

# **NetAttest EPS**

認証連携設定例

【連携機器】フルノシステムズ ACERA 1010/ACERA 1020/UNIFAS Managed Server

【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、フルノシステムズ社製無線アクセスポイント ACERA 1010/ACERA 1020 および無線ネットワーク管理システム UNIFAS Managed Server 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 ACERA 1010/ACERA 1020/UNIFAS Managed Server 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. ACERA 1010/ACERA 1020/ UNIFAS Managed Server の設定....	13
3-1 UNIFAS Managed Server の設定の流れ.....	13
3-2 UNIFAS Managed Server のログイン.....	14
3-3 UNIFAS Managed Server へセキュリティグループの登録.....	16
3-4 UNIFAS Managed Server へ ACERA を登録.....	21
4. EAP-TLS 認証でのクライアント設定.....	28
4-1 Windows 10 での EAP-TLS 認証.....	28
4-1-1 クライアント証明書のインポート.....	28
4-1-2 サプリカント設定.....	30
4-2 iOS(iPhone 6)での EAP-TLS 認証.....	31
4-2-1 クライアント証明書のインポート.....	31
4-2-2 サプリカント設定.....	32
4-3 Android(Pixel C)での EAP-TLS 認証.....	33
4-3-1 クライアント証明書のインポート.....	33
4-3-2 サプリカント設定.....	34
5. EAP-PEAP 認証でのクライアント設定.....	35
5-1 Windows 10 のサプリカント設定.....	35
5-2 iOS(iPhone 6)のサプリカント設定.....	36

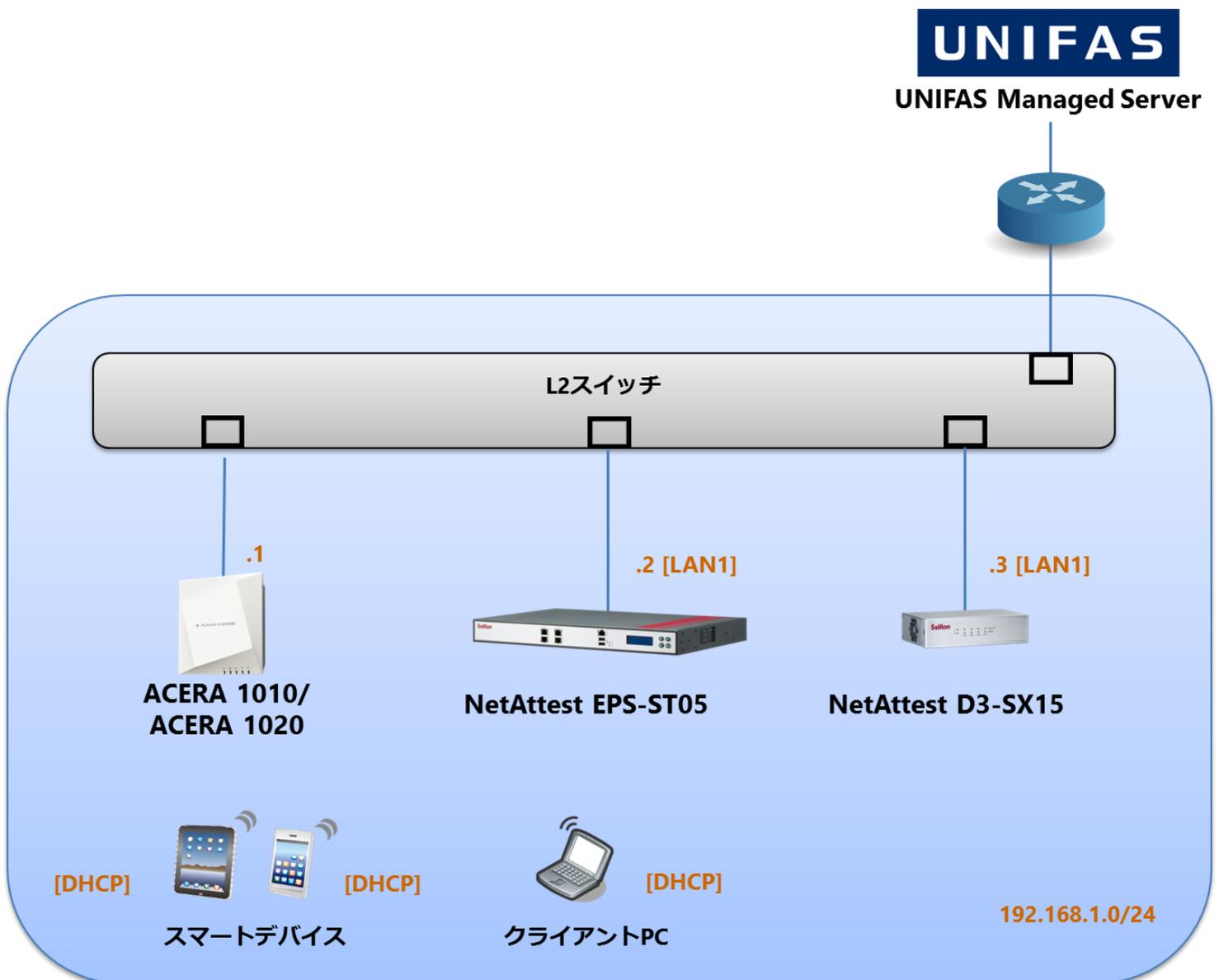
5-3 Android(Pixel C)のサブリカント設定.....	37
<b>6. 動作確認結果.....</b>	<b>38</b>
6-1 EAP-TLS 認証.....	38
6-2 EAP-PEAP(MS-CHAP V2)認証.....	38

# 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-SX15 の DHCP サーバーから払い出す
- UNIFAS Managed Server はその他の機器とは別のセグメントに配置
- RADIUS の通信は ACERA 1010/ACERA 1020 と EPS の間で行われる



## 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	4.8.9
ACERA 1010/ ACERA 1020	フルノシステムズ	RADIUS クライアント (無線アクセスポイント)	01.04
UNIFAS Managed Server	フルノシステムズ	無線ネットワーク管理システム	2.60
Let's note	Panasonic	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブプリカント
iPhone 6	Apple	802.1X クライアント (Client SmartPhone)	10.2
Pixel C	Google	802.1X クライアント (Client Tablet)	7.1.1
NetAttest D3-SX15	ソリトンシステムズ	DHCP/DNS サーバー	4.2.9

### 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
ACERA 1010/ ACERA 1020	192.168.1.1/24		secret
UNIFAS Managed Server	別セグメントに配置		
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。

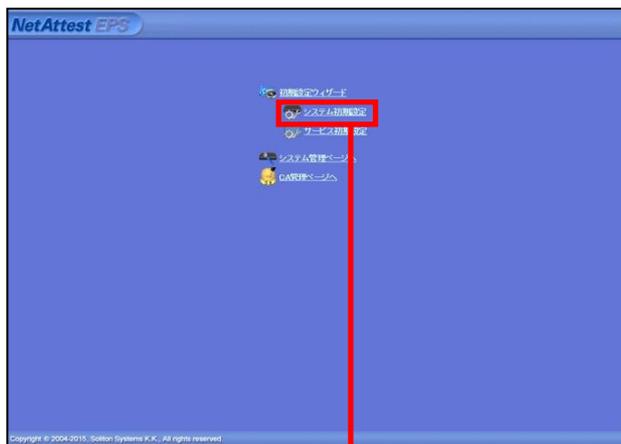
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

## 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.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 © 2004-2016, 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

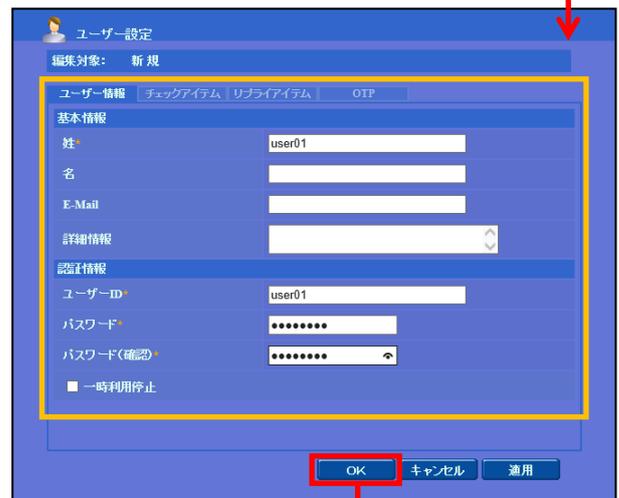
## 2-4 ユーザーの登録

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。



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)

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

# 3. ACERA 1010/ACERA 1020/ UNIFAS Managed Server の設定

## 3-1 UNIFAS Managed Server の設定の流れ

---

下記は ACERA 1010/ACERA 1020 の初期設定が完了していることを前提に、UNIFAS Managed Server の設定手順を示したものです。

1. UNIFAS Managed Server へのログイン
2. UNIFAS Managed Server へセキュリティグループの登録
3. UNIFAS Managed Server へ ACERA の登録

## 3-2 UNIFAS Managed Server のログイン

UNIFAS Managed Server の設定を行うには、ブラウザでアクセスする必要があります。

アクセス URL:

https:// <UNIFAS Managed Server>/UNIFAS/MS/admin/login.php

アクセスすると下記のようなログイン画面が表示されます。

各項目に値を入力しログインしてください。

項目	値
管理サイト名	mysite
ログイン ID	admin
ログインパスワード	admin

### 【管理サイト】

ログイン対象となる管理サイト名を入力します。

- トップサイト名 : (例) FURUNOSYSTEMS
- サブサイト名 : (例) Soliton
- サブサイト名.トップサイト名 : (例) Soliton.FURUNOSYSTEMS

### 【ログイン ID】

対象サイトの管理者ログイン ID を入力します。

### 【ログインパスワード】

対象サイトの管理者ログインパスワードを入力します。

ログインすると、下記画面が表示されますので「管理メニュー」をクリックしてください。

「管理メニュー」を押下すると管理者メニュー画面が表示されます。

※下記画面は、ログイン画面の管理サイト名において、サブサイト名.トップサイト名でログインした状態です。

### 3-3 UNIFAS Managed Server へセキュリティグループの登録

アクセスポイントに紐付けを行うセキュリティグループの作成を行います。

「管理者メニュー」画面の[サイト管理] - [セキュリティグループ管理]を選択します。



UNIFAS Managed Server (HELP)  
管理者メニュー  
Soliton.FURUNOSYSTEMS

UNIFAS  
トップサイト管理へ戻る ログアウト

マイアカウント

- 管理者情報の変更
- ログインパスワードの変更

サイト管理

- 稼働スケジュール管理
- MACグループ管理
- セキュリティグループ管理**
- アクセスポイント管理
- 固定ユーザ管理
- 固定MAC管理
- ゲスト申請管理
- ゲストユーザ管理
- ゲスト認証管理
- UNIFAS認証管理
- 未登録アクセスポイント検出管理
- サイト設定
- 通知設定
- MORS設定
- サイトログ
- サイト内情報検索
- インポート/エクスポート
- 運用モード切替設定
- 外部連携設定

Copyright (C) FURUNO SYSTEMS CO.,LTD.

「セキュリティグループ管理」画面が表示されます。【グループの追加】ボタンを押下してください。



UNIFAS Managed Server (HELP)  
セキュリティグループ管理  
Soliton.FURUNOSYSTEMS

UNIFAS  
トップサイト管理へ戻る ログアウト

管理者メニュー

グループの追加

グループ名	ESSID	VLAN番号	編集
グループの追加			

Copyright (C) FURUNO SYSTEMS CO.,LTD.

「新規セキュリティグループ」画面が表示されます。下記画面の枠で示した項目の設定を行います。  
 枠で示した項目以外については任意で設定を行ってください。

UNIFAS Managed Server (HELP) UNIFAS

セキュリティグループ更新・削除 トップサイト管理へ戻る ログアウト

soliton.FURUNDYSYSTEMS

---

管理者メニュー セキュリティグループ設定

ESSID (*)	SolitonLab
グループ名(表示名) (*)	SolitonLab (最大 40 桁)
VLAN (*)	<input type="radio"/> VLANを使用する。VLAN No. <input type="text"/> (1~4092) <input type="radio"/> Dynamic VLANを使用する。 <input checked="" type="radio"/> VLANを使用しない。
QoS プライオリティ (*)	3
接続制限 (*)	<input checked="" type="radio"/> 制限しない。 <input type="radio"/> 制限する。制限台数: <input type="text"/> (1~127)
ステルスモード (*)	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
無線リンク監視	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 (監視レベル: <input type="text"/> 再接続待ち時間: <input type="text"/> 秒)
無線セパレータ (*)	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 (例外アドレス <input type="text"/> )
動作モード (*)	<input checked="" type="radio"/> 通常 <input type="radio"/> MDRS モード (MDRSフィルタ <input type="text"/> )
MACフィルタ (*)	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効 (MACグループ: <input type="text"/> レベル: <input type="radio"/> 標準 <input checked="" type="radio"/> 高)
認証方式 (*)	RADIUS認証 (WPA2-Enterprise / AES)
暗号方式 (*)	なし / UNIFAS 認証 B、RADIUS 認証で指定
WEP設定 ※暗号方式にWEPを選択時に必須です。	
暗号化キー	<input type="text"/> <small>(64bitは10桁、128bitは26桁の16進数を入力)</small> <small>自動生成 64bit(10桁) 128bit(26桁)</small>
WPA-PSK設定 ※暗号方式にWPA-PSK/WPA2-Personal/WPA-Mixedを選択時に必須です。	
PSK (Pre-Shared Key)	<input type="text"/> <small>(8~63桁の英数記号/スペースを入力)</small> <small>自動生成 63桁</small>
キー更新間隔	1800 秒 (1~9999)
PMF	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効(自動選択) <input type="radio"/> 有効(必須)

項目	値
ESSID	SolitonLab
グループ名	SolitonLab
ステルスモード	無効
認証方式	RADIUS 認証(WPA2-Enterprise / AES)
暗号方式	なし/UNIFAS 認証 B、RADIUS 認証で指定

RADIUS設定 ※認証方式でRADIUS認証を選択時に必須です。

認証サーバ	
プライマリ	
ホスト名	192.168.1.2
ポート番号	1812
クレデンシャル	secret (最大 16 桁)
セカンダリ ※任意	
ホスト名	
ポート番号	1812
クレデンシャル	(最大 16 桁)
共通設定	
デリミタ	-
アカウントingサーバ	
プライマリ	
ホスト名	
ポート番号	1813
クレデンシャル	(最大 16 桁)
セカンダリ ※任意	
ホスト名	
ポート番号	1813
クレデンシャル	(最大 16 桁)
共通設定	
デリミタ	-

稼働スケジュール ※スケジュールを選択した場合、スケジュール期間は既定モードと反対の状態となります。

既定モード (*)	<input checked="" type="radio"/> 稼働 <input type="radio"/> 非稼働
スケジュール	- 未設定 -

UNIFAS認証A オプション

認証画面設定	
使用画面 (*)	<input checked="" type="radio"/> 共通画面 <input type="radio"/> カスタム画面
カスタム画面アーカイブファイル	参照... ファイルが選択されていません。(未アップロード)
高速認証機能	
機能利用 (*)	<input type="radio"/> 無効 <input checked="" type="radio"/> 有効
Managed Server不在時認証ポリシー (*)	<input checked="" type="radio"/> 通過 <input type="radio"/> 拒否
メールアドレス認証	
機能利用 (*)	<input checked="" type="radio"/> 無効 <input type="radio"/> 有効
ID有効期間	1 日 (1 - 365)
1回に接続できる時間	15 分 (1 - 4320)
1日の利用回数	4 回 (1 - 1440)

更新 リセット

### 【ESSID】

ESSIDを入力してください。

### 【グループ名】

セキュリティグループ名を入力します。(UNIFAS 上で表示させる名前です)

項目	値
ホスト名	192.168.1.2
ポート番号	1812
クレデンシャル	secret

## 【ステルスモード】

有効/無効のいずれかを選択してください。

## 【認証方式】

認証方式は以下の赤枠の中から選択してください。

- なし
- UNIFAS認証A (独自方式)
- UNIFAS認証A (独自方式/RADIUS)
- UNIFAS認証B (802.1x / WEP)
- UNIFAS認証B (WPA2-Enterprise / TKIP)
- UNIFAS認証B (WPA2-Enterprise / AES)
- UNIFAS認証B (WPA2-Enterprise / Auto)
- UNIFAS認証B (WPA-Enterprise / TKIP)
- UNIFAS認証B (WPA-Enterprise / AES)
- UNIFAS認証B (WPA-Enterprise / Auto)
- UNIFAS認証B (WPA-Mixed Ent / TKIP)
- UNIFAS認証B (WPA-Mixed Ent / AES)
- UNIFAS認証B (WPA-Mixed Ent / Auto)
- RADIUS認証 (802.1x / WEP)
- RADIUS認証 (WPA2-Enterprise / TKIP)
- RADIUS認証 (WPA2-Enterprise / AES)
- RADIUS認証 (WPA2-Enterprise / Auto)
- RADIUS認証 (WPA-Enterprise / TKIP)
- RADIUS認証 (WPA-Enterprise / AES)
- RADIUS認証 (WPA-Enterprise / Auto)
- RADIUS認証 (WPA-Mixed Ent / TKIP)
- RADIUS認証 (WPA-Mixed Ent / AES)
- RADIUS認証 (WPA-Mixed Ent / Auto)
- RADIUS MAC認証SINGLE (独自方式)
- RADIUS MAC認証HYBRID (独自方式)

## 【暗号方式】

認証方式に RADIUS 認証を選択した場合、「なし/UNIFAS 認証 B、RADIUS 認証で指定」を選択してください。

- なし / UNIFAS認証B、RADIUS認証で指定
- WEP
- TKIP (WPA-PSK)
- TKIP (WPA2-Personal)
- TKIP (WPA-Mixed)
- AES (WPA-PSK)
- AES (WPA2-Personal)
- AES (WPA-Mixed)
- Auto (WPA-PSK)
- Auto (WPA2-Personal)
- Auto (WPA-Mixed)

## 【RADIUS サーバー】

RADIUS サーバーは、プライマリ・セカンダリを登録することができます。

【ホスト名】 RADIUS サーバー NetAttest EPS を指定 (FQDN もしくは、IP アドレス)

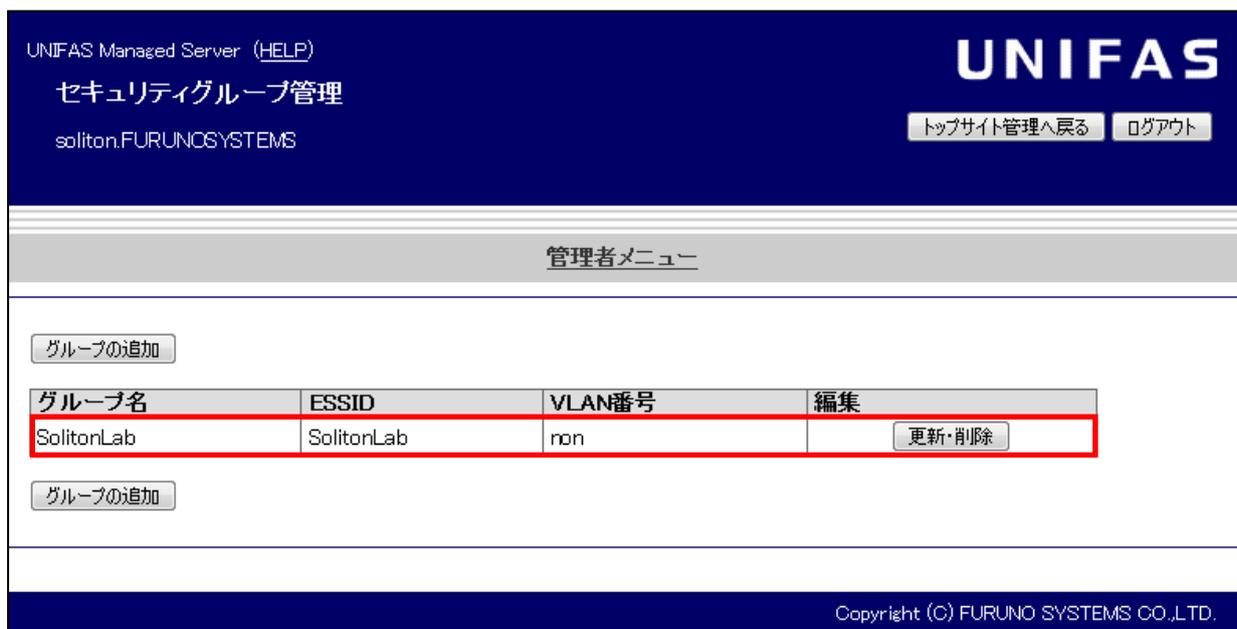
【ポート番号】 1812 (RADIUS サーバーで利用するポート番号)

【クレデンシャル】 secret (最大 16 桁まで設定可能)

設定項目を入力後、【追加】ボタンを押下します。セキュリティグループが登録されると下記画面が表示されます。



【セキュリティグループ設定】を選択すると、下記画面が表示されます。登録したグループ名が表示されていることを確認してください。

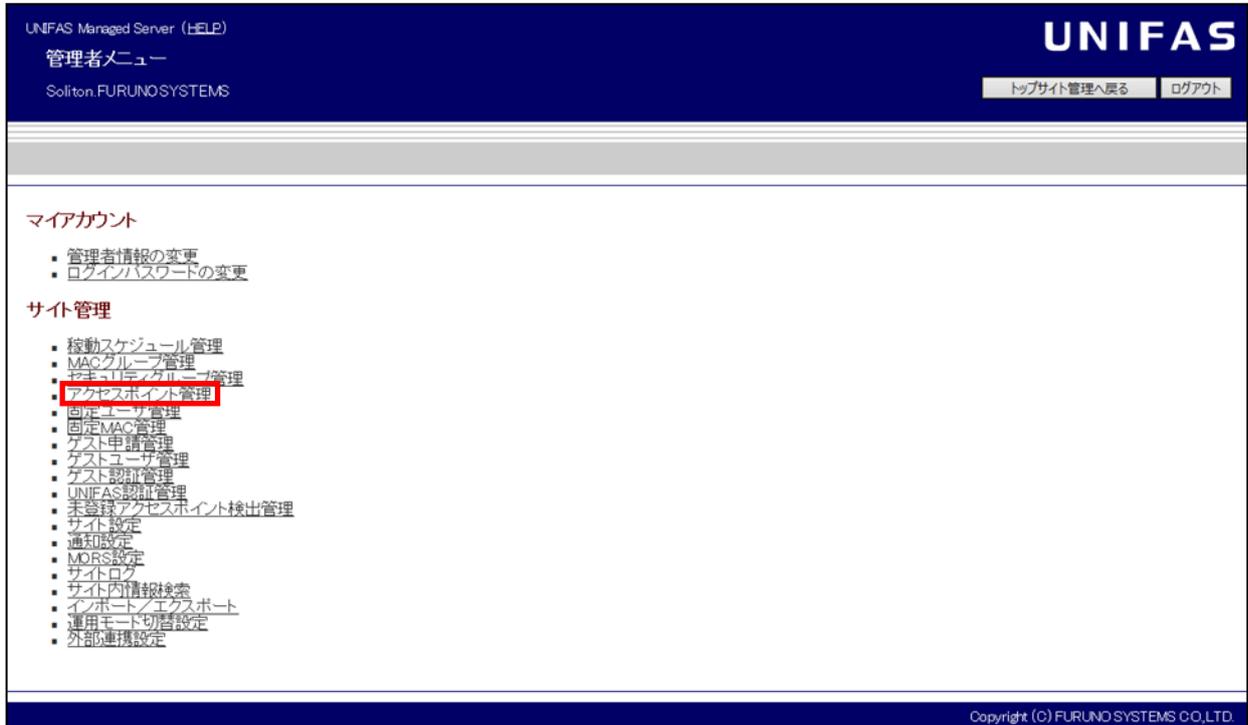


【管理者メニュー】を選択すると、「管理者メニュー」画面に戻ります。

## 3-4 UNIFAS Managed Server へ ACERA を登録

アクセスポイントの追加・更新・削除を行います。

「管理者メニュー」画面の [サイト管理] - [アクセスポイント管理]を選択します。



UNIFAS Managed Server (HELP)  
管理者メニュー  
Soliton.FURUNOSYSTEMS

UNIFAS  
トップサイト管理へ戻る ログアウト

マイアカウント

- 管理者情報の変更
- ログインパスワードの変更

サイト管理

- 稼働スケジュール管理
- MACグループ管理
- アクセスポイント管理
- 固定ユーザ管理
- 固定MAC管理
- ゲスト申請管理
- ゲストユーザ管理
- ゲスト認証管理
- UNIFAS認証管理
- 未登録アクセスポイント検出管理
- サイト設定
- 通知設定
- MORS設定
- サイトログ
- サイト内情報検索
- インポート/エクスポート
- 運用モード切替設定
- 外部連携設定

Copyright (C) FURUNO SYSTEMS CO.,LTD.

「アクセスポイント管理者」画面の [アクセスポイント管理] - [アクセスポイント設定]を選択します。



UNIFAS Managed Server (HELP)  
アクセスポイント管理  
Soliton.FURUNOSYSTEMS

UNIFAS  
トップサイト管理へ戻る ログアウト

管理者メニュー

アクセスポイント管理メニュー

- アクセスポイント設定
- アクセスポイント設定スケジュール
- アクセスポイントSNMP設定
- ワイレスディスプレイ設定
- アクセスポイントセルフチェック
- アクセスポイントアラート設定
- アクセスポイントマップ管理
- アクセスポイント再起動

Copyright (C) FURUNO SYSTEMS CO.,LTD.

「アクセスポイント設定」画面が表示されます。

【アクセスポイントの追加】ボタンを押下してください。

UNIFAS Managed Server (HELP) **UNIFAS**  
アクセスポイント設定  
Soliton.FURUNOSYSTEMS [トップサイト管理へ戻る](#) [ログアウト](#)

管理者メニュー アクセスポイント管理

**アクセスポイントの追加**

アクセスポイント名	機種	Version	最終起動時刻	稼働状況	情報表示	編集
<a href="#">アクセスポイントの追加</a>						

Copyright (C) FURUNO SYSTEMS CO.,LTD.

「アクセスポイント機種選択」画面が表示されます。登録を行うアクセスポイントの機種を選択し、【選択】ボタンを押下してください。

機種: **ACERA1010**  
**ACERA1020**  
ACERA900  
ACERA950  
ACERA850M  
ACERA850F  
ACERA810  
ACERA800/WN-802  
WN-801

[選択](#)

ACERA 1010 または ACERA 1020 を選択します。

UNIFAS Managed Server (HELP) **UNIFAS**  
アクセスポイント機種選択  
soliton.FURUNOSYSTEMS [トップサイト管理へ戻る](#) [ログアウト](#)

管理者メニュー アクセスポイント管理 **アクセスポイント設定**

機種: **ACERA1020** [選択](#)

Copyright (C) FURUNO SYSTEMS CO.,LTD.

「新規アクセスポイント」画面が表示されます。

下記画面の枠で示した項目の設定を行います。枠で示した項目以外については、任意で設定を行ってください。

UNIFAS Managed Server (HELP)UNIFAS

アクセスポイント更新・削除トップサイト管理へ戻る ログアウト

soliton.FURUNGSYSTEMS

---

管理者メニュー アクセスポイント管理 **アクセスポイント設定**

---

機種名	ACERA1020
アクセスポイント名	AP01@soliton.FURUNGSYSTEMS
メモ	<input type="text" value=""/> (最大40文字)
利用場所	屋内 ▾
<b>有線LAN設定</b>	
DHCPの利用 ※DHCPを使用する場合は通常、IPアドレス・サブネットマスク・デフォルトゲートウェイ・DNSサーバの値が取得されます。	
<input type="checkbox"/> 使用する	
IPアドレス (*)	<input type="text" value="192.168.1.1"/>
サブネットマスク (*)	24 bit (0~32)
デフォルトゲートウェイ	<input type="text" value="192.168.1.254"/>
DNSサーバ (*)	プライマリ (*) <input type="text" value="8.8.8.8"/>
	セカンダリ <input type="text" value="8.8.4.4"/>
VLAN (*)	<input type="checkbox"/> 使用する VLAN No. <input type="text" value=""/> (1~4092)
Managed Server URL (*)	<input type="text" value="https://UNIFAS.co.jp/UNIFAS/MS/"/> (最大128文字)
PROXY Server	<input type="text" value=""/> (最大128文字)
PROXY Server ポート番号	<input type="text" value="8080"/> (0~65535)
VLANハイブリッド	無効 ▾
<b>ステーション設定</b>	
ステーション機能の利用	
<input checked="" type="radio"/> 使用しない <input type="radio"/> 無線LAN1を使用する <input type="radio"/> 無線LAN2を使用する	
<b>無線バンドステアリング機能</b>	
無効 ▾	
<b>無線LAN1設定</b>	
バンド	
11n/ac機能	
11n/acモード	
11n/acショートG設定	
11n/acパケット集約	
チャンネル	
送信出力	
無線通信公平化機能	
セキュリティグループ ※使用する場合に1つ以上選択して下さい。	
オンラインモード <input type="text" value="SolitonLab"/>	
オフラインモード(任意) <input type="text" value="SolitonLab"/>	

無線LAN 2 設定

バンド	802.11b/g				
11n 機能	有効				
11n モード	20MHz				
11n ショートG設定	使用しない				
11n パケット集約	A-MPDU/A-MSDU				
チャンネル	1 (802.11b/g) <input type="checkbox"/> 動的切替を有効にする				
送信出力	4				
無線通信公平化機能	無効				
セキュリティグループ ※使用する場合に1つ以上選択して下さい	<table border="1"> <tr> <td>オンラインモード</td> <td>オフラインモード (任意)</td> </tr> <tr> <td>SolitonLab</td> <td>SolitonLab</td> </tr> </table>	オンラインモード	オフラインモード (任意)	SolitonLab	SolitonLab
オンラインモード	オフラインモード (任意)				
SolitonLab	SolitonLab				

無線LAN IPマスカレード設定

IPマスカレードの利用	<input type="checkbox"/> 使用する
無線側IPアドレス (*) ※IPマスカレードを使用する場合、このアドレスが無線LAN端末のデフォルトゲートウェイとなります。	<input type="text"/>
サブネットマスク (*)	0 bit (0~32)
有線LAN側からの通信フィルタ(*)	<input checked="" type="checkbox"/> 使用する

DHCPサーバ設定

DHCPサーバ機能の利用 ※DHCPサーバ機能を利用する場合、DHCPプールIP開始アドレス/終了アドレス・DHCPリース時間の設定が必要です。	<input type="checkbox"/> 使用する				
DHCP使用時のDNSサーバ ※IPマスカレード使用時、DNSサーバの設定がない場合、有線LAN設定のDNSサーバ設定(有線側DHCP有効時は取得したDNSサーバ設定)で動作します。	<table border="1"> <tr> <td>プライマリ</td> <td><input type="text"/></td> </tr> <tr> <td>セカンダリ</td> <td><input type="text"/></td> </tr> </table>	プライマリ	<input type="text"/>	セカンダリ	<input type="text"/>
プライマリ	<input type="text"/>				
セカンダリ	<input type="text"/>				
DHCPプールIP開始アドレス (*)	<input type="text"/>				
DHCPプールIP終了アドレス (*)	<input type="text"/>				
DHCPリース時間 (*)	60 分(1~720)				

運用モード切替設定

オフラインモード切替	<input type="checkbox"/> 自動
監視機器IPアドレス	<input type="text"/>

未登録アクセスポイント検出設定

検出インタフェイス	無線LAN1
-----------	--------

【アクセスポイント名】

アクセスポイントのホスト名を入力してください。

## 【有線 LAN 設定】

- ・ IP アドレス、サブネットマスク、デフォルトゲートウェイアドレスを入力します。  
アクセスポイントを DHCP 設定で動作させる場合、「DHCP の利用」の「使用する」のチェックボックスにチェックを入れてください。
- ・ DNS サーバーを登録してください。  
プライマリ DNS サーバの登録は必須です。
- ・ Managed Server URL を入力します。  
(例) https://FQDN or IP アドレス/UNIFAS/MS/

## 【無線 LAN 設定】

- ・ バンド  
無線通信の周波数帯を指定します。  
※ACERA 1010/ACERA 1020 では無線 LAN の 1 と 2 でバンドを入れ替えることはできません。
- ・ 11n/ac 機能  
11n 機能の「有効」「無効」を選択します。
- ・ 11n/ac モード  
11n において「20MHz」（標準）モードと「40MHz」（拡張）モードの指定を行います。  
※本設定項目は、11n 機能を「有効」と設定した場合のみ、有効となります。  
※無線 LAN 1 では、「80MHz」も選択可。
- ・ 11n/ac ショート GI 設定  
11n においてショート GI 設定を使用するか、使用しないか指定を行います。  
※本設定項目は、11n 機能を「有効」と設定した場合のみ、有効となります。
- ・ 11n/ac パケット集約  
11n においてパケット集約方式を「無効」、「A-MSDU」、「A-MPDU」、「A-MPDU/A-MSDU」から選択します。  
※本設定項目は、11n 機能を「有効」と設定した場合のみ、有効となります。
- ・ チャンネル  
無線通信の周波数帯の詳細を指定します。  
「自動設定」を選択した場合は ACERA 起動時に空いているチャンネルを使用します。  
「動的切替」を有効にした場合、稼働中チャンネルが重なった際に自動的に空いているチャンネルに切り替わります。

・送信出力

アクセスポイントの送信電波出力を設定します。

数値が大きいほど、出力は大きくなります。範囲は0～4です。

・無線通信公平化機能（デフォルト値：無効）

11b/11g/11nまたは、11a/11n/11acが混在する無線環境において、無線バンドに関わらずクライアント毎に無線空間時間を公平に割り当てることにより、通信効率を改善する設定を行います。

有効 … クライアント毎に無線空間時間を公平に割り当て、混在時の通信効率を改善します。

無効 … クライアントの能力に応じ、無線空間時間を割り当てます。

※ACERA 1010 の場合、本設定項目は表示されません。

・セキュリティグループ

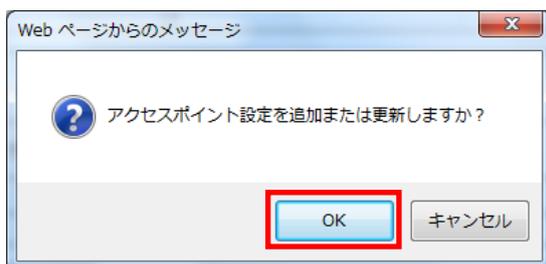
「セキュリティグループ管理」で登録したセキュリティグループ名が表示されます。

アクセスポイントでサービスするセキュリティグループを選択します。

無線 LAN1、LAN2 がありますので、それぞれの無線機に紐付けるセキュリティグループを選択します。無線 LAN 毎に複数選択することが可能です。

設定項目を入力し【追加】ボタンを押下すると、下記画面が表示されます。

【OK】ボタンを押下してください。



アクセスポイント設定が登録されると下記画面が表示されます。

UNIFAS Managed Server (HELP) **UNIFAS**  
新規アクセスポイント  
Soliton.FURUNOSYSTEMS [トップサイト管理へ戻る](#) [ログアウト](#)

管理者メニュー [アクセスポイント管理](#) **アクセスポイント設定**

アクセスポイントを追加しました。

Copyright (C) FURUNO SYSTEMS CO.,LTD.

[アクセスポイント設定]を選択し、登録した情報が表示されていることを確認してください。

UNIFAS Managed Server (HELP) **UNIFAS**  
アクセスポイント設定  
soliton.FURUNOSYSTEMS [トップサイト管理へ戻る](#) [ログアウト](#)

管理者メニュー [アクセスポイント管理](#)

[アクセスポイントの追加](#)

アクセスポイント名	機種	Version	最終起動時刻	稼働状況	情報表示	編集
AP01	ACERA1020				イベントログ ▼ <a href="#">一覧</a>	<a href="#">更新・削除</a>

[アクセスポイントの追加](#)

Copyright (C) FURUNO SYSTEMS CO.,LTD.

これにて ACERA 1010/ACERA 1020 の設定は終了です。

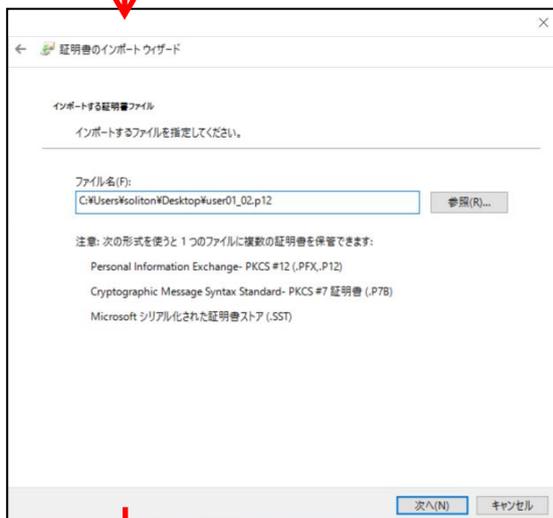
設定した電波 (ESSID) が出ていることを確認してください。

# 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

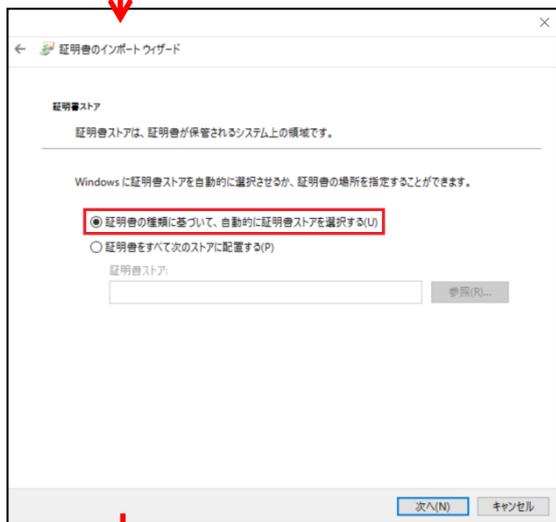
### 4-1-1 クライアント証明書のインポート

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\_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

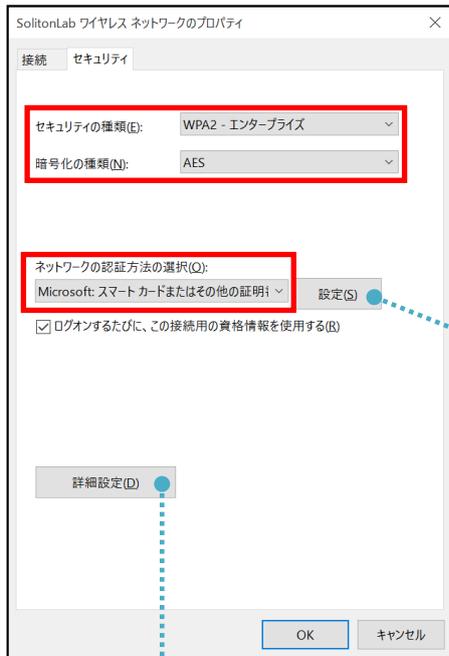


## 4-1-2 サプリカント設定

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

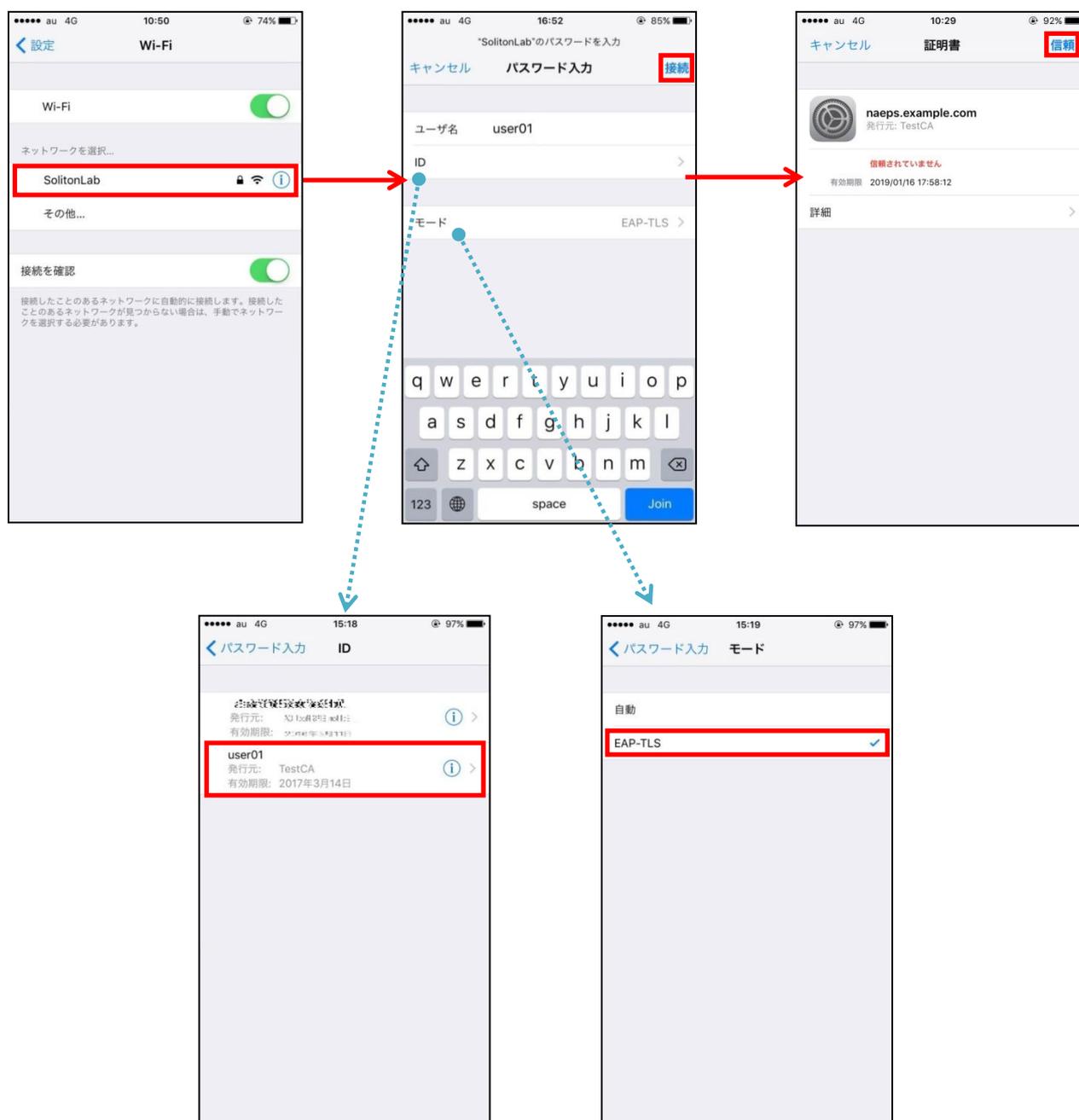
UNIFAS Managed Server で設定した SSID を選択し、サプリカントの設定を行います。

※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(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 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 7.1.1 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。

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 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

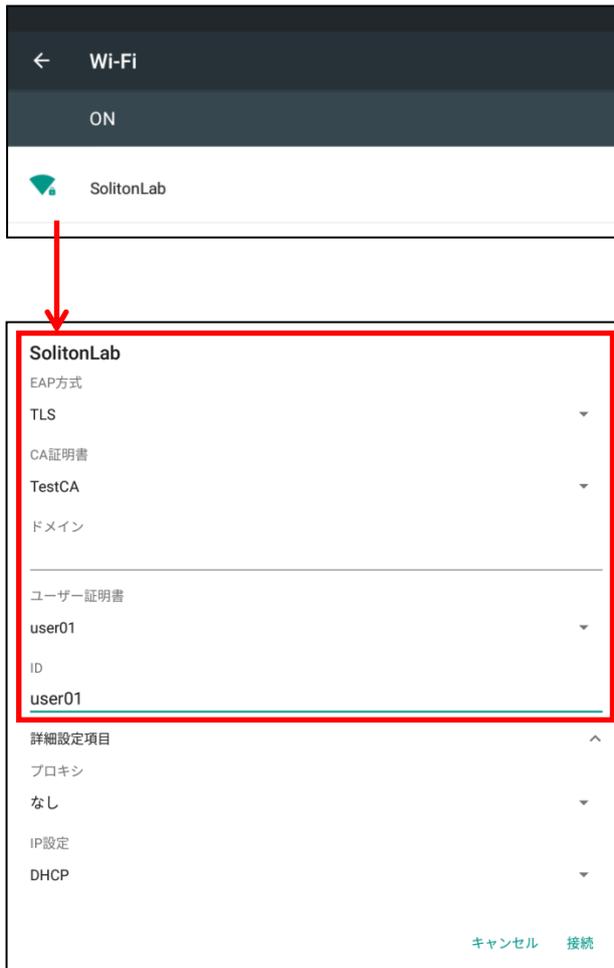
## 4-3-2 サプリカント設定

UNIFAS Managed Server 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ください。

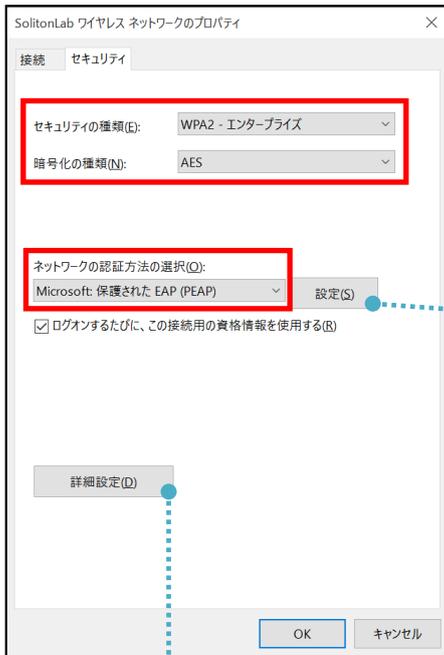


項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

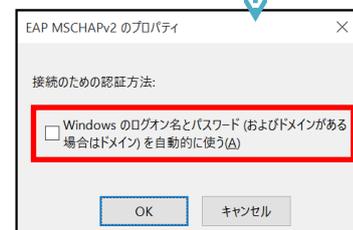
# 5. EAP-PEAP 認証でのクライアント設定

## 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	
- 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

UNIFAS Managed Server で設定した ESSID 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
ユーザー名	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

UNIFAS Managed Server で設定した ESSID 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	Login OK: [user01] (from client RadiusClient port 0 cli 34-F3-9A-1E-4F-CE)																		
ACERA 1010/ ACERA 1020/ UNIFAS Managed Server	<table border="1"><thead><tr><th>種別</th><th>認証</th></tr></thead><tbody><tr><td>日時</td><td>2017-01-12 14:27:45</td></tr><tr><td>アクセスポイント</td><td>AP01</td></tr><tr><td>ESSID</td><td>SolitonLab</td></tr><tr><td>BSSID</td><td>00:D0:1D:1A:93:19</td></tr><tr><td>MAC Address</td><td>34:F3:9A:1E:4F:CE</td></tr><tr><td>ID</td><td></td></tr><tr><td>発生場所</td><td>authinfo</td></tr><tr><td>発生理由</td><td>Radius_Authhticated(192.168.1.2)</td></tr></tbody></table>	種別	認証	日時	2017-01-12 14:27:45	アクセスポイント	AP01	ESSID	SolitonLab	BSSID	00:D0:1D:1A:93:19	MAC Address	34:F3:9A:1E:4F:CE	ID		発生場所	authinfo	発生理由	Radius_Authhticated(192.168.1.2)
種別	認証																		
日時	2017-01-12 14:27:45																		
アクセスポイント	AP01																		
ESSID	SolitonLab																		
BSSID	00:D0:1D:1A:93:19																		
MAC Address	34:F3:9A:1E:4F:CE																		
ID																			
発生場所	authinfo																		
発生理由	Radius_Authhticated(192.168.1.2)																		

### 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	Login OK: [user01] (from client RadiusClient port 0 cli 34-F3-9A-1E-4F-CE via proxy to virtual server) Login OK: [user01] (from client RadiusClient port 0 cli 34-F3-9A-1E-4F-CE)																		
ACERA 1010/ ACERA 1020/ UNIFAS Managed Server	<table border="1"><thead><tr><th>種別</th><th>認証</th></tr></thead><tbody><tr><td>日時</td><td>2017-01-12 14:46:36</td></tr><tr><td>アクセスポイント</td><td>AP01</td></tr><tr><td>ESSID</td><td>SolitonLab</td></tr><tr><td>BSSID</td><td>00:D0:1D:1A:93:19</td></tr><tr><td>MAC Address</td><td>34:F3:9A:1E:4F:CE</td></tr><tr><td>ID</td><td></td></tr><tr><td>発生場所</td><td>authinfo</td></tr><tr><td>発生理由</td><td>Radius_Authhticated(192.168.1.2)</td></tr></tbody></table>	種別	認証	日時	2017-01-12 14:46:36	アクセスポイント	AP01	ESSID	SolitonLab	BSSID	00:D0:1D:1A:93:19	MAC Address	34:F3:9A:1E:4F:CE	ID		発生場所	authinfo	発生理由	Radius_Authhticated(192.168.1.2)
種別	認証																		
日時	2017-01-12 14:46:36																		
アクセスポイント	AP01																		
ESSID	SolitonLab																		
BSSID	00:D0:1D:1A:93:19																		
MAC Address	34:F3:9A:1E:4F:CE																		
ID																			
発生場所	authinfo																		
発生理由	Radius_Authhticated(192.168.1.2)																		

