

# ***NetAttest EPS***

認証連携設定例

【連携機器】 BUFFALO FS-M1266

【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 社製フリースポット導入キット FS-M1266 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。社内端末は IEEE802.1X 認証、ゲスト端末（FREESPOT 利用者）は FREESPOT 認証を使う構成です。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 FS-M1266 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.....	3
1-1 構成図.....	3
1-2 環境.....	4
1-2-1 機器.....	4
1-2-2 認証方式.....	4
1-2-3 ネットワーク設定.....	4
2. NetAttest EPS の設定.....	5
2-1 初期設定ウィザードの実行.....	5
2-2 システム初期設定ウィザードの実行.....	6
2-3 サービス初期設定ウィザードの実行.....	7
2-4 ユーザーの登録.....	8
2-5 クライアント証明書の発行.....	9
3. FS-M1266 の設定.....	10
3-1 IP アドレスの設定.....	11
3-2 RADIUS サーバーの設定.....	12
3-3 無線の設定.....	13
3-3-1 FREESPOT 用 SSID を有効.....	13
3-3-2 認証用 SSID の作成.....	14
4. EAP-TLS 認証でのクライアント設定.....	15
4-1 Windows 10 での EAP-TLS 認証.....	15
4-1-1 クライアント証明書のインポート.....	15
4-1-2 サプリカント設定.....	17
4-2 iOS での EAP-TLS 認証.....	18
4-2-1 クライアント証明書のインポート.....	18
4-2-2 サプリカント設定.....	19
4-3 Android での EAP-TLS 認証.....	20
4-3-1 クライアント証明書のインポート.....	20
4-3-2 サプリカント設定.....	21
5. EAP-PEAP 認証でのクライアント設定.....	22
5-1 Windows 10 での EAP-PEAP 認証.....	22

5-1-1 Windows 10 のサブリカント設定 .....	22
5-2 iOS での EAP-PEAP 認証 .....	23
5-2-1 iOS のサブリカント設定 .....	23
5-3 Android での EAP-PEAP 認証 .....	24
5-3-1 Android のサブリカント設定 .....	24
<b>6. 動作確認結果 .....</b>	<b>25</b>
6-1 EAP-TLS 認証 .....	25
6-2 EAP-PEAP 認証 .....	25

# 1. 構成

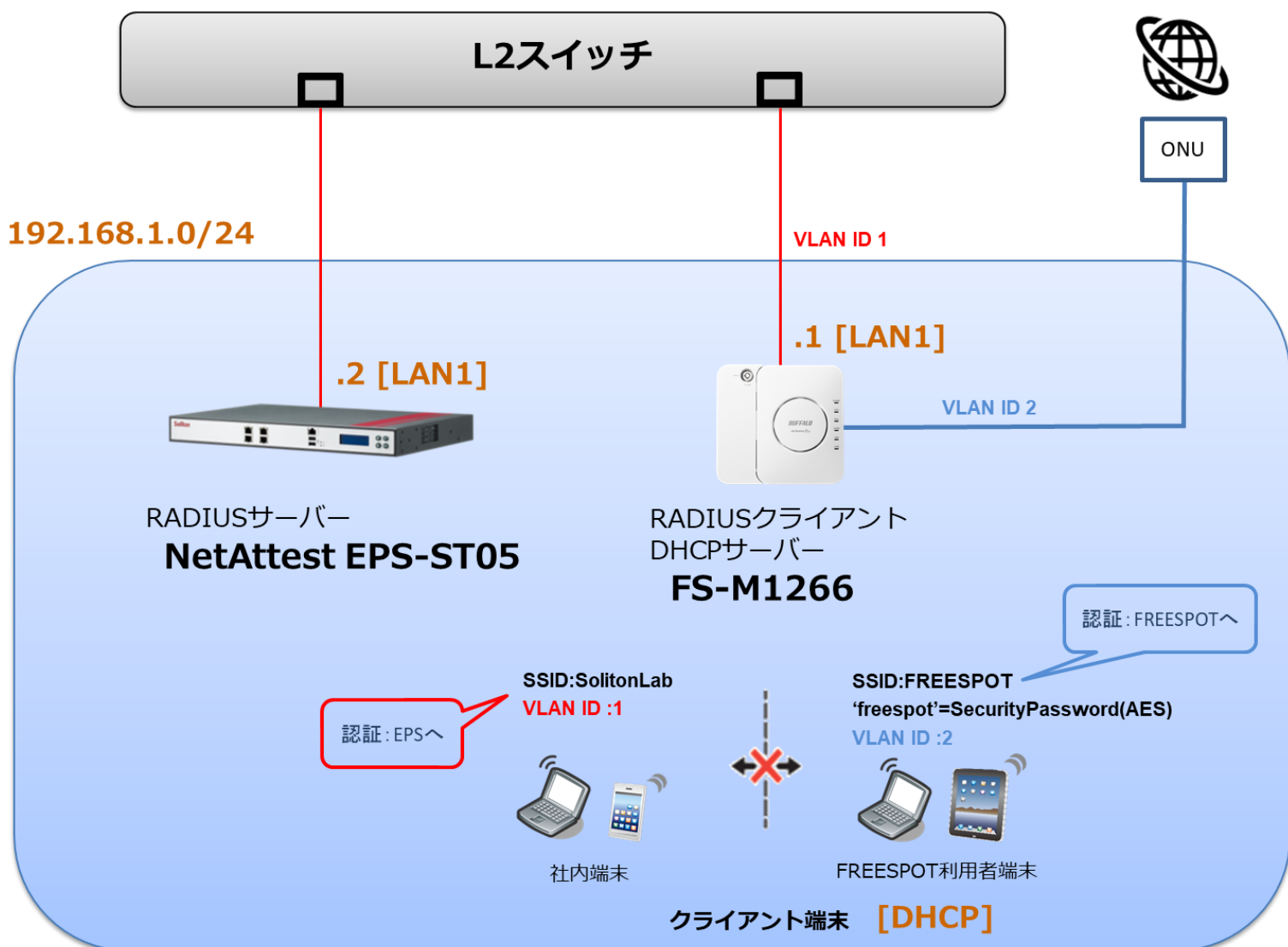
## 1-1 構成図

以下の環境を構成します。

ユースケース：社内端末は IEEE802.1X 認証を利用

ゲスト端末（FREESPOT 利用者）は FREESPOT 認証を利用

- 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端末の IP アドレスは、FS-M1266 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
FS-M1266	BUFFALO	RADIUS クライアント (フリースポット導入キット) DHCP サーバー	Ver. 4.00 (R2.01)
VAIO Pro PB	VAIO	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)	12.0
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0

## 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
FS-M1266	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。

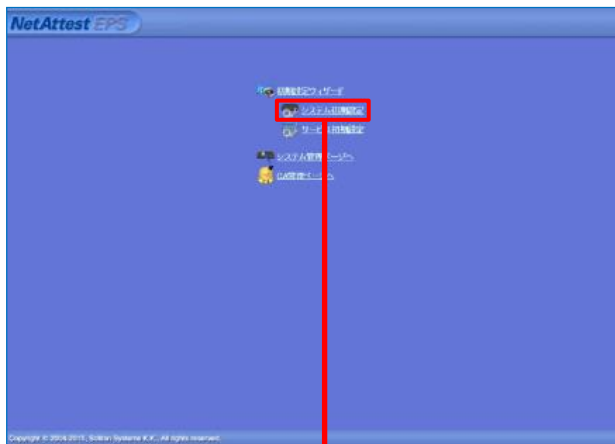
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行



## 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



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

---

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

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

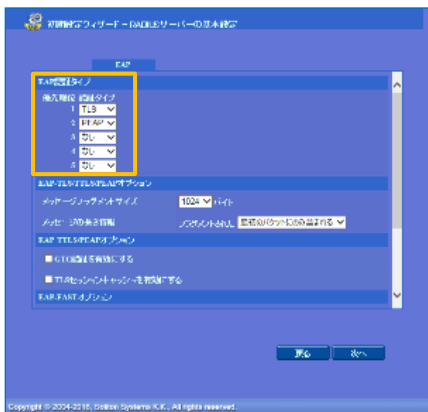
## 2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

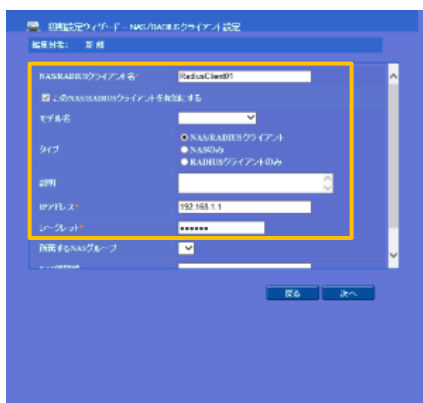
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定 (全般)
- RADIUS サーバーの基本設定 (EAP)
- RADIUS サーバーの基本設定 (証明書検証)
- NAS/RADIUS クライアント設定



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。

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

項目	値
姓	user01
ユーザーID	user01
パスワード	password

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

## 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. FS-M1266 の設定

BUFFALO 社製フリースポット導入キット FS-M1266 の設定を行います。

FS-M1266 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。

FS-M1266 の初期 IP アドレスは 192.168.11.1 です。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



FREESPOT をご使用いただくには上記の設定の他にインターネット回線を FS-M1266 の WAN 端子に接続する必要があります。FREESPOT、WAN 側の詳しい説明は BUFFALO FS-M1266 の製品ページからマニュアルをご参照ください。

FS-M1266 のマニュアル : <https://d.buffalo.jp/fs-m1266>

### 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。

[WAN/LAN]-[LAN 設定]をクリックし、No.1 の編集をクリックします。

LAN側インターフェース設定

VLAN設定

No	状態	VLAN名	VLAN ID	IPアドレス	ト-フィルター	SPAMメール対策	ポップアップ	接続時間制限	利用者認証	Wi-Cert 認証	
1	有効	Management	1	192.168.11.1/24	無効	無効	無効	無効	無効	無効	編集
2	無効	FREESPOT	2	192.168.12.1/24	無効	有効	無効	無効	有効	無効	編集
3	無効	CUSTOM_0	3	192.168.13.1/24	無効	有効	無効	無効	有効	無効	編集
4	無効	CUSTOM_1	4	192.168.14.1/24	無効	有効	無効	無効	有効	無効	編集
5	無効	CUSTOM_2	5	192.168.15.1/24	無効	有効	無効	無効	有効	無効	編集

インターネット

FS-M1266 Version 4.00

インターフェース設定

IP アドレスと割り当て IP アドレスを変更し、「修正保存」ボタンをクリックします。

VLAN情報の編集

VLAN名	Management		
VLAN ID	1		
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	
ルーティング	ルーティング		
DHCP サーバー	<input checked="" type="checkbox"/> 使用する		
	割り当て IP アドレス	192.168.1.3	から 32 台
	除外アドレス		
	リース期間	48	時間
	デフォルトゲートウェイの通知	エアステーションのLAN側IPアドレス	
DNSサーバーの通知	エアステーションのLAN側IPアドレス		

修正保存 編集を終了して前の画面へ戻る

項目	値
IP アドレス	192.168.1.1
割り当て IP アドレス	192.168.1.3

## 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 設定]をクリックし、プライマリーRADIUS サーバーの設定をします。

サーバー名に RADIUS サーバーの IP アドレスを入力し、Shared Secret に RADIUS サーバーのシークレットで設定した内容を設定します。

最後に「設定」ボタンをクリックして、設定を保存します。

**RADIUSサーバー**

プライマリーRADIUSサーバー

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

セカンダリーRADIUSサーバー

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

設定

項目	値
サーバー名	192.168.1.2
Shared Secret	secret

### 3-3 無線の設定

FREESPOT 用 SSID と認証用 SSID の設定を行います。

ここでは Index1、2 の両方を有効にする例を示します。

#### 3-3-1 FREESPOT 用 SSID を有効

[無線設定]-[SSID 設定]をクリックします。

以下の画面から Index1 の「編集」ボタンをクリックします。

Index	状態	SSID	VLAN	VLAN ID	2.4GHz	5GHz	認証	暗号化		
1	無効	FREESPOT	FREESPOT	2	<input type="radio"/>	<input type="radio"/>	認証を行わない	暗号化なし	<b>編集</b>	削除
2	無効	*freespot*=SecurityPassword(AES)	FREESPOT	2	<input type="radio"/>	<input type="radio"/>	WPA2/WPA(混在)-PSK	TKIP/AES(混在)	編集	削除

新規追加

以下の画面で、無線 LAN の項目の有効を選択します。

無線LAN  有効  無効

SSID \*freespot\*=SecurityPas

「修正保存」ボタンをクリックします。

**修正保存** 編集を終了して前の画面へ戻る

Index2 の「編集」ボタンをクリックします。

Index	状態	SSID	VLAN	VLAN ID	2.4GHz	5GHz	認証	暗号化		
1	有効	FREESPOT	FREESPOT	2	<input type="radio"/>	<input type="radio"/>	認証を行わない	暗号化なし	編集	削除
2	無効	*freespot*=SecurityPassword(AES)	FREESPOT	2	<input type="radio"/>	<input type="radio"/>	WPA2/WPA(混在)-PSK	TKIP/AES(混在)	<b>編集</b>	削除

新規追加

以下の画面で、無線 LAN の項目の有効を選択します。

無線LAN  有効  無効

SSID \*freespot\*=SecurityPas

「修正保存」ボタンをクリックします。

**修正保存** 編集を終了して前の画面へ戻る



## 3-3-2 認証用 SSID の作成

[無線設定]-[SSID 設定]をクリックし、以下の画面から「新規追加」ボタンをクリックします。

Index	状態	SSID
1	無効	FREESPOT
2	有効	'freespot'=Sec

新規追加

無線 LAN の項目で「有効」を選択します。

SSID に任意の文字を入力し、使用するデバイスで「2.4GHz」と「5GHz」を選択します。

無線の認証の項目で「WPA2-EAP」を選択します。

RADIUS の項目で「ネットワーク設定内の RADIUS サーバー設定を使用する」を選択します。

最後に「修正保存」をクリックして設定を保存します。

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
優先制御	優先
VLAN ID	VLAN モード: Untagged, VLAN: Management, VLAN ID: 1
次の場合に有効にする	通常時と緊急時
ANY接続	<input checked="" type="checkbox"/> 許可する
プライバシーセパレーター	使用しない
ロードバランス(同時接続台数制限)	2.4GHz: 128 / 128, 5GHz: 128 / 128
無線の認証	WPA2-EAP
暗号化方式	AES
キー更新間隔	60 分
Management Frame Protection	無効
追力認証	追加認証を行わない
RADIUS	ネットワーク設定内のRADIUSサーバー設定を使用する
修正保存	編集を終了して前の画面へ戻る

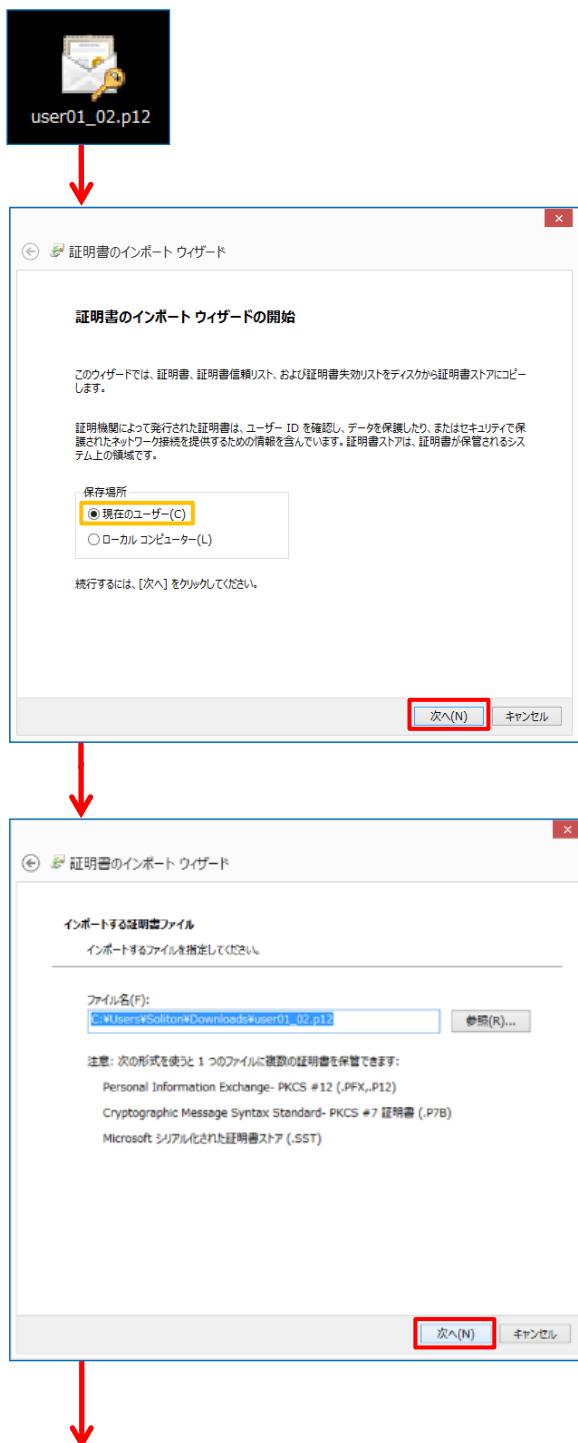
項目	値
無線 LAN	有効
SSID	SolitonLab
使用デバイス	2.4GHz、5GHz
無線の認証	WPA2-EAP
RADIUS	ネットワーク設定内の・・・

## 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。



証明書インポート 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や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】

「2-4 ユーザーの登録」で設定したパスワードを入力

証明書インポート 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:

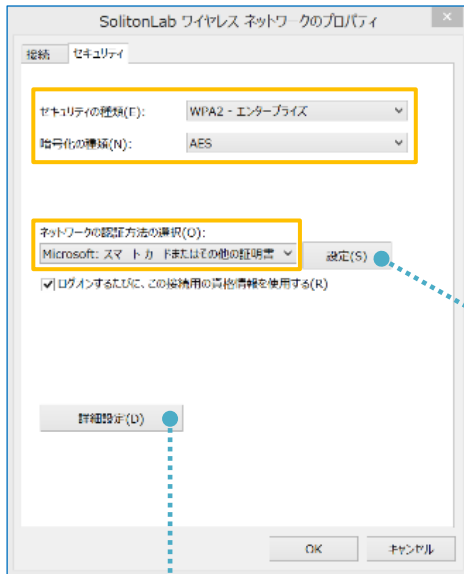
選択された証明書ストア	ウィザードで自動的に決定されます
内容	PEM
ファイル名	C:\Users\Soliton\Downloads\User01_02.p12

完了(F) キャンセル

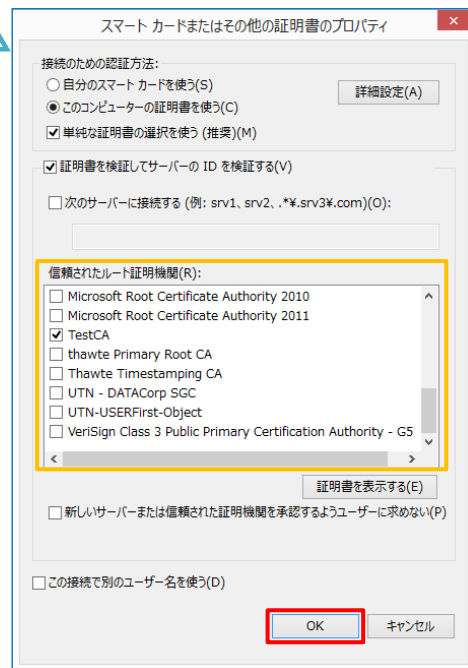
## 4-1-2 サプリカント設定

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 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)

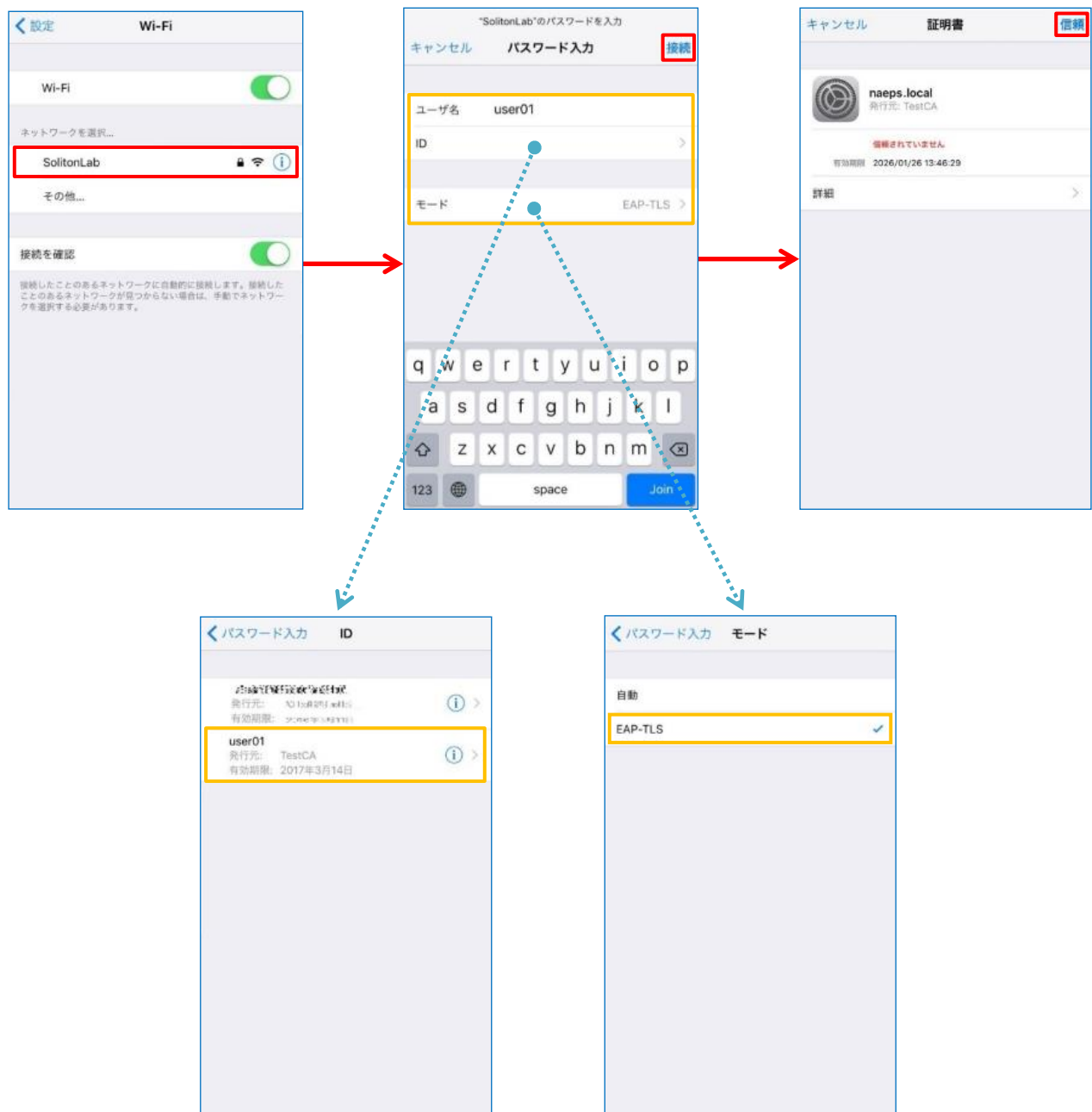
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

## 4-2-2 サプリカント設定

FS-M1266 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 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。

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

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

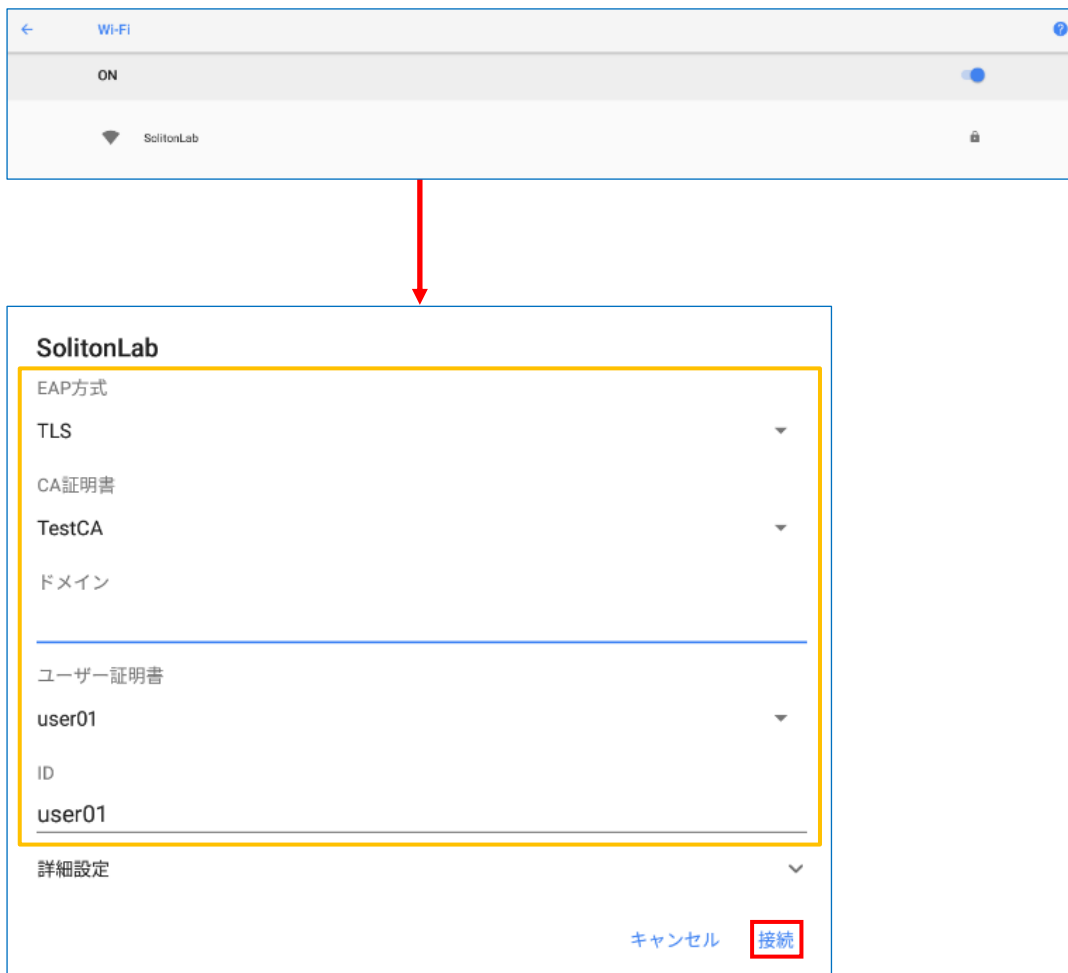
パッケージの内容:  
ユーザーキー1個  
ユーザー証明書1件  
CA証明書1件

キャンセル

## 4-3-2 サプリカント設定

FS-M1266 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」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

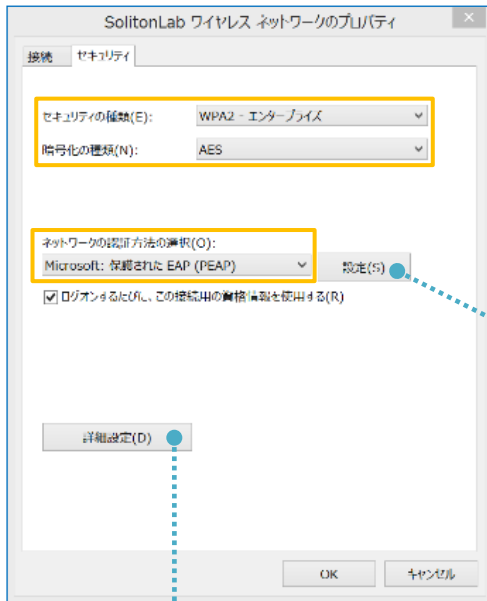


# 5. EAP-PEAP 認証でのクライアント設定

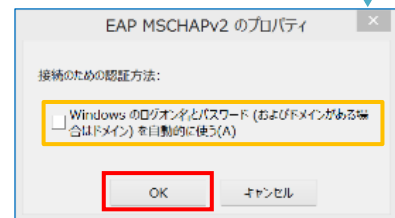
## 5-1 Windows 10 での EAP-PEAP 認証

### 5-1-1 Windows 10 のサブクライアント設定

[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 のサブリカント設定

FS-M1266 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。

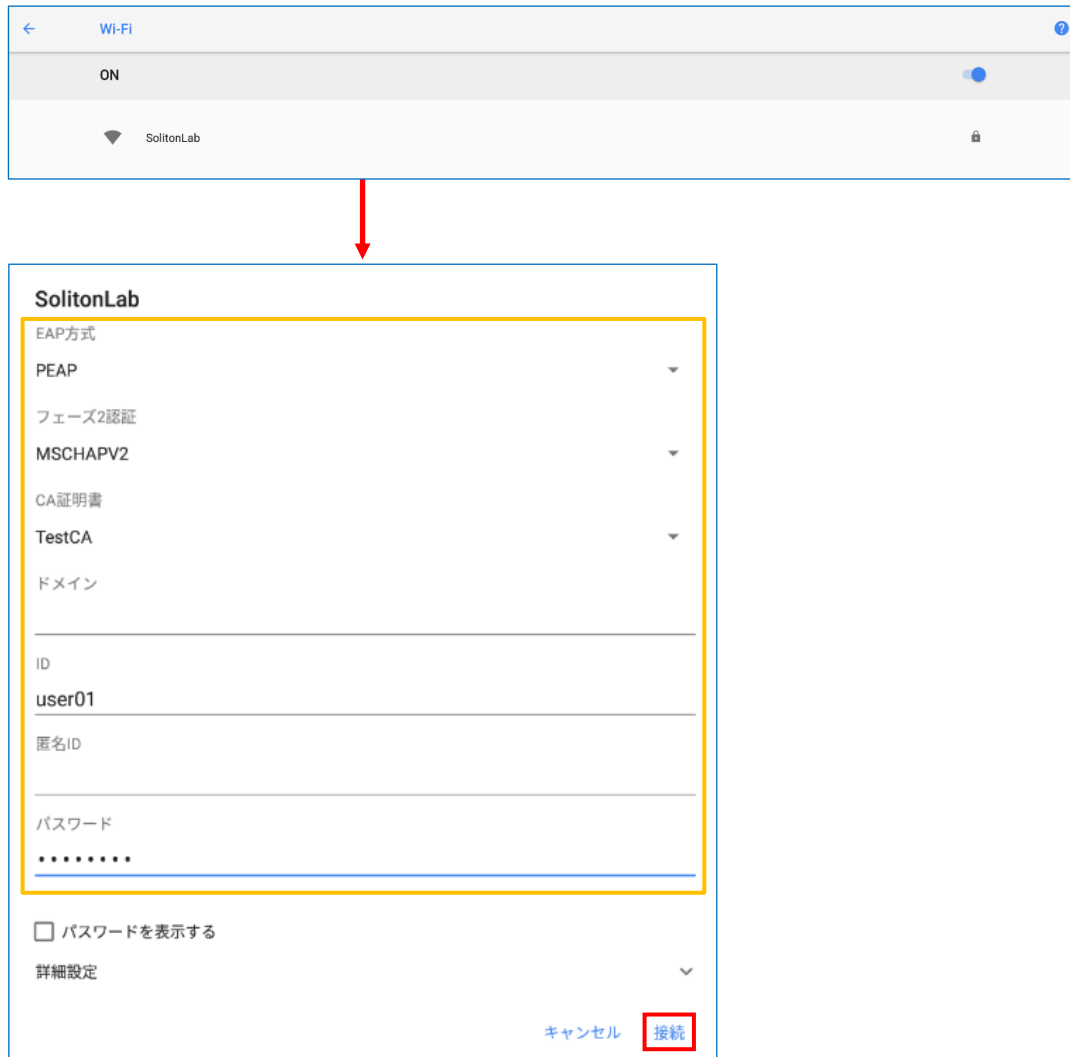


項目	値
ユーザ名	user01
パスワード	password
モード	自動

## 5-3 Android での EAP-PEAP 認証

### 5-3-1 Android のサブリカント設定

FS-M1266 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	Login OK: [user01] (from client RadiusClient01 port 0 cli 40-A3-CC-32-10-A4)
FS-M1266	AUTH w10.2 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 40:a3:cc:32:10:a4

### 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)
FS-M1266	AUTH w10.2 (5GHz): Authenticated (WPA2-EAP: TTL 1800) User [user01] - 40:a3:cc:32:10:a4

