Net'Attest EPS 設定例

連携機器：

Meru MC1500、AP1020i

Case：TLS 方式での認証

Version 1.1

株式会社ソリトンシステムズ

Net'Attest®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 サーバプライアンス Net'Attest EPS とメルー・ネットワークス社製 無線 LAN コントローラ MC1500、無線アクセスポイント AP 1020i 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 MC1500、AP1020i 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 Net'Attest EPS 8

2-1 Net'Attest 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 9

2-4 Authenticator(RADIUS Client)の登録 11

2-5 RADIUS サーバ基本設定 12

2-6 ユーザーの登録 13

2-7 ユーザー証明書の発行 14

3 Meru MC1500、AP1020i 15

3-1 Meru MC1500、AP1020i 設定の流れ 15

3-2 RADIUS サーバの登録 16

3-3 無線アクセスポイントの接続 17

3-4 無線セキュリティ設定 1 （Security Profile の設定） 18

3-5 無線セキュリティ設定 2 （ESS Profile の設定） 19

4 クライアント PC の設定 20

4-1 クライアント PC 設定の流れ 20

4-2 ワイヤレスネットワーク接続先の登録 21

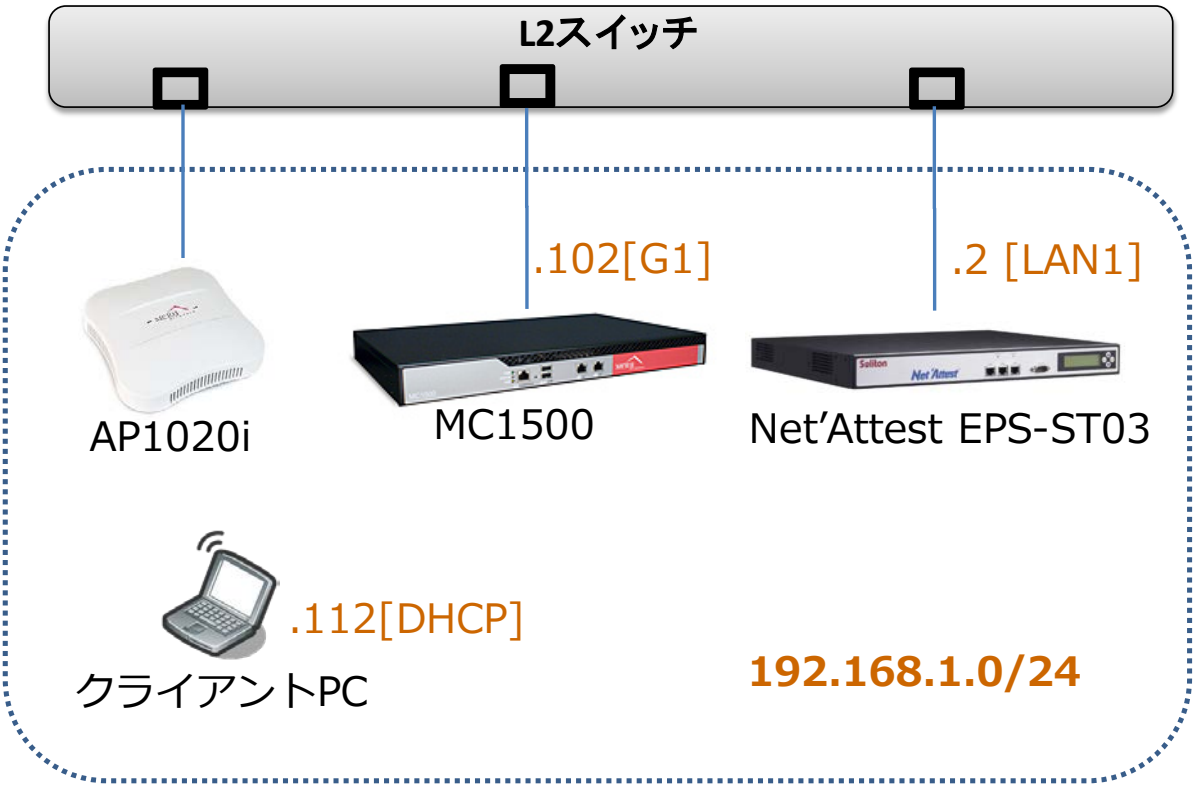
4-3 ユーザー証明書のインポート 23

4-4 インポートされたユーザー証明書の確認 26

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. 4.2.0
Authenticator (認証機器)	Meru Networks	MC1500	Ver.4.1-55
		AP1020i	Ver.4.1-55
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	MC1500	AP1020i	Client PC
IP アドレス	192.168.1.2/24	192.168.1.102/24	–	192.168.1.112 (DHCP)
RADIUS port (Authentication)	UDP 1812		–	
RADIUS port (Accounting)	UDP 1813		–	
RADIUS Secret (Key)	soliton		–	

2 Net'Attest EPS

2-1 Net'Attest EPS 設定の流れ

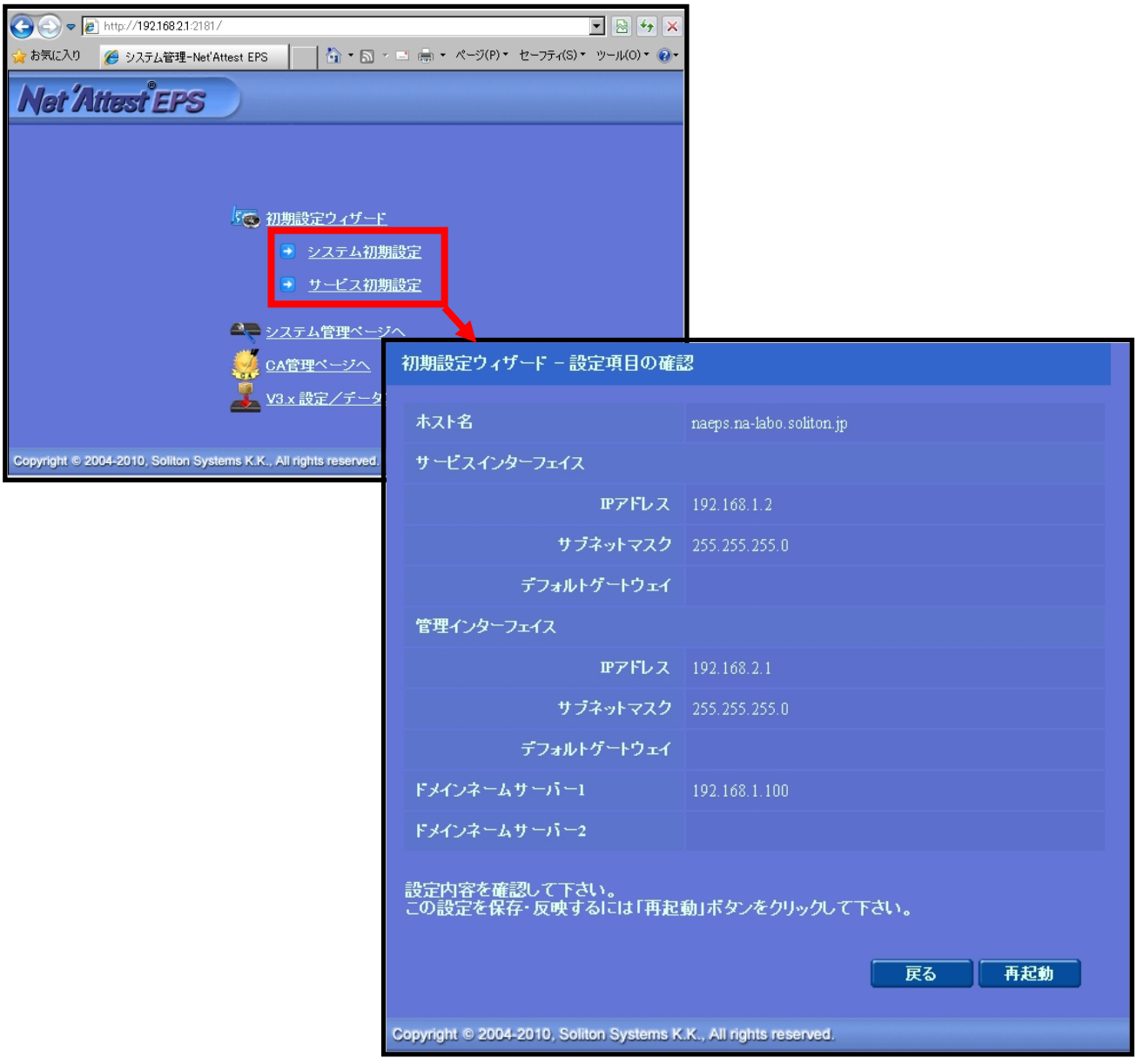
設定の流れ

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



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】

・Meru

【IP アドレス(Authenticator)】

・192.168.1.102

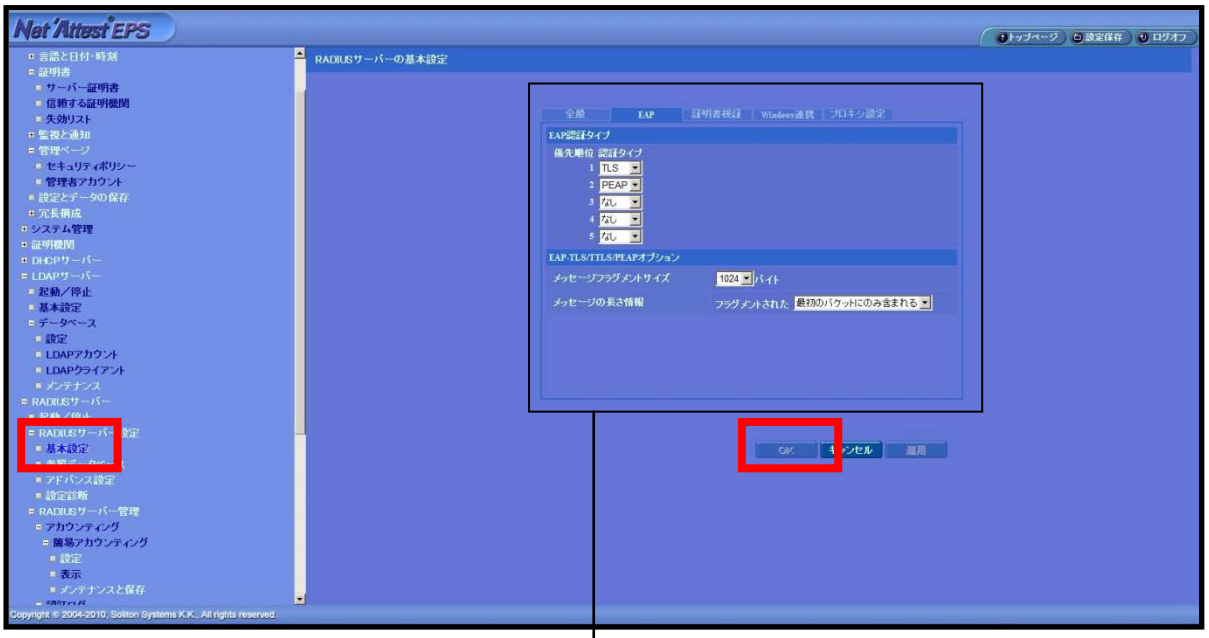
【シークレット】

・soliton

2-5 RADIUS サーバ基本設定

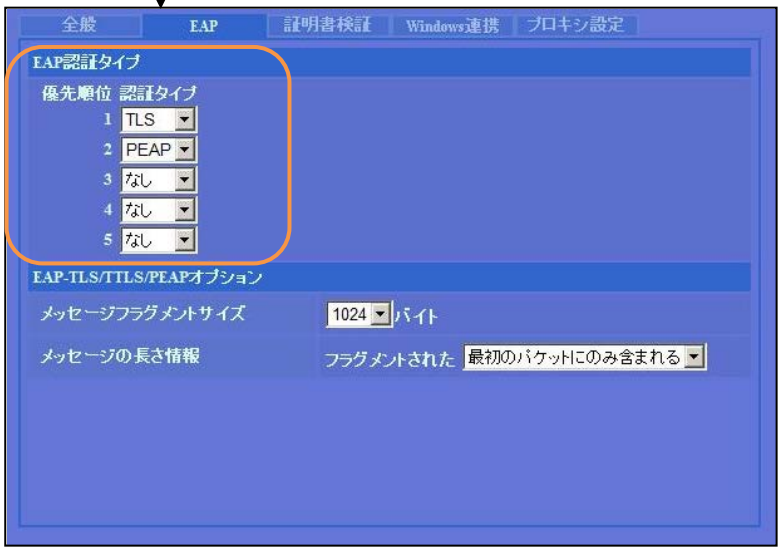
WebGUI より、RADIUS サーバの基本設定を行います。

「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】

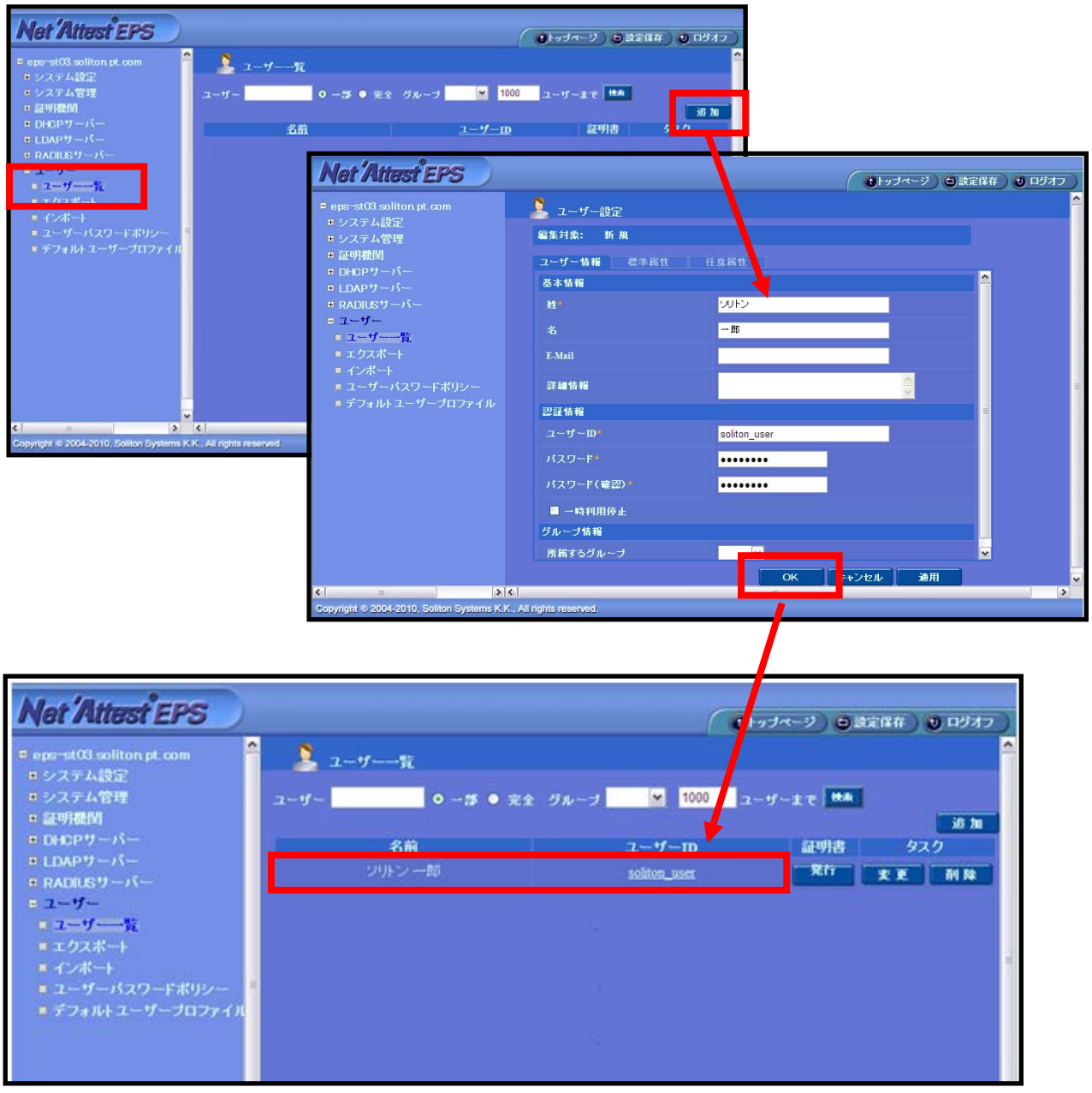
・1)TLS



2-6 ユーザーの登録

WebGUI より、ユーザー登録を行います。

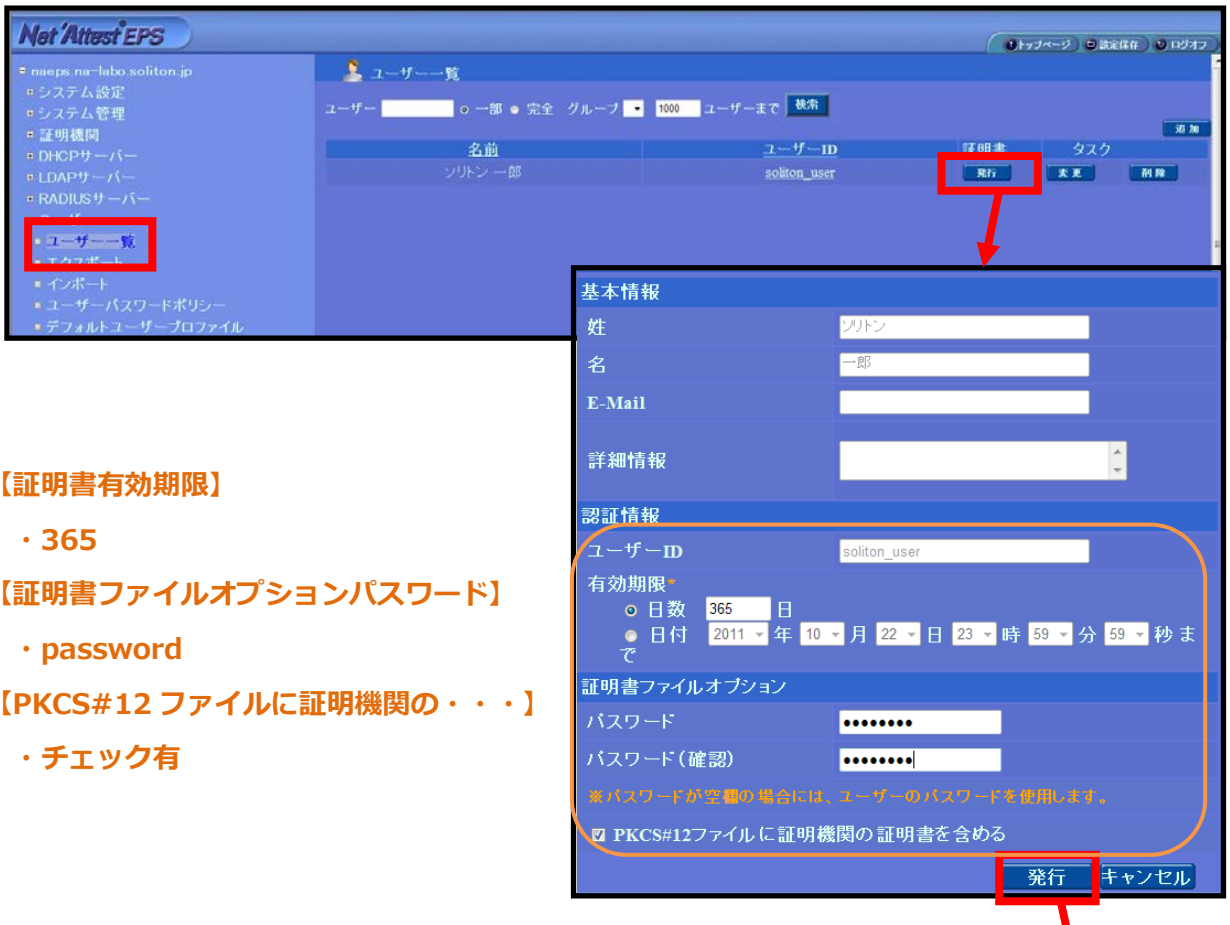
「ユーザー」→「ユーザー一覧」から、『追加』ボタンでユーザー登録を始めます。



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】

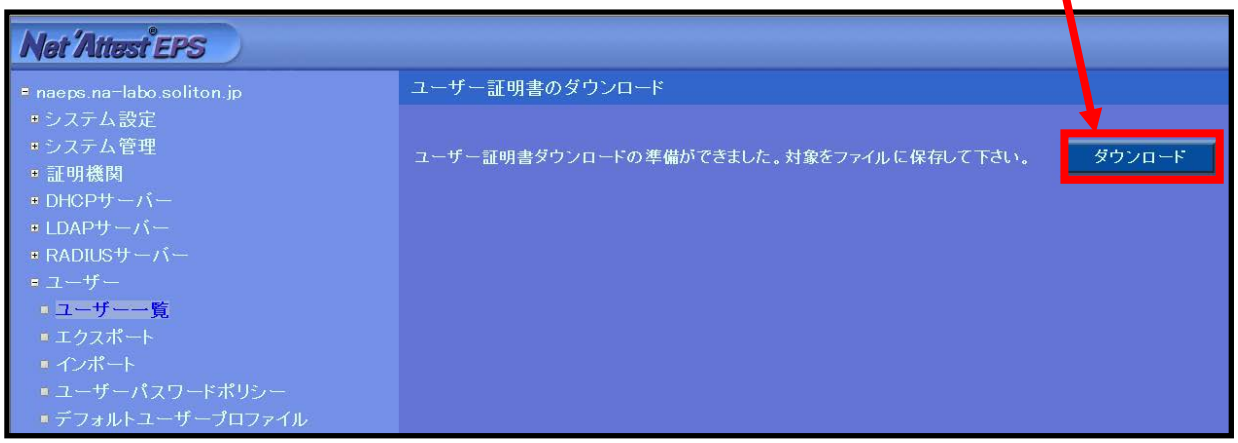
・365

【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 Meru MC1500、AP1020i

3-1 Meru MC1500、AP1020i 設定の流れ

本書では、管理 WebGUI から各種設定を実施する方法を紹介します。

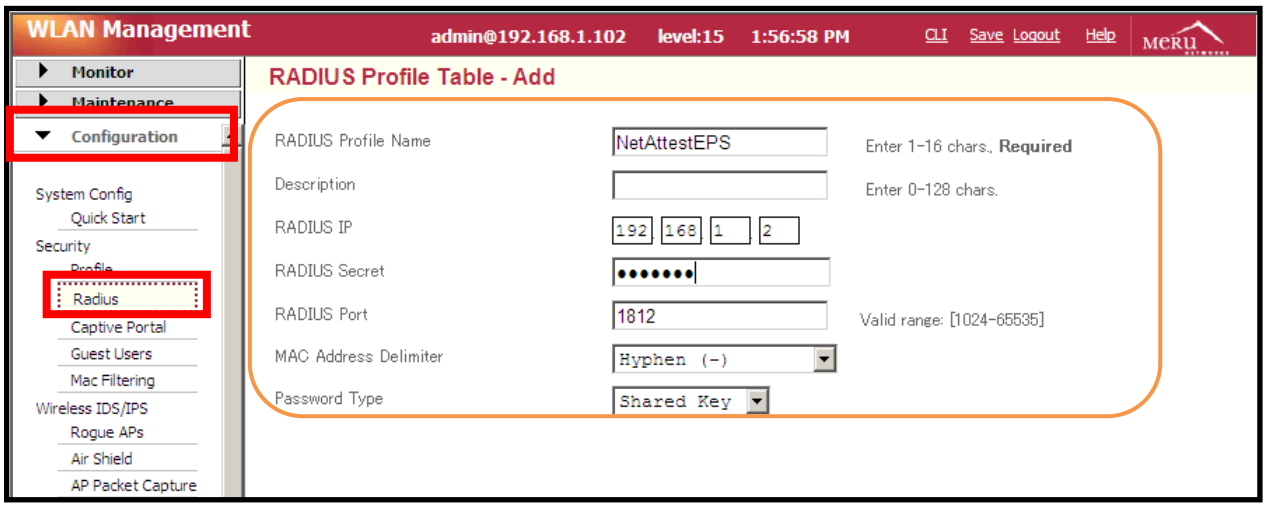
設定の流れ

1. RADIUS サーバの登録（RADIUS Profile の設定）
2. 無線アクセスポイントの接続
3. 無線セキュリティ設定１（Security Profile の設定）
4. 無線セキュリティ設定２（ESS Profile の設定）

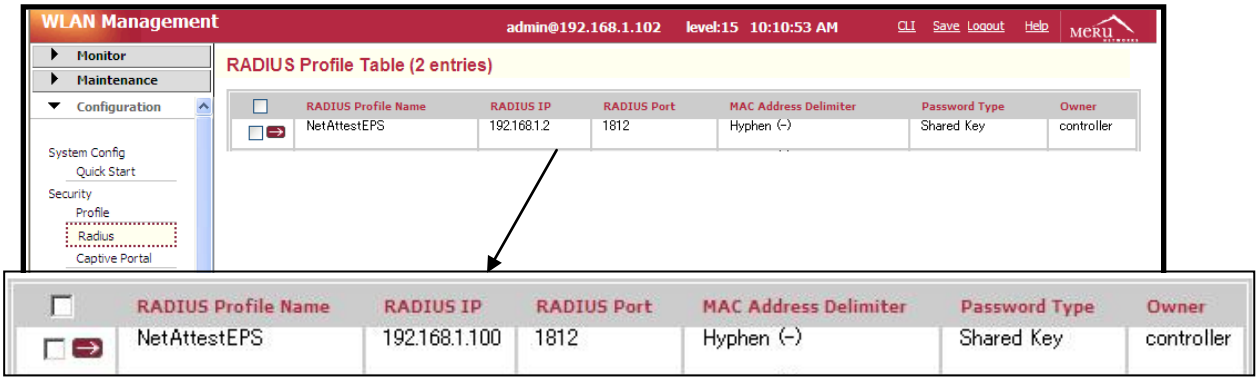
3-2 RADIUS サーバの登録

RADIUS サーバの設定をします。

TOP ページの[Configuration]リンクをクリックし、Security メニューの[Radius]リンクをクリックします。右側の画面下にある[Add]ボタンをクリックすると、RADIUS 設定項目が表示されますので、値を入力します。



【RADIUS Profile Name】
・NetAttestEPS
【RADIUS IP】
・192.168.1.2
【RADIUS Secret】
・soliton
【RADIUS Port】
・1812
【MAC Address Delimiter】
・Hyphen (-)
【Password Type】
・Shared Key

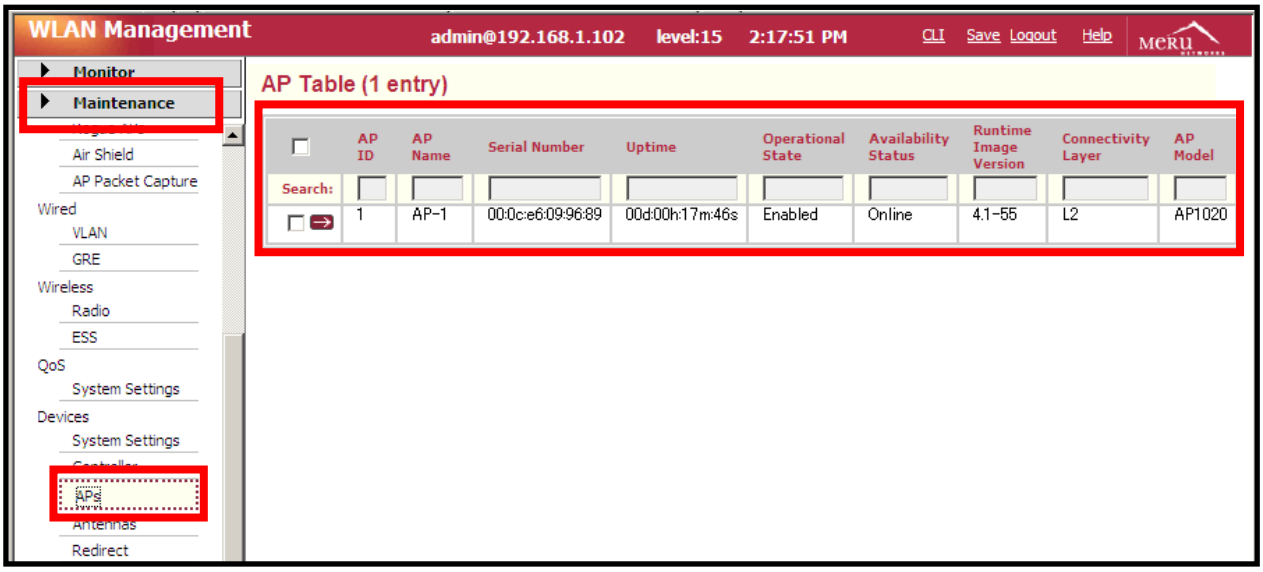


3-3 無線アクセスポイントの接続

AP1020i が MC1500 に自動認識されていることを確認します。

AP1020i を MC1500 と同じネットワークセグメントに接続後、MC1500 の管理 WebGUI の左側のメニューから[Maintenance]をクリックし、Devices の[APs]をクリックします。

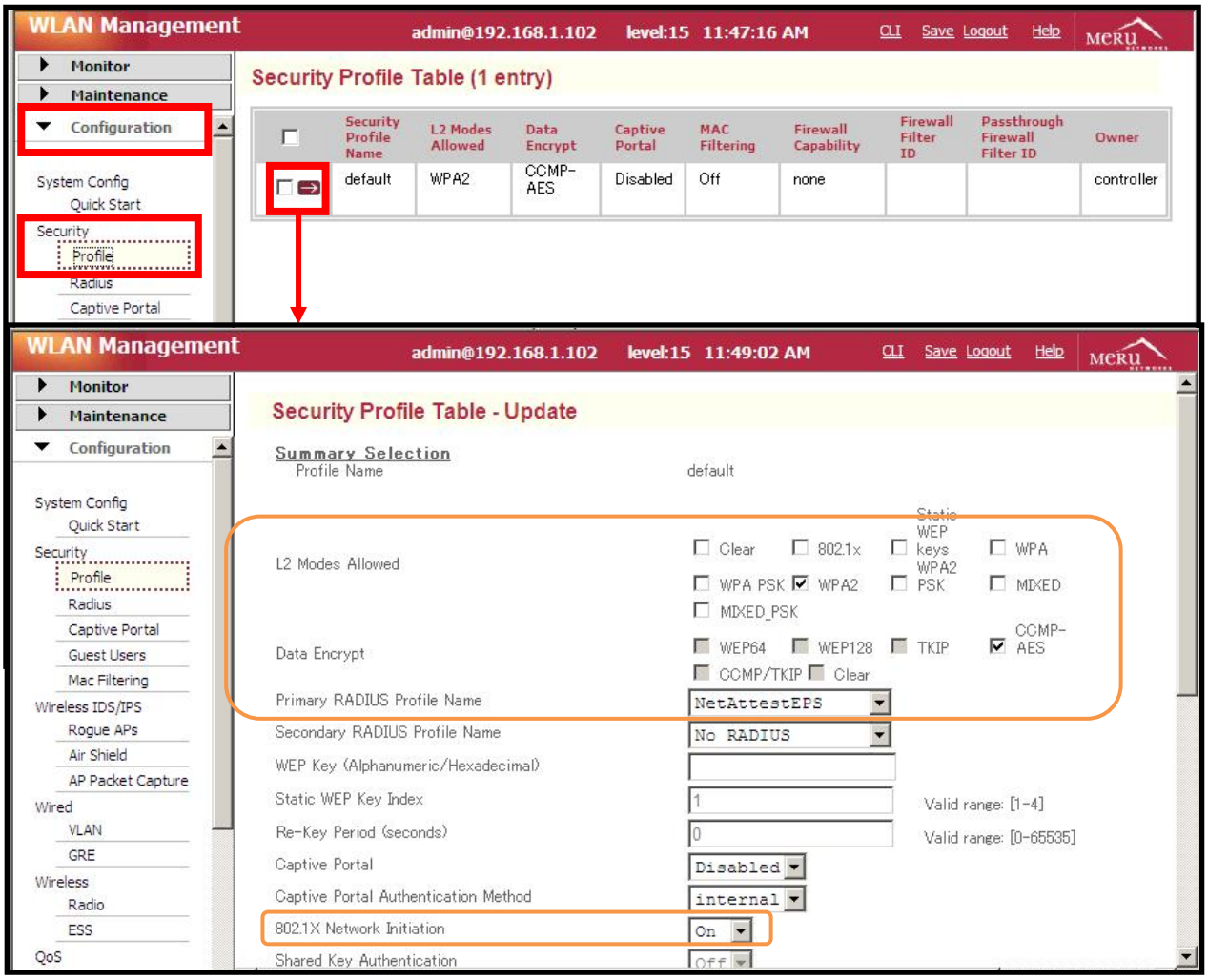
右側の AP Table に無線アクセスポイントが表示されていることを確認します。



3-4 無線セキュリティ設定１（Security Profile の設定）

無線の暗号化方式を設定します。

左側のメニューから[Configuration]をクリックし、Security の[Profile]リンクをクリックします。その後、Security Profile Name ”default” の➡をクリックし、右側の設定項目に値を入力します。



【L2 Modes Allowed】

・WPA2（チェック）

【Data Encrypt】

・CCMP-AES（チェック）

【Primary RADIUS Profile Name】

・NetAttestEPS

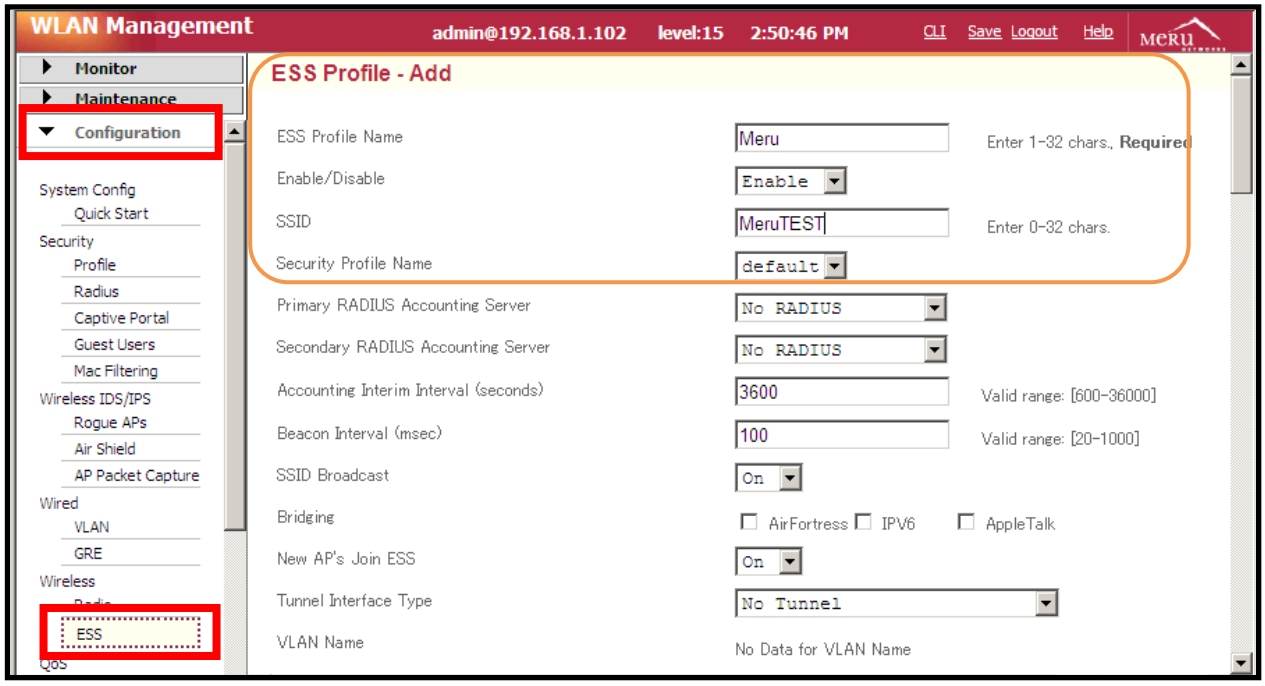
【802.1X Network Initiation】

・ON

3-5 無線セキュリティ設定２（ESS Profile の設定）

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[Configuration]をクリックします。Wireless の[ESS]リンクをクリックし、右側の画面下にある[Add]をクリックし、設定項目に値を入力します。



【ESS Profile Name】

・Meru

【Enable/Disable】

・Enable

【SSID】

・MeruTEST

【Security Profile Name】

・default

4 クライアント PC の設定

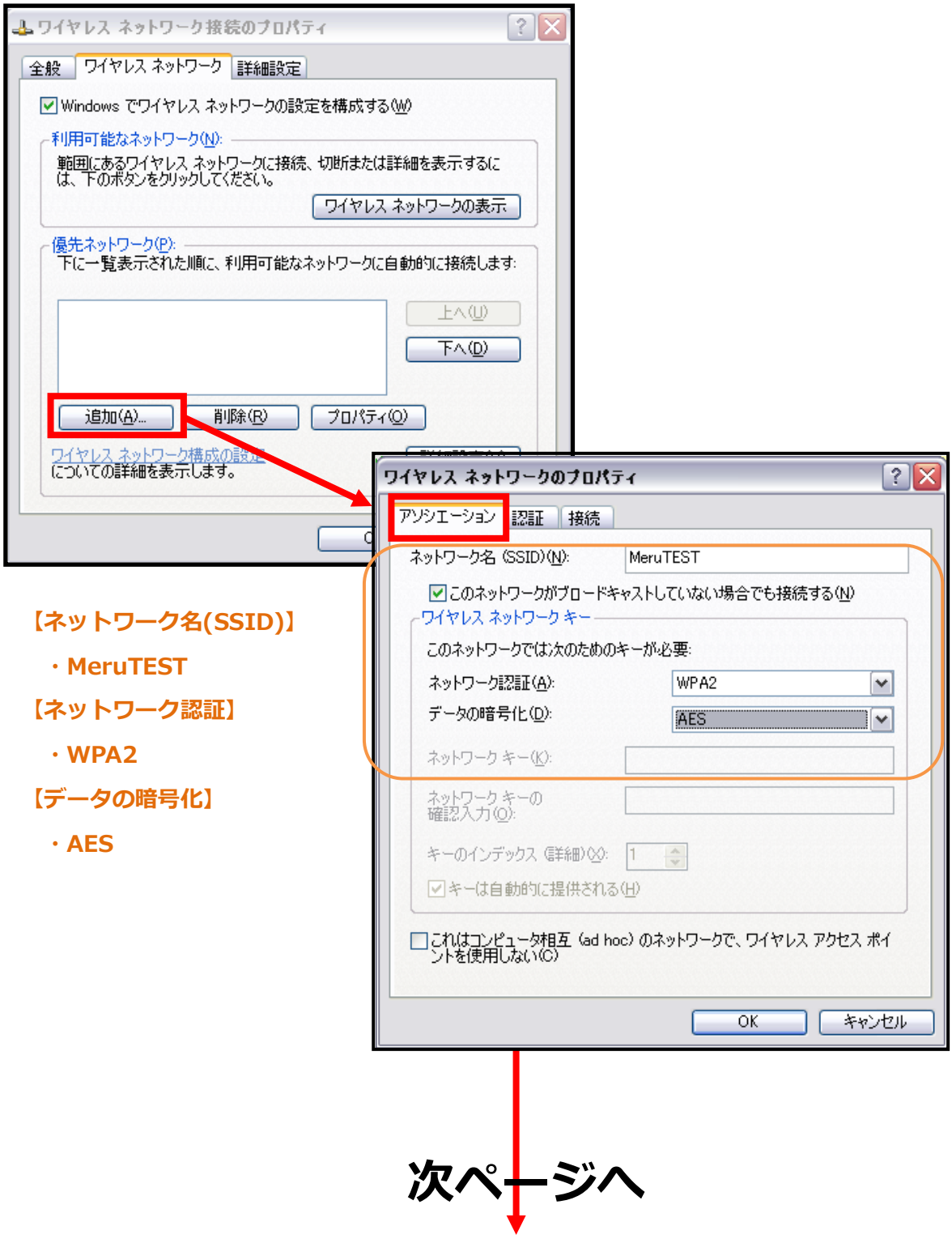
4-1 クライアント PC 設定の流れ

設定の流れ

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)】

・MeruTEST

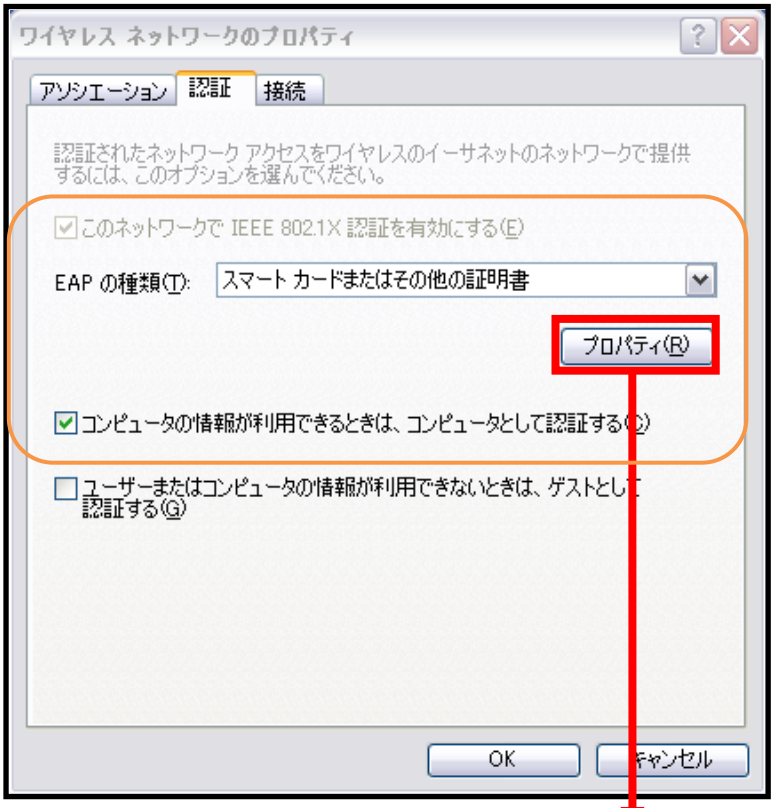
【ネットワーク認証】

・WPA2

【データの暗号化】

・AES

次ページへ

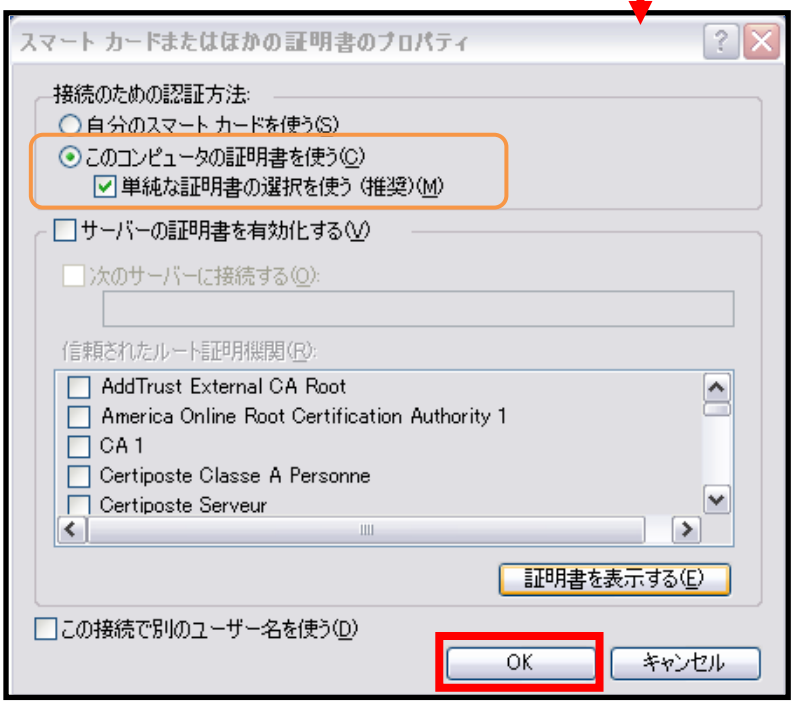


【EAP の種類】

・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

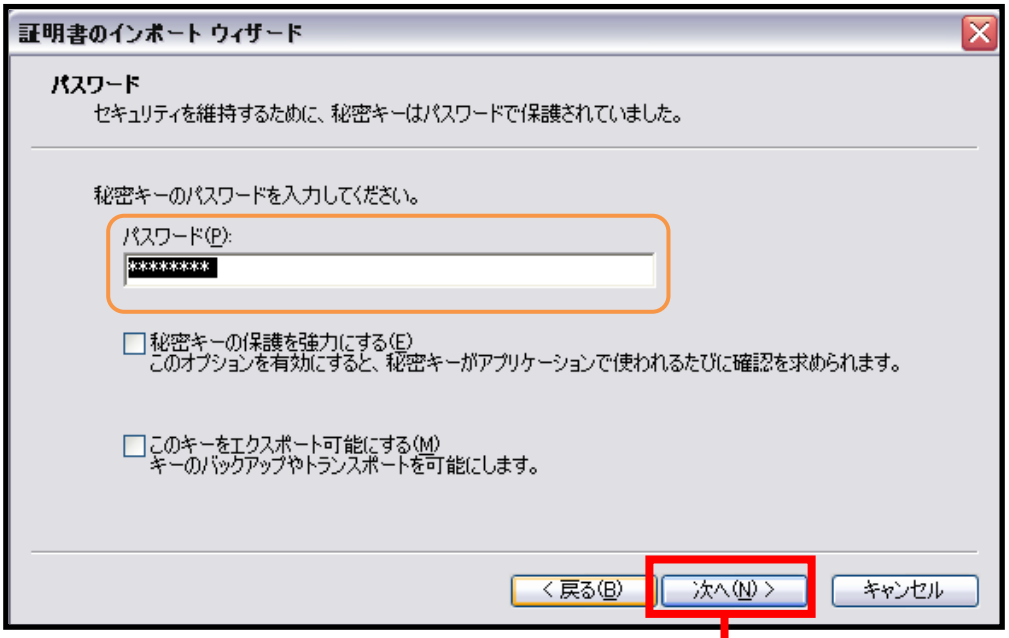
【単純な証明書の選択を使う】

・チェック有

4-3 ユーザー証明書のインポート

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。

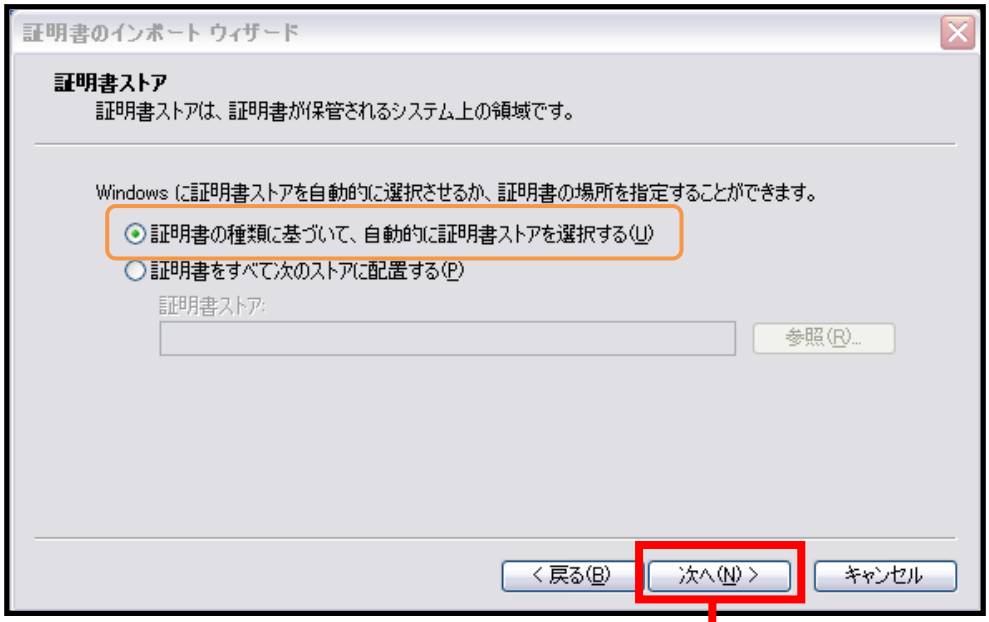
本書では、デスクトップ上に保存されている「soliton_user_0E.p12」アイコンをダブルクリックします。



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】

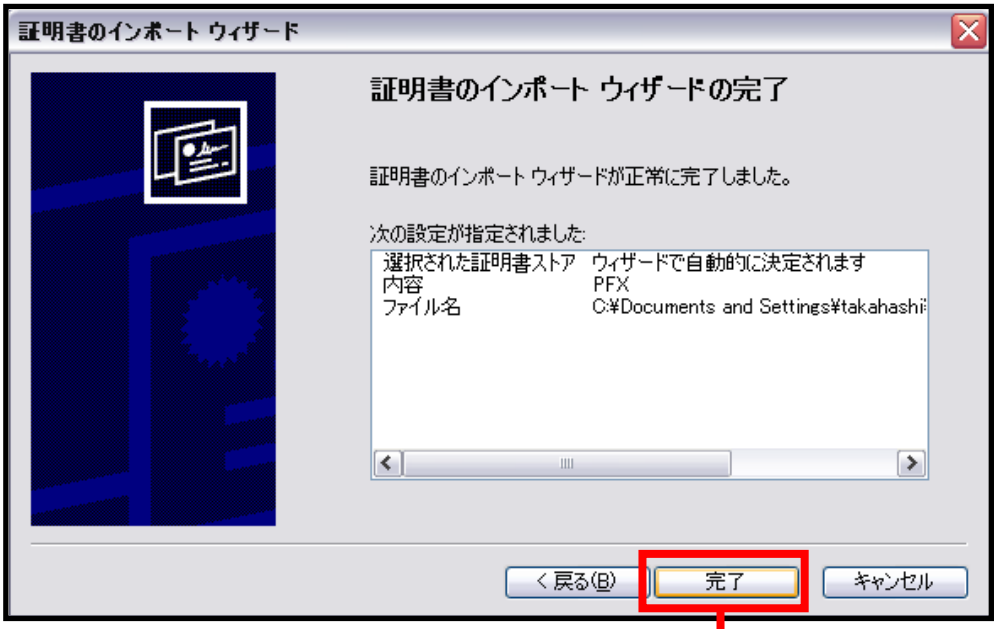
・password

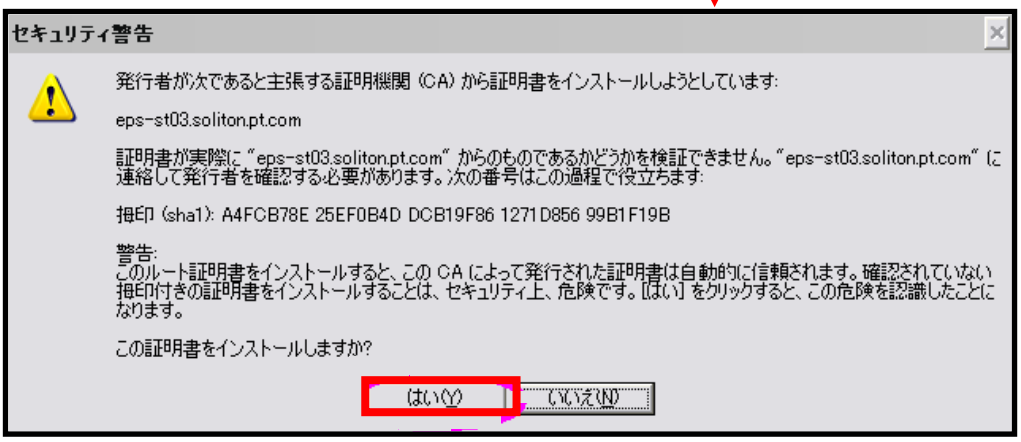


【証明書の種類に基づいて・・・】

・チェック有

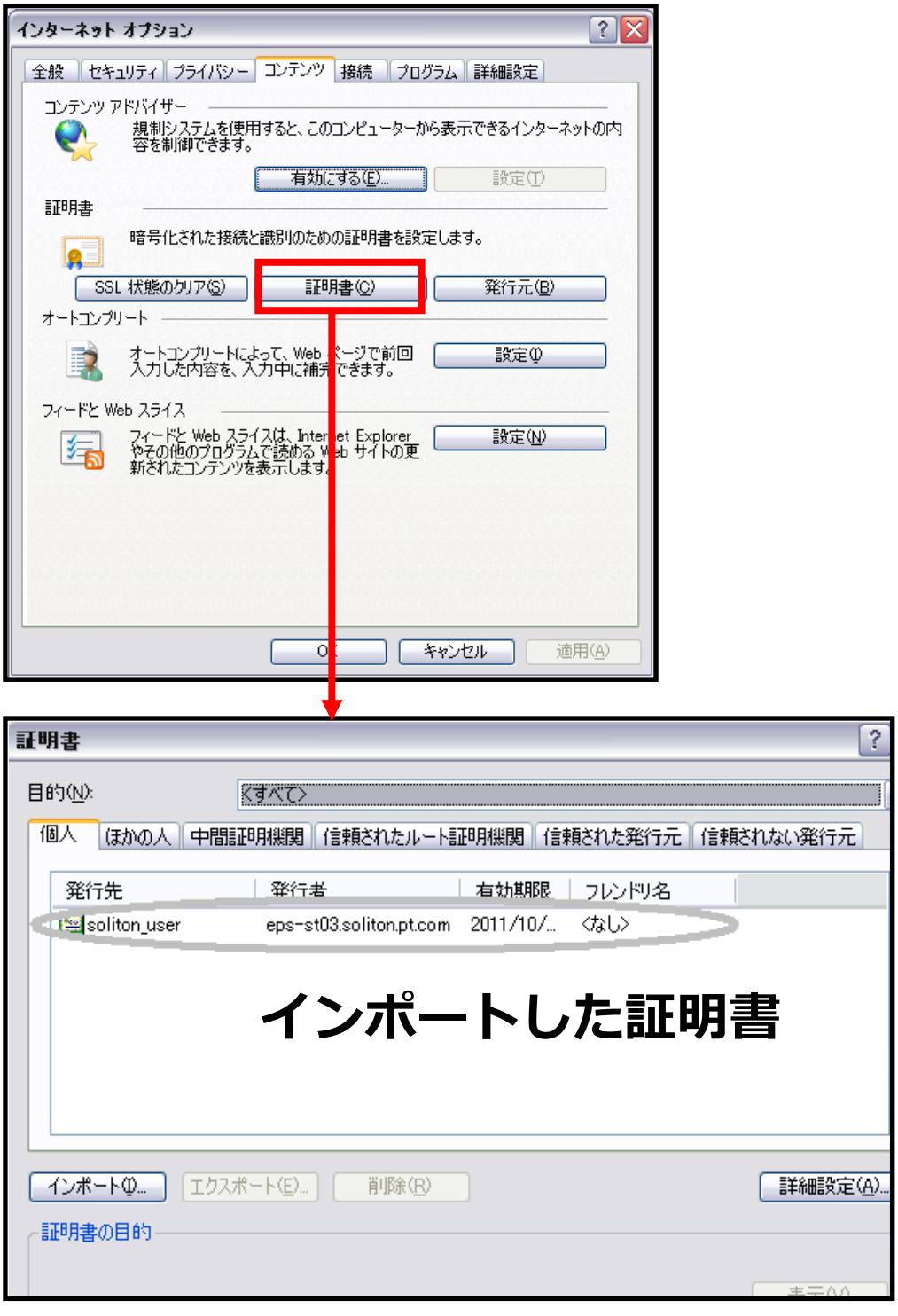
次ページへ


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。



改訂履歴

日付	版	改訂内容
2011/2/10	1.0	初版作成
2012/9/10	1.1	RADIUS Port を TCP から UDP に修正