

# **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。

NetAttest は、株式会社ソリトンシステムズの登録商標です。

その他、本書に掲載されている会社名、製品名は、それぞれ各社の商標または登録商標です。  
本文中に ™、®、© は明記していません。

# 目次

1. 構成.....	6
1-1 構成図 .....	6
1-2 環境 .....	7
1-2-1 機器 .....	7
1-2-2 認証方式 .....	7
1-2-3 ネットワーク設定.....	7
2. NetAttest EPS の設定 .....	8
2-1 初期設定ウィザードの実行 .....	8
2-2 システム初期設定ウィザードの実行 .....	9
2-3 サービス初期設定ウィザードの実行 .....	10
2-4 ユーザーの登録.....	11
2-5 クライアント証明書の発行 .....	12
3. WAPM-2133TR の設定 .....	13
3-1 IP アドレスの設定 .....	14
3-2 RADIUS サーバーの設定 .....	15
3-3 無線の設定 .....	16
4. EAP-TLS 認証でのクライアント設定 .....	17
4-1 Windows 10 での EAP-TLS 認証 .....	17
4-1-1 クライアント証明書のインポート.....	17
4-1-2 サプリカント設定.....	19
4-2 iOS での EAP-TLS 認証 .....	20
4-2-1 クライアント証明書のインポート.....	20
4-2-2 サプリカント設定.....	21
4-3 Android での EAP-TLS 認証 .....	22
4-3-1 クライアント証明書のインポート.....	22
4-3-2 サプリカント設定.....	23
5. EAP-PEAP 認証でのクライアント設定 .....	24
5-1 Windows 10 での EAP-PEAP 認証.....	24
5-1-1 Windows 10 のサプリカント設定 .....	24

---

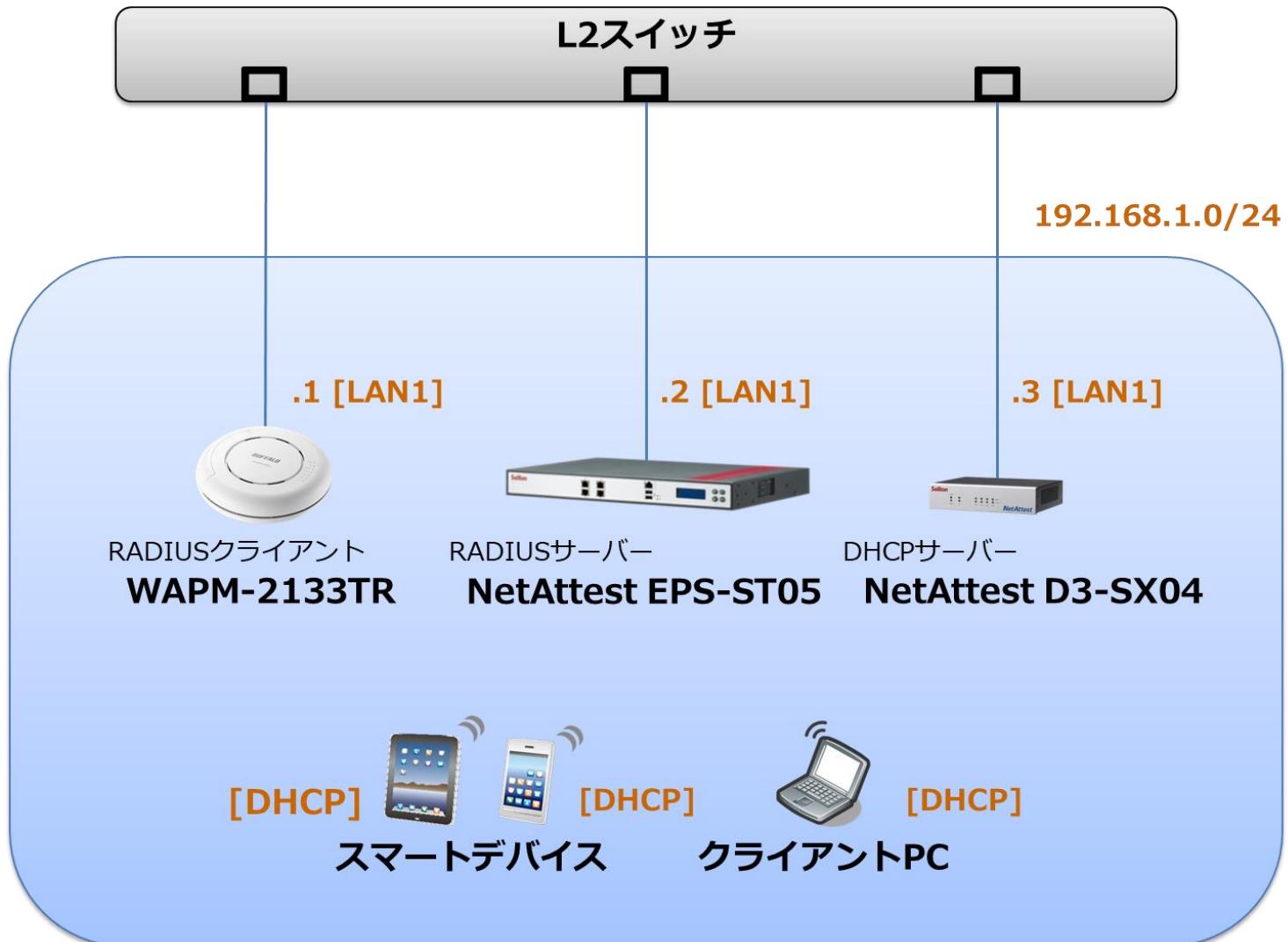
5-2 iOS での EAP-PEAP 認証 .....	25
5-2-1 iOS のサブリカント設定 .....	25
5-3 Android での EAP-PEAP 認証 .....	26
5-3-1 Android のサブリカント設定 .....	26
6. 動作確認結果 .....	27
6-1 EAP-TLS 認証 .....	27
6-2 EAP-PEAP 認証 .....	27

# 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 標準サブリカント
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。

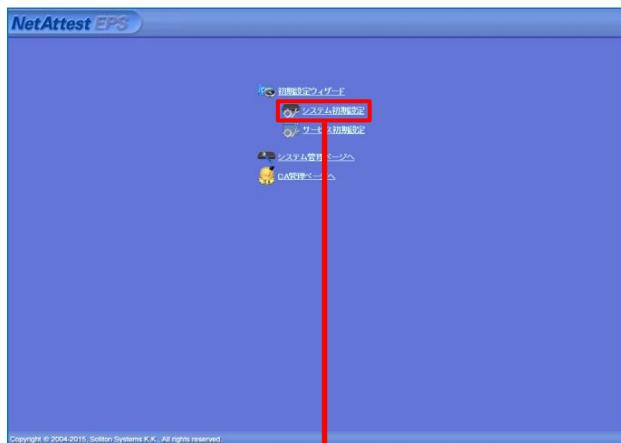
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

## 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



Initial Setup Wizard - Confirmation of settings

Setting contents are confirmed. To save and reflect, click the 'Restart' button.

Network Clock	
NTP Server-1	
NTP Server-2	
NTP Server-3	
Sync Clock	Ineffective

EPS License	
Max User Number	200
Max NAS/RADIUS Client Number	20
External Server Registration	Ineffective
RADIUS Port	Ineffective
Windows Domain Registration	Ineffective
Group	Ineffective
MAC Address Registration	Ineffective
Port Control	Ineffective

[Back](#) [Restart](#)

Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

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

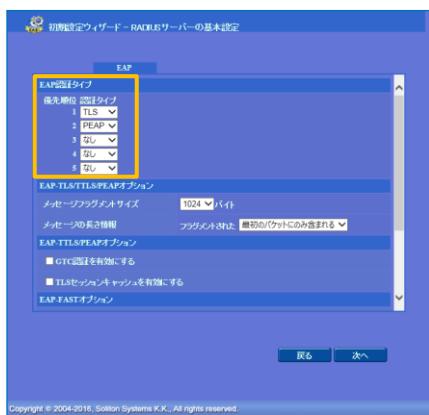
## 2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

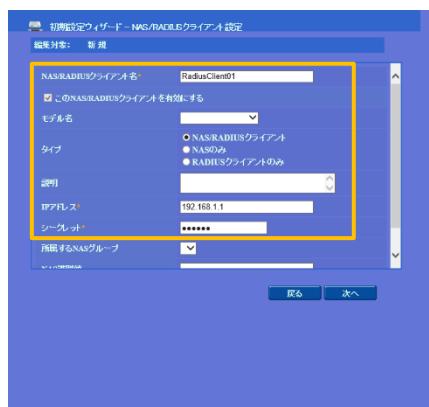
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定



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。

The screenshot shows the 'User List' screen of the NetAttest EPS management interface. On the left sidebar, under the 'User' section, the 'User List' option is selected. In the main area, there is a table with one row containing a user named 'test user'. To the right of the table is a toolbar with three buttons: 'New', 'Edit', and 'Delete'. A red arrow points from the 'New' button to the 'User Setting' dialog box below.

**User List Screen:**

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test			<span>発行</span> <span>変更</span> <span>削除</span>

**User Setting Dialog Box:**

編集対象: 新規

ユーザー情報		OIP
姓*	user01	
名		
E-Mail		
詳細情報		
ユーザーID*	user01	
パスワード*	password	
パスワード(確認)*	password	
<input type="checkbox"/> 一時利用停止		

OK キャンセル 適用

**User List Screen (After Addition):**

A red box highlights the newly added user 'user01' in the table. The 'user01' row has a red border around it.

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test			<span>発行</span> <span>変更</span> <span>削除</span>
user01	user01			<span>発行</span> <span>変更</span> <span>削除</span>

## 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)

The screenshot shows the NetAttest EPS management interface. On the left sidebar, under the 'User' section, 'User List' is selected. In the main area, a table lists users: 'test user' (User ID: test) and 'user01' (User ID: user01). A red box highlights the 'Issuance' button for 'user01'. A red arrow points from this button to the 'Issuance' button on the detailed user edit page.

**User List Page (Top Level):**

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test		<b>発行</b>	変更 削除
user01	user01		<b>発行</b>	変更 削除

The screenshot shows the 'Edit User' page for 'user01'. It includes sections for 'Basic Information' (Name: user01), 'Detailed Information' (E-Mail: user01), and 'Certification Information'. The 'Certification Information' section is highlighted with a yellow box, showing fields for 'User ID' (user01), 'Validity Period' (set to 365 days), and 'PKCS#12 File Option' (checkbox checked). A red box highlights the 'Issuance' button at the bottom right. A red arrow points from this button to the 'Issuance' button on the certificate download page.

**User Detail Edit Page (Second Level):**

編集対象: user01

基本情報

姓: user01  
名: user01  
E-Mail: user01

詳細情報

ユーザーID: user01  
有効期限: ● 日数: 365 日  
● 日付: 2016 年 7 月 9 日 23 時 59 分 59 秒まで

証明書ファイルオプション

パスワード: \_\_\_\_\_  
パスワード(確認): \_\_\_\_\_  
※パスワードが空欄の場合は、ユーザーのパスワードを使用します。

PKCS#12ファイルに証明機関の証明書を含める

**発行** **キャンセル**

The screenshot shows the 'User Certificate Download' page. It displays a message: 'ユーザー証明書ダウンロードの準備ができました。対象をファイルに保存して下さい。' (The preparation for user certificate download is complete. Save the target to a file.) A red box highlights the 'Download' button. A red arrow points from this button to the 'Download' button on the final confirmation page.

**User Certificate Download Page (Third Level):**

ユーザー証明書ダウンロード

ユーザー証明書ダウンロードの準備ができました。対象をファイルに保存して下さい。

**ダウンロード**

### 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。

The screenshot shows the web-based configuration interface for the BUFFALO WAPM-2133TR. The main menu on the left includes Home, 詳細設定 (selected), システム情報, ログアウト, 機能設定, 無線 (with options for SSID and channel), その他 (with options for firmware update and reset), and 緊急時モード (Emergency Mode). A red arrow points from the 'Home' tab to the 'IPアドレス' section of the 'LAN側IPアドレス設定' (LAN Side IP Address Setting) page. The 'IPアドレス' section contains fields for IPアドレスの取得方法 (Manual), IPアドレス (192.168.1.1), サブネットマスク (255.255.255.0), and デフォルトゲートウェイ (192.168.1.254). Below it are sections for DNSサーバー (Primary: 192.168.1.1, Secondary: 192.168.1.254) and DHCPサーバー (Enabled: No). A red box highlights the 'IPアドレス' field. Another red arrow points from the 'IPアドレス' field to the 'IPアドレス' table below.

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。

The screenshot shows the configuration interface for the BUFFALO AirStation Pro WAPM-2133TR. The left sidebar contains navigation links for HOME, LOGOUT, LAN設定, ネットワーク設定 (selected), RADIUS (selected), RADIUS設定 (highlighted with a red box), ユーザー管理, ブリッジ, Link Integrity設定, ProxyArp設定, 無線設定, 管理設定, and 機器診断.

**RADIUS設定**

**RADIUSサーバー**

サーバー	<input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	192.168.1.2
認証ポート	1812
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	1813
Shared Secret	●●●●●●●●●●
Session-Timeout	3600 秒

**セカンダリ-RADIUSサーバー**

サーバー	<input type="radio"/> 内蔵 <input checked="" type="radio"/> 外部
サーバー名	
認証ポート	1812
Accounting	<input checked="" type="checkbox"/> 使用する
Accountingポート	1813
Shared Secret	
Session-Timeout	3600 秒

**PMKキャッシュ**

PMKキャッシュ機能	使用しない
共有キー	

**内蔵RADIUSサーバー**

EAP内部認証	PEAP(MS-PEAP)
EAP証明書ファイル形式	PKCS#12(*.pfx / *.p12)
EAP証明書ファイル	<input type="button" value="参照..."/>
EAP証明書ファイル・パスワード	
Shared Secret	
Session-Timeout	
Termination-Action	サーバー サーバー名 認証ポート Accounting Accounting ポート Shared Secret Session-Timeout

**設定**

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。

**SSID設定 - SSIDの編集**

Index	状態	SSID	VLAN ID	2.4GHz	5GHz Low	5GHz High	認証	暗号化
SSIDの設定は登録されていません								

**新規追加**

**SSID設定 - SSIDの編集**

Index	状態	SSID	VLAN ID	2.4GHz	5GHz Low	5GHz High	認証	暗号化
SSIDの設定は登録されていません								

**使用可能SSID**

2.4GHz	5GHz Low	5GHz High
16 /16	16 /16	16 /16

**ステアリング ポリシー**

無効
----

**無線LAN**

<input checked="" type="radio"/> 有効	<input type="radio"/> 無効
-------------------------------------	--------------------------

**SSID**

SolitonLab
------------

**使用デバイス**

<input checked="" type="checkbox"/> 2.4GHz	<input checked="" type="checkbox"/> 5GHz Low	<input checked="" type="checkbox"/> 5GHz High
--	--	---

**ステアリング**

無効		
優先		
VLANモード	VLAN ID	追加VLAN ID
Untagged Port	1	
通常時と緊急時		
<input checked="" type="checkbox"/> 許可する		
使用しない		
2.4GHz	5GHz Low	5GHz High
128 /128	128 /128	128 /128
WPA2-EAP		
AES		
60 分		
無効		
追加認証を行わない		
ネットワーク設定内のRADIUSサーバー設定を使用する		

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

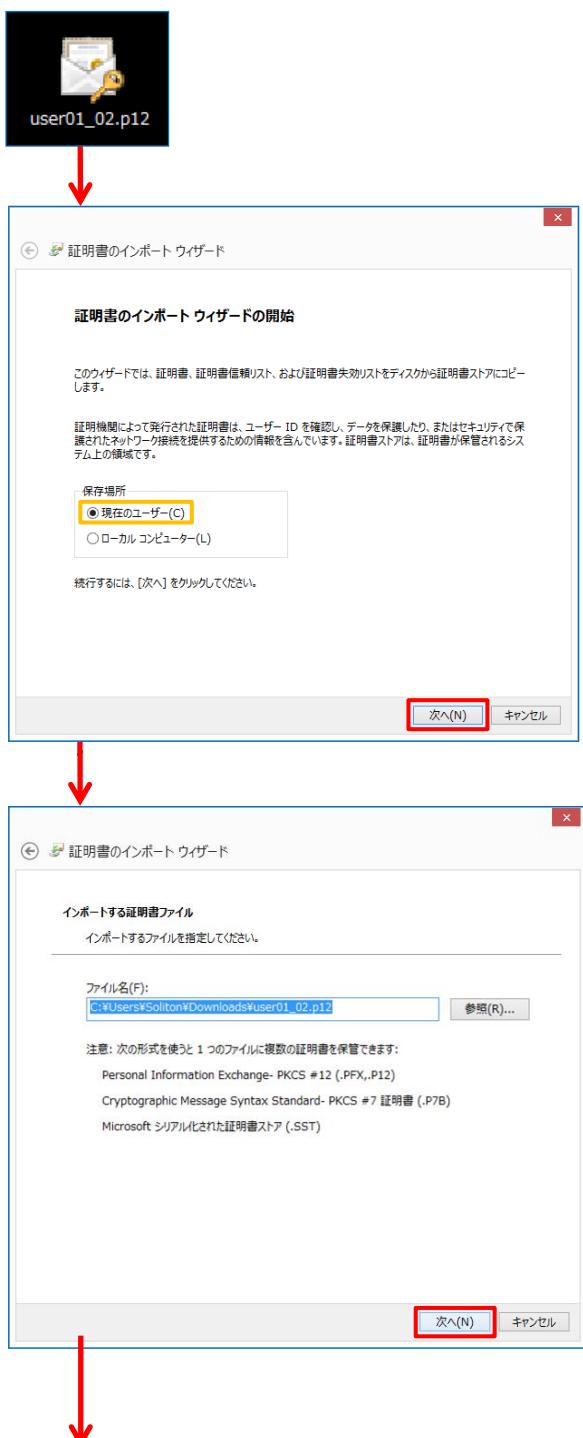
項目	値
無線の認証	WPA2-EAP
RADIUS	ネットワーク設定内の・・・

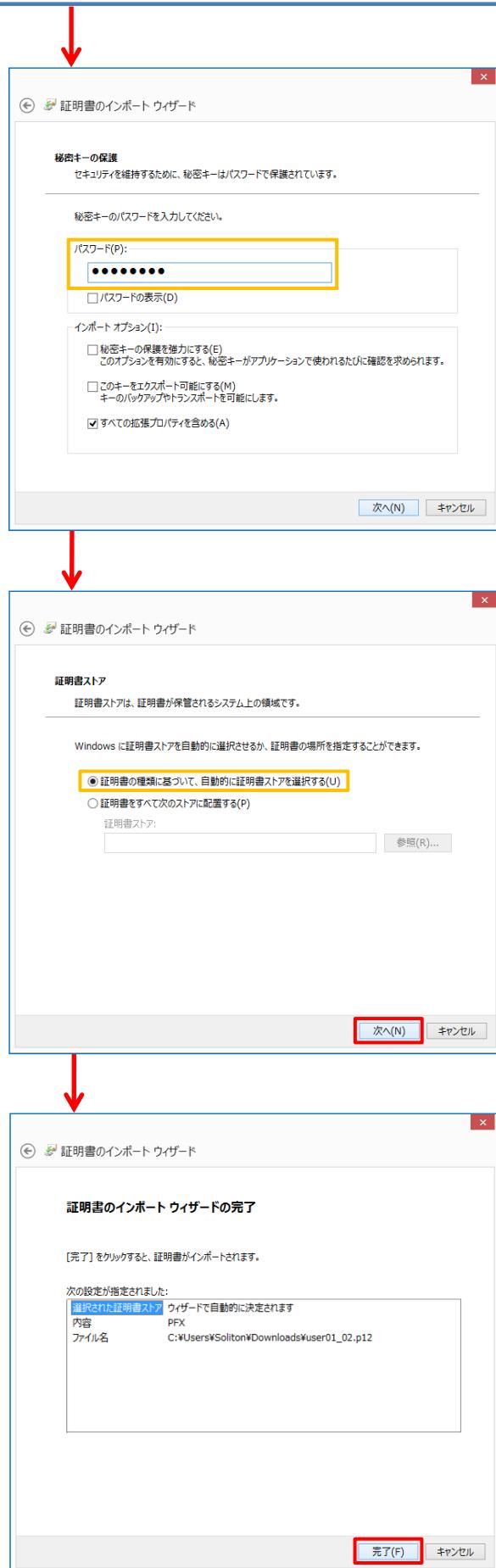
## 4. EAP-TLS 認証でのクライアント設定

### 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】**

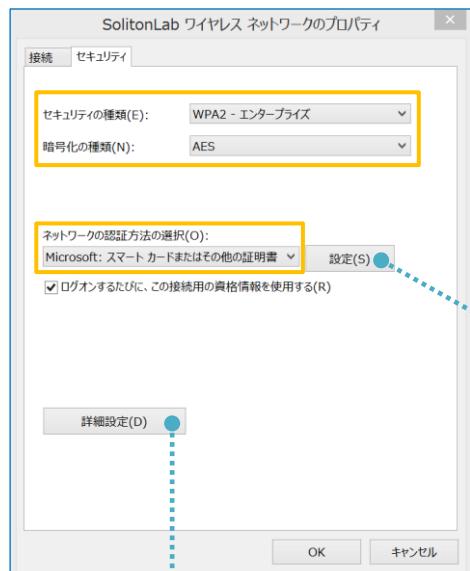
NetAttest EPS で証明書を発行した際に  
設定したパスワードを入力

## 4-1-2 サプリカント設定

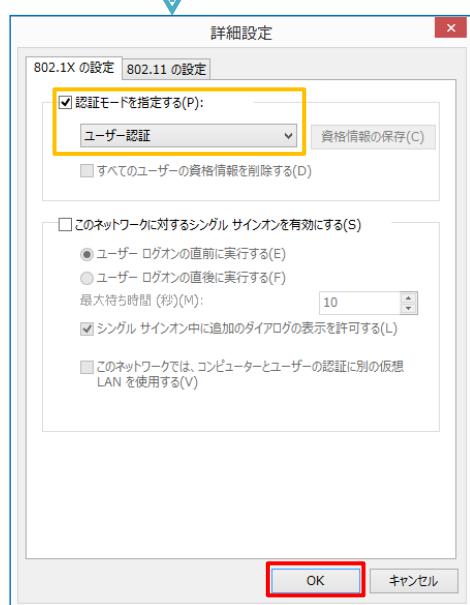
Windows 標準サプリカントで TLS の設定を行います。

※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。

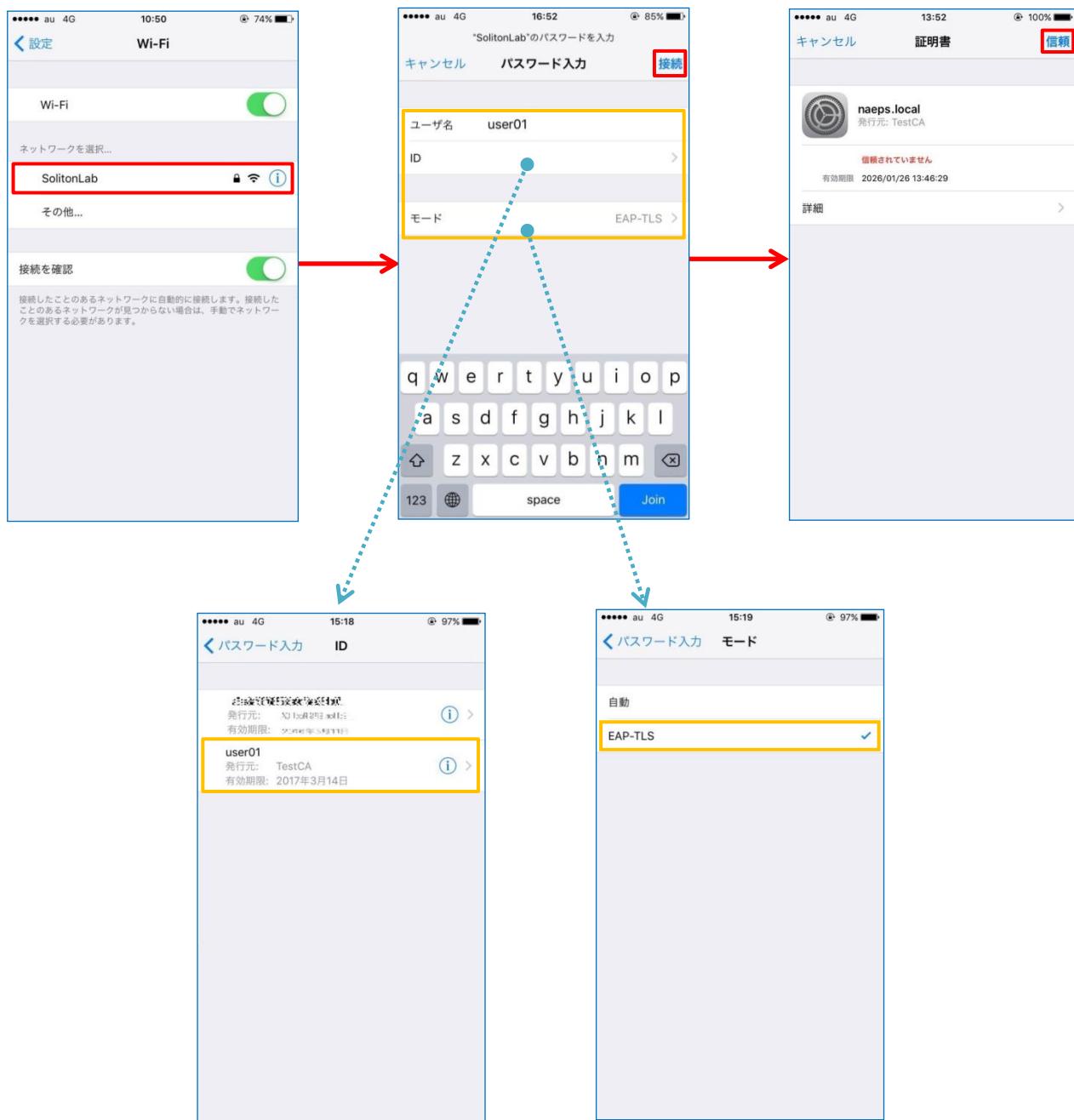
## 4-2-2 サプリカント設定

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。

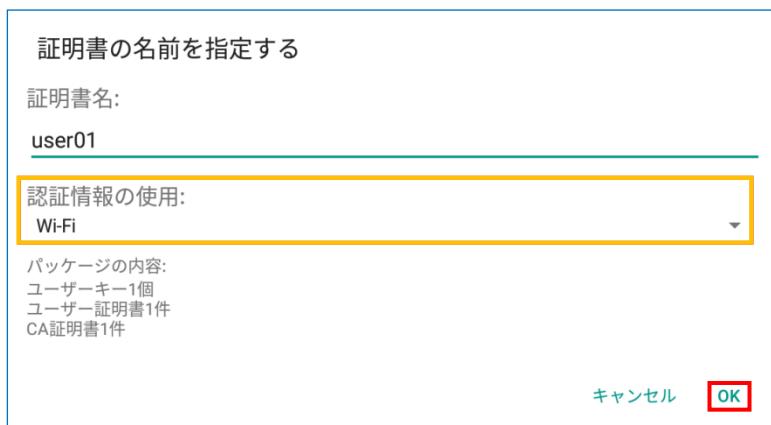
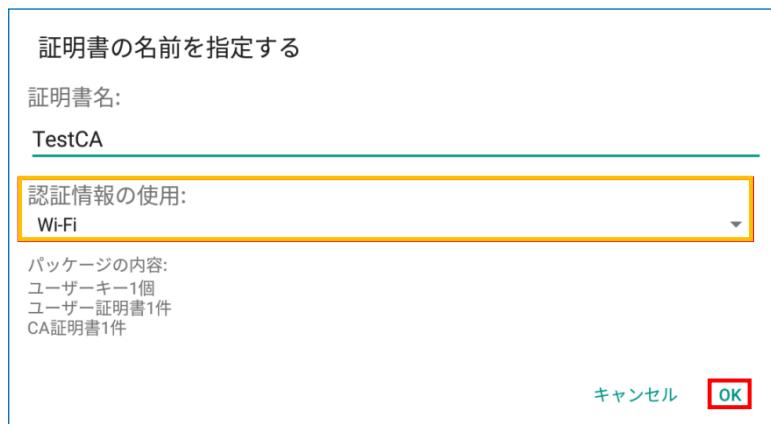
- 1) SD カードにクライアント証明書を保存し、インポートする方法※1
- 2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※2
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※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、メールにより、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。

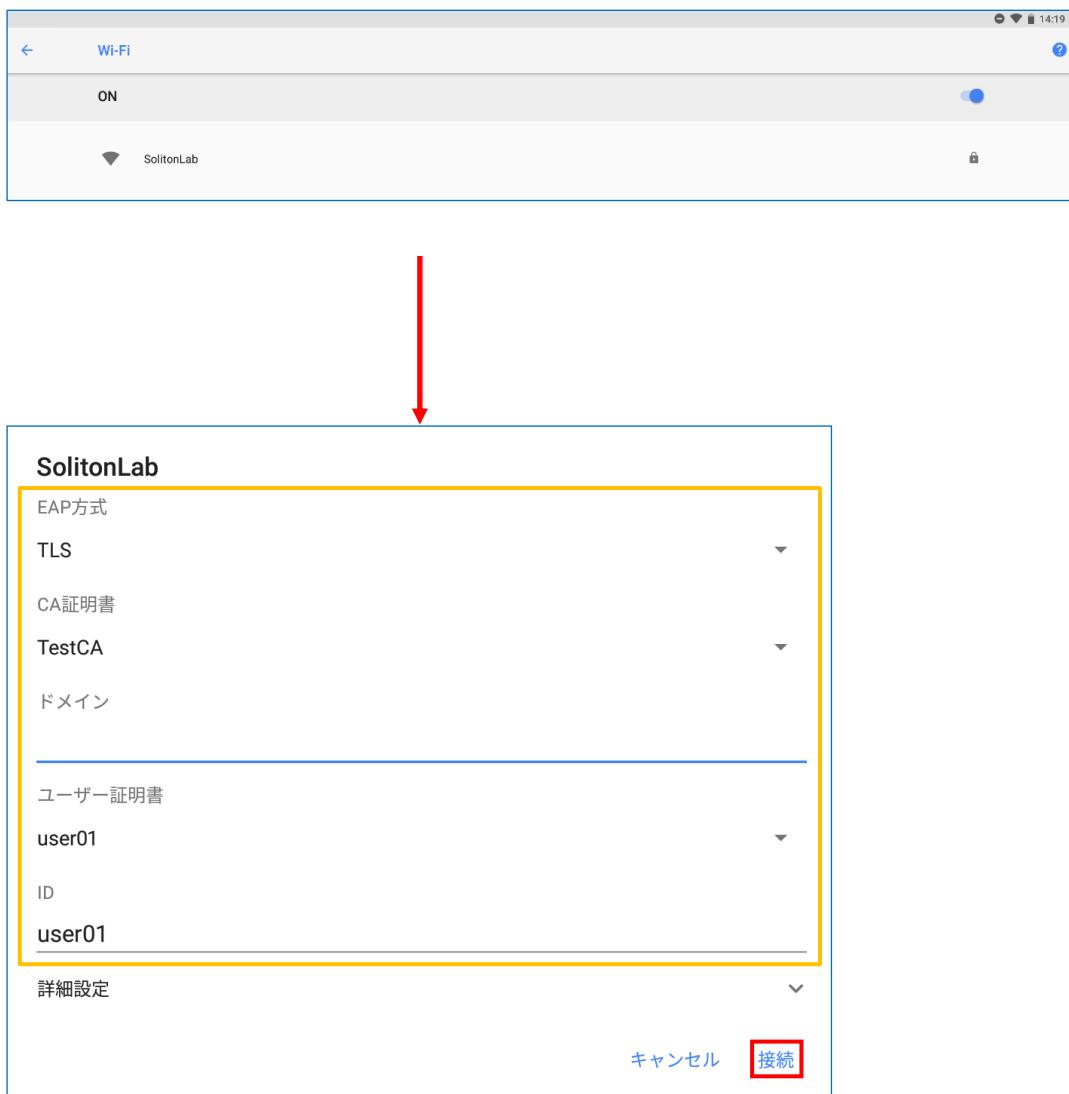


### 4-3-2 サプリカント設定

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 のサブリカント設定

[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。

The diagram illustrates the configuration process for EAP-PEAP authentication on Windows 10. It shows five main windows and their settings:

- Wireless Network Properties (セキュリティ)**:
 

セキュリティの種類(E):	WPA2 - エンタープライズ
暗号化の種類(N):	AES
ネットワークの認証方法の選択(O):	Microsoft: 保護された EAP (PEAP)
ログオンするたびに、この接続用の資格情報を使用する(R):	<input checked="" type="checkbox"/>
- セキュリティの種類** (Table):
 

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
- 保護された EAP のプロパティ**:
 

接続のための認証方法:	<input checked="" type="checkbox"/> 証明書を検証してサーバーの ID を検証する(V)
接続前の通知(T):	<input type="checkbox"/> サーバー名またはルート証明書が指定されなかった場合にユーザーに通知します
接続方法を選択する(S):	<input checked="" type="checkbox"/> セキュリティで保護されたパスワード (EAP-MSCHAP v2)
認証モード:	<input checked="" type="checkbox"/> 高速再接続を有効にする(F)
認証モード:	<input type="checkbox"/> ネットワーク アクセス保護を強制する(N)
認証モード:	<input type="checkbox"/> サーバーに暗号化ペイントの TLV がない場合は切断する(D)
認証モード:	<input type="checkbox"/> ID プライバシーを有効にする(I)
- EAP MSCHAPv2 のプロパティ**:
 

接続のための認証方法:	<input type="checkbox"/> Windows のログオン名とパスワード (およびドメインがある場合はドメイン) を自動的に使う(A)
-------------	--
- 認証モードを指定する** (Table):
 

項目	値
認証モードを指定する	ユーザー認証
- 接続のための認証方法** (Table):
 

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 のサブリカント設定

WAPM-2133TR で設定した SSID を選択し、サブ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。

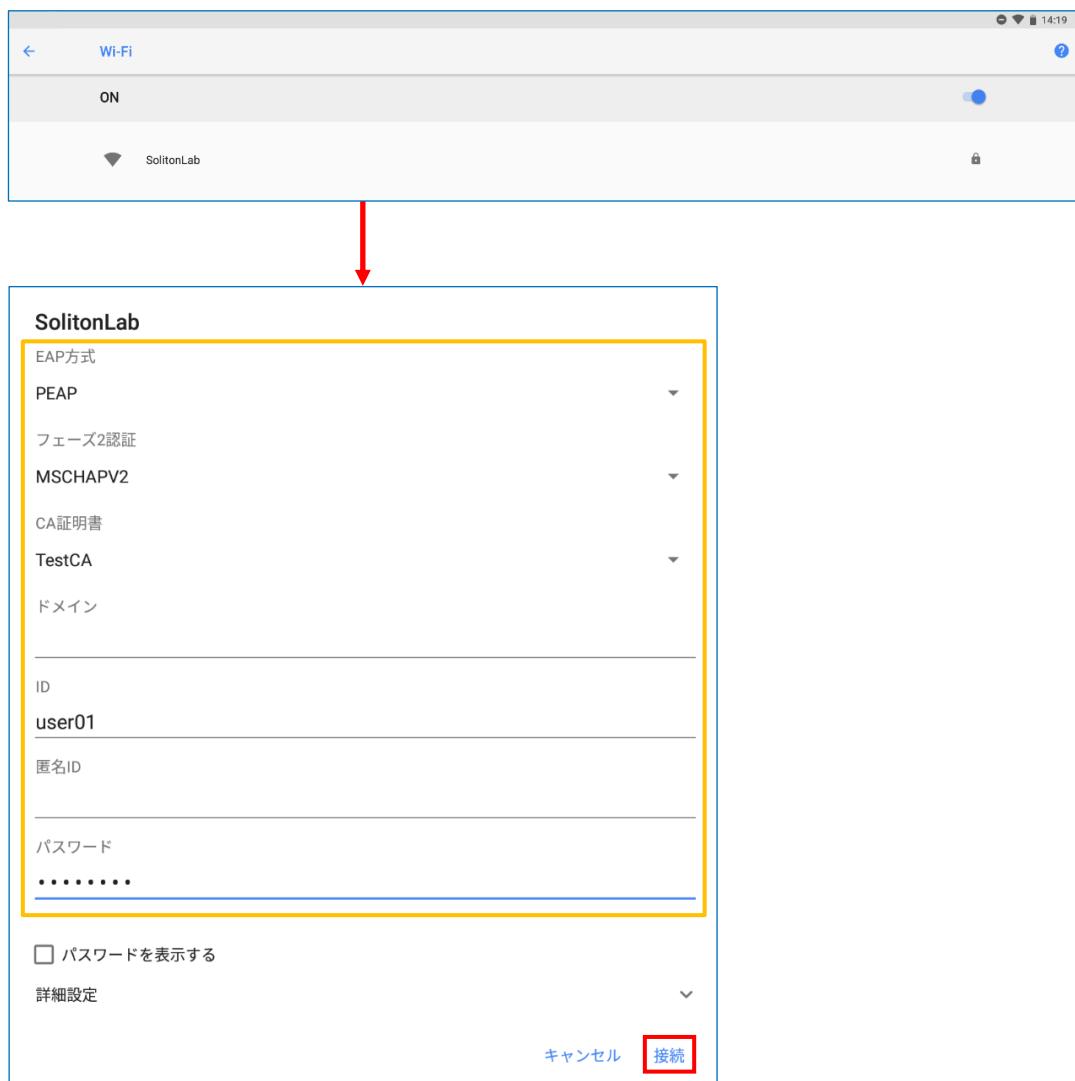


項目	値
ユーザ名	user01
パスワード	password
モード	自動

## 5-3 Android での EAP-PEAP 認証

### 5-3-1 Android のサブリカント設定

WAPM-2133TR で設定した SSID を選択し、サブ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