** A table listing synchronization configurations.
 

コンフィグ名	削除
RA-CONFIG2	<input type="button" value="削除"/>
- 同期装置 一覧 (Sync Device List):** A table listing synchronized devices.
 

コンフィグ名	同期装置名	IP アドレス	同期装置種別	削除
RA-CONFIG2	RA-OYA	192.168.0.10	MASTER	<input type="button" value="削除"/>

最後に親で設定した情報を子1、子2へ反映させます。  
以下操作は、親の機器で行います。

■設定内容の同期

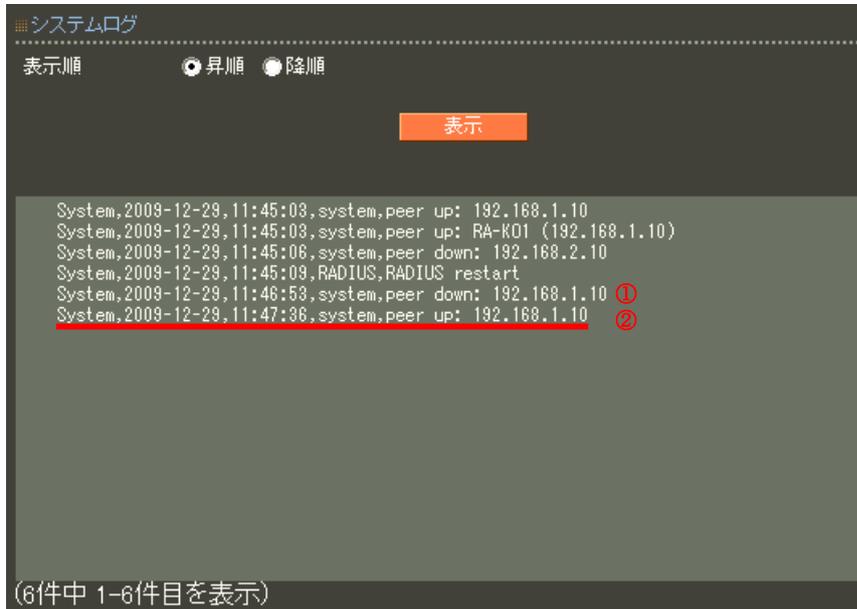
設定情報の同期の設定 (管理機能/システム/設定情報の同期)

子1、子2に該当するコンフィグ欄の強制同期にある **実行** ボタンを押します。

The screenshot shows the '同期実行 一覧' (Sync Execution List) section. It contains a table with columns for configuration name, forced sync, log sync, log acquisition, and RADIUS settings. The '実行' (Execute) button in the forced sync column for 'RA-CONFIG2' is circled in red.

コンフィグ名	強制同期	ログ同期	ログ取得	RADIUS		
RA-CONFIG2	<input type="button" value="実行"/>	<input type="button" value="実行"/>	<input type="button" value="実行"/>	<input type="button" value="起動"/>	<input type="button" value="再起動"/>	<input type="button" value="停止"/>
RA-						

「強制同期」を実行すると、親の設定内容が子へ反映されます。  
その際既に運用を開始している場合は、親のログを子に同期する必要がありますので、「ログ同期」も実行してください。但し、強制同期処理中は、ログ同期ができませんので処理が完了してから行ないます。  
強制同期の処理完了は、親のシステムログに記録される②” peer up” により状況を確認する事ができます。  
処理中は、①” peer down” のログが記録されます。



※親子連携機能を使用する場合、必ずNTPサーバを設定の上ご利用ください。

最後に全ての機器でRADIUSサーバ(RADIUS/サーバ/起動・停止)を起動します。

以上で親子連携の設定は終了です。

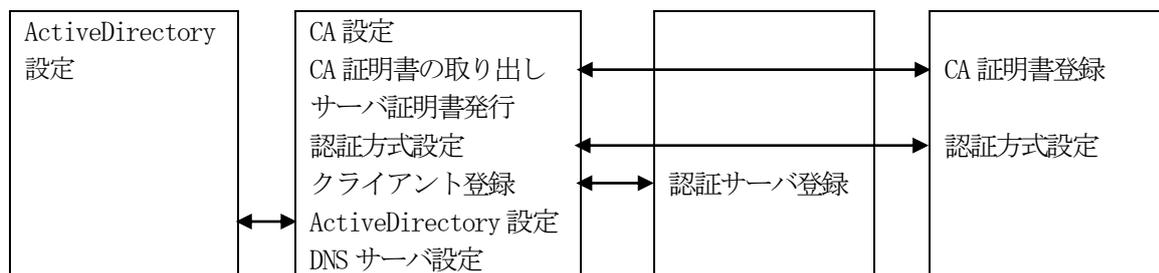
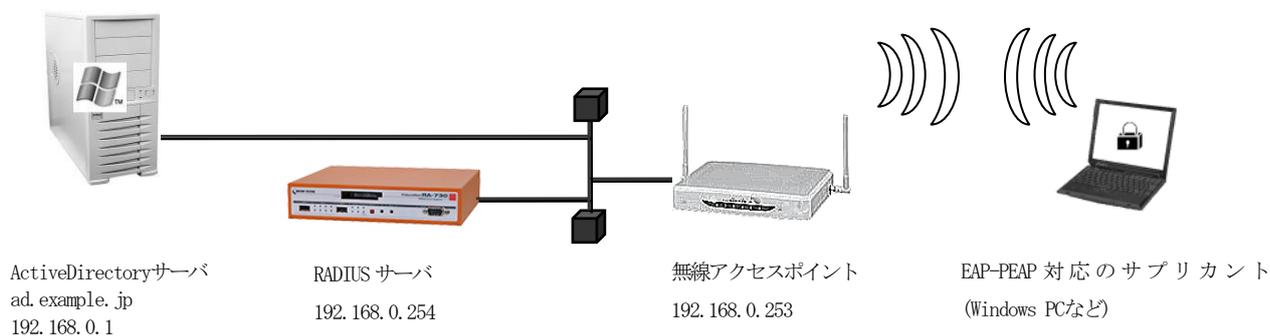
### 3. 連携機能を利用する

#### 3.1. ActiveDirectory 連携機能を利用する

##### ■ 概要

ここでは、ユーザ認証に ActiveDirectory を用いたユーザ認証の例を紹介します。

##### ■ 構成



ユーザ認証に ActiveDirectory を用いるには、以下設定を行います。

- CA作成
- RAのサーバ証明書を発行
- 認証方式などの基本設定
- クライアント（無線アクセスポイント）の登録
- ActiveDirectoryの設定
- DNSサーバの設定
- ADユーザプロファイル設定

## ■ 設定例

この例ではドメインコントローラ 1 台の構成で ActiveDirectory を運営している環境へ無線アクセスポイントを追加し、ユーザの認証に ActiveDirectory を使用する場合の例となります。

また、無線による接続は既存の全てのユーザではなく、一部のユーザのみ許可を与えるものとします。ActiveDirectory には新たに Wireless というセキュリティグループを作成し、Wireless グループに所属するメンバーのみ無線アクセスが行えるよう RADIUS サーバを設定します。ActiveDirectory を用いた認証を行う場合の RADIUS サーバは、ActiveDirectory に対して無線アクセスポイントからの認証の橋渡しを行います。ActiveDirectory を用いて認証する場合は認証プロトコルとして **EAP-PEAP** を使用します。設定ウィザードを使って設定する場合は EAP-PEAP 用に証明書の発行が必要になりますので、「RADIUS (EAP)」を選択します。

設定条件：

ドメインコントローラ	192.168.0.1
AD ドメイン	ad.example.jp
所属グループ	Wireless
Admin ユーザ名	administrator
Admin パスワード	administratorpass
認証方式	EAP-PEAP
応答アトリビュート	使用しない

最初に RADIUS サーバを動作させる環境、RADIUS サーバの設定を行います。

### ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS、NTP サーバを使用しないのであれば特に設定する必要はありません。



基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	<input type="button" value="編集"/>
Ether1	通信モード	Auto	
	IPアドレス	192.168.1.254/24	<input type="button" value="編集"/>
Ether2	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
デフォルトゲートウェイ			<input type="button" value="編集"/>

## CA の設定 (CA/CA/CRL)

EAP-PEAP 認証を使用する場合は CA の設定が必要になります。

また、CA の作成や証明書の発行を行う際は内蔵時計が正しく設定されているか確認することをお奨めします。

CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要で、例では以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

The screenshot shows a configuration form for a CA. The fields and their values are as follows:

- バージョン: 3
- 鍵長: 1024
- Signature Algorithm: SHA-256
- Subject:
  - Common Name: sample\_ca
  - email: (empty)
  - Organizational Unit: (empty)
  - Organization: (empty)
  - Locality: (empty)
  - State or Province: (empty)
  - Country: JP
- 有効期間:
  - 終了日時: 2035 年 12 月 31 日
- パスワード: (masked with dots)
- 失効リスト更新間隔: 365

※CA の再編集はできませんので設定の際は内容を十分確認してください。

また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

CA 作成後は CA 証明書画面より **取り出し** ボタンを押下して CA 証明書を取得し、サプライカントへインストールします。

## 【RADIUS サーバの設定】

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

設定例：

The screenshot shows a configuration form for a RADIUS server certificate. The '証明書' (Certificate) section includes fields for version (3), key length (1024), signature algorithm (SHA-256), and subject information (Common Name: RA\_Server, Country: JP). The '有効期間' (Validity Period) is set from 2025年12月31日 14時59分. The 'X.509証明書v3拡張 (RFC3280)' section has 'Key Usage' with 'digitalSignature' and 'keyEncipherment' checked, and 'Extended Key Usage' set to 'serverAuth'. The 'Netscape拡張' section has 'nsCertType' set to 'server'. A '設定' (Settings) button is at the bottom.

※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 KeyUsage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を必要とするかは通信相手のソフトウェアに依存します。

認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**、**EAP-PEAP**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。(EAP-PEAP を使用するには EAP-TLS も選択する必要があります。)  
 シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバは CA の証明書一覧で確認することができます。また、設定ウィザードを使った場合は自動的に入力されます。

DNS の設定 (管理機能/ネットワーク/DNS)

DNS の設定で所属する example.jp ドメインを管理している DNS サーバ (ここでは ActiveDirectory ドメインコントローラと同一) **192.168.0.1** を指定します。

ActiveDirectory の設定 (RADIUS/サーバ/ActiveDirectory)

ActiveDirectory 画面では、ActiveDirectory の **ドメイン名** と **管理者ユーザ ID**、**管理者パスワード** にドメインコントローラの **Administrator 権限のユーザの管理者 ID** とパスワードを入力します。所属グループは今回新たに追加した **Wireless** を指定します。

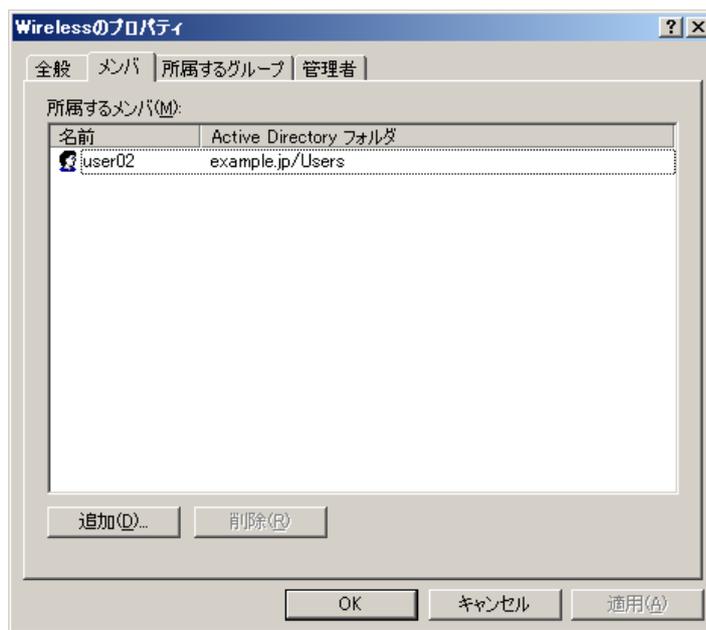
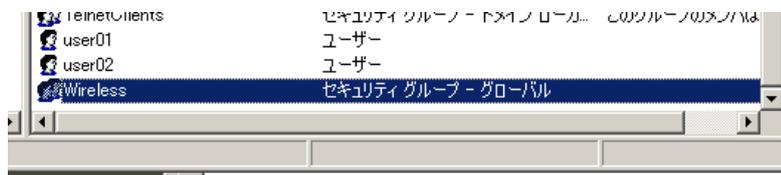
## 所属グループについて

ActiveDirectory による認証で、“所属グループ”の設定をおこなうと、ActiveDirectory のユーザ情報の一部である『所属するグループ』情報を認証識別子として用いて認証を行います。“所属グループ”の設定を行わない場合はActiveDirectory に登録された全てのユーザで認証が可能になります。

認証する必要があるユーザのみ特定のグループに所属させ、この機能を用いて認証を行うことで意図しないユーザの認証を破棄することができます。

例) ActiveDirectory 上の user01、user02 のうち、user02 のみ認証を行いたい。

- ①ActiveDirectory にて 特定のグループ(Wireless)を作成し、user02 を所属させる。
- ②RADIUS サーバにて ActiveDirectory の設定で所属グループに Wireless を指定する



以上の設定で Wireless グループに所属するユーザ user02 のみ認証することができます。その他の user01 や Administrator、Guest といった Wireless グループに属さないユーザは認証できません。

また、ActiveDirectory 連携時、認証可能なユーザは「運用管理機能/ユーザ情報/AD ユーザ情報」画面にて確認することができます。



### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

クライアント新規追加画面では、全ての項目を設定します。IP アドレスは無線アクセスポイントの IP アドレス、シークレットは無線アクセスポイントへ設定したものと同一ものを設定します。

クライアント新規追加

クライアント名	AP-01
IPアドレス	192.168.0.253
シークレット	secret
アドレスプール	指定しない

設定

### AD ユーザの設定 (RADIUS/ユーザ/AD ユーザ)

この例では応答アトリビュートは使用しませんので AD ユーザは **指定しない** のままとします。

ADユーザ

ユーザプロフィール 指定しない

設定

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

起動・停止

現在の状態 停止中

起動

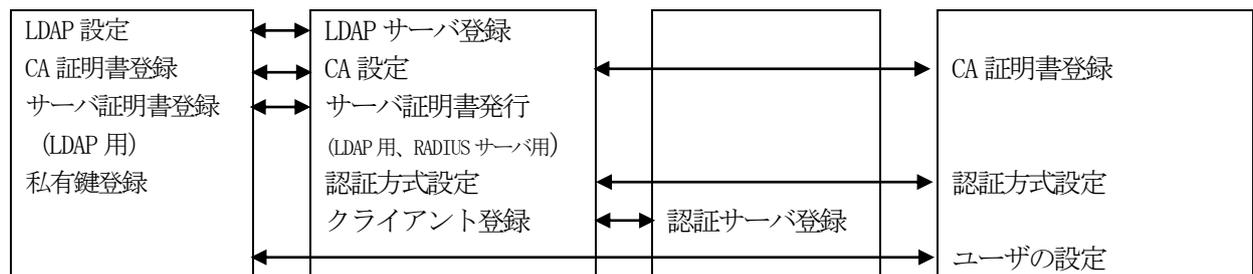
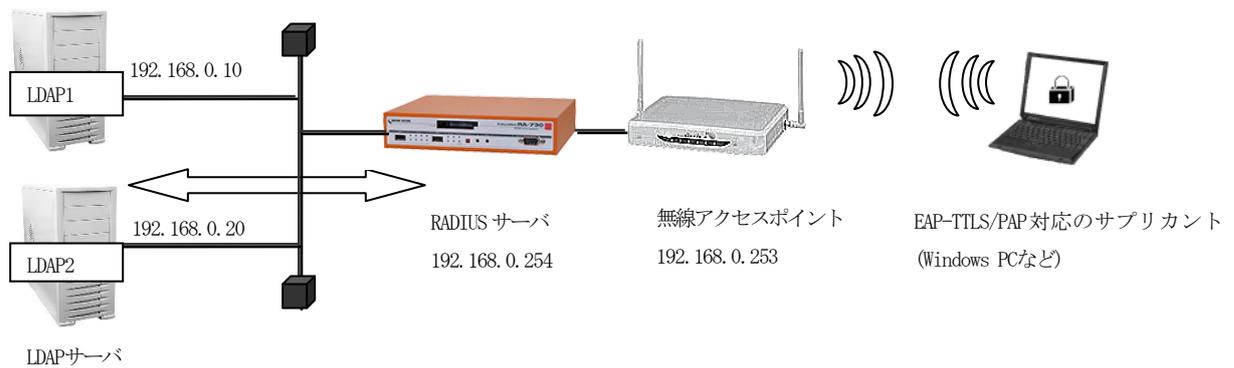
以上で設定は終了です。

### 3.2. LDAP 連携を利用する

#### ■ 概要

ここではLDAP サーバに登録されているユーザで認証を行う例を紹介します。

#### ■ 構成



ここではLDAP サーバを2つ用意し、ユーザ検索をLDAP1, LDAP2, RADIUS サーバローカルの順に行います。ユーザ認証にはEAP-TTLS/PAPを用い、RADIUS サーバとLDAP 間はLDAPS による暗号化通信を行うものとします。

LDAP 連携を使用するにはRADIUS サーバに対して以下設定を行います。

- CA の作成
- RADIUS サーバ証明書を発行
- LDAPS で使用するLDAP1, LDAP2 用のサーバ証明書及びRADIUS サーバ用のクライアント証明書を発行
- 認証方式や使用ポートなどの基本設定
- RADIUS クライアント (無線アクセスポイント) の登録
- LDAP サーバの登録
- RADIUS サーバ ローカルユーザの登録

## ■ 設定例

ここでは下記の内容で設定を行います。EAP-TTLS 及び LDAPS 用に証明書を発行する必要があるため設定ウィザードを使って設定する場合は「RADIUS (EAP)」を選択します。

設定条件：

<LDAP1>

LDAP 名	LDAP1
IP アドレス	192.168.0.10
ポート	636
ベース DN	o=ldap1, c=jp
バインド DN	cn=Manager, o=ldap1, c=jp
パスワード	secret1
フィルタオブジェクト	なし
フィルタアトリビュート	uid
セキュリティ	LDAPS

<LDAP2>

LDAP 名	LDAP2
IP アドレス	192.168.0.20
ポート	636
ベース DN	o=ldap2, c=jp
バインド DN	cn=Manager, o=ldap2, c=jp
パスワード	Secret2
フィルタオブジェクト	なし
フィルタアトリビュート	uid
セキュリティ	LDAPS

ローカルユーザ ID	user03
パスワード	pass03
認証方式	EAP-TTLS/PAP
RADIUS クライアント	無線アクセスポイント(192.168.0.253)
ユーザ検索順	LDAP1, LDAP2, LOCAL

ネットワークの設定 (管理機能/ネットワーク/基本設定)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。  
 MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。  
 ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS、NTP サーバを  
 使用しないのであれば特に設定する必要はありません。

基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	<input type="button" value="編集"/>
	MTU	1500	
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	<input type="button" value="編集"/>
	MTU	1500	
	通信モード	Auto	
デフォルトゲートウェイ			<input type="button" value="編集"/>

CA の設定 (CA/CA/CRL)

CA の作成や証明書の発行を行う際は内蔵時計が正しく設定されているか確認することをお奨めします。CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力必須です。例では以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name sample\_ca

email

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035 年 12 月 31 日

パスワード

パスワード

失効リスト更新間隔

失効リスト更新間隔 365

※CA の再編集はできませんので設定の際は内容を十分確認してください。  
また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。



[ldap クライアント用]

証明書

バージョン

鍵長

Signature Algorithm

Subject

Common Name

email

Organizational Unit

Organization

Locality

State or Province

Country

有効期間

開始日時

終了日時

パスワード

パスワード

X509証明書v3拡張 (RFC3280)

Key Usage

digitalSignature  nonRepudiation

keyEncipherment  dataEncipherment

keyAgreement  keyCertSign

cRLSign  encipherOnly

decipherOnly

Extended Key Usage

CRL Distribution Points

Netscape拡張

nsCertType

client  server

email  objSign

sslCA  emailCA

objCA

nsComment

証明書

表示条件  全て  未失効

No.	S/N	Subject	有効期間	失効日時
1	01	RA_Server	2013-11-26 06:39:35 2025-12-31 14:59:00	
2	02	ldap1	2013-11-26 06:41:54 2025-12-31 14:59:00	
3	03	ldap2	2013-11-26 06:42:33 2025-12-31 14:59:00	
4	04	ldap client	2013-11-26 06:43:34 2025-12-31 14:59:00	

## 認証方式の設定 (RADIUS/サーバ/基本設定)

認証方式に **EAP-TLS**, **EAP-TTLS**, 内部認証で使用するプロトコルを選択します。  
RADIUS サーバ証明書は**本装置の証明書を使用する**を選択し、シリアルナンバーで  
前項にて発行した RADIUS サーバ証明書を指定します。

※ EAP-TTLS を利用するには EAP-TLS も選択する必要があります

## RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの IP アドレス **192.168.0.253** を設定します。  
シークレットは無線アクセスポイントへ設定したものと同じものを入力します。

## LDAP の設定 (RADIUS/サーバ/LDAP)

LDAP 画面下段 LDAP サーバ一覧より **新規追加** を押下して LDAP サーバを追加します。  
設定条件に従い、各項目を設定します。

<LDAP1>

LDAP 名	ldap1
IP アドレス	192.168.0.10
ポート	636
ベース DN	o=ldap1, c=jp
バインド DN	cn=Manager, o=ldap1, c=jp
パスワード	secret1
フィルタオブジェクト	なし

フィルタアトリビュート	uid
セキュリティ	LDAPS
シリアルナンバ	CA にて作成したクライアント(ldap クライント)用のもの
証明書検証	検証する

## &lt;LDAP2&gt;

LDAP 名	Ldap2
IP アドレス	192.168.0.20
ポート	636
ベース DN	o=ldap2, c=jp
バインド DN	cn=Manager, o=ldap1, c=jp
パスワード	Secret2
フィルタオブジェクト	なし
フィルタアトリビュート	uid
セキュリティ	LDAPS
シリアルナンバ	CA にて作成したクライアント(ldap クライント)用のもの
証明書検証	検証する

No. は LDAP サーバの認証の順番を指定します。LDAP1, LDAP2 の順に設定する場合は空欄でかまいません。ポートは一般的に LDAP では 389、LDAPS では 636 が使われます。証明書検証で **検証する** に設定した場合は LDAP サーバの証明書が不正だった場合にその LDAP サーバを認証に使用しません。LDAP1 設定後、同様に LDAP2 の設定を追加します。

設定例：

The screenshot shows a configuration window titled "LDAP新規追加" (LDAP New Add). The settings are as follows:

- No. : [Empty]
- LDAP名 : LDAP1
- LDAPサーバ : 192.168.0.10
- ポート : 636
- ベースDN : o=ldap1,c=jp
- バインドDN : cn=Manager,o=ldap1,c=jp
- パスワード : secret1
- フィルタオブジェクト : [Empty]
- フィルタアトリビュート : uid
- セキュリティ :  None  StartTLS  LDAPS
- シリアルナンバ : 04
- 証明書検証 :  検証する  検証しない

A "設定" (Settings) button is located at the bottom right of the form.

LDAP サーバの登録が終わったら LDAP への問い合わせを有効にします。

LDAP 画面の上段より **設定・編集** ボタンを押し設定画面を開きます。LDAP を「使用する」、認証順序「LDAP → Local」を選択して設定します。



The screenshot shows the LDAP configuration interface. At the top, there is a title 'LDAP'. Below it, there are two rows of radio button options. The first row is for 'LDAP' usage, with '使用しない' (not selected) and '使用する' (selected). The second row is for '認証順序' (authentication order), with 'Local → LDAP' (selected) and 'LDAP → Local' (not selected). At the bottom center, there is an orange button labeled '設定' (Settings).

#### ユーザ基本情報プロファイルの作成 (RADIUS/プロファイル/ユーザ基本情報)

設定条件に従い 認証方式に EAP-TTLS/PAP, CHAP を指定したプロファイルを作成します。プロファイル名は **base\_user** とします。



The screenshot shows the 'ユーザ基本情報プロファイル 新規追加' (Add New User Basic Information Profile) screen. It contains several fields: 'プロフィール名' (Profile Name) is 'base\_user'; '認証方式' (Authentication Method) is 'EAP-TTLS/PAP,CHAP'; '同時接続数' (Simultaneous Connections) is empty; 'IPアドレス割り当て' (IP Address Assignment) has radio buttons for '未使用' (selected), 'RADIUSクライアント', 'アドレスプール', and '固定'; 'アドレスプール' (Address Pool) is '指定しない' (None). An orange '設定' (Settings) button is at the bottom.

#### ユーザプロファイルの作成 (RADIUS/プロファイル/ユーザプロファイル)

作成したユーザ基本プロファイル **base\_user** を選択してユーザプロファイルを作成します。プロフィール名は **user** とします。



The screenshot shows the 'ユーザプロファイル 新規追加' (Add New User Profile) screen. It contains several fields: 'プロフィール名' (Profile Name) is 'user'; '基本' (Basic) is 'base\_user'; '認証' (Authentication) is '指定しない' (None); '証明書' (Certificate) is '指定しない' (None); '応答' (Response) is '指定しない' (None); 'グループ' (Group) is '指定しない' (None). An orange '設定' (Settings) button is at the bottom.

ローカルユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **user03**、パスワードに **pass03** を入力します。  
(LDAP1 に user01、LDAP2 に user02 が存在するものとします)  
プロファイルは先ほど作成したユーザプロファイル **user** を指定します。  
入力後 **設定** ボタンを押下します。

ユーザ新規追加

ユーザID user03

パスワード ●●●●●●

プロファイル 指定しない

固定IPアドレス払い出し

IPアドレス

ネットマスク

備考

備考

アカウントのロック

ロック  ロックしない  ロックする

設定

LDAP ユーザ設定 (RADIUS/ユーザ/LDAP ユーザ)

ここでは応答アトリビュートは使用しませんので、LDAP ユーザの設定では「指定しない」を選択します。

RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

起動/停止

現在の状態 停止中

起動

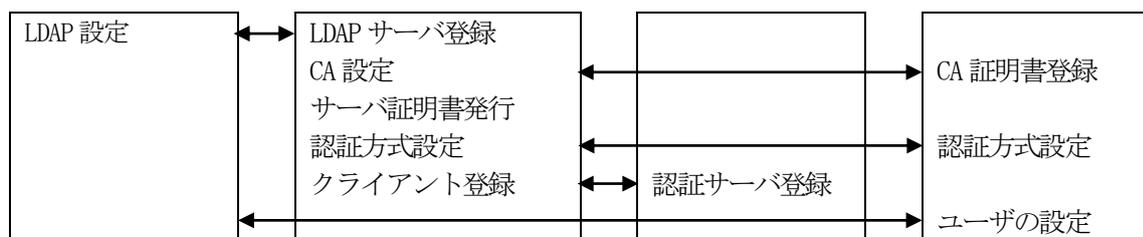
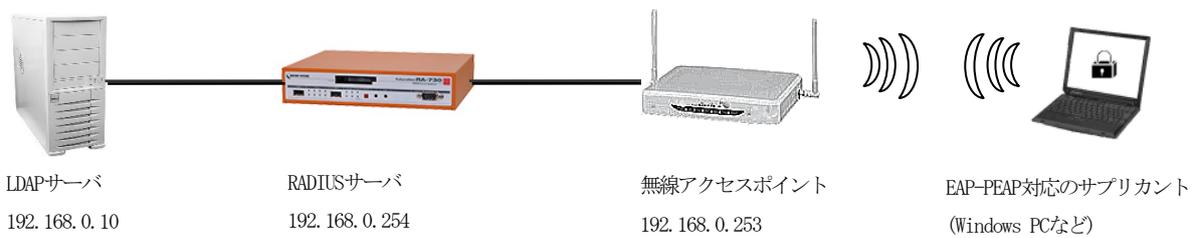
以上で設定は終了です。

### 3.3. LDAP 連携でEAP-PEAP認証を利用する

#### ■ 概要

ここではLDAP サーバに登録されているユーザでEAP-PEAP 認証を利用する例を紹介します。

#### ■ 構成



ここでは、ユーザ検索をLDAP サーバ、RADIUS サーバ ローカルの順に行います。LDAP 連携を使用するにはRADIUS サーバに対して以下設定を行います。

- CA の作成
- RADIUS サーバ証明書の発行
- 認証方式や使用ポートなどの基本設定
- RADIUS クライアント（無線アクセスポイント）の登録
- LDAP サーバの登録

## ■ 設定例

ここでは下記の内容で設定を行います。EAP-PEAP 用に証明書を発行する必要があるため設定ウィザードを使って設定する場合は「RADIUS (EAP)」を選択します。

設定条件：

<LDAP>

LDAP 名	LDAP1
IP アドレス	192.168.0.10
ポート	389
ベース DN	o=ldap1, c=jp
バインド DN	cn=Manager, o=ldap1, c=jp
パスワード	secret1
フィルタオブジェクト	なし
フィルタオブジェクト	なし
フィルタアトリビュート	uid
セキュリティ	なし

### ネットワークの設定 (管理機能/ネットワーク/基本設定)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。  
MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。  
ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS、NTP サーバを使用しないのであれば特に設定する必要はありません。



The screenshot shows a configuration window titled '基本情報' (Basic Information). It contains a table with the following data:

Interface	Property	Value	Action
Ether0	IP アドレス	192.168.0.254/24	編集
	MTU	1500	
	通信モード	Auto	
Ether1	IP アドレス	192.168.1.254/24	編集
	MTU	1500	
	通信モード	Auto	
Ether2	IP アドレス	192.168.2.254/24	編集
	MTU	1500	
	通信モード	Auto	
デフォルトゲートウェイ			編集

## CA の設定 (CA/CA/CRL)

CA の作成や証明書の発行を行う際は内蔵時計が正しく設定されているか確認することをお奨めします。CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力は必須です。例では以下の設定でCAを作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※CAの再編集はできませんので設定の際は内容を十分確認してください。  
また、CAを削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

The screenshot shows a configuration form for a CA. The fields are as follows:

- バージョン: 3
- 鍵長: 1024 (dropdown)
- Signature Algorithm: SHA-256 (dropdown)
- Subject:
  - Common Name: sample\_ca
  - email: samp@example.co.jp
  - Organizational Unit: (empty)
  - Organization: (empty)
  - Locality: (empty)
  - State or Province: (empty)
  - Country: JP
- 有効期間:
  - 終了日時: 2035 年 12 月 31 日
- パスフレーズ:
  - パスフレーズ: (masked with dots)
- 失効リスト更新間隔:
  - 失効リスト更新間隔: 365

A "設定" (Settings) button is located at the bottom right of the form.

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

設定例：

The screenshot shows the configuration for a new certificate. The '証明書' (Certificate) section is expanded, showing the following settings:

- バージョン: 3
- 鍵長: 1024
- Signature Algorithm: SHA-256
- Subject: Common Name: RA\_Server
- 有効期間: 開始日時 (empty), 終了日時: 2025年12月31日14時59分

The 'X.509証明書v3拡張 (RFC3280)' section is also expanded, showing the following settings:

- Key Usage:  digitalSignature,  keyEncipherment,  nonRepudiation,  dataEncipherment,  keyAgreement,  keyCertSign,  cRLSign,  encipherOnly,  decipherOnly
- Extended Key Usage: serverAuth
- CRL Distribution Points: (empty)

The 'Netscape拡張' section is also expanded, showing the following settings:

- nsCertType:  client,  server,  email,  objsign,  sslCA,  emailCA,  objCA
- nsComment: (empty)

At the bottom, there is a '設定' (Settings) button.

※ 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 KeyUsage 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 を必要とするかは通信相手のソフトウェアに依存します。

認証方式の設定 (RADIUS/サーバ/基本設定)

RADIUS 基本設定画面を開き認証方式として **EAP-TLS**, **EAP-PEAP** を選択します。  
RADIUS サーバ証明書は**本装置の証明書を使用する**を選択し、シリアルナンバーは前項にて発行した RADIUS サーバ証明書を指定します。(例 01)

※ EAP-PEAP を利用するには EAP-TLS も選択する必要があります

RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの IP アドレス **192.168.0.253** を設定します。  
シークレットは無線アクセスポイントへ設定したものと同じものを入力します。

クライアント新規追加	
クライアント名	AP-01
IPアドレス	192.168.0.253
シークレット	secret
アドレスグループ	指定しない
<b>設定</b>	

LDAP の設定 (RADIUS/サーバ/LDAP)

LDAP サーバ一覧 で **新規追加** を押下して LDAP サーバを追加します。  
設定条件に従い、各項目を設定します。

LDAP 名	LDAP1
IP アドレス	192.168.0.10
ポート	389
ベース DN	o=ldap1, c=jp
バインド DN	cn=Manager, o=ldap1, c=jp
パスワード	secret1
フィルタオブジェクト	なし
フィルタアトリビュート	uid
セキュリティ	なし

No. はLDAP サーバの認証の順番を指定します。

設定例：

LDAP サーバの登録が終わったらLDAP への問い合わせを有効にします。LDAP 画面の上段より **設定・編集** ボタンを押して設定画面を開きます。LDAP を「使用する」、認証順序「LDAP → Local」を選択して設定します。

#### ユーザ基本情報プロフィールの作成 (RADIUS/プロフィール/ユーザ基本情報)

今回、応答アトリビュートは使用しませんので、プロフィールは作成する必要はありません。

#### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

今回、応答アトリビュートは使用しませんので、プロフィールは作成する必要はありません。

#### LDAP ユーザ設定 (RADIUS/ユーザ/LDAP ユーザ)

応答アトリビュートは使用しませんので、LDAP ユーザの設定では「指定しない」を選択します。

## RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。



以上で設定は終了です。

以下 Ver1. 8. 4 以降の LDAP 連携について補足情報です。

PAP、EAP-TTLS/PAP に加え以下の認証方式が利用可能になりました。

- EAP-PEAP
- CHAP
- EAP-TTLS/CHAP
- EAP-MD5
- EAP-TTLS/EAP-MD5

それぞれの認証方式を利用する上で注意点などがありますので、ユーザズガイド Ver1. 8. 4 以降に記載されている”LDAP 連携機能における認証について”をご一読ください。

## 【 参考情報 】

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

```
% echo -n 'password' | iconv -f UTF-8 -t UTF-16LE | openssl dgst -md4
```

といった手順で、NTLM ハッシュを生成することが可能です。

下記に EAP-PEAP 認証方式で”csRANLMDHash”アトリビュート利用時のスキーマ例を記載いたします。

## ■Open LDAP の場合

```
attributetype ( 1.3.6.1.4.1.20376.3.389.3.1.1 NAME 'csRANLMDHash'
  DESC 'NTLM Hash'
  EQUALITY caseIgnoreIA5Match
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 {32}
  SINGLE-VALUE )

objectclass ( 1.3.6.1.4.1.20376.3.389.4.1 NAME 'csRAAttributes'
  SUP top AUXILIARY
  DESC 'Century Systems RA-Series Attributes'
  MAY ( csRANLMDHash ) )
```

上記 OID (1.3.6.1.4.1.20376.3.389.3.1.1,

1.3.6.1.4.1.20376.3.389.4.1) は、弊社で正式に割り当てを行っておりますので、このままご利用頂いても差し支えありません。

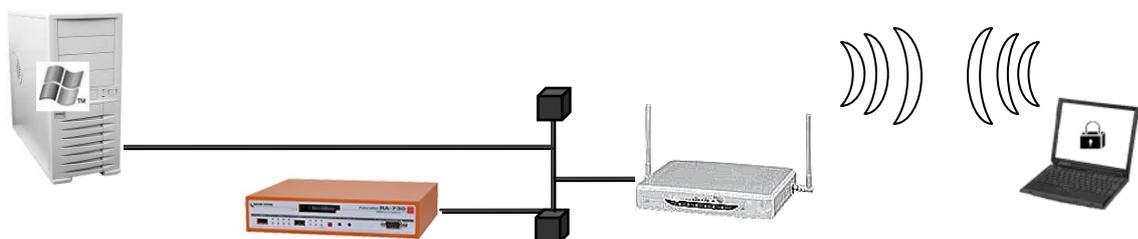
### 3.4. ActiveDirectory をLDAPとして利用する

#### ■ 概要

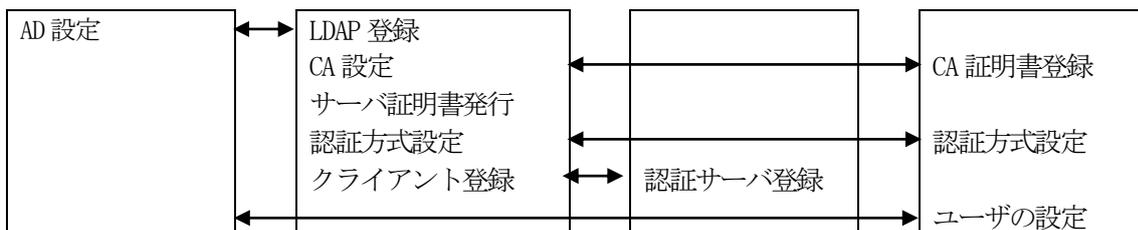
ここではActiveDirectory をLDAP として使用する例を紹介します。また LDAP ユーザプロファイルの例として応答アトリビュートでSession-Timeout を返すものとします。

※ActiveDirectory をLDAP として利用する場合の認証方式は、EAP-TTLS/PAP と PAP のみとなります。

#### ■ 構成



ActiveDirectoryサーバ ad.example.jp 192.168.0.1	RADIUSサーバ 192.168.0.254	無線AP 192.168.0.253	EAP-TTLS/PAP対応のサブクライアント (Windows PCなど)
--	----------------------------	-----------------------	---



ActiveDirectory をLDAP として使用する場合も通常のLDAP 設定と変わりません。ここでは認証方式をEAP-TTLS/PAP とし、応答アトリビュートに関わるプロファイル設定が加わります。

- CA の設定
- RADIUS サーバ証明書を発行
- 認証方式や使用ポート、アトリビュート作成などの基本設定
- RADIUS クライアントとして無線アクセスポイントを登録
- LDAP サーバの登録
- プロファイル作成
- LDAP ユーザプロファイルの設定

## ■ 設定例

ここでは下記の内容で設定を行います。設定ウィザードを使って設定する場合は「RADIUS (EAP)」を選択します。

設定条件：

ドメインコントローラホスト名	ad
ドメインコントローラ IP アドレス	192.168.0.1
Active Directory ドメイン	example.jp
ポート	389
ドメインコントローラ管理者 ID	administrator
ドメインコントローラ管理者パスワード	adminpassword
セキュリティ	なし
認証方式	EAP-TTLS/PAP
RADIUS クライアント	無線アクセスポイント (192.168.0.253)
ユーザ検索順	LDAP1 → LOCAL
応答アトリビュート	Session-Timeout 180 秒

### ネットワークの設定 (管理機能/ネットワーク/基本設定)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS、NTP サーバを使用しないのであれば特に設定する必要はありません。

基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
デフォルトゲートウェイ			<input type="button" value="編集"/>

### CA の設定 (CA/CA/CRL)

EAP-TTLS 等の証明書を必要とする認証を使用する場合は CA が必要です。

また、CA の作成や証明書の発行を行う際は内蔵時計が正しく設定されているか確認することをお奨めします。

CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要で、例では以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256

Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※ CA の再編集はできませんので設定の際は内容を十分確認してください。  
また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

The screenshot shows a configuration form for a Certificate Authority (CA). The form is titled "CA" and contains the following sections and fields:

- バージョン**: 3
- 鍵長**: 1024 (dropdown menu)
- Signature Algorithm**: SHA-256 (dropdown menu)
- Subject**:
  - Common Name: sample\_ca
  - email: samp@example.co.jp
  - Organizational Unit: (empty)
  - Organization: (empty)
  - Locality: (empty)
  - State or Province: (empty)
  - Country: JP
- 有効期間**:
  - 終了日時: 2035 年 12 月 31 日
- パスフレーズ**: (password field with 10 dots)
- 失効リスト更新間隔**: 365

A "設定" (Settings) button is located at the bottom right of the form.

### RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

設定例：

証明書

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name RA\_Server

email

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

開始日時 年 月 日 時 分

終了日時 2025年12月31日14時59分

パスフレーズ

パスフレーズ

設定

X.509証明書v3拡張 (RFC3280)

Key Usage

digitalSignature  nonRepudiation

keyEncipherment  dataEncipherment

keyAgreement  keyCertSign

cRLSign  encipherOnly

decipherOnly

Extended Key Usage serverAuth

CRL Distribution Points

Netscape拡張

nsCertType

client  server

email  objsign

sslCA  emailCA

objCA

nsComment

- Key Usage : digitalSignature およびkeyEncipherment
- Extended Key Usage : serverAuth

実際にどの Key Usage/Extended Key Usage を必要とするかは通信相手のソフトウェアに依存します。

認証方式の設定 (RADIUS/サーバ/基本設定)

認証方式に **EAP-TLS**, **EAP-TTLS** , 内部認証で使用するプロトコルを選択します。  
RADIUS サーバ証明書は**本装置の証明書を使用する**を選択し、シリアルナンバーで  
前項にて発行した RADIUS サーバ証明書を指定します。

※EAP-TTLS の利用にはEAP-TLS も選択されている必要があります。

RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの IP アドレス **192.168.0.253** を設定します。  
シークレットは無線アクセスポイントへ設定したものと同じものを入力します。

LDAP の設定 (RADIUS/サーバ/LDAP)

LDAP 画面下段 LDAP サーバ一覧より **新規追加** を押して LDAP サーバを追加します。  
設定条件に従い、各項目を設定します。

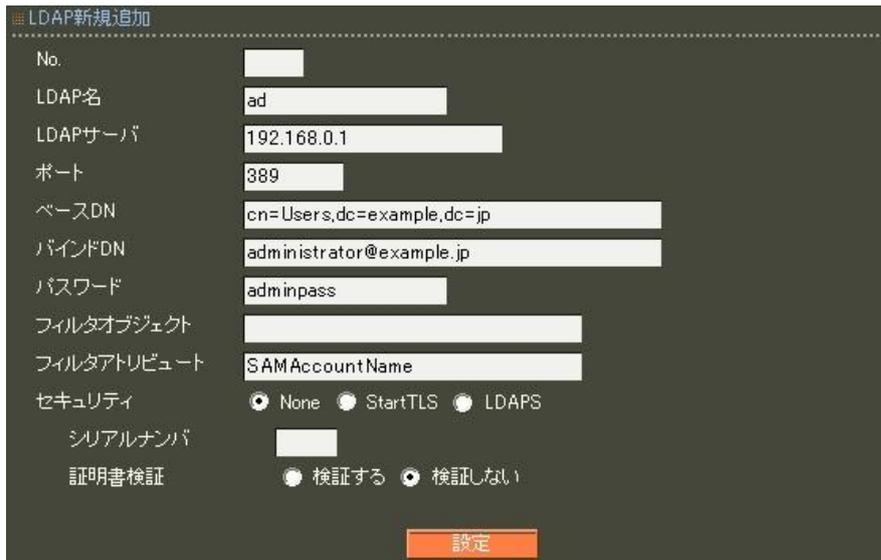
LDAP 名	ad
IP アドレス	192.168.0.1
ポート	389
ベース DN	cn=Users, dc=example, dc=jp ※1
バインド DN	administrator@example.jp
パスワード	adminpass
フィルタオブジェクト	なし

フィルタアトリビュート	sAMAccountName ※2
セキュリティ	None
証明書検証	検証しない

※1 Active Directory ドメインを要素毎に dc で指定します。

※2 Active Directory のユーザ名は User オブジェクトの sAMAccountName として保存されます。

No. は LDAP サーバの認証の順番を指定します。ここでは入力する必要はありません。ポートは一般的に LDAP では 389、LDAPS では 636 が使われます。証明書検証するに設定した場合は LDAP サーバの証明書が不正だった場合にその LDAP サーバを認証に使用しません。



LDAP新規追加

No.

LDAP名

LDAPサーバ

ポート

ベースDN

バインドDN

パスワード

フィルタオブジェクト

フィルタアトリビュート

セキュリティ  None  StartTLS  LDAPS

シリアルナンバ

証明書検証  検証する  検証しない

LDAP サーバの登録が終わったら LDAP への問い合わせを有効にします。LDAP 画面の上段より **設定・編集** ボタンを押し設定画面を開きます。LDAP を「使用する」、認証順序「LDAP → Local」を選択して設定します。



LDAP

LDAP  使用しない  使用する

認証順序  Local → LDAP  LDAP → Local

### アトリビュートの作成 (RADIUS/サーバ/アトリビュート)

ここで応答アトリビュートで返したいアトリビュートを作成します。  
本例で使用する **Sesstion-Timeout** は standard アトリビュートとして登録済みのため、今回はここで行う作業はありません。

### ユーザ基本情報プロフィールの作成 (RADIUS/プロフィール/ユーザ基本情報)

設定条件に従い 認証方式を **EAP-TTLS/PAP, CHAP** でプロフィールを作成します。  
プロフィール名は **base\_user** とします。

ユーザ基本情報プロフィール 新規追加

プロフィール名	base_user
認証方式	EAP-TTLS/PAP,CHAP
同時接続数	
IPアドレス割り当て	<input checked="" type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input type="radio"/> アドレスプール <input type="radio"/> 固定
アドレスプール	指定しない

設定

### 応答アトリビュートプロフィールの作成 (RADIUS/プロフィール/応答アトリビュート)

ここで Session-Timeout を返すため応答アトリビュートを作成します。プロフィール名は **reply** とします。作成したプロフィールは応答アトリビュート画面の下段に応答アトリビュート一覧として表示されます。一覧より **reply** プロファイルのアトリビュート欄にある **新規追加** ボタンを押してアトリビュートを追加します。アトリビュートから **Session-Timeout** を選択し、値に **180** を入力します。

設定例：

応答アトリビュートプロフィール 新規追加

プロフィール名	reply
---------	-------

設定

応答アトリビュート 新規追加

プロフィール名	reply
アトリビュート	Session-Timeout
値	180

設定

### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

作成したユーザ基本プロフィール **base\_user** と応答アトリビュートプロフィール **reply** を選択してユーザプロフィールを作成します。プロフィール名は **user** とします。

プロフィール名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	reply
グループ	指定しない

設定

### LDAP ユーザ設定 (RADIUS/ユーザ/LDAP ユーザ)

ここでLDAP ユーザに応答アトリビュートを返すプロフィールと設定します。LDAP ユーザ画面より LDAP 名 **ad** の行にある **編集** ボタンを押して LDAP ユーザ変更画面を開きます。

先ほど作成したユーザプロフィール **user** を選択して **設定** ボタンを押します。

ユーザプロフィール	user
-----------	------

設定

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

現在の状態	停止中
-------	-----

起動

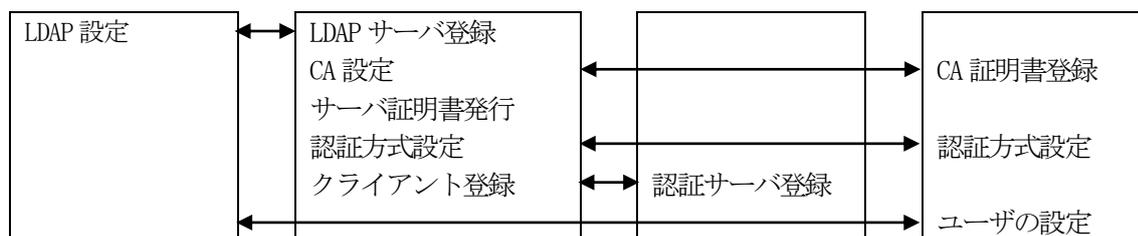
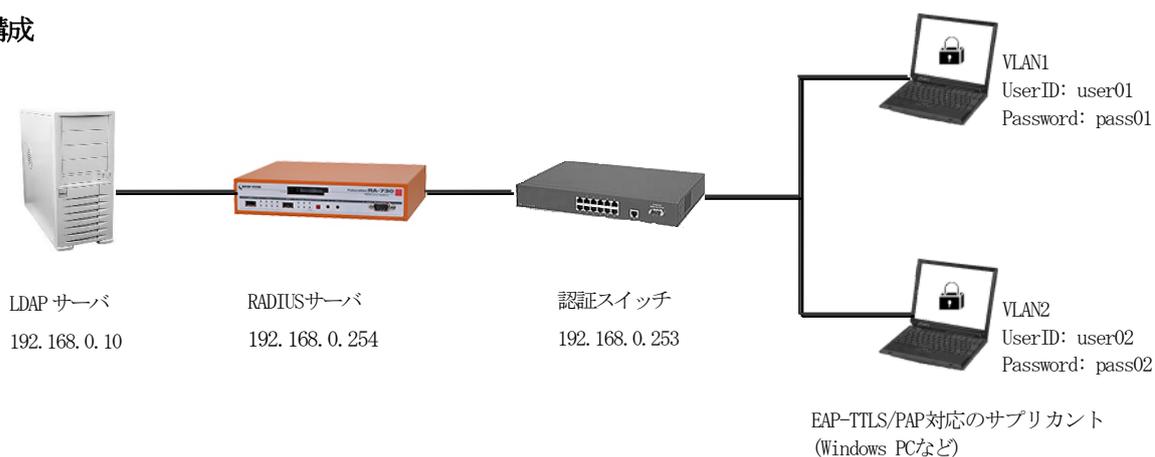
以上で設定は終了です。

## 3.5. LDAPサーバから応答アトリビュートを取得する

## ■ 概要

ここでは、LDAP サーバを用いて認証を行い、応答アトリビュートをユーザ毎に登録されている LDAP サーバより取得する方法を紹介します。

## ■ 構成



ここではLDAPサーバのみでユーザ認証を行い（ローカルにはユーザを登録しません）、VLAN情報をLDAPより取得して、認証スイッチに応答アトリビュートとして渡すために以下の設定を行います。

- CAの作成
- RADIUSサーバ証明書を発行
- 認証方式や使用ポートなどの基本設定
- RADIUSクライアント（無線アクセスポイント）を登録
- LDAPサーバの登録

## ■ 設定例

ここでは下記の内容で設定を行います。EAP-TTLS 用に証明書を発行する必要があるため設定ウィザードを使って設定する場合は「RADIUS (EAP)」を選択します。

設定条件：

LDAP 名	LDAP1
IP アドレス	192.168.0.10
ポート	389
ベース DN	o=ldap1, c=jp
バインド DN	cn=Manager, o=ldap1, c=jp
パスワード	secret1
フィルタオブジェクト	なし
フィルタアトリビュート	uid
セキュリティ	None

LDAP サーバには、「uid」、「radTunnelType」、「radTunnelMediumType」、「radTunnelPrivGroupId」がスキーマにて定義されており、既に以下の内容が登録されているものとします。

uid : user01

radTunnelType : 13	(VLAN)
radTunnelMediumType :	6 (802)
radTunnelPrivGroupId :	VLAN1

uid : user02

radTunnelType : 13	(VLAN)
radTunnelMediumType :	6 (802)
radTunnelPrivGroupId :	VLAN2

### ネットワークの設定 (管理機能/ネットワーク/基本設定)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS、NTP サーバを使用しないのであれば特に設定する必要はありません。

基本情報			
Ether0	IPアドレス	192.168.0.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether1	IPアドレス	192.168.1.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
Ether2	IPアドレス	192.168.2.254/24	
	MTU	1500	<input type="button" value="編集"/>
	通信モード	Auto	
デフォルトゲートウェイ			<input type="button" value="編集"/>

## CA の設定 (CA/CA/CRL)

CA の作成や証明書の発行を行う際は内蔵時計が正しく設定されているか確認することをお奨めします。CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力は必須です。例では以下の設定でCAを作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※CA の再編集はできませんので設定の際は内容を十分確認してください。  
また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

設定例：

The screenshot shows a configuration form for a CA. The '証明書' (Certificate) section includes fields for version (3), key length (1024), signature algorithm (SHA-256), subject (Common Name: RA\_Server), email, organizational unit, organization, locality, state or province, and country (JP). The validity period is set from 2025/12/31 14:59. The 'X.509証明書v3拡張 (RFC3280)' section has 'Key Usage' checked for 'digitalSignature' and 'keyEncipherment', and 'Extended Key Usage' set to 'serverAuth'. The 'Netscape拡張' section has 'nsCertType' set to 'server' and 'emailCA'. A '設定' (Settings) button is at the bottom.

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 KeyUsage 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 を必要とするかは通信相手のソフトウェアに依存します。

#### 認証方式の設定 (RADIUS/サーバ/基本設定)

RADIUS 基本設定画面を開き認証方式として **EAP-TLS**, **EAP-TTLS** を選択します。  
RADIUS サーバ証明書は**本装置の証明書を使用する**を選択し、シリアルナンバーで前項にて発行した RADIUS サーバ証明書を指定します。

EAP-TTLS を利用するには EAP-TLS も選択する必要があります

#### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの IP アドレス **192.168.0.253** を設定します。  
シークレットは無線アクセスポイントへ設定したものと同じものを入力します。

クライアント名	SW-01
IPアドレス	192.168.0.253
シークレット	secret
アドレスグループ	指定しない

設定

#### LDAP の設定 (RADIUS/サーバ/LDAP)

LDAP 画面の上段より **設定・編集** ボタンを押し設定画面を開きます。LDAP を「**使用する**」、認証順序「**LDAP → Local**」を選択して設定します。

LDAP	<input type="radio"/> 使用しない	<input checked="" type="radio"/> 使用する
認証順序	<input type="radio"/> Local → LDAP	<input checked="" type="radio"/> LDAP → Local

設定

LDAP 画面中段 LDAP アトリビュートマップ一覧より **新規追加** を押して RADIUS のアトリビュートと LDAP のアトリビュートの対応付けを行います。

この設定を行う事で認証が成功した場合、認証応答パケットに LDAP サーバより取得したアトリビュート値がセットされます。応答プロファイルを作成する必要がありません。

但し、LDAP サーバより取得した値以外に応答アトリビュートとして返したい場合は、応答アトリビュートプロファイルを作成する必要があります。

ここでは、設定条件に従い、以下の3つを追加します。

RADIUS アトリビュート :	Tunnel-Type
LDAP アトリビュート :	radTunnelType
RADIUS アトリビュート :	Tunnel-Medium-Type
LDAP アトリビュート :	radTunnelMediumType
RADIUS アトリビュート :	Tunnel-Private-Group-ID
LDAP アトリビュート :	radTunnelPrivGroupId

設定例 :

LDAPアトリビュートマップ新規追加

RADIUSアトリビュート: Tunnel-Type

LDAPアトリビュート: radTunnelType

設定

LDAPアトリビュートマップ新規追加

RADIUSアトリビュート: Tunnel-Medium-Type

LDAPアトリビュート: radTunnelMediumType

設定

LDAPアトリビュートマップ新規追加

RADIUSアトリビュート: Tunnel-Private-Group-ID

LDAPアトリビュート: radTunnelPrivGroup

設定

LDAP 画面下段 LDAP サーバ一覧より **新規追加** を押下して LDAP サーバを追加します。設定条件に従い、各項目を設定します。

LDAP 名	ldap1
IP アドレス	192.168.0.10
ポート	389
ベース DN	o=ldap1, c=jp
バインド DN	cn=Manager, o=ldap1, c=jp
パスワード	secret
フィルタオブジェクト	なし

フィルタアトリビュート	uid
セキュリティ	None

設定例：

LDAP新規追加

---

No.

LDAP名

LDAPサーバ

ポート

ベースDN

バインドDN

パスワード

フィルタオブジェクト

フィルタアトリビュート

セキュリティ  None  StartTLS  LDAPS

シリアルナンバ

証明書検証  検証する  検証しない

[設定](#)

全てのLDAP 設定が終了すると以下ようになります。

LDAP

LDAP	使用する
認証順序	LDAP → Local

[設定・編集](#)

---

LDAPアトリビュートマッピング一覧

RADIUSアトリビュート	LDAPアトリビュート	編集	削除
Tunnel-Type	radTunnelType	<a href="#">編集</a>	<a href="#">削除</a>
Tunnel-Medium-Type	radTunnelMediumType	<a href="#">編集</a>	<a href="#">削除</a>
Tunnel-Private-Group-ID	radTunnelPrivGroupId	<a href="#">編集</a>	<a href="#">削除</a>

[新規追加](#)

---

LDAP サーバ一覧

No.	LDAP名	編集	削除
1	LDAP1	<a href="#">編集</a>	<a href="#">削除</a>

[新規追加](#)

RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。



以上で設定は終了です。

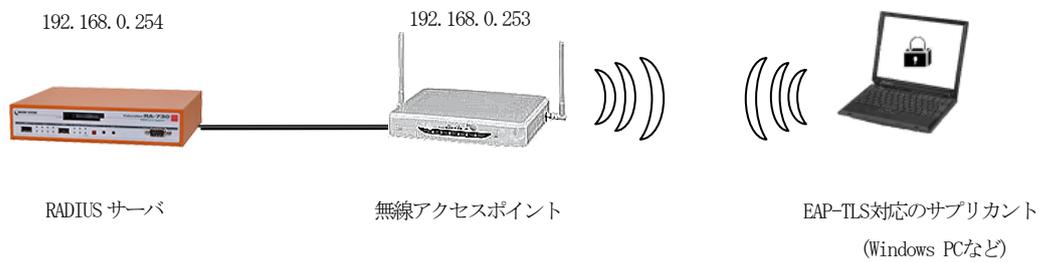
## 4. ファイル読み込み機能を利用する

### 4.1. 既存プロファイルに新規でユーザを追加する

#### ■ 概要

ここでは、GUI 操作以外にテキストファイルで作成したユーザ情報ファイルを読み込ませ、既に登録されているプロファイルに新規でユーザを登録する例を紹介します。

#### ■ 構成



本例では既に、下記内容でユーザが登録されているものとし、ここに user11 と user12 を追加します。

ユーザ基本情報プロファイル名	base_user
ユーザプロファイル名	user
ユーザ ID	user01~user05

なおテキストで作成する形式は、「設定情報の保存」で取得される内容に準じたものになっています。詳細については、ユーザズガイドの付録[ユーザ設定情報のファイルフォーマット]をご参照ください。

**【ユーザセクション記述例】**

既に必要となるプロファイル類は登録済みですので、ユーザセクションのみを記述します。

```
[RADIUS|ユーザ]
create user
  config_id=
  user_id=user11
  password=pass11
  profile=user
  locked=off
  ipaddress=
  netmask=
  notes=

create user
  config_id=
  user_id=user12
  password=pass12
  profile=user
  locked=off
  ipaddress=
  netmask=
  notes=
```

**【ユーザの登録】**

メニューより「RADIUS」－「ユーザ」－「ファイル読み込み」から RADIUS ユーザファイル読み込み画面を開きます。リセットは“しない”、設定ファイルにこれまでに作成した設定ファイルを指定して、  
**復帰** ボタンを押下します。



以上で新しいユーザの登録が行なわれます。

**ファイル読み込みのリセットについて**

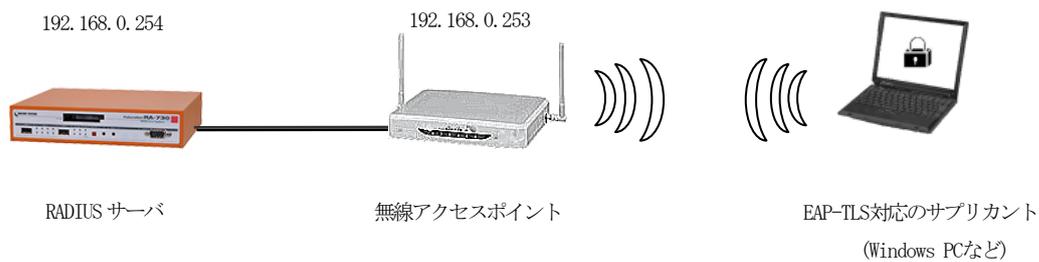
リセットで「する」を選択すると登録されているプロファイル、ユーザをリセット(削除)した上で新規にユーザ登録を行います。そのため上記記述以外にプロファイルセクションを指定する必要があります。リセットで「しない」を選択すると既存の設定のままユーザのみが追加されます。

## 4.2. 新規でユーザプロフィールとユーザを登録する

## ■ 概要

ここでは、GUI 操作以外にテキストファイルで作成したユーザ情報ファイルを読み込ませ、新規でユーザプロフィールとユーザを登録する例を紹介します。

## ■ 構成



本例では既に、下記内容でユーザが登録されているものとし、新たにユーザプロフィール user2 とそれに所属するユーザ user21 と user22 を登録します。

ユーザ基本情報プロフィール名	base_user
証明書プロフィール名	cert
ユーザプロフィール名	user
ユーザ ID	user01~user05

なおテキストで作成する形式は、「設定情報の保存」で取得される内容に準じたものになっています。詳細については、ユーザズガイドの付録[ユーザ設定情報のファイルフォーマット]をご参照ください。

**【ユーザプロフィール、ユーザセクション記述例】**

既に必要となるユーザ基本情報プロフィール等は登録済みですので、登録するユーザプロフィールとユーザセクションを記述します。

```
[RADIUS|プロフィール|ユーザプロフィール]
```

```
create userprofile
  config_id=
  profile_name=user2
  base=base_user
  auth=
  cert=cert
  resp=
  group=
```

```
[RADIUS|ユーザ]
```

```
create user
  config_id=
  user_id=user21
  password=pass21
  profile=user2
  locked=off
  ipaddress=
  netmask=
  notes=
```

```
create user
  config_id=
  user_id=user22
  password=pass22
  profile=user2
  locked=off
  ipaddress=
  netmask=
  notes=
```

### 【ユーザの登録】

メニューより「RADIUS」－「ユーザ」－「ファイル読み込み」から RADIUS ユーザファイル読み込み画面を開きます。リセットは“しない”、設定ファイルにこれまでに作成した設定ファイルを指定して、

**復帰** ボタンを押下します。



以上で新しいユーザの登録が行なわれます。

### ファイル読み込みのリセットについて

リセットで「する」を選択すると登録されているプロファイル、ユーザをリセット(削除)した上で新規にユーザ登録を行います。そのため上記記述以外にリセット(削除)したプロファイルセクションおよびそれに所属するユーザを指定する必要があります。

リセットで「しない」を選択すると既存の設定のまま新規で登録するプロファイル、ユーザが追加されます。

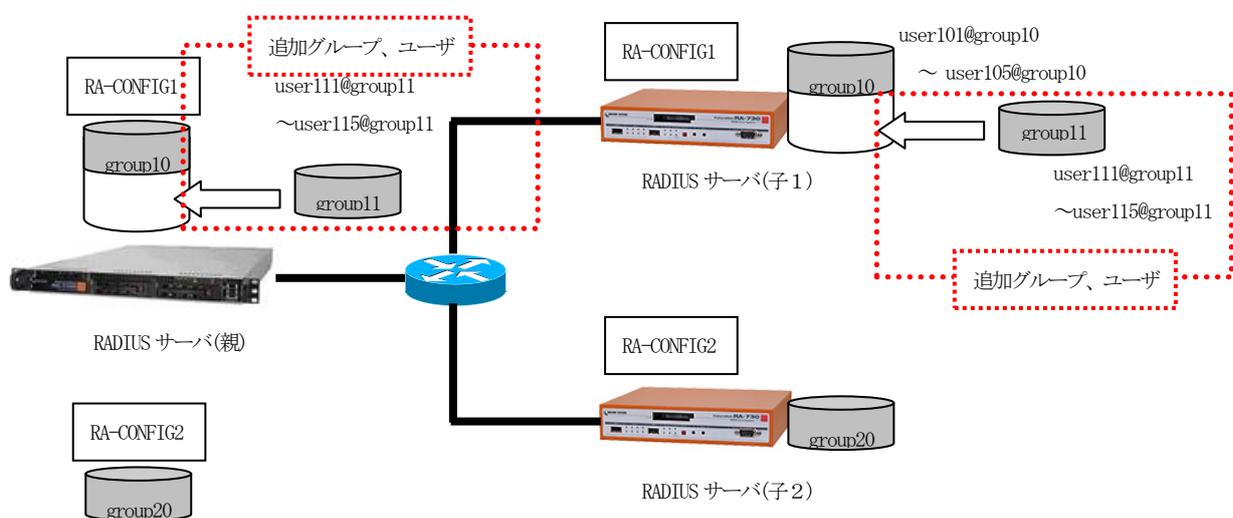
## 4.3. 証明書を発行する

## ■ 概要

ここでは、親子連携の構成を利用し、ユーザの登録とそのユーザ証明書を発行する例を紹介します。

## ■ 構成

本例では既に EAP-TLS 認証を用いて user101@group10 ~ user105@group10 というグループ ID のユーザが” RA-CONFIG1” コンフィグに既に登録済みで、新たに user111@group11 ~ user115@group11 というグループ ID のユーザを追加し証明書を発行します。



## 設定条件

コンフィグ名 (※)	RA-CONFIG1
ユーザ名	user111~user115
ユーザプロファイル名	userprof11
グループプロファイル名	realm11
グループ ID	group11
形式	UserID@GroupID
認証方式	EAP-TLS
証明書	
バージョン	3
鍵長	1024
Signature Algorithm	SHA-256
Key Usage	keyEncipherment
Extended Key Usage	clientAuth
ファイル読み込み時の動作	追加

※親子連携時、1 台の親と 1 台の子で共有されるコンフィグの名称

ユーザ user101~user105@group10 は既に下記内容で登録済みとします。

ユーザ基本プロフィール名	base1
ユーザプロフィール名	userprof10
グループ ID プロファイル名	realm10

ユーザなどの作成と証明書の発行は、それぞれ別の設定ファイルを作成(※)し、親機の「RADIUS/ユーザ/ファイル読み込み」から設定ファイルを読み込み、強制同期機能により親から子へ反映させます。読み込むファイルの形式は「設定の保存」で得られるファイルに準じたものになっています。

※ユーザなどの作成と、ユーザ証明書の発行を1つのファイルにして読み込ませる事はできません。

## ■ 設定例

### (1) プロファイルの作成

グループ ID の指定を行うためプロファイルの作成に関する記述を行います。

既存のプロファイルを用いてユーザを作成する場合は必要ありません。

グループ ID の作成は[RADIUS|プロファイル|グループ ID]セクションで指定します。

### グループ ID プロファイルセクション記述例

```
[RADIUS|プロファイル|グループ ID]
create group
  config_id=RA-CONFIG1
  profile_name=realm11
  group_id=group11
  format=
```

グループ ID プロファイルセクションにて config\_id にコンフィグ名 **RA-CONFIG1**、profile\_name に既存のプロファイルと重複しない名前を指定します。ここでは **realm11** とします。group\_id にグループ ID の **group11** を指定します。format は UserID@GroupID 形式なので指定する必要はありません。

次に先ほど作成したグループ ID プロファイルを指定するユーザプロファイルを作成します。ユーザプロファイルの作成は[RADIUS|プロファイル|ユーザプロファイル]セクションで指定します。

#### ユーザプロファイルセクション記述例

```
[RADIUS|プロファイル|ユーザプロファイル]
create userprofile
  config_id=RA-CONFIG1
  profile_name=userprof11
  base=base1
  auth=
  cert=
  resp=
  group=realm11
```

EAP-TLS 認証を指定しているユーザ基本プロファイルはすでに登録済みのbase1 を指定するものとします。config\_id にコンフィグ名 **RA-CONFIG1**、profile\_name は既存のプロファイルと重複しない名前を指定します。ここでは **userprof11** とします。ユーザ基本プロファイルは **base1**、グループ ID は **realm11** をそれぞれ指定します。

以上でプロファイルの作成は終了です。

## (2) ユーザの作成

続いてユーザの作成を行います。ユーザの作成は [RADIUS|ユーザ]セクションで行います。config\_id にコンフィグ名 **RA-CONFIG1**、user\_id に作成するユーザ ID、password にパスワード、profile に先ほどのユーザプロファイル **userprof11** を指定します。ここに作成するユーザ全てについて記述します。

## ユーザセクション記述例

```
[RADIUS|ユーザ]
create user
  config_id=RA-CONFIG1
  user_id=user111
  password=user111pass
  profile=userprof11
  locked=off
  ipaddress=
  netmask=
  notes=

create user
  config_id=RA-CONFIG1
  user_id=user112
  password=user112pass
  profile=userprof11
  locked=off
  ipaddress=
  netmask=
  notes=
  :
  :

create user
  config_id=RA-CONFIG1
  user_id=user115
  password=user115pass
  profile=userprof11
  locked=off
  ipaddress=
  netmask=
  notes=
```

既存のユーザと重複したユーザ ID を指定することはできませんので、内容に誤りがないか確認ください。

## (3) 証明書の発行

証明書の発行は [RADIUS|ユーザ|証明書発行] セクションで行います。証明書発行セクションもユーザの作成と同様に証明書を発行したいユーザ数分記述します。

## 証明書発行セクション記述例

```
[RADIUS|ユーザ|証明書発行]
create cert
  user=user111@group11
  config_id=RA-CONFIG1
  passphrase=user111@group11pass
  version=3
  key_length=1024
  sign_algorithm=SHA-1
  subject_email=
  subject_cn=user111@group11
  subject_ou=
  subject_o=
  subject_l=
  subject_s=
  subject_c=JP
  not_before_year=
  not_before_month=
  not_before_day=
  not_before_hour=
  not_before_min=
  not_after_year=2020
  not_after_month=12
  not_after_day=31
  not_after_hour=14
  not_after_min=59
  digitalSignature=on
  nonRepudiation=
  keyEncipherment=
  dataEncipherment=
  keyAgreement=
  keyCertSign=
  cRLSign=
  encipherOnly=
  decipherOnly=
  ExtendedKeyUsage=clientAuth
  CRLDistributionPoints=
  csr=

create cert
  user=user112@group11
```

### 【ユーザの登録／証明書発行】

ユーザの追加は、(1) と (2) の記述をまとめたファイルを作成、また証明書発行は、(3) の内容を別のファイルに保存します。

親子連携構の場合は、以下操作を親機で行います。

メニューの「RADIUS」－「ユーザ」－「ファイル読み込み」から RADIUS ユーザファイル読み込み画面を開きます。リセットは **しない**、設定ファイルにこれまでに作成した設定ファイルを指定し、適用するコンフィグ名を選択して、**復帰** ボタンを押下します。  
以上で新しいユーザの追加、証明書の発行が行なわれます。



発行された証明書は、証明書画面から取り出しを行い、パスフレーズを使用してサブクライアントへ設定します

#### ファイル読み込みのリセットについて

リセットで「する」を選択すると登録されているプロファイル、ユーザをリセット(削除)した上で新規に登録を行います。そのため上記記述以外にリセット(削除)したプロファイルセクションおよびそれに所属するユーザを指定する必要があります。

リセットで「しない」を選択すると既存の設定のまま新規で登録するプロファイル、ユーザが追加されます。

最後に親に追加した内容を子側へ反映させます。この操作も親機で行います。

メニューの「管理機能」－「システム」－「設定情報の同期」画面を開きます。

同期実行 一覧より更新対象のコンフィグ名欄の強制同期 **実行** ボタンを押下します。

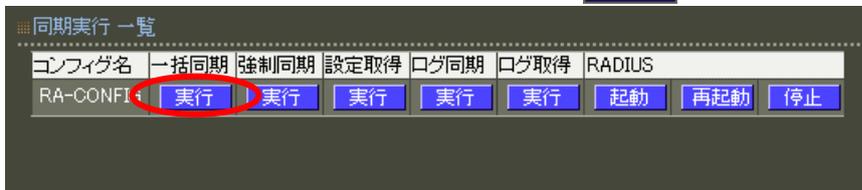


※ 同期処理中の子側では認証/アカウント処理を行う事はできません。

(補足)

- ・親子連携以外の構成では、各セクションの config\_id 値を指定する必要はありません。
- ・親子連携以外の同期構成において、[同期コンフィグ]設定で **即時実行** を指定している場合は強制同期を行う必要はありません。逐次対向機器へ同期されます。

一括処理 を選択している場合は、一括同期 **実行** ボタンを押下します。



以上で設定は終了です。

## 5. 認証プロファイル/応答プロファイルを利用する

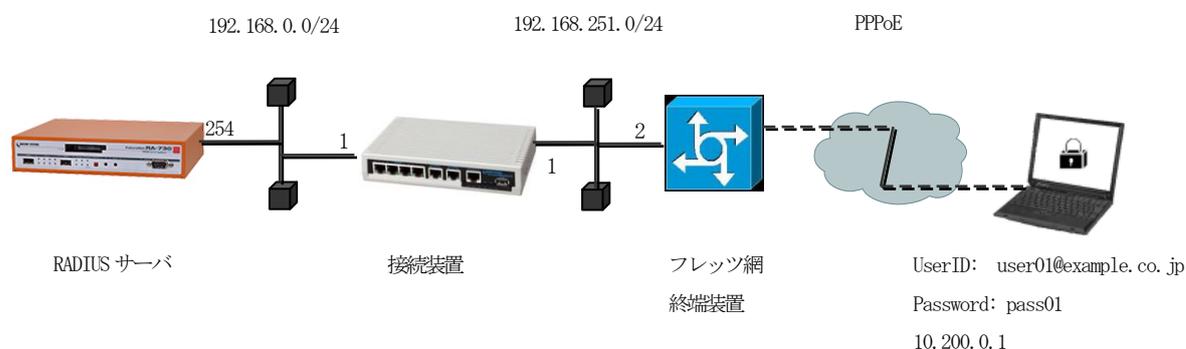
### 5.1. フレッツナンバーアシストを利用する

#### ■ 概要

ここではNTT 地域会社により提供されているフレッツ・オフィス/フレッツ・オフィスワイドサービス環境の認証サーバとして使用し、NTT 東日本様提供のフレッツナンバーアシストサービスを利用する例を紹介します。この設定により、ユーザ ID、パスワード、フレッツナンバー(※)で認証の可否を行う事ができます。

※契約のフレッツ・アクセスサービス毎に固有に割り当てられている情報

#### ■ 構成



#### ■ 設定例

ここでは[1.1. PAP/CHAP 認証を利用する]で紹介した内容が既に設定されている事を前提として、フレッツナンバーアシストサービスを利用するための追加設定について説明いたします。

設定は、(1) 認証プロファイルを利用して設定する方法 と (2) ユーザ毎に設定する方法の2つがあります。認証プロファイルに設定するとそのプロファイルを使用する全てのユーザに適用されます。環境に応じてご利用ください。

設定条件：

ユーザ ID	user01
パスワード	pass01
認証プロファイル名	auth
フレッツナンバー	COP12345678

## (1) 認証プロファイルを利用して設定する方法

### 認証アトリビュート設定 (RADIUS/プロファイル/認証アトリビュート)

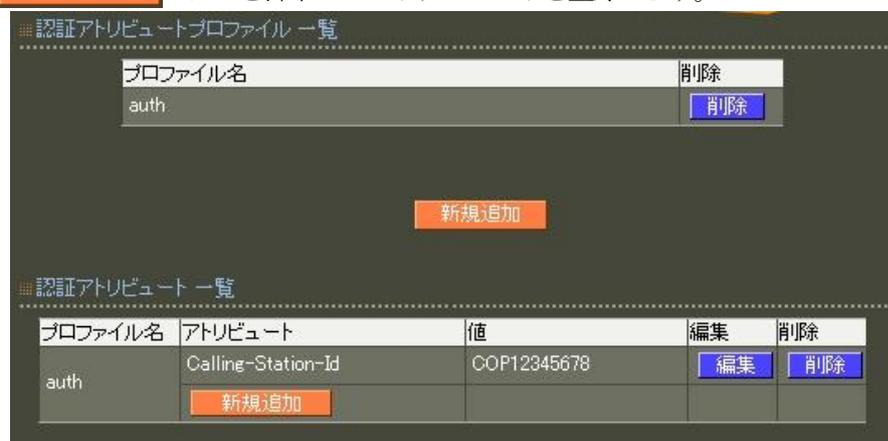
網側より通知されるフレッツナンバーを認証アトリビュートプロファイルに登録を行います。

認証アトリビュート画面を開き認証アトリビュートプロファイル一覧にある **新規追加** ボタンを押下します。

認証アトリビュートプロファイル 新規追加でプロファイル名 **auth** と入力、**設定** ボタンを押下して、プロファイルに登録します。

認証アトリビュート一覧にある **新規追加** ボタンを押下します。

アトリビュートのプルダウンメニューより、Calling-Station-Id を選択後、値に **COP12345678** を指定し、**設定** ボタンを押下してアトリビュートを登録します。



### ユーザ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)

ここでは、ユーザで使用するユーザプロファイルに前項で作成した認証アトリビュートプロファイルを指定します。ユーザプロファイル画面を開き、編集するユーザプロファイルの **編集** ボタンを押下します。認証欄のプルダウンメニューより、先ほど作成したプロファイル **auth** を選択して、**設定** ボタンを押下します。



以上で設定は、終了です。

## (2) ユーザ毎に設定する方法

### ユーザ設定 (RADIUS/ユーザ/ユーザ)

網側より通知されるフレッツナンバーを既存 user01 ユーザの認証アトリビュートとして登録を行います。  
 ユーザー一覧より詳細欄にある **表示** ボタンを押下します。

認証欄の **新規追加** ボタンを押下し、下記内容を指定後、**設定** ボタンを押下します。

- ・アトリビュート：プルダウンメニューより **Calling-Station-Id** を選択
- ・値：**COP12345678** を指定
- ・動作モード：プルダウンメニューより **上書き** を選択

The screenshot shows a web-based configuration interface for a user. The main section is titled "ユーザ設定" (User Settings) and contains the following fields:

ユーザID	user01
プロフィール	user
IPアドレス	10.200.0.1
ネットマスク	255.255.255.0
備考	
ロック	ロックしない

Below these fields are three buttons: "編集" (Edit), "削除" (Delete), and "ユーザー一覧" (User List).

The detailed view section, "ユーザ設定 (詳細)" (User Settings (Details)), is expanded to show the following sections:

- ユーザプロフィール** (User Profile): user
- 基本** (Basic): base\_user (with "編集" button)
- 認証** (Authentication):
 

認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	未使用
アドレスプール	
- 応答** (Response): reply
 

Calling-Station-Id	COP12345678 (上書き)	"編集" button	"削除" button
"新規追加" button			
- グループ** (Group): group
- 証明書** (Certificate):

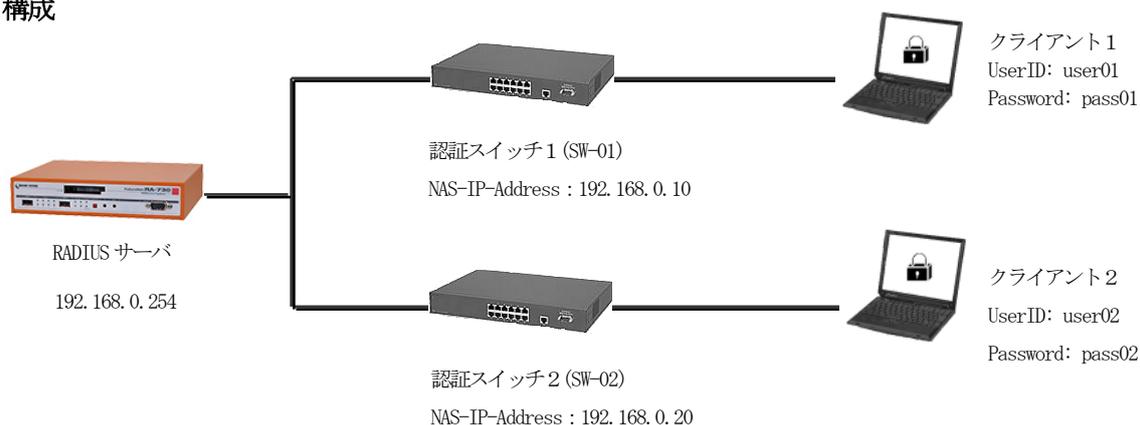
以上で設定は終了です。

## 5.2. 認証スイッチ毎に接続可能なユーザを限定する

## ■ 概要

ここでは認証アトリビュートプロファイルを用いて認証スイッチ毎に接続可能なユーザを限定する例を紹介します。

## ■ 構成



## ■ 設定例

認証スイッチ単位でユーザを識別するには、どの認証スイッチからの認証要求なのかを識別するための情報を追加する必要があります。このように認証時に使う情報は、認証アトリビュートプロファイルを用います。また認証アトリビュートプロファイルでは、認証スイッチの識別に利用する認証アトリビュートを指定し、ユーザプロファイルに認証アトリビュートプロファイルを登録します。ここでは認証アトリビュートに NAS-IP-Address を使います。

設定条件：

RADIUS サーバの IP アドレス		192.168.0.254 (Ether0)
認証スイッチ 1	クライアント名	SW-01
	IP アドレス	192.168.0.10
	シークレット	secret1
認証スイッチ 2	クライアント名	SW-02
	IP アドレス	192.168.0.20
	シークレット	secret2
ユーザ ID/パスワード		user01/pass01 user02/pass02
認証方式		EAP-PEAP

※この設定例では、[1.4. EAP-PEAP 認証を利用する]で紹介した設定が行われている前提で、当設定に必要な箇所のみ記載しております。

## クライアントの登録 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして認証スイッチの情報を設定します。

ここでは、設定条件に沿って下記設定を行います。

IP アドレスは認証スイッチの IP アドレス、シークレットは認証スイッチに設定したものと同一ものを設定します。




クライアント名	IPアドレス	アドレスプール	編集	削除
SW-01	192.168.0.10		編集	削除
SW-02	192.168.0.20		編集	削除

## 認証アトリビュートプロファイルの登録 (RADIUS/プロファイル/認証アトリビュート)

ここで認証スイッチを識別するために利用する認証アトリビュートを登録します。

まず画面上段の **新規追加** を押下して認証アトリビュートプロファイルを作成します。認証アトリビュートプロファイルは認証スイッチの数分作成します。

それぞれのプロファイル名を **sw1attr**、**sw2attr** とします。

続いて認証アトリビュート一覧の **新規追加** ボタンを押下してアトリビュートを追加します。

### アトリビュートの追加



プロファイル名	アトリビュート	値	編集	削除
sw1attr	NAS-IP-Address	192.168.0.10	編集	削除
sw2attr				

認証アトリビュート新規追加画面ではアトリビュートから NAS-IP-Address を選択し、値として sw1attr の値には認証スイッチ1の IP アドレス 192.168.0.10、sw2attr の値には認証スイッチ2の IP アドレス 192.168.0.20 を設定します。

プロファイル名	sw2attr
アトリビュート	NAS-IP-Address
値	192.168.0.20

設定

#### ユーザプロファイルの登録 (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も認証スイッチの数だけ作成します。

ここでは認証スイッチ1用にユーザ基本情報プロファイル **base\_user**、認証アトリビュートプロファイル **sw1attr** を選択したユーザプロファイル **sw1user** を、認証スイッチ2用に同じくユーザ基本情報プロファイル **base\_user**、認証アトリビュートプロファイル **sw2attr** を選択した **sw2user** を作成します。

#### 認証スイッチ1用ユーザプロファイル作成

プロファイル名	sw1user
基本	base_user
認証	sw1attr
証明書	指定しない
応答	指定しない
グループ	指定しない

#### ユーザの登録 (RADIUS/ユーザ/ユーザ)

作成したユーザプロファイルを該当するスイッチで認証させたいユーザに適用します。

認証スイッチ1のユーザは、ユーザプロファイル **sw1user** を、認証スイッチ2のユーザは **sw2user** を選択してユーザを作成します。

#### 認証スイッチ1用ユーザ作成

ユーザID	user01
パスワード	●●●●●●
プロファイル	sw1user

固定IPアドレス払い出し

IPアドレス	
ネットマスク	

備考

備考	
----	--

アカウントのロック

ロック  ロックしない  ロックする



No.	lock	ユーザID	プロファイル	IPアドレス	詳細	証明書	備考
1		user01	sw1user	-	表示	発行	
2		user02	sw2user	-	表示	発行	

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。



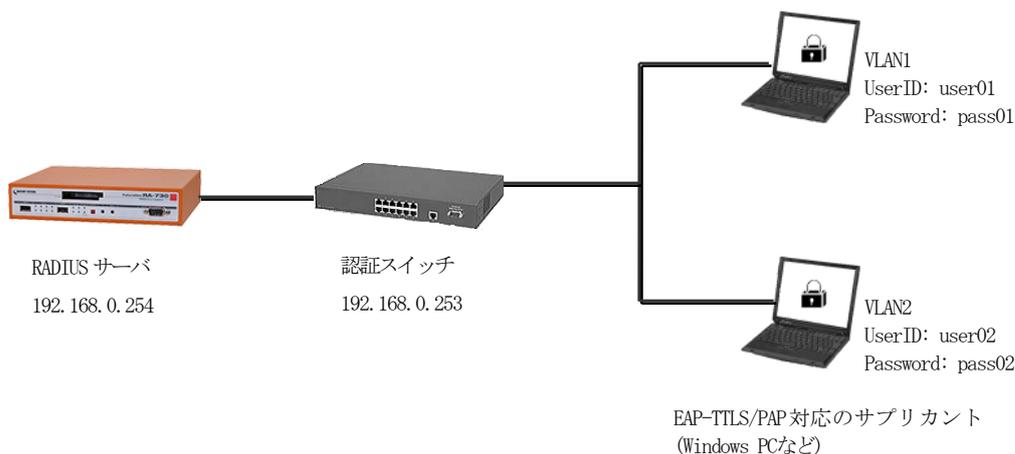
以上で設定は終了です。

## 5.3. ユーザ毎にVLAN IDを設定する

## ■ 概要

ここでは応答アトリビュートプロファイルを用いて認証スイッチへユーザ毎にVLAN IDを指定する例を紹介します。

## ■ 構成



## ■ 設定例

応答アトリビュートは、認証されたユーザに対して送信されます。

応答アトリビュートを使用するには応答アトリビュートプロファイルを作成し、ユーザプロファイルに作成した応答アトリビュートプロファイルを登録します。

ここではVLANの指定に下記アトリビュートを使用します。

設定条件：

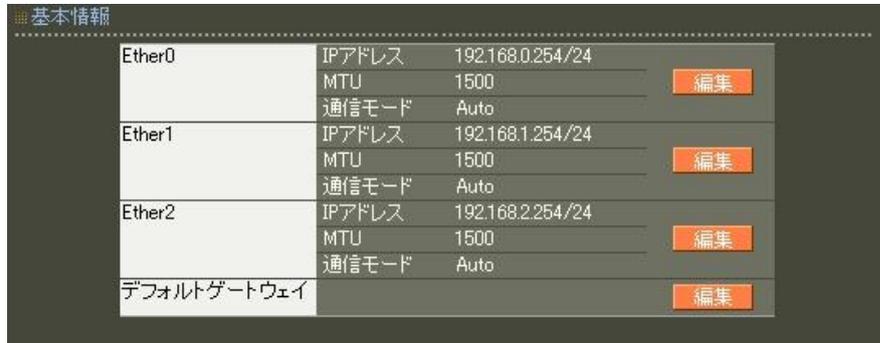
RADIUS サーバの IP アドレス		192.168.0.254 (Ether0)	
認証スイッチの IP アドレス		192.168.0.253	
認証スイッチのシークレット		secret	
ユーザ ID	パスワード	user01	pass01
	Tunnel-Type		13 (VLAN)
	Tunnel-Medium-Type		6 (802)
	Tunnel-Private-Group-ID		VLAN1 or VLAN2
ユーザ ID	パスワード	user02	pass02
	Tunnel-Type		13 (VLAN)
	Tunnel-Medium-Type		6 (802)
	Tunnel-Private-Group-ID		VLAN2
認証方式		EAP-PEAP	
認証/アカウントングポート		1812/1813	

## ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.254/24** に設定します。

MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。

ここでは初期値のままとします。デフォルトゲートウェイは外部の DNS や NTP サーバを使用しないのであれば特に設定する必要はありません。



## CA の設定 (CA/CA/CRL)

EAP-PEAP 認証を使用する場合は CA の設定が必要になります。

CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているかご確認ください。

CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要です。

ここでは以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※CA の再編集はできませんので設定の際は内容を十分確認してください。

また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name sample\_ca

email samp@example.co.jp

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035 年 12 月 31 日

パスフレーズ

失効リスト更新間隔

失効リスト更新間隔 365

設定

CA 作成後は、CA 証明書画面より **取り出し** ボタンを押下して CA 証明書を取得し、サブリカントへインストールします。

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下して追加します。

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。

但し、実際にどの **Key Usage/Extended Key Usage** を必要とするかは通信相手のソフトウェアに依存します。

- **Key Usage** : digitalSignature および keyEncipherment
- **Extended Key Usage** : serverAuth

The screenshot shows the configuration interface for a RADIUS server certificate. The '証明書' (Certificate) section is expanded, showing the following settings:

- バージョン: 3
- 鍵長: 1024
- Signature Algorithm: SHA-256
- Subject: Common Name: RA\_Server, Country: JP
- 有効期間: 開始日時: [ ]年[ ]月[ ]日[ ]時[ ]分, 終了日時: 2025年12月31日14時59分
- パスフレーズ: [ ]

The 'X.509証明書v3拡張 (RFC3280)' section is also expanded, showing the following settings:

- Key Usage:  digitalSignature,  keyEncipherment,  nonRepudiation,  dataEncipherment,  keyAgreement,  keyCertSign,  cRLSign,  encipherOnly,  decipherOnly
- Extended Key Usage: serverAuth
- CRL Distribution Points: [ ]

The 'Netscape拡張' section is also expanded, showing the following settings:

- nsCertType:  client,  server,  email,  objsign,  sslCA,  emailCA,  objCA
- nsComment: [ ]

A '設定' (Settings) button is located at the bottom of the form.

### 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**、**EAP-PEAP**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。EAP-PEAP を使用するには EAP-TLS も選択する必要があります。

シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバは CA の証明書一覧で確認することができます。また、設定ウィザードを使った場合は自動的に入力されます。なおポート番号は、RADIUS クライアントの設定と同一になるよう指定します。

The screenshot shows a configuration interface for RADIUS server certificates. It is divided into two main sections: 'ポート番号' (Port Number) and 'RADIUSサーバ証明書' (RADIUS Server Certificate). Under 'ポート番号', there are radio buttons for '1645/1646', '1812/1813', '1645/1646と1812/1813', and '手動設定'. Below these are input fields for '認証用' and 'アカウント用'. The 'RADIUSサーバ証明書' section has radio buttons for '使用しない' and '本装置の証明書を使用する', with the latter selected. A 'シリアルナンバ' (Serial Number) input field contains '01'. At the bottom, there is a '設定' (Settings) button.

### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして認証スイッチの情報を設定します。

ここでは、設定条件に沿って下記設定を行います。

IP アドレスは認証スイッチの IP アドレス、シークレットは認証スイッチに設定したものと同一ものを設定します。

The screenshot shows a configuration interface for adding a new RADIUS client. The title is 'クライアント新規追加'. It contains four input fields: 'クライアント名' (Client Name) with 'SW-01', 'IPアドレス' (IP Address) with '192.168.0.253', 'シークレット' (Secret) with 'secret', and 'アドレスグループ' (Address Group) with a dropdown menu set to '指定しない'. A '設定' (Settings) button is located at the bottom.

## ユーザ基本情報プロファイルの作成 (RADIUS/プロファイル/ユーザ基本情報)

設定条件に従い 認証方式に **EAP-PEAP** を設定します。プロファイル名は **base\_user** とします。

ユーザ基本情報プロファイル 新規追加

プロファイル名: base\_user

認証方式: EAP-PEAP

同時接続数:

IPアドレス割り当て:  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール: 指定しない

設定

## 応答アトリビュートプロファイルの登録 (RADIUS/プロファイル/応答アトリビュート)

ここでVLAN ID を認証スイッチへ送信するための応答アトリビュートを登録します。まず応答アトリビュートプロファイル一覧の **新規追加** を押下して応答アトリビュートプロファイルを作成します。ここでは VLAN1, VLAN2 それぞれに対応するプロファイル名を **vlan1, vlan2** として2つ作成します。VLAN が複数ある場合はその数分作成します。

※後述する[7.1 アトリビュートをユーザ毎に設定]では、ユーザ毎に異なるアトリビュートをユーザの個別設定で設定する例を紹介しています。

続いて応答アトリビュート一覧の **新規追加** を押下してアトリビュートを追加します。応答アトリビュート新規追加画面では Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-ID の各アトリビュートを追加します。

アトリビュート **Tunnel-Type** の値は **13**、アトリビュート **Tunnel-Medium-Type** の値は **6**、アトリビュート **Tunnel-Private-Group-ID** の値は各 VLAN ID にあわせてプロファイルvlan1 では **VLAN1**、vlan2 では **VLAN2** とします。

応答アトリビュートプロファイル一覧

プロファイル名	削除
vlan1	削除
vlan2	削除

新規追加

応答アトリビュート一覧

プロファイル名	アトリビュート	値	編集	削除
vlan1	Tunnel-Type	13	編集	削除
	Tunnel-Medium-Type	6	編集	削除
	Tunnel-Private-Group-ID	VLAN1	編集	削除
新規追加				
vlan2	Tunnel-Type	13	編集	削除
	Tunnel-Medium-Type	6	編集	削除
	Tunnel-Private-Group-ID	VLAN2	編集	削除
新規追加				

ユーザプロファイルの登録 (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も VLAN の数だけ作成します。

それぞれのユーザに該当する VLAN の応答アトリビュートプロファイルを指定します。ここでは VLAN1 用にユーザ基本情報プロファイル **base\_user**、応答アトリビュートプロファイル **vlan1** を選択したユーザプロファイル **vlan1user** を、VLAN2 用に同じくユーザ基本情報プロファイル **base\_user**、応答アトリビュートプロファイル **vlan2** を選択した **vlan2user** を作成します。

ユーザプロファイル	プロファイル名	基本	認証	応答	グループ	証明書	編集	削除
	vlan1user	base_user		vlan1			編集	削除
	vlan2user	base_user		vlan2			編集	削除

ユーザの登録 (RADIUS/ユーザ/ユーザ)

あとは VLAN1 に属するユーザ、つまり応答アトリビュートで VLAN ID として VLAN1 を返したいユーザは **vlan1user** のユーザプロファイルを、VLAN2 を返したいユーザは **vlan2user** のユーザプロファイルを選択してユーザを作成します。

ユーザ							
No.	lock	ユーザID	プロファイル	IPアドレス	詳細	証明書	備考
1		user01	vlan1user	-	表示	発行	
2		user02	vlan2user	-	表示	発行	

RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。



以上で設定は終了です。

## 6. IPアドレスの払い出しを設定する

### 6.1. アドレスプール機能を利用する

#### ■ 概要

ここではフレッツ網を利用した PPPoE 接続時に RADIUS サーバで設定したアドレスプールより IP アドレスの払い出しを行う例を紹介します。

#### ■ 構成



#### ■ 設定例

アドレスプールから IP アドレスを払い出すには、以下の 2 つの方法があります。  
いずれの場合もアドレスプールを作成し、IP アドレスの割り当て方法としてアドレスプールを選択します。

- (1) ユーザ基本プロファイルで指定する方法
- (2) RADIUS クライアントで指定する方法

ここでは下記の内容で設定を行います。

設定条件：

アドレスプール名	pool
開始 IP アドレス	10.10.10.1
終了 IP アドレス	10.10.10.50
ネットマスク	255.255.255.0

## アドレスプールの作成 (RADIUS/サーバ/アドレスプール)

設定条件に従い、アドレスプール名、開始IPアドレス、終了IPアドレス、ネットマスクの各項目を設定して **設定** ボタンを押下します。

アドレスプール新規追加	
アドレスプール名	pool
開始IPアドレス	10.10.10.1
終了IPアドレス	10.10.10.50
ネットマスク	255.255.255.0

### (1) ユーザ基本プロフィールで指定する方法

## IP アドレス割り当て設定 (RADIUS/プロフィール/ユーザ基本情報)

プロフィールで指定する場合はユーザ基本情報プロフィール画面で IP アドレス割り当てで**アドレスプール**を指定し、**アドレスプール名**を選択します。

ユーザ基本情報プロフィール 新規追加	
プロフィール名	user_base
認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	<input type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input checked="" type="radio"/> アドレスプール <input type="radio"/> 固定
アドレスプール	pool

### (2) RADIUS クライアントで指定する方法

## IP アドレス割り当て設定 (RADIUS/サーバ/クライアント)

クライアントで指定する場合は、作成した**アドレスプール名**を選択し、ユーザ基本情報プロフィールの IP アドレス割り当ては **未使用** を選択します。

クライアント新規追加	
クライアント名	client
IPアドレス	192.168.251.2
シークレット	secret
アドレスプール	pool

ユーザ基本情報プロフィール 新規追加	
プロフィール名	user_base
認証方式	PAP/CHAP
同時接続数	
IPアドレス割り当て	<input checked="" type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input type="radio"/> アドレスプール <input type="radio"/> 固定
アドレスプール	指定しない

以上で設定は終了です。

## 6.2. ユーザ毎に固定 IP アドレスを設定する

## ■ 概要

ここではユーザ毎に固定の IP アドレスを払い出す方法を紹介します。  
この設定を行ったユーザは、いつ接続を行っても常に同じ IP アドレスを使うことができます。

## ■ 構成



## ■ 設定例

ユーザ毎に固定の IP アドレスを払い出すには、ユーザ基本情報プロファイルの IP アドレス割り当てで固定を選択し、各ユーザの作成(または編集)時に IP アドレスを指定します。

ここでは下記の内容で設定を行います。

設定条件：

ユーザ名	user01
IP アドレス	172.123.123.1
ネットマスク	255.255.255.0

## IP アドレス割り当て方法の設定 (RADIUS/プロファイル/ユーザ基本情報)

ユーザ基本情報プロファイルで IP アドレス割り当て方法として **固定** を選択します。

ユーザ基本情報プロファイル 変更

プロファイル名 base\_user

認証方式 PAP/CHAP

同時接続数

IPアドレス割り当て  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール 指定しない

### ユーザ毎の IP アドレス設定 (RADIUS/ユーザ/ユーザ)

ユーザ作成(または編集)画面にて IP アドレスとネットマスクを設定します。



The screenshot shows a configuration page for a user. The user ID is 'user01'. The password field is masked with dots. The profile is set to 'user'. Under the '固定IPアドレス払い出し' (Fixed IP address assignment) section, the IP address is '172.123.123.1' and the netmask is '255.255.255.0'. These two fields are circled in red. Below this is a '備考' (Remarks) field and an 'アカウントのロック' (Account lock) section with radio buttons for 'ロックしない' (Do not lock) and 'ロックする' (Lock).

以上で設定は終了です。

## 7. ユーザの個別設定機能を利用する

### 7.1. ユーザ毎にVLAN IDを設定する

#### ■ 概要

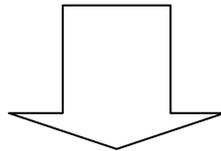
ここではユーザの個別設定機能によりプロファイルで指定した内容とは別にユーザ毎に異なるアトリビュートを設定する例を紹介します。

[5.3 ユーザ毎にVLAN IDを設定する]では、ユーザ毎に応答アトリビュートプロファイルとユーザプロファイルを作成する例を紹介しました。

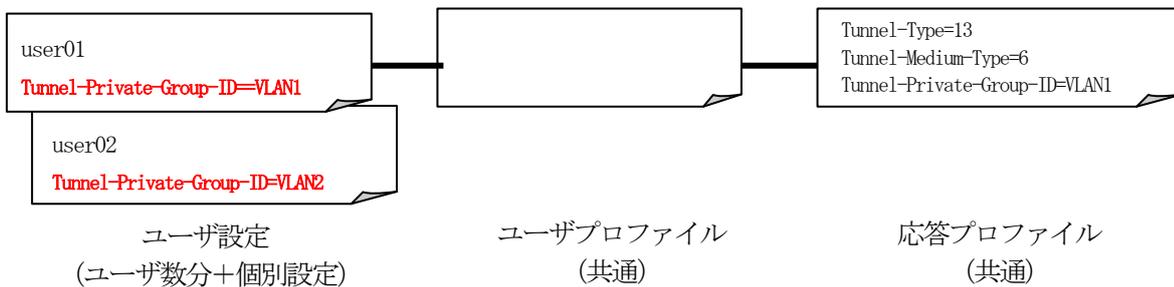
本節では、ユーザの個別設定機能でユーザ毎に異なる値のみ設定し、その他の共通の値は応答アトリビュートプロファイル1つにまとめる例を紹介します。

#### ■ 構成

[5.3 ユーザ毎にVLAN IDを設定する]では、



[7.1 アトリビュートをユーザ毎に設定する]では、



## ■ 設定例

VLAN の設定は次の 3 つのアトリビュートを用います。

Tunnel-Type	13 (VLAN)
Tunnel-Medium-Type	6 (802)
Tunnel-Private-Group-ID	VLAN1

各ユーザで使用する共通のアトリビュートは[5.3 ユーザ毎に VLAN ID を設定する]同様、応答アトリビュートプロファイルで設定し、Tunnel-Private-Group-ID のみユーザ毎に設定を行います。

この例では、[5.3 ユーザ毎に VLAN ID を設定する]から変更となる点のみを記載しておりますので、その他の設定については、前述の内容をご参照ください。

### 応答アトリビュートプロファイルの登録 (RADIUS/プロファイル/応答アトリビュート)

ここで VLAN ID を返すために使う応答アトリビュートを登録します。まず応答アトリビュートプロファイル一覧の **新規追加** ボタンを押下して応答アトリビュートプロファイルを作成します。

[5.3 ユーザ毎に VLAN ID を設定する]では、VLAN1, VLAN2 それぞれに対応するプロファイルを作成しましたが、ここでは共通のプロファイルとして vlan1 のみ作成します。

続いて応答アトリビュート一覧の **新規追加** ボタンを押下してアトリビュートを追加します。応答アトリビュート新規追加画面では Tunnel-Type, Tunnel-Medium-Type, Tunnel-Private-Group-ID の各アトリビュートを追加します。

Tunnel-Type の値は 13、Tunnel-Medium-Type の値は 6 を設定します。Tunnel-Private-Group-ID は個別設定を行わなかったユーザに対してデフォルトで返す値として VLAN1 を設定しておきます。

The screenshot displays the configuration interface for response attribute profiles. It is divided into two main sections:

- 応答アトリビュートプロファイル一覧 (Response Attribute Profile List):** This section shows a table with one entry:
 

プロファイル名 (Profile Name)	削除 (Delete)
vlan1	<input type="button" value="削除"/>

 Below this table is an orange **新規追加 (New Add)** button.
- 応答アトリビュート一覧 (Response Attribute List):** This section shows a table of attributes for the 'vlan1' profile:
 

プロファイル名 (Profile Name)	アトリビュート (Attribute)	値 (Value)	編集 (Edit)	削除 (Delete)
vlan1	Tunnel-Type	13	<input type="button" value="編集"/>	<input type="button" value="削除"/>
	Tunnel-Medium-Type	6	<input type="button" value="編集"/>	<input type="button" value="削除"/>
	Tunnel-Private-Group-ID	VLAN1	<input type="button" value="編集"/>	<input type="button" value="削除"/>

 An orange **新規追加 (New Add)** button is located at the bottom of this table.

### ユーザプロファイルの登録 (RADIUS/プロファイル/ユーザプロファイル)

各ユーザ共通のプロファイルを作成します。

ここでは、ユーザ基本情報プロファイル **base\_user**、応答アトリビュートプロファイル **vlan1** を選択したユーザプロファイル **vlanuser** を作成します。

プロファイル名	基本	認証	応答	グループ	証明書	編集	削除
vlanuser	base_user		vlan1			編集	削除

### ユーザ毎のアトリビュート設定 (RADIUS/ユーザ/ユーザ)

次にユーザ毎のVLAN IDを設定します。

ここではuser01にはVLAN1、user02にはVLAN2を指定します。

user01は、設定を行わず(※)、user02に対して個別設定を行います。

ユーザー一覧から詳細欄の[表示]ボタンを押下し、ユーザ設定画面を開きます。

No.	lock	ユーザID	プロファイル	IPアドレス	詳細	証明書
1		user01	vlanuser	-	表示	発行
2		user02	vlanuser	-	表示	発行

※応答アトリビュートプロファイルで指定したアトリビュート(Tunnel-Private-Group-ID)値が送信されます。

画面下段の ユーザ設定(詳細) に現在の設定が表示されています。ここでユーザ毎に個別のアトリビュートの設定を行います。新たにアトリビュートを追加する場合は[新規追加]ボタンを押下します。ここでは編集したいアトリビュート Tunnel-Private-Group-ID としてデフォルトの値を設定しているので、Tunnel-Private-Group-ID の行にある[編集]ボタンを押下して編集画面を開きます。

ユーザプロファイル		vlanuser	
基本	base1	編集	
認証方式	PAP/CHAP		
同時接続数			
IPアドレス割り当て	未使用		
アドレスプール			
認証	新規追加		
応答	vlan1		
Tunnel-Medium-Type	6	編集	
Tunnel-Private-Group-ID	VLAN1	編集	
Tunnel-Type	13	編集	
	新規追加		
グループ			
証明書			

編集画面を開いたらアトリビュートの値を編集します。動作モードはデフォルトの値を置き換えますので **上書き** を選択し、**設定** ボタンを押下します。



アトリビュート 新規追加 (ユーザ: user02)

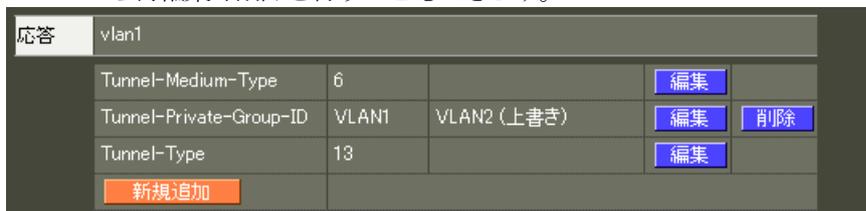
アトリビュート	Tunnel-Private-Group-ID
値	VLAN2
動作モード	上書き

設定

個別設定の内容はユーザ設定(詳細)欄で確認することができます。左側にプロファイルの値、右側に個別設定の値が表示されます。

つまりこの設定を行ったユーザは、ユーザ設定(詳細)で指定した値が優先される動作となります。

またここから再編集や削除を行うこともできます。



応答	vlan1		
Tunnel-Medium-Type	6		編集
Tunnel-Private-Group-ID	VLAN1	VLAN2 (上書き)	編集 削除
Tunnel-Type	13		編集
	新規追加		

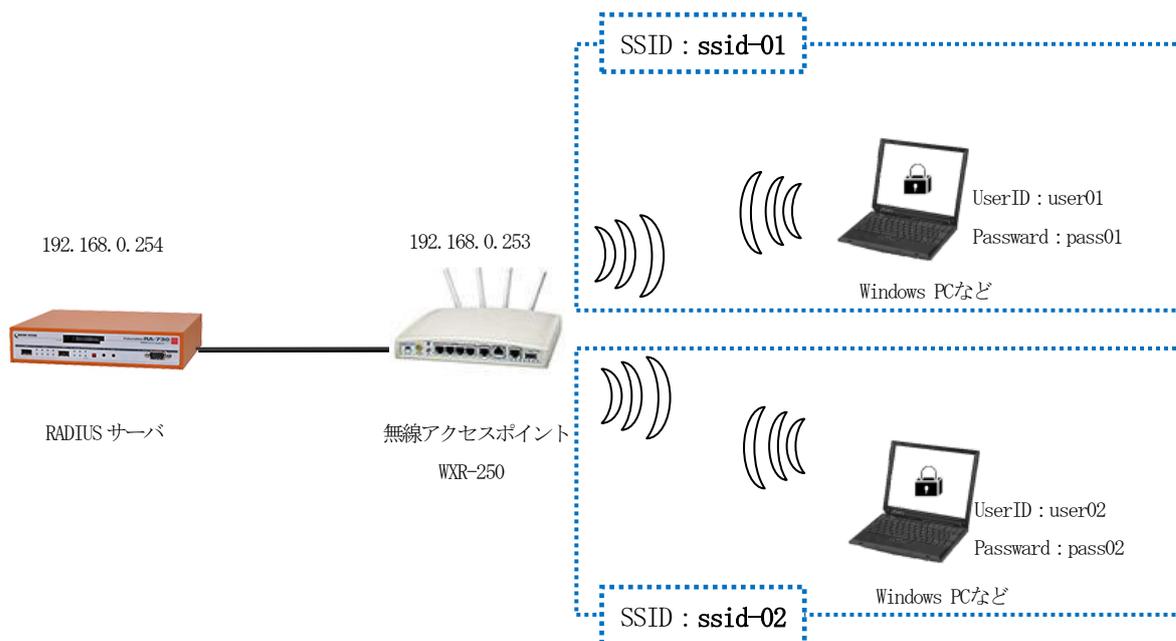
以上で設定は終了です。

## 7.2. 無線アクセスポイント (SSID) 毎に接続可能なユーザを限定する

## ■ 概要

ここでは、無線アクセスポイントに複数の SSID が設定されている場合、SSID 毎に接続するユーザを限定する設定例を紹介します。

## ■ 構成



## ■ 設定例

ここでは、ユーザ認証を行う認証方式などの基本設定やプロファイル、ユーザは、全て設定されていることを前提とし SSID 毎に認証するユーザを限定する設定のみを記載しています。認証方式などの設定については、[1. 各種認証方式を利用する]をご参照ください。

アクセスポイントの SSID を識別するためには、アトリビュートとして、**Called-Station-Id** を利用します。ここでは、**Called-Station-Id** に、「無線 LAN インタフェースの MAC アドレス : SSID」(※) が設定されているものとしてこれを利用します。 ※ (例) 「00-80-6D-AA-AA-AA:ssid-01」機種などによっては、アトリビュートの内容が異なる場合がありますので、アトリビュート内容を確認の上ご利用ください。

無線のアクセスポイントには、既に SSID として **ssid-01** と **ssid-02** が登録されているものとします。

また、ユーザ **user01** は、**ssid-01** への接続のみを許可、**user02** は、**ssid-02** への接続のみを許可する設定を行います。

ユーザ毎のアトリビュート設定 (RADIUS/ユーザ/ユーザ)

認証に利用するアトリビュートとして **Called-Station-Id** を用いる場合、設定済みのユーザに対して個別設定を行います。(認証プロファイルを利用する事も可能です)

ここでは user01 には **ssid-01**、user02 には **ssid-02** を指定します。

ユーザー一覧から詳細欄の[表示]ボタンを押下し、ユーザ設定画面を開きます。



No.	lock	ユーザID	プロファイル	IPアドレス	詳細	証明書	備考
1		user01	user	-	<a href="#">表示</a>	<a href="#">表示</a>	
2		user02	user	-	<a href="#">表示</a>	<a href="#">表示</a>	

画面下段の ユーザ設定(詳細) に現在の設定が表示されています。ここでユーザ毎に個別のアトリビュートの設定を行います。新たに認証用のアトリビュートを追加する場合は、認証欄にある[新規追加]ボタンを押下します。



ユーザ設定

ユーザID user01  
プロファイル user  
IPアドレス  
ネットマスク  
備考  
ロック ロックしない

[編集](#) [削除](#) [ユーザー一覧](#)

ユーザ設定(詳細)

ユーザプロファイル user

基本 base\_user [編集](#)

認証方式 EAP-PEAP  
同時接続数  
IPアドレス割り当て 未使用  
アドレスプール

認証 [新規追加](#)

応答 [新規追加](#)

グループ  
証明書

ここでは追加したいアトリビュート **Called-Station-Id** を選択、値に SSID **ssid-01** を指定、動作モードは **上書き** を選択し **設定** ボタンを押下します。



アトリビュート 新規追加 (ユーザ: user01)

アトリビュート	Called-Station-Id
値	00-80-6D-AA-AA-
動作モード	上書き

個別設定の内容はユーザ設定 (詳細) 欄で確認することができます。左側にプロファイルの値、右側に個別設定の値が表示されます。この例では、認証プロファイルを利用していないのでプロファイルの内容は表示されません。



認証	
Called-Station-Id	00-80-6D-AA-AA-ssid-01 (上書き)

新規追加 編集 削除

以上で設定は終了です。

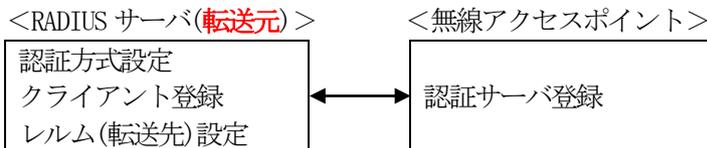
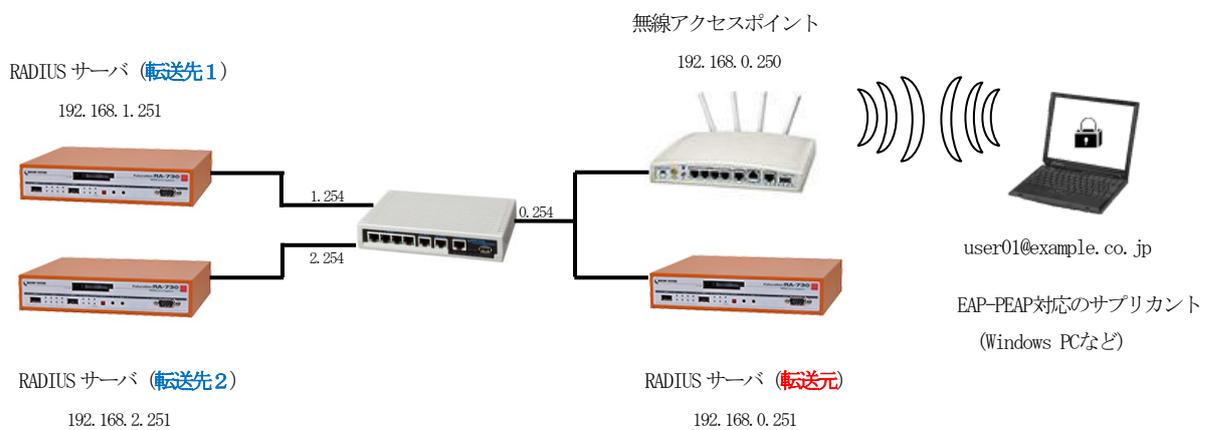
## 8. RADIUS Proxy機能を利用する

### 8.1. 全ての認証要求を転送する設定を行う

#### ■ 概要

ここでは、認証方式はEAP-PEAPを使用し、全ての認証をRADIUSサーバ(転送元)からRADIUSサーバ(転送先)へ転送する例を紹介します。また本構成では、RADIUSサーバ(転送先)は、設定情報の同期、二重化が行われているものとします。

#### ■ 構成



EAP-PEAP 認証を利用して無線アクセスポイント接続の認証を全て RADIUS サーバ(転送先)へ転送する設定を行うには、1. RADIUS サーバ(転送元)と 2. RADIUS サーバ(転送先)に対して以下の設定を行います。

1. RADIUS サーバ(転送元)
  - ・認証方式や使用ポートなどの基本設定
  - ・RADIUS クライアント(無線アクセスポイント)の登録
  - ・レルムの登録
2. RADIUS サーバ(転送先)
  - ・CA の設定
  - ・RADIUS サーバ用のサーバ証明書の発行
  - ・認証方式や使用ポートなどの基本設定
  - ・RADIUS クライアント(RADIUS サーバ(転送元))の登録
  - ・ユーザの登録

※無線アクセスポイントでは、RADIUS サーバ(転送元)の IP アドレスと RADIUS サーバ(転送先)に設定する共通のシークレットを指定します。

またサブクライアントでは、ユーザ ID/パスワードの設定の他、RADIUS サーバ(転送先)で発行した CA 証明書の登録を行います。

## 1. RADIUS サーバ(転送元) 設定

### ■ 設定例

ここでは下記の内容で設定を行います。

設定条件：

RADIUS サーバ(転送元)の IP アドレス		192. 168. 0. 251 (Ether0)
デフォルトゲートウェイ		192. 168. 0. 254
無線アクセスポイントの IP アドレス		192. 168. 0. 250
無線アクセスポイントのシークレット		secret0
認証方式		PAP/CHAP(※1)
認証/アカウントポート		1812/1813
RADIUS サーバ証明書		使用しない
転送先サーバ1	IP アドレス	192. 168. 1. 251
	認証ポート	1812
	アカウントポート	1813
	シークレット	secret12
転送先サーバ2	IP アドレス	192. 168. 2. 251
	認証ポート	1812
	アカウントポート	1813
	シークレット	secret12

※1 RADIUS サーバ(転送元)内で EAP-PEAP 認証の処理を行わない(転送のみ)場合は、EAP の認証方式を選択する必要はありません。

## ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.251/24**、デフォルトゲートウェイの IP アドレスを **192.168.1.254** に設定します。

MTU 及び通信モードはお使いの環境に合わせて設定してください。

基本情報			
Ether0	IPアドレス	192.168.0.251/24	編集
	MTU	1500	
	通信モード	Auto	
Ether1	IPアドレス		編集
	MTU	1500	
	通信モード	Auto	
Ether2	IPアドレス		編集
	MTU	1500	
	通信モード	Auto	
デフォルトゲートウェイ		192.168.0.254	編集

## 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

設定条件に従い、ポート番号に、**1812/1813**、認証方式に **PAP/CHAP**、RADIUS サーバ証明書に **使用しない** を選択します。以上を設定して **設定** ボタンを押下します。

ポート番号		RADIUSサーバ証明書	
<input type="radio"/> 1645/1646		<input checked="" type="radio"/> 使用しない	
<input checked="" type="radio"/> 1812/1813		<input type="radio"/> 本装置の証明書を使用する	
<input type="radio"/> 1645/1646と1812/1813		シリアルナンバ	<input type="text"/>
<input type="radio"/> 手動設定			
認証用	<input type="text"/>		
アカウント用	<input type="text"/>		
認証方式			
<input checked="" type="checkbox"/> PAP/CHAP	<input type="checkbox"/> EAP-MD5		
<input type="checkbox"/> EAP-TLS	<input type="checkbox"/> EAP-PEAP		
<input type="checkbox"/> EAP-TTLS			
<b>設定</b>			

## RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの情報を設定します。

設定条件に従い IP アドレスは、無線アクセスポイントの IP アドレス **192.168.0.250**、シークレットは無線アクセスポイントに設定したものと同一もの **secret0** を設定します。クライアント名は、**AP-01** とします。以上を設定して **設定** ボタンを押下します。

クライアント新規追加	
クライアント名	<input type="text" value="AP-01"/>
IPアドレス	<input type="text" value="192.168.0.250"/>
シークレット	<input type="text" value="secret0"/>
アドレスブール	<input type="text" value="指定しない"/>
<b>設定</b>	

## レلم(転送先)の設定 (RADIUS/サーバ/レلم)

最初にレلم付ユーザのデフォルトの転送先を設定します。

種別に **デフォルト**、動作に **forward**、設定条件に従い転送先サーバ 1、転送先サーバ 2 にそれぞれの IP アドレス、認証ポート、アカウントティングポート、シークレットを設定します。レلم名は **default** とします。以上を設定して **設定** ボタンを押下します。

レلم新規追加

レلم名	default
種別	デフォルト
優先度	
指定文字列	
一致条件	完全一致
動作	forward
転送先サーバ1	192.168.1.251
認証ポート1	1812
アカウントティングポート1	1813
シークレット1	secret12
転送先サーバ2	192.168.2.251
認証ポート2	1812
アカウントティングポート2	1813
シークレット2	secret12

設定

次にレلمなしユーザのデフォルトの転送先を設定します。

種別に **レلمなし**、動作に **forward**、設定条件に従い転送先サーバ 1、転送先サーバ 2 にそれぞれの IP アドレス、認証ポート、アカウントティングポート、シークレットを設定します。レلم名は **norealm** とします。以上を設定して **設定** ボタンを押下します。

レلم新規追加

レلم名	norealm
種別	レلمなし
優先度	
指定文字列	
一致条件	完全一致
動作	forward
転送先サーバ1	192.168.1.251
認証ポート1	1812
アカウントティングポート1	1813
シークレット1	secret12
転送先サーバ2	192.168.2.251
認証ポート2	1812
アカウントティングポート2	1813
シークレット2	secret12

設定

上記設定を行うと以下のように2つの転送先が表示されます。

優先度	レルム名	動作	編集	削除
64000	default	forward	編集	削除
65000	norealm	forward	編集	削除

## RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。



以上で、RADIUS サーバ(転送元)の設定は終了です。

## 2. RADIUS サーバ(転送先)設定

### ■ 設定例

転送先サーバ1および2は、設定情報の同期、および二重化の設定が事前に行われている事とします。設定情報の同期、および二重化の設定については、「[2. 冗長化機能を利用する](#)」を参照ください。

転送先2については、CA、基本情報、プロファイル、ユーザ設定は、設定情報の同期機能により設定の同期が行われるため個別に設定する必要はありません。ここでは、主に転送先1の設定画面について説明いたします。

設定条件：

RADIUS サーバ (転送先1)	IP アドレス	192.168.1.251 (Ether0)
	デフォルトゲートウェイ	192.168.1.254
RADIUS サーバ (転送先2)	IP アドレス	192.168.2.251 (Ether0)
	デフォルトゲートウェイ	192.168.2.254
RADIUS サーバ(転送元)の IP アドレス		192.168.0.251
RADIUS サーバ(転送元)のシークレット		secret12
ユーザ ID		user01
パスワード		pass01
グループ ID		example.co.jp
認証方式		EAP-PEAP
認証/アカウンティングポート		1812/1813

## ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.1.251/24** に設定します。  
 デフォルトゲートウェイの IP アドレスを **192.168.1.254** に設定します。  
 MTU 及び通信モードはお使いの環境に合わせて設定してください。

The screenshot shows a configuration window titled '基本情報' (Basic Information). It contains a table of network settings:

Interface	Property	Value	Action
Ether0	IPアドレス	192.168.1.251/24	編集
	MTU	1500	
	通信モード	Auto	
Ether1	IPアドレス		編集
	MTU	1500	
	通信モード	Auto	
Ether2	IPアドレス		編集
	MTU	1500	
	通信モード	Auto	
デフォルトゲートウェイ		192.168.1.254	編集

## CA の設定 (CA/CA/CRL)

EAP-PEAP 認証を使用する場合は CA の設定が必要になります。  
 CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているかご確認ください。  
 CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要です。  
 ここでは以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
Email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※CA の再編集はできませんので設定の際は内容を十分確認してください。  
 また、CA を削除した場合は発行済みの全ての証明書も削除されます。

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name sample\_ca

email samp@example.co.jp

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035 年 12 月 31 日

パスフレーズ

パスフレーズ

失効リスト更新間隔

失効リスト更新間隔 365

設定

CA 作成後は、CA 証明書画面より **取り出し** ボタンを押下して CA 証明書を取得し、サブリカントへインストールします。

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

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 KeyUsage** を指定するようにします。

但し、実際にどの **Key Usage/Extended Key Usage** を必要とするかは通信相手のソフトウェアに依存します。

- **Key Usage** : digitalSignature および keyEncipherment
- **Extended Key Usage** : serverAuth

The screenshot shows the configuration for a new RADIUS server certificate. The 'Certificate' section is set to Version 3, Key Length 1024, and Signature Algorithm SHA-256. The 'Subject' section has Common Name RA\_Server. The 'Validity Period' section shows start and end times. The 'Key Usage' section has checkboxes for digitalSignature and keyEncipherment checked. The 'Extended Key Usage' section has a dropdown menu set to serverAuth. The 'Netscape Extension' section has checkboxes for nsCertType (client, server, email, objsign, sslCA, emailCA, objCA). The 'Passphrase' section has a field for the passphrase. A '設定' (Settings) button is at the bottom.

## 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**、**EAP-PEAP**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。  
EAP-PEAP を使用するには EAP-TLS も選択する必要があります。

シリアルナンバーには先ほど発行したサーバ証明書のシリアルナンバーを入力します。シリアルナンバーは CA の証明書一覧で確認することができます。また、設定ウィザードを使った場合は自動的に入力されます。  
なおポート番号は、RADIUS クライアント (RADIUS サーバ(転送元)のレルム) の設定と同一になるよう指定します。以上を設定して **設定** ボタンを押下します。

ポート番号

- 1645/1646
- 1812/1813
- 1645/1646と1812/1813
- 手動設定

認証用

アカウント用

RADIUSサーバ証明書

- 使用しない
- 本装置の証明書を使用する

シリアル番号

認証方式

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

設定

### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとしてRADIUS サーバ(転送元)の情報を設定します。  
設定条件に従い IP アドレスはRADIUS サーバ(転送元)の IP アドレス、シークレットはRADIUS サーバ(転送元)のレلم設定で設定したものと同じものを設定します。クライアント名は、**RADIUS\_Proxy** とします。  
以上を設定して **設定** ボタンを押下します。

クライアント新規追加

クライアント名

IPアドレス

シークレット

アドレスプール

設定

ユーザはプロファイルという概念により、設定単位にグループ化を行うことができます。このプロファイルにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロファイル、ユーザプロファイルの作成が必要です。

### ユーザ基本情報プロファイルの作成 (RADIUS/プロファイル/ユーザ基本情報)

設定条件に従い認証方式に **EAP-PEAP** を設定します。プロファイル名は **base\_user** とします。  
以上を設定して **設定** ボタンを押下します。

ユーザ基本情報プロファイル 新規追加

プロファイル名

認証方式

同時接続数

IPアドレス割り当て  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール

設定

### グループ ID の設定 (RADIUS/プロフィール/グループ ID)

グループ ID として **example.co.jp** を設定します。プロフィール名は **group** とします。  
以上を設定して **設定** ボタンを押下します。

グループIDプロフィール 新規追加

プロフィール名

グループID

形式  UserID@GroupID  GroupID#UserID

**設定**

### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

作成したユーザ基本プロフィール **base\_user**、グループプロフィール **group** を指定してユーザプロフィール **user** を作成します。以上を設定して **設定** ボタンを押下します。

ユーザプロフィール 新規追加

プロフィール名

基本

認証

証明書

応答

グループ

**設定**

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **user01**、パスワードに **pass01** を入力します。  
プロフィールは先ほど作成したユーザプロフィールを指定します。  
以上を設定して **設定** ボタンを押下します。

ユーザ 新規追加

ユーザID

パスワード

プロフィール

固定IPアドレス払い出し

IPアドレス

ネットマスク

備考

備考

アカウントのロック

ロック  ロックしない  ロックする

**設定**

RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。



以上で RADIUS サーバ([転送先](#))の設定は終了です。

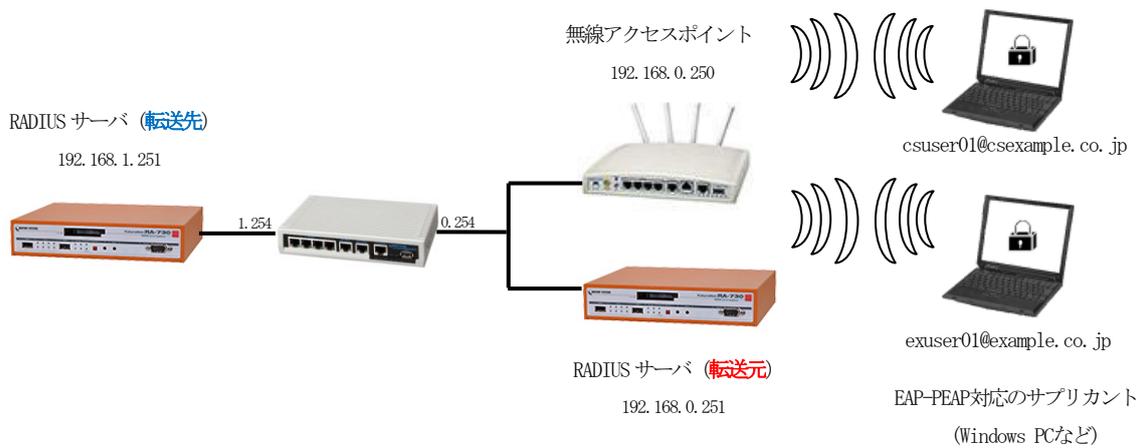
8.2. 特定のレルムに属するユーザをローカルで認証する設定を行う

■ 概要

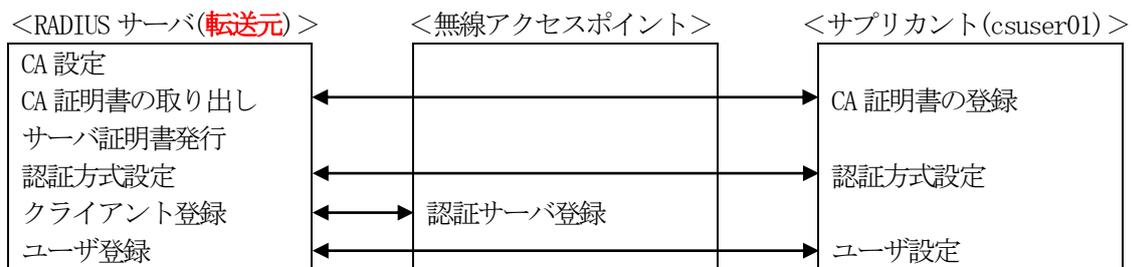
ここでは認証方式は EAP-PEAP を使用し、特定のレルムに属するユーザの認証要求を RADIUS サーバ(転送元)で認証を行い、それ以外は RADIUS サーバ(転送先)へ転送する例を紹介します。

なお RA シリーズでは、認証要求等に含まれるユーザ名の @ より後ろの文字列をレルムとして扱います。

■ 構成



【csuser01@csexample.co.jp ユーザに関する設定】



【exuser01@example.co.jp ユーザに関する設定】



EAP-PEAP 認証を利用して無線アクセスポイント接続の認証で特定のレールのみを RADIUS サーバ(転送元)で認証を行うには、1. RADIUS サーバ(転送元)と 2. RADIUS サーバ(転送先)に対して以下の設定を行います。

1. RADIUS サーバ(転送元)
  - CA の設定(特定のレールに属するユーザ用)
  - RADIUS サーバ用のサーバ証明書の発行(転送元用)
  - 認証方式や使用ポートなどの基本設定
  - RADIUS クライアント(無線アクセスポイント)の登録
  - ユーザの登録(特定のレールに属するユーザ)
  
2. RADIUS サーバ(転送先)
  - CA の設定(特定のレールに属するユーザ以外用)
  - RADIUS サーバ用のサーバ証明書の発行(転送先用)
  - 認証方式や使用ポートなどの基本設定
  - RADIUS クライアント (RADIUS サーバ(転送元)) の登録
  - ユーザの登録(特定のレールに属するユーザ以外)

※無線アクセスポイントでは、RADIUS サーバ(転送元)の IP アドレスと RADIUS サーバ(転送元)に設定する共通のシークレットを指定します。

またサブリカントでは、ユーザ ID/パスワードの設定の他、特定のレールに属するユーザは、RADIUS サーバ(転送元)で発行した CA 証明書、特定のレールに属するユーザ以外は、RADIUS サーバ(転送先)で発行した CA 証明書の登録を行います。

## 1. RADIUS サーバ(転送元) 設定

### ■ 設定例

ここでは下記の内容で設定を行います。

設定条件：

RADIUS サーバ(転送元)の IP アドレス		192.168.0.251 (Ether0)
デフォルトゲートウェイ		192.168.0.254
無線アクセスポイントの IP アドレス		192.168.0.250
無線アクセスポイントのシークレット		secret0
認証方式		EAP-PEAP
認証/アカウントポート		1812/1813
RADIUS サーバ証明書		使用する
転送先サーバ	IP アドレス	192.168.1.251
	認証ポート	1812
	アカウントポート	1813
	シークレット	secret12
ユーザ ID		csuser01
パスワード		pass01
グループ ID		csexample.co.jp

## ネットワークの設定 (管理機能/ネットワーク/基本情報)

Ether0 の IP アドレスを **192.168.0.251/24**、デフォルトゲートウェイの IP アドレスを **192.168.1.254** に設定します。MTU 及び通信モードはお使いの環境に合わせて設定してください。

基本情報			
Ether0	IPアドレス	192.168.0.251/24	
	MTU	1500	編集
	通信モード	Auto	
Ether1	IPアドレス		
	MTU	1500	編集
	通信モード	Auto	
Ether2	IPアドレス		
	MTU	1500	編集
	通信モード	Auto	
デフォルトゲートウェイ		192.168.0.254	編集

## CA の設定 (CA/CA/CRL)

EAP-PEAP 認証を使用する場合は CA の設定が必要になります。

CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているかご確認ください。

CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要です。ここでは以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	cs_ca
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※CA の再編集はできませんので設定の際は内容を十分確認してください。  
また、CA を削除した場合は発行済みの全ての証明書も削除されます。

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name cs\_ca

email

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035 年 12 月 31 日

パスフレーズ

パスフレーズ

失効リスト更新間隔

失効リスト更新間隔 365

設定

CA 作成後は、CA 証明書画面より **取り出し** ボタンを押下して CA 証明書を取得し、サブリカントへインストールします。

## RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

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 KeyUsage** を指定するようにします。

但し、実際にどの **Key Usage/Extended Key Usage** を必要とするかは通信相手のソフトウェアに依存します。

- **Key Usage** : digitalSignature および keyEncipherment
- **Extended Key Usage** : serverAuth

The screenshot shows the configuration interface for a RADIUS server certificate. The '証明書' (Certificate) section is expanded, showing the following settings:

- バージョン: 3
- 鍵長: 1024
- Signature Algorithm: SHA-256
- Subject: Common Name: CS\_Server
- Country: JP
- 有効期間: 開始日時 (empty), 終了日時: 2025年12月31日14時59分

The 'X509証明書v3拡張 (RFC3280)' section is expanded, showing the following settings:

- Key Usage:  digitalSignature,  keyEncipherment,  nonRepudiation,  dataEncipherment,  keyCertSign,  encipherOnly
- Extended Key Usage: serverAuth

The 'Netscape拡張' section is also visible, showing the following settings:

- nsCertType:  client,  server,  email,  objsign,  sslCA,  emailCA,  objCA
- nsComment: (empty)

A '設定' (Settings) button is located at the bottom of the form.

### 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**、**EAP-PEAP**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。EAP-PEAP を使用するには EAP-TLS も選択する必要があります。

シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバは CA の証明書一覧で確認することができます。なおポート番号は、RADIUS クライアント(無線アクセスポイント)の設定と同一になるよう指定します。以上を設定して **設定** ボタンを押下します。

The screenshot shows a configuration interface for RADIUS server certificates. It is divided into three main sections:

- ポート番号 (Port Number):** Radio buttons for 1645/1646, 1812/1813, 1645/1646と1812/1813, and 手動設定 (Manual Setting). Below are input fields for 認証用 (Authentication) and アカウンティング用 (Accounting).
- RADIUSサーバ証明書 (RADIUS Server Certificate):** Radio buttons for 使用しない (Do not use) and 本装置の証明書を使用する (Use device certificate). A text field for シリアルナンバ (Serial Number) contains '01'.
- 認証方式 (Authentication Method):** Checkboxes for PAP/CHAP, EAP-MD5, EAP-TLS (checked), EAP-PEAP (checked), and EAP-TTLS.

A **設定** (Settings) button is located at the bottom center.

### RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして無線アクセスポイントの情報を設定します。

設定条件に従い IP アドレスは、無線アクセスポイントの IP アドレス **192.168.0.250**、シークレットは無線アクセスポイントに設定したものと同一のもの **secret0** を設定します。クライアント名は、**AP-01** とします。以上を設定して **設定** ボタンを押下します。

The screenshot shows the 'クライアント新規追加' (Add New Client) configuration screen. It contains the following fields:

- クライアント名 (Client Name): AP-01
- IPアドレス (IP Address): 192.168.0.250
- シークレット (Secret): secret0
- アドレスグループ (Address Group): 指定しない (None) (dropdown menu)

A **設定** (Settings) button is located at the bottom center.

## レلم(転送先)の設定 (RADIUS/サーバ/レلم)

最初に、レلم「csexample.co.jp」ユーザが、本RADIUSサーバ(転送元)で認証を行うための設定を行います。種別に **指定文字列**、優先度に **100**、指定文字列に **csexample.co.jp**、一致条件に **完全一致**、動作に **local** を設定します。レلم名は **csexample** とします。以上を設定して **設定** ボタンを押下します。

## ☆[指定文字列] と [一致条件]の指定例

No	レلم	設定対象	指定文字列	一致条件
(1)	example.co.jp	(1)のみ	example.co.jp	完全一致
(2)	sub1.example.co.jp	(2)のみ	sub1.example.co.jp	完全一致
(3)	sub2.example.co.jp	(2)~(4)	.example.co.jp	後方一致
(4)	sub3.example.co.jp			

## ☆[優先度]

優先度が小さいレلم設定から順番に一致判定が行われます。

次にレルム付ユーザのデフォルトの転送先を設定します。

これによりレルム「example. co. jp」ユーザの要求が、RADIUS サーバ(転送先)で認証されるようになります。種別に **デフォルト**、動作に **forward**、設定条件に従い転送先サーバ1に IP アドレス、認証ポート、アカウントングポート、シークレットを設定します。レルム名は **default** とします。

以上を設定して **設定** ボタンを押下します。

レルム新規追加

レルム名	default
種別	デフォルト
優先度	
指定文字列	
一致条件	完全一致
動作	forward
転送先サーバ1	192.168.1.251
認証ポート1	1812
アカウントングポート1	1813
シークレット1	secret12
転送先サーバ2	
認証ポート2	
アカウントングポート2	
シークレット2	

設定

最後にレルムなしユーザのデフォルトの転送先を設定します。

種別に **レルムなし**、動作に **forward**、設定条件に従い転送先サーバ1に IP アドレス、認証ポート、アカウントングポート、シークレットを設定します。レルム名は **norealm** とします。

以上を設定して **設定** ボタンを押下します。

レルム新規追加

レルム名	norealm
種別	レルムなし
優先度	
指定文字列	
一致条件	完全一致
動作	forward
転送先サーバ1	192.168.1.251
認証ポート1	1812
アカウントングポート1	1813
シークレット1	secret12
転送先サーバ2	
認証ポート2	
アカウントングポート2	
シークレット2	

設定

上記設定を行うと以下のように3つの設定が表示されます。

優先度	レルム名	動作	編集	削除
100	csexample	local	編集	削除
64000	default	forward	編集	削除
65000	norealms	forward	編集	削除

ユーザはプロファイルという概念により、設定単位にグループ化を行うことができます。このプロファイルにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロファイル、ユーザプロファイルの作成が必要です。

#### ユーザ基本情報プロファイルの作成 (RADIUS/プロファイル/ユーザ基本情報)

設定条件に従い認証方式に **EAP-PEAP** を設定します。プロファイル名は **base\_user** とします。以上を設定して **設定** ボタンを押下します。

ユーザ基本情報プロファイル 新規追加

プロファイル名

認証方式

同時接続数

IPアドレス割り当て  未使用  RADIUSクライアント  アドレスプール  固定

アドレスプール

**設定**

#### グループIDの設定 (RADIUS/プロファイル/グループID)

グループIDとしてレルム **csexample.co.jp** を設定します。プロファイル名は **group** とします。以上を設定して **設定** ボタンを押下します。

グループIDプロファイル 新規追加

プロファイル名

グループID

形式  UserID@GroupID  GroupID#UserID

**設定**

### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

作成したユーザ基本プロフィール **base\_user**、グループプロフィール **group** を指定してユーザプロフィール名 **user** を作成します。以上を設定して **設定** ボタンを押下します。

ユーザプロフィール 新規追加

プロフィール名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	group

設定

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **csuser01**、パスワードに **pass01** を入力します。プロフィールは先ほど作成したユーザプロフィールを指定します。以上を設定して **設定** ボタンを押下します。

ユーザ 新規追加

ユーザID	csuser01
パスワード	●●●●●●
プロフィール	user

固定IPアドレス払い出し

IPアドレス	
ネットマスク	

備考

備考	
----	--

アカウントのロック

ロック	<input checked="" type="radio"/> ロックしない <input type="radio"/> ロックする
-----	---

設定

### RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。

起動・停止

現在の状態	停止中
-------	-----

起動

以上で RADIUS サーバ(転送元)の設定は終了です。

## 2. RADIUS サーバ(転送先)設定

ここでは、レルム「example. co. jp」ユーザの認証に関する設定を行います。

設定条件：

RADIUS サーバ(転送先)の IP アドレス	192. 168. 1. 251
デフォルトゲートウェイ	192. 168. 1. 254
RADIUS サーバ(転送元)の IP アドレス	192. 168. 0. 251
RADIUS サーバ(転送元)のシークレット	secret12
認証方式	EAP-PEAP
認証/アカウントティングポート	1812/1813
RADIUS サーバ証明書	使用する
ユーザ ID	exuser01
パスワード	pass01
グループ ID	example. co. jp

### CA の設定 (CA/CA/CRL)

EAP-PEAP 認証を使用する場合は CA の設定が必要になります。

CA の作成や証明書の発行を行う際は証明書の有効期限を正しく認識させる為、内蔵時計が正しく設定されているかご確認ください。

CA の作成では Common Name、有効期間、パスフレーズ、失効リスト更新間隔 の入力が必要で

ここでは以下の設定で CA を作成します。

鍵長	1024
Signature Algorithm	SHA-256
Common Name	ex_ca
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※CA の再編集はできませんので設定の際は内容を十分確認してください。

また、CA を削除した場合は発行済みの全ての証明書も削除されます。

CA

バージョン 3

鍵長 1024

Signature Algorithm SHA-256

Subject

Common Name ex\_ca

email

Organizational Unit

Organization

Locality

State or Province

Country JP

有効期間

終了日時 2035年12月31日

パスフレーズ

パスフレーズ

失効リスト更新間隔

失効リスト更新間隔 365

設定

CA 作成後は、CA 証明書画面より **取り出し** ボタンを押下して CA 証明書を取得し、サブリカントへインストールします。

#### RADIUS サーバ証明書の発行 (CA/証明書)

RADIUS サーバで使用するサーバ証明書の発行を行います。  
証明書画面から **新規追加** ボタンを押下します。

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 KeyUsage** を指定するようにします。

但し、実際にどの **Key Usage/Extended Key Usage** を必要とするかは通信相手のソフトウェアに依存します。

- **Key Usage** : digitalSignature および keyEncipherment
- **Extended Key Usage** : serverAuth

### 認証方式の設定、サーバ証明書の登録 (RADIUS/サーバ/基本情報)

認証方式に **EAP-TLS**、**EAP-PEAP**、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。EAP-PEAP を使用するには EAP-TLS も選択する必要があります。シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバは CA の証明書一覧で確認することができます。また、設定ウィザードを使った場合は自動的に入力されます。なおポート番号は、RADIUS クライアントの設定と同一になるよう指定します。

## RADIUS クライアントの設定 (RADIUS/サーバ/クライアント)

RADIUS クライアントとして RADIUS サーバ(転送元)の情報を設定します。

IP アドレスは RADIUS サーバ(転送元)の IP アドレス、シークレットは RADIUS サーバ(転送元)のレلم設定で設定したものと同一ものを設定します。以上を設定して **設定** ボタンを押下します。

クライアント新規追加

クライアント名	RADIUS_Proxy
IPアドレス	192.168.0.251
シークレット	secret12
アドレスグループ	指定しない

設定

ユーザはプロフィールという概念により、設定単位にグループ化を行うことができます。このプロフィールにより類似した設定内容のユーザを簡単に追加したり、同じグループのユーザの設定を一括して変更することができます。ユーザの作成にはユーザ基本情報プロフィール、ユーザプロフィールの作成が必要です。

## ユーザ基本情報プロフィールの作成 (RADIUS/プロフィール/ユーザ基本情報)

設定条件に従い認証方式に **EAP-PEAP** を設定します。プロフィール名は **base\_user** とします。以上を設定して **設定** ボタンを押下します。

ユーザ基本情報プロフィール 新規追加

プロフィール名	base_user
認証方式	EAP-PEAP
同時接続数	
IPアドレス割り当て	<input checked="" type="radio"/> 未使用 <input type="radio"/> RADIUSクライアント <input type="radio"/> アドレスグループ <input type="radio"/> 固定
アドレスグループ	指定しない

設定

## グループ ID の設定 (RADIUS/プロフィール/グループ ID)

グループ ID として **example.co.jp** を設定します。プロフィール名は **group** とします。以上を設定して **設定** ボタンを押下します。

グループIDプロフィール 新規追加

プロフィール名	group
グループID	example.co.jp
形式	<input checked="" type="radio"/> UserID@GroupID <input type="radio"/> GroupID#UserID

設定

### ユーザプロフィールの作成 (RADIUS/プロフィール/ユーザプロフィール)

作成したユーザ基本プロフィール **base\_user**、グループプロフィール **group** を指定してユーザプロフィール **user** を作成します。以上を設定して **設定** ボタンを押下します。

ユーザプロフィール 新規追加

プロフィール名	user
基本	base_user
認証	指定しない
証明書	指定しない
応答	指定しない
グループ	group

設定

### ユーザ作成 (RADIUS/ユーザ/ユーザ)

設定条件に従いユーザ ID に **exuser01**、パスワードに **pass01** を入力します。プロフィールは先ほど作成したユーザプロフィールを指定します。以上を設定して **設定** ボタンを押下します。

ユーザ 新規追加

ユーザID	exuser01
パスワード	●●●●●●
プロフィール	user

固定IPアドレス払い出し

IPアドレス	
ネットマスク	

備考

備考	
----	--

アカウントのロック

ロック	<input checked="" type="radio"/> ロックしない <input type="radio"/> ロックする
-----	---

設定

RADIUS サーバ機能 (RADIUS/サーバ/起動・停止)

最後に **起動** ボタンを押下して RADIUS サーバを起動します。



以上で RADIUS サーバ([転送先](#))の設定は終了です。

RA シリーズ 設定例集 Ver1.9.0

---

2014 年 01 月版  
発行 センチュリー・システムズ株式会社  
(c)2014 CENTURY SYSTEMS Co., Ltd ALL rights reserved.

---