

NetAttest EPS

認証連携設定例

【連携機器】 Hewlett Packard Aruba IAP 305

【Case】 IEEE802.1X EAP-TLS/EAP-PEAP

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、Hewlett Packard 社製無線アクセスポイント Aruba IAP 305 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 Aruba IAP 305 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. NetAttest D3 の設定.....	13
3-1 スコープの設定.....	14
3-2 IP アドレスの静的割り当て.....	15
3-3 DHCP サーバーの起動.....	16
4. Aruba IAP 305 の設定.....	17
4-1 WLAN 設定.....	18
4-2 VLAN 設定.....	19
4-3 セキュリティ設定.....	20
4-4 アクセス設定.....	21
5. EAP-TLS 認証でのクライアント設定.....	22
5-1 Windows 10 での EAP-TLS 認証.....	22
5-1-1 クライアント証明書のインポート.....	22
5-1-2 サプリカント設定.....	24
5-2 iOS での EAP-TLS 認証.....	25
5-2-1 クライアント証明書のインポート.....	25
5-2-2 サプリカント設定.....	26
5-3 Android での EAP-TLS 認証.....	27

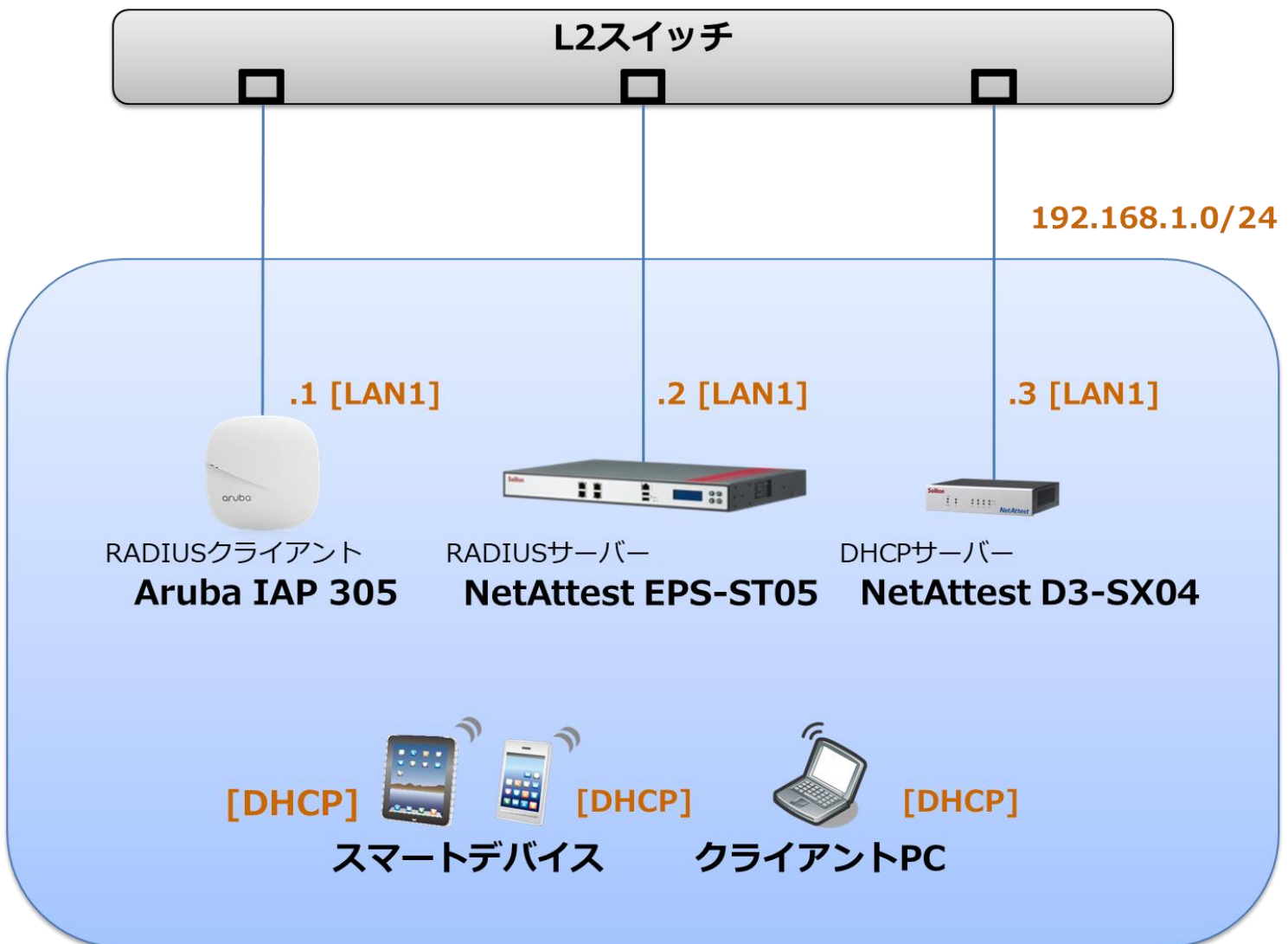
5-3-1 クライアント証明書インポート.....	27
5-3-2 サプリカント設定.....	28
6. EAP-PEAP 認証でのクライアント設定.....	29
6-1 Windows 10 での EAP-PEAP 認証.....	29
6-1-1 Windows 10 のサプリカント設定.....	29
6-2 iOS での EAP-PEAP 認証.....	30
6-2-1 iOS のサプリカント設定.....	30
6-3 Android での EAP-PEAP 認証.....	31
6-3-1 Android のサプリカント設定.....	31
7. 動作確認結果.....	32
7-1 EAP-TLS 認証.....	32
7-2 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



1-2 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	4.10.3
Aruba IAP 305	Hewlett Packard	RADIUS クライアント (無線アクセスポイント)	v6.5x
Surface	Microsoft	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブリカント
iPhone 7	Apple	802.1X クライアント (Client SmartPhone)	iOS 11.2.6
nova	Huawei	802.1X クライアント (Client Tablet)	Android 7.0
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.15

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
Aruba IAP 305	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。

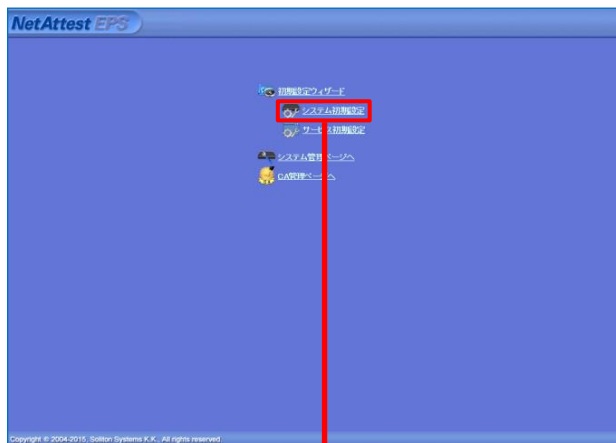
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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
- ド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

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.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。

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

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

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

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」画面。ユーザー「user01」の「発行」ボタンが赤い枠で囲われ、赤い矢印が下を指している。

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

編集対象: user01

基本情報

姓: user01

名:

E-Mail:

詳細情報

認証情報

ユーザーID: user01

有効期限: 365 日

証明書ファイルオプション

パスワード:

パスワード(確認):

PKCS#12ファイルに証明機関の証明書を含める

発行 キャンセル

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

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

3. NetAttest D3 の設定

Aruba IAP 305 は、デフォルトでは DHCP にて IP アドレスを取得するよう設定されています。しかし、EPS に RADIUS クライアントとして登録するためには IP アドレスを静的に指定する必要があります。今回は Aruba IAP 305 に静的に IP アドレスを割り当てるために、NetAttest D3 の静的割り当て機能を使用して IP アドレスを払い出すことにします。

NetAttest D3 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、Google Chrome から [http://192.168.2.1:2181/]にアクセスしてください。NetAttest D3 では以下の設定を行います。

- DHCP サーバーの起動
- スコープの設定
- IP アドレスの静的割り当て

3-1 スコープの設定

[DHCPサービス]-[スコープ]から[追加]ボタンでスコープを追加します。今回は、端末に払い出す IP アドレスを[192.168.1.100-140]にするため、以下のように設定します。



項目	値
スコープの設定	
- ネットワーク	192.168.1.0
- サブネットマスク	255.255.255.0
- ルーター	192.168.1.254
- ドメイン名	solitonlab.com
- ドメインネームサーバー	192.168.1.3
レンジの設定	
- レンジ開始アドレス	192.168.1.1
- レンジ終了アドレス	192.168.1.140
- 除外レンジ開始アドレス	192.168.1.2
- 除外レンジ終了アドレス	192.168.1.99

3-2 IP アドレスの静的割り当て

Aruba IAP 305 の MAC アドレスに IP アドレスを静的に割り当てるため、事前に Aruba IAP 305 の MAC アドレスを確認してください。

[DHCP サービス]-[静的割り当て]から[追加]ボタンで IP アドレスの静的割り当てを行います。Aruba IAP 305 の MAC アドレスと、静的に割り当てる IP アドレスを指定します。



項目	値
ホスト名	Aruba
IP アドレス	192.168.1.1
MAC アドレス	11:22:33:44:55:66



3-3 DHCP サーバーの起動

[DHCP サービス]-[サーバー状態]にて[起動]ボタンを押し、DHCP サーバーを起動します。

The screenshot displays the NetAttest D3 management console. The left sidebar shows a navigation menu with 'DHCPサービス' expanded and 'サーバー状態' selected. The main content area is titled 'DHCP - サーバー状態' and shows the following information:

- 動作状態: 停止
- サーバー稼働状態: 停止
- 冗長化状態: 冗長化しない
- IP使用率(%): 0% (0 / 0 max)

At the bottom of the page, there is a row of control buttons: '起動' (highlighted with a red box), '停止', 'Active昇格', '初期化', 'リース情報全消去', 'MACアドレス使用履歴全消去', and '状態の更新'.

4. Aruba IAP 305 の設定

Aruba IAP 305 は初期値として IP アドレスが設定されていません。管理画面にアクセスするためには、DHCP サーバーが動作している環境で利用するか、またはコンソールケーブルを用いて IP アドレスを設定する必要があります。今回は、D3 で静的に割り当てた IP アドレスを仕様し、管理画面へのアクセスを行います。

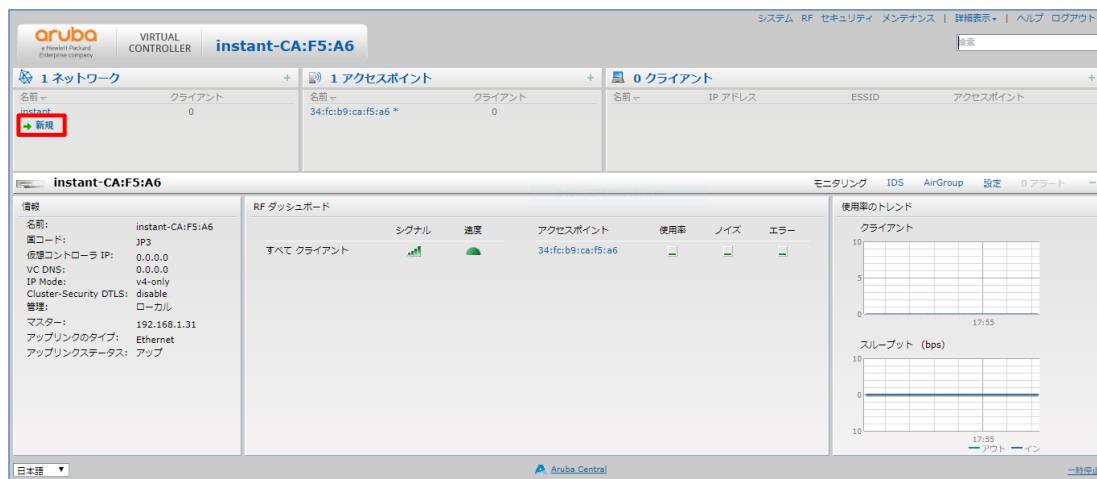
アクセスする URL は、<http://192.168.1.1>、
初期ユーザー名/パスワードは、admin/admin です。

セットアップは下記の流れで行います。

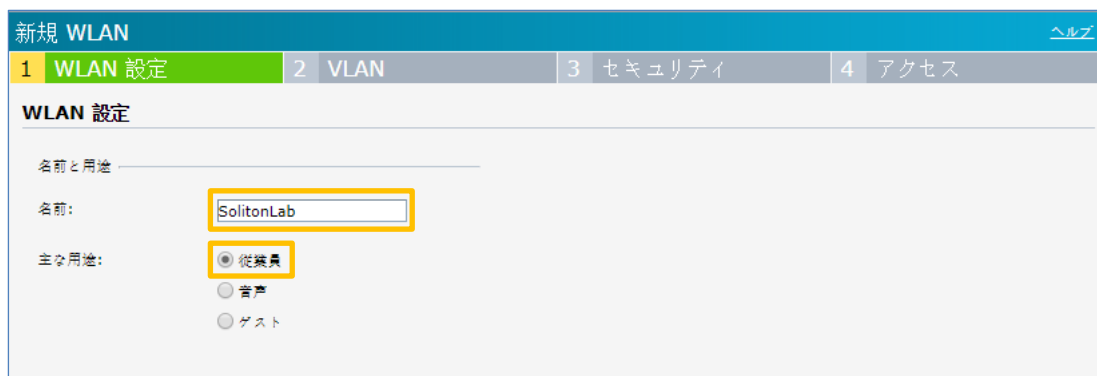
1. WLAN 設定
2. VLAN 設定
3. セキュリティ設定
4. アクセス設定

4-1 WLAN 設定

「新規」ボタンより、SSID を作成します。デフォルト状態では「instant」という SSID が登録されていますが、新規に SSID を作成すると自動的に消去されます。



「名前」欄に SSID を設定します。ここで設定した文字列 SSID 名として出力されます。



項目	値
名前	SolitonLab
主な用途	従業員

- ・ 従業員 → ゲスト、音声以外
- ・ 音声 → Wi-Fi を利用して音声通話が発生する場合
- ・ ゲスト → Web 認証

4-2 VLAN 設定

クライアント IP の割り当てが「ネットワーク割り当て」の場合、Instant AP はブリッジとして動作し、SSID と紐付けた VLAN 上にある DHCP サーバーより IP アドレスを取得します。クライアント VLAN の割り当てが「デフォルト」の場合、VLAN との紐付けをせず、Instant AP が所属するネットワークに接続されます。

新規 WLAN ヘルプ

1 WLAN 設定 2 VLAN 3 セキュリティ 4 アクセス

クライアント IP と VLAN の割り当て

クライアント IP の割り当て: 仮想コントローラ管理 ネットワーク割り当て

クライアント VLAN の割り当て: デフォルト スタティック ダイナミック

項目	値
クライアント IP の割り当て	ネットワーク割り当て
クライアント VLAN の割り当て	デフォルト

4-3 セキュリティ設定

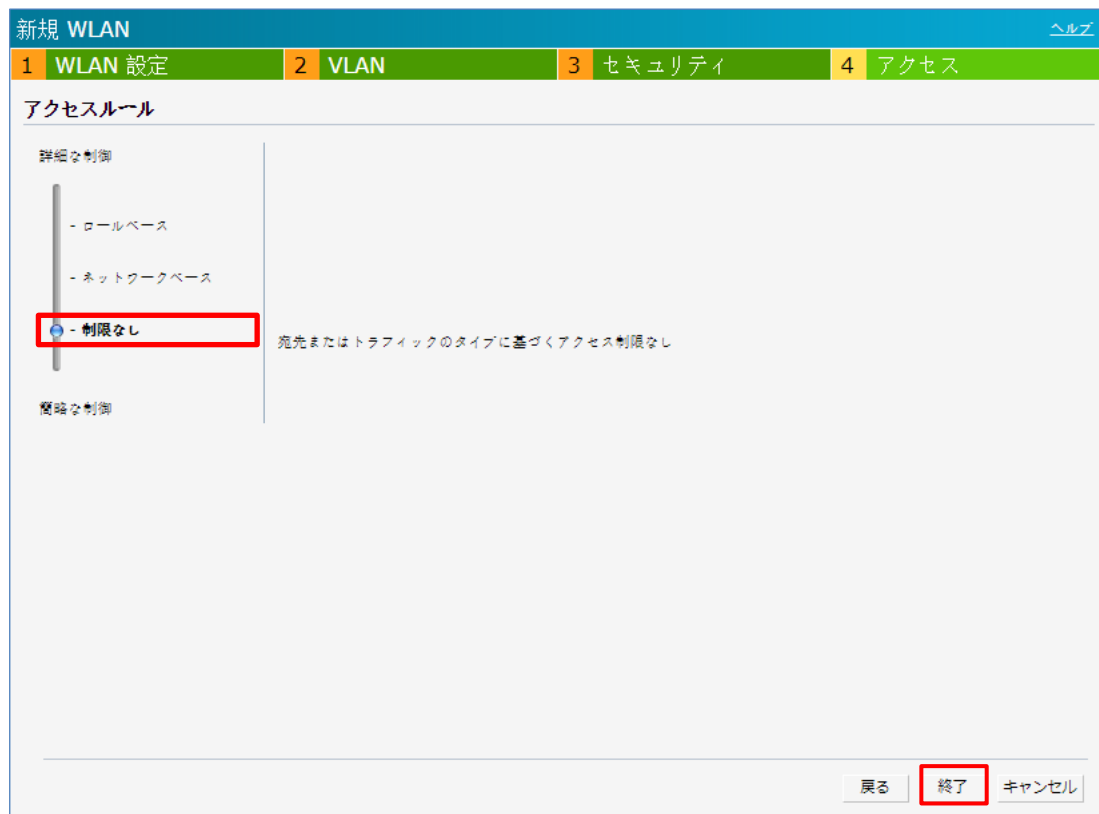
セキュリティレベルの設定を行います。外部認証サーバーとして EPS を指定してください。

The screenshot shows the 'Security Level' configuration page. The 'Security Level' slider is set to 'Enterprise' (エンタープライズ). The 'Authentication Server 1' dropdown is set to 'Internal Server' (内部サーバー). A modal window for adding a new server is open, with fields for Name (NetAttestEPS), IP Address (192.168.1.2), RadSec (None), Authentication Port (1812), Accounting Port (1813), Shared Key, and Key Re-entry (secret).

項目	値
認証サーバー	外部サーバー
- 名前	NetAttestEPS
- IP アドレス	192.168.1.2
- RadSec	無効
- 認証ポート	1812
- アカウンティングポート	1813
- 共有キー/共有キーの再入力	secret

4-4 アクセス設定

セキュリティ画面にて「次へ」を押下するとアクセスルールの設定画面が表示されます。今回はアクセス制限を行いませんので「制限なし」を選択し、終了を押下します。



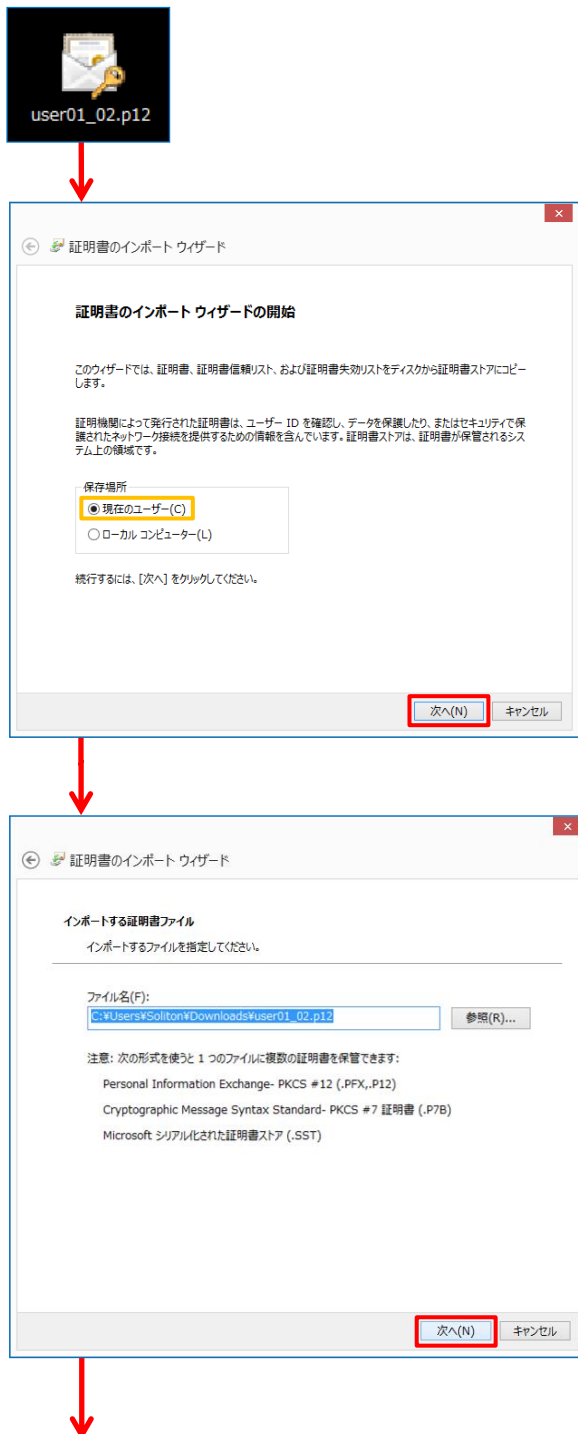
以上で Aruba IPA 305 の設定は完了です。

5. EAP-TLS 認証でのクライアント設定

5-1 Windows 10 での EAP-TLS 認証

5-1-1 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。



証明書の入ポート 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)

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

証明書の入ポート 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

証明書の入ポート 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	PFX
ファイル名	C:\Users\Soliton\Downloads\User01_02.p12

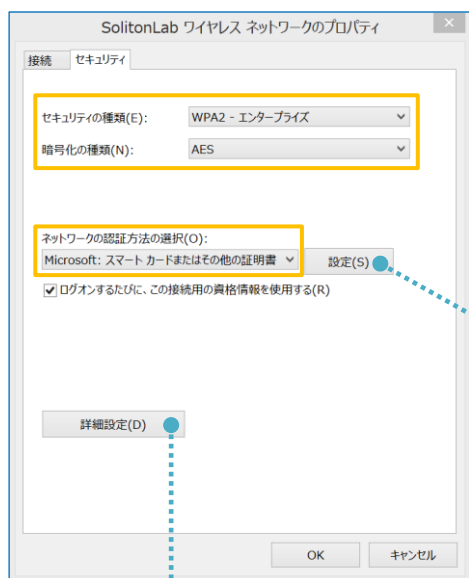
完了(F) キャンセル

5-1-2 サプリカント設定

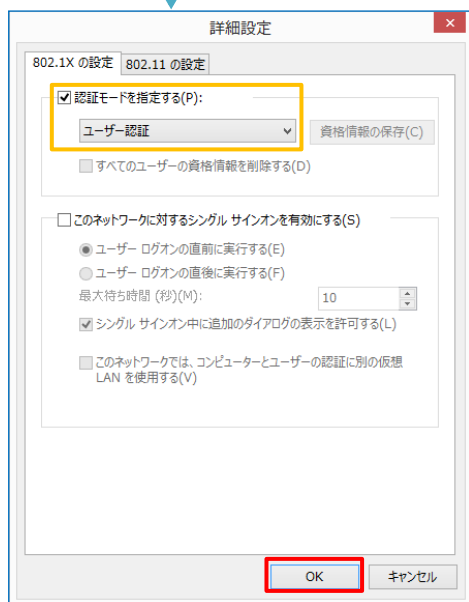
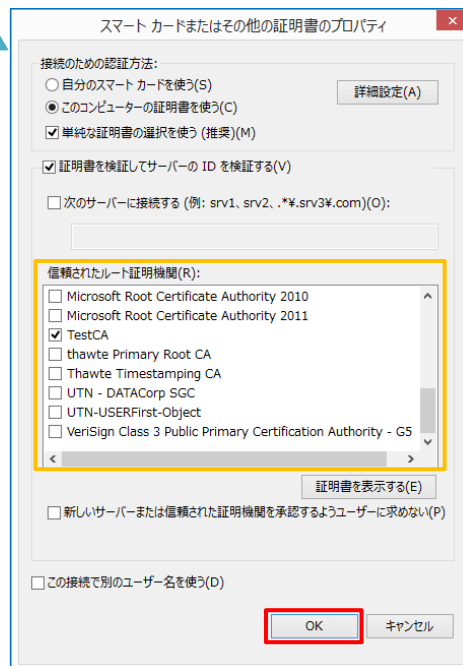
Windows 標準サプリカントで TLS の設定を行います。

※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

5-2 iOS での EAP-TLS 認証

5-2-1 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)

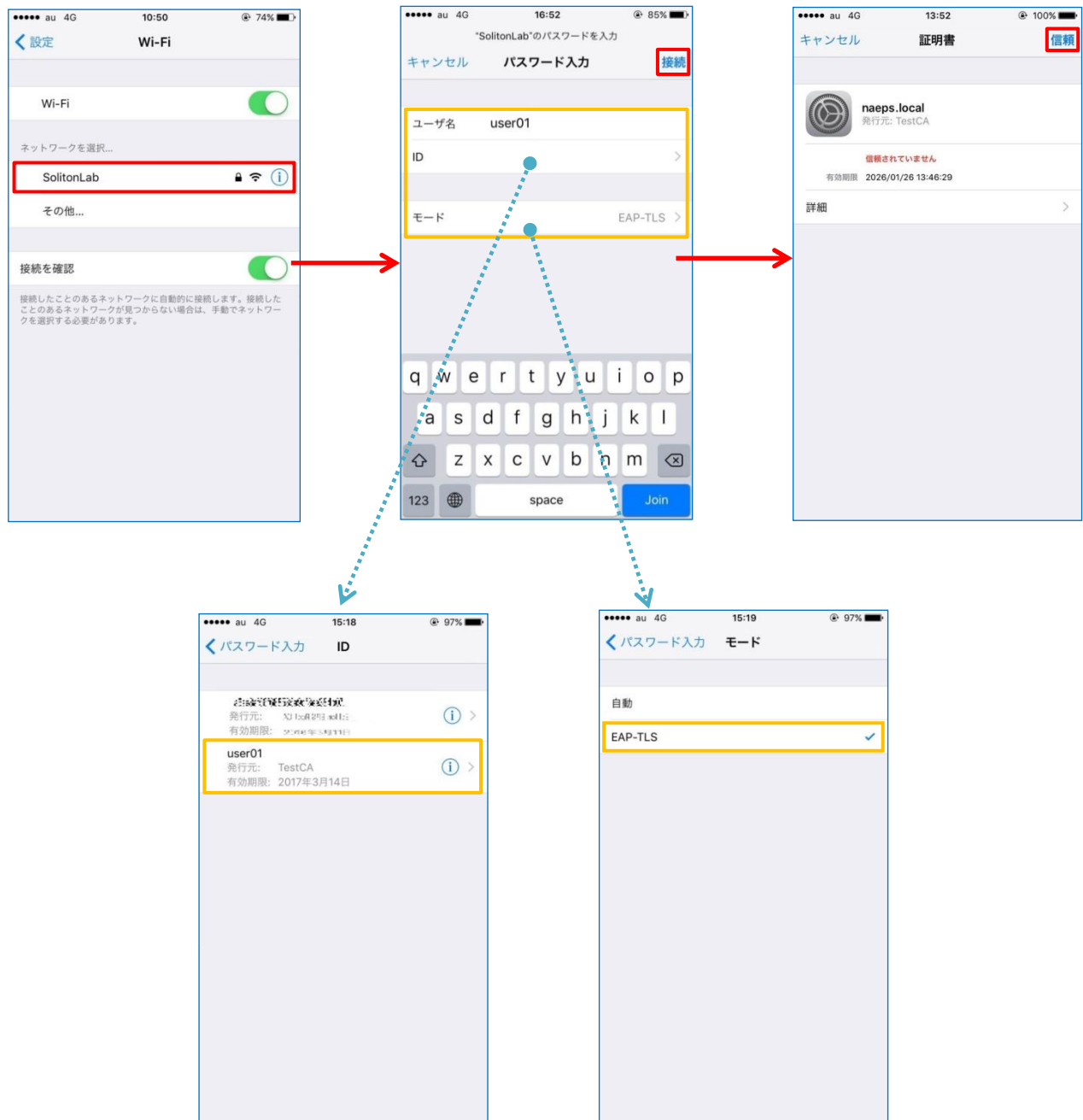
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

5-2-2 サプリカント設定

Aruba IAP 305 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。



5-3 Android での EAP-TLS 認証

5-3-1 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 7.0 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。

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:
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

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

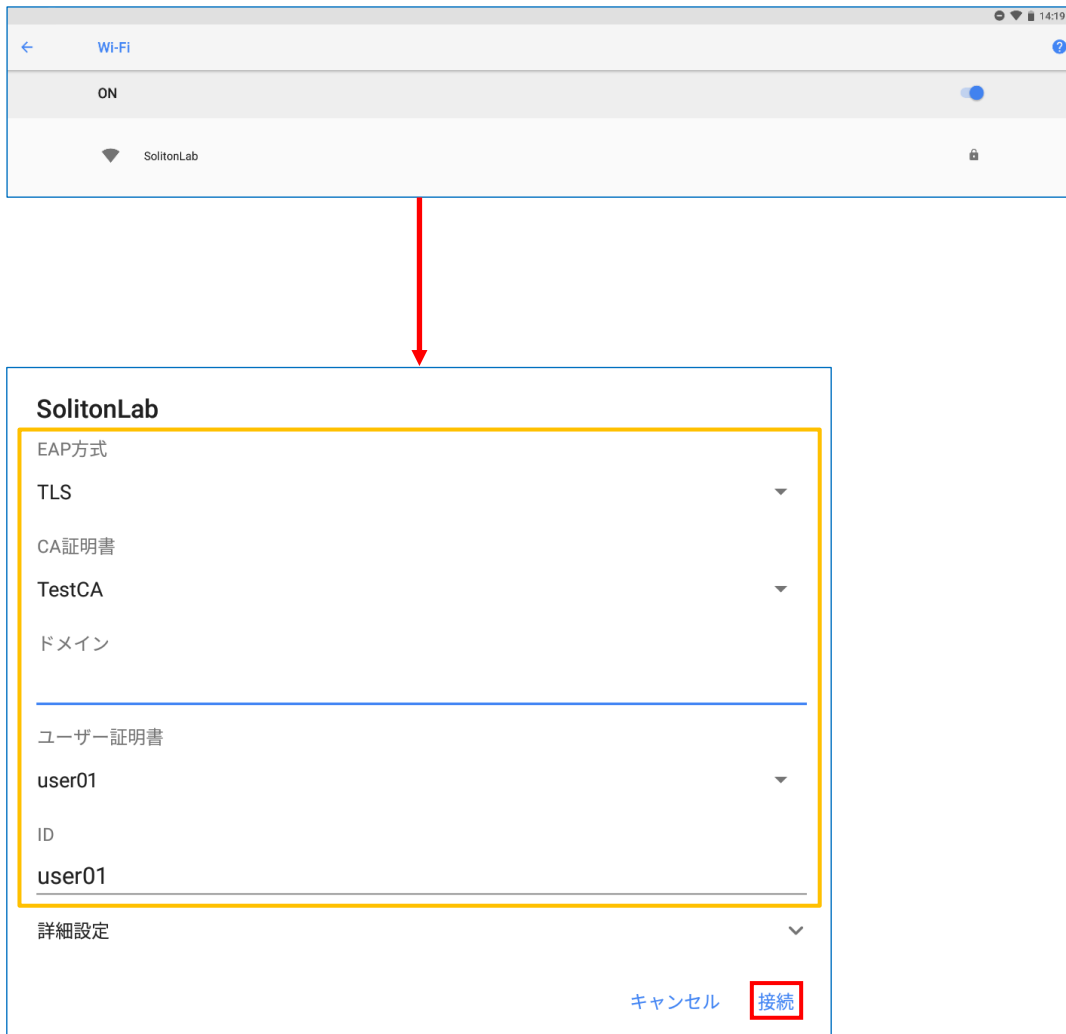
キャンセル

5-3-2 サプリカント設定

Aruba IAP 305 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。



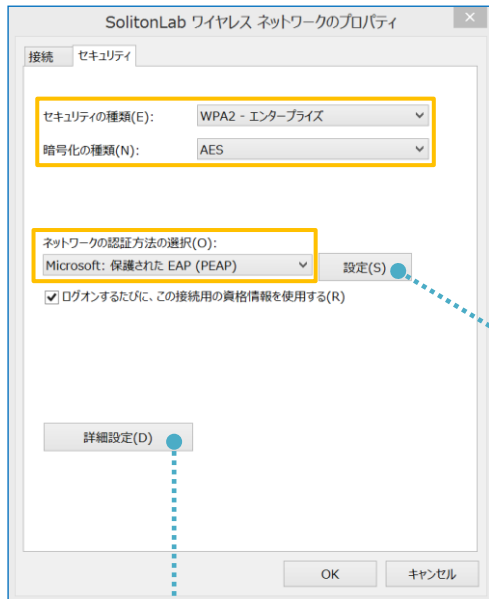
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

6. EAP-PEAP 認証でのクライアント設定

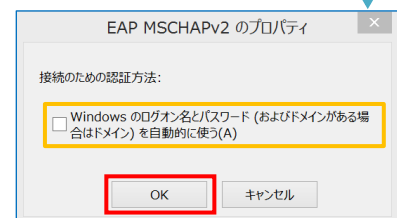
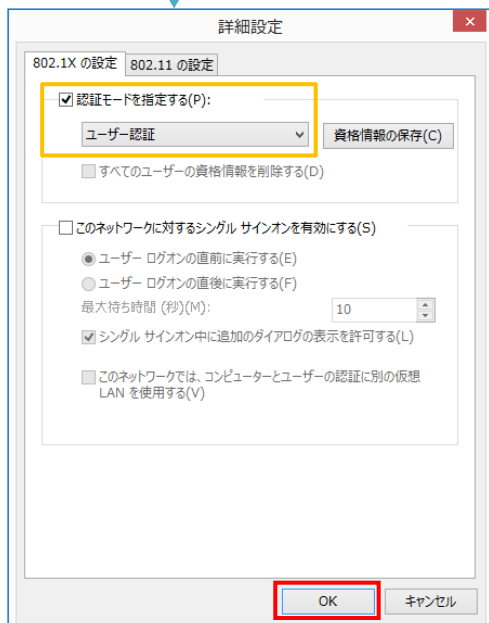
6-1 Windows 10 での EAP-PEAP 認証

6-1-1 Windows 10 のサブライアント設定

[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
- Windows のログオン名と・・・	Off

6-2 iOS での EAP-PEAP 認証

6-2-1 iOS のサブリカント設定

Aruba IAP 305 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。

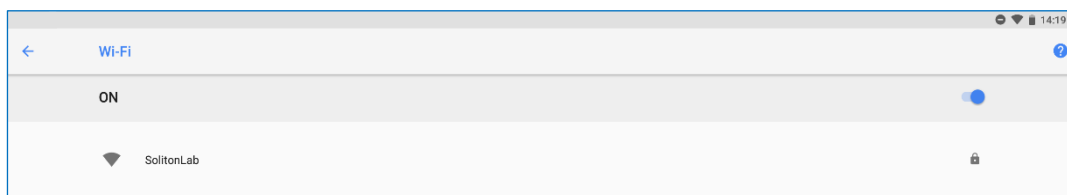


項目	値
ユーザ名	user01
パスワード	password
モード	自動

6-3 Android での EAP-PEAP 認証

6-3-1 Android のサブリカント設定

Aruba IAP 305 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 ▼

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

7. 動作確認結果

7-1 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[11573]: notice 2018/06/12 16:59:05 Login OK: [user01] (from client WirelessAP port 0 cli 701ce72f9f54)																								
Aruba IAP 305	<table border="1"> <thead> <tr> <th>名前</th> <th>IP アドレス</th> <th>MAC アドレス</th> <th>OS</th> <th>ESSID</th> <th>アクセスポイント</th> <th>チャンネル</th> <th>タイプ</th> <th>ロール</th> <th>IPv6 Address</th> <th>シグナル</th> <th>速度 (mbps)</th> </tr> </thead> <tbody> <tr> <td>user01</td> <td>192.168.1.100</td> <td>70:1ce7:2f:9f:54</td> <td>--</td> <td>SolitonLab</td> <td>34:fc:b9:ca:f5:a6</td> <td>100E</td> <td>AC</td> <td>SolitonLab</td> <td>fe80::ad1a:2. 57</td> <td></td> <td>234</td> </tr> </tbody> </table>	名前	IP アドレス	MAC アドレス	OS	ESSID	アクセスポイント	チャンネル	タイプ	ロール	IPv6 Address	シグナル	速度 (mbps)	user01	192.168.1.100	70:1ce7:2f:9f:54	--	SolitonLab	34:fc:b9:ca:f5:a6	100E	AC	SolitonLab	fe80::ad1a:2. 57		234
名前	IP アドレス	MAC アドレス	OS	ESSID	アクセスポイント	チャンネル	タイプ	ロール	IPv6 Address	シグナル	速度 (mbps)														
user01	192.168.1.100	70:1ce7:2f:9f:54	--	SolitonLab	34:fc:b9:ca:f5:a6	100E	AC	SolitonLab	fe80::ad1a:2. 57		234														

7-2 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[19514]: notice 2018/06/12 17:21:04 Login OK: [user01] (from client WirelessAP port 0 cli 701ce72f9f54 via proxy to virtual server) naeps radiusd[19514]: notice 2018/06/12 17:21:04 Login OK: [user01] (from client WirelessAP port 0 cli 701ce72f9f54)																								
Aruba IAP 305	<table border="1"> <thead> <tr> <th>名前</th> <th>IP アドレス</th> <th>MAC アドレス</th> <th>OS</th> <th>ESSID</th> <th>アクセスポイント</th> <th>チャンネル</th> <th>タイプ</th> <th>ロール</th> <th>IPv6 Address</th> <th>シグナル</th> <th>速度 (mbps)</th> </tr> </thead> <tbody> <tr> <td>user01</td> <td>192.168.1.100</td> <td>70:1ce7:2f:9f:54</td> <td>--</td> <td>SolitonLab</td> <td>34:fc:b9:ca:f5:a6</td> <td>100E</td> <td>AC</td> <td>SolitonLab</td> <td>fe80::ad1a:2. 57</td> <td></td> <td>234</td> </tr> </tbody> </table>	名前	IP アドレス	MAC アドレス	OS	ESSID	アクセスポイント	チャンネル	タイプ	ロール	IPv6 Address	シグナル	速度 (mbps)	user01	192.168.1.100	70:1ce7:2f:9f:54	--	SolitonLab	34:fc:b9:ca:f5:a6	100E	AC	SolitonLab	fe80::ad1a:2. 57		234
名前	IP アドレス	MAC アドレス	OS	ESSID	アクセスポイント	チャンネル	タイプ	ロール	IPv6 Address	シグナル	速度 (mbps)														
user01	192.168.1.100	70:1ce7:2f:9f:54	--	SolitonLab	34:fc:b9:ca:f5:a6	100E	AC	SolitonLab	fe80::ad1a:2. 57		234														

