NetAttest EPS 設定例

連携機器：

Alcatel-Lucent OmniSwitch 6850

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 とアルカテル・ルーセント社製 Omni Switch6850 における 802.1X 認証環境の構築について、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

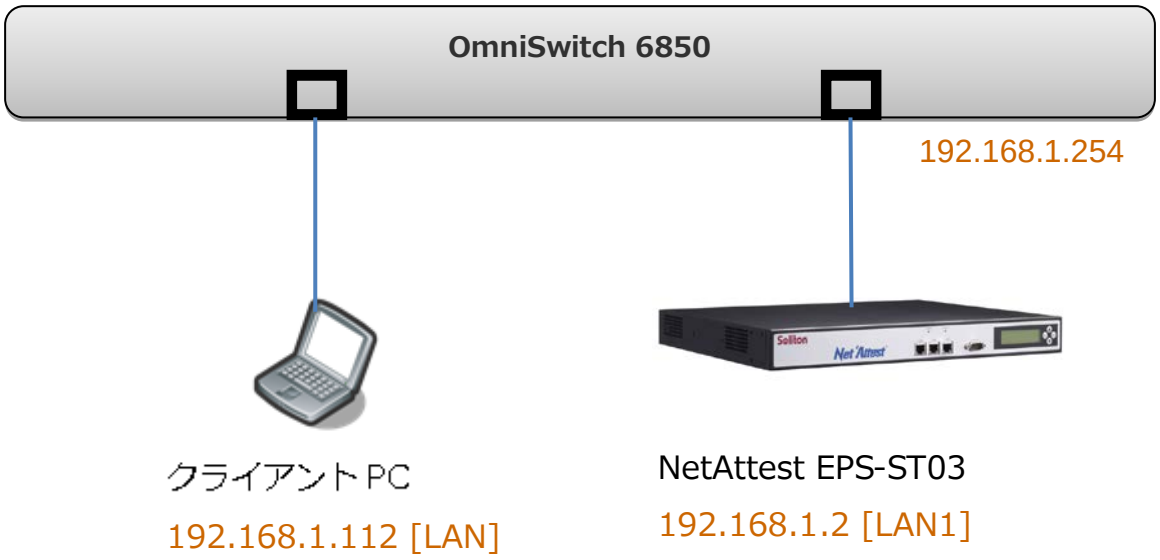
本書は、当社での検証に基づき、NetAttest EPS 及び Omni Switch 6850 の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

目次

1 構成

1-1 構成図

・有線 LAN で接続する機器は L2 スイッチに収容



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-ST03	Ver. 4.2.3
Authenticator	Alcatel Lucent	Omni Switch 6850	
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	Omni Switch 6850	Client PC
IP アドレス	192.168.1.2	192.168.1.214	192.168.1.112 (DHCP)
RADIUS port (Authentication)	UDP 1812		–
RADIUS port (Accounting)	UDP 1813		–
RADIUS Secret (Key)	soliton		–

2NetAttest EPS

2-1 NetAttest EPS 設定の流れ

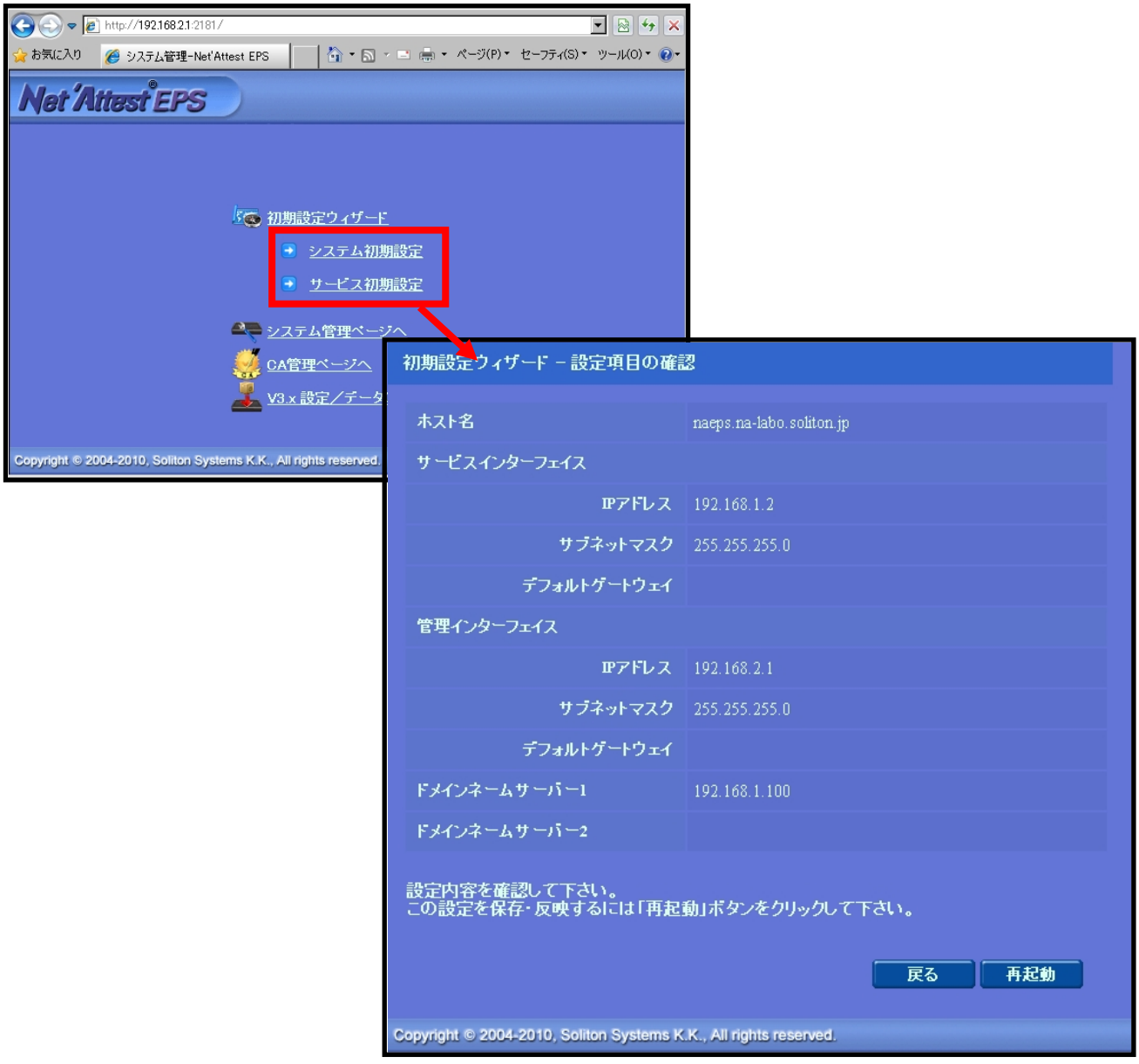
設定の流れ

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

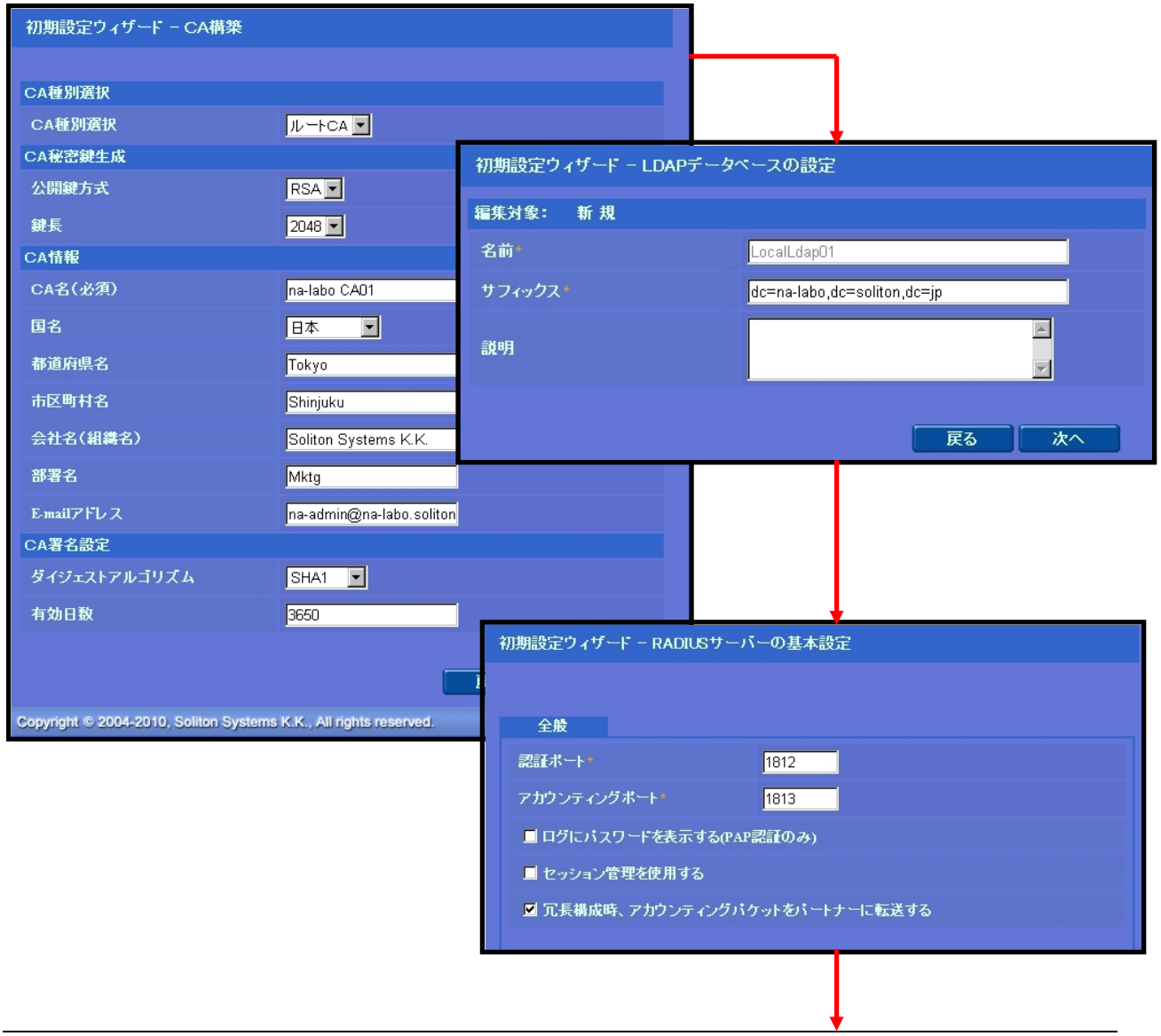


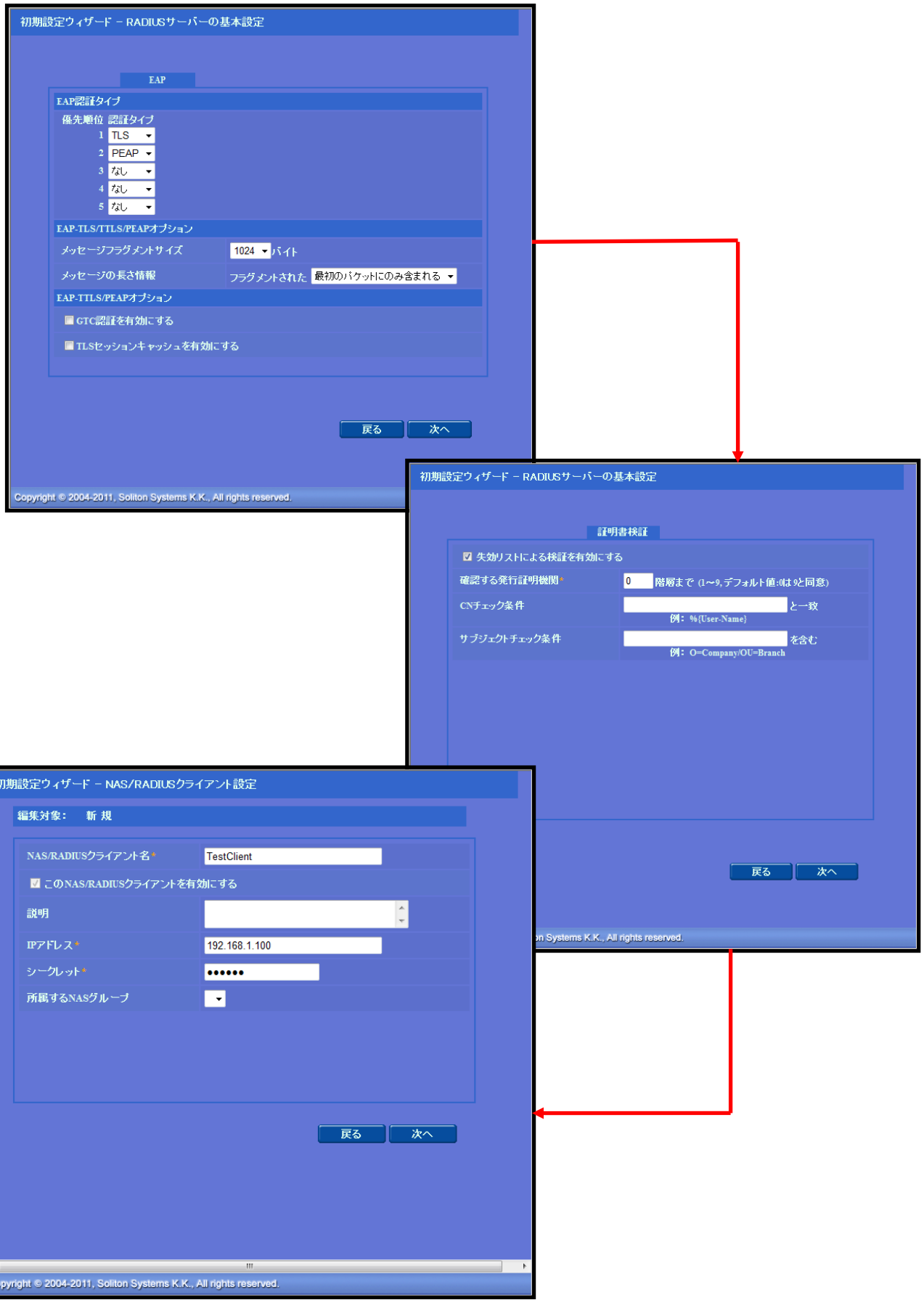
2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

本書では、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 サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定

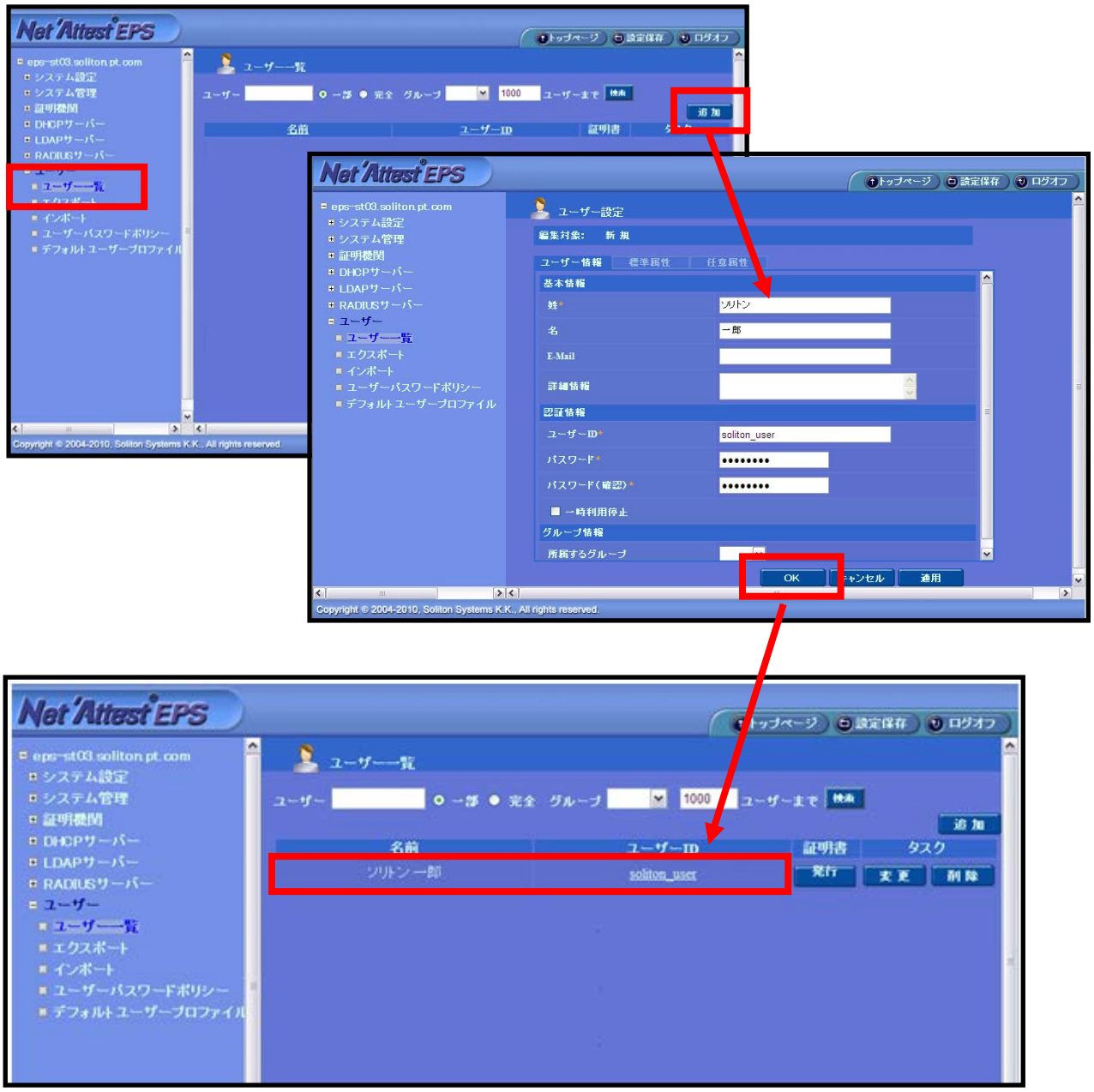



初期設定ウィザード – RADIUSサーバーの基本設定
EAP
EAP認証タイプ
優先順位 認証タイプ
1 TLS
2 PEAP
3 なし
4 なし
5 なし
EAP-TLS/TTLS/PEAPオプション
メッセージフラグメントサイズ 1024 バイト
メッセージの長さ情報 フラグメントされた 最初のパケットにのみ含まれる
EAP-TLS/PEAPオプション
GTC認証を有効にする
TLSセッションキャッシュを有効にする
戻る
次へ
Copyright © 2004-2011, Soliton Systems K.K., All rights reserved.
初期設定ウィザード – RADIUSサーバーの基本設定
証明書検証
失効リストによる検証を有効にする
確認する発行証明機関* 0 階層まで (1～9, デフォルト値:0は9と同意)
CNチェック条件 と一致
例: %{User-Name}
サブジェクトチェック条件 を含む
例: O=Company/OU=Branch
戻る
次へ
Systems K.K., All rights reserved.
初期設定ウィザード – NAS/RADIUSクライアント設定
編集対象: 新 規
NAS/RADIUSクライアント名* TestClient
このNAS/RADIUSクライアントを有効にする
説明
IPアドレス* 192.168.1.100
シークレット* ••••••
所属するNASグループ
戻る
次へ
Copyright © 2004-2011, Soliton Systems K.K., All rights reserved.

2-4 ユーザーの登録

WebGUI より、ユーザー登録を行います。

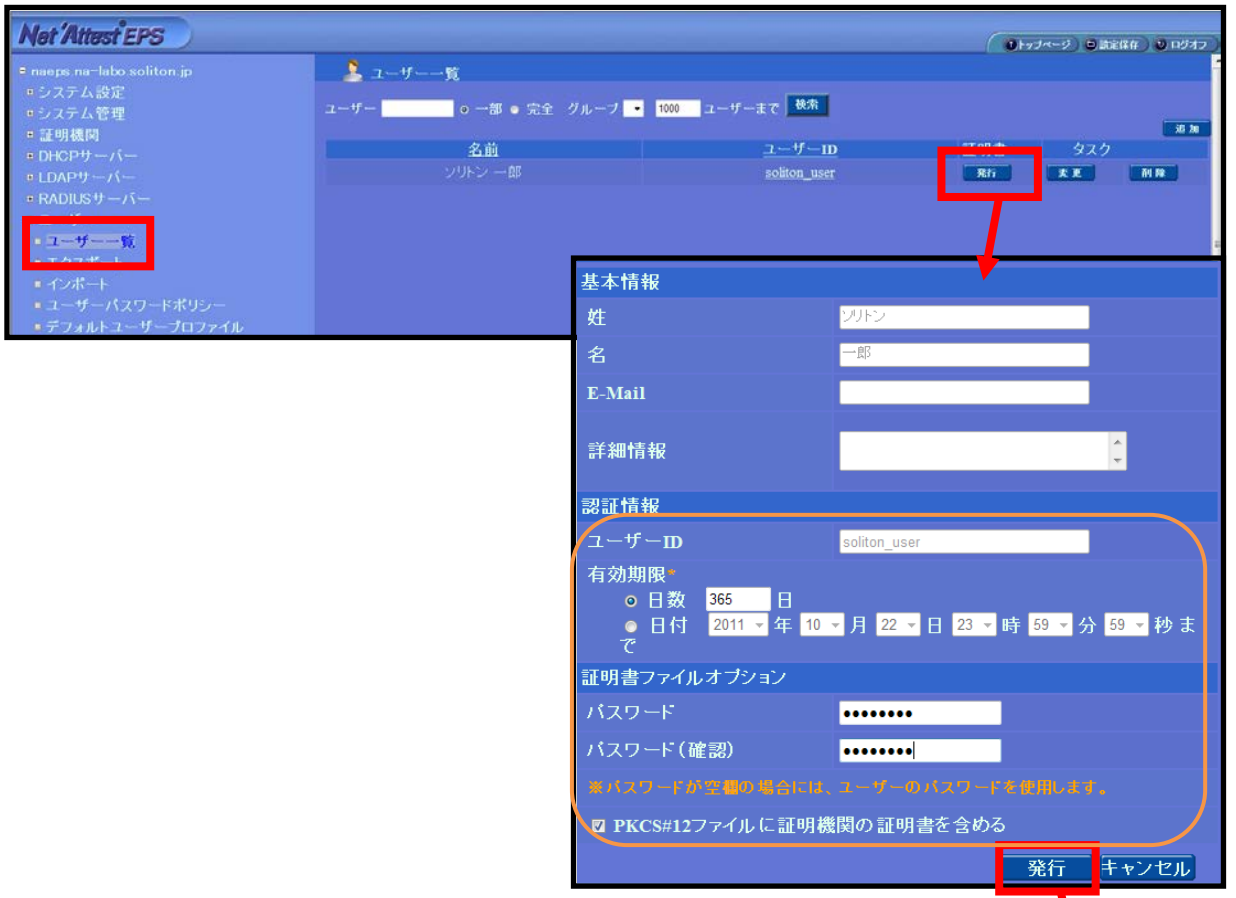
「ユーザー」→「ユーザー一覧」から、『追加』ボタンでユーザー登録を始めます。

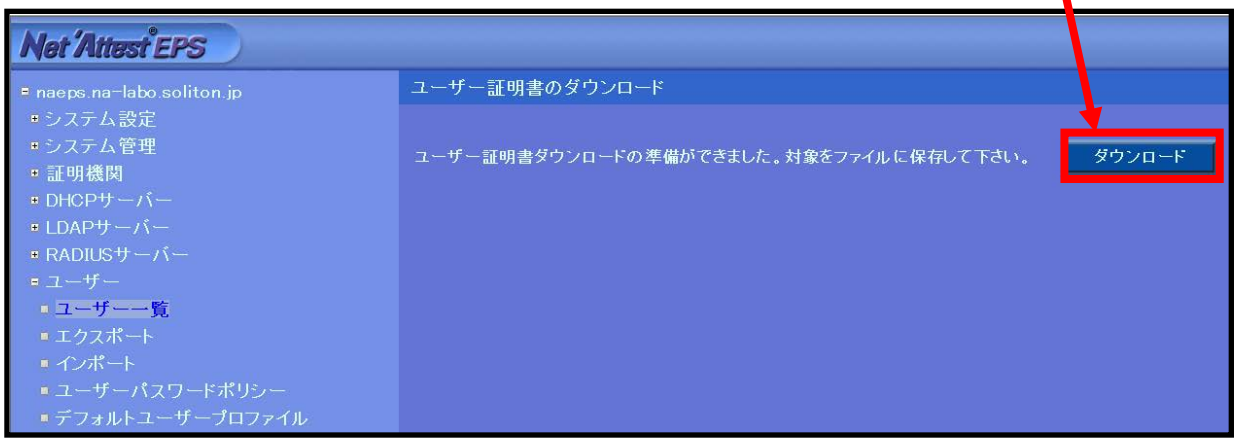


2-5 ユーザー証明書の発行

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。





3 Omni Switch6850

3-1 設定

Alcatel-Lucent 社製スイッチ Omni Switch 6850 を設定するためには、WebGUI または CLI を用います。本書では WebGUI を用いて各種設定を実施する方法を紹介します。

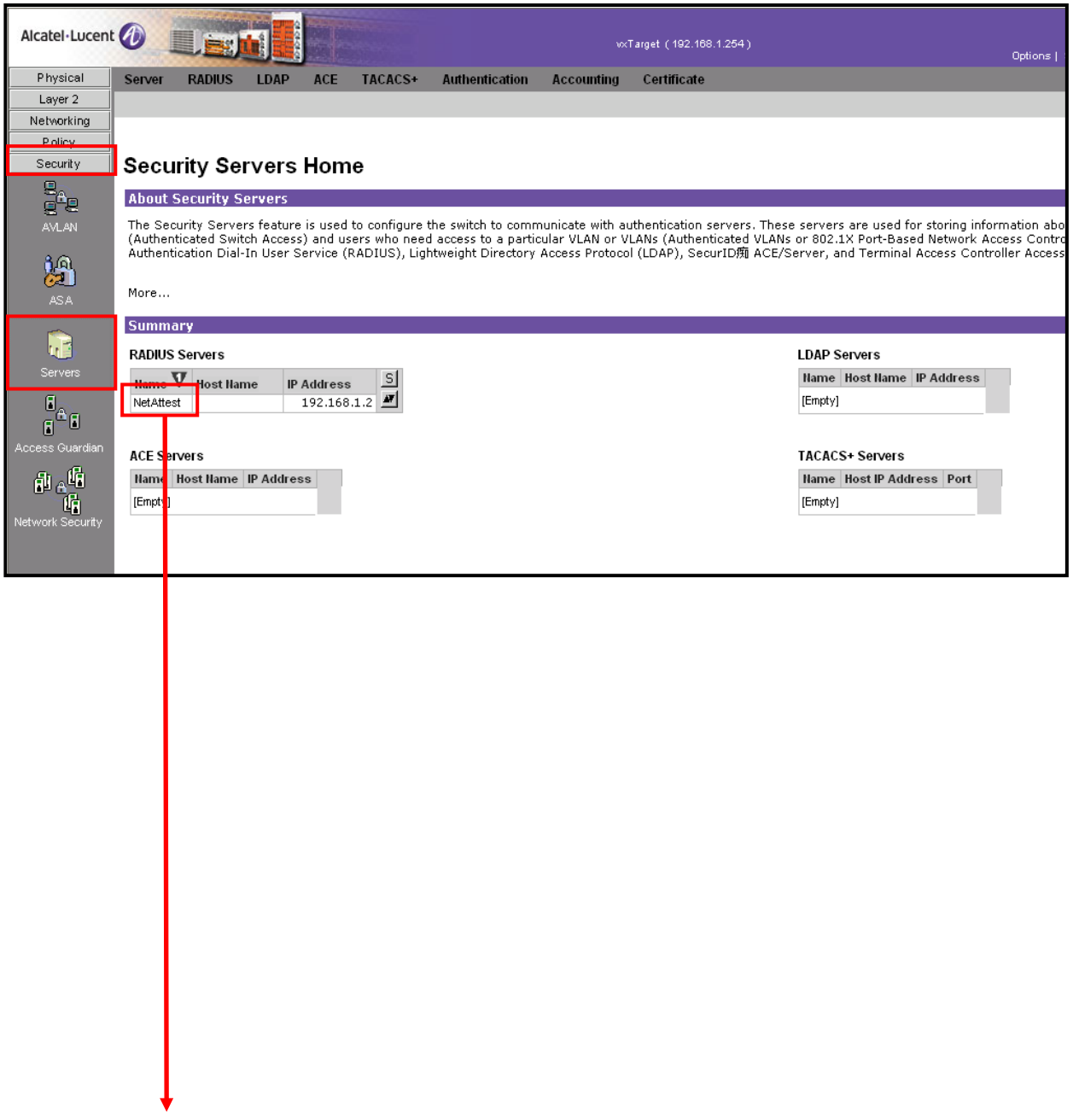
3-2 Omni Switch 6850 の設定

3-2-1 Radius サーバーの登録

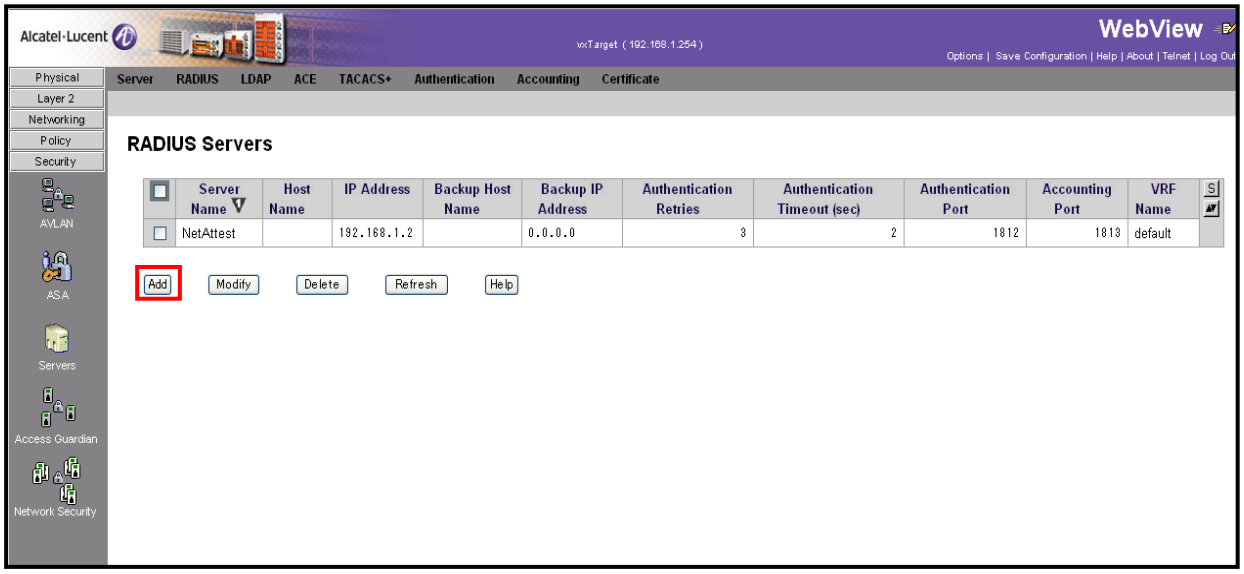
RADIUS サーバーとして NetAttest EPS を登録します。

[Security]メニューを展開し、[Servers]リンクをクリックします。

「Summary」項目の中「RADIUS Servers」欄の[Name]の下の[Empty]から RADIUS の登録をします。



RADIUS Servers 登録ページが開くので[Add]ボタンをクリックし値を入力します。



入力値

[Server Name]
NetAttest

[IP Adress]
192.168.1.2

[Backup Host Name]
0.0.0.0

[Authentication Retries]
3

[Authentication Timeout (sec)]
2

[Authentication Port]
1812

[Accounting Port]
1813

[VRF Name]
default

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

Windows XP での設定

1. ユーザー証明書のインポート
2. ワイヤレスネットワーク接続先の登録

Windows 7 での設定

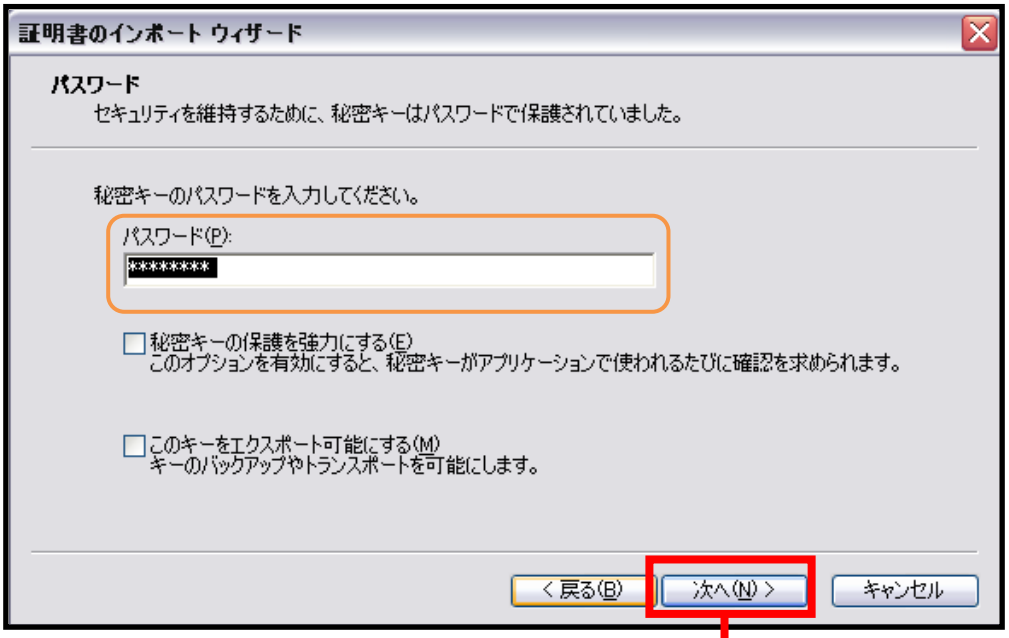
3. ユーザー証明書のインポート
4. ワイヤレスネットワーク接続先の登録

4-2 Windows XP での設定

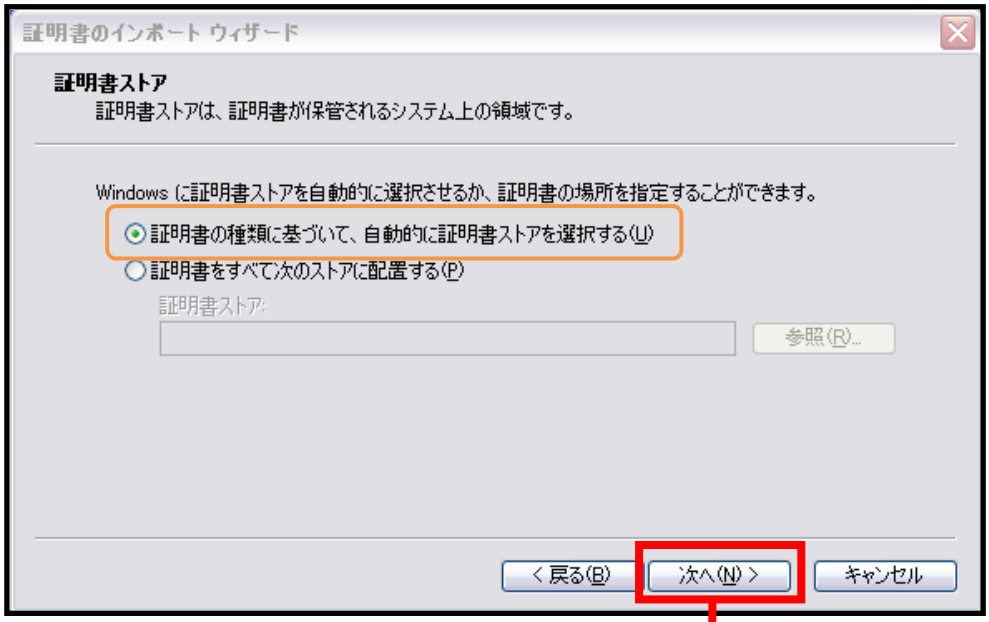
4-2-1 ユーザー証明書のインポート

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。

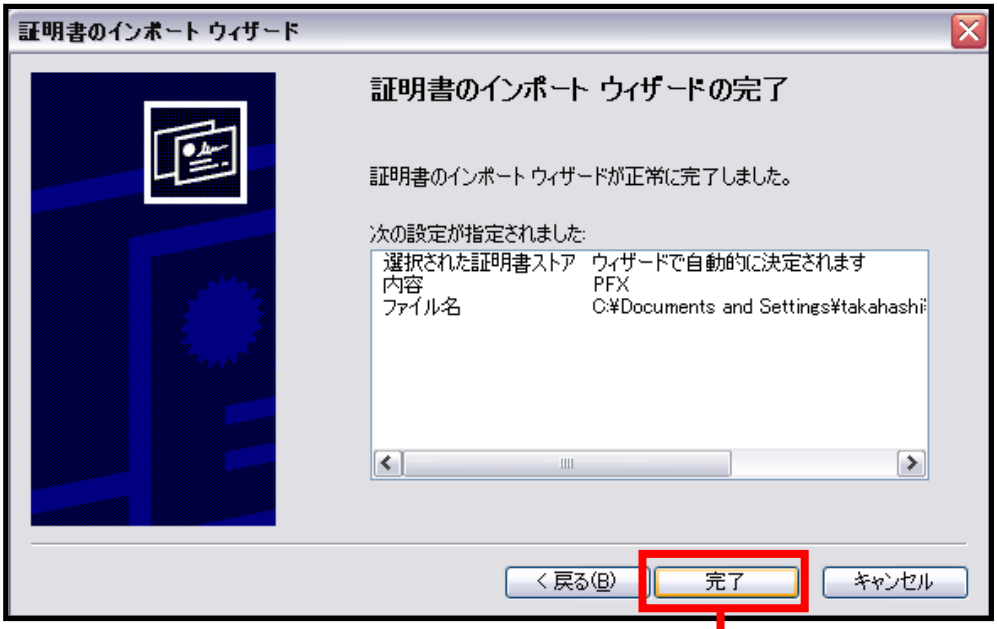


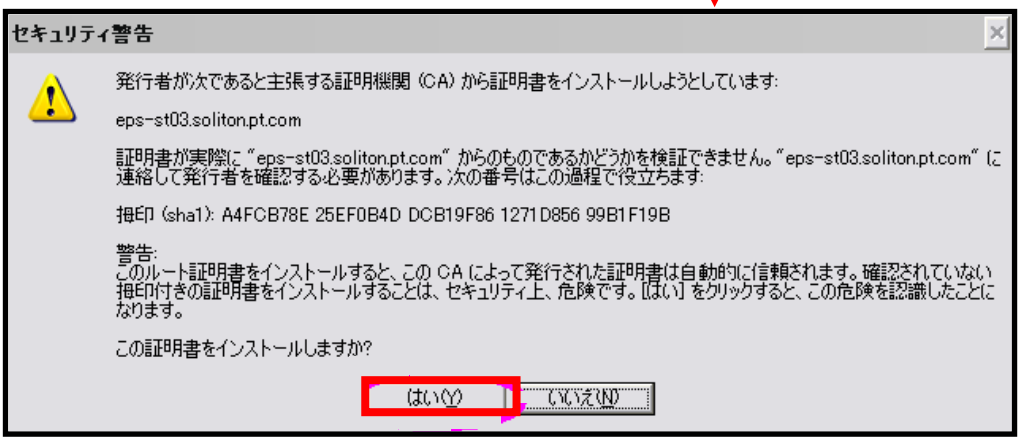
NetAttest EPS にてユーザー証明書を発行した際に設定したパスワードを入力します。



【証明書の種類に基づいて・・・】

・チェック有


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

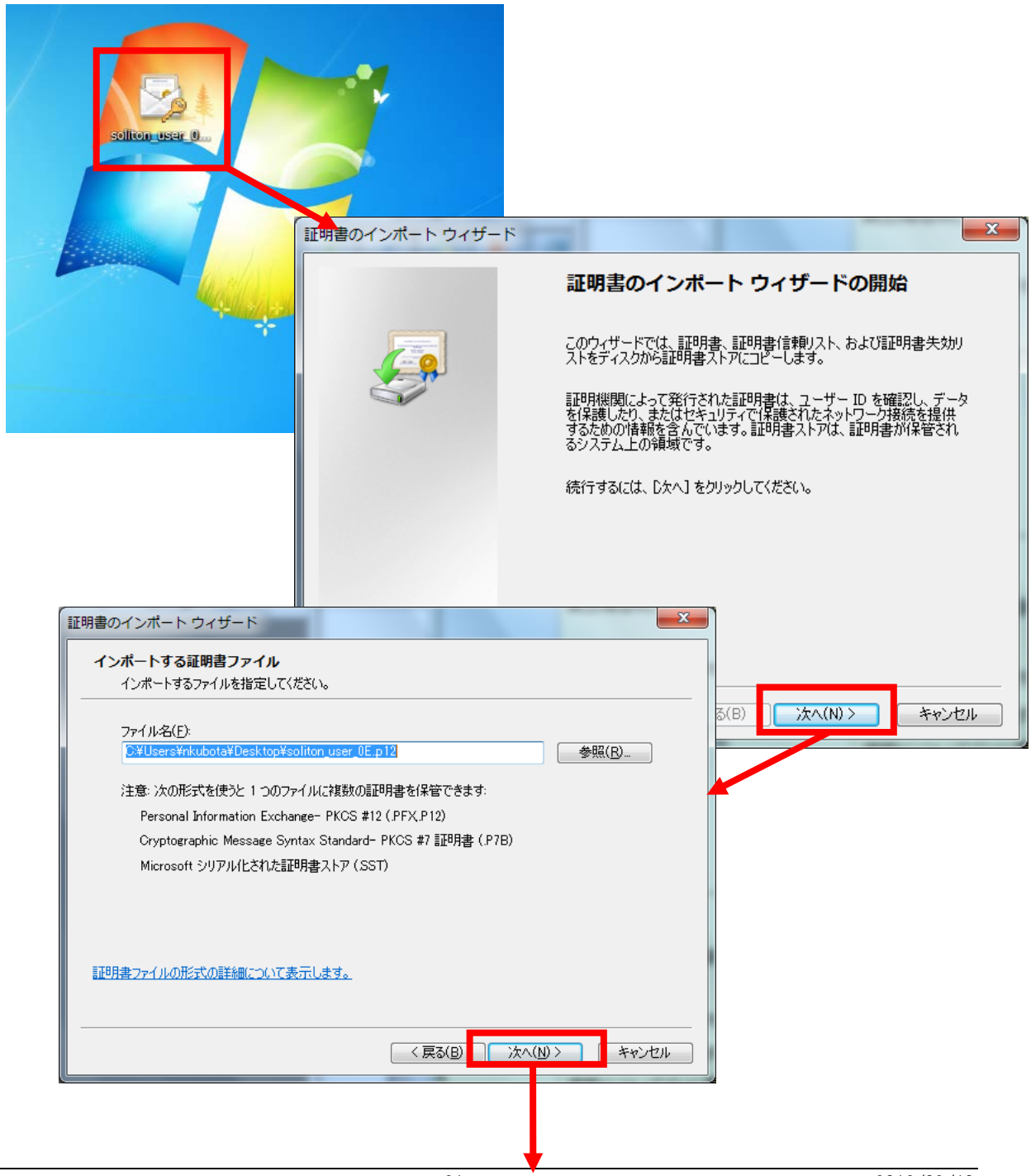

セキュリティ警告
発行者が次であると主張する証明機関 (CA) から証明書をインストールしようとしています:
eps-st03.soliton.pt.com
証明書が実際に "eps-st03.soliton.pt.com" からのものであるかどうかを検証できません。"eps-st03.soliton.pt.com" に連絡して発行者を確認する必要があります。次の番号はこの過程で役立ちます:
拇印 (sha1): A4FCB78E 25EF0B4D DCB19F86 1271D856 99B1F19B
警告:
このルート証明書をインストールすると、この CA によって発行された証明書は自動的に信頼されます。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)

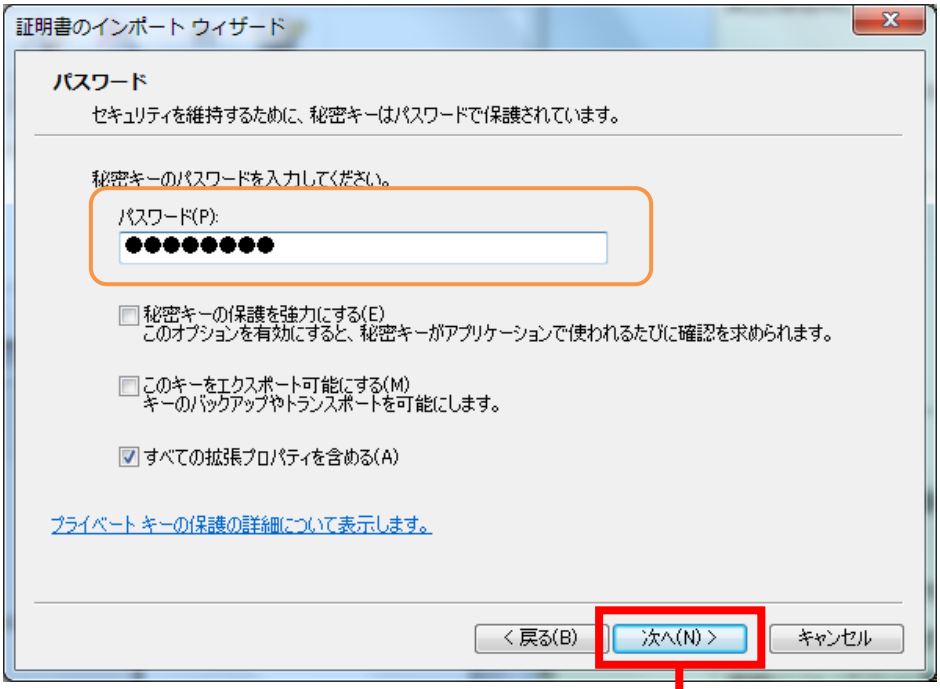
4-3 Windows 7 での設定

4-3-1 ユーザー証明書のインポート

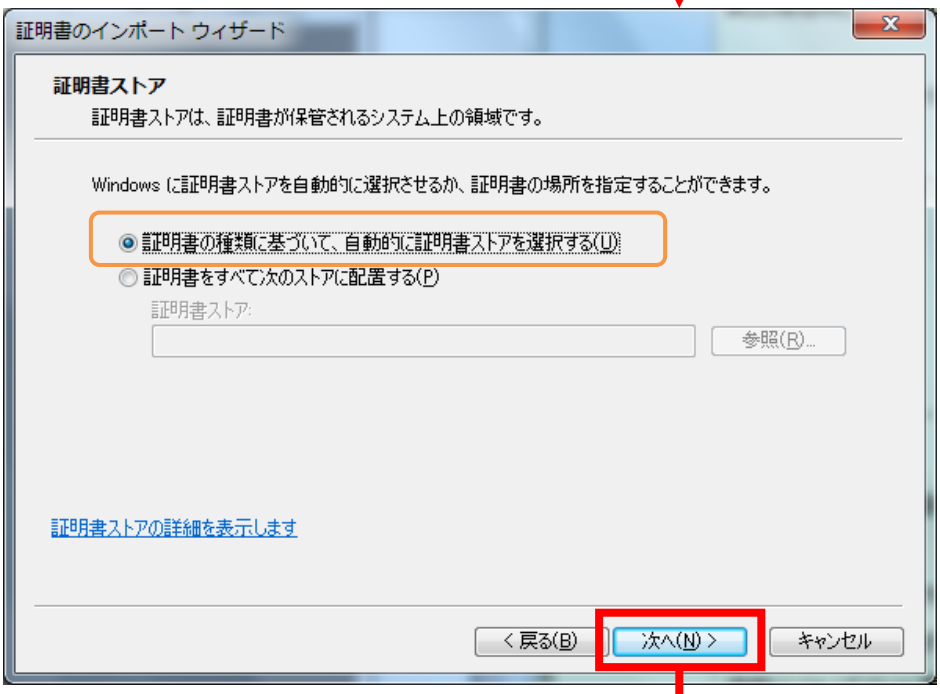
NetAttest EPS からダウンロードしたユーザー証明書をインポートします。

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。



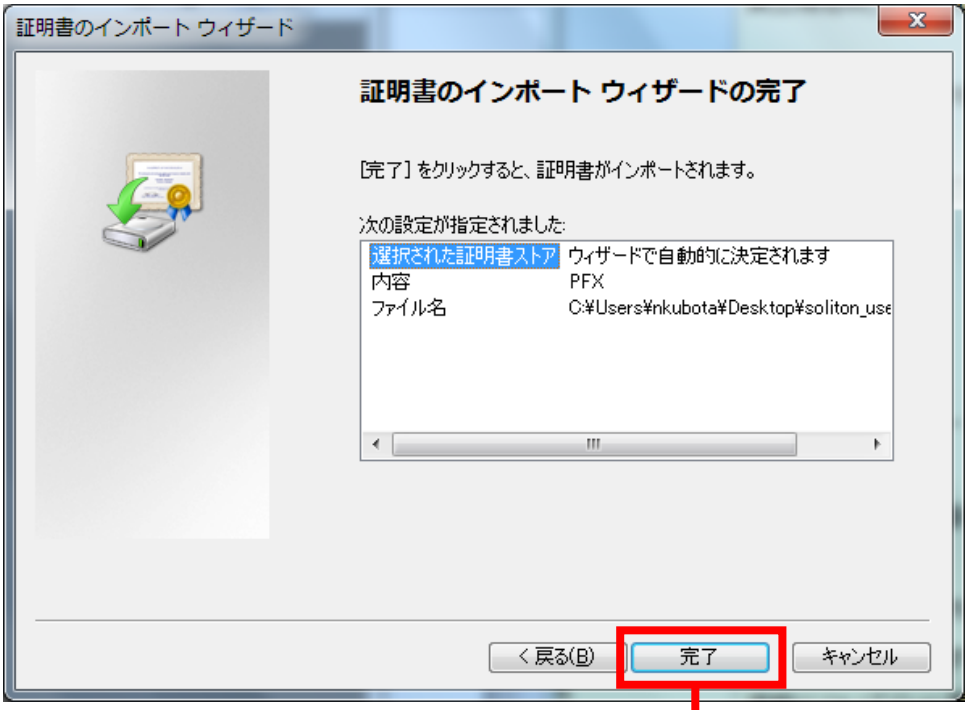


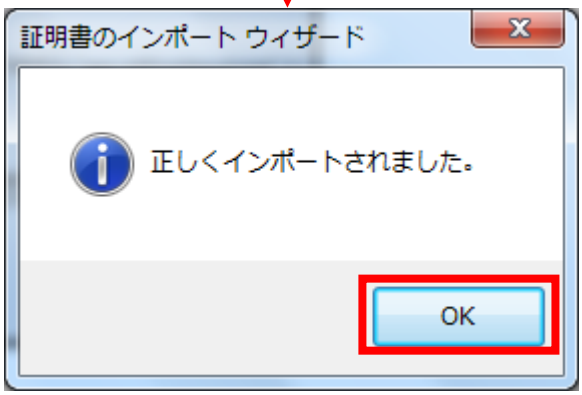
NetAttest EPS にてユーザー証明書を発行した際に設定したパスワードを入力します。



【証明書の種類に基づいて・・・】

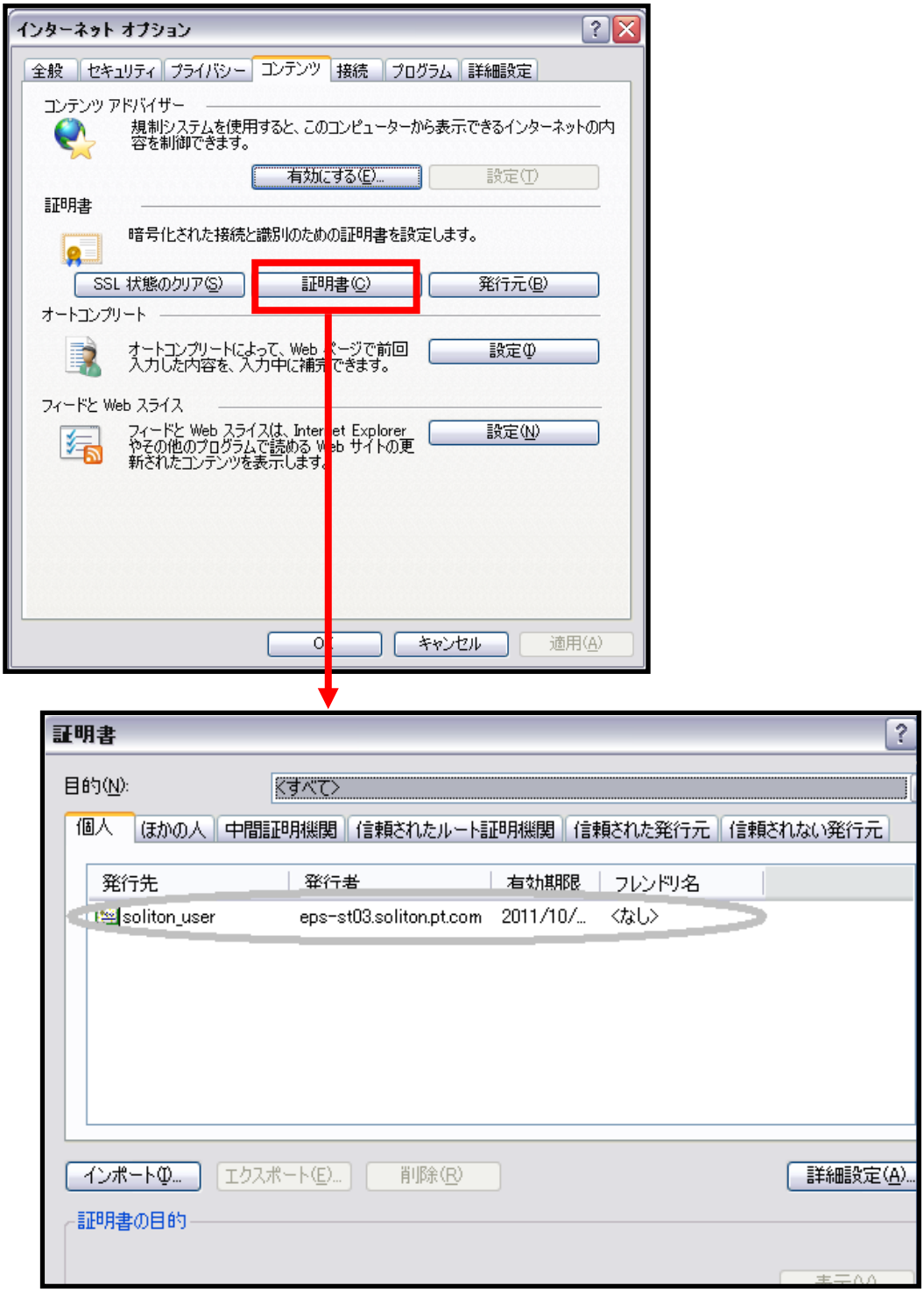
・チェック有


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
[完了] をクリックすると、証明書がインポートされます。
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:¥Users¥nkubota¥Desktop¥soliton_use
< 戻る(B)
完了
キャンセル


証明書のインポート ウィザード
正しくインポートされました。
OK

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
2012/2/1	1.0	初版作成
2012/9/10	1.1	RADIUS Port を TCP から UDP に修正