NetAttest EPS 設定例

連携機器：

BUFFALO WAPS-APG600H

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 BUFFALO 社製 無線 LAN アクセスポイント WAPS-APG600H の 802.1x 環境での接続について、設定例を示したものです。

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ー出力、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ー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

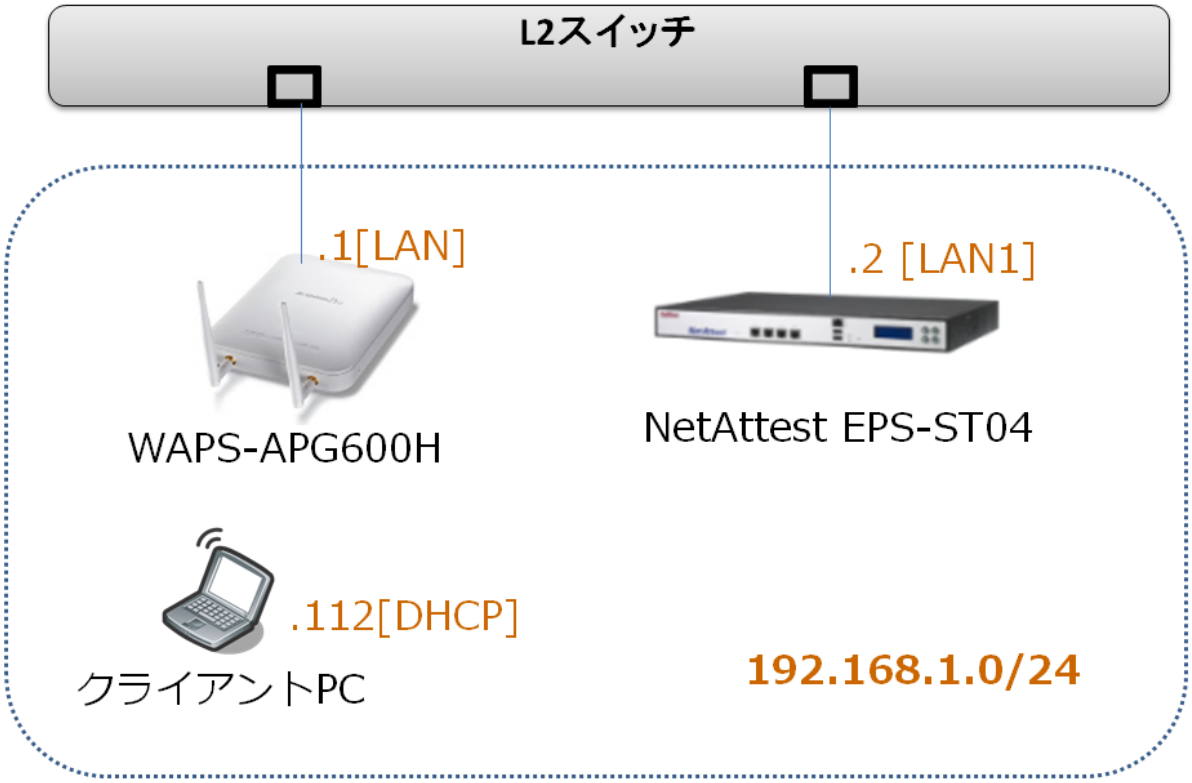
本書は、当社での検証に基づき、NetAttest EPS 及び WAPS-APG600H の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

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
・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 (認証サーバー)	Soliton Systems	NetAttest EPS ST-04	Ver. 4.6.0
Authenticator (認証機器)	BUFFALO	WAPS-APG600H	Ver. 1.8.4
Client PC / Supplicant (802.1x クライアント)	Panasonic	Let's note CF-SX2	Windows 7 SP1 Windows 標準サプリカント

1-2-2 認証方式

IEEE 802.1x EAP-TLS

1-2-3 ネットワーク設定

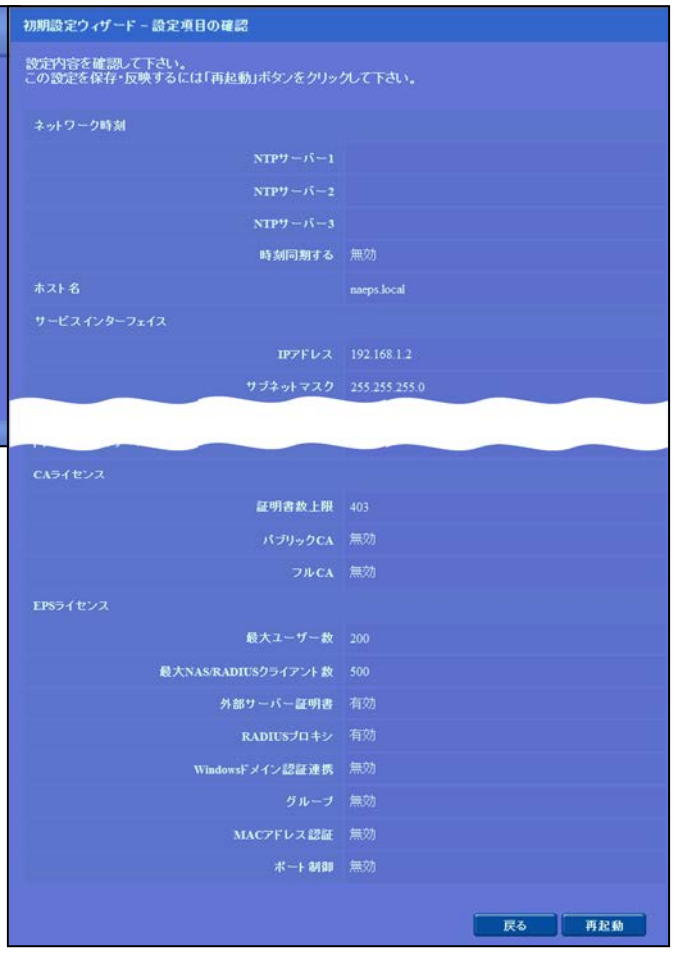
	EPS-ST04	WAPS-APG600H	Client PC
IP アドレス	192.168.1.2/24	192.168.1.1/24	192.168.1.112/24 (DHCP)
RADIUS port (Authentication)	UDP 1812		–
RADIUS port (Accounting)	UDP 1813		–
RADIUS Secret (Key)	secret		–

2 NetAttest EPS の設定

2-1 システム初期設定ウィザードの実行

http://192.168.2.1:2181(LAN2 デフォルト)にアクセスしシステム初期設定ウィザードを使用して、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



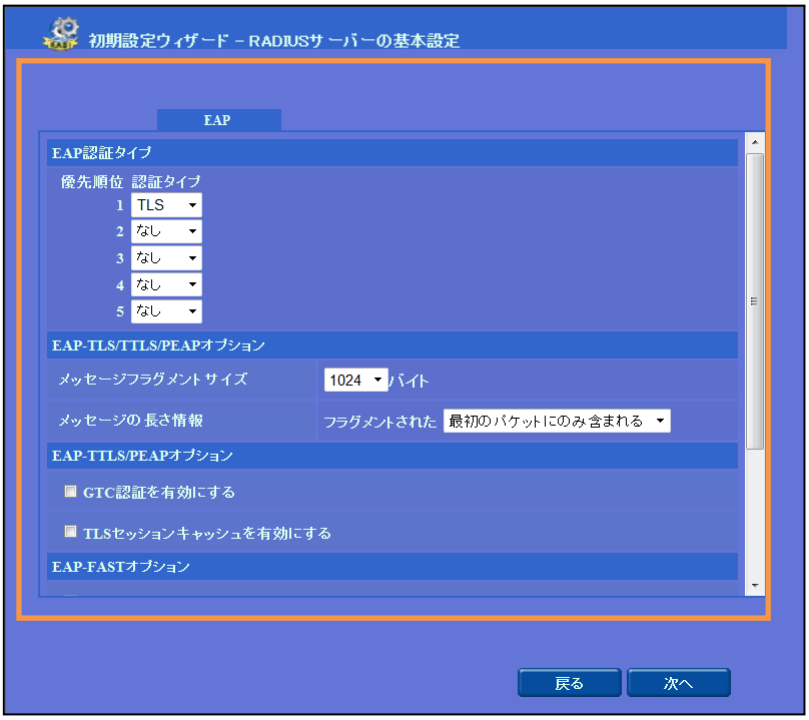
2-2 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

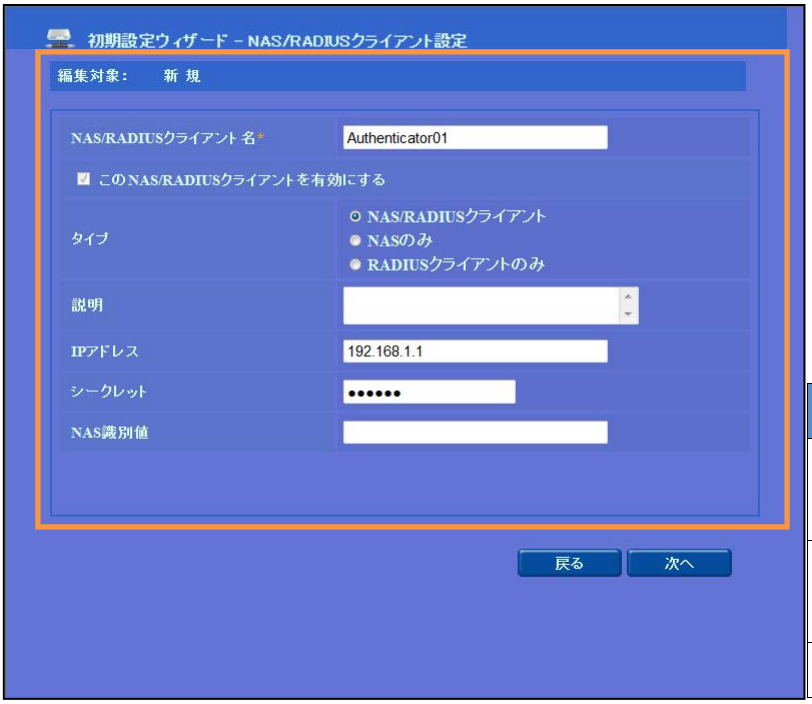
本手順書では値を記載しているもの以外はすべてデフォルト設定で行いました。

- 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

項目	値
CA 名	TestCA



項目	値
認証タイプ	TLS



項目	値
NAS/RADIUS クライアント名	Authenticator01
IP アドレス (Authenticator)	192.168.1.1
シークレット	secret

2-3 認証ユーザーの追加登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

「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。

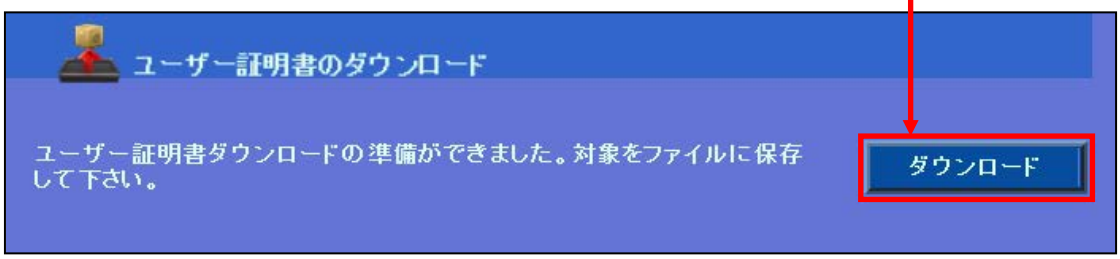
項目	値
姓	user01
ユーザーID	user01
パスワード	password

2-4 クライアント証明書の発行

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クライアント証明書を発行します。(クライアント証明書は user01_02.p12 という名前で保存)

項目	値
証明書有効期限	365
PKCS#12 ファイルに証明機関の証明書を含める	チェック有



3 BUFFALO WAPS-APG600H

3-1 BUFFALO WAPS-APG600H 設定の流れ

BUFFALO 社製無線アクセスポイント WAPS-APG600H を設定するためには、専用の設定・管理ツール「AirStation Admin Tools」やシリアルコンソールを利用する方法、管理 WebGUI を利用する方法などが存在しますが、本書では、シリアルコンソールを利用して WAPS-APG600H に IP アドレスを設定し、その後、管理 WebGUI から各種設定を実施する方法を紹介します。

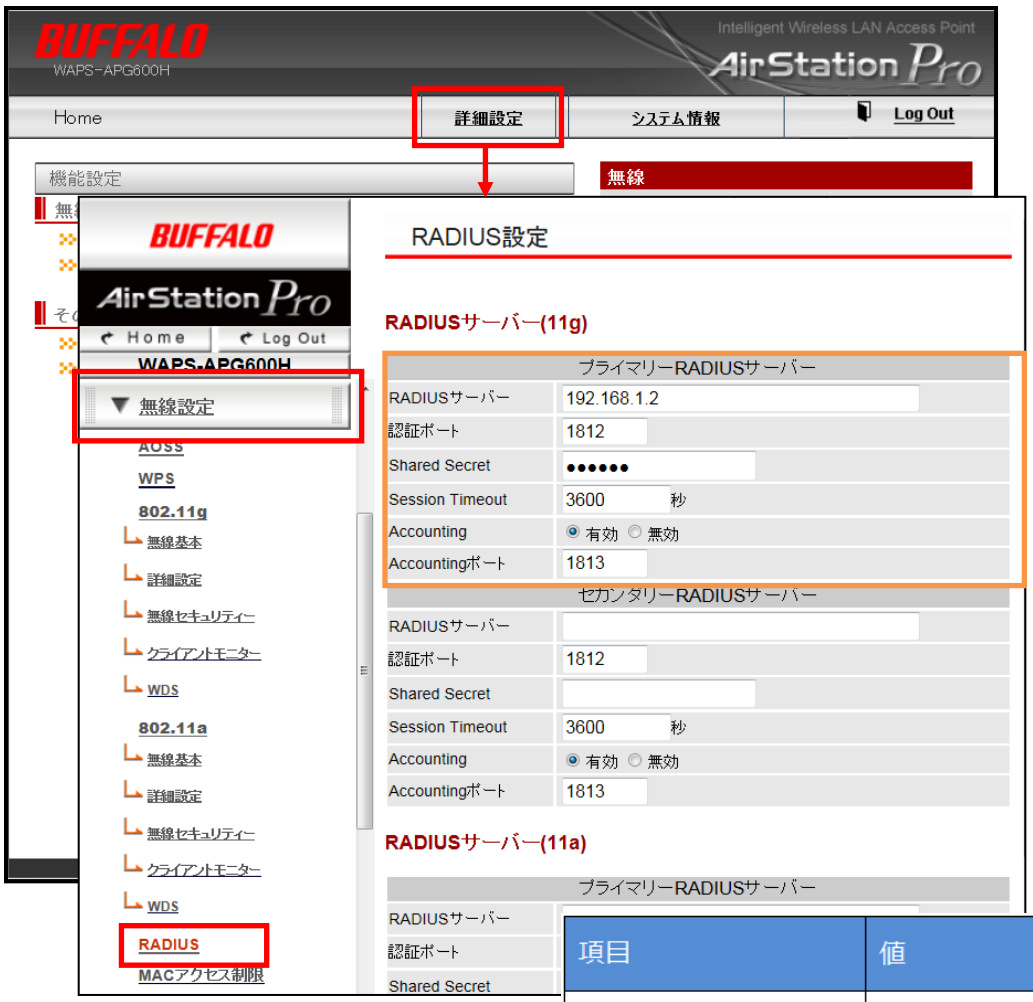
設定の流れ

1. RADIUS サーバーの登録
2. 無線基本設定
3. 無線セキュリティー設定

3-2 RADIUS サーバーの登録

RADIUS サーバーの設定をします。

TOP ページの[詳細設定]リンクをクリックします。[無線設定]メニューを展開し、[RADIUS]リンクをクリックします。右側に RADIUS 設定項目が表示されますので、プライマリーサーバーの項目に値を入力します。



項目	値
RADIUS サーバー	192.168.1.2
認証ポート	1812
Shared secret	secret
Accounting	有効にチェック
Accounting ポート	1813

3-3 無線基本設定

無線 LAN 端末が接続する無線ネットワークの名前を設定します。

左側のメニューから[無線設定]を展開し、802.11g の[無線基本]リンクをクリックします。

右側の無線基本(11g)にて設定します。

項目	値
有線 LAN	有効にチェック
SSID	WAPS_APG600H_G

3-4 無線セキュリティー設定

「無線セキュリティー設定」では、認証方法と無線の暗号化方式を設定します。

左側のメニューから[無線設定]を選択し、802.11g の[無線セキュリティー]をクリックします。

右側の無線セキュリティー(11g)にて設定します。

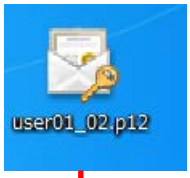
項目	値
認証方式	WPA-EAP
WPA タイプ	WPA/WPA2 mixed mode-EAP
暗号化方式	TKIP/AES mixed mode
追加認証	追加認証を行わない

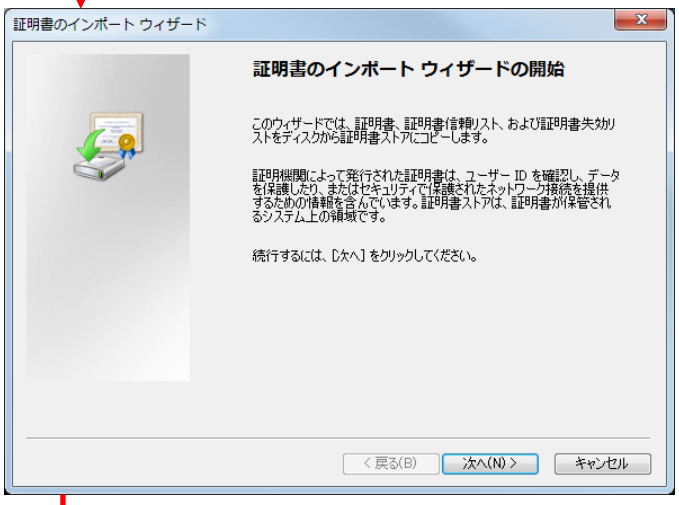
NetAttest EPS による RADIUS 認証を行うためには、「EAP」がついている方式を選択します。また、選択した認証方式により設定可能な[無線の暗号化]も決定されます。

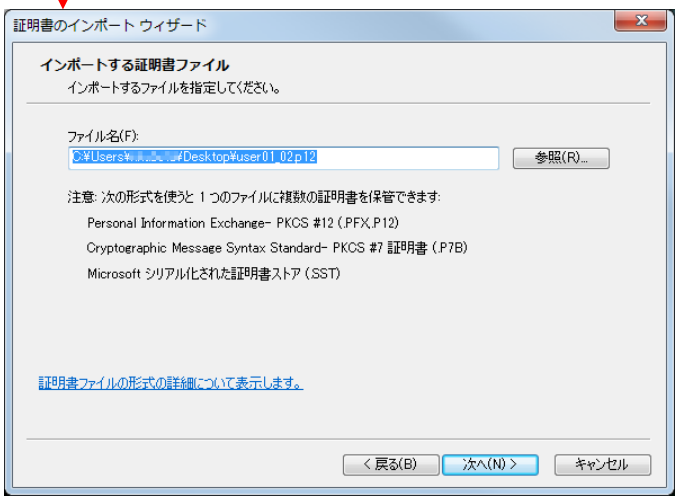
4 無線 LAN クライアントの設定

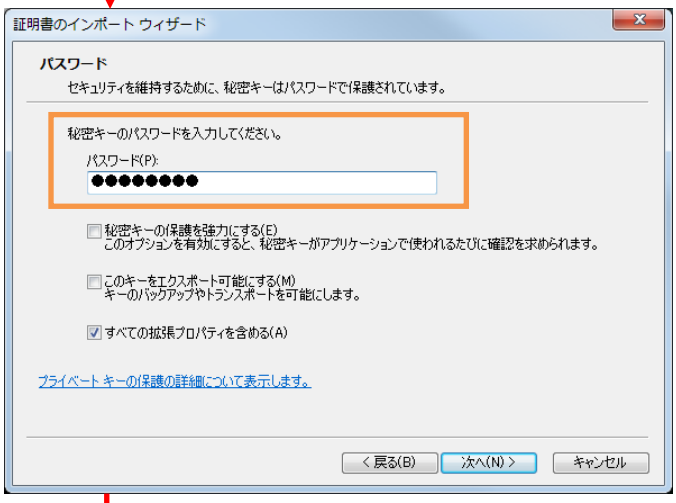
4-1 Windows7 へのデジタル証明書のインストール

PC にクライアント証明書をインストールします。ダウンロードしておいたクライアント証明書(user01_02.p12)をダブルクリックすると証明書インポートウィザードが実行されます。



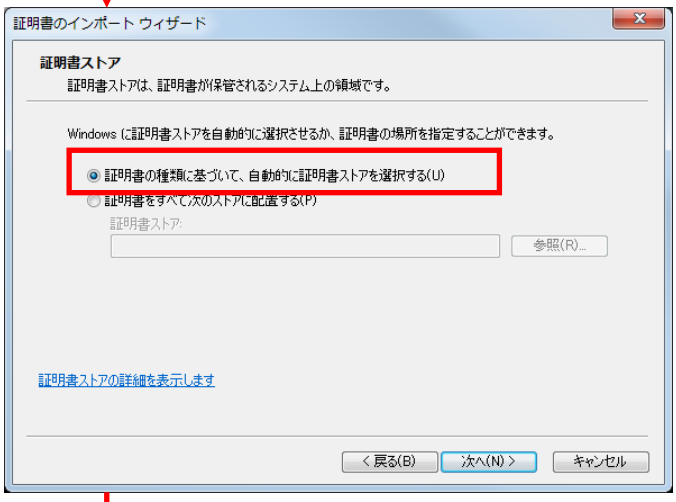


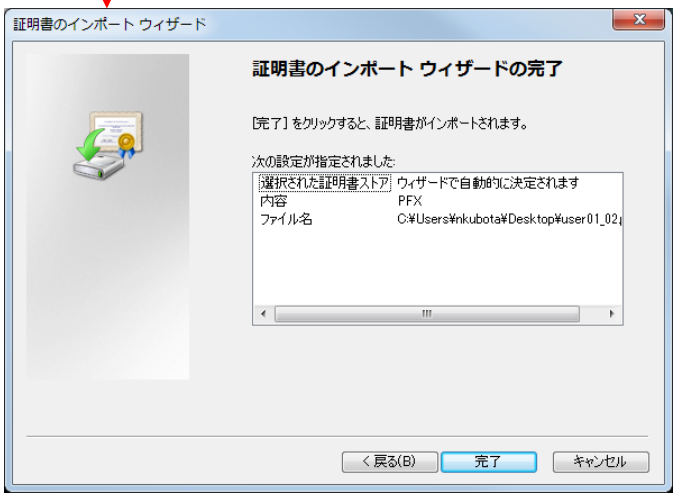




項目	値
パスワード	証明書を発行したユーザーのパスワード、もしくは証明書発行時に設定した証明書ファイルオプションのパスワード

iPhone 構成ユーティリティを利用し iOS デバイスにデジタル証明書をインストールする場合は、【このキーをエクスポート可能にする】チェックを入れる必要があります。

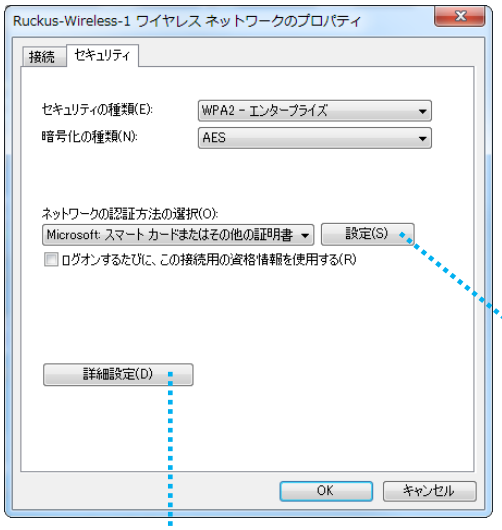




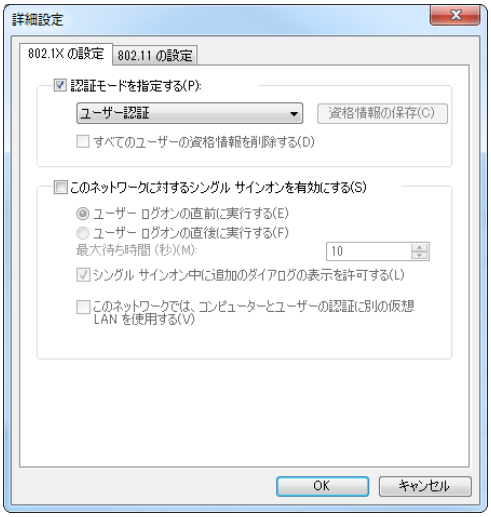
4-2 サプリカントの設定

Windows 標準サプリカントで TLS の設定を行います。

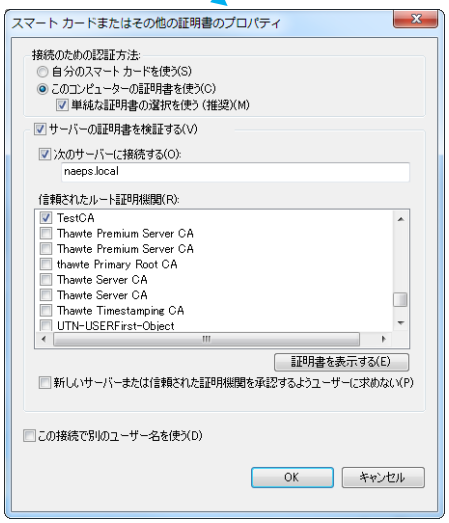
[ワイヤレスネットワークのプロパティ]の「セキュリティ」タブから以下の設定を行います。



項目	値
セキュリティの種類	WPA2-エンタープライズ
暗号化の種類	AES
ネットワーク認証の・・	Microsoft スマートカード・・



項目	値
認証モードを指定する	ユーザー認証



項目	値
接続のための認証方法	
- このコンピューターの・・	On
- 単純な証明書の選択・・・	On
サーバー証明書の検証をする	On
次のサーバーに接続する	naeps.local
信頼されたルート証明機関	TestCA

改訂履歴

日付	版	改訂内容
2013/11/13	1.0	初版作成