NetAttest EPS
認証連携設定例

【連携機器】アイ・オー・データ機器 WHG-AC1750A シリーズ

【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、アイ・オー・データ機器社製無線アクセスポイント WHG-AC1750A 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 WHG-AC1750A 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。

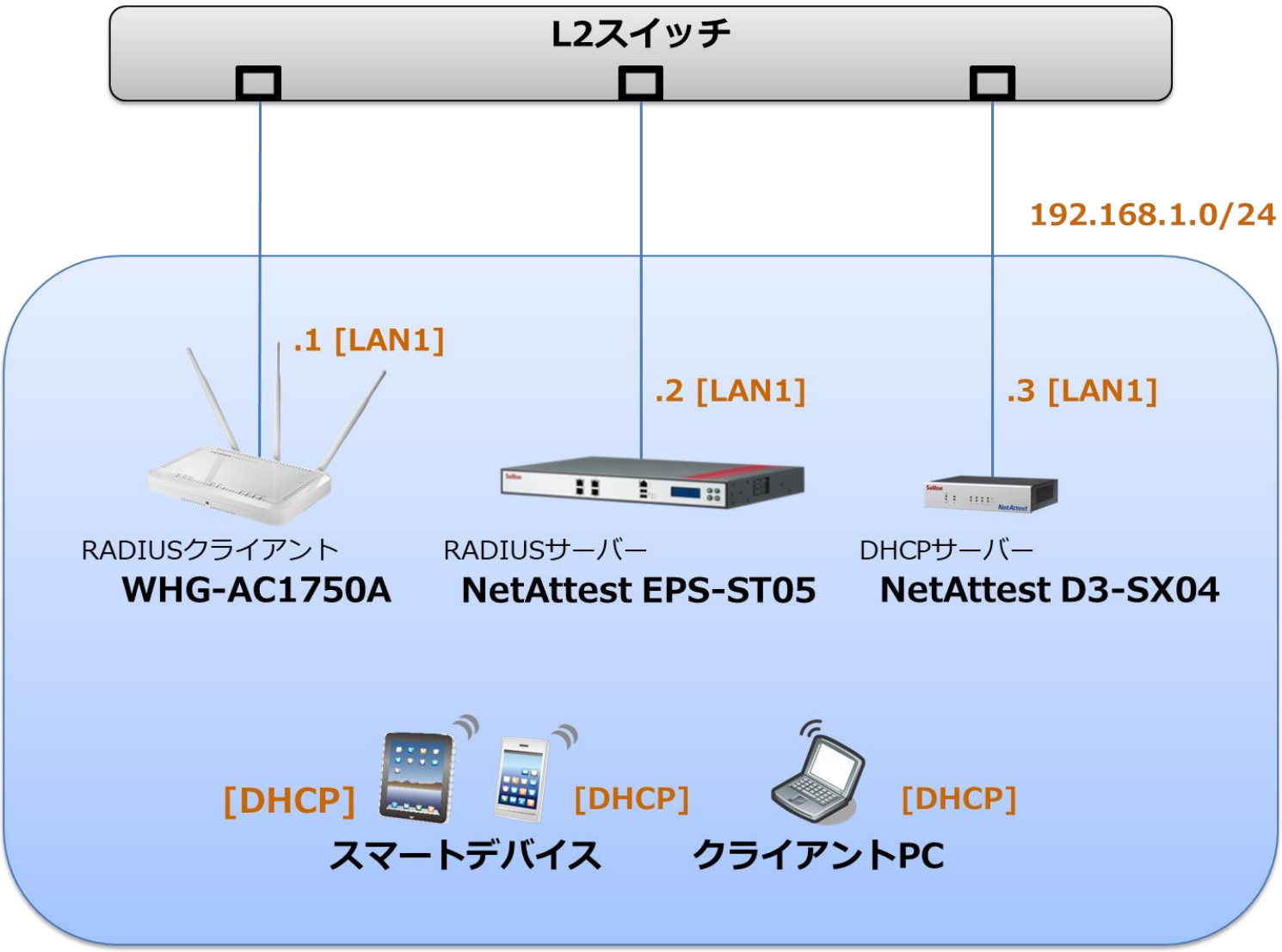
目次

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	4.10.3
WHG-AC1750A	アイ・オー・データ機器	RADIUS クライアント (無線アクセスポイント)	3.02
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
iPhone 7	Apple	802.1X クライアント (Client SmartPhone)	12.0
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	4.2.16

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
WHG-AC1750A	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。

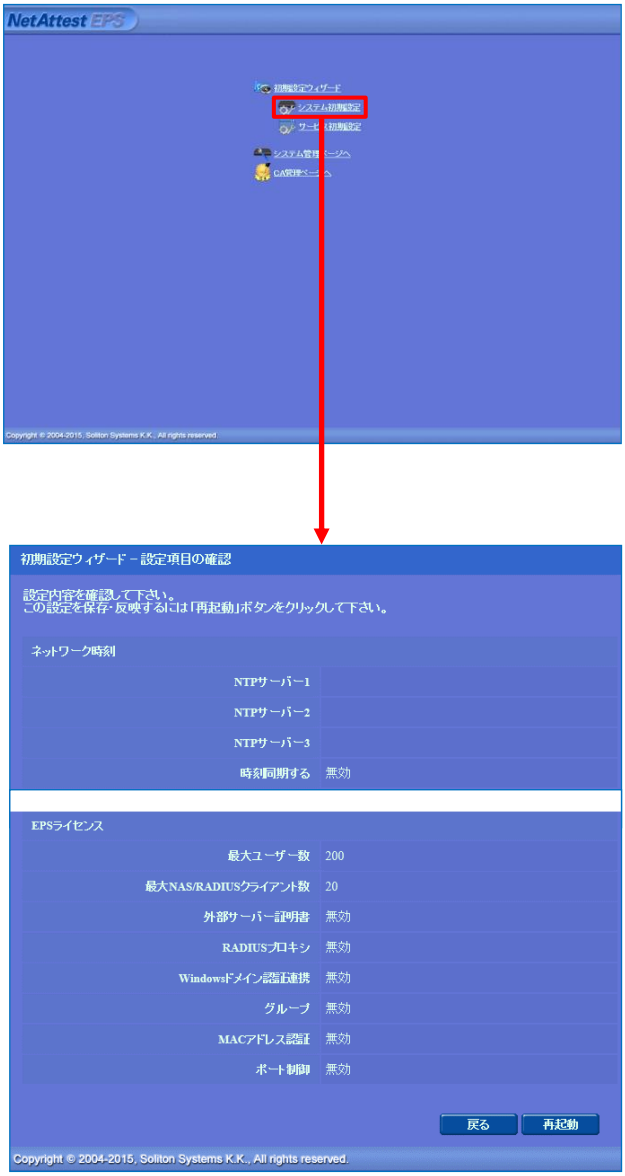
下記のような流れでセットアップを行います。

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

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



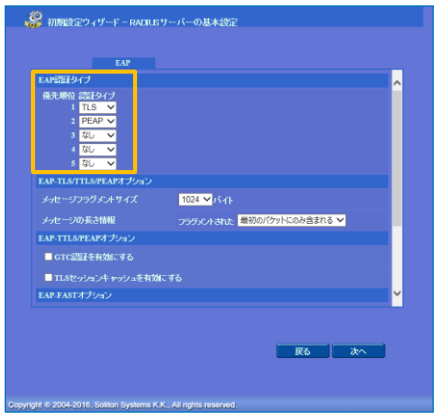
項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

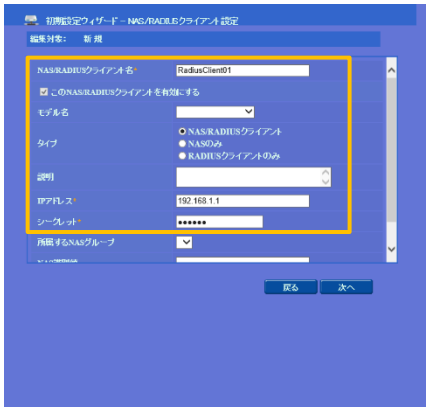
サービス初期設定ウィザードを実行します。

- 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. WHG-AC1750A シリーズの設定

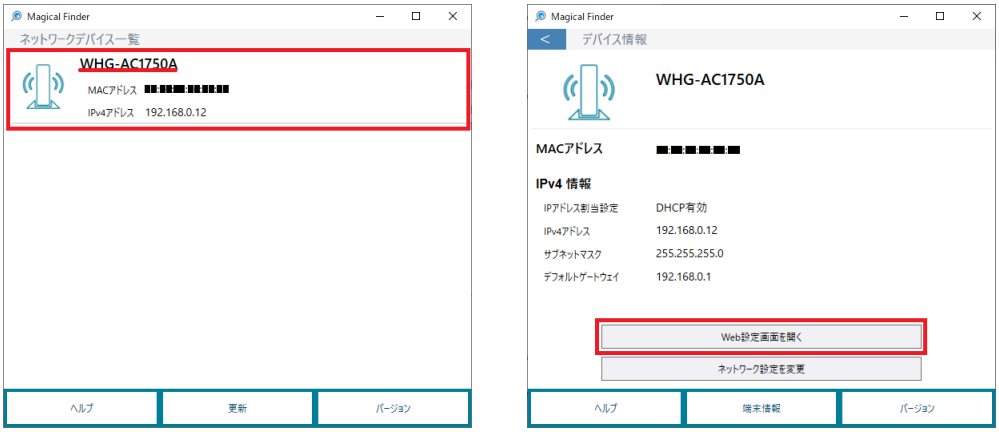
アイ・オー・データ機器の無線アクセスポイント、WHG-AC1750A シリーズ（WHG-AC1750A、WHG-AC1750A-E)の設定を行います。WHG-AC1750A シリーズの設定は WebGUI を利用します。本書では代表して WHG-AC1750A での設定を記載します。購入時の IP アドレスは DHCP 設定となっていますので、専用ツール「Magical Finder」を使い設定を行います。

「Magical Finder」は下記 Web ページにアクセスし、お使いの OS を選んでダウンロードします。

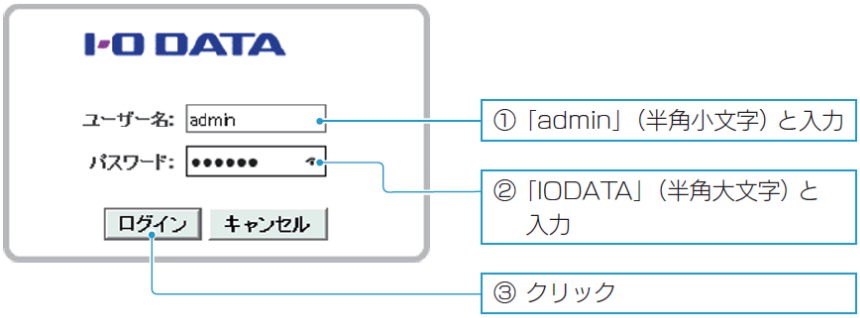
http://www.iodata.jp/r/3022

Magical Finder を起動すると、下記のように対象製品が表示されます。

設定を行う機器を選択し、「Web 設定画面を開く」をクリックし設定画面を起動します。



設定画面が起動したら、ユーザー名/パスワードを入力しログインします。

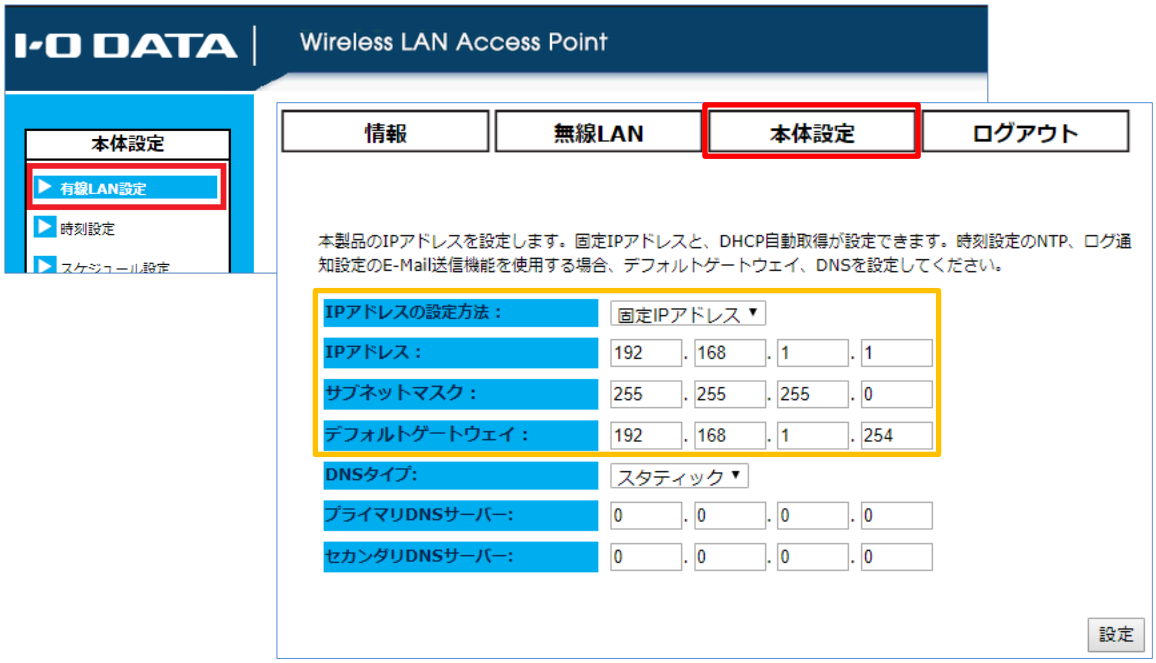


WHG-AC1750Aのセットアップは下記の流れで行います。

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

3-1 IP アドレスの設定

設定画面を開いたら、画面上部の[本体設定]→画面左の[有線 LAN 設定]をクリックし、WHG-AC1750A の IP アドレス設定画面を開きます。



項目	値
IP アドレスの設定方法	固定 IP アドレス
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

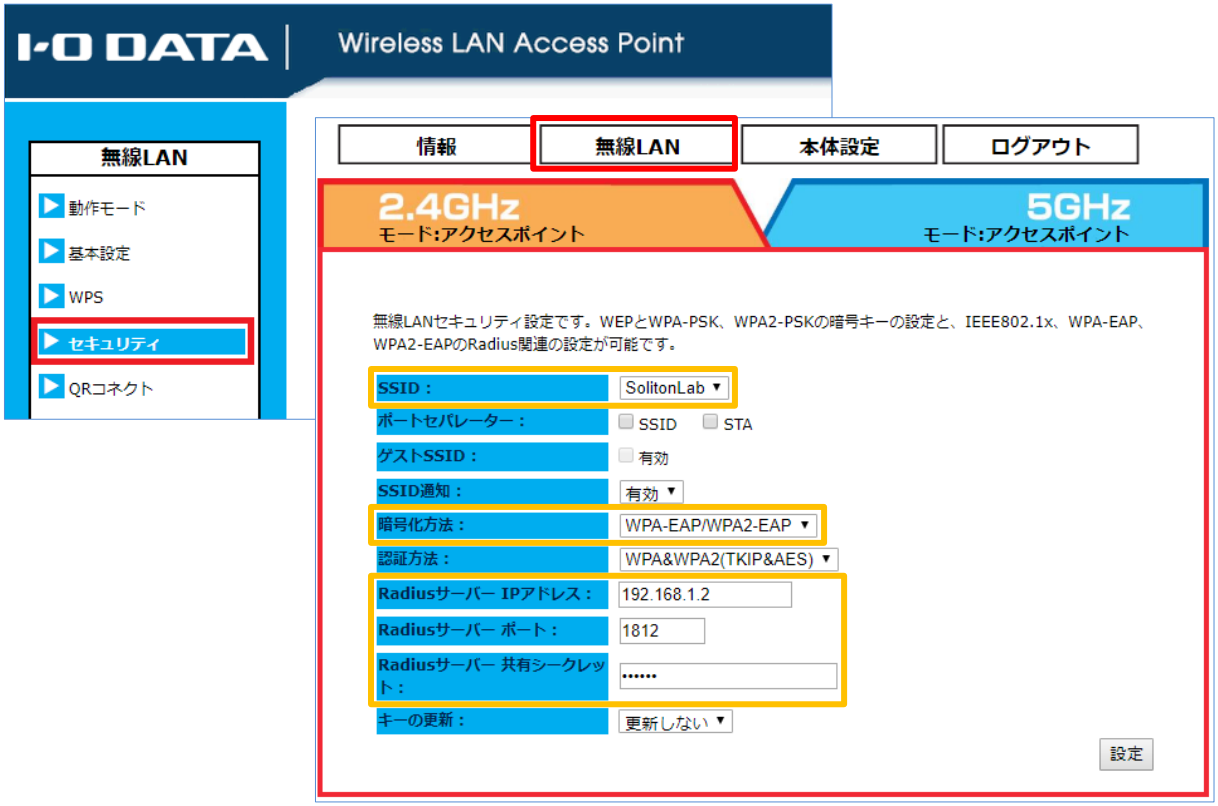
3-2 無線の設定

WHG-AC1750A に無線 LAN の SSID 情報を設定します。設定画面より[無線 LAN]-[基本設定]を選択し、基本設定画面から無線と SSID の設定を行います。無線の周波数帯(2.4GHz モード/5GHz モード)は、ご利用の端末環境に応じて選択してください。

項目	値
無線機能	有効
SSID1	SolitonLab

3-3 RADIUS サーバーの設定

WHG-AC1750A に認証サーバーの情報を設定します。設定画面より[無線 LAN]-[セキュリティ]を選択し、無線 LAN セキュリティの設定を行います。



項目	値
SSID	SolitonLab
暗号化方法	WPA-EAP/WPA2-EAP
Radius サーバーIP アドレス	192.168.1.2
Radius サーバーポート	1812
Radius サーバー共有シークレット	secret

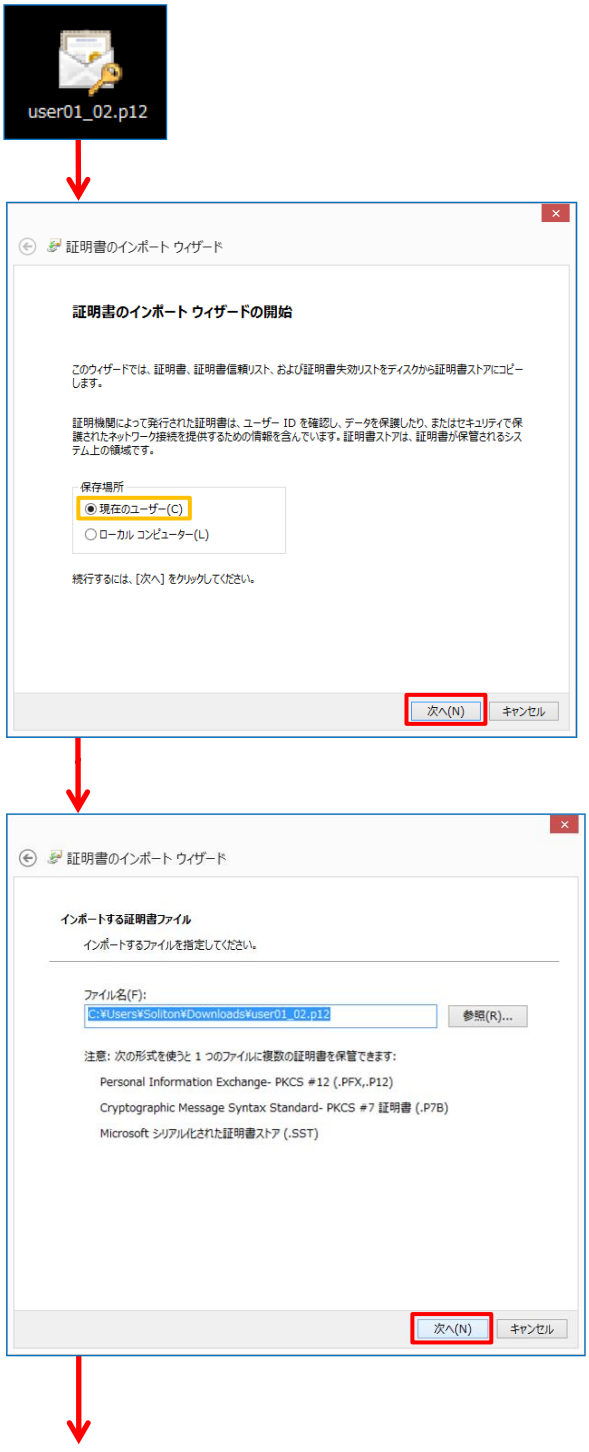
以上で WHG-AC1750A の設定は完了です。

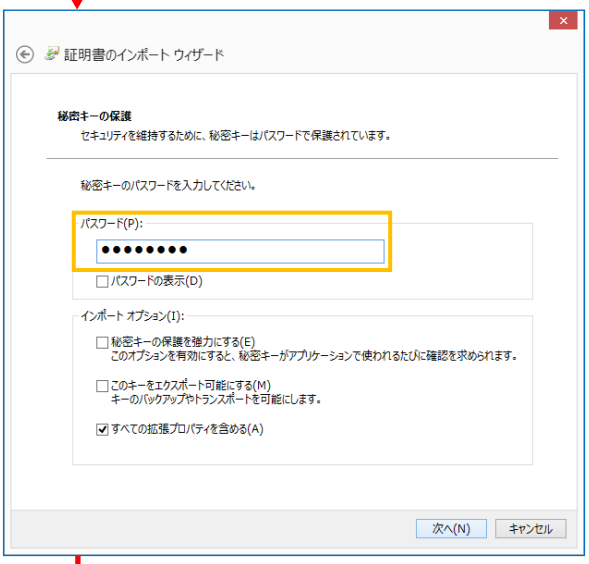
4. EAP-TLS 認証でのクライアント設定

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

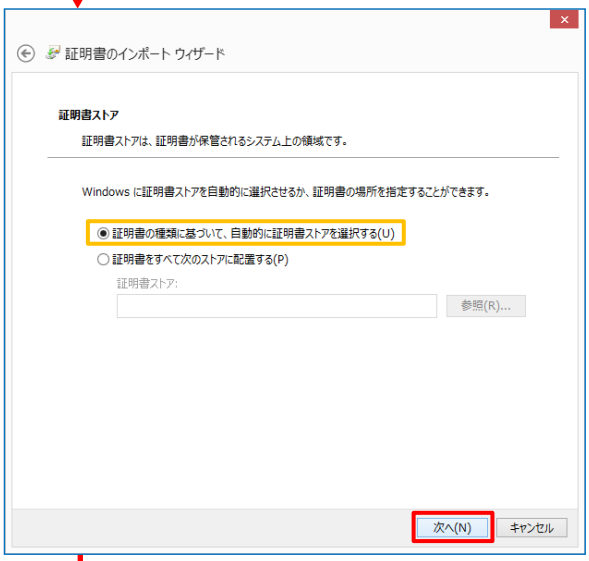
PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書(user01_02.p12)をダブルクリックすると、証明書インポートウィザードが実行されます。

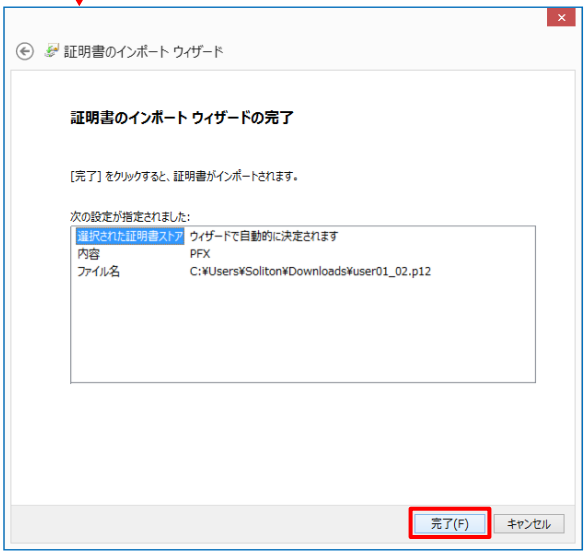




【パスワード】

「2-4 ユーザーの登録」で設定したパスワードを入力

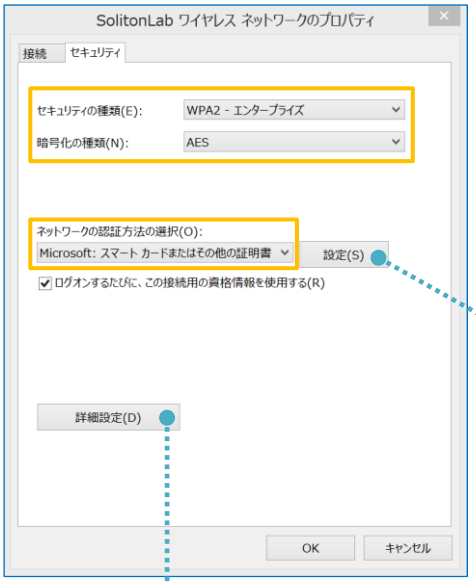




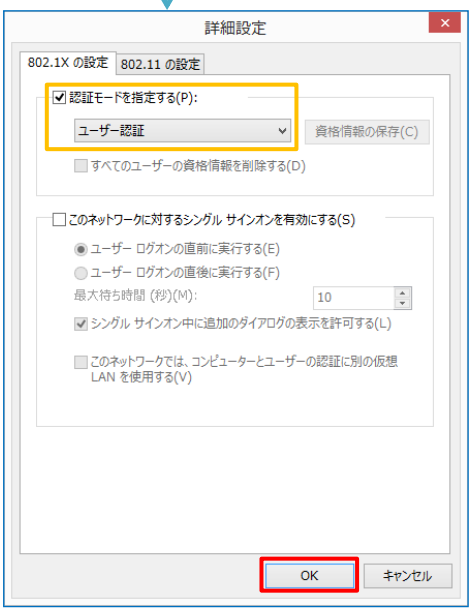
4-1-2 サプリカント設定

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)

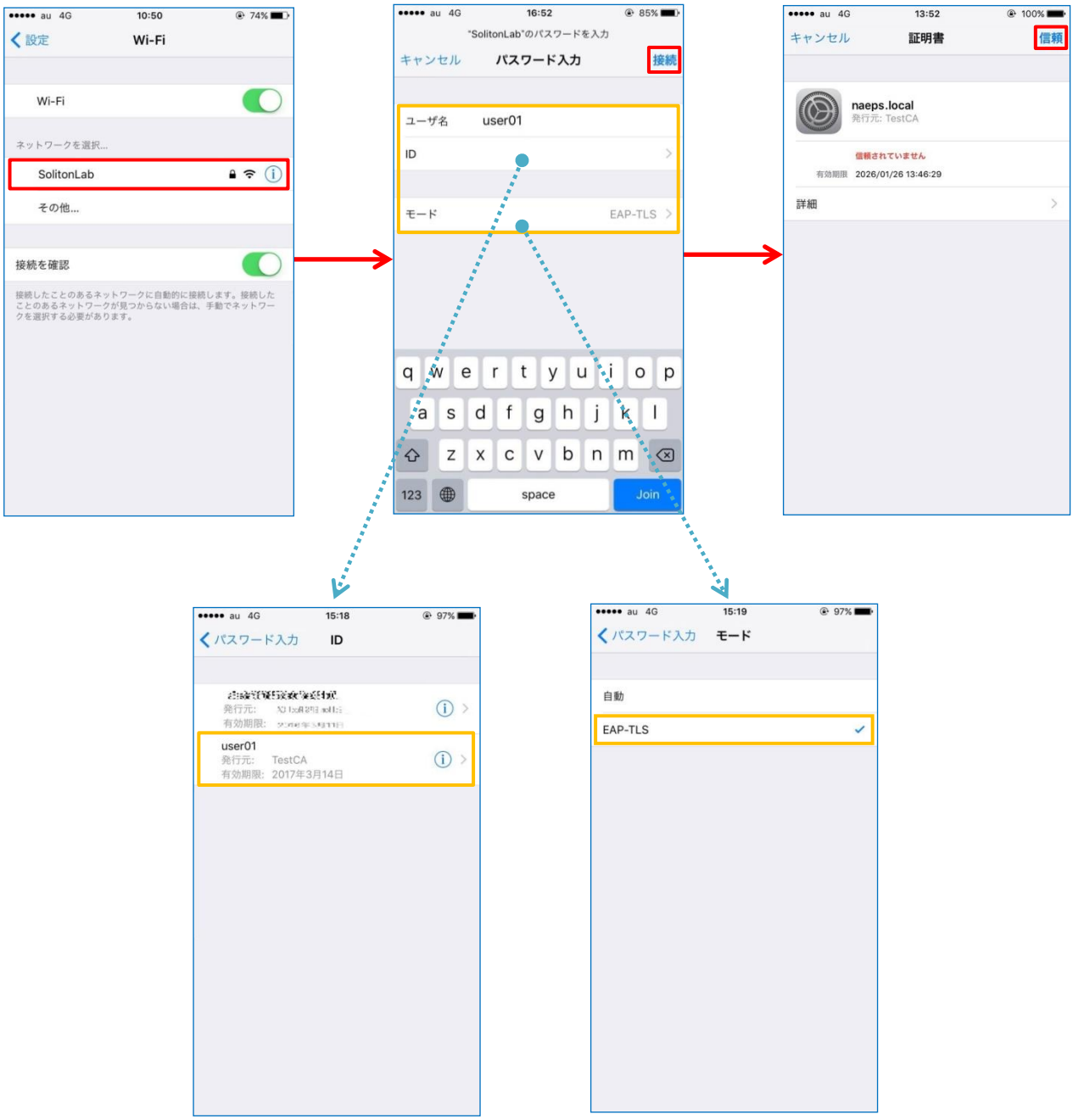
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

WHG-AC1750A 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

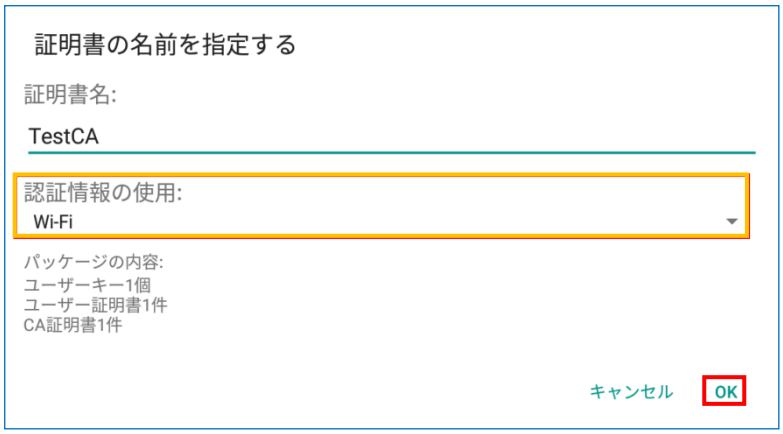
4-3-1 クライアント証明書のインポート

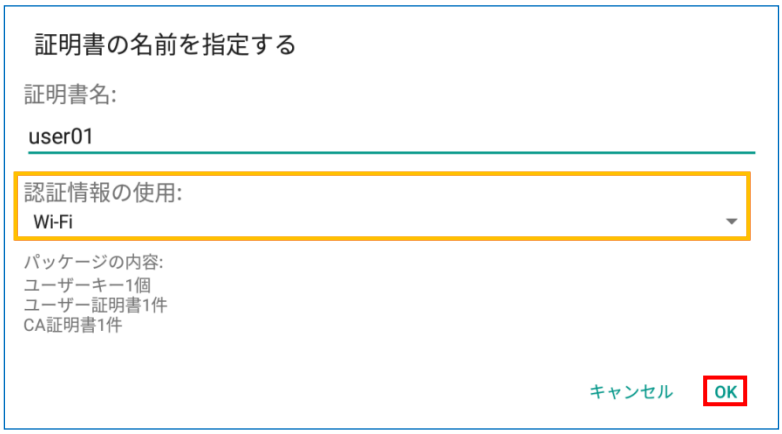
NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

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。

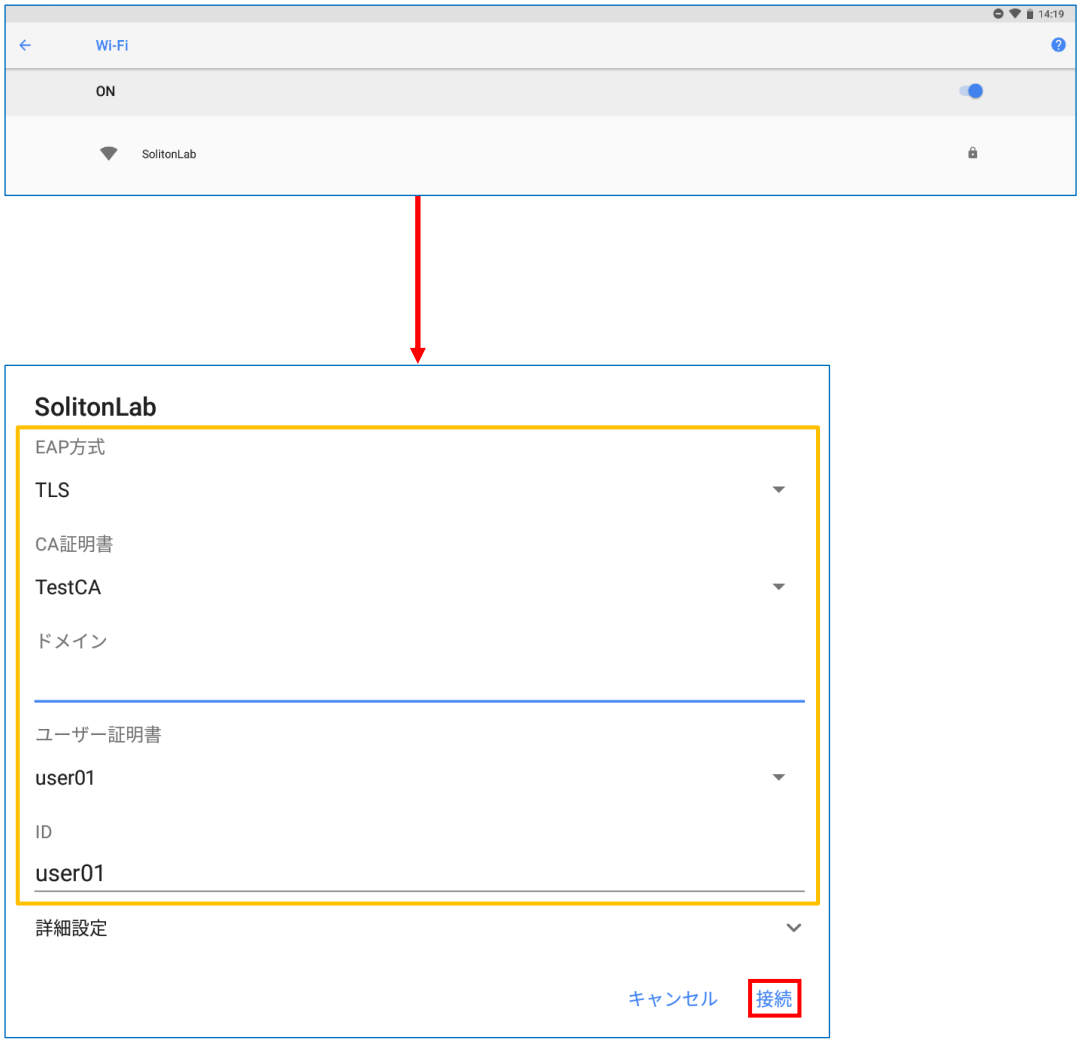




4-3-2 サプリカント設定

WHG-AC1750A 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。



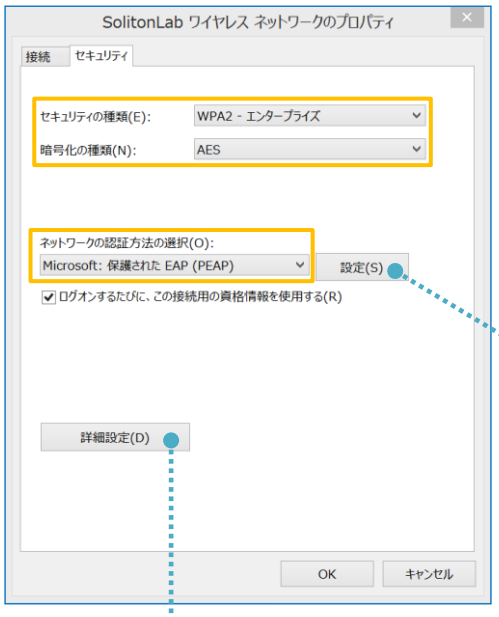
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

5. EAP-PEAP 認証でのクライアント設定

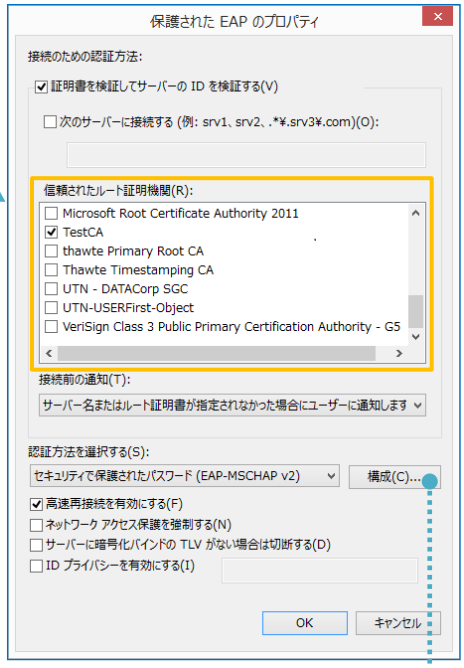
5-1 Windows 10 での EAP-PEAP 認証

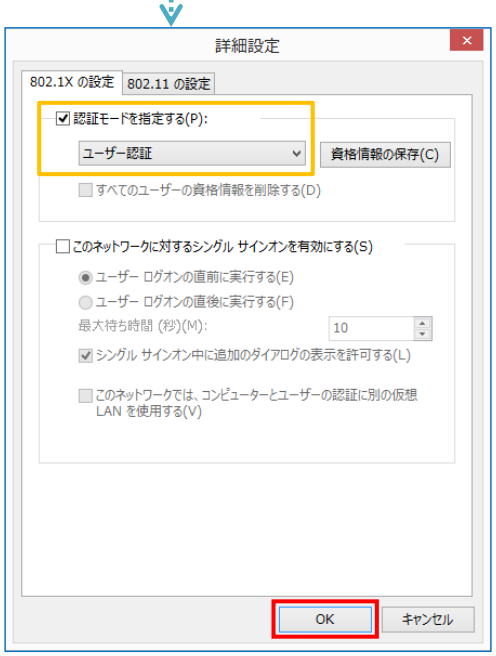
5-1-1 Windows 10 のサプリカント設定

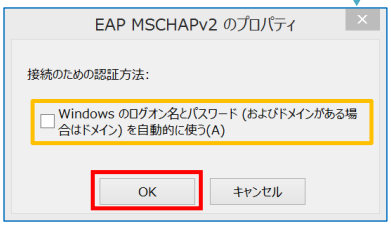
[ワイヤレスネットワークのプロパティ] の「セキュリティ」タブから以下の設定を行います。



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

WHG-AC1750A 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。

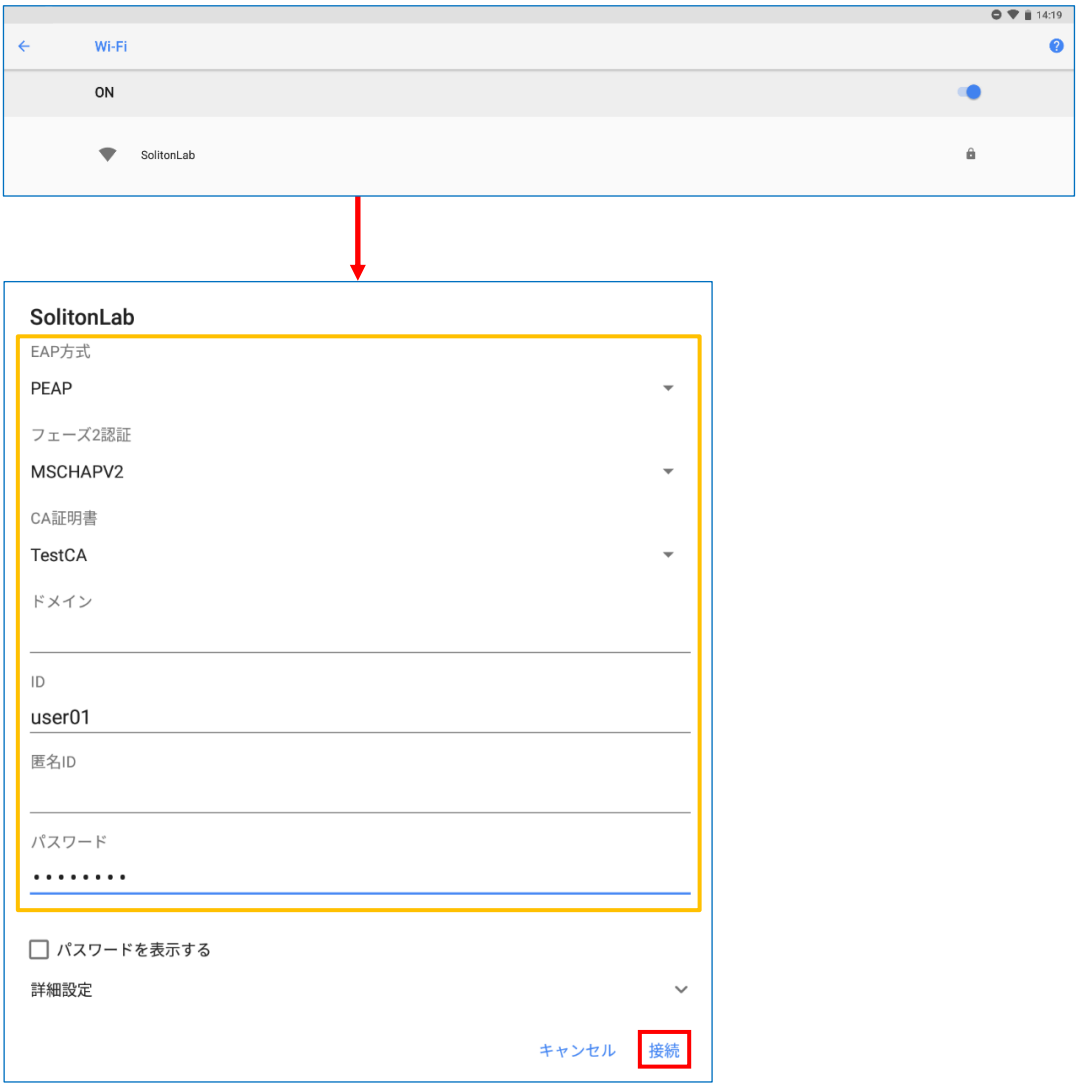
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。

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

WHG-AC1750A 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	Login OK: [user01] (from client RadiusClient01 port 1 cli 40:A3:CC:32:10:A4)
WHG-AC1750A	[SYSTEM]: Station [40:a3:cc:32:10:a4] WPA/WPA2 authentication successful [SYSTEM]: Station [40:a3:cc:32:10:a4] start authentication [SYSTEM]: Station [40:a3:cc:32:10:a4] Encryption Information WPA2-EAP(AES) [SYSTEM]: Station [40:a3:cc:32:10:a4] associated to [34:76:c5:50:65:83]

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 1 cli 40:A3:CC:32:10:A4 via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 1 cli 40:A3:CC:32:10:A4)
WHG-AC1750A	[SYSTEM]: Station [40:a3:cc:32:10:a4] WPA/WPA2 authentication successful [SYSTEM]: Station [40:a3:cc:32:10:a4] start authentication [SYSTEM]: Station [40:a3:cc:32:10:a4] Encryption Information WPA2-EAP(AES) [SYSTEM]: Station [40:a3:cc:32:10:a4] associated to [34:76:c5:50:65:83]

改訂履歴

日付	版	改訂内容
2018/10/31	1.0	初版作成
2019/03/19	2.0	ロゴ画像差し替え