NetAttest EPS
認証連携設定例

【連携機器】NEC プラットフォームズ NA1500A

【Case】IEEE802.1X EAP-TLS/EAP-PEAP

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、NEC プラットフォームズ社製無線アクセスポイント NA1500A 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 NA1500A 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。

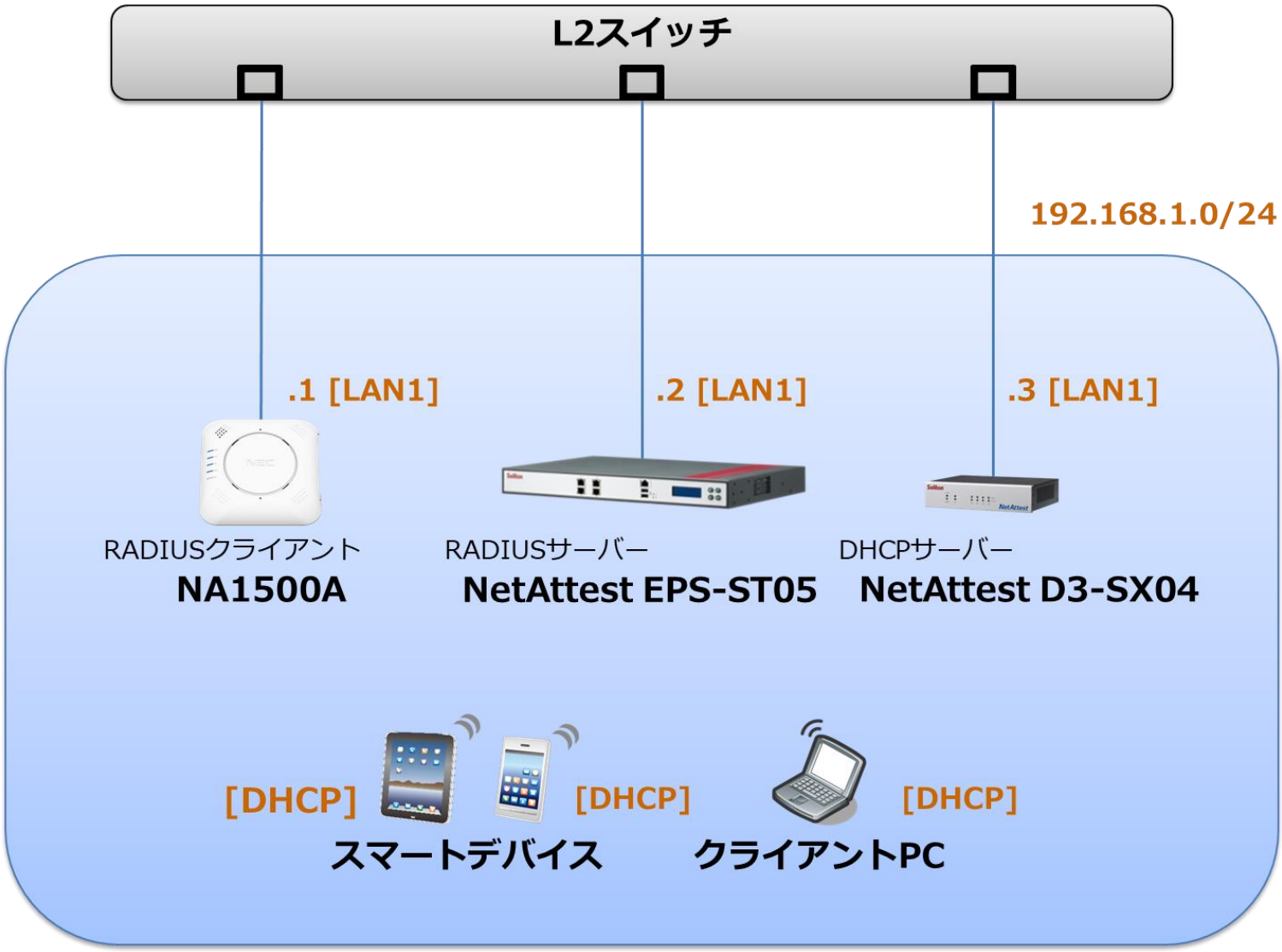
目次

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	4.10.4
NA1500A	NEC プラットフォームズ	RADIUS クライアント (無線アクセスポイント)	1.0.26
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 Smart Phone)	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	4.2.17

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
NA1500A	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。

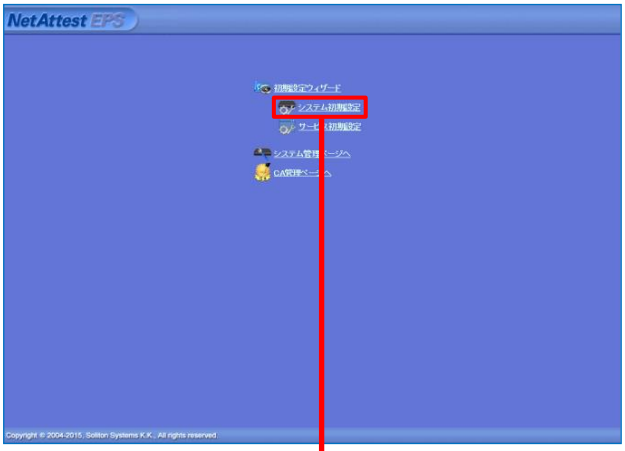
下記のような流れでセットアップを行います。

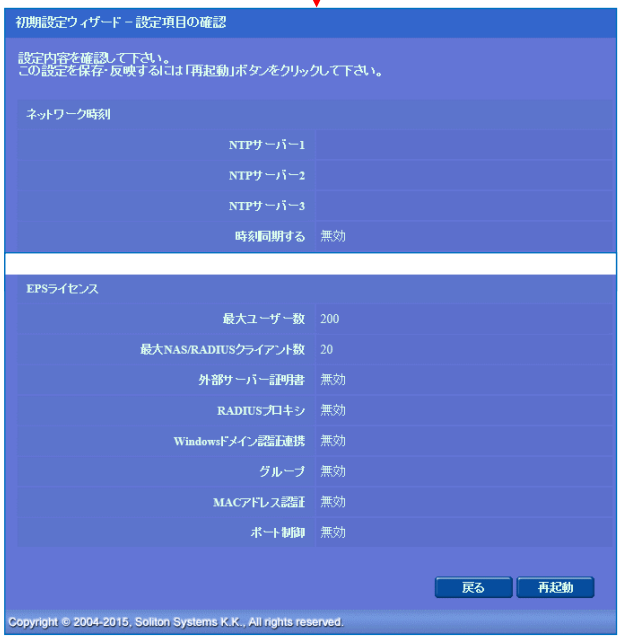
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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





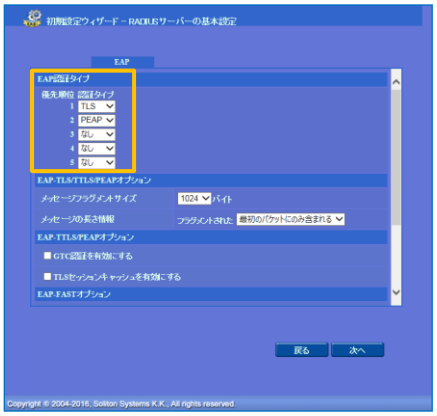
項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

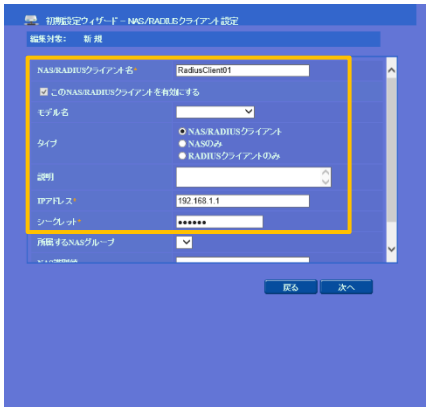
サービス初期設定ウィザードを実行します。

- 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

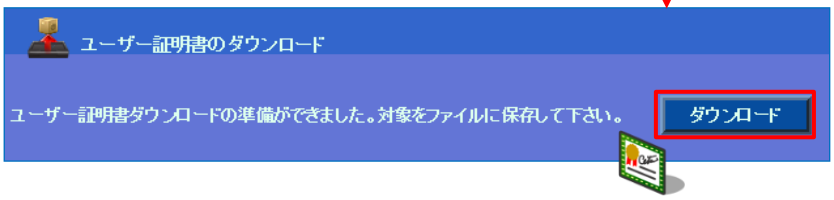
NetAttest EPS の管理画面より、認証ユーザーの登録を行います。[ユーザー]-[ユーザー一覧]から、「追加」ボタンでユーザー登録を行います。

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

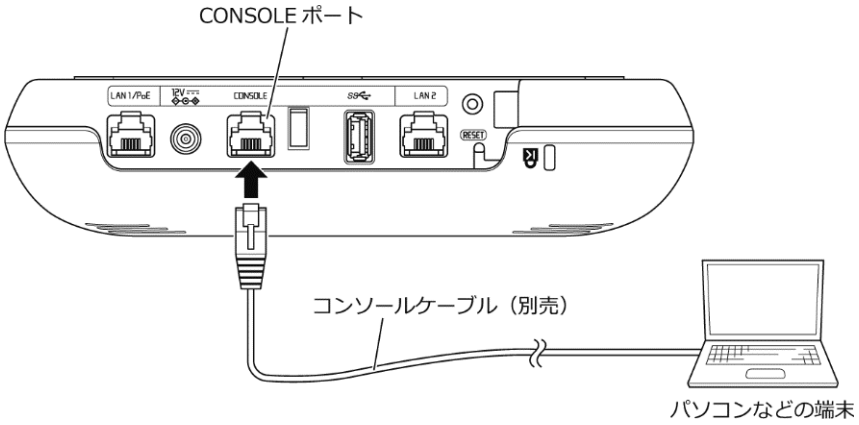


3. NA1500A の設定

3-1 ローカルコンソールによる設定

1) NA1500A の電源を切ります。

2) NA1500A の CONSOLE ポートとパソコンなどの端末を、コンソールケーブル ZB-NA-CON1 (別売)で接続してください。



※パソコンなどの端末側で USB 端子を使用する場合は、市販の USB-RS232C 変換ケーブルを使用してください。

3) パソコンなどの端末の電源を入れてください。

4) パソコンなどの端末で、ターミナルソフトを下記のように設定変更します。

通信速度	: 9600 boud
データ長	: 8bit
パリティ	: なし
ストップビット	: 1bit
フロー制御	: なし

※あらかじめ作成したコンフィグの流し込みを行う場合は、取りこぼしを防ぐため、ターミナルソフトを送信遅延(1 ミリ秒/字以上)に設定してください。

5) ターミナルソフトから NA1500A にアクセスします。
※NA1500A に接続しているシリアルポート番号を指定します。(例) 接続方法：COM1

6) NA1500A の電源を入れます。
※しばらく待つと、「login:」と表示されます。

7) NA1500A にログインします。

管理者権限ユーザー名(login)と管理者権限パスワード(Password)の初期値は、

管理者権限ユーザー名(login) ：config

管理者権限パスワード(Password) ：config

です。はじめて NA1500A にログインする場合は、管理者権限ユーザー名(login)と管理者権限パスワード(Password)の変更が必要です。

ログインに成功すると、ターミナルソフト上で、「AP#」と表示されます。

8) 「config」コマンドを入力し、グローバルコンフィグレーションモードに入ります。

グローバルコンフィグレーションモードでは、下記のとおり、プロンプトが変化します

```
AP# config
Enter configuration commands, one per line. End with CTRL+Z.
AP(config)#
```

9) 以下の設定を入力します。

```
AP(config)# interface vlan u
AP(config-vlan u)# ip address 192.168.1.1/24
AP(config-vlan u)# ip route 192.168.1.254
AP(config-vlan u)# vlan enable
AP(config-vlan u)# exit

AP(config)# ssid SolitonLab
AP(config-ssid SolitonLab)# max-associations 50
AP(config-ssid SolitonLab)# vlan u
AP(config-ssid SolitonLab)# encryption mode wpa2 aes
AP(config-ssid SolitonLab)# authentication type dot1x
AP(config-ssid SolitonLab)# radius host ip 192.168.1.2 acct-port 1813 auth-port 1812
                                retransmit 3 timeout 3 key 0 secret
AP(config-ssid SolitonLab)# radio-device both
AP(config-ssid SolitonLab)# hide bssid
AP(config-ssid SolitonLab)# enable-ssid
AP(config-ssid SolitonLab)# exit
AP(config)# radio-enable both
AP(config)# write memory
```

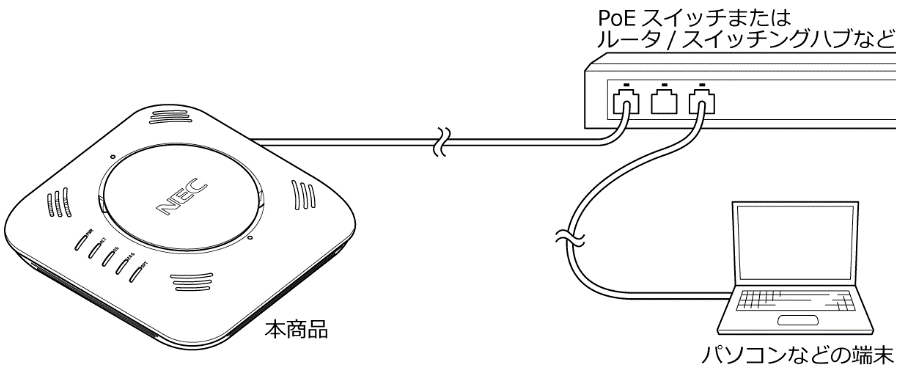
10) 「exit」コマンドを入力し、グローバルコンフィグレーションモードに抜け出ます。

その後、再度「exit」コマンドを入力し、NA1500A よりログアウトします。

```
AP(config)# exit
AP#exit
```

3-2 SSH/Telnet 接続による設定(CLI)

1) NA1500A が有線 LAN 接続している LAN 上にパソコンなどの端末を接続します。



2) パソコンなどの端末で、ターミナルソフトを下記のように設定します。

IP アドレス	あらかじめローカルコンソールで設定した固定 IP アドレスまたは DHCP サーバーから割り振られた IP アドレスを指定してください	
TCP ポート	SSH の場合	: 22
	telnet の場合	: 23

3) ターミナルソフトから NA1500A にアクセスします。

4) NA1500A にログインします。

※管理者権限ユーザー名(login)と管理者権限パスワード(Password)の初期値は、

管理者権限ユーザー名(login) : config

管理者権限パスワード(Password) : config

です。はじめて NA1500A にログインする場合は、管理者権限ユーザー名(login)と管理者権限パスワード(Password)の変更が必要です。

ログインに成功すると、ターミナルソフト上で「AP#」と表示されます。

※以降、コマンド入力がないまま約 5 分(初期値)経過すると強制的にログアウトされます。

5) 以降は、3-1 章の 8)と同様に設定します。

また、ＰＣ上で動くＧＵＩ設定ツールもご用意しております。本ツールのダウンロードとご使用方法については、ＮＥＣプラットフォームズの NA1500A ホームページまでアクセスしてください。

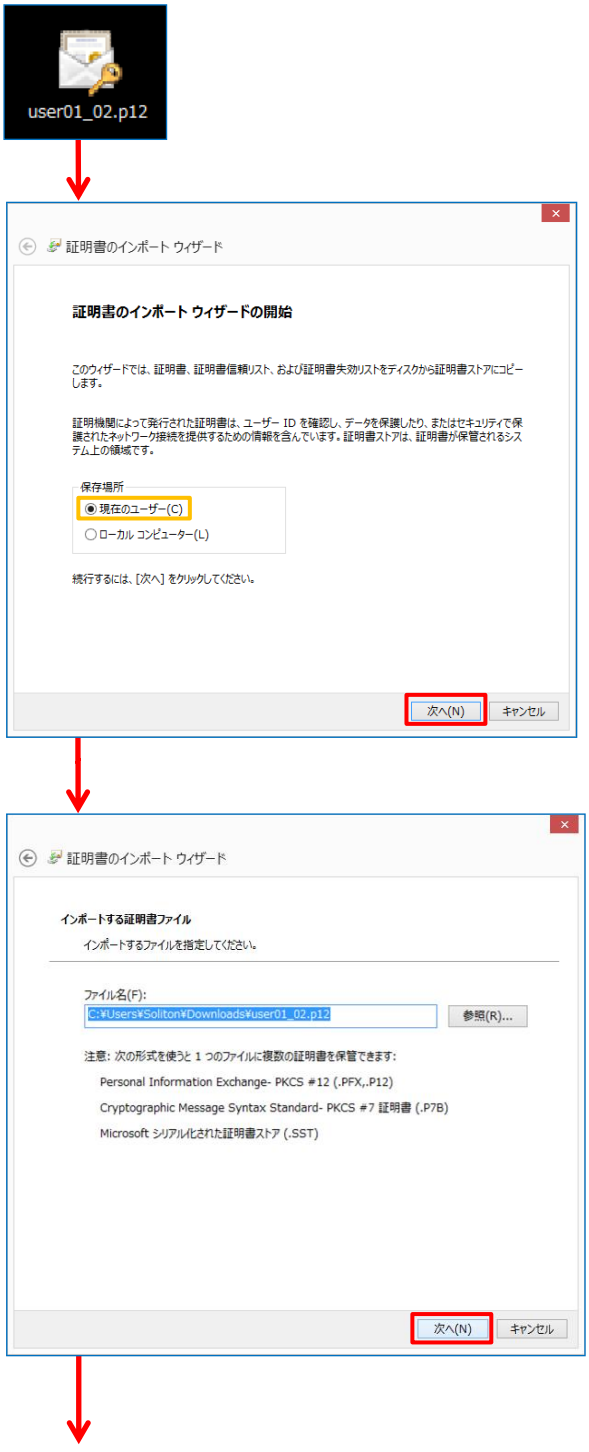
https://www.necplatforms.co.jp/product/na1500a/

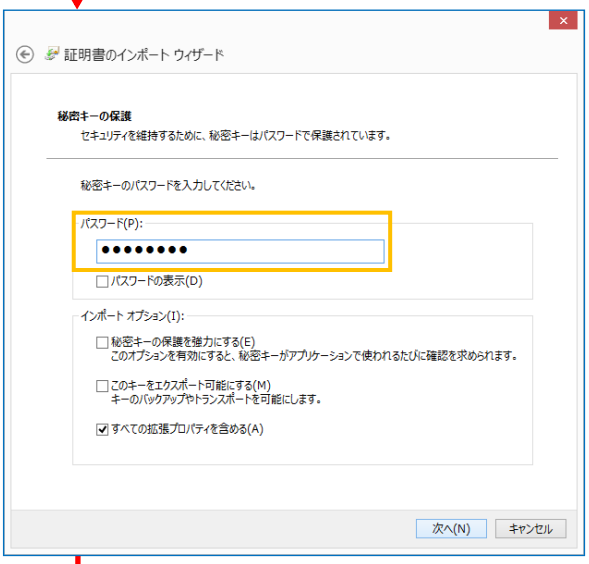
4. EAP-TLS 認証でのクライアント設定

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

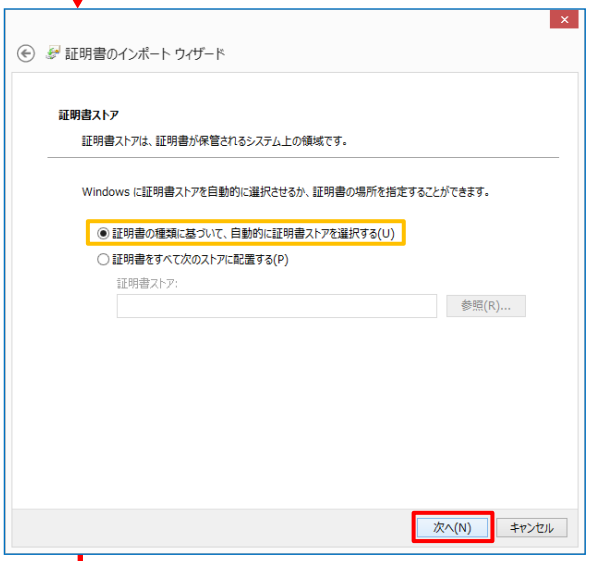
PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書(user01_02.p12)をダブルクリックすると、証明書インポートウィザードが実行されます。

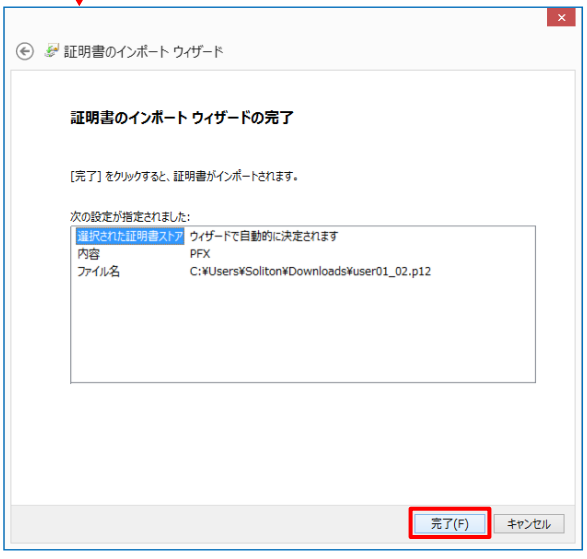




【パスワード】

「2-4 ユーザーの登録」で設定したパスワードを入力

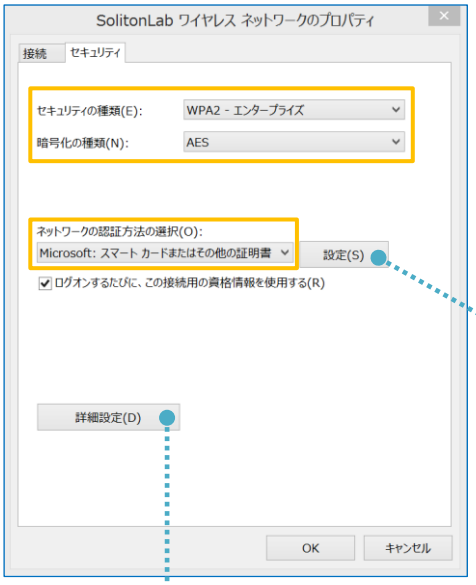




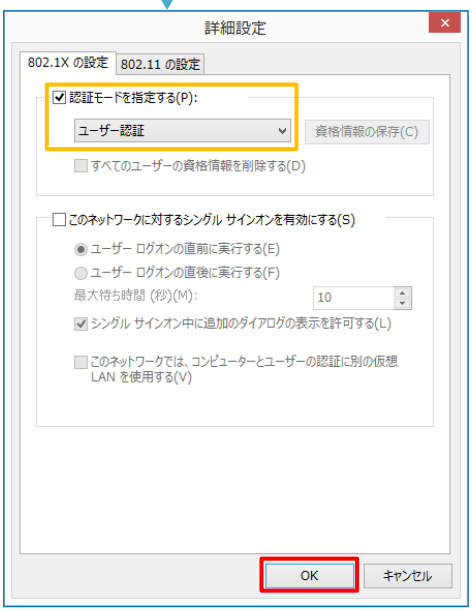
4-1-2 サプリカント設定

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)

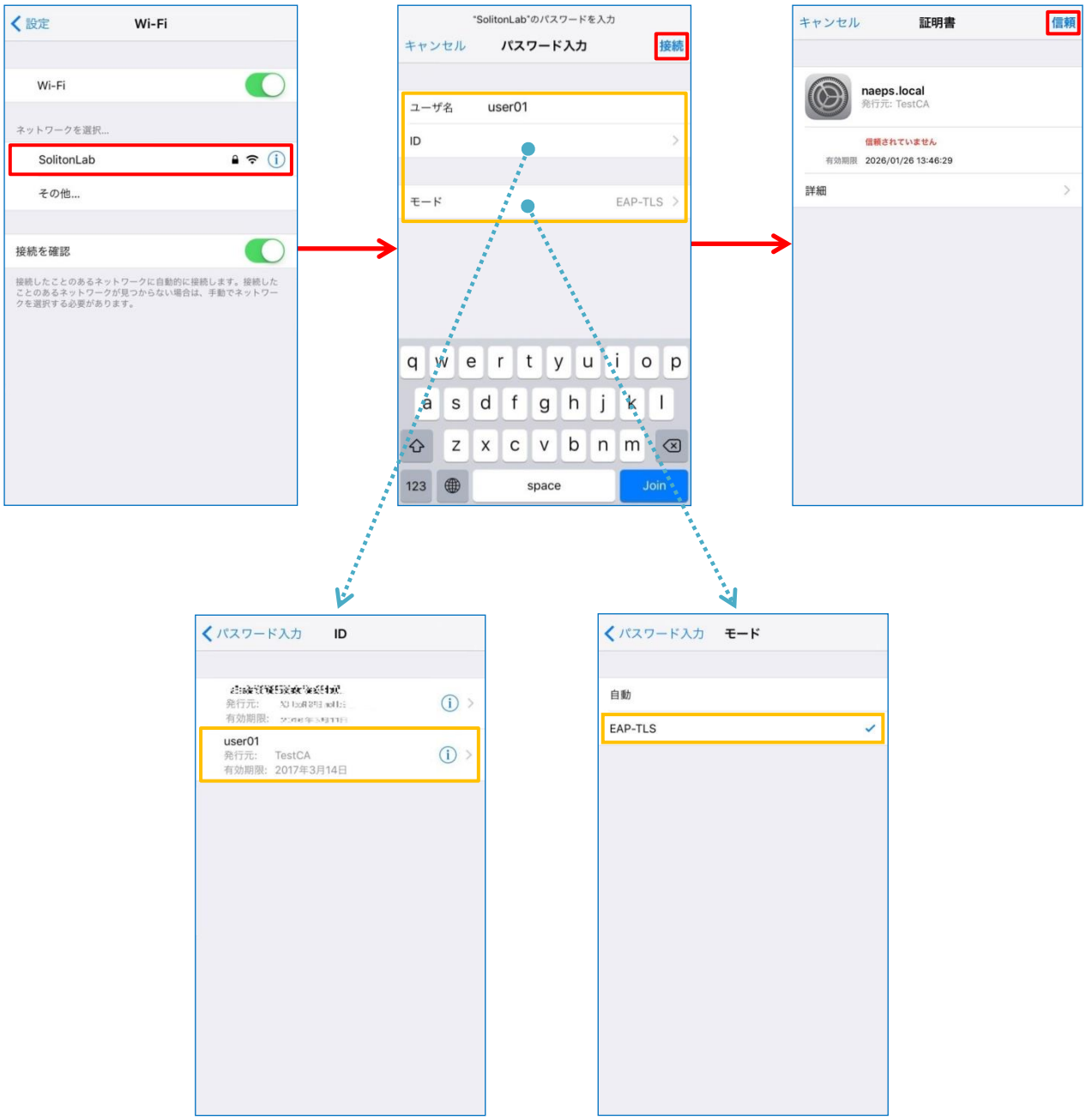
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

NA1500A 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

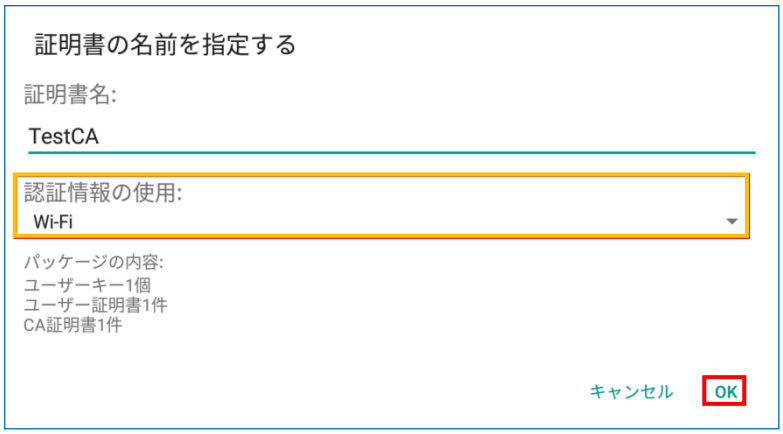
4-3-1 クライアント証明書のインポート

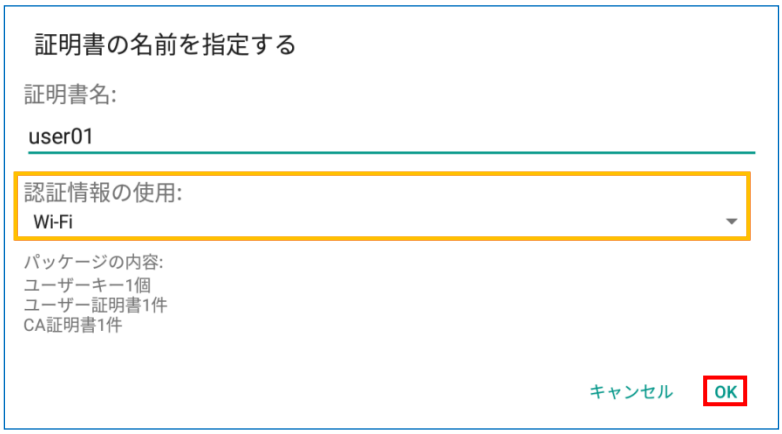
NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

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。

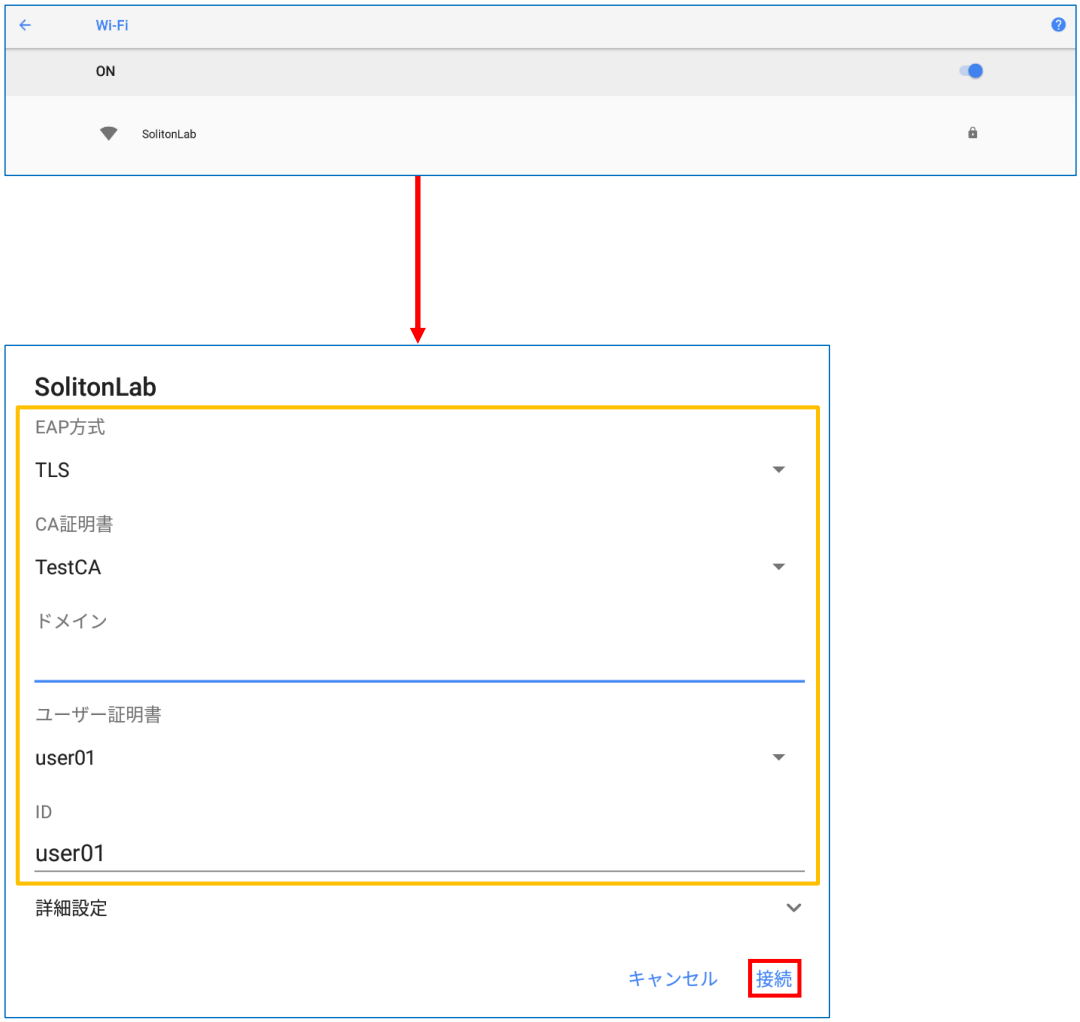
Android 8.1.0 では証明書インポート時に用途別に証明書ストアが選択できますが、本書では無線 LAN への接続を行うため「Wi-Fi」を選択しています。





4-3-2 サプリカント設定

NA1500A 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。



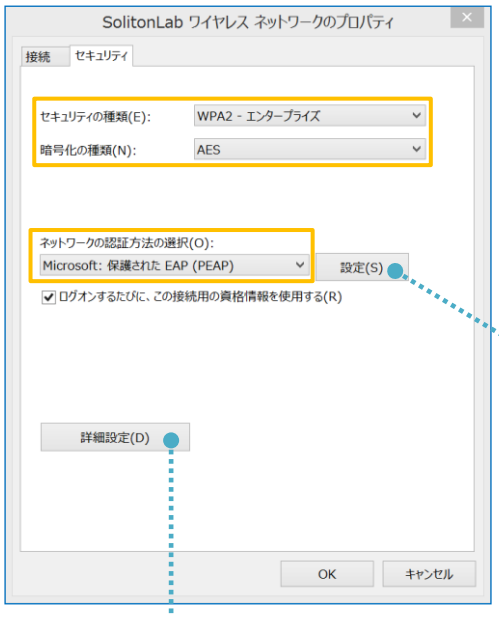
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

5. EAP-PEAP 認証でのクライアント設定

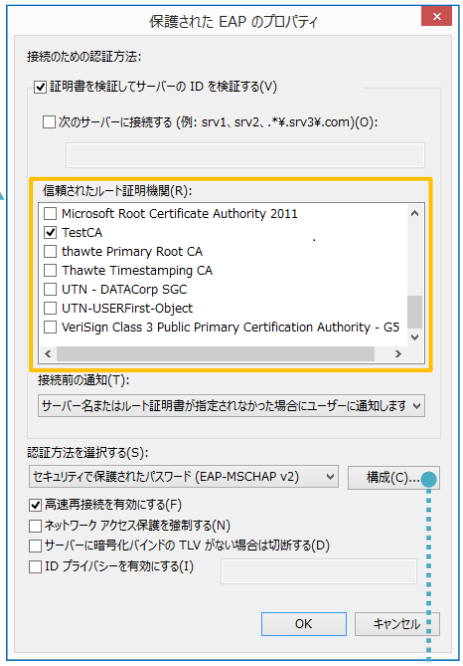
5-1 Windows 10 での EAP-PEAP 認証

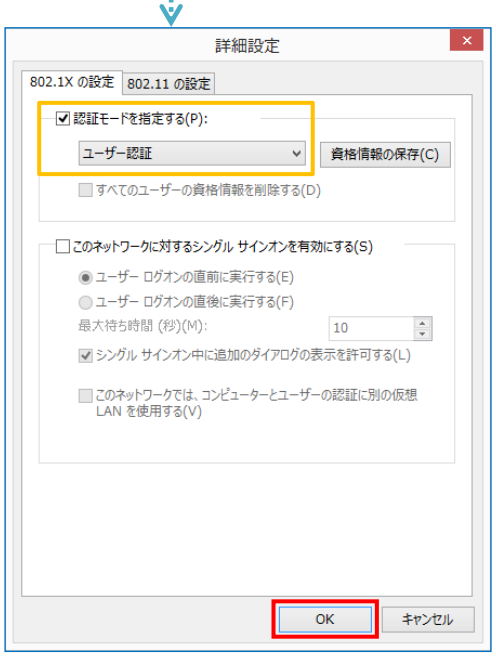
5-1-1 Windows 10 のサプリカント設定

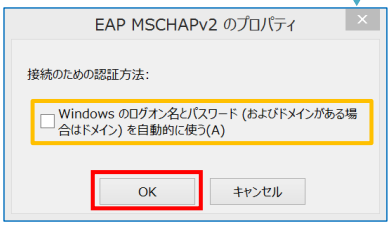
[ワイヤレスネットワークのプロパティ] の「セキュリティ」タブから以下の設定を行います。



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

NA1500A 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。

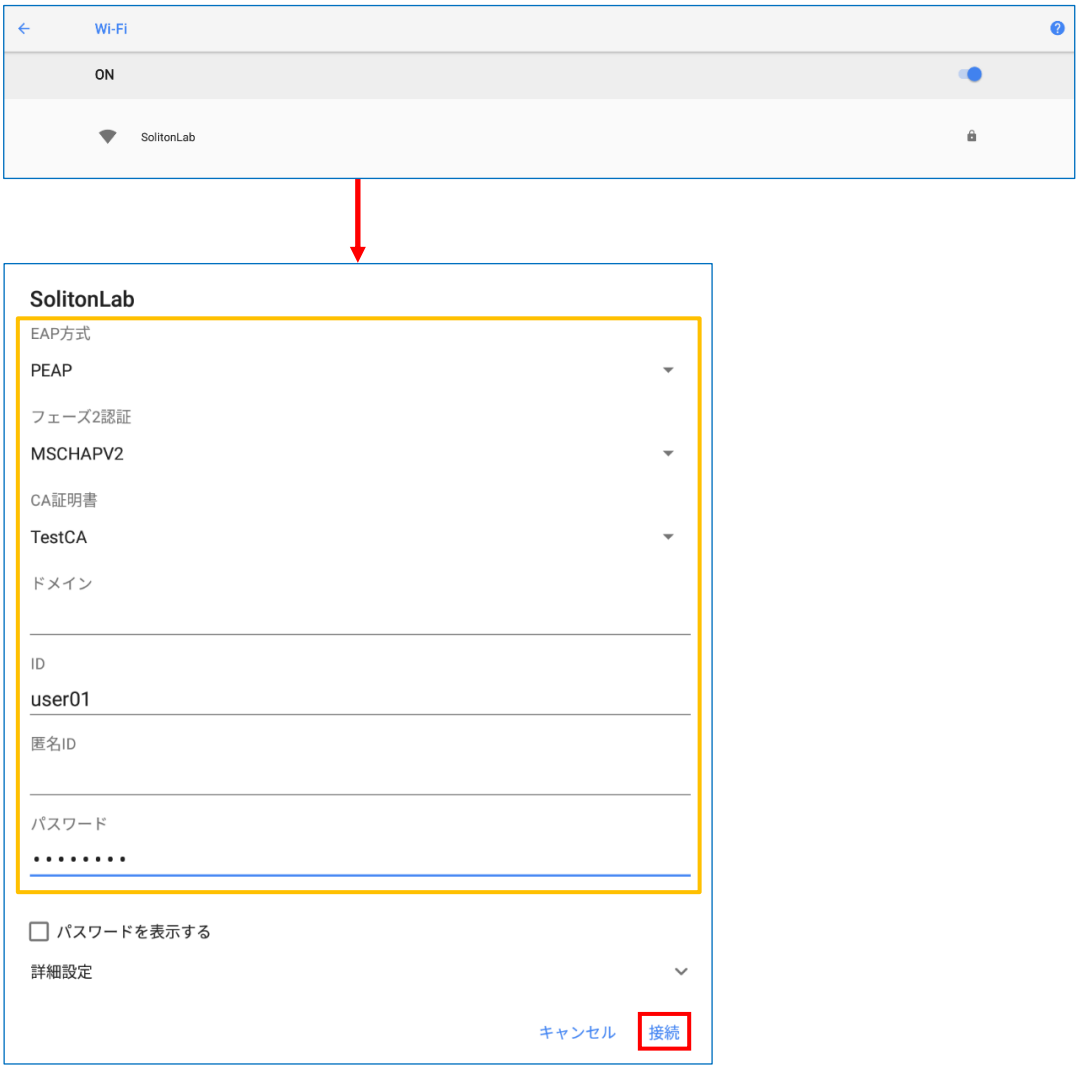
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し接続します。

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

NA1500A 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

NA1500A のログを表示するには、3-1 章、3-2 章と同様に NA1500A にログインし、「config」コマンドを入力しグローバルコンフィグレーションモードに入ります。このモードで「show associations」を入力します。

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)
NA1500A	AP(config)# show associations [radio0] [radio1] association 1 MAC Address.. 40:a3:cc:32:10:a4 SSID..... SolitonLab Mode..... 11NG_HT20 Security..... WPA2 (AES) RSSI..... 56 Associated..... 00:02:58 AP(config)#

6-2 EAP-PEAP 認証

EAP-PEAP 認証が成功した場合のログ表示例

NA1500A のログを表示するには、3-1 章、3-2 章と同様に NA1500A にログインし、「config」コマンドを入力しグローバルコンフィグレーションモードに入ります。このモードで「show associations」を入力します。

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)
NA1500A	AP(config)# show associations [radio0] [radio1] association 1 MAC Address.. 40:a3:cc:32:10:a4 SSID..... SolitonLab Mode..... 11NG_HT20 Security..... WPA2 (AES) RSSI..... 56 Associated..... 00:02:58 AP(config)#

改訂履歴

日付	版	改訂内容
2018/12/11	1.0	初版作成