

Net'Attest EPS 設定例

連携機器：

Meru MC1500、AP1020i

Case：TLS 方式での認証

Version 1.1

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。
<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、AP10 20i 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。

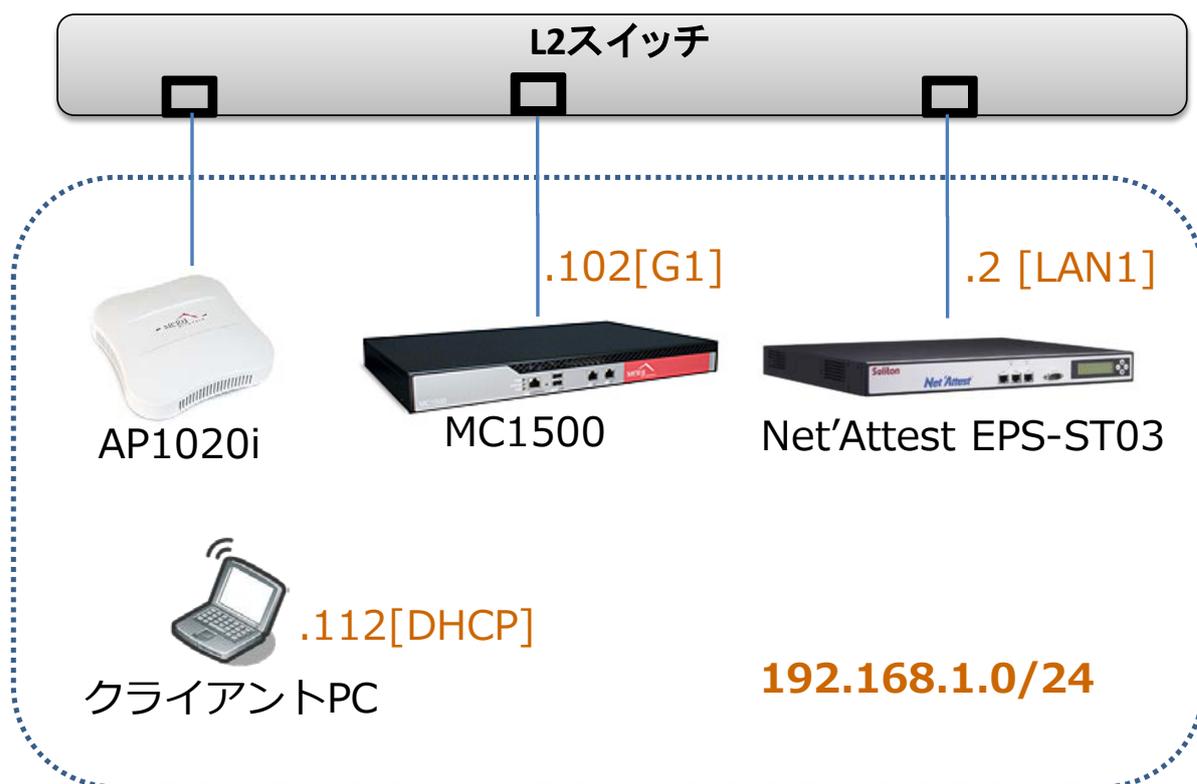
目次

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 標準サブプリカント

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

初期設定ウィザード

- システム初期設定
- サービス初期設定

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.

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

The image displays three overlapping screenshots of the Soliton initial setup wizard interface, which has a blue header and white content area.

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.jp

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: (empty text area)

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 shows the Net Attest EPS WebGUI interface. On the left is a sidebar menu with 'NAS/RADIUSクライアント一覧' highlighted. The main area displays a table with columns for 'NAS/RADIUSクライアント名', 'IPアドレス', '説明', and 'マスク'. A red box highlights the '追加' (Add) button in the top right corner, with a red arrow pointing to the modal form. The modal form is titled '編集対象: 新規' and contains the following fields:

- NAS/RADIUSクライアント名*: Meru
- このNAS/RADIUSクライアントを有効にする
- 説明: [Empty text box]
- IPアドレス*: 192.168.1.102
- シークレット*: [Masked text box]
- 所属するNASグループ: [Dropdown menu]

At the bottom of the modal form, the 'OK' button is highlighted with a red box, along with 'キャンセル' and '適用' buttons.

【NAS/RADIUS クライアント名】

・ Meru

【IP アドレス(Authenticator)】

・ 192.168.1.102

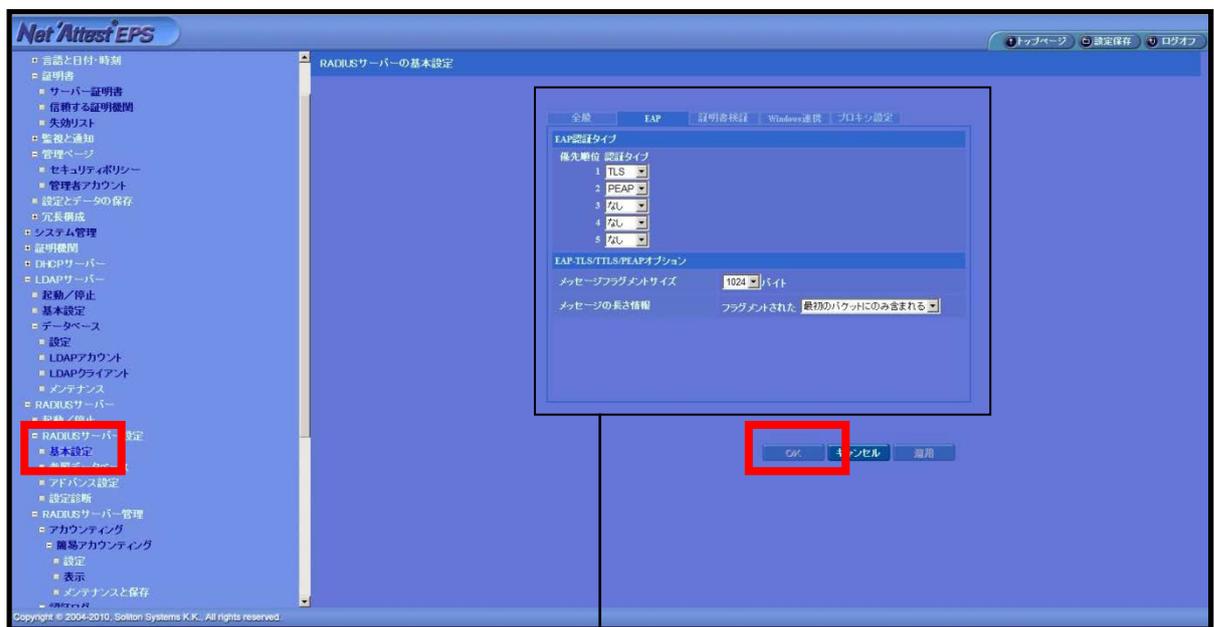
【シークレット】

・ soliton

2-5 RADIUS サーバ基本設定

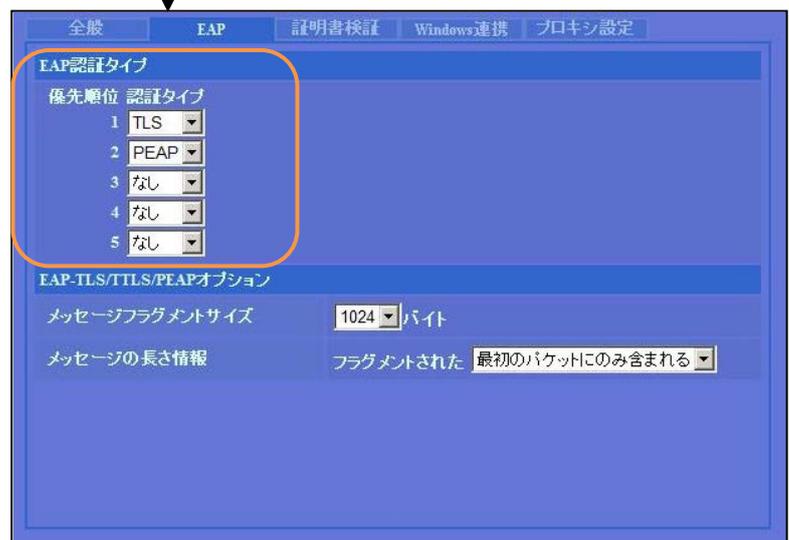
WebGUI より、RADIUS サーバの基本設定を行います。

「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。

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:** Fill out the 'ユーザー設定' (User Settings) form. The 'OK' button is highlighted in red.
- Step 3:** The newly added user is visible in the 'ユーザー一覧' table. The user name 'ソリトン 一郎' and user ID 'soliton_user' are 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	変更 削除

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

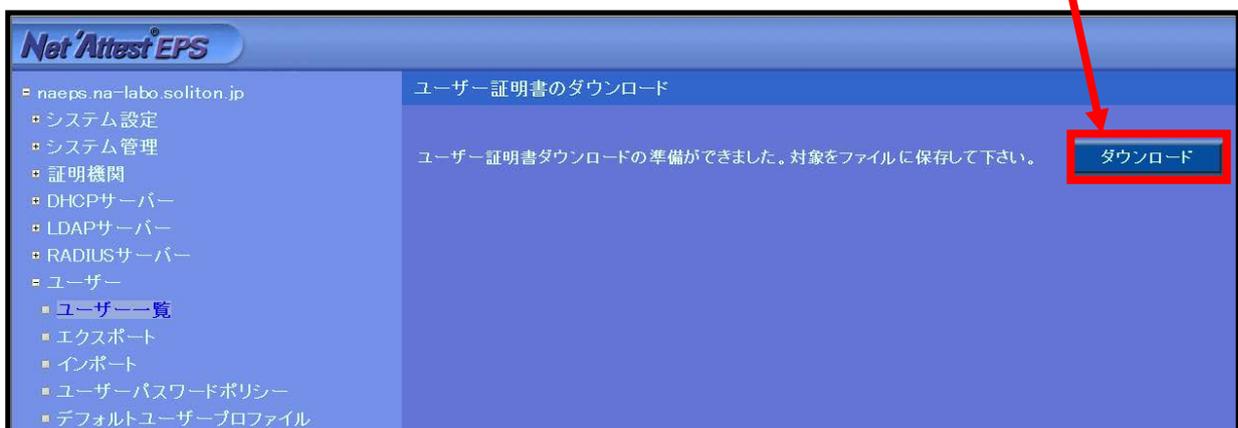
【証明書ファイルオプションパスワード】

- ・ password

【PKCS#12 ファイルに証明機関の・・・】

- ・ チェック有

The screenshot shows the '基本情報' (Basic Information) section of the NetAttest EPS WebGUI. The '有効期限*' (Valid Period) is set to 365 days. The '証明書ファイルオプション' (Certificate File Option) section has 'パスワード' (Password) and 'パスワード (確認)' (Password (Confirm)) fields. The 'PKCS#12ファイルに証明機関の証明書を含める' (Include certificates of the certificate authority in PKCS#12 file) checkbox is checked. The '発行' (Issue) button is highlighted with a red box and a red arrow.



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。

WLAN Management admin@192.168.1.102 level:15 1:56:58 PM CLI Save Logout Help MCRU

RADIUS Profile Table - Add

RADIUS Profile Name: Enter 1-16 chars., Required

Description: Enter 0-128 chars.

RADIUS IP:

RADIUS Secret:

RADIUS Port: Valid range: [1024-65535]

MAC Address Delimiter:

Password Type:

[RADIUS Profile Name] **[RADIUS Port]**

• NetAttestEPS

• 1812

[RADIUS IP]

• 192.168.1.2

[MAC Address Delimiter]

• Hyphen (-)

[RADIUS Secret]

• soliton

[Password Type]

• Shared Key

WLAN Management admin@192.168.1.102 level:15 10:10:53 AM CLI Save Logout Help MCRU

RADIUS Profile Table (2 entries)

<input type="checkbox"/>	RADIUS Profile Name	RADIUS IP	RADIUS Port	MAC Address Delimiter	Password Type	Owner
<input type="checkbox"/>	NetAttestEPS	192.168.1.2	1812	Hyphen (-)	Shared Key	controller

<input type="checkbox"/>	RADIUS Profile Name	RADIUS IP	RADIUS Port	MAC Address Delimiter	Password Type	Owner
<input type="checkbox"/>	NetAttestEPS	192.168.1.100	1812	Hyphen (-)	Shared Key	controller

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。

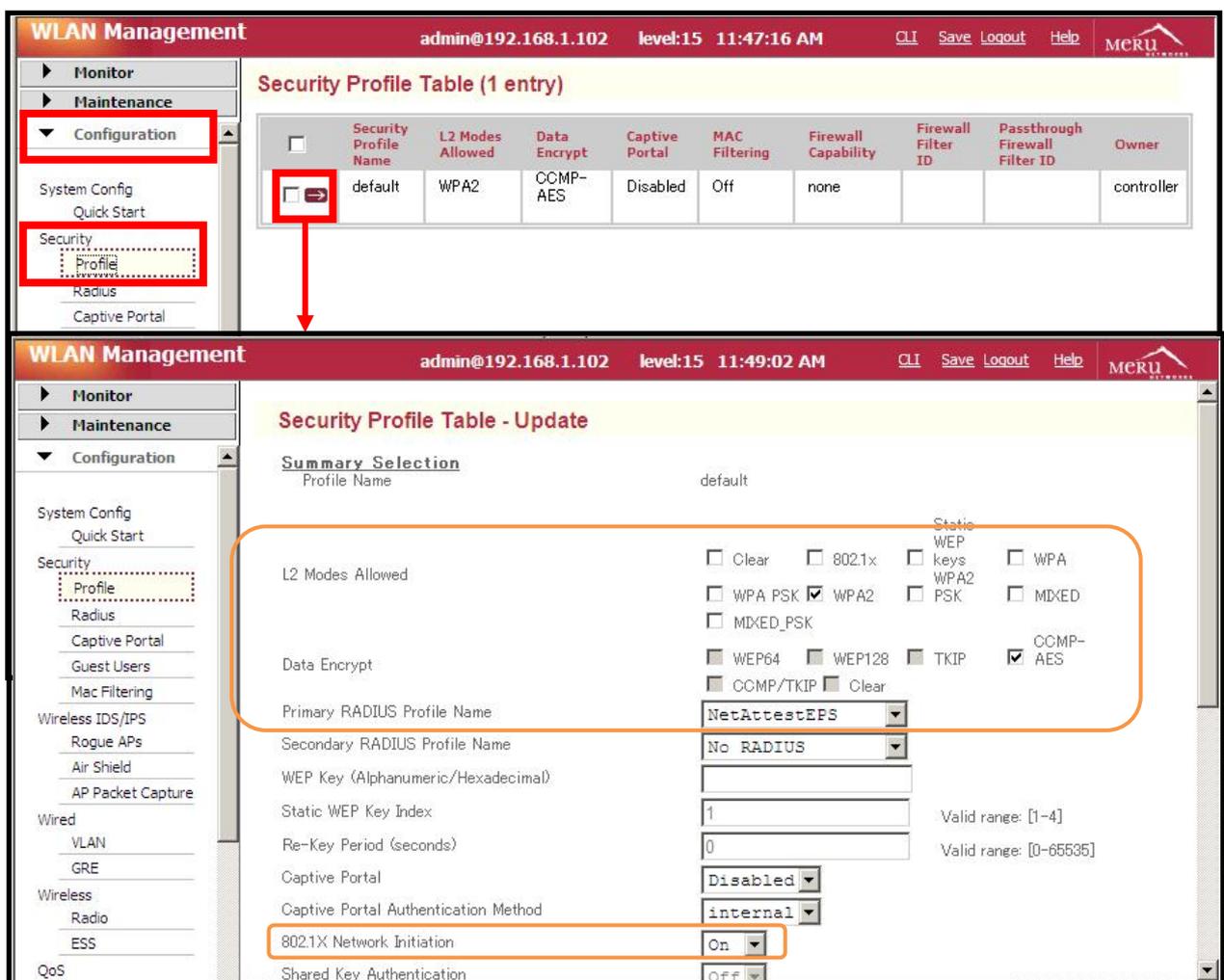
The screenshot displays the WLAN Management interface. The left sidebar menu has 'Maintenance' highlighted with a red box, and 'APs' under the 'Devices' section is also highlighted with a red box. The main content area shows the 'AP Table (1 entry)' with a table containing one entry for AP1020i. The table columns are: AP ID, AP Name, Serial Number, Uptime, Operational State, Availability Status, Runtime Image Version, Connectivity Layer, and AP Model. The entry for AP1020i shows it is online and has a runtime image version of 4.1-55.

AP ID	AP Name	Serial Number	Uptime	Operational State	Availability Status	Runtime Image Version	Connectivity Layer	AP Model
1	AP-1	000c:e6:09:96:89	00d:00h:17m:46s	Enabled	Online	4.1-55	L2	AP1020

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。



The screenshot shows the WLAN Management interface. The top part displays the 'Security Profile Table (1 entry)' with the following data:

Security Profile Name	L2 Modes Allowed	Data Encrypt	Captive Portal	MAC Filtering	Firewall Capability	Firewall Filter ID	Passthrough Firewall Filter ID	Owner
default	WPA2	CCMP-AES	Disabled	Off	none			controller

The bottom part shows the 'Security Profile Table - Update' form. The following settings are highlighted in orange boxes:

- L2 Modes Allowed:** WPA2 (checked)
- Data Encrypt:** CCMP-AES (checked)
- Primary RADIUS Profile Name:** NetAttestEPS
- 802.1X Network Initiation:** On

[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。

The screenshot displays the 'WLAN Management' interface for an MCRU device. The top navigation bar shows the user 'admin@192.168.1.102' and the time '2:50:46 PM'. The left sidebar is divided into 'Monitor', 'Maintenance', and 'Configuration'. The 'Configuration' menu is expanded, and the 'ESS' option is selected. The main content area is titled 'ESS Profile - Add' and contains the following configuration fields:

Field	Value	Notes
ESS Profile Name	Meru	Enter 1-32 chars., Required
Enable/Disable	Enable	
SSID	MeruTEST	Enter 0-32 chars.
Security Profile Name	default	
Primary RADIUS Accounting Server	No RADIUS	
Secondary RADIUS Accounting Server	No RADIUS	
Accounting Interim Interval (seconds)	3600	Valid range: [600-36000]
Beacon Interval (msec)	100	Valid range: [20-1000]
SSID Broadcast	On	
Bridging	<input type="checkbox"/> AirFortress <input type="checkbox"/> IPV6 <input type="checkbox"/> AppleTalk	
New AP's Join ESS	On	
Tunnel Interface Type	No Tunnel	
VLAN Name	No Data for VLAN Name	

【ESS Profile Name】

- Meru

【Enable/Disable】

- Enable

【SSID】

- MeruTEST

【Security Profile Name】

- default

4 クライアント PC の設定

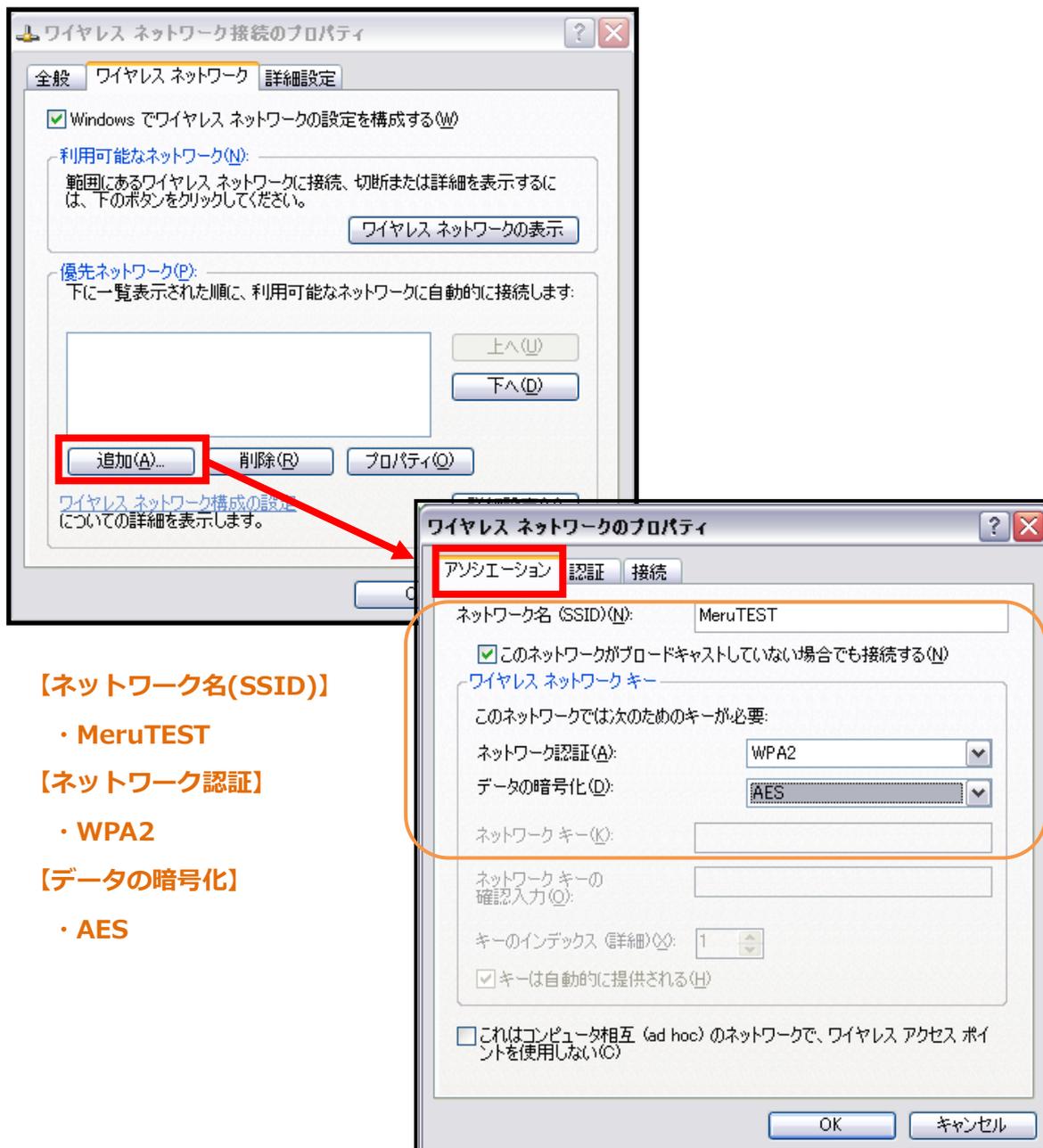
4-1 クライアント PC 設定の流れ

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

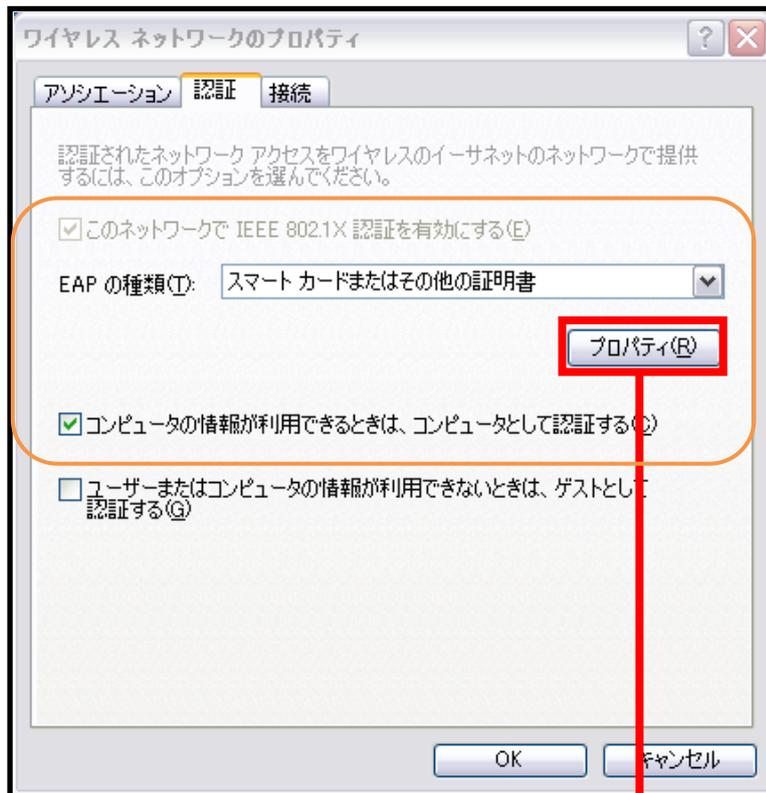
【ネットワーク認証】

- ・ WPA2

【データの暗号化】

- ・ AES

次ページへ

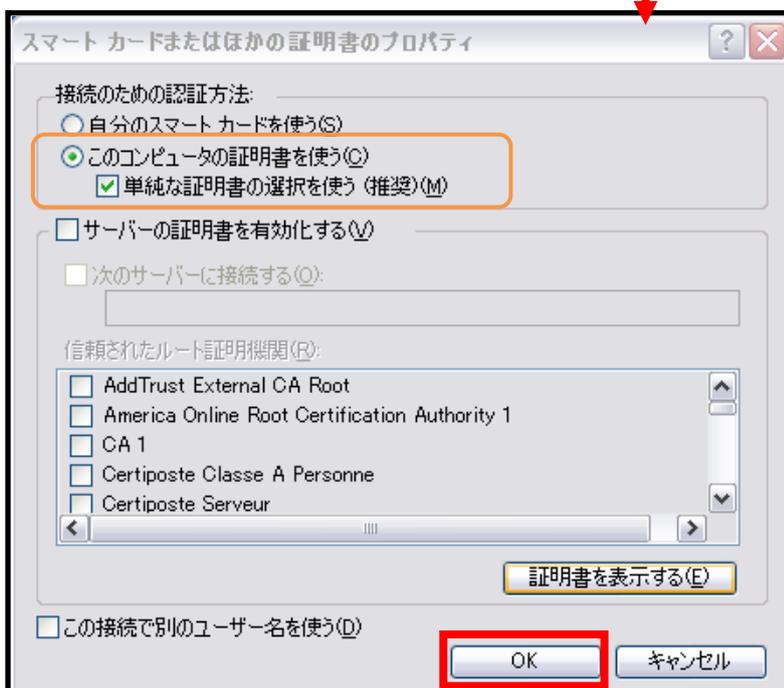


【EAP の種類】

- ・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。



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

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)

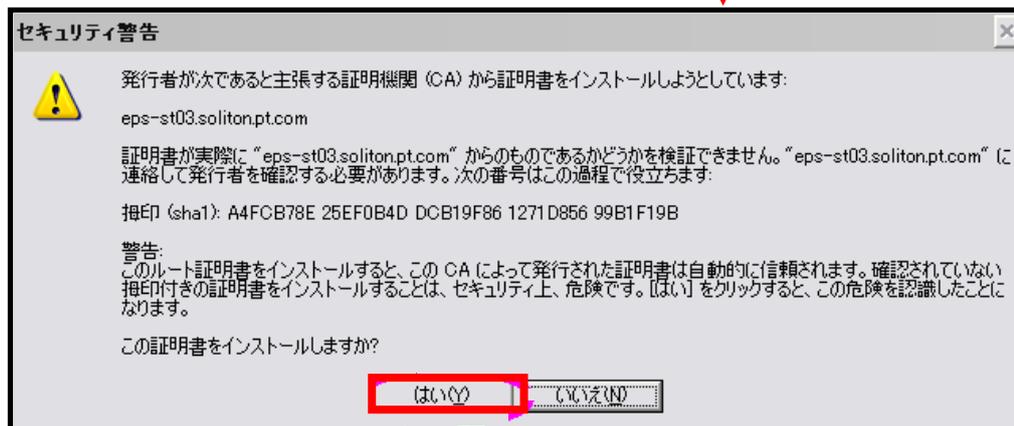
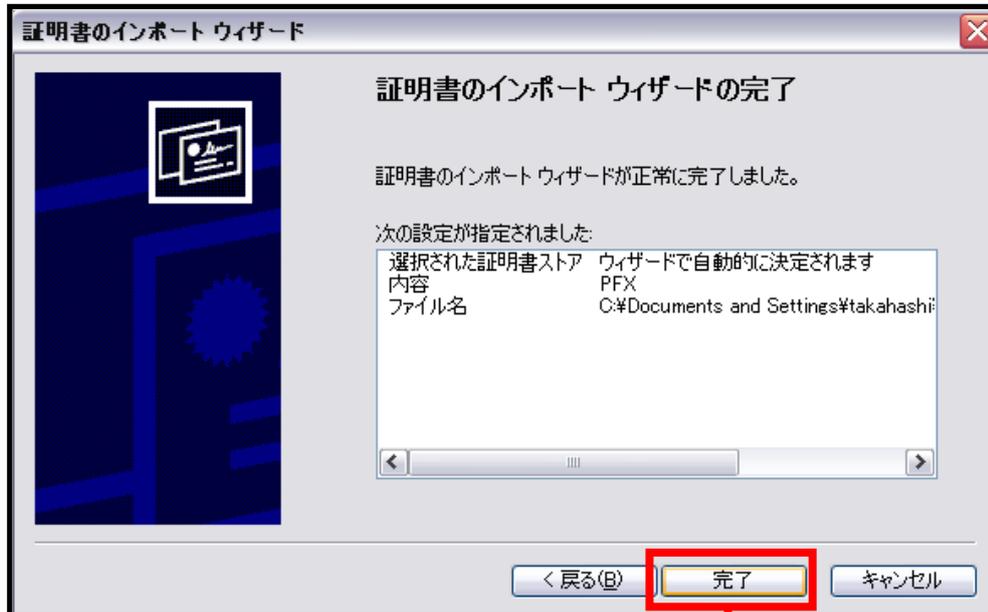
証明書ストア:
参照(R)...

< 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。

