

# ***NetAttest EPS***

認証連携設定例

【連携機器】 Aruba 7005/AP-205

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

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、Aruba 社製無線 LAN コントローラー7005 および無線アクセスポイント AP-205 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 7005/AP-205 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
1-1-1 機器.....	7
1-1-2 認証方式.....	7
1-1-3 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. Aruba 7005 の設定.....	13
3-1 Aruba 7005 設定の流れ.....	13
Aruba の設定項目.....	14
3-1-1 Controller の基本設定.....	14
3-1-2 AP の基本設定.....	16
3-1-3 SSID の設定.....	19
3-1-4 Control Plane Security の設定.....	20
3-1-5 AP プロビジョニングの設定.....	20
4. EAP-TLS 認証でのクライアント設定.....	22
4-1 Windows 8.1 での EAP-TLS 認証.....	22
4-1-1 クライアント証明書のインポート.....	22
4-1-2 サブリカント設定.....	24
4-2 iOS(iPhone 6)での EAP-TLS 認証.....	25
4-2-1 クライアント証明書のインポート.....	25
4-2-2 サブリカント設定.....	26
4-3 Android(Nexus 7)での EAP-TLS 認証.....	27
4-3-1 クライアント証明書のインポート.....	27
4-3-2 サブリカント設定.....	28

---

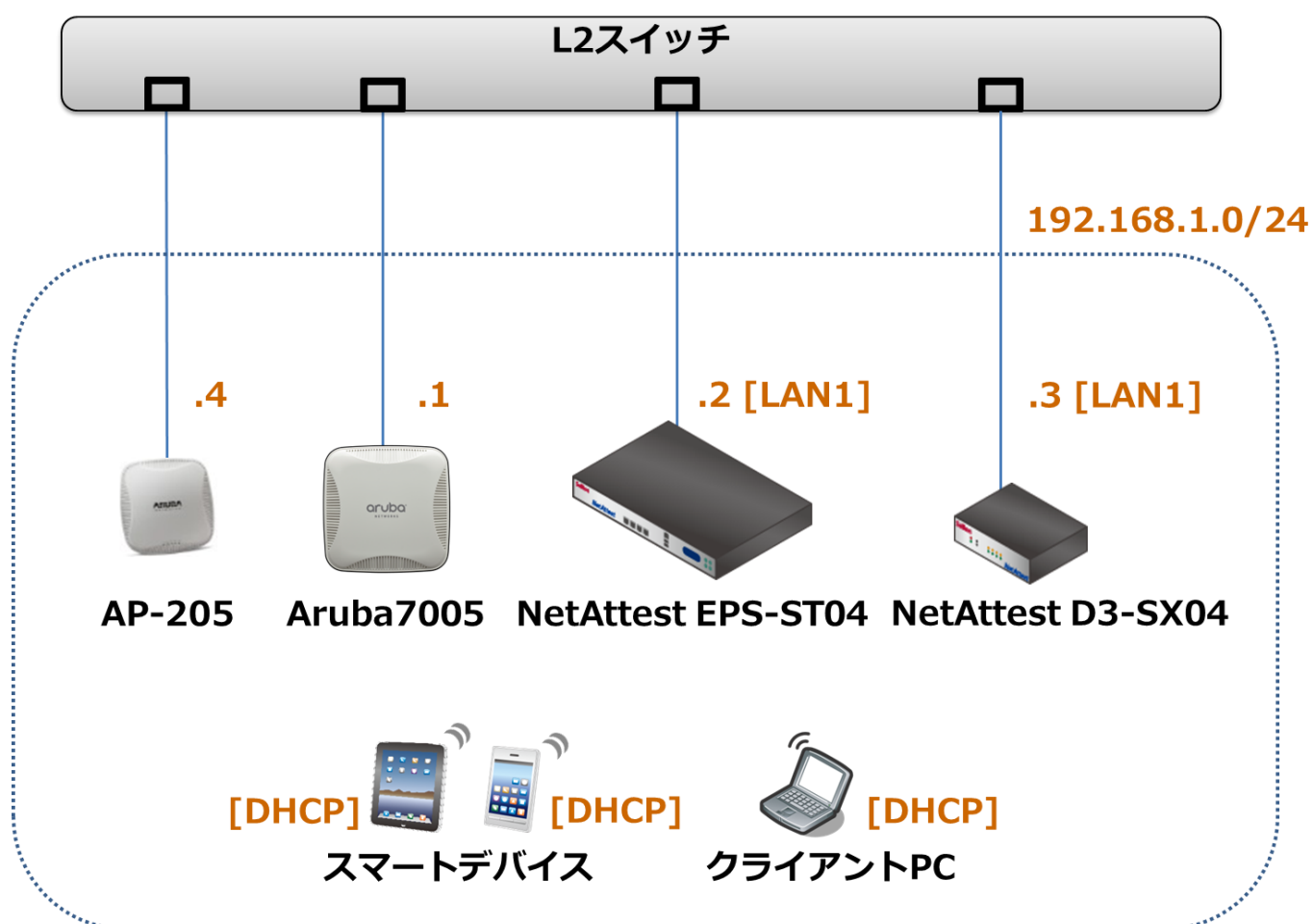
5. EAP-PEAP 認証でのクライアント設定.....	29
5-1 Windows 8.1 のサブリカント設定 .....	29
5-2 iOS(iPhone 6)のサブリカント設定 .....	30
5-3 Android(Nexus 7)のサブリカント設定.....	31
6. 動作確認結果 .....	32
6-1 EAP-TLS 認証.....	32
6-2 EAP-PEAP 認証.....	32

# 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



## 1-1-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS ST-04	Soliton Systems	RADIUS/CA サーバー	4.8.4
7005	Aruba	RADIUS クライアント (無線 LAN コントローラー)	6.4.2.12
AP-205	Aruba	アクセスポイント	6.4.2.12
Surface	MicroSoft	802.1X クライアント (Client PC)	Windows 8.1 64bit Windows 標準サブプリカント
iPhone 6	Apple	802.1X クライアント (Client SmartPhone)	9.2.1
Google Nexus 7	ASUS	802.1X クライアント (Client Tablet)	5.1
NetAttest D3 SX-04	Soliton Systems	DHCP/DNS サーバー	4.2.2

## 1-1-2 認証方式

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

## 1-1-3 ネットワーク設定

製品名	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS ST-04	192.168.1.2/24	UDP 1812	secret
7005	192.168.1.1/24		secret
AP-205	192.168.1.4/24		
Client PC	DHCP	-	-
Client SmartPhone	DHCP	-	-
Client Tablet	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。

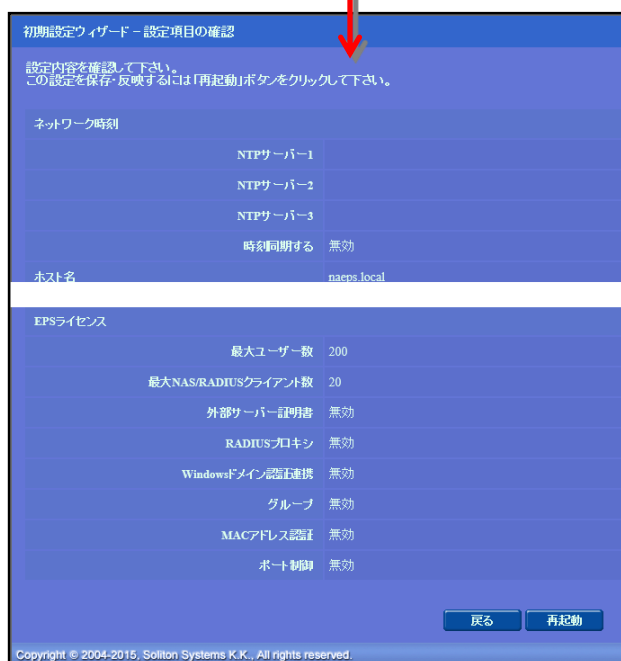
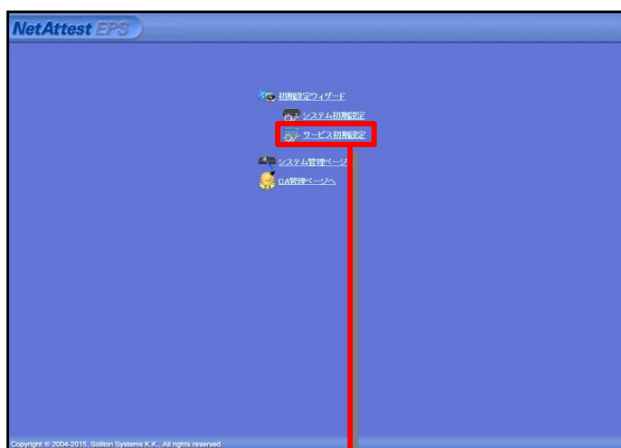
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行



## 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



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RSMデータベースの鍵を使用する

基本の署名  
署名アルゴリズム: SHA256

CA情報  
CA名(必須): TestCA  
国名: 日本  
都道府県名: 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

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: 無し  
4: 無し  
5: 無し

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: フラグメントなし (最初のフラグメントのみ含まれる)

EAP-TLS/PEAPオプション  
 GTC認証を有効にする  
 TLSセッションチェックを有効にする

EAP-FASTオプション

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:

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 ユーザー一覧画面のスクリーンショット。左側のメニューで「ユーザー」->「ユーザー一覧」が選択されています。中央には「ユーザー一覧」の検索欄と「追加」ボタンがあります。下部にはユーザーリストのテーブルがあり、「user01」の「発行」ボタンが赤い枠で囲まれています。

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
user01	user01		発行	変更 削除

ユーザー編集画面のスクリーンショット。編集対象は「user01」です。「認証情報」セクションが黄色でハイライトされており、有効期限が「365日」に設定されています。「証明書ファイルオプション」セクションで「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ます。「発行」ボタンが赤い枠で囲まれています。

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。このメッセージが表示された後、「ダウンロード」ボタンが赤い枠で囲まれています。

## 3. Aruba 7005 の設定

### 3-1 Aruba 7005 設定の流れ

---

Aruba 社製無線 LAN コントローラー Aruba 7005 は、WEBGUI または CLI を用いて設定が行えます。本書ではより設定の分かりやすい WEBGUI を用いて各種設定を実施する方法を紹介します。今回設定するのは以下の項目です。

- Contoroller の基本設定
    - IP アドレス、VLAN 等
  - AP の基本設定
    - APGroup、認証方式等
  - SSID の基本設定
    - SSID 設定、暗号強度設定
  - Control Plane security
    - コントローラーAP 間の鍵交換
  - AP プロビジョニングの設定
    - AP の IP アドレス指定・Radio 起動
- 
- 
-

## Aruba の設定項目

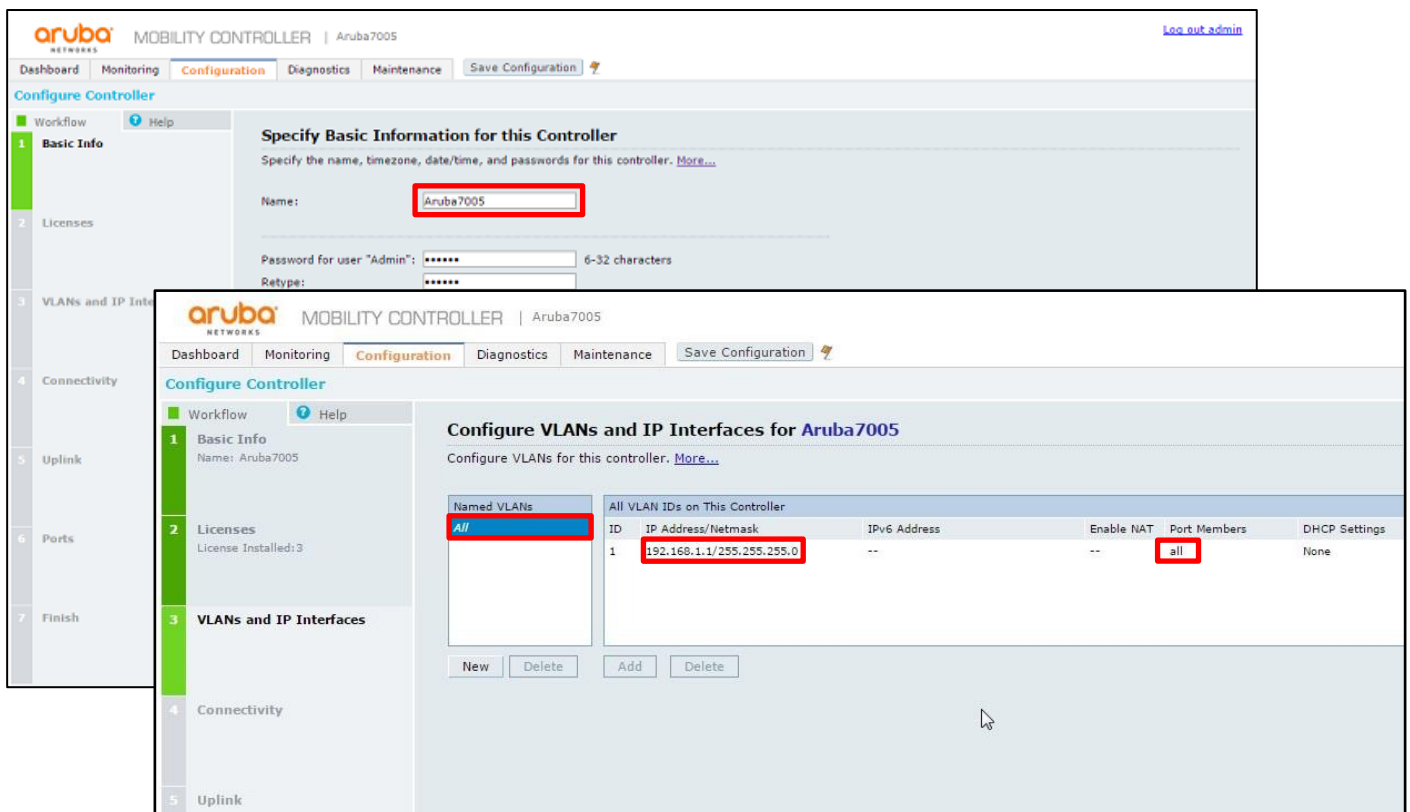
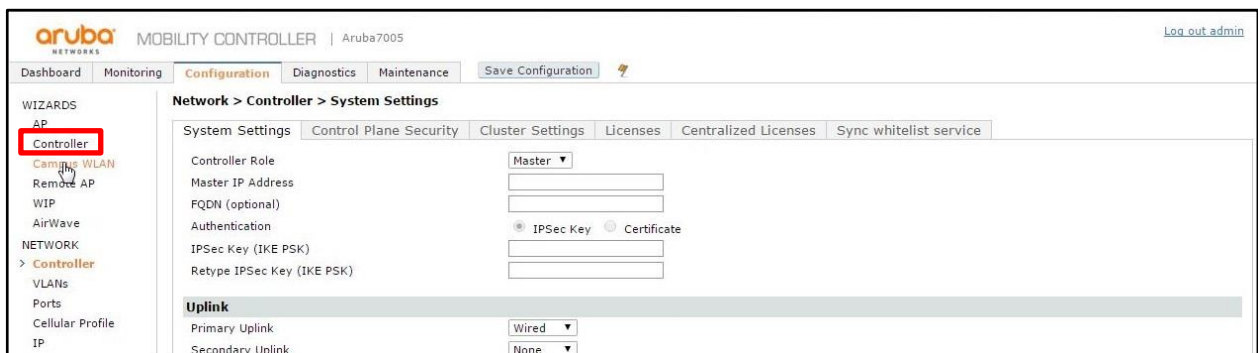
### 3-1-1 Controller の基本設定

Controller 側の基本設定を Wizard にて行います。

[Configuration]タブをクリックします。[WIZARDS]メニューから、[Controller]をクリックします。

ウィザードが開始されるので[Basic Info]にて[Name]に Controller の名前を指定します。

[VLANs and IP Interface]にて Named VLANs の[All]選択し、Vlan を[1]、Port を[All]と指定します。その他は特に変更の必要はありません。



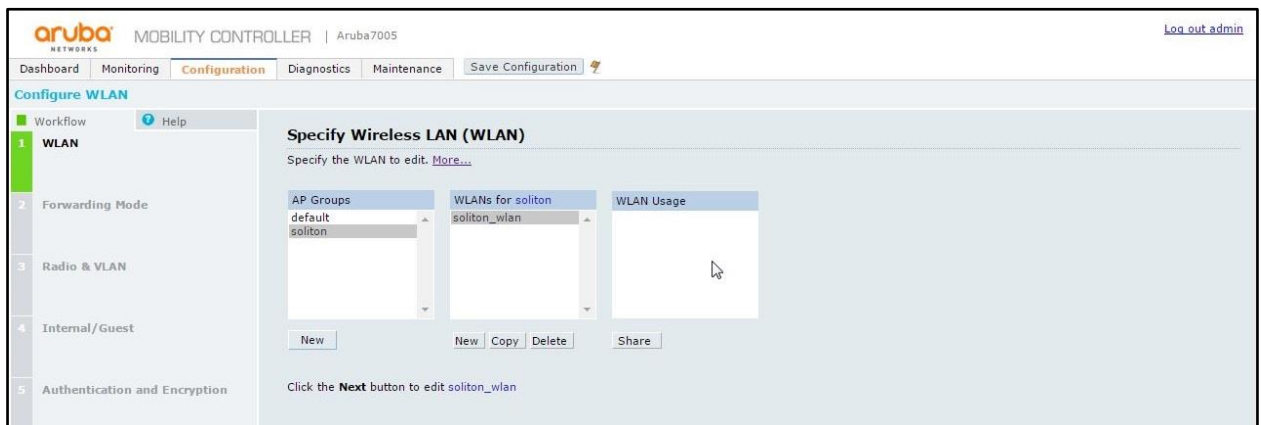
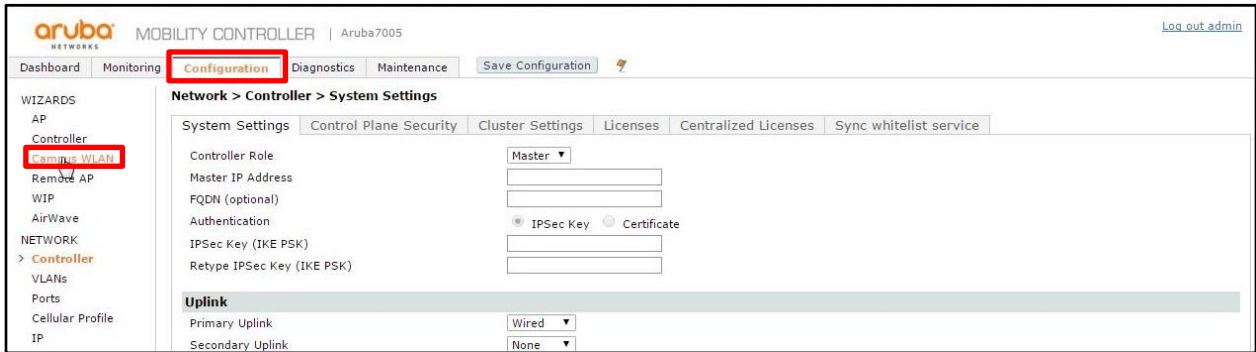
最後に設定を確認して[Finish]をクリックします。

The screenshot displays the Aruba Mobility Controller web interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration', 'Diagnostics', and 'Maintenance'. The 'Configuration' tab is active, and the 'Configure WLAN' page is shown. A sidebar on the left lists the configuration steps: 1. WLAN, 2. Forwarding Mode, 3. Radio & VLAN, 4. Internal/Guest, 5. Authentication and Encryption, 6. Captive Portal, 7. Authentication Server, 8. Role Assignment, and 9. WLAN Configured. The main content area shows a 'Configuration of soliton\_wlan in Group soliton is Complete' message. Below this is a 'Campus WLAN Wizard Configuration Summary' box, which is highlighted with a red border. The summary lists the configuration steps: 1. WLAN (APGroup: soliton, SSID: soliton\_wlan), 2. Forwarding Mode (Tunnel), and 3. Radio & VLAN (Radio Type: all, VLAN: 1). At the bottom of the summary box, there are links for 'Printable config summary' and 'Commands to be pushed'. Below the summary, there are two green arrows with instructions: 'To configure another WLAN click [again](#).' and 'To complete the Wizard and apply the settings you have specified, click the **Finish** button below'. At the bottom right of the page, there are three buttons: 'Back', 'Finish' (highlighted with a red border), and 'Cancel'.

### 3-1-2 AP の基本設定

AP の基本設定を Wizard にて行います。

[Configuration]タブをクリックし、[WIZARDS]メニューから[Campus WLAN]をクリックします。ウィザードが開始されるので、以下のように設定します。



項目	設定値
AP Group	soliton
WLANs for	soliton_wlan





**Specify Radio Type and VLAN for soliton\_wlan in Group soliton**

Specify the radio type on which this WLAN is available, as well as the VLAN in which users connecting to this WLAN are to be placed by default. Note: you can override the VLAN specified below by configuring per-role VLANs in Step 8. [More...](#)

Radio Type: All  
 Broadcast SSID: Yes  
 VLAN: 1

項目	設定値
Radio Type	All
Broadcast SSID	Yes
VLAN	1

**Specify Usage Scenario for soliton\_wlan in Group soliton**

Guest WLANs allow guests to access the Internet, while blocking access to the internal network. Guest WLANs are not encrypted, and at most require Web-based authentication. Internal WLANs typically employ encryption and stronger layer 2 authentication. [More...](#)

Is this WLAN intended for internal use or for use by guests?  
 Internal  
 Guest

**Specify Authentication and Encryption for soliton\_wlan in Group soliton**

The authentication and encryption options below are grouped by the level of security they guarantee. [More...](#)

**More Secure**

- Strong encryption with 802.1x authentication.
- Strong encryption with shared-key authentication.
- Weak encryption, with optional authentication.
- Open - no authentication or encryption.

**Less Secure**

Authentication:  WPA-2 Enterprise  
 WPA Enterprise

Encryption: aes,tkip

項目	設定値
Encryption	aes,tkip

外部 Radius サーバを指定します。NetAttestEPS にて設定した値を登録します。  
 ただし、[Name]については任意の名前を使用できます。

項目	設定値
Name	netattestST04
IP address	192.168.1.2
Auth port	1812
Acct port	1813
Shared key	secret
Retype key	secret

項目	設定値
Default role	authenticated
Server-derived roles	off

[9 WLAN Configured]にて設定に誤りが無いことを確認して[Finish]をクリックします。  
 その後の画面で[Close]をクリックしてウィザードを終了します。

### 3-1-3 SSID の設定

左のメニューから[WIRELESS]の中の、[AP Configuration]をクリックします。

[Wireless LAN]、[Virtual AP]、[soliton\_wlan-vap\_prof]の順に展開し、[SSID]をクリックします。

[SSID Profile >]の右側に[soliton\_wlan-ssid\_prof]が選択されていることを確認します。

[Network Name(SSID)]を記入し、[802.11 Security]の WPA2、AES にチェックを入れます。

The screenshot shows the Aruba Mobility Controller configuration page for the 'soliton' AP group. The left sidebar has 'WIRELESS' > 'AP Configuration' selected. The main area shows 'Profiles' and 'Profile Details' for 'soliton\_wlan-ssid\_prof'. The 'Network Name (SSID)' is 'SolitonLab'. Under '802.11 Security', 'WPA2' and 'AES' are selected.

項目	設定値
Network Name	SolitonLab

### 3-1-4 Control Plane Security の設定

Control Plane Security の設定を行います。

[Configuration]タブをクリックします。[NETWORK]メニューを展開し、[Controller]リンクをクリックします。[Control Plane Security]タブをクリックして[Disabled]にチェックを入れます。最後に[Apply]をクリックします。

※デフォルトでは有効になっています。

The screenshot shows the Aruba Mobility Controller web interface. The 'Configuration' tab is selected, and the 'Control Plane Security' sub-tab is active. The 'Control Plane Security' checkbox is checked, and the 'Disabled' radio button is selected. The 'Number of AP Whitelist Entries' is set to 1. The 'Apply' button is highlighted.

### 3-1-5 AP プロビジョニングの設定

AP のプロビジョニングを行います。

[Configuration]タブをクリックします。[WIRELESS]メニューを展開し、[AP Installation]リンクをクリックするとコントローラーで確認できる AP が表示されます。対象の AP にチェックを入れて [Provision]をクリックします。

The screenshot shows the Aruba Mobility Controller web interface. The 'WIRELESS' menu is expanded, and 'AP Installation' is selected. A table lists APs with columns for AP Name, AP Group, AP IP, AP Type, AP MAC Address, AP Serial Number, Flags, and Status. The first row is highlighted, and the 'Provision' button is visible below the table.

AP Name	AP Group	AP IP	AP Type	AP MAC Address	AP Serial Number	Flags	Status
84:d4:7e:c1:d3:e8	soliton	192.168.1.4	205	84:d4:7e:c1:d3:e8	CM0550895		Up 2h:22m:47s

[Provisioning]画面へ遷移します。[IP Setting]にて AP へ指定するアドレスを入力します。  
最後に[Apply and Reboot]をクリックします。AP が自動的に再起動します。

中略

AP IP Address	AP Name	AP Group	SNMP System Location	Mesh Role	AP Type	Serial Number
192.168.1.4	84:d4:7e:c1:d3:e8	soliton		none	205	CM0550895

項目	設定値
IP Address	192.168.1.4
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.1

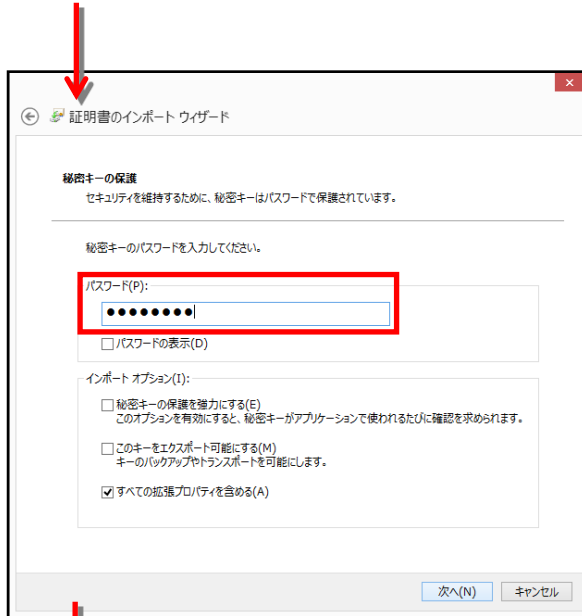
## 4. EAP-TLS 認証でのクライアント設定

### 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。

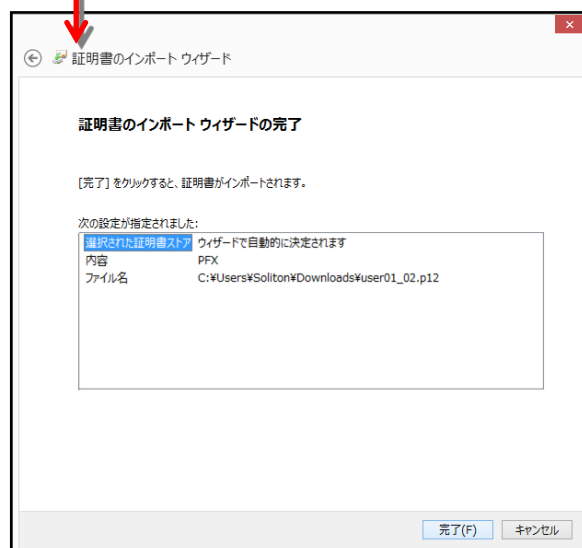
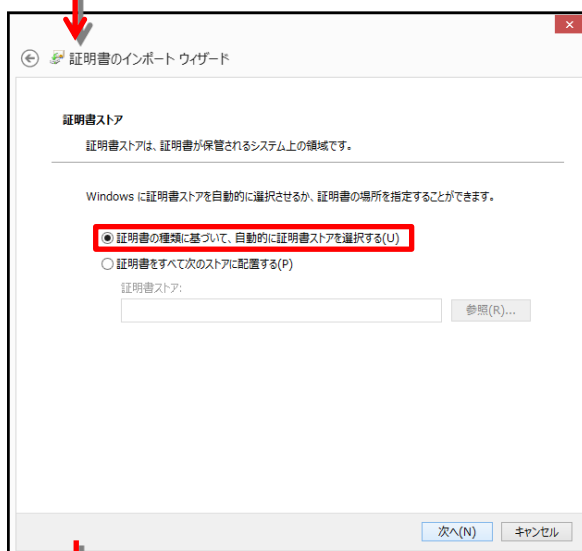




【パスワード】

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

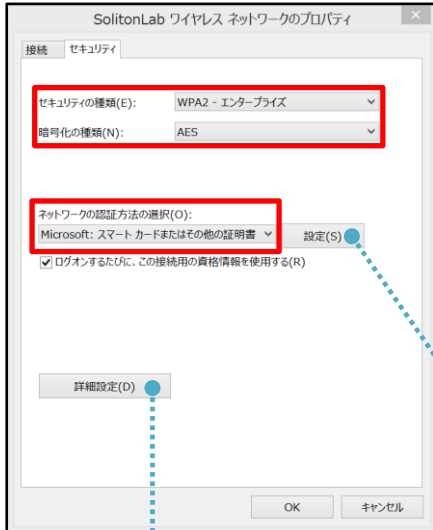


### 4-1-2 サプリカント設定

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
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



## 4-2 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)

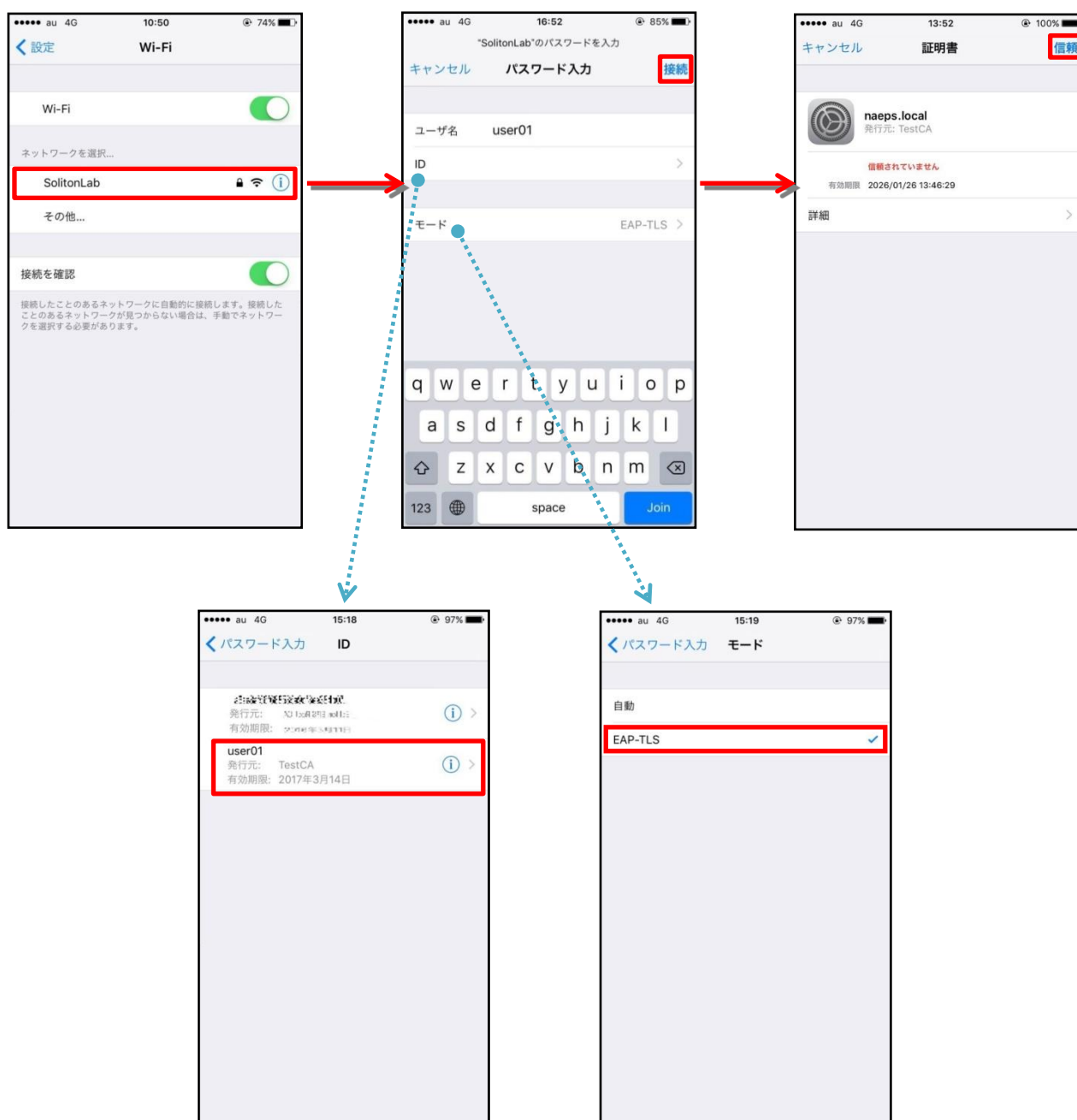
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

## 4-2-2 サプリカント設定

7005/AP-205 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(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。

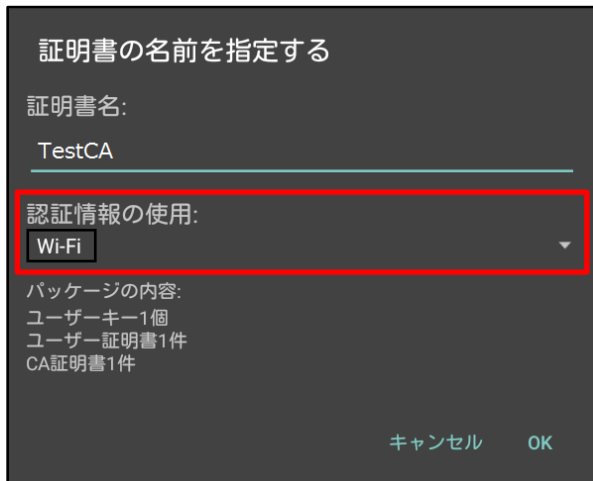
- 1) SD カードにクライアント証明書を保存し、インポートする方法※1
- 2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※2
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※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。

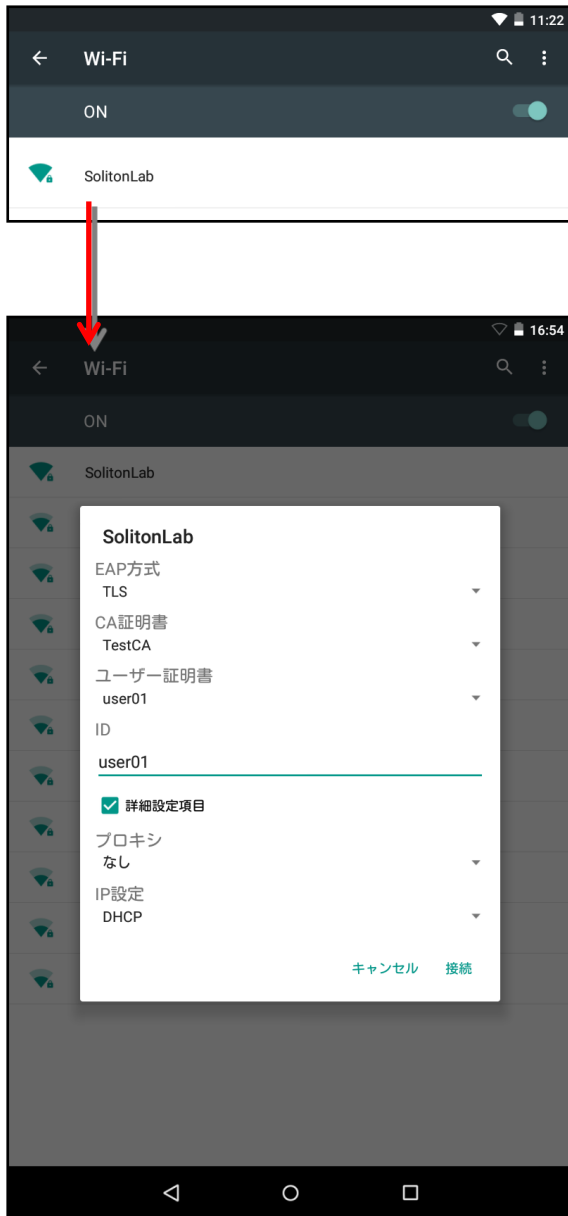


## 4-3-2 サプリカント設定

7005/AP-205 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。

「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。

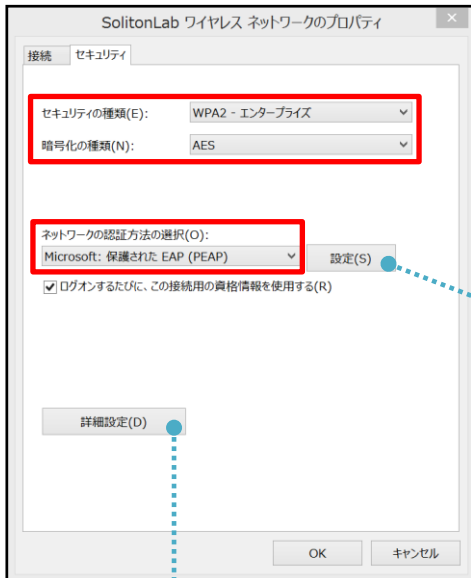


項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

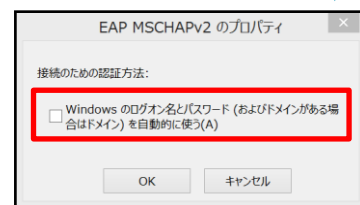
# 5. EAP-PEAP 認証でのクライアント設定

## 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



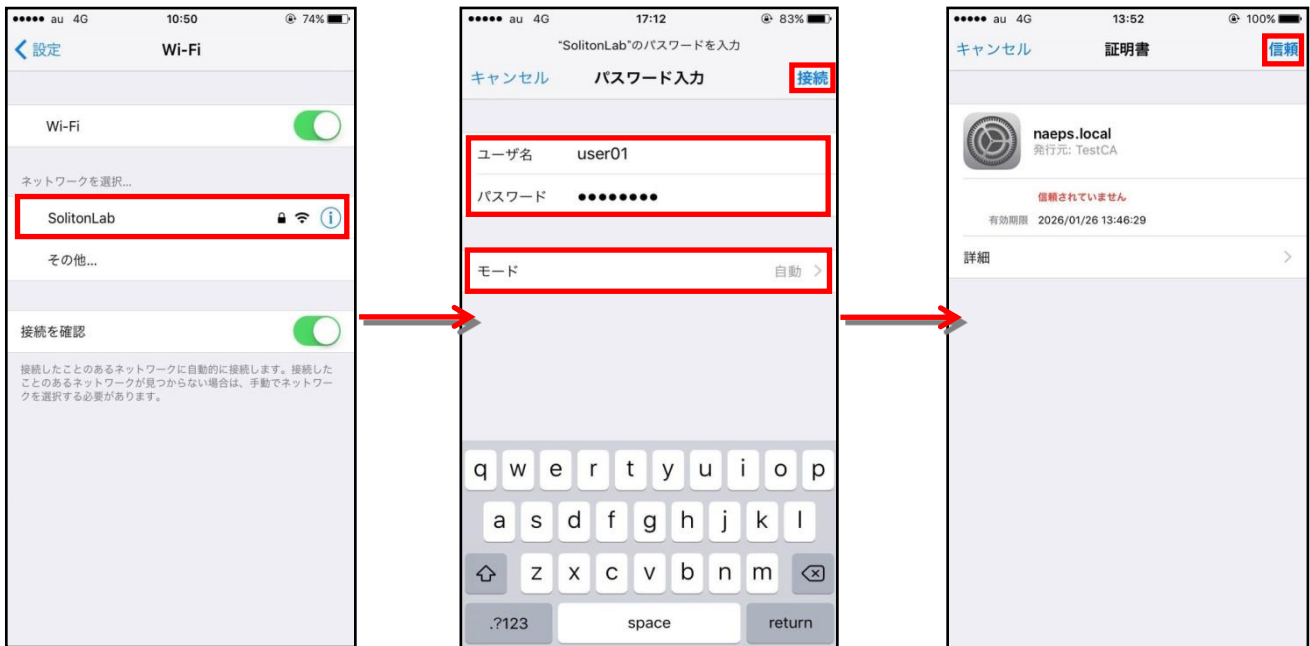
項目	値
認証モードを指定する	ユーザー認証

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

## 5-2 iOS(iPhone 6)のサブリカント設定

7005/AP-205 で設定した SSID を設定し、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「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。

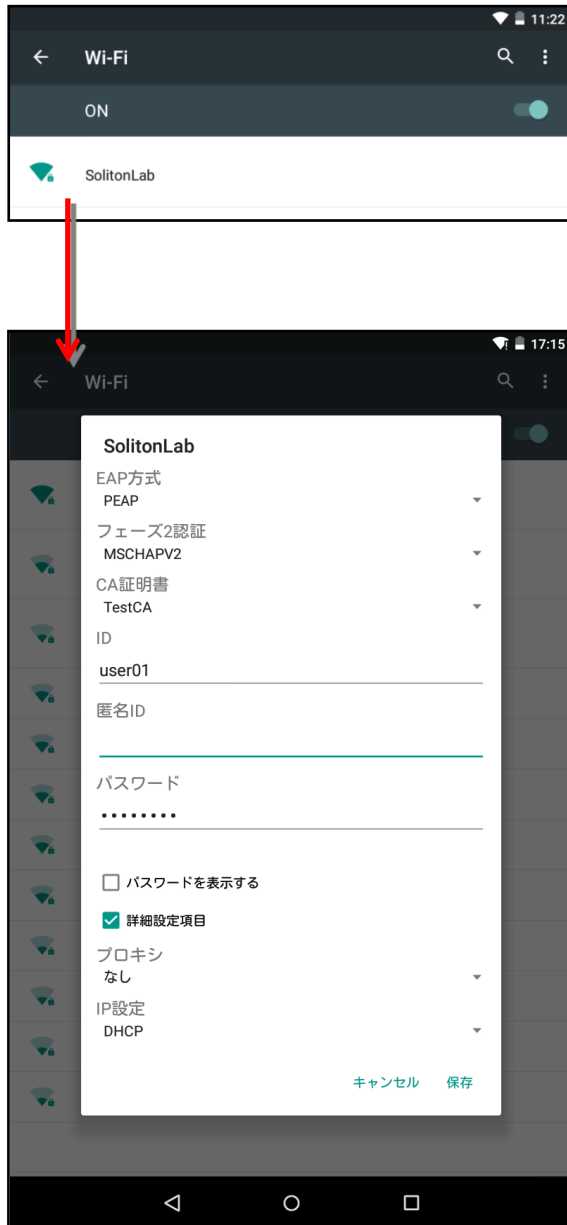


項目	値
ユーザー名	user01
パスワード	password
モード	自動

### 5-3 Android(Nexus 7)のサブリカント設定

7005/AP-205 で設定した SSID を設定し、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。

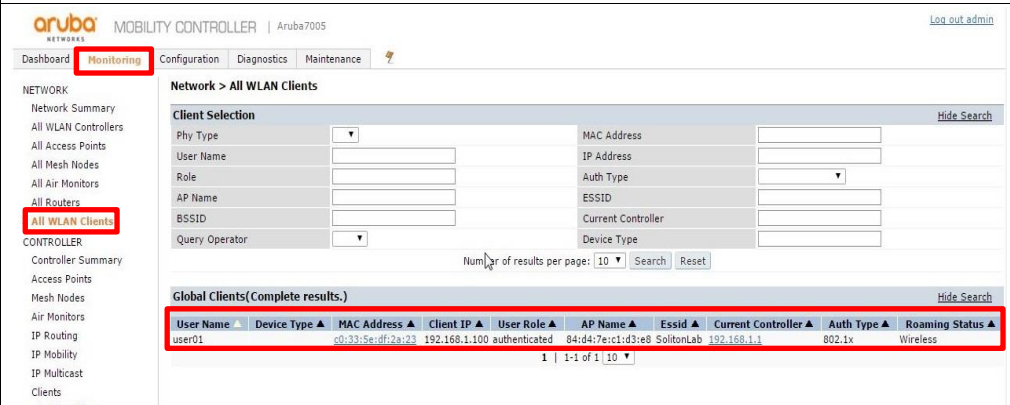


項目	値
EAP 方式	PEAP
フェーズ 2 認証	MSCHAPV2
CA 証明書	TestCA
ID	user01
パスワード	password

## 6. 動作確認結果

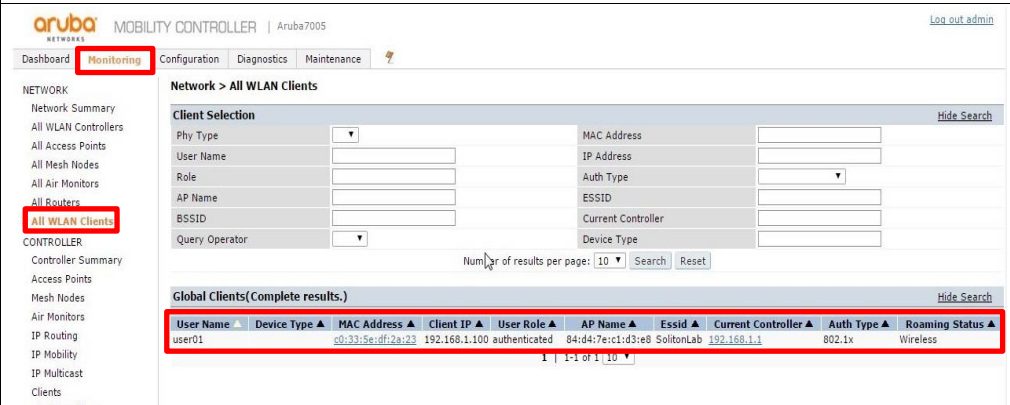
### 6-1 EAP-TLS 認証

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
NetAttest EPS	naeps radiusd[2540]: notice 2016/03/23 16:09:07 Login OK: [user01] (from client RadiusClient01 port 0 cli C0335EDF2A23)
Aruba7005	 <p>ログインユーザ名、端末の MAC アドレス、端末の IP アドレス、認証タイプ等を表示</p>

### 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	naeps radiusd[6923]: notice 2016/03/23 17:09:09 Login OK: [user01] (from client RadiusClient01 port 0 cli C0335EDF2A23 via proxy to virtual server) naeps radiusd[6923]: notice 2016/03/23 17:09:09 Login OK: [user01] (from client RadiusClient01 port 0 cli C0335EDF2A23)
Aruba7005	 <p>ログインユーザ名、端末の MAC アドレス、端末の IP アドレス、認証タイプ等を表示</p>



## 改訂履歴

日付	版	改訂内容
2016/05/18	1.0	初版作成