

NetAttest EPS 設定例

連携機器：

ACERA800ST

Case：TLS 方式での認証

Version 1.0

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 © 2012, Soliton Systems K.K. , All rights reserved.

はじめに

本書について

本書は CA 内蔵 RADIUS サーバプライアンス NetAttest EPS と FURUNOS YSTEMS 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。
<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 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。

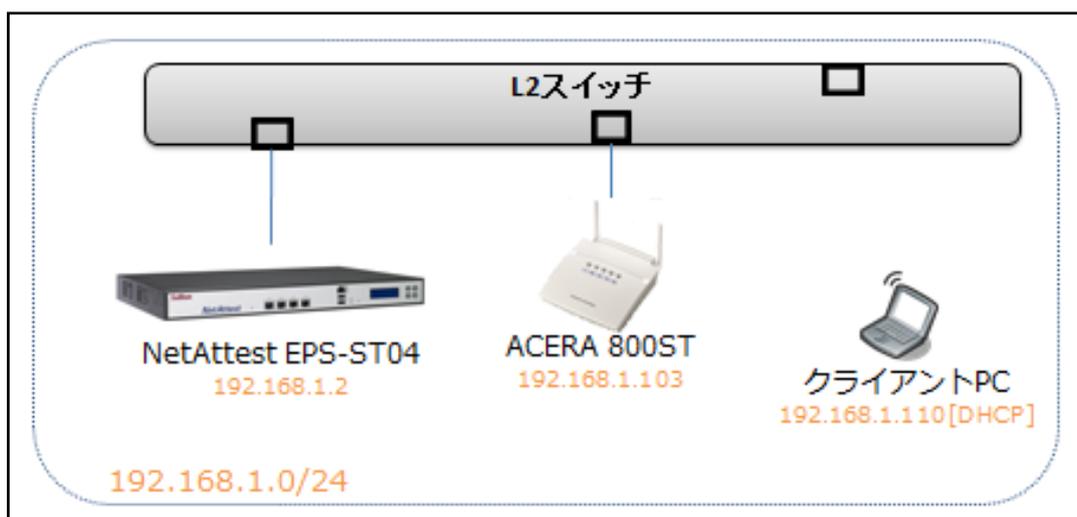
目次

1	構成.....	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 サーバー基本設定	12
2-6	ユーザーの登録.....	13
2-7	ユーザー証明書の発行	13
3	ACERA800ST.....	15
3-1	ACERA800ST 設定の流れ	15
3-2	ACERA800ST の ESSID の設定.....	16
3-3	ACERA800ST の再起動	18
4	クライアント PC の設定.....	19
4-1	クライアント PC 設定の流れ.....	19
4-2	ワイヤレスネットワーク接続先の登録.....	20
4-3	ユーザー証明書のインポート	22
4-4	インポートされたユーザー証明書の確認.....	25

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-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

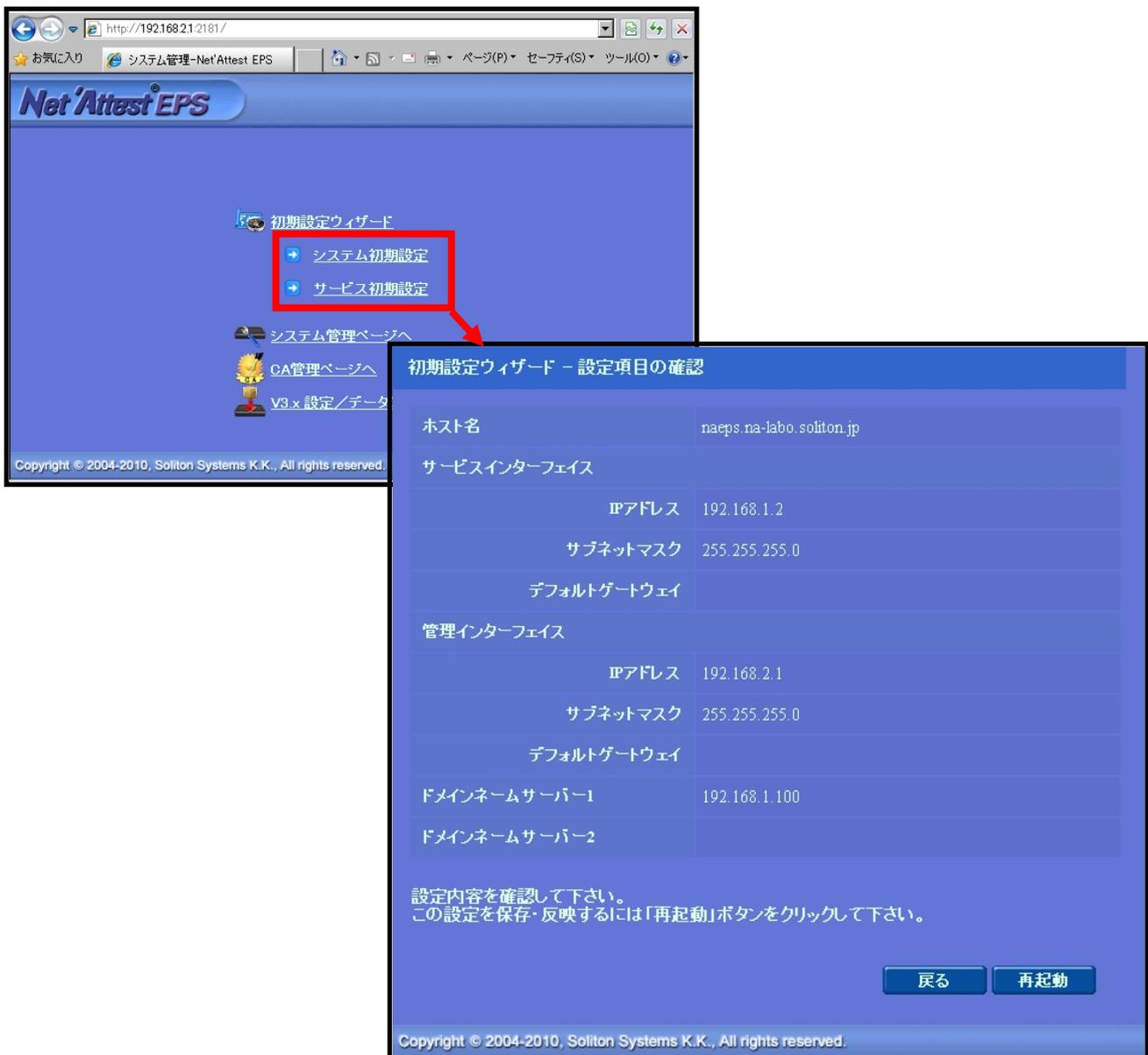
設定の流れ

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



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、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）

The image displays three overlapping screenshots of the Soliton initial setup wizard interface.

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: [空欄]

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

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。

The screenshot displays the Net Attest EPS WebGUI. The sidebar menu on the left has 'NAS/RADIUSクライアント' selected. The main area shows a table with columns for 'NAS/RADIUSクライアント名', 'IPアドレス', '説明', and 'タスク'. A red box highlights the '追加' (Add) button in the top right corner. Below the table, a configuration form for 'NAS/RADIUSクライアント設定' is shown, with the edit target set to 'ACERA800ST'. The form fields are: 'NAS/RADIUSクライアント名*' (ACERA800ST), a checked checkbox 'このNAS/RADIUSクライアントを有効にする', '説明' (スタンドアロン), 'IPアドレス*' (192.168.1.103), 'シークレット*' (masked with dots), and '所属するNASグループ' (dropdown menu).

【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。

The screenshots illustrate the following steps:

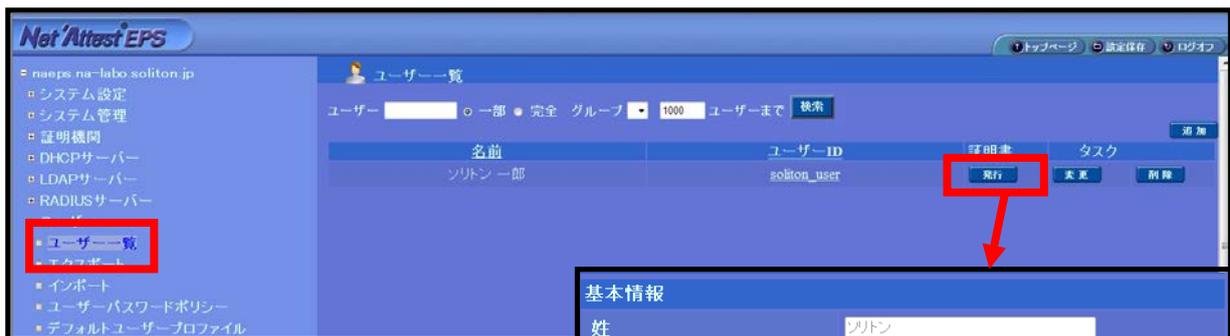
- Accessing the 'ユーザー一覧' (User List) page and clicking the '追加' (Add) button.
- Completing the 'ユーザー設定' (User Settings) form with the following details:
 - 姓 (Surname): ソリトン
 - 名 (Name): 一郎
 - E-Mail: [Empty]
 - 詳細情報 (Detailed Information): [Empty]
 - 認証情報 (Authentication Information):
 - ユーザーID (User ID): soliton_user
 - パスワード (Password): [Masked]
 - パスワード(確認) (Password Confirmation): [Masked]
 - 一時利用停止 (Temporary Suspension): [Unchecked]
 - グループ情報 (Group Information): [Empty]
- Clicking the 'OK' button to save the user.
- Returning to the 'ユーザー一覧' (User List) page, where the new user is listed in the table:

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

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】

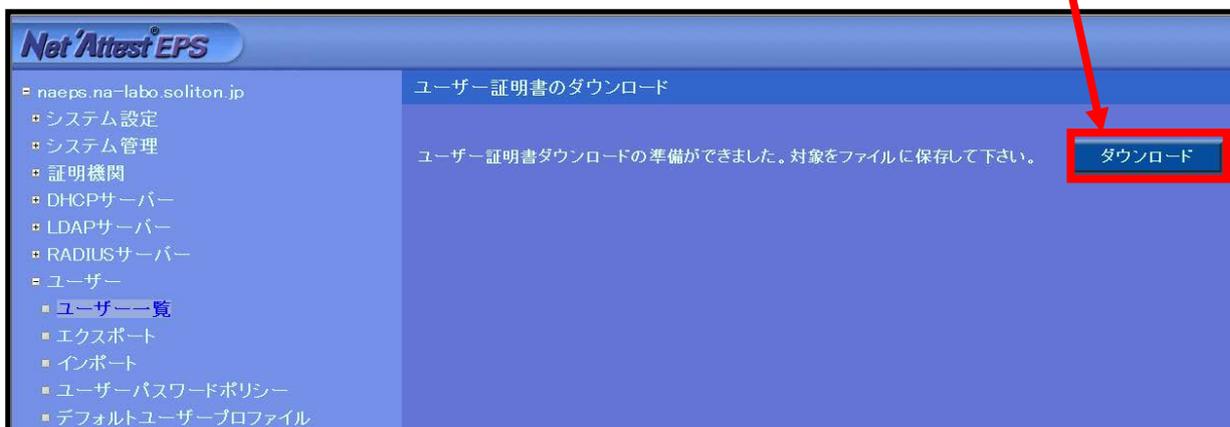
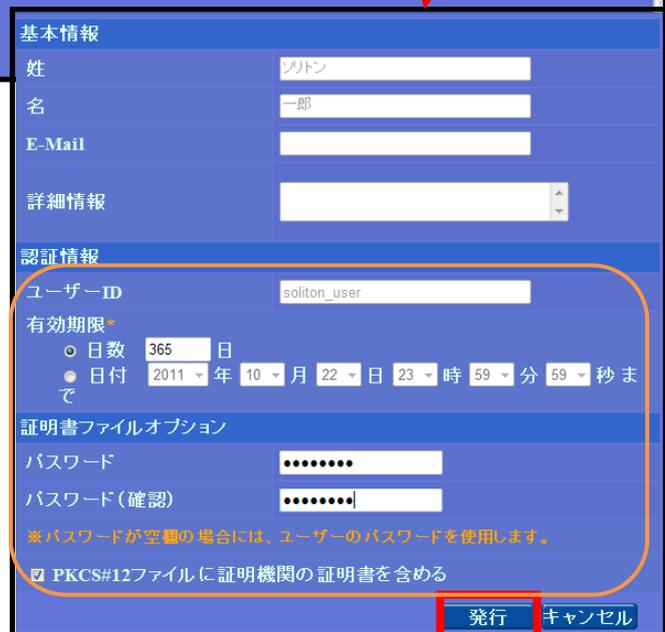
- ・ 365

【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)

保存
変更を適用して再起動

無線LAN1 セキュリティ設定 ESSID 1

設定のコピー ESSID 1 へ下記設定内容を コピー

設定

ESSID 有効 無効 ?

ESSID ?

VLAN ID ?

DTIMインターバル ?

ステルスモード 有効 無効 ?

any拒否 有効 無効 ?

無線セパレータ 有効 無効 ?

無線セパレータポリシー 通過 遮断 ?

無線セパレータ例外アドレス ?

MACアドレスフィルタリング 有効 無効 ?

対象MACアドレス ?

暗号化設定

暗号方式 ?

WEP設定

モード: Open Shared ?

キー ?

WPA固有設定

暗号化方式 TKIP AES ?

パスフレーズ ?

GTK更新間隔 ?

事前認証 有効 無効 ?

WPA, 802.1x共通設定

プライマリ認証サーバ ?

プライマリ認証サーバポート ?

プライマリ認証サーバクレデンシャル ?

セカンダリ認証サーバ ?

セカンダリ認証サーバポート ?

セカンダリ認証サーバクレデンシャル ?

- ・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 WPA2-Enterprise を選択しています。

なし
WEP
WPA-PSK
WPA2-Personal
WPA2-Enterprise
IEEE802.1x

- ・ 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固有設定	
暗号化方式	<input type="radio"/> TKIP <input checked="" type="radio"/> AES
パスフレーズ	TESTSAMPLE
GTK更新間隔	7200
事前認証	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効

- ・ 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。

WPA , 802.1x共通設定	
プライマリ認証サーバ	192.168.1.2
プライマリ認証サーバポート	1812
プライマリ認証サーバクレデンシャル	se{soliton
セカンダリ認証サーバ	
セカンダリ認証サーバポート	1812
セカンダリ認証サーバクレデンシャル	

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。

保存
変更を適用して再起動

無線LAN1 セキュリティ設定 ESSID 1

設定のコピー ESSID 1 ▼ へ下記設定内容を コピー

設定 有効 無効

ESSID

VLAN ID

DTIMインターバル

ステルスモード 有効 無効

any拒否 有効 無効

無線セパレータ 有効 無効

無線セパレータポリシー 通過 遮断

無線セパレータ例外アドレス

MACアドレスフィルタリング 有効 無効

対象MACアドレス

暗号化設定

暗号方式

WEP設定

モード: Open Shared

キー

WPA固有設定

暗号化方式 TKIP AES

パスフレーズ

GTK更新間隔

事前認証 有効 無効

WPA, 802.1x共通設定

プライマリ認証サーバ

プライマリ認証サーバポート

プライマリ認証サーバクレデンシャル

セカンダリ認証サーバ

セカンダリ認証サーバポート

セカンダリ認証サーバクレデンシャル

4 クライアント PC の設定

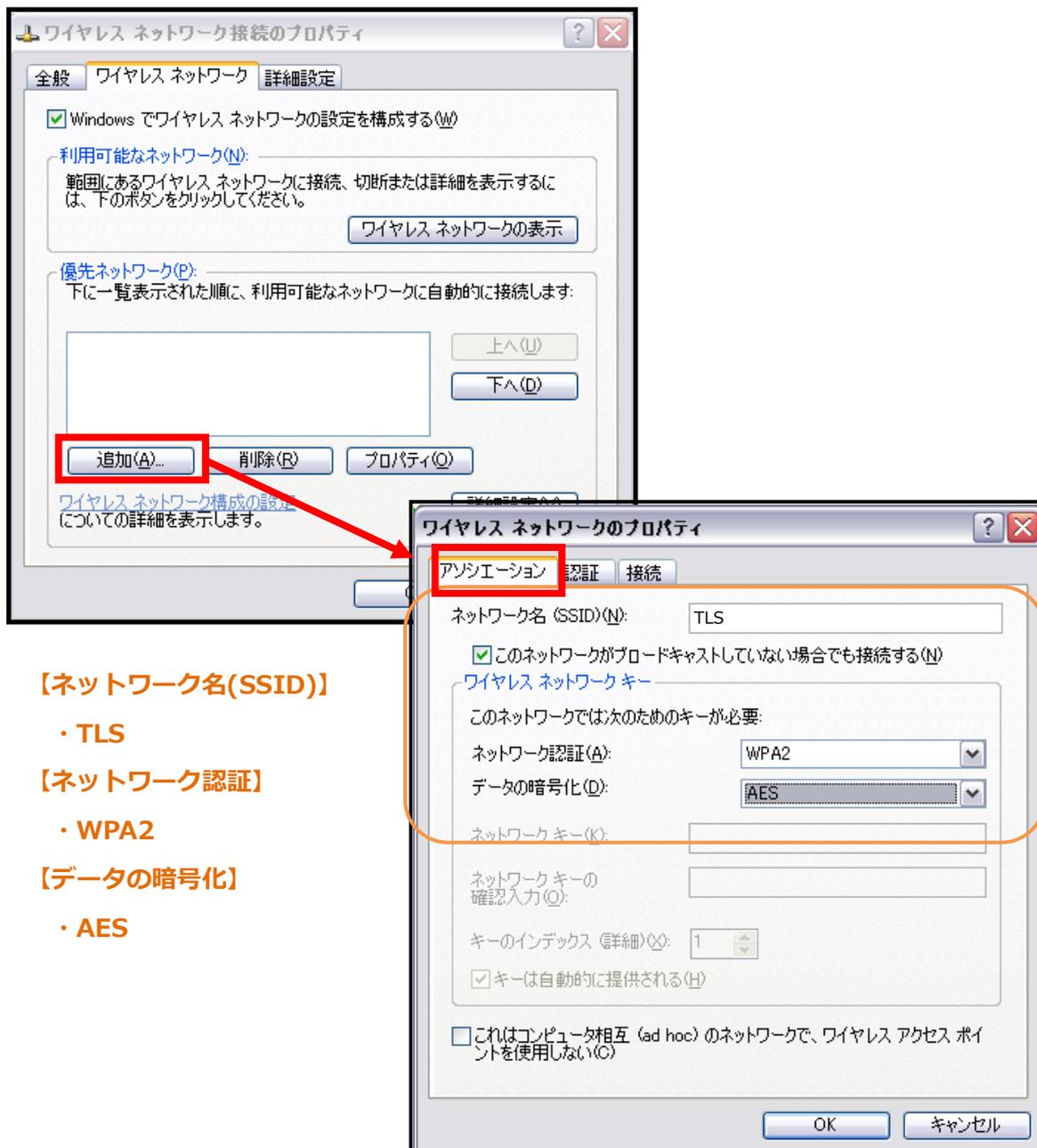
4-1 クライアント PC 設定の流れ

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

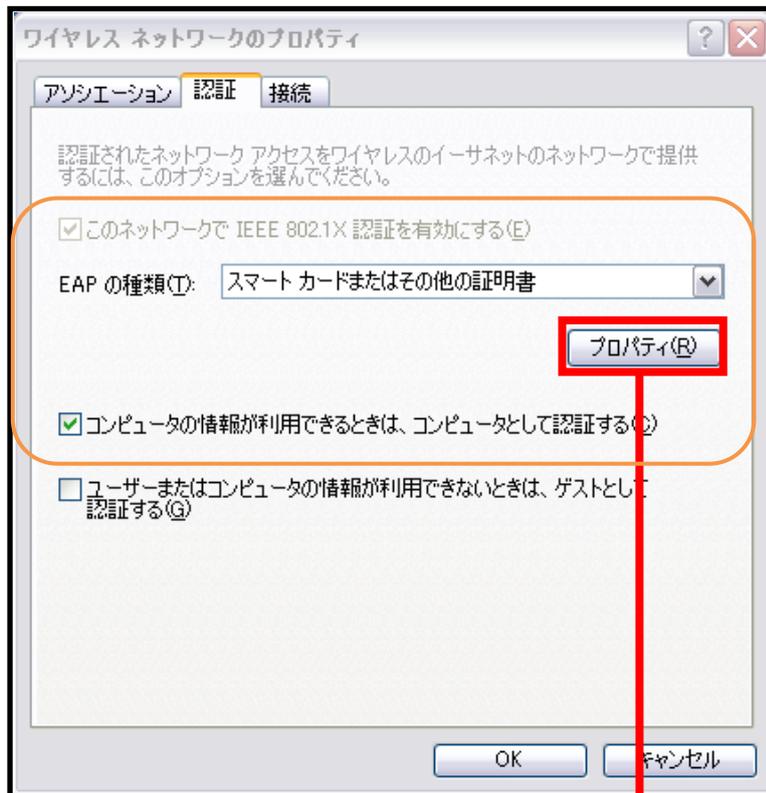
【ネットワーク認証】

- ・ WPA2

【データの暗号化】

- ・ AES

次ページへ

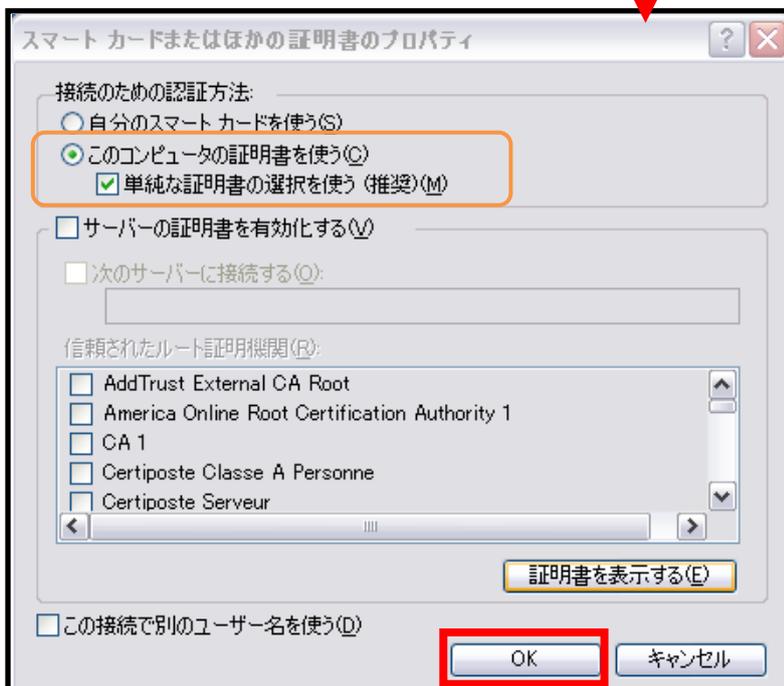


【EAP の種類】

- ・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。



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。

【パスワード】

・ password

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)

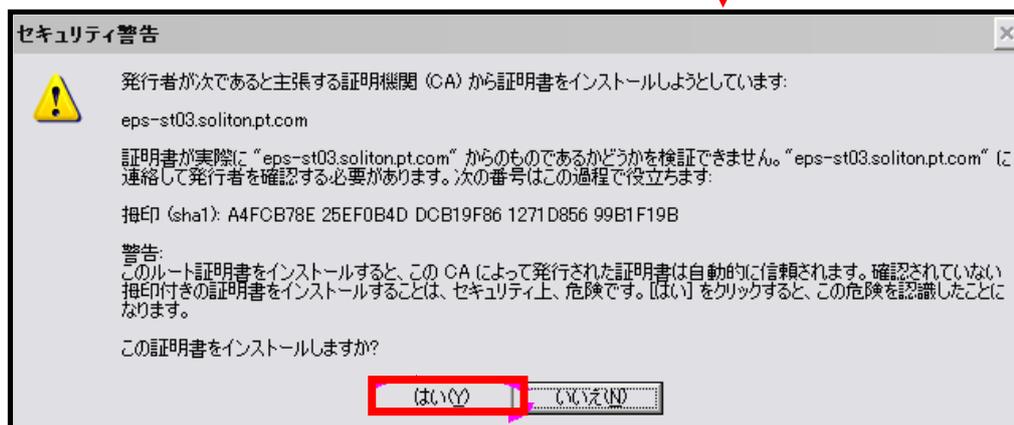
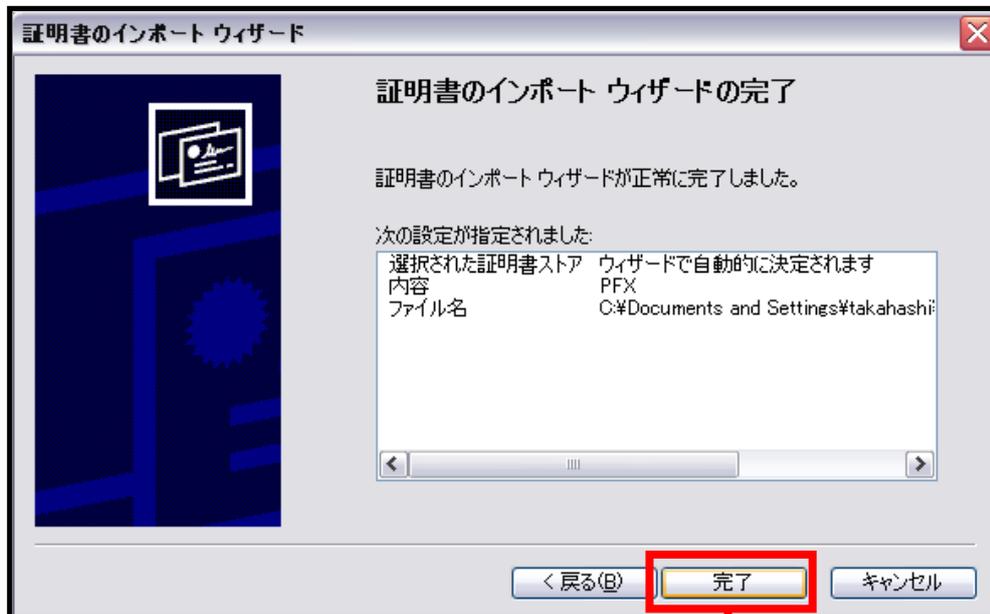
証明書ストア:
参照(R)...

< 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

次ページへ



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。

