EAP 対応 RADIUS サーバアプライアンス

FutureNet RA シリーズ

設定事例集

Ver 1.8.13(a)

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 Ver1.8.13 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、Ver1.4.0 以前の設定事例集をご利用ください。

商標の表示

－ 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. ＩＰ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ＩＰ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

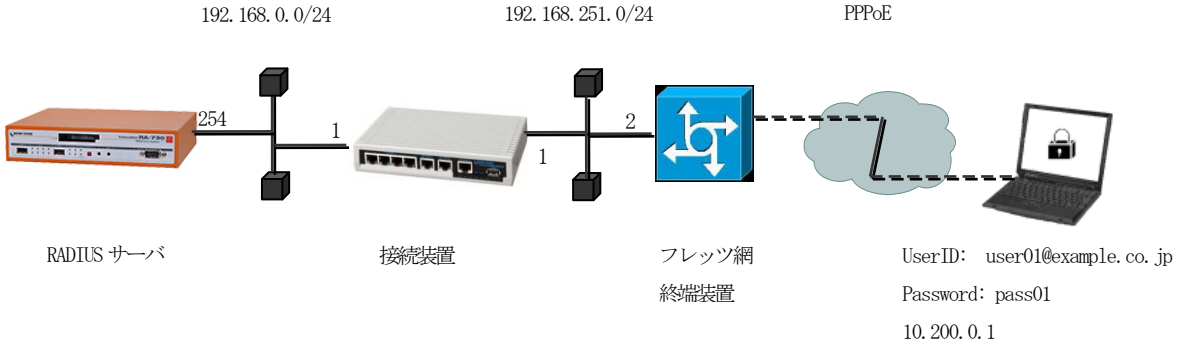
1. 各種認証方式を利用する

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/アカウンティングポート	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。

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/アカウンティ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。

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。

ユーザ基本プロファイルの登録（RADIUS／プロファイル／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ァイルを作成します。
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。
プロファイル名は **base_user** とします。

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ァイルを作成します。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。

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 **example.co.jp** を設定します。プロファイル名は **group** とします。

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情報プロファイル **base_user** とグループプロファイル **group** を選択してユーザプロファイルを作成します。プロファイル名は **user** とします。

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 **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。

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。

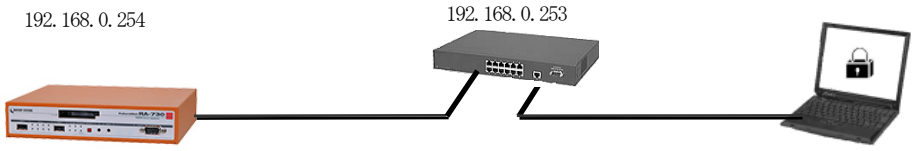
以上で設定は終了です。

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/アカウンティングポート	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。

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/アカウンティ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。

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じものを設定します。

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）

ユーザを作成するにはユーザ基本情報プロファイルを作成します。
設定条件に従い認証方式に PAP/CHAP に設定します。
プロファイル名は base_user とします。

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情報プロファイル base_user を指定してユーザプロファイル user を作成します。

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。

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。

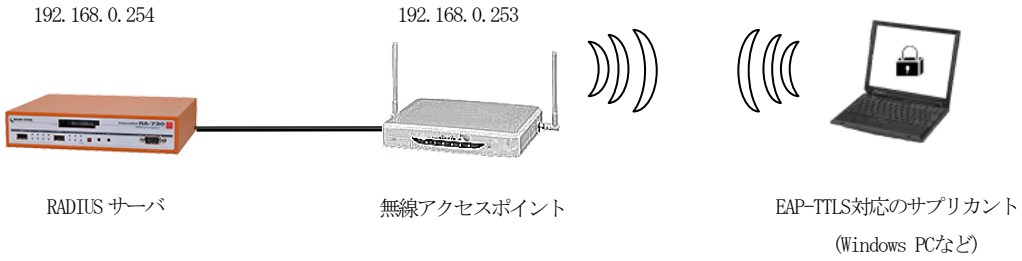
以上で設定は終了です。

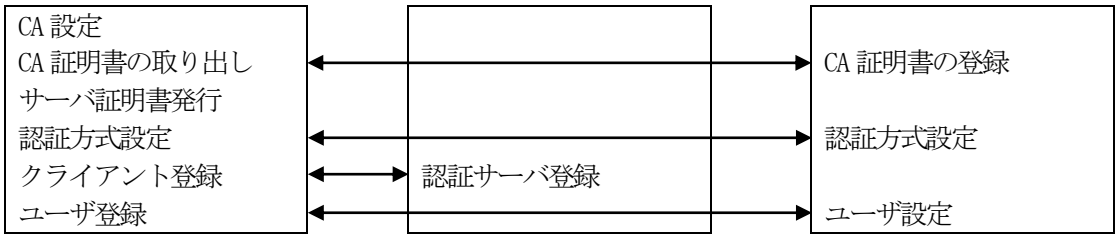
1.3. EAP-TTLS 認証を利用する

■ 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。
またサプリカントでは、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。

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 の入力が必須です。
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。

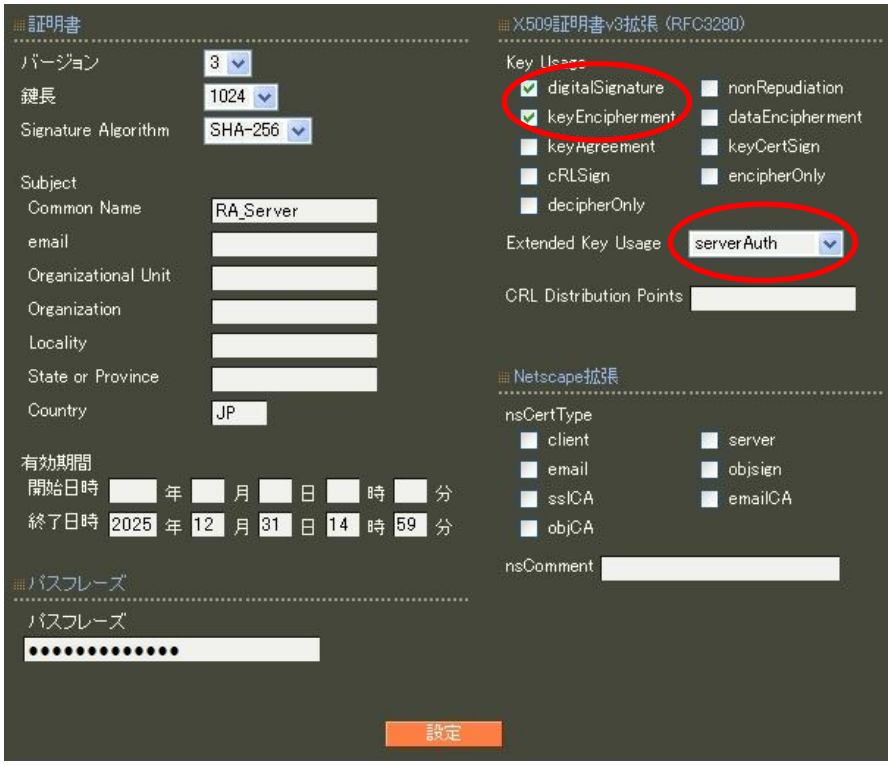
CA 作成後は CA 証明書画面より 取り出し ボタンを押下して CA 証明書を取得し、サプリカントへインストールします。

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。

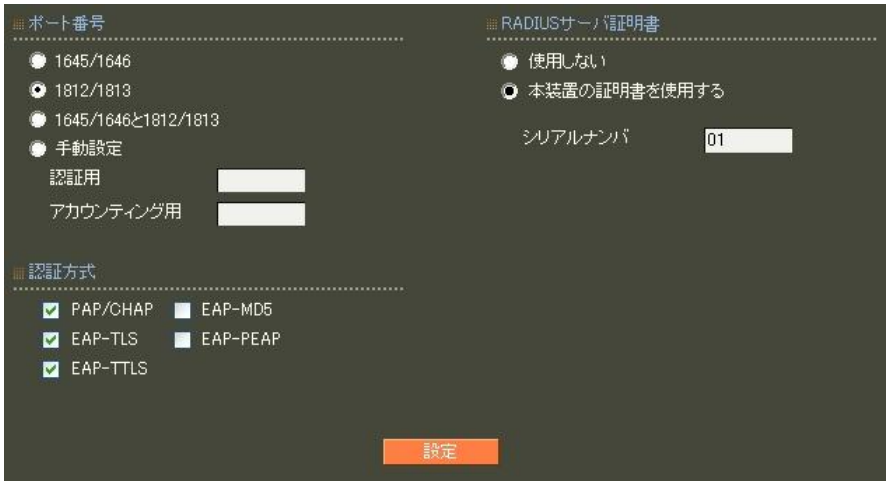
バージョン3 のサーバ証明書を作成する場合には、通常最低限以下の Key Usage/Extended KeyUsage を指定するようにします。
但し、実際にどの Key Usage/Extended Key Usage を必要とするかは通信相手のソフトウェアに依存します。

- 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-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。

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-TTLS/PAP,CHAP** を設定します。プロファイル名は **base_user** とします。

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** を指定してユーザプロファイル **user** を作成します。

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。

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。

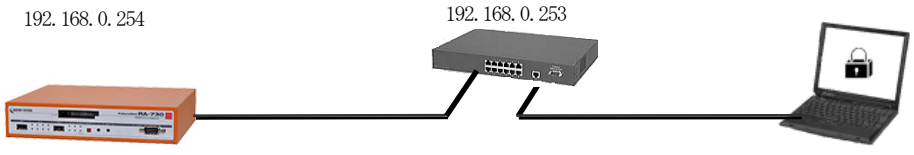
以上で設定は終了です。

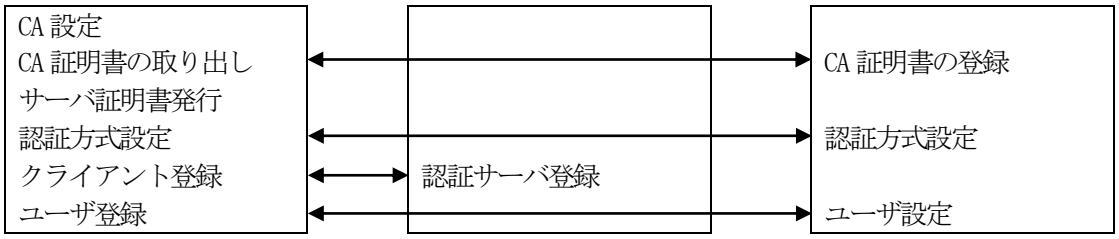
1.4. EAP-PEAP 認証を利用する

■ 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。
またサプリカントでは、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。

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 の入力が必須です。
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。

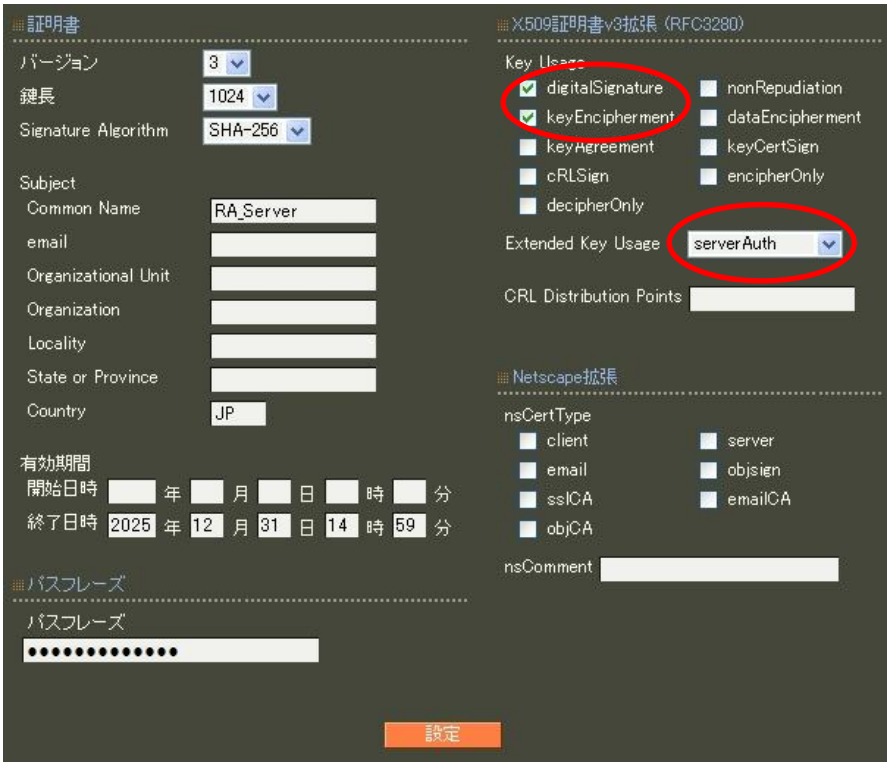
CA 作成後は、CA 証明書画面より 取り出し ボタンを押下して CA 証明書を取得し、サプリカントへインストールします。

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じものを設定します。

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。

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。

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。

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。

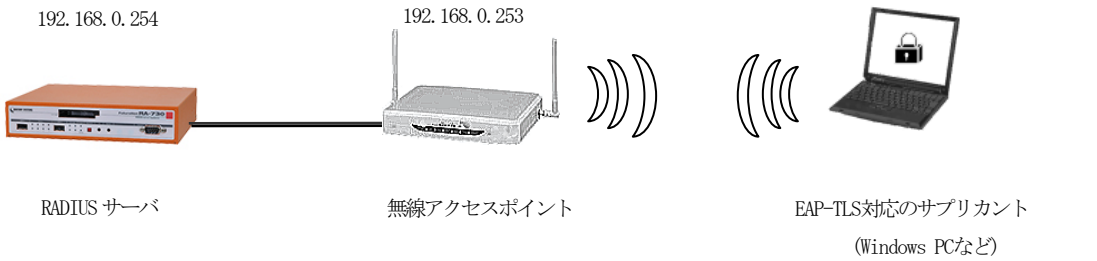
以上で設定は終了です。

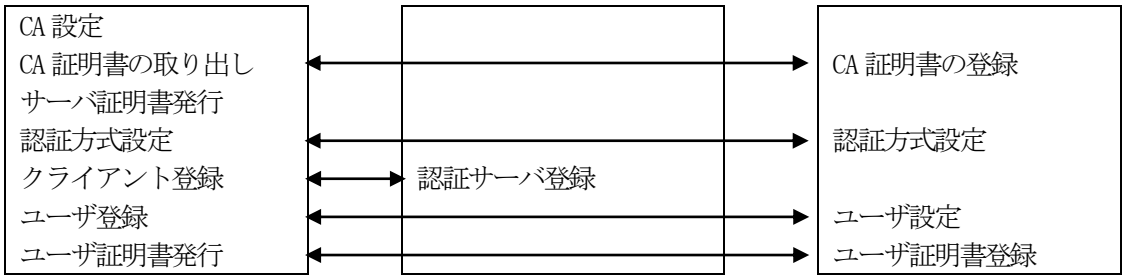
1.5. EAP-TLS 認証を利用する

■ 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。
またサプリカントでは、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。

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 の入力が必須です。
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

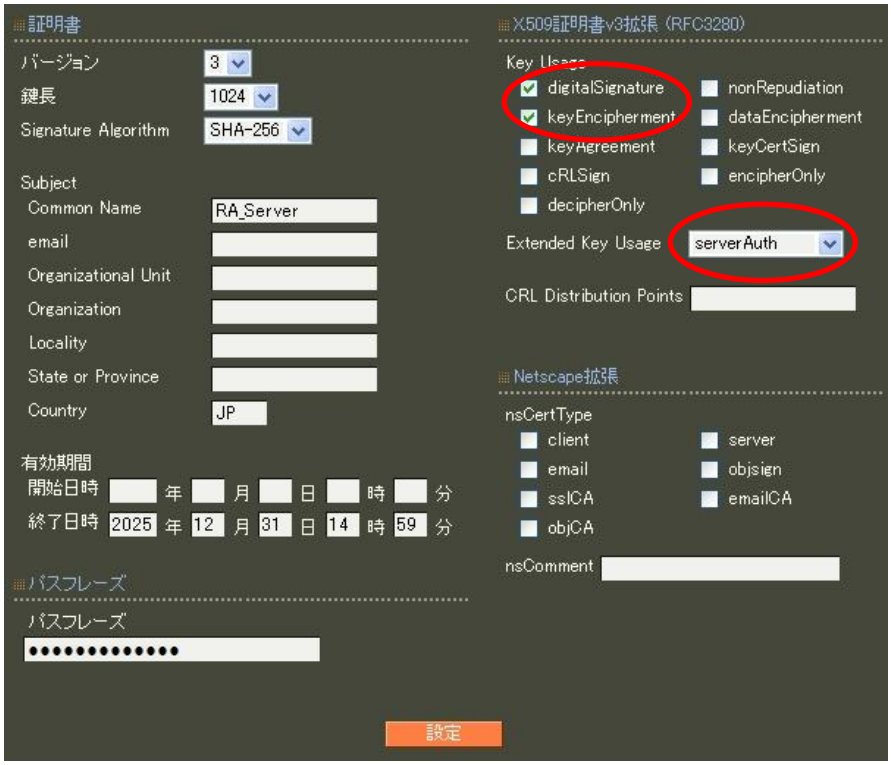
※[失効リスト更新間隔]で指定した間隔で失効リストの更新を行わなかった場合、証明書が有効な場合でも認証ができなくなります。必ず失効リストの更新処理を設定した間隔で行ってください。
また更新した失効リストを有効にするには、RADIUS サービスの再起動が必要になります。
CA の再編集はできませんので設定の際は内容を十分確認してください。
また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

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



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。

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。

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)

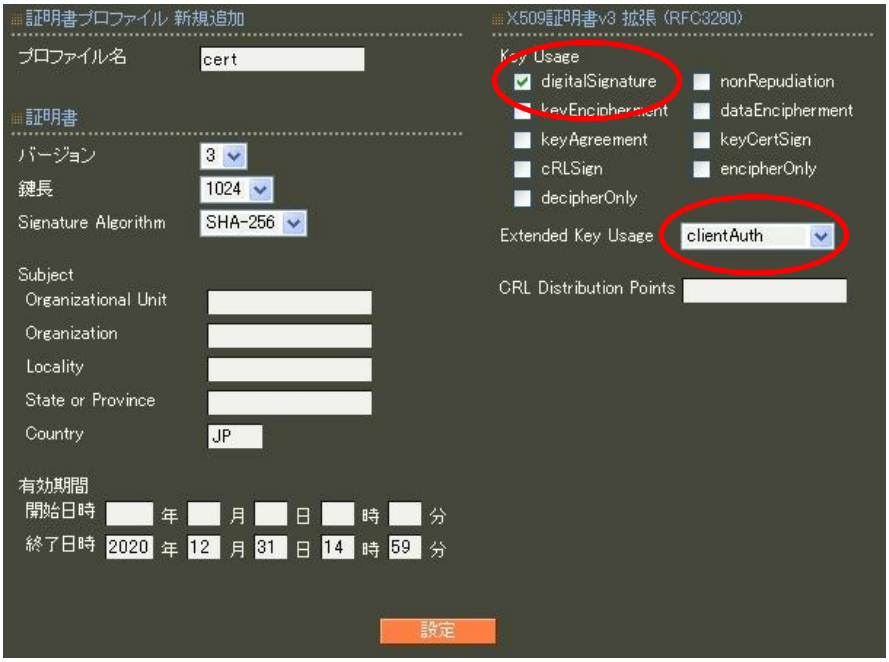
設定条件に従い認証方式に EAP-TLS に設定します。プロファイル名は base_user とします。

証明書プロファイルの作成　(RADIUS／プロファイル／証明書)

証明書プロファイルを作成しておくと EAP-TLS 認証で必要なユーザ証明書の発行が簡単に行えるようになります。

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良いでしょう。

・Key Usage：digitalSignature
・Extended Key Usage：clientAuth



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。

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プ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。

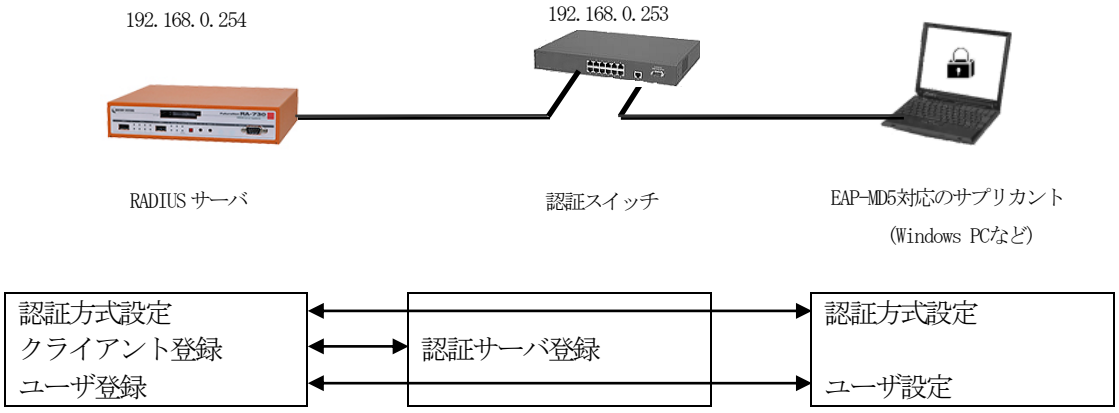
以上で設定は終了です。

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。
またサプリカントでは、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ません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。

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。

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じものを設定します。

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。

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。

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。

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。

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、ユーザー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

SLAVE 側

設定情報の同期設定

同期コンフィグ一覧

同期装置一覧

上記設定後は、下記画面の様になります。

・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。

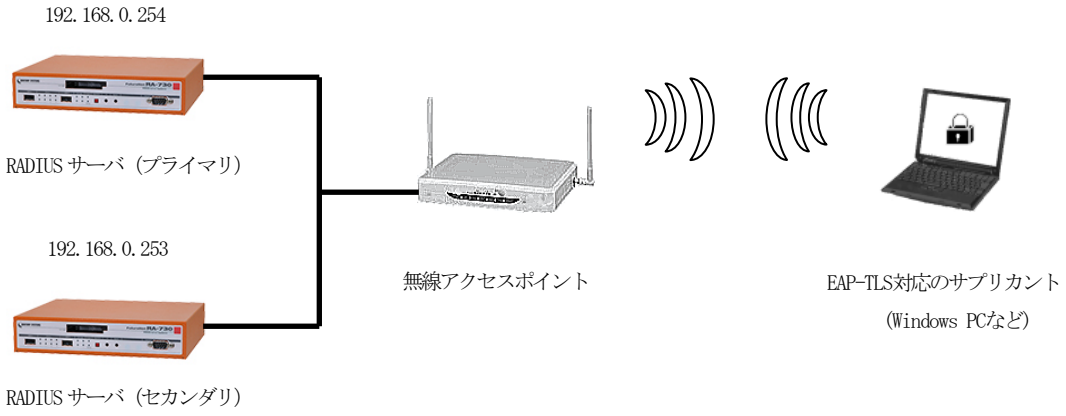
以上で設定は終了です。

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/アカウンティ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。

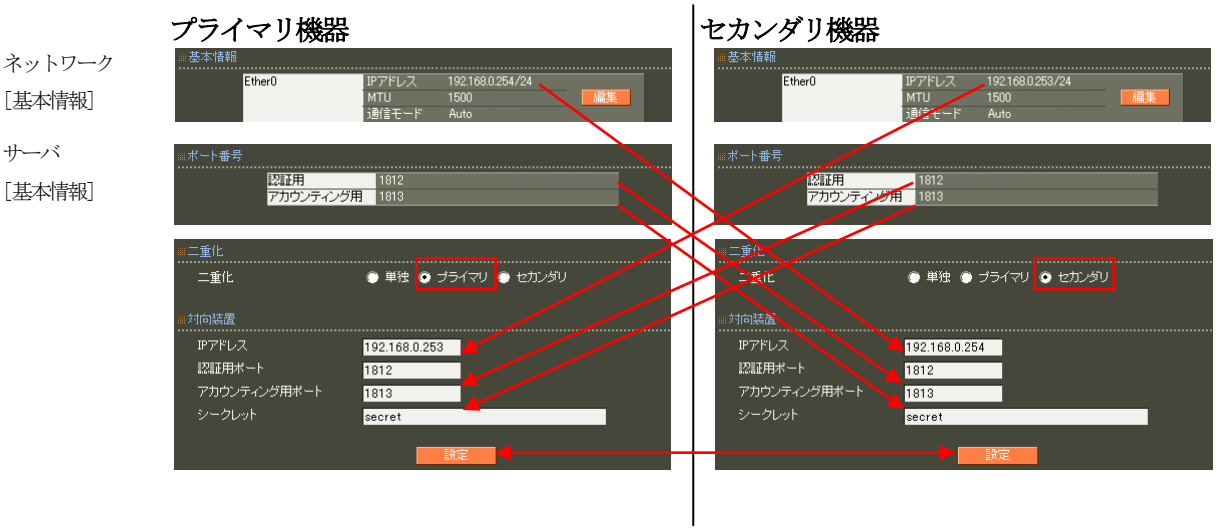
※二重化機能を使用する場合、必ずNTPサーバを設定の上ご利用ください。

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
アカウンティング用ポート	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、アカウンティング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。

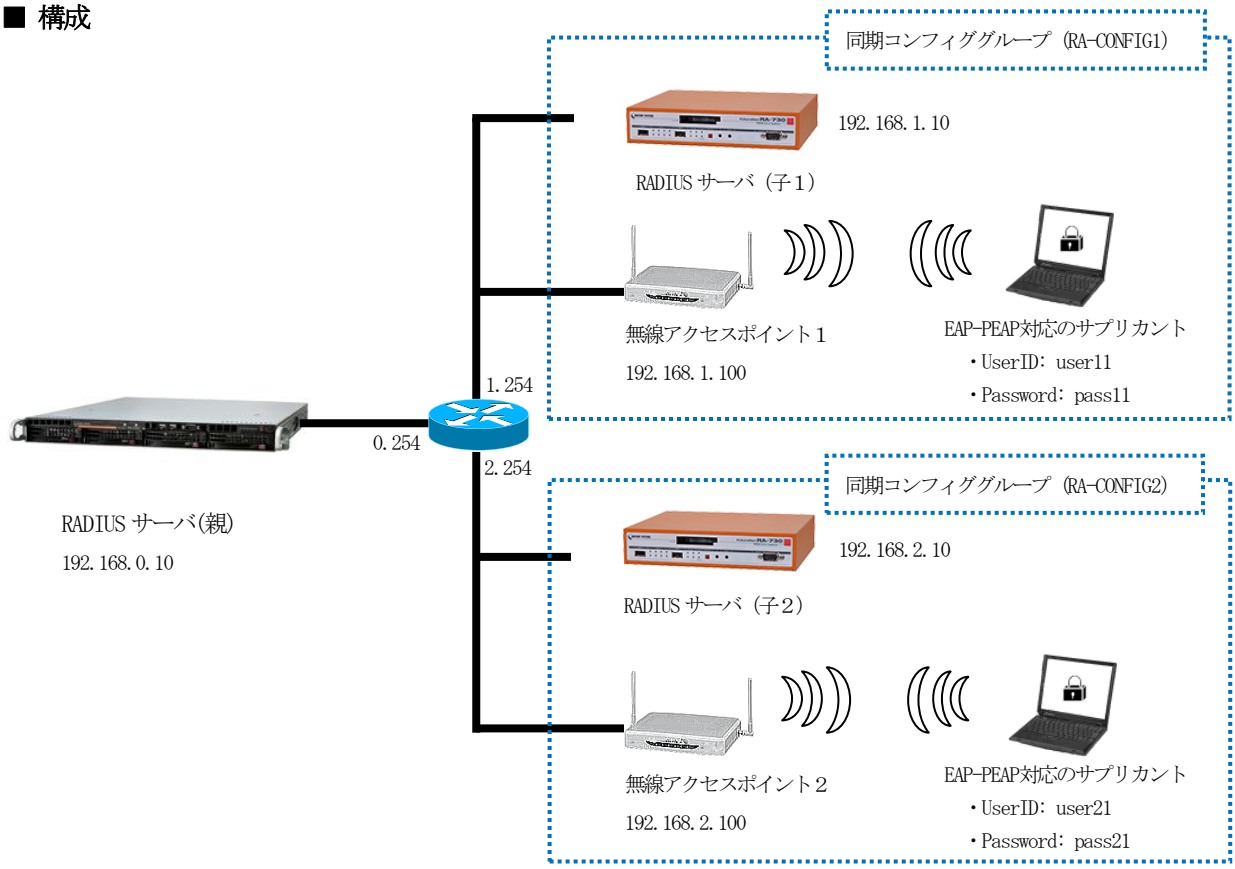
以上で設定は終了です。

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/アカウンティ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/アカウンティ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、認証及びアカウンティングに使用するポート、シークレットの設定を行います。
サプリカントでは、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
アカウンティング用ポート	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。

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-KO1
同期装置名（子２）	RA-KO2

設定情報の同期で 設定・編集 ボタンを押して、親の情報を設定します。

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：

子２設定例：

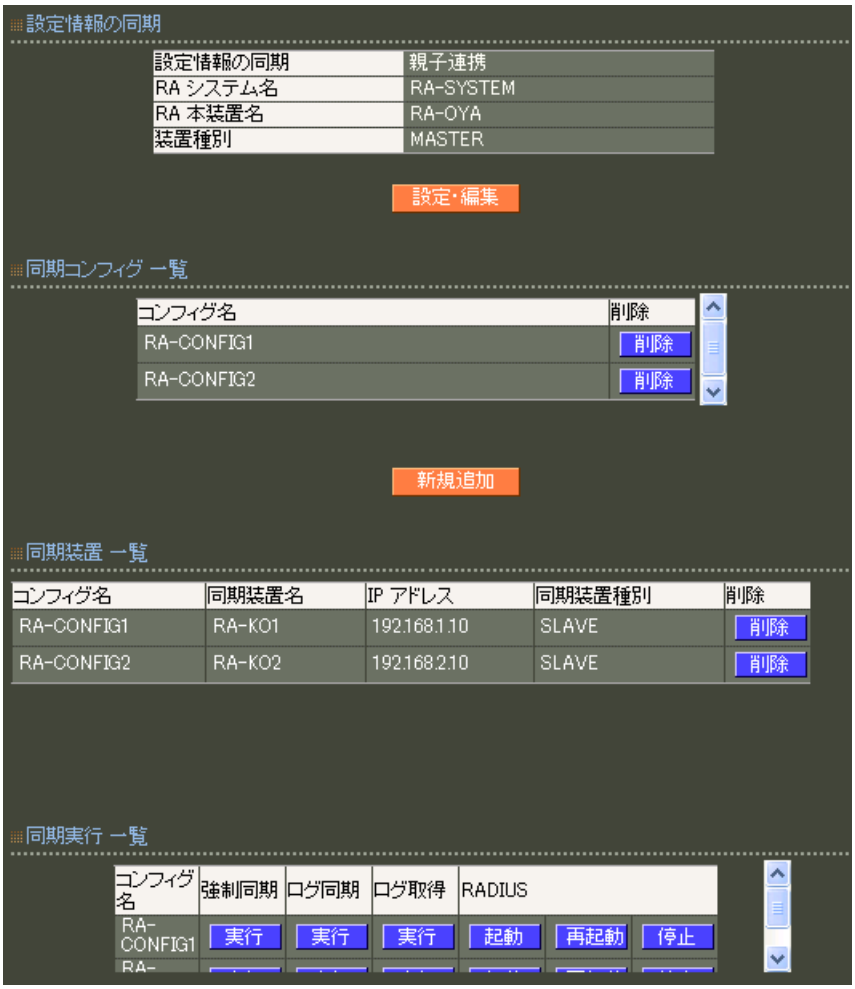
同期装置一覧で、各コンフィグに所属する装置を追加します。

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：

子２設定例：

上記設定完了後、以下の画面が表示されます。



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 の入力が必須です。
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 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)

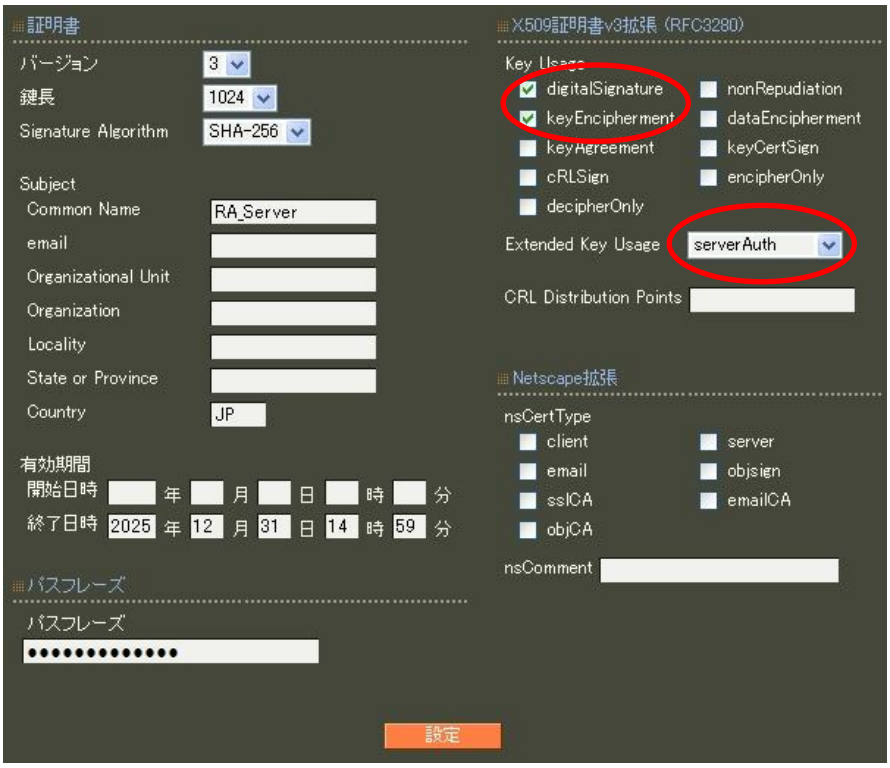
CA にて RADIUS サーバの証明に使用するサーバ証明書を発行します。

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：

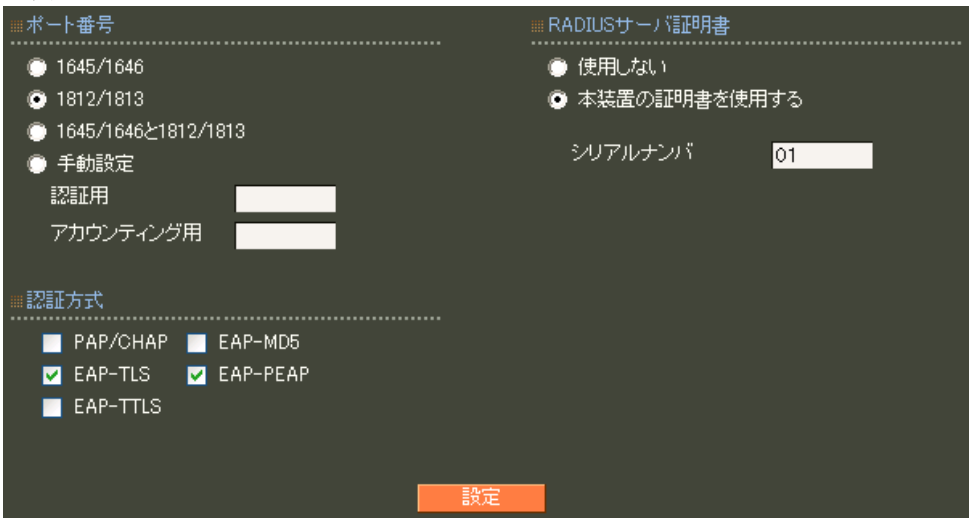


※ バージョン3 のサーバ証明書を作成する場合には、通常最低限以下の
Key Usage/Extended KeyUsage を指定するようにします。
・Key Usage：digitalSignature および keyEncipherment
・Extended Key Usage：serverAuth
実際にどの Key Usage/Extended Key Usage を必要とするかは通信相手のソフトウェアに依存します。

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。

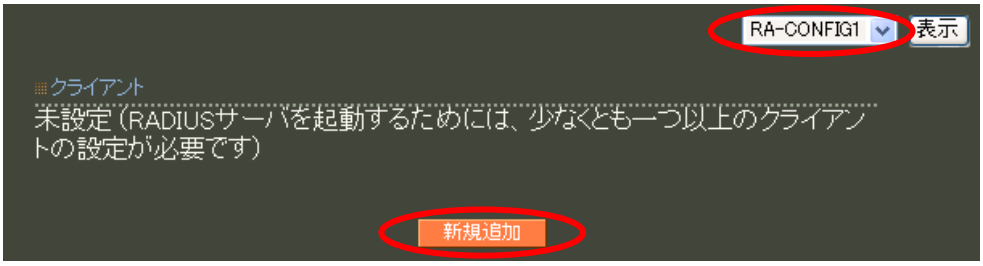
設定例：



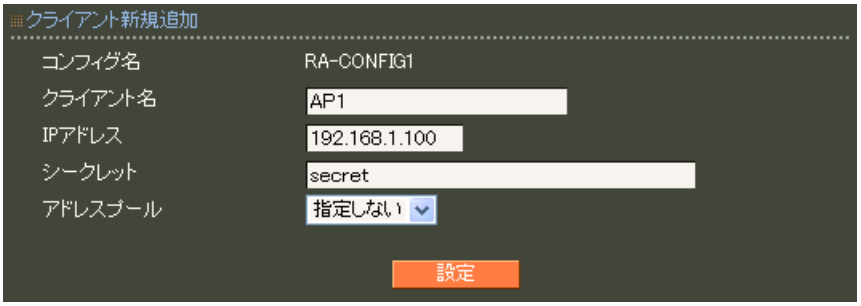
RADIUS クライアントの設定　(RADIUS／サーバ／クライアント)

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じものを設定します。

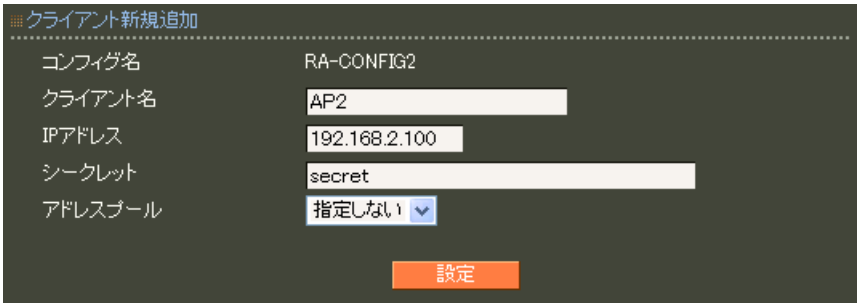
ここでも、子１、子２のコンフィグを指定して 新規追加 ボタンを押下します。



子１設定例：



子２設定例：



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／プロファイル／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

子２設定例：

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)

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：

子２設定例：

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。

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のユーザを作成することができます。

子１設定例：

子２設定例：

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）

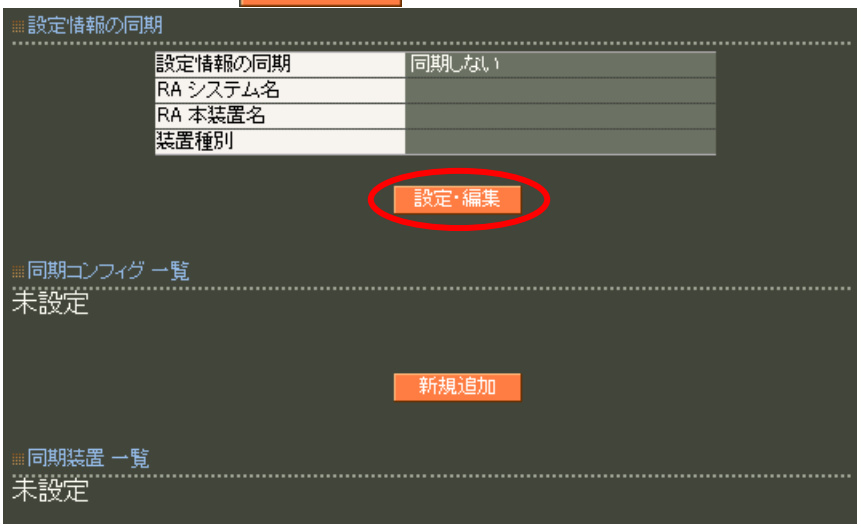
子１、子２のそれぞれの Ether0 の IP アドレスに **192.168.1.10/24、192.168.2.10/24** に設定します。MTU 及び通信モード、Ether1、Ether2 はお使いの環境に合わせて設定してください。
ここでは初期値のままとします。
デフォルトゲートウェイをそれぞれ 192.168.1.254、192.168.2.254 に設定します。

子１の場合

子２の場合

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

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

子２の場合

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。

「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。

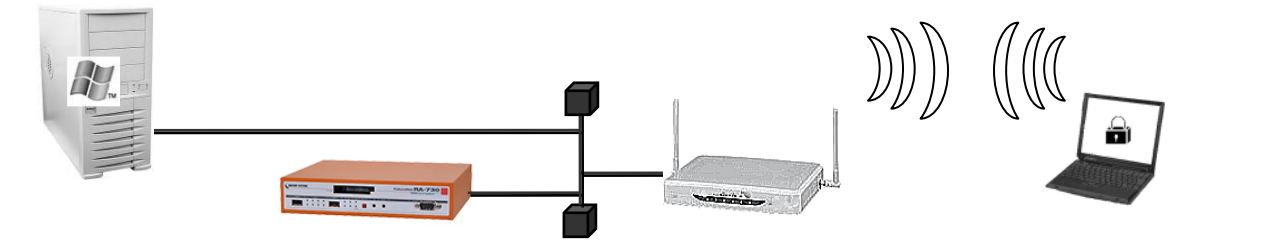
3. 連携機能を利用する

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

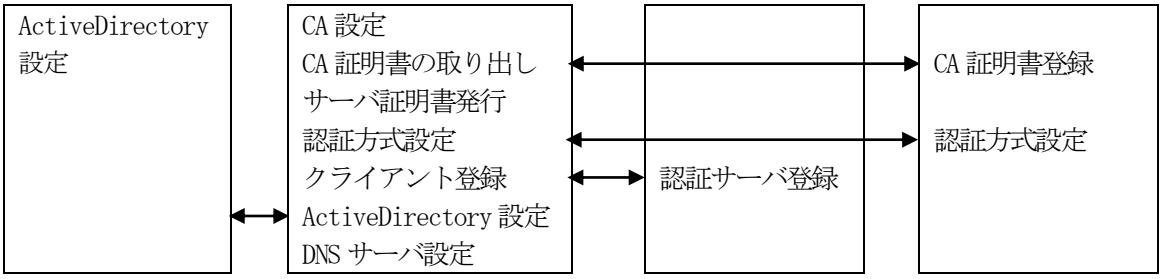


ActiveDirectoryサーバ
ad.example.jp
192.168.0.1

RADIUS サーバ
192.168.0.254

無線アクセスポイント
192.168.0.253

EAP-PEAP 対応のサプリカント
(Windows PCなど)



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

初めに 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。

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。

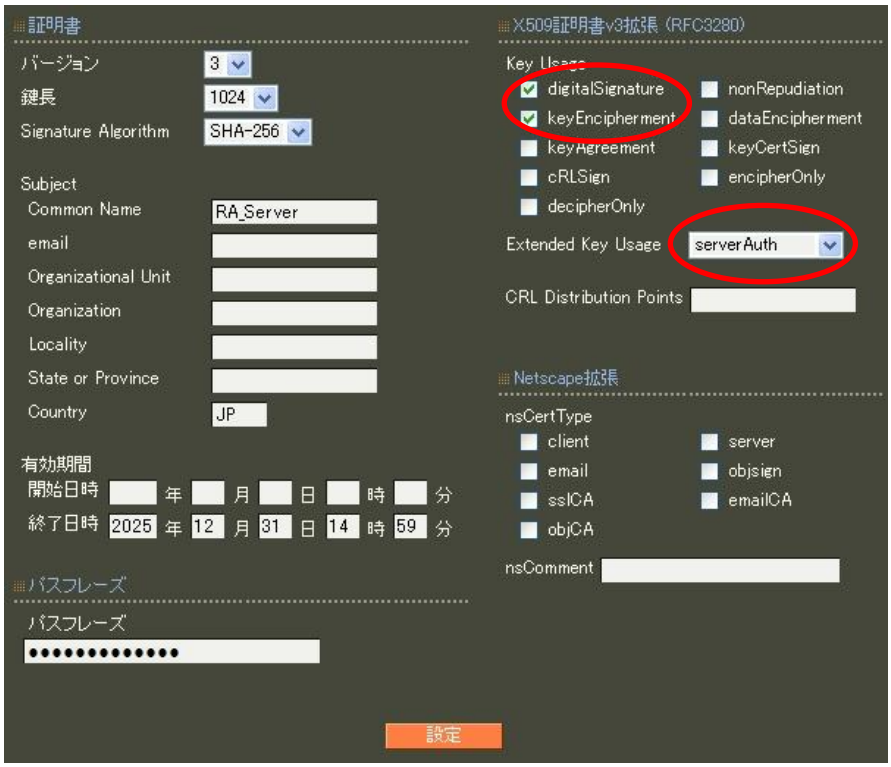
CA 作成後は CA 証明書画面より 取り出し ボタンを押下して CA 証明書を取得し、サプリカントへインストールします。

【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：



※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）

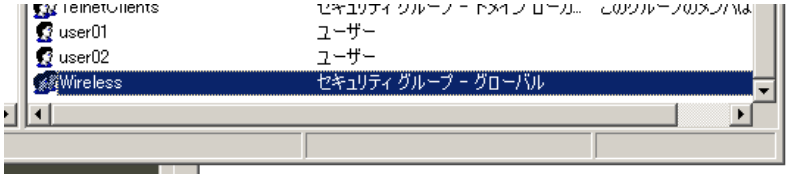
ActiveDirectory 画面では、ActiveDirectory の**ドメイン名と管理者ユーザ ID、管理者パスワードに**ドメインコントローラの **Administrator 権限のユーザの管理者 ID** と**パスワード**を入力します。所属グループは今回新たに追加した **Wireless** を指定します。

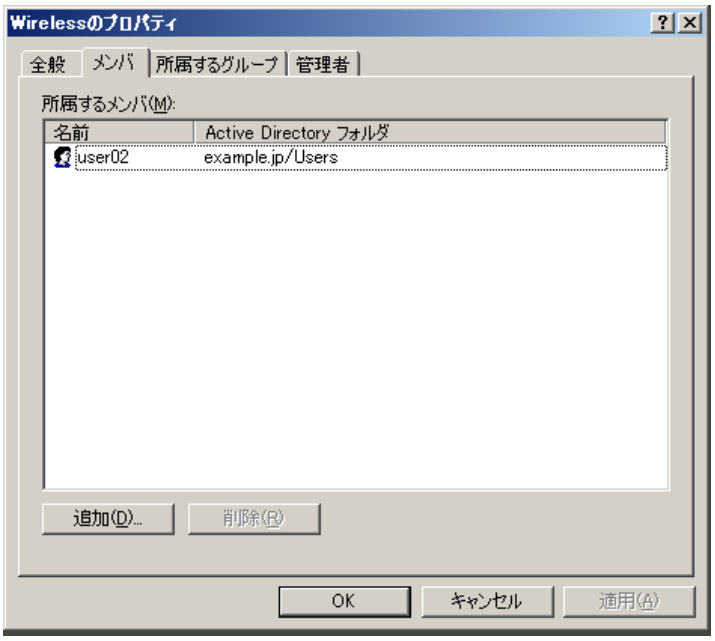
所属グループについて

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。
認証する必要の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じものを設定します。

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。

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。

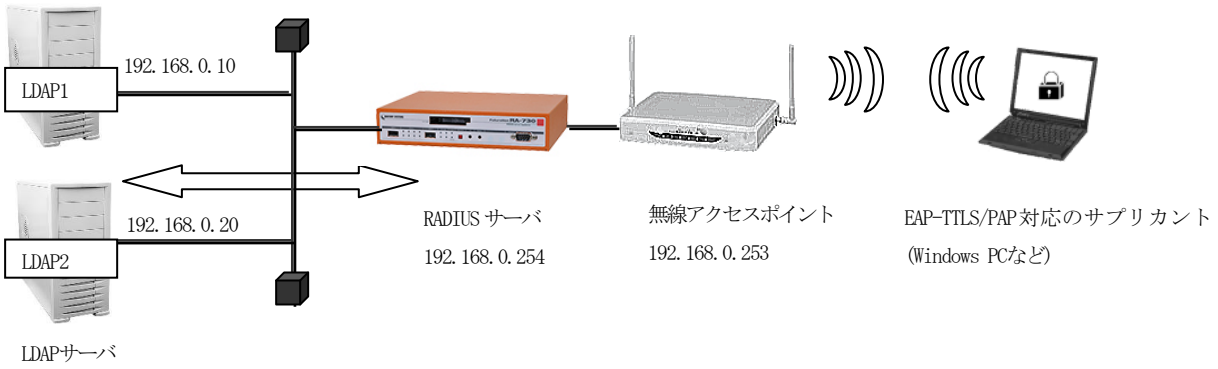
以上で設定は終了です。

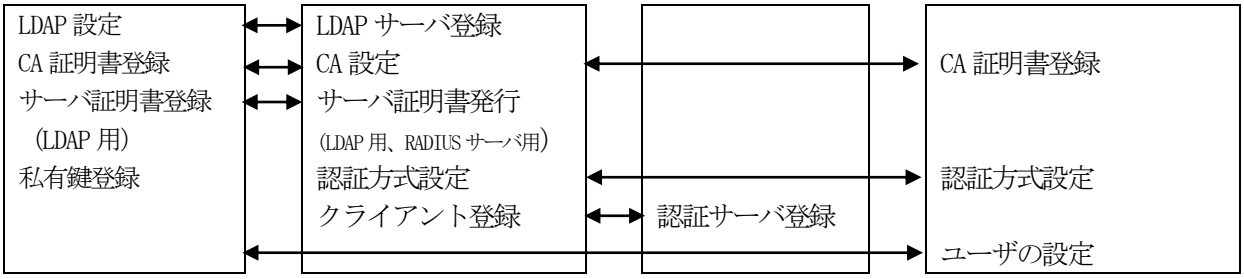
3.2. LDAP 連携を利用する

■ 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。

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

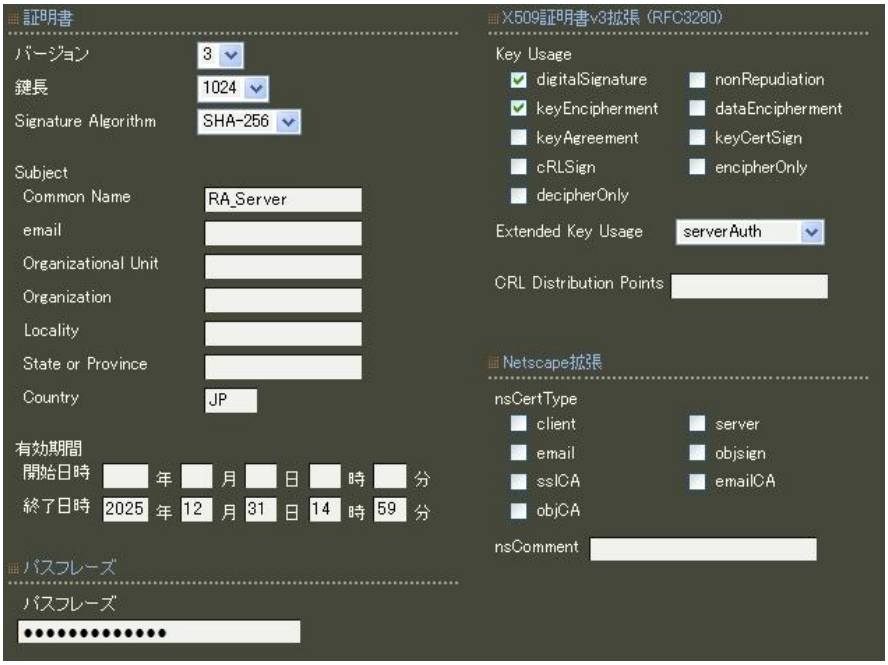
※CA の再編集はできませんので設定の際は内容を十分確認してください。
　また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

証明書の発行 (CA／証明書)

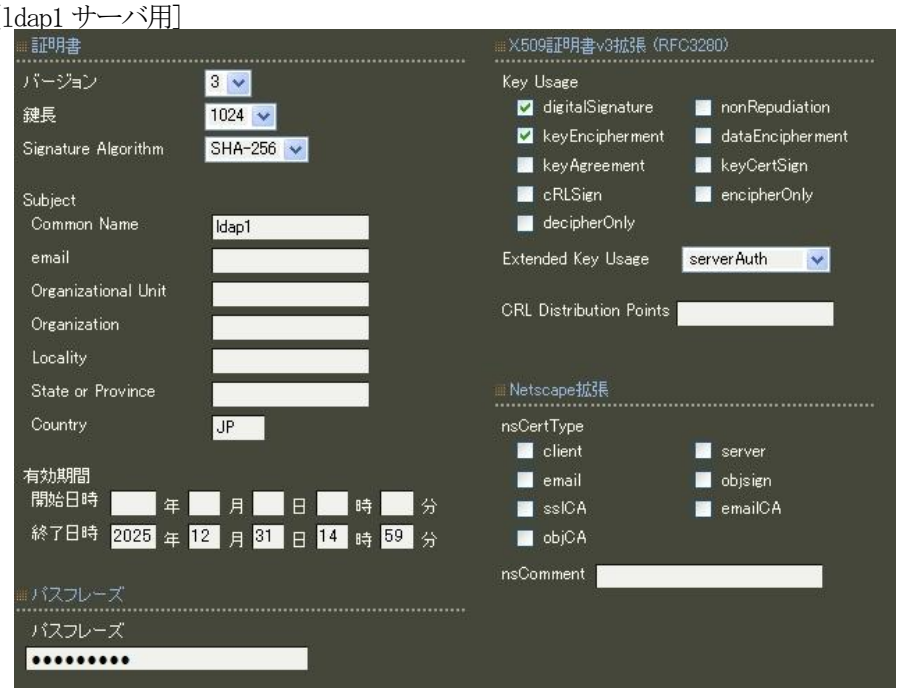
ここではEAP-TTLS で使用する RADIUS サーバ証明書及び、LDAPS で使用する LDAP1、LDAP2 用の２通のサーバ証明書とクライアント(RADIUS サーバ)証明書を発行します。証明書画面から 新規追加 ボタンを押下します。
発行した LDAPS サーバ用の証明書及び秘密鍵を取り出し、LDAP サーバへ登録します。

※ LDAP を利用する際は LDAP サーバに対して RADIUS サーバが接続を行うクライアントになります。したがって LDAPS で使用する証明書は、LDAP サーバがサーバ用、RADIUS サーバがクライアント用となります。

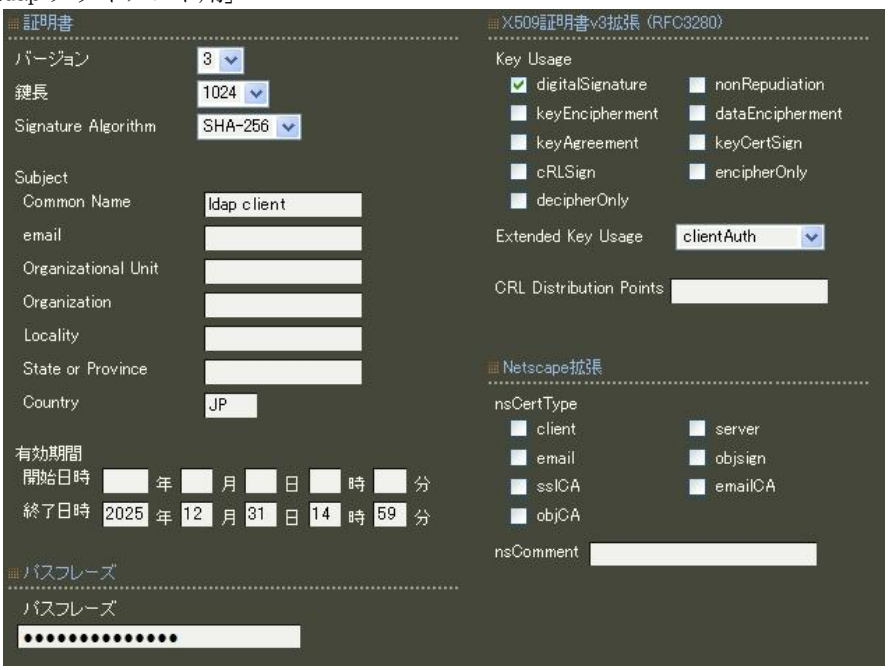
[RADIUS サーバ用]



[ldap1 サーバ用]

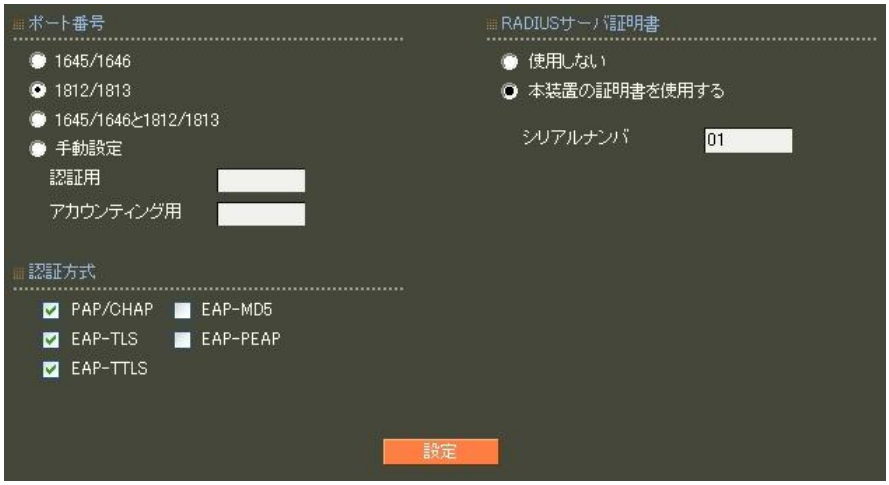


[ldap クライアント用]



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

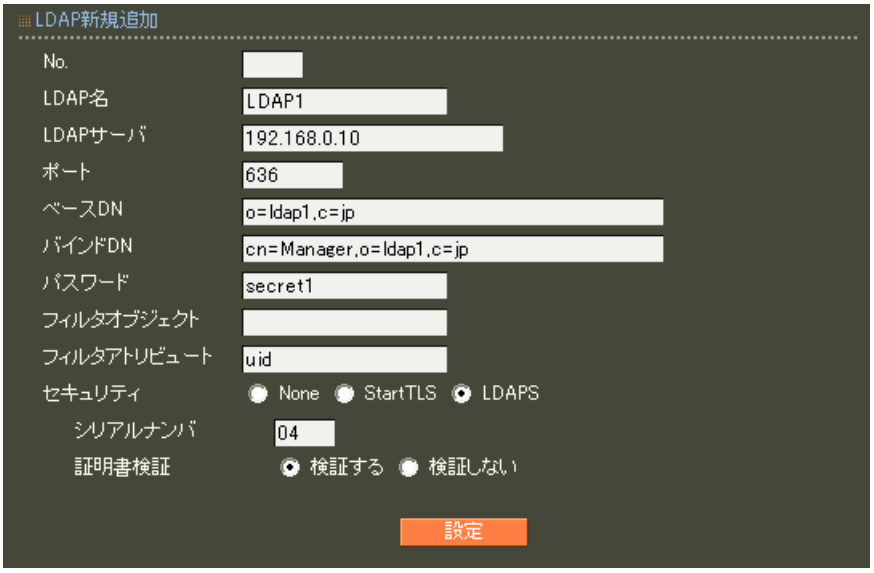
フィルタアトリビュート	uid
セキュリティ	LDAPS
シリアルナンバ	CA にて作成したクライアント(ldap ｸﾗｲｱﾝﾄ)用のもの
証明書検証	検証する

＜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=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 ｸﾗｲｱﾝﾄ)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：



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。

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。

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。プロファイル名は **user** とします。

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。

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。

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。

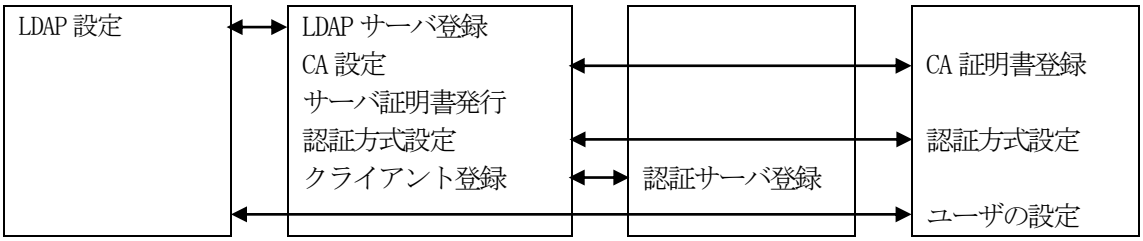
■ 構成

LDAPサーバ
192.168.0.10

RADIUSサーバ
192.168.0.254

無線アクセスポイント
192.168.0.253

EAP-PEAP対応のサプリカント
(Windows PCなど)



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。

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。

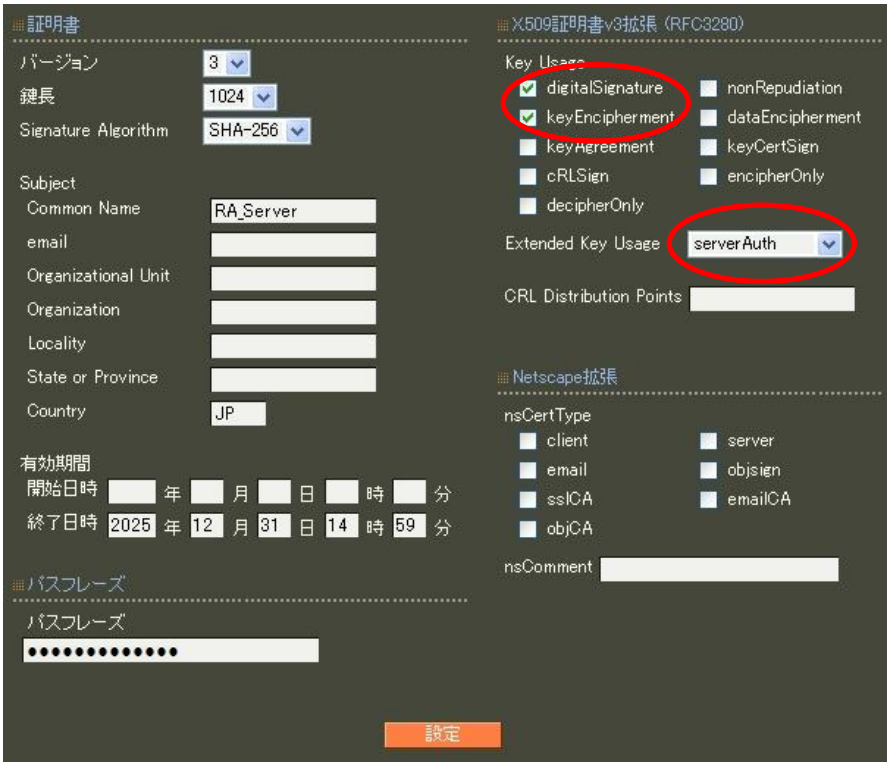
鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※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：



※ 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。

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ァイルの作成（RADIUS／プロファイル／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、プロファイルは作成する必要はありません。

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）

今回、応答アトリビュートは使用しませんので、プロファイ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、ユーザーズガイド 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”csRANTLMHash”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 'csRANTLMHash'
  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 ( csRANTLMHash ) )
```

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。

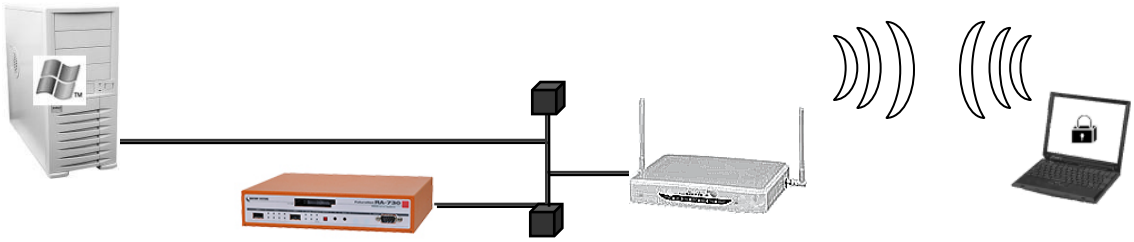
3.4. ActiveDirectory をLDAPとして利用する

■ 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

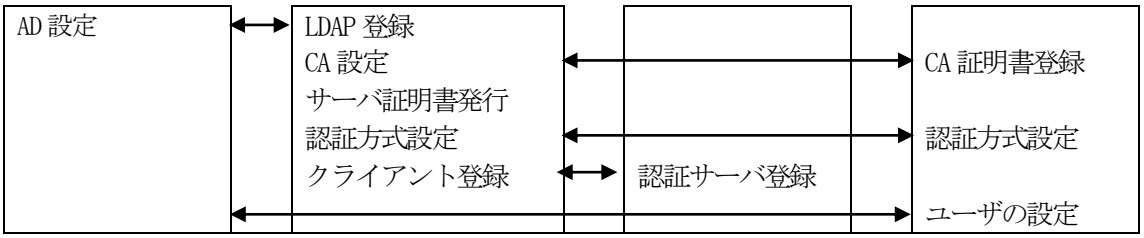


ActiveDirectoryサーバ
ad.example.jp
192.168.0.1

RADIUSサーバ
192.168.0.254

無線AP
192.168.0.253

EAP-TTLS/PAP対応のサプリカント
(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。

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

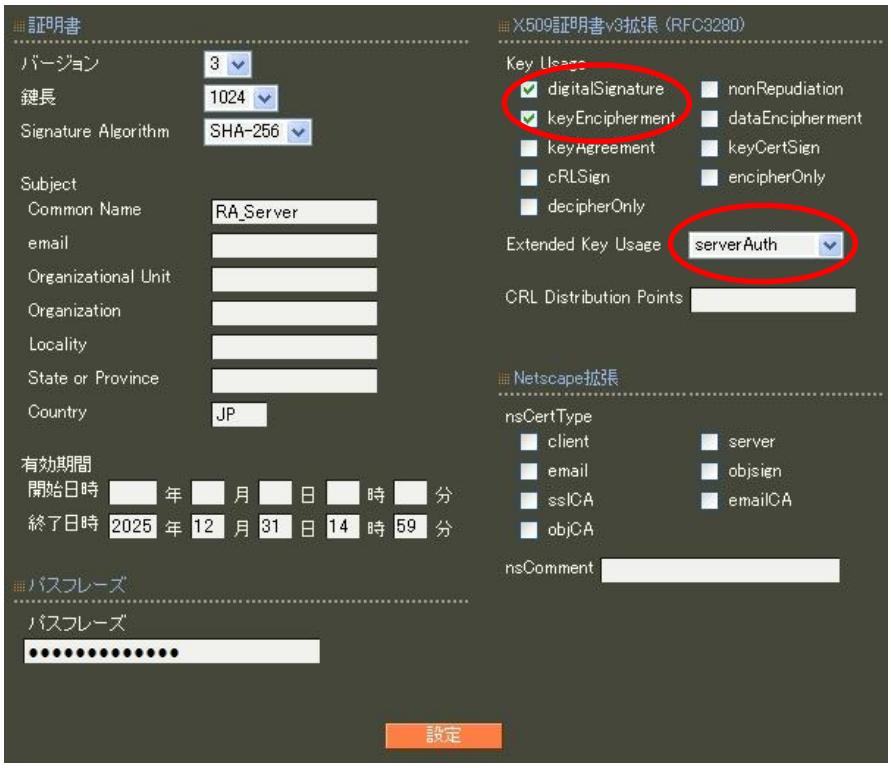
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※ 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：

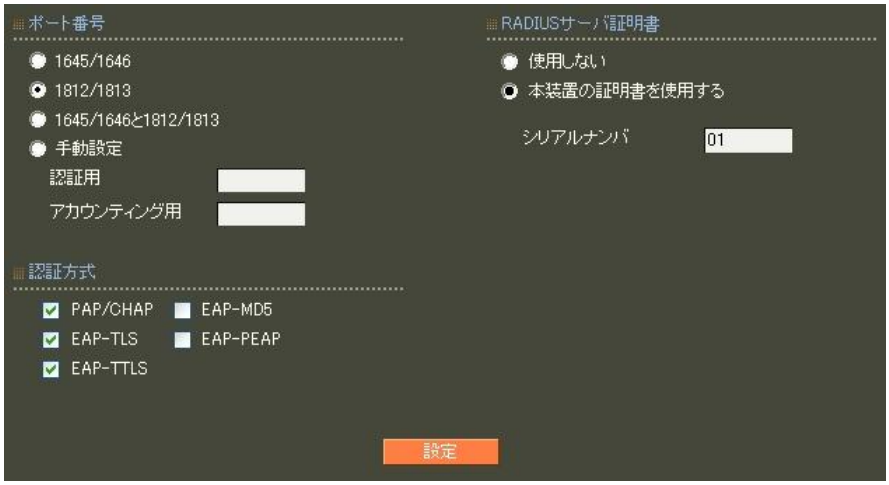


・Key Usage：digitalSignature および keyEncipherment
・Extended Key Usage：serverAuth

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。
※2Active 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。ここでは入力の必要はありません。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 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。

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を **EAP-TTLS/PAP,CHAP** で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。

応答アトリビュートプロファイルの作成（RADIUS／プロファイル／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。プロファイル名は **reply** とします。作成したプロファイ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：

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** と応答アトリビュートプロファイル **reply** を選択してユーザプロファイルを作成します。プロファイル名は **user** とします。

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ァイルと設定します。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ァイル **user** を選択して 設定 ボタンを押します。

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。

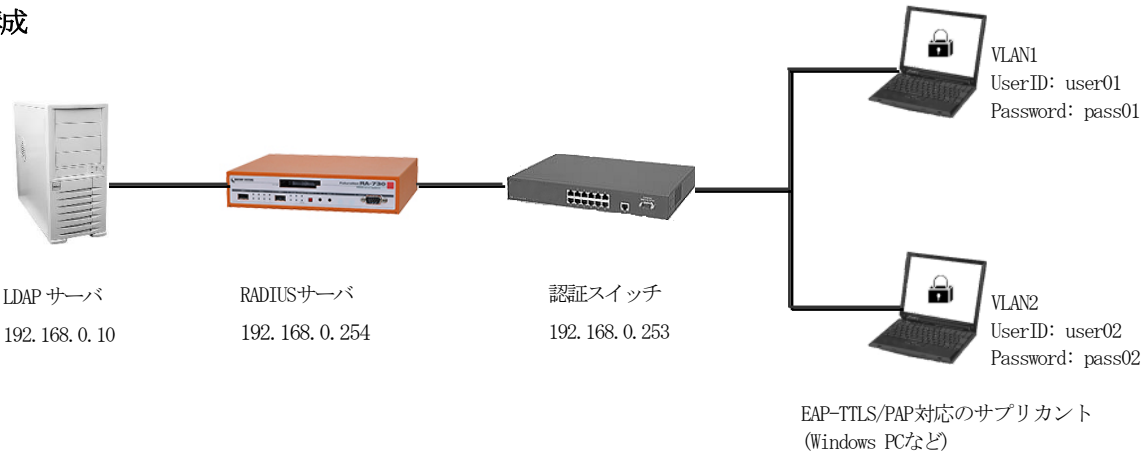
以上で設定は終了です。

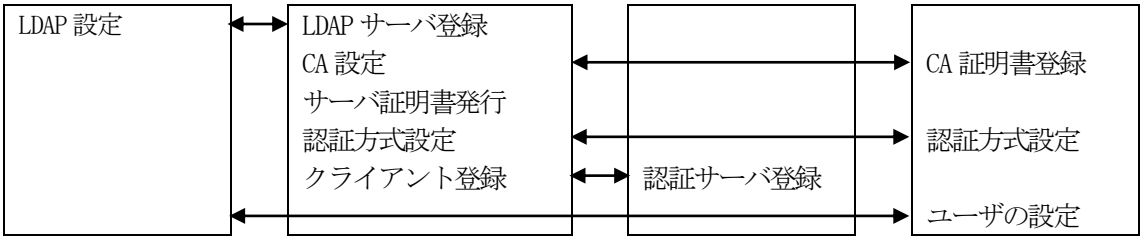
3.5. LDAPサーバから応答アトリビュートを取得する

■ 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。

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。

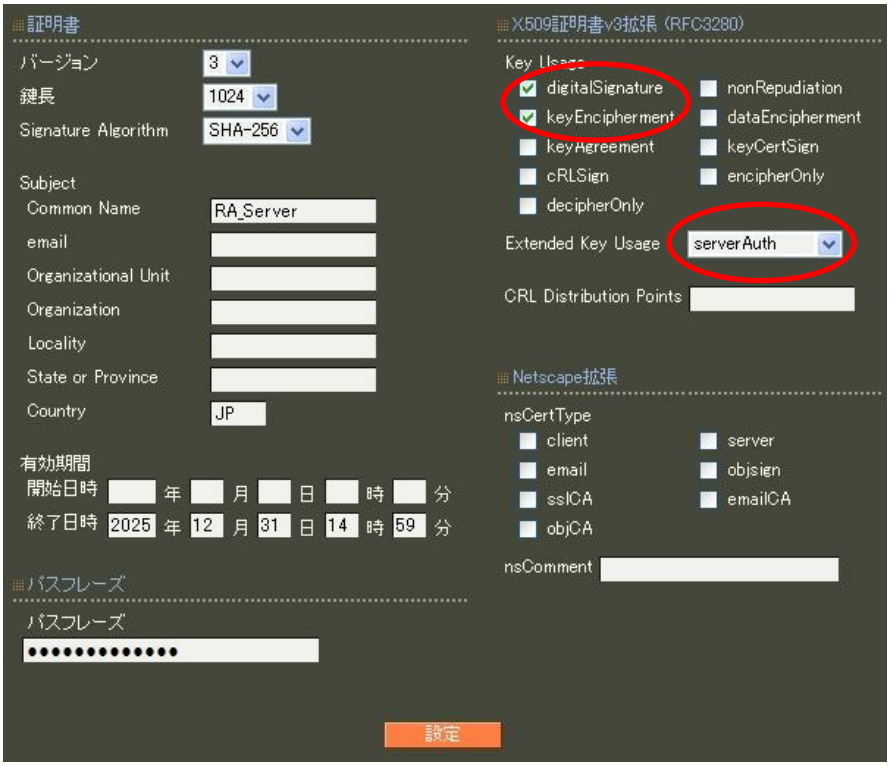
鍵長	1024
Signature Algorithm	SHA-256
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※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：



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 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 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：

全ての LDAP 設定が終了すると以下のようになります。

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。

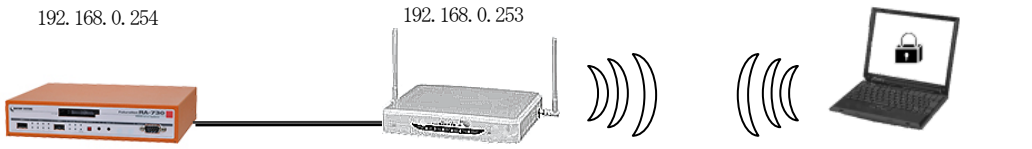
4. ファイル読み込み機能を利用する

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、ユーザーズガイドの付録[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

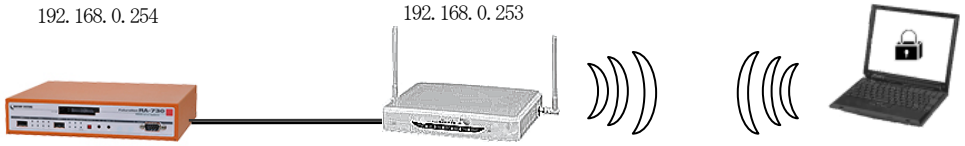
リセットで「する」を選択すると登録されているプロファイル、ユーザをリセット(削除)した上で新規にユーザ登録を行います。そのため上記記述以外にプロファイルセクションを指定する必要があります。
リセットで「しない」を選択すると既存の設定のままユーザのみが追加されます。

4.2. 新規でユーザプロファイ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ァイ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ァイル 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ァイル名	base_user
証明書プロファイル名	cert
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、ユーザーズガイドの付録[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。

【ユーザプロファイル、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ァイル等は登録済みですので、登録するユーザプロファイルとユーザセクションを記述します。

```
[RADIUS|プロファイル|ユーザプロファイル]
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。

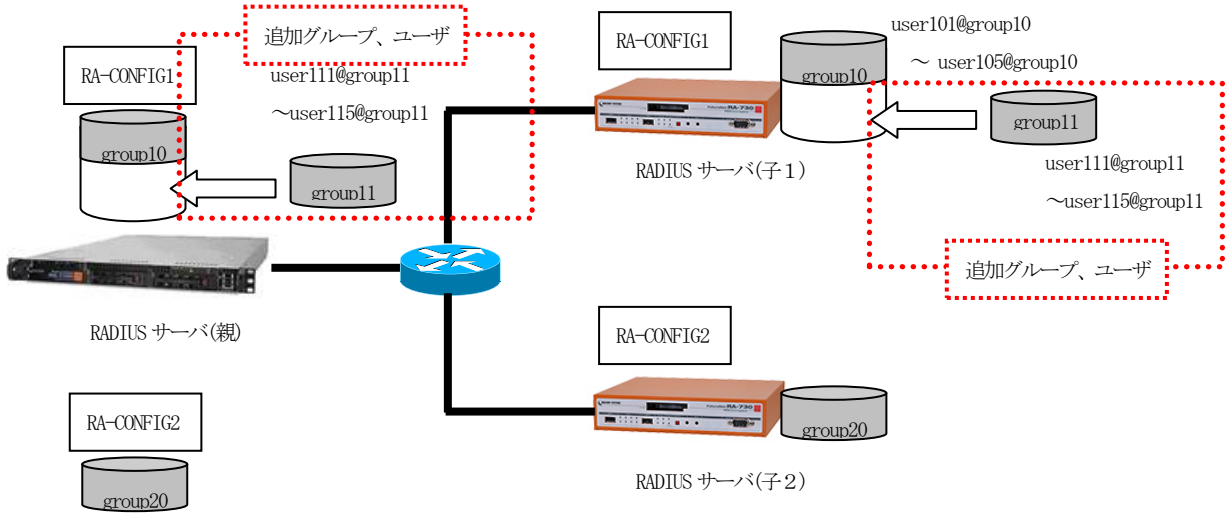
4.3. 証明書を発行する

■ 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	gruop11
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。

ユーザ基本プロファイル名	base1
ユーザプロファイル名	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=
  enciperOnly=
  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。

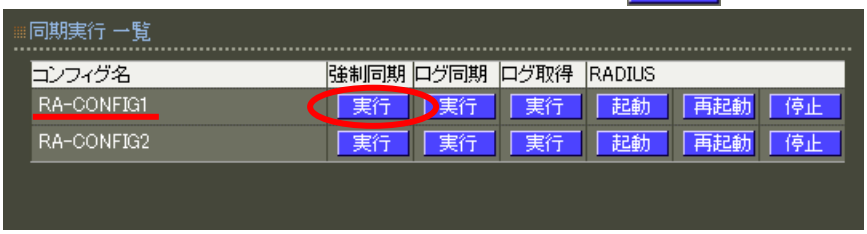
メニューの「RADIUS」－「ユーザ」－「ファイル読み込み」から RADIUS ユーザファイル読み込み画面を開きます。リセット は **しない** 、設定ファイルにこれまでに作成した設定ファイルを指定し、適用するコンフィグ名を選択して、復帰ボタンを押下します。
以上で新しいユーザの追加、証明書の発行が行なわれます。

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プリカントへ設定します

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/アカウンティング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。

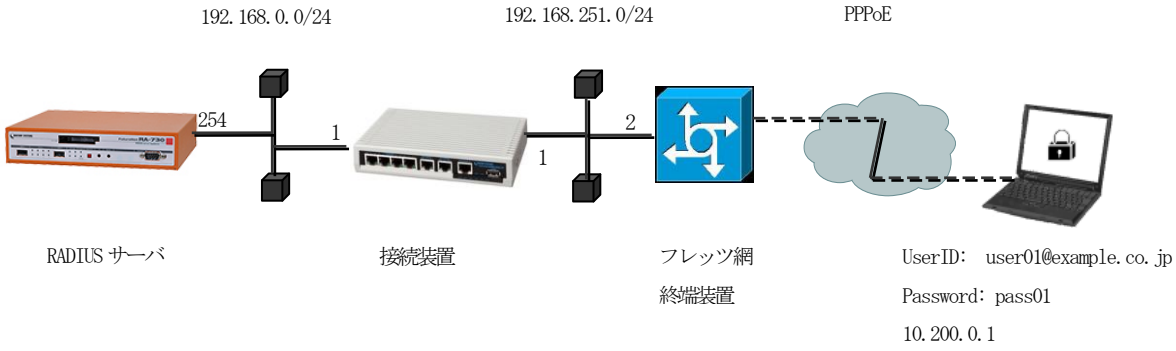
5. 認証プロファイル/応答プロファイルを利用する

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、プロファイルを登録します。
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

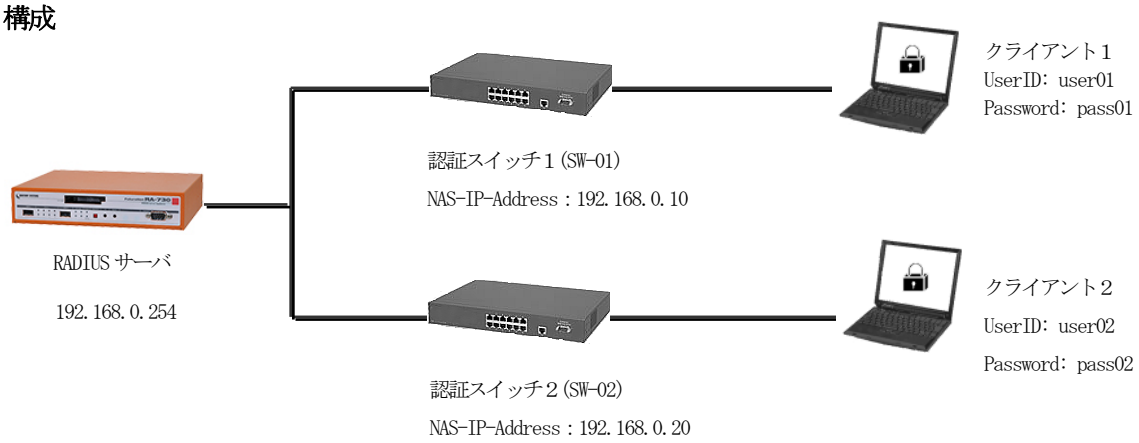
以上で設定は終了です。

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じものを設定します。

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

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。

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

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

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。

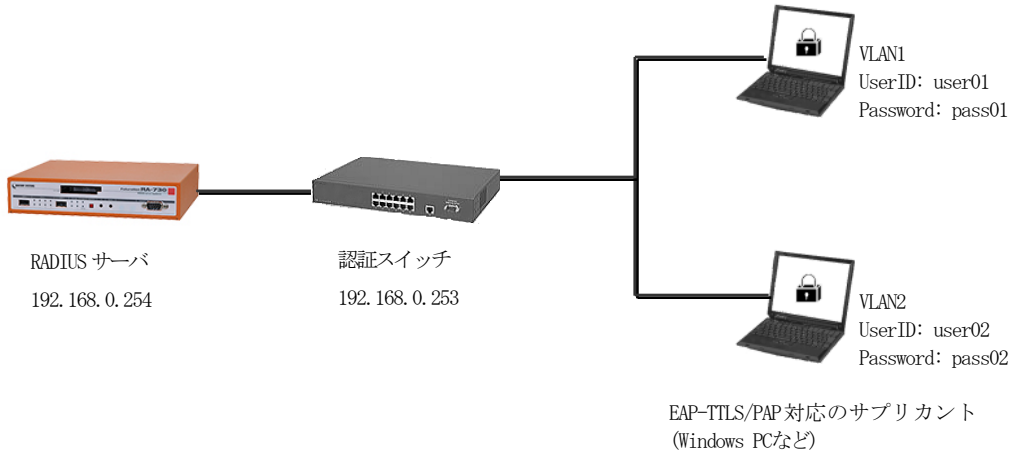
以上で設定は終了です。

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。

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 の入力が必須です。
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。

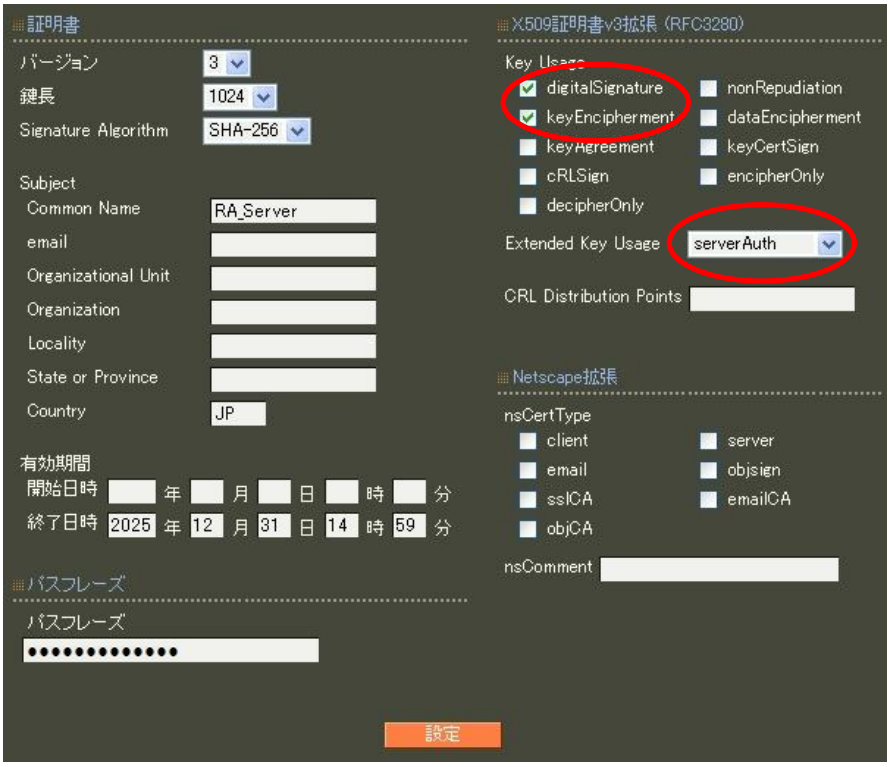
CA 作成後は、CA 証明書画面より 取り出し ボタンを押下して CA 証明書を取得し、サプリカントへインストールします。

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 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じものを設定します。

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。

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。

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。

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。

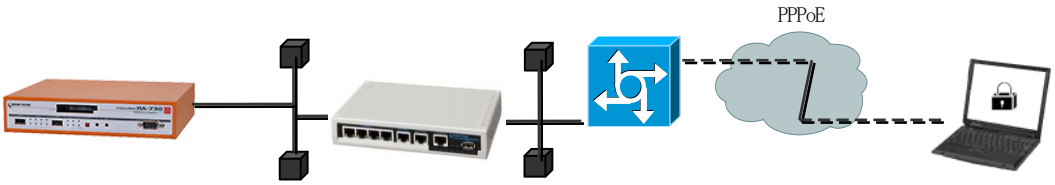
6. ＩＰアドレスの払い出しを設定する

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

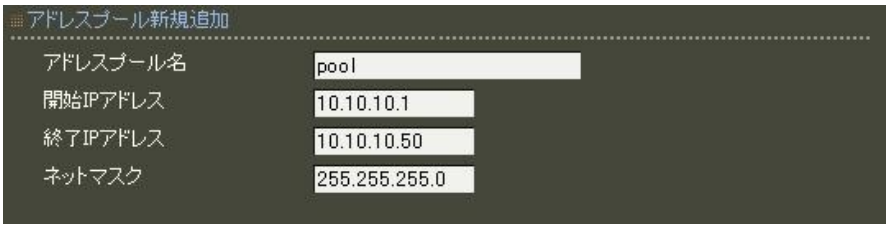
ここでは下記の内容で設定を行います。

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。



（1）ユーザ基本プロファイルで指定する方法

IP アドレス割り当て設定（RADIUS／プロファイル／ユーザ基本情報）

プロファイルで指定する場合はユーザ基本情報プロファイル画面で 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。

（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ァイルの IP アドレス割り当ては **未使用** を選択します。

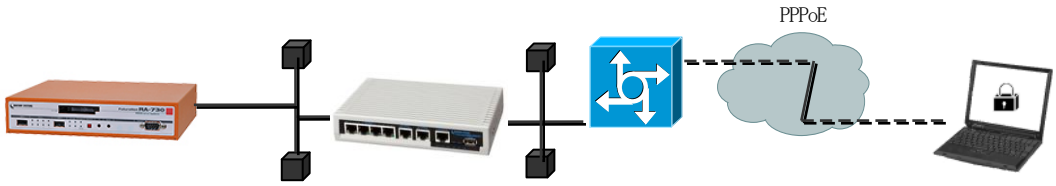
以上で設定は終了です。

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。

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

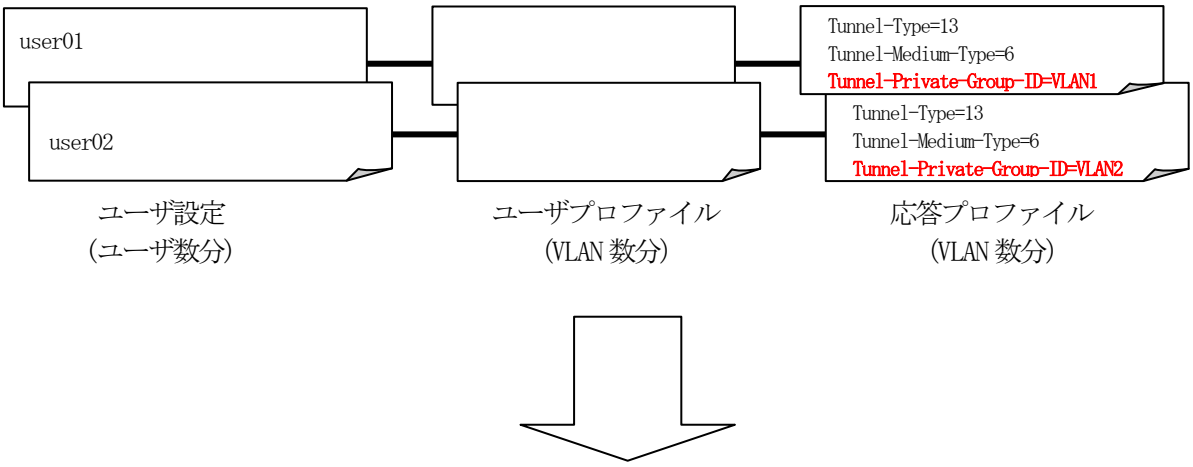
7.1. ユーザ毎にVLAN IDを設定する

■ 概要

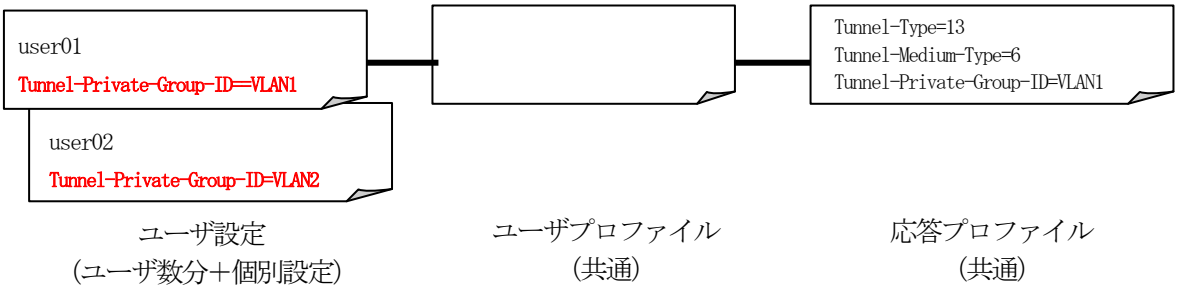
ここではユーザの個別設定機能によりプロファイルで指定した内容とは別にユーザ毎に異なるアトリビュートを設定する例を紹介します。
[5.3 ユーザ毎に VLAN ID を設定する]では、ユーザ毎に応答アトリビュートプロファイルとユーザプロファイルを作成する例を紹介しました。
本節では、ユーザの個別設定機能でユーザ毎に異なる値のみ設定し、その他の共通の値は応答アトリビュートプロファイル１つにまとめる例を紹介します。

■ 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、Tunnnel-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。

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)

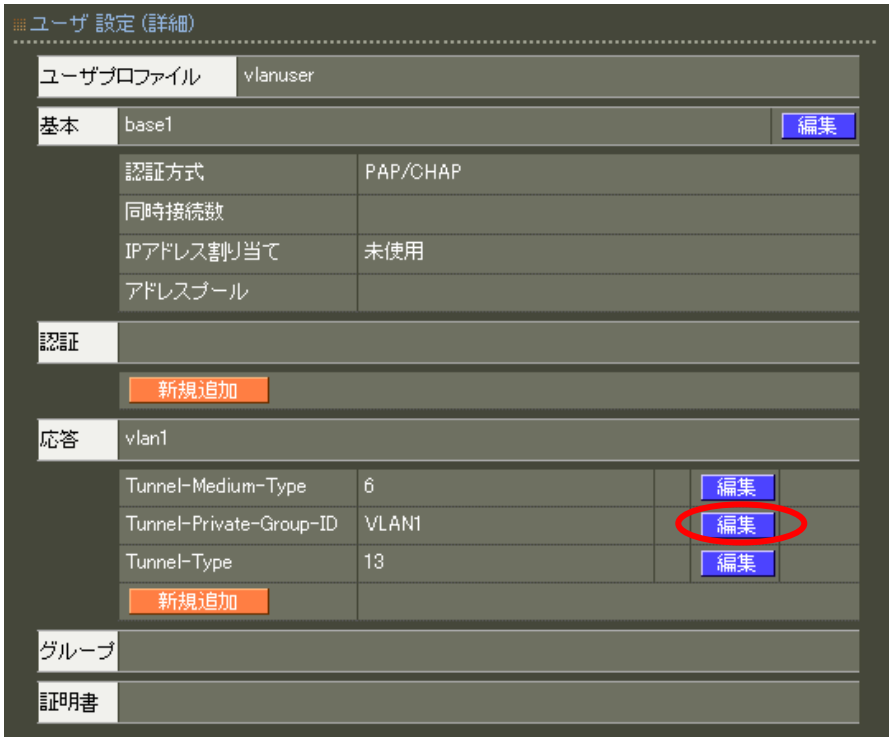
各ユーザ共通のプロファイルを作成します。
ここでは、ユーザ基本情報プロファイル **base_user**、応答アトリビュートプロファイル **vlan1** を選択したユーザプロファイル **vlanuser** を作成します。

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。

※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。



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。

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。

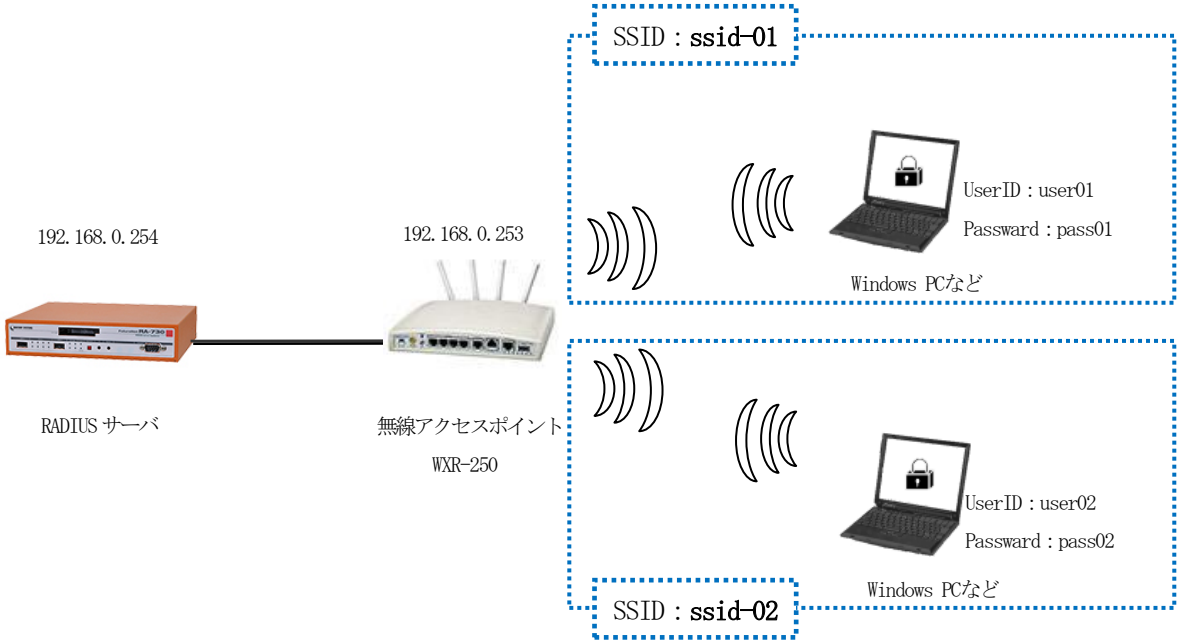
以上で設定は終了です。

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。

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。

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。

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。

以上で設定は終了です。

RA シリーズ 設定事例集 1.8.13(a)

2013 年 12 月版
発行 センチュリー・システムズ株式会社