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。

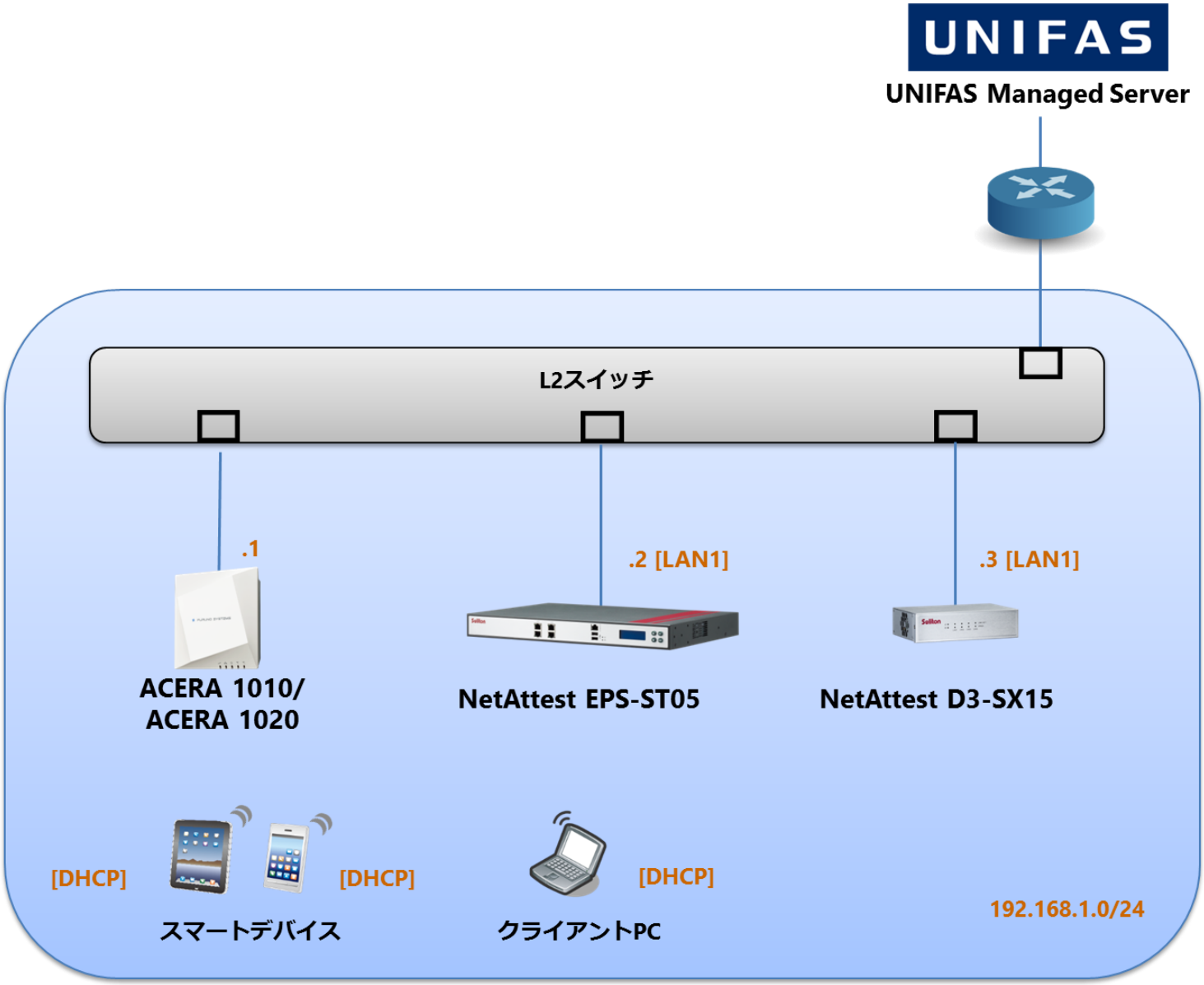
目次

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。

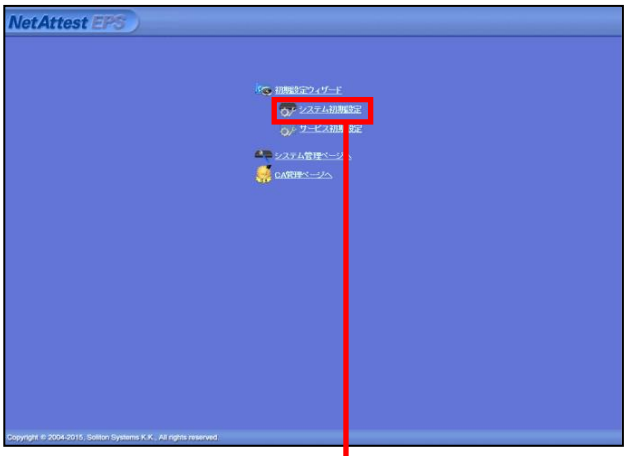
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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



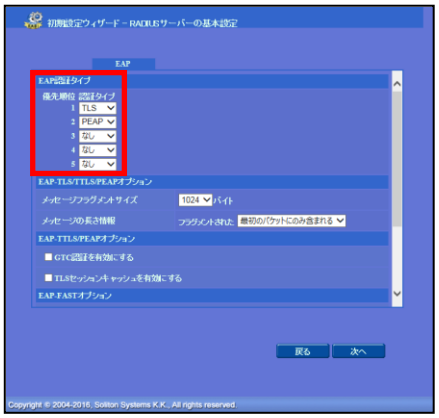
項目	値
ホスト名	naeps.example.com
IP アドレス	デフォルト
ライセンス	なし

2-3 サービス初期設定ウィザードの実行

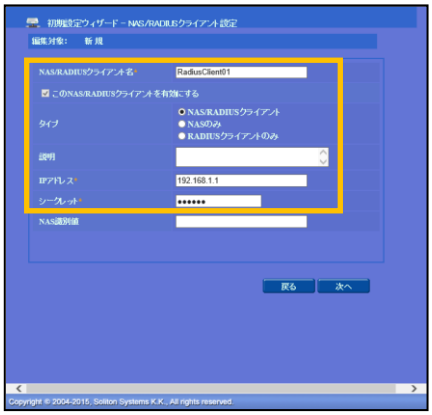
サービス初期設定ウィザードを実行します。

- 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

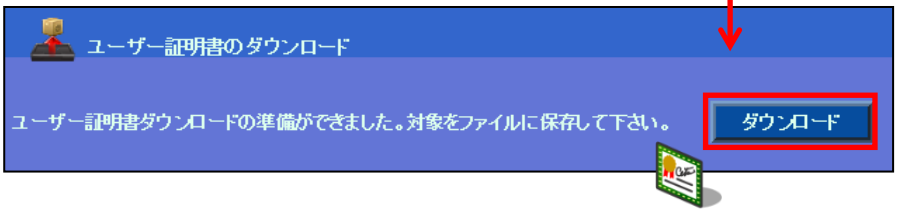
2-5 クライアント証明書の発行

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

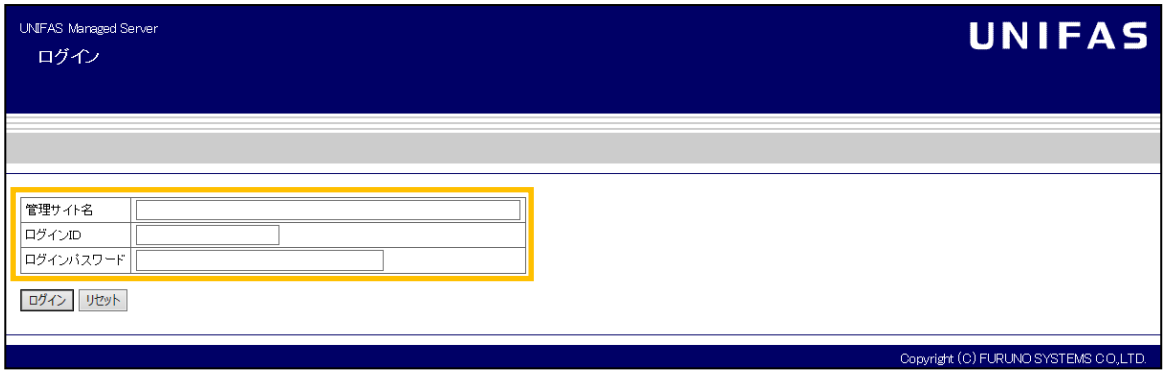
UNIFAS Managed Server の設定を行うには、ブラウザでアクセスする必要があります。

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

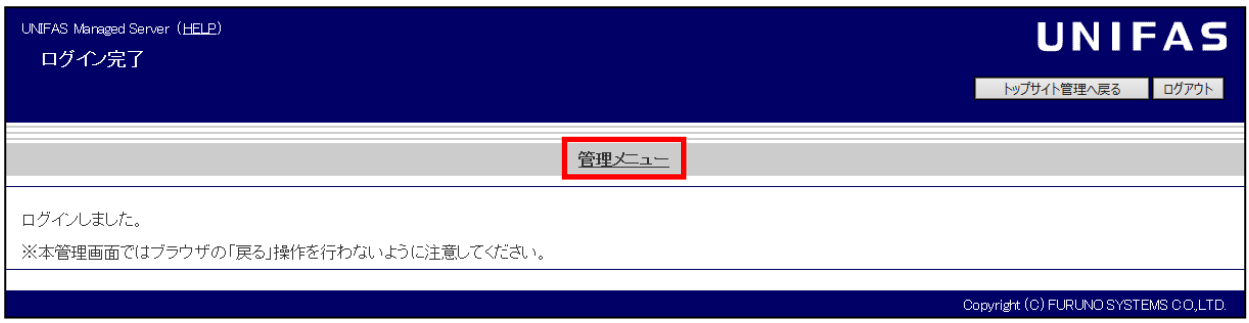
【ログイン ID】

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】

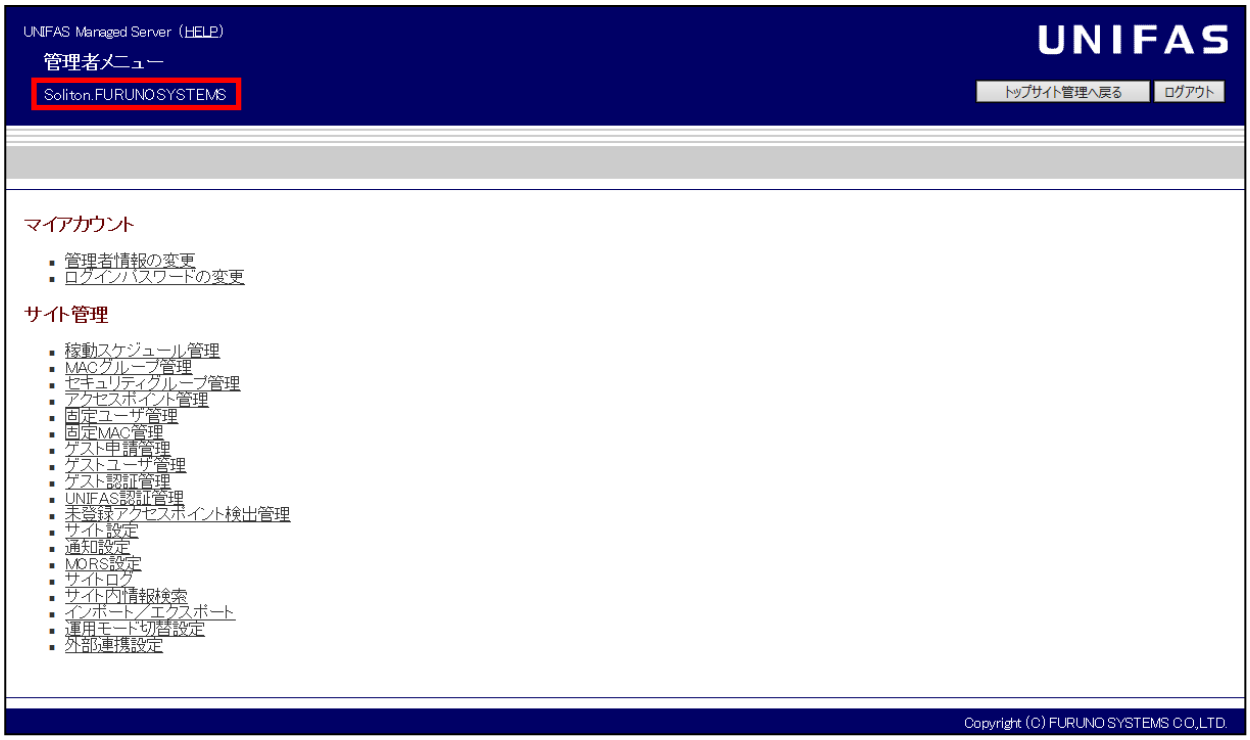
対象サイトの管理者ログインパスワードを入力します。

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。

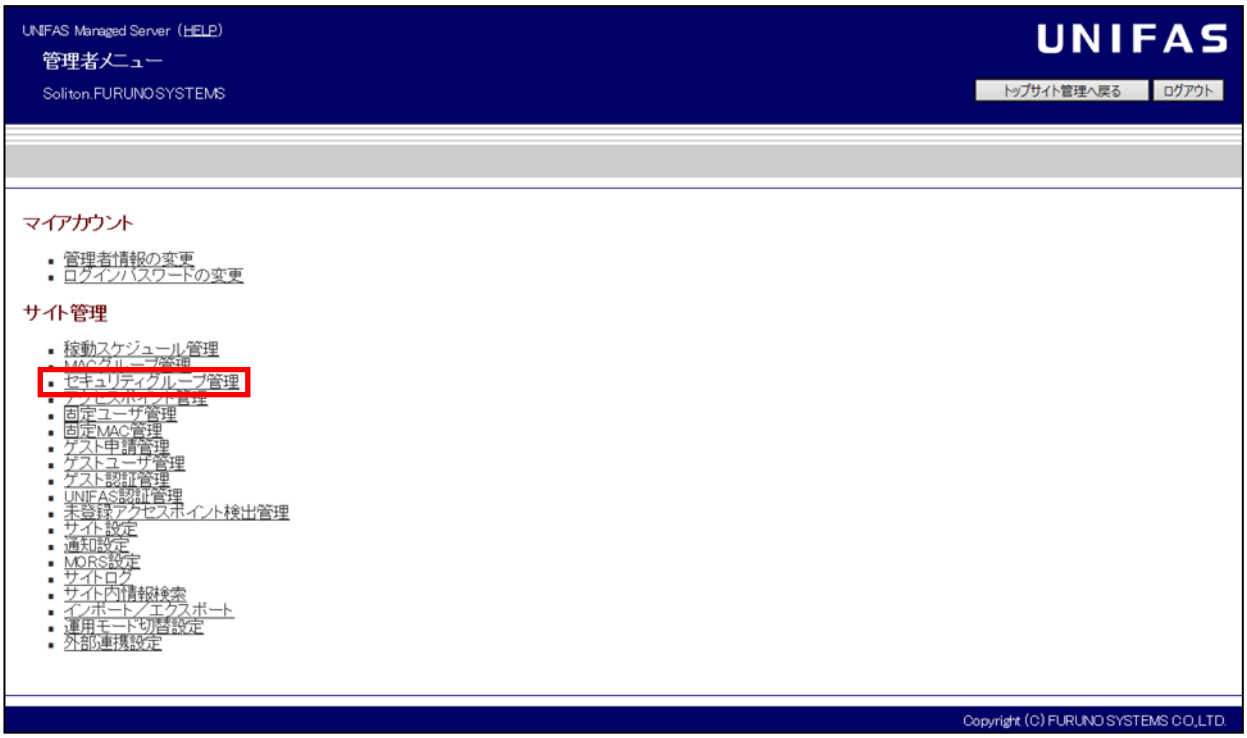
※下記画面は、ログイン画面の管理サイト名において、サブサイト名.トップサイト名で
ログインした状態です。



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

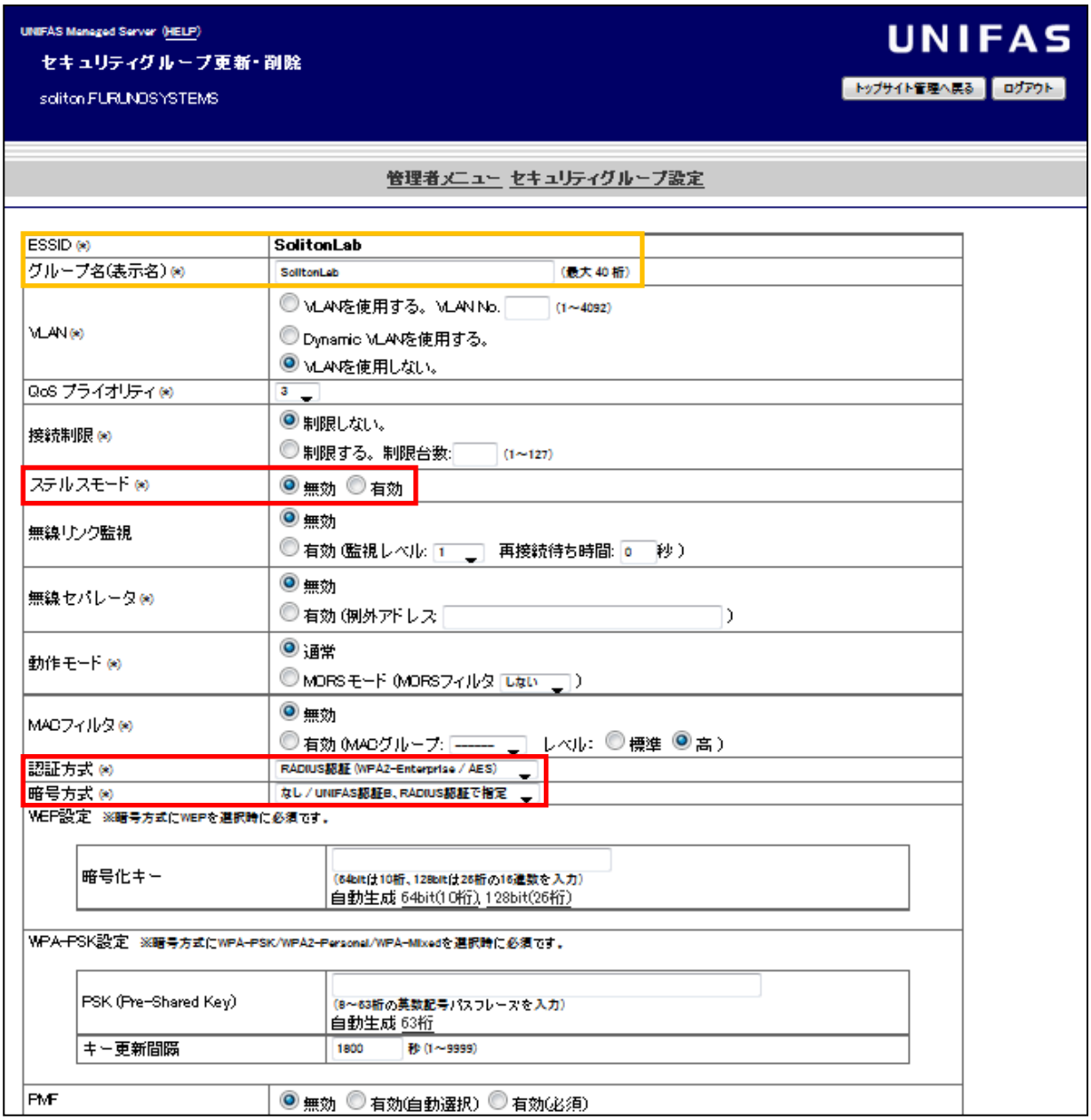
アクセスポイントに紐付けを行うセキュリティグループの作成を行います。

「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。



「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。

「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。



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

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

【ESSID】

ESSID を入力してください。

【グループ名】

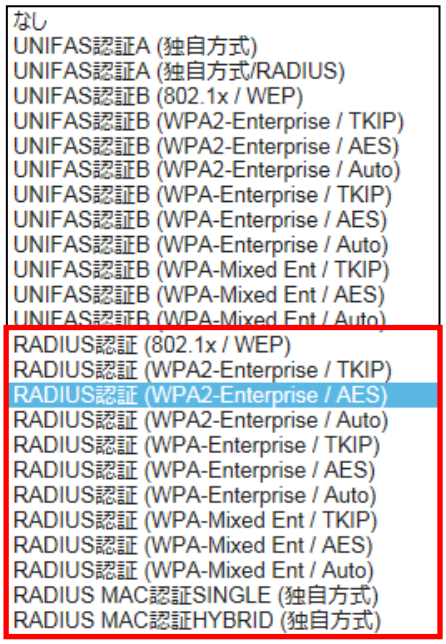
セキュリティグループ名を入力します。（UNIFAS 上で表示させる名前です）

【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。

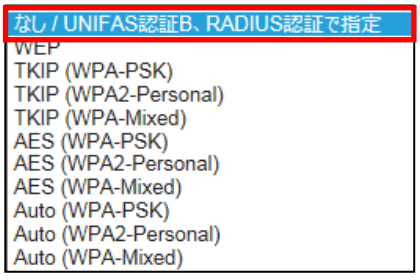
【認証方式】

認証方式は以下の赤枠の中から選択してください。



【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。



【RADIUS サーバー】

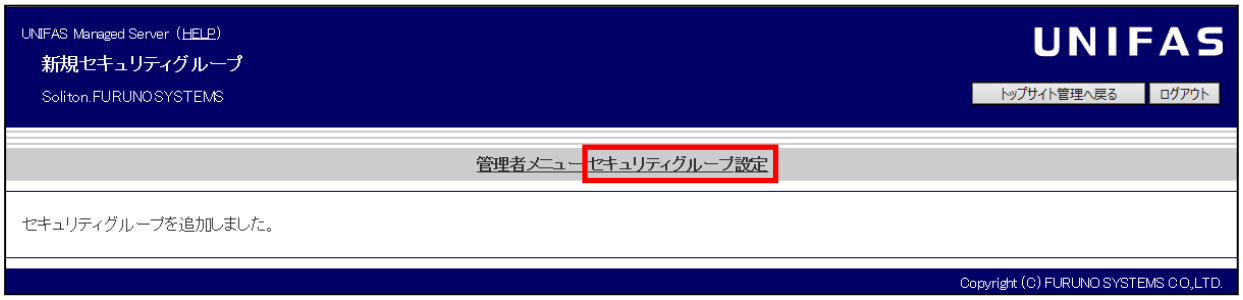
RADIUS サーバーは、プライマリ・セカンダリを登録することができます。

【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。



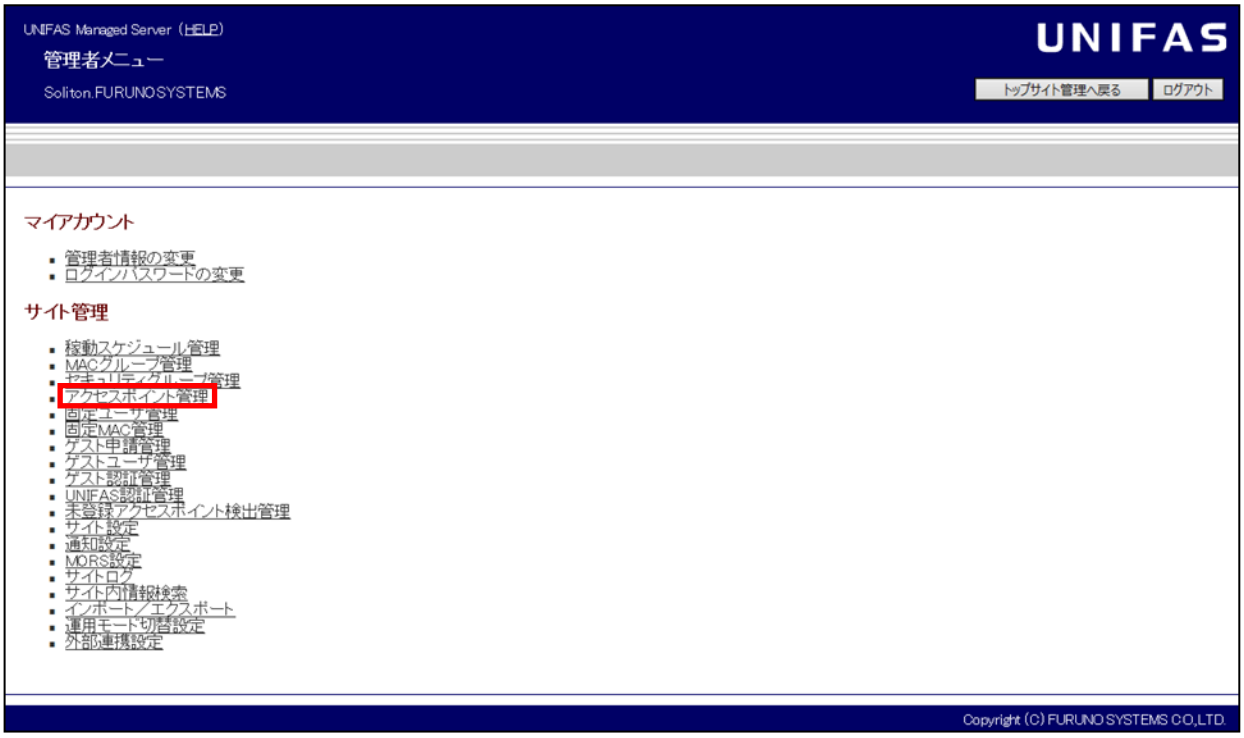
［セキュリティグループ設定］を選択すると、下記画面が表示されます。登録したグループ名が表示されていることを確認してください。

[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。

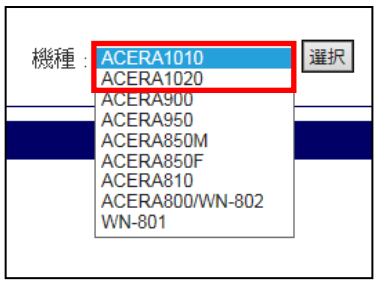


「アクセスポイント管理者」画面の [アクセスポイント管理] - [アクセスポイント設定]を選択します。

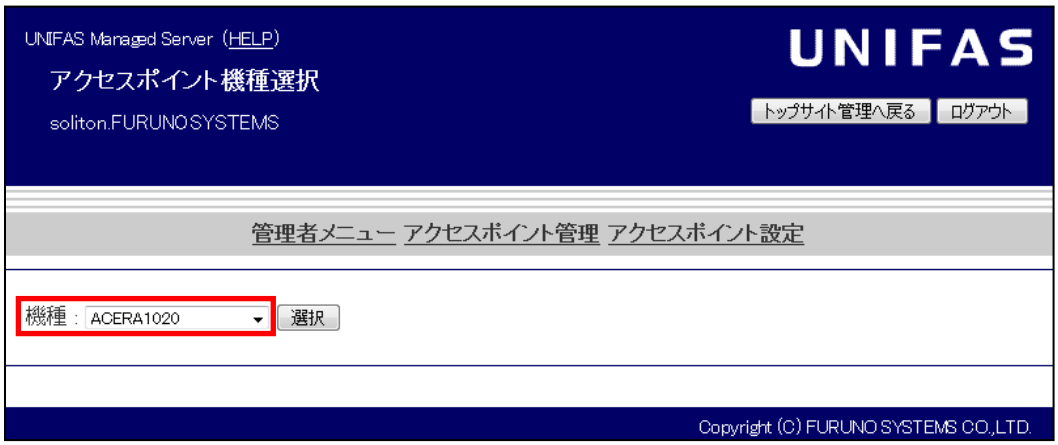
「アクセスポイント設定」画面が表示されます。

【アクセスポイントの追加】ボタンを押下してください。

「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。

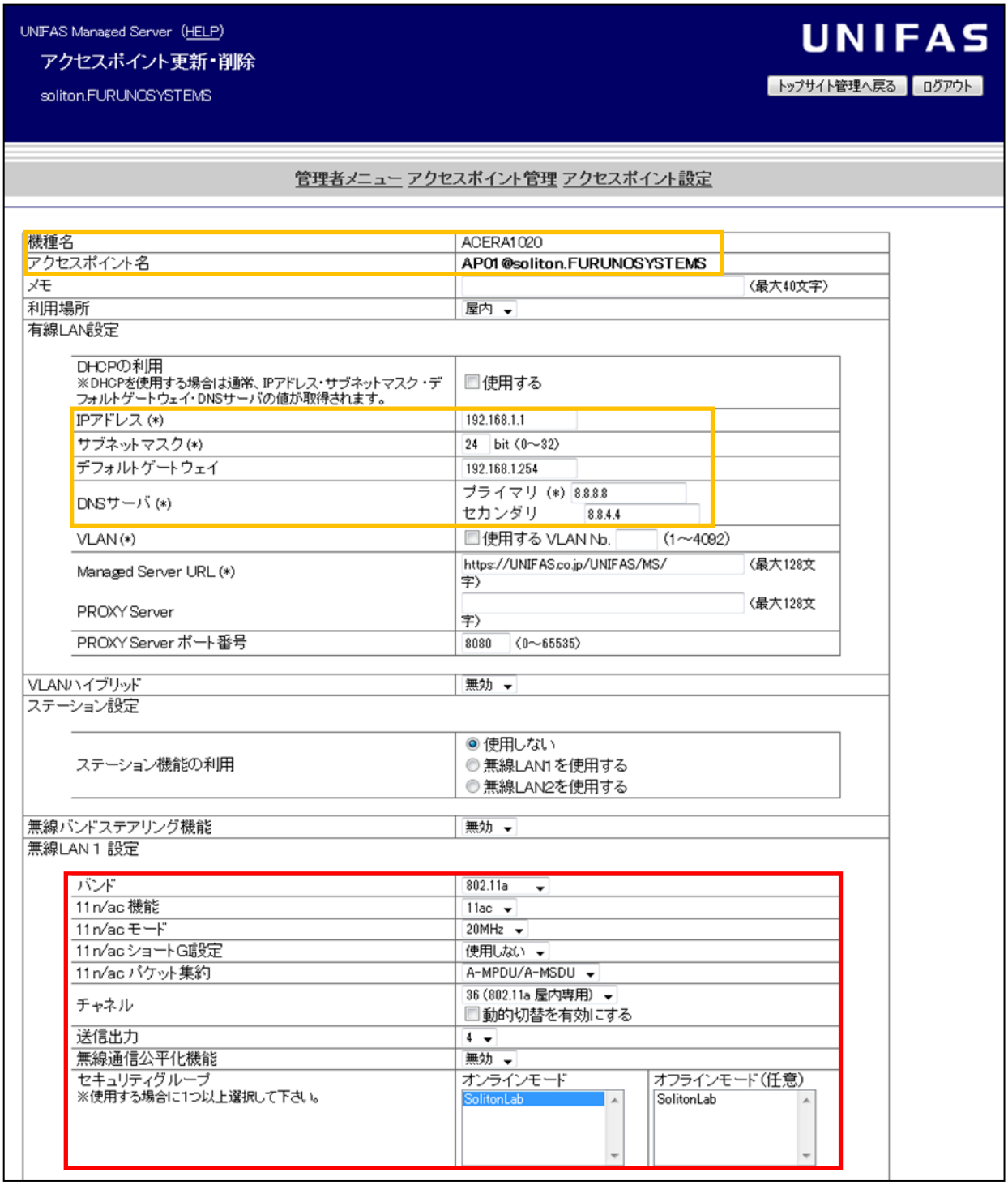


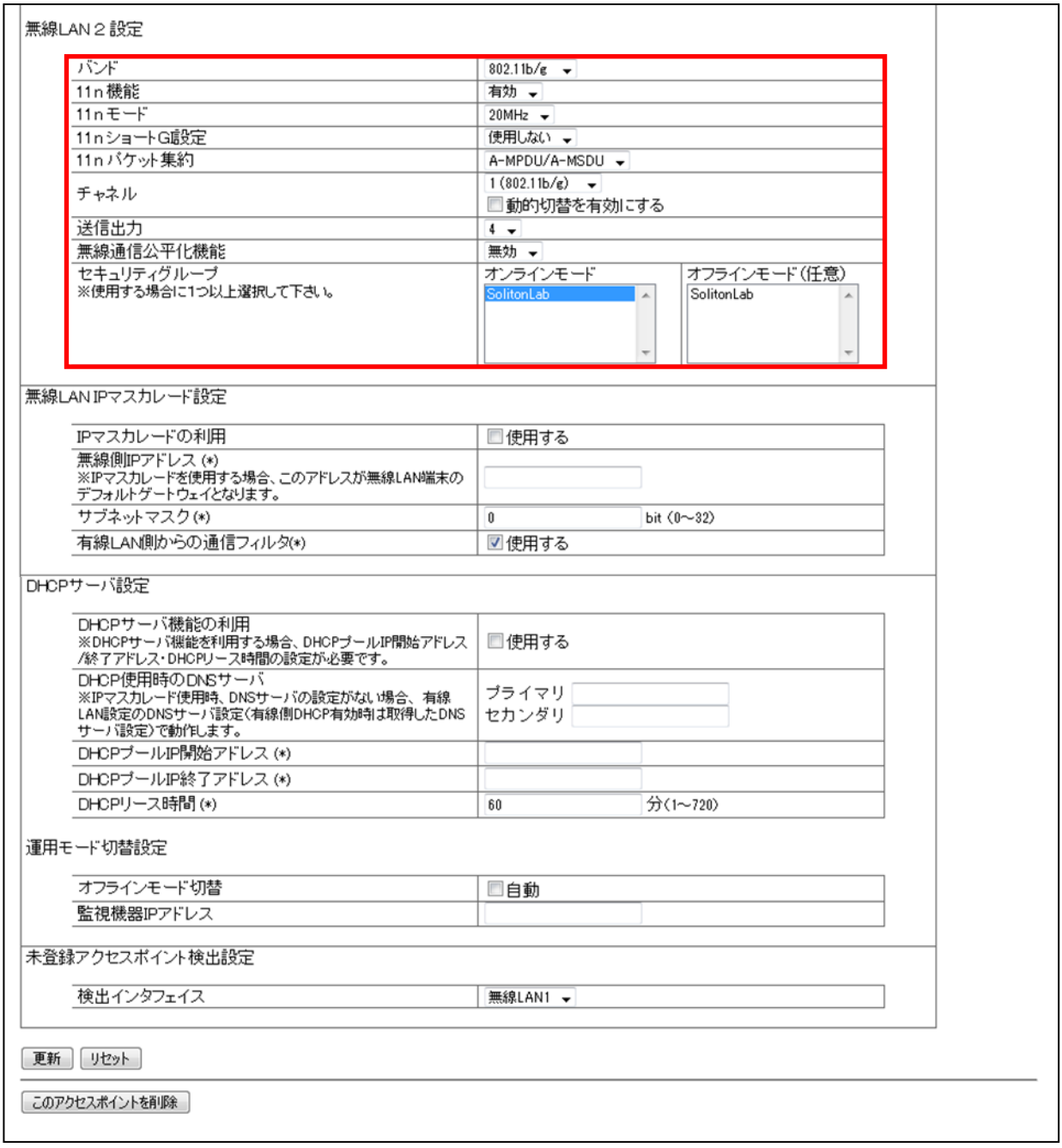
ACERA 1010 または ACERA 1020 を選択します。



「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。





【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、稼働中チャネルが重なった際に自動的に空いているチャ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。

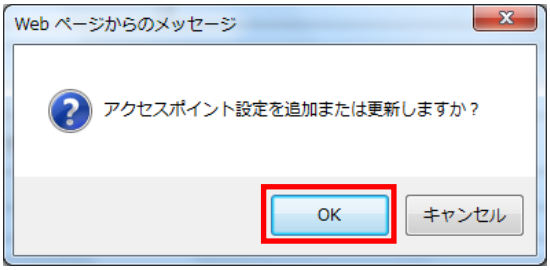
アクセスポイントでサービスするセキュリティグループを選択します。

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。

[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。

これにて ACERA 1010/ACERA 1020 の設定は終了です。

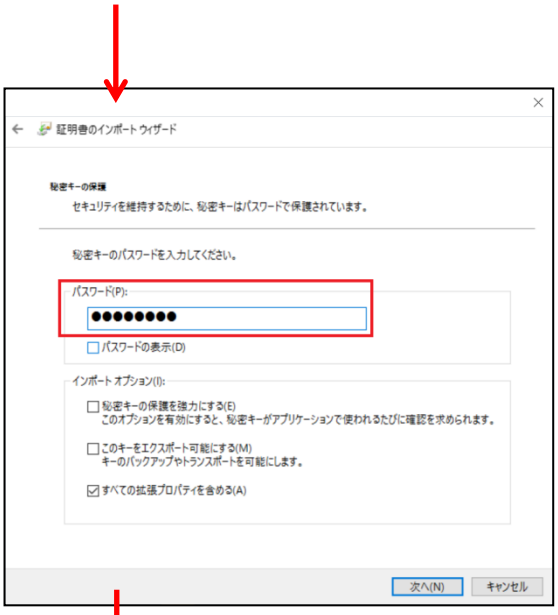
設定した電波（ESSID）が出ていることを確認してください。

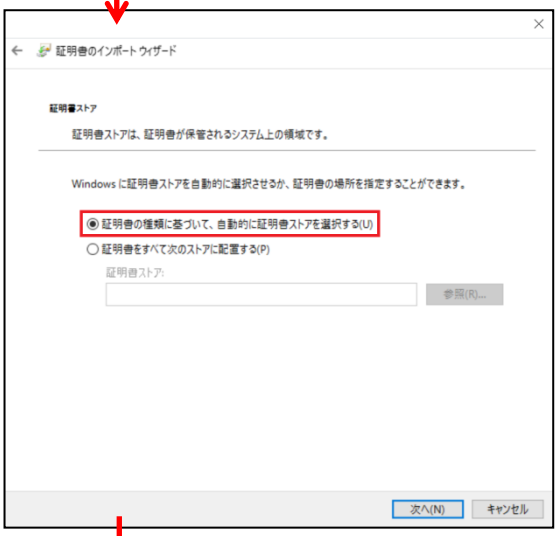
4. EAP-TLS 認証でのクライアント設定

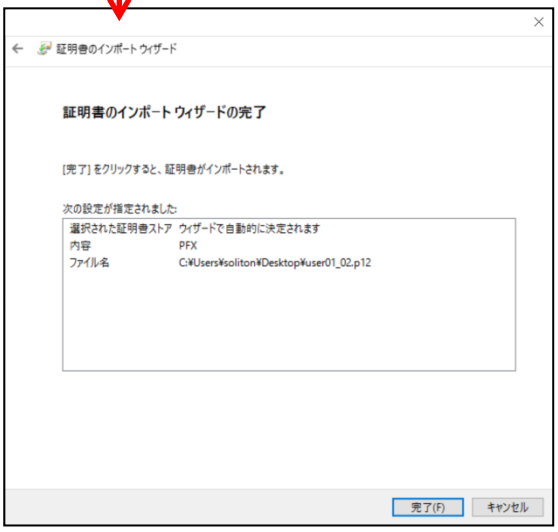
4-1 Windows 10 での EAP-TLS 認証

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

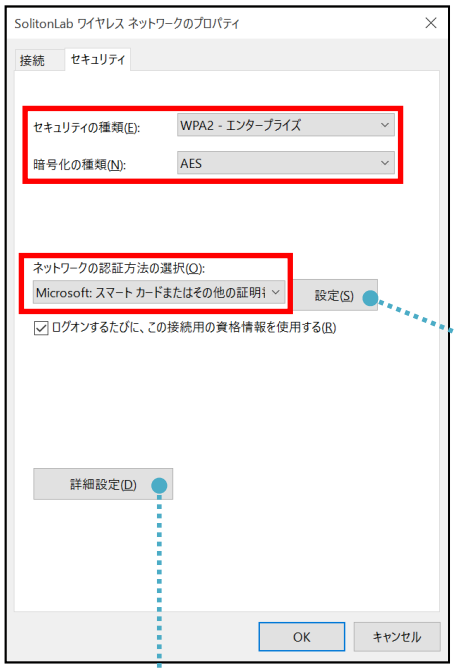
発行した際に設定したパスワードを入力

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
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

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。

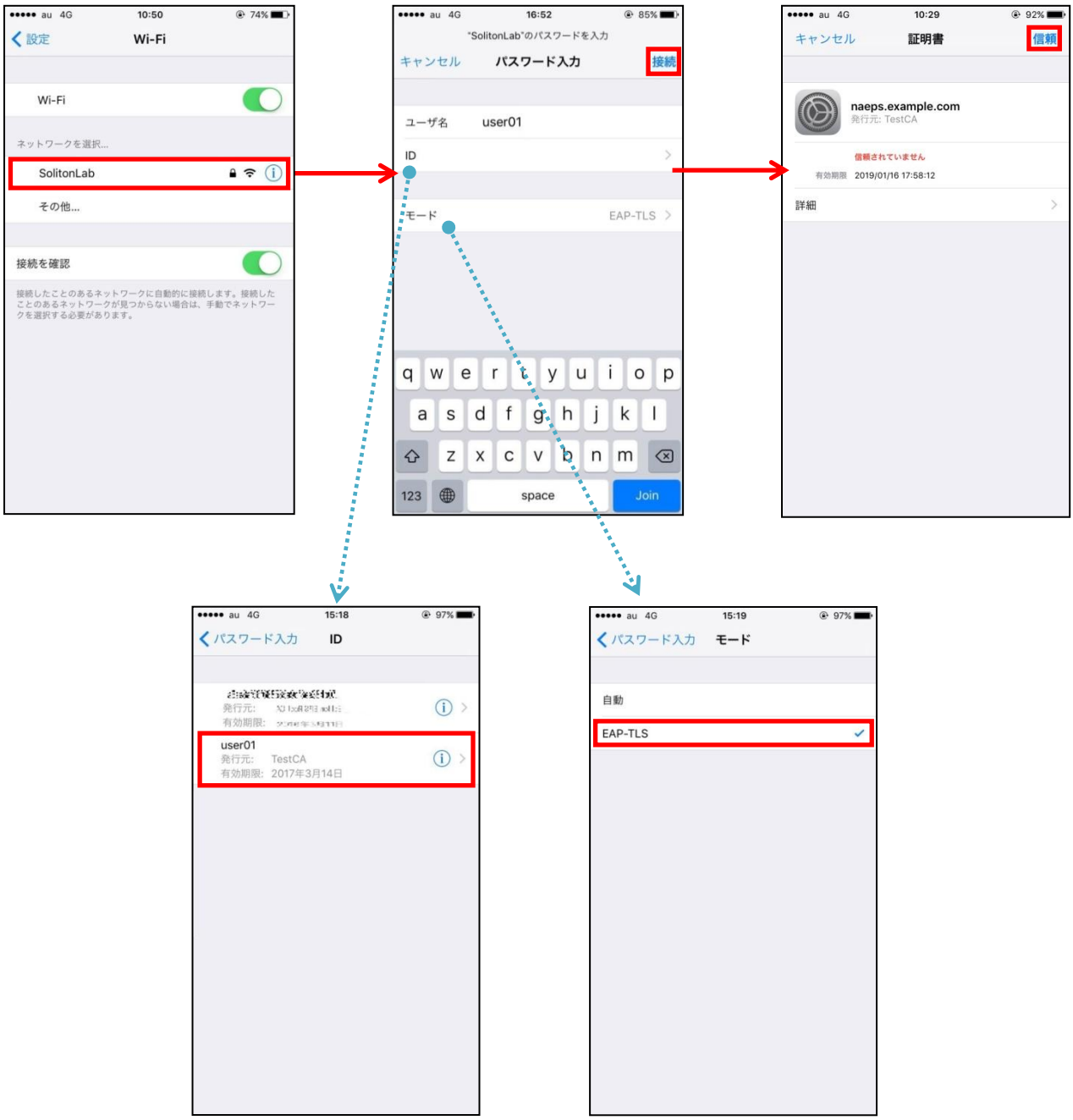
※本項では TLS の設定のみ記載します。その他の認証方式の設定に関しては付録をご参照ください。

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

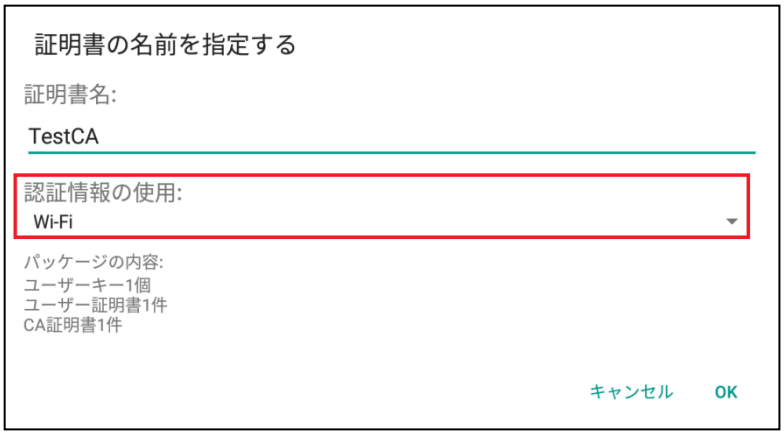
4-3-1 クライアント証明書のインポート

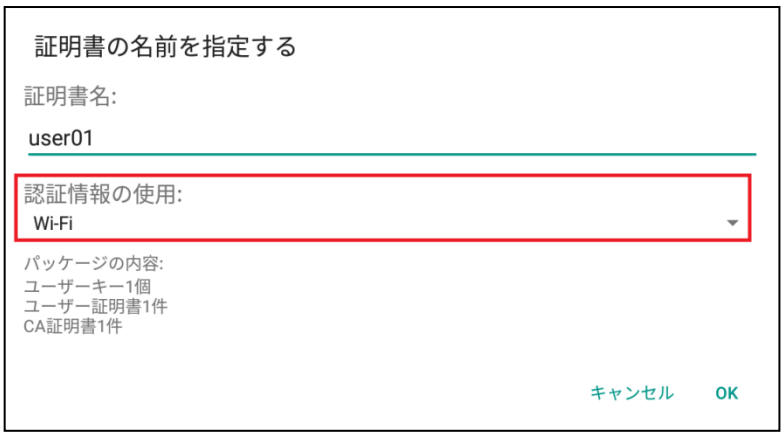
NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

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、メーラーにより、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。





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。

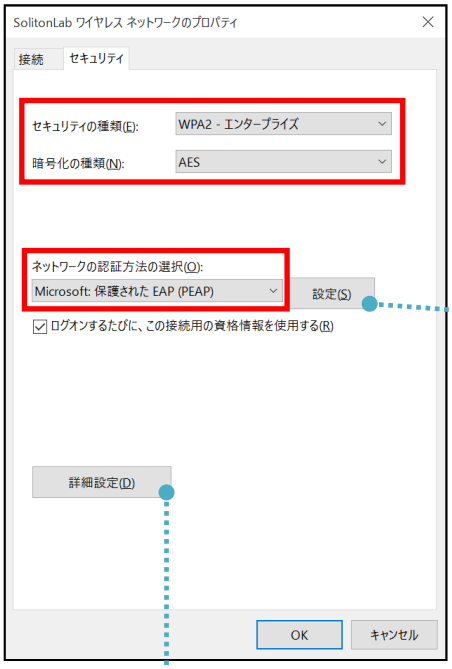
CA 証明書とユーザー証明書は、インポートした証明書を選択してください。

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

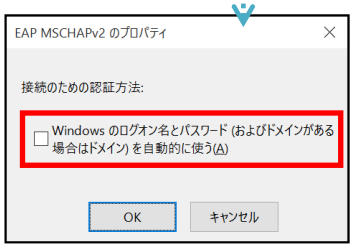
5. EAP-PEAP 認証でのクライアント設定

5-1 Windows 10 のサプリカント設定

[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)のサプリカント設定

UNIFAS Managed Server で設定した ESSID を選択し、サプ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)のサプリカント設定

UNIFAS Managed Server で設定した ESSID を選択し、サプ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

<table>
<tr><th>製品名</th><th>ログ表示例</th></tr>
<tr><td>NetAttest EPS</td><td>Login OK: [user01] (from client RadiusClient port 0 cli 34-F3-9A-1E-4F-CE)</td></tr>
<tr><td>ACERA 1010/
ACERA 1020/
UNIFAS Managed Server</td><td>
<table>
<tr><td>種別</td><td>認証</td></tr>
<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_Authticated(192.168.1.2)</td></tr>
</table>
</td></tr>
</table>

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

<table>
<tr><th>製品名</th><th>ログ表示例</th></tr>
<tr><td>NetAttest EPS</td><td>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)</td></tr>
<tr><td>ACERA 1010/
ACERA 1020/
UNIFAS Managed Server</td><td>
<table>
<tr><td>種別</td><td>認証</td></tr>
<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_Authticated(192.168.1.2)</td></tr>
</table>
</td></tr>
</table>

改訂履歴

日付	版	改訂内容
2017/02/16	1.0	初版作成