

# ***NetAttest EPS***

認証連携設定例

【連携機器】 ELECOM WAB-M2133

【Case】 IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)

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、ELECOM 社製無線アクセスポイント WAB-M2133 の IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)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 WAB-M2133 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. WAB-M2133 の設定.....	13
3-1 IP アドレスの設定.....	13
3-2 RADIUS の設定.....	14
3-3 無線の有効化設定.....	15
3-4 暗号化方式の設定.....	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(iPad Air 2)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 (Pixel C)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 のサプリカント設定.....	24

---

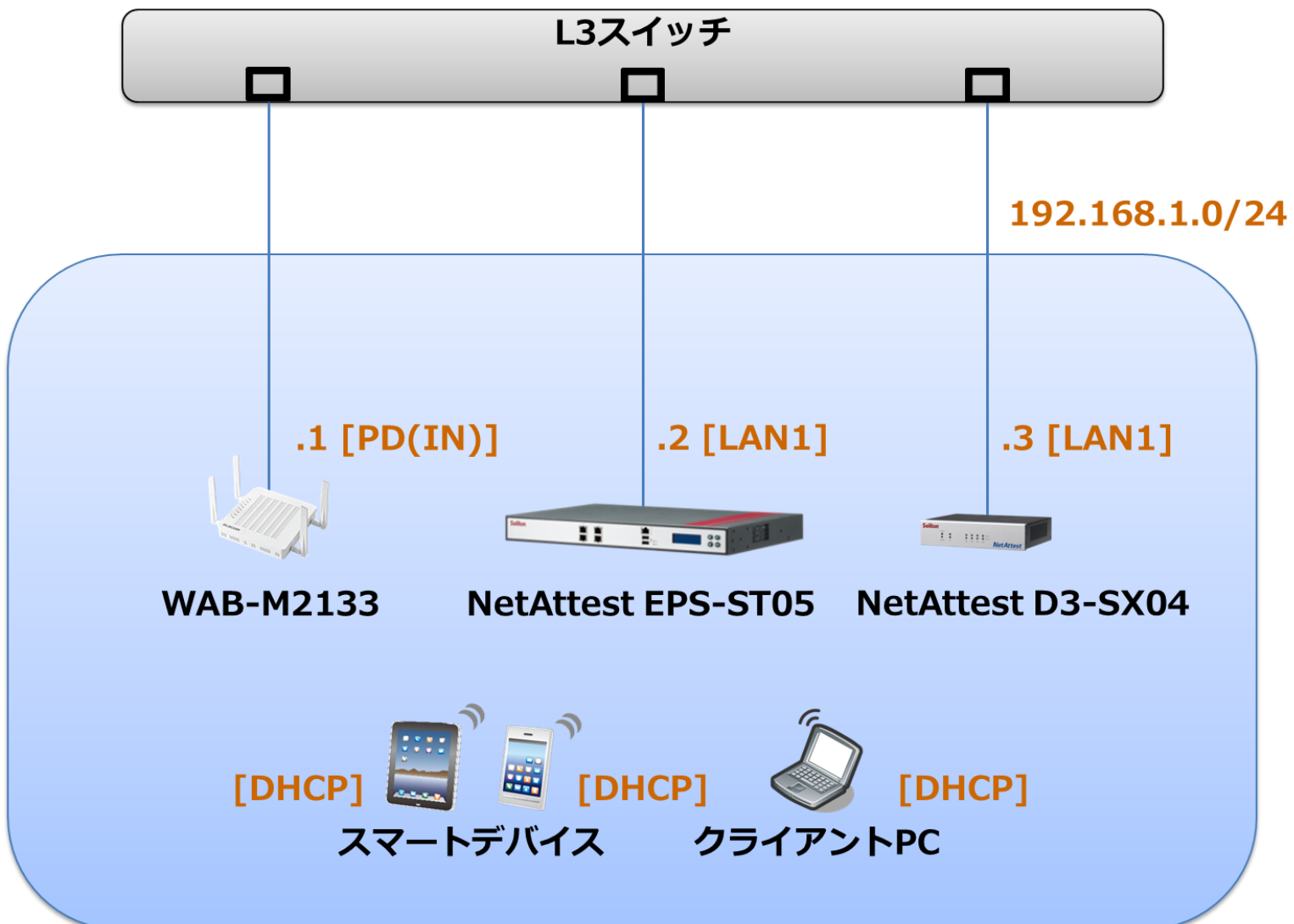
5-2 iOS(iPad Air 2)のサブリカント設定.....	25
5-3 Android(Pixel C)のサブリカント設定.....	26
<b>6. 動作確認結果 .....</b>	<b>27</b>
6-1 EAP-TLS 認証.....	27
6-2 EAP-PEAP(MS-CHAP V2)認証 .....	27

# 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 L3 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	4.8.11
WAB-M2133	ELECOM	RADIUS クライアント (無線アクセスポイント)	1.0.0
XPS 13	Dell	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブリカント
iPad Air 2	Apple	802.1X クライアント (Client Tablet①)	10.3.1
Pixel C	Google	802.1X クライアント (Client Tablet②)	7.1.2
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.11

### 1-2-2 認証方式

IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)

### 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
WAB-M2133	192.168.1.1/24		secret
Client PC	DHCP	-	-
Client Tablet①	DHCP	-	-
Client Tablet②	DHCP	-	-
NetAttest D3-SX04	192.168.1.3/24		

## 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

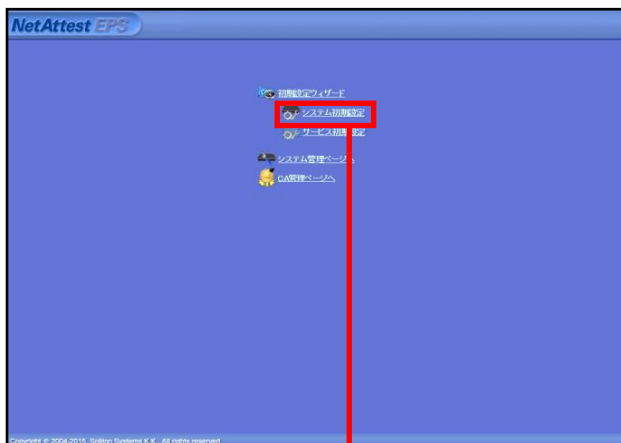


## 2-2 システム初期設定ウィザードの実行

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
- メインネームサーバーの設定



初期設定ウィザード - 設定項目の確認

設定内容を確認して下さい。  
この設定を保存・反映するには「再起動」ボタンをクリックして下さい。

ネットワーク時刻	
NTPサーバー1	
NTPサーバー2	
NTPサーバー3	
時刻同期する	無効
ホスト名	naeps.local
EPSライセンス	
最大ユーザー数	200
最大NAS/RADIUSクライアント数	20
外部サーバー証明書	無効
RADIUSプロキシ	無効
Windowsドメイン/認証連携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効

戻る 再起動

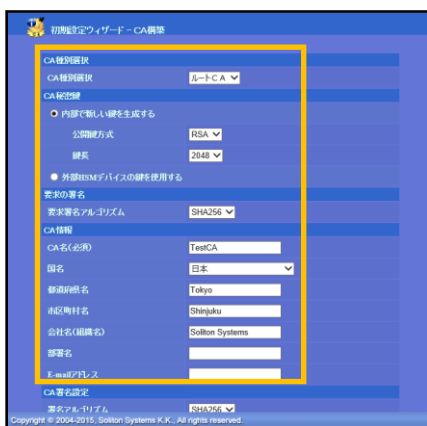
Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

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。

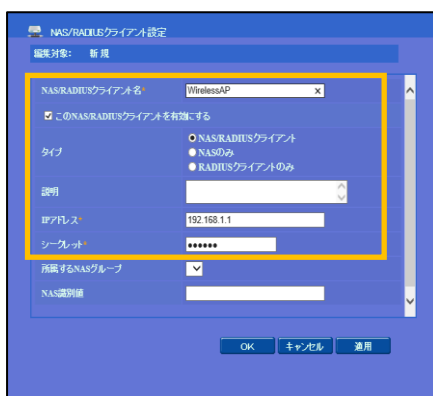
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定 (全般)
- RADIUS サーバーの基本設定 (EAP)
- RADIUS サーバーの基本設定 (証明書検証)
- NAS/RADIUS クライアント設定



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	WirelessAP
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 NetAttest EPS management interface. On the left is a sidebar menu with 'ユーザー一覧' (User List) highlighted. The main area shows a table of users with columns for '名前' (Name), 'ユーザーID' (User ID), '最終認証成功日時' (Last successful authentication date), '証明書' (Certificate), and 'タスク' (Task). A red box highlights the '追加' (Add) button in the top right of the table. Below the table is a 'ユーザー設定' (User Settings) form. The form has tabs for 'ユーザー情報' (User Information), 'チェックアイテム' (Check Items), 'リプライアイテム' (Reply Items), and 'OTP'. The 'ユーザー情報' tab is active, showing fields for '姓' (Surname), '名' (Name), 'E-Mail', 'ユーザーID', 'パスワード', and 'パスワード(確認)'. A red box highlights the 'OK' button at the bottom of the form. A red arrow points from the 'OK' button back to the '追加' button in the user list.

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

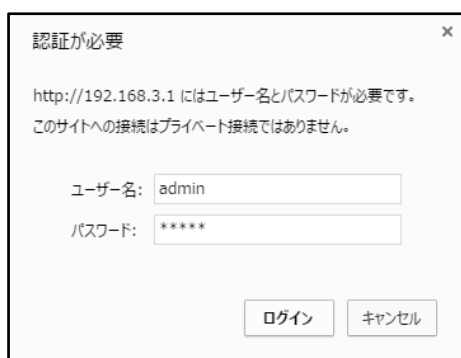
## 3. WAB-M2133 の設定

### 3-1 IP アドレスの設定

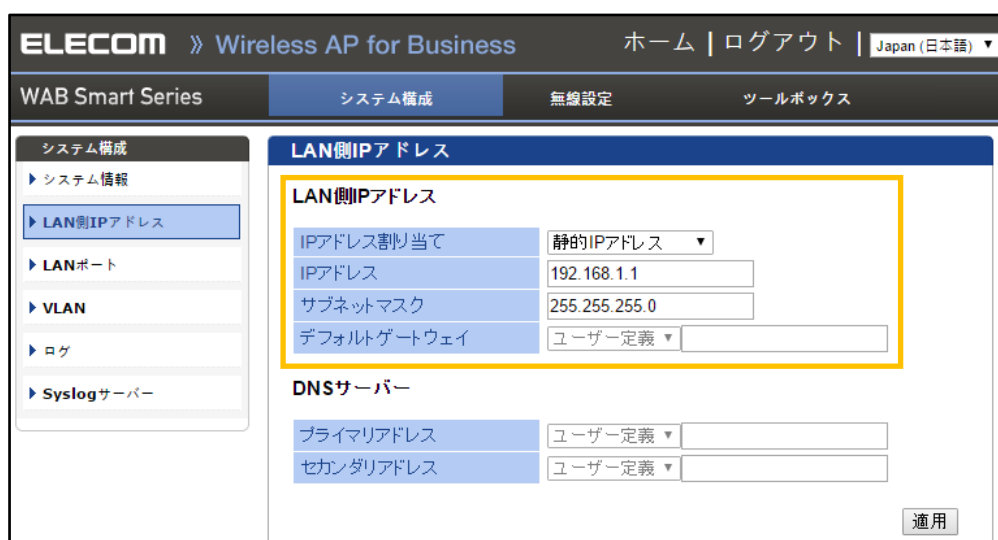
工場出荷状態の WAB-M2133 は、起動時に DHCP サーバーからアドレスを取得します。取得できなかった場合には、自動的に IP アドレス「192.168.3.1/24」を自身に割り当てます。設定を行う PC に適切な IP アドレスを設定した後、Web ブラウザを起動し、アドレスバーに IP アドレスを入力し、設定を開始します。

Web 管理画面にログインし、設定を開始します。

※初期設定では、ユーザー名 : admin パスワード : admin です。



[システム構成] - [LAN 側 IP アドレス]をクリックし、IP アドレス割り当てに「192.168.1.1」、サブネットマスクに「255.255.255.0」を入力し、「適用」をクリックします。



項目	値
IP アドレス	192.168.1.1
サブネットマスク	255.255.255.0

## 3-2 RADIUS の設定

RADIUS サーバーの登録を行います。[無線設定] - [RADIUS] - [RADIUS 設定]をクリックします。  
RADIUS サーバー(2.4G)の RADIUS サーバー(NetAttest EPS)の IP アドレス「192.168.1.2」、  
RADIUS サーバーとの共有シークレット(secret)を入力し、「適用」をクリックします。  
※5GHz を利用する場合は、RADIUS サーバー(5G)にて同様の設定を行います。

The screenshot shows the configuration page for RADIUS settings. The left sidebar has 'RADIUS' and 'RADIUS設定' highlighted. The main content area is titled 'RADIUS設定' and contains two sections: 'RADIUSサーバー (2.4G)' and 'RADIUSサーバー (5G)'. The '2.4G' section is highlighted with a yellow box and contains the following fields:

プライマリRADIUSサーバー	
RADIUSタイプ	<input checked="" type="radio"/> 外部 <input type="radio"/> 内部
RADIUSサーバー	192.168.1.2
認証ポート	1812
共有シークレット	.....
セッションタイムアウト	3600 秒
管理	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
管理ポート	1813

The '5G' section contains similar fields but is currently empty.

項目	値
RADIUS サーバー	192.168.1.2
認証ポート	1812
共有シークレット	secret

### 3-3 無線の有効化設定

WAB-M2133 の無線機能を有効にします。 [無線設定] - [2.4GHz 11bgn] - [基本設定]をクリックします。無線で「有効」のラジオボタンをクリックし、SSID(elecom2g-m2133)を入力して「適用」をクリックします。

※5GHz を利用する場合は、 [5GHz 11ac 11an] - [基本設定]にて同様の設定を行います。

The screenshot shows the configuration page for the ELECOM Wireless AP for Business. The page is titled "ELECOM Wireless AP for Business" and includes navigation links for "ホーム | ログアウト | Japan (日本語)". The main menu shows "WAB Smart Series" with sub-menus for "システム構成", "無線設定", and "ツールボックス". The "無線設定" menu is expanded, showing options for "WPS", "ゲストネットワーク", "2.4GHz 11bgn", and "5GHz 11ac 11an". The "2.4GHz 11bgn" menu is further expanded to show "基本設定", "詳細設定", "セキュリティ", and "クライアント". The "基本設定" page is displayed, showing the "2.4 GHz 基本設定" section. The "無線" option is selected with the "有効" radio button. The "無線通信モード" is set to "11b/g/n", the "有効 SSID 数" is "1", and the "SSID1" is "elecom2g-m2133" with a "VLAN ID" of "1". Other settings include "オートチャンネル" (無効), "チャンネル" (Ch 1), "チャンネル帯域幅" (Auto, +CH(+4)), and "BSS BasicRateSet" (1,2,5,5,6,11,12,24 Mbps). The "適用" button is highlighted with a red box.

2.4 GHz 基本設定	
無線	<input checked="" type="radio"/> 有効 <input type="radio"/> 無効
無線通信モード	11b/g/n
有効 SSID 数	1
SSID1	elecom2g-m2133
VLAN ID	1
オートチャンネル	<input type="radio"/> 有効 <input checked="" type="radio"/> 無効
チャンネル	Ch 1
チャンネル帯域幅	Auto, +CH(+4)
BSS BasicRateSet	1,2,5,5,6,11,12,24 Mbps

適用 キャンセル

### 3-4 暗号化方式の設定

無線の暗号化設定を行います。[無線設定] - [2.4GHz 11bgn] - [セキュリティ]をクリックします。認証方式を「WPA-EAP」、WPA タイプを「WPA/WPA2 mixed mode EAP」、暗号化タイプを「TKIP/AES mixed mode」を選択し、「適用」をクリックします。

※5GHz を利用する場合は、[5GHz 11ac 11an] - [セキュリティ]にて同様の設定を行います。

The screenshot shows the configuration page for a wireless AP. The left sidebar contains a navigation menu with the following items: 無線設定, WPS, ゲストネットワーク, 2.4GHz 11bgn (with sub-items: 基本設定, 詳細設定, セキュリティ), クライアント, WDS, MACフィルター, 5GHz 11ac 11an (with sub-items: 基本設定, 詳細設定, セキュリティ, クライアント, WDS, MACフィルター), RADIUS, and RADIUS設定. The 'セキュリティ' item under '2.4GHz 11bgn' is highlighted with a red box. The main content area is titled 'セキュリティ' and '2.4 GHz ワイヤレスセキュリティ設定'. It contains several fields: SSID (elecom2g-m2133), ブロードキャストSSID (有効), セパレーター機能 (無効), 接続制限台数 (50/50), 認証方式 (WPA-EAP), WPAタイプ (WPA/WPA2 mixed mode-EAP), 暗号化タイプ (TKIP/AES mixed mode), キー更新間隔 (60分), and 追加認証 (追加認証なし). A yellow box highlights the authentication settings. At the bottom right, there are two buttons: '適用' (Apply) and 'キャンセル' (Cancel), with '適用' highlighted by a red box.

2.4 GHz ワイヤレスセキュリティ設定	
SSID	elecom2g-m2133
ブロードキャストSSID	有効
セパレーター機能	無効
接続制限台数	50 / 50
認証方式	WPA-EAP
WPAタイプ	WPA/WPA2 mixed mode-EAP
暗号化タイプ	TKIP/AES mixed mode
キー更新間隔	60 分
追加認証	追加認証なし

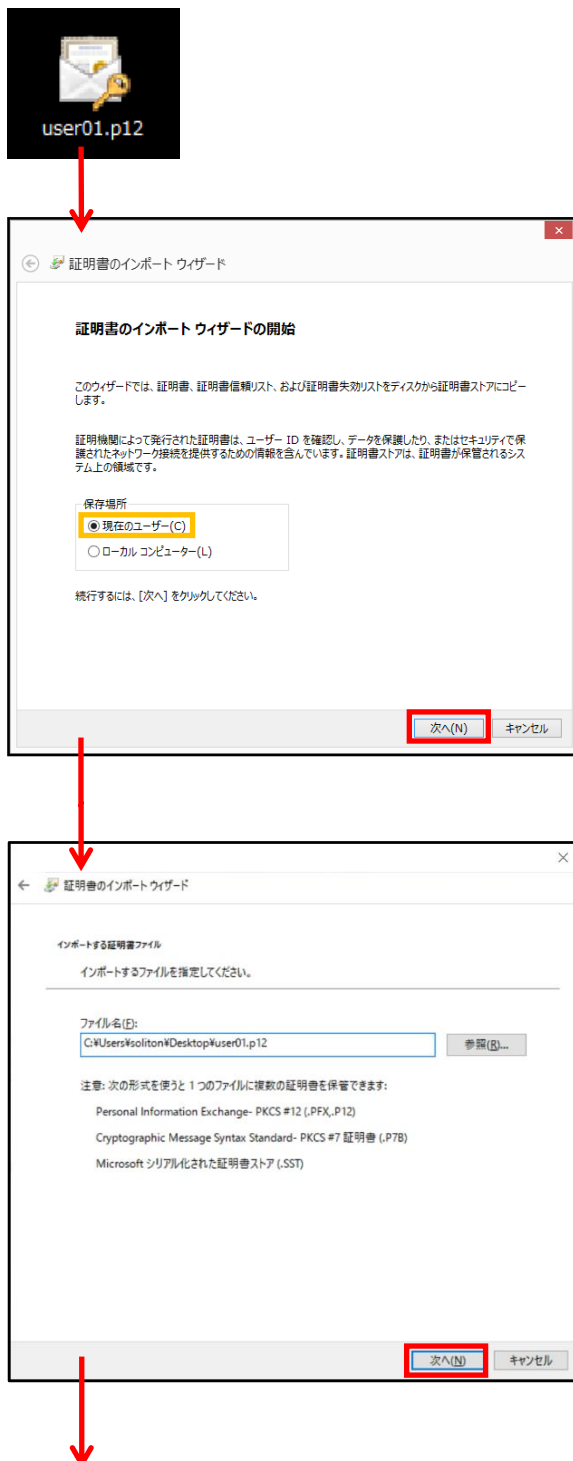


## 4. EAP-TLS 認証でのクライアント設定

### 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。



証明書のインポート ウィザード

**秘密キーの保護**  
セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):  
●●●●●●

パスワードの表示(D)

インポート オプション(O):

秘密キーの保護を強化にする(E)  
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。

このキーをエクスポート可能にする(M)  
キーのバックアップとトランスポートを可能にします。

すべての拡張プロパティを含める(A)

次へ(N) キャンセル

【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:

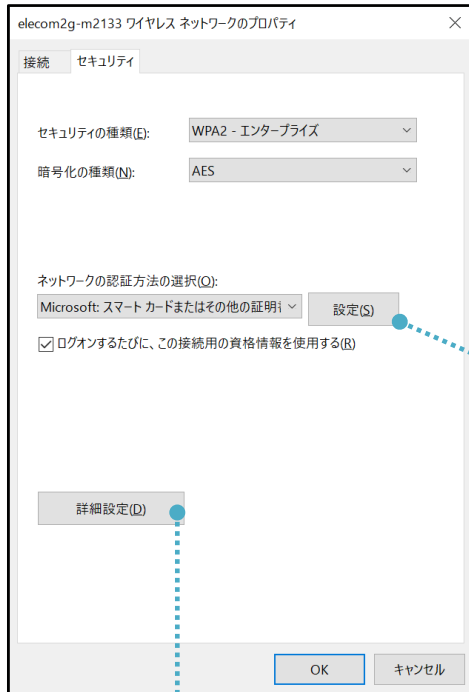
選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\soliton\Desktop\User01.p12

完了(F) キャンセル

## 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
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

項目	値
認証モードを指定する	ユーザー認証

## 4-2 iOS(iPad Air 2)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) 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。

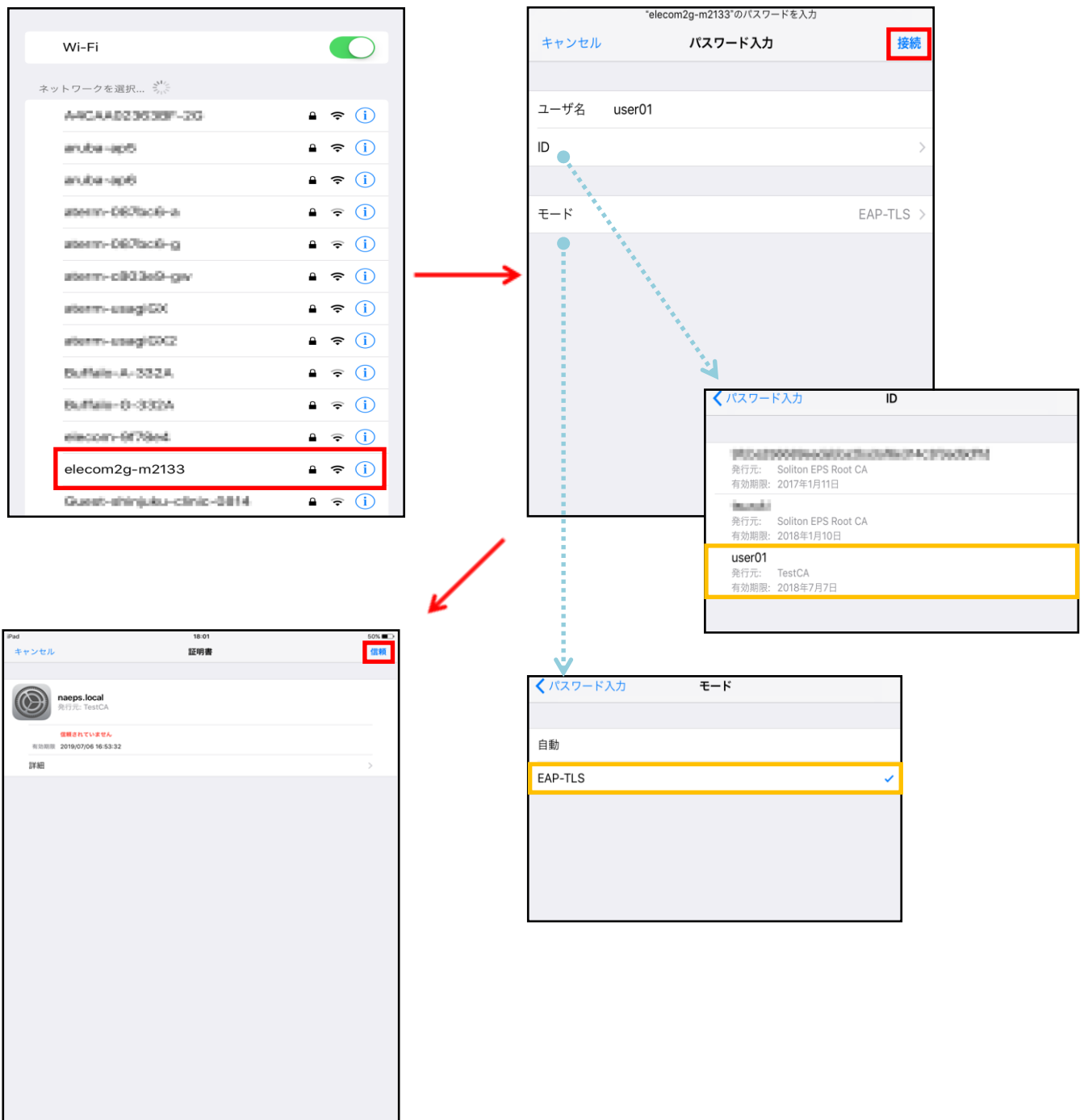
## 4-2-2 サプリカント設定

WAB-M2133 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 (Pixel C)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、下記の方法などがあります。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、メーカーにより、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 7.1.2 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。

証明書の名前を指定する

証明書名:  
TestCA

認証情報の使用:  
Wi-Fi

パッケージの内容:  
ユーザーキー1個  
ユーザー証明書1件  
CA証明書1件

キャンセル OK

証明書の名前を指定する

証明書名:  
user01

認証情報の使用:  
Wi-Fi

パッケージの内容:  
ユーザーキー1個  
ユーザー証明書1件  
CA証明書1件

キャンセル OK

## 4-3-2 サプリカント設定

WAB-M2133 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擇して下さい。

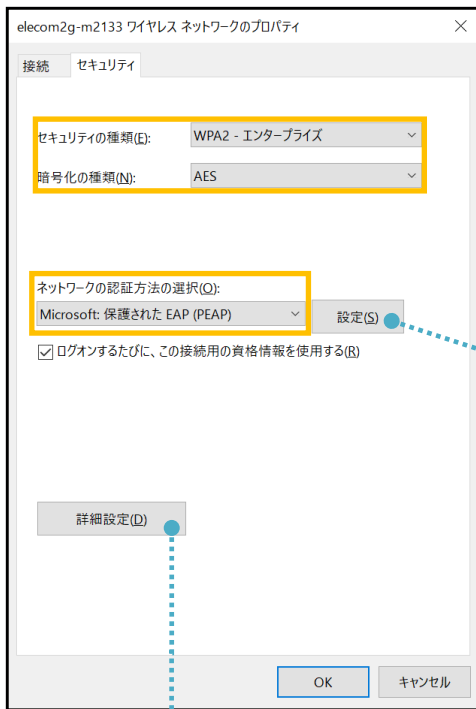


項目	値
EAP方式	TLS
CA証明書	TestCA
ユーザー証明書	user01
ID	user01

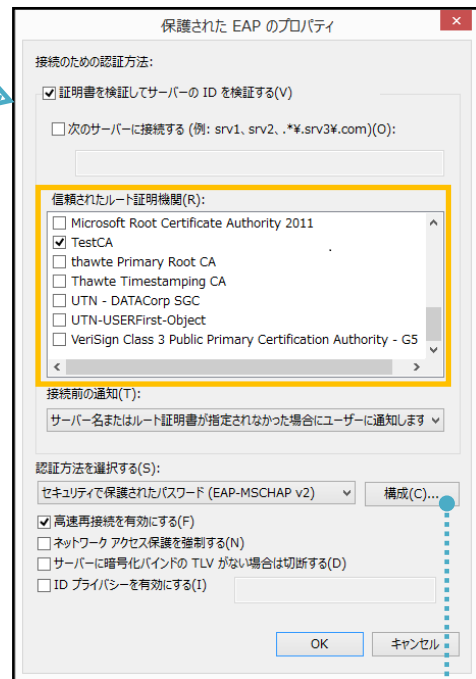
# 5. EAP-PEAP 認証でのクライアント設定

## 5-1 Windows 10 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。



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	
- 証明書を検証してサーバーの ID を・・・	On
- 信頼されたルート認証機関	TestCA



## 5-2 iOS(iPad Air 2)のサブリカント設定

WAB-M2133 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。

The process is shown in three steps:

- Selecting the SSID 'elecom2g-m2133' in the Wi-Fi settings.
- Entering the password on the 'パスワード入力' screen. The fields are:
 

項目	値
ユーザ名	user01
パスワード	password
モード	自動
- Accepting the certificate trust warning on the '証明書' screen by selecting '信頼'.

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

### 5-3 Android(Pixel C)のサブリカント設定

WAB-M2133 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」には、インポートした CA 証明書を選択してください。



**elecom2g-m2133**

EAP方式

PEAP ▼

フェーズ2認証

MSCHAPV2 ▼

CA証明書

TestCA ▼

ドメイン

---

ID

user01

---

匿名ID

---

パスワード

.....

パスワードを表示する

詳細設定項目 ▲

プロキシ

なし ▼

IP設定

DHCP ▼

キャンセル 保存

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 WirelessAP port 0 cli C4-8E-8F-F9-F8-F7)
WAB-M2133	Jul 10 14:30:20 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : authenticated Jul 10 14:30:20 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : starting accounting session 31532E7D-00000000 Jul 10 14:30:20 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : pairwise key handshake completed (RSN) Jul 10 14:30:07 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : associated

### 6-2 EAP-PEAP(MS-CHAP V2)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 WirelessAP port 0 cli C4-8E-8F-F9-F8-F7 via proxy to virtual server) Login OK: [user01] (from client WirelessAP port 0 cli C4-8E-8F-F9-F8-F7)
WAB-M2133	Jul 10 14:57:21 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : authenticated Jul 10 14:57:21 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : starting accounting session 31532E7D-00000012 Jul 10 14:57:21 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : pairwise key handshake completed (RSN) Jul 10 14:57:13 [WLAN]: Wireless 5G (SSID1), STA(c4:8e:8f:f9:f8:f7) : associated

## 改訂履歴

日付	版	改訂内容
2017/07/31	1.0	初版作成