NetAttest EPS 設定例

連携機器：

アライドテレシス AT-TQ2403

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 CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS とアライドテレシス社製 無線アクセスポイント AT-TQ2403 の 802.1X 環境での接続について、設定例を示したものです。

各機器の管理 IP アドレス設定など、基本設定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を前提として記述します。

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

このマニュアル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、NetAttest EPS 及び AT-TQ2403 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 6

1-1 構成図 6

1-2 環境 7

2 NetAttest EPS 8

2-1 NetAttest EPS 設定の流れ 8

2-2 システム初期設定ウィザードの実行 9

2-3 サービス初期設定ウィザードの実行 10

2-4 Authenticator(RADIUS Client)の登録 11

2-5 RADIUS サーバ基本設定 12

2-6 ユーザーの登録 13

2-7 ユーザー証明書の発行 14

3 アライドテレシス AT-TQ2403 15

3-1 アライドテレシス AT-TQ2403 設定の流れ 15

3-2 管理アクセス用パスワード設定および SSID 設定 16

3-3 セキュリティ設定の変更 17

4 クライアント PC の設定 18

4-1 クライアント PC 設定の流れ 18

4-2 ワイヤレスネットワーク接続先の登録 19

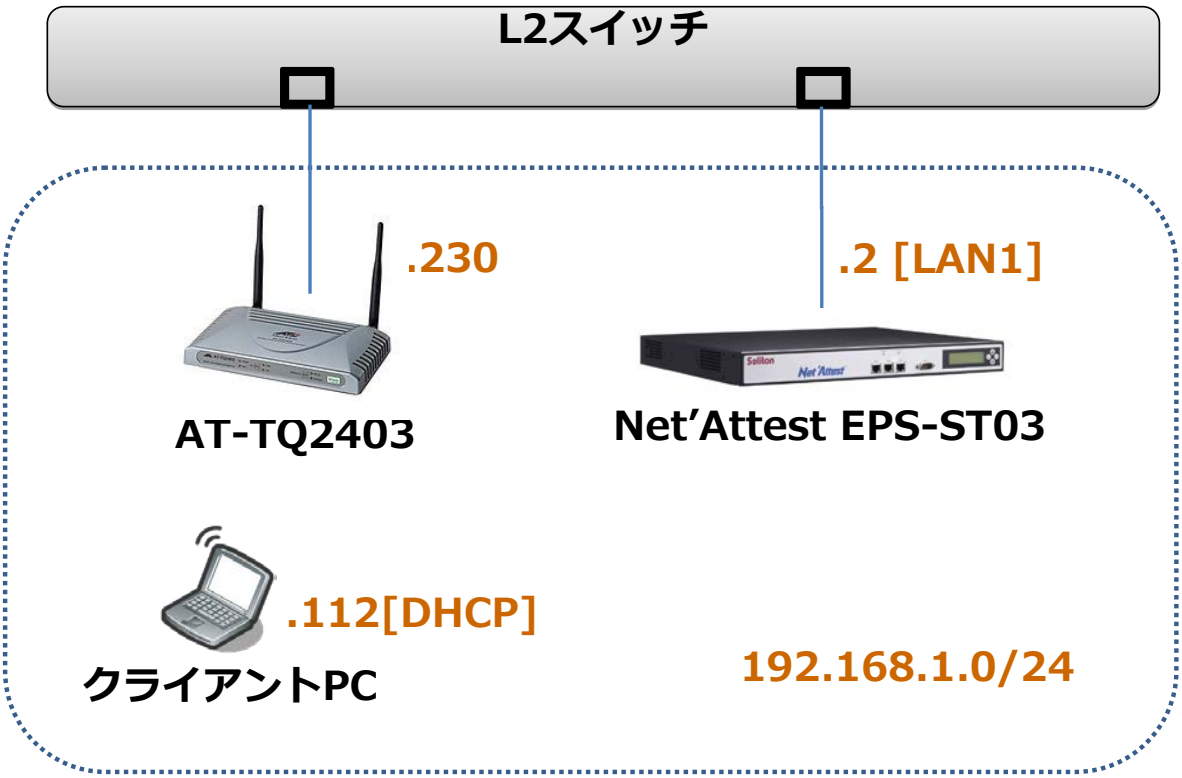
4-3 ユーザー証明書のインポート 21

4-4 インポートされたユーザー証明書の確認 24

1 構成

1-1　　構成図

・有線LANで接続する機器はL2スイッチに収容
・有線LANと無線LANは同一セグメント
・無線LANで接続するクライアントPCのIPアドレスは、
Net'Attest EPS-ST03のDHCPサーバから払い出す



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 (認証サーバ)	Soliton Systems	NetAttest EPS ST-03	Ver. 4.2.1
Authenticator (認証機器)	アライドテレシス	AT-TQ2403	Ver. 3.0.2
Client PC / Supplicant (802.1x クライアント)	Panasonic Microsoft	Let's note CF-W7	Windows XP SP3 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	AT-TQ2403	Client PC
IP アドレス	192.168.1.2/24	192.168.1.230/24	192.168.1.112 (DHCP)
RADIUS port (Authentication)	UDP 1812		
RADIUS port (Accounting)	UDP 1813		
RADIUS Secret (Key)	password		

2 NetAttest EPS

2-1　NetAttest EPS 設定の流れ

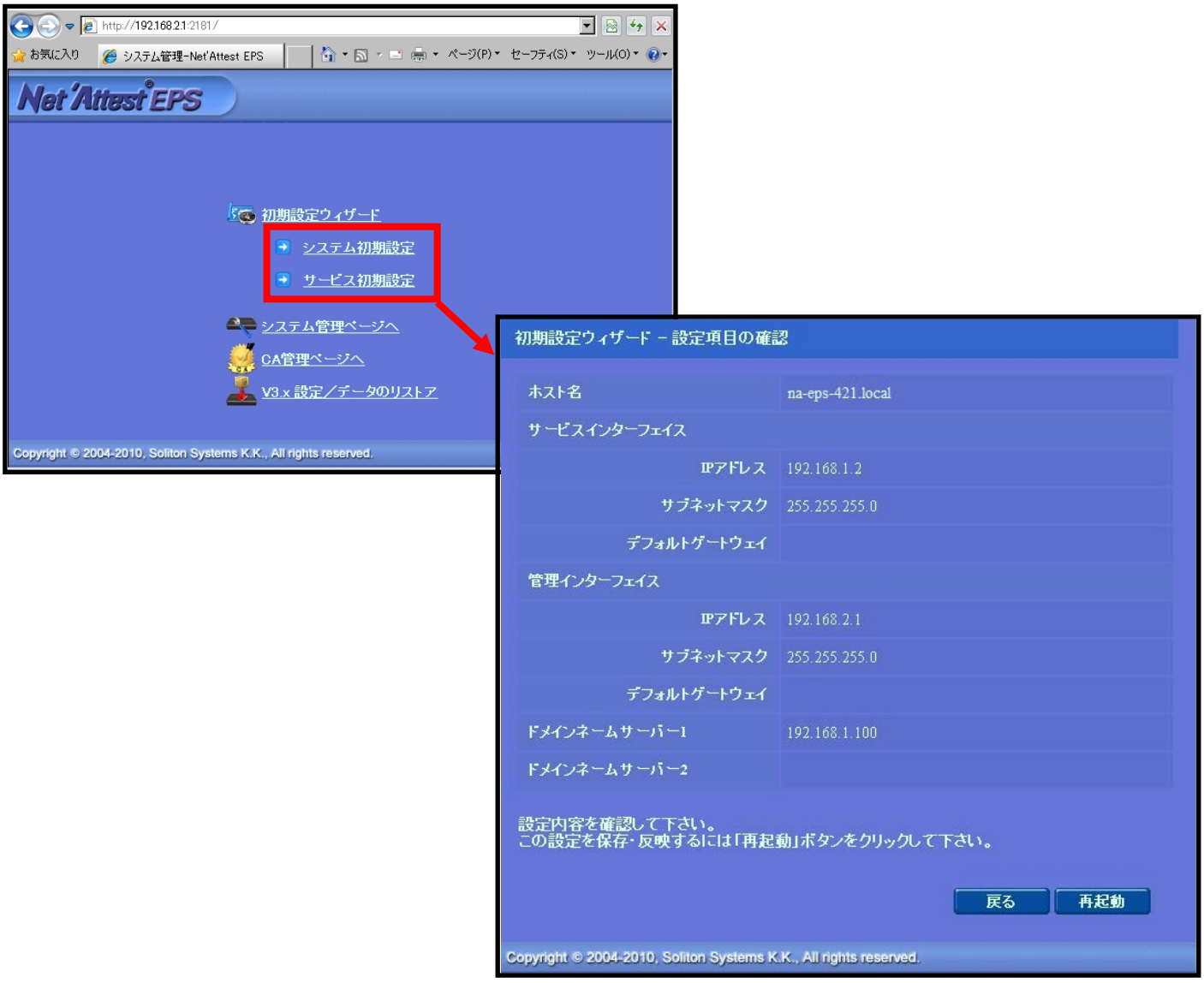
設定の流れ

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。

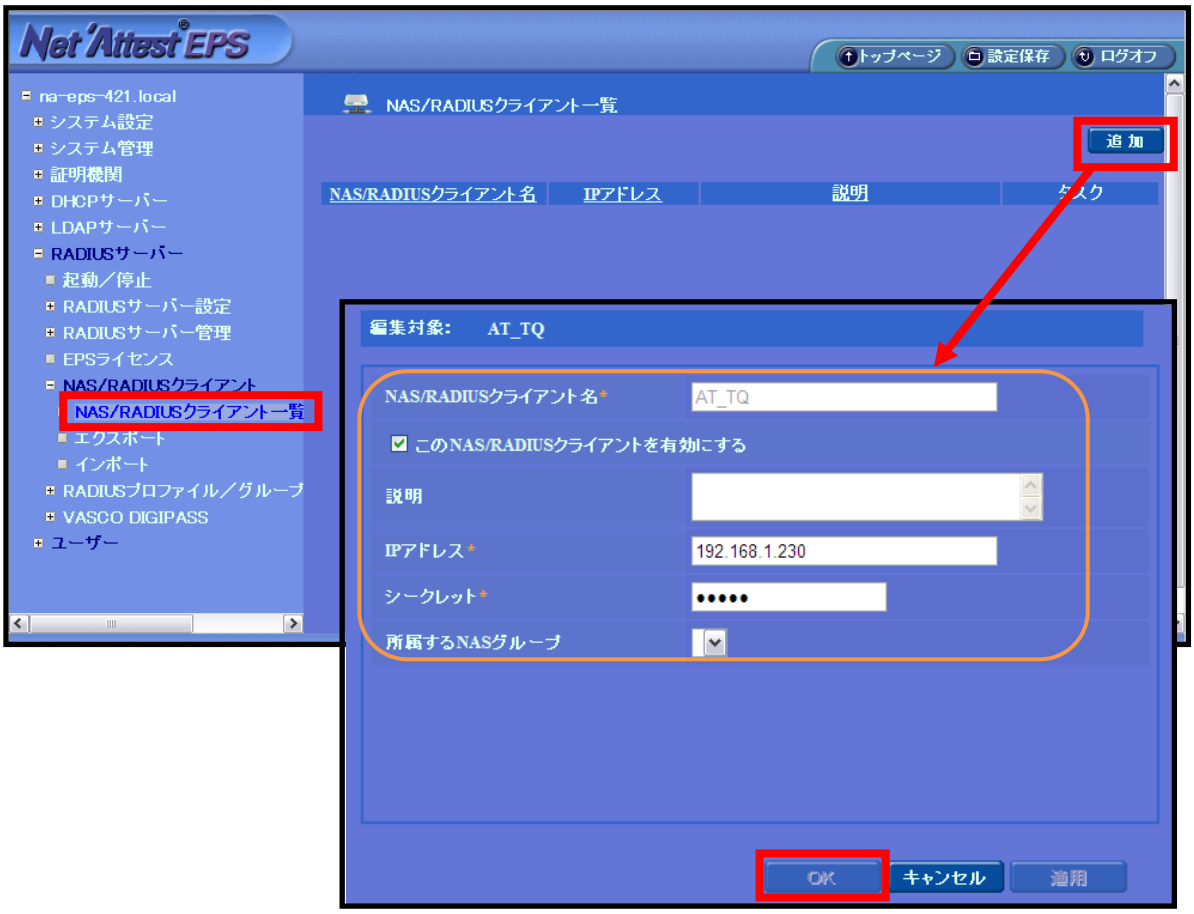
本書では、黒文字の項目のみ、設定しました。

- 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】

・AT_TQ

【IP アドレス(Authenticator)】

・192.168.1.230

【シークレット】

・password

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】

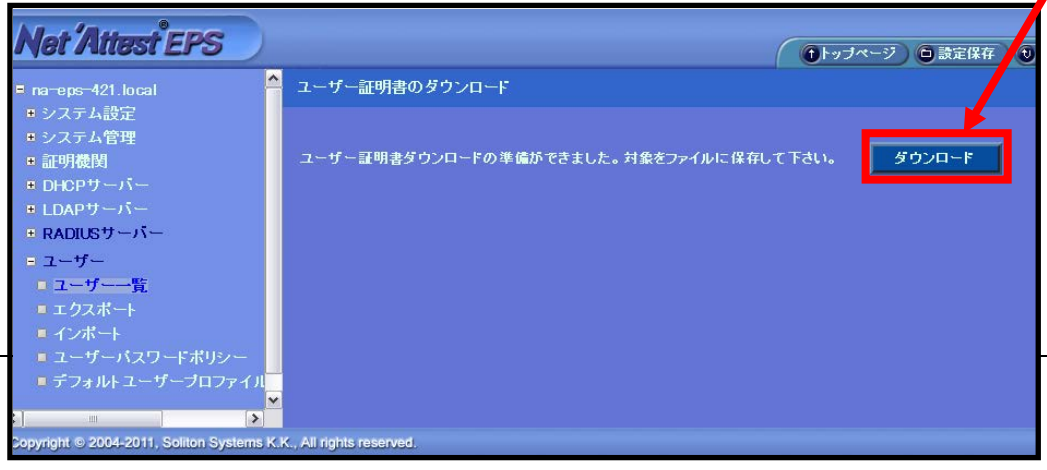
・365

【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 アライドテレシス AT-TQ2403

3-1　アライドテレシス AT-TQ2403 設定の流れ

本書では、Web GUI を利用して AT-TQ2403 の各種設定を実施する方法を紹介します。

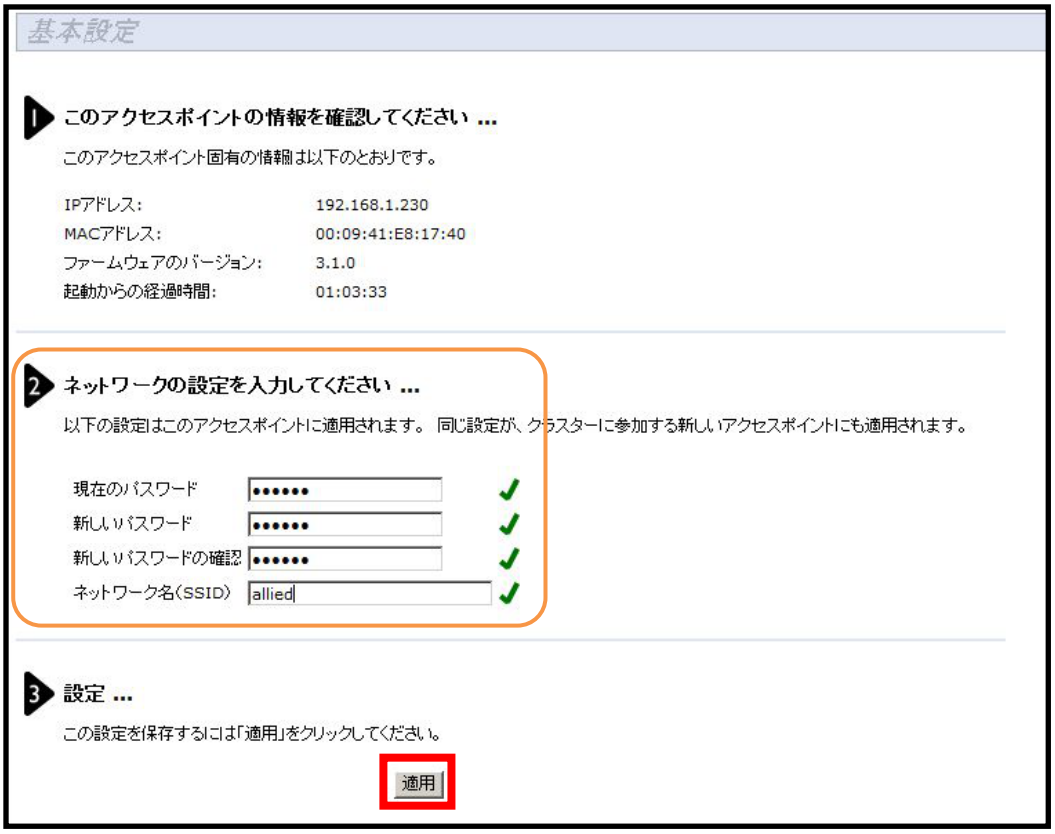
設定の流れ

1. 管理アクセス用パスワード設定および SSID 設定
2. 内部ネットワーク　セキュリティー設定

3-2　管理アクセス用パスワード設定および SSID 設定

機器、初回ログイン時、管理アクセス用パスワードの設定と SSID の設定が求められます。適宜設定し、『適用』ボタンを押下します。

また、IP アドレスはデフォルト設定で 192.168.1.230 になっていますが、今回は初期設定を流用します。



【現在のパスワード】

・friend（※初期パスワード）

【新しいパスワード】、【新しいパスワードの確認】

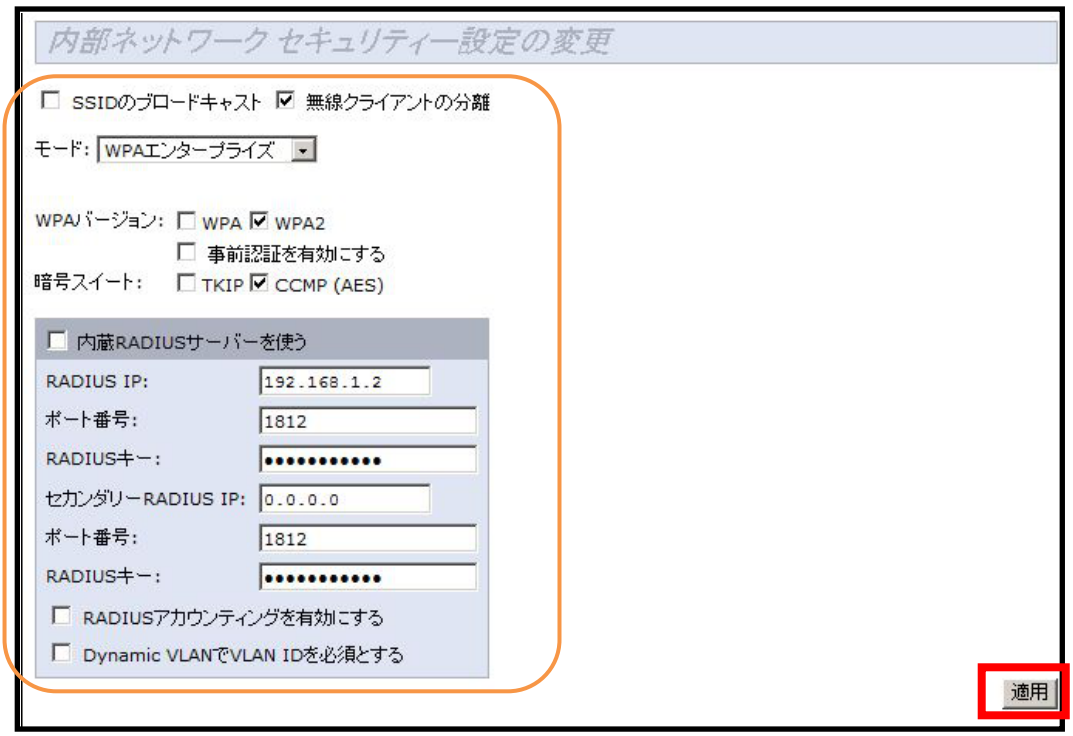
・適宜

【ネットワーク名（SSID）】

・allied

3-3　セキュリティー設定の変更

設定メニューの「セキュリティー」から RADIUS 関連、無線認証関連の設定を行います。



【SSID のブロードキャスト】

・チェックなし

【無線クライアントの分離】

・チェックあり

【モード】

・WPA エンタープライズ

【WPA バージョン】

・WPA2 のみチェックあり

【暗号スイート】

・CCMP(AES)　チェックあり

【内蔵 RADIUS サーバーを使う】

・チェックなし

【RADIUS IP】

・192.168.1.2

【ポート番号】

・1812

【RQADIUS キー】

・password

4 クライアント PC の設定

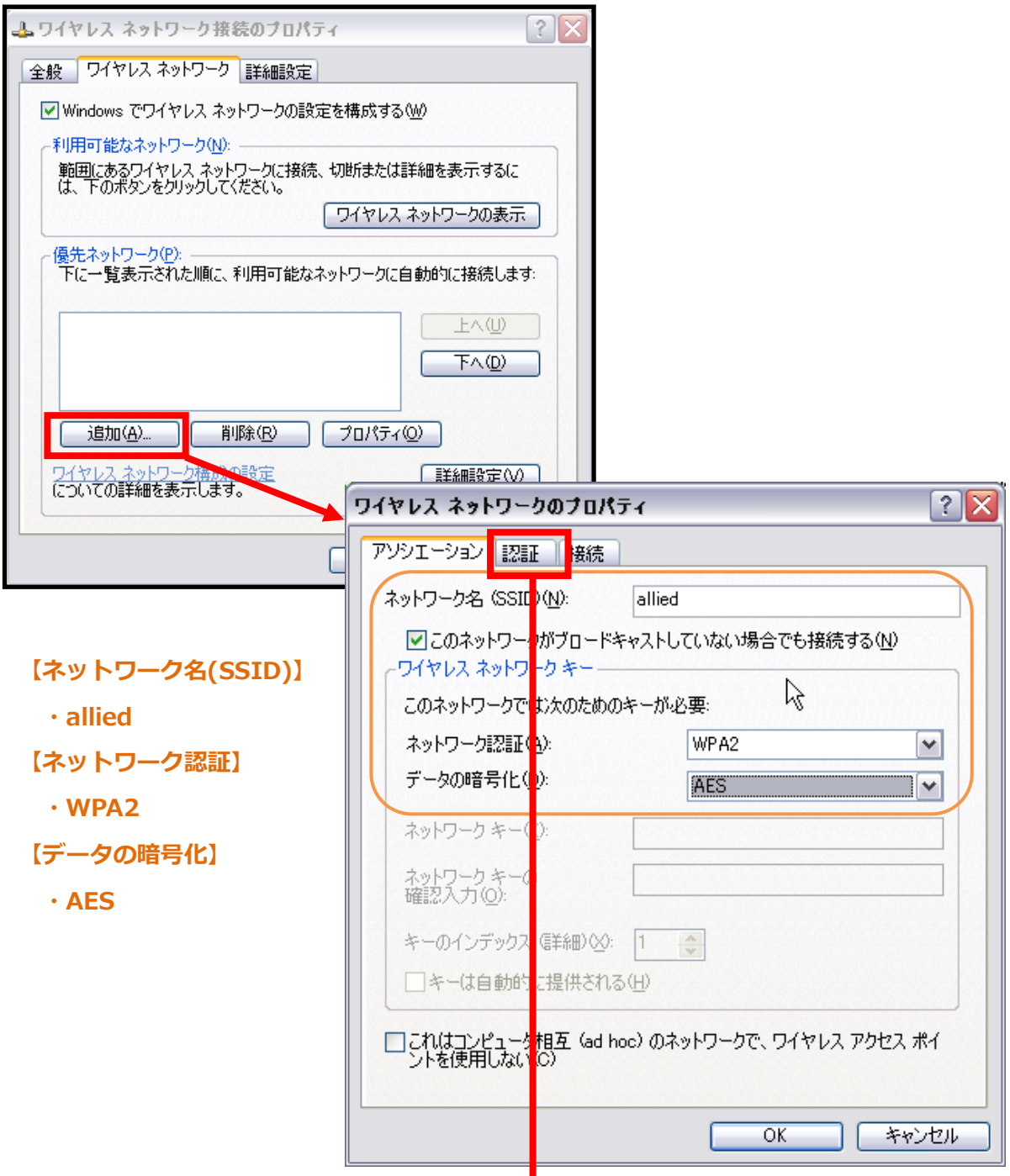
4-1　クライアント PC 設定の流れ

設定の流れ

1. ワイヤレスネットワーク接続先の登録
2. ユーザー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)】

・allied

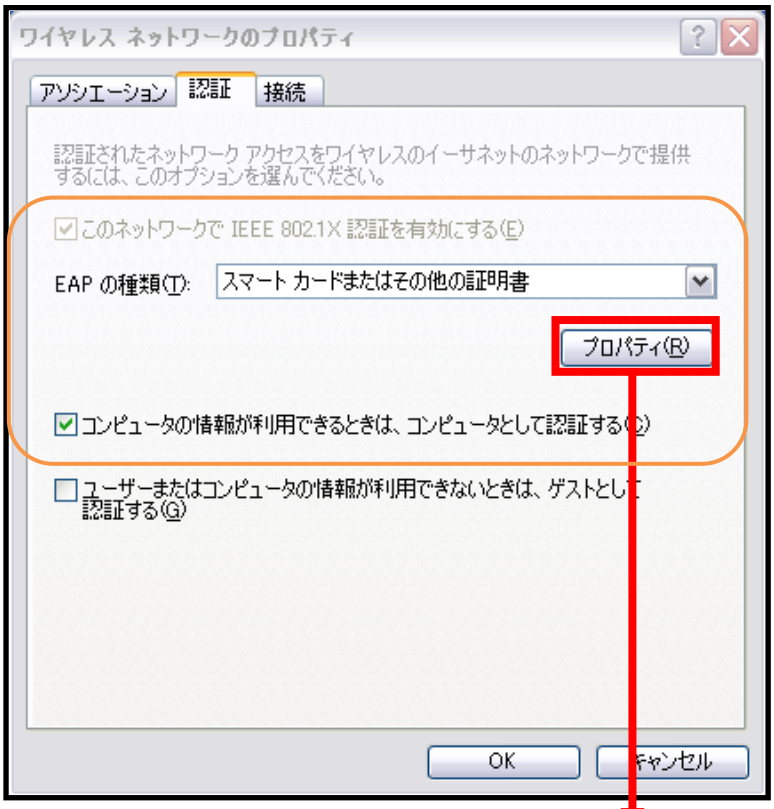
【ネットワーク認証】

・WPA2

【データの暗号化】

・AES

次ページへ

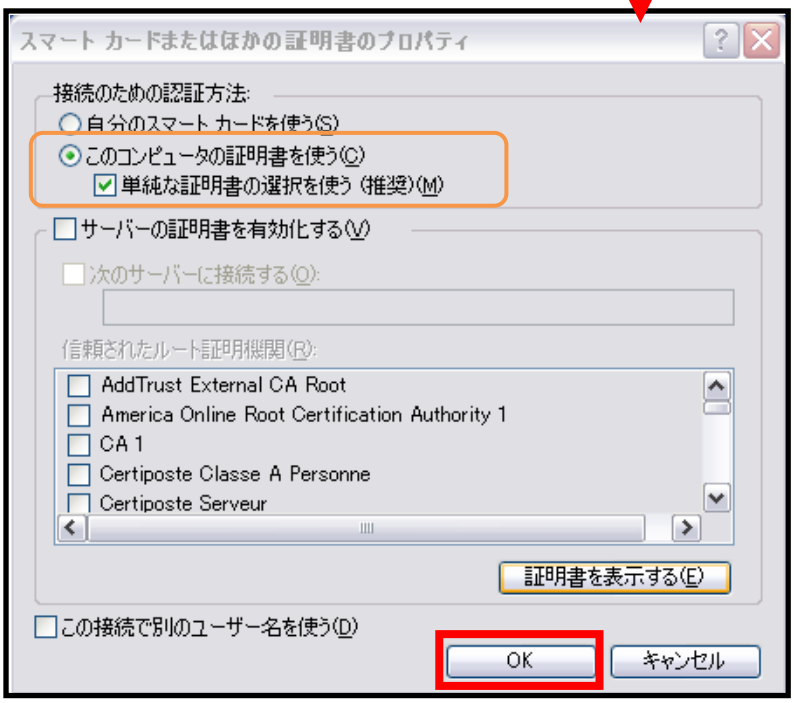


【EAP の種類】

・スマートカードまたはその他の証明書

【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】

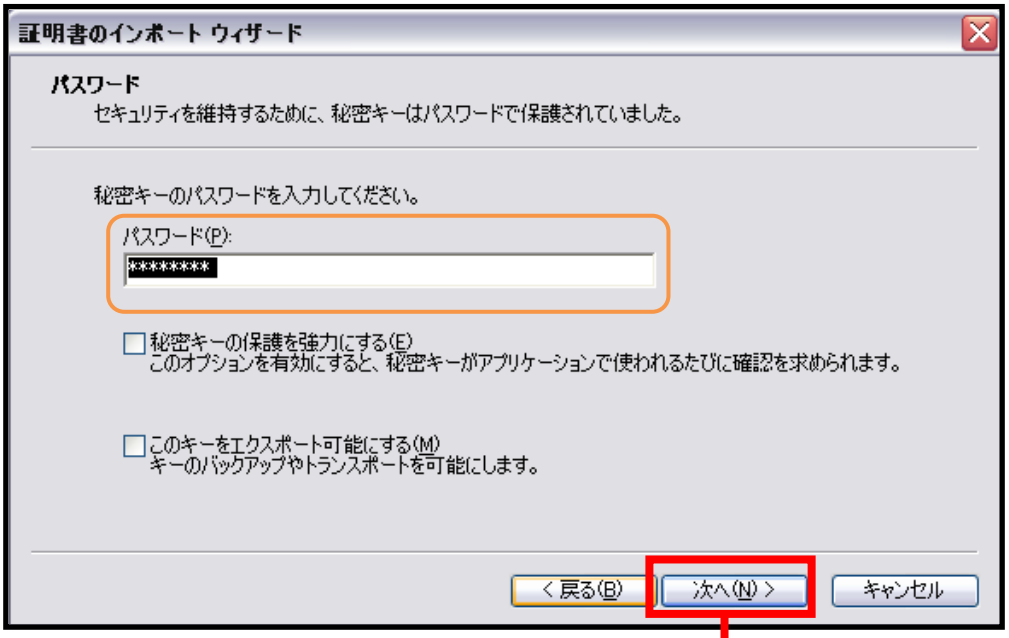
・チェック有

4-3　ユーザー証明書のインポート

NetAttest 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。

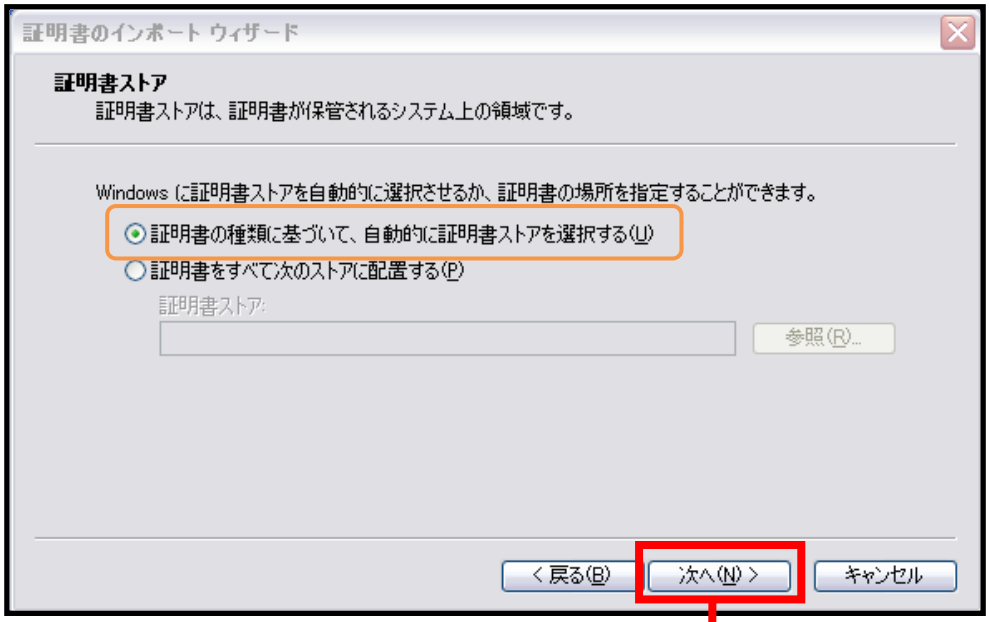
次ページへ



NetAttest 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】

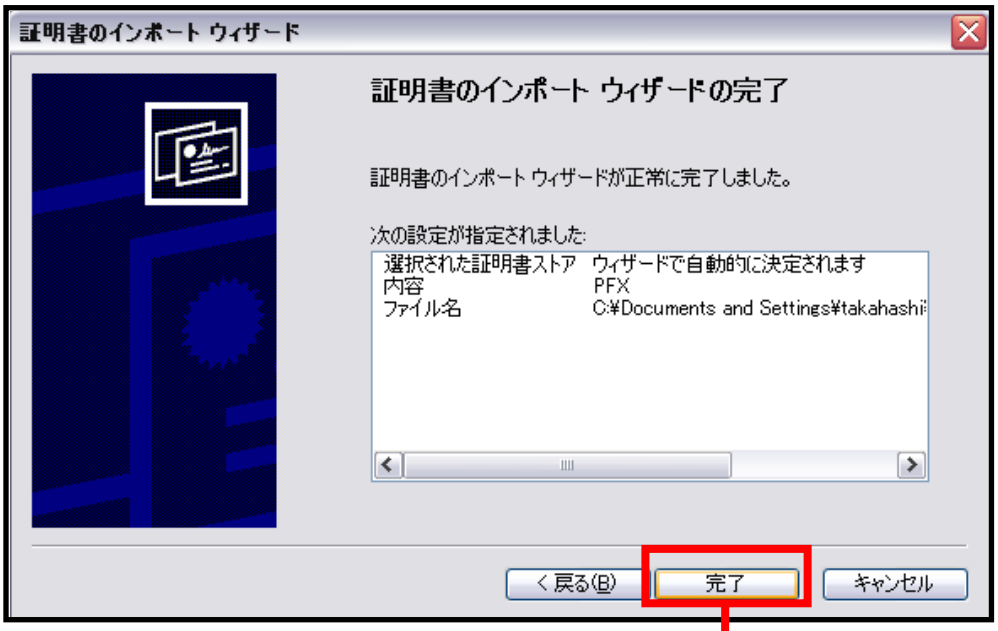
・password

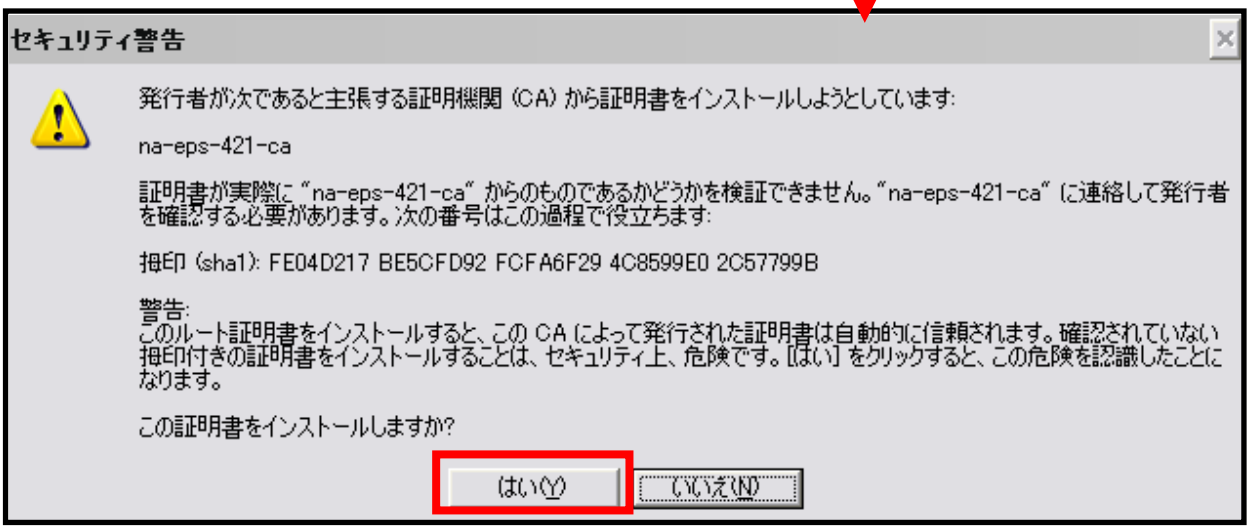


【証明書の種類に基づいて・・・】

・チェック有

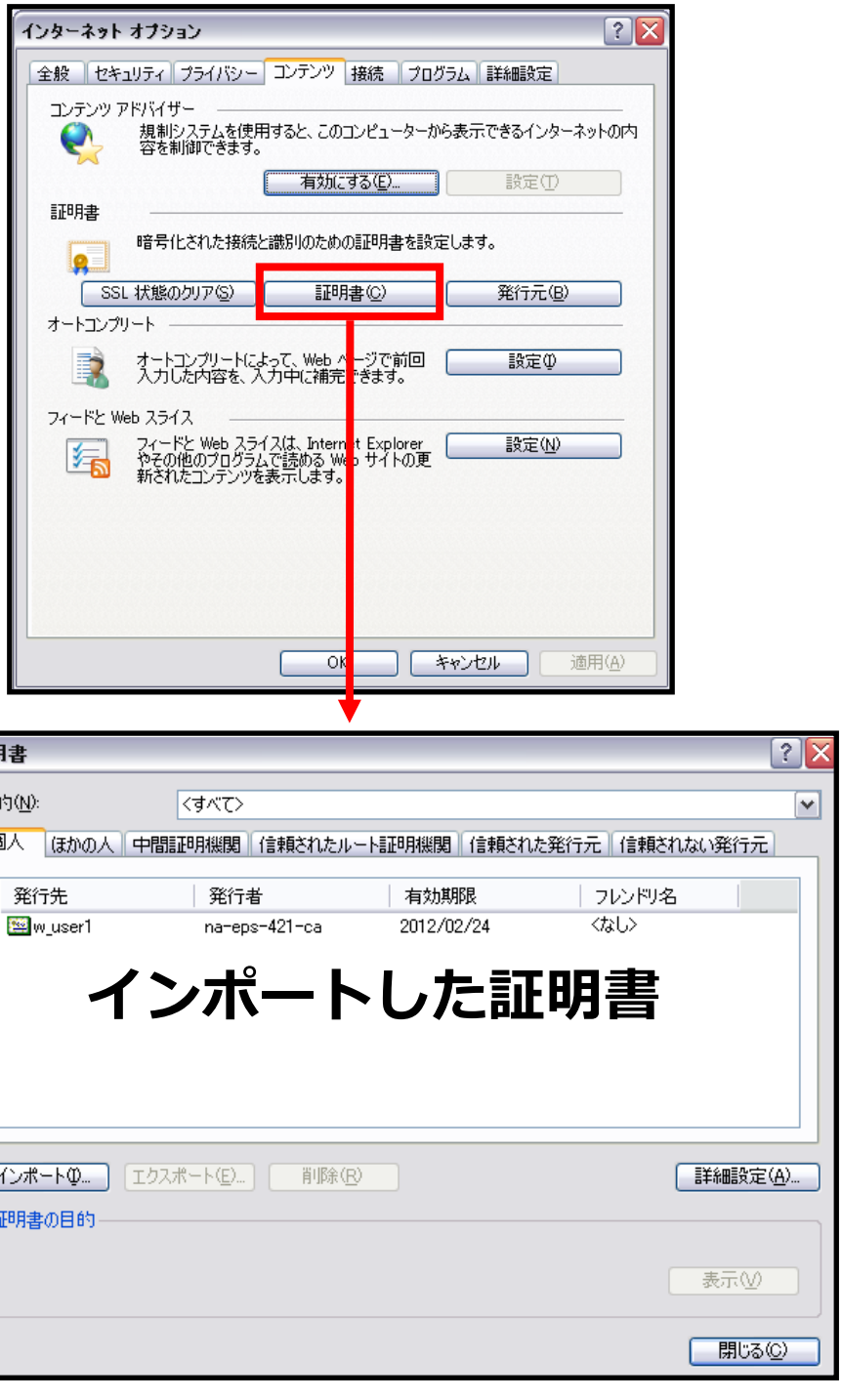
次ページへ


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:
na-eps-421-ca
証明書が実際に "na-eps-421-ca" からのものであるかどうかを検証できません。"na-eps-421-ca" 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): FE04D217 BE5CFD92 FCFA6F29 4C8599E0 2C57799B
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。



改訂履歴

日付	版	改訂内容
2012/3/29	1.0	初版作成
2012/9/10	1.1	RADIUS Port を TCP から UDP に修正