NetAttest EPS
認証連携設定例

【連携機器】BUFFALO WAPM-2133TR/WAPM-1266R/
WAPM-1266WDPR/WAPS-1266

【Case】IEEE802.1X EAP-TLS/EAP-PEAP

Rev2.0

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、BUFFALO 社製無線アクセスポイント WAPM-2133TR 及び WAPM-1266R/WAPM-1266WDPR/WAPS-1266 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 WAPM-2133TR/WAPM-1266R/WAPM-1266WDPR/WAPS-1266 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。

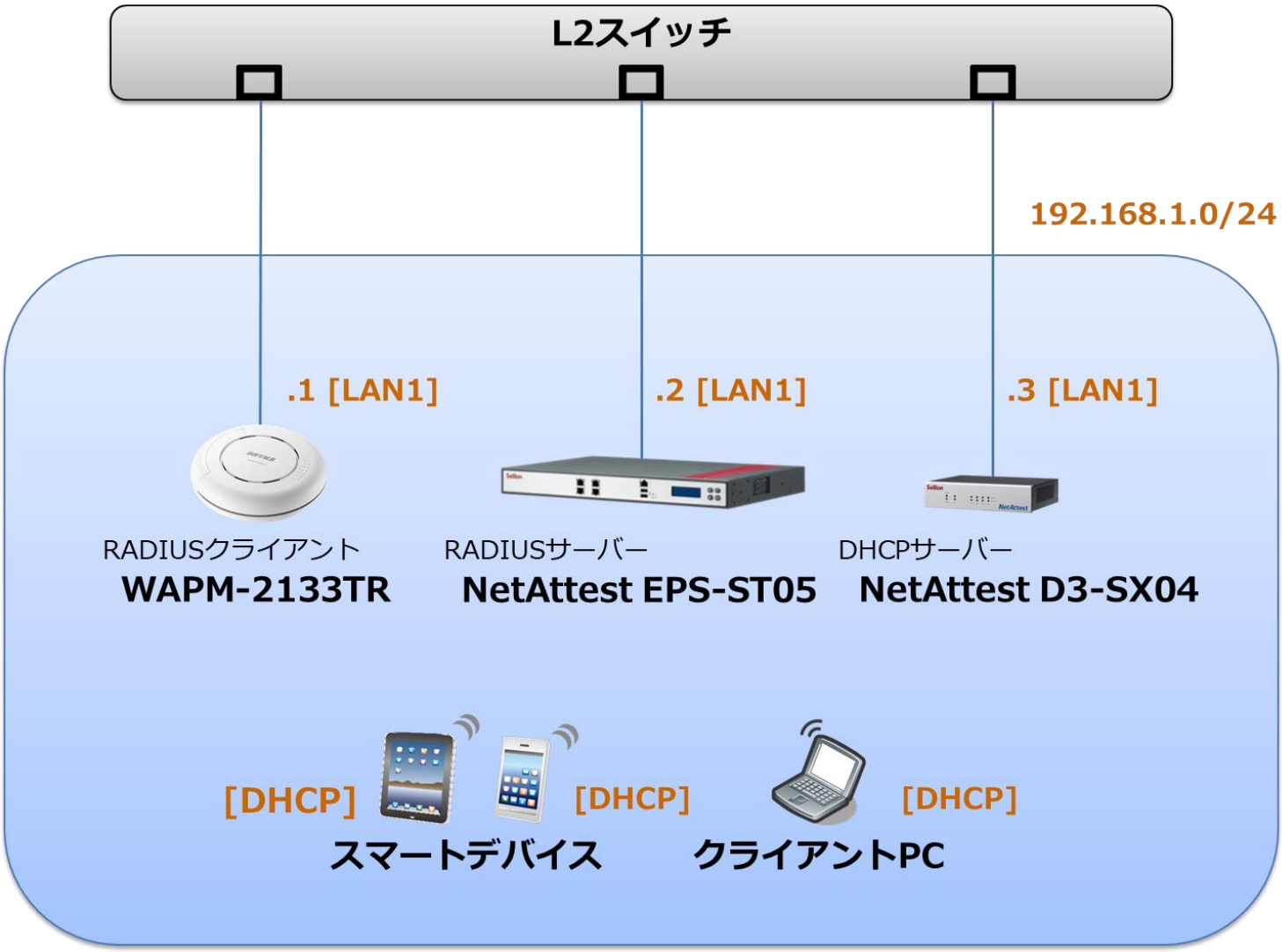
目次

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-ST05	ソリトンシステムズ	RADIUS/CA サーバー	4.10.2
WAPM-2133TR	BUFFALO	RADIUS クライアント (無線アクセスポイント)	1.07
Surface	Microsoft	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サプリカント
iPhone 7	Apple	802.1X クライアント (Client SmartPhone)	11.2.6
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.15

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
WAPM-2133TR	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。

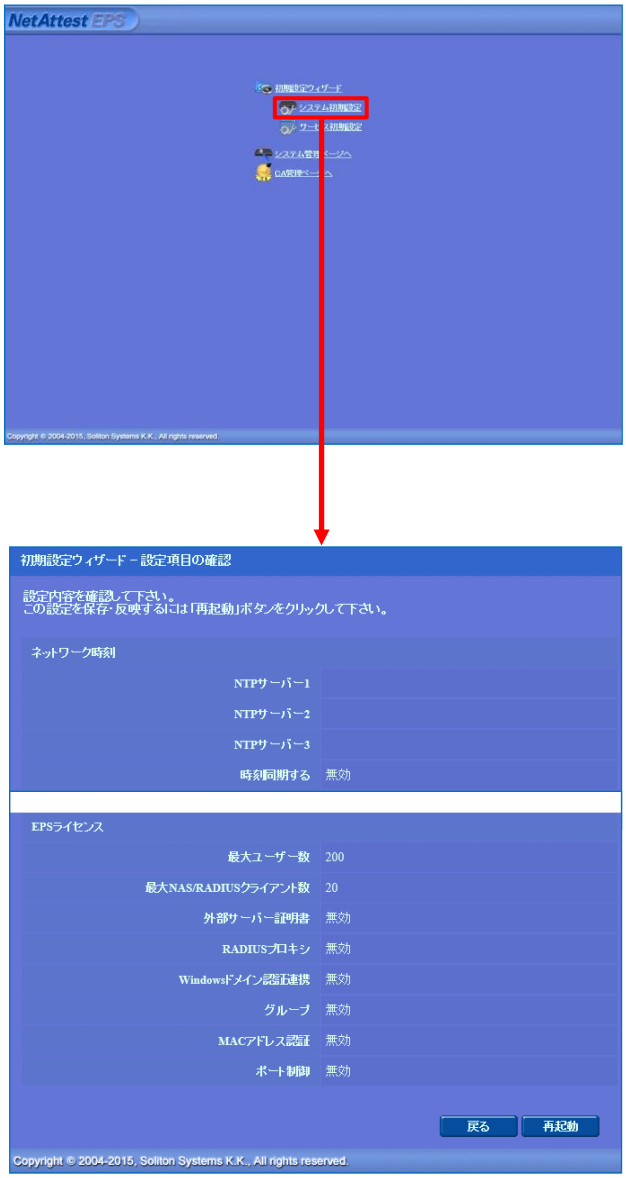
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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
- ドメインネームサーバーの設定



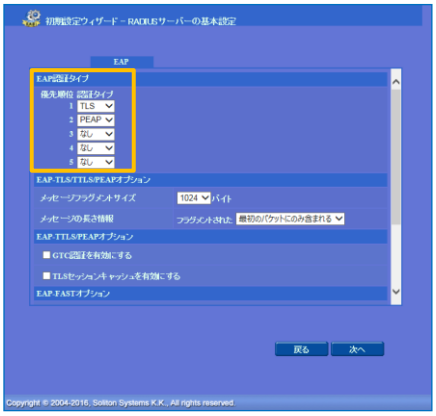
項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

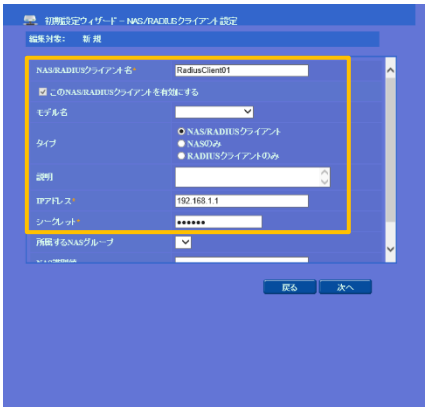
サービス初期設定ウィザードを実行します。

- 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

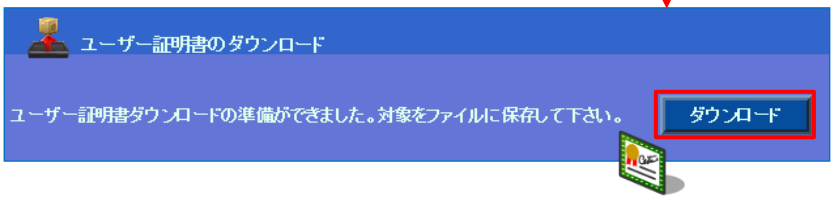
NetAttest EPS の管理画面より、認証ユーザーの登録を行います。[ユーザー]-[ユーザー一覧]から、「追加」ボタンでユーザー登録を行います。

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_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. WAPM-2133TR の設定

BUFFALO社製無線アクセスポイントWAPM-2133TRおよびWAPM-1266R、WAPM-1266WDPR、WAPS-1266 は同一の方法で設定が可能です。そのため本書では、代表して WAPM-2133TR を使用して設定を行います。

WAPM-2133TR を設定するためには、ネットワーク管理ソフトウェア「WLS-ADT」を利用する方法や管理 WebGUI を利用する方法がありますが、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。

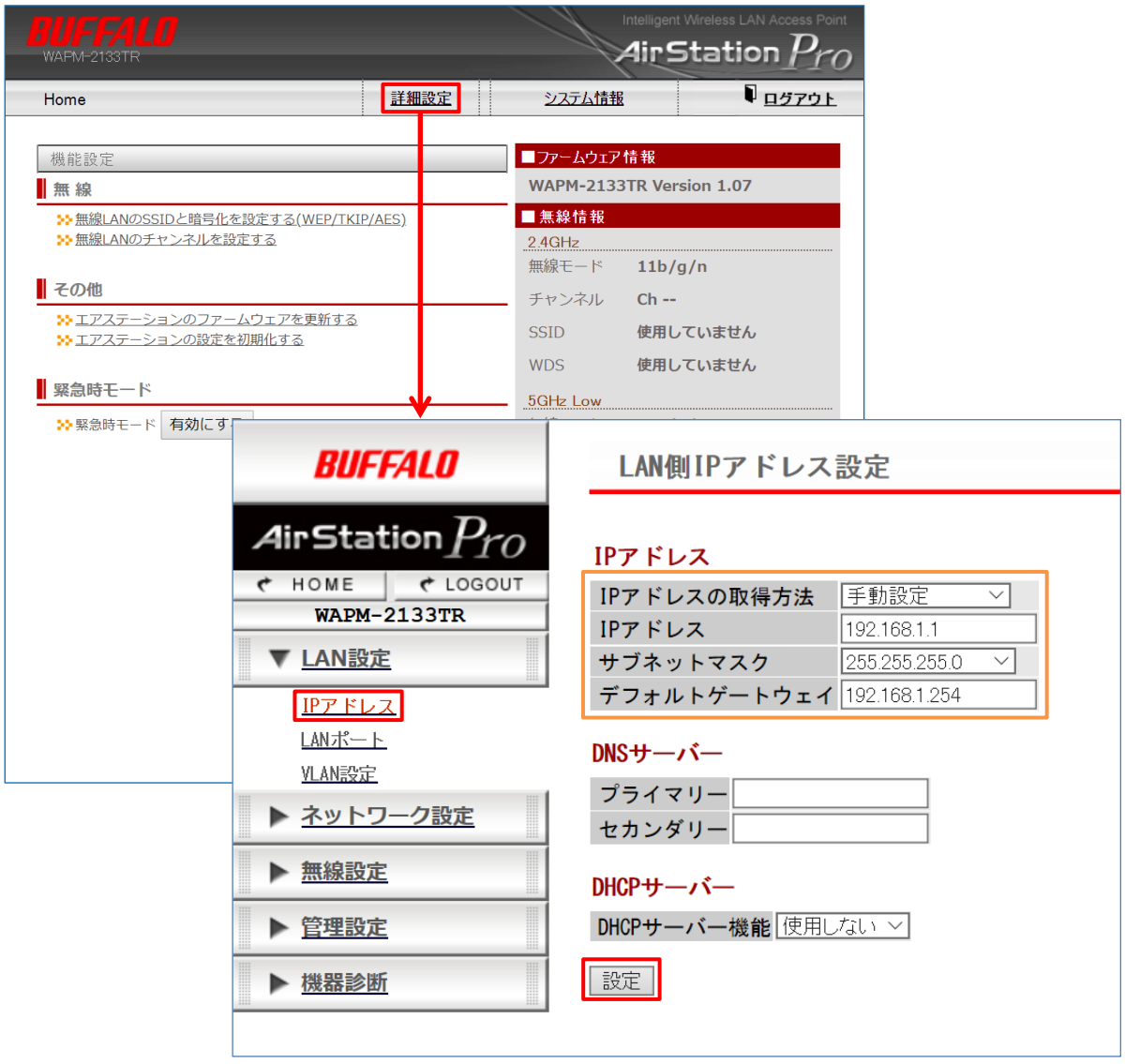
購入時の WAPM-2133TR は、IP アドレスを DHCP サーバーから取得するよう設定されています。DHCP サーバーがない環境に設置する場合、IP アドレスに 192.168.11.100 が割り当てられます。端末に適切な IP アドレスを設定して Web ブラウザより管理画面にアクセスし、設定を開始します。初期のユーザー名/パスワードは admin/password です。

セットアップは下記の流れで行います。

1. IP アドレスの設定
2. RADIUS サーバーの設定
3. 無線の設定

3-1 IP アドレスの設定

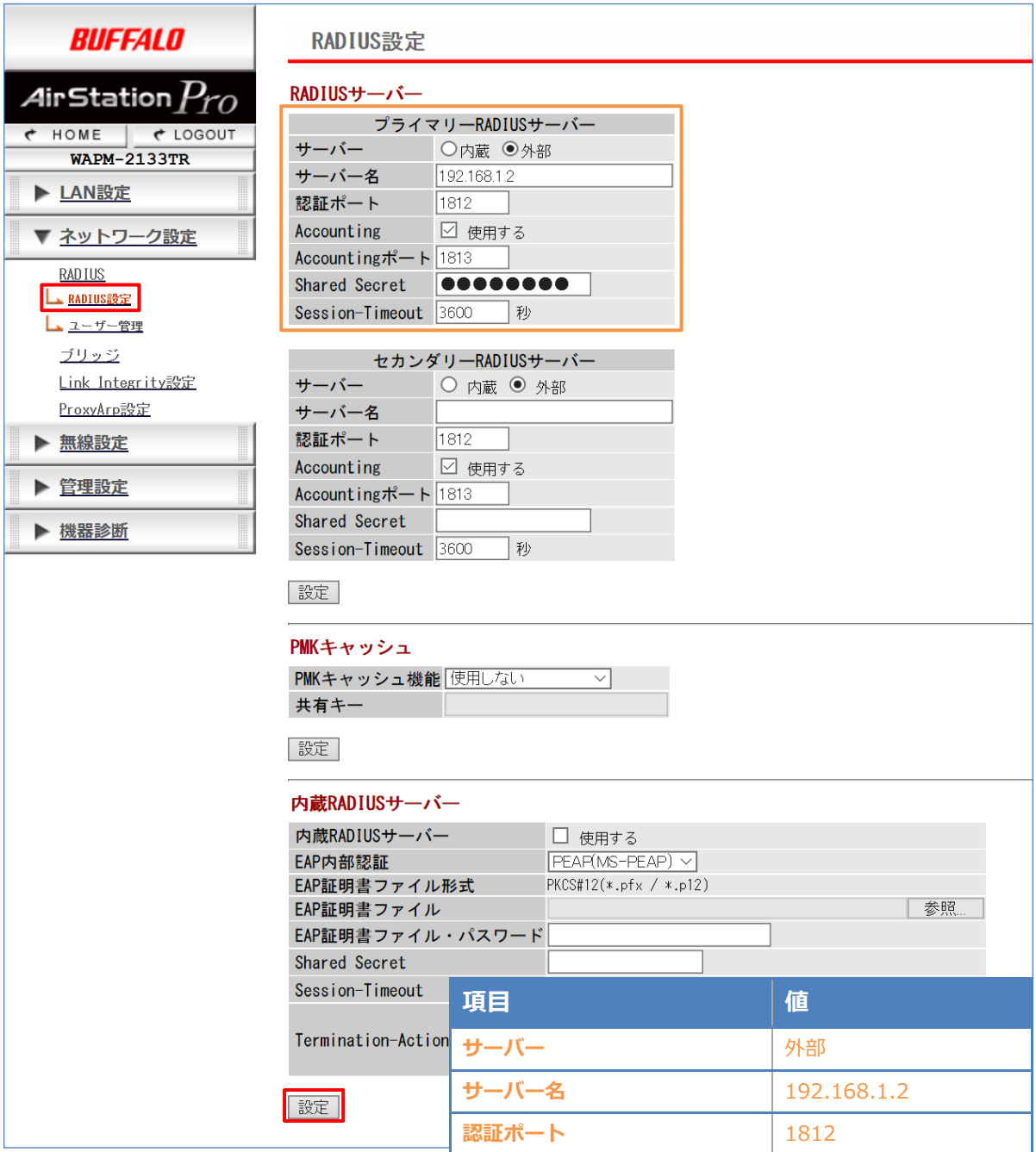
トップページより詳細設定ページに進み IP アドレスの設定を行います。[LAN 設定]-[IP アドレス]をクリックし、表示される「LAN 側 IP 設定」にて IP アドレスを指定します。



項目	値
IP アドレスの取得方法	手動設定
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

3-2 RADIUS サーバーの設定

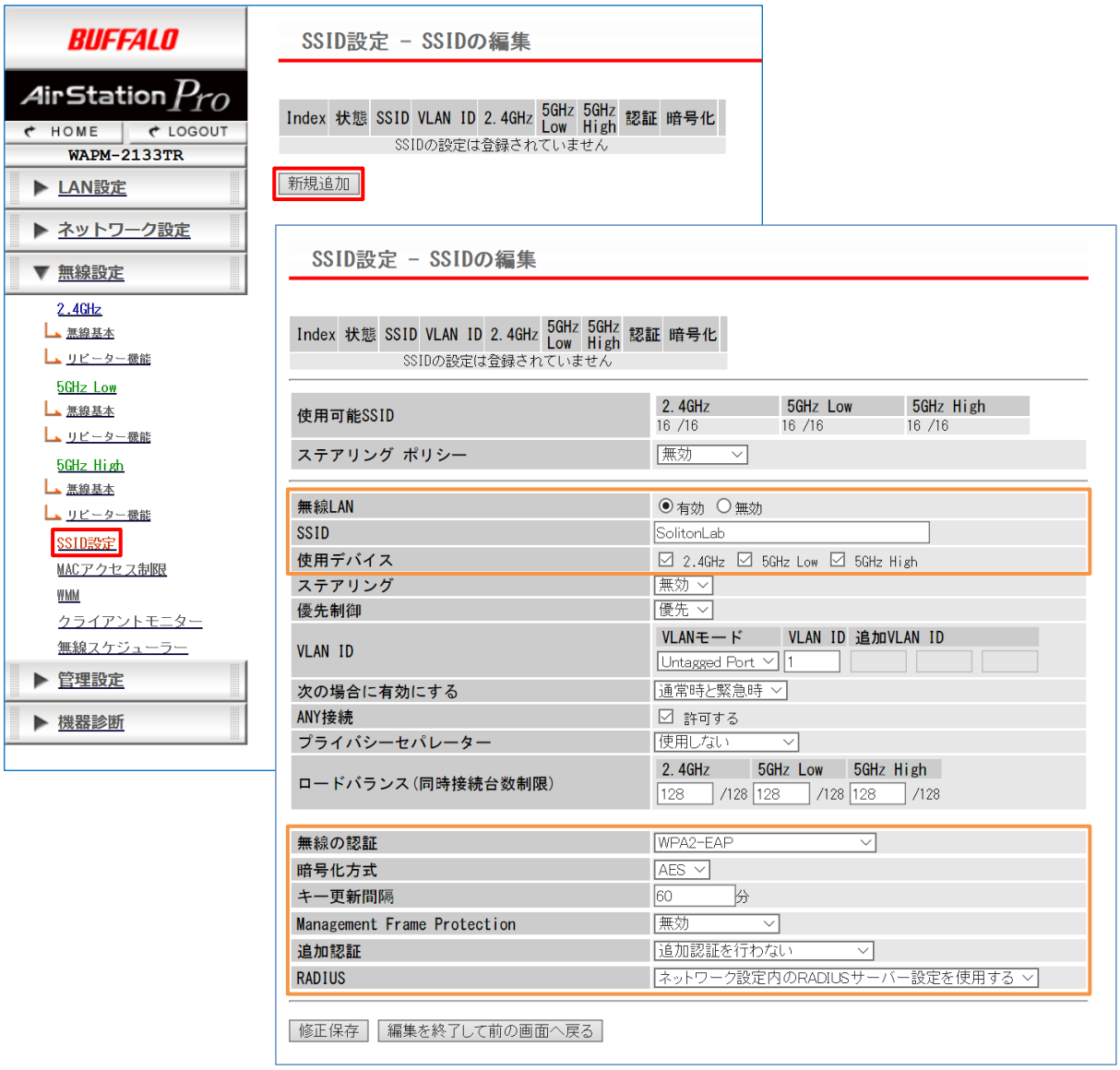
RADIUS サーバーの設定を行います。[ネットワーク設定]-[RADIUS]-[RADIUS 設定]にてプライマリーRADIUS サーバーを指定します。



項目	値
サーバー	外部
サーバー名	192.168.1.2
認証ポート	1812
Accounting	使用する
Accounting ポート	1813
Shared Secret	secret
Session-Timeout	3600 秒

3-3 無線の設定

クライアント端末が接続する SSID の設定を行います。[無線設定]-[SSID 設定]を開き、「新規追加」より設定を行います。



項目	値
無線 LAN	有効
SSID	SolitonLab
使用デバイス	2.4GHz, 5GHz Low, 5GHz High

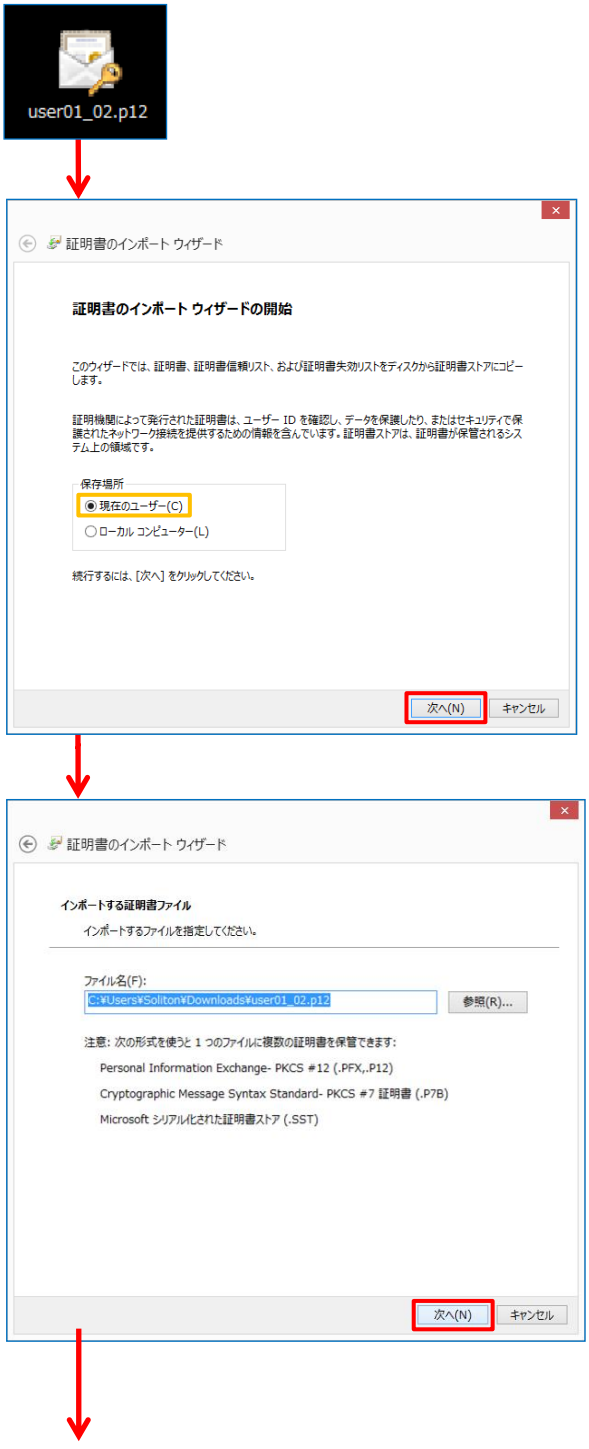
項目	値
無線の認証	WPA2-EAP
RADIUS	ネットワーク設定内の・・・

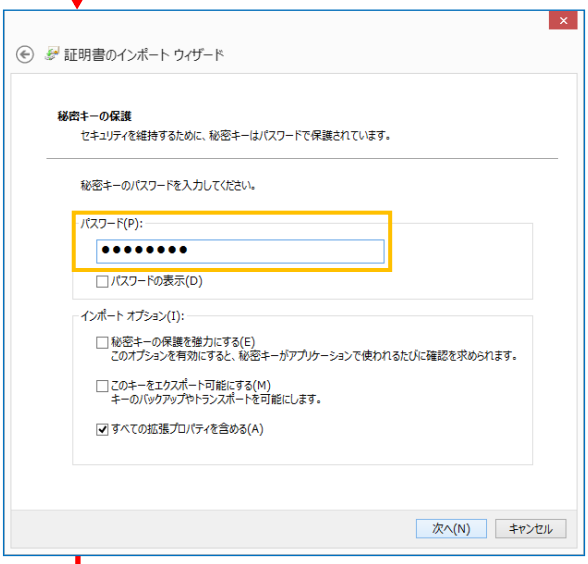
4. EAP-TLS 認証でのクライアント設定

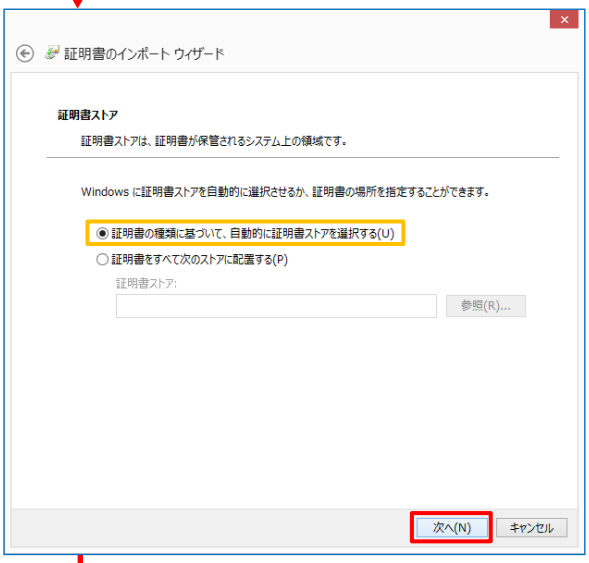
4-1 Windows 10 での EAP-TLS 認証

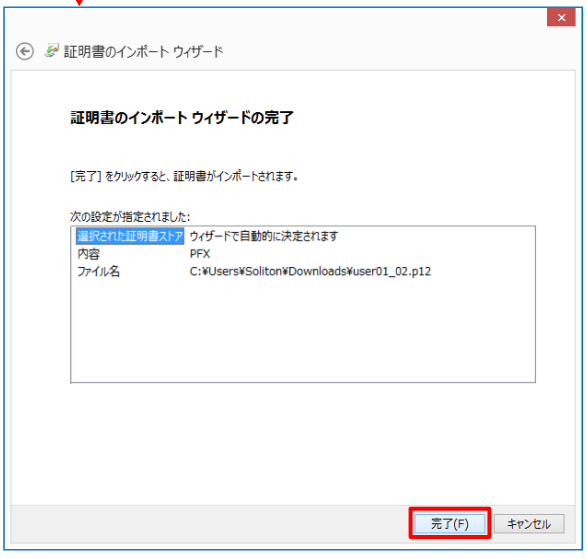
4-1-1 クライアント証明書のインポート

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_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

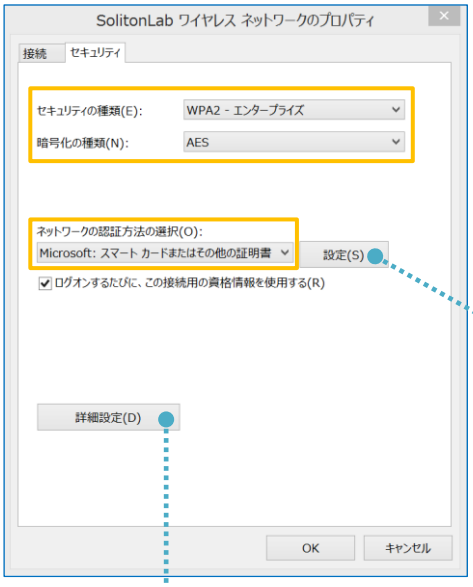
設定したパスワードを入力

4-1-2 サプリカント設定

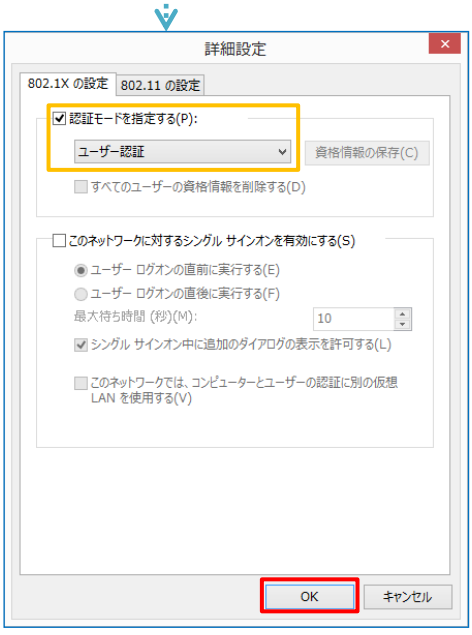
Windows 標準サプリカントで TLS の設定を行います。

※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 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。

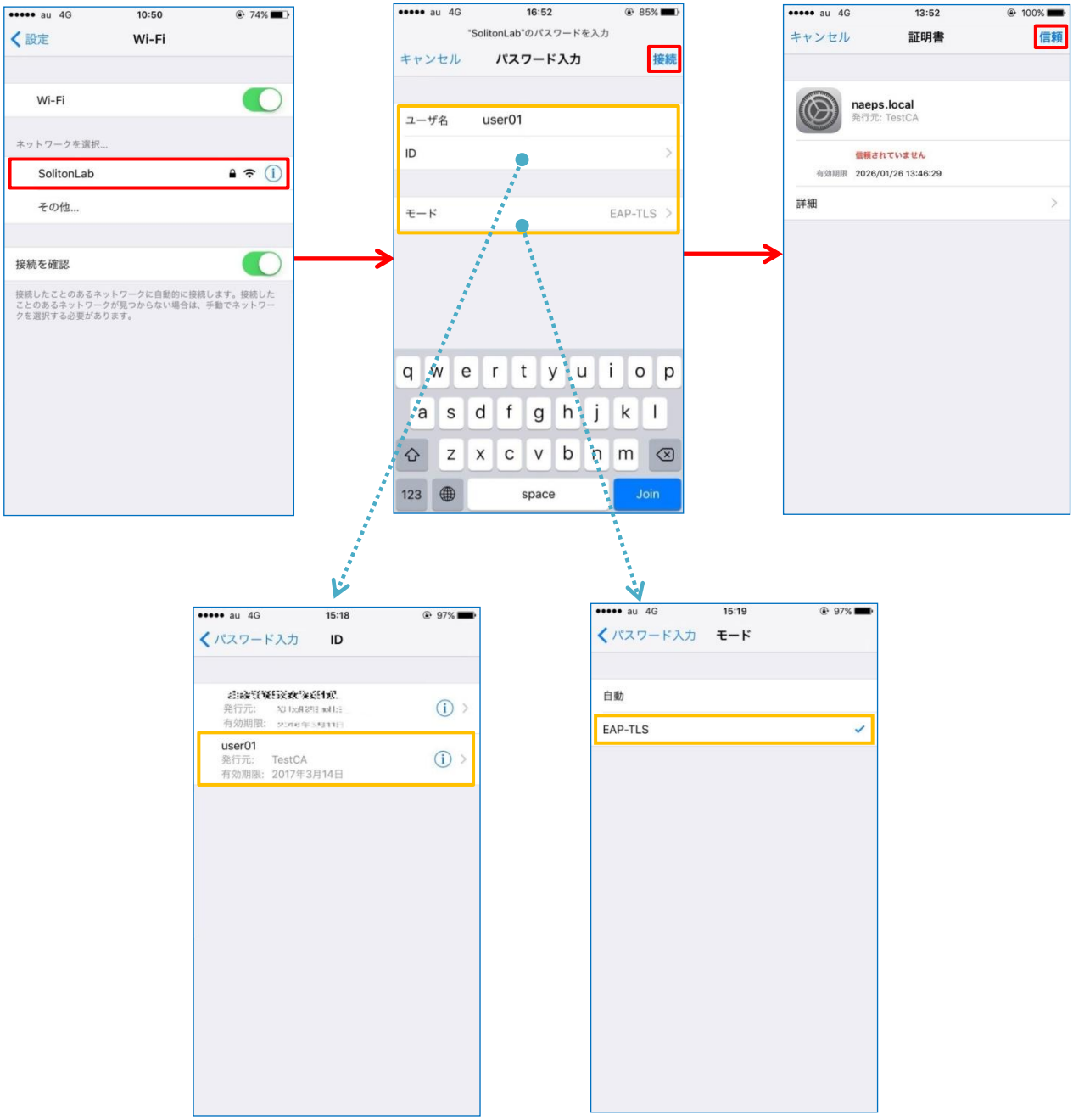
4-2-2 サプリカント設定

WAPM-2133TR 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

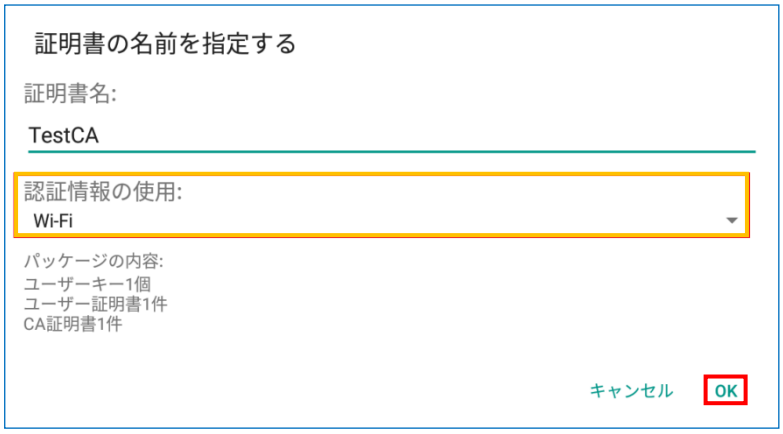
4-3-1 クライアント証明書のインポート

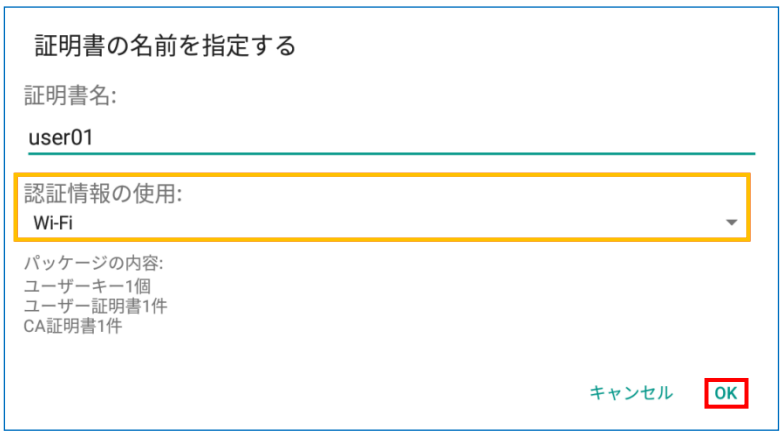
NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

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。



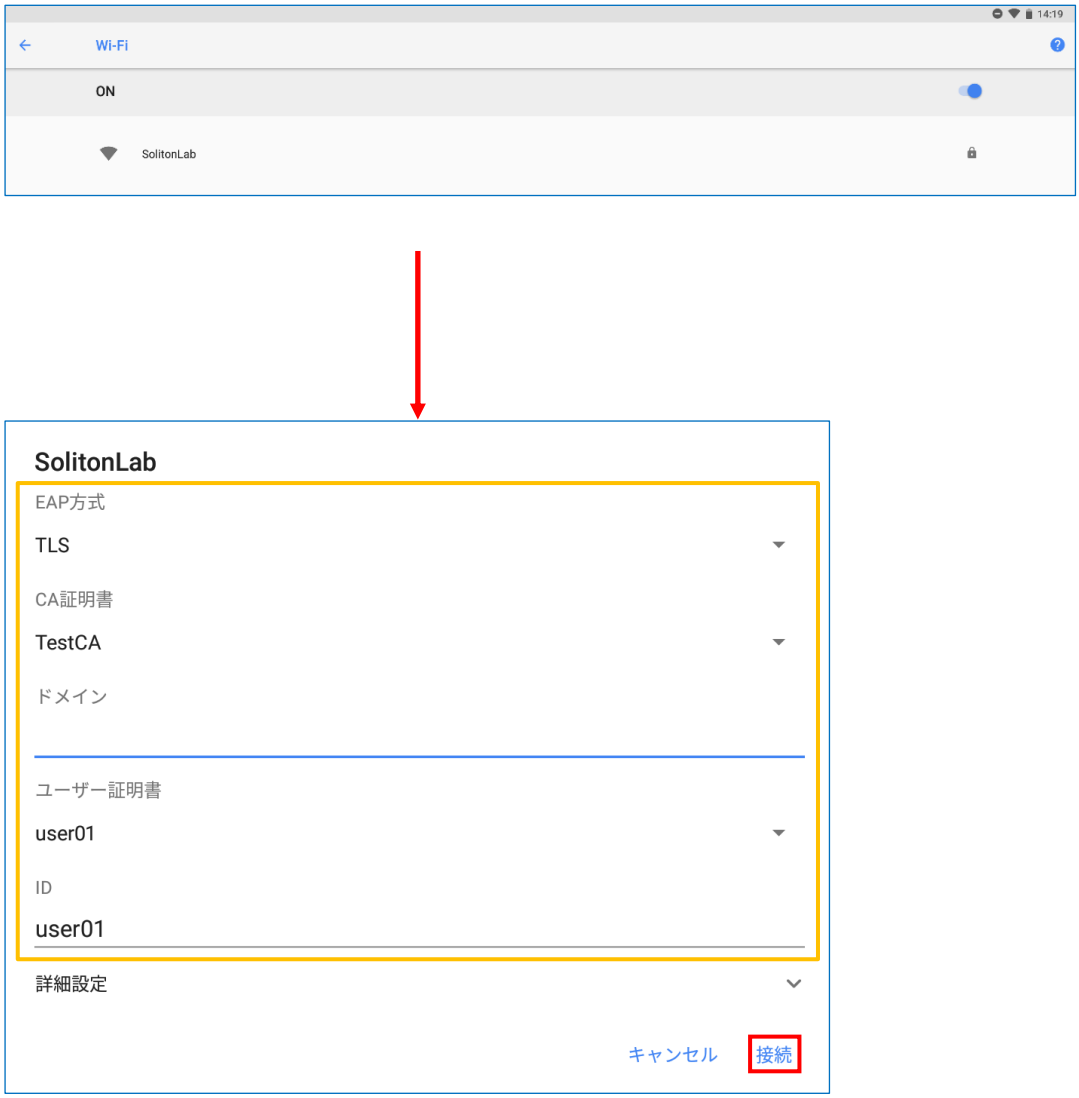


4-3-2 サプリカント設定

WAPM-2133TR 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。



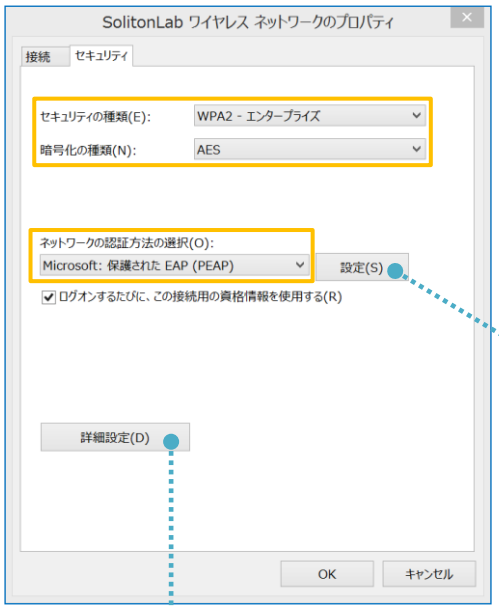
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

5. EAP-PEAP 認証でのクライアント設定

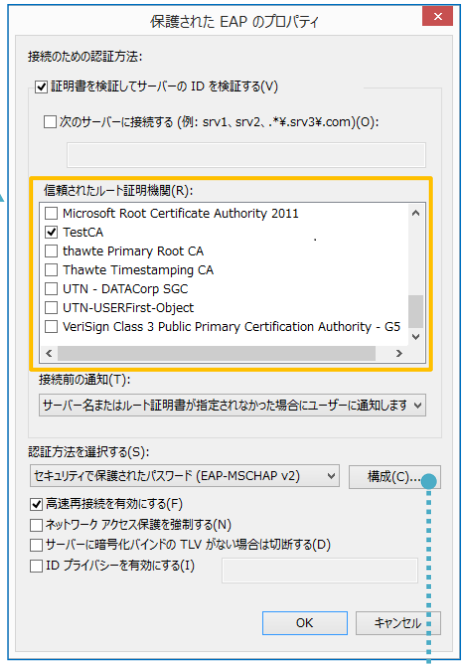
5-1 Windows 10 での EAP-PEAP 認証

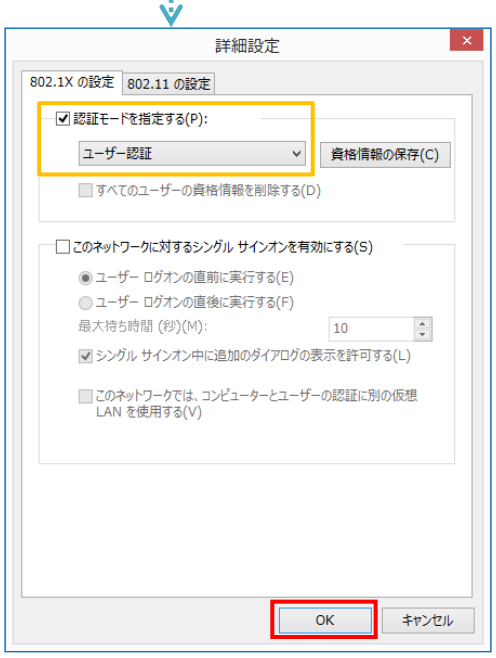
5-1-1 Windows 10 のサプリカント設定

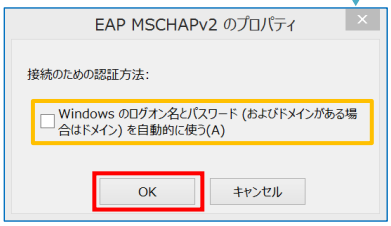
[ワイヤレスネットワークのプロパティ] の「セキュリティ」タブから以下の設定を行います。



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

WAPM-2133TR 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。

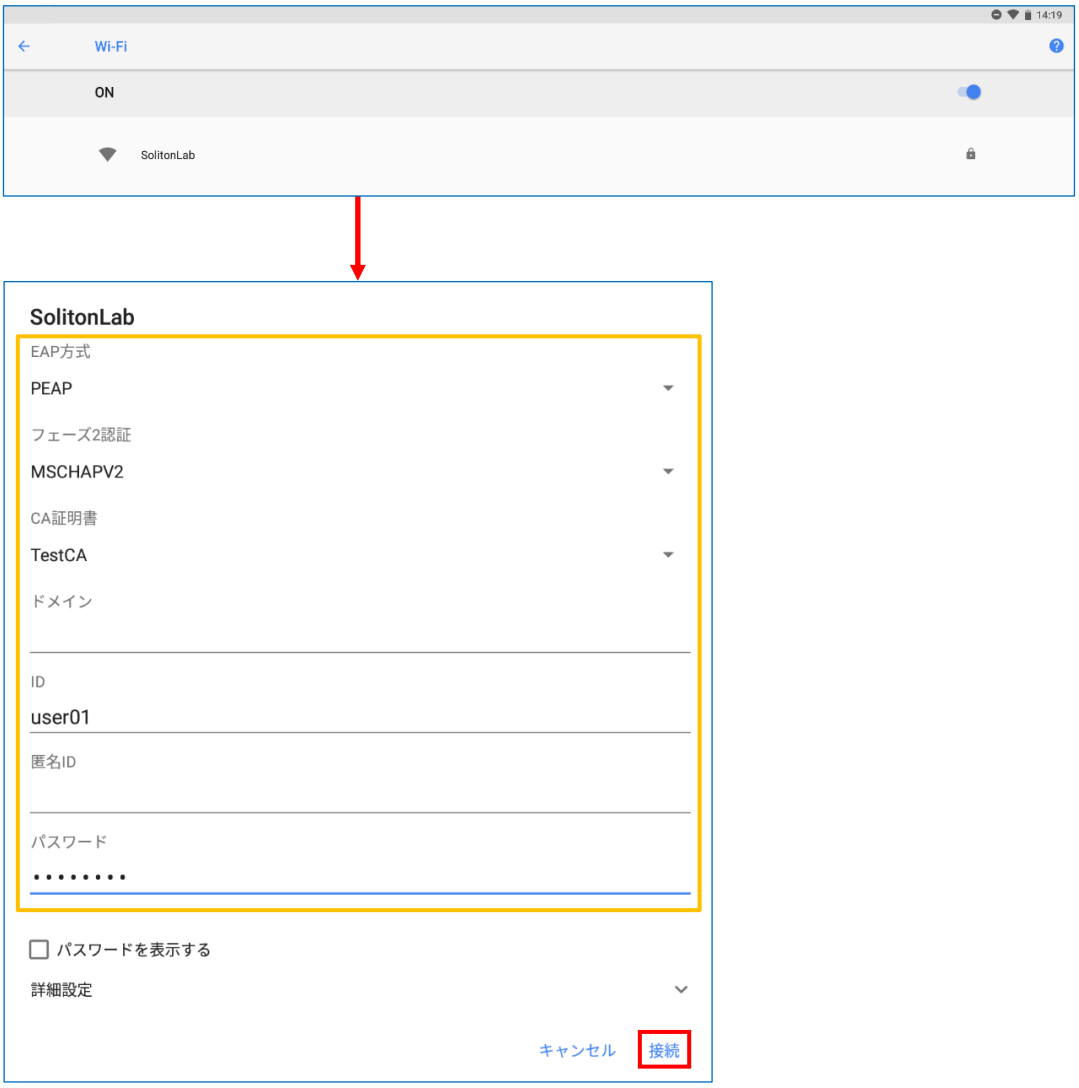
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。

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

WAPM-2133TR 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

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	notice 2018/03/28 17:04:07 Login OK: [user01] (from client RadiusClient01 port 0 cli 11223344566)
WAPM-2133TR	2018/03/28 17:04:07 AUTH wl2.0 (5GHz High): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 11:22:33:44:55:66

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	notice 2018/03/28 16:58:40 Login OK: [user01] (from client RadiusClient01 port 0 cli 11223344566 via proxy to virtual server) notice 2018/03/28 16:58:40 Login OK: [user01] (from client RadiusClient01 port 0 cli 11223344566)
WAPM-2133TR	2018/03/28 16:58:40 AUTH wl0.0 (5GHz Low): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 11:22:33:44:55:66

改訂履歴

日付	版	改訂内容
2018/04/04	1.0	初版作成
2019/03/20	2.0	ロゴ画像差し替え