NetAttest EPS 設定例

連携機器：

ACERA800ST

Case：TLS 方式での認証

Version 1.0

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 サーバープライアンス NetAttest EPS と FURUNOSYSTEMS 社製 無線アクセスポイント ACERA800ST 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)	ユーザーが入力する文字を、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
%, $, >	一般ユーザーのプロンプトを表します。
#	特権ユーザー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 ACERA800ST 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

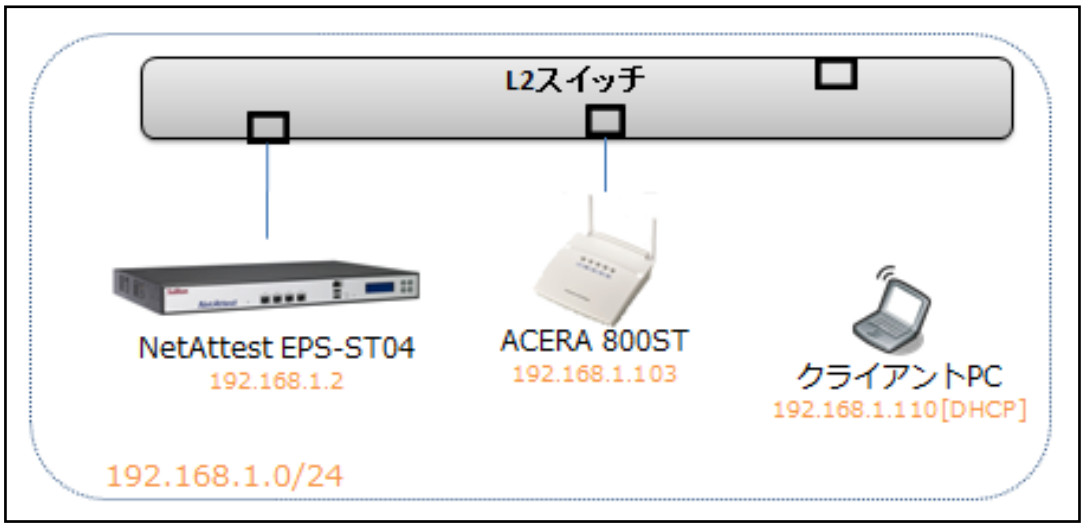
1 構成

1−1　　構成図

・有線 LAN 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、
NetAttest EPS-ST04 の DHCP サーバーから配付

・RADIUS の通信は、ACERA800ST と EPS 間で行われる



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 (認証サーバー)	Soliton Systems	NetAttest EPS ST-04	Ver. 4.4.1
無線 Access Point	FURUNOSYSTEMS	ACERA800ST	07.04
Client PC / Supplicant (802.1x クライアント)	HP Microsoft	ProBook 5220m	Windows 7 SP1 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-ST04	ACERA800ST	Client PC
IP アドレス	192.168.1.2/24	192.168.1.103/24	192.168.1.110 (DHCP)
RADIUS port (Authentication)	UDP 1812		
RADIUS port (Accounting)	UDP 1813		
RADIUS Secret (Key)	soliton		

2 NetAttest EPS

2-1 NetAttest EPS 設定の流れ

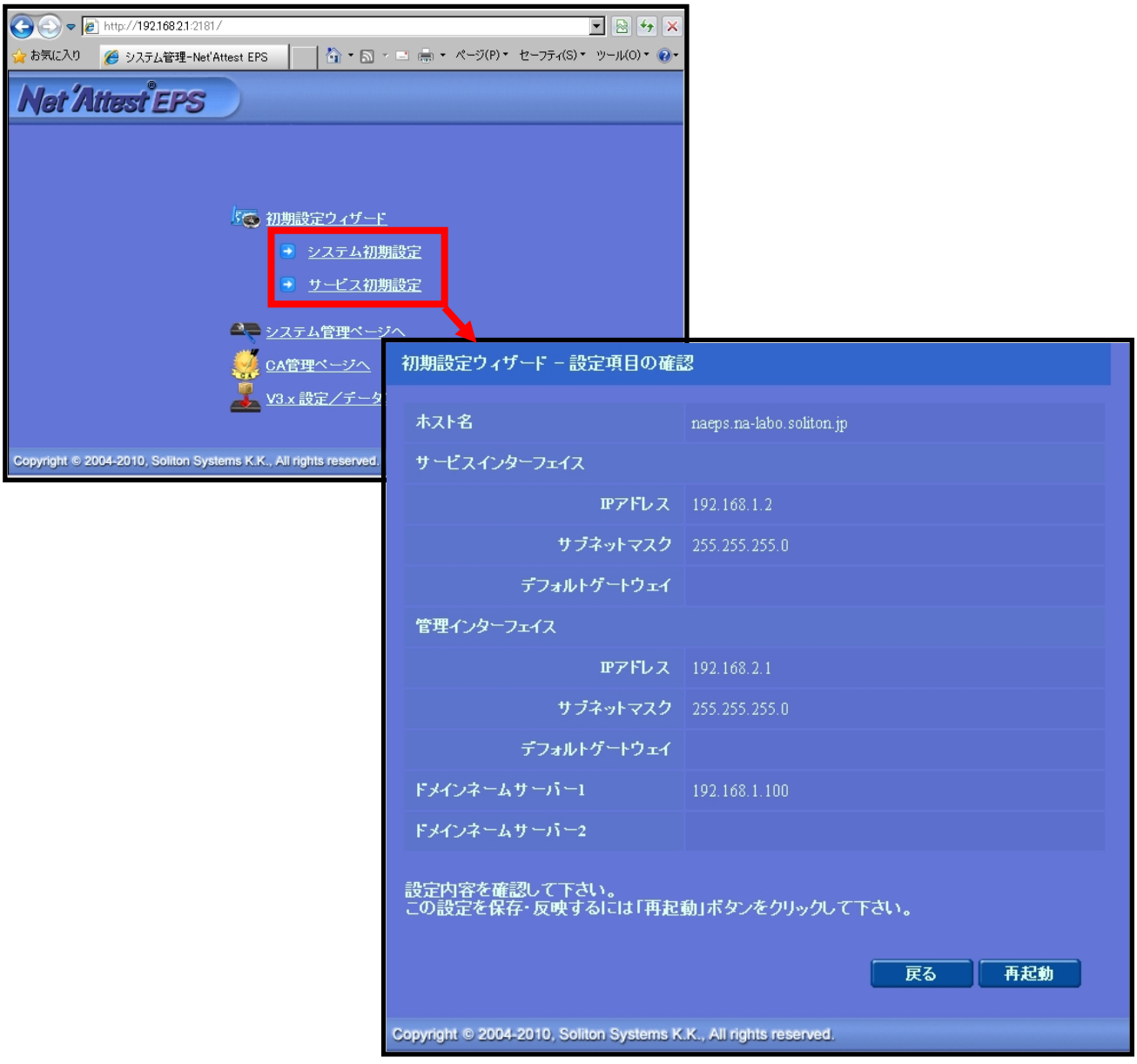
設定の流れ

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
- ◆ ドメインネームサーバーの設定

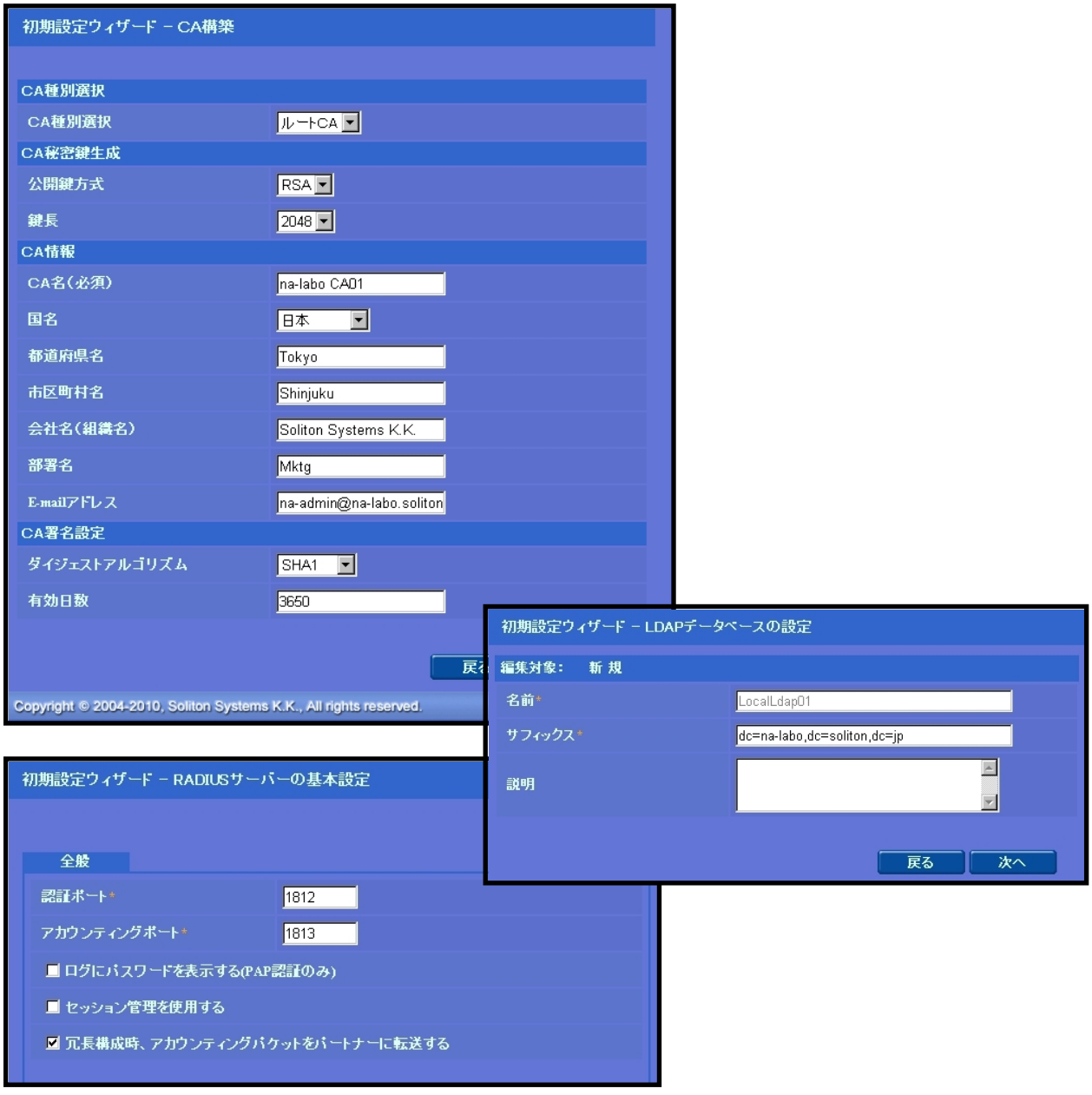


2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

本書では、下記項目を図のように設定しました。

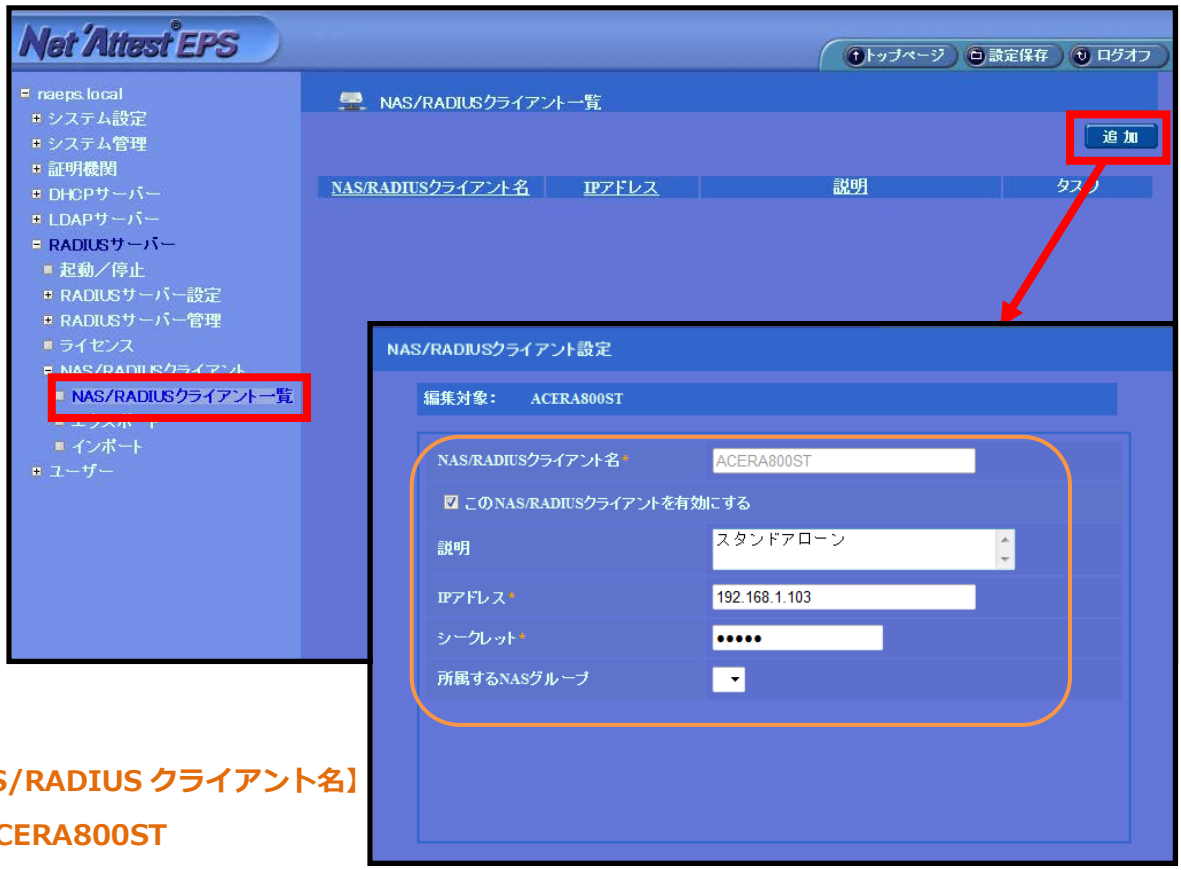
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）



2-4 Authenticator(RADIUS Client)の登録

WebGUI より、RADIUS Client の登録を行います。

「RADIUS サーバー設定」→「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】

・ACERA800ST

【IP アドレス(Authenticator)】

・192.168.1.103

【シークレット】

・soliton

2-5 RADIUS サーバー基本設定

WebGUI より、RADIUS サーバーの基本設定を行います。

「RADIUS サーバー」→「RADIUS サーバー設定」→「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

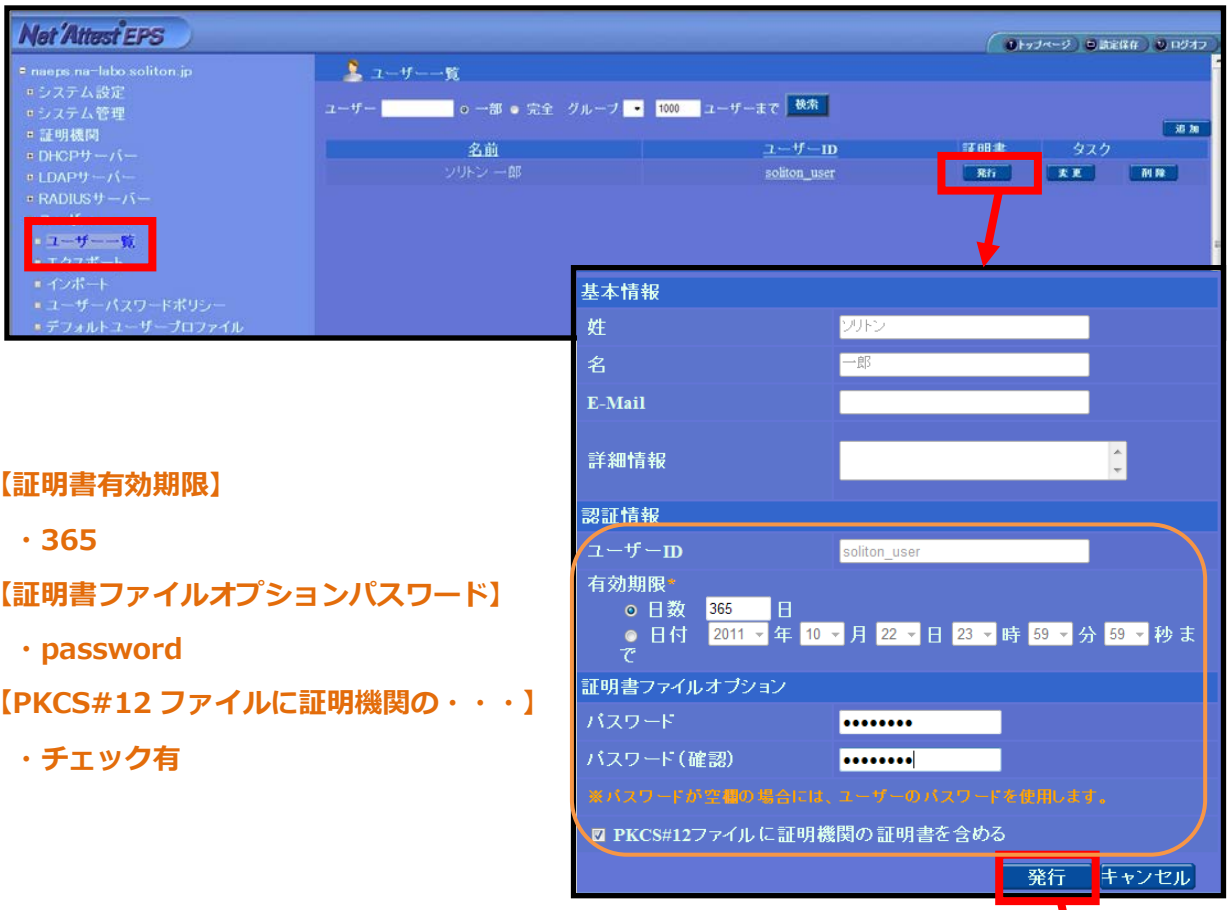
WebGUI より、ユーザー登録を行います。

「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。

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】

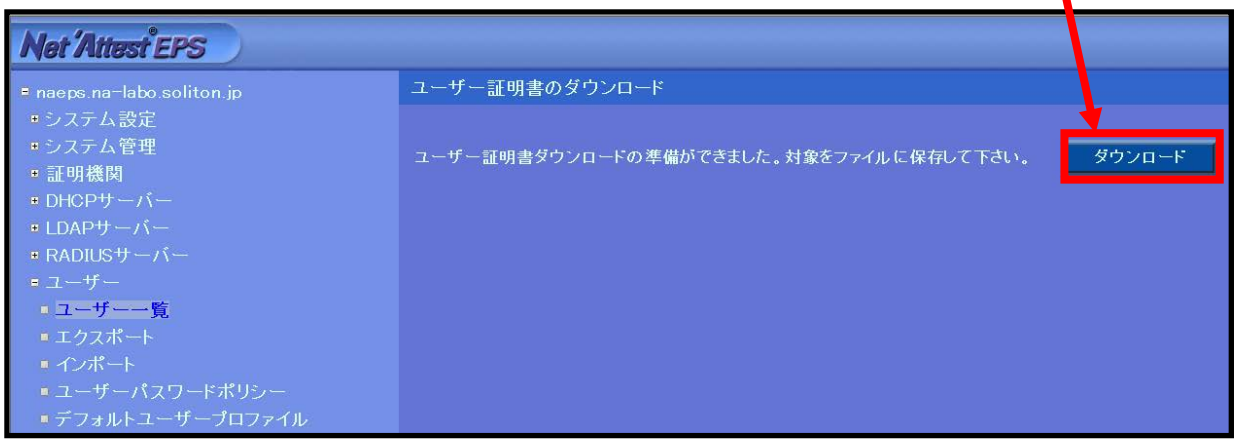
・365

【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 ACERA800ST

3-1 ACERA800ST 設定の流れ

設定の流れ

1. ACERA800ST の ESSID の設定
2. ACERA800ST の再起動

3-2 ACERA800ST の ESSID の設定

ACERA800ST に ESSID を設定します。

ACERA800ST では複数 ESSID を設定できますが、ESSID 毎にセキュリティを変更できますので、RADIUS サーバーを登録する場合も ESSID 毎に登録します。ここでは以下のパラメータを設定しています。

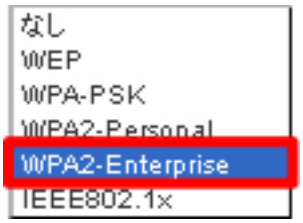
◆ESSID の有効/無効　　◆ESSID

◆ステルスモードの有効/無効　◆暗号方式

◆WPA 固有設定　　◆WPA、802.1x 共通設定（RADIUS サーバーの登録）

・暗号方式

暗号方式には以下の方式を選択頂けますが、RADIUS サーバーをご利用頂く場合は WPA2-Enterprise（暗号化が TKIP/AES の場合）もしくは IEEE802.1x（暗号化が WEP の場合）を選択ください。ここでは WAP2-Enterprise を選択しています。



・WPA 固有設定

WPA 固有設定では、WPA2-Enterprise で利用する暗号化方式を設定します。TKIP/AES から選択します。ここでは AES を選択しています。パスフレーズは自動的に配信されるため入力する必要はありません。必要に応じて事前認証なども選択頂けます。

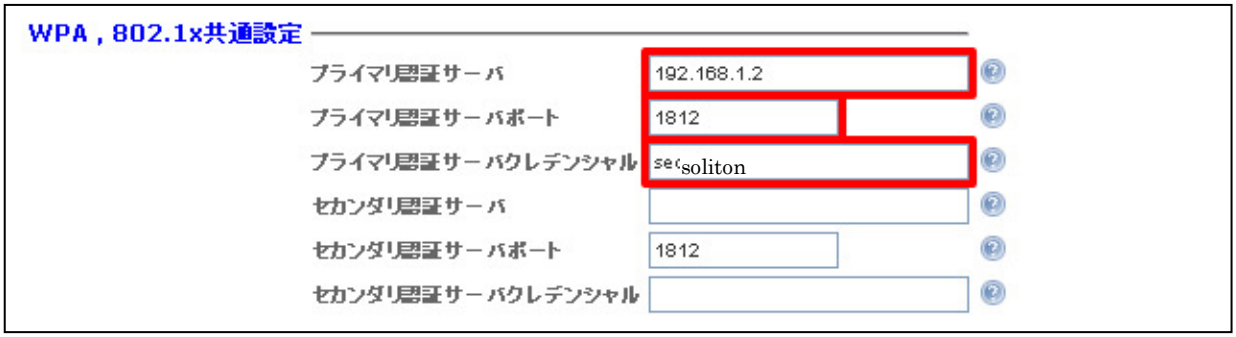
・WPA、802.1x 共通設定　（RADIUS サーバーの登録）

RADIUS サーバーは、プライマリ・セカンダリを登録頂けます。

【ホスト名】RADIUS サーバー NetAttest EPS を指定(FQDN もしくは IP アドレス)

【ポート番号】1812（RADIUS サーバーで利用するポート番号)

【クレデンシャル(Secret)】最大 16 桁となります。



3-3 ACERA800ST の再起動

変更した設定内容を保存し、変更を適用するために再起動を行います。

ACERA800ST の設定は以上となります。

4 クライアント PC の設定

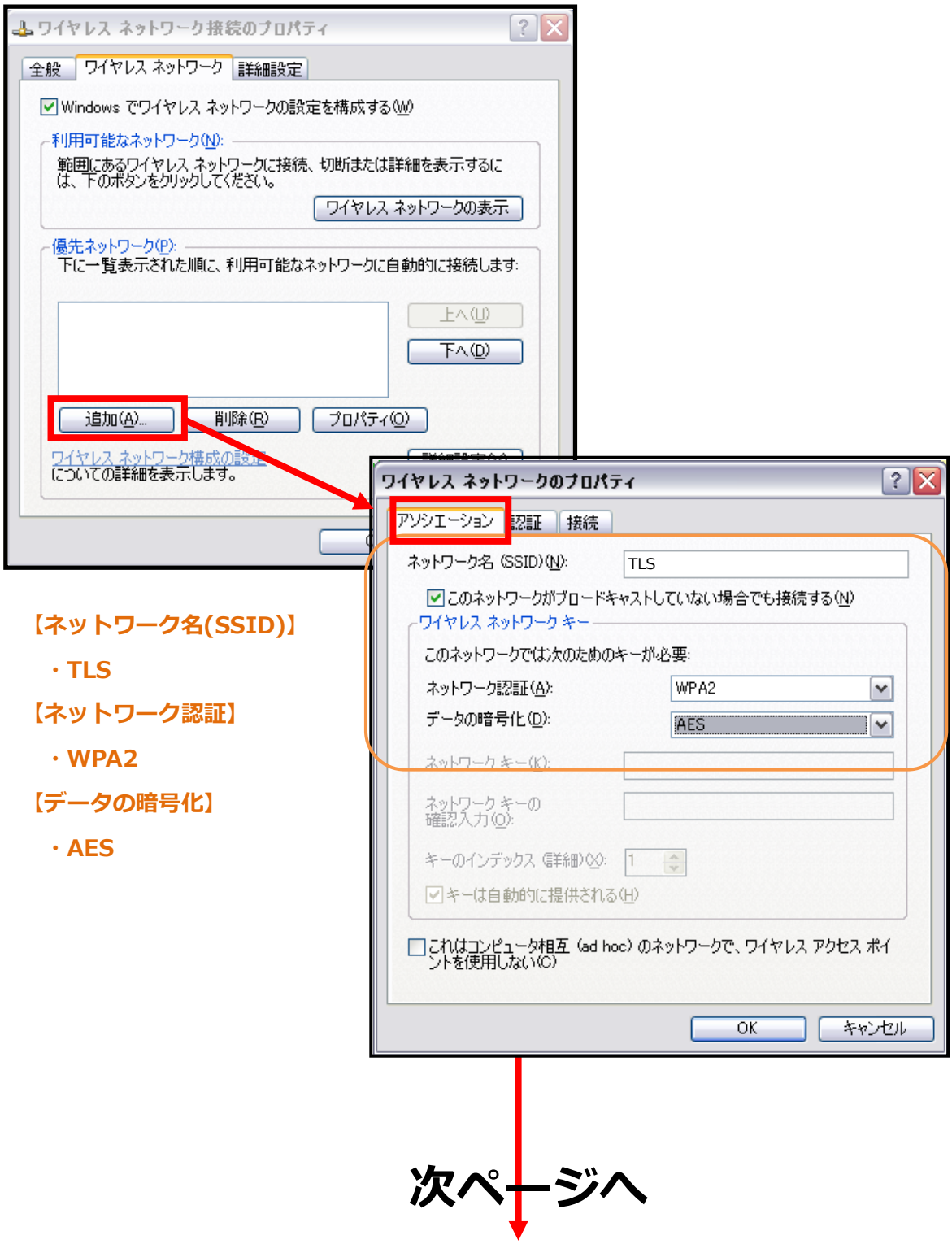
4-1 クライアント PC 設定の流れ

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)】

・TLS

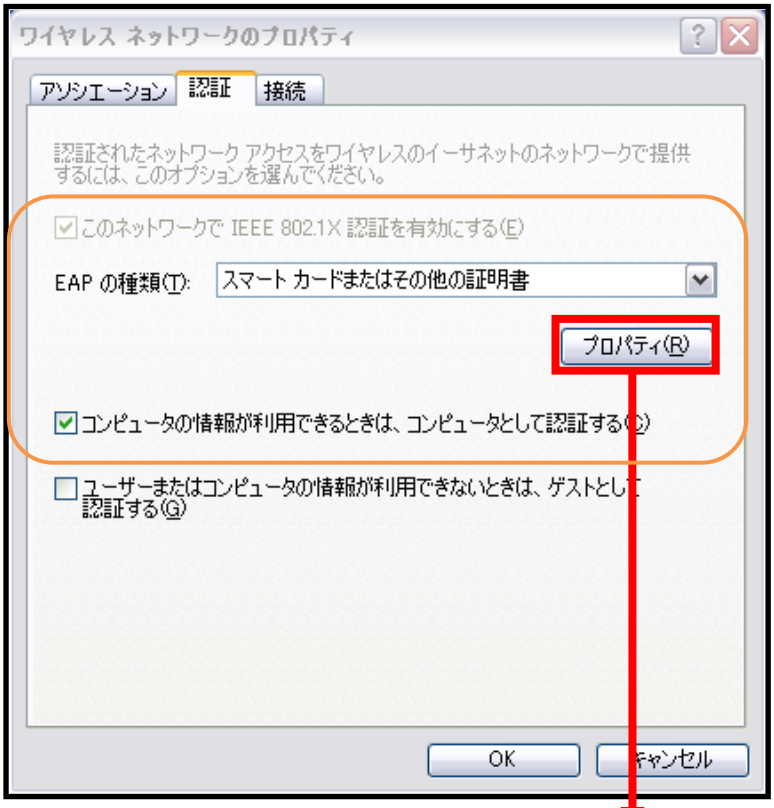
【ネットワーク認証】

・WPA2

【データの暗号化】

・AES

次ページへ

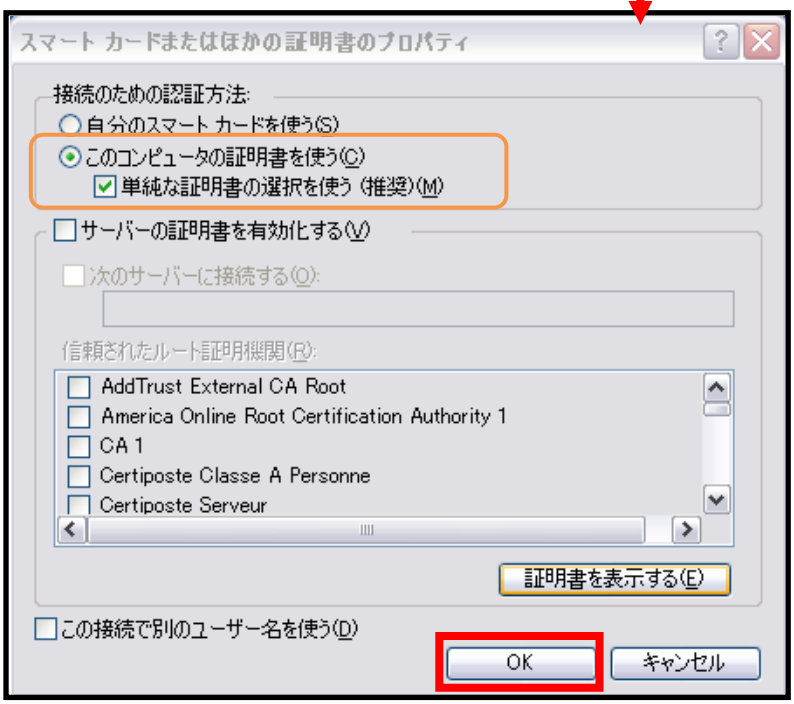


【EAP の種類】

・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

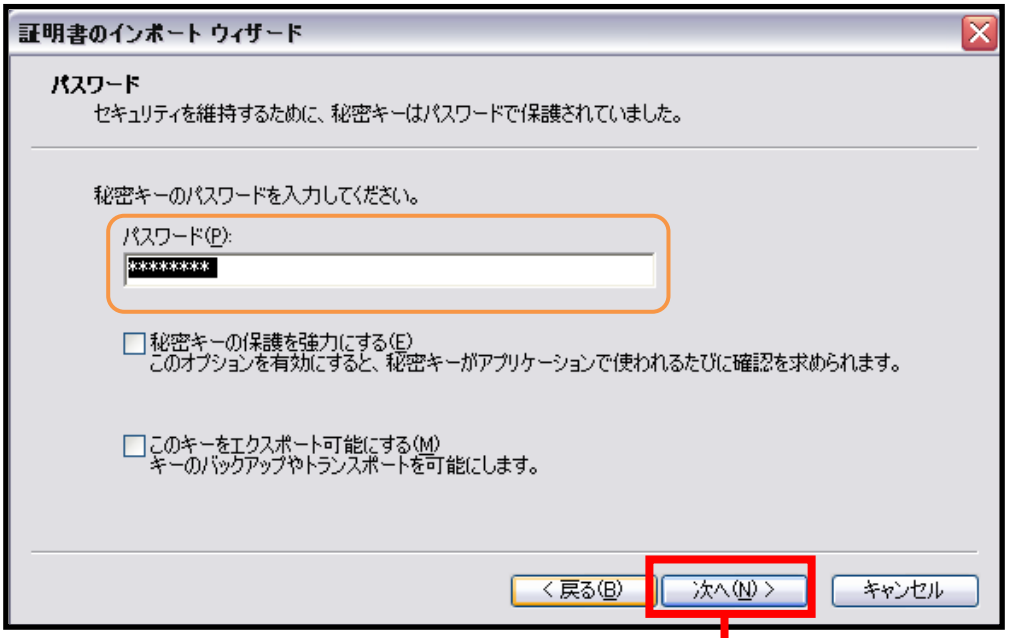
【単純な証明書の選択を使う】

・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。

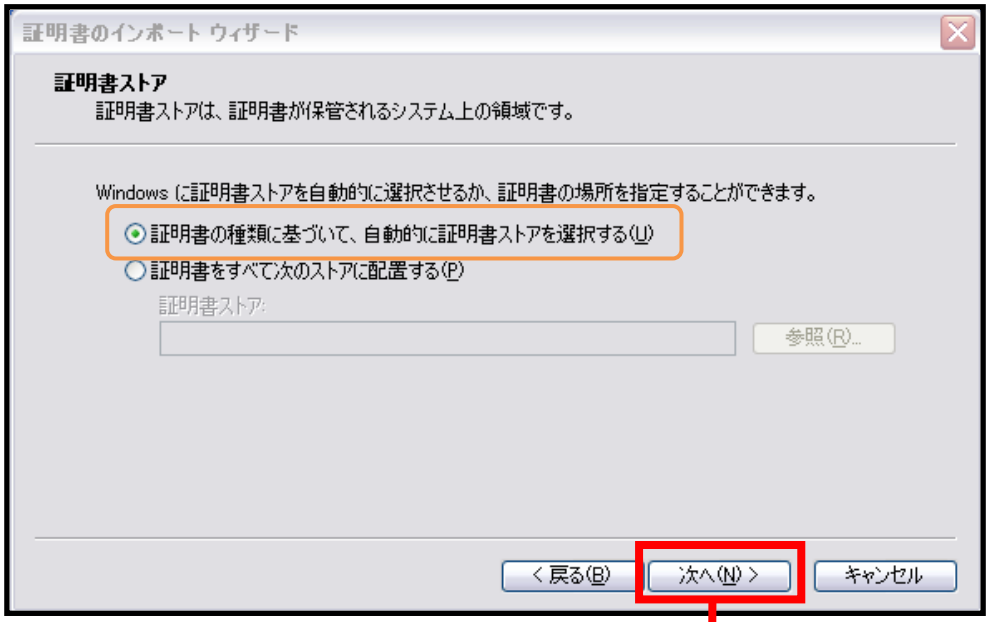
本書では、デスクトップ上に保存されている「soliton_user_0E.p12」アイコンをダブルクリックします。



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】

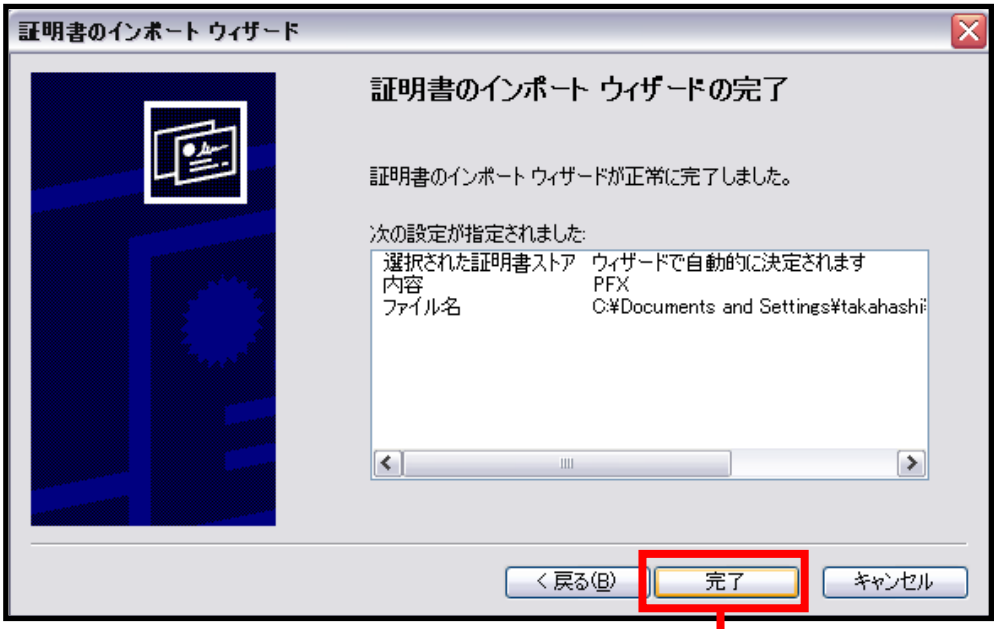
・password

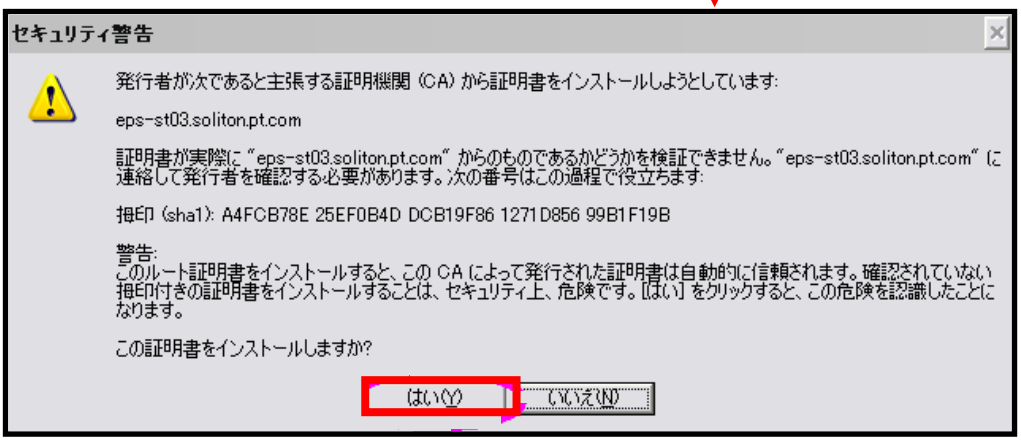


【証明書の種類に基づいて・・・】

・チェック有

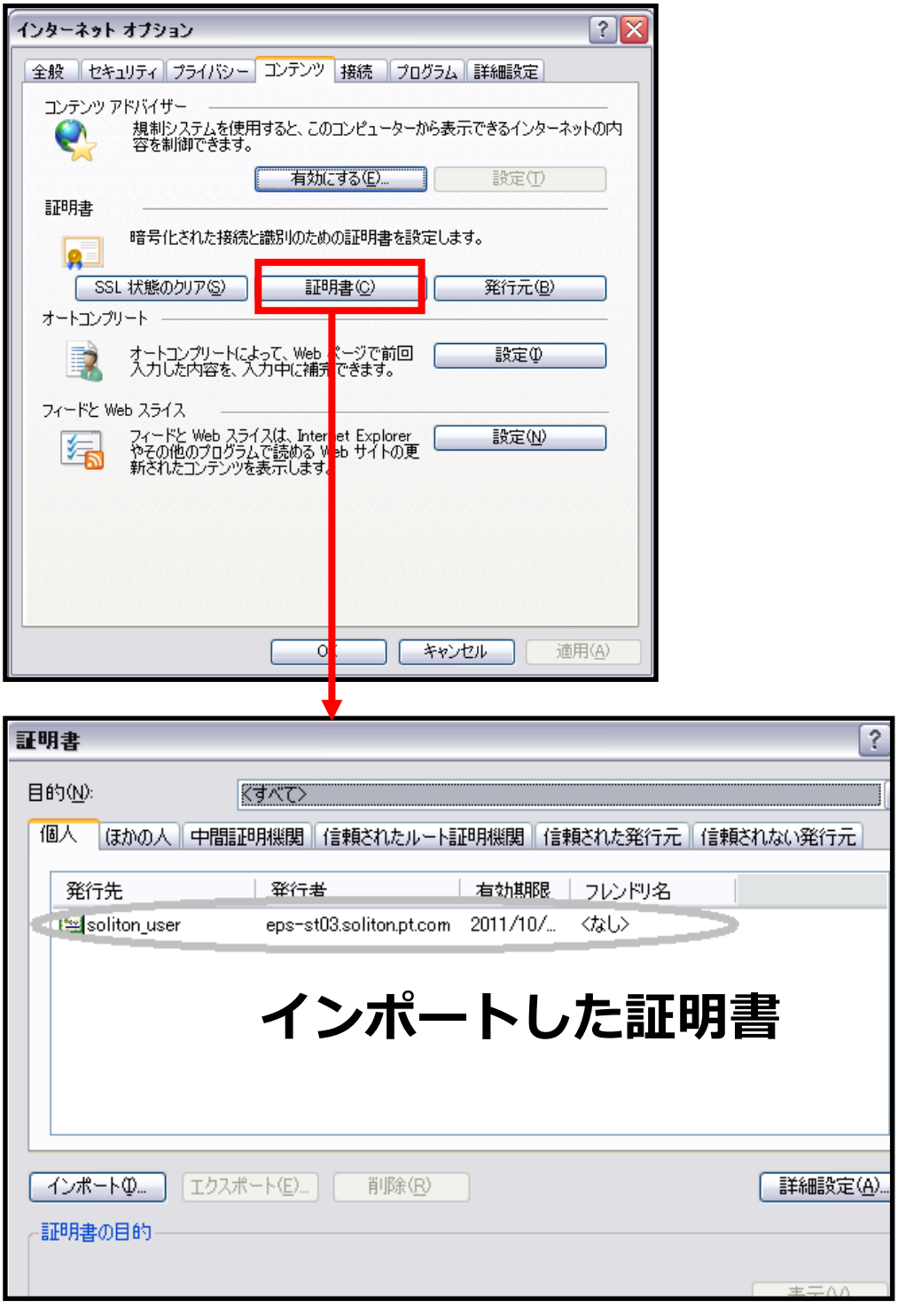
次ページへ


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:
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。



改訂履歴

日付	版	改訂内容
2012/9/28	1.0	初版作成