

Net'Attest EPS 設定例

連携機器：

Cisco Aironet1140

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 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。
<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 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。

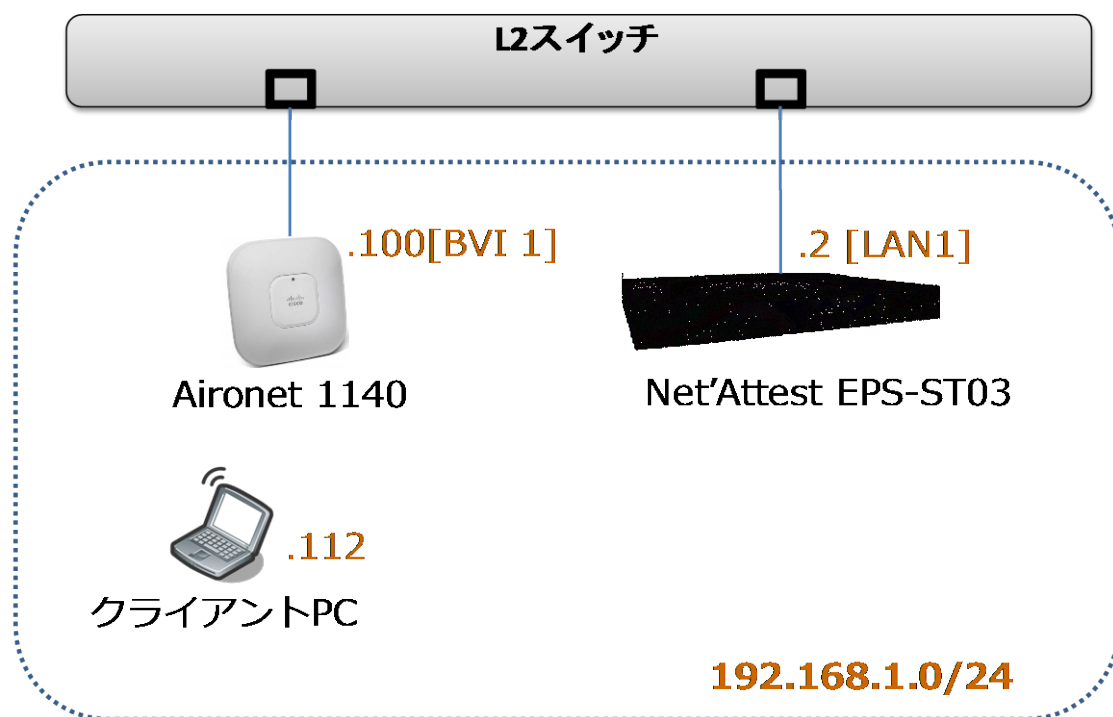
目次

1	構成	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	Cisco Aironet 1140	15
3-1	Cisco Aironet 1140 設定の流れ	15
3-2	IP アドレスの確認	16
3-3	SSID、無線セキュリティ、RADIUS サーバの設定	17
3-4	RADIUS 通信ポート番号の変更	19
3-5	無線 Interfaces の有効化	20
4	クライアント PC の設定	21
4-1	クライアント PC 設定の流れ	21
4-2	ワイヤレスネットワーク接続先の登録	22
4-3	ユーザー証明書のインポート	24
4-4	インポートされたユーザー証明書の確認	27
5	各機器 認証/接続ステータス	28
5-1	Net'Attest EPS 認証ステータス	28
5-2	Cisco Aironet1140 接続成功時ステータス	29

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	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

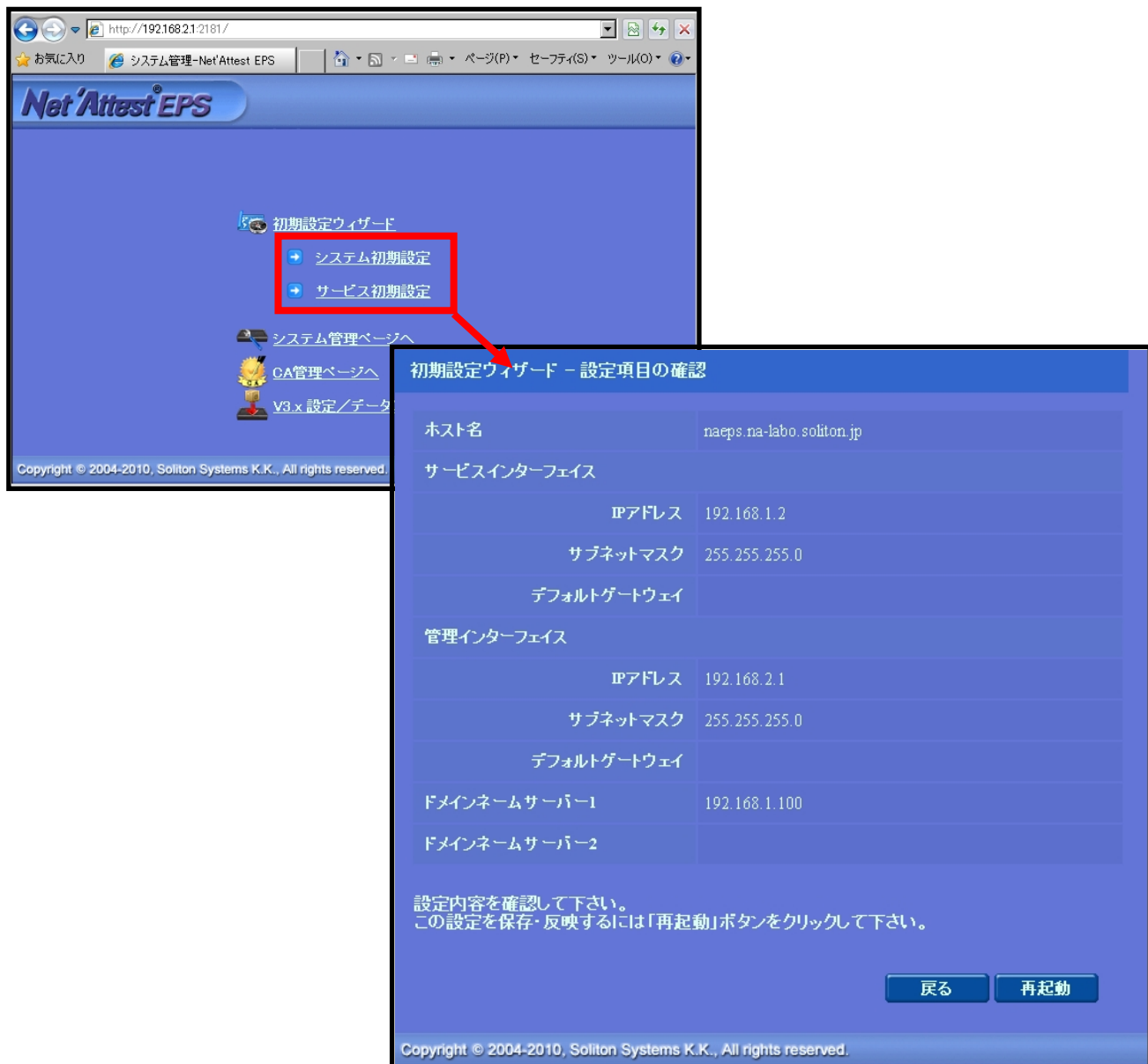
設定の流れ

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



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

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.com

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

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

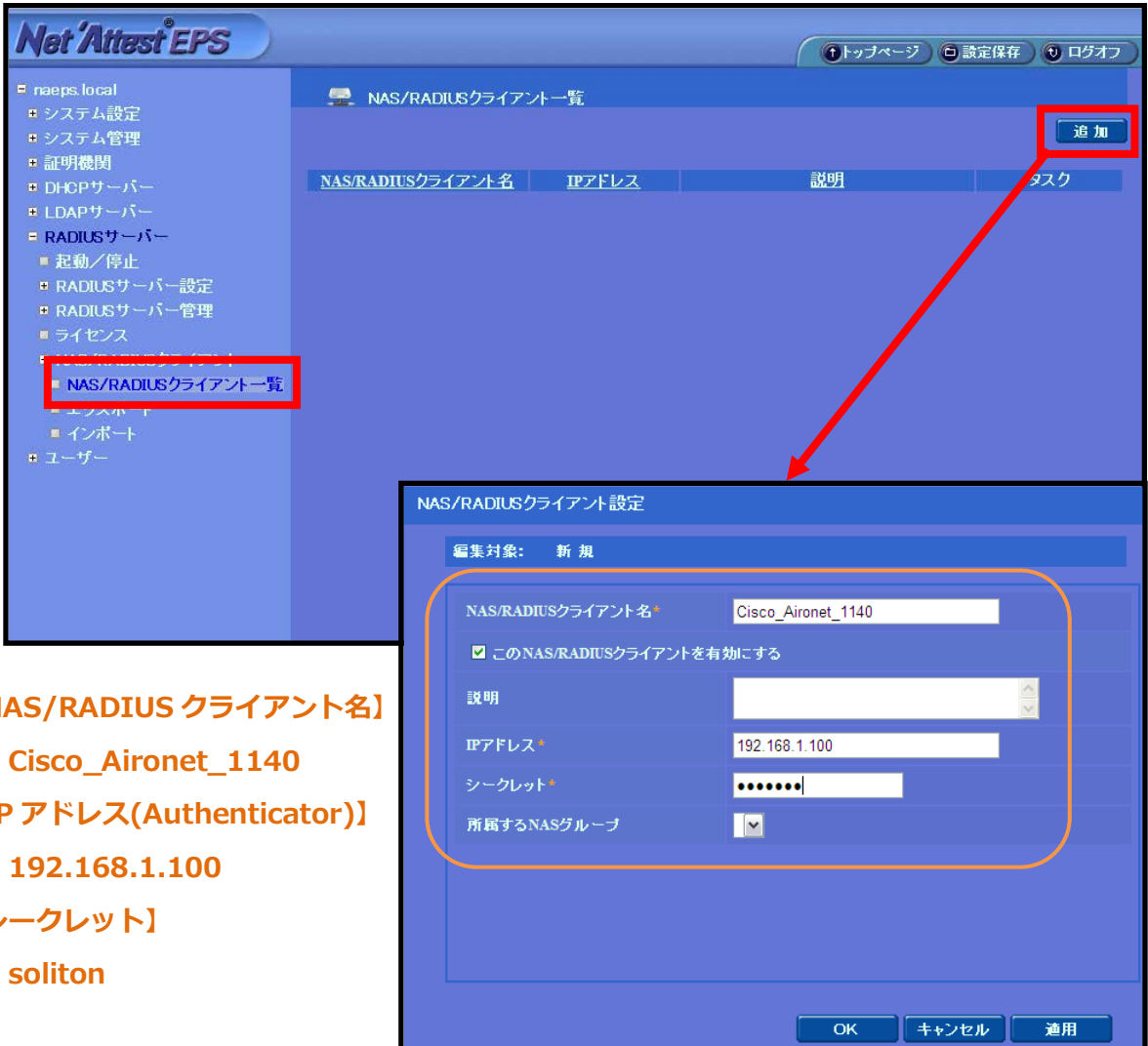
認証ポート*: 1812
アカウントングポート*: 1813

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】

- Cisco_Aironet_1140

【IP アドレス(Authenticator)】

- 192.168.1.100

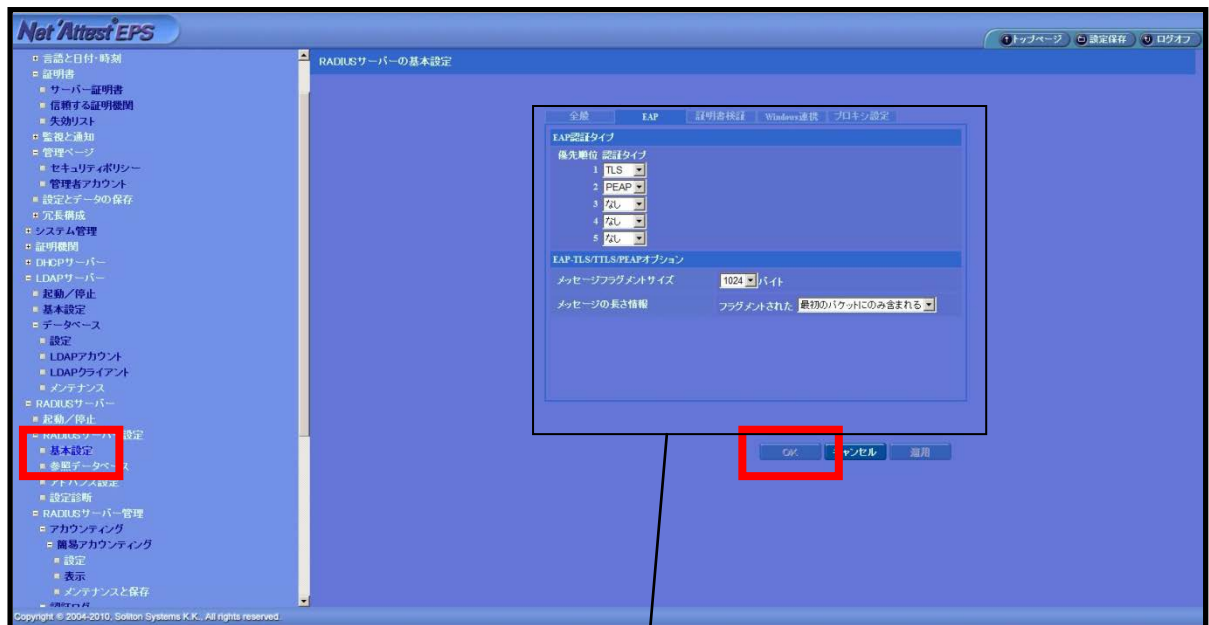
【シークレット】

- soliton

2-5 RADIUS サーバ基本設定

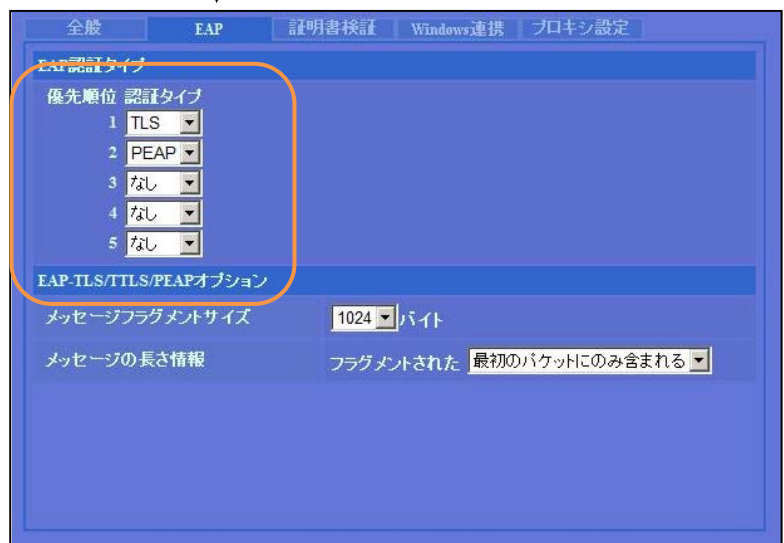
WebGUI より、RADIUS サーバの基本設定を行います。

「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。

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

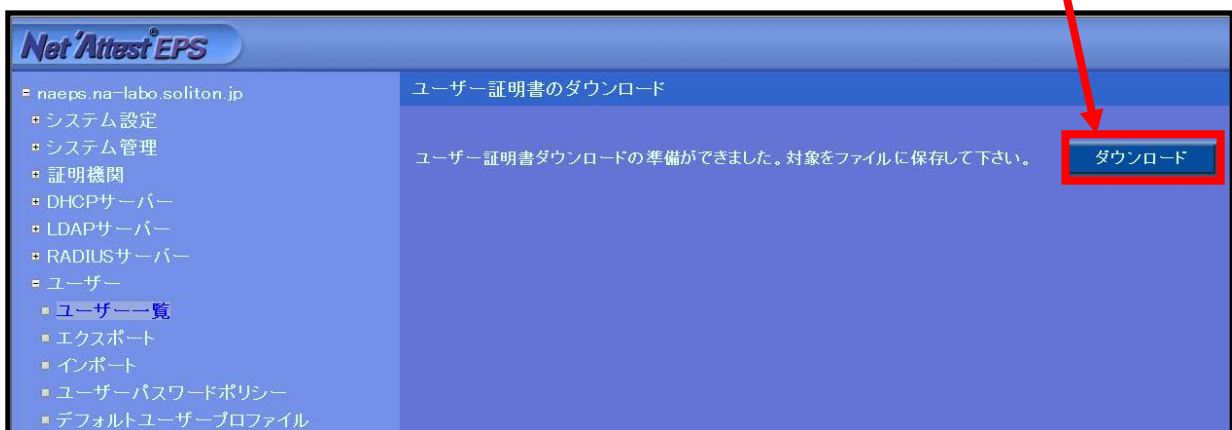
【証明書ファイルオプションパスワード】

- ・ 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 user profile page. 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 Options) section is highlighted with an orange box, showing the password field and the checked option 'PKCS#12ファイルに証明機関の証明書を含める'.



3 Cisco Aironet 1140

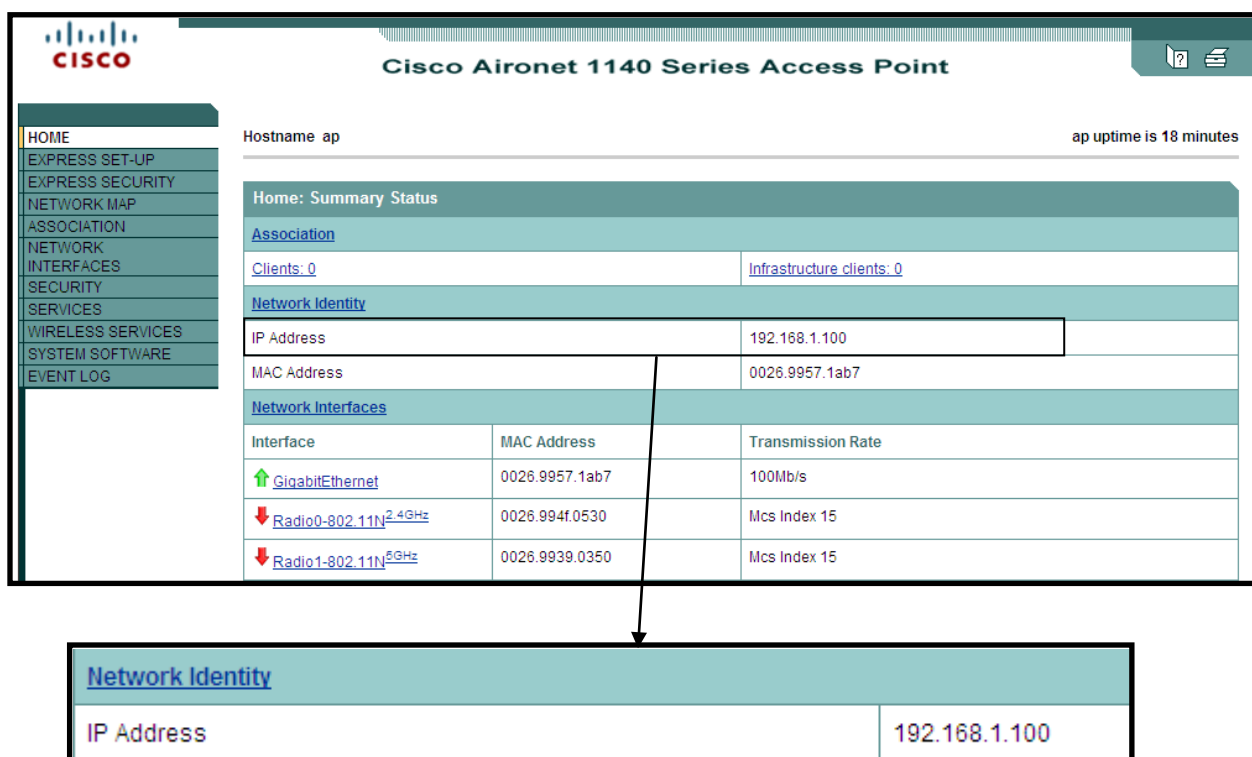
3-1 Cisco Aironet 1140 設定の流れ

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。



The screenshot displays the configuration page for a Cisco Aironet 1140 Series Access Point. The page title is "Cisco Aironet 1140 Series Access Point". The hostname is "ap" and the uptime is 18 minutes. The "Home: Summary Status" section shows the following details:

Association	
Clients: 0	Infrastructure clients: 0

Network Identity	
IP Address	192.168.1.100
MAC Address	0026.9957.1ab7

Network Interfaces		
Interface	MAC Address	Transmission Rate
↑ GigabitEthernet	0026.9957.1ab7	100Mb/s
↓ Radio0-802.11N ^{2.4GHz}	0026.994f.0530	Mcs Index 15
↓ Radio1-802.11N ^{5GHz}	0026.9939.0350	Mcs Index 15

An arrow points from the IP Address field in the "Network Identity" section to a magnified view below:

Network Identity	
IP Address	192.168.1.100

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。

The screenshot shows the Cisco Aironet 1140 Series Access Point WebGUI. The left sidebar has 'EXPRESS SECURITY' highlighted with a red box. The main content area is titled 'Express Security Set-Up' and 'SSID Configuration'. The SSID is 'AP-TEST' and 'Broadcast SSID in Beacon' is checked. Under 'VLAN', 'No VLAN' is selected. Under 'Security', 'WPA' is selected. The RADIUS Server is '192.168.1.2' and the RADIUS Server Secret is 'soliton'. The 'Apply' button is highlighted with a red box.

【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 Cisco Aironet 1140 Series Access Point ap uptime is 25 minutes

Hostname ap

SECURITY

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		Radio0-802.11N ^{2.4GHz}	0026.994f.0530 ✓	with EAP		no addition	Optional

Radio0-802.11N^{2.4GHz} Encryption Settings

Encryption Mode	WEP		Cipher						Key Rotation
	MIC	PPK	TKIP	WEP40bit	WEP128bit	CKIP	CMIC	AES CCM	
Cipher			✓						

Radio1-802.11N^{5GHz} 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。

The screenshot shows the configuration page for the Cisco Aironet 1140 Series Access Point, specifically the Server Manager section. The page is titled "Cisco Aironet 1140 Series Access Point" and "SERVER MANAGER GLOBAL PROPERTIES". The hostname is "ap" and the uptime is 32 minutes. The "Security: Server Manager" section is active, showing the "Backup RADIUS Server" configuration. The "Current Server List" section is also active, showing a list of RADIUS servers. The "Authentication Port (optional)" is set to 1812 and the "Accounting Port (optional)" is set to 1813. The "Apply" button is highlighted with a red box.

Section	Field	Value
Backup RADIUS Server	Backup RADIUS Server	(Hostname or IP Address)
	Shared Secret	
Current Server List	Server	192.168.1.2 (Hostname or IP Address)
	Shared Secret
Authentication Port (optional)	Port	1812 (0-65536)
	Port	1813 (0-65536)

[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。

The screenshot shows the configuration page for the Radio0-802.11N2.4GHz interface. The 'SETTINGS' tab is selected. The 'Enable Radio' checkbox is checked, and the 'Apply' button is highlighted. The current status is 'Disabled'.

【Enable Radio】
・ Enable チェック有

設定確認

The screenshot shows the 'Network Interfaces: Summary' table. The 'Radio0-802.11N2.4GHz' interface is shown as 'Enabled' and 'Up'.

Network Interfaces: Summary			
System Settings			
IP Address (Static)	192.168.1.100		
IP Subnet Mask	255.255.255.0		
Default Gateway	0.0.0.0		
MAC Address	0028.9957.1ab7		
Interface Status		Radio0-802.11N2.4GHz	Radio1-802.11N5GHz
Software Status	Enabled ↑	Enabled ↑	Disabled ↓
Hardware Status	Up ↑	Up ↑	Down ↓
Interface Resets	2	2	0

4 クライアント PC の設定

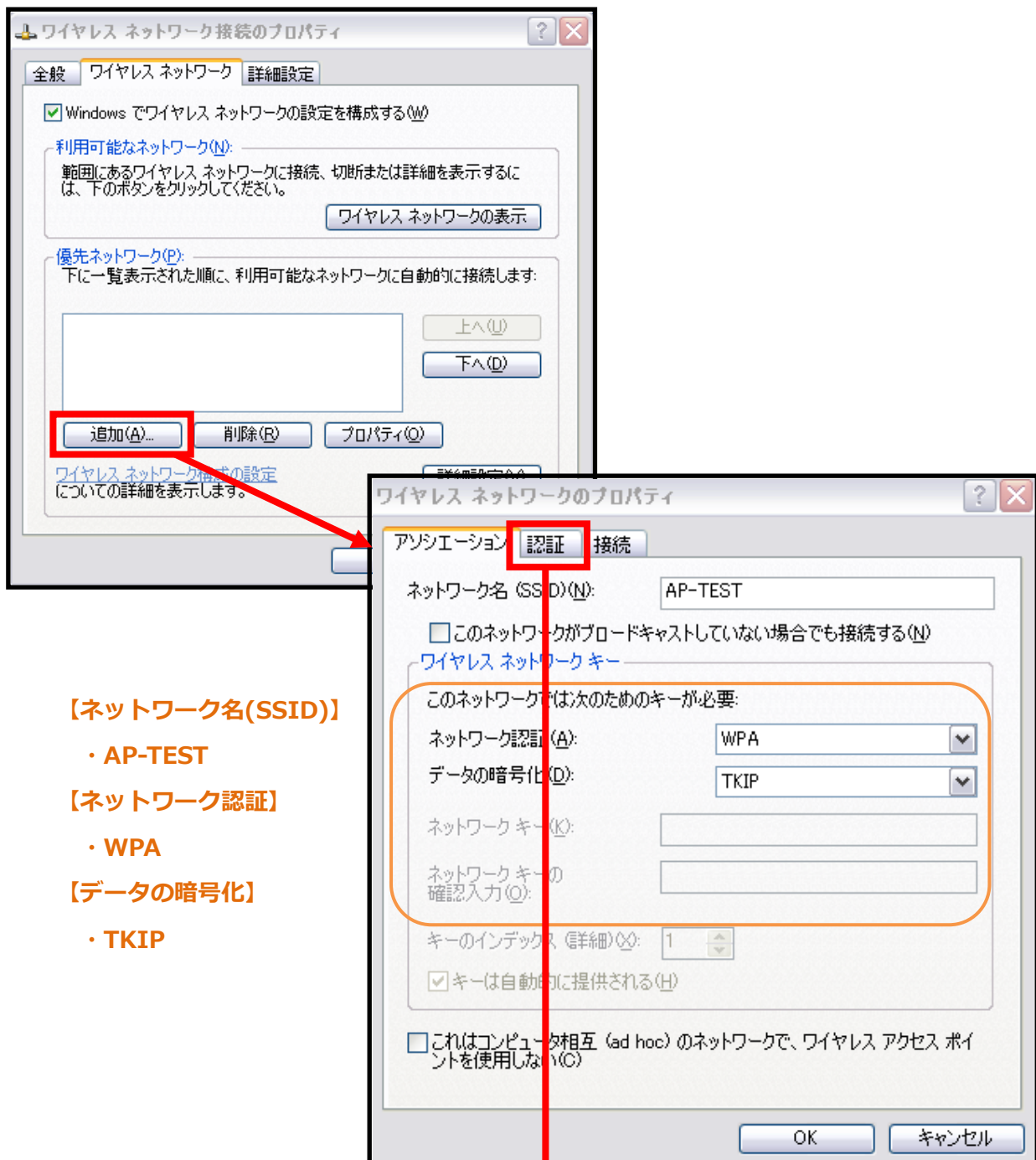
4-1 クライアント PC 設定の流れ

設定の流れ

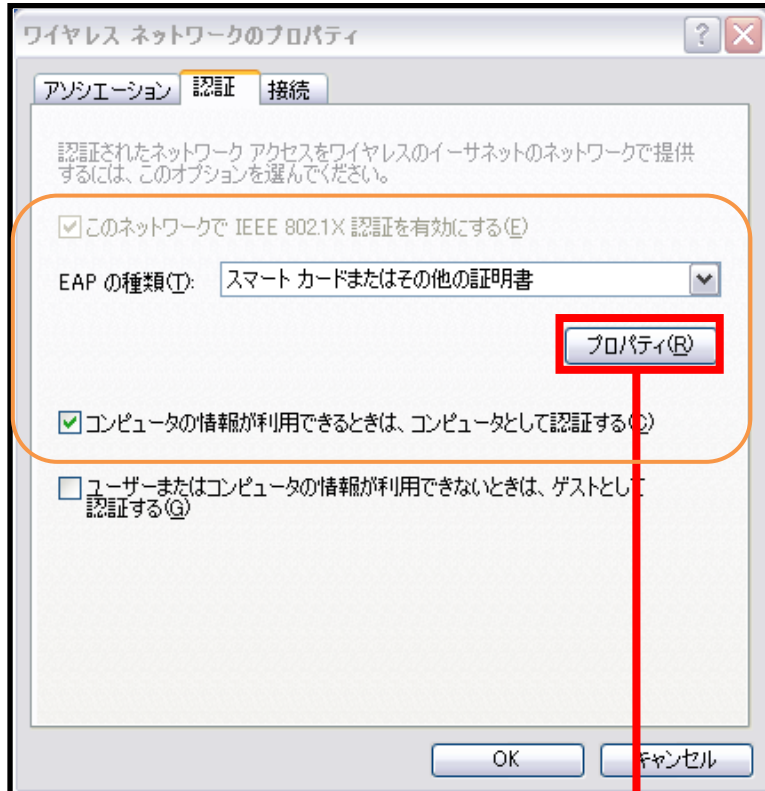
1. ワイヤレスネットワーク接続先の登録
2. ユーザ証明書のインポート

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。

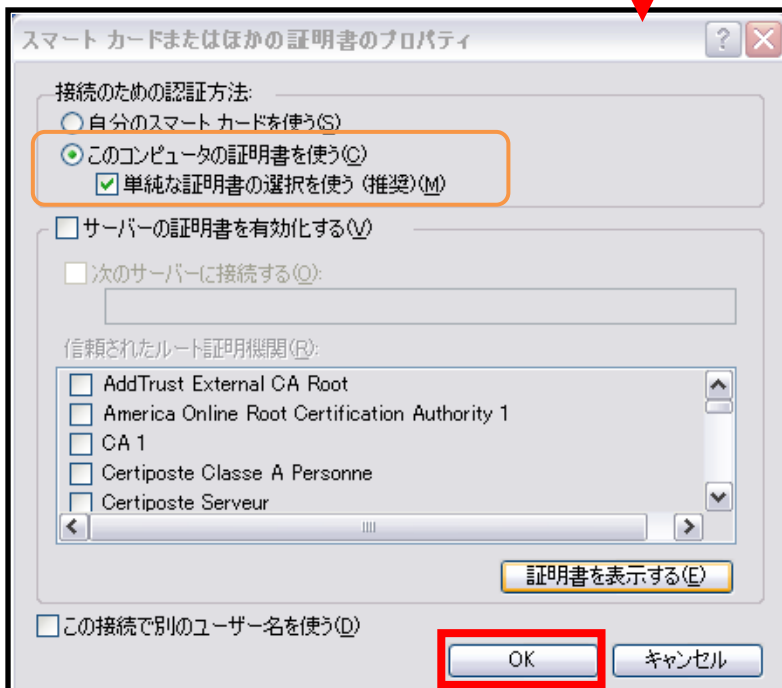


次ページへ



【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(L)
 証明書をすべて次のストアに配置する(P)

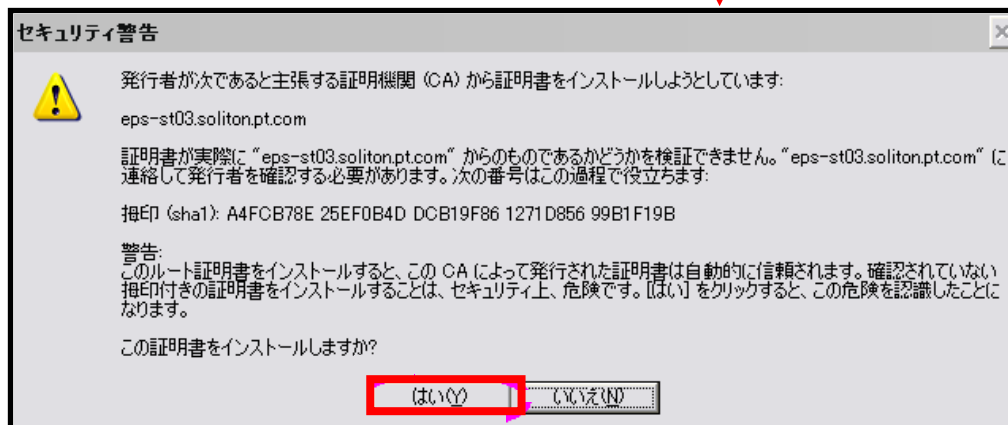
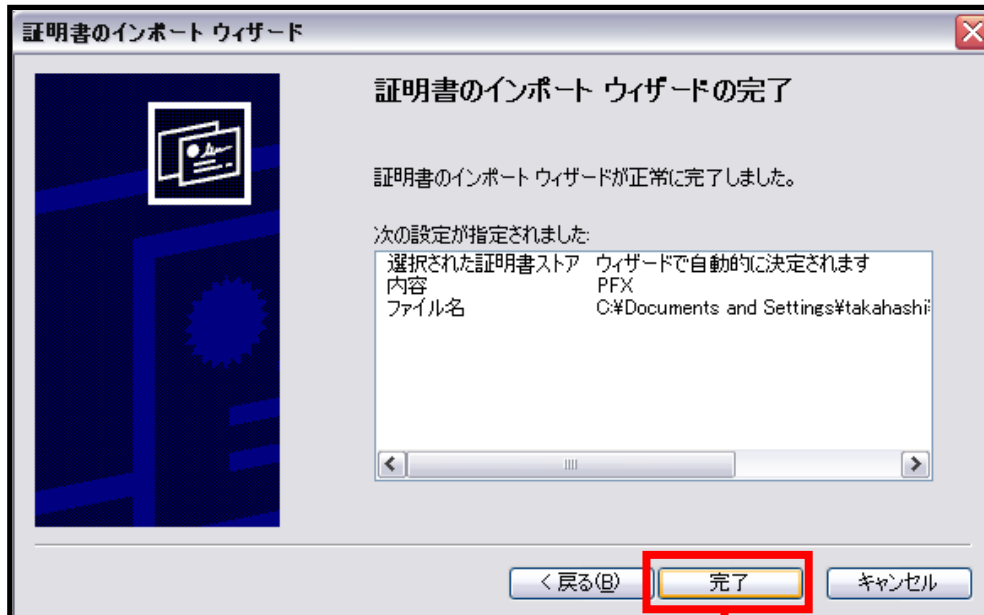
証明書ストア:
参照(R)...

< 戻る(B) **次へ(N) >** キャンセル

【証明書の種類に基づいて・・・】

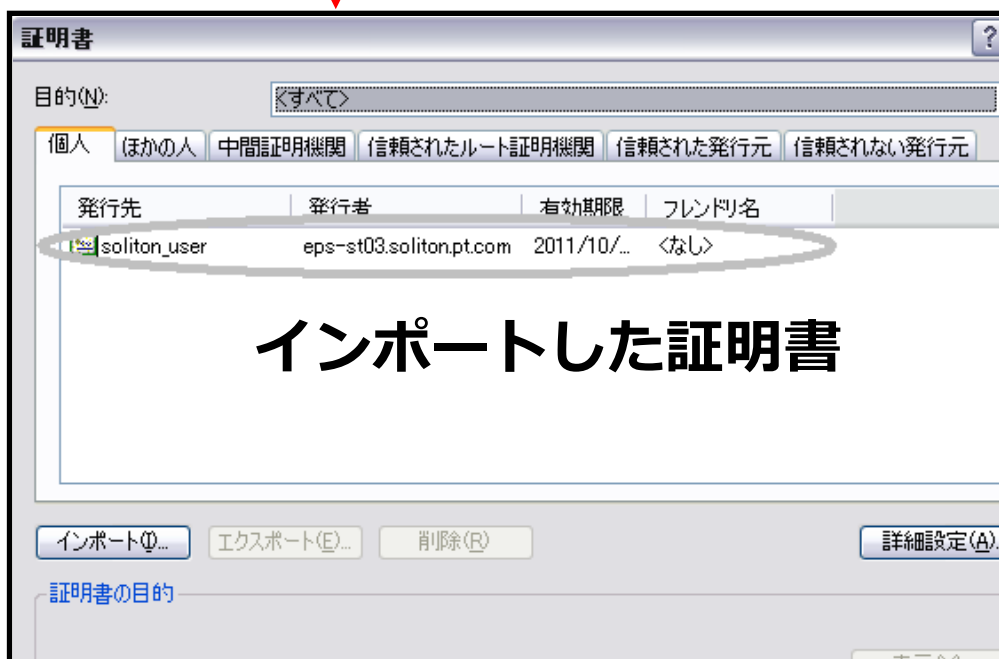
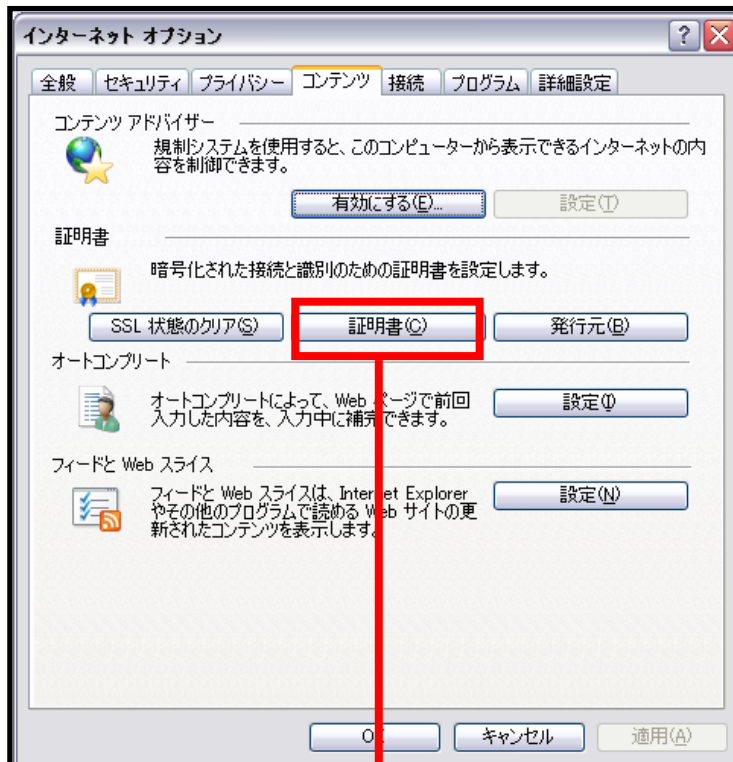
・ チェック有

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。



The screenshot shows the Net'Attest EPS web interface. On the left is a navigation menu with the following items: 証明機関, DHCPサーバー, LDAPサーバー, RADIUSサーバー (expanded), 起動/停止, RADIUSサーバー設定, RADIUSサーバー管理 (expanded), アカウンティング, 認証ログ (expanded), 表示 (highlighted with a red box), メンテナンスと保存, セッション管理, and ライセンス. The main content area is titled '認証ログの表示' and contains a table with the following data:

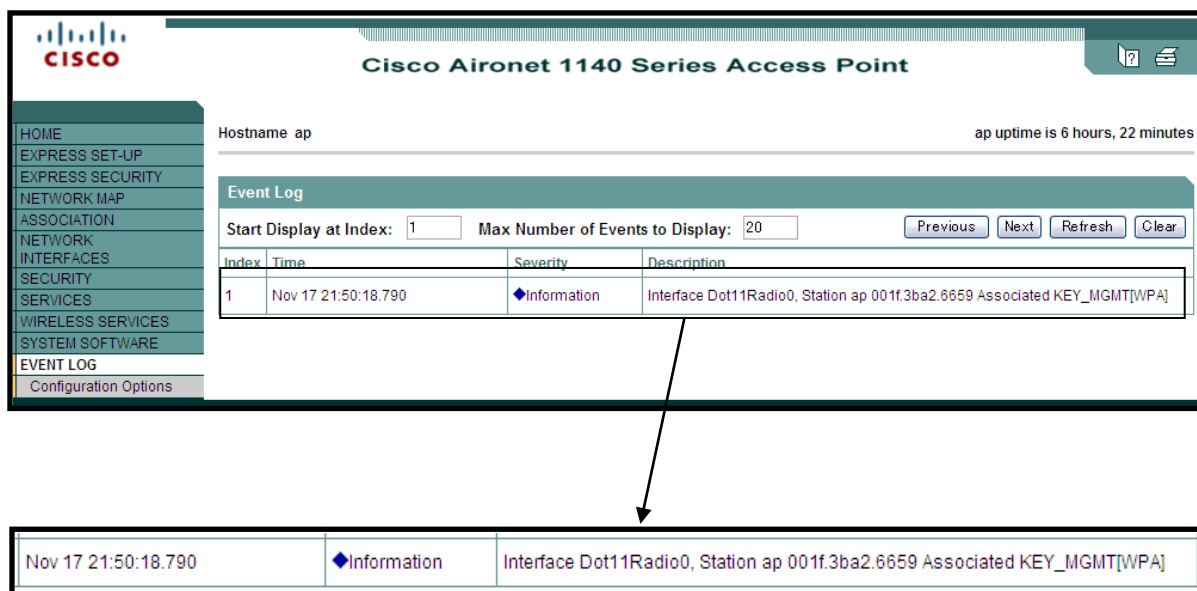
日時	種別	Priority	イベント
Nov 22 17:26:31	radiusd[5388]		Login OK: [soliton_user] (from client Cisco_Aironet_1140 port 332 cli 001f.3ba2.6659)

An arrow points from the '表示' menu item to a detailed view of a log entry, which is shown in a separate box below:

Nov 22 17:20:55	radiusd[2187]		Login OK: [soliton_user] (from client Cisco_Aironet_1140 port 332 cli 001f.3ba2.6659)
-----------------	---------------	--	---

5-2 Cisco Aironet1140 接続成功時ステータス

「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。



The screenshot displays the Cisco Aironet 1140 Series Access Point configuration interface. The left sidebar contains navigation options: HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, EVENT LOG, and Configuration Options. The main content area shows the configuration for Hostname 'ap' with an uptime of 6 hours, 22 minutes. The 'Event Log' section is active, showing a table with columns for Index, Time, Severity, and Description. A single event is listed at index 1, occurring at 11:50:18.790 on Nov 17, with an Information severity level. The description is 'Interface Dot11Radio0, Station ap 001f.3ba2.6659 Associated KEY_MGMT[WPA]'. An arrow points from this event to a magnified view below.

Index	Time	Severity	Description
1	Nov 17 21:50:18.790	Information	Interface Dot11Radio0, Station ap 001f.3ba2.6659 Associated KEY_MGMT[WPA]

Nov 17 21:50:18.790	Information	Interface Dot11Radio0, Station ap 001f.3ba2.6659 Associated KEY_MGMT[WPA]
---------------------	-------------	---

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