

NetAttest EPS

認証連携設定例

【連携機器】 ELECOM WAB-S1167-PS/WAB-I1750-PS/

WDB-433SU2M2 シリーズ

【Case】 IEEE802.1X EAP-TLS 認証/EAP-PEAP(MS-CHAPv2)

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-S1167-PS/WAB-I1750-PS および無線子機 WDB-433SU2M2 シリーズの IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAPv2)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、WAB-S1167-PS/WAB-I1750-PS および WDB-433SU2M2 シリーズ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 システム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-S1167-PS/WAB-I1750-PS 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 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 Windows 7 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.....	22
4-3 iOS (iPhone 6)での EAP-TLS 認証.....	23
4-3-1 クライアント証明書のインポート.....	23
4-3-2 サプリカント設定.....	24
4-4 Android (Google Nexus 7)での EAP-TLS 認証.....	25
4-4-1 クライアント証明書のインポート.....	25
4-4-2 サプリカント設定.....	26

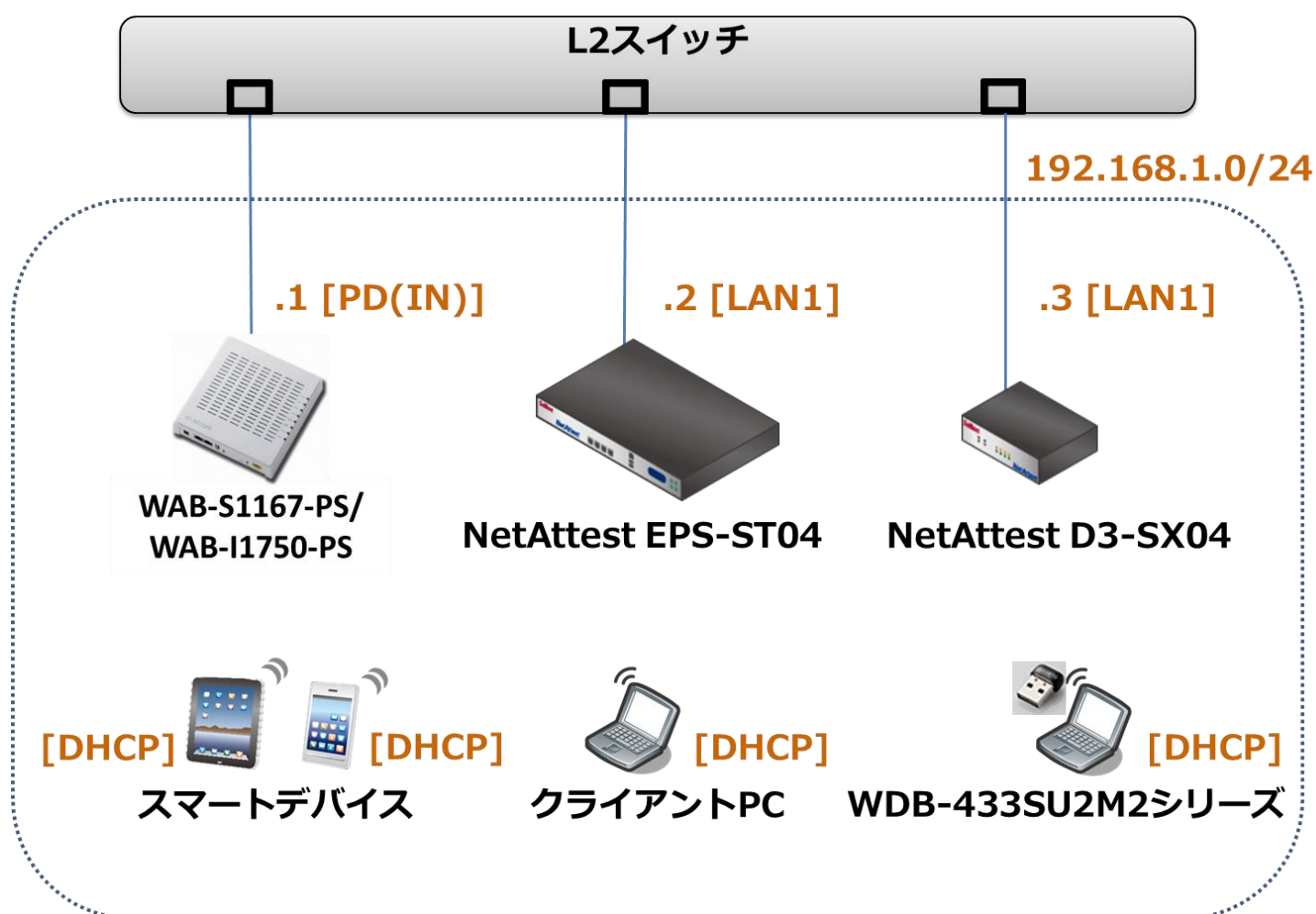
5. EAP-PEAP 認証でのクライアント設定.....	27
5-1 Windows 8.1 でのサブリカント設定.....	27
5-2 Windows 7 のサブリカント設定	28
5-3 iOS (iPhone 6)のサブリカント設定	29
5-4 Android (Google Nexus 7)のサブリカント設定	30
6. 動作確認結果	31
6-1 EAP-TLS 認証.....	31
6-2 EAP-PEAP 認証.....	31

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	Ver. 4.8.4
WAB-S1167-PS WAB-I1750-PS	ELECOM	RADIUS クライアント	Ver.1.4.17
Surface	Microsoft	Client PC (802.1X クライアント)	Windows 8.1 (64bit) Windows 標準サブリカント
iPhone 6	Apple	Client SmartPhone (802.1X クライアント)	9.2.1
Google Nexus 7	ASUS	Client Tablet (802.1X クライアント)	5.1.1
WDB-433SU2M2 シリーズ (ThinkPad X61)	ELECOM (Lenovo)	無線 LAN 子機 (Client PC) (802.1X クライアント)	Ver.1027.5.105.2015 Windows 8.1 (64bit)/7 (64bit/32bit) Windows 標準サブリカント
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 認証/IEEE802.1X EAP-PEAP(MS-CHAPv2)認証

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
WAB-S1167-PS WAB-I1750-PS	192.168.1.1/24		secret
Client PC	DHCP	-	-
Client SmartPhone	DHCP	-	-
Client Tablet	DHCP	-	-
Client PC (WDB-433SU2M2 シリーズ)	DHCP	-	-

2. NetAttest EPS の設定

2-1 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。

下記のような流れでセットアップを行います。

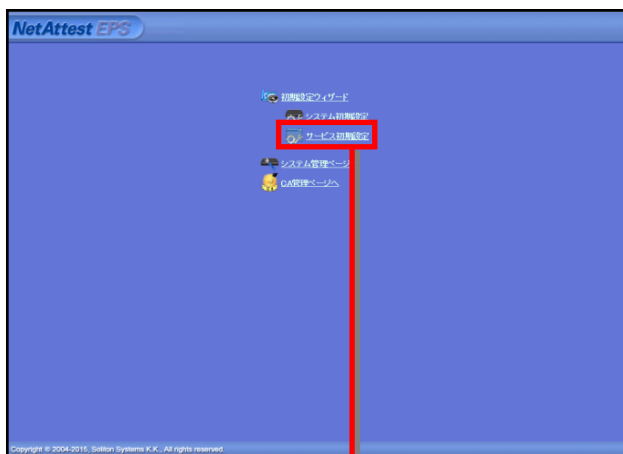
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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
 郵便番号: Tokyo
 非営利性: Shingaku
 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
 3 TLS
 4 TLS
 5 TLS

EAP-TLS/TLS/EAP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: フラグメントされた、最初のみ(ワイルドカードのみ含まれる)

EAP-TLS/PEAPオプション
 TLS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-FAST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/削除: 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:
 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。

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_02.p12 という名前で保存)

NetAttest EPS 管理画面の「ユーザー一覧」ページ。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。認証情報セクションの「有効期限」が「365 日」に設定されている。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。

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ダイアログ。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。右下の「ダウンロード」ボタンが赤い枠で囲われている。

3. WAB-S1167-PS/WAB-I1750-PS の設定

3-1 IP アドレスの設定

工場出荷状態の WAB-S1167-PS/WAB-I1750-PS 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 ブラウザより 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]-[2.4GHz 11bgn]-[RADIUS]をクリックします。RADIUS サーバー(NetAttest EPS)の IP アドレス、RADIUS サーバーとの共有シークレットを入力し、「適用」をクリックします。

※5GHz を利用する場合は、RADIUS サーバー(11a)にて同様の設定を行います。

The screenshot shows the configuration page for RADIUS servers. The primary RADIUS server (11g) is highlighted with a yellow border. The settings for the primary server are as follows:

プライマリRADIUSサーバー	
RADIUSサーバー	192.168.1.2
認証ポート	1812
共有シークレット	secret
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 secondary RADIUS server (11a) settings are as follows:

セカンダリRADIUSサーバー	
RADIUSサーバー	
認証ポート	1812
共有シークレット	secret
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

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-S1167-PS/WAB-I1750-PS 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、[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。SSID には、任意の値を入力します。

The screenshot shows the configuration interface for the ELECOM Wireless AP for Business. The page title is 'ELECOM Wireless AP for Business' with navigation links for 'ホーム', 'ログアウト', and 'Japan (日本語)'. The main menu includes 'WAB Smart Series', 'システム構成', '無線設定', and 'ツールボックス'. The left sidebar shows a tree view with '無線設定' expanded, containing 'WPS', 'ゲストネットワーク', '2.4GHz 11bgn' (with '基本設定' selected), '詳細設定', 'セキュリティ', 'クライアント', 'WDS', and '5GHz 11ac 11an' (with '基本設定', '詳細設定', and 'セキュリティ' listed). The main content area is titled '基本設定' and '2.4 GHz 基本設定'. A red box highlights the '無線' section, which includes:

- 無線: 有効 無効
- 無線通信モード: 11b/g/n
- 有効 SSID 数: 1
- SSID1: elecom2g01-XXXXXX (with a 'VLAN ID' label and a '1' in a small input field below it)

 Below this, the 'オートチャンネル' section is visible with:

- オートチャンネル: 有効 無効
- チャンネル: Ch 11
- チャンネル帯域幅: Auto, +Ch 7
- BSS BasicRateSet: 1,2,5,11 Mbps

 At the bottom right, there are '適用' and 'キャンセル' buttons.

項目	値
無線	有効
無線通信モード	11b/g/n
有効 SSID 数	1
SSID1	elecom2g01-XXXXXX VLAN ID : 1

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 interface for the ELECOM Wireless AP for Business. The 'Security' tab is selected, and the '2.4 GHz Wireless Security Settings' section is visible. The following settings are shown:

項目	値
SSID	elecom2g01-XXXXXX
ブロードキャストSSID	有効
セバレータ機能	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

項目	値
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

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。



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】

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	PEX
ファイル名	C:\Users\W\Desktop\User01_02.p12

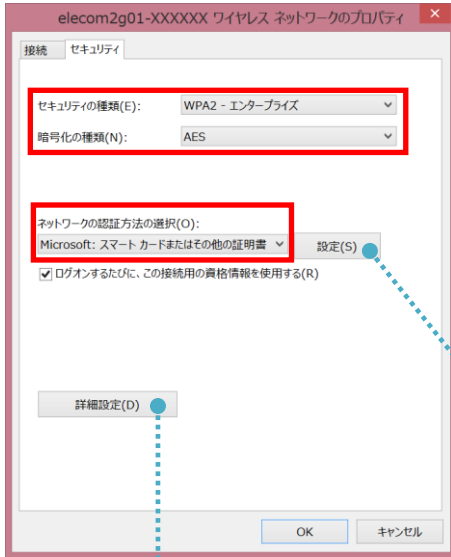
完了(F) キャンセル

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。

※本項では TLS の設定のみを記載します。その他の認証方式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
認証モードを指定する	ユーザー認証

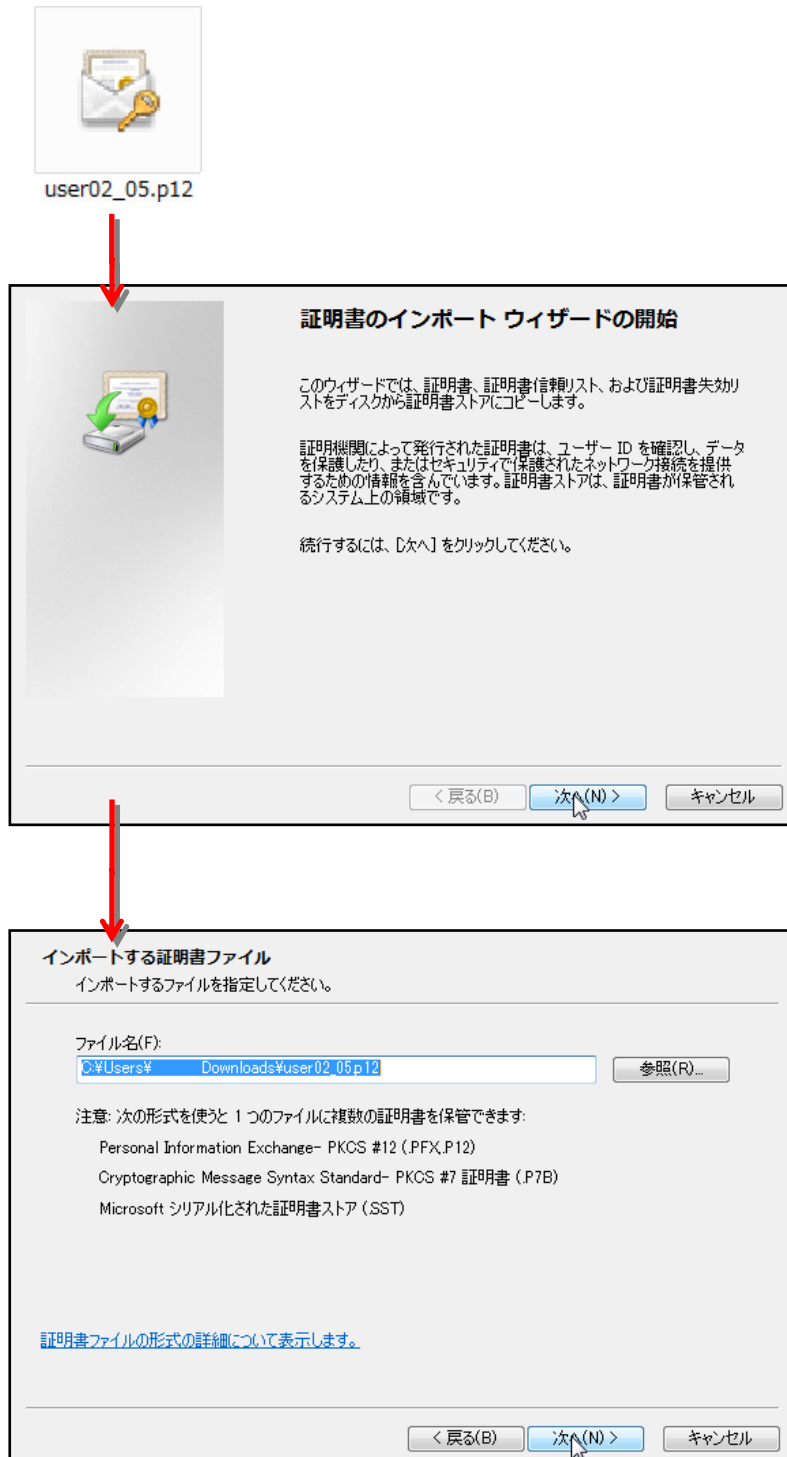


項目	値
接続のための認証方法	
- このコンピューターの . . .	On
- 単純な証明書の選択を . . .	On
証明書を検証してサーバーの . . .	On
信頼されたルート証明機関	TestCA

4-2 Windows 7 での EAP-TLS 認証

4-2-1 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 (user02_05.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

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):

秘密キーの保護を強力にする(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)

[プライベートキーの保護の詳細について表示します。](#)

< 戻る(B) **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:

[証明書ストアの詳細を表示します](#)

< 戻る(B) **次へ(N) >** キャンセル

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\%\$%\Downloads\%user02_05

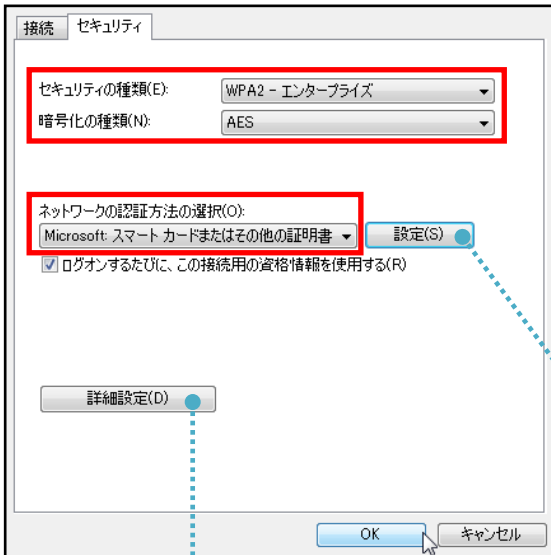
< 戻る(B) **完了** キャンセル

4-2-2 サプリカント設定

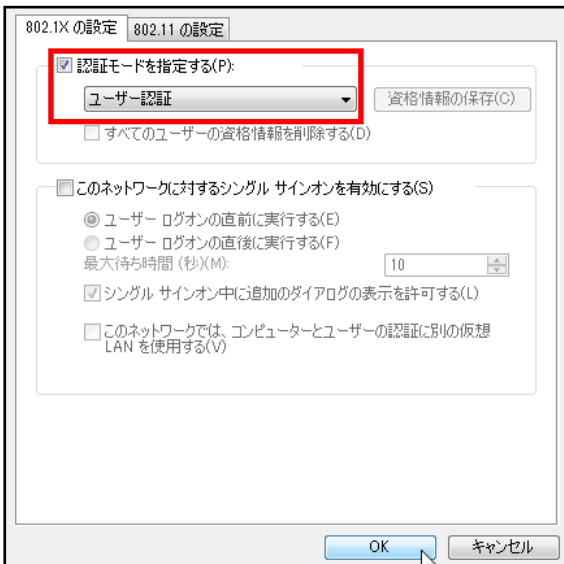
Windows 標準サプリカントで TLS の設定を行います。

※本項では TLS の設定のみを記載します。その他の認証方式の設定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
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・・・	On
- 単純な証明書の選択を・・・	On
証明書を検証してサーバー・・・	On
信頼されたルート証明機関	TestCA

4-3 iOS (iPhone 6)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 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。

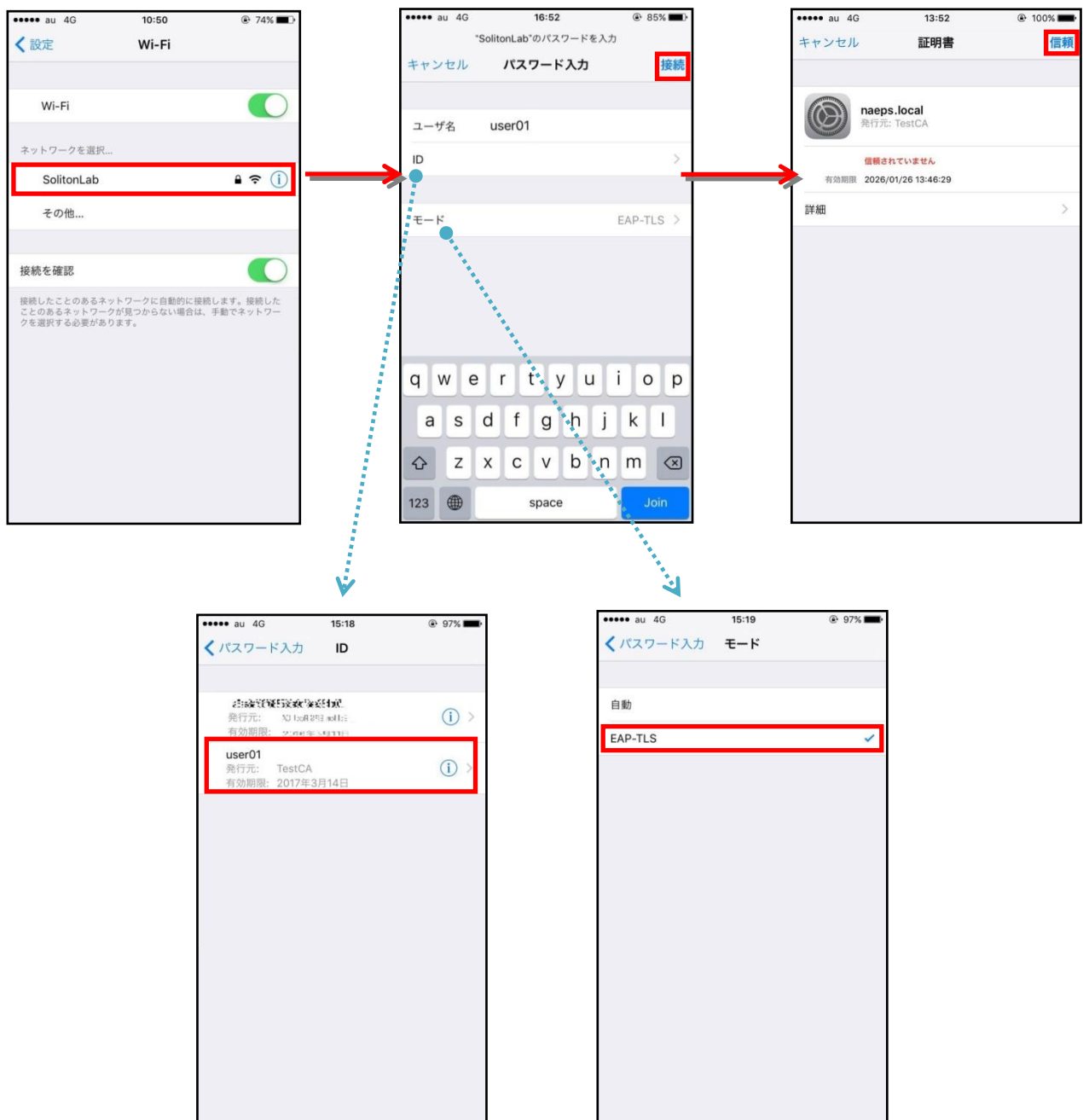
- 1) Mac OS を利用して Apple Configurator を使う方法
- 2) クライアント証明書をメールに添付し iOS デバイスに送り、インポートする方法
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)

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。

4-3-2 サプリカント設定

WAB-S1167-PS/WAB-I1750-PS で設定した SSID をタップし、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。



4-4 Android (Google Nexus 7)での EAP-TLS 認証

4-4-1 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。

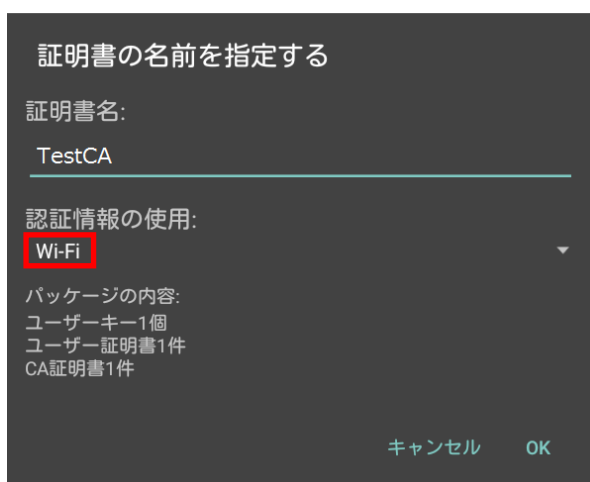
- 1) SD カードにクライアント証明書を保存し、インポートする方法※1
- 2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※2
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※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。

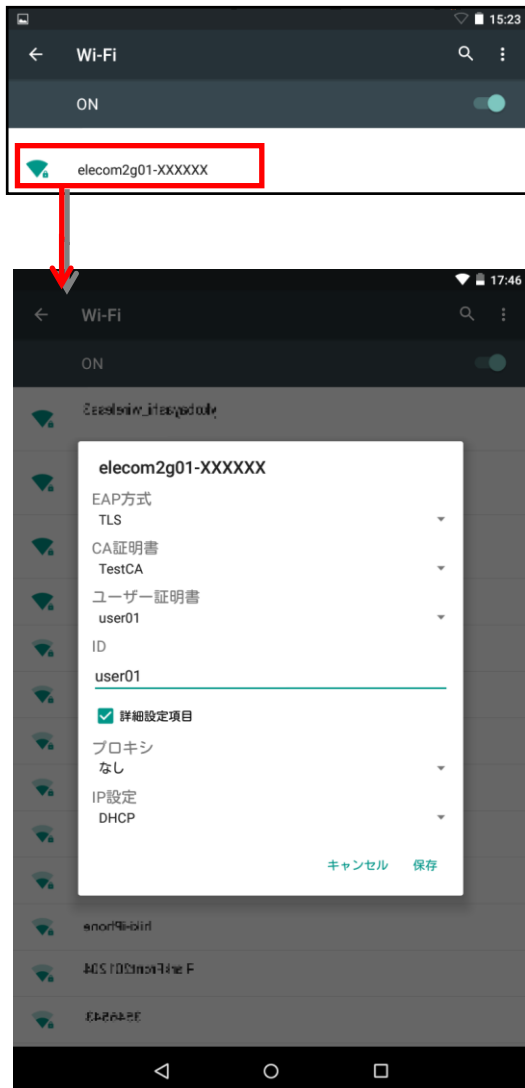
※3 メーカーや OS バージョンにより、Soliton KeyManager が正常に動作しない場合があります。事前にご検証ください。

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。



4-4-2 サプリカント設定

WAB-S1167-PS/WAB-I1750-PS で設定した SSID をタップし、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。
 「ID」には証明書を発行したユーザーアカウントの 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。

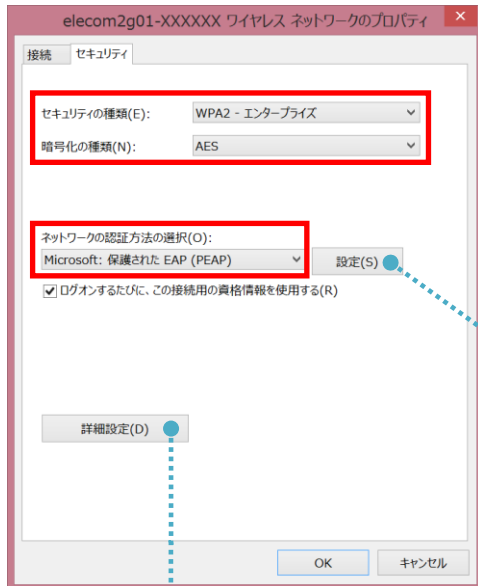


項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

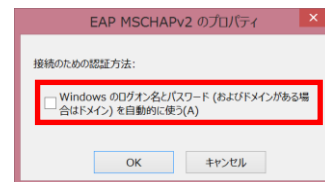
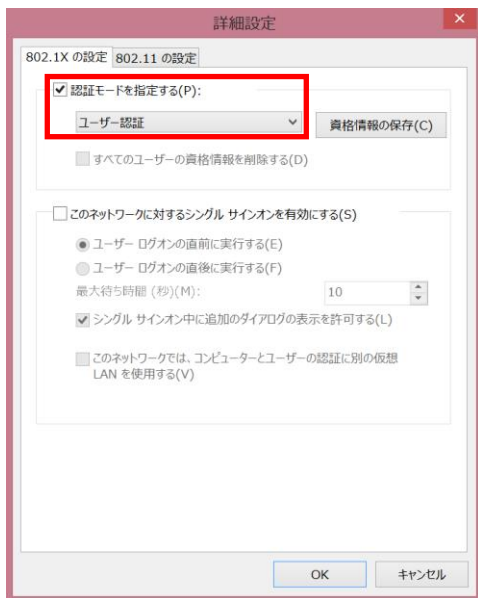
5. EAP-PEAP 認証でのクライアント設定

5-1 Windows 8.1 で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

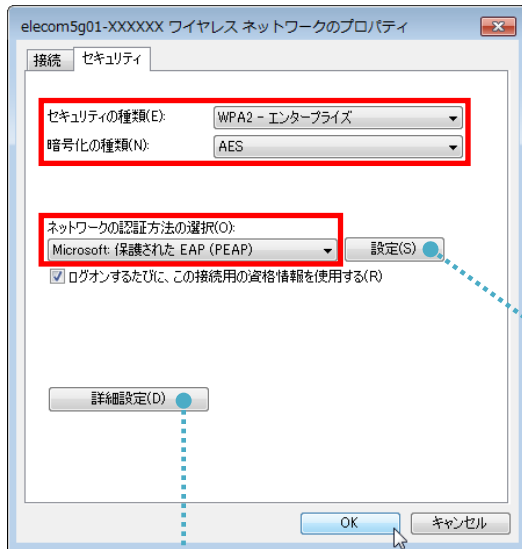


項目	値
認証モードを指定する	ユーザー認証

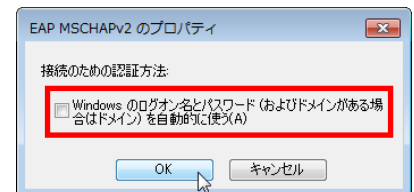
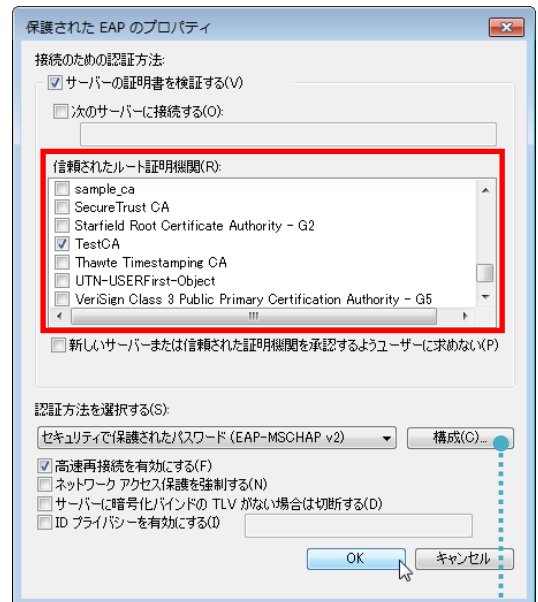
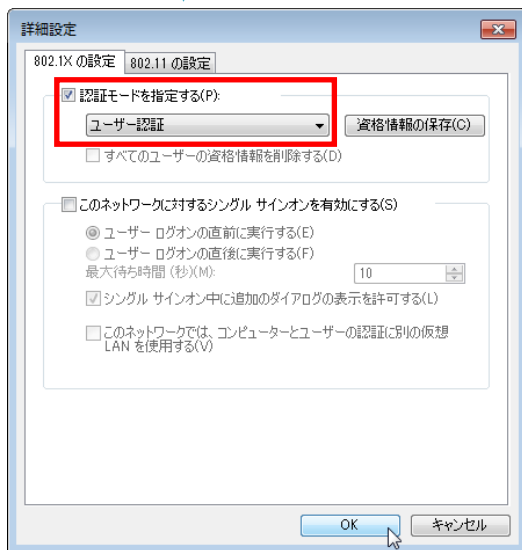
項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA

5-2 Windows 7 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



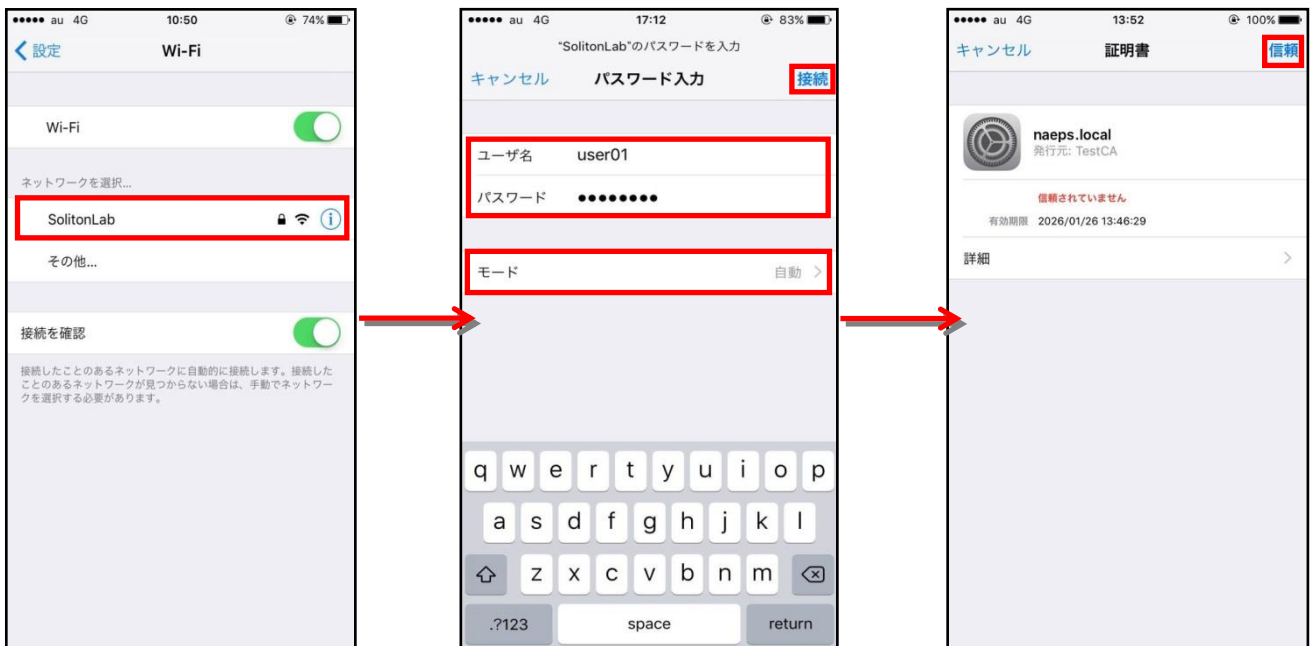
項目	値
認証モードを指定する	ユーザー認証

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

5-3 iOS (iPhone 6)のサブリカント設定

WAB-S1167-PS/WAB-I1750-PS で設定した SSID をタップし、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。

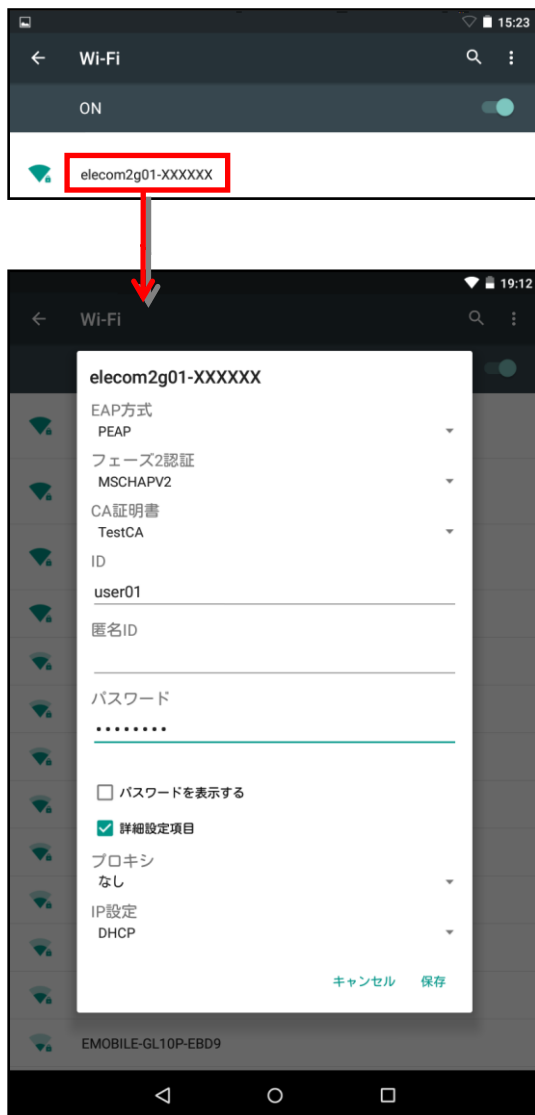
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。



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

5-4 Android (Google Nexus 7)のサブリカント設定

WAB-S1167-PS/WAB-I1750-PS で設定した SSID をタップし、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。「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
EPS	naeps radiusd[2486]: notice 2016/03/15 17:10:27 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23)
WAB-S1167-PS WAB-I1760-PS	Mar 15 17:10:29 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : authenticated Mar 15 17:10:29 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : starting accounting session 4EFA36B-0000001A Mar 15 17:10:29 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : pairwise key handshake completed (RSN) Mar 15 17:10:29 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : associated

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
EPS	naeps radiusd[2486]: notice 2016/03/15 16:27:43 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23 via proxy to virtual server) naeps radiusd[2486]: notice 2016/03/15 16:27:43 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23)
WAB-S1167-PS WAB-I1760-PS	Mar 15 16:27:45 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : authenticated Mar 15 16:27:45 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : starting accounting session 4EFA36B-00000000 Mar 15 16:27:45 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : pairwise key handshake completed (RSN) Mar 15 16:27:31 [WLAN]: Wireless 2.4G (SSID1), STA(c0:33:5e:df:2a:23) : associated

改訂履歴

日付	版	改訂内容
2016/04/25	1.0	初版作成