

NetAttest EPS

認証連携設定例

【連携機器】ゼブラ・テクノロジーズ AP7532

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

Rev1.1

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、ゼブラ・テクノロジーズ社製無線アクセスポイント AP7532 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。

なお、本書は FXC 株式会社の協力により作成されております。

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 AP7532 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. AP7532 の設定.....	13
3-1 アクセスポイントの設定.....	13
3-2 RADIUS の設定.....	15
4. EAP-TLS 認証でのクライアント設定.....	17
4-1 Windows 8.1 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(iPhone 6)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(Google Nexus 7)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 8.1 のサプリカント設定.....	24
5-2 iOS(iPhone 6)のサプリカント設定.....	25
5-3 Android(Google Nexus 7)のサプリカント設定.....	26

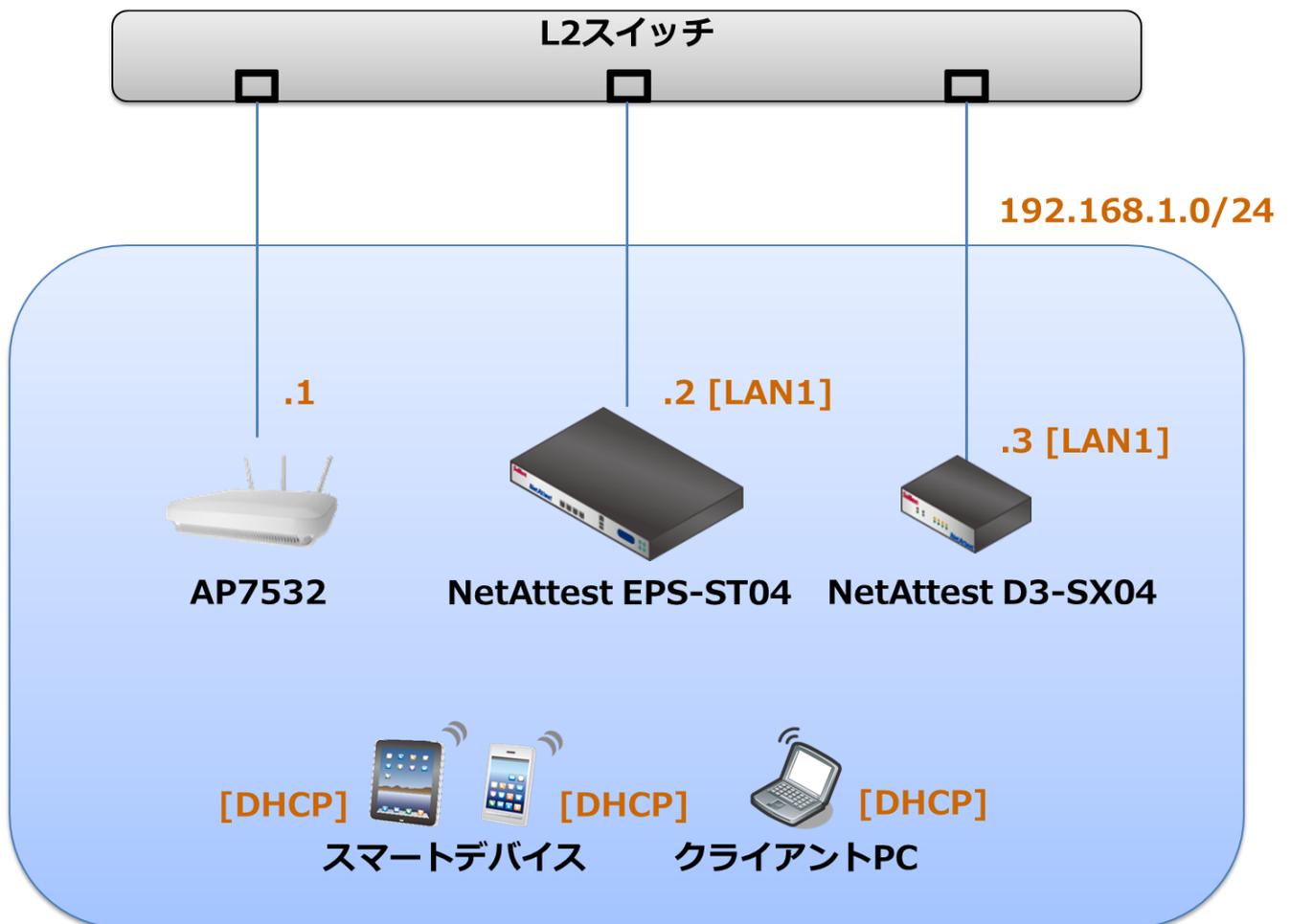
6. 動作確認結果	27
6-1 EAP-TLS 認証	27
6-2 EAP-PEAP(MS-CHAP V2)認証	27

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 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-ST04	Soliton Systems	RADIUS/CA サーバー	4.8.5
AP7532	ゼブラ・テクノロジーズ	RADIUS クライアント (無線アクセスポイント)	5.8.1.0-012R
Surface	MicroSoft	802.1X クライアント (Client PC)	Windows 8.1 64bit Windows 標準サブリカント
iPhone 6	Apple	802.1X クライアント (Client SmartPhone)	9.3.1
Google Nexus 7	ASUS	802.1X クライアント (Client Tablet)	5.1
NetAttest D3-SX04	Soliton Systems	DHCP/DNS サーバー	4.2.2

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-ST04	192.168.1.2/24	UDP 1812	secret
AP7532	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。

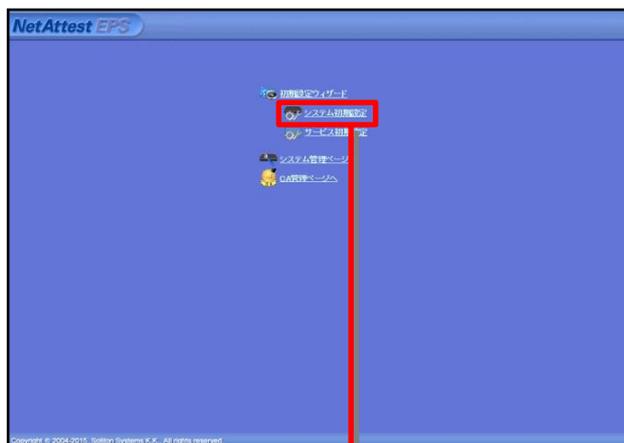
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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
- 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

初期設定ウィザード - CA構築

CA種別選択
CA種別選択: ルートCA

CA秘密鍵
 内部で新しい鍵を生成する
公開鍵方式: RSA
鍵長: 2048
 外部HSMデバイスの鍵を使用する

要求の署名
要求署名アルゴリズム: SHA256

CA情報
CA名(必須): TestCA
国名: 日本
郵便府県名: Tokyo
市区町村名: Shinjuku
会社名(組織名): Soliton Systems
部署名:
E-mailアドレス:
CA署名設定
署名アルゴリズム: SHA256

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

項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA

初期設定ウィザード - RADIUSサーバーの基本設定

EAP

EAP認証タイプ
優先順位: 認証タイプ
1: TLS
2: PEAP
なし
なし
なし

EAP-TLS/TLS/PEAPオプション
メッセージフラグメントサイズ: 1024 バイト
メッセージの長さ情報: フラグメントされ、各フラグメントにのみ含まれる

EAP-TLS/PEAPオプション
 GTC認証を有効にする
 TLSセッションキャッチャーを有効にする

EAP-EASTオプション

戻る 次へ

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

項目	値
EAP 認証タイプ	
1	TLS
2	PEAP

初期設定ウィザード - NAS/RADIUSクライアント設定

編集対象: 新規

NAS/RADIUSクライアント名: RadiusClient01

このNAS/RADIUSクライアントを有効にする

タイプ
 NAS/RADIUSクライアント
 NASのみ
 RADIUSクライアントのみ

説明:
IPアドレス: 192.168.1.1
シークレット: *****
NAS識別値:

戻る 次へ

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

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 NetAttest EPS management interface. The 'ユーザー一覧' (User List) section is active, displaying a table with one user: 'test user' with ID 'test'. A red box highlights the '追加' (Add) button. An inset shows the 'ユーザー設定' (User Settings) dialog box for adding a new user. The dialog has fields for '姓' (Last Name) 'user01', '名' (First Name), 'E-Mail', 'ユーザーID' (User ID) 'user01', 'パスワード' (Password), and 'パスワード(確認)' (Confirm Password). A red box highlights the 'OK' button at the bottom of the dialog.

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

The final screenshot shows the 'ユーザー一覧' table with two users: 'test user' and 'user01'. The 'user01' row is highlighted with a red box, indicating successful registration.

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)

NetAttest EPS 管理画面の「ユーザー一覧」タブ。検索条件は「一部」で「user01」が検索結果として表示されている。右側の「発行」ボタンが赤い枠で囲われている。

ユーザー「user01」の詳細設定画面。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。発行ボタンが赤い枠で囲われている。

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

ユーザー証明書のダウンロード完了画面。メッセージ：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。ダウンロードボタンが赤い枠で囲われている。

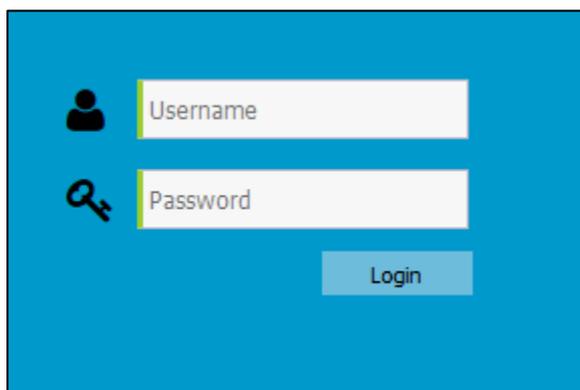
3. AP7532 の設定

3-1 アクセスポイントの設定

AP7532 の設定は WebGUI または CLI にて行います。本書では WebGUI での設定例について紹介します。

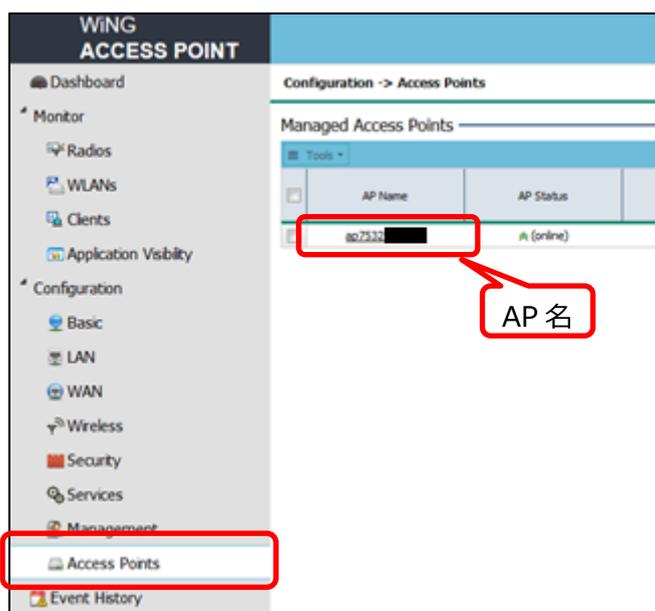
Web ブラウザより AP7532 の Web 管理画面ログインし、設定を開始します。

※初期 IP アドレス、アカウント、パスワードは設定マニュアルを参照してください。



・ログイン画面

画面左メニューから[Access Point]を選択します。その後、AP 名をクリックします。



Edit (鉛筆マーク) をクリックし、IP アドレスを編集します。最後に画面右下の[Apply]をクリックします。

Edit (鉛筆マーク) をクリックし、IP アドレスを編集します。最後に画面右下の[Apply]をクリックします。

The screenshot shows the configuration page for an AP7532. The 'LAN IP Interface Settings' section contains a table with the following data:

Interface	Description	IP Address	Edit
VLAN1		192.168.1.1/24	

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。

左メニューから[Wireless]を選択します。新規登録の場合は、[Add]、登録済みデータを変更する場合は、対象の設定名をクリックします。

Configuration -> Wireless

Radio Settings

2.4GHz Channel: smart Power: smart (dBm) Data Rate: default Antenna Gain: 0 (dB)

5GHz Channel: smart Power: smart (dBm) Data Rate: 11ac Antenna Gain: 0 (dB)

Wireless LAN MeshConnex

+ Add Delete Number of WLANs: 1

<input type="checkbox"/>	Name	Enable	SSID	VLAN	Authentication Type	2.4GHz	5GHz
<input type="checkbox"/>	SolitonLab	✓	SolitonLab	1	eap	✓	✓

Apply Discard

※画面は、登録済みの場合

SSID、認証方式、RADIUS サーバーを設定します。

設定後、画面右下の[Apply]をクリックします。画面が設定済み一覧に移行しますので、再度、画面右下の[Apply]をクリックします。

The screenshot displays the configuration page for a wireless LAN on a WING Access Point. The page is titled 'Configuration -> Wireless' and includes a sidebar with navigation options like Dashboard, Monitor, Radios, WLANs, Clients, Application Visibility, Configuration, Basic, LAN, WAN, Wireless, Security, Services, Management, Access Points, and Event History. The main configuration area is divided into sections: 'Wireless LAN' (with sub-tab 'MeshConnex'), 'RADIUS', 'WLAN Rate-Limit', and 'Other Settings'. The 'Wireless LAN' section includes fields for Name (SolitonLab), Enable (checked), SSID (SolitonLab), Band (2.4 GHz and 5 GHz checked), VLAN (1), and Description (Test). The 'Security' section has radio buttons for Open, Secure-PSK, Secure-802.1x (selected), and Guest. The 'RADIUS' section has radio buttons for Self Authentication, Controller Authentication, and External Authentication (selected), with fields for Primary and Secondary Servers and Shared Secrets. The 'WLAN Rate-Limit' section has checkboxes for Enable and fields for Per-Client and Aggregate(WLAN) rates. The 'Other Settings' section has checkboxes for Client Roam Assist and Voice VLAN. The 'Apply' button at the bottom right is highlighted with a red box.

項目	値
SSID	SolitonLab
Security	Secure-802.1x
RADIUS サーバー	192.168.1.2
Shared Secret	secret

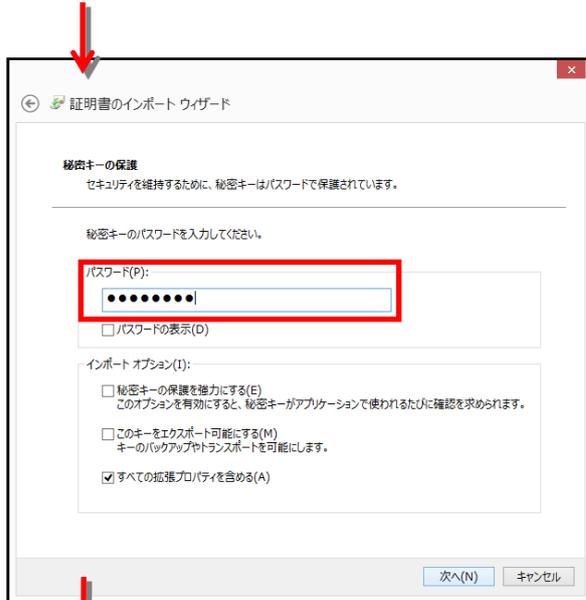
4. EAP-TLS 認証でのクライアント設定

4-1 Windows 8.1 での EAP-TLS 認証

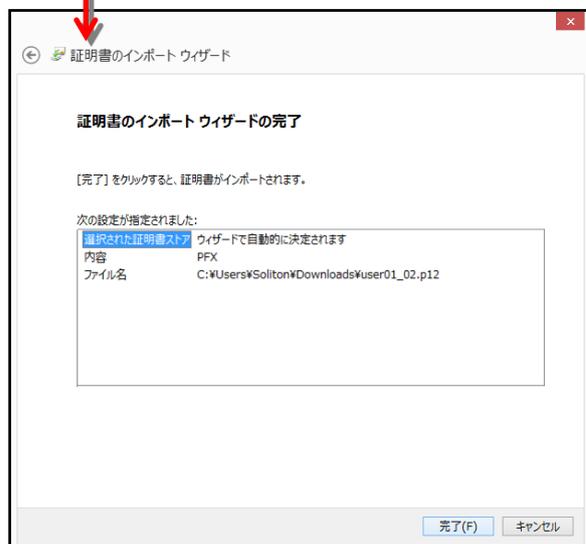
4-1-1 クライアント証明書のインポート

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
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(iPhone 6)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)

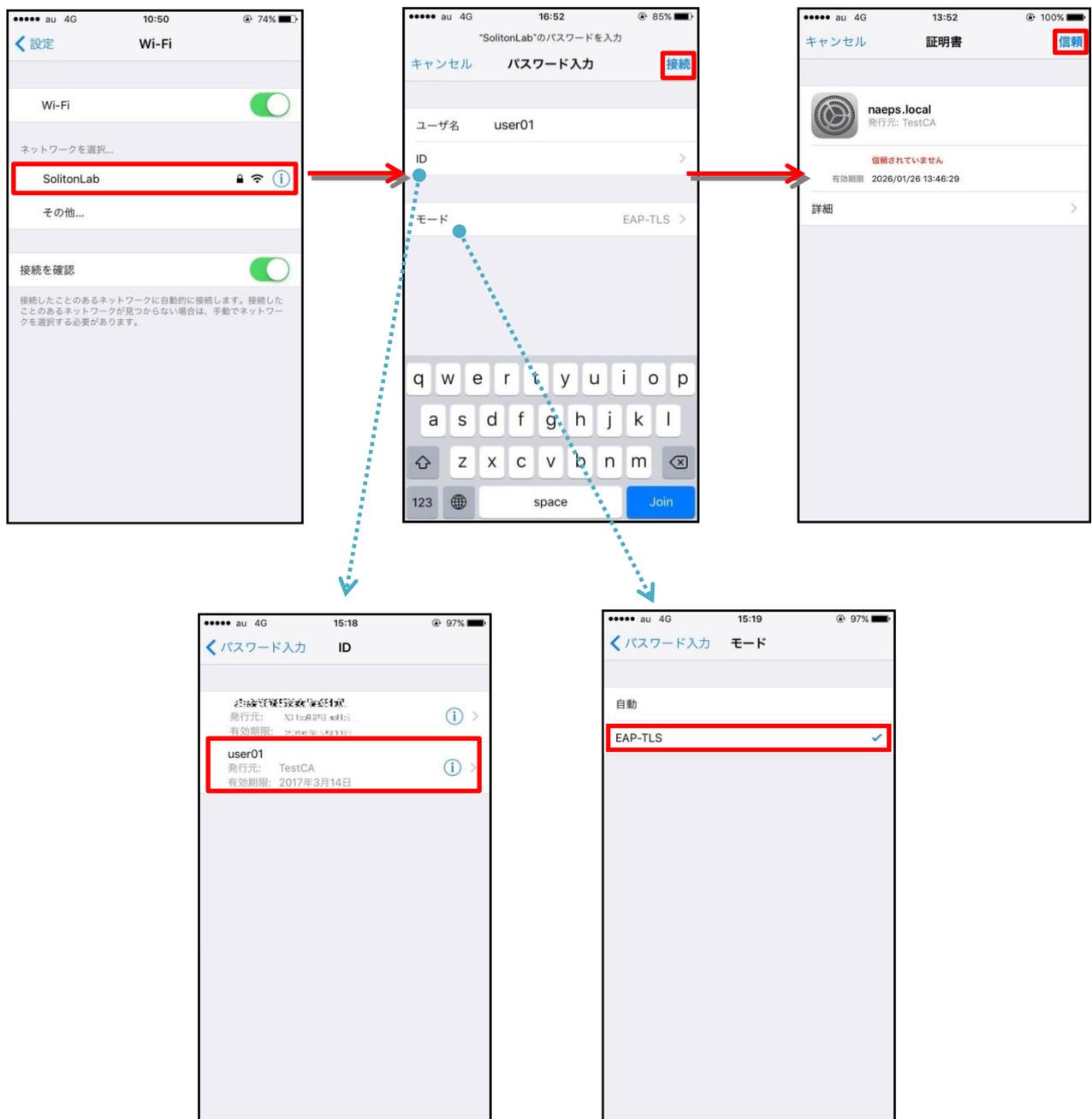
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

AP7532 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、「ユーザー名」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、「ユーザー名」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(Google Nexus 7)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。

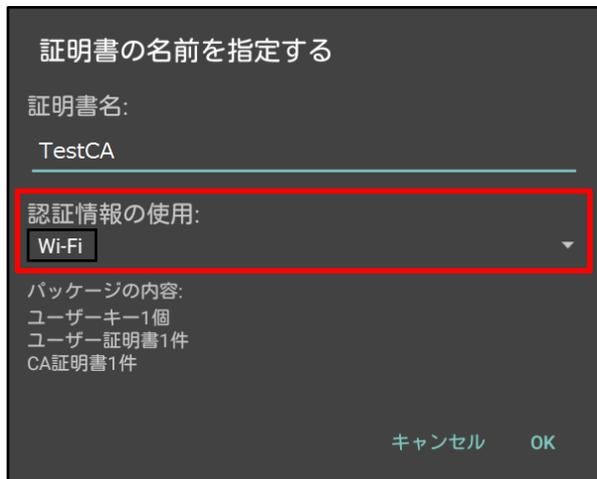
- 1) SD カードにクライアント証明書を保存し、インポートする方法※1
- 2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※2
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※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 5.1 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 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

AP7532 で設定した SSID を選択し、サブ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 8.1 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

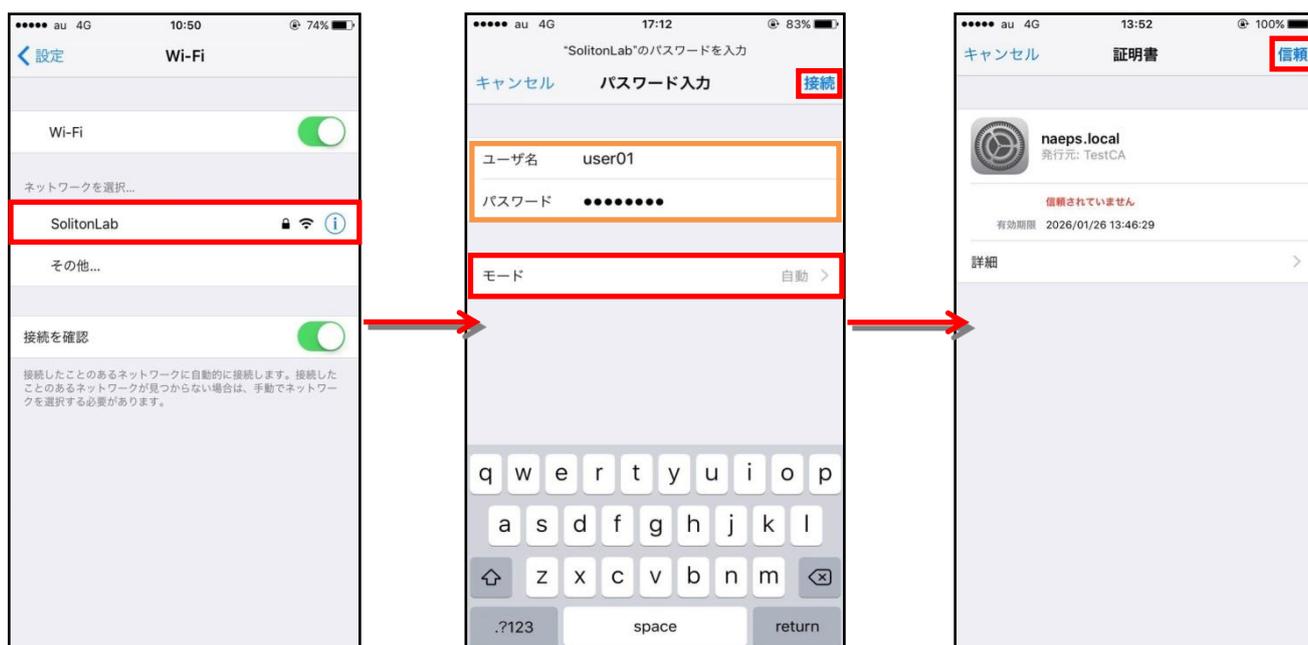
項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA

5-2 iOS(iPhone 6)のサブリカント設定

AP7532 で設定した SSID を選択し、サブリカントの設定を行います。

「ユーザー名」、「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。

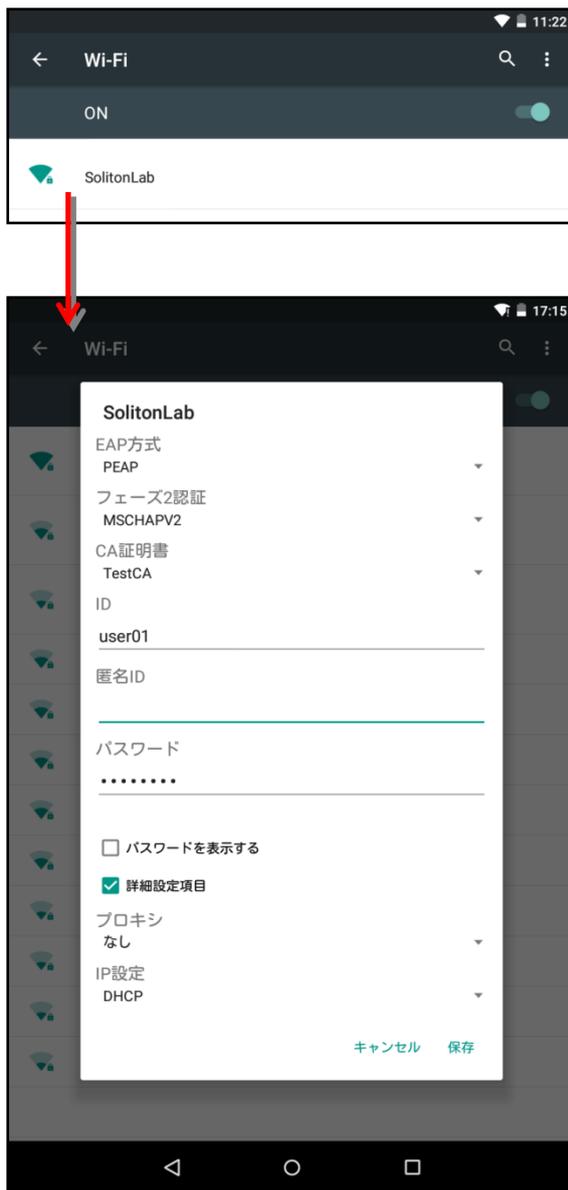


項目	値
ユーザー名	user01
パスワード	password
モード	自動

5-3 Android(Google Nexus 7)のサブリカント設定

AP7532 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。



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	May 24 14:45:20 naeps radiusd[15541]: notice 2016/05/24 14:45:20 Login OK: [user01] (from client RadiusClient port 1 cli 54-4E-90-18-F2-AB)
AP7532	2016-05-24 14:46:16 ap7532-XXXXXX DOT11 WPA_WPA2_SUCCESS Client '54-4E-90-18-F2-AB' completed WPA2-AES handshake on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' 2016-05-24 14:46:16 ap7532-XXXXXX DOT11 EAP_SUCCESS Client '54-4E-90-18-F2-AB' 802.1x/EAP (type:eap-tls) authentication success on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' username user01 2016-05-24 14:46:13 ap7532-XXXXXX DOT11 CLIENT_ASSOCIATED Client '54-4E-90-18-F2-AB' associated to wlan 'SolitonLab' ssid 'SolitonLab' on radio 'ap7532-XXXXXX:R2'

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	May 24 14:59:36 naeps radiusd[15541]: notice 2016/05/24 14:59:36 Login OK: [user01] (from client RadiusClient port 1 cli 54-4E-90-18-F2-AB via proxy to virtual server) May 24 14:59:36 naeps radiusd[15541]: notice 2016/05/24 14:59:36 Login OK: [user01] (from client RadiusClient port 1 cli 54-4E-90-18-F2-AB)
AP7532	2016-05-24 15:00:32 ap7532-XXXXXX DOT11 WPA_WPA2_SUCCESS Client '54-4E-90-18-F2-AB' completed WPA2-AES handshake on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' 2016-05-24 15:00:32 ap7532-XXXXXX DOT11 EAP_SUCCESS Client '54-4E-90-18-F2-AB' 802.1x/EAP (type:peap) authentication success on wlan 'SolitonLab' radio 'ap7532-XXXXXX:R2' username user01 2016-05-24 15:00:29 ap7532-XXXXXX DOT11 CLIENT_ASSOCIATED Client '54-4E-90-18-F2-AB' associated to wlan 'SolitonLab' ssid 'SolitonLab' on radio 'ap7532-XXXXXX:R2'

