

NetAttest EPS 設定例

連携機器：

アライドテレシス AT-TQ2403

Case：TLS 方式での認証

Version 1.1

NetAttest®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 サーバーアプライアンス NetAttest EPS とアライドテレシス社製 無線アクセスポイント AT-TQ2403 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、NetAttest EPS 及び AT-TQ2403 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。

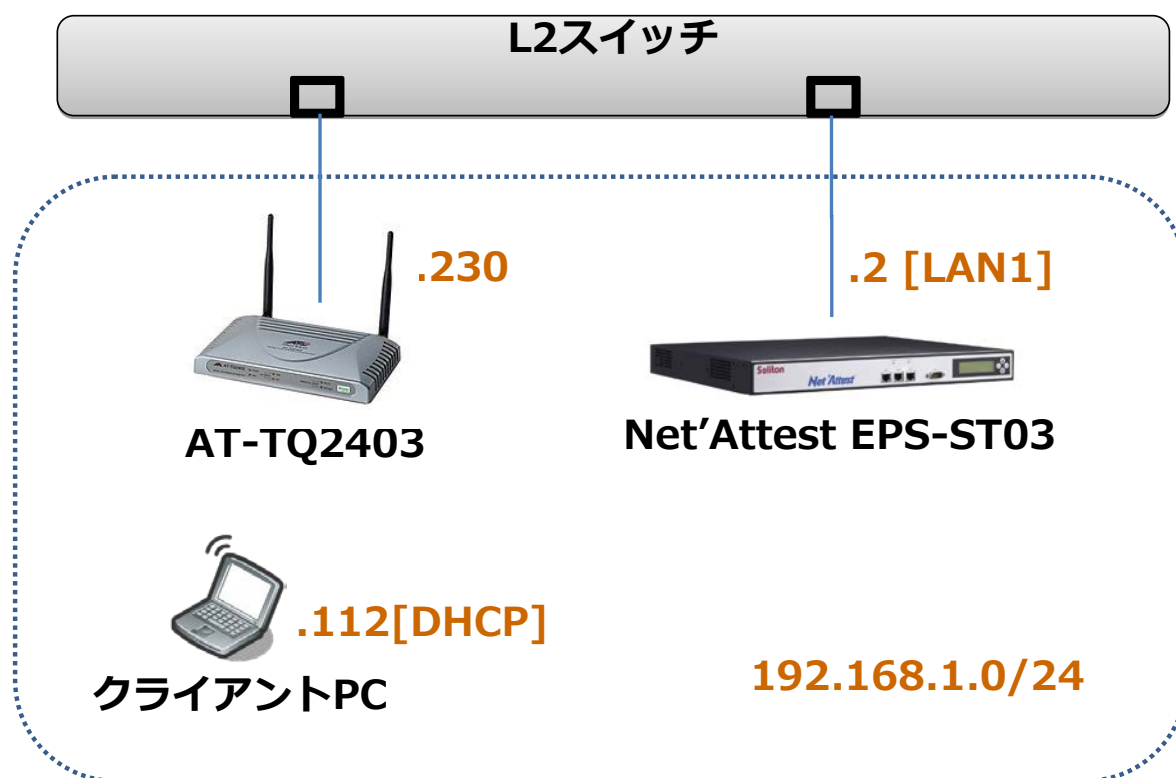
目次

1	構成	6
1-1	構成図.....	6
1-2	環境.....	7
2	NetAttest EPS	8
2-1	NetAttest 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	アライドテレシス AT-TQ2403	15
3-1	アライドテレシス AT-TQ2403 設定の流れ	15
3-2	管理アクセス用パスワード設定および SSID 設定	16
3-3	セキュリティ設定の変更	17
4	クライアント PC の設定.....	18
4-1	クライアント PC 設定の流れ.....	18
4-2	ワイヤレスネットワーク接続先の登録.....	19
4-3	ユーザー証明書のインポート	21
4-4	インポートされたユーザー証明書の確認.....	24

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	NetAttest EPS ST-03	Ver. 4.2.1
Authenticator (認証機器)	アライドテレシス	AT-TQ2403	Ver. 3.0.2
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	AT-TQ2403	Client PC
IP アドレス	192.168.1.2/24	192.168.1.230/24	192.168.1.112 (DHCP)
RADIUS port (Authentication)	UDP 1812		
RADIUS port (Accounting)	UDP 1813		
RADIUS Secret (Key)	password		

2 NetAttest EPS

2-1 NetAttest 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

システム管理ページへ
CA管理ページへ
V3.x 設定 / データのリストア

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

初期設定ウィザード - 設定項目の確認

ホスト名	na-eps-421.local
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 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
 内部で新しい鍵を生成する
公開鍵方式: RSA
鍵長: 2048
 外部HSMデバイスの鍵を使用する

CA情報
CA名(必須): na-eps-421-ca
国名: 日本
都道府県名: 東京都
市区町村名: 新宿区
会社名(組織名): ソリトンシステムズ
部署名:
E-mailアドレス:
CA署名設定
署名アルゴリズム: SHA1
有効日数: 3650

初期設定ウィザード - LDAPデータベースの設定

編集対象: LocalLdap01
名前: LocalLdap01
サフィックス: dc=local
説明:
データベースの再構築
データベースの再構築

戻る 次へ

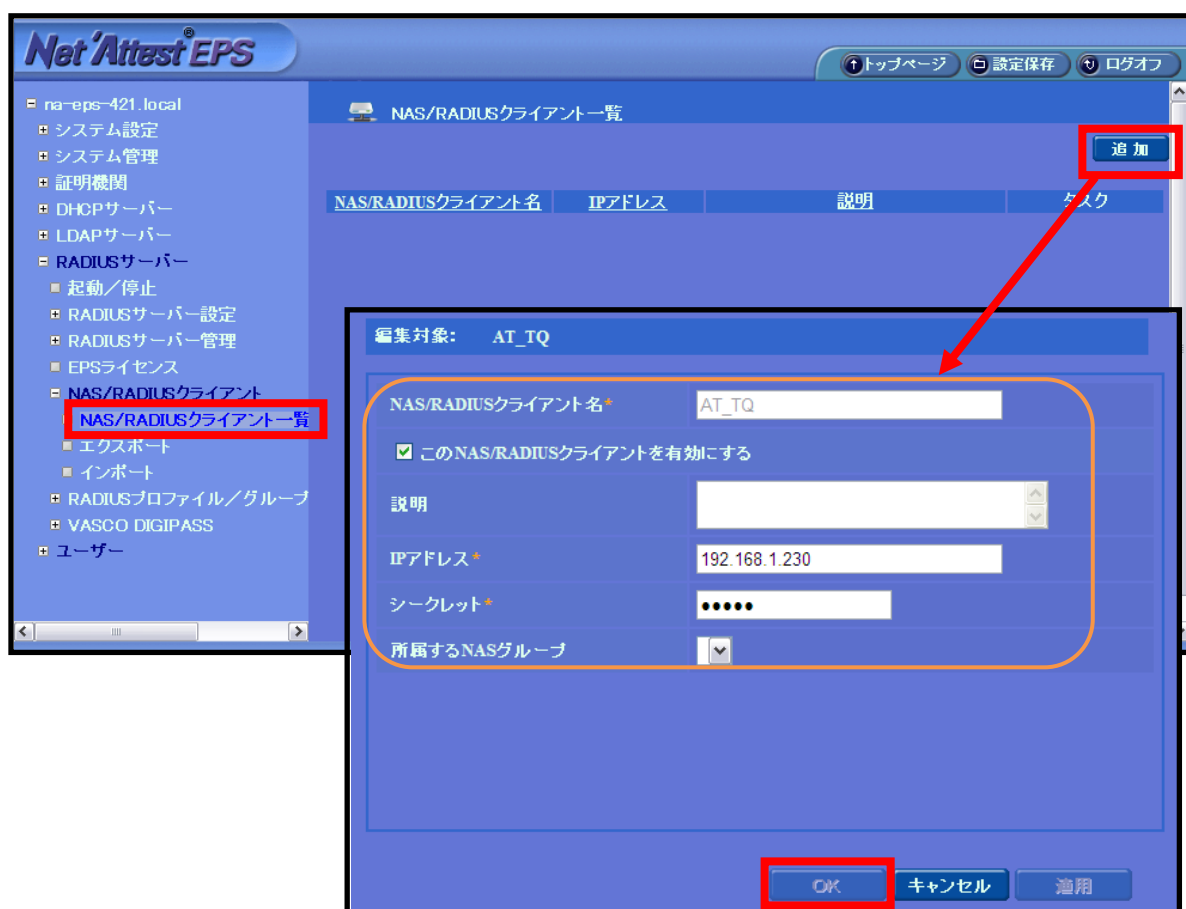
初期設定ウィザード - RADIUSサーバーの基本設定

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。



【NAS/RADIUS クライアント名】

- ・ AT_TQ

【IP アドレス(Authenticator)】

- ・ 192.168.1.230

【シークレット】

- ・ password

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。

The screenshot displays the Net Attest EPS WebGUI interface. The left sidebar shows a navigation menu with 'RADIUSサーバ設定' expanded to '基本設定'. The main content area is titled 'RADIUSサーバの基本設定' and has tabs for '全般', 'EAP', '証明書検証', 'Windows連携', and 'プロキシ設定'. The 'EAP' tab is active, showing a table for 'EAP認証タイプ' with 5 rows. The first row is highlighted with an orange box, showing priority 1 and type 'TLS'. Below the table are sections for 'EAP-TLS/TTLS/PEAPオプション' and 'EAP-TTLS/PEAPオプション' with various configuration options.

優先順位	認証タイプ
1	TLS
2	なし
3	なし
4	なし
5	なし

【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 in red.
- Step 2:** Access the 'ユーザー設定' (User Settings) page. The '姓' (Surname) field is highlighted in orange.
- Step 3:** Access the 'ユーザー一覧' (User List) page. The 'w_user1' user is selected, and the '発行' (Issue) button is highlighted in red.

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

ユーザー一覧

名前	ユーザーID	証明書	タスク
w_user1	w_user1		発行 変更 削除

編集対象: w_user1

基本情報

姓: w_user1

名:

E-Mail:

詳細情報

認証情報

ユーザーID: w_user1

有効期限*

● 日数 365 日

● 日付 2012 年 2 月 24 日 23 時 59 分 59 秒まで

証明書ファイルオプション

パスワード:

パスワード(確認):

*パスワードが空欄の場合は、ユーザーのパスワードを使用します。

PKCS#12ファイルに証明機関の証明書を含める

発行 キャンセル

ユーザー証明書のダウンロード

ユーザー証明書ダウンロードの準備ができました。対象をファイルに保存して下さい。

ダウンロード

3 アライドテレシス AT-TQ2403

3-1 アライドテレシス AT-TQ2403 設定の流れ

本書では、Web GUI を利用して AT-TQ2403 の各種設定を実施する方法を紹介
します。

設定の流れ

1. 管理アクセス用パスワード設定および SSID 設定
2. 内部ネットワーク セキュリティー設定

3-2 管理アクセス用パスワード設定および SSID 設定

機器、初回ログイン時、管理アクセス用パスワードの設定と SSID の設定が求められます。適宜設定し、『適用』ボタンを押下します。

また、IP アドレスはデフォルト設定で 192.168.1.230 になっていますが、今回は初期設定を流用します。

基本設定

1 このアクセスポイントの情報を確認してください ...
このアクセスポイント固有の情報には以下のとおりです。

IPアドレス:	192.168.1.230
MACアドレス:	00:09:41:E8:17:40
ファームウェアのバージョン:	3.1.0
起動からの経過時間:	01:03:33

2 ネットワークの設定を入力してください ...
以下の設定はこのアクセスポイントに適用されます。同じ設定が、クラスターに参加する新しいアクセスポイントにも適用されます。

現在のパスワード	✓
新しいパスワード	✓
新しいパスワードの確認	✓
ネットワーク名(SSID)	allied	✓

3 設定 ...
この設定を保存するには「適用」をクリックしてください。

適用

【現在のパスワード】

- ・ friend (※初期パスワード)

【新しいパスワード】、【新しいパスワードの確認】

- ・ 適宜

【ネットワーク名 (SSID)】

- ・ allied

3-3 セキュリティー設定の変更

設定メニューの「セキュリティー」から RADIUS 関連、無線認証関連の設定を行います。

内部ネットワーク セキュリティー設定の変更

SSIDのブロードキャスト 無線クライアントの分離

モード: WPAエンタープライズ

WPAバージョン: WPA WPA2
 事前認証を有効にする

暗号スイート: TKIP CCMP (AES)

内蔵RADIUSサーバーを使う

RADIUS IP: 192.168.1.2
 ポート番号: 1812
 RADIUSキー: ●●●●●●●●

セカンダリーRADIUS IP: 0.0.0.0
 ポート番号: 1812
 RADIUSキー: ●●●●●●●●

RADIUSアカウントングを有効にする
 Dynamic VLANでVLAN IDを必須とする

適用

【SSIDのブロードキャスト】

- ・チェックなし

【無線クライアントの分離】

- ・チェックあり

【モード】

- ・WPAエンタープライズ

【WPAバージョン】

- ・WPA2のみチェックあり

【暗号スイート】

- ・CCMP(AES) チェックあり

【内蔵RADIUSサーバーを使う】

- ・チェックなし

【RADIUS IP】

- ・192.168.1.2

【ポート番号】

- ・1812

【RADIUSキー】

- ・password

4 クライアント PC の設定

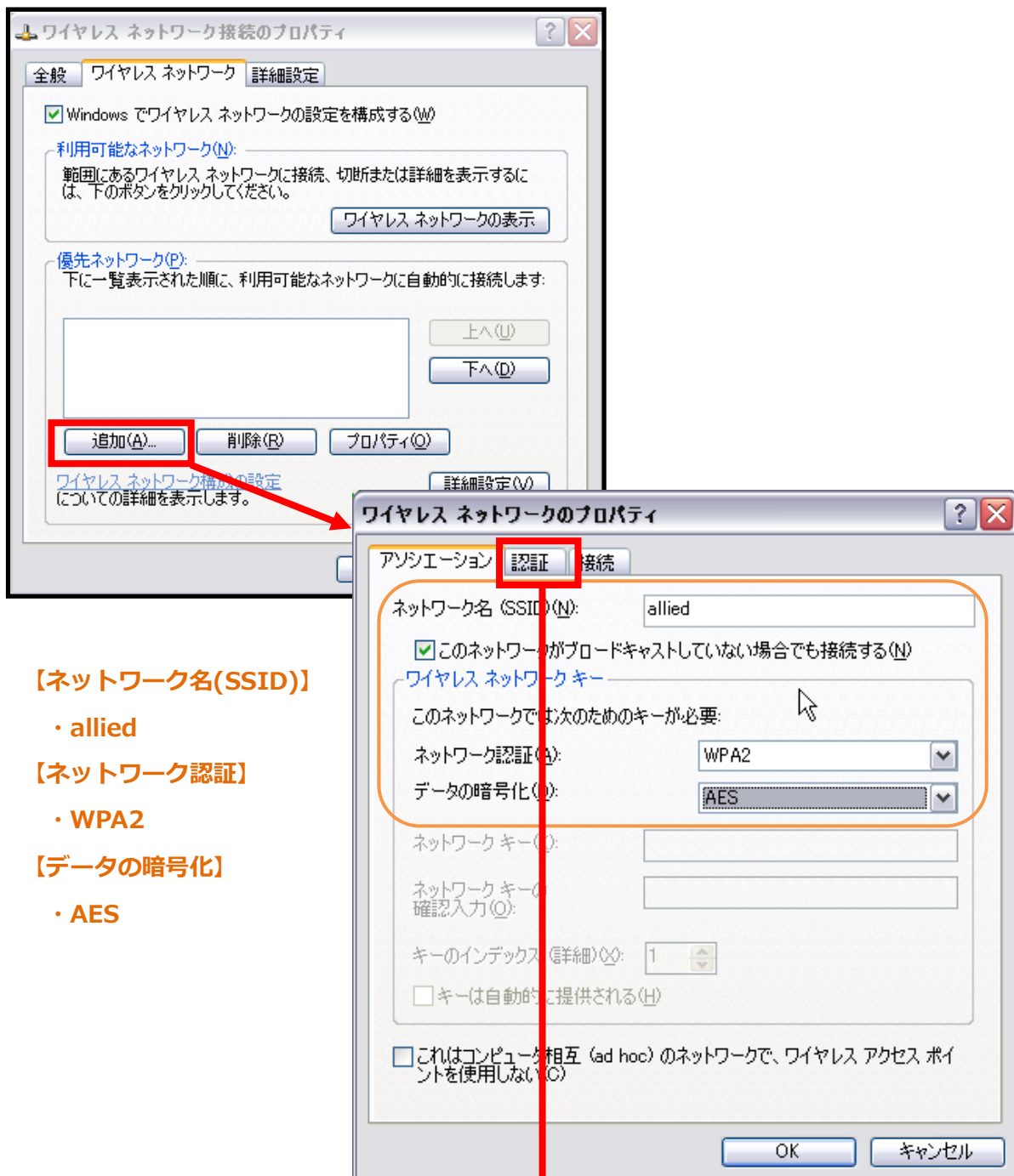
4-1 クライアント PC 設定の流れ

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)】

- ・ allied

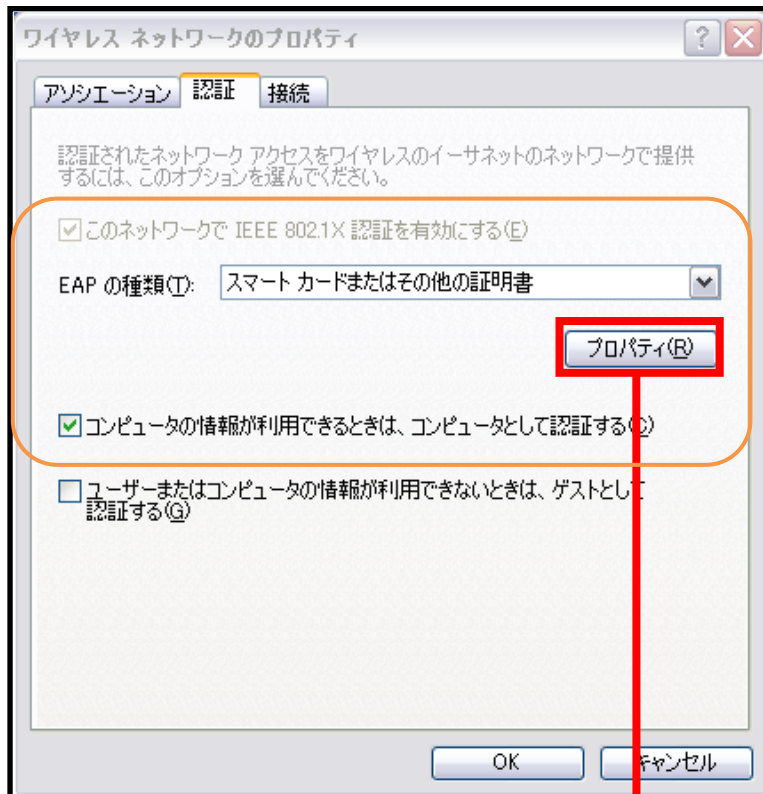
【ネットワーク認証】

- ・ WPA2

【データの暗号化】

- ・ AES

次ページへ

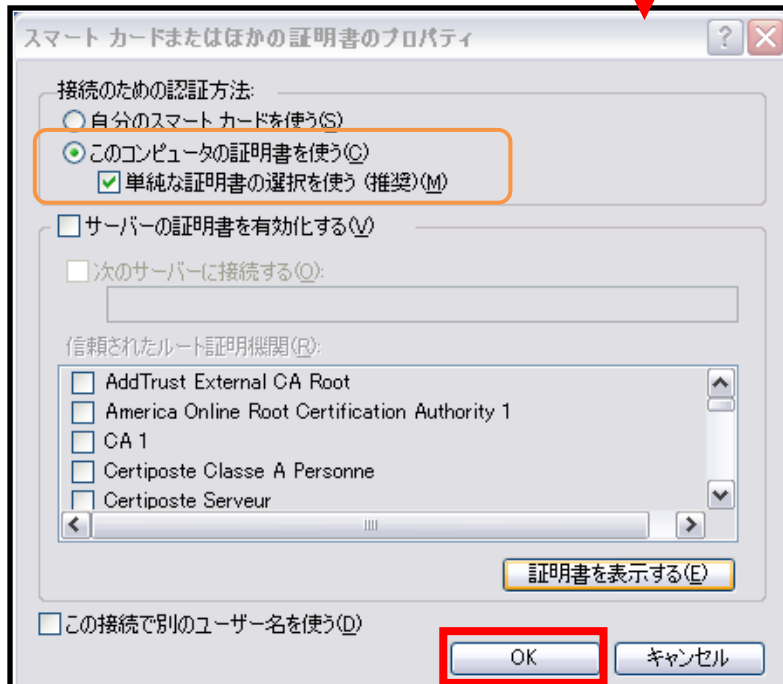


【EAP の種類】

- ・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

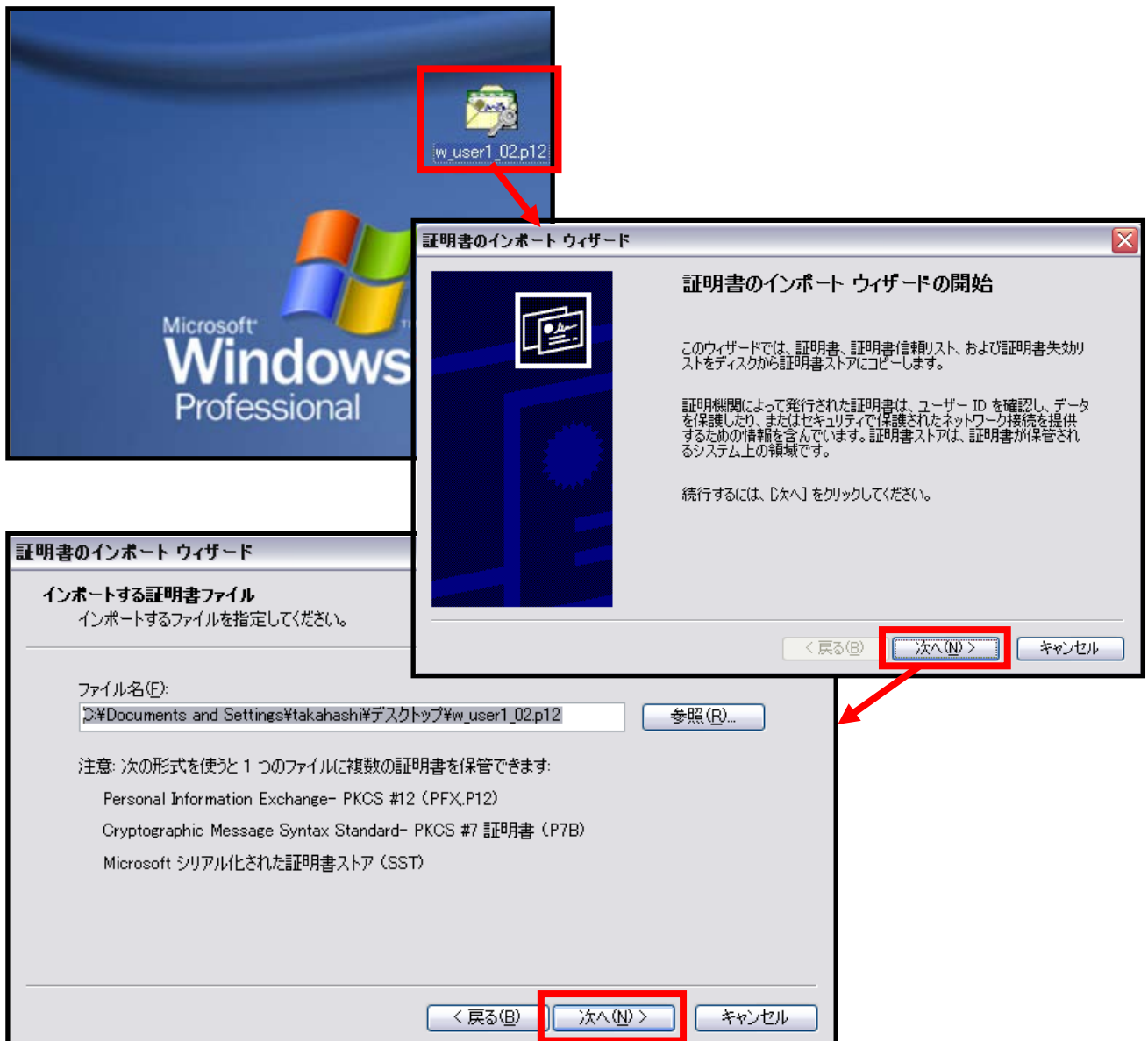
【単純な証明書の選択を使う】

- ・チェック有

4-3 ユーザー証明書のインポート

NetAttest 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。



次ページへ

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

NetAttest 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)

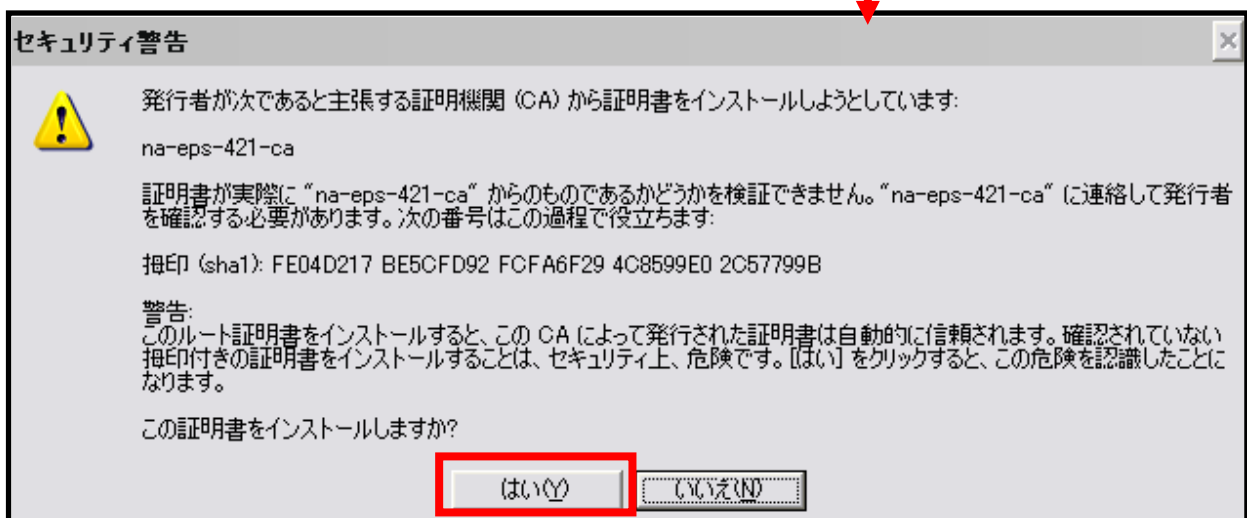
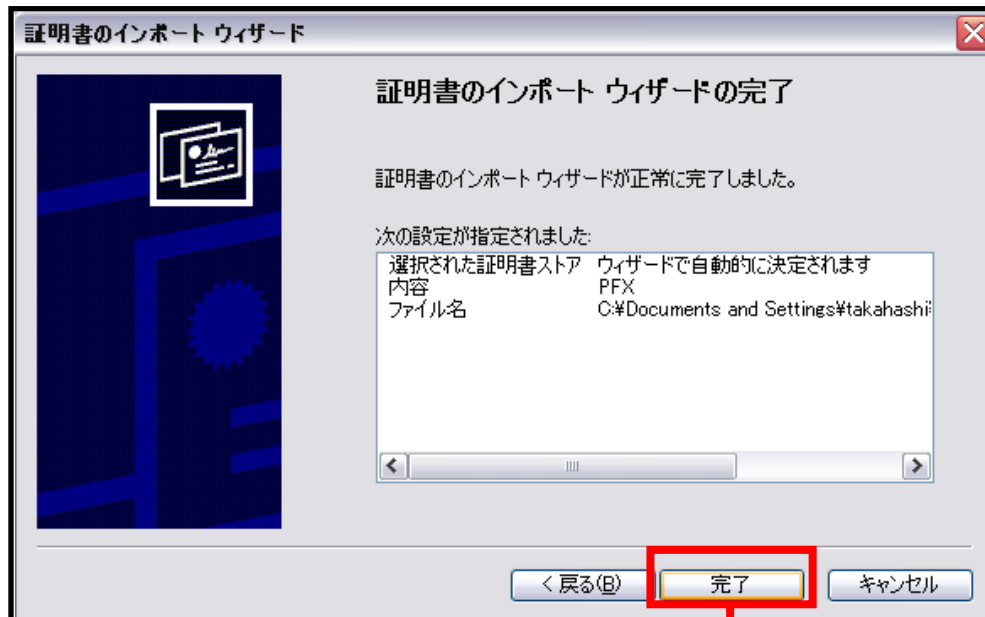
証明書ストア:
参照(R)...

< 戻る(B) **次へ(N) >** キャンセル

【証明書の種類に基づいて・・・】

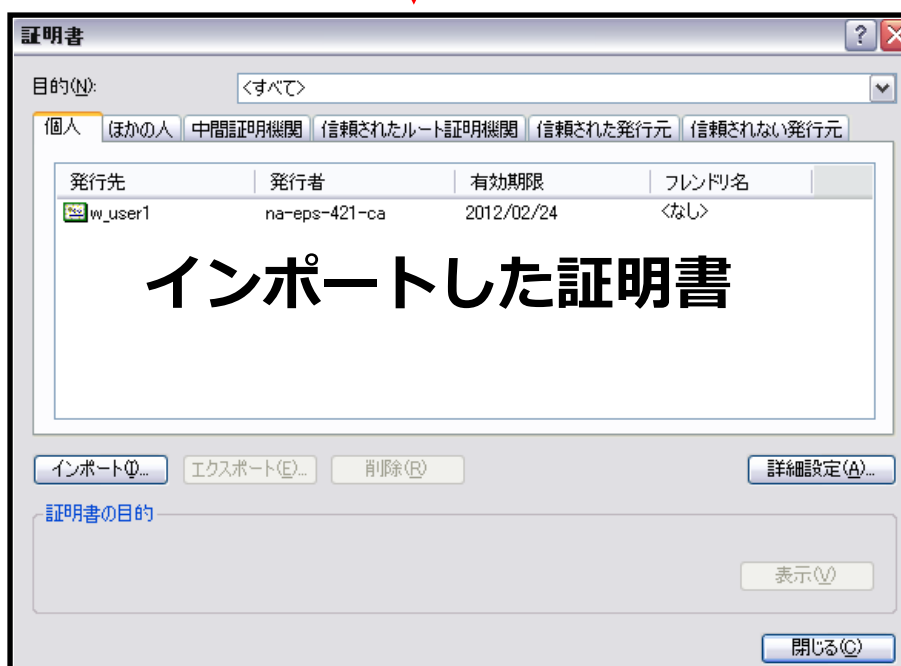
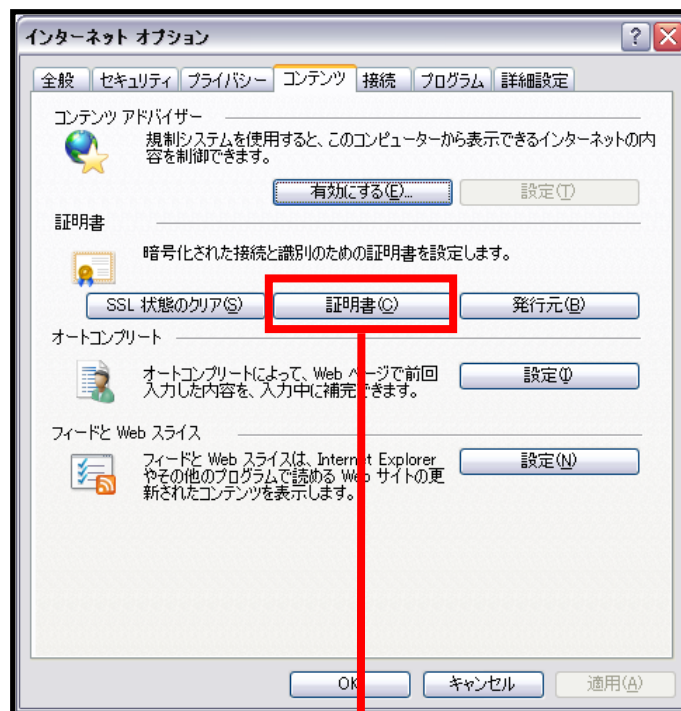
・ チェック有

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。



改訂履歴

日付	版	改訂内容
2012/3/29	1.0	初版作成
2012/9/10	1.1	RADIUS Port を TCP から UDP に修正