

NetAttest EPS 設定例

連携機器：

Alcatel-Lucent OmniSwitch 6850

Case：TLS 方式での認証

Version 1.1

NetAttest®は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本文中に ™、®、©は明記していません。

Copyright © 2011, Soliton Systems K.K. , All rights reserved.

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。 |
| <i>ABCDabcd1234</i> (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。

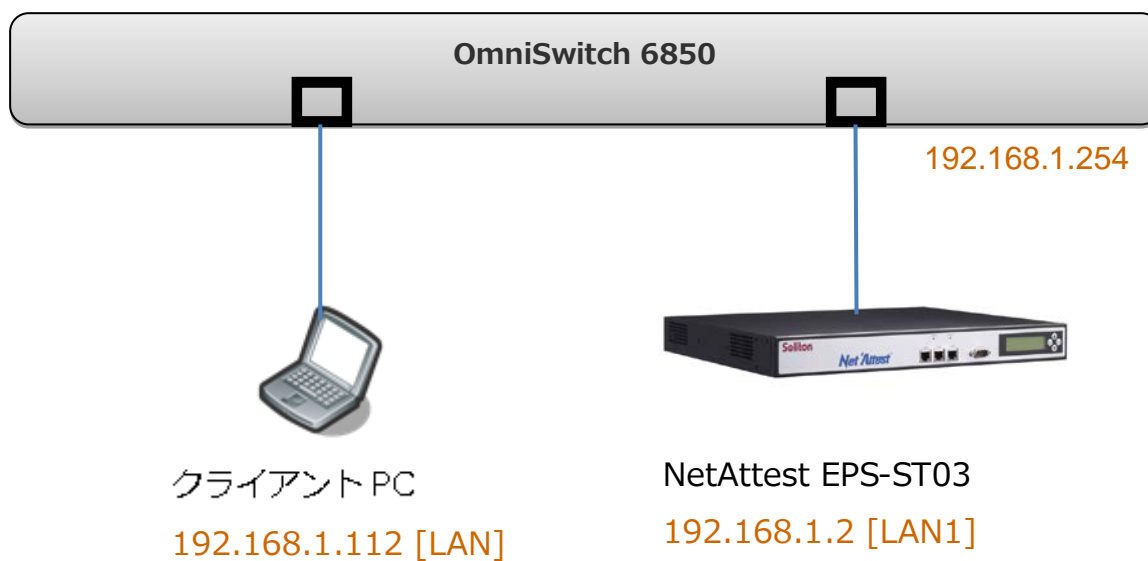
目次

| | |
|--------------------------------|----|
| 1 構成 | 6 |
| 1-1 構成図 | 6 |
| 1-2 環境 | 6 |
| 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 |
| 2-5 ユーザーの登録 | 12 |
| 2-7 ユーザー証明書の発行 | 13 |
| 3 Alcatel-Lucent | 14 |
| 3-1 設定 | 14 |
| 3-2 Omni Switch 6850 の設定 | 15 |
| 4. クライアント PC の設定 | 17 |
| 4-1 クライアント PC 設定の流れ | 17 |
| 4-2 Windows XP での設定 | 18 |
| 4-3 Windows 7 での設定 | 21 |
| 4-4 インポートされたユーザー証明書の確認 | 23 |

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 標準サブリカント |

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

The screenshot shows the Net'Attest EPS web interface. The '初期設定ウィザード' (Initial Setup Wizard) menu is visible, with 'システム初期設定' (System Initial Setup) highlighted. A red arrow points to a confirmation window titled '初期設定ウィザード - 設定項目の確認' (Initial Setup Wizard - Confirmation of Settings). This window displays the following configuration details:

| 初期設定ウィザード - 設定項目の確認 | |
|---------------------|--------------------------|
| ホスト名 | naeps.na-labo.soliton.jp |
| サービスインターフェイス | |
| IPアドレス | 192.168.1.2 |
| サブネットマスク | 255.255.255.0 |
| デフォルトゲートウェイ | |
| 管理インターフェイス | |
| IPアドレス | 192.168.2.1 |
| サブネットマスク | 255.255.255.0 |
| デフォルトゲートウェイ | |
| ドメインネームサーバー1 | 192.168.1.100 |
| ドメインネームサーバー2 | |

設定内容を確認して下さい。
この設定を保存・反映するには「再起動」ボタンをクリックして下さい。

戻る 再起動

Copyright © 2004-2010, Soliton Systems K.K., All rights reserved.

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

The image shows a sequence of three screenshots from the Soliton initial setup wizard, connected by red arrows indicating the flow of the process.

初期設定ウィザード - CA構築

CA種別選択
CA種別選択: ルートCA

CA秘密鍵生成
公開鍵方式: RSA
鍵長: 2048

CA情報
CA名(必須): na-labo CA01
国名: 日本
都道府県名: Tokyo
市区町村名: Shinjuku
会社名(組織名): Soliton Systems K.K.
部署名: Mktg
E-mailアドレス: na-admin@na-labo.soliton

CA署名設定
ダイジェストアルゴリズム: SHA1
有効日数: 3650

Copyright © 2004-2010, Soliton Systems K.K., All rights reserved.

初期設定ウィザード - LDAPデータベースの設定

編集対象: 新規

名前*: LocalLdap01
サフィックス*: dc=na-labo,dc=soliton,dc=jp
説明:

戻る 次へ

初期設定ウィザード - RADIUSサーバーの基本設定

全般

認証ポート*: 1812
アカウントングポート*: 1813

ログにパスワードを表示する(PAP認証のみ)
 セッション管理を使用する
 冗長構成時、アカウントングパケットをパートナーに転送する

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 最初のバケットにのみ含まれる

EAP-TTLS/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 0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

in 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。

The screenshots illustrate the user registration process in the Net'Attest EPS WebGUI:

- Step 1:** Access the 'ユーザー一覧' (User List) page. The '追加' (Add) button is highlighted in red.
- Step 2:** The 'ユーザー設定' (User Settings) form is displayed. Fields include: 姓* (Surname: ソリトン), 名 (Name: 一郎), E-Mail, 詳細情報 (Detailed Information), 認証情報 (Authentication Information) with fields for ユーザーID* (User ID: soliton_user), パスワード* (Password), and パスワード(確認)* (Confirm Password). The 'OK' button is highlighted in red.
- Step 3:** The 'ユーザー一覧' (User List) page shows the newly added user. The user entry is highlighted in red:

| 名前 | ユーザーID | 証明書 | タスク |
|---------|--------------|-----|----------|
| ソリトン 一郎 | soliton_user | 発行 | 実行 変更 削除 |

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。

The screenshot displays the NetAttest EPS WebGUI interface. The left sidebar contains a navigation menu with the following items: naeps.na-labo.soliton.jp, システム設定, システム管理, 証明機関, DHCPサーバー, LDAPサーバー, RADIUSサーバー, ユーザー一覧 (highlighted), インポート, ユーザーパスワードポリシー, and デフォルトユーザープロフィール. The main content area is titled 'ユーザー一覧' and shows a table of users. The user 'soliton_user' is selected, and the '発行' (Issue) button is highlighted. A detailed view of the user's certificate information is shown, including fields for name, email, user ID, validity period, and password. The '発行' button is highlighted again. The bottom screenshot shows the 'ダウンロード' (Download) button highlighted, indicating the certificate is ready for download.

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。

Alcatel-Lucent vxTarget (192.168.1.254) Options

Physical Server RADIUS LDAP ACE TACACS+ Authentication Accounting Certificate

Layer 2

Networking

Policy

Security

AVLAN

ASA

Servers

Access Guardian

Network Security

Security Servers Home

About Security Servers

The Security Servers feature is used to configure the switch to communicate with authentication servers. These servers are used for storing information about (Authenticated Switch Access) and users who need access to a particular VLAN or VLANs (Authenticated VLANs or 802.1X Port-Based Network Access Control Authentication Dial-In User Service (RADIUS), Lightweight Directory Access Protocol (LDAP), SecurID, ACE/Server, and Terminal Access Controller Access

More...

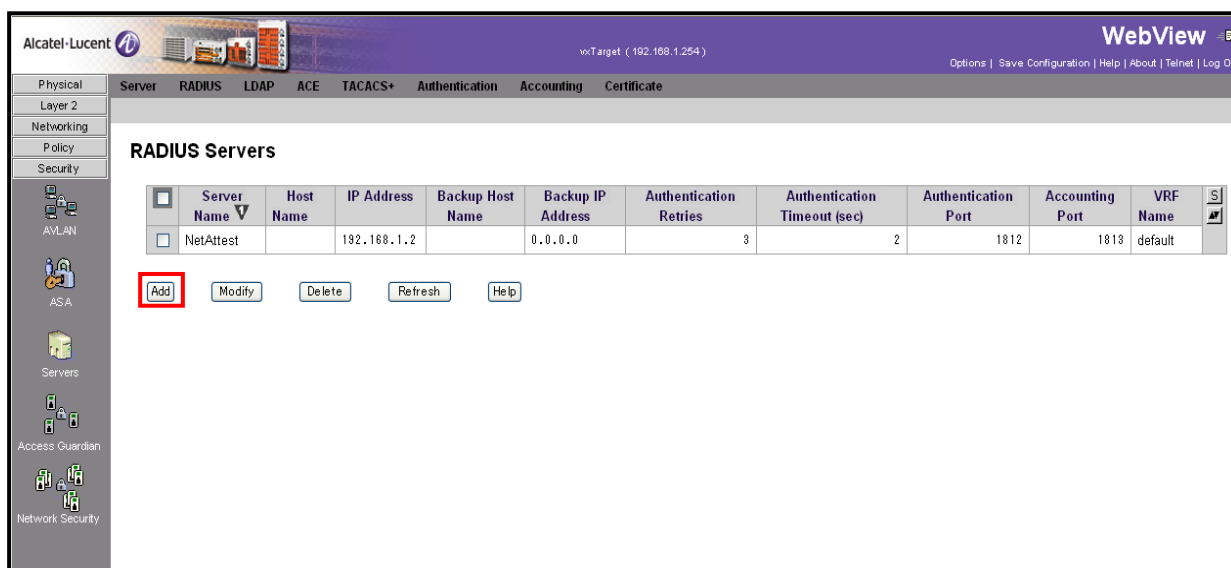
Summary

| Name | Host Name | IP Address |
|-----------|-----------|-------------|
| NetAttest | | 192.168.1.2 |

| Name | Host Name | IP Address |
|---------|-----------|------------|
| [Empty] | | |

| Name | Host Name | IP Address | Port |
|---------|-----------|------------|------|
| [Empty] | | | |

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。



The screenshot shows the Alcatel-Lucent WebView interface for configuring RADIUS Servers. The page title is "RADIUS Servers". Below the title is a table with the following columns: Server Name, Host Name, IP Address, Backup Host Name, Backup IP Address, Authentication Retries, Authentication Timeout (sec), Authentication Port, Accounting Port, and VRF Name. The table contains one entry: NetAttest, with IP Address 192.168.1.2, Backup IP Address 0.0.0.0, Authentication Retries 3, Authentication Timeout (sec) 2, Authentication Port 1812, Accounting Port 1813, and VRF Name default. Below the table are buttons for Add, Modify, Delete, Refresh, and Help. The "Add" button is highlighted with a red box.

| Server Name | Host Name | IP Address | Backup Host Name | Backup IP Address | Authentication Retries | Authentication Timeout (sec) | Authentication Port | Accounting Port | VRF Name |
|-------------|-----------|-------------|------------------|-------------------|------------------------|------------------------------|---------------------|-----------------|----------|
| NetAttest | | 192.168.1.2 | | 0.0.0.0 | 3 | 2 | 1812 | 1813 | default |

入力値

[Server Name]
NetAttest

[IP Address]
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。



証明書のインポート ウィザード

パスワード
セキュリティを維持するために、秘密キーはパスワードで保護されていました。

秘密キーのパスワードを入力してください。

パスワード(P):

秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。

< 戻る(B) **次へ(N) >** キャンセル

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。

証明書のインポート ウィザード

証明書ストア
証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

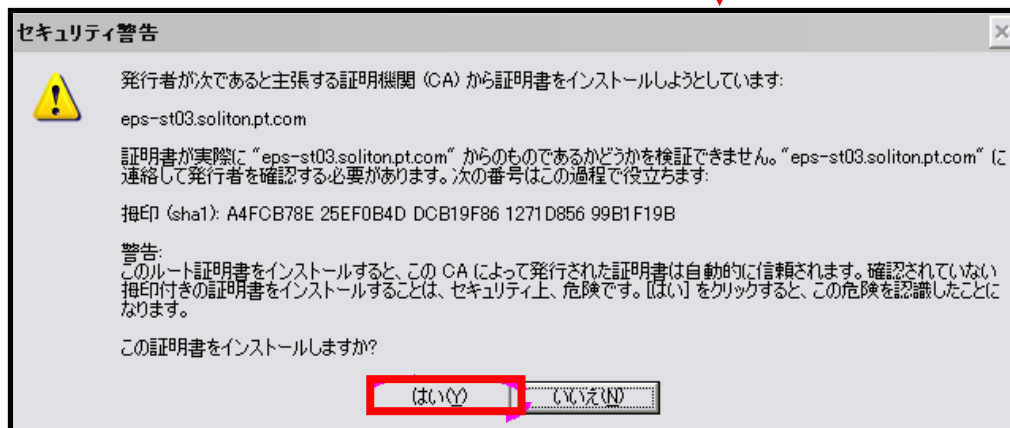
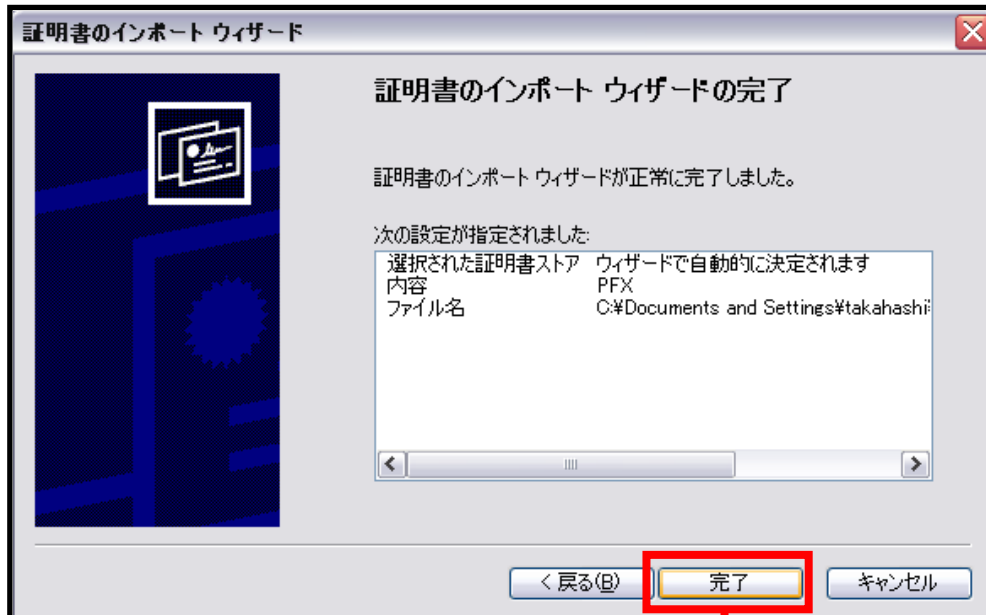
証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

証明書をすべて次のストアに配置する(P)

証明書ストア:
参照(R)...

< 戻る(B) **次へ(N) >** キャンセル

【証明書の種類に基づいて・・・】
・チェック有

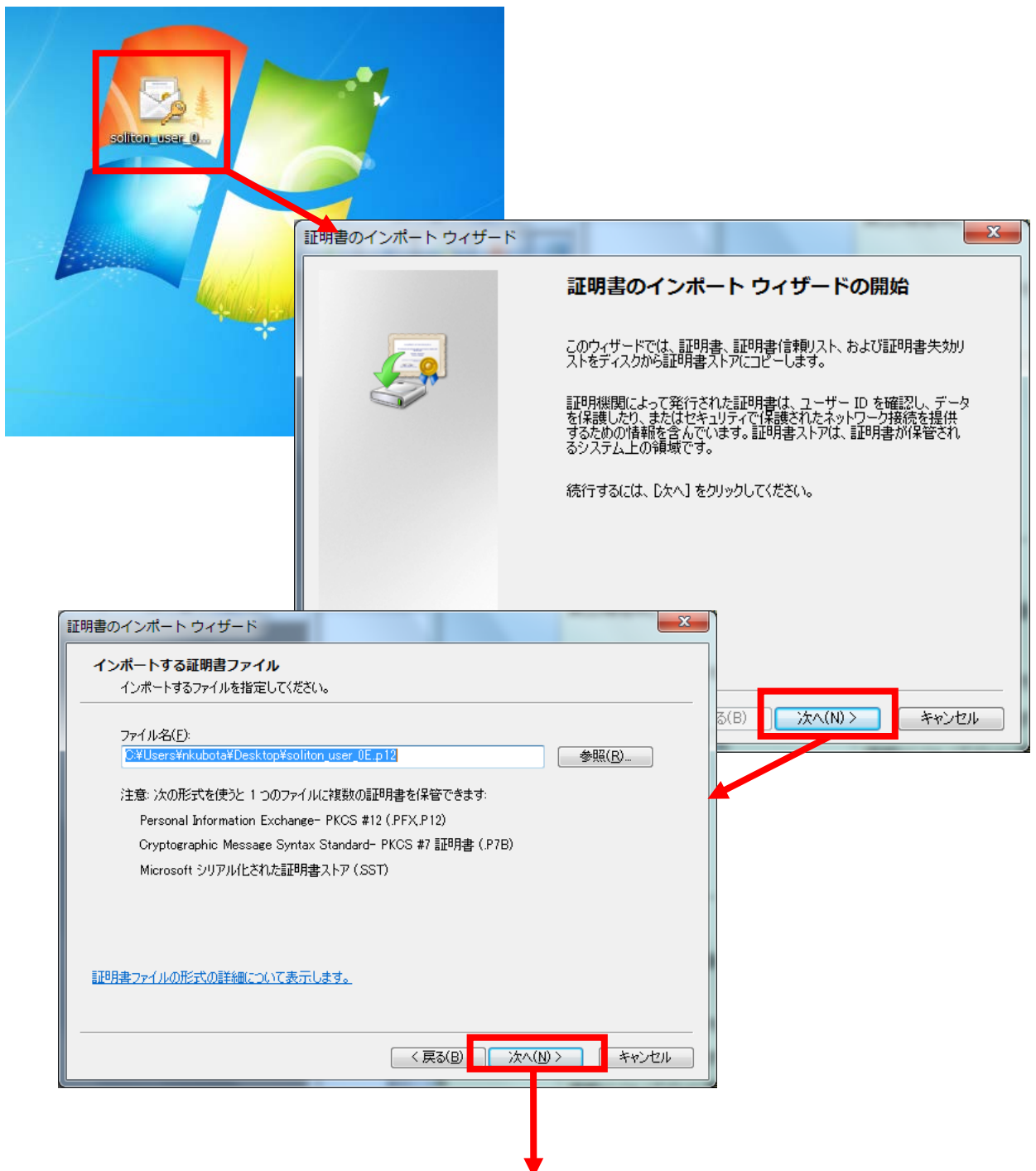


4-3 Windows 7 での設定

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。



証明書のインポート ウィザード

パスワード

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):
●●●●●●●●

秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。

すべての拡張プロパティを含める(A)

[プライベート キーの保護の詳細について表示します。](#)

< 戻る(B) **次へ(N) >** キャンセル

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。

証明書のインポート ウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

証明書の種類に基づいて、自動的に証明書ストアを選択する(U)

証明書をすべて次のストアに配置する(P)

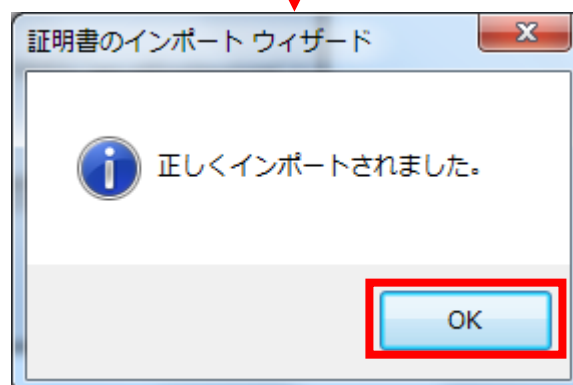
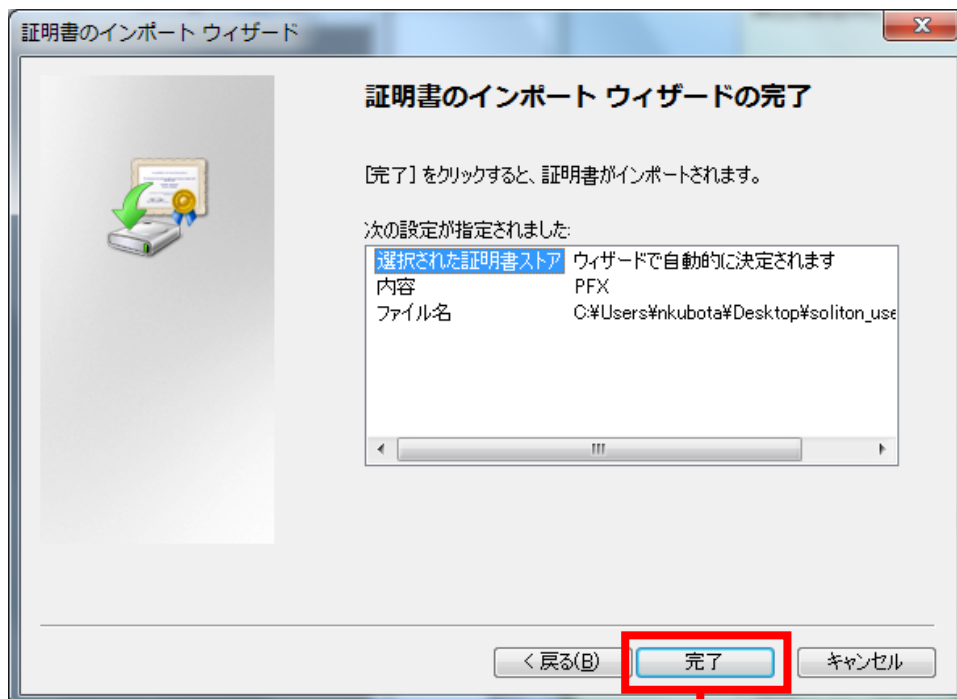
証明書ストア:
[] 参照(R)...

[証明書ストアの詳細を表示します](#)

< 戻る(B) **次へ(N) >** キャンセル

【証明書の種類に基づいて・・・】

・チェック有



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。

