NetAttest EPS
認証連携設定例

【連携機器】サイレックス・テクノロジー SX-AP-4800AN2

【Case】IEEE802.1X EAP-TLS/EAP-PEAP

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

本書はオールインワン認証アプライアンス NetAttest EPS と、サイレックス・テクノロジー社製無線アクセスポイント SX-AP-4800AN2 の IEEE802.1X EAP-TLS / EAP-PEAP 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 SX-AP-4800AN2 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。

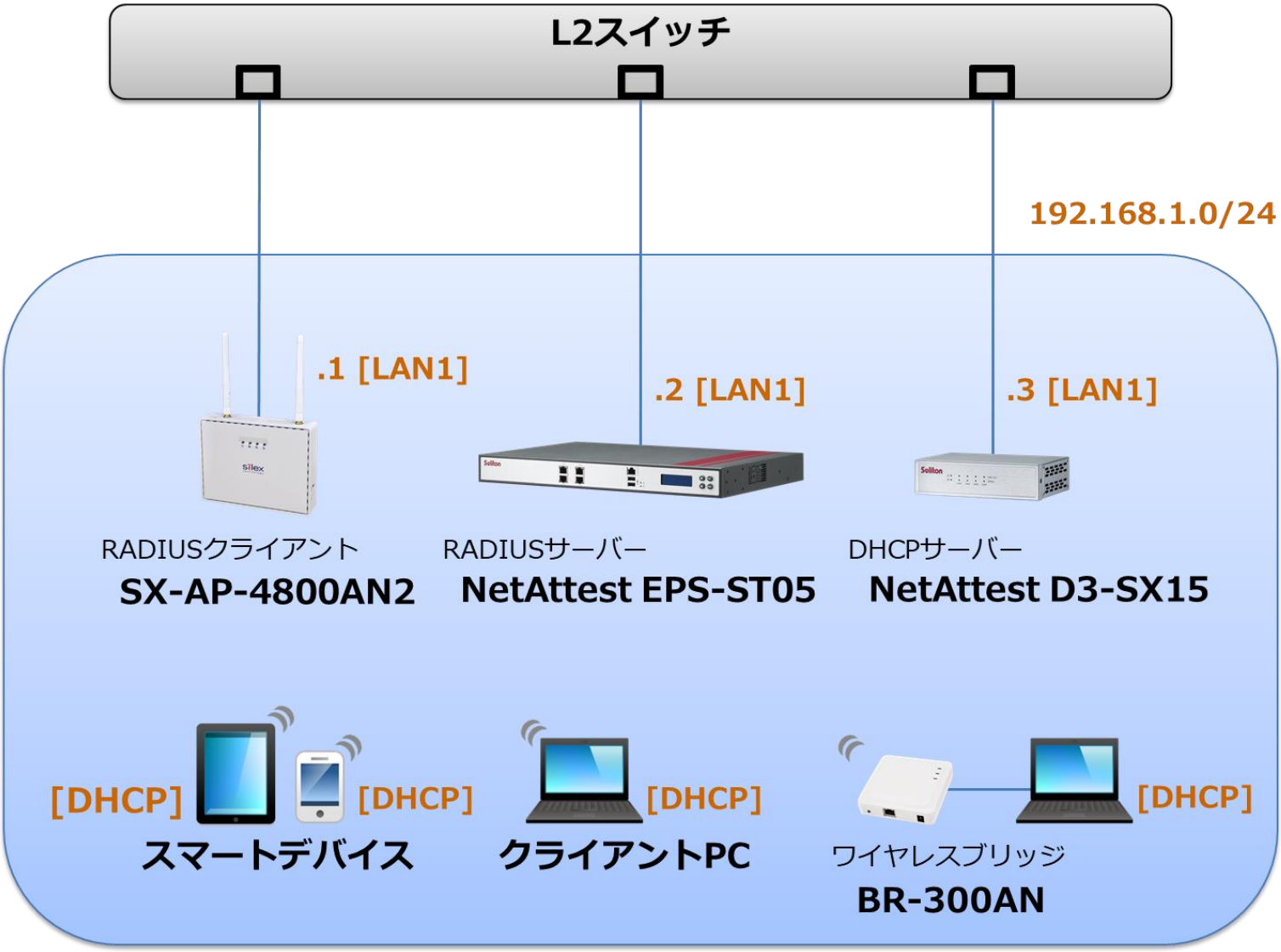
目次

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-SX15 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-ST05	ソリトンシステムズ	RADIUS/CA サーバー	4.10.4
SX-AP-4800AN2	サイレックス・テクノロジー	RADIUS クライアント (無線アクセスポイント)	1.0.2
BR-300AN	サイレックス・テクノロジー	802.1X クライアント (ワイヤレスブリッジ)	1.6.0
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サプリカント
iPad Air 2	Apple	802.1X クライアント (Client SmartPhone)	12.2
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0
NetAttest D3-SX15	ソリトンシステムズ	DHCP/DNS サーバー	4.2.17

1-2-2 認証方式

IEEE802.1X EAP-TLS/EAP-PEAP

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-ST05	192.168.1.2/24	UDP 1812	secret
SX-AP-4800AN2	192.168.1.1/24		secret
BR-300AN	DHCP		
VAIO Pro PB	DHCP	-	-
iPad Air 2	DHCP	-	-
Pixel C	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。

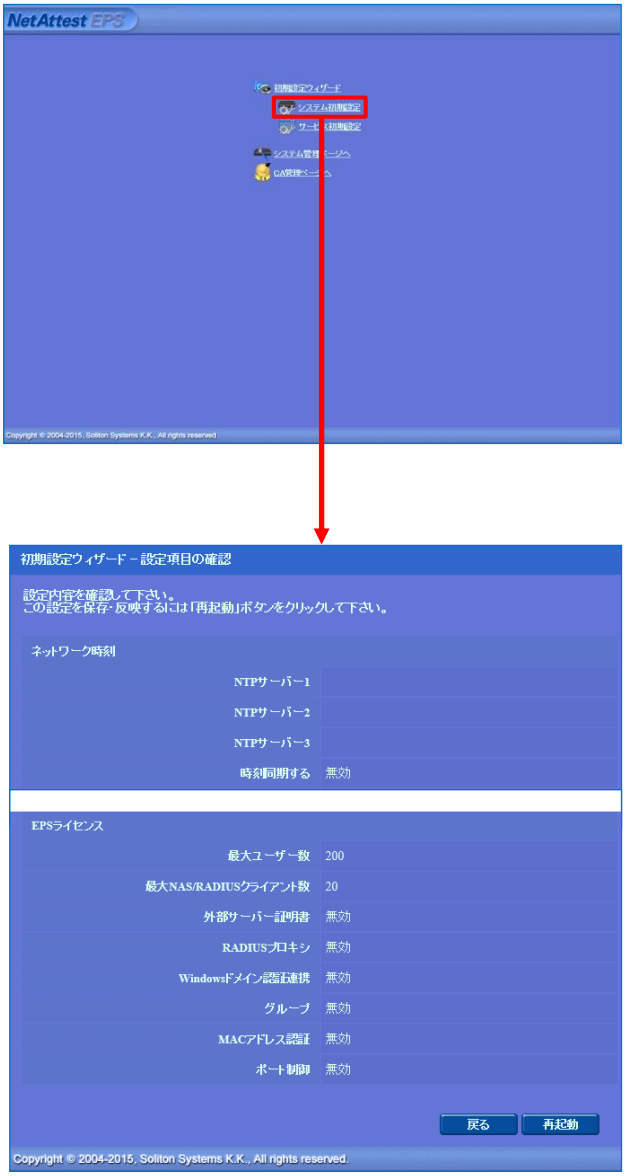
下記のような流れでセットアップを行います。

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

管理ページにアクセスしたら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
- ドメインネームサーバーの設定



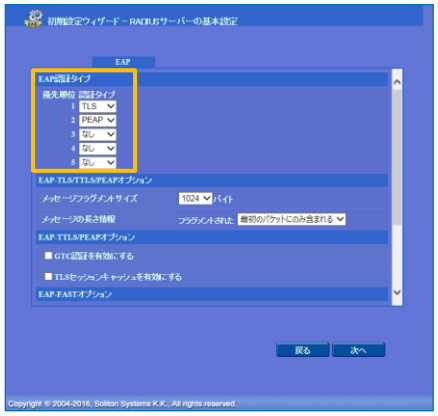
項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

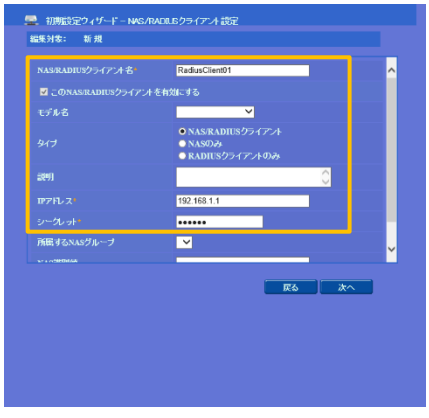
サービス初期設定ウィザードを実行します。

- 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

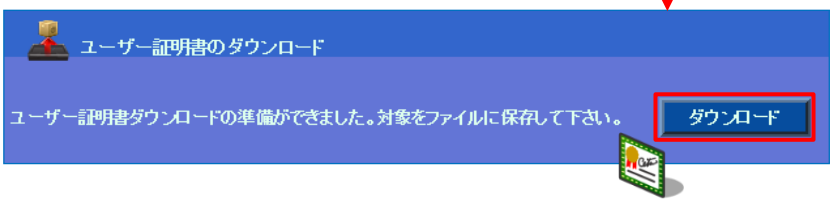
2-5 クライアント証明書の発行

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.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



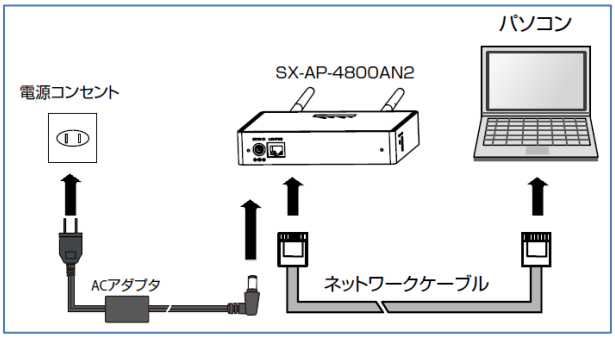
3. SX-AP-4800AN2 の設定

3-1 設定モードの実行

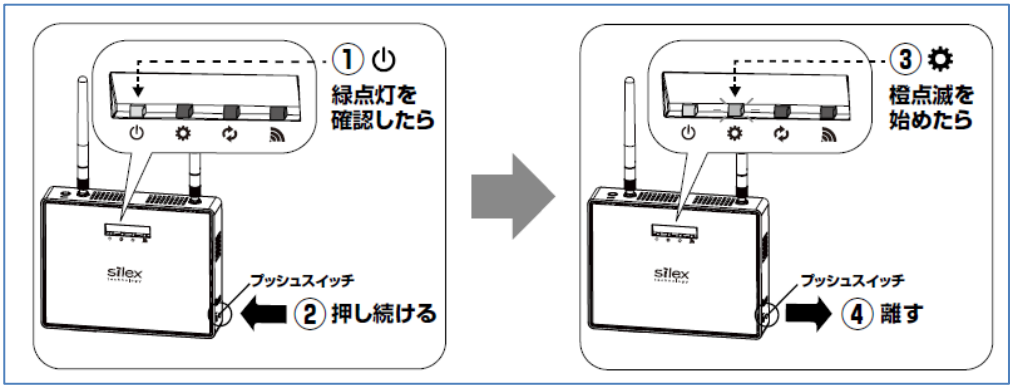
SX-AP-4800AN2 の初期設定は本体内部の Web 設定ページから行います。

下記手順で本体内部 Web 設定ページにアクセスしてください。

1. 設定用の管理端末と SX-AP-4800AN2 をネットワークケーブルで直接接続。



2. SX-AP-4800AN2 に付属の AC アダプタを接続し、AC アダプタのプラグをコンセントに差し込む。
3. 電源投入後、筐体上部の「Power」LED が緑色に点灯したら「SET1」(プッシュスイッチ)を先の細いもので数秒(約 3 秒)押し込む。
4. 筐体上部の「Mode」LED が橙点滅に変わったらプッシュスイッチを離す。



5. 管理端末で Web ブラウザ(Internet Explorer など)を起動すると SX-AP-4800AN2 の Web 設定ページが起動する。

◆ 表示されない場合はアドレスバーに「http://silex」と入力してください。

3-2 Web 設定ページを利用したセットアップ

Web 設定ページが開いたら必要な個所の設定を行います。必要最低限の項目は下記の通りです。
無線 LAN に関連する部分の設定については利用する環境によって異なります。
ご利用環境に併せて設定してください。下記は 2.4GHz で設定した場合の一例です。

1. 「TCP/IP 設定」内の下記項目

項目	値
DHCP	DISABLE
IP アドレス	192.168.1.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.1.254

2. 「無線 LAN 共通設定」の下記項目

項目	値
無線モード	802.11n/b/g/
チャネル帯域幅	20MHz
通信チャネル	11

3. 「無線 LAN 基本設定」の下記項目

項目	値
インタフェース	ENABLE
SSID	任意文字列(1-32 文字の文字列)
ステルスモード	DISABLE
ネットワーク認証	WPA2-Enterprise

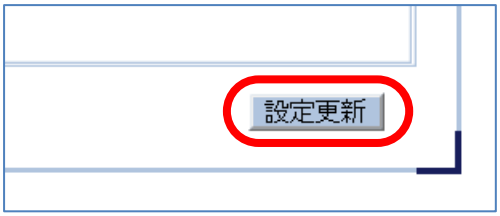
4. 「WPA/WPA2 設定」の下記項目

項目	値
暗号方式	AES
グループ鍵更新間隔	60

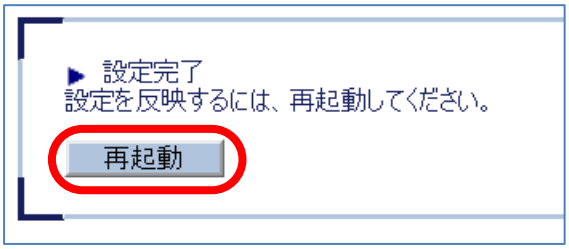
5. 「RADIUS サーバ設定」の下記項目

項目	値
サーバ IP アドレス	192.168.1.2
ポート番号	1812
シークレットキー	secret

6. 設定実施後、画面右下の「更新」ボタンを押下する



7. 再起動を促すメッセージが表示されるので「再起動」ボタンを押下する



8. 再起動後、ネットワークケーブルを管理端末から外し実際の利用環境に接続し直して完了

4. EAP-TLS 認証でのクライアント設定

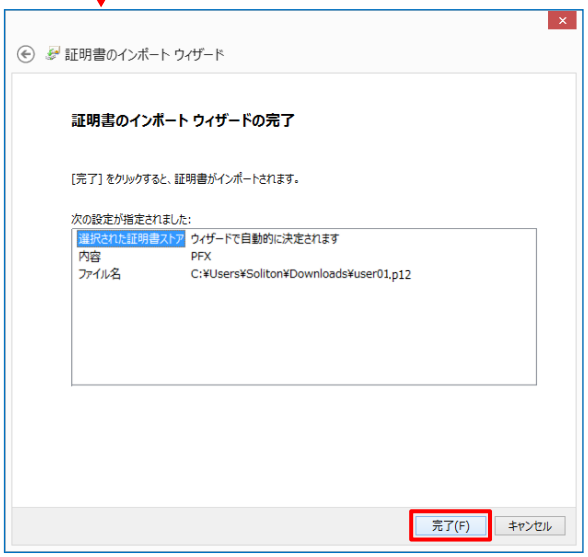
4-1 Windows 10 での EAP-TLS 認証

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.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】

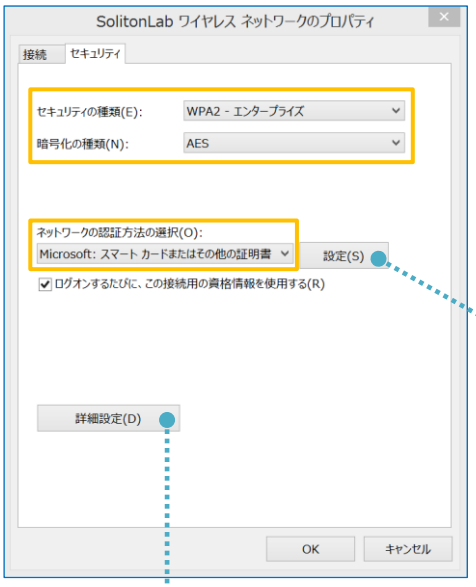
「2-4 ユーザーの登録」で設定したパスワードを入力



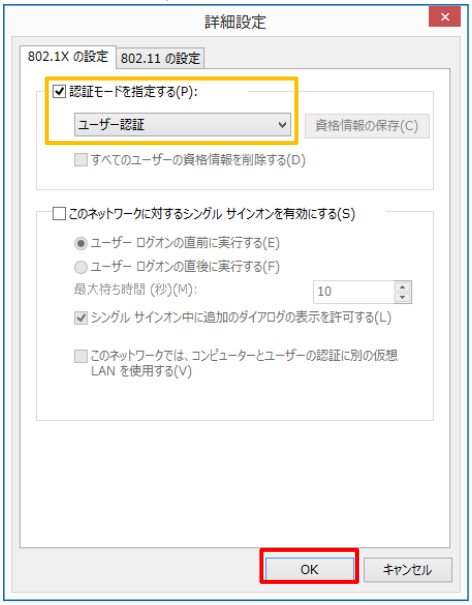
4-1-2 サプリカント設定

Windows 標準サプリカントで TLS の設定を行います。

[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 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には下記などがあります。

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)

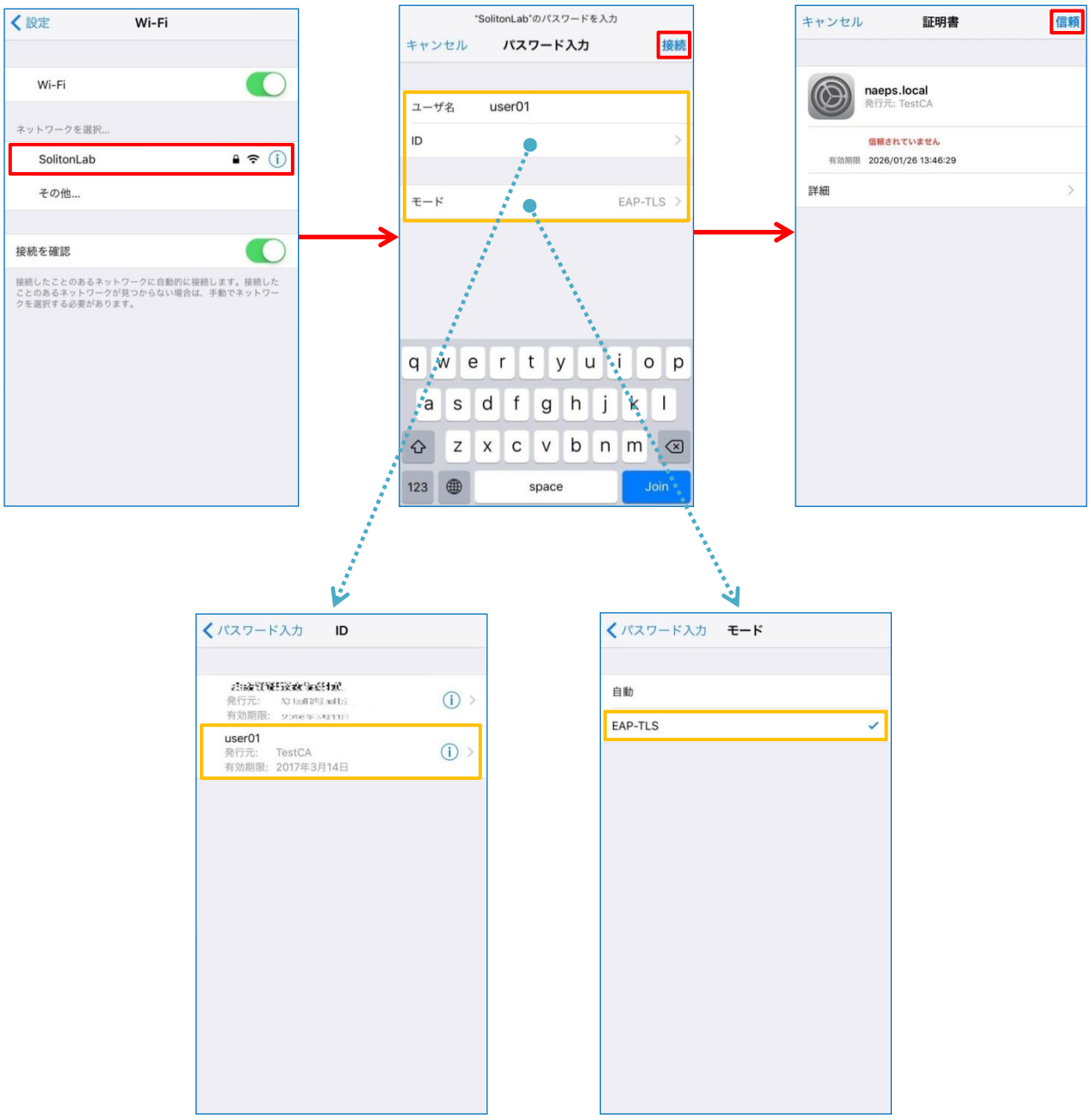
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

SX-AP-4800AN2 で設定した SSID を選択し、サプリカントの設定を行います。

まず、「ユーザ名」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 での EAP-TLS 認証

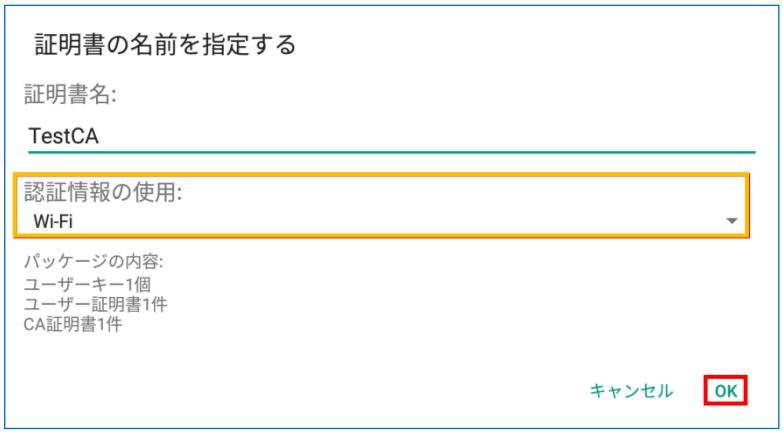
4-3-1 クライアント証明書のインポート

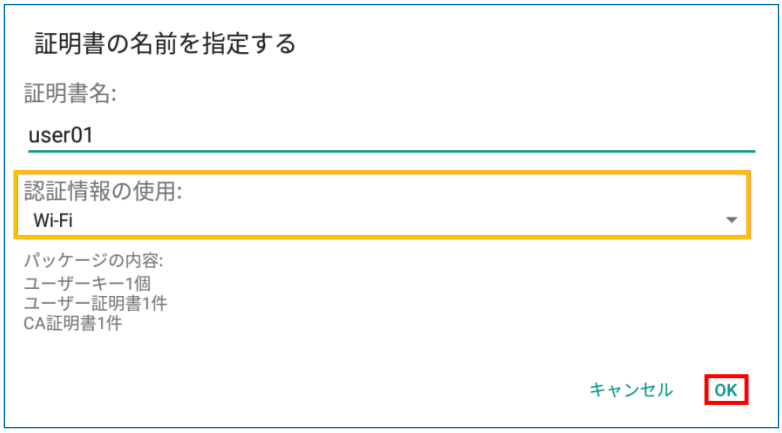
NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

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 8.1.0 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 への接続を行うため「Wi-Fi」を選択しています。

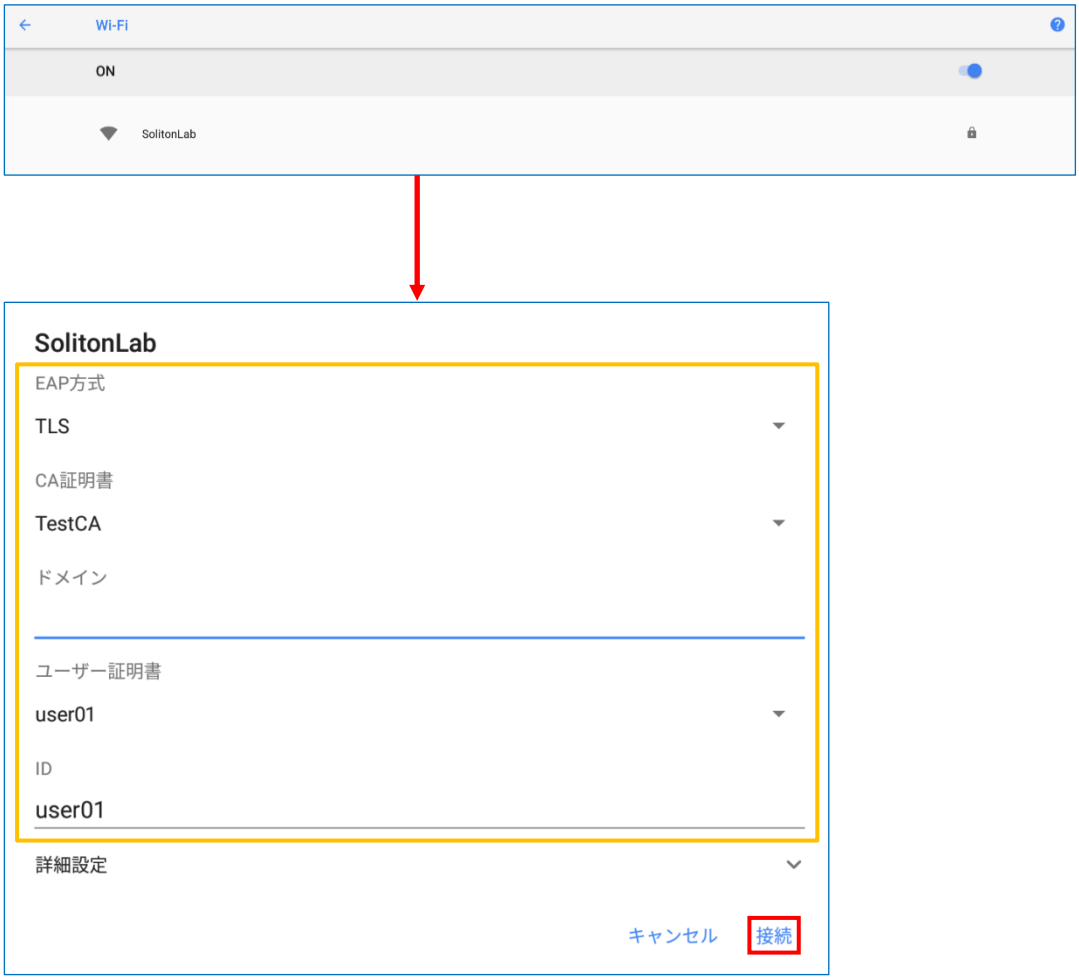




4-3-2 サプリカント設定

SX-AP-4800AN2 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」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

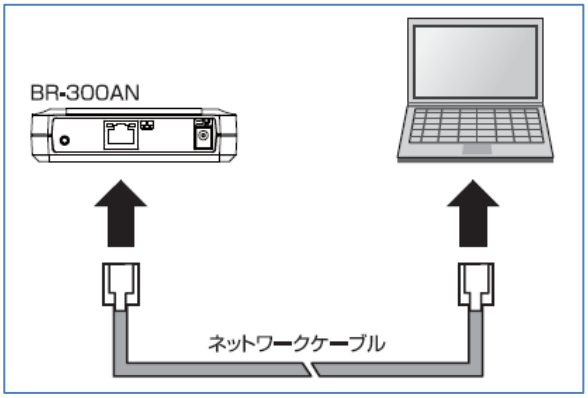
4-4 BR-300AN での EAP-TLS 認証

4-4-1 管理画面へアクセス

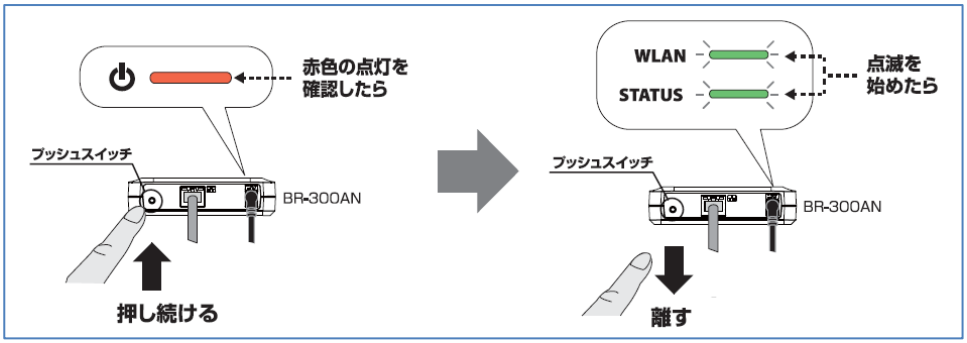
BR-300AN に NetAttest EPS から発行したクライアント証明書をインポートするには本体内部の Web 設定ページを使用します。

下記手順で本体内部 Web 設定ページにアクセスしてください。

1. 設定用の管理端末と BR-300AN を付属のネットワークケーブルで直接接続。



2. BR-300AN に付属の AC アダプタを接続し、AC アダプタのプラグをコンセントに差し込む。
3. 電源投入後、筐体上部の「POWER」LED が赤色に点灯したらプッシュスイッチを数秒押し込む。
4. 筐体上部の「WLAN」LED と「STATUS」LED が緑色で同時点滅を開始したらプッシュスイッチを離す。



5. 管理端末で Web ブラウザ(Internet Explorer など)を起動すると BR-300AN の Web 設定ページが起動する。

◆ 表示されない場合はアドレスバーに「http://silex」と入力してください。

4-4-2 無線 LAN 設定

Web 設定ページが開いたらクライアント証明書のインポートと必要な個所の設定を行います。必要最低限の項目は下記の通りです。

1. 「詳細設定」タブに移動

2. 「無線 LAN 基本設定」内の下記項目

項目	値
無線モード	Infra
無線規格	AUTO
SSID	SX-AP-4800AN2 に設定した SSID
SSID フィルタ	OFF(※ 環境により ON)
ネットワーク認証	WPA2
IEEE802.1x 認証	ON

3. 「IEEE802.1x 認証設定」内の下記項目

項目	値
IEEE802.1x 認証モード	EAP-TLS

4. 「WPA/WPA2 設定」内の下記項目

項目	値
暗号化方式	AES

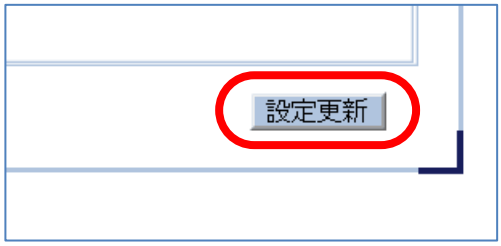
5. 「IEEE802.1x 認証ユーザ設定」内の下記項目

項目	値
IEEE802.1x ユーザ名	user01

6. 「IEEE802.1X 接続機器設定」内の下記項目

項目	値
接続機器フィルタ	ON
接続機器アドレス	※ BR-300AN を接続する機器の MAC アドレス

7. 設定実施後、画面右下の「更新」ボタンを押下する



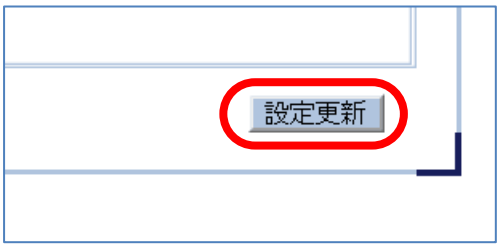
4-4-3 クライアント証明書のインポート

1. 「証明書設定」メニューに移動

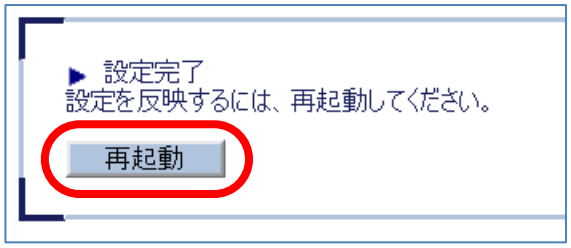
2. 「クライアント証明書」内の「証明書ファイル」欄を選択後、「参照」ボタンより NetAttest EPS で発行したクライアント証明書ファイルを指定し、「パスワード」を入力

3. 「CA 証明書」内の「証明書ファイル」欄を選択後、「参照」ボタンより NetAttest EPS で発行したクライアント証明書ファイルを指定する

4. 設定実施後、画面右下の「更新」ボタンを押下する



5. 再起動を促すメッセージが表示されるので「再起動」ボタンを押下する

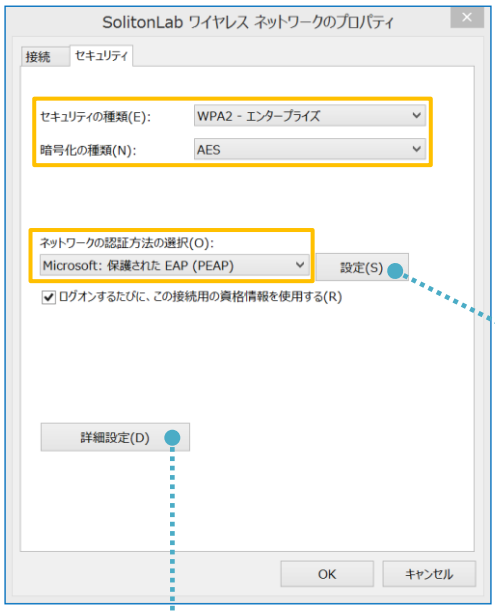


5. EAP-PEAP 認証でのクライアント設定

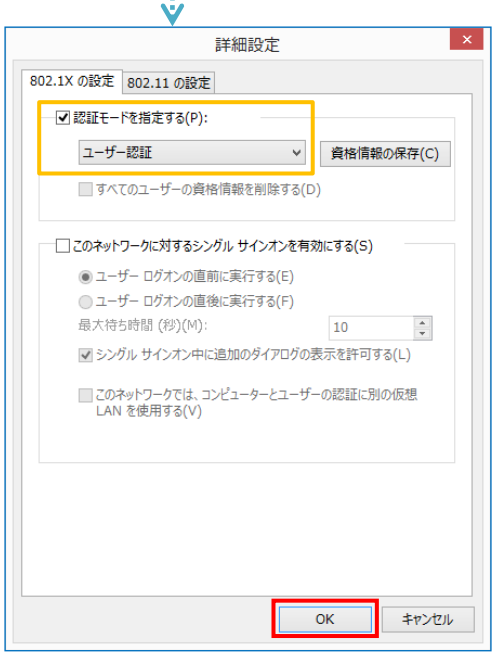
5-1 Windows 10 での EAP-PEAP 認証

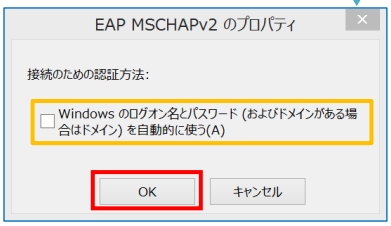
5-1-1 Windows 10 のサプリカント設定

[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
- Windows のログオン名と・・・	Off

5-2 iOS での EAP-PEAP 認証

5-2-1 iOS のサプリカント設定

SX-AP-4800AN2 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。

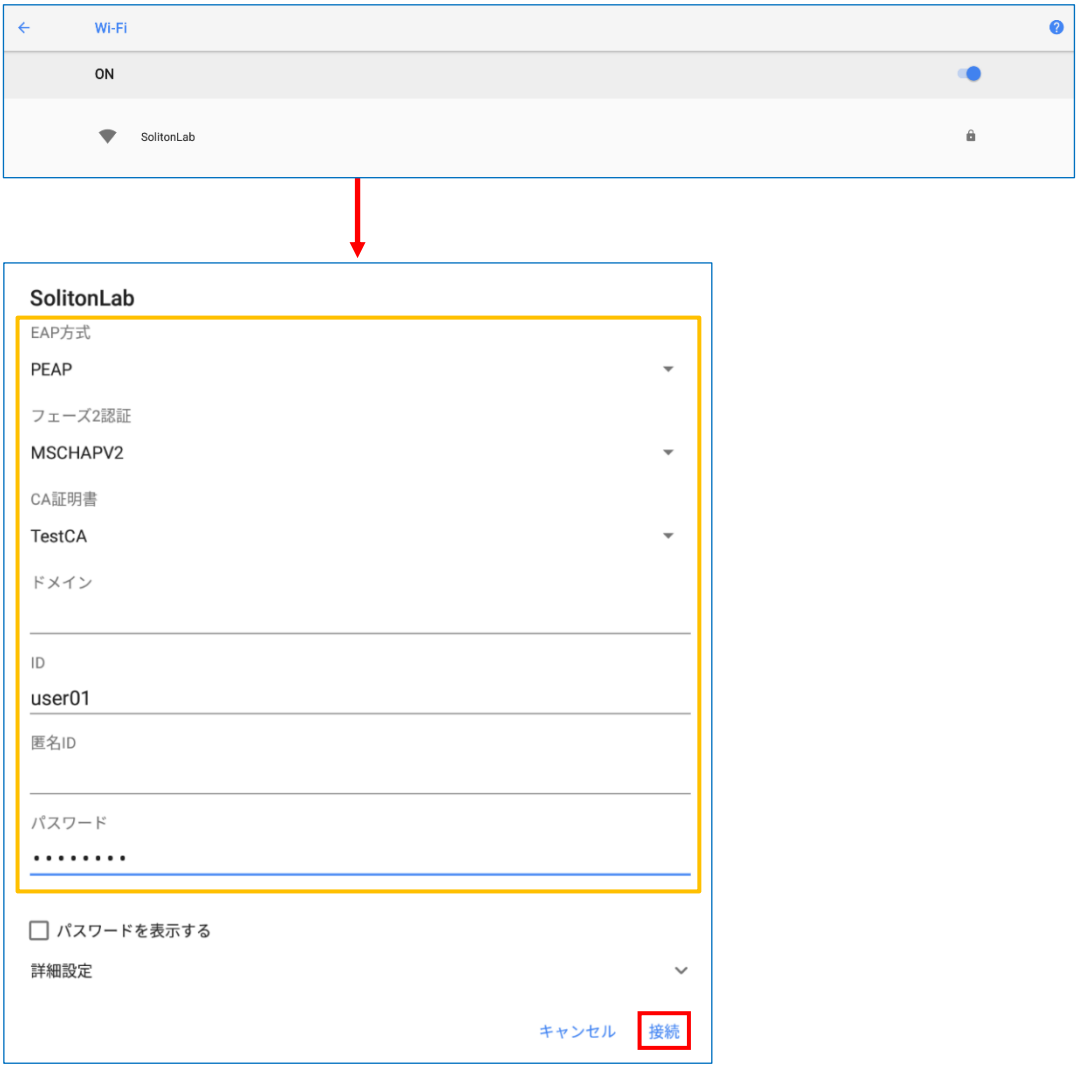
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。

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

5-3 Android での EAP-PEAP 認証

5-3-1 Android のサプリカント設定

SX-AP-4800AN2 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

5-4 BR-300AN での EAP-PEAP 認証

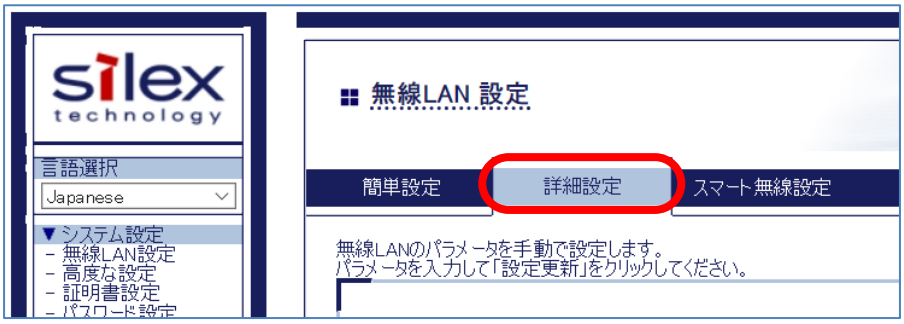
5-4-1 BR-300AN のサプリカント設定

BR-300AN にサプリカントの設定を行うには本体内部の Web 設定ページより行います。

Web 設定ページへのアクセスは「4-4-1 管理画面へアクセス」をご参照ください。

Web 設定ページが開いたら必要な個所の設定を行います。必要最低限の項目は下記の通りです。

1. 「詳細設定」タブに移動



2. 「無線 LAN 基本設定」内の下記項目

項目	値
無線モード	Infra
無線規格	AUTO
SSID	SX-AP-4800AN2 に設定した SSID
SSID フィルタ	OFF(※ 環境により ON)
ネットワーク認証	WPA2
IEEE802.1x 認証	ON

3. 「IEEE802.1x 認証設定」内の下記項目

項目	値
IEEE802.1x 認証モード	PEAP

4. 「WPA/WPA2 設定」内の下記項目

項目	値
暗号化方式	AES

5. 「内部認証方式設定」内の下記項目

項目	値
内部認証方式	MSCHAPv2

6. 「サーバ証明書検証設定」内の下記項目

項目	値
サーバ証明書の検証	OFF

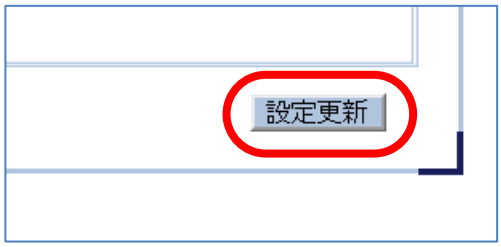
7. 「IEEE802.1x 認証ユーザ設定」内の下記項目

項目	値
IEEE802.1x ユーザ名	user01
パスワード	secret

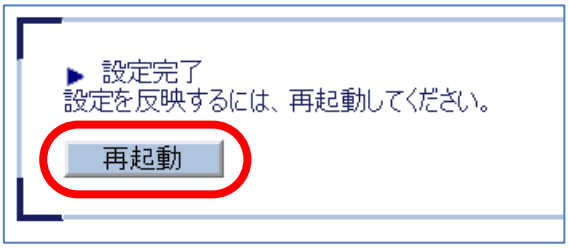
8. 「IEEE802.1X 接続機器設定」内の下記項目

項目	値
接続機器フィルタ	ON
接続機器アドレス	※ BR-300AN を接続する機器の MAC アドレス

9. 設定実施後、画面右下の「更新」ボタンを押下する



10. 再起動を促すメッセージが表示されるので「再起動」ボタンを押下する



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	Login OK: [user01] (from client RadiusClient01 port 0 cli 40-A3-CC-32-10-A4)
SX-AP-4800AN2	ath0: STA 40:a3:cc:32:10:a4 IEEE 802.1X: authenticated - EAP type: 13 ((null))

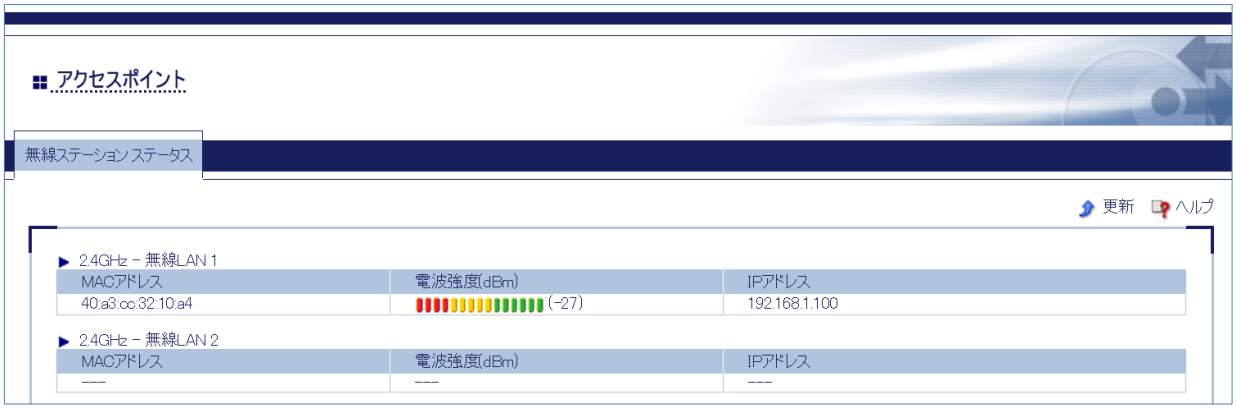
6-2 EAP-PEAP 認証

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	Login OK: [user01] (from client RadiusClient01 port 0 cli 40-A3-CC-32-10-A4 via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 0 cli 40-A3-CC-32-10-A4)
SX-AP-4800AN2	ath0: STA 40:a3:cc:32:10:a4 IEEE 802.1X: authenticated - EAP type: 13 ((null))

6-3 端末接続状況

SX-AP-4800AN2 管理画面の[ステータス表示]-[無線ステーション]にて確認できます。



改訂履歴

日付	版	改訂内容
2019/11/06	1.0	初版作成