NetAttest EPS
認証連携設定例

【連携機器】BUFFALO WAPM-1750D

【Case】IEEE802.1x EAP-TLS, EAP-PEAP(MS-CHAPv2)認証

Rev1.0

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 CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS と BUFFALO 社製無線アクセスポイント WAPM-1750D の IEEE802.1x EAP-TLS, EAP-PEAP(MS-CHAPv2)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。

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 WAPM-1750D 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。

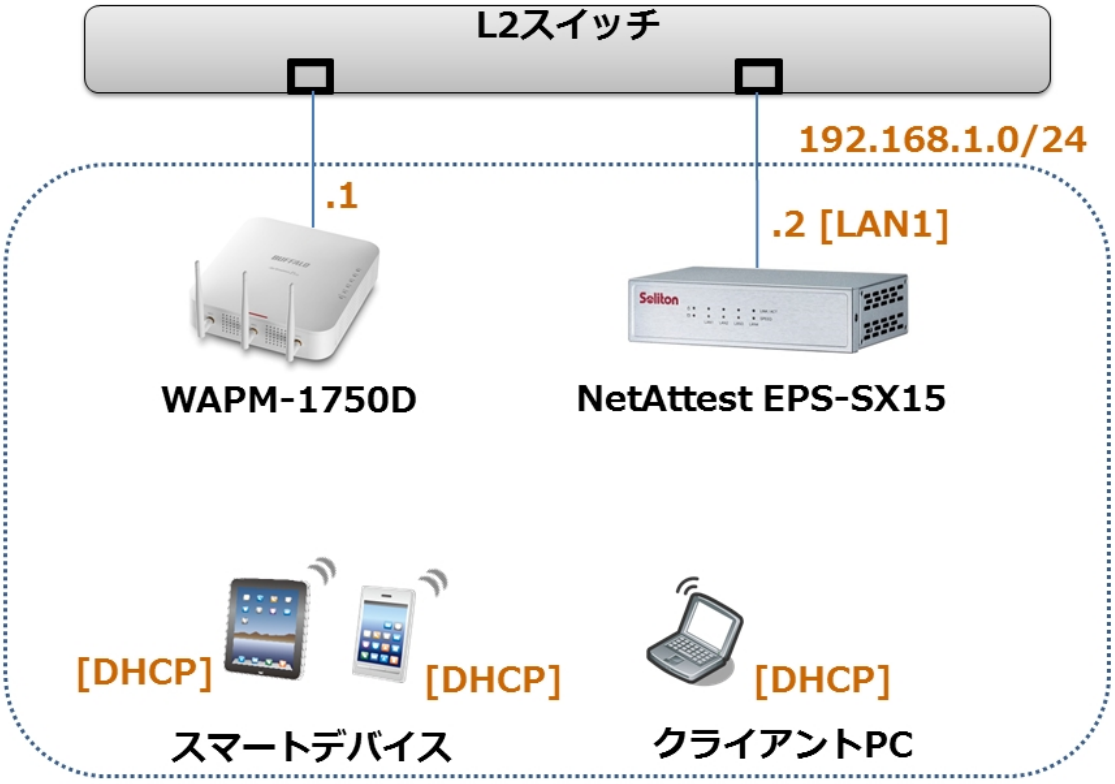
目次

構成

1-1 構成図

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。

- 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 EPS-ST04 の DHCP サーバーから払い出す



環境

1-1-1機器

製品名	メーカー	役割	バージョン
NetAttest EPS-SX15	Soliton Systems	RADIUS/CA サーバー	Ver. 4.8.7
WAPM-1750D	BUFFALO	RADIUS クライアント	Ver. 1.0.3
Surface Pro	Microsoft	Client PC (802.1X クライアント)	Windows 8.1 64bit Windows 標準サプリカント
iPad	Apple	Client Tablet (802.1X クライアント)	Ver. 8.0.2
Galaxy S5	Google	Client Phone (802.1X クライアント)	Ver. 5.0

1-1-2 認証方式

IEEE802.1x EAP-TLS 認証, IEEE802.1x EAP-MS-PEAP 認証

1-1-3 ネットワーク設定

	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS-ST04	192.168.1.2/24	UDP 1812	secret
WAPM-1750D	192.168.1.1/24		secret
Client PC	DHCP	-	-
Client Tablet	DHCP	-	-
Client Phone	DHCP	-	-

NetAttest EPS の設定

2-1 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、インターネットエクスプローラーから「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、インターネットエクスプローラーから「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。

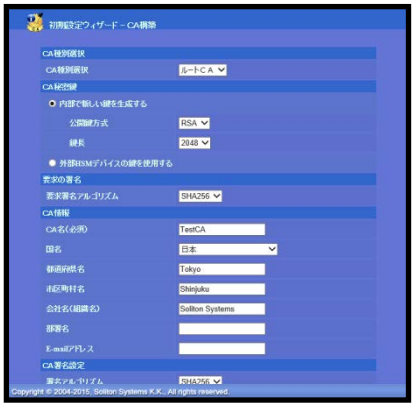
- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定
- メインネームサーバーの設定

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

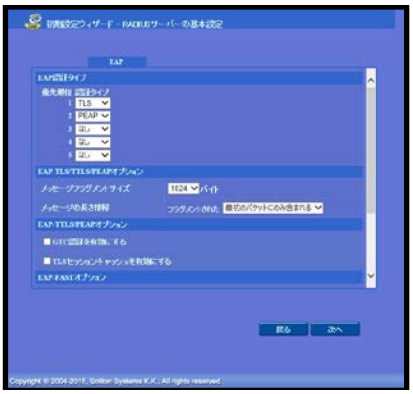
2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

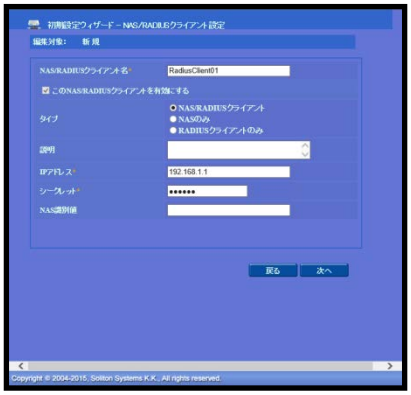
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定



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	RadiusClient
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

BUFFALO WAPM-1750D

3-1 BUFFALO WAPM-1750D 設定の流れ

BUFFALO 社製無線アクセスポイント WAPM-1750D を設定するためには、専用の設定・管理ツール「エアステーション設定ツール（Windows）」やシリアルコンソールを利用する方法、管理 Web GUI を利用する方法などが存在しますが、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。

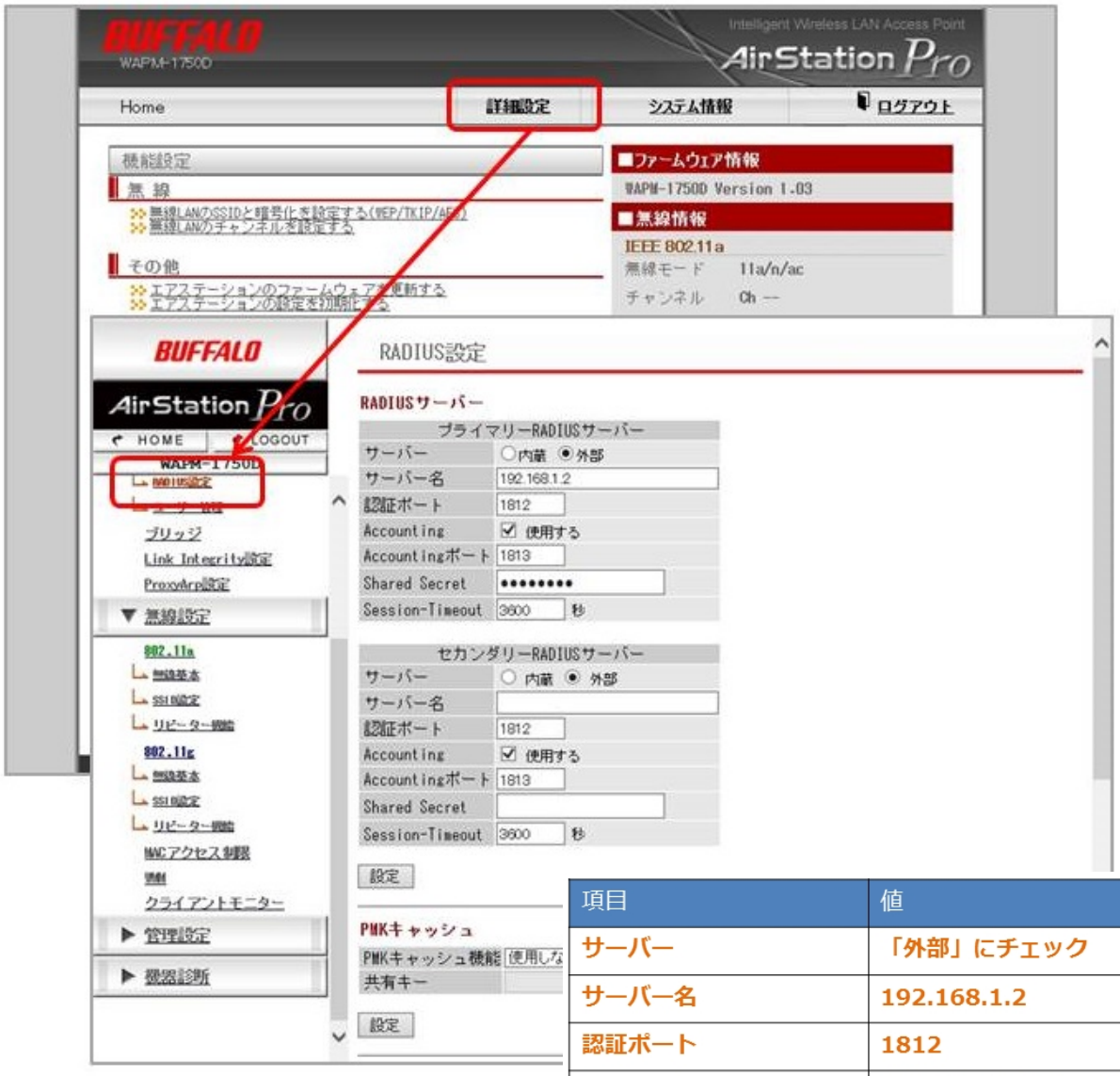
設定の流れ

1. RADIUS サーバーの登録
2. 無線基本設定
3. 無線セキュリティー設定

3-1-1　RADIUS サーバーの登録

RADIUS サーバーの設定をします。

TOP ページの［詳細設定］リンクをクリックします。［無線設定］メニューを展開し、［RADIUS 設定］リンクをクリックします。右側に RADIUS 設定項目が表示されますので、プライマリー認証サーバーの項目に値を入力します。



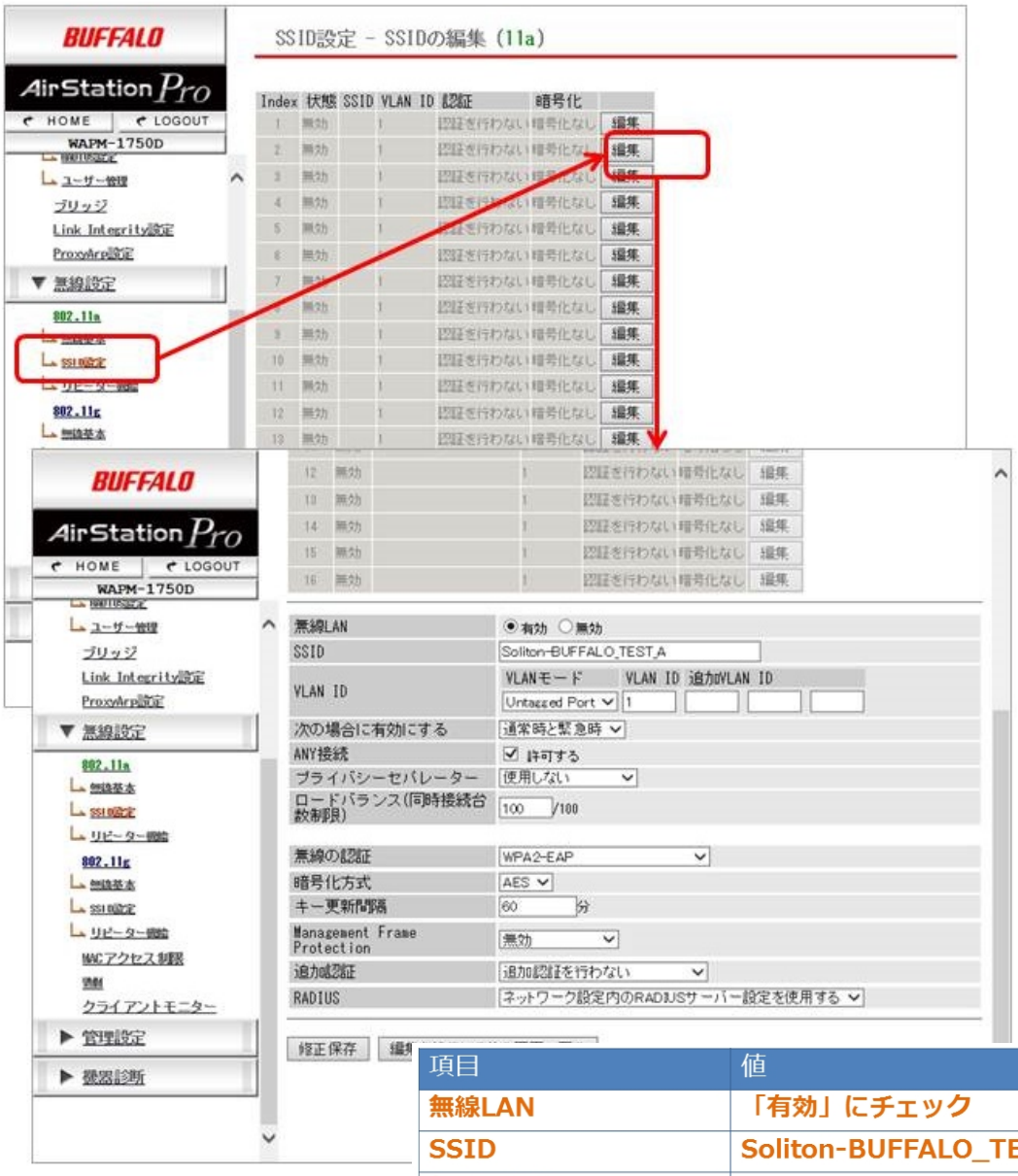
項目	値
サーバー	「外部」にチェック
サーバー名	192.168.1.2
認証ポート	1812
Accounting	「使用する」にチェック
Accountingポート	1823
Shared Secret	secret

3-1-2 無線基本設定

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 [無線設定] を展開し、802.11a の [SSID 設定]リンクをクリックします。

[編集]ボタンをクリックし、無線 LAN の設定を行います。



項目	値
無線LAN	「有効」にチェック
SSID	Soliton-BUFFALO_TEST_A
無線の認証	WPA2-EAP
RADIUS	ネットワーク設定内のRADIUSサーバーを使用する

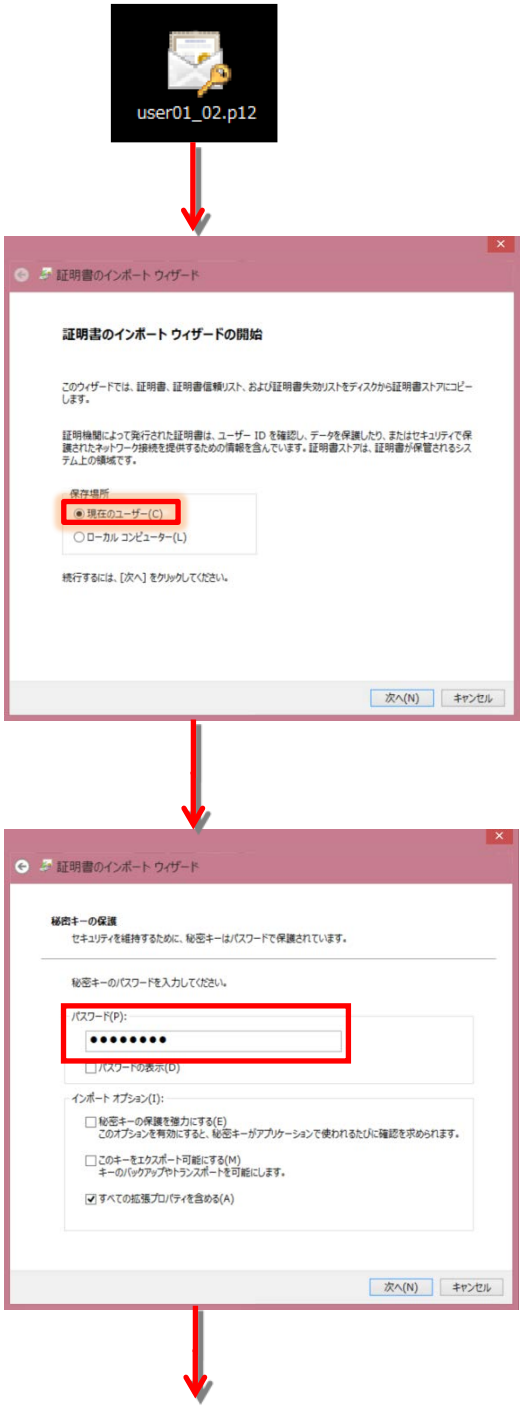
NetAttest EPS による RADIUS 認証を行うためには、「EAP」がついている方式を選択します。
また、選択した認証方式により設定可能な [無線の暗号化] も決定されます。

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 デジタル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

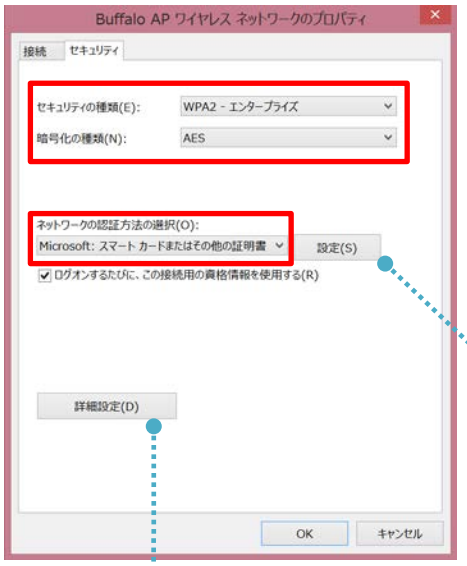

証明書のインポート ウィザード
証明書ストア
証明書ストアは、証明書が保管されるシステム上の領域です。
Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。
証明書の種類に基づいて、自動的に証明書ストアを選択する(U)
証明書をすべて次のストアに配置する(P)
証明書ストア:
参照(R)...
次へ(N)
キャンセル
証明書のインポート ウィザード
証明書のインポート ウィザードの完了
[完了] をクリックすると、証明書がインポートされます。
次の設定が指定されました:
選択された証明書ストア
ウィザードで自動的に決定されます
内容
PFX
ファイル名
C:¥Users¥soliton¥AppData¥Local¥Microsoft¥Windows¥INetCach
完了(F)
キャンセル

サプリカント設定

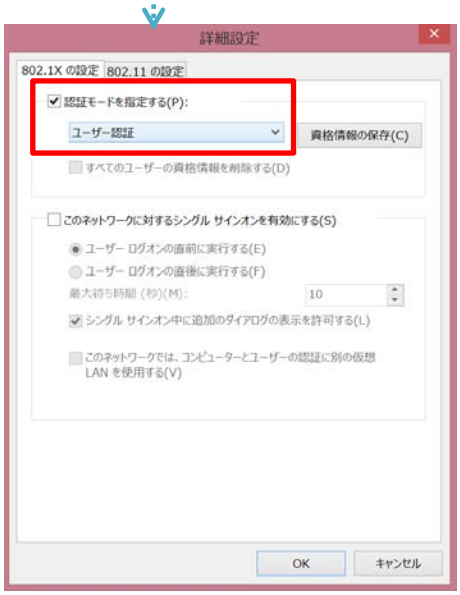
Windows 標準サプリカントで TLS の設定を行います。

※本項では TLS の設定のみを記載します。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・・	On
- 単純な証明書の選択・・・	On
証明書を検証してサーバー・・・	On
信頼されたルート証明機関	TestCA

4-2 iOS (iPad)での EAP-TLS 認証

4-2-1 デジタル証明書のインポート

NetAttest EPS から発行したデジタル証明書を 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) デジタル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)

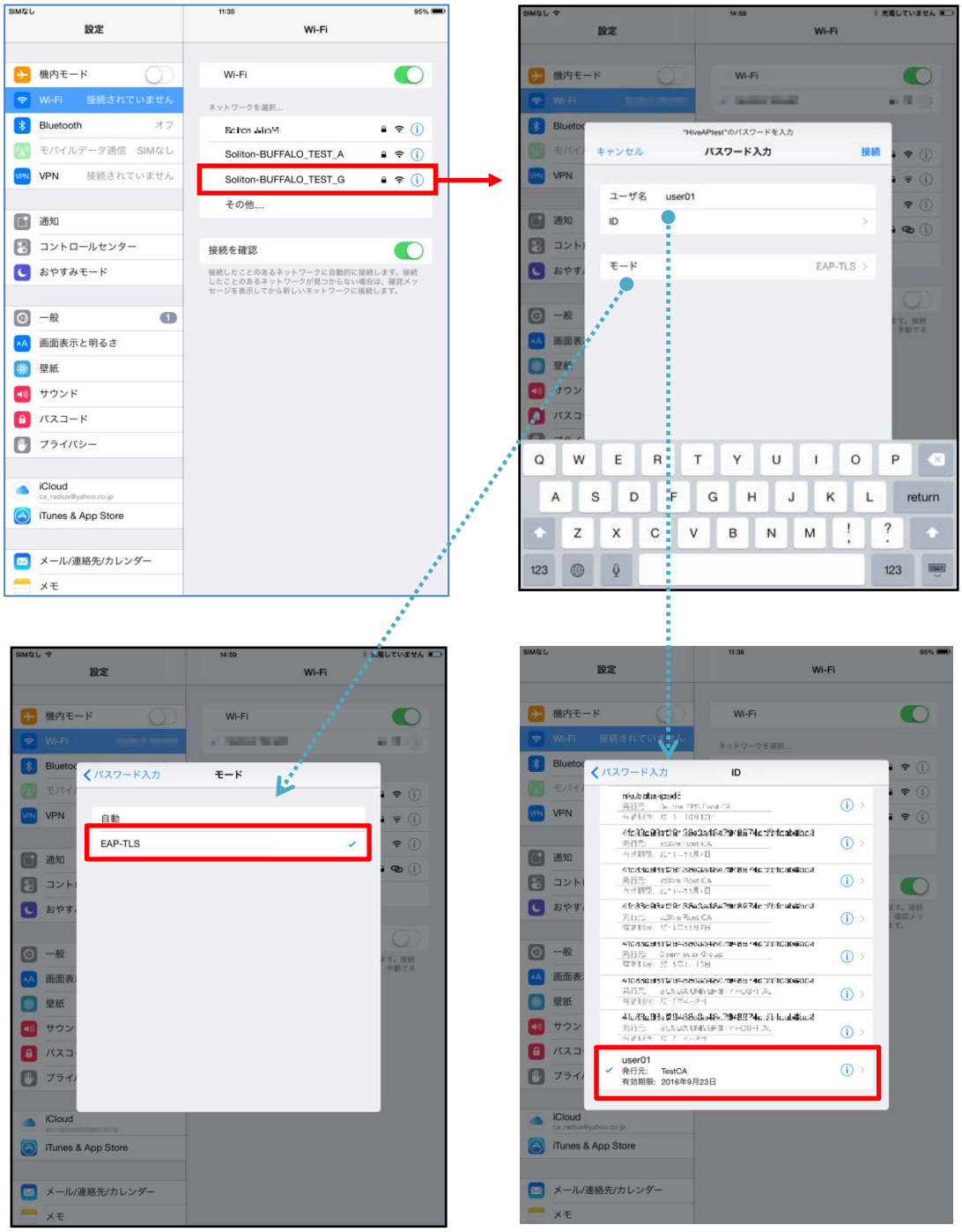
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

サプリカント設定

WAPM-1750D で設定した SSID をタップし、サプリカントの設定を行います。

※本項では TLS の設定のみを記載します。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アカウントの 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ユーザー証明書を選択します。



4-3 Android (Galaxy S5)での EAP-TLS 認証

4-3-1 デジタル証明書のインポート

NetAttest EPS から発行したデジタル証明書を 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 証明書とユーザー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 カードにデジタル証明書を保存し、インポートする方法※1
2) デジタル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。

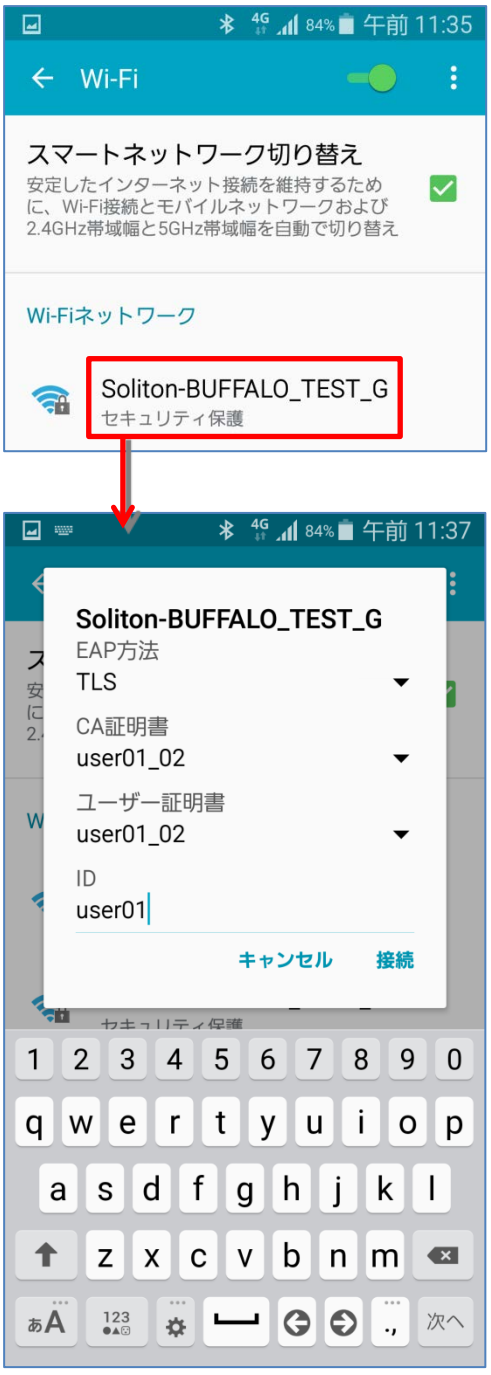
Android 5.0 では証明書インポート時に用途別に証明書ストアが選択できますが、本書では無線 LAN 接続を行うため「Wi-Fi」を選択しています。

4-3-2 サプリカント設定

WAPM-1750D で設定した SSID をタップし、サプリカントの設定を行います。

※本項では TLS の設定のみを記載します。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アカウントの 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
セキュリティ	802.1X EAP
EAP 方式	TLS
CA 証明書	user01_02
ユーザー証明書	user01_02
ID	user01

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 のサプリカント設定

WAPM-1750D で設定した SSID をタップし、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。

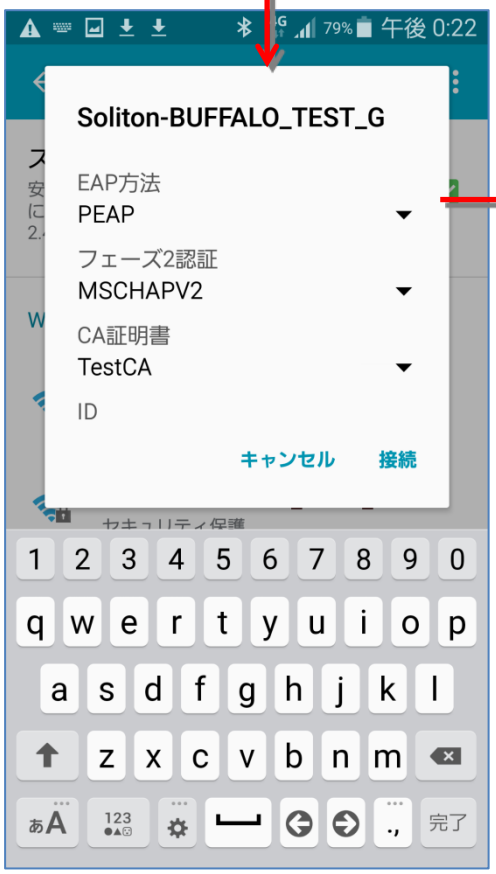
項目	値
ユーザー名	user01
パスワード	password
モード	自動

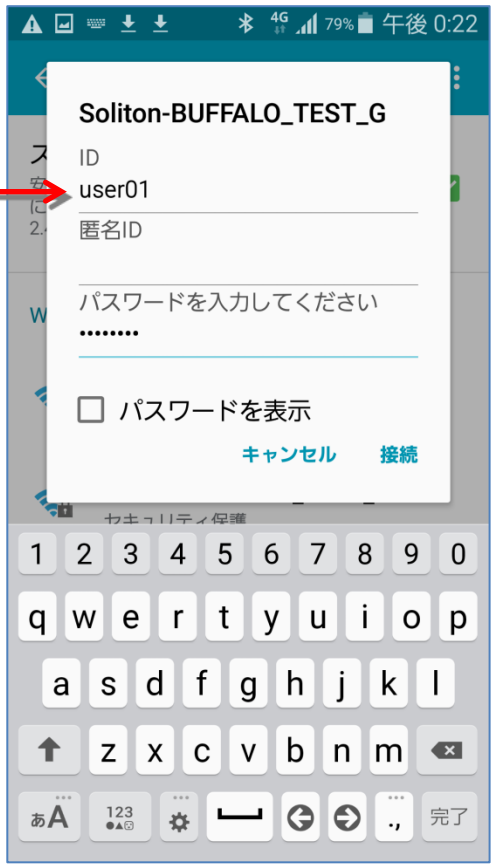
5-3 Android のサプリカント設定

WAPM-1750D で設定した SSID をタップし、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。「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
セキュリティ	802.1X EAP
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





改訂履歴

日付	版	改訂内容
2016/09/02	1.0	初版作成