EAP 対応 RADIUS サーバアプライアンス

FutureNet RA-1100

FutureNet RA-730

FutureNet RA-630

設定事例集

Ver 1.4.0

センチュリー・システムズ 株式会社

はじめに

本書はRA-1100/RA-730/RA-630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、設定の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RAの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Ver1.8.4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、Ver1.3.0以前の設定事例集をご利用ください。

商標の表示

－　目次　－

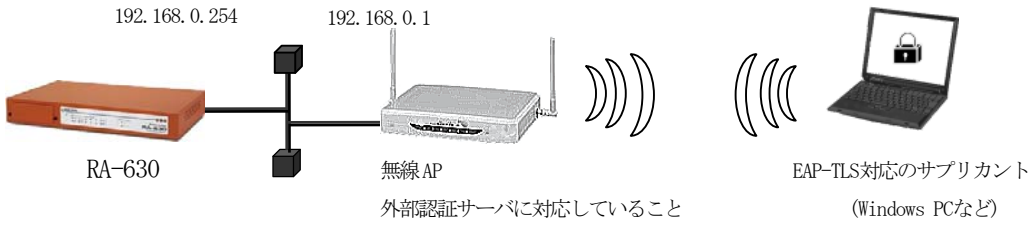
事例 1. 無線アクセスポイントでEAP-TLS認証を使用する

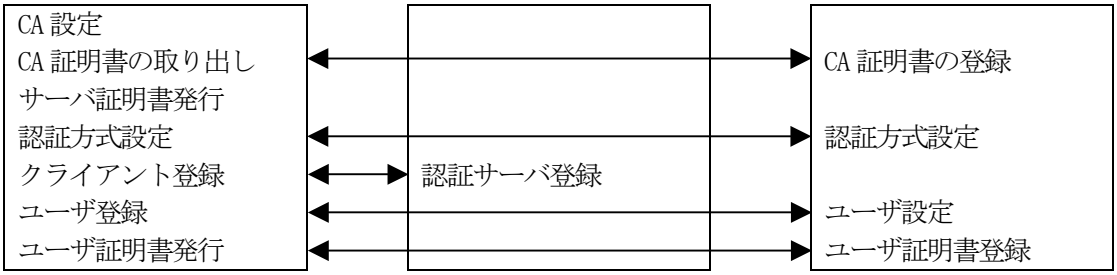
１．概要

ここでは無線LAN接続のセキュリティ向上の為、RA-1100/RA-730/ RA-630(以下RA)を使ったEAP-TLS認証を行う場合の例を紹介します。使用する無線アクセスポイント(以下無線 AP)が RADIUS による外部認証サーバに対応しており、かつサプリカントが EAP-TLS に対応している必要があります。

２．構成

無線 LAN を使用している環境に RA を追加するには、RA を無線 AP と通信できるネットワークに接続します。





無線 LAN 接続の認証に EAP-TLS 認証を使用するには RA に対して下記の設定を行います。

CA の設定
RA 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 クライアントとして無線 AP の登録
ユーザの登録
EAP-TLS 認証用にユーザ証明書を発行

無線 AP に対しては認証サーバ(*1) として RA の IP アドレス、認証及びアカウンティングに使用するポートの指定、シークレットの設定を行います。
サプリカントでは、RA で発行したユーザ証明書の登録を行います。

*1　使用する機器により呼び名が変わります。各機器のマニュアルを参照してください

３．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：

RA の IP アドレス	192.168.0.254 (Ether0)
無線 AP の IP アドレス	192.168.0.1
IP アドレスの払い出し	無線 AP で行う
アドレスプール	使用しない
ユーザ ID	user01
パスワード	pass01
認証方式	EAP-TLS
認証アトリビュートの追加	なし
応答アトリビュートの追加	なし
グループ ID	group1

初めに RADIUS サーバを動作させる環境、RA 本体の設定を行います。

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 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 等の証明書を必要とする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。

鍵長	**1024**
Signature Algorithm	**SHA-1**
Common Name	**sample_ca**
email	**samp@example.co.jp**
Country	**JP**
有効期間(終了日時)	**2015 / 12 / 31**
パスフレーズ	**passsample**
失効リスト更新間隔	**30**

※[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

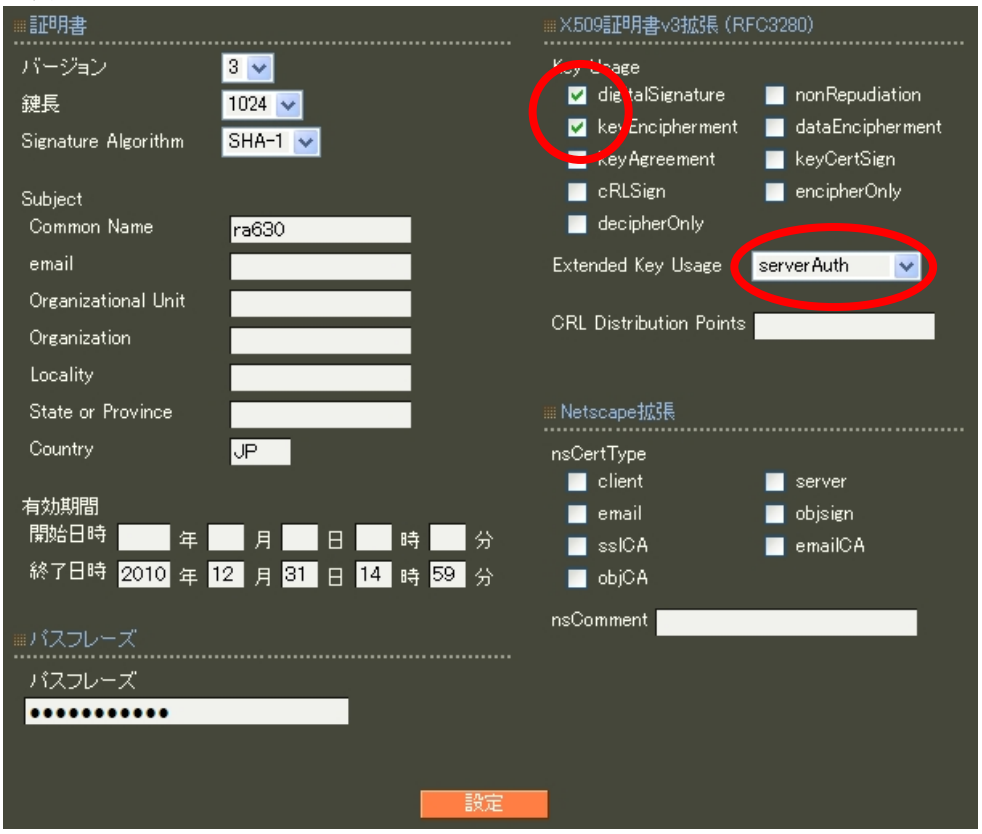
合でも認証ができなくなります。必ず失効リストの更新処理を設定した間隔で行ってください。
また更新した失効リストを有効にするには、RADIUS サービスの再起動が必要になります。
CA の再編集はできませんので設定の際は内容を十分確認してください。
また、CA を削除した場合は発行済みの全ての証明書も削除されます。ご注意ください。

動作環境が整ったところでRADIUS サーバの設定を行います。

RADIUS サーバ証明書の発行（CA／証明書）

CA にて RA の証明に使用するサーバ証明書を発行します。
証明書画面から 新規追加 ボタンで追加します。

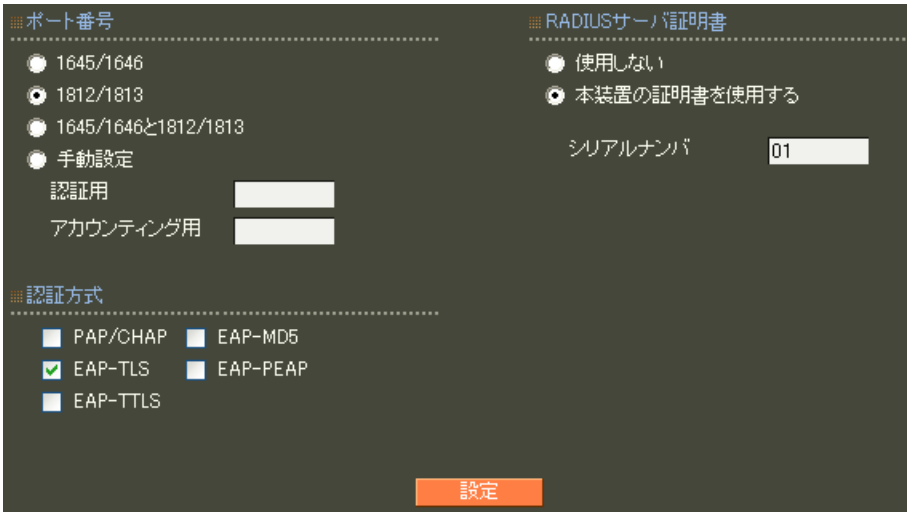
設定例：



※ 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** 、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)

　ここでの RADIUS クライアントは無線 AP です。Windows PC ではありません。
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 AP の IP アドレス、シークレットは無線 AP へ設定したものと同じものを設定します。

設定例：

※無線 AP では認証サーバ(RADIUS サーバ)として RA の IP アドレスを指定します。

RADIUS サーバの設定後は実際に認証するユーザの作成です。

RA の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「ユーザプロファイル」が必要で、ユーザプロファイルの作成には最低限「ユーザ基本情報プロファイル」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** 、IP アドレス割り当てを **未使用** 、アドレスプールを **指定しない** に設定します。プロファイル名は base1 とします。

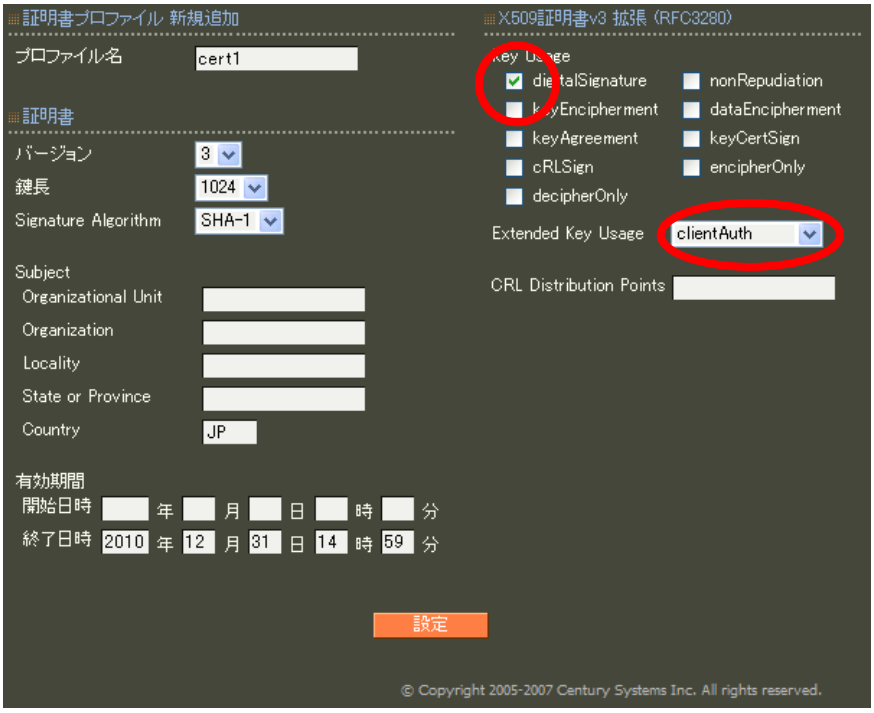
グループ ID プロファイルの作成　(RADIUS／プロファイル／グループ ID)

グループ ID は realm に相当するものです。ここでは設定条件に従いグループ ID に group1 を設定します。ここではプロファイル名も group1 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。

設定例：



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(**base1**)、グループ ID プロファイル(**group1**)、証明書プロファイル(**cert1**)を指定してユーザプロファイル(**user1**)を作成します。

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)

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。固定 IP 払い出しはここでは使用しませんのでそのままにします。以上を入力して 設定 を押すことによりユーザが追加されます。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、同じグループ ID）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。パスフレーズは証明書画面に表示されています。この取り出した証明書およびパスフレーズをユーザに渡してください。
以上でRAの設定は終了です。最後にRADIUSサーバを起動します。

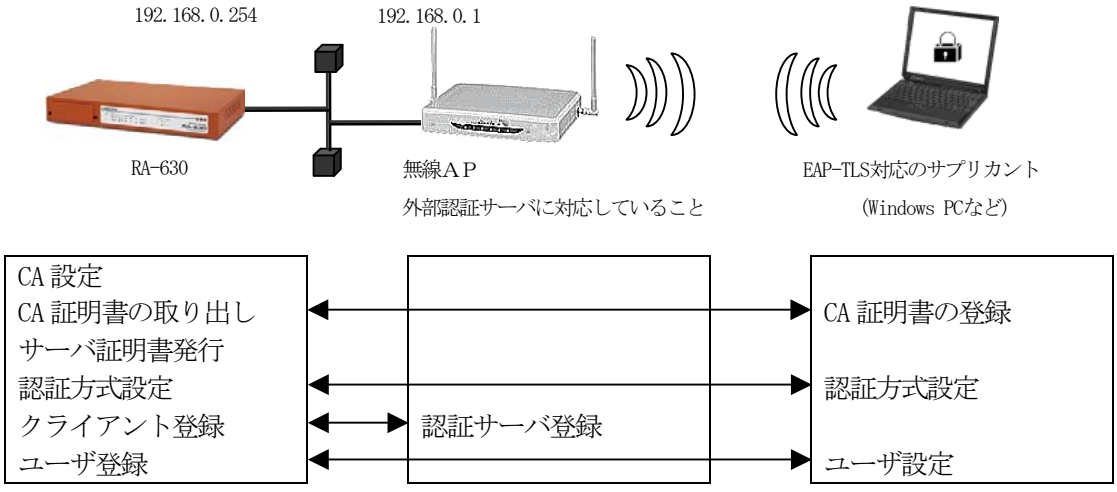
事例 2. 無線アクセスポイントでEAP-TTLS認証を使用する

１．概要

ここでは前章に引き続き、無線 LAN 接続のセキュリティ向上の為、RA-1100/RA-730/RA-630（以下 RA）を使った EAP-TTLS 認証を行う場合の例を紹介します。前章同様使用する無線アクセスポイント（以下無線 AP）は RADIUS による外部認証サーバに対応しており、なおかつサプリカントが EAP-TTLS に対応している必要があります。

２．構成

無線 LAN を使用している環境に RA を追加するには、RA を無線 AP と通信できるネットワークに接続します。



無線 LAN 接続の認証に EAP-TTLS 認証を使用するには RA に対して

CA の設定
RA 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 クライアントとして無線 AP の登録
ユーザの登録

を行います。無線 AP に対しては認証サーバ(*1) として RA の IP アドレスを指定します。サプリカントでは認証方法及びユーザ ID/パスワードの設定を行います。

*1 使用する機器により呼び名が変わります。各機器のマニュアルを参照してください

３．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：

RA の IP アドレス	192.168.0.254 (Ether0)
無線 AP の IP アドレス	192.168.0.1
IP アドレスの払い出し	無線 AP で行う
アドレスプール	使用しない
ユーザ ID	user01
パスワード	pass01
認証方式	EAP-TTLS/CHAP
認証アトリビュートの追加	なし
応答アトリビュートの追加	なし
グループ ID	なし

初めに RADIUS サーバを動作させる環境、RA 本体の設定を行います。

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 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 等の証明書を必要とする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ため、
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-1**
Common Name	**sample_ca**
email	**samp@example.co.jp**
Country	**JP**
有効期間(終了日時)	**2015 / 12 / 31**
パスフレーズ	**passsample**
失効リスト更新間隔	**30**

※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。

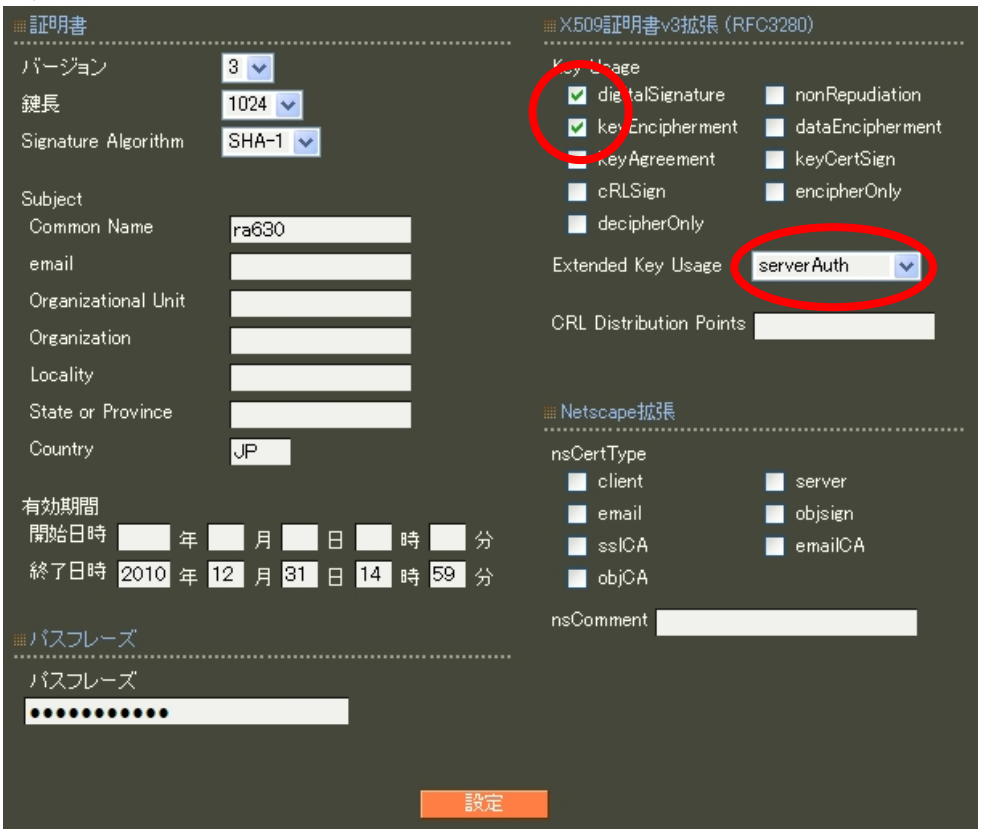
CA 作成後は CA 証明書画面より 取り出し ボタンを押下して CA 証明書を取得し、ユーザへ渡してください。

動作環境が整ったところで RADIUS サーバの設定を行います。

RADIUS サーバ証明書の発行（CA／証明書）

CA にて RA の証明に使用するサーバ証明書を発行します。
証明書画面から 新規追加 ボタンで追加します。

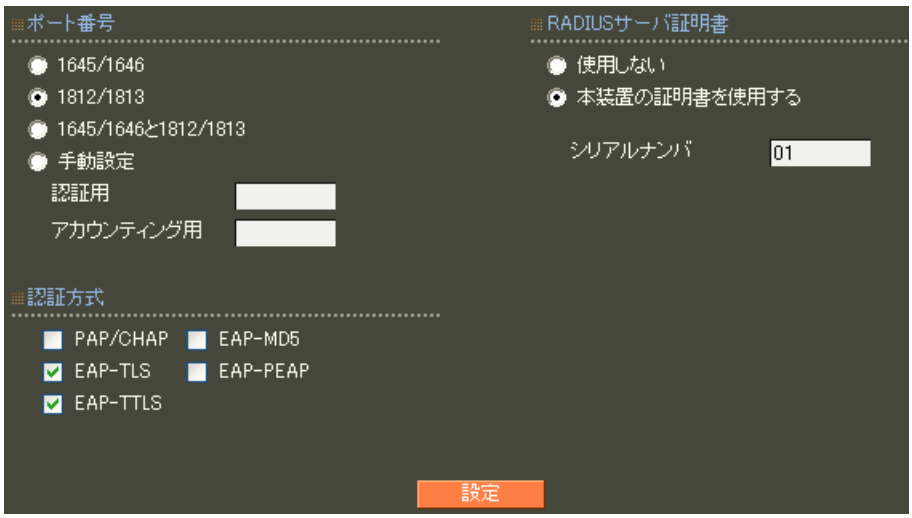
設定例：



※ 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－TTLS** 、内部認証で使用するプロトコル、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-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)
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）

ここでの RADIUS クライアントは無線 AP です。Windows PC ではありません。
クライアント新規追加画面の全ての項目を埋めます。IP アドレスは無線 AP の IP アドレス、シークレットは無線 AP へ設定したものと同じものを設定します。

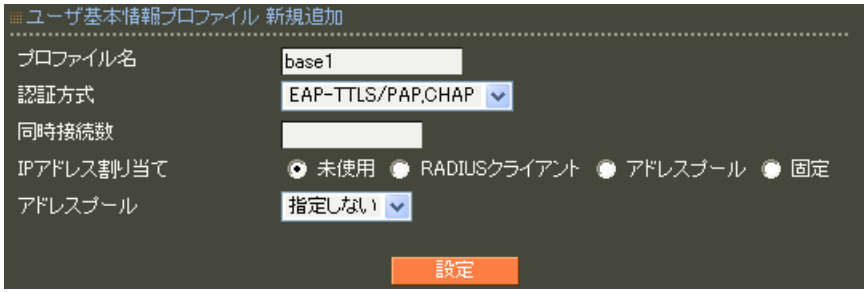
設定例：

※無線 AP では認証サーバ(RADIUS サーバ)として RA の IP アドレスを指定します。

RADIUS サーバの設定後は実際に認証するユーザの作成です。
RA の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プロファイルが必要であり、ユーザプロファイルの作成には最低限ユーザ基本情報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** 、IP アドレス割り当てを**未使用**、
アドレスプールを**指定しない**に設定します。プロファイル名は **base1** 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(**base1**)を指定してユーザプロファイル(**user1**)を作成します。

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)

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。

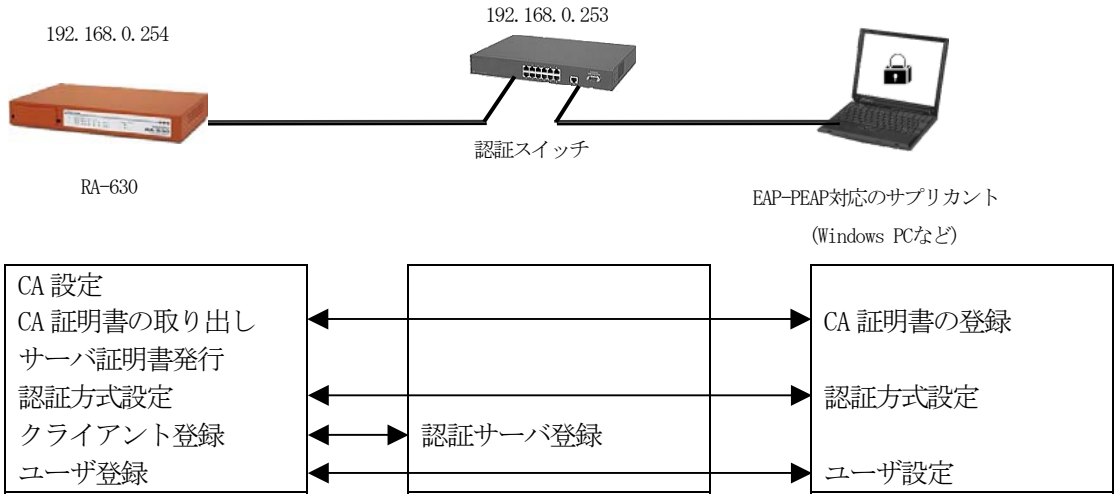
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例 3. 認証スイッチでEAP-PEAP認証を使用する

１．概要

ここでは認証スイッチ(以下認証 SW)の認証サーバとして RA-1100/RA-730/RA-630（以下 RA）を使用する例を紹介します。認証方法は EAP-PEAP を使用します。

２．構成



認証 SW を使って EAP-PEAP 認証を使用するには RA に対して下記の設定を行います。

CA の設定
RA 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 クライアントとして認証 SW の登録
ユーザの登録

認証 SW に対しては認証サーバ(*1) として RA の IP アドレスを指定します。
サプリカントではユーザ ID/パスワードの設定の他、RA で発行した CA 証明書の登録を行います。

*1 使用する機器により呼び名が変わります。各機器のマニュアルを参照してください

３．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：

RA の IP アドレス	192.168.0.254 (Ether0)
認証 SW の IP アドレス	192.168.0.253
IP アドレスの払い出し	なし
アドレスプール	使用しない
ユーザ ID	user01
パスワード	pass01
認証方式	EAP-PEAP
認証アトリビュートの追加	なし
応答アトリビュートの追加	なし
グループ ID	なし

初めに RADIUS サーバを動作させる環境、RA 本体の設定を行います。

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 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 等の証明書を必要とする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-1**
Common Name	**sample_ca**
email	**samp@example.co.jp**
Country	**JP**
有効期間(終了日時)	**2015 / 12 / 31**
パスフレーズ	**passsample**
失効リスト更新間隔	**30**

※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。

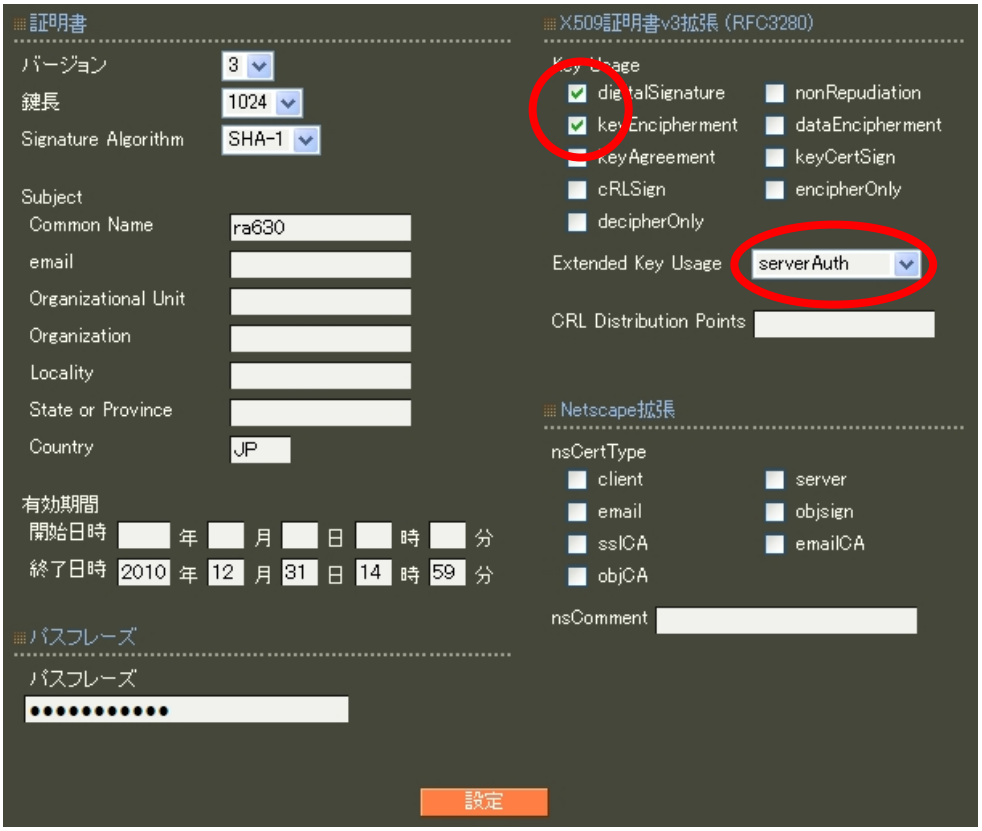
CA 作成後は CA 証明書画面より 取り出し ボタンを押下して CA 証明書を取得し、ユーザへ渡してください。

動作環境が整ったところで RADIUS サーバに対する設定を行います。

RADIUS サーバ証明書の発行（CA／証明書）

CA にて RA の証明に使用するサーバ証明書を発行します。
証明書画面から 新規追加 ボタンで追加します。

設定例：



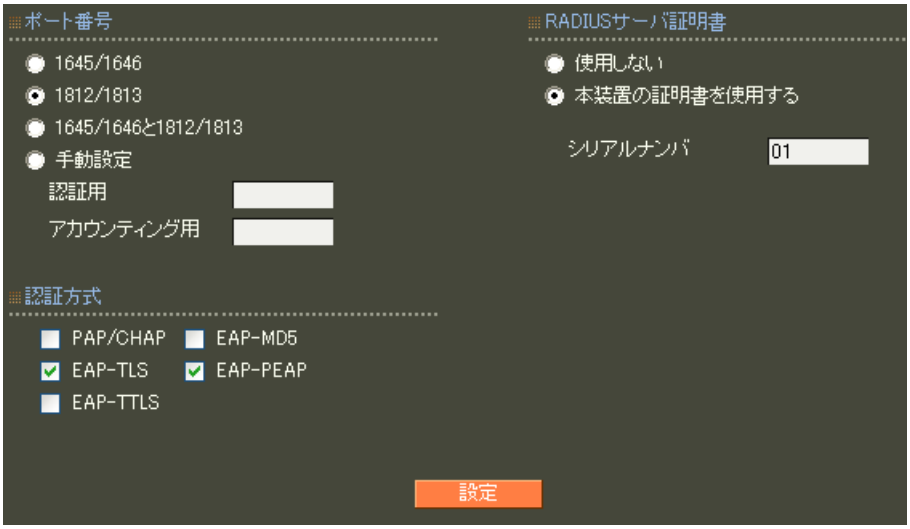
※ バージョン3 のサーバ証明書を作成する場合には、通常最低限以下の Key Usage/Extended KeyUsage を指定するようにします。

・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）

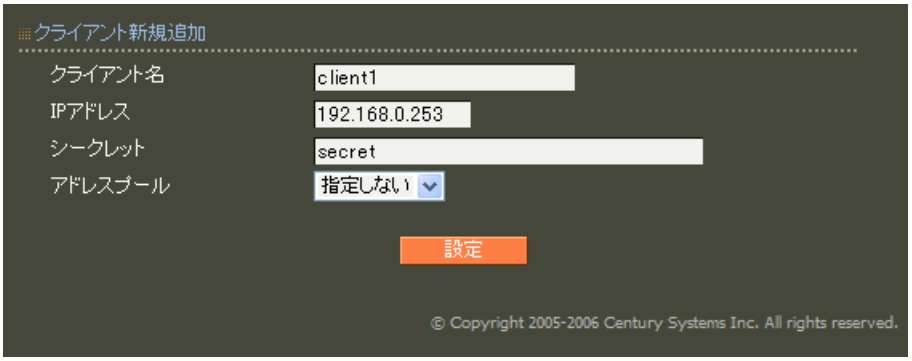
認証方式に **EAP-TLS** 、 **EAP-PEAP** 、RADIUS サーバ証明書に **本装置の証明書を使用する** を選択します。(EAP-PEAP を使用するには EAP-TLS も選択する必要があります。
シリアルナンバには先ほど発行したサーバ証明書のシリアルナンバを入力します。シリアルナンバは CA の証明書一覧で確認することができます。また、設定ウィザードを使った場合は自動的に入力されます。



RADIUS クライアントの設定（RADIUS／サーバ／クライアント）

ここでの RADIUS クライアントは認証 SW です。Windows PC ではありません。
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 SW の IP アドレス、シークレットは認証 SW へ設定したものと同じものを設定します。

設定例：



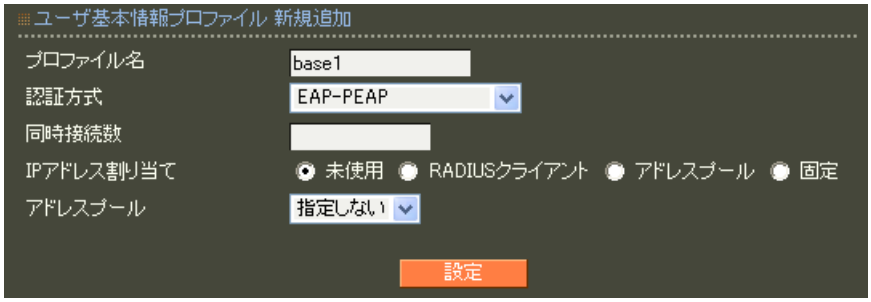
※　認証 SW では認証サーバ(RADIUS サーバ)として RA の IP アドレスを指定します。

RADIUS サーバの設定後は実際にログインするユーザの作成です。

RA の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プロファイルが必要であり、ユーザプロファイルの作成には最低限ユーザ基本情報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** 、IP アドレス割り当てを**未使用**、
アドレスプールを**指定しない**に設定します。プロファイル名は **base1** 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(**base1**)を指定してユーザプロファイル(**user1**)を作成します。

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)

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。固定 IP 払い出しはここでは使用しませんのでそのままにします。以上を入力して 設定 を押すことによりユーザが追加されます。

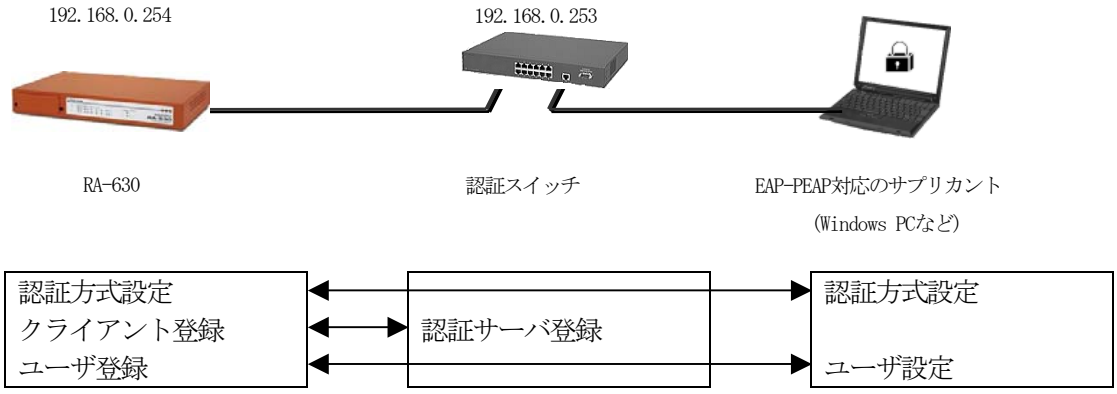
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例 4. 認証スイッチでEAP-MD5認証を使用する

１．概要

ここでは認証スイッチ(以下認証SW)の認証サーバとしてRA-1100/RA-730/RA-630（以下RA）を使用する例を紹介します。認証方法はEAP-MD5を使用します。

２．構成



認証SWを使って EAP-MD5認証を使用するにはRAに対して下記の設定を行います。

認証方式や使用ポートなどの基本設定
RADIUSクライアントとして認証SWを登録
ユーザの登録

認証SWに対しては認証サーバ(*1) としてRAのIPアドレスを指定します。
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。

*1 使用する機器により呼び名が変わります。各機器のマニュアルを参照してください

３．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：

RAのIPアドレス	192.168.0.254 (Ether0)
無線APのIPアドレス	192.168.0.253
IPアドレスの払い出し	RADIUSクライアント
アドレスプール	使用しない

ユーザ ID	user01
パスワード	pass01
認証方式	EAP-MD5
認証アトリビュートの追加	なし
応答アトリビュートの追加	なし
グループ ID	なし

初めに RADIUS サーバを動作させる環境、RA 本体の設定を行います。

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 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）

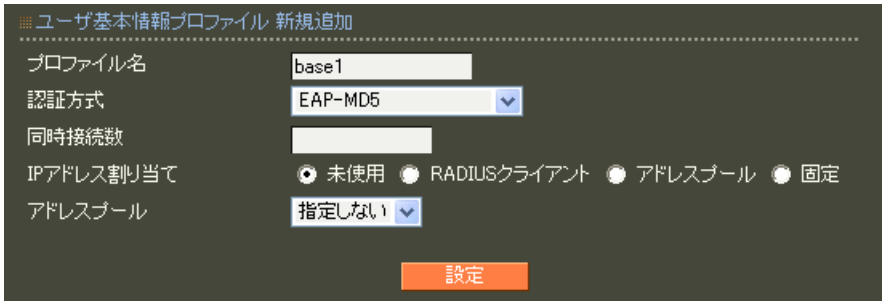
ここでの RADIUS クライアントは認証 SW です。Windows PC ではありません。
クライアント新規追加画面の全ての項目を設定します。IP アドレスは認証 SW の IP アドレス、シークレットは認証 SW へ設定したものと同じものを設定します。

※認証 SW では認証サーバ(RADIUS サーバ)として RA の IP アドレスを指定します。

RADIUS サーバの設定後は実際に認証するユーザの作成です。
RA のユーザはプロファイルという概念により、設定単位の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することや、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プロファイルが必要であり、ユーザプロファイルの作成には最低限ユーザ基本情報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** 、IP アドレス割り当てを **RADIUS クライアント**、
アドレスプールを**指定しない**に設定します。プロファイル名は **base1** 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(**base1**)を指定してユーザプロファイル(**user1**)を作成します。

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)

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。固定 IP 払い出しはここでは使用しませんのでそのままにします。以上を入力して 設定 を押下することによりユーザが追加されます。

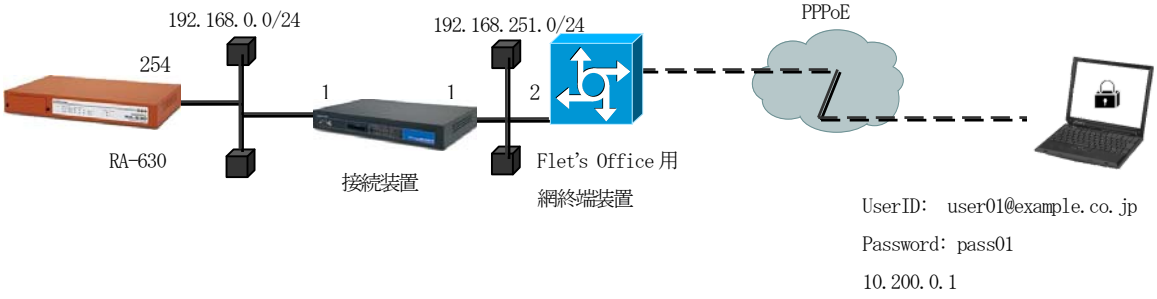
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例 5. Flet’s Office環境でPAP/CHAP認証を使用する

１．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RA-1100/RA-730/RA-630（以下RA）を使用する例を紹介します。

２．構成



RA をフレッツオフィス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。

RADIUS クライアントとしての網終端装置の登録
網終端装置へ向けたルートの作成
ユーザの登録
応答アトリビュートの登録

３．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 (PAP/CHAP)」を選択します。

設定条件：

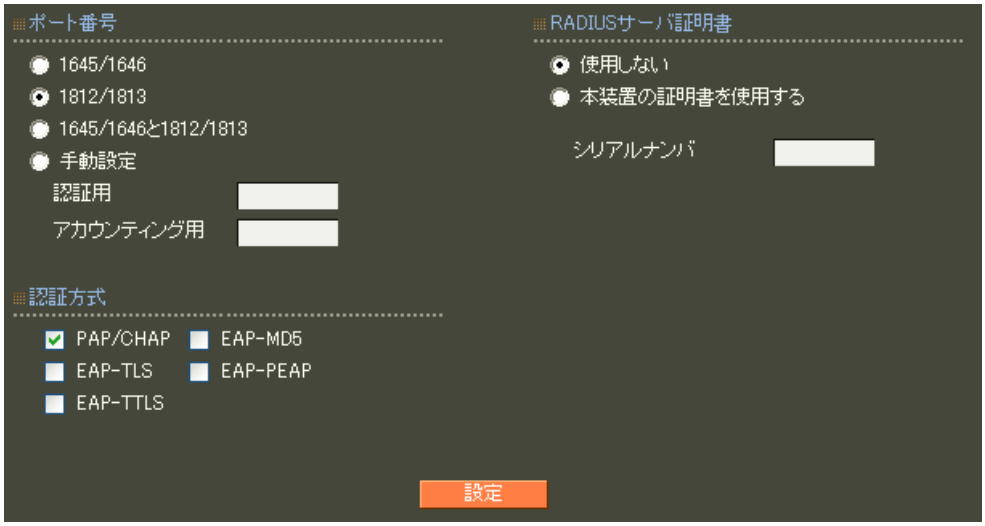
ユーザ ID	user01
パスワード	pass01
グループ ID	example.co.jp
認証方式	PAP/CHAP
IP 割り当て	固定 10.200.0.1
網への接続装置 IP アドレス	192.168.0.1
網終端装置 IP アドレス	192.168.251.2

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作成します。スタティックルートでもかまいませんが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）

RADIUS 基本設定画面を開き認証方式として PAP/CHAP を選択します。



アトリビュートの登録（RADIUS／サーバ／アトリビュート）

認証に使用するアトリビュートはここで登録します。この例題で使用する アトリビュートは standard アトリビュートとして登録済みですのでここではなにもしません。

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の作成が必要です。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 base1 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に使う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 **group1** 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 **base1** とグループ ID **group1** 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 **fletsuser** 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 **fletsuser** 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。
入力後 設定 ボタンを押すことによりユーザが追加されます。

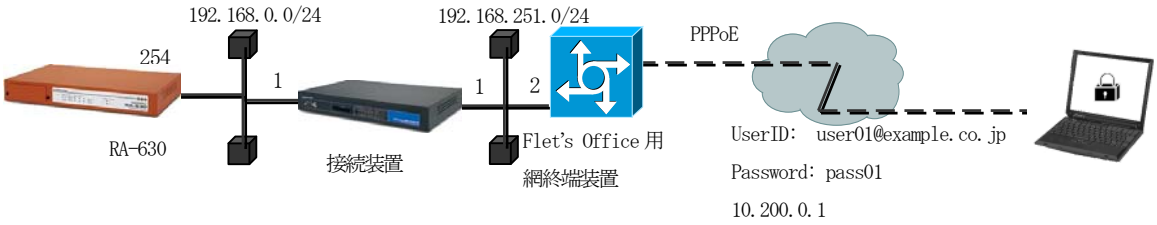
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例 6. Flet’s Office環境でフレッツナンバーアシストを利用する

１． 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 RA-1100/RA-730/RA-630（以下 RA）を使用し、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。

２． 構成



RA をフレッツオフィス環境における認証サーバとして使用し、フレッツナンバーアシストサービスを使用するには以下の設定を行います。

RADIUS クライアントとしての網終端装置の登録
網終端装置へ向けたルートの作成
ユーザの登録（事例５．参照）
応答アトリビュートの登録
認証アトリビュートの登録

３． 設定例

ここでは事例５．でご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ご説明いたします。
設定は、認証プロファイルを利用して設定する方法と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。
ご利用環境に応じてご利用ください。

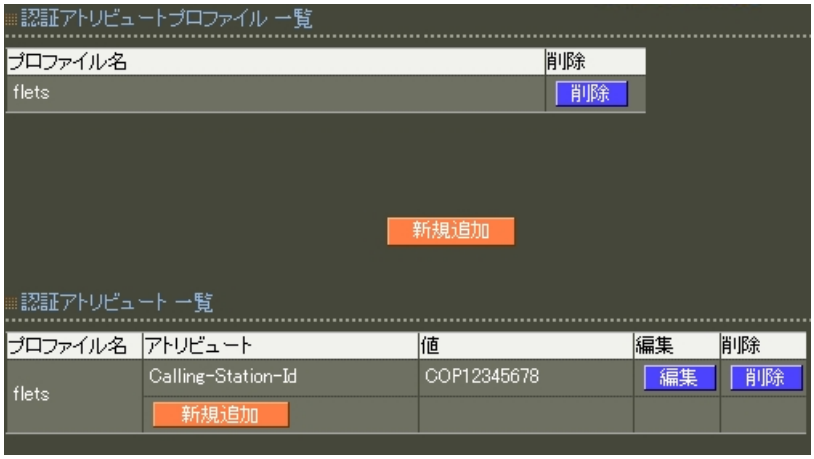
設定条件：

ユーザ ID	user01
パスワード	pass01
認証プロファイル名	flets
お客様 ID(回線 ID)	COP12345678

ー認証プロファイルを利用して設定する方法ー

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お客様 ID（回線 ID）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”flets”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”を指定します。 設定 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作成した認証アトリビュートプロファイルを設定します。
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 flets を選択して 設定 ボタンを押下します。

ーユーザ毎に設定する方法ー

ユーザ設定 (RADIUS／ユーザ／ユーザ)

網側より通知されるお客様 ID (回線 ID) 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

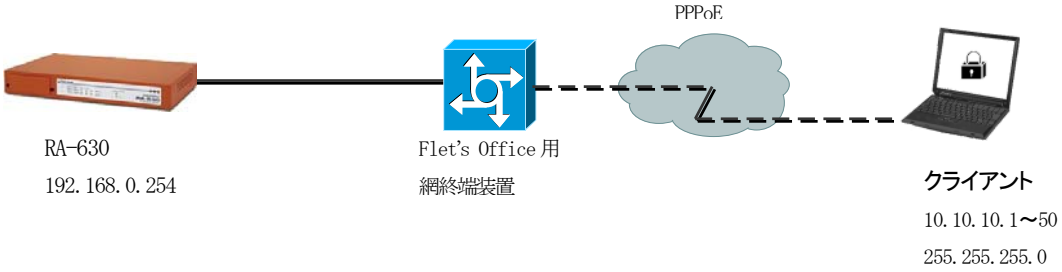
以上で RA の設定は終了です。

事例 7. アドレスプールからIPアドレスを払い出す

１．概要

ここではユーザへの IP アドレス払い出しをアドレスプールから行う例を紹介します。

２．構成



アドレスプールから IP アドレスを払い出すには、

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

の２つの方法があります。どちら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。

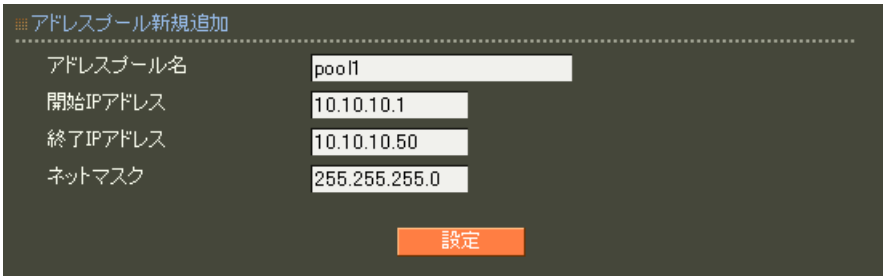
３．設定例

アドレスプールの作成（RADIUS／サーバ／アドレスプール）

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。

設定例：

アドレスプール名	pool1
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



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）

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 アドレス割り当てに**アドレスプール**を指定し、アドレスプールを選択します。

また、クライアントで指定する場合はクライアント画面で**アドレスプール**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。

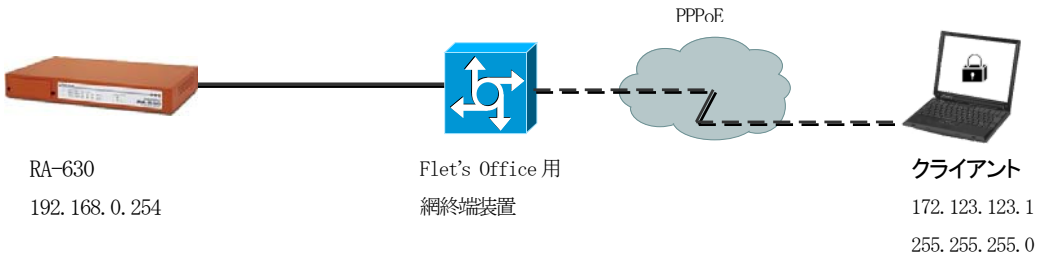
以上で RA の設定は終了です。

事例 8. ユーザ毎に固定のIPアドレスを払い出す

１．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。

２．構成

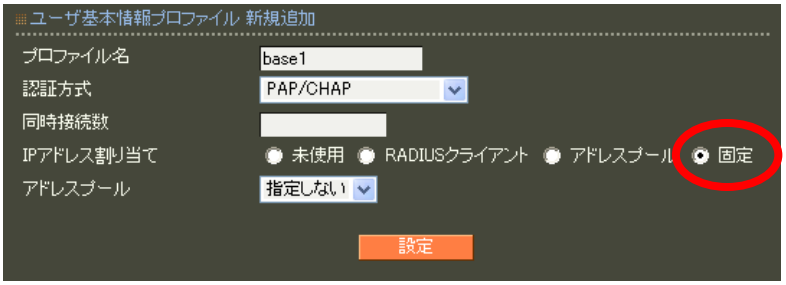


ユーザ毎に固定の IP アドレスを払い出すには、ユーザ基本情報プロファイルの IP アドレス割り当てで固定を選択し、各ユーザの作成(または編集)時に IP アドレスを指定します。

３．設定例

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。

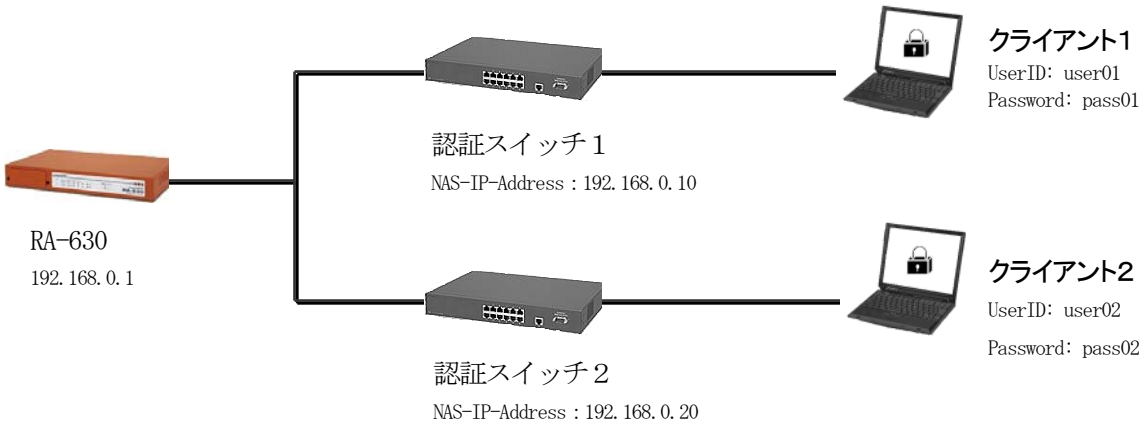
以上で RA の設定は終了です。

事例 9. 認証スイッチ毎に接続可能なユーザを限定する

１．概要

ここでは認証アトリビュートを用いて認証スイッチ（以下認証 SW）毎に接続可能なユーザを限定する例を紹介します。

２．構成



３．設定例

認証 SW 単位でユーザを識別するには、どの認証 SW からの認証要求なのか識別する情報を追加する必要があります。このような認証時に使う情報を追加する場合は、認証アトリビュートを用います。認証アトリビュートを使用するには認証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登録します。ここでは認証 SW の識別に NAS-IP-Address を使います。

クライアントの登録（RADIUS／サーバ／クライアント）

ここでの RADIUS クライアントは認証 SW です。下記設定で各認証 SW を登録します。
クライアント名：**sw1**, IP アドレス：**192.168.0.10**, シークレット：**secret1**
クライアント名：**sw2**, IP アドレス：**192.168.0.20**, シークレット：**secret2**

※この時点では NAS-IP-Address については考える必要はありません。

アトリビュートの登録（RADIUS／サーバ／アトリビュート）

認証に使用するアトリビュートはここで登録します。この例題で使用する NAS-IP-Address は standard アトリビュートとして登録済みですのでここではなにもしません。

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の作成が必要です。この例題ではプロファイル名を **base1** 、認証方式を **PAP/CHAP** とします。IP アドレスの払い出しは行いませんので **未使用** を選択します。

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 SW を識別するために使う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 SW の数分作成します。ここでは後でわかりやすくするためそれぞれのプロファイル名を **sw1attr、sw2attr** とします。
続いて下段の表中の 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 SW 1 の IP アドレス **192.168.0.10** 、sw2attr の値には認証 SW2 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SWの数だけ作成します。認証アトリビュートプロファイルそれぞれ、認証SWそれぞれに対応するプロファイルと捉えるとわかりやすいでしょう。ここでは認証SW1用にユーザ基本情報プロファイル **base1**、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SW2用に同じくユーザ基本情報プロファイル **base1** 、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。

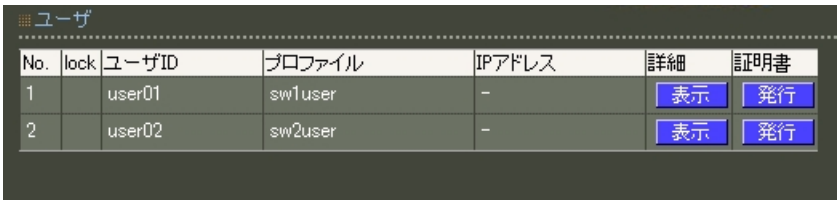
認証SW１用ユーザプロファイル作成

このユーザプロファイルで選択した認証アトリビュートプロファイルで設定されているアトリビュートが、このユーザプロファイルを使用するユーザの認証で使われます。

ユーザの登録（RADIUS／ユーザ／ユーザ）

以上で、認証SW単位にユーザを識別する準備が整いました。あとは認証SW1のユーザはユーザプロファイル **sw1user** を、認証SW2 のユーザは **sw2user** を選択してユーザを作成することにより認証アトリビュートを用いてユーザの認証が行えます。

認証SW1 なら sw1user、SW2 なら sw2user



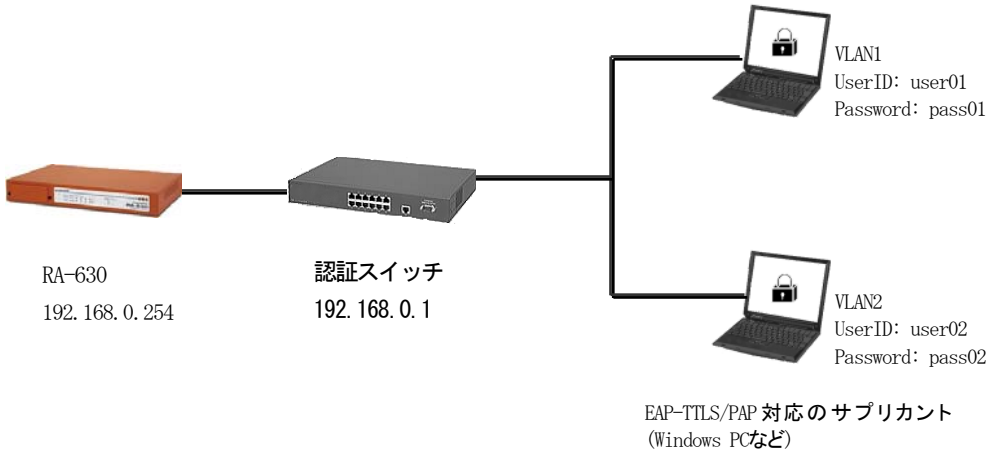
以上でRAの設定は終了です。最後にRADIUSサーバを起動します。

事例10. ユーザ毎に応答アトリビュートを設定する

１．概要

ここでは応答アトリビュートを用いて認証スイッチ（認証SW）へユーザ毎にVLAN IDを指定する例を紹介します。

２．構成



３．設定例

認証が通ったユーザに情報を返すには応答アトリビュートを用います。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。

Tunnel-Type	13 (VLAN)
Tunnel-Medium-Type	6 (802)
Tunnel-Private-Group-ID	VLAN1 or VLAN2

クライアントの登録（RADIUS／サーバ／クライアント）

ここでのRADIUSクライアントは認証SWです。クライアントとして認証SWを登録します。
クライアント名：**sw1**, IPアドレス：**192.168.0.1**, シークレット：**secret**とします。

アトリビュートの登録（RADIUS／サーバ／アトリビュート）

応答アトリビュートで使用するアトリビュートはここで登録します。この例題で使用するアトリビュートは standard アトリビュートとして登録済みですのでここではなにも行いません。

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の作成が必要です。この例題ではプロファイル名を **base1** 、認証方式を **EAP-PEAP** とします。IP アドレスの払い出しは行いませんので **未使用** を選択します。

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 を返すために使う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 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てください。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 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。応答アトリビュートプロファイルそれぞれが、各々の VLAN に対応するプロファイルと捉えるとわかりやすいでしょう。ここでは VLAN1 用にユーザ基本情報プロファイル **base1**、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 **base1** 、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）

以上で応答アトリビュートを返す準備ができました。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することで応答アトリビュートを使用できるようになります。

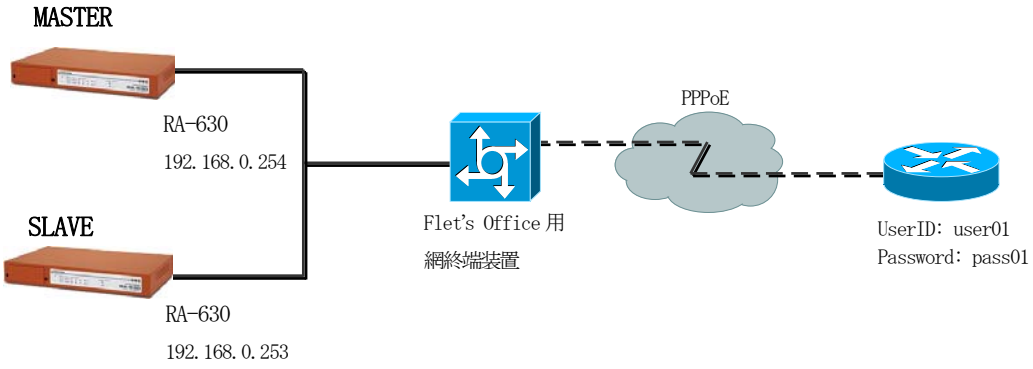
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例11. 設定情報の同期を利用する

１．概要

ここではRA-1100/RA-730/RA-630（以下RA）の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。

２．構成



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

３．設定例

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

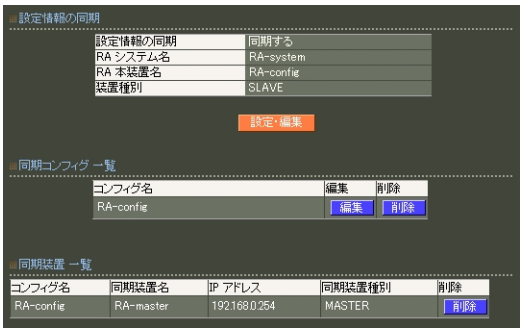
SLAVE 側

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 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。

下記画面は、二重化が設定されている場合の画面表示例です。

・同期装置の追加では、対向の同期装置を追加します。

※　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。

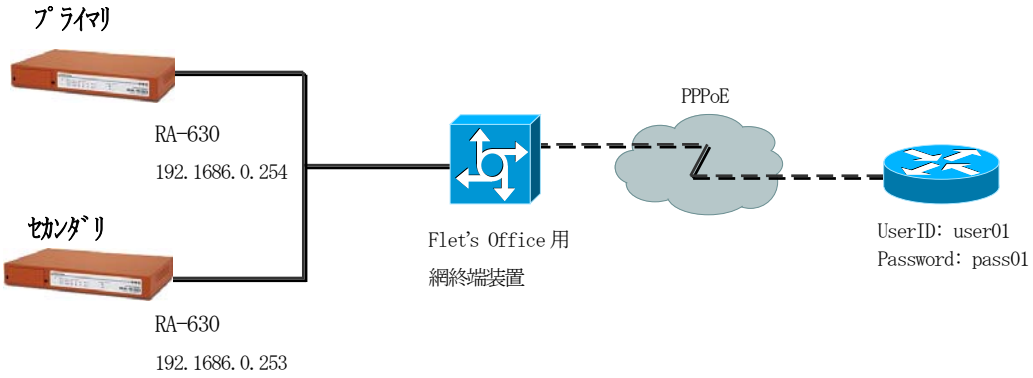
以上で RA の設定は終了です。

事例12. RADIUS機能の二重化を利用する

１．概要

ここではRA-1100/RA-730/RA-630（以下RA）の二重化による冗長構成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一方の機器で障害が発生しても継続して認証/アカウンティング処理を行う事ができます。

２．構成



RAを二重化するには、事前にそれぞれの機器でＩＰアドレスの設定を行ってください。

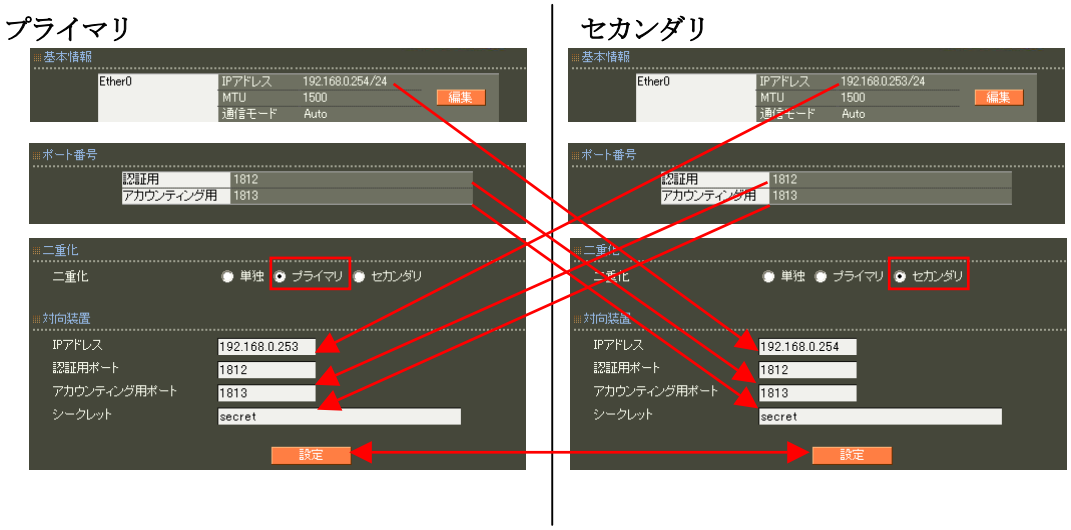
３．設定例

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。

以上で RA の設定は終了です。最後に双方の RADIUS サーバを(再)起動します。

※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。

RA のプライマリ機器に障害が発生した場合､RA 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 クライアント自身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 RA が登録されているか確認ください。

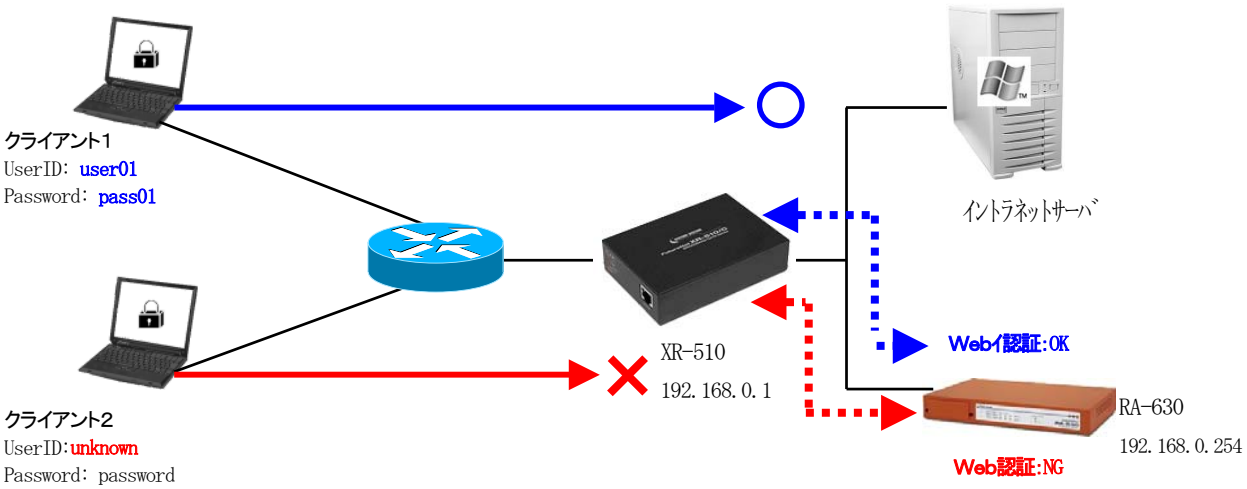
※　二重化機能を使用する場合、必ず NTP サーバを設定の上ご利用ください。

事例 13. XR シリーズの Web 認証機能の認証サーバとして使用する

１．概要

ここでは XR シリーズのＷｅｂ認証機能の認証サーバとして RA-1100/RA-730/RA-630（以下 RA）を用いる例を紹介します。

２．構成



XR シリーズの Web 認証機能の認証サーバとして使用するには RA に対して以下設定を行います。

・認証方式として PAP/CHAP を設定
・RADIUS クライアントとして XR の IP アドレスを登録
・ユーザの登録

設定ウィザードを使用する場合は RADIUS(PAP/CHAP) を選択します。

３．設定例

ここでは、下記設定条件で設定を行います。

認証方式の設定 (RADIUS／サーバ／基本機能)

RADIUS 基本情報画面を開き、認証方式として **PAP/CHAP** を選択します。

クライアントの登録（RADIUS／サーバ／クライアント）

Web 認証を行う XR をクライアントとして登録します。
ここではクライアント名 **xr** 、IP アドレス **192.168.0.1**、
シークレットを **xrsecret** とします。

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）

下記設定でユーザ基本情報プロファイルを作成します。

プロファイル名	**base1**
認証方式	**PAP/CHAP**
IP アドレス割り当て	**未使用**
アドレスプール	**指定しない**

ユーザプロファイルの登録（RADIUS／プロファイル／ユーザ）

ユーザプロファイル新規追加画面よりユーザ基本プロファイル **base1** を選択したプロファイルを作成します。プロファイル名は **xruser1** とします。

ユーザの登録（RADIUS／ユーザ／ユーザ）

続いて XR のユーザを登録します。ここでは設定条件に従いユーザ ID **user01** 、 パスワード **pass01** の設定で作成します。以上で XR の Web 認証機能の認証サーバとして使用する準備が整いました。

以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例14. XRシリーズのIPsecでX.509証明書を使用する

１．概要

ここではXRシリーズのIPsec機能でRA-1100/RA-730/RA-630（以下RA）で発行したX.509証明書を利用する例を紹介します。

２．設定例

XRシリーズのIPsec機能では外部X.509証明書を利用するには証明書の内容をXRの設定画面に入力する必要があります。手順としてはRAにてCAを設定、XR用の証明書を発行、CA証明書、失効リスト、XR用の証明書と私有鍵をPEM形式で取得、各ファイルをエディタ等で開きXRの設定画面へ貼り付けて設定となります。

CA証明書の取得（CA／CA/CRL）

「CA」－「CA/CRL」を選択し、CA証明書画面を開きます。画面左下にあるCA証明書の取得から形式を **PEM** として 取り出し ボタンを押下してCA証明書をファイルとして保存します。ここでは仮にファイル名を **ca.pem** とします。

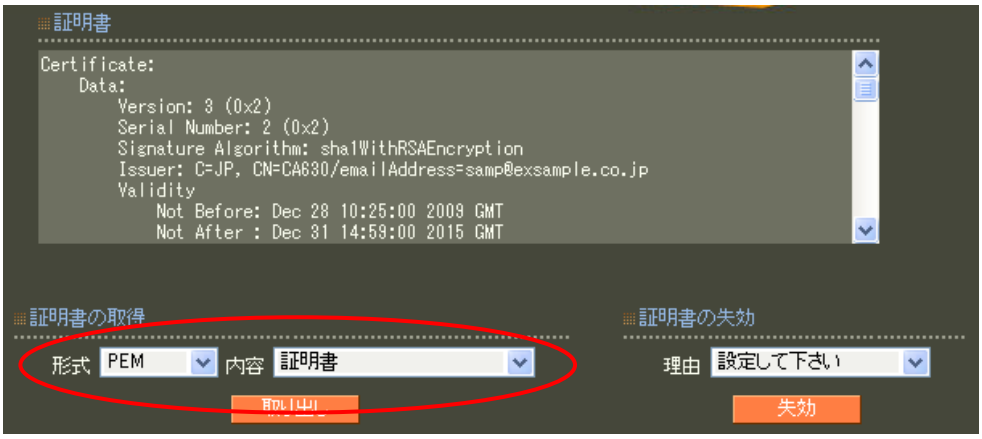
失効リストの取得（CA／CA/CRL）

CA 証明書同様の手順で失効リストを **PEM** 形式のファイルとして保存します。
失効リストのファイル名は **crl.pem** とします。

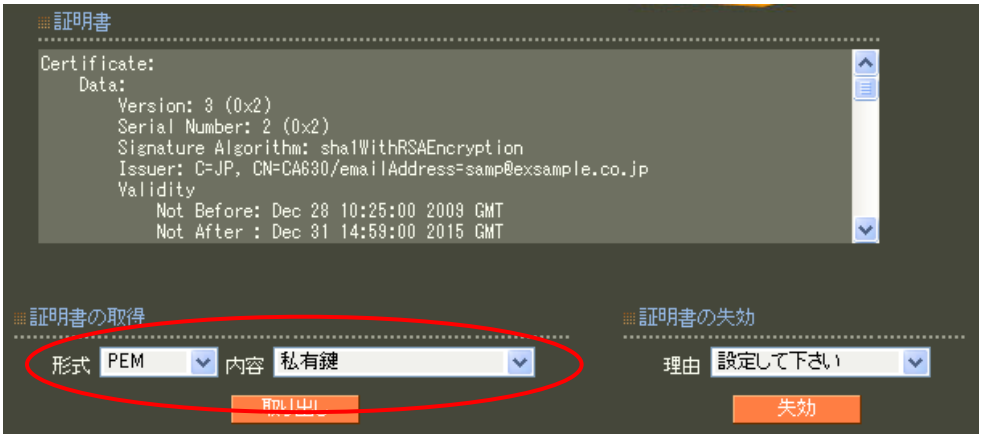
証明書の取得（CA／証明書）

続いて XR 用の証明書を取得します。ここでは既に XR 用の証明書が発行されているものとします。証明書の取得は「CA」→「証明書」を選択し、証明書一覧から取得したい証明書のシリアルナンバ（S/N）をクリックします。

シリアルナンバをクリックすると選択したシリアルナンバの証明書の画面が開きます。
ここで証明書及び私有鍵を取得します。まず形式 **PEM** 、内容 **証明書** を選択し 取り出し ボタンを押下して証明書を取得します。ファイル名は **xrlcert.pem** とします。作成時のパスフレーズは忘れずにメモしておいてください。



続いて内容 **私有鍵** を選択して取得します。ファイル名は **xr1key.pem** とします。

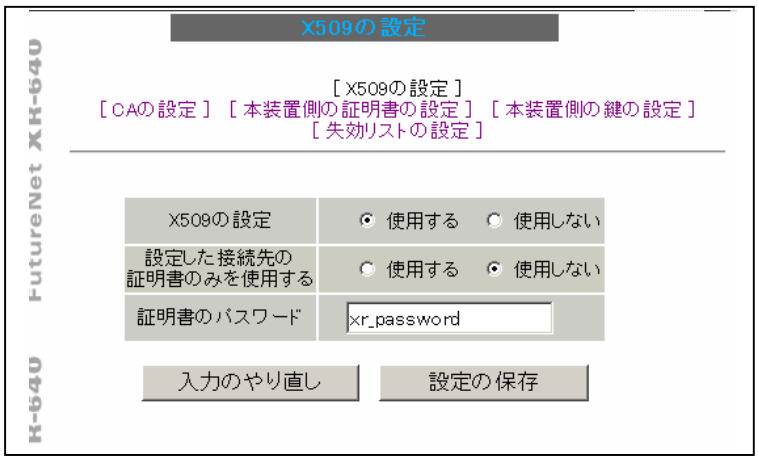


同様の作業を繰り返し対向の XR 用の証明書及び私有鍵も取得します。ファイル名は **xr2cert.pem** 、**xr2key.pem** とします。以上でRAの作業は終了です。

以下の作業はXRに対する作業になります。ここではXR-640を例に紹介します。

X.509証明書を使用する設定

「各種サービスの設定」－「IPsecサーバ」－「X.509の設定」を開きます。



[X.509の設定]画面にてX.509の設定の『**使用する**』を選択し、証明書のパスワードにRAで発行した証明書の**パスフレーズ**を入力して設定します。

CA証明書の取り込み

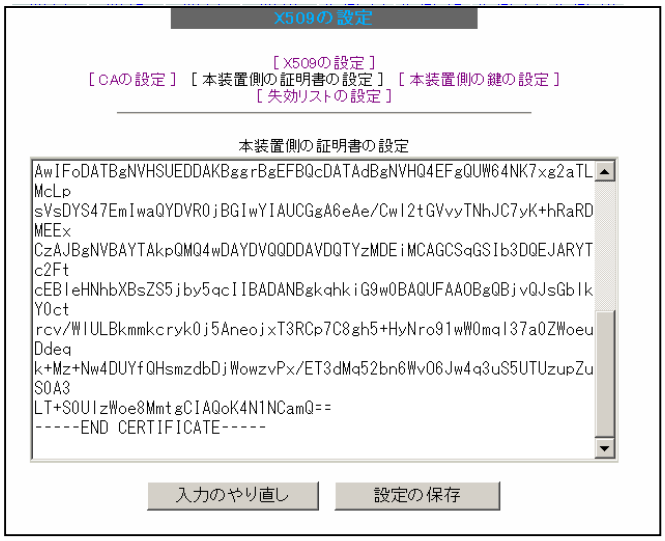
保存したCA証明書 **ca.pem** をエディタ等で開きます。ファイルの内容を全てコピーし、[CAの設定]画面の入力欄に貼り付けて 設定の保存 ボタンを押下して設定します。

失効リストの取り込み

CA 証明書同様に失効リスト **crl.pem** の内容を［失効リストの設定］画面に貼り付けて
設定の保存 ボタンを押下して設定します。

XR 自身の証明書・私有鍵の取り込み

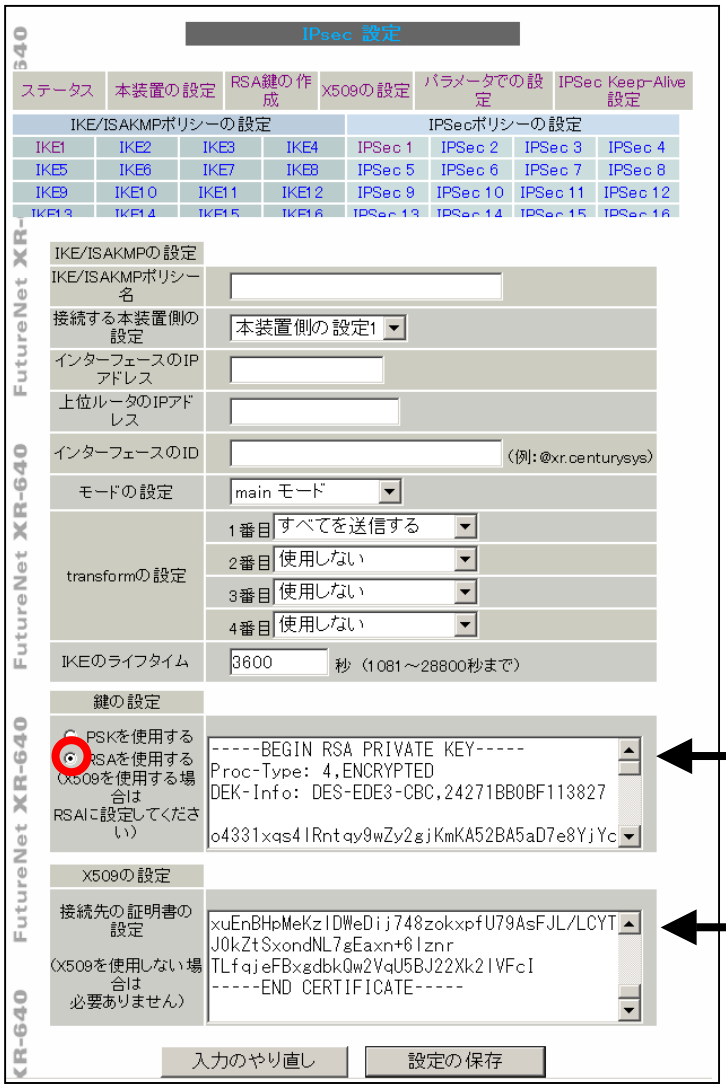
［本装置側の証明書の設定］では設定を行っている XR 自身の証明書 **xrlcert.pem** を貼り付けます。



[本装置側の鍵の設定]では設定を行っている XR 自身の私有鍵 **xr1key.pem** を貼り付けます。

対向機の証明書・私有鍵の取り込み

対向機の証明書及び私有鍵は IKE/ISAKMP ポリシーの設定画面で行います。



証明書 **xr2cert.pem** の内容を画面下 X.509 の設定へ、私有鍵 **xr2key.pem** の内容を鍵の設定の入力欄へ貼り付け、鍵の設定の **RSA を使用する** を設定します。その他の設定は通常の IPsec の設定のとおりです。以上で X.509 の設定は終了です。

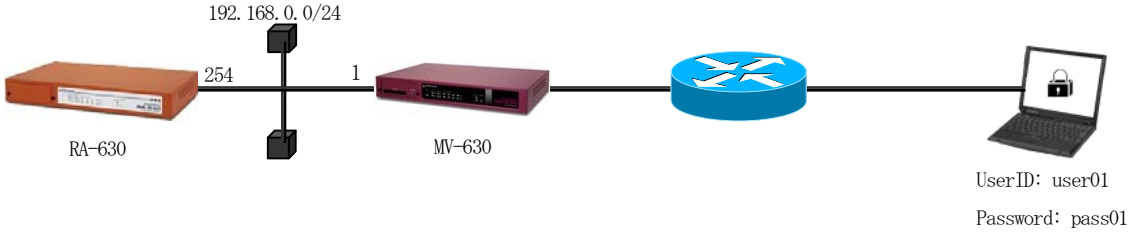
対向機上で設定を行う際は証明書及び私有鍵の設定位置を逆にします。
(xr1*.pem の位置へ xr2*.pem を設定、 xr2*.pem の位置へ xr1*.pem を設定)

事例15. MV-630の外部認証サーバに使用する

１．概要

ここではMV シリーズの外部認証サーバとしてRA-1100/RA-730/RA-630（以下RA）を用いる例を紹介します。

２．構成



MV シリーズの認証サーバとして使用するにはRA に対して以下設定を行います。

認証方式としてPAP/CHAP を設定
RADIUS クライアントとしてMV のIP アドレスを登録
MV のユーザグループを応答アトリビュートとして登録
ユーザの登録

MV で使用する証明書をRA で発行したい場合はCA の設定も必要になります。

３．設定例

ここではMV シリーズのユーザ認証のみをRA で行い、プライベートCA は使わない例を紹介します。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。

※RA の認証局(CA)を使う場合は「RADIUS(EAP)」を選択します。

設定条件：

ユーザID	user01
パスワード	pass01
MV のグループ(応答アトリビュートで返す)	group1
認証方式	PAP/CHAP
MV630 のIP アドレス	192.168.0.1
プライベートCA	使用しない

※ここでいうMV のグループはRA のグループID とは異なります。

ネットワークの設定（管理機能／ネットワーク／基本設定）

RA の IP アドレス及びデフォルトルートを設定し、MV との通信が行えるようにします。

認証方式の設定（RADIUS／サーバ／基本設定）

認証方式として **PAP/CHAP** を選択します。ここで設定したポート番号は MV の Radius Server 設定時に使用します。

クライアントの登録（RADIUS／サーバ／クライアント）

ここでの RADIUS クライアントは MV です。クライアント名 **mv**, IP アドレス **192.168.0.1**, シークレット **mvsecret** とします。

アトリビュートの登録（RADIUS／サーバ／アトリビュート）

応答アトリビュートで MV のグループを返すためにアトリビュートを登録します。
まず、ベンダ一覧下の 新規追加 ボタンを押下して、ベンダ名 **Century**、ベンダ ID **20376** でベンダを登録します。ベンダを登録すると画面下のベンダ固有アトリビュート一覧に追加されますので Century の横にある 新規追加 を押下してアトリビュートを登録します。
入力内容は タイプ名 **MV-Group**、タイプ **1** 、フォーマット **text** とします。

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の作成が必要です。この例題ではプロファイル名を **base1** 、認証方式を **PAP/CHAP** とします。IP アドレスの払い出しは **未使用** を選択します。

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）

ここで認証時にユーザへ返す MV のグループを登録します。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。プロファイル名は **mvgroup1** とします。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新規追加画面を開きます。
アトリビュートの内容は アトリビュートに **MV-Group** を選択し、値に MV のグループを入力します。ここでは **group1** と設定します。MV のグループが複数ある場合はグループ毎に応答アトリビュートプロファイルを作成します。グループがわかるようなプロファイル名をつけておくとよいでしょう。

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新規追加画面よりユーザ基本プロファイル **base1** 、応答アトリビュートプロファイル **mvgroup1** を選択したプロファイルを作成します。プロファイル名は **mvuser1** とします。ユーザプロファイルも MV のグループの数だけ作成します。応答アトリビュートプロファイルそれぞれ、グループそれぞれに対応するプロファイルと捉えるとわかりやすいでしょう。

このユーザプロファイルで選択した応答アトリビュートプロファイルで設定されているアトリビュートが、このユーザプロファイルを使用するユーザの認証が成功したときに返されます。

ユーザの登録（RADIUS／ユーザ／ユーザ）

続いて MV のユーザをグループ毎にユーザプロファイルを選択して登録していきます。ここではユーザ ID **user01** 、 パスワード **pass01** のユーザを group1 のユーザプロファイル **mvuser1** を選択して作成します。以上で MV の外部認証サーバとして使用する準備が整いました。

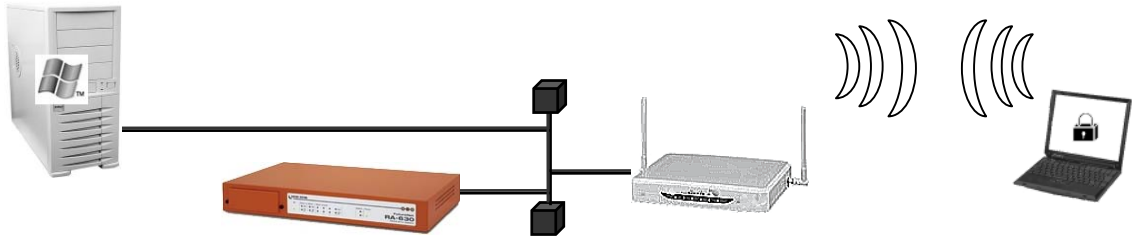
以上で設定は終了です。最後に RADIUS サーバを起動します。

事例16. ActiveDirectoryに登録されたユーザで認証を行う

１．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。

２．構成

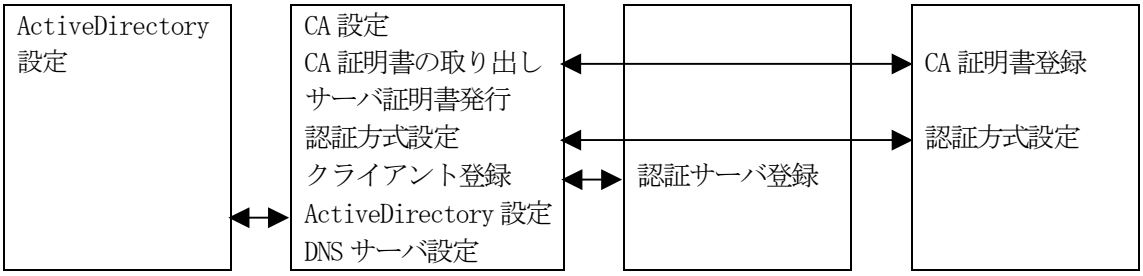


ActiveDirectoryサーバ
ad.example.jp
192.168.0.2

RA-630
192.168.0.254

無線AP
192.168.0.1

EAP-TTLS/PAP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RAに対して以下設定を行います。

CA作成
サーバ証明書の発行
認証方式の設定
クライアントの登録
ActiveDirectoryの設定
DNSサーバの設定
ADユーザプロファイル設定
RADIUSサーバ再起動

３．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AP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RAを設定します。ActiveDirectoryを用いた認証を行う場合のRAは、ActiveDirectoryに対して無線AP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	192.168.0.2
ADドメイン	example.jp
所属グループ	Wireless
Adminユーザ名	administrator
Adminパスワード	adminpassword
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、RA本体の設定を行います。

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-1**
Common Name	**sample_ca**
email	**samp@example.jp**
Country	**JP**
有効期間(終了日時)	**2015 / 12 / 31**

パスフレーズ	passsample
失効リスト更新間隔	30

※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、ユーザへ渡してください。

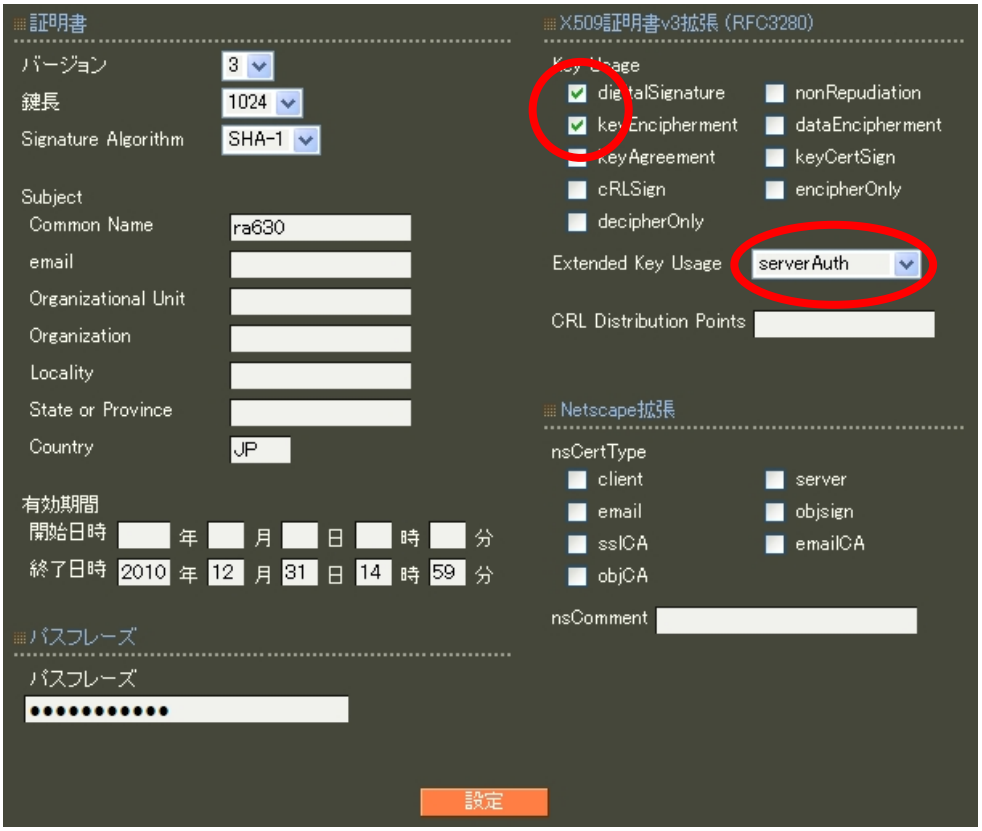
【RADIUS サーバの設定】

動作環境が整ったところで RADIUS サーバに対する設定を行います。

RADIUS サーバ証明書の発行 (CA／証明書)

CA にて RA の証明に使用するサーバ証明書を発行します。
証明書画面から 新規追加 ボタンで追加します。

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。

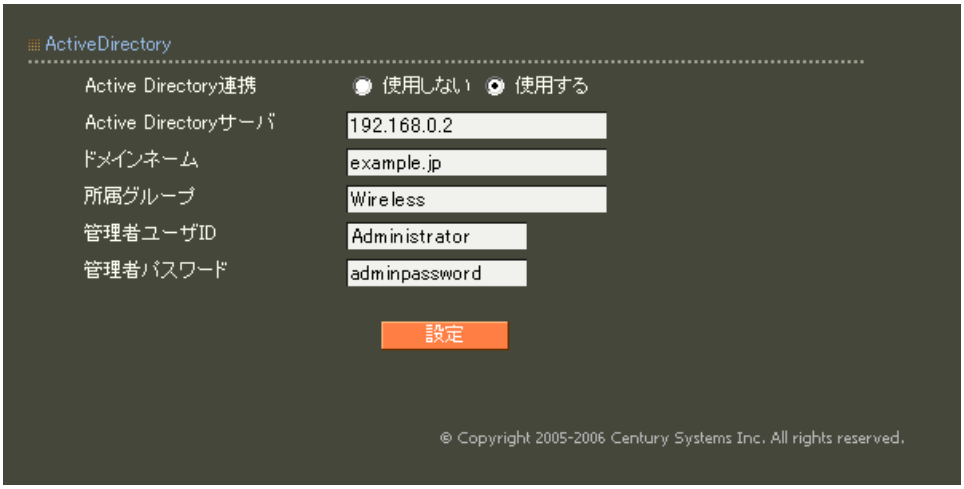
DNS の設定（管理機能／ネットワーク／DNS）

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） **192.168.0.2** を指定します。

ActiveDirectory の設定 (RADIUS／サーバ／ActiveDirectory)

ActiveDirectory 画面では**ドメインコントローラの IP アドレス**を **Active Directory サーバへ設定します。管理者ユーザ ID、管理者パスワード**は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。

設定例：

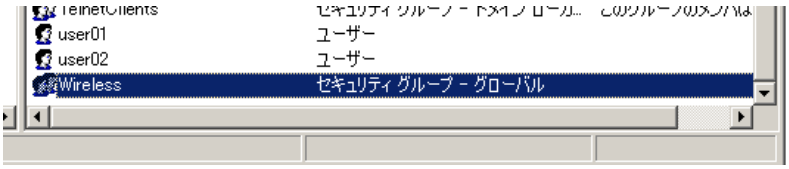


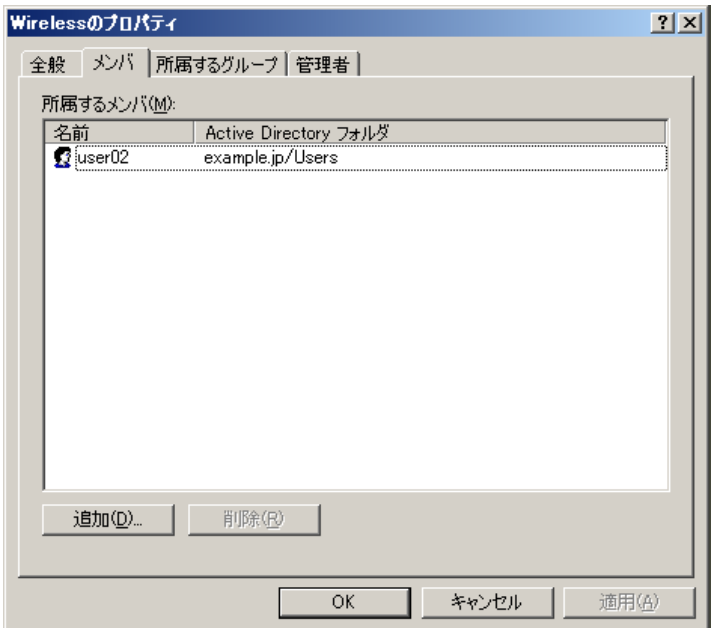
所属グループについて

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が成功することを防止できます。

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

①AD にて 特定のグループ(Wireless)を作成し、user02 を所属させる。
②RA 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 のみ認証が成功します。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が失敗します。

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）

ここでの RADIUS クライアントは無線 AP です。Windows PC ではありません。
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 AP の IP アドレス、シークレットは無線 AP へ設定したものと同じものを設定します。

設定例：

※無線 AP では認証サーバ(RADIUS サーバ)として RA の IP アドレスを指定します。

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。

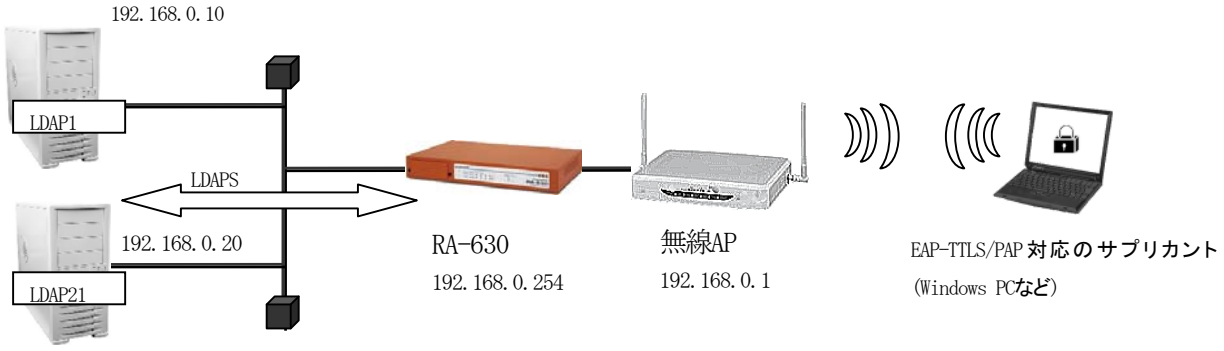
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例17. LDAPサーバに登録されたユーザで認証を行う

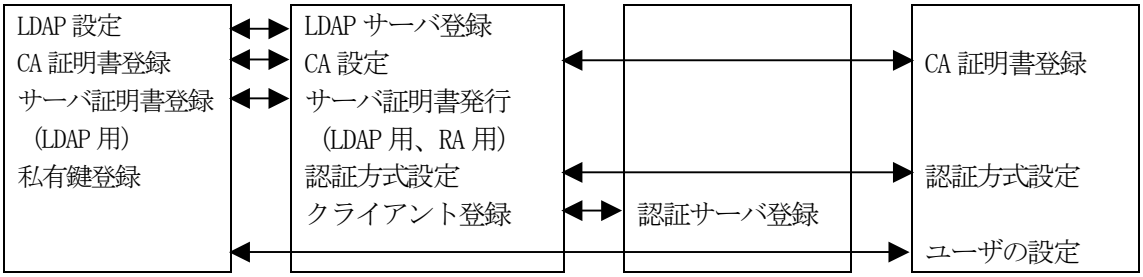
１．概要

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。

２．構成



LDAPサーバ



ここではLDAP を２つ用意し、ユーザ検索をLDAP1, LDAP2, RA ローカルの順に行います。
ユーザ認証にはEAP-TTLS/PAP を用い、RA－LDAP 間はLDAPS による暗号化通信を行うものとします。
LDAP を用いるにはRA に対して以下設定を行います。

CA の作成
EAP-TTLS 用にRA の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RA 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 クライアントとして無線AP を登録
LDAP サーバの登録
ローカルユーザの登録

３．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 AP(192.168.0.1)
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-1
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2015 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	30

※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 RA のサーバ証明書及び、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(RA)証明書を発行します。証明書画面から 新規追加 ボタンで追加します。
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 RA 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、RA がクライアント用となります。

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 RA 用の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 AP の IP アドレス **192.168.0.1** を設定します。
シークレットは無線 AP 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	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(RA)用のもの
証明書検証	検証する

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
シリアルナンバ	CA にて作成したクライアント(RA)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 **base1** 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 **base1** 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 **userprof1** 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 **userprof1** を指定します。
固定 IP 払い出しは行いませんので未入力とします。
入力後 

を押すことによりユーザが追加されます。

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。

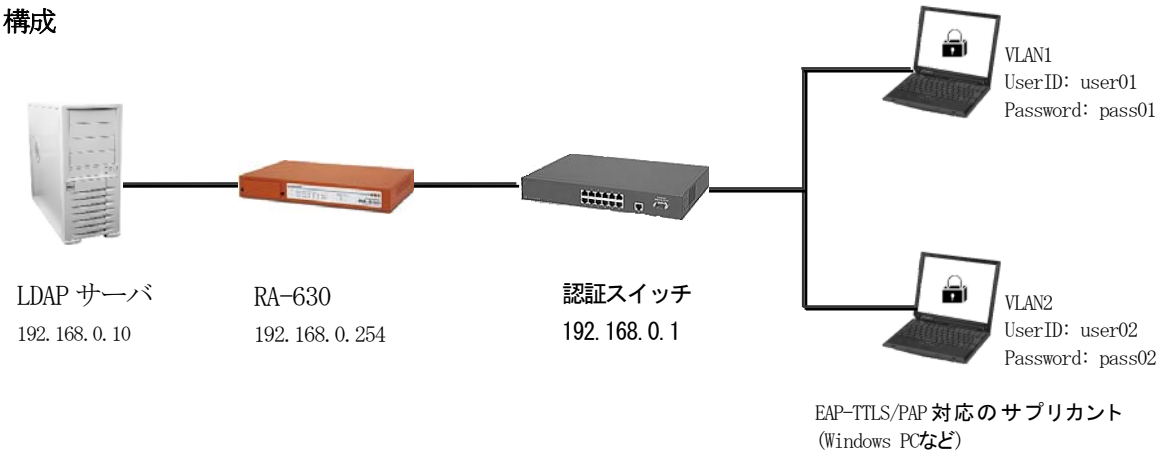
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

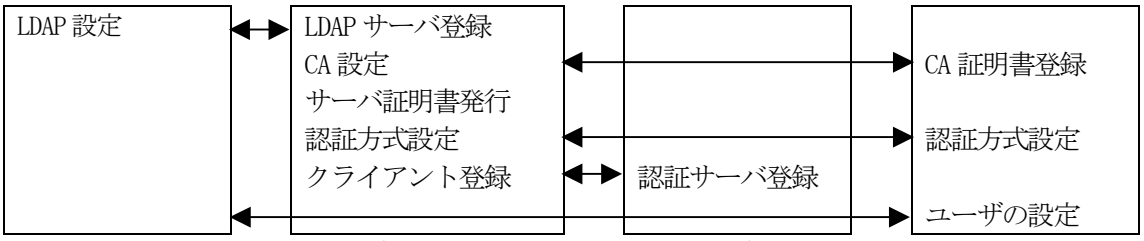
事例18. LDAPサーバから応答アトリビュートを取得する

１．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。

２．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以下の設定を行います。

CAの作成
EAP-TTLS用にRAの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クライアントとして無線APを登録
LDAPサーバの登録

３．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。

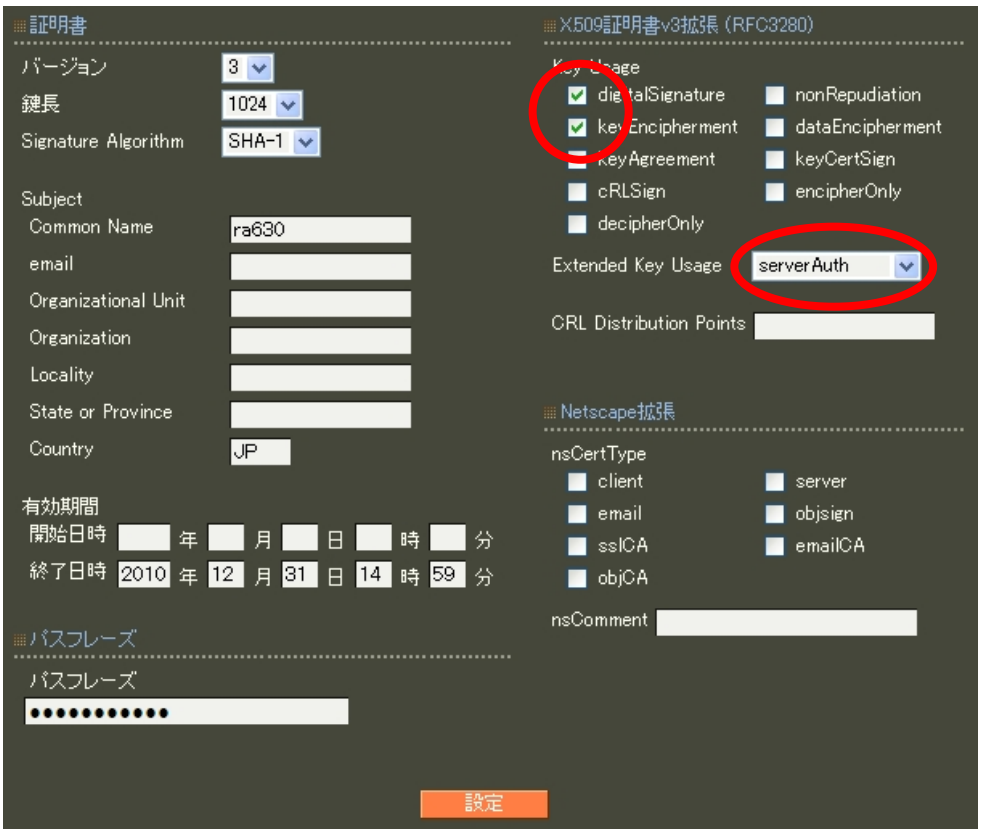
鍵長	1024
Signature Algorithm	SHA-1
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2015 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	30

※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 EAP-TTLS に使用するサーバ証明書を発行します。
証明書画面から 新規追加 ボタンで追加します。

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 RA 用の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 AP の IP アドレス **192.168.0.1** を設定します。
シークレットは無線 AP へ設定したものと同じものを入力します。

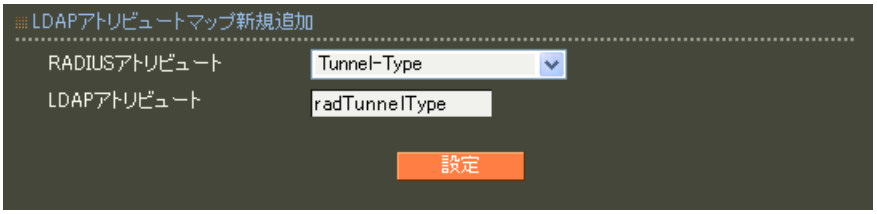
LDAP の設定（RADIUS／サーバ／LDAP）

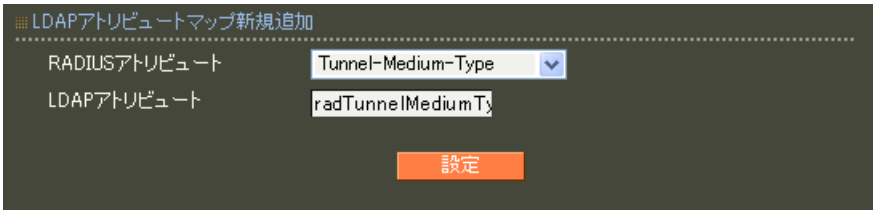
LDAP 画面の上段より 設定・編集 ボタンを押し設定画面を開きます。LDAP を「**使用する**」、認証順序「**LDAP → Local**」を選択して設定します。

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：



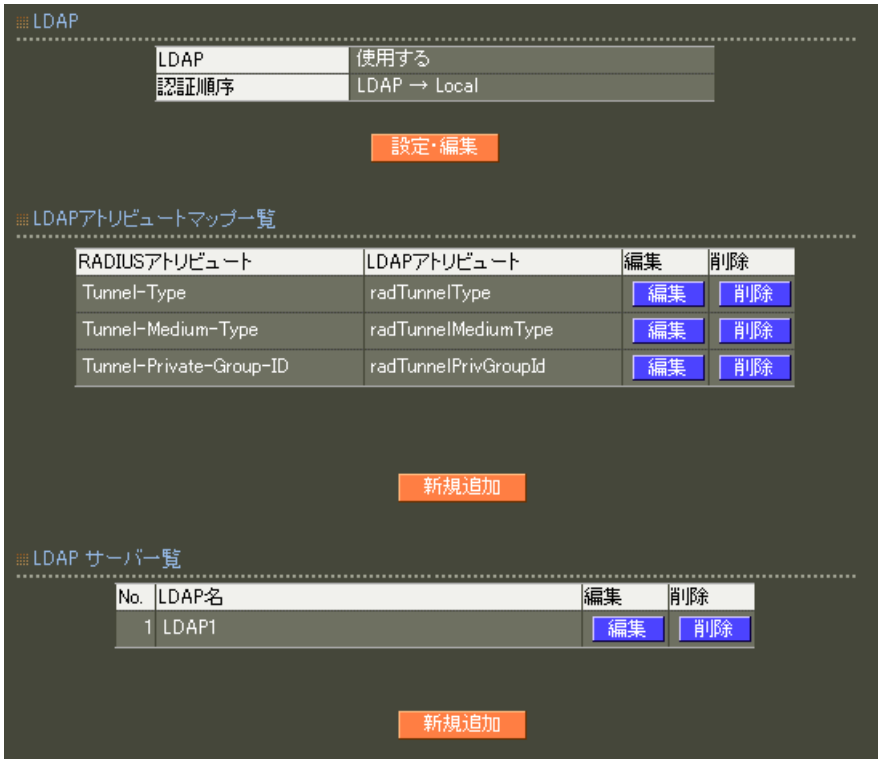


LDAP 画面下段　LDAP サーバ一覧より 新規追加 を押して LDAP サーバを追加します。
設定条件に従い、各項目を設定します。

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	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。



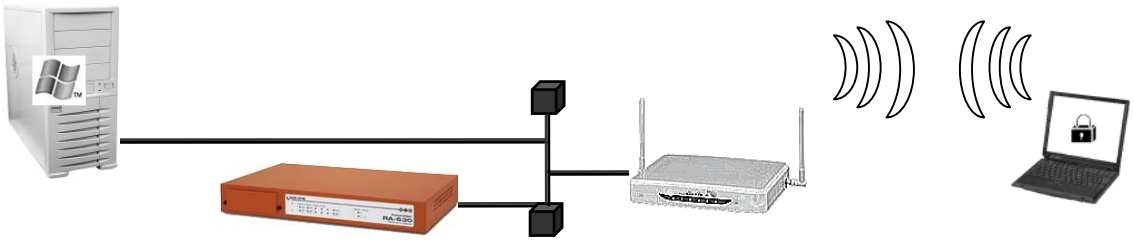
以上で RA の設定は終了です。RADIUS サーバを再起動して設定を反映させます。念のためここで設定の保存を行っておくとよいでしょう。

事例19. ActiveDirectoryをLDAPとして利用する

１．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。

２．構成

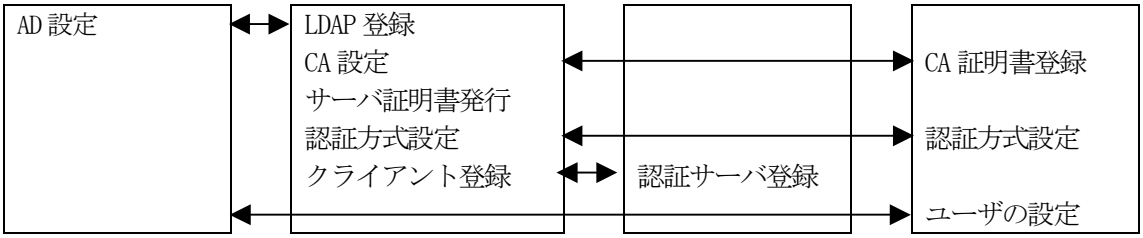


ActiveDirectoryサーバ
ad.example.jp
192.168.0.2

RA-630
192.168.0.254

無線AP
192.168.0.1

EAP-TTLS/PAP対応のサプリカント
(Windows PCなど)



ここではActiveDirectoryをLDAPとして用いる例を紹介します。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、EAP-TTLSのためのCA設定と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
EAP-TTLSで使用するRAの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AP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

３．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	192.168.0.2
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 AP(192.168.0.1)
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。

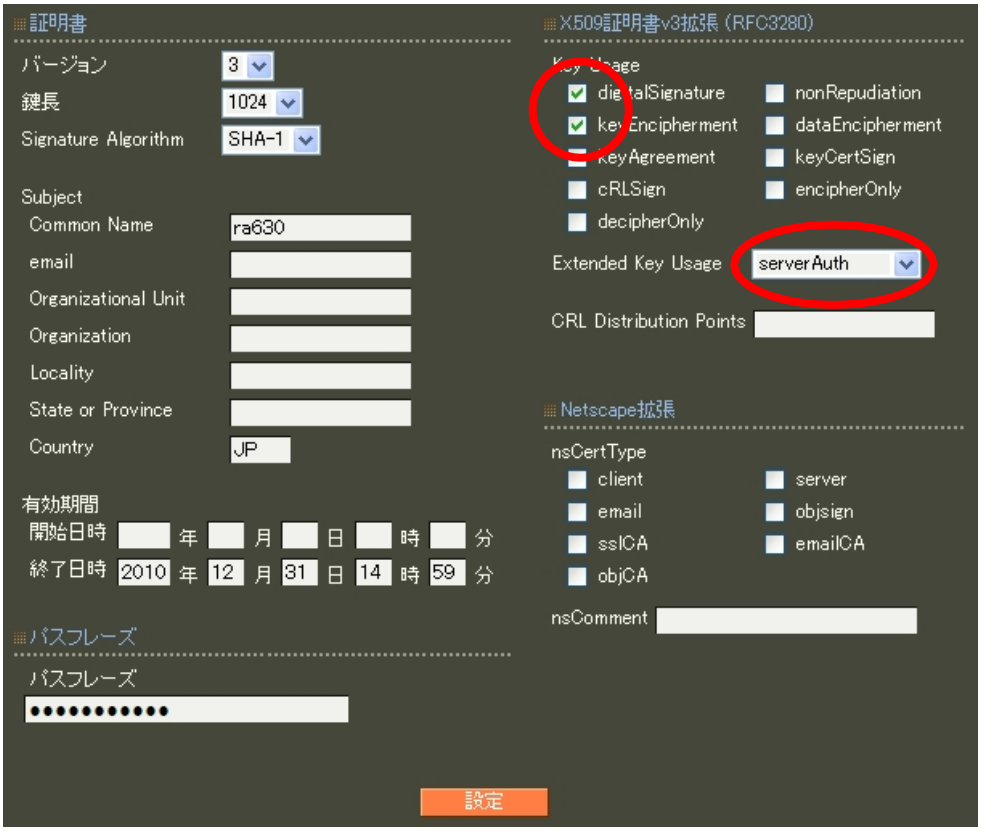
鍵長	**1024**
Signature Algorithm	**SHA-1**
Common Name	**sample_ca**
email	**samp@example.co.jp**
Country	**JP**
有効期間(終了日時)	**2015 / 12 / 31**
パスフレーズ	**passsample**
失効リスト更新間隔	**30**

※ 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 EAP-TTLS に使用するサーバ証明書を発行します。
証明書画面から 新規追加 ボタンで追加します。

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** と **EAP-TTLS** を選択します。
(EAP-TTLS の利用には EAP-TLS も選択されている必要があります。)
また、RADIUS サーバ証明書の **本装置の証明書を使用する** を選択し、シリアルナンバに
先ほど発行したサーバ証明書のシリアルナンバを 16 進数で入力します。
設定ウィザードを使って設定いる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 クライアントとして無線 AP の IP アドレス **192.168.0.1** を設定します。
シークレットは無線 AP 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**
LDAP サーバ	**192.168.0.2**
ポート	**389**
ベース DN	**cn=Users, dc=example, dc=jp**

Active Directory ドメインを要素毎に dc で指定します。

バインド DN	**Administrator@example.jp**
パスワード	**adminpassword**
フィルタオブジェクト	**なし**
フィルタアトリビュート	**sAMAccountName**

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。

セキュリティ	**None**
証明書検証	**検証しない**

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 **base1** 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
resp1 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 resp1 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。

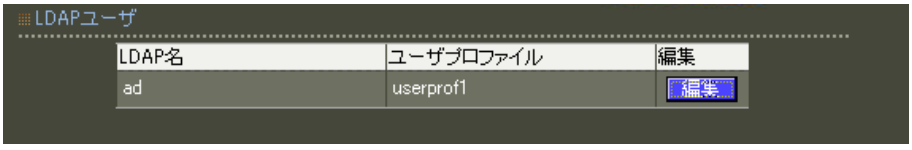
設定例：

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 **base1** と応答アトリビュートプロファイル **resp1** 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 **userprof1** 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 **userprof1** を選択して 設定 ボタンを押します。

以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

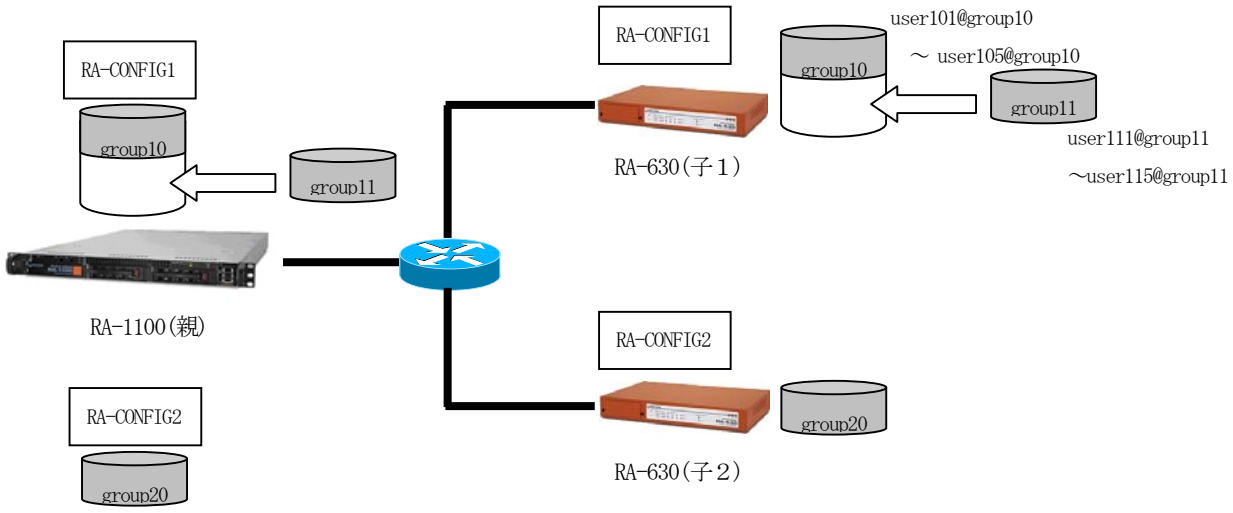
事例20. ユーザを一括で作成する

１．概要

ここでは、親子連携の構成を利用し、ユーザの一括作成と証明書を発行する例を紹介します。

２．構成

本例では既に EAP-TLS 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５件追加します。



設定条件

コンフィグ名（※）	RA-CONFIG1
ユーザ名	user111～user115
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-1
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

ユーザ名 user101～user105@group10 は既に
　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
という条件で登録済みとします。

ユーザの一括作成、証明書の発行は、それぞれ設定ファイルを作成し、RA-1100（親）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ることで行います。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。

３．設定例

ユーザの一括作成に必要なセクションは［RADIUS|ユーザ］ですが、ここではグループ ID を指定するためにプロファイルの作成を行うセクションが必要となります。

【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。

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 base 、グループ ID は group でそれぞれ指定します。プロファイルの作成準備は以上で終了です。

【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繰り返して記述します。

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=pass111
  profile=userprof11
  locked=off
  ipaddress=
  netmask=

create user
  config_id=RA-CONFIG1
  user_id=user112
  password=pass112
  profile=userprof11
  locked=off
  ipaddress=
  netmask=

      :
      :
create user
  config_id=RA-CONFIG1
  user_id=user115
  password=pass115
  profile=userprof11
  locked=off
  ipaddress=
  netmask=
```

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。

【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を繰り返し記述します。

証明書発行セクション記述例

```
[RADIUS|ユーザ|証明書発行]
create cert
  config_id=RA-CONFIG1
  user=user111@group11
  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=2015
  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
  config_id=RA-CONFIG1
```

※プロファイル作成、ユーザ作成と証明書発行を１つのファイルにして同時に設定する事はできません。それぞれ別の設定ファイルとして保存しご利用ください。

【ユーザ一括作成／証明書発行】

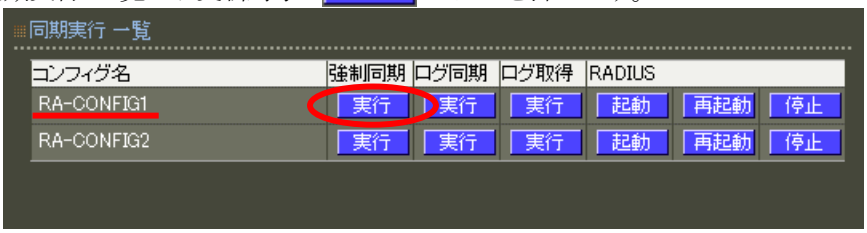
RA-1100（親）で操作を行います。
メニューの「RADIUS」－「ユーザ」－「ファイル読み込み」から RADIUS ユーザファイル読み込み画面を開きます。リセット は “しない”、設定ファイルにこれまでに作成した設定ファイルを指定、適用するコンフィグ名を選択して、復帰 ボタンを押します。
以上で新しいユーザの追加、証明書の発行が行なわれます。

ファイル読み込みのリセットについて

ここでリセット「する」を選択すると登録されている既存のユーザをリセット(削除)した上で新規にユーザ登録を行います。リセット「しない」を選択すると既存のユーザはそのまま設定ファイルに記述されたユーザの追加を行います。

【設定情報の同期】

最後に追加内容を子側へ反映させます。この操作も RA-1100（親）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 実行 ボタンを押します。



※ 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、一括同期処理（ 実行 ボタンを押します）を行なってください。

以上で RA の設定は終了です。

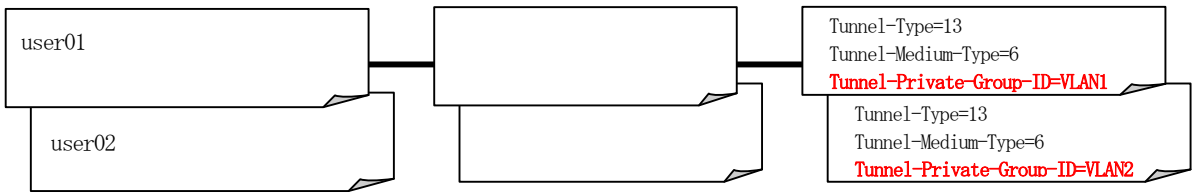
事例21. ユーザ毎に個別のアトリビュートを追加する

１．概要

ここではユーザ個別設定によりユーザにプロファイルとは別の、ユーザ毎のアトリビュートを設定する例を紹介します。[事例 10. ユーザ毎に応答アトリビュートを設定する]でおこなった VLAN の設定を、個別アトリビュートを使って設定します。事例 10 ではユーザ毎に応答アトリビュートプロファイルを作成し、ユーザ毎にユーザプロファイルを作成していました。このような設定を行う際は、ユーザ個別設定にユーザ毎に異なる値のみ設定することで、その他の共通の値を応答アトリビュートプロファイル１つにまとめることができます。

２．構成

【事例 10】



ユーザ設定
(ユーザ数分)

ユーザプロファイル
(ユーザ数分)

応答プロファイル
(ユーザ数分)

【本事例】

ユーザ設定
(ユーザ数分＋個別設定)

ユーザプロファイル
(共通)

応答プロファイル
(共通)

ユーザ毎に異なる設定のみ個別設定に行う。

３．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

これらは事例 10 同様、応答アトリビュートプロファイルを作成して指定します。この中でユーザ毎に設定を変えたい Tunnnel-Private-Group-ID のみ個別設定で対応します。

クライアントの登録 (RADIUS／サーバ／クライアント)

ここでの RADIUS クライアントは認証 SW です。クライアントとして認証 SW を登録します。クライアント名 sw1, IP アドレス 192.168.0.1, シークレット secret とします。

アトリビュートの登録 (RADIUS／サーバ／アトリビュート)

応答アトリビュートで使用するアトリビュートをここで登録します。この例題で使用するアトリビュートは standard アトリビュートとして登録済みですのでここではなにもしません。

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の作成が必要です。この例題ではプロファイル名を base1 、認証方式を PAP/CHAP とします。IP アドレスの払い出しは行いませんので 未使用 を選択します。

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 を返すために使う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 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。事例 10 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。続いて下段の表中の 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）

ユーザプロファイルも応答アトリビュートプロファイル同様、共通のもの１つ作成します。ユーザ基本情報プロファイルとして base1、応答アトリビュートプロファイルに vlan1 を選択しユーザプロファイル vlanuser を作成します。

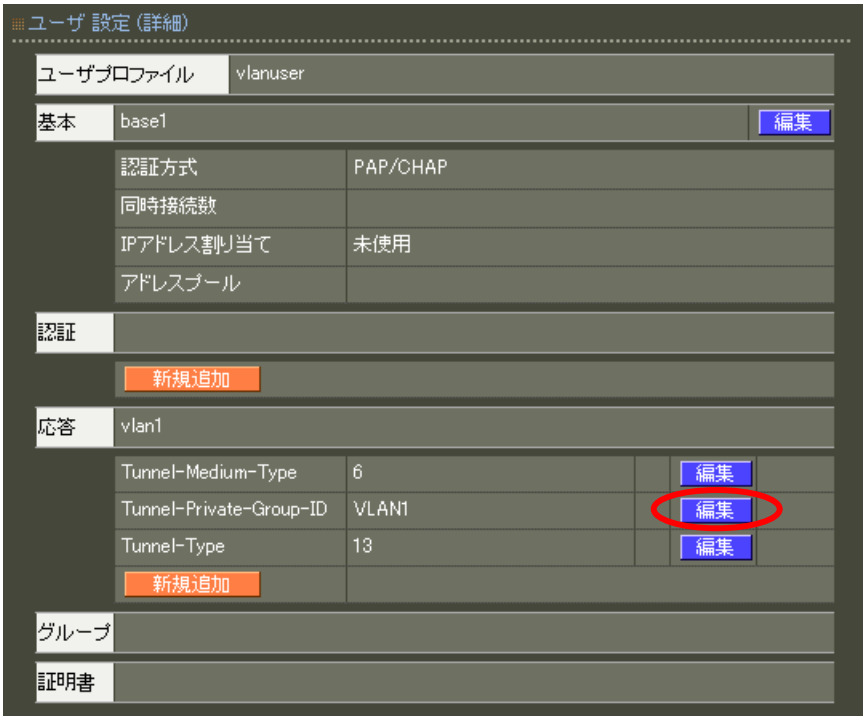
ユーザの登録（RADIUS／ユーザ／ユーザ）

これまでに作成したユーザプロファイル vlanuser を選択してユーザを作成していきます。ここではユーザ個別設定を気にする必要はありません。

ユーザ毎のアトリビュート設定（RADIUS／ユーザ／ユーザ）

ここでは user01 には VLAN1、user02 には VLAN2 を指定しますので、user01 はデフォルトのままなにも行わず、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。新たにアトリビュートを追加する場合は[新規追加]ボタンを押して追加します。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」を選択します。[設定]ボタンを押すことで個別設定の入力が完了します。

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。ここから再編集や削除を行うことができます。

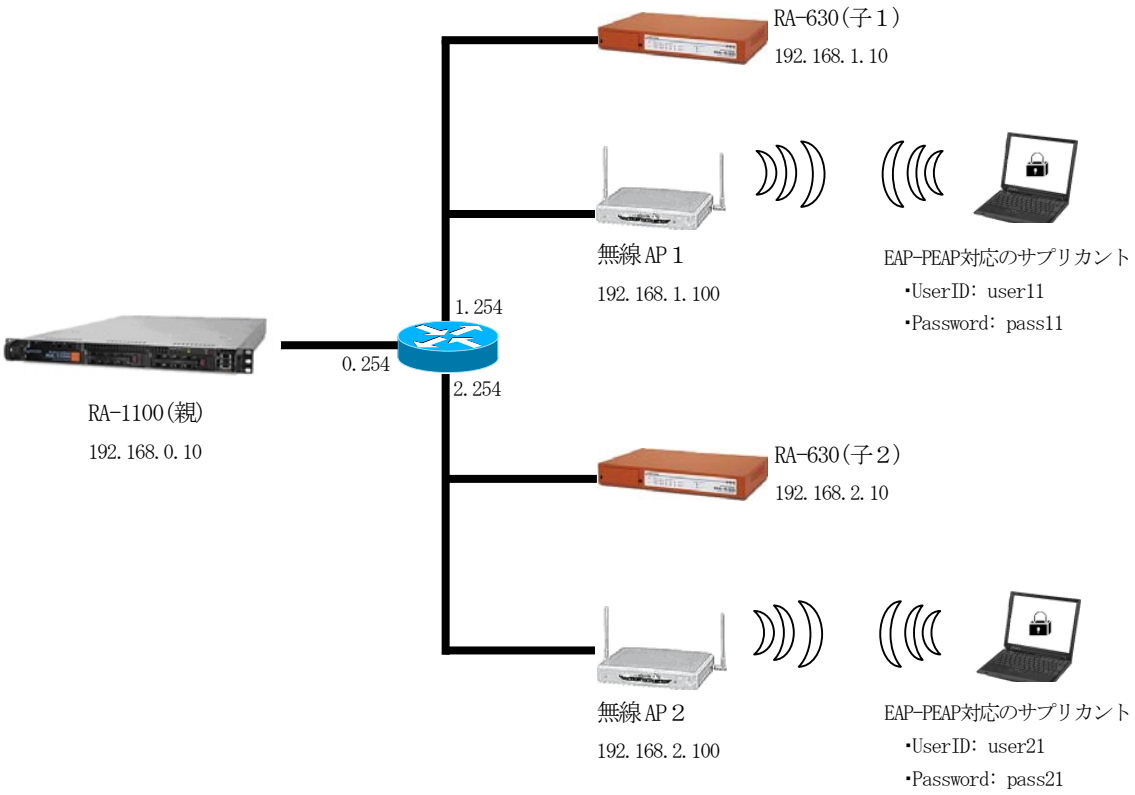
以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

事例22. 親子連携機能を使用する

１．概要

ここではRA-1100/RA-730/RA-630（以下RA）の親子連携機能による冗長構成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継続して親側で認証/アカウンティング処理を行う事ができます。RADIUS 認証に関する設定は、親で管理する事ができます。

２．構成



親子連携を利用し、無線LAN接続の認証に EAP-PEAP 認証を使用するにはRA-1100（親）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
RA 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 クライアントとして無線 AP 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）

次にRA-630（子）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

最後にRA-1100（親）でそれぞれのRA-630（子）に対して、強制同期を実行すれば設定は完了です。

　無線 AP１、AP2 に対しては、認証サーバ(*1) としてプライマリの認証サーバ子１または子２のRA-630 の IP アドレスを、セカンダリの認証サーバとして親の RA-1100 の IP アドレスを設定し、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、RA-1100（親）またはRA-630（子）から取得したCA 証明書の登録を行います。

*1　使用する機器により呼び名が変わります。各機器のマニュアルを参照してください

３．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 AP のクライアント名	AP1 AP2	AP1	AP2
無線 AP の IP アドレス	192.168.1.100 192.168.2.100	192.168.1.100	192.168.2.100
無線 AP のシークレット	secret	secret	secret
認証アトリビュートの追加	なし	なし	なし
応答アトリビュートの追加	なし	なし	なし
グループ ID	なし	なし	なし
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(RA-1100)を動作させる環境、本体の設定を行います。

３．１　親（RA-1100）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：

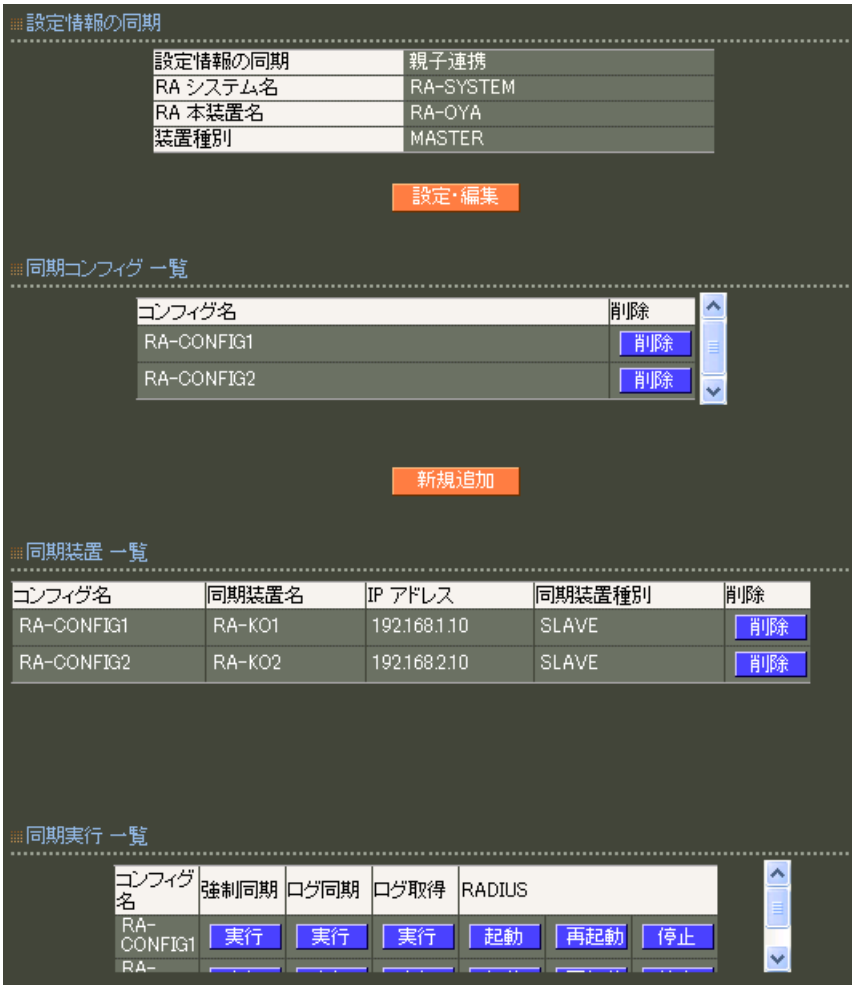
同期装置一覧で、各コンフィグに所属する装置を追加します。

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 ボタンで追加します。

ここでは、下記条件で設定を行います。

鍵長	1024
Signature Algorithm	SHA-1
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	samplepass
失効リスト更新間隔	30

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)

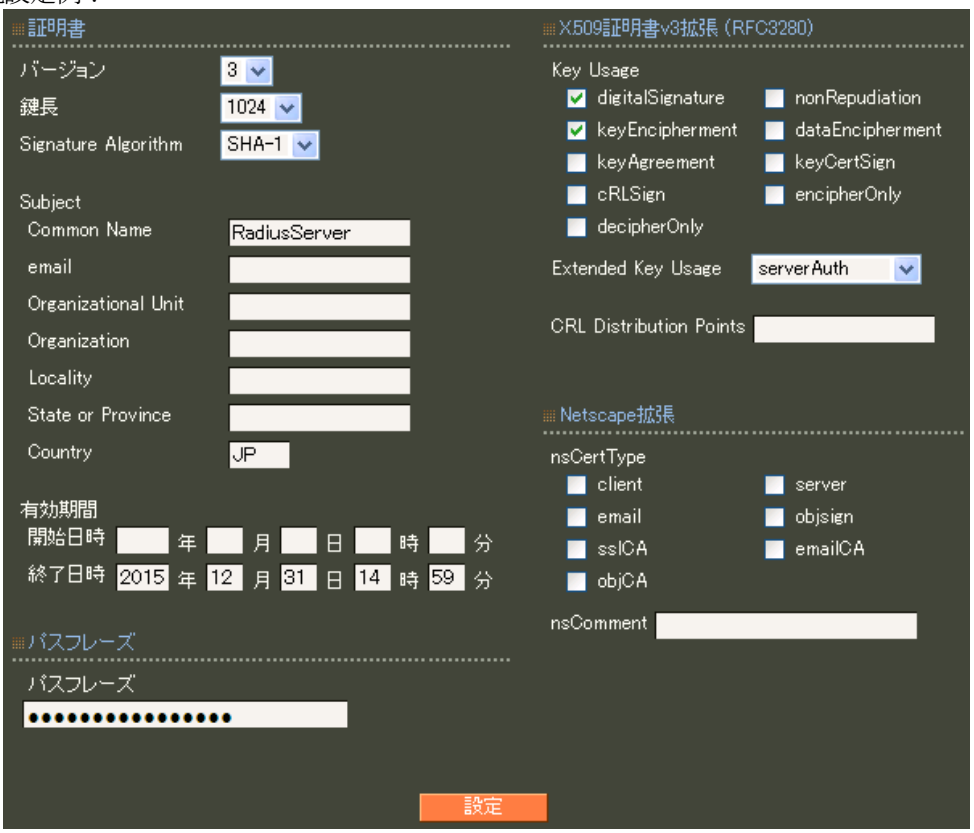
CA にて RADIUS サーバの証明に使用するサーバ証明書を発行します。

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-1
Common Name	RadiusServer
Country	JP
有効期間(終了日時)	2015 / 12 / 31 14 : 59
パスフレーズ	RadiusServerpass
Key Usage	DigitalSignature KeyEncipherment
Extended Key Usage	serverAuth

証明書画面から 新規追加 ボタンで追加します。

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

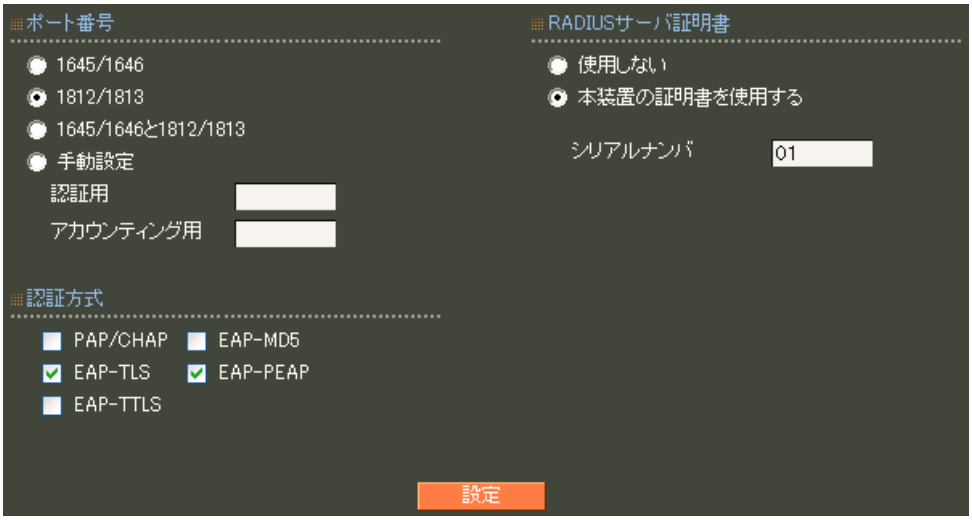
・Extended Key Usage：serverAuth

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。

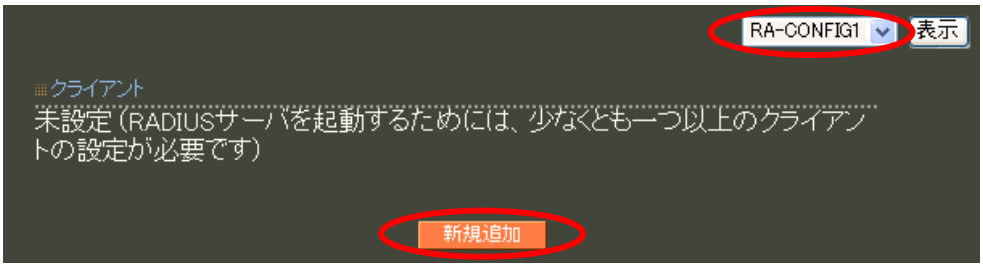
設定例：



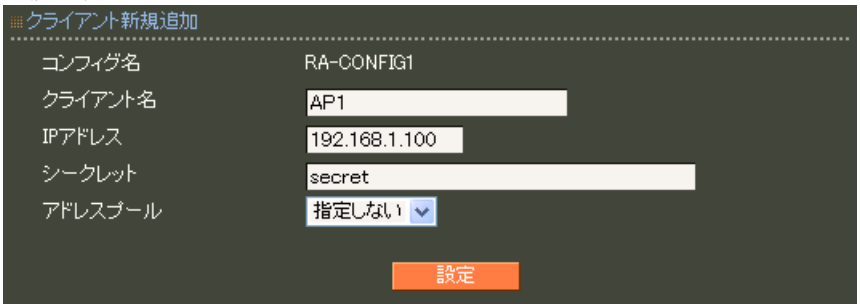
RADIUS クライアントの設定　(RADIUS／サーバ／クライアント)

　ここでの RADIUS クライアントは無線 AP です。
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 AP の IP アドレス、シークレットは無線 AP へ設定したものと同じものを設定します。

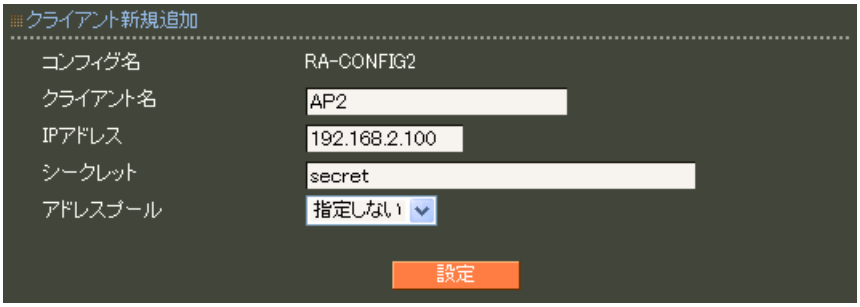
ここでも、**子１、子２のコンフィグを指定して** 新規追加 **ボタンで追加します。**



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 新規追加 ボタンで追加します。

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：

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 新規追加 ボタンで追加します。

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 新規追加 ボタンで追加します。

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 を押すことによりユーザが追加されます。
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(RA-630)を動作させる環境の設定を行います。

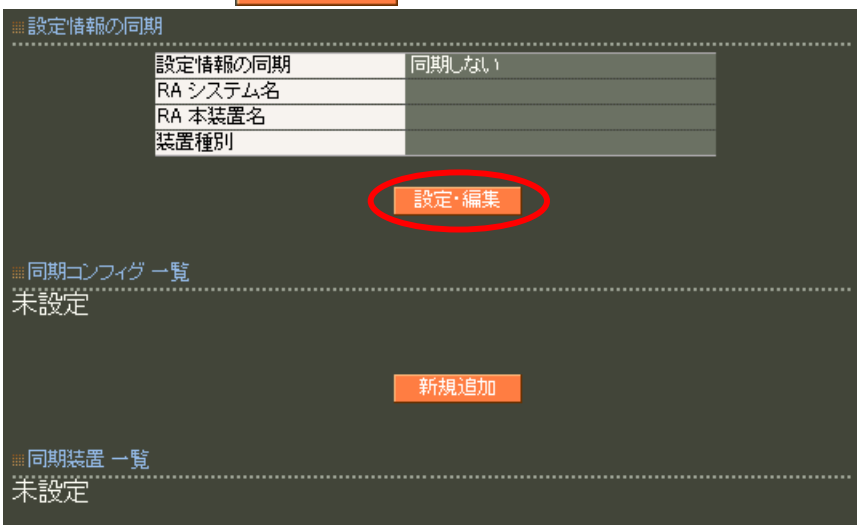
３．２　子（RA-630）の環境設定

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。
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）

設定情報の同期画面で 設定･編集 ボタンで設定します。



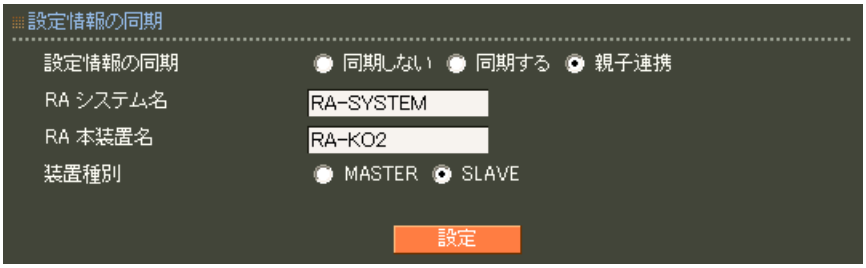
ここでは、RA-1100（親）で設定した内容に基づき下記設定を行います。

	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設定例：

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設定例：



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を追加します。

子１、子２設定例：

以上でRA-630（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表示例：

子２表示例：

最後にRA-1100（親）で設定した情報をRA-630（子１、子２）へ反映させます。
以下の操作は、RA-1100（親）で行います。

３．３　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”peer up”②により状況を確認する事ができます。処理中は、”peer down”①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。

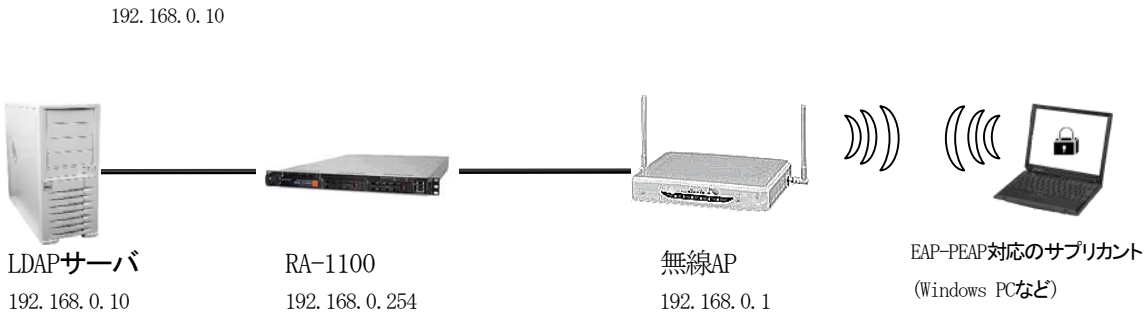
以上で親子連携の設定は終了です。最後に全ての機器でRADIUSサーバを起動します。

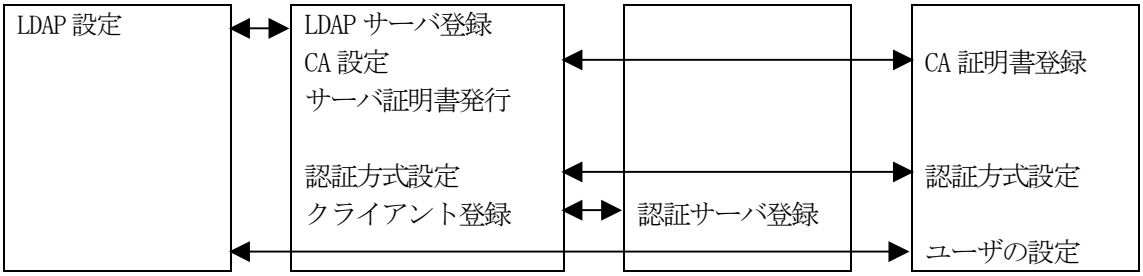
事例23. LDAPサーバに登録されたユーザでEAP-PEAP認証を行う

１．概要

ここではLDAPサーバに登録されているユーザでEAP-PEAP認証を行う例を紹介します。
(EAP-PEAP認証可能な機種/ファームウェアに限ります)

２．構成





ここでは、ユーザ検索をLDAP,RAローカルの順に行います。
ユーザ認証にはEAP-PEAPを用います。LDAPを用いるにはRAに対して以下設定を行います。

CAの作成
EAP-PEAP用にRAの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クライアントとして無線APを登録
LDAPサーバの登録

３．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。

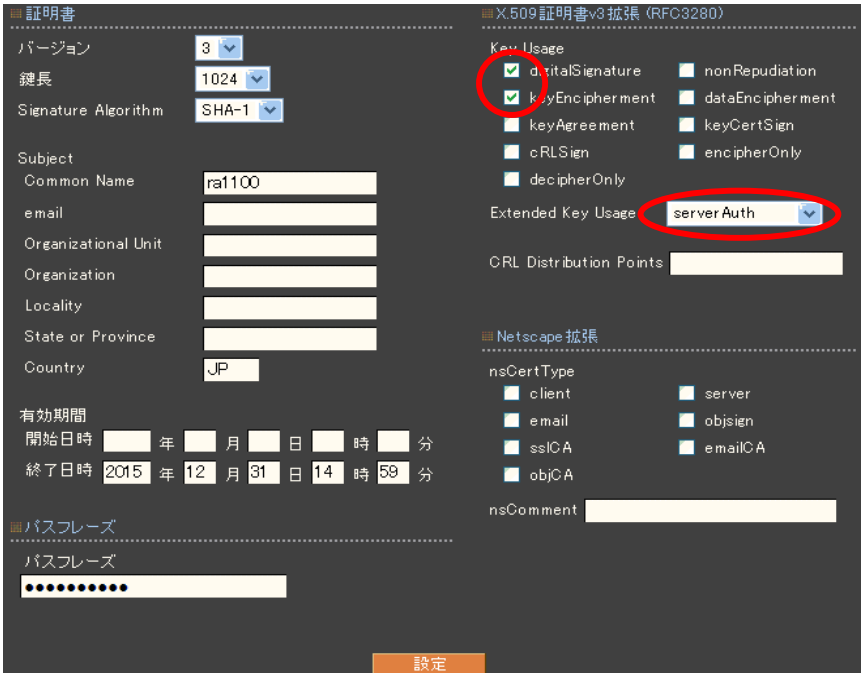
鍵長	1024
Signature Algorithm	SHA-1
Common Name	sample_ca
email	samp@example.co.jp
Country	JP
有効期間(終了日時)	2035 / 12 / 31
パスフレーズ	passsample
失効リスト更新間隔	365

※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)

CA にて EAP-PEAP で使用する RA のサーバ証明書を発行します。
証明書画面から 新規追加 ボタンで追加します。

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 RA 用の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 AP の IP アドレス **192.168.0.1** を設定します。
シークレットは無線 AP 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。

以上で RA の設定は終了です。最後に RADIUS サーバを起動します。

以下 Ver1.8.4 以降の LDAP 連携について補足情報です。

今までの 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
- EAPTTLS/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。
このままご利用頂いても差し支えございません。

RA-1100/RA-730/RA-630 設定事例集 1.4.0

2010 年 12 月版
発行 センチュリー・システムズ株式会社