# Net'Attest EPS　設定例

## 連携機器：

## FortiGate-80C、FortiAP-220B

## Case：TLS 方式での認証

Version 1.1

株式会社ソリトンシステムズ

# はじめに

## 本書について

本書は、弊社 CA 内蔵 RADIUS サーバプライアンス Net'Attest EPS と、フォーティネットジャパンの FortiGate-80C、FortiAP-220B との 802.1x 環境での接続について、その設定例を示したものです。

各機器の管理 IP アドレスの設定などの基本設は、既に完了しているものとします。設定例は、管理者アカウントでログインし、設定可能な状態になっていることとします。

## 表記方法

| 表記方法 | 説明 |
|---|---|
| ABCDabcd1234 (normal) | コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例を示します。 |
| **ABCDabcd1234 (bold)** | ユーザが入力する文字を、画面上のコンピュータ出力と区別して示します。 |
| *ABCDabcd1234 (italic)* | 変数を示します。実際に使用する特定の名前または値で置き換えます。 |

| 表記方法 | 説明 |
|---|---|
| 『 』 | 参照するドキュメントを示します。 |
| 「 」 | 参照する章、節、ボタンやメニュー名、強調する単語を示します。 |
| [キー] | キーボード上のキーを表します。 |
| [キー1]+[キー2] | [キー1]を押しながら[キー2]を押すことを表します。 |

## 表記方法(コマンドライン)

| 表記方法 | 説明 |
|---|---|
| %, $, > | 一般ユーザのプロンプトを表します。 |
| # | 特権ユーザのプロンプトを表します。 |
| [filename] | [ ] は省略可能な項目を示します。この例では、filename は省略してもよいことを示しています。 |

## アイコンについて

| アイコン | 説明 |
|---|---|
|  | 利用の参考となる補足的な情報をまとめています。 |
|  | 注意事項を説明しています。場合によっては、データの消失、機器の破損の可能性があります。 |

## 画面表示例について

本書で使用している画面(画面キャプチャ)やコマンド実行結果は、実機での表示と、若干の違いがある場合があります。

## ご注意

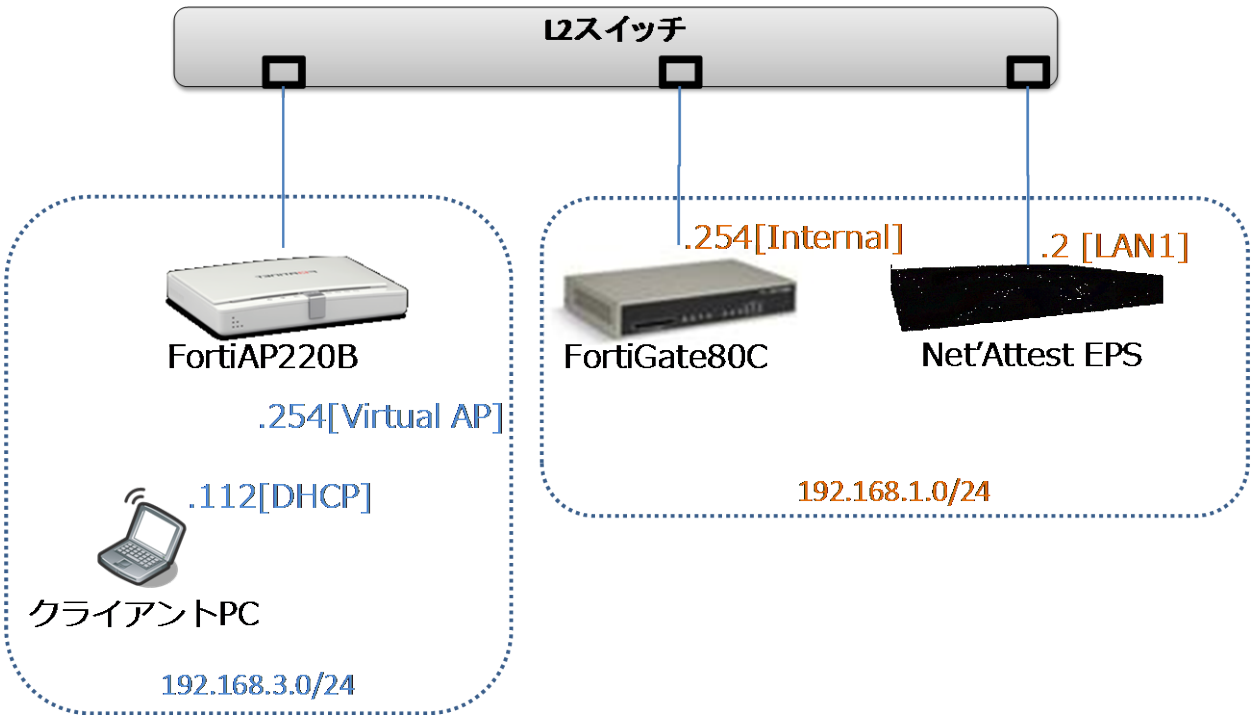
本書は、当社での検証に基づき、Net'Attest EPS 及び FortiGate、FortiAP の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

# 目次

# 1 構成

## 1-1　　構成図

・有線LANで接続する機器はすべて、L2スイッチに収容
・無線LANは別セグメントで、FortiGateのDHCPサーバからIPアドレスを払いだす



# 1-2　環境

## 1-2-1　機器

| 役割 | メーカー | 製品名 | SW バージョン |
|---|---|---|---|
| Authentication Server<br>(認証サーバ) | Soliton Systems | Net'Attest EPS ST-03 | Ver. 4.0.3 |
| Authenticator<br>(認証機器) | Fortinet | FortiGate-80C | Ver. 4.0　MR2 |
| | | FortiAP-220B | – |
| Client PC　/ Supplicant<br>(802.1x クライアント) | Panasonic<br>Microsoft | Let's note CF-W7 | Windows XP　SP3<br>Windows 標準サプリカント |

## 1-2-2　認証方式

IEEE 802.1x TLS

## 1-2-3　ネットワーク設定

| | EPS-ST03 | FortiGate-80C | FortiAP-220B | Client PC |
|---|---|---|---|---|
| IP アドレス | 192.168.1.2/24 | 192.168.1.254/24<br>(Internal)<br>192.168.3.254/24<br>(Virtual-AP) | – | 192.168.3.112<br>(DHCP) |
| RADIUS port<br>(Authentication) | UDP 1812 | | | – |
| RADIUS port<br>(Accounting) | UDP 1813 | | | – |
| RADIUS Secret<br>(Key) | soliton | | | – |

# 2 Net'Attest EPS

## 2-1 Net'Attest EPS 設定の流れ

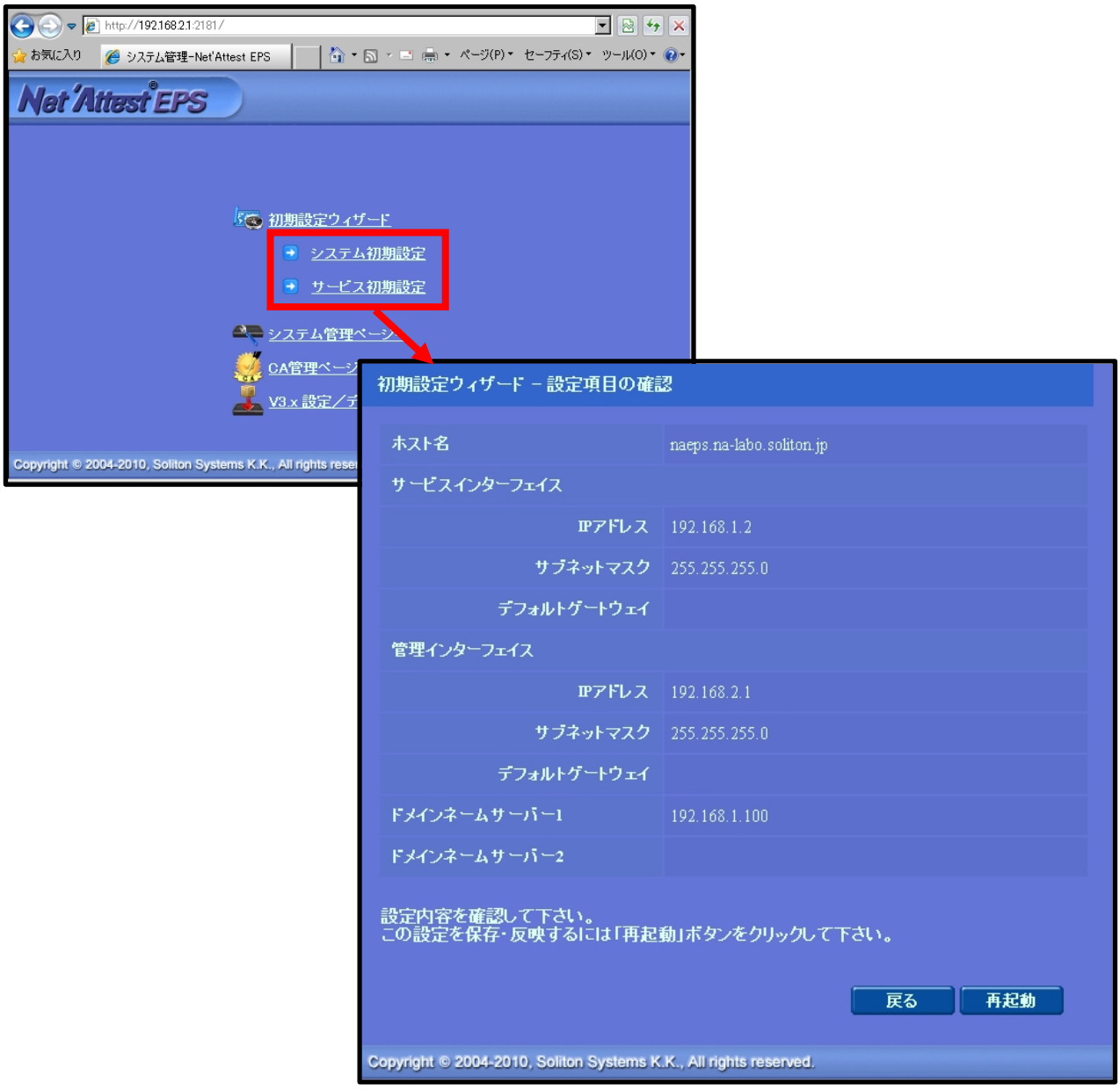
設定の流れ

1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

## 2-2 システム初期設定ウィザードの実行

システム初期設定ウィザードを使用し、以下の項目を設定します。

- ◆ タイムゾーンと日付・時刻の設定
- ◆ ホスト名の設定
- ◆ サービスインターフェイスの設定
- ◆ 管理インターフェイスの設定
- ◆ メインネームサーバの設定

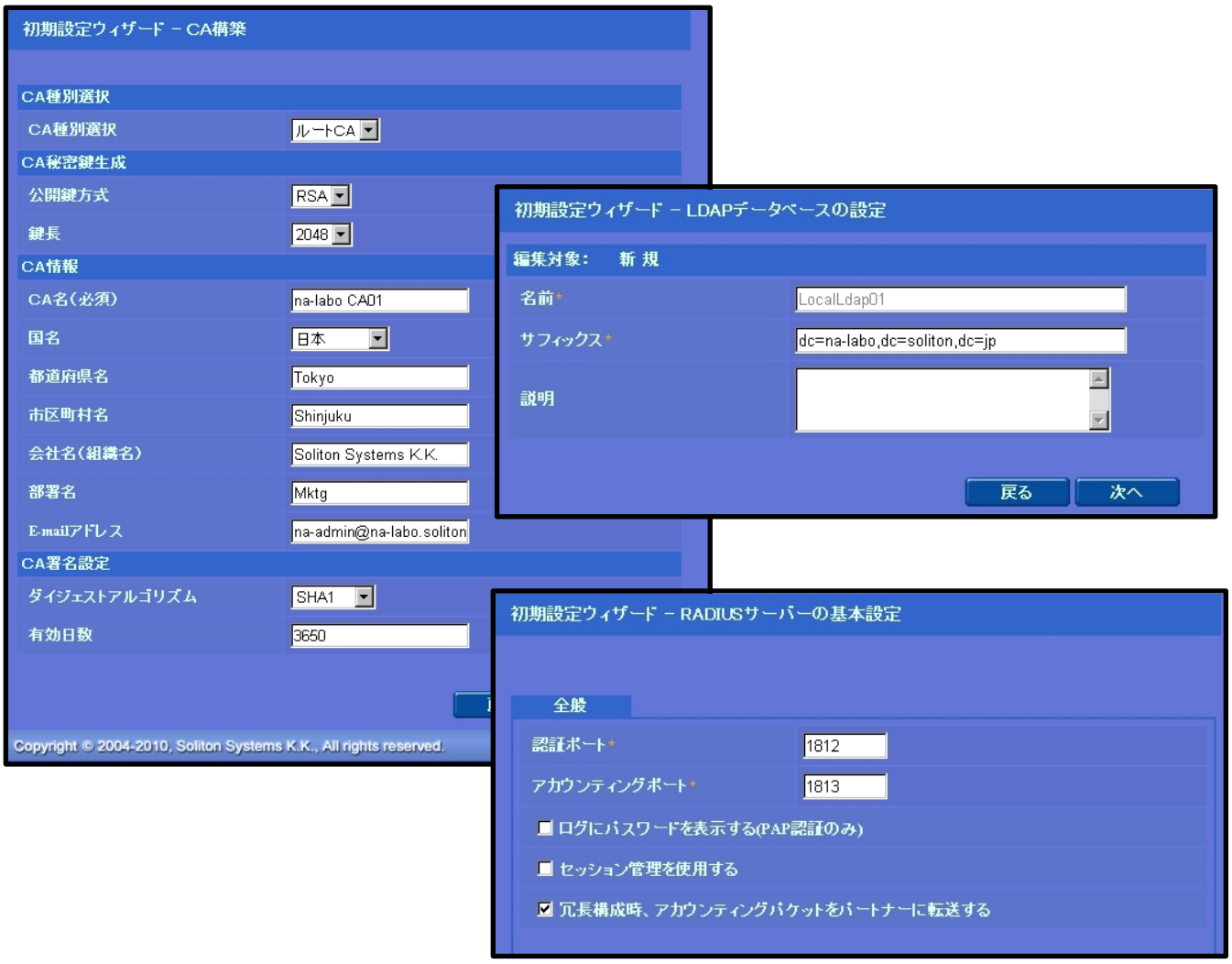


# 2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

本書では、黒文字の項目のみ、設定しました。

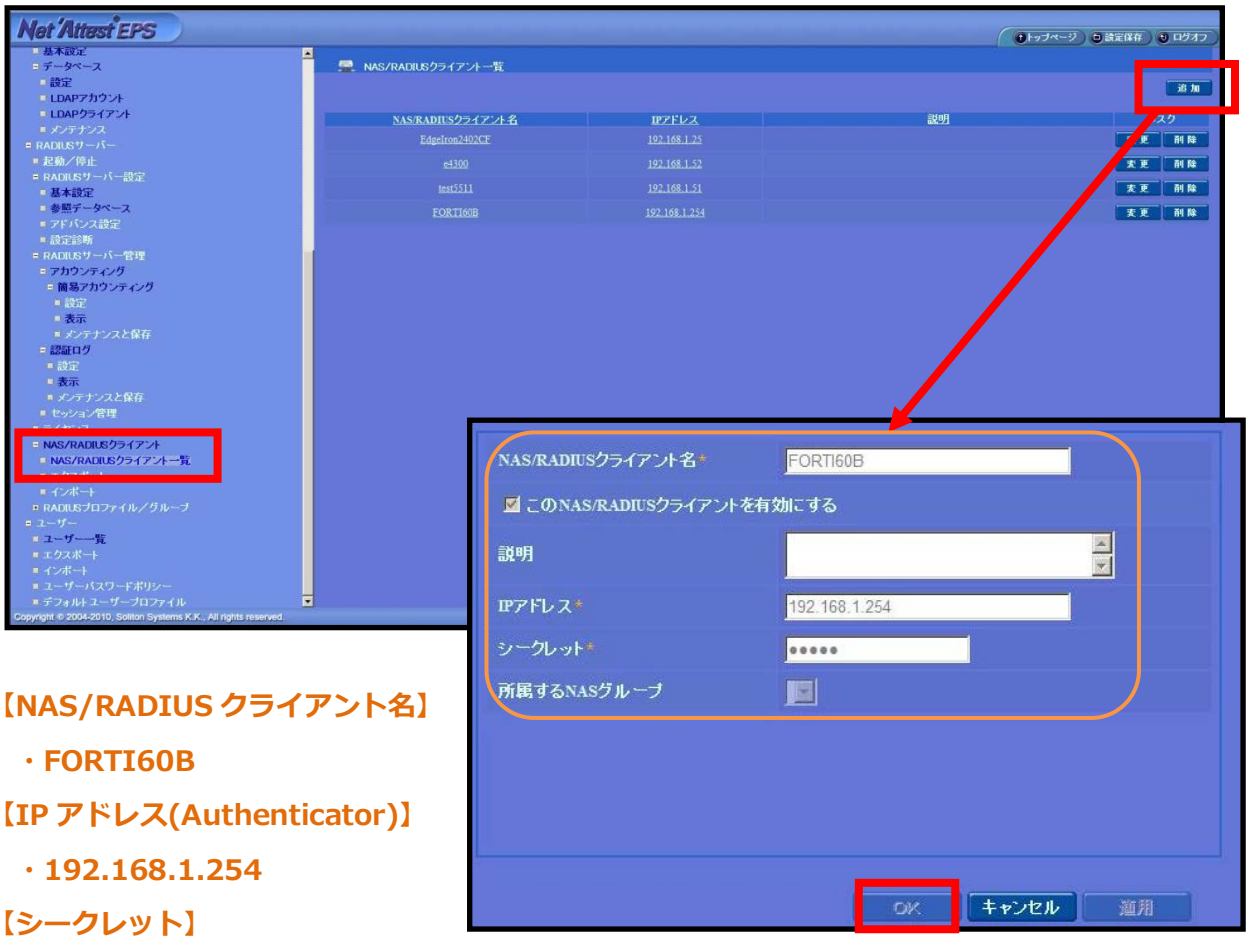
- CA 構築
- LDAP データベースの設定
- RADIUS サーバの基本設定（全般）
- RADIUS サーバの基本設定（EAP）
- RADIUS サーバの基本設定（証明書検証）
- NAS/RADIUS クライアント設定



# 2-4 Authenticator(RADIUS Client)の登録

WebGUI より、RADIUS Client の登録を行います。

「RADIUS サーバ設定」→「NAS/RADIUS クライアント追加」から、RADIUS Client の追加を行います。




**【NAS/RADIUS クライアント名】**

**・FORTI60B**

**【IP アドレス(Authenticator)】**

**・192.168.1.254**

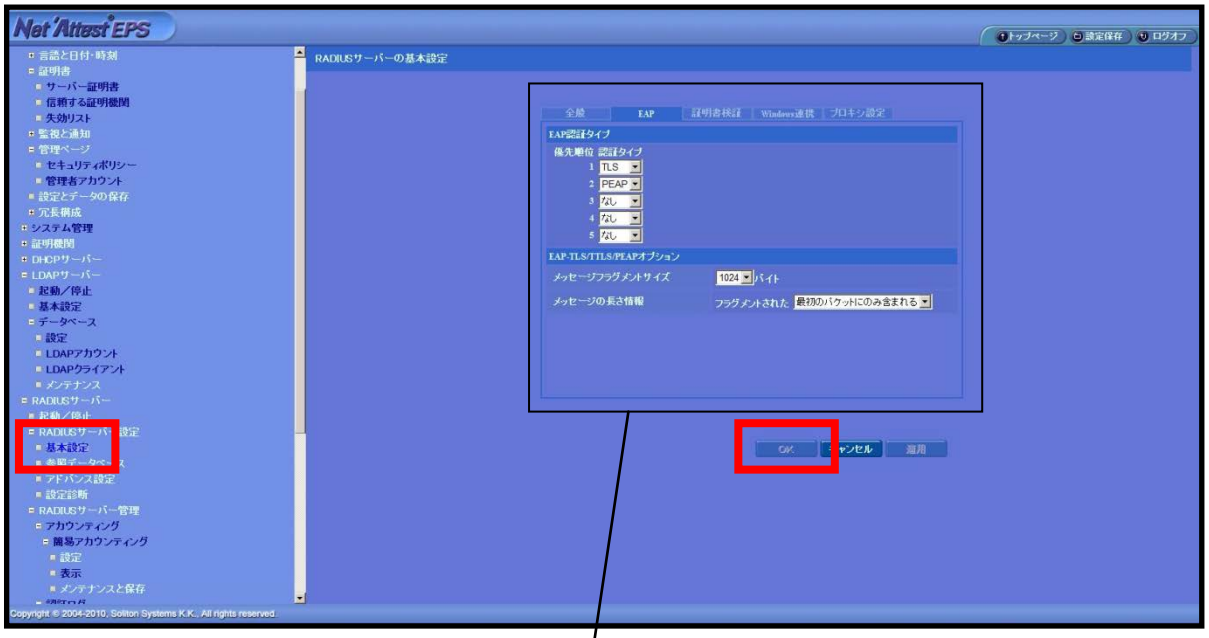
**【シークレット】**

**・soliton**

# 2-5 RADIUS サーバ基本設定

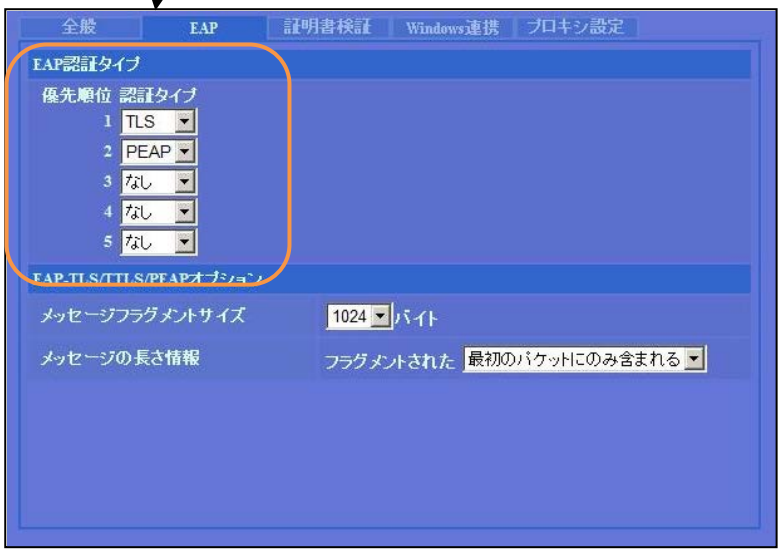
WebGUI より、RADIUS サーバの基本設定を行います。

「RADIUS サーバ」→「RADIUS サーバ設定」→「基本設定」→「EAP」から設定を行います。




**【優先順位　認証タイプ】**

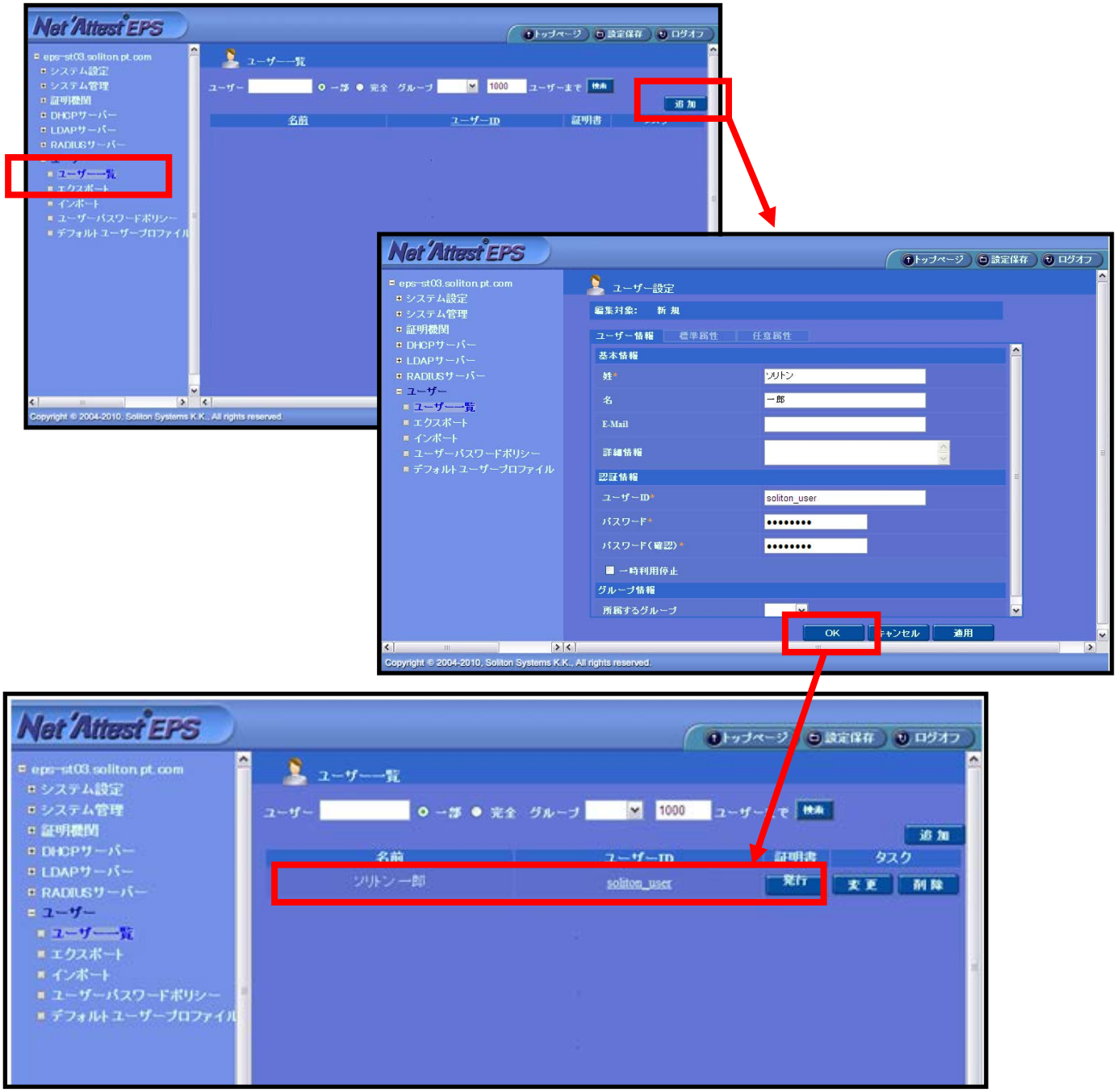
**・1)TLS**



## 2-6 ユーザーの登録

WebGUI より、ユーザー登録を行います。

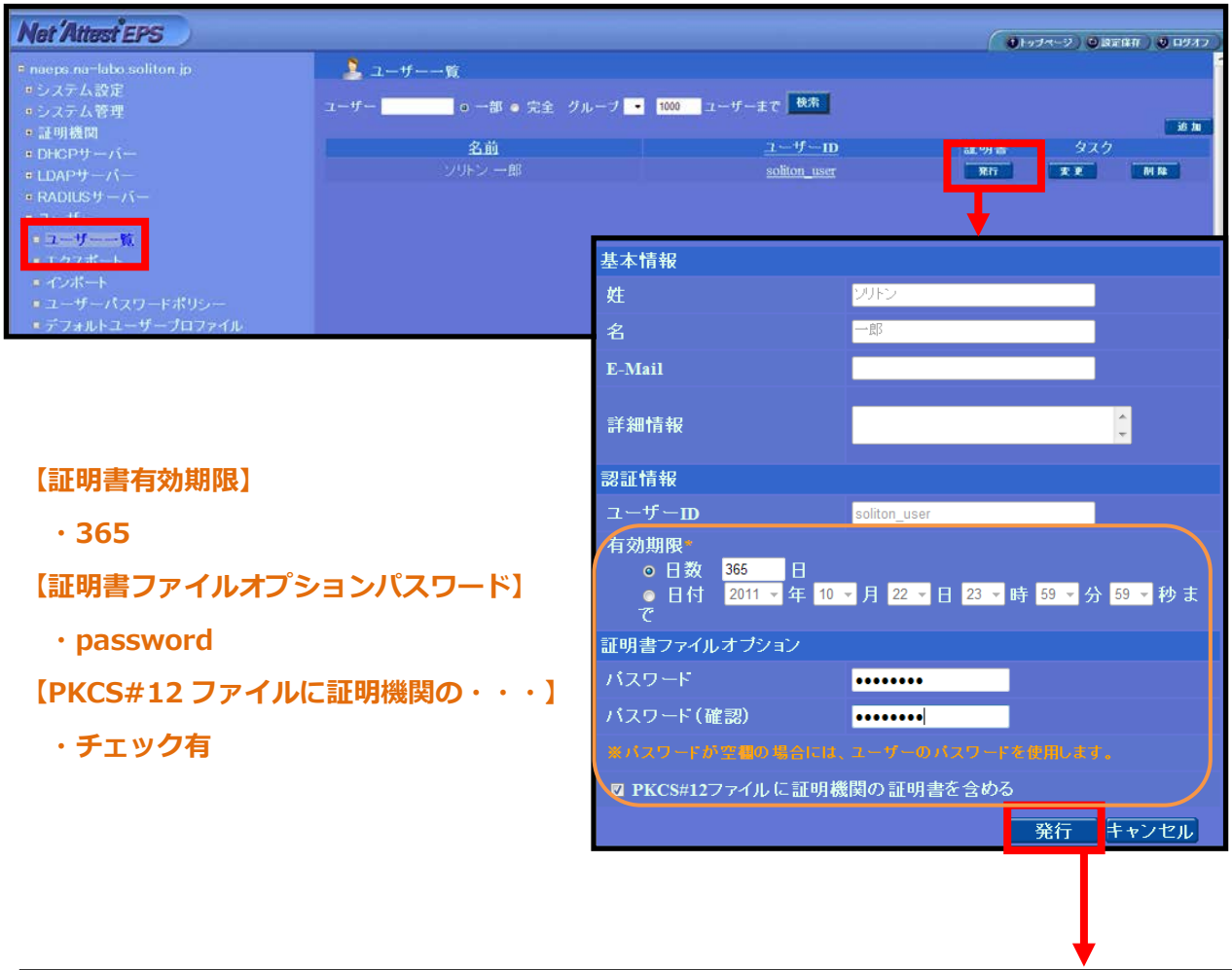
「ユーザー」→「ユーザー一覧」から、『追加』ボタンでユーザー登録を始めます。



## 2-7 ユーザー証明書の発行

WebGUI より、ユーザー証明書の発行を行います。

「ユーザー」→「ユーザー一覧」から、該当するユーザーの「証明書」の欄の『発行』ボタンでユーザー証明書の発行を始めます。




**【証明書有効期限】**

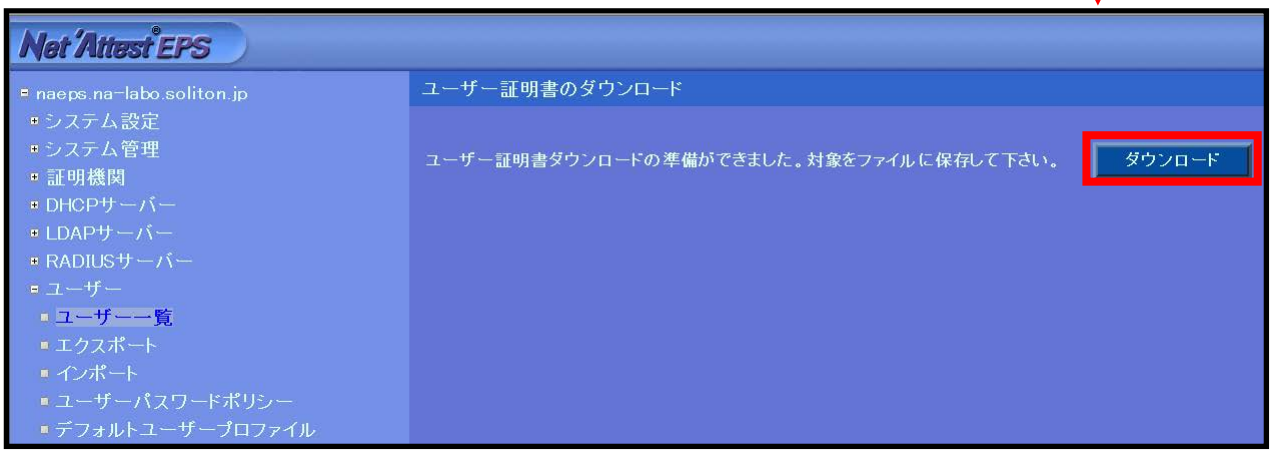
**・365**

**【証明書ファイルオプションパスワード】**

**・password**

**【PKCS#12 ファイルに証明機関の・・・】**

**・チェック有**



# 3 FortiGate-80C/FortiAP-220B

## 3-1 FortiGate-80C/FortiAP-220B 設定の流れ

設定の流れ

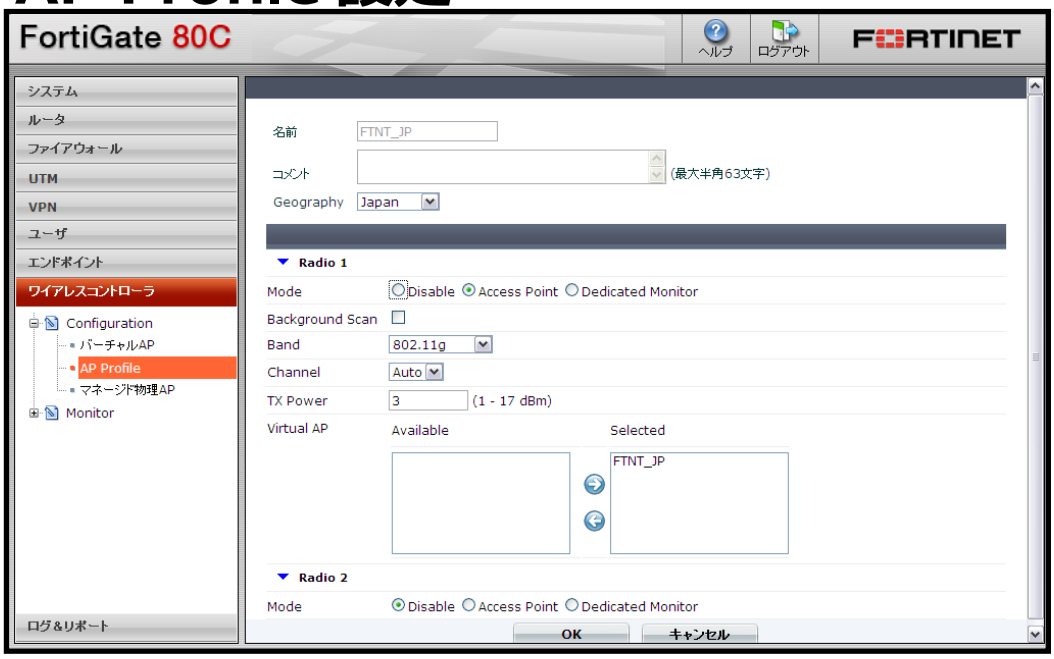
1. RADIUS サーバの登録
2. virtual-AP の設定

## 3-2 AP Profile、マネージド物理 AP の確認

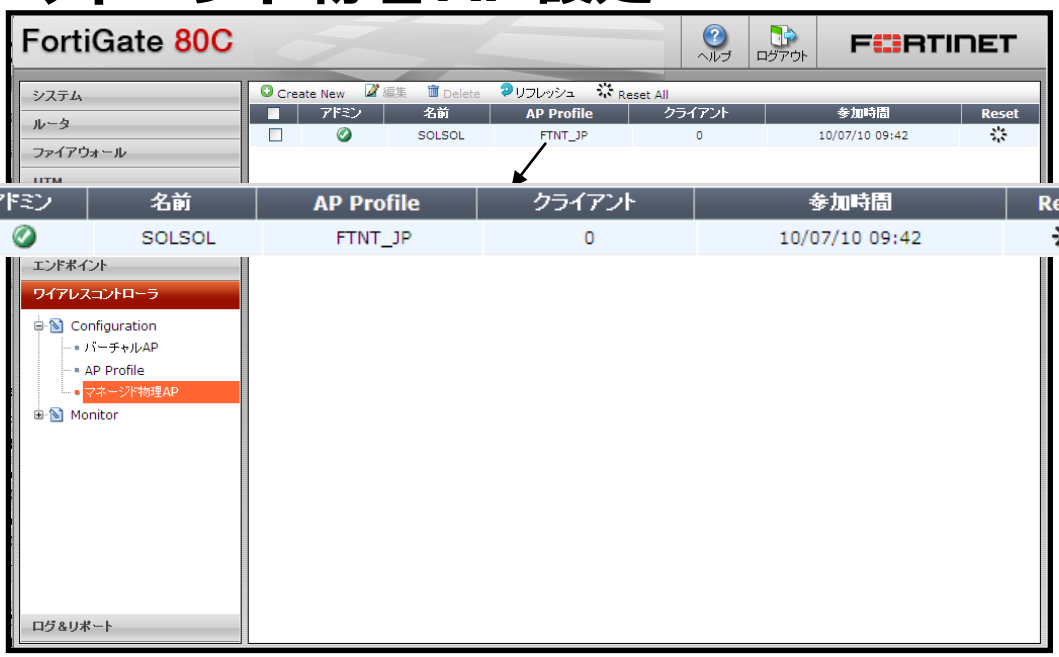
既に基本接続設定は終了している為、

「AP Profile」および「マネージド物理 AP」は下記のように設定されています。

# AP Profile 設定



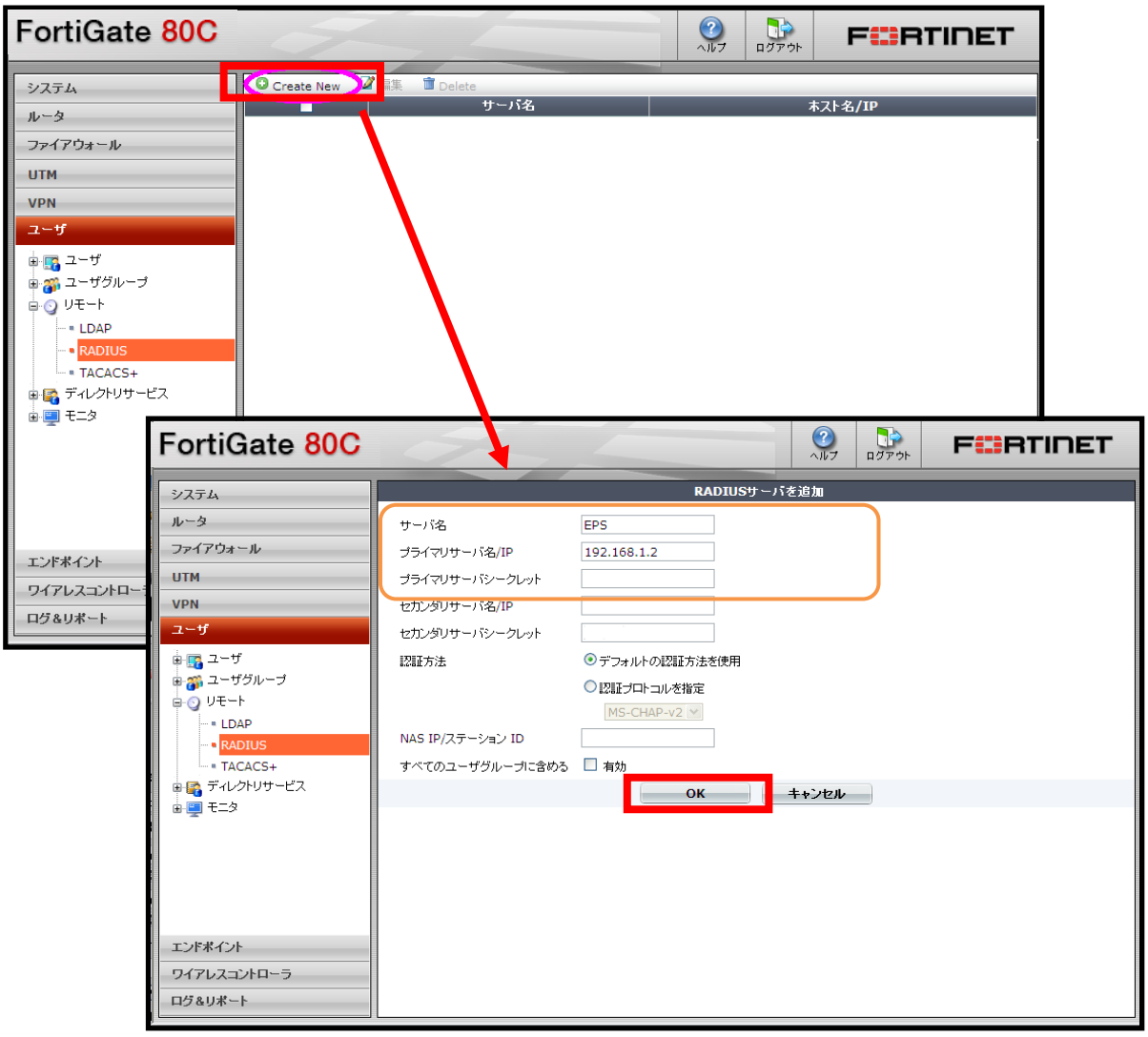

# マネージド物理 AP 設定



## 3-3 RADIUS サーバの登録

WebGUI より、RADIUS サーバの登録を行います。

「ユーザ」→「リモート」→「RADIUS」から、「Create New」を押下し、RADIUS サーバの登録を行います。




**【サーバ名】**

**・EPS**

**【プライマリサーバ名/IP (Authentication Server)】**

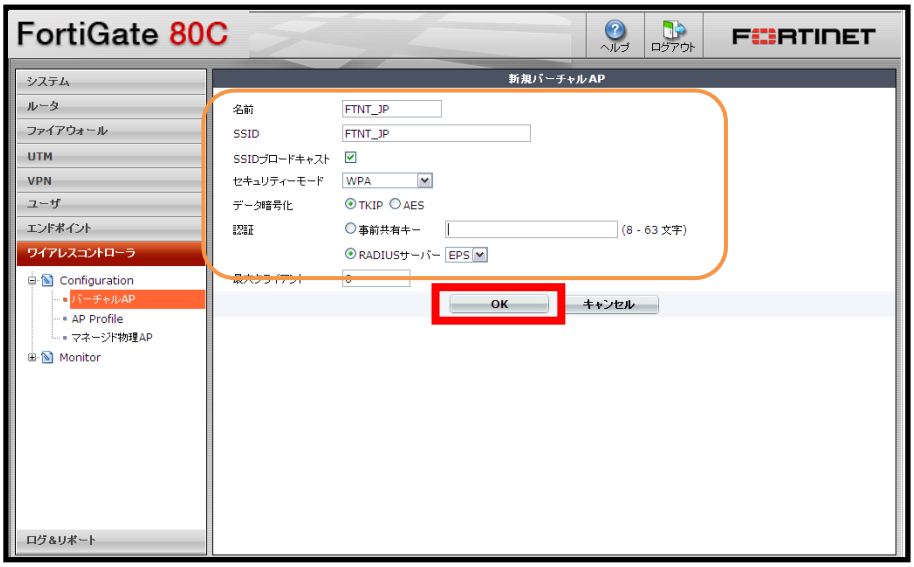
**・192.168.1.2**

**【プライマリサーバシークレット】**

**・soliton**

## 3-4 バーチャル AP の登録

「ワイアレスコントローラ」の設定にて「Configuration」→「バーチャル AP」から「Create New」を押下し、バーチャル AP の追加を行います




**【名前】**

**・FINT_JP**

**【SSID】**

**・FINT_JP**

**【SSID ブロードキャスト】**

**・チェック有**

**【セキュリティモード】**

**・WPA**

**【データ暗号化】**

**・TKIP**

**【RADIUS サーバ】**

**・EPS**

# 4 クライアント PC の設定

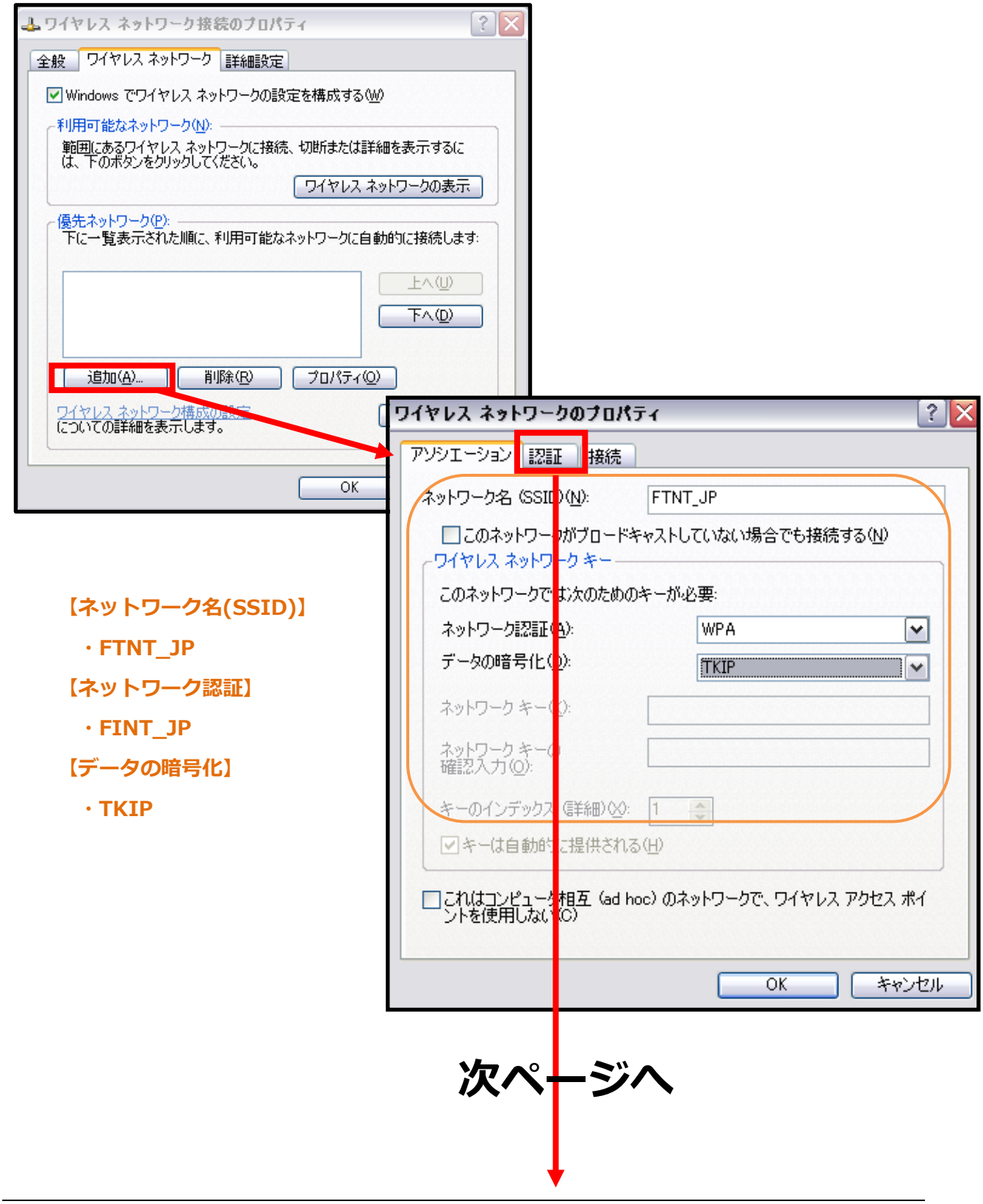
## 4-1 クライアント PC 設定の流れ

設定の流れ

1. ワイヤレスネットワーク接続先の登録
2. ユーザ証明書のインポート

## 4-2 ワイヤレスネットワーク接続先の登録

ワイヤレスネットワーク接続先の登録を行います。




**【ネットワーク名(SSID)】**

**・FTNT_JP**

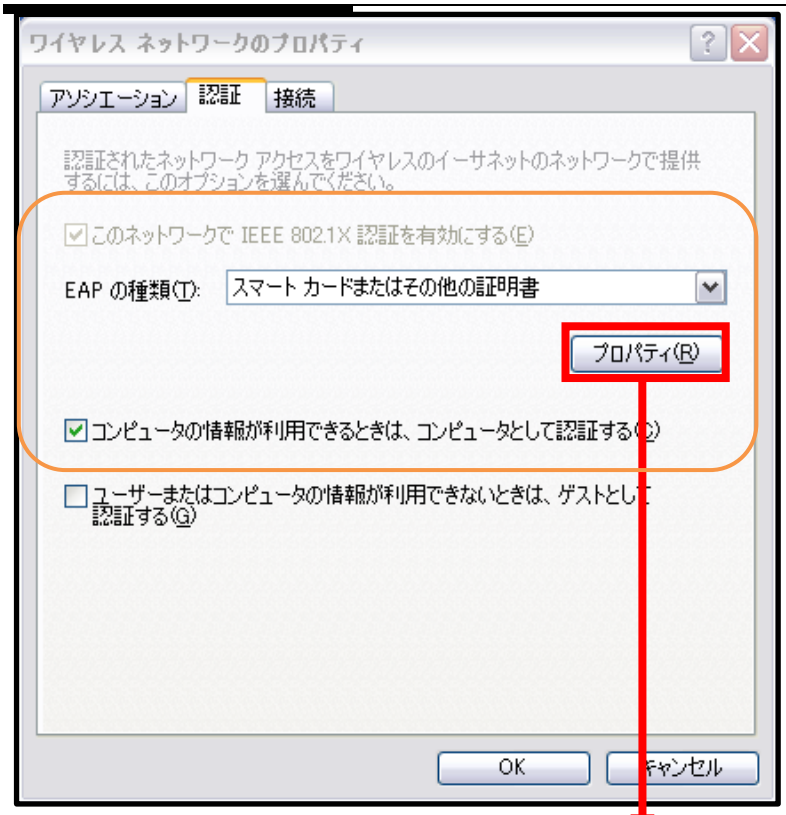
**【ネットワーク認証】**

**・FINT_JP**

**【データの暗号化】**

**・TKIP**

**次ページへ**

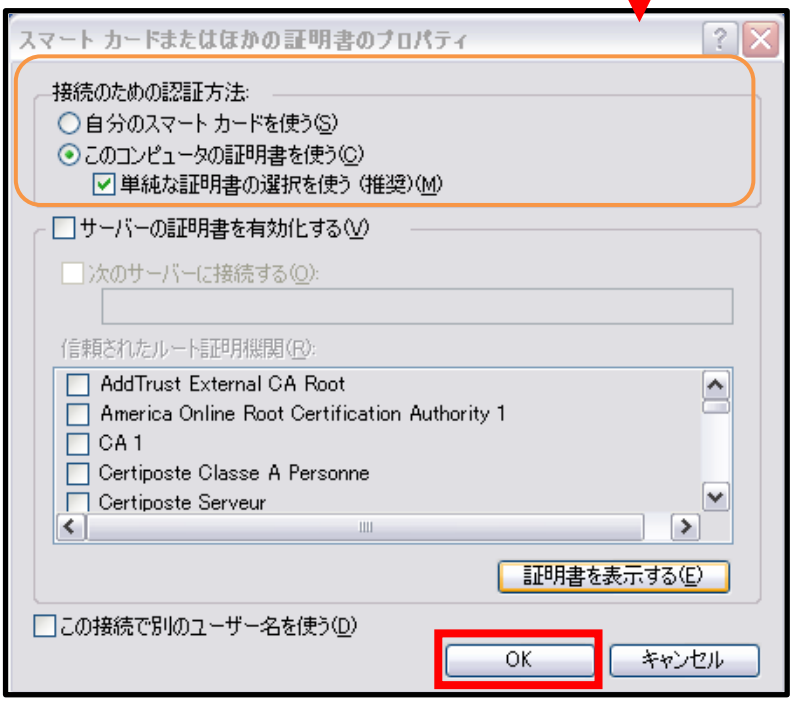



【EAP の種類】

・スマートカードまたはその他の証明書設定

【コンピュータの情報が利用できる・・・】

・チェック有




【接続のための認証方法】

・このコンピュータの証明書を使う

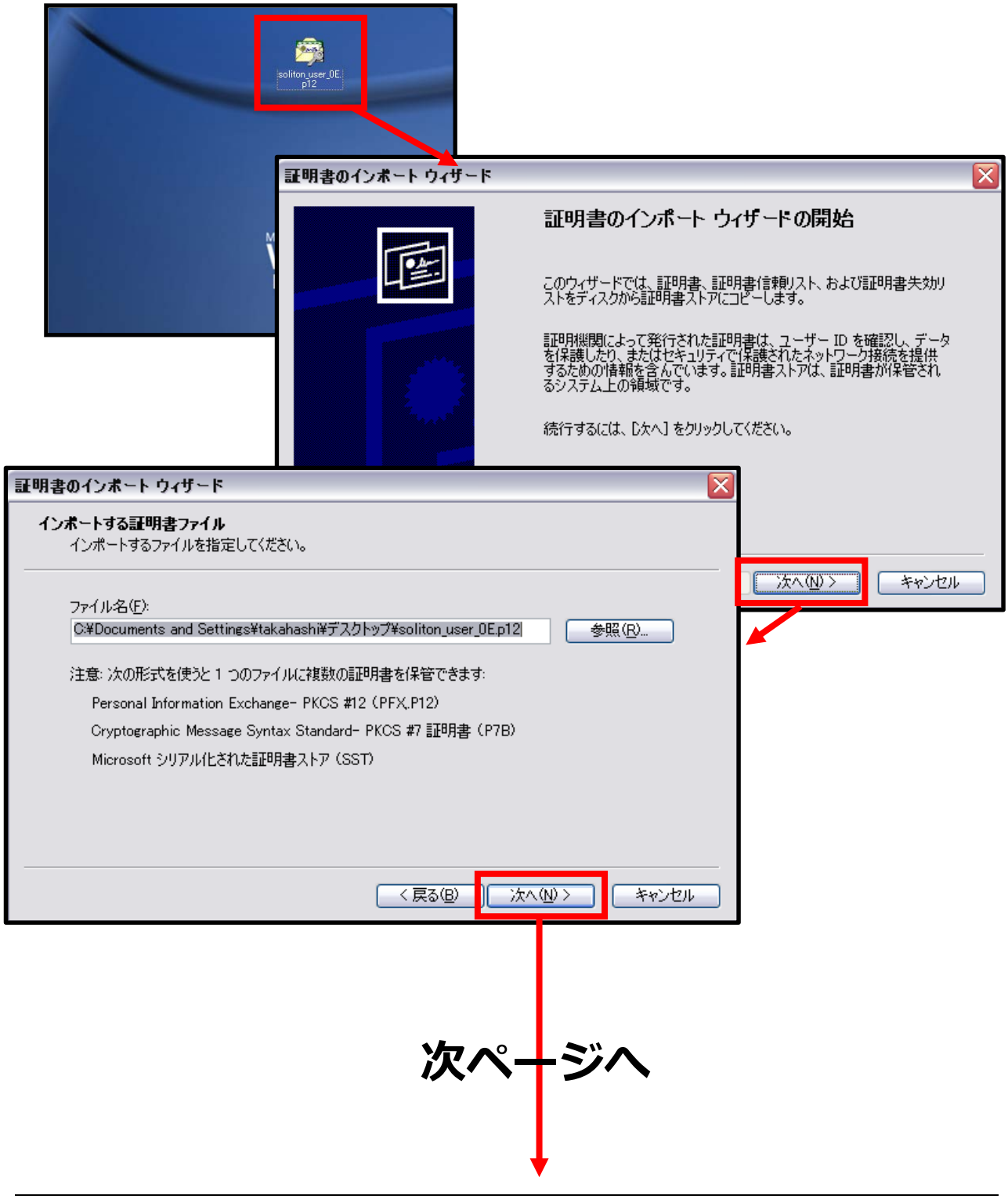
【単純な証明書の選択を使う】

・チェック有

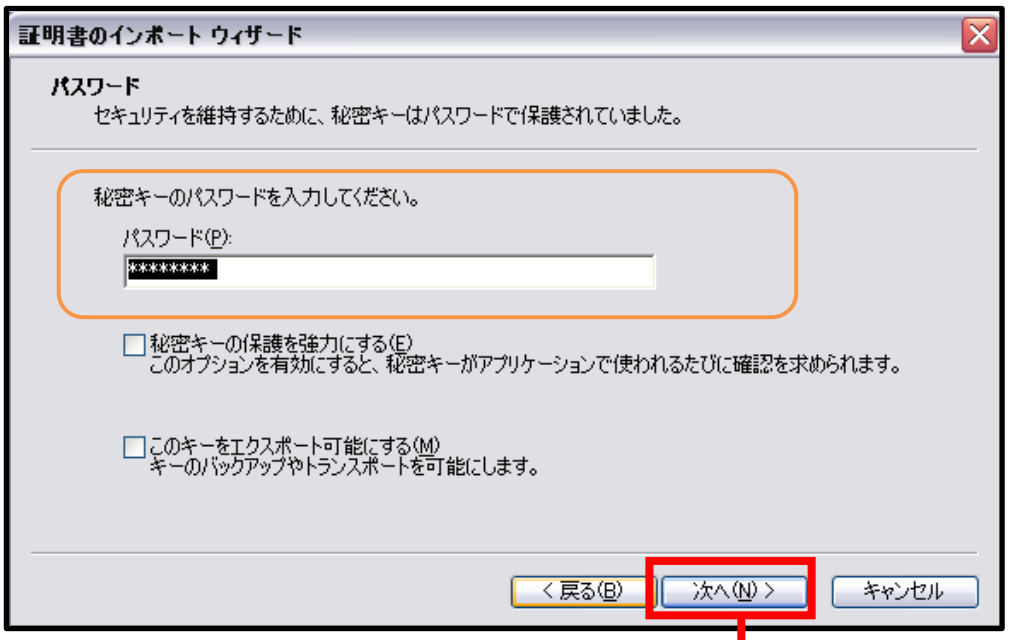
# 4-3 ユーザー証明書のインポート

Net'Attest EPS からダウンロードしたユーザー証明書をインポートします。

本書では、デスクトップ上に保存されている「soliton_user_0E.p12」アイコンをダブルクリックします。



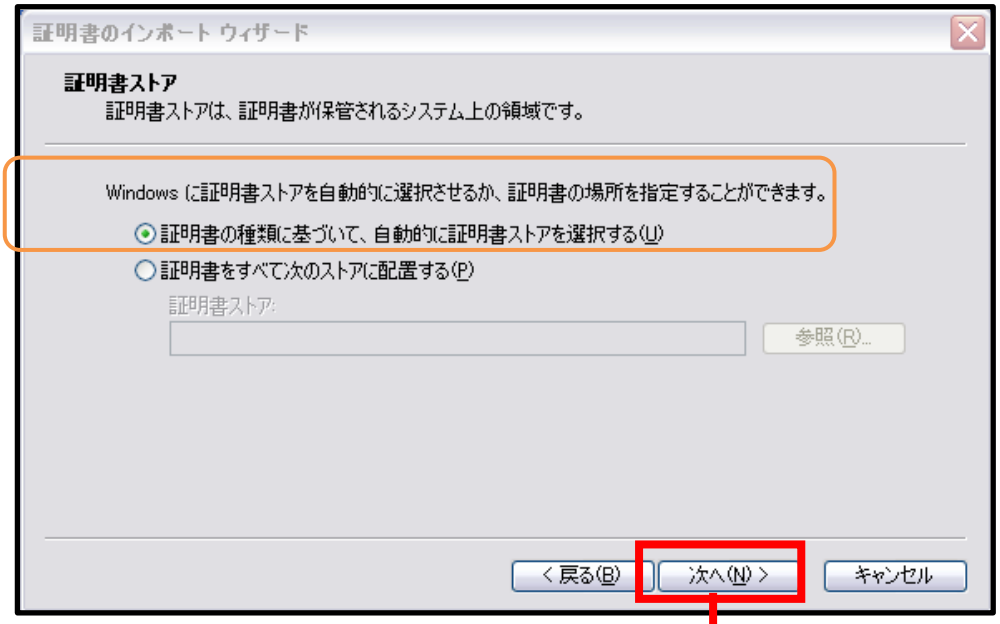

次ページへ




**Net'Attest EPS にてユーザー証明書を発行した際に設定したパスワードを入力します。**

**【パスワード】**

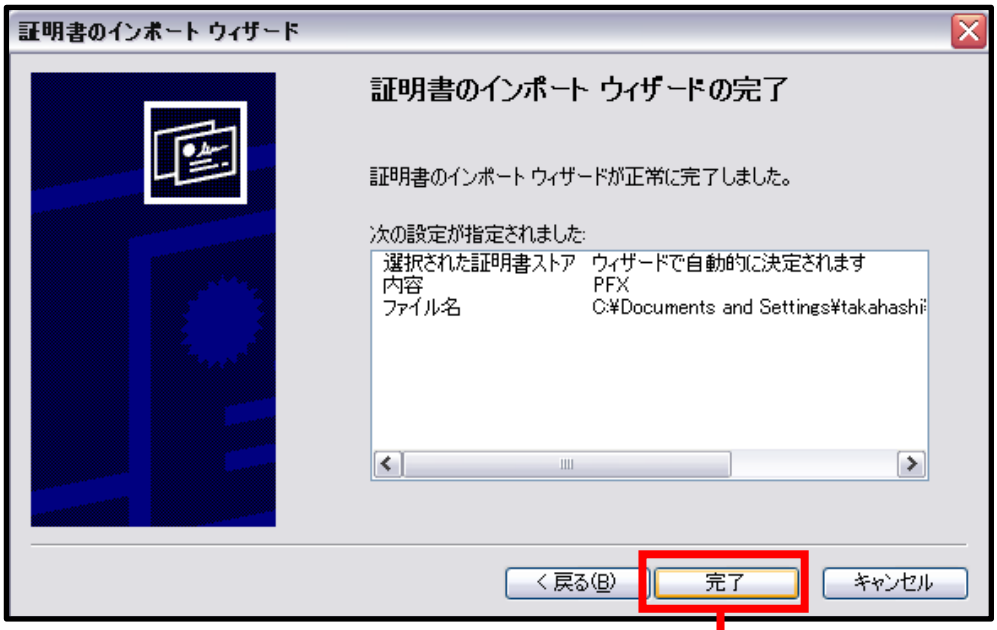
**・password**

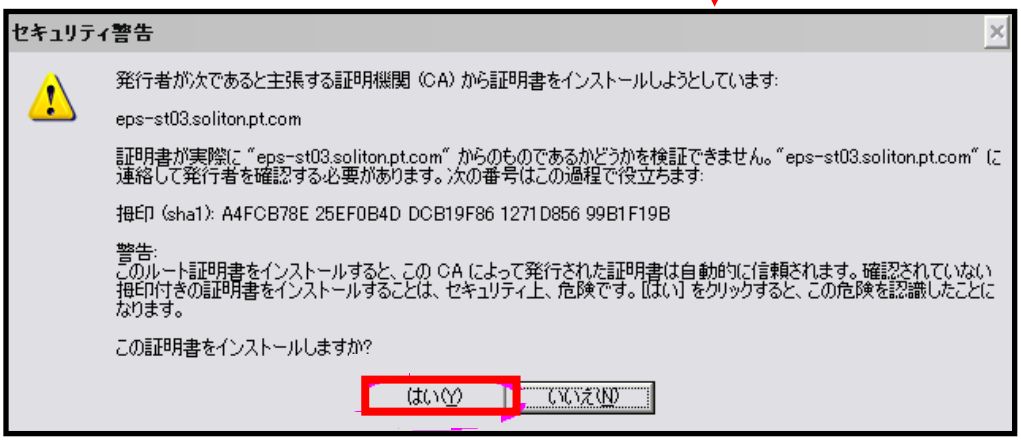



**【証明書の種類に基づいて・・・】**

**・チェック有**

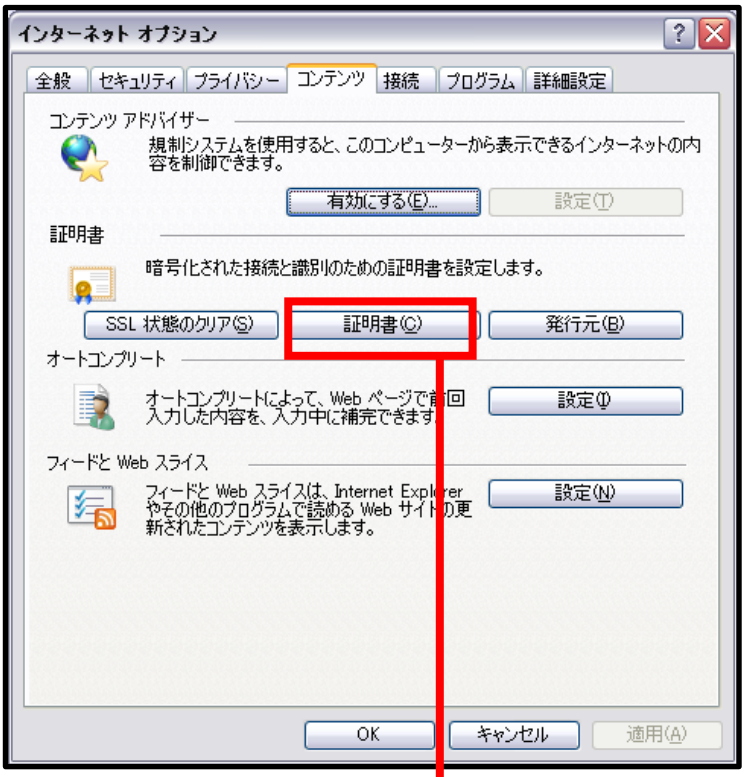
**次ページへ**

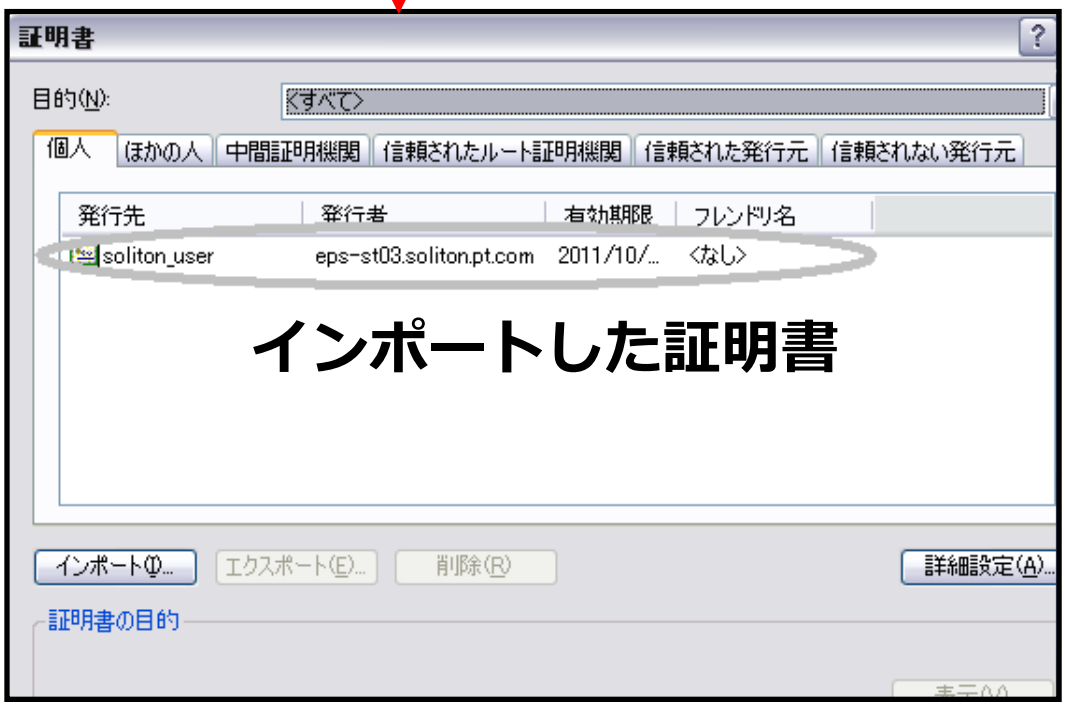

証明書のインポート ウィザード
証明書のインポート ウィザードの完了
証明書のインポート ウィザードが正常に完了しました。
次の設定が指定されました:
選択された証明書ストア ウィザードで自動的に決定されます
内容 PFX
ファイル名 C:¥Documents and Settings¥takahashi
< 戻る(B)
完了
キャンセル


セキュリティ警告
発行者が次であると主張する証明機関 (CA) から証明書をインストールしようとしています:
eps-st03.soliton.pt.com
証明書が実際に "eps-st03.soliton.pt.com" からのものであるかどうかを検証できません。"eps-st03.soliton.pt.com" に連絡して発行者を確認する必要があります。次の番号はこの過程で役立ちます:
拇印 (sha1): A4FCB78E 25EF0B4D DCB19F86 1271D856 99B1F19B
警告:
このルート証明書をインストールすると、この CA によって発行された証明書は自動的に信頼されます。確認されていない拇印付きの証明書をインストールすることは、セキュリティ上、危険です。[はい] をクリックすると、この危険を認識したことになります。
この証明書をインストールしますか?
はい(Y)
いいえ(N)

## 4-4 インポートされたユーザー証明書の確認

Internet Explorer より、「ツール」→「インターネットオプション」→「コンテンツ」タブを開きます。



# 5 各機器　認証/接続ステイタス

## 5-1 Net'Attest EPS　認証ステイタス

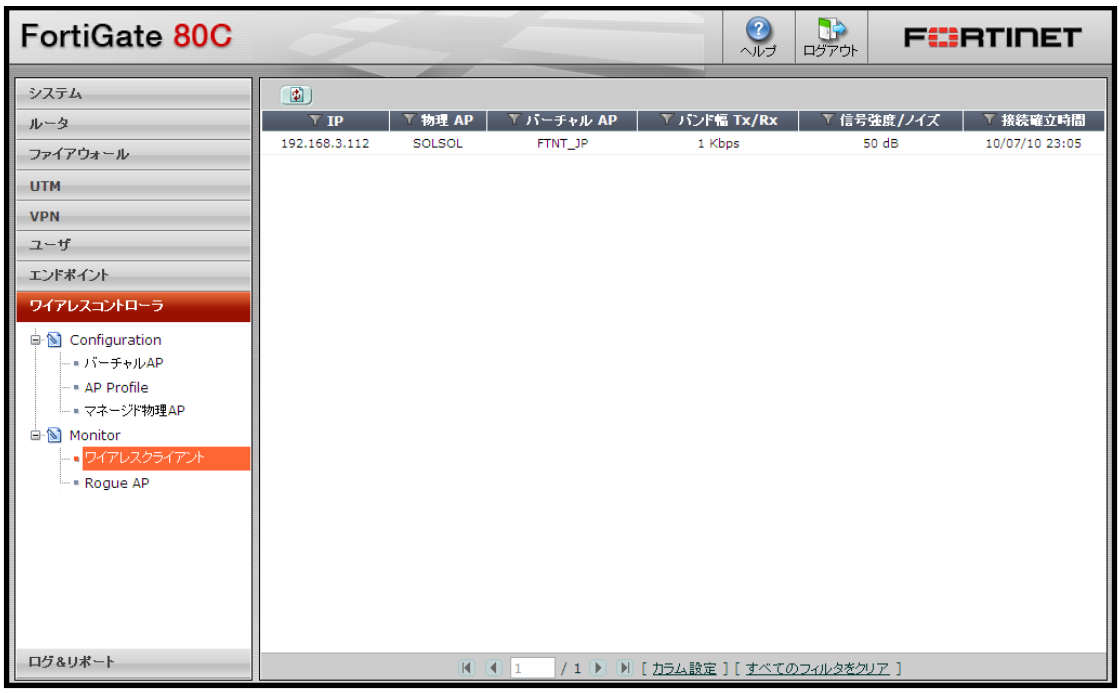
「RADIUS サーバ」→「RADIUS サーバ管理」→「認証ログ」→「表示」を選択します。

下記のように、認証に成功したログを確認することができます。

## 5-2 FortiGate/FortiAP　接続成功時ステイタス

「ワイアレスコントローラ」→「MONITOR」→「ワイアレスクライアント」を選択します。

下記のように、接続に成功したクライアントの IP アドレスなどを確認することができます。




以上

# 改訂履歴

| 日付 | 版 | 改訂内容 |
|---|---|---|
| 2010/12/3 | 1.0 | 本書作成 |
| 2012/9/10 | 1.1 | RADIUS Port を TCP から UDP に修正 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |