

NetAttest EPS

認証連携設定例

【連携機器】 NEC プラットフォームズ NA1000W/NA1000A

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

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、NEC プラットフォームズ社製無線 LAN アクセスポイント NA1000W/NA1000A 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 NA1000W/NA1000A 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.....	5
1-1 構成図	5
1-2 環境	6
1-2-1 機器	6
1-2-2 認証方式	6
1-2-3 ネットワーク設定	6
2. NetAttest EPS の設定	7
2-1 初期設定ウィザードの実行	7
2-2 システム初期設定ウィザードの実行	8
2-3 サービス初期設定ウィザードの実行	9
2-4 ユーザーの登録.....	10
2-5 クライアント証明書の発行	11
3. NA1000W/NA1000A の設定	12
3-1 設定の流れ	12
3-2 動作モードの変更.....	13
3-3 IP アドレスの設定	14
3-4 SSID の設定	15
3-5 RADIUS 認証の設定	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

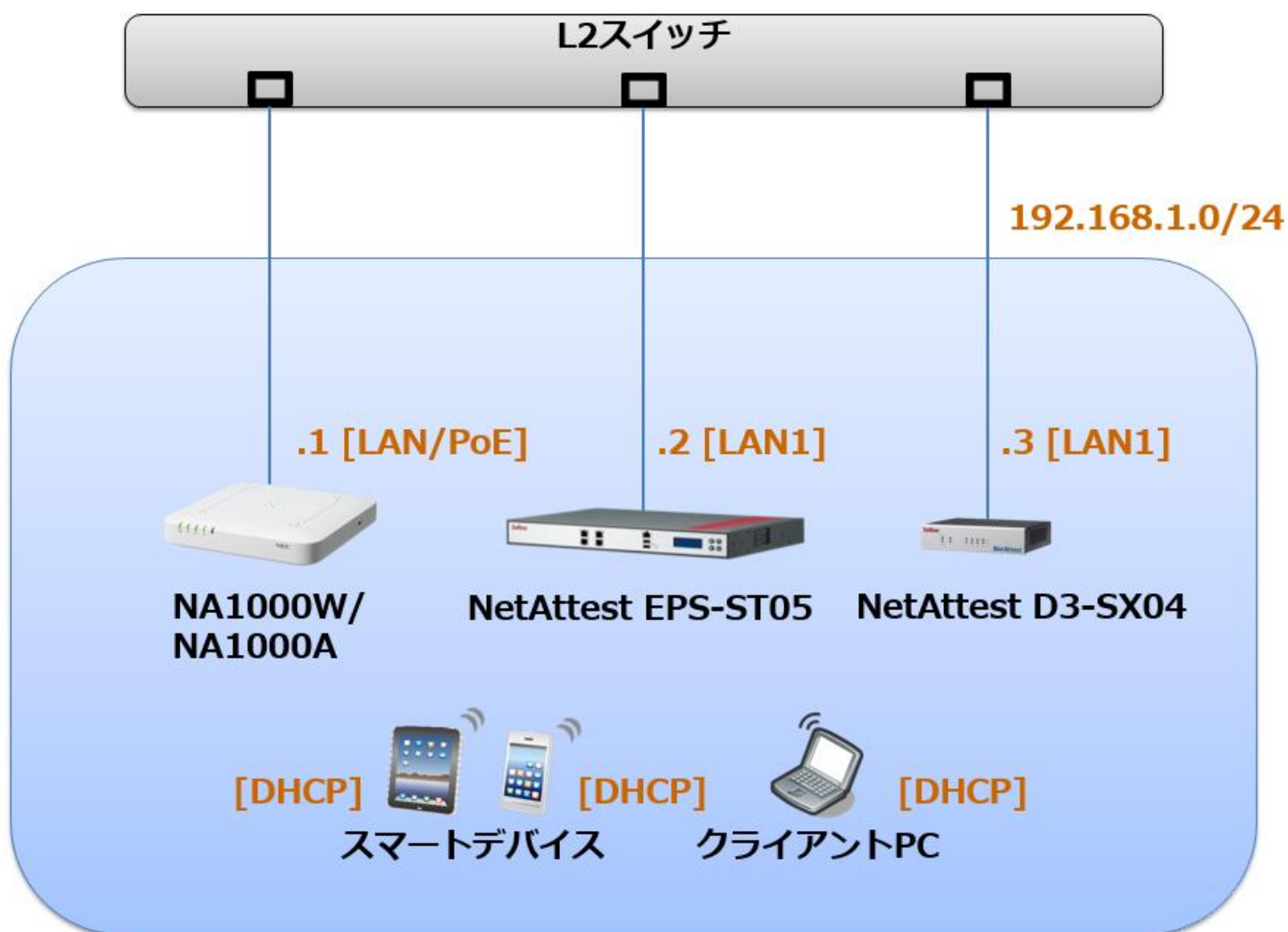
5-1 Windows 10 のサブリカント設定	24
5-2 iOS(iPad Air 2)のサブリカント設定.....	25
5-3 Android(Pixel C)のサブリカント設定.....	26

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	4.8.13
NA1000W/NA1000A	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)	ファームウェア Ver 1.2 設定ツール Ver 2.00_019
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)	10.3.3
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
NA1000W/NA1000A	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。

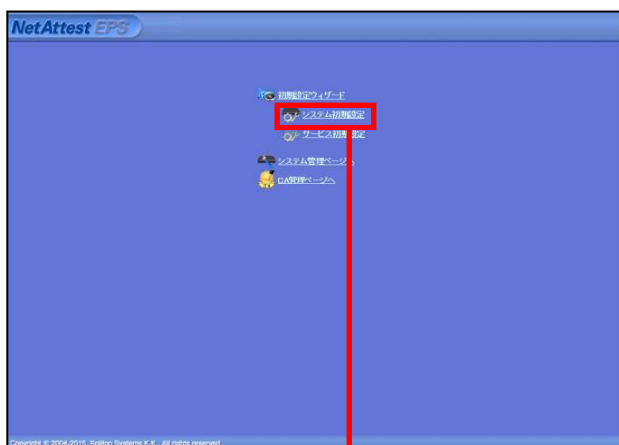
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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.example.com

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	500
外部サーバー証明書	有効
RADIUSプロキシ	有効
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 © 2004-2017, 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	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。

NetAttest EPS ユーザー登録画面のスクリーンショット。左側のメニューで「ユーザー」を選択し、「ユーザー一覧」をクリックします。右側の「追加」ボタンをクリックすると、ユーザー登録のダイアログが表示されます。

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

ダイアログ内の「OK」ボタンをクリックすると、ユーザーが登録されます。登録後、ユーザー一覧画面に「user01」が追加されます。

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)



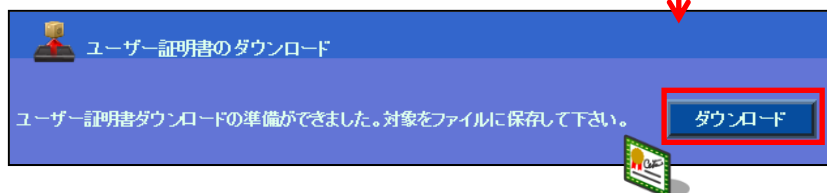
NetAttest EPS 管理画面の「ユーザー一覧」画面。左側のメニューで「ユーザー」>「ユーザー一覧」が選択されている。中央にはユーザー一覧のテーブルがあり、2つのユーザー（test user, user01）がリストアップされている。右側の「発行」ボタンが赤枠で囲まれている。

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



「ユーザー証明書のダウンロード」画面。編集対象は user01。基本情報、詳細情報、証明書情報、証明書ファイルオプションが設定されている。証明書情報の有効期限が 365 日と設定されている。証明書ファイルオプションで「PKCS#12ファイルに証明機関の証明書を含める」がチェックされている。右下の「発行」ボタンが赤枠で囲まれている。

項目	値
証明書有効期限	365 日
PKCS#12 ファイルに証明機関の・・・	チェック有り



「ユーザー証明書のダウンロード」画面。メッセージが表示されている：「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。」。右下の「ダウンロード」ボタンが赤枠で囲まれている。

3. NA1000W/NA1000A の設定

3-1 設定の流れ

NECプラットフォームズ社製 無線 LAN アクセスポイント NA1000W/NA1000A を設定するためには、専用の設定ツール、管理コンソールソフトウェアを利用する方法などが存在しますが、本書では、設定ツールから各種設定を実施する方法を紹介します。

下記の流れで設定を行います。

1. 動作モードの変更
2. IP アドレスの設定
3. SSID の設定
4. RADIUS 認証の設定

3-2 動作モードの変更

設定ツールから NA1000W/NA1000A にログインし、動作モードを自律型 AP モードに変更します。【ログイン】押下後、自律型 AP モードへの切り替えを促す表示が出ますので、【はい】を選択し、自律型 AP モードに変更します。その後、NA1000W/NA1000A が再起動します。

※初回ログイン時の接続先 IP アドレス、パスワードは、設定ツールの取扱説明書をご参照ください。



NA1000W/NA1000A 設定ツール Ver2.00_019

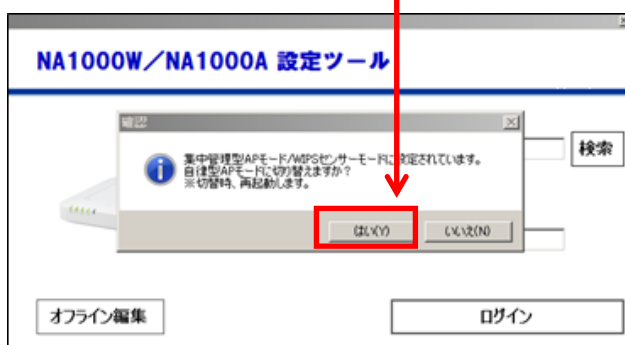
接続先IPアドレス: xxx.xxx.xxx.xxx 検索

ユーザー名: config

パスワード: *****

オフライン編集 ログイン

項目	値
接続先 IP アドレス	設定ツールの取扱説明書を参照
パスワード	設定ツールの取扱説明書を参照



NA1000W/NA1000A 設定ツール

集中管理型APモード/MSPSセンサーモードに設定されています。
自律型APモードに切り替えますか？
※切替時、再起動します。

はい(Yes) いいえ(No)

オフライン編集 ログイン

3-3 IP アドレスの設定

再度、設定ツールから NA1000W/NA1000A にログインし、IP アドレスの設定を行います。
【基本設定】の IP アドレス、サブネットマスク、デフォルトゲートウェイを入力します。



NA1000W/NA1000A 設定ツール Ver2.00_019

接続先IPアドレス: xxx.xxx.xxx.xxx 検索

ユーザー名: config

パスワード: *****

オフライン編集 ログイン



NA1000W/NA1000A 設定ツール Ver2.00_019

LOAD SAVE

基本設定 無線LAN設定 メンテナンス モード切替

動作モード 自定義APモード

※ IP直接指定 ○ DHCP

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

プライマリDNS: . . .

セカンダリDNS: . . .

DNSサフィックス:

管理 VLAN ID 0

項目	値
IP 直接指定 / DHCP	IP 直接指定
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

3-4 SSID の設定

【無線 LAN 設定】を押し、SSID などの設定画面にいきます。

【編集】を押下し、SSID 名、動作周波数、セキュリティモード、認証方式を設定します。

NA1000W/NA1000A 設定ツール

基本設定 | 無線LAN設定 | メンテナンス | モード切替

無線LAN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
 プライマリDNS:
 セカンダリDNS:
 DNSサーバアドレス:
 マネージメント VLAN ID: 0

Ver2.00.019

NA1000W/NA1000A 設定ツール

基本設定 | 無線LAN設定 | メンテナンス | モード切替

無線LAN設定

2.4GHz 周波数帯域: IEEE802.11n
 チャンネル幅: 20/40MHz
 動作チャンネル: 1
 5GHz 周波数帯域: IEEE802.11ac
 チャンネル幅: 20/40/80MHz
 動作チャンネル: 36 (W52)

No	状態	SSID	使用周波数	セキュリティモード	編集	クリア
01	無効				編集	クリア
02	無効				編集	クリア
03	無効				編集	クリア
04	無効				編集	クリア
05	無効				編集	クリア
06	無効				編集	クリア
07	無効				編集	クリア
08	無効				編集	クリア
09	無効				編集	クリア
10	無効				編集	クリア
11	無効				編集	クリア
12	無効				編集	クリア
13	無効				編集	クリア
14	無効				編集	クリア
15	無効				編集	クリア
16	無効				編集	クリア

Ver2.00.019

NA1000W/NA1000A 設定ツール

基本設定 | 無線LAN設定 | メンテナンス | モード切替

無線LAN設定

2.4GHz 周波数帯域: IEEE802.11n
 チャンネル幅: 20/40MHz
 動作チャンネル: 1
 5GHz 周波数帯域: IEEE802.11ac
 チャンネル幅: 20/40/80MHz
 動作チャンネル: 36 (W52)

SSID: SolitonLab
 セキュリティモード: WPA2
 認証方式: IEEE802.1X
 高度な設定:
 確定:
 キャンセル:
 SSID_PROFILE_ID: 1

Ver2.00.019

項目	値
SSID	SolitonLab
2.4GHz	チェック有り
5GHz	チェック有り
セキュリティモード	WPA2 を選択
認証方式	IEEE802.1X を選択

3-5 RADIUS 認証の設定

前ページの編集画面にて【RADIUS 認証設定】を押し、認証設定を行います。

NAS ID、RADIUS 認証サーバーの IP アドレス、ポート番号、共有鍵を設定します。

最後に【SAVE】を押して設定完了となります。その後、NA1000W/NA1000A が再起動します。



項目	値
NAS ID	NA1000 の MAC アドレス -SolitonLab (任意入力)
RADIUS 認証サーバー IP アドレス	192.168.1.2
ポート番号	1812
共有鍵	secret

【設定】押下後、【SAVE】を押します。

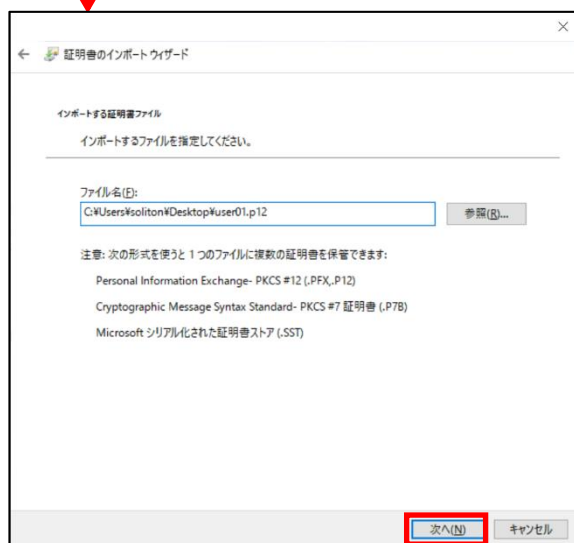
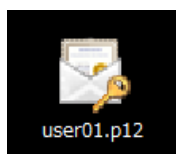


4. EAP-TLS 認証でのクライアント設定

4-1 Windows 10 での EAP-TLS 認証

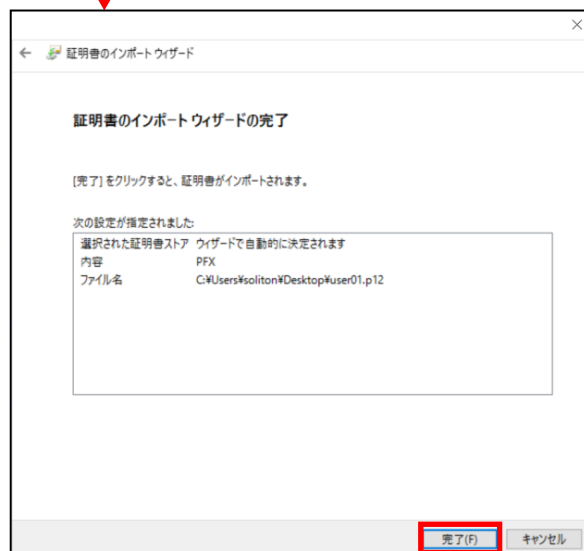
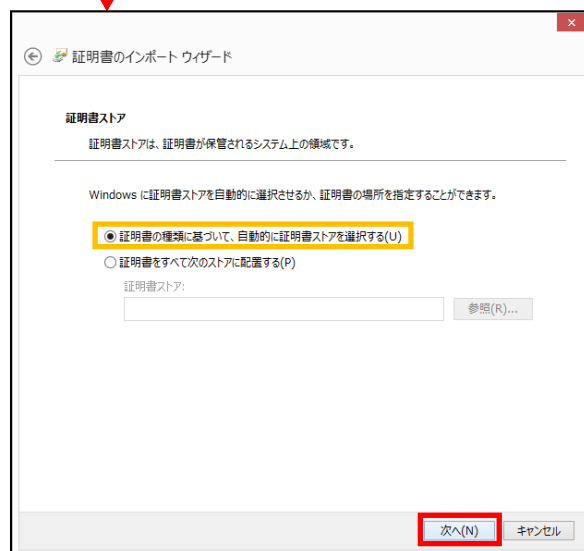
4-1-1 クライアント証明書のインポート

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.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。





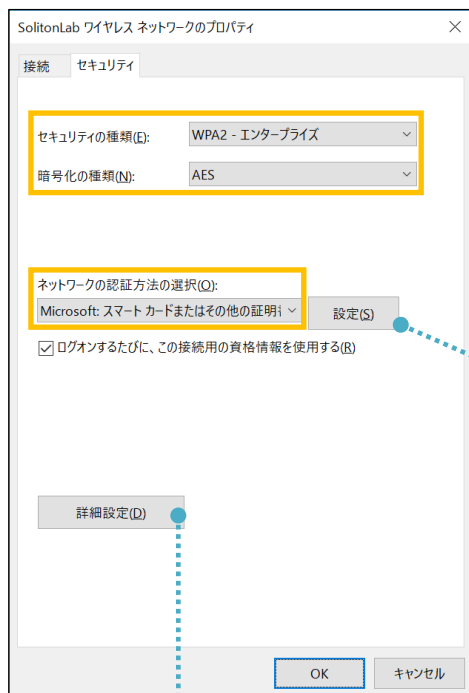
【パスワード】
NetAttest EPS で証明書を
発行した際に設定したパスワードを入力



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。

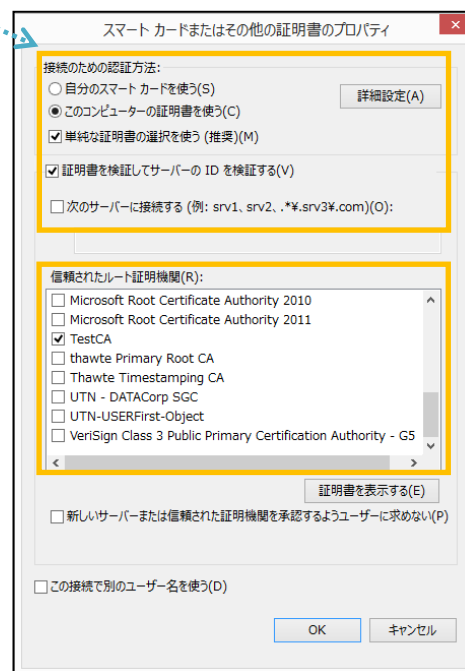
[ワイヤレスネットワークのプロパティ] の「セキュリティ」タブから以下の設定を行います。



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(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。

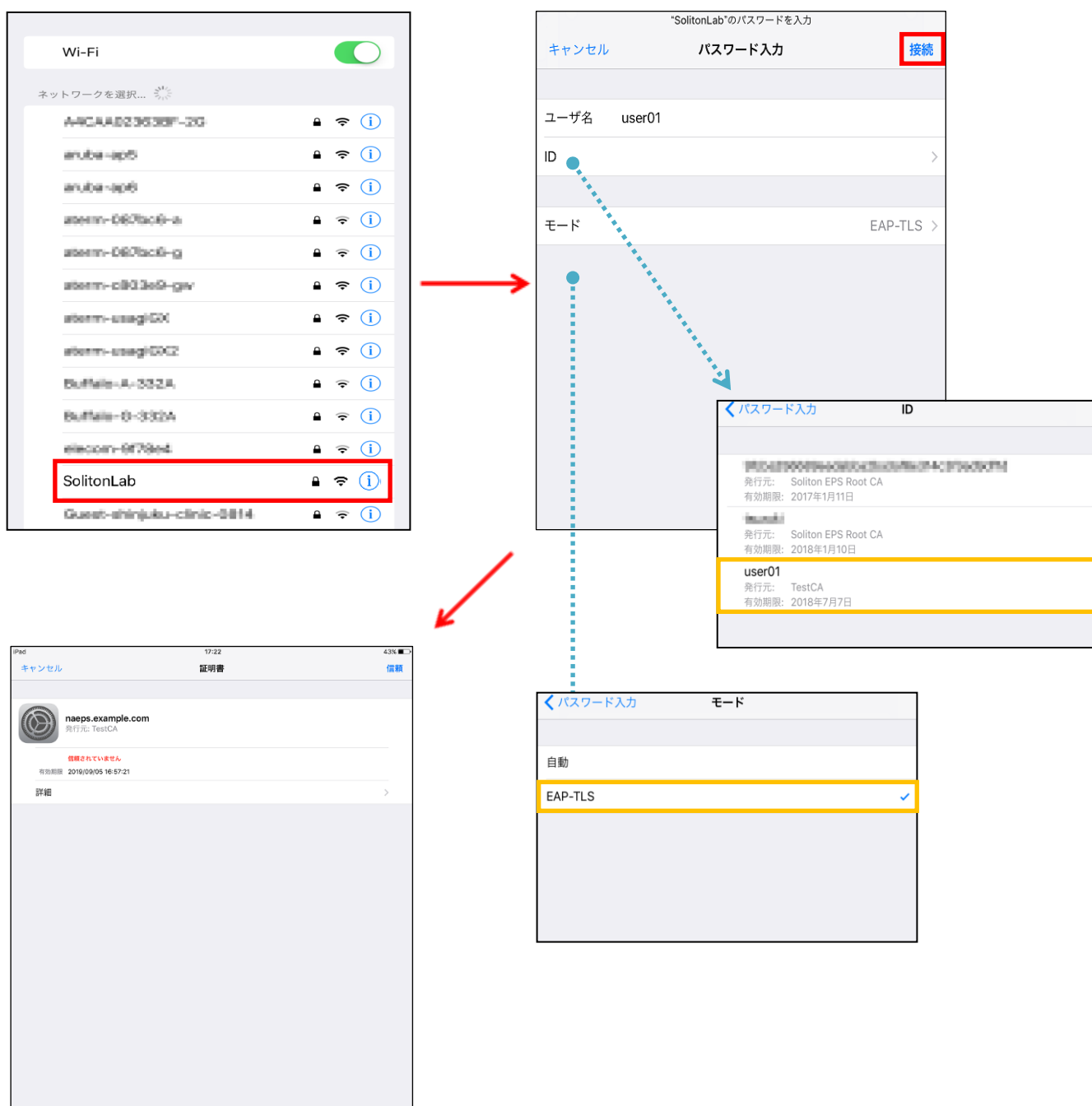
4-2-2 サプリカント設定

NA1000W/NA1000A 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「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:
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

NA1000W/NA1000A 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。

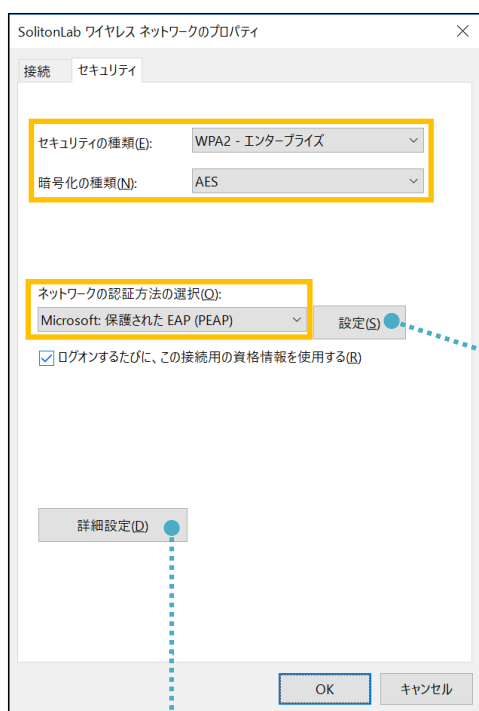


項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

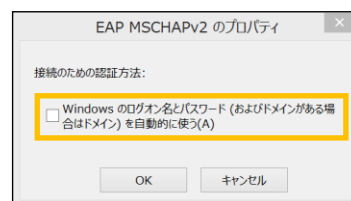
5. EAP-PEAP 認証でのクライアント設定

5-1 Windows 10 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

NA1000W/NA1000A 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 involves three main steps on an iPad:

- Wi-Fi Selection:** In the Wi-Fi settings, the network 'SolitonLab' is selected from the list of available networks.
- Password Entry:** A screen titled 'パスワード入力' (Password Entry) appears. The username 'user01' and password 'password' are entered. The mode is set to '自動' (Automatic).
- Certificate Trust:** A screen titled '証明書' (Certificate) appears, showing a warning that the certificate is not trusted. The user is prompted to trust the certificate for 'naeps.example.com'.

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

NA1000W/NA1000A 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。



↓

SolitonLab

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 接続

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

改訂履歴

日付	版	改訂内容
2017/09/20	1.0	初版作成
2019/03/19	2.0	ロゴ画像差し替え