Net'Attest EPS 設定例

連携機器：

Cisco Aironet1140

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

本書は弊社 CA 内蔵 RADIUS サーバプライアンス Net'Attest EPS と Cisco Systems Aironet1140 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 アドレスの設定などの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
%, $, >	一般ユーザのプロンプトを表します。
#	特権ユーザ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

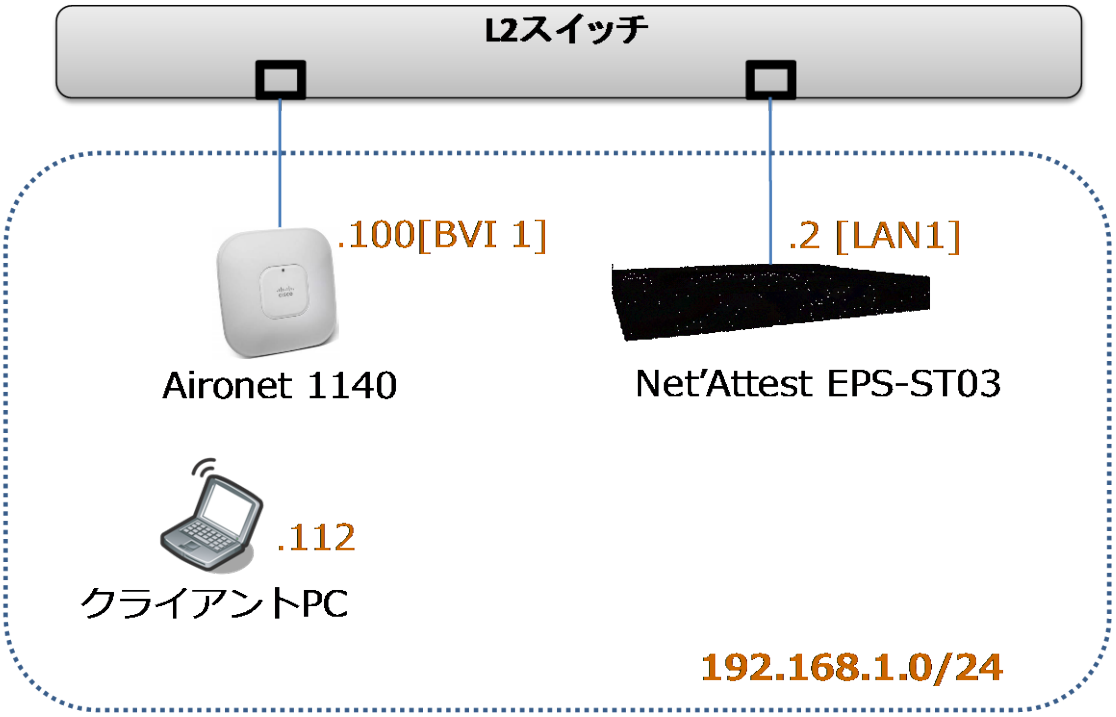
本書は、当社での検証に基づき、Net'Attest EPS 及び Aironet1140 の操作方法を記載したものです。すべての環境での動作を保証するものではありません。

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
・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、
Net'Attest EPS-ST03のDHCPサーバから払い出す



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)	Soliton Systems	Net'Attest EPS ST-03	Ver. 4.0.5
Authenticator (認証機器)	Cisco Systems	Aironet 1140	Ver. 12.4(21a)JA1
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	Aironet 1140	Client PC
IP アドレス	192.168.1.2/24	192.168.1.100/24	192.168.1.112 (DHCP)
RADIUS port (Authentication)	UDP 1812（※1）		–
RADIUS port (Accounting)	UDP 1813（※1）		–
RADIUS Secret (Key)	soliton		–

（※1）Aironet1140 は Web 設定の場合、UDP1645（Authentication）、UDP1646（Accounting）がデフォルト値になりますので変更が必要です

2 Net'Attest EPS

2-1 Net'Attest EPS 設定の流れ

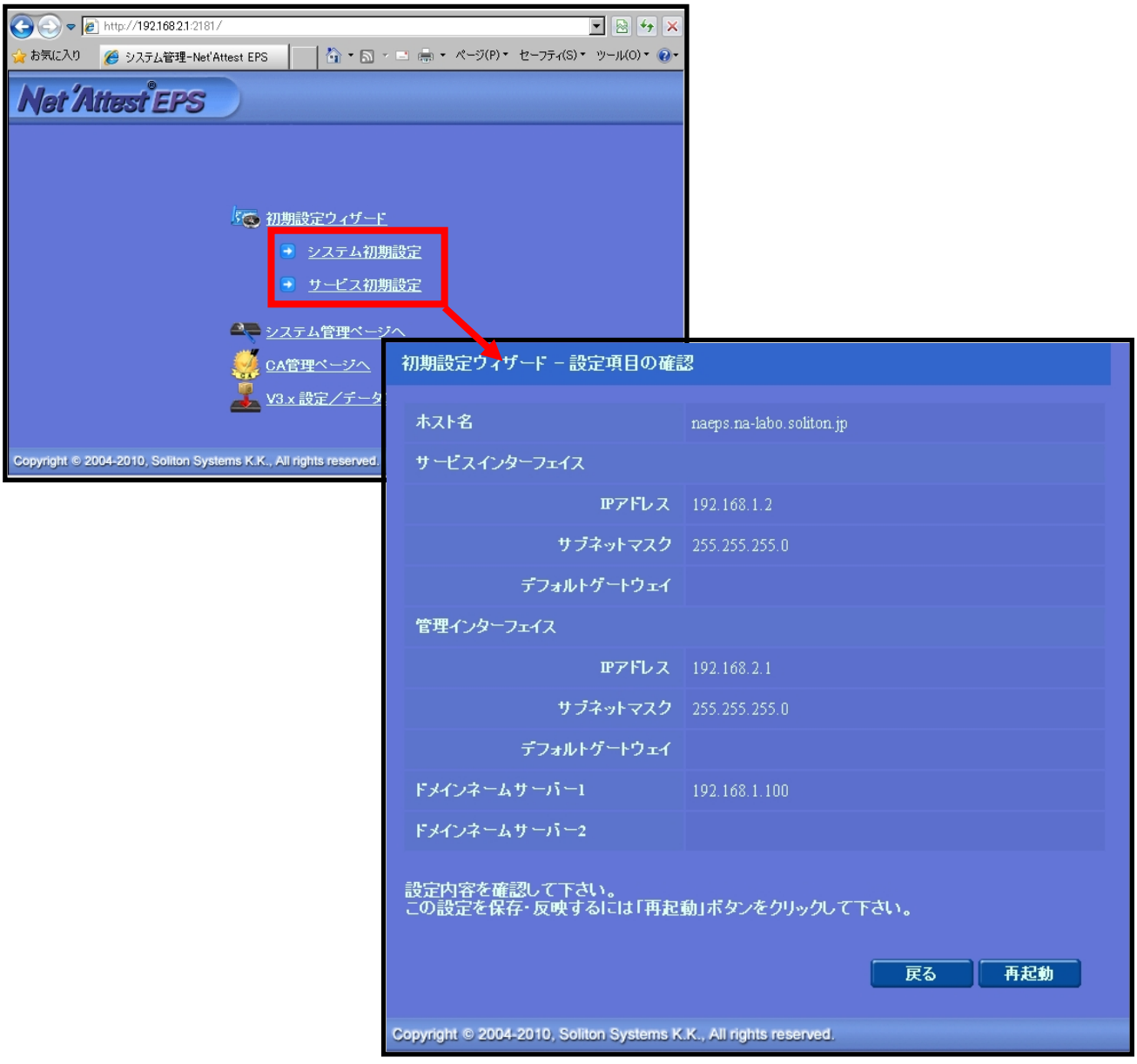
設定の流れ

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。

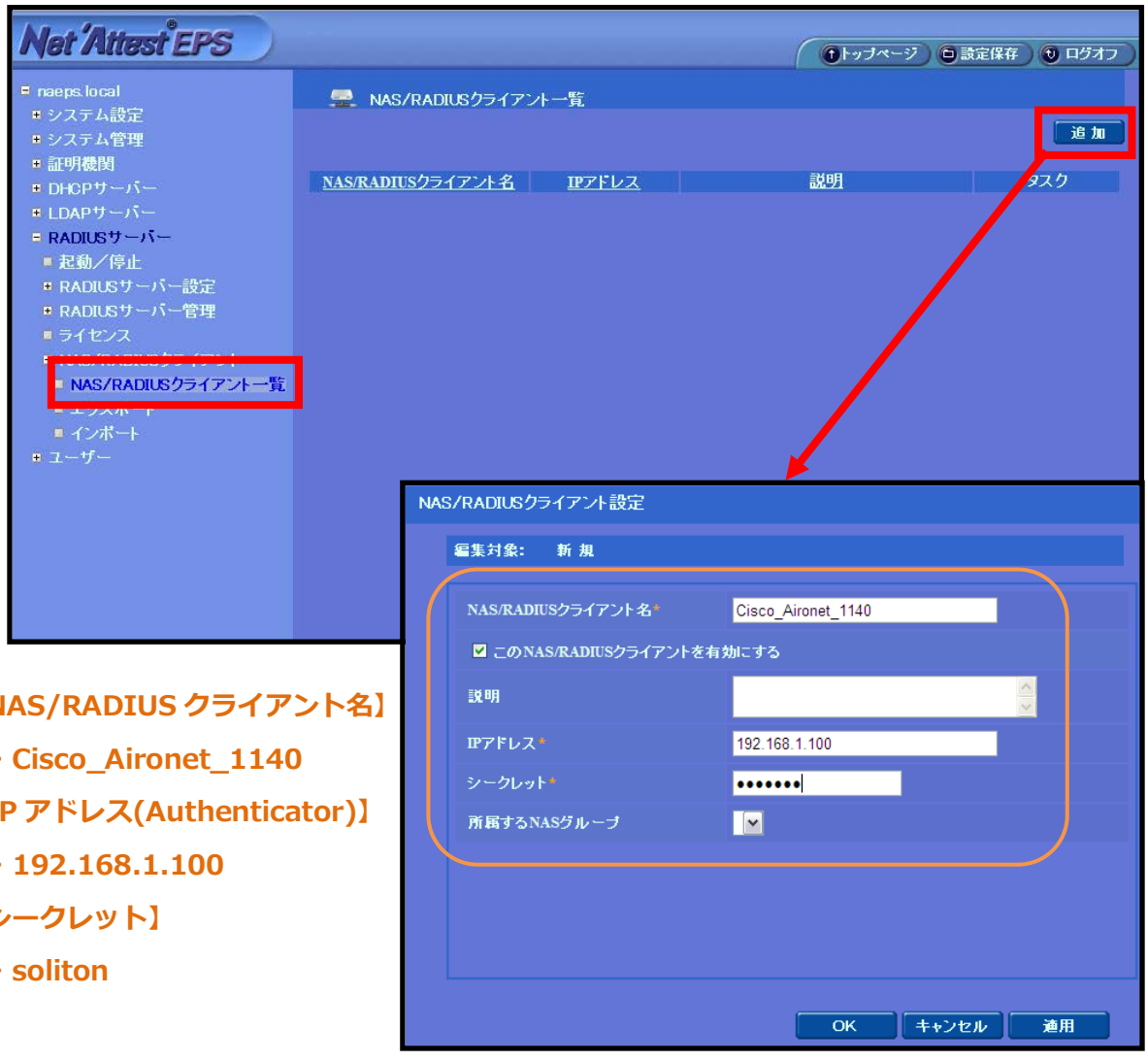
本書では、黒文字の項目のみ、設定しました。

- CA 構築
- LDAP データベースの設定
- RADIUS サーバの基本設定（全般）
- RADIUS サーバの基本設定（EAP）
- RADIUS サーバの基本設定（証明書検証）
- NAS/RADIUS クライアント設定

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】

・Cisco_Aironet_1140

【IP アドレス(Authenticator)】

・192.168.1.100

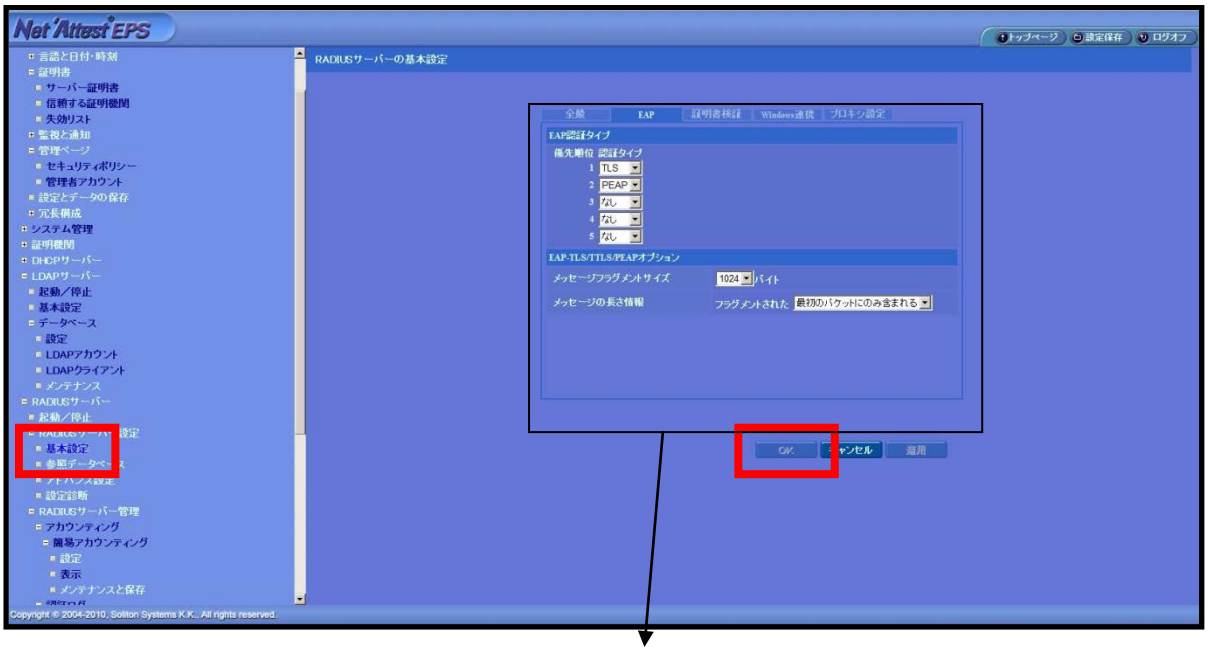
【シークレット】

・soliton

2-5 RADIUS サーバ基本設定

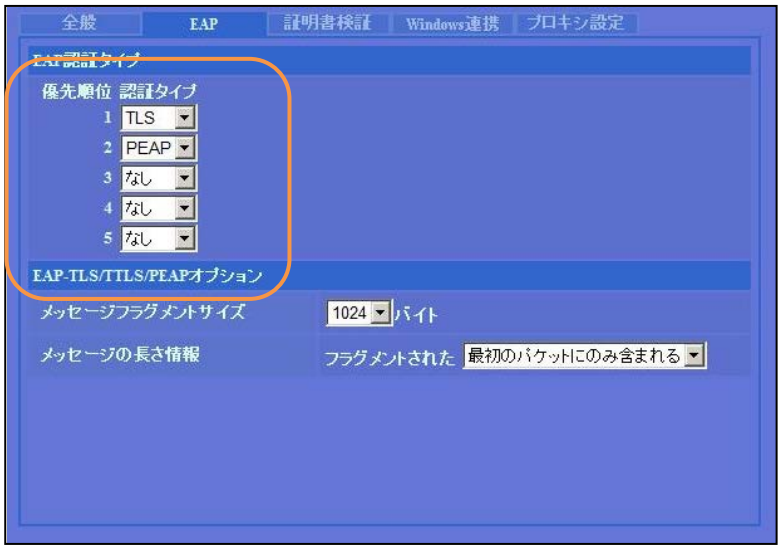
WebGUI より、RADIUS サーバの基本設定を行います。

「RADIUS サーバ」→「RADIUS サーバ設定」→「基本設定」→「EAP」から設定を行います。



【優先順位　認証タイプ】

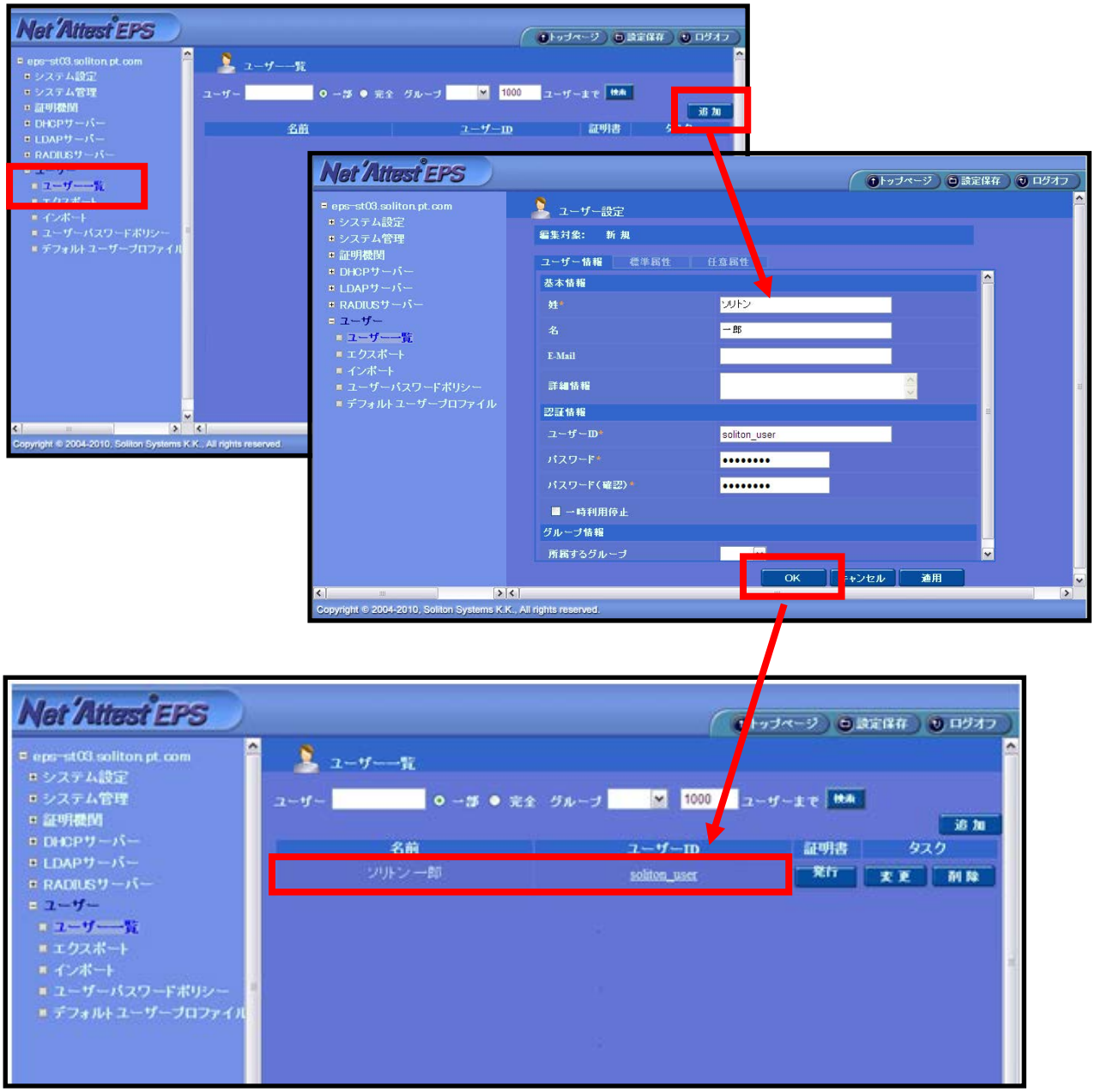
・1)TLS



2-6 ユーザーの登録

WebGUI より、ユーザー登録を行います。

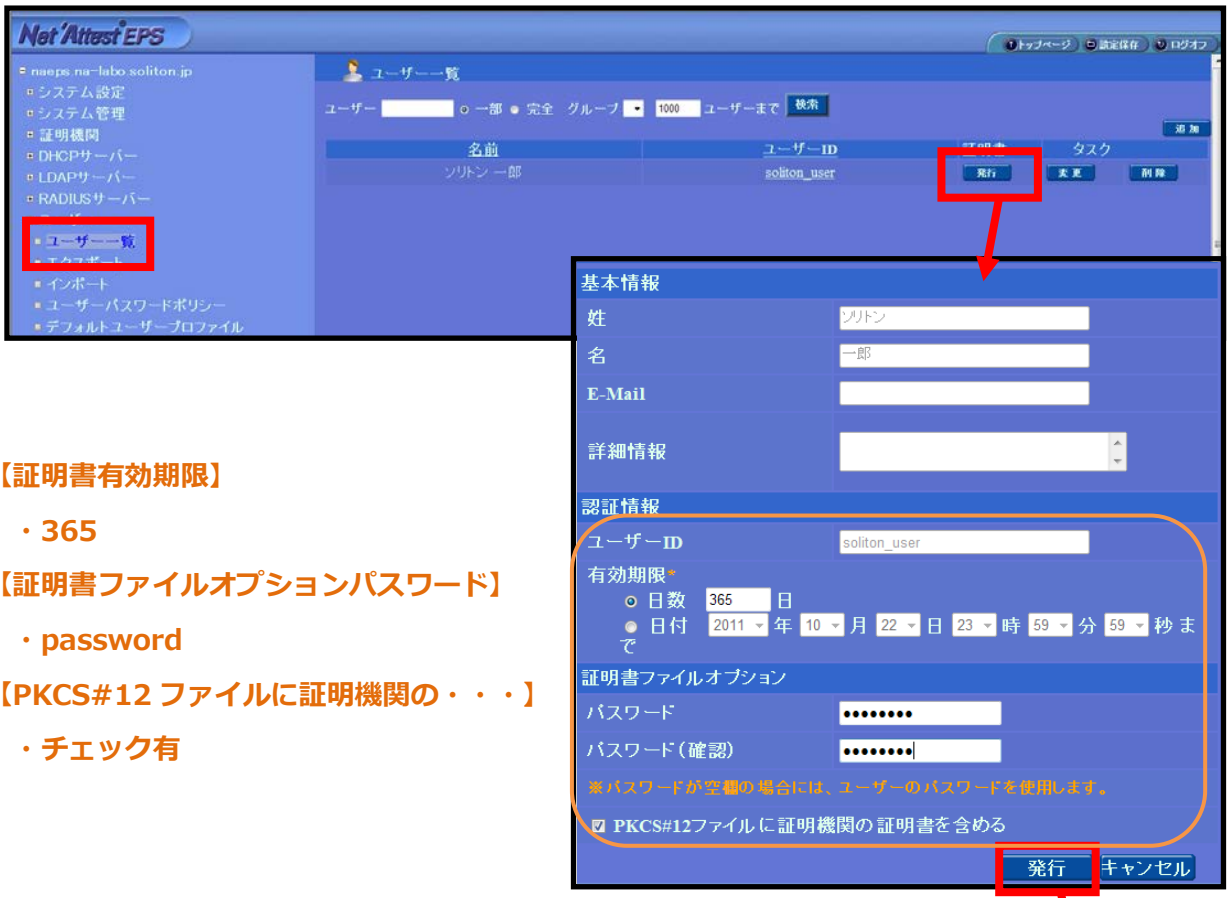
「ユーザー」→「ユーザー一覧」から、『追加』ボタンでユーザー登録を始めます。



2-7 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】

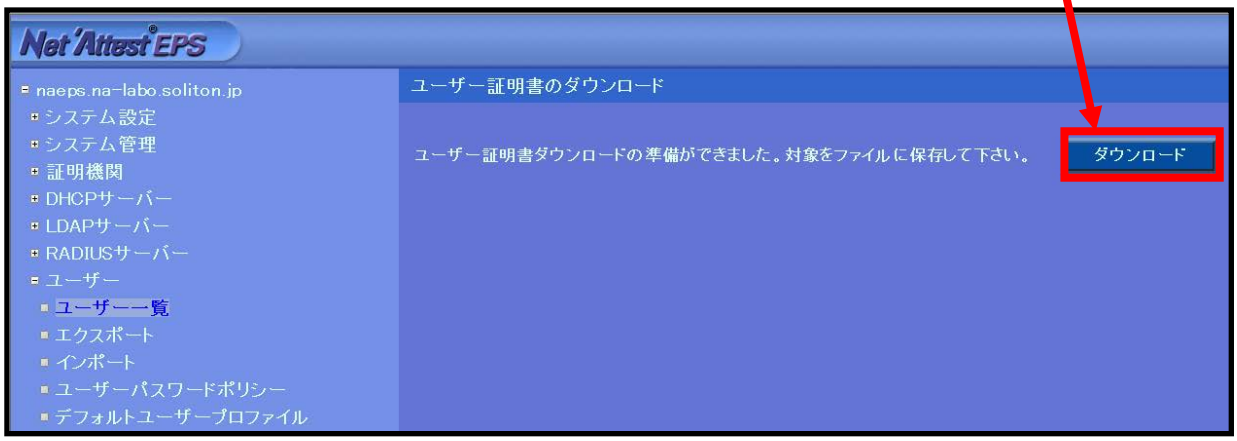
・365

【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 Cisco Aironet 1140

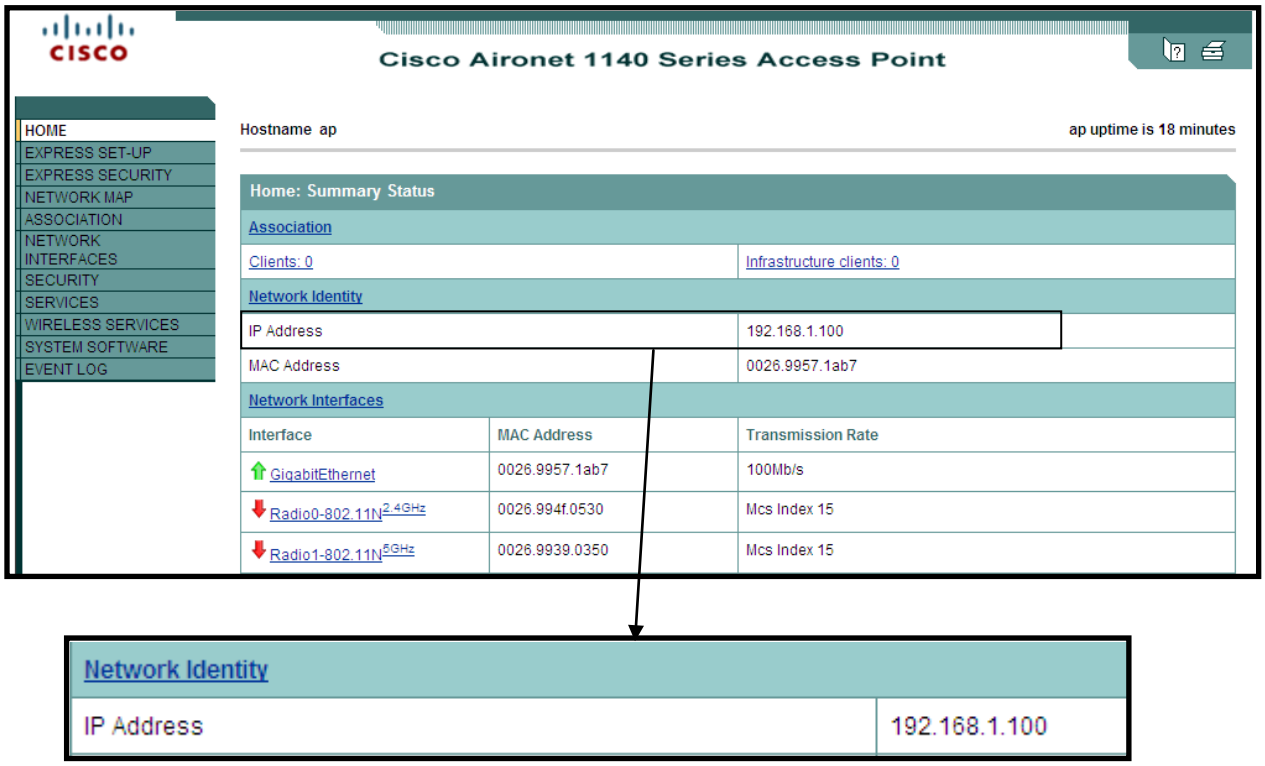
3-1 Cisco Aironet 1140 設定の流れ

設定の流れ

1. SSID、無線セキュリティ、RADIUS サーバなどの設定（Express Security）
2. RADIUS 通信のポート番号変更（Server Manager）
3. 無線 Interfaces の有効化（Network Interfaces）

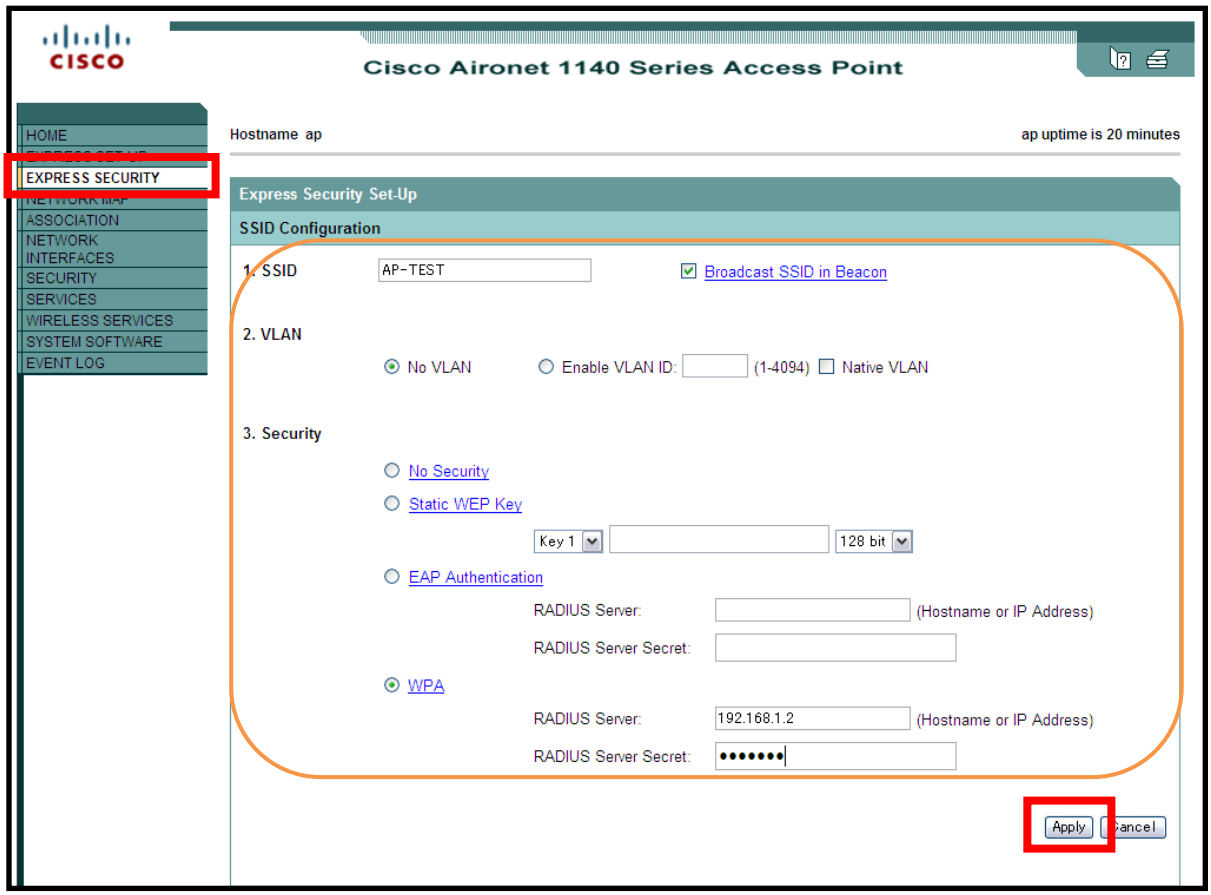
3-2 IP アドレスの確認

初期設定にて、インターフェース（BVI 1）の IP アドレスは、下記のように設定しています。



3-3 SSID、無線セキュリティ、RADIUS サーバの設定

WebGUI より、Express Security 設定にて、SSID、無線セキュリティ、RADIUS サーバの設定を行います。



【SSID】

・AP－TEST

【Broadcast SSID in Beacon】

・チェック有

【VLAN】

・No VLAN　チェック

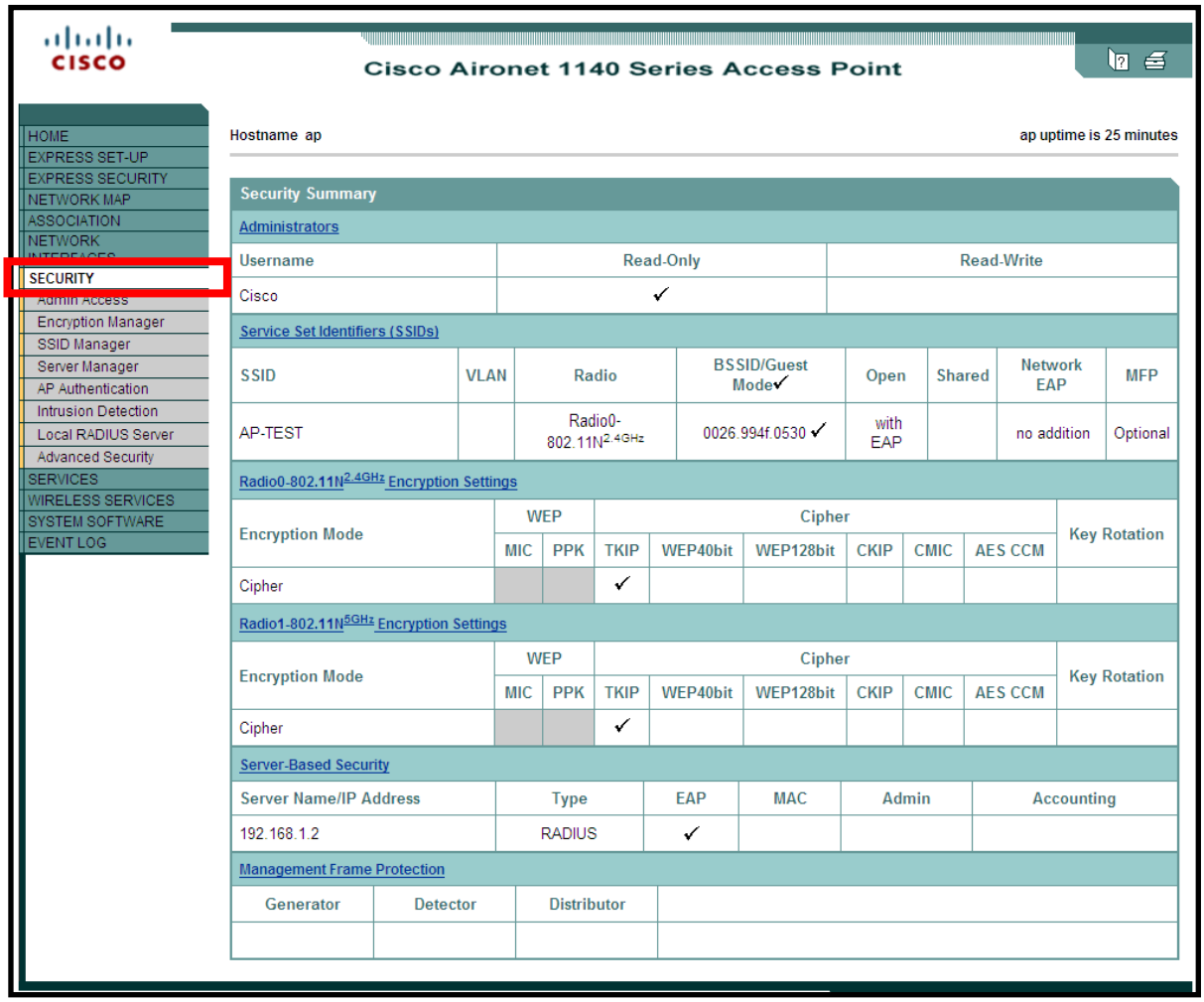
【WPA】

・チェック有

・[RADIUS Server]　192.168.1.2

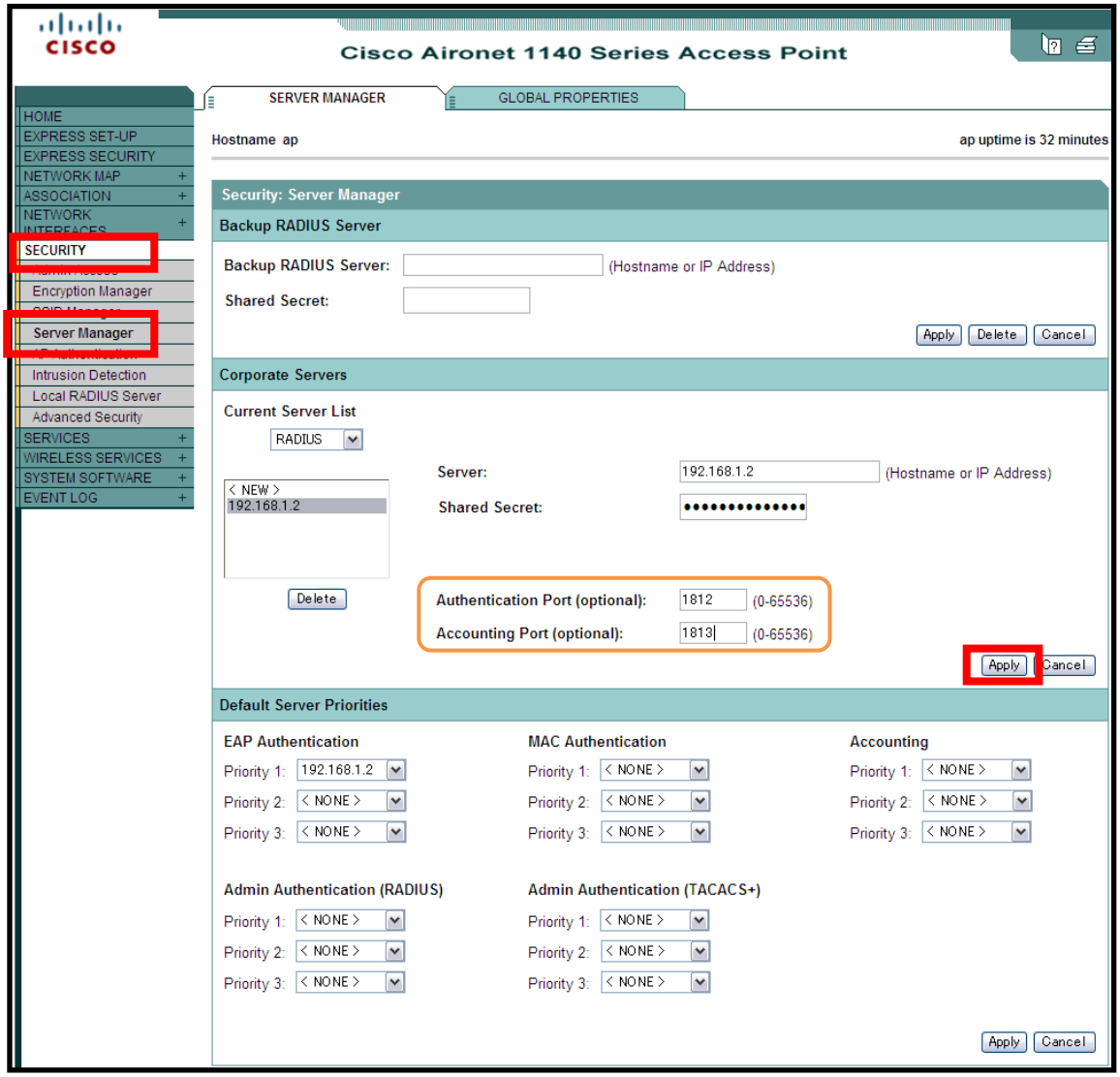
・[RADIUS Server Secret]　soliton

設定確認


Cisco Aironet 1140 Series Access Point
HOME
EXPRESS SET-UP
EXPRESS SECURITY
NETWORK MAP
ASSOCIATION
NETWORK
SECURITY
Admin Access
Encryption Manager
SSID Manager
Server Manager
AP Authentication
Intrusion Detection
Local RADIUS Server
Advanced Security
SERVICES
WIRELESS SERVICES
SYSTEM SOFTWARE
EVENT LOG
Hostname ap
ap uptime is 25 minutes
Security Summary
Administrators
Username
Read-Only
Read-Write
Cisco
✓
Service Set Identifiers (SSIDs)
SSID
VLAN
Radio
BSSID/Guest Mode
Open
Shared
Network EAP
MFP
AP-TEST
Radio0-802.11N2.4GHz
0026.994f.0530 ✓
with EAP
no addition
Optional
Radio0-802.11N2.4GHz Encryption Settings
Encryption Mode
WEP
Cipher
Key Rotation
MIC
PPK
TKIP
WEP40bit
WEP128bit
CKIP
CMIC
AES CCM
Cipher
✓
Radio1-802.11N5GHz Encryption Settings
Encryption Mode
WEP
Cipher
Key Rotation
MIC
PPK
TKIP
WEP40bit
WEP128bit
CKIP
CMIC
AES CCM
Cipher
✓
Server-Based Security
Server Name/IP Address
Type
EAP
MAC
Admin
Accounting
192.168.1.2
RADIUS
✓
Management Frame Protection
Generator
Detector
Distributor

3-4 RADIUS 通信ポート番号の変更

Express Security で設定したプロファイルは、RADIUS サーバとの通信で使用するポート番号が 1645（Auth）、1646（Accounting）になっているため、変更します。



【Authentication Port】

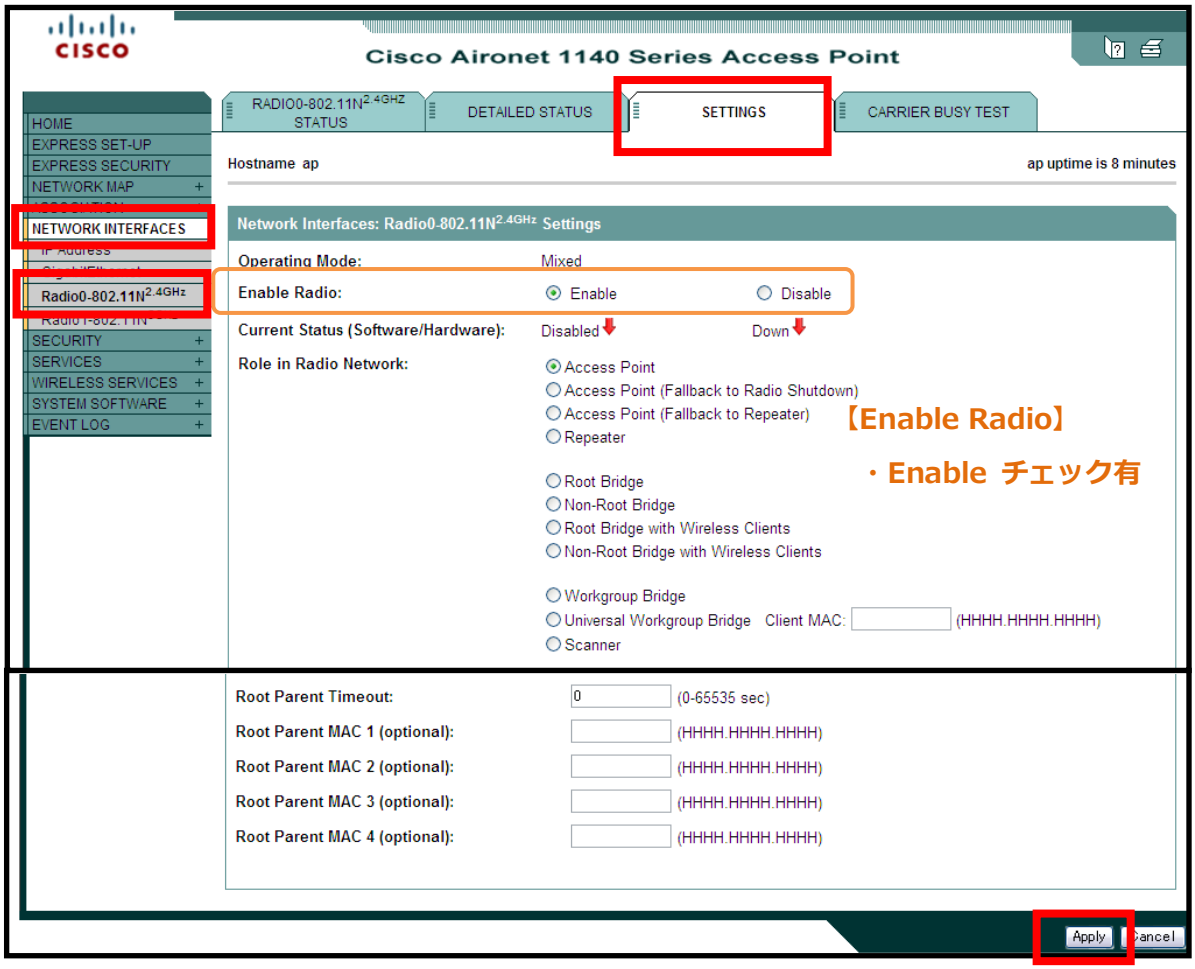
・1812

【Accounting Port】

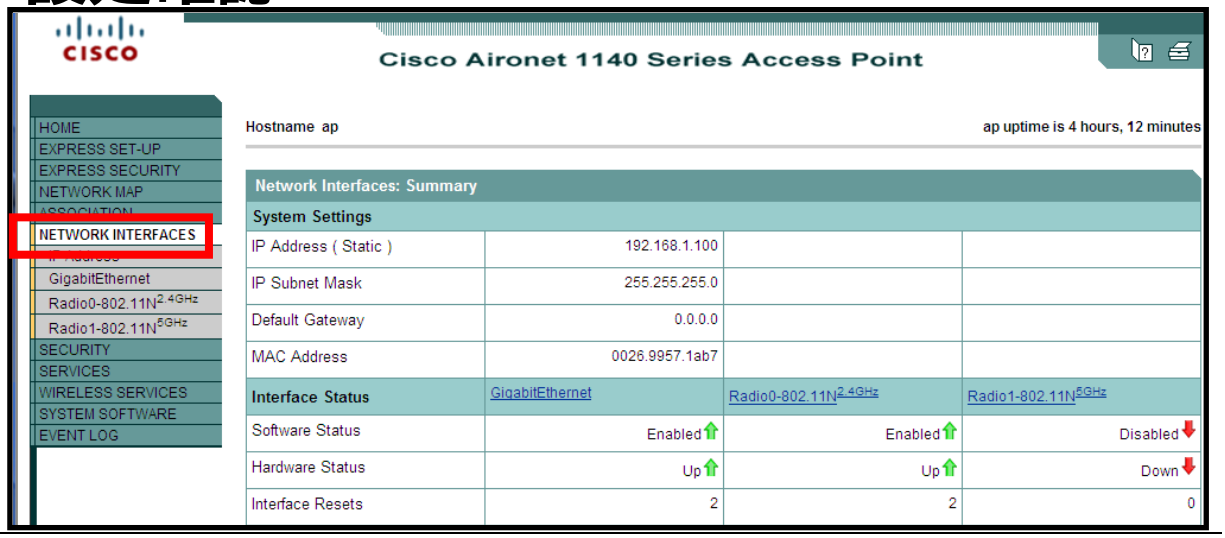
・1813

3-5 無線 Interfaces の有効化

無線 Interfaces の shutdown を解除し無線を利用できるようにします。



設定確認



4 クライアント PC の設定

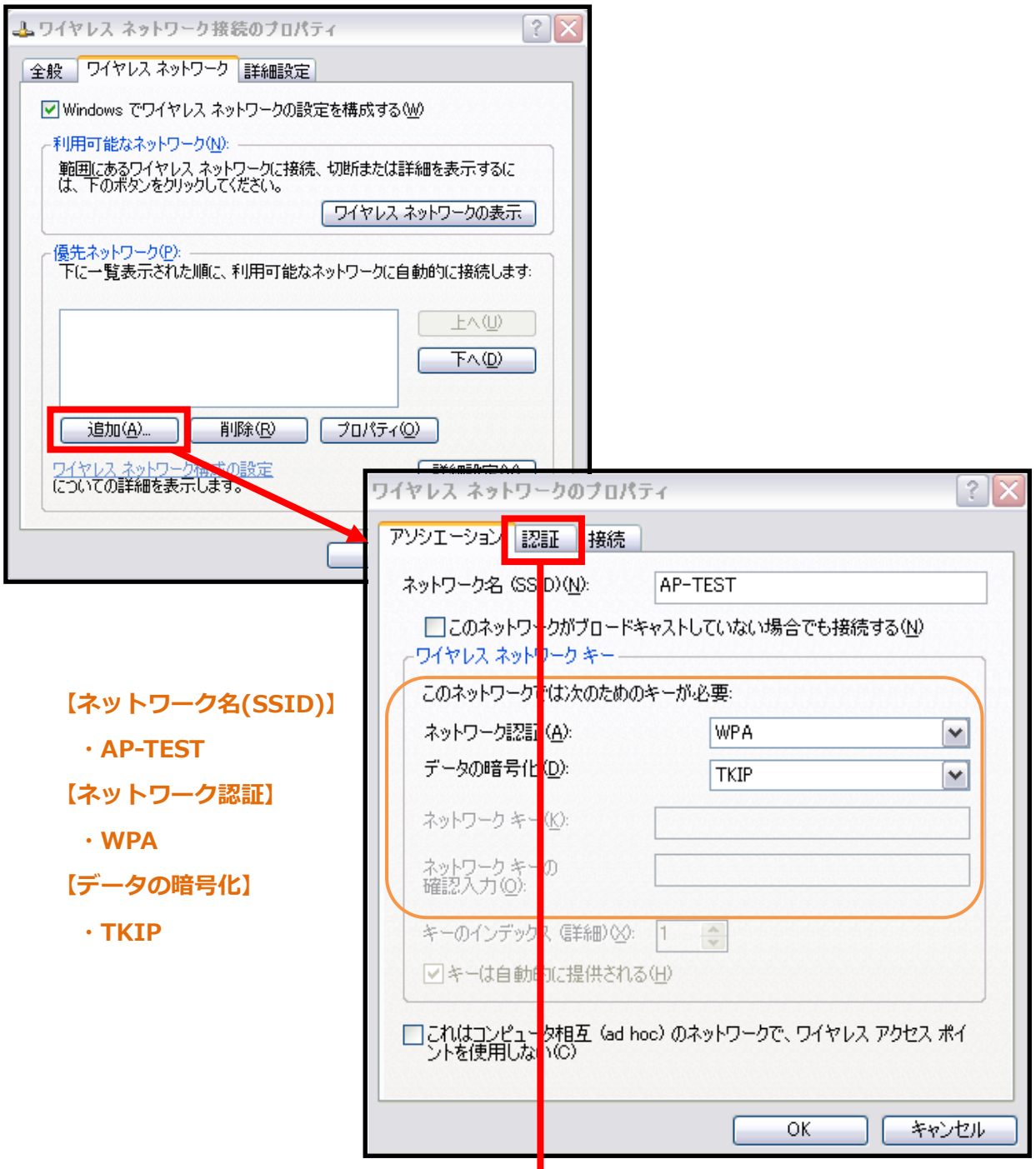
4-1 クライアント PC 設定の流れ

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)】

・AP-TEST

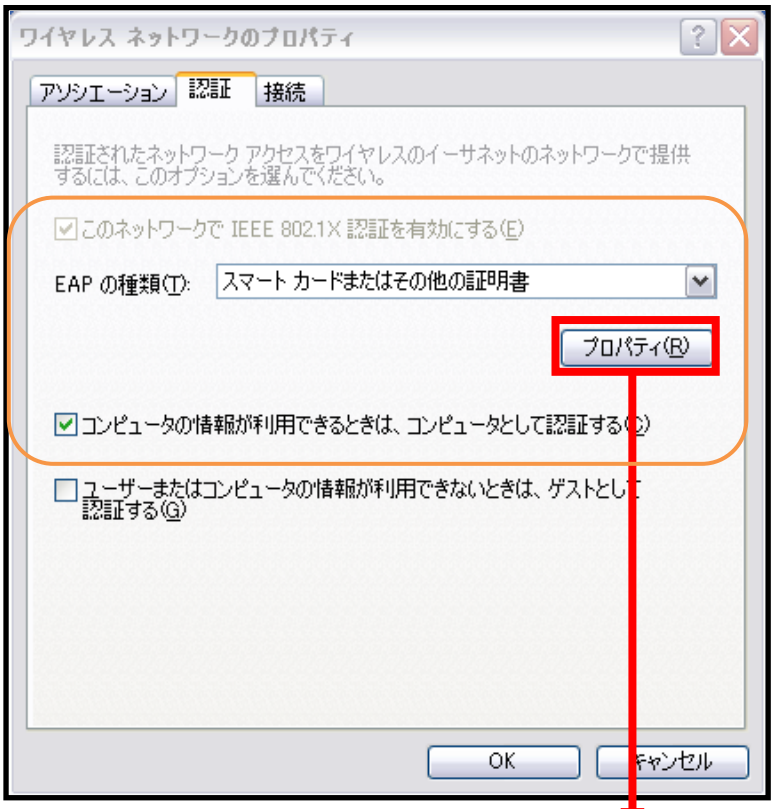
【ネットワーク認証】

・WPA

【データの暗号化】

・TKIP

次ページへ

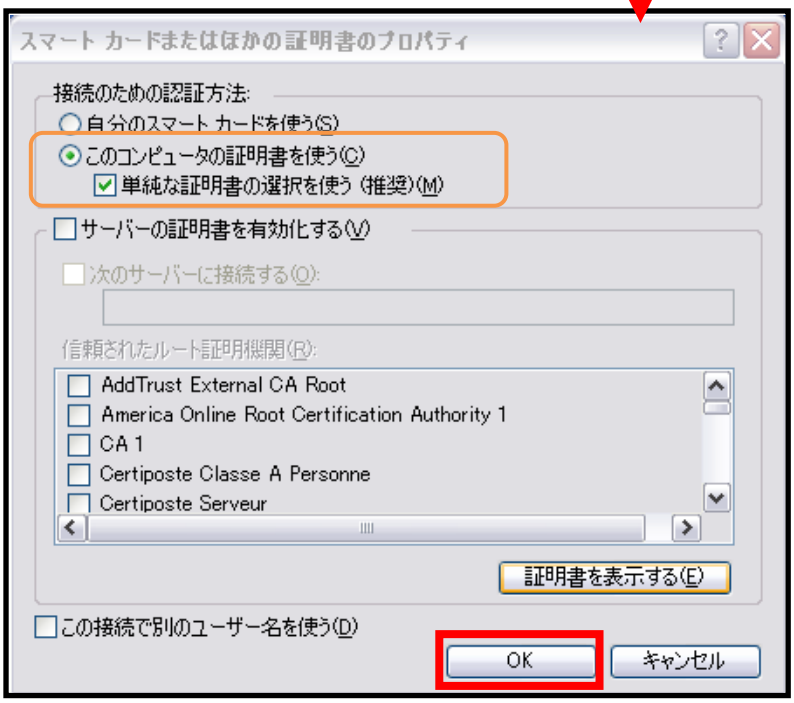


【EAP の種類】

・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

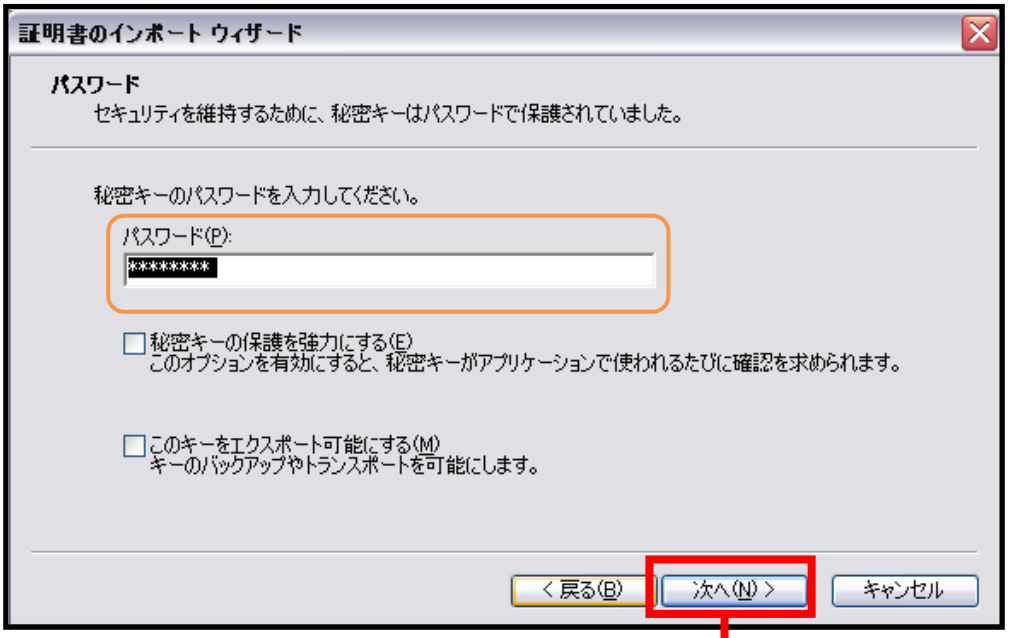
【単純な証明書の選択を使う】

・チェック有

4-3 ユーザー証明書のインポート

Net'Attest 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。

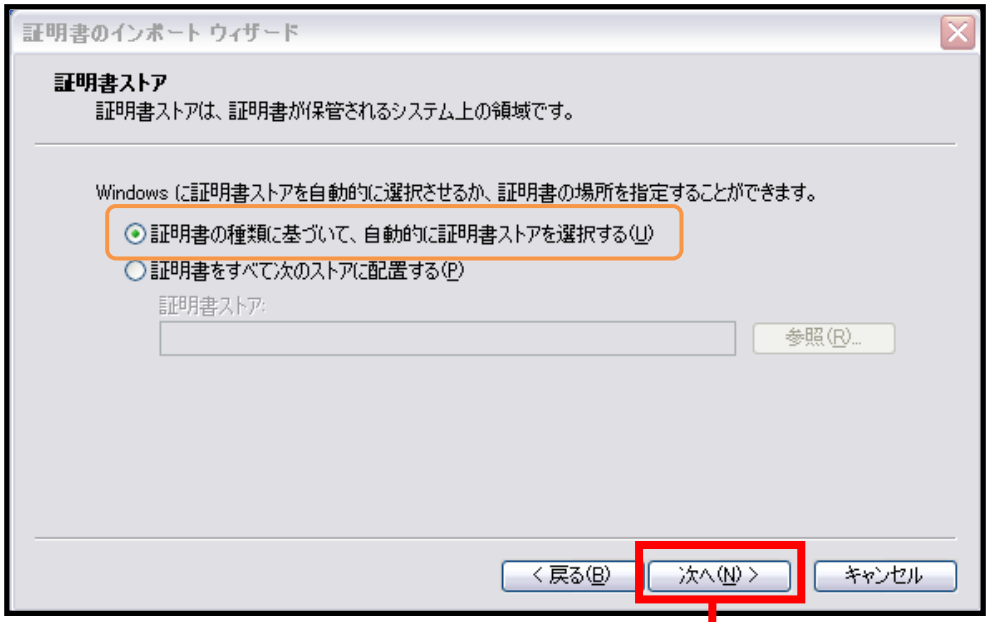
本書では、デスクトップ上に保存されている「soliton_user_0E.p12」アイコンをダブルクリックします。



Net'Attest 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】

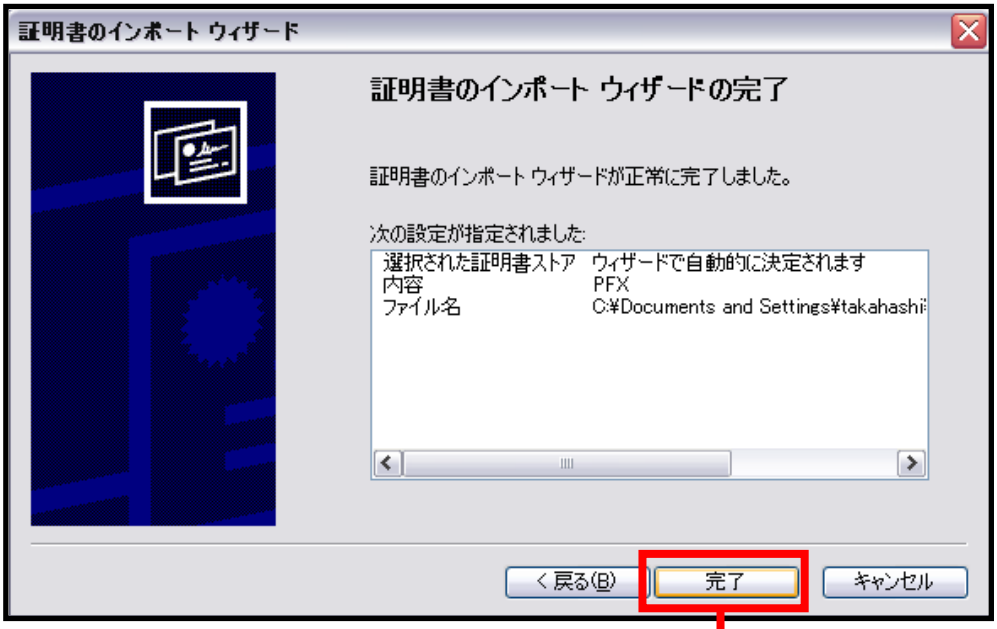
・password

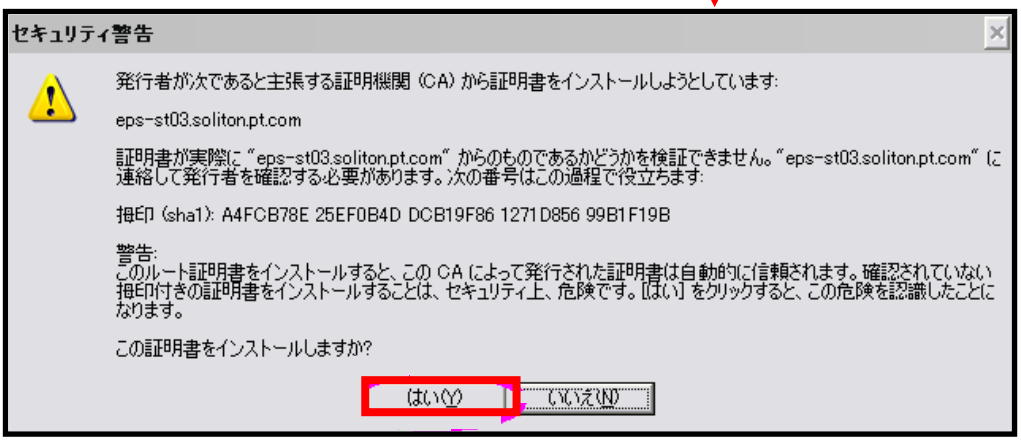


【証明書の種類に基づいて・・・】

・チェック有

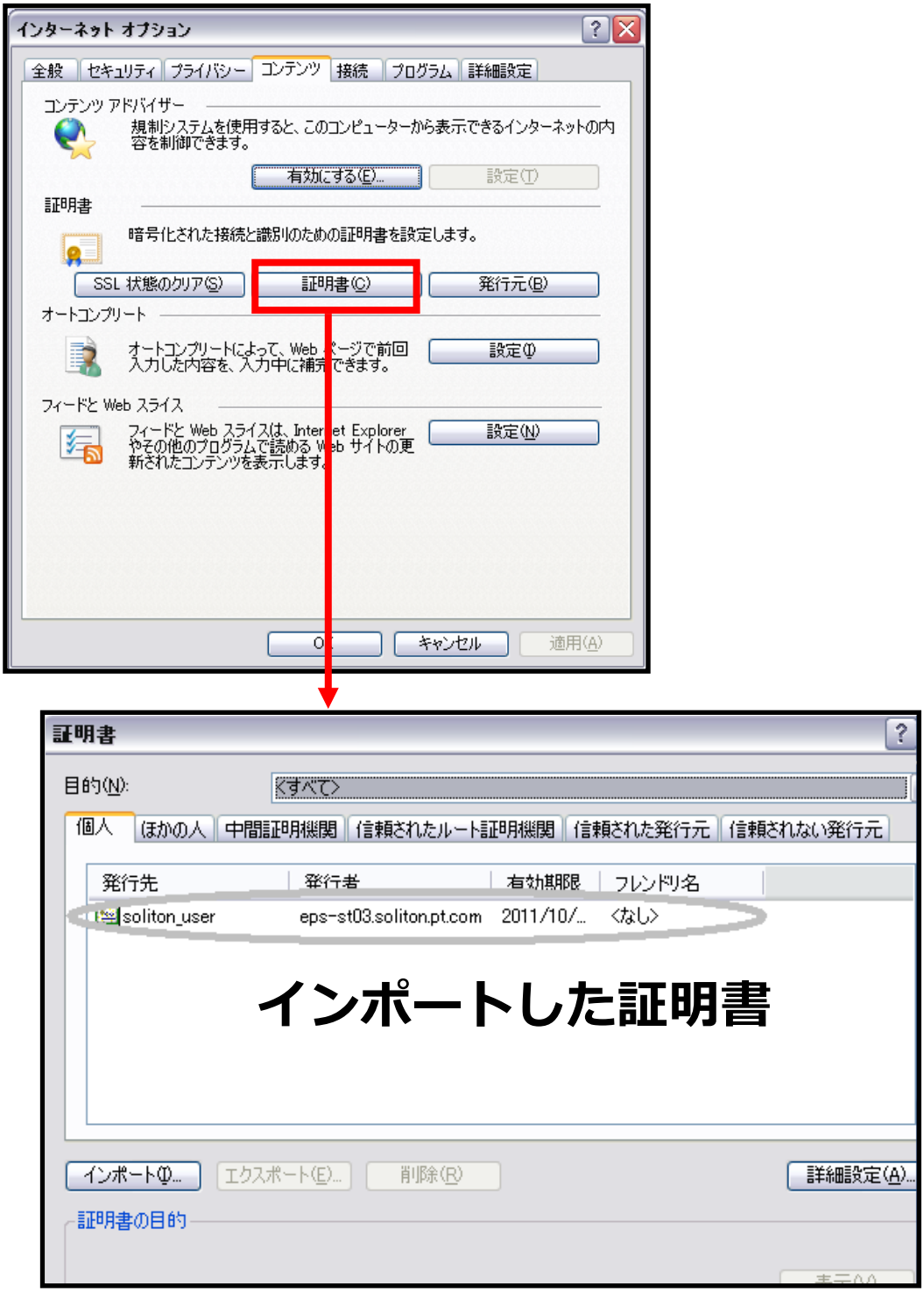
次ページへ


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。

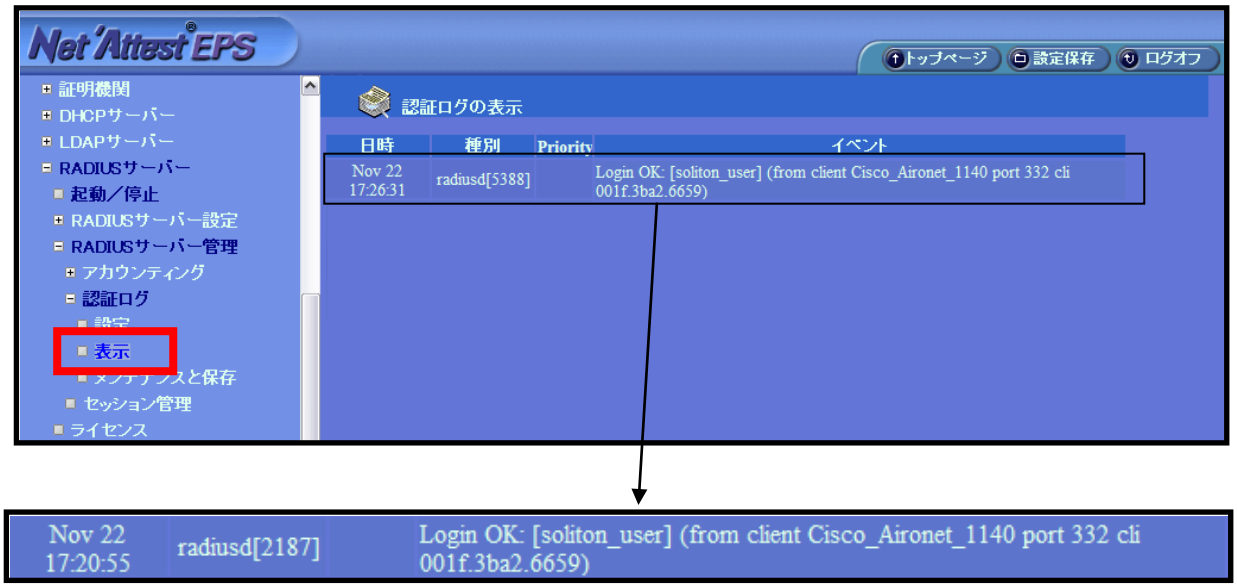


5 各機器　認証/接続ステイタス

5-1 Net'Attest EPS　認証ステイタス

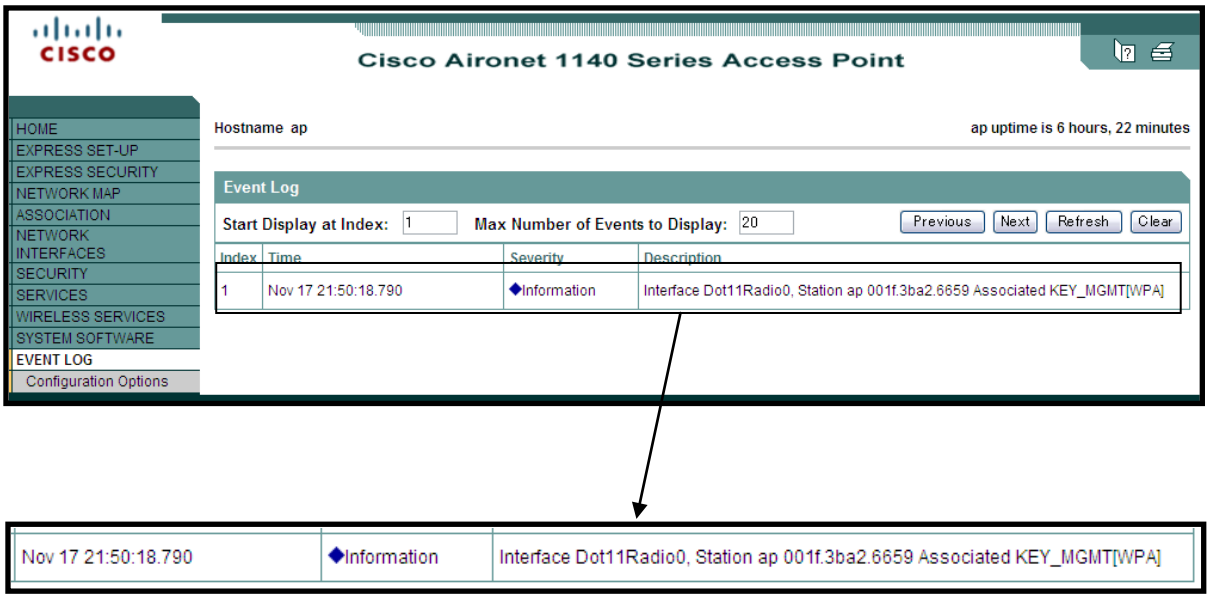
「RADIUS サーバー」→「RADIUS サーバー管理」→「認証ログ」→「表示」を選択します。

下記のように、認証に成功したログを確認することができます。



5-2 Cisco Aironet1140　接続成功時ステイタス

「EVENT LOG」にて、接続に成功したことを確認することができます。



以上

改訂履歴

日付	版	改訂内容
2010/11/30	1.0	初版作成
2012/9/10	1.1	RADIUS Port を TCP から UDP に修正