NetAttest EPS
認証連携設定例

【連携機器】ゼブラ・テクノロジーズ AP7532

【Case】IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)

Rev1.1

株式会社ソリトンシステムズ

はじめに

本書について

本書はオールインワン認証アプライアンス NetAttest EPS と、ゼブラ・テクノロジーズ社製無線アクセスポイント AP7532 の IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)環境での接続について、設定例を示したものです。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。

なお、本書は FXC 株式会社の協力により作成されております。

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、NetAttest EPS 及び AP7532 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

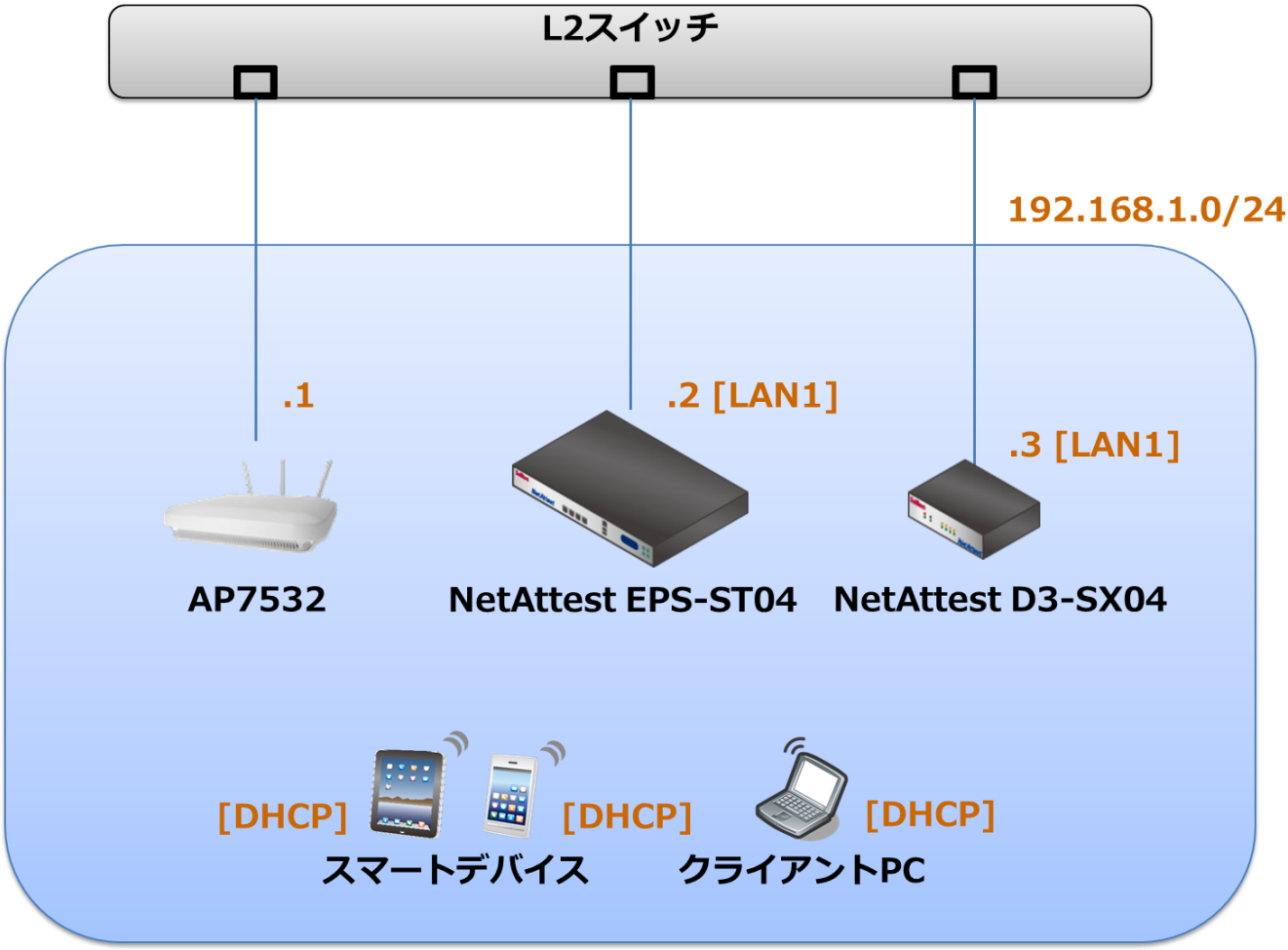
1-1 構成図

以下の環境を構成します。

・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、NetAttest D3-SX04 の DHCP サーバーから払い出す



1-2 環境

1-2-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS-ST04	Soliton Systems	RADIUS/CA サーバー	4.8.5
AP7532	ゼブラ・テクノロジーズ	RADIUS クライアント (無線アクセスポイント)	5.8.1.0-012R
Surface	MicroSoft	802.1X クライアント (Client PC)	Windows 8.1 64bit Windows 標準サプリカント
iPhone 6	Apple	802.1X クライアント (Client SmartPhone)	9.3.1
Google Nexus 7	ASUS	802.1X クライアント (Client Tablet)	5.1
NetAttest D3-SX04	Soliton Systems	DHCP/DNS サーバー	4.2.2

1-2-2 認証方式

IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)

1-2-3 ネットワーク設定

機器	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS-ST04	192.168.1.2/24	UDP 1812	secret
AP7532	192.168.1.1/24		secret
Client PC	DHCP	-	-
Client SmartPhone	DHCP	-	-
Client Tablet	DHCP	-	-

2. NetAttest EPS の設定

2-1 初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.2.1:2181/」にアクセスしてください。

下記のような流れでセットアップを行います。

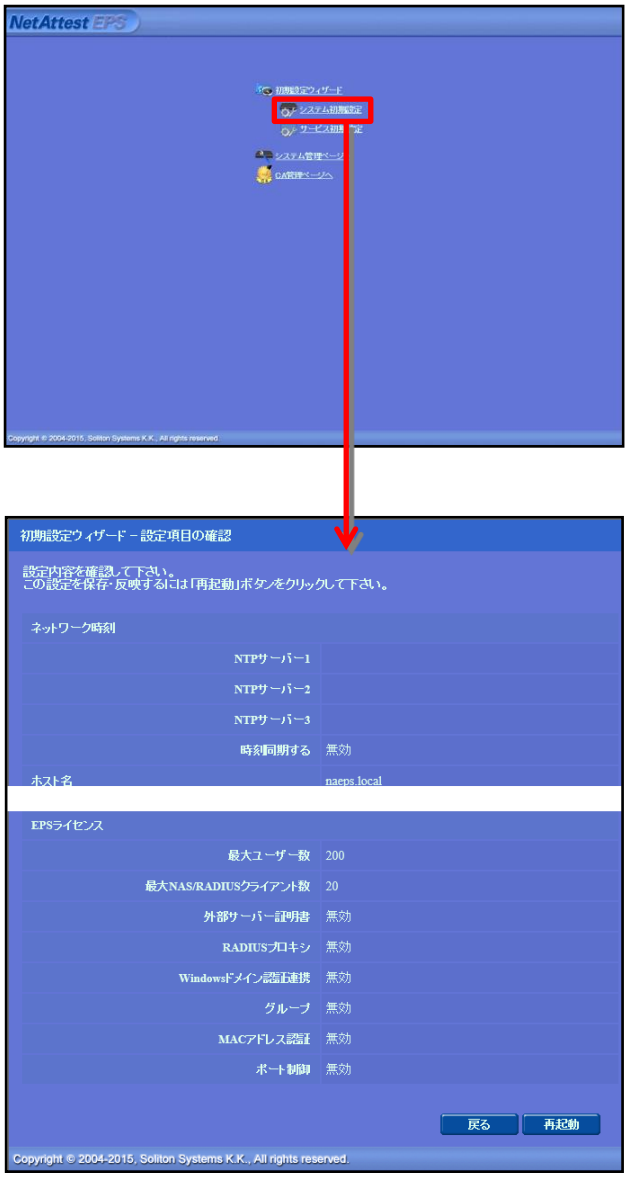
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

2-2 システム初期設定ウィザードの実行

NetAttest EPS の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは「192.168.2.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.2.1:2181/」にアクセスしてください。

その後、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ーの設定

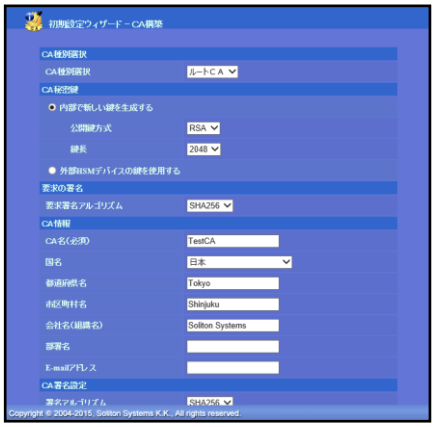


項目	値
ホスト名	naeps.local
IP アドレス	デフォルト
ライセンス	なし

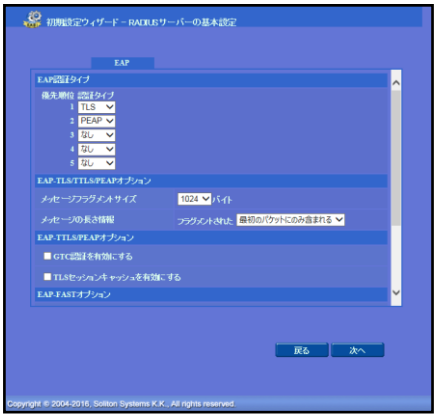
2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

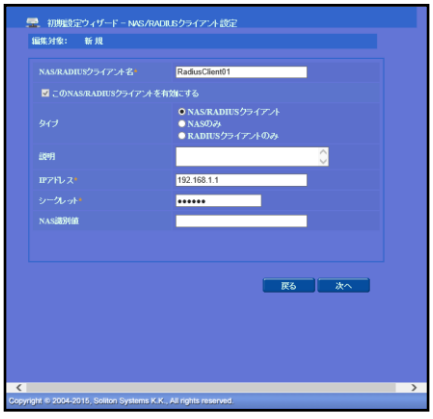
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定



項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA



項目	値
EAP 認証タイプ	
1	TLS
2	PEAP

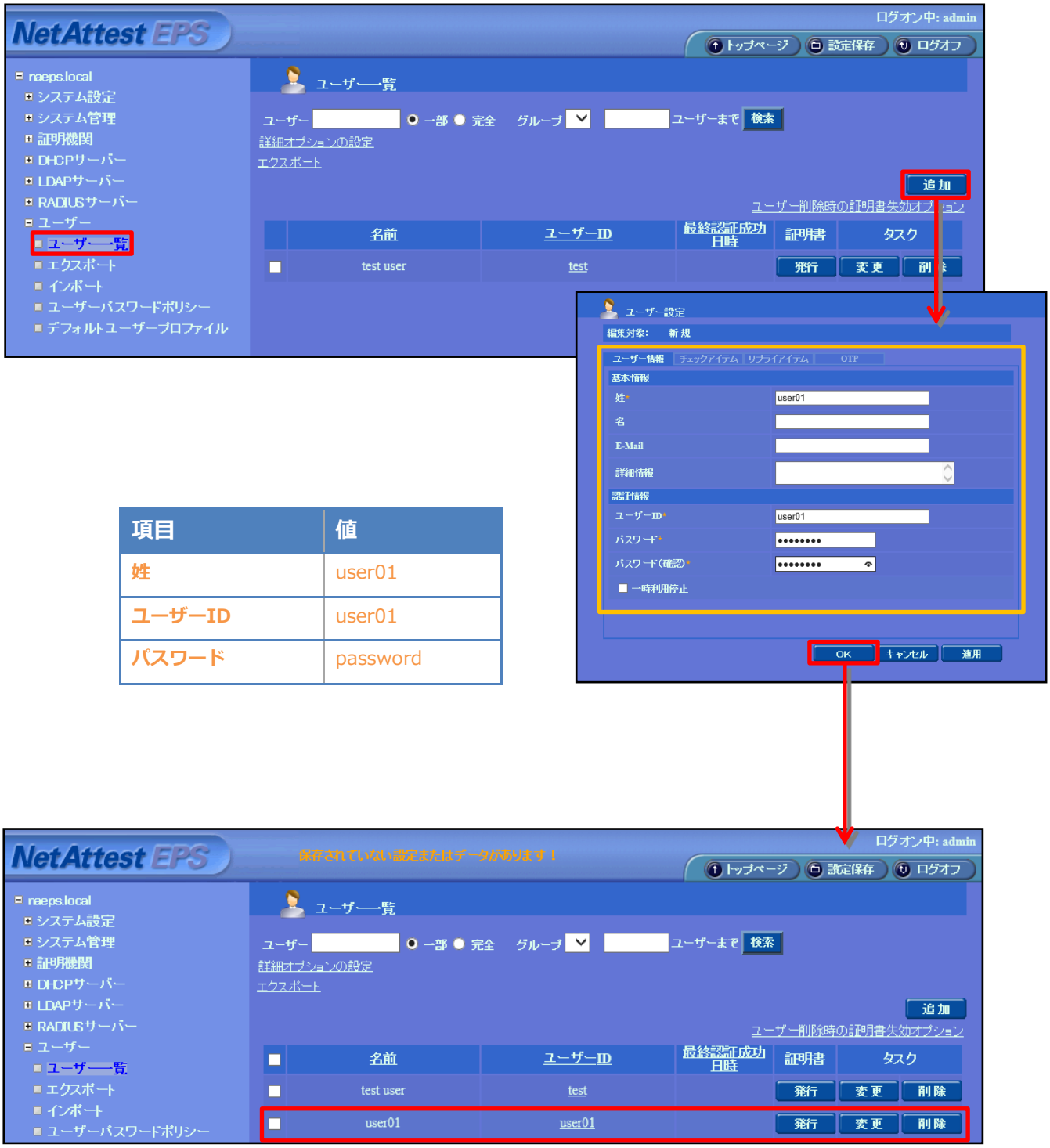


項目	値
NAS/RADIUS クライアント名	RadiusClient01
IP アドレス	192.168.1.1
シークレット	secret

2-4 ユーザーの登録

NetAttest EPS の管理画面より、認証ユーザーの登録を行います。

「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行います。



項目	値
姓	user01
ユーザーID	user01
パスワード	password

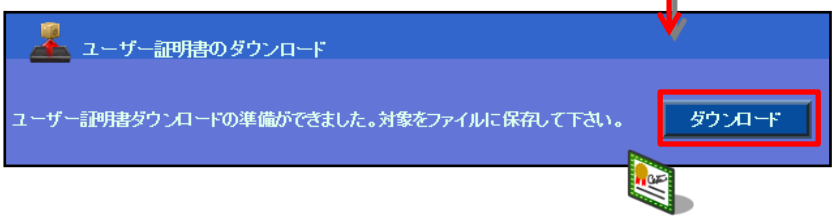
2-5 クライアント証明書の発行

NetAttest EPS の管理画面より、クライアント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クライアント証明書を発行します。

(クライアント証明書は、user01_02.p12 という名前で保存)

項目	値
証明書有効期限	365
PKCS#12 ファイルに証明機関の・・・	チェック有



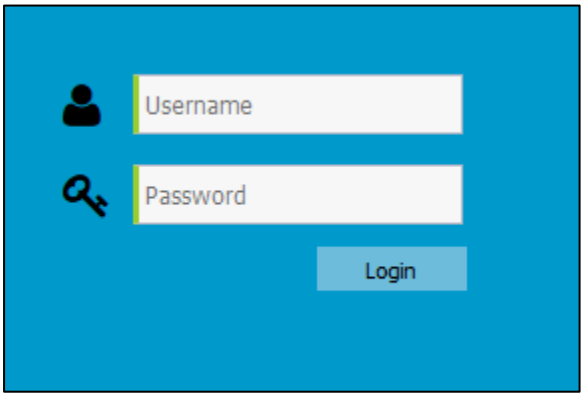
3. AP7532 の設定

3-1 アクセスポイントの設定

AP7532 の設定は WebGUI または CLI にて行います。本書では WebGUI での設定例について紹介します。

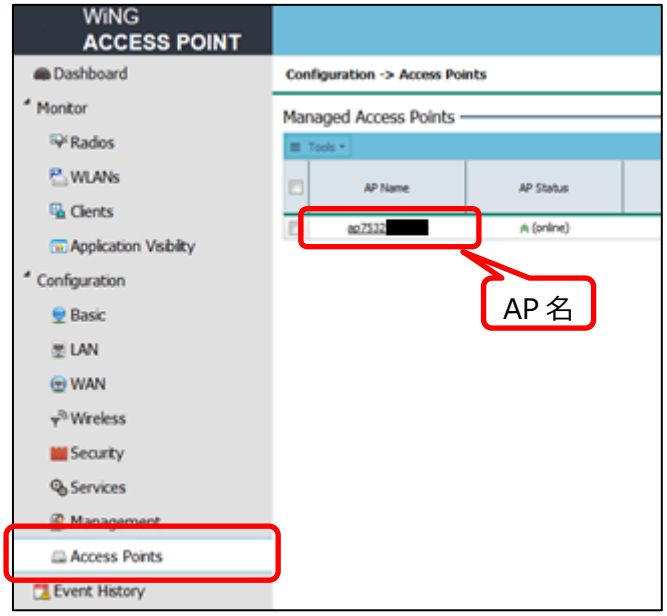
Web ブラウザより AP7532 の Web 管理画面ログインし、設定を開始します。

※初期 IP アドレス、アカウント、パスワードは設定マニュアルを参照してください。



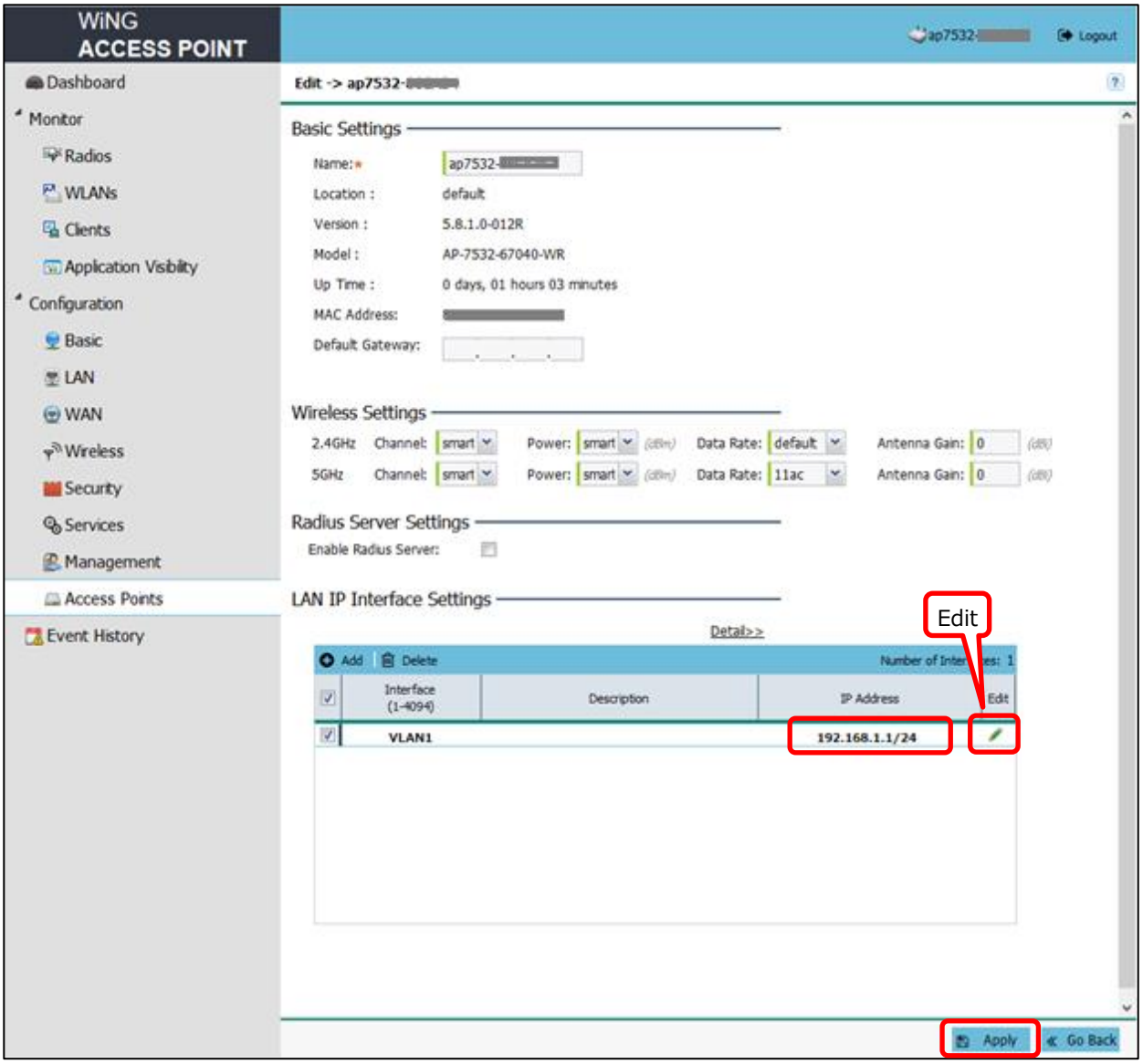
・ログイン画面

画面左メニューから[Access Point]を選択します。その後、AP 名をクリックします。



Edit（鉛筆マーク）をクリックし、IP アドレスを編集します。最後に画面右下の[Apply]をクリックします。

Edit（鉛筆マーク）をクリックし、IP アドレスを編集します。最後に画面右下の[Apply]をクリックします。

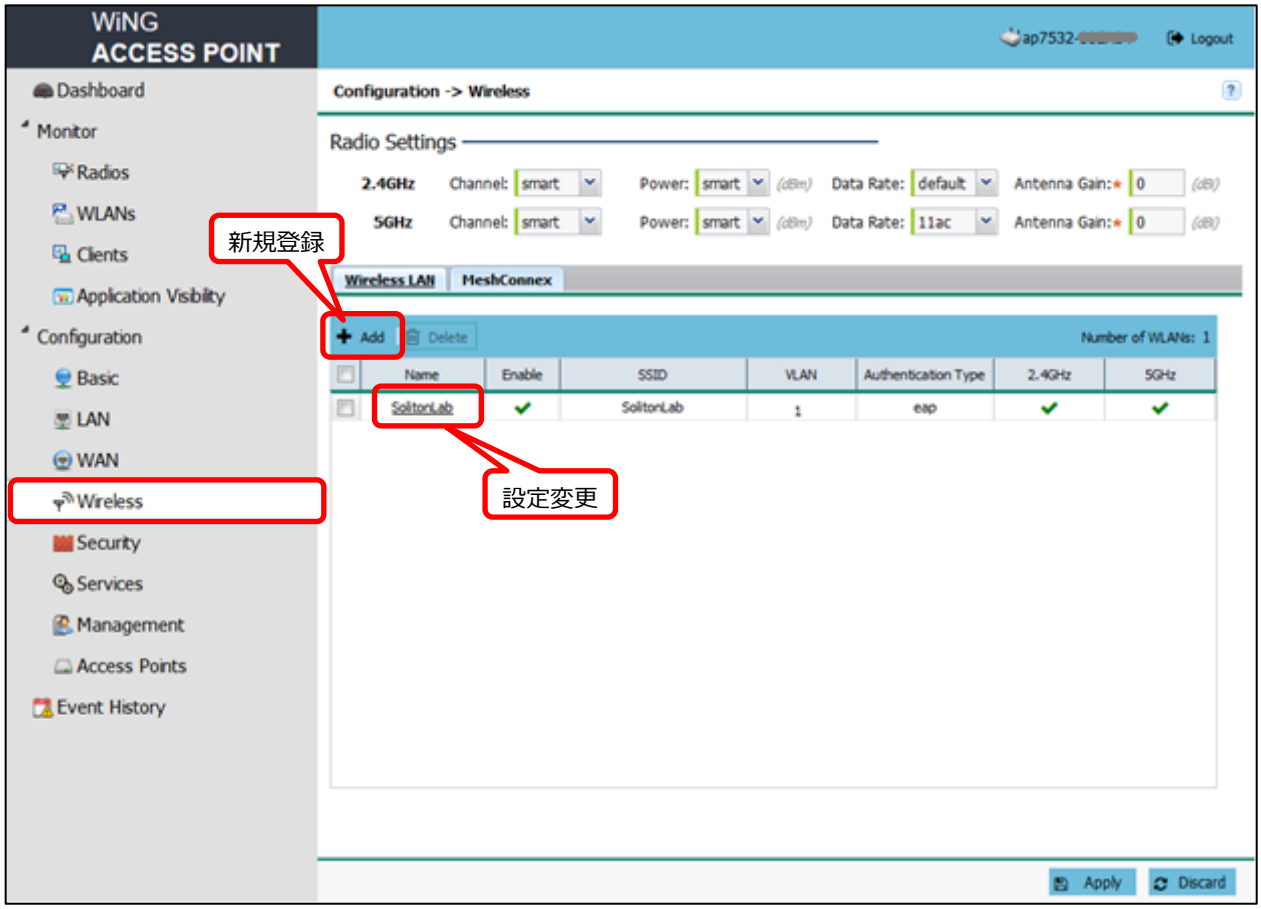


項目	値
IP アドレス	192.168.1.1
サブネットマスク	255.255.255.0

3-2 RADIUS の設定

RADIUS サーバーの登録を行います。

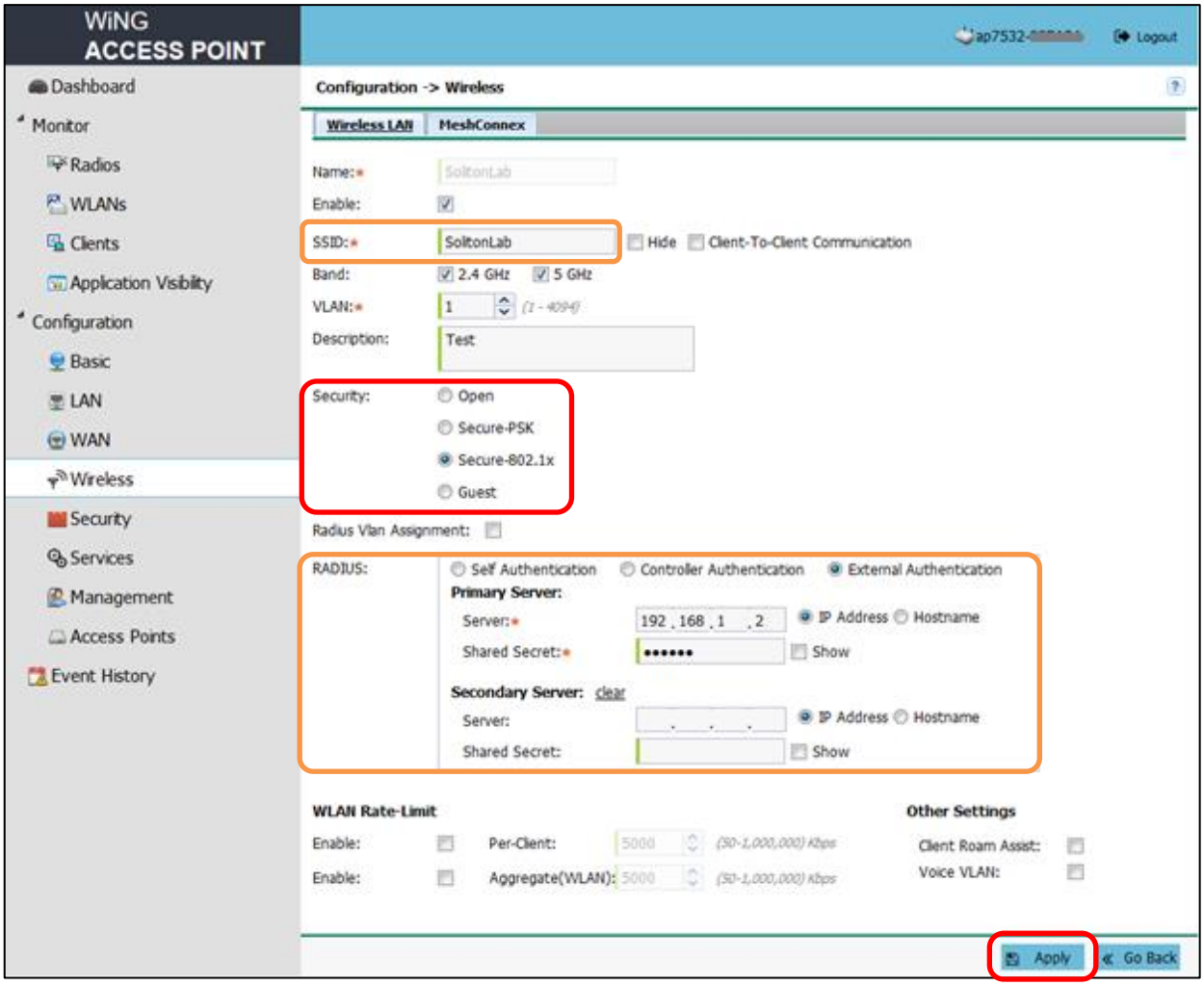
左メニューから[Wireless]を選択します。新規登録の場合は、[Add]、登録済みデータを変更する場合は、対象の設定名をクリックします。



※画面は、登録済みの場合

SSID、認証方式、RADIUS サーバーを設定します。

設定後、画面右下の[Apply]をクリックします。画面が設定済み一覧に移行しますので、再度、画面右下の[Apply]をクリックします。



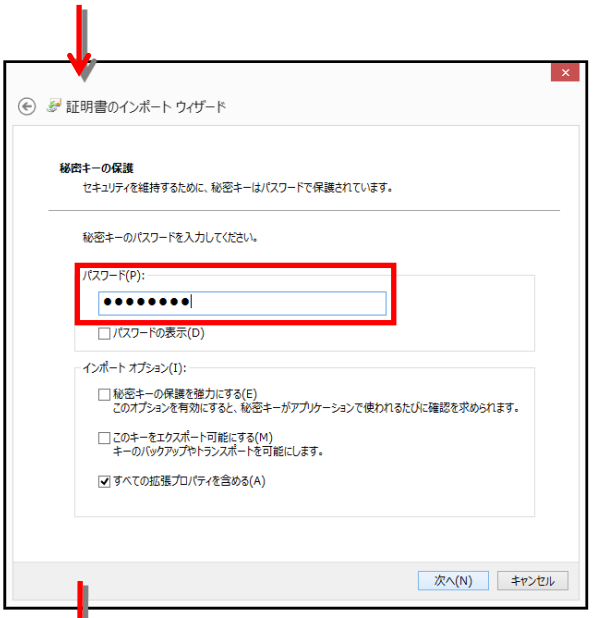
項目	値
SSID	SolitonLab
Security	Secure-802.1x
RADIUS サーバー	192.168.1.2
Shared Secret	secret

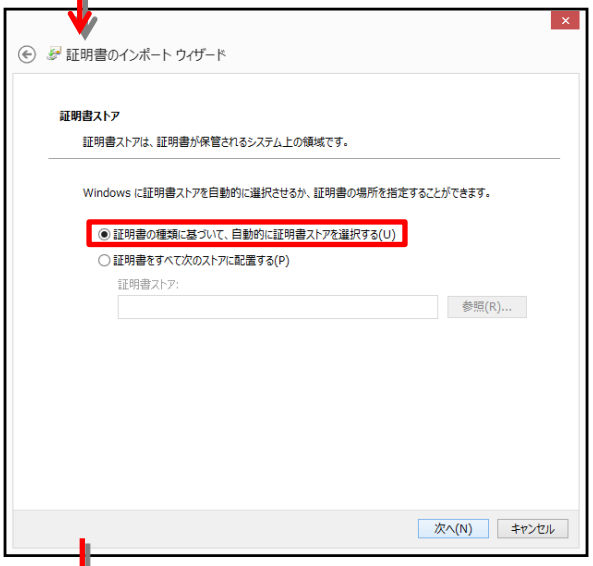
4. EAP-TLS 認証でのクライアント設定

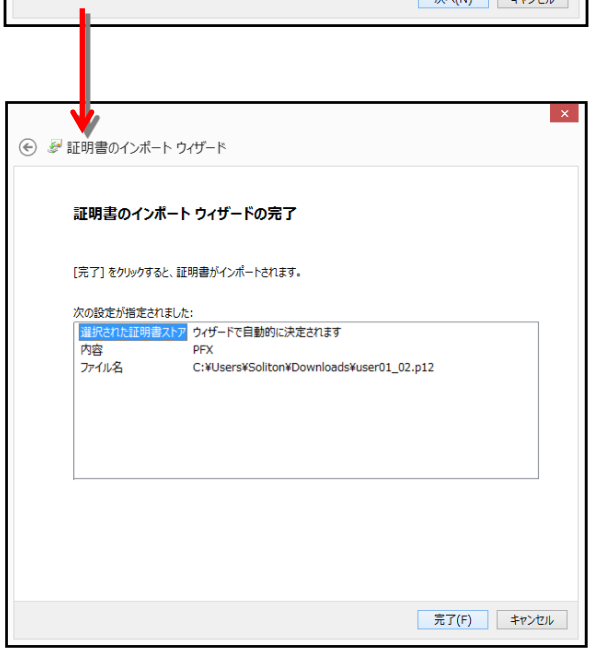
4-1 Windows 8.1 での EAP-TLS 認証

4-1-1 クライアント証明書のインポート

PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書(user01_02.p12)をダブルクリックすると、証明書インポートウィザードが実行されます。







【パスワード】

NetAttest EPS で証明書を

発行した際に設定したパスワードを入力

4-1-2 サプリカント設定

Windows 標準サプリカントで TLS の設定を行います。

※本項では TLS の設定のみ記載します。その他の認証方式の設定に関しては付録をご参照ください。

[ワイヤレスネットワークのプロパティ] の [セキュリティ] タブから以下の設定を行います。

項目	値
セキュリティの種類	WPA2-エンタープライズ
暗号化の種類	AES
ネットワークの認証・・・	Microsoft: スマートカード・・・

項目	値
認証モードを指定する	ユーザー認証

項目	値
接続のための認証方法	
- このコンピューターの証明書を・・・	On
- 単純な証明書の選択を使う(推奨)	On
証明書を検証してサーバーの ID を・・・	On
信頼されたルート証明機関	TestCA

4-2 iOS(iPhone 6)での EAP-TLS 認証

4-2-1 クライアント証明書のインポート

NetAttest EPS から発行したクライアント証明書を iOS デバイスにインポートする方法として、下記の方法などがあります。

1) Mac OS を利用して Apple Configurator を使う方法
2) クライアント証明書をメールに添付し iOS デバイスに送り、インポートする方法
3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)

いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

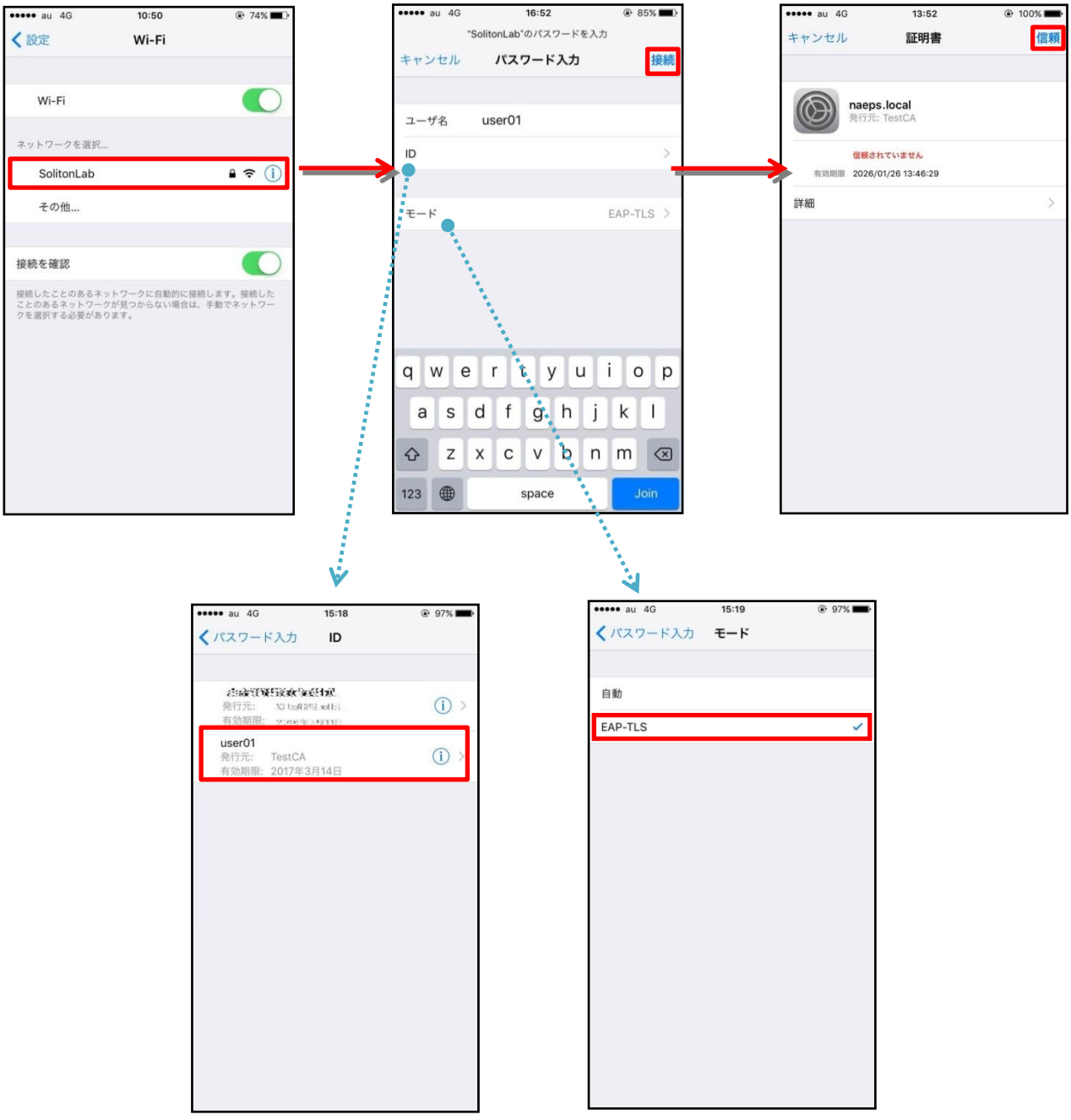
4-2-2 サプリカント設定

AP7532 で設定した SSID を選択し、サプリカントの設定を行います。

※本項では TLS の設定のみ記載します。その他の認証方式の設定に関しては付録をご参照ください。

まず、「ユーザー名」には証明書を発行したユーザーのユーザーID を入力します。次に「モード」より「EAP-TLS」を選択します。その後、「ユーザー名」の下の「ID」よりインポートされたクライアント証明書を選択します。

※初回接続時は「信頼されていません」と警告が出るので、「信頼」を選択し、接続します。



4-3 Android(Google Nexus 7)での EAP-TLS 認証

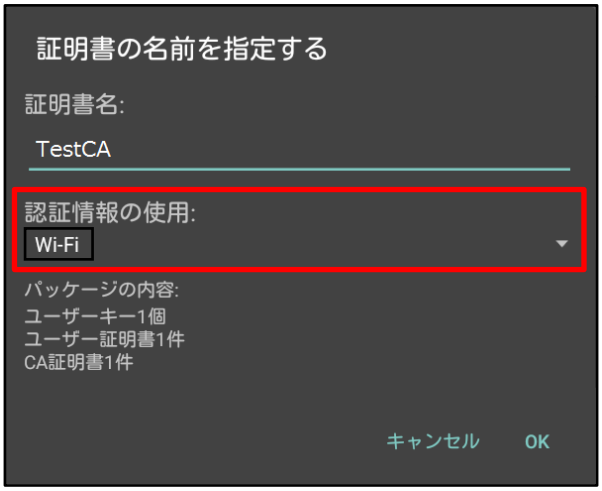
4-3-1 クライアント証明書のインポート

NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

1) SD カードにクライアント証明書を保存し、インポートする方法※1
2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※2
3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※1 メーカーや OS バージョンにより、インポート方法が異なる場合があります。事前にご検証ください。
※2 メーカーや OS バージョン、メーラーにより、インポートできない場合があります。事前にご検証ください。
※3 メーカーや OS バージョンにより、Soliton KeyManager が正常に動作しない場合があります。事前にご検証ください。

Android 5.1 では証明書インポート時に用途別に証明書ストアが選択できますが、
本書では無線 LAN 接続を行うため「Wi-Fi」を選択しています。

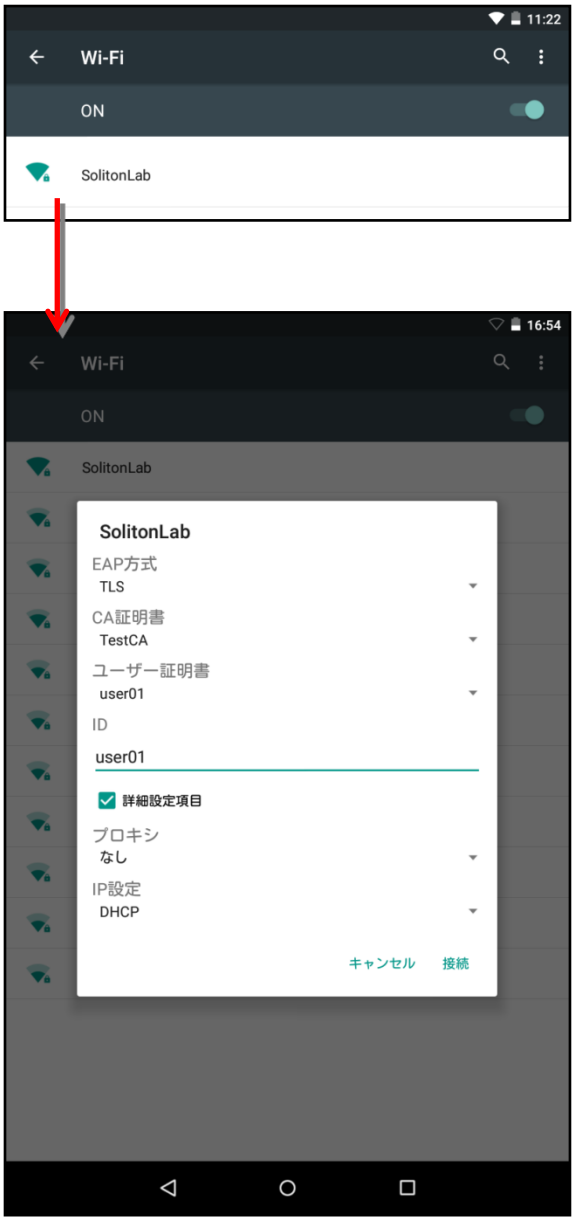


4-3-2 サプリカント設定

AP7532 で設定した SSID を選択し、サプリカントの設定を行います。

※本項では TLS の設定のみ記載します。その他の認証方式の設定に関しては付録をご参照ください。

「ID」には証明書を発行したユーザーのユーザーID を入力します。CA 証明書とユーザー証明書は、インポートした証明書を選択して下さい。

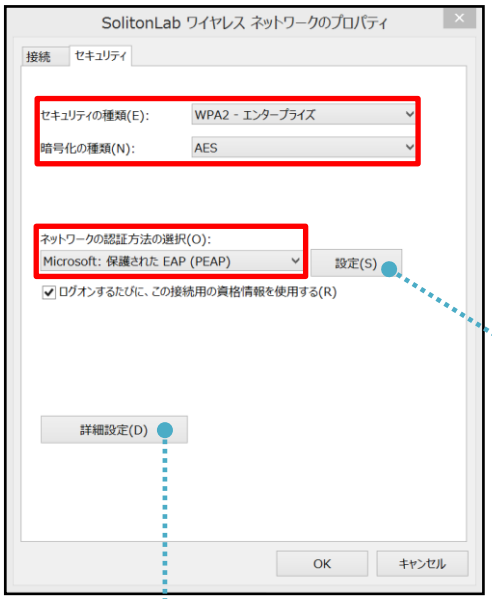


項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

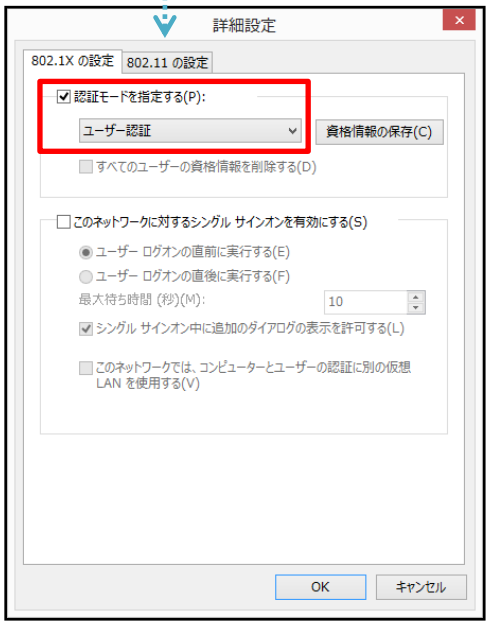
5. EAP-PEAP 認証でのクライアント設定

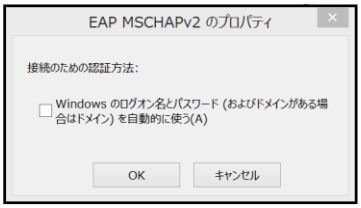
5-1 Windows 8.1 のサプリカント設定

[ワイヤレスネットワークのプロパティ] の「セキュリティ」タブから以下の設定を行います。



項目	値
セキュリティの種類	WPA2-エンタープライズ
暗号化の種類	AES
ネットワークの認証・・・	Microsoft: 保護された EAP





項目	値
認証モードを指定する	ユーザー認証

項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA

5-2 iOS(iPhone 6)のサプリカント設定

AP7532 で設定した SSID を選択し、サプリカントの設定を行います。

「ユーザー名」、「パスワード」には”2-4 ユーザー登録”で設定したユーザーID、パスワードを入力してください。

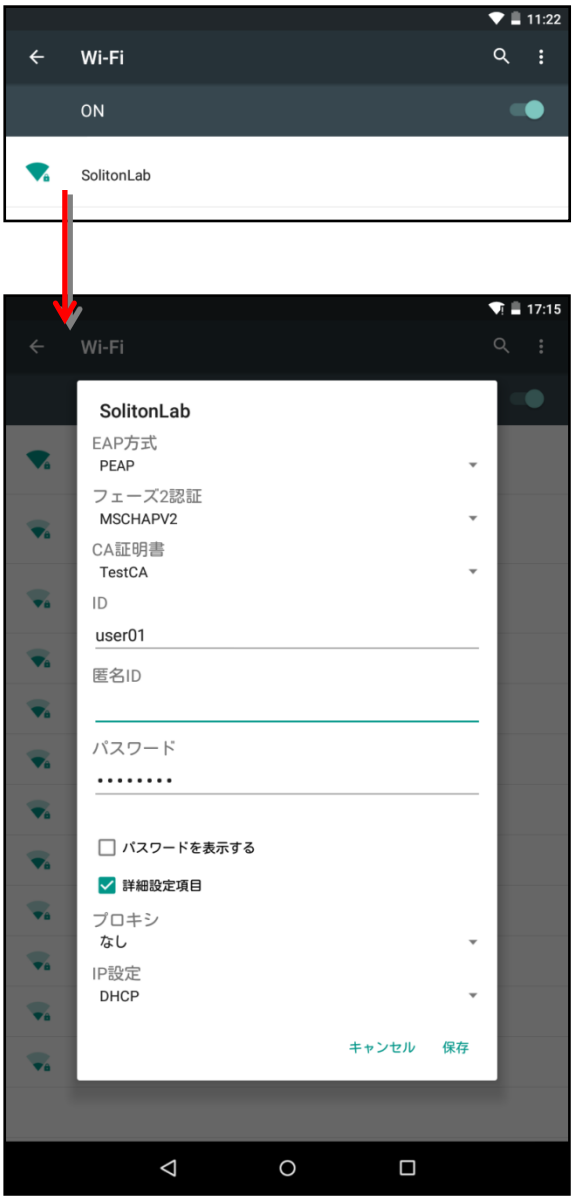
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。

項目	値
ユーザー名	user01
パスワード	password
モード	自動

5-3 Android(Google Nexus 7)のサプリカント設定

AP7532 で設定した SSID を選択し、サプリカントの設定を行います。

「ID」「パスワード」には”2-4 ユーザー登録”で設定したユーザーID、パスワードを入力してください。「CA 証明書」には、インポートした CA 証明書を選択してください。



項目	値
EAP 方式	PEAP
フェーズ 2 認証	MSCHAPV2
CA 証明書	TestCA
ID	user01
パスワード	password

6. 動作確認結果

6-1 EAP-TLS 認証

EAP-TLS 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	May 24 14:45:20 naeps radiusd[15541]: notice 2016/05/24 14:45:20 Login OK: [user01] (from client RadiusClient port 1 cli 54-4E-90-18-F2-AB)
AP7532	2016-05-24 14:46:16 ap7532-XXXXXX DOT11 WPA_WPA2_SUCCESS Client '54-4E-90-18-F2-AB' completed WPA2-AES handshake on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' 2016-05-24 14:46:16 ap7532-XXXXXX DOT11 EAP_SUCCESS Client '54-4E-90-18-F2-AB' 802.1x/EAP (type:eap-tls) authentication success on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' username user01 2016-05-24 14:46:13 ap7532-XXXXXX DOT11 CLIENT_ASSOCIATED Client '54-4E-90-18-F2-AB' associated to wlan 'SolitonLab' ssid 'SolitonLab' on radio 'ap7532-XXXXXX:R2'

6-2 EAP-PEAP(MS-CHAP V2)認証

EAP-PEAP 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	May 24 14:59:36 naeps radiusd[15541]: notice 2016/05/24 14:59:36 Login OK: [user01] (from client RadiusClient port 1 cli 54-4E-90-18-F2-AB via proxy to virtual server) May 24 14:59:36 naeps radiusd[15541]: notice 2016/05/24 14:59:36 Login OK: [user01] (from client RadiusClient port 1 cli 54-4E-90-18-F2-AB)
AP7532	2016-05-24 15:00:32 ap7532-XXXXXX DOT11 WPA_WPA2_SUCCESS Client '54-4E-90-18-F2-AB' completed WPA2-AES handshake on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' 2016-05-24 15:00:32 ap7532-XXXXXX DOT11 EAP_SUCCESS Client '54-4E-90-18-F2-AB' 802.1x/EAP (type:peap) authentication success on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' username user01 2016-05-24 15:00:29 ap7532-XXXXXX DOT11 CLIENT_ASSOCIATED Client '54-4E-90-18-F2-AB' associated to wlan 'SolitonLab' ssid 'SolitonLab' on radio 'ap7532-XXXXXX:R2'

改訂履歴

日付	版	改訂内容
2016/10/03	1.0	初版作成
2016/11/01	1.1	微修正