

Net'Attest EPS 設定例

連携機器：

FortiGate-80C、FortiAP-220B

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 © 2010, Soliton Systems K.K. , All rights reserved.

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、フォーティネットジャパンの FortiGate-80C、FortiAP-220B との 802.1x 環境での接続について、その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とします。

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

本書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 FortiGate、FortiAP 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。

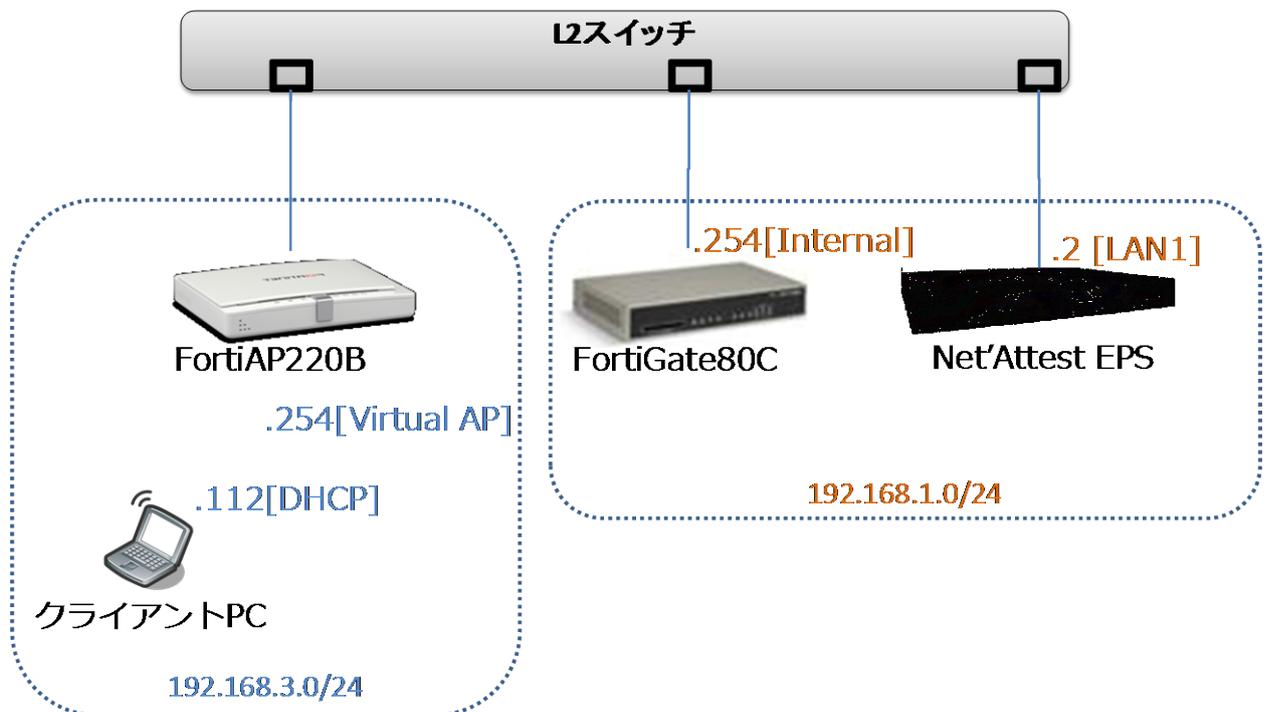
目次

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.....	10
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	FortiGate-80C/FortiAP-220B.....	15
3-1	FortiGate-80C/FortiAP-220B 設定の流れ.....	15
3-1	AP Profile、マネージド物理 AP の確認.....	16
3-2	RADIUS サーバの登録.....	17
3-3	バーチャル AP の登録.....	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
5	各機器 認証/接続ステータス.....	26
5-1	Net'Attest EPS 認証ステータス.....	26
5-2	FortiGate/FortiAP 接続成功時ステータス.....	27

1 構成

1-1 構成図

- ・有線LANで接続する機器はすべて、L2スイッチに収容
- ・無線LANは別セグメントで、FortiGateのDHCPサーバからIPアドレスを払いだす



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. 4.0.3
Authenticator (認証機器)	Fortinet	FortiGate-80C	Ver. 4.0 MR2
		FortiAP-220B	—
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	FortiGate-80C	FortiAP-220B	Client PC
IP アドレス	192.168.1.2/24	192.168.1.254/24 (Internal) 192.168.3.254/24 (Virtual-AP)	—	192.168.3.112 (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

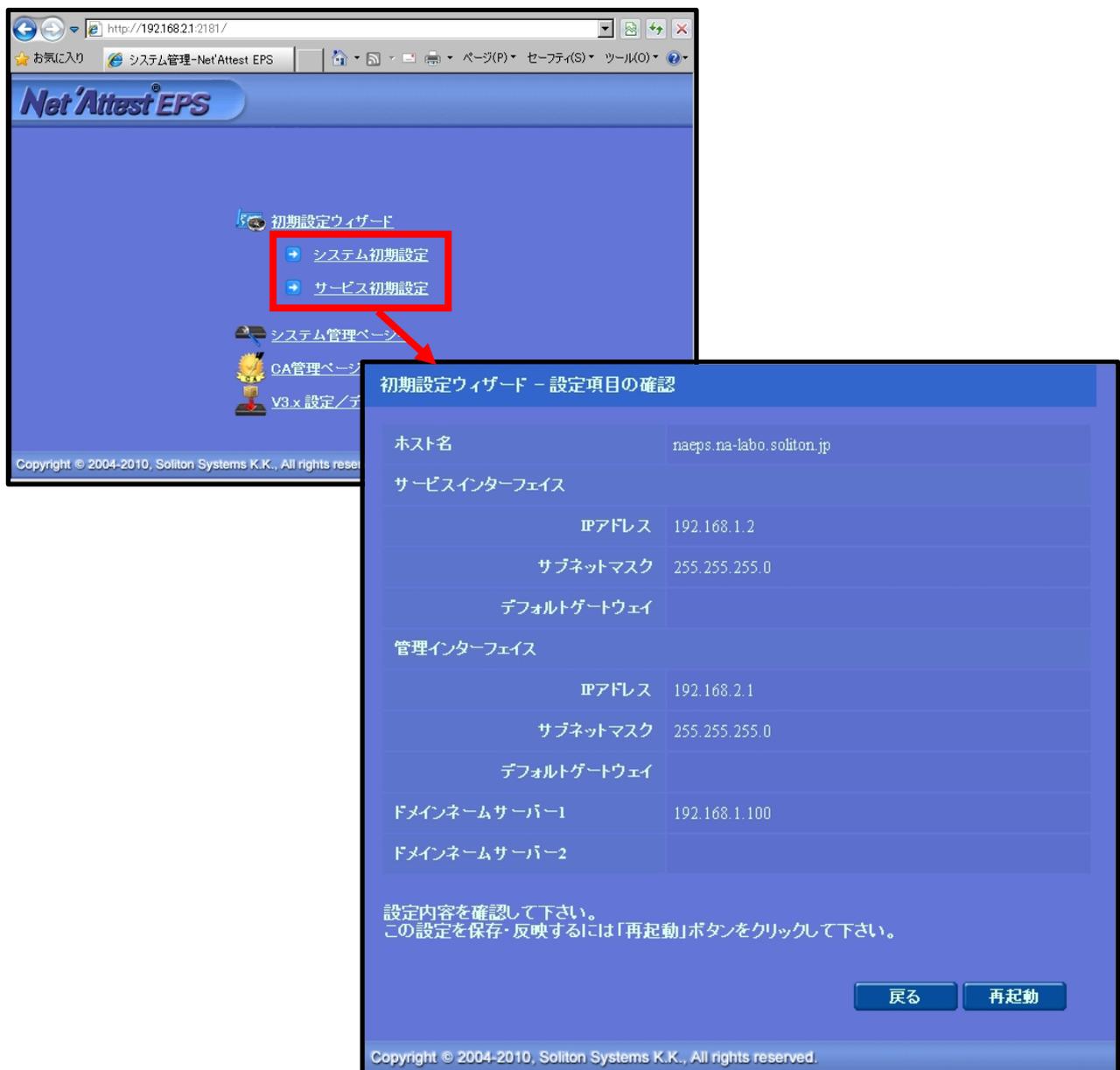
設定の流れ

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 - 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、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

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 navigation menu with 'NAS/RADIUSクライアント' selected. The main area shows a table of existing clients:

NAS/RADIUSクライアント名	IPアドレス	説明	操作
EdgeIron2402CE	192.168.1.25		更新 削除
ed100	192.168.1.52		更新 削除
test5511	192.168.1.51		更新 削除
FORTI60B	192.168.1.254		更新 削除

The modal dialog for adding a new client contains the following information:

- NAS/RADIUSクライアント名*: FORTI60B
- このNAS/RADIUSクライアントを有効にする
- 説明: [Empty field]
- IPアドレス*: 192.168.1.254
- シークレット*: [Masked field]
- 所属するNASグループ: [Dropdown menu]

Buttons at the bottom of the dialog are OK, キャンセル, and 適用.

【NAS/RADIUS クライアント名】

・ FORTI60B

【IP アドレス(Authenticator)】

・ 192.168.1.254

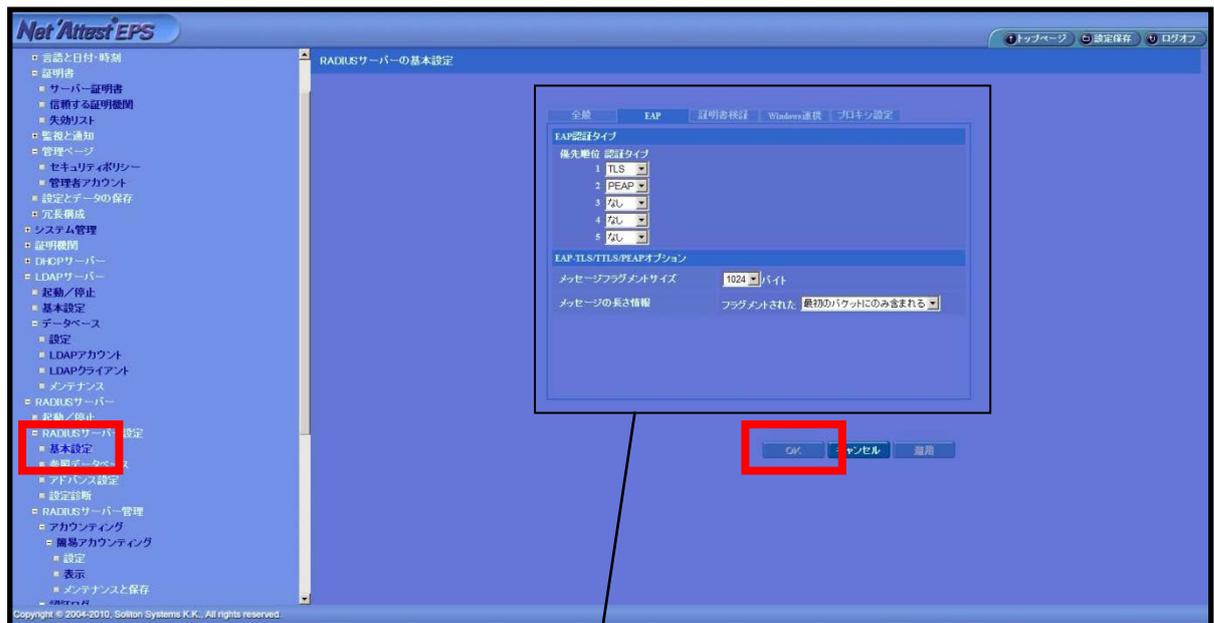
【シークレット】

・ soliton

2-5 RADIUS サーバ基本設定

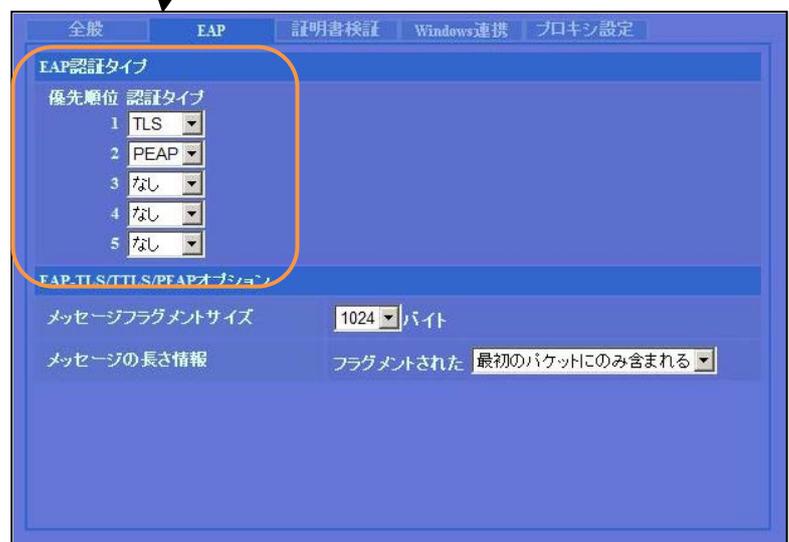
WebGUI より、RADIUS サーバの基本設定を行います。

「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 steps to register a user 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 with a red box.
- Step 2:** The 'ユーザー設定' (User Settings) form is displayed. The 'OK' button is highlighted with a red box.
- Step 3:** The 'ユーザー一覧' (User List) page is shown again, with the '実行' (Execute) button highlighted for the newly added user.

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

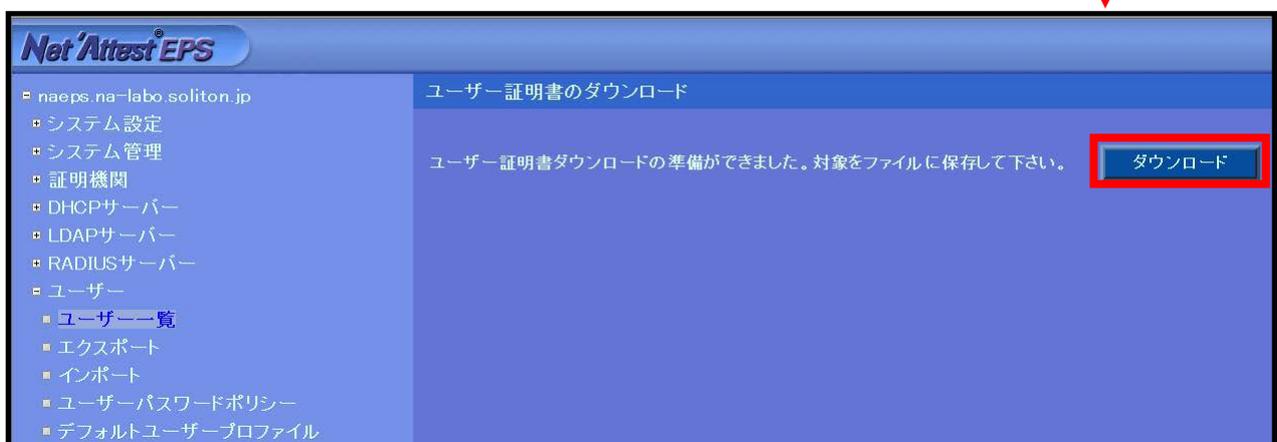
【証明書ファイルオプションパスワード】

- ・ password

【PKCS#12 ファイルに証明機関の・・・】

- ・ チェック有

The screenshot shows the configuration form for issuing a certificate. The '有効期限*' (Validity Period) is set to 365 days. The '証明書ファイルオプション' (Certificate File Option) section has the 'パスワード' (Password) field set to 'password' and the 'PKCS#12ファイルに証明機関の証明書を含める' (Include certificates of the CA in PKCS#12 file) checkbox checked. The '発行' (Issue) button is highlighted with a red box, and a red arrow points down to the next step.



3 FortiGate-80C/FortiAP-220B

3-1 FortiGate-80C/FortiAP-220B 設定の流れ

設定の流れ

1. RADIUS サーバの登録
2. virtual-AP の設定

3-2 AP Profile、マネージド物理 AP の確認

既に基本接続設定は終了している為、

「AP Profile」 および「マネージド物理 AP」 は下記のように設定されています。

AP Profile 設定

FortiGate 80C

名前: FTNT_JP
 コメント: (最大半角63文字)
 Geography: Japan

Radio 1

Mode: Disable Access Point Dedicated Monitor
 Background Scan:
 Band: 802.11g
 Channel: Auto
 TX Power: 3 (1 - 17 dBm)
 Virtual AP: Available Selected
 FTNT_JP

Radio 2

Mode: Disable Access Point Dedicated Monitor

OK キャンセル

マネージド物理 AP 設定

FortiGate 80C

アドミン	名前	AP Profile	クライアント	参加時間	Reset
✓	SOLSOL	FTNT_JP	0	10/07/10 09:42	⚙️

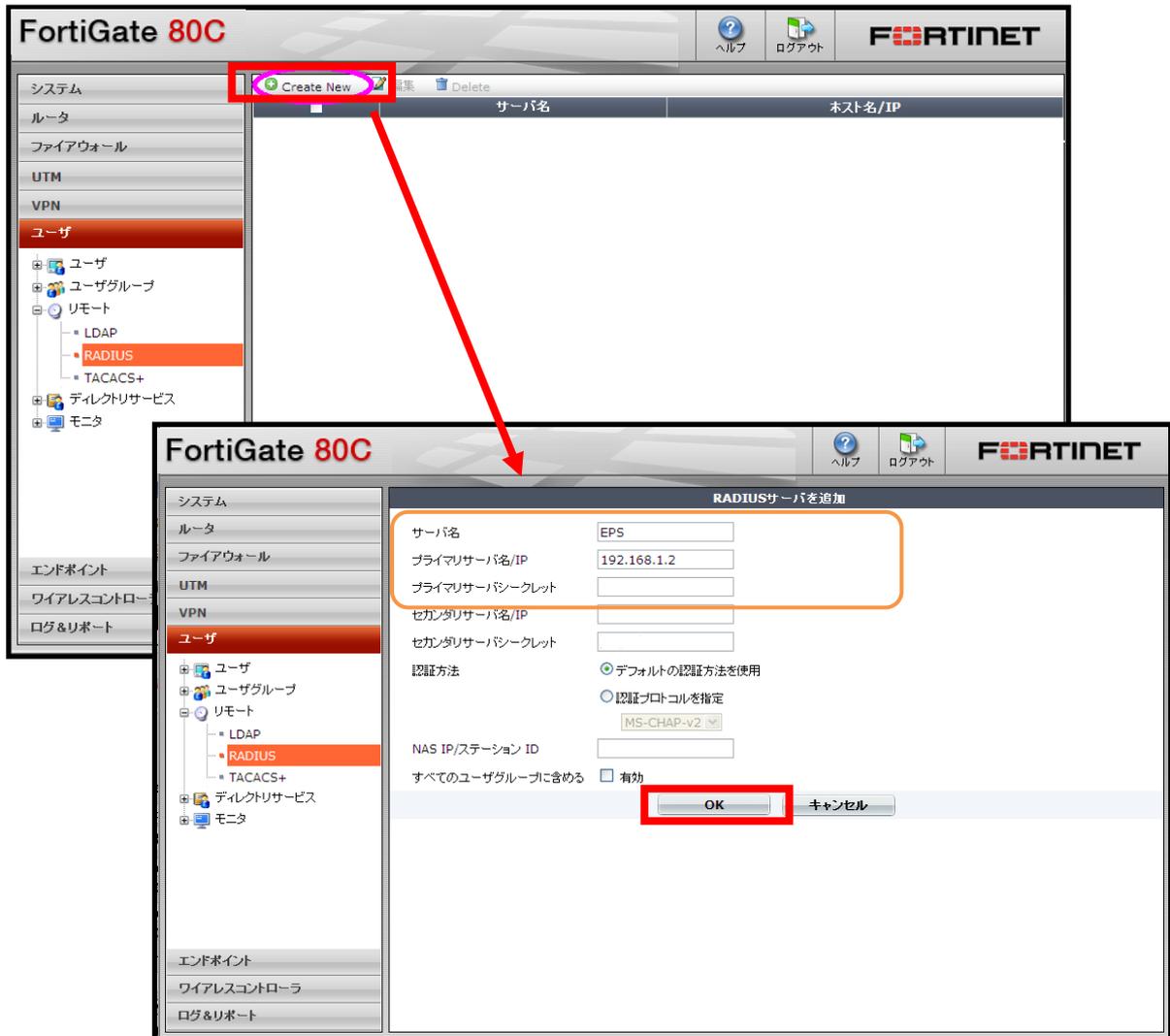
アドミン 名前 AP Profile クライアント 参加時間 Reset

✓ SOLSOL FTNT_JP 0 10/07/10 09:42 ⚙️

3-3 RADIUS サーバの登録

WebGUI より、RADIUS サーバの登録を行います。

「ユーザ」 → 「リモート」 → 「RADIUS」 から、「Create New」を押下し、RADIUS サーバの登録を行います。



【サーバ名】

- ・ EPS

【プライマリサーバ名/IP (Authentication Server)】

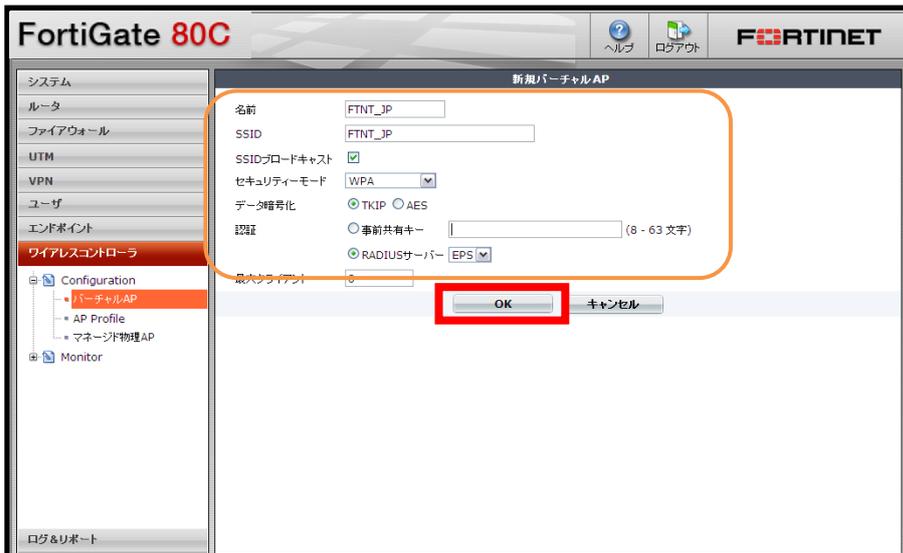
- ・ 192.168.1.2

【プライマリサーバシークレット】

- ・ soliton

3-4 バーチャル AP の登録

「ワイアレスコントローラ」の設定にて「Configuration」→「バーチャル AP」から「Create New」を押下し、バーチャル AP の追加を行います



【名前】

- ・ FINT_JP

【SSID】

- ・ FINT_JP

【SSIDブロードキャスト】

- ・ チェック有

【セキュリティモード】

- ・ WPA

【データ暗号化】

- ・ TKIP

【RADIUS サーバ】

- ・ EPS

4 クライアント PC の設定

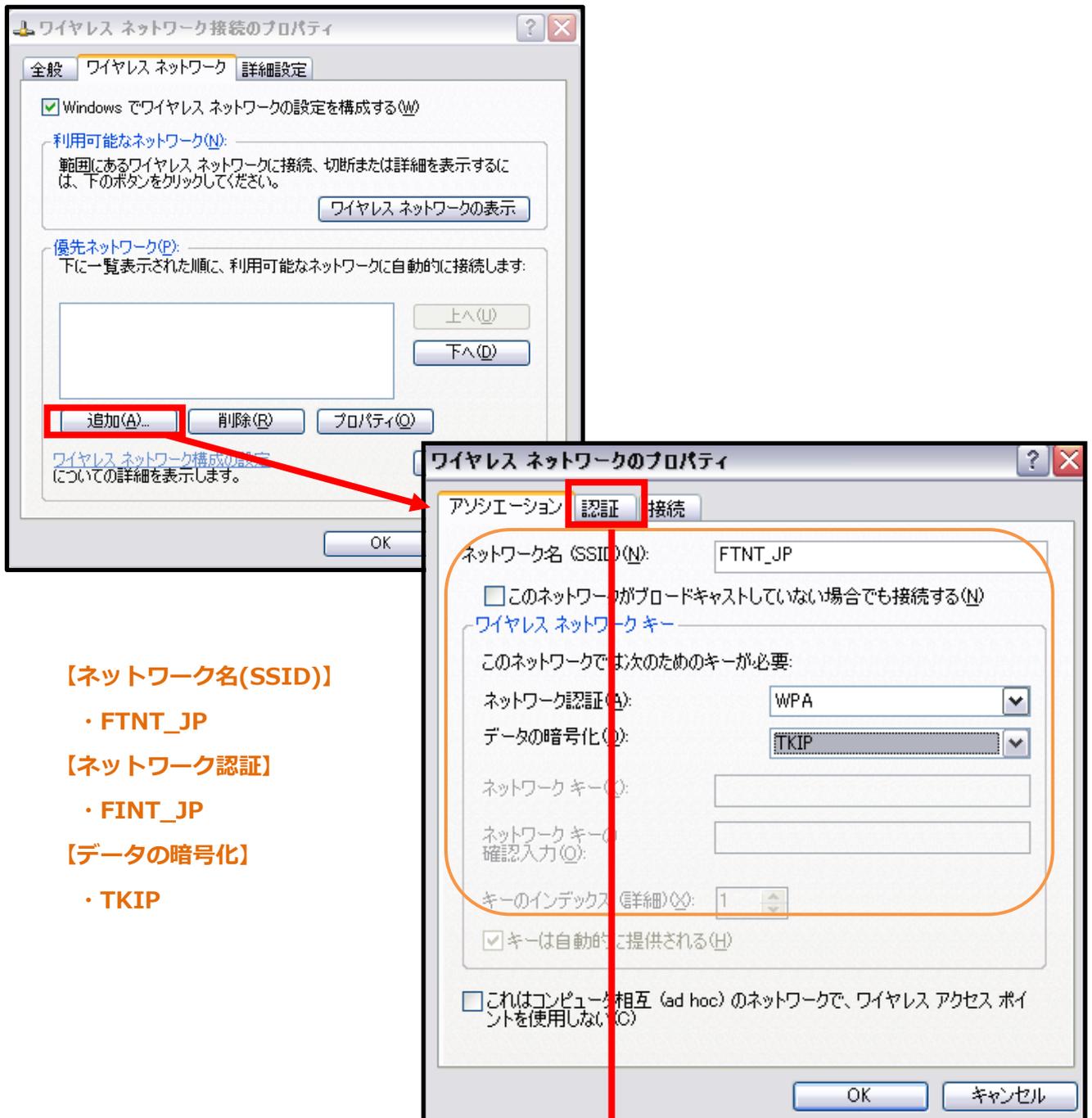
4-1 クライアント PC 設定の流れ

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)】

- ・ FTNT_JP

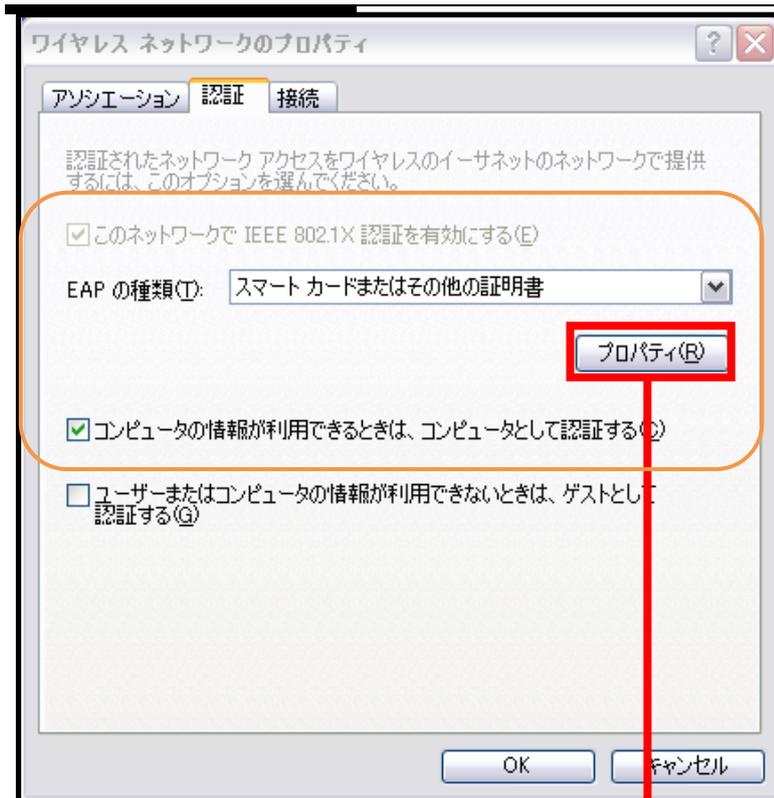
【ネットワーク認証】

- ・ WPA

【データの暗号化】

- ・ TKIP

次ページへ

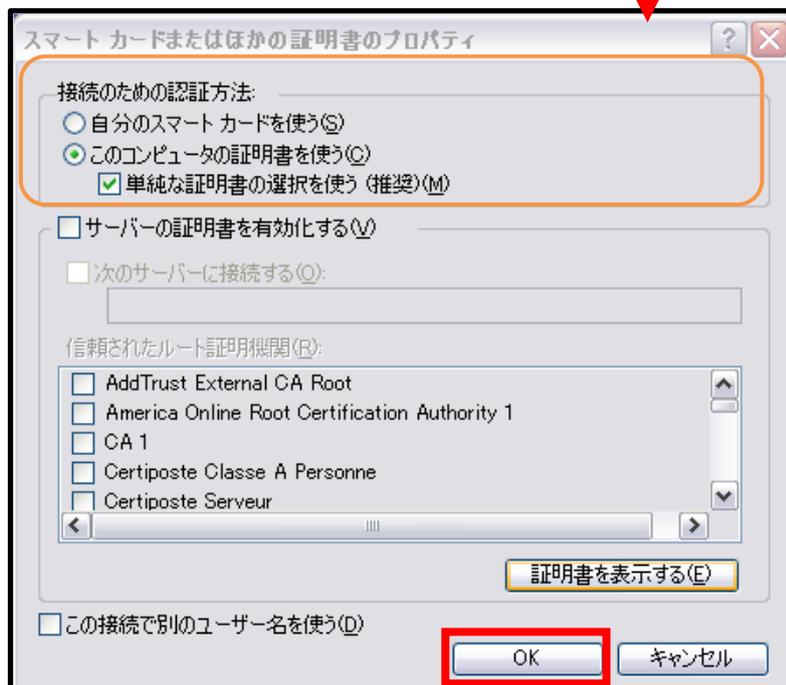


【EAP の種類】

- ・スマートカードまたはその他の証明書設定

【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

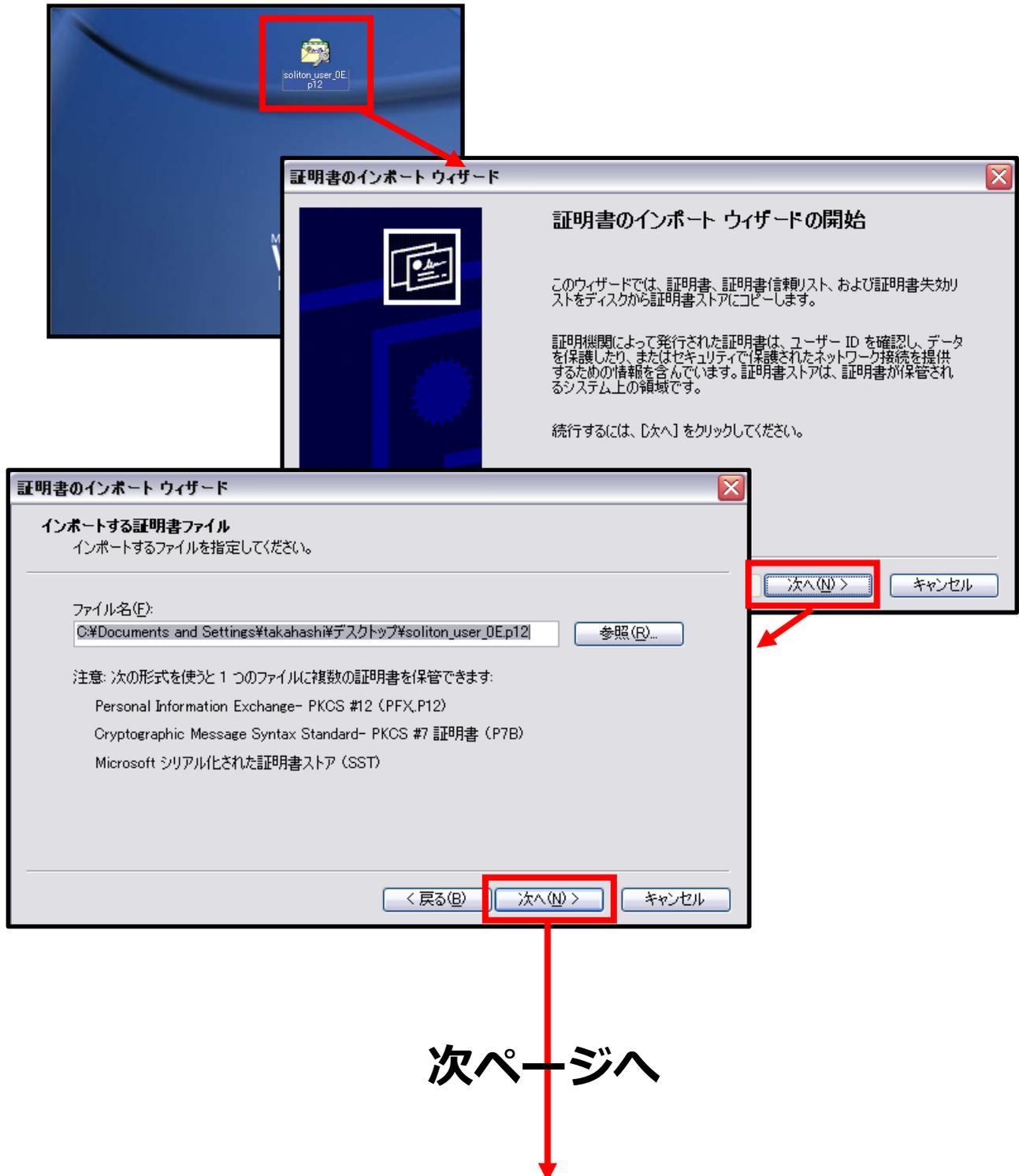
【単純な証明書の選択を使う】

- ・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)

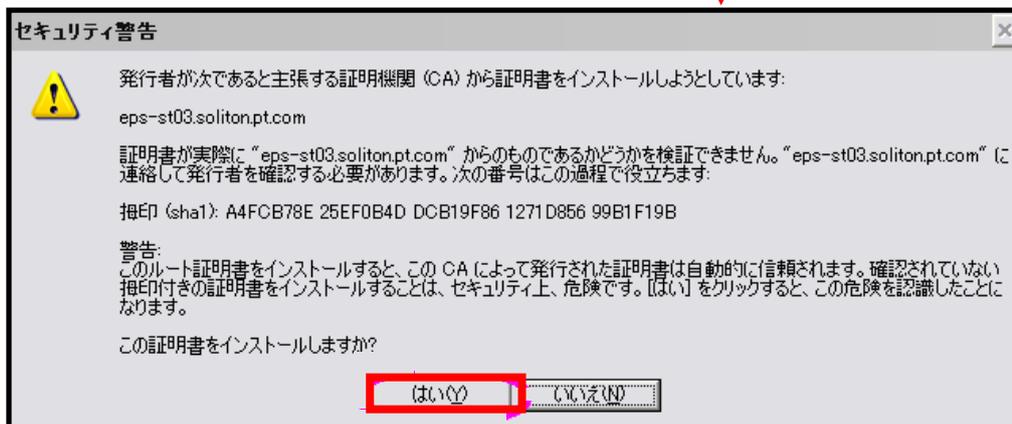
証明書ストア:
参照(R)...

< 戻る(B) **次へ(N) >** キャンセル

【証明書の種類に基づいて・・・】

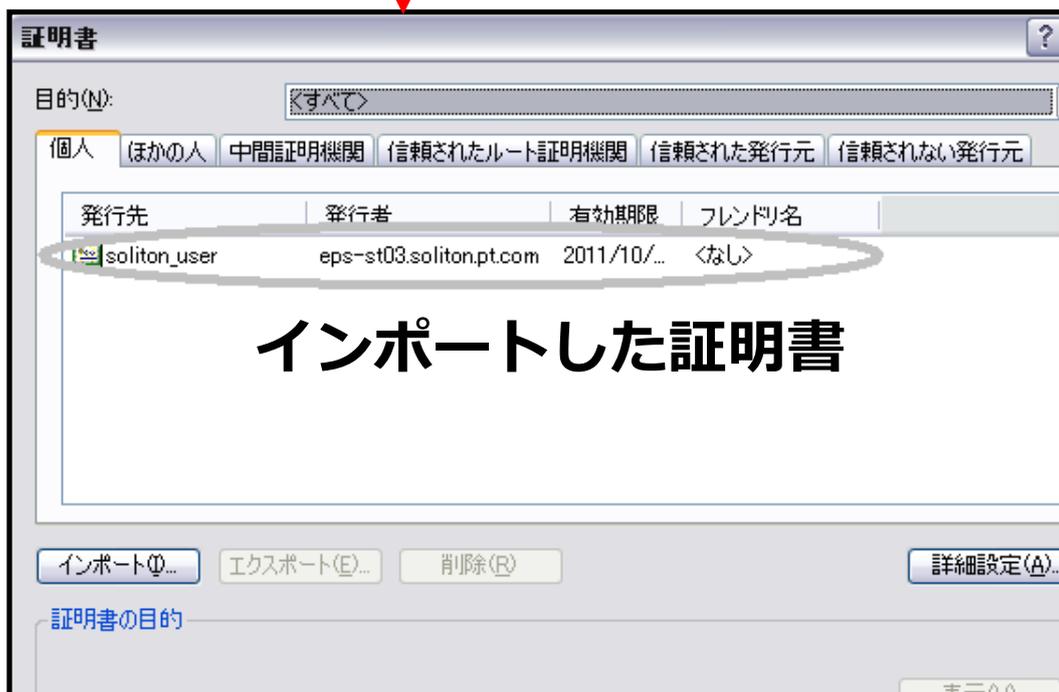
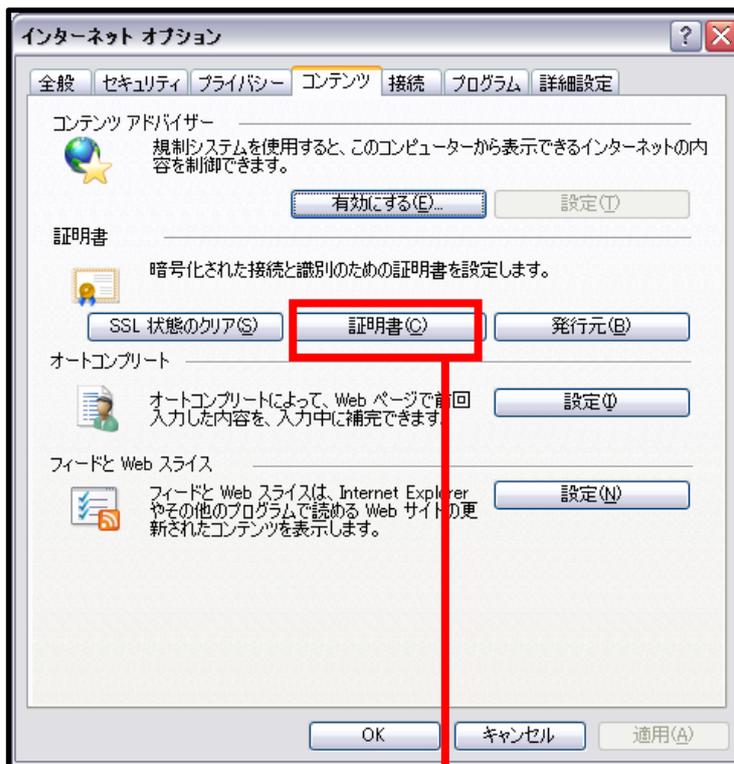
・ チェック有

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。



5 各機器 認証/接続ステータス

5-1 Net'Attest EPS 認証ステータス

「RADIUS サーバ」 → 「RADIUS サーバ管理」 → 「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。

The screenshot shows the Net'Attest EPS web interface. The left sidebar contains a navigation menu with the following items:

- eps-st03.soliton.pt.com
- システム設定
- システム管理
- 証明機関
- DHCPサーバー
- LDAPサーバー
- RADIUSサーバー
 - 起動/停止
 - RADIUSサーバー設定
 - RADIUSサーバー管理
 - アカウントing
 - 認証ログ
 - 設定
 - 表示
 - メンテナンスと保存
 - セッション管理
 - ライセンス
- NAS/RADIUSクライアント
- RADIUSプロファイル/グループ
- ユーザー

The main content area displays the '認証ログの表示' (Display Authentication Log) page. It features a table with the following columns: 日時 (Date/Time), 種別 (Type), Priority, and イベント (Event). The table contains five entries, all of which are successful logins (Login OK) for the user 'soliton_user' via EAP authentication.

日時	種別	Priority	イベント
Oct 12 11:22:07	radiusd[2220]		Login OK: [soliton_user/<via Auth-Type = EAP>] (from client FORTI60B port 0 cli 00-16-6F-60-3B-36)
Oct 12 11:22:07	radiusd[2220]		Login OK: [soliton_user/<via Auth-Type = EAP>] (from client FORTI60B port 0 cli 00-16-6F-60-3B-36 via TLS tunnel)
Oct 12 11:09:39	radiusd[2220]		Login OK: [soliton_user/<via Auth-Type = EAP>] (from client FORTI60B port 0 cli 00-16-6F-60-3B-36)
Oct 12 11:09:39	radiusd[2220]		Login OK: [soliton_user/<via Auth-Type = EAP>] (from client FORTI60B port 0 cli 00-16-6F-60-3B-36 via TLS tunnel)
Oct 12 10:58:09	radiusd[2220]		Login OK: [soliton_user/<via Auth-Type = EAP>] (from client FORTI60B port 0 cli 00-16-6F-60-3B-36)
Oct 12 10:58:09	radiusd[2220]		Login OK: [soliton_user/<via Auth-Type = EAP>] (from client FORTI60B port 0 cli 00-16-6F-60-3B-36 via TLS tunnel)

Copyright © 2004-2010, Soliton Systems K.K., All rights reserved.

5-2 FortiGate/FortiAP 接続成功時ステータス

「ワイアレスコントローラ」→「MONITOR」→「ワイアレスクライアント」を選択します。

下記のように、接続に成功したクライアントのIPアドレスなどを確認することができます。

The screenshot displays the FortiGate 80C web interface. The left sidebar shows the navigation menu with 'ワイアレスコントローラ' (Wireless Controller) selected, and 'Monitor' > 'ワイアレスクライアント' (Wireless Clients) highlighted. The main content area shows a table of connected wireless clients.

IP	物理 AP	バーチャル AP	バンド幅 Tx/Rx	信号強度/ノイズ	接続確立時間
192.168.3.112	SOLSOL	FTNT_JP	1 Kbps	50 dB	10/07/10 23:05

At the bottom of the interface, there are navigation controls showing '1 / 1' and buttons for '[カラム設定]' (Column Settings) and '[すべてのフィルタをクリア]' (Clear all filters).

以上

