

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

【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 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 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 の設定.....	13
3-1 ACERA 1010/ACERA 1020 設定の流れ.....	13
3-2 ACERA へログイン.....	14
3-3 IP アドレス設定.....	15
3-4 無線設定.....	17
3-5 ESSID 設定.....	18
3-6 設定反映.....	21
4. EAP-TLS 認証でのクライアント設定.....	22
4-1 Windows 10 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(Pixel C)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

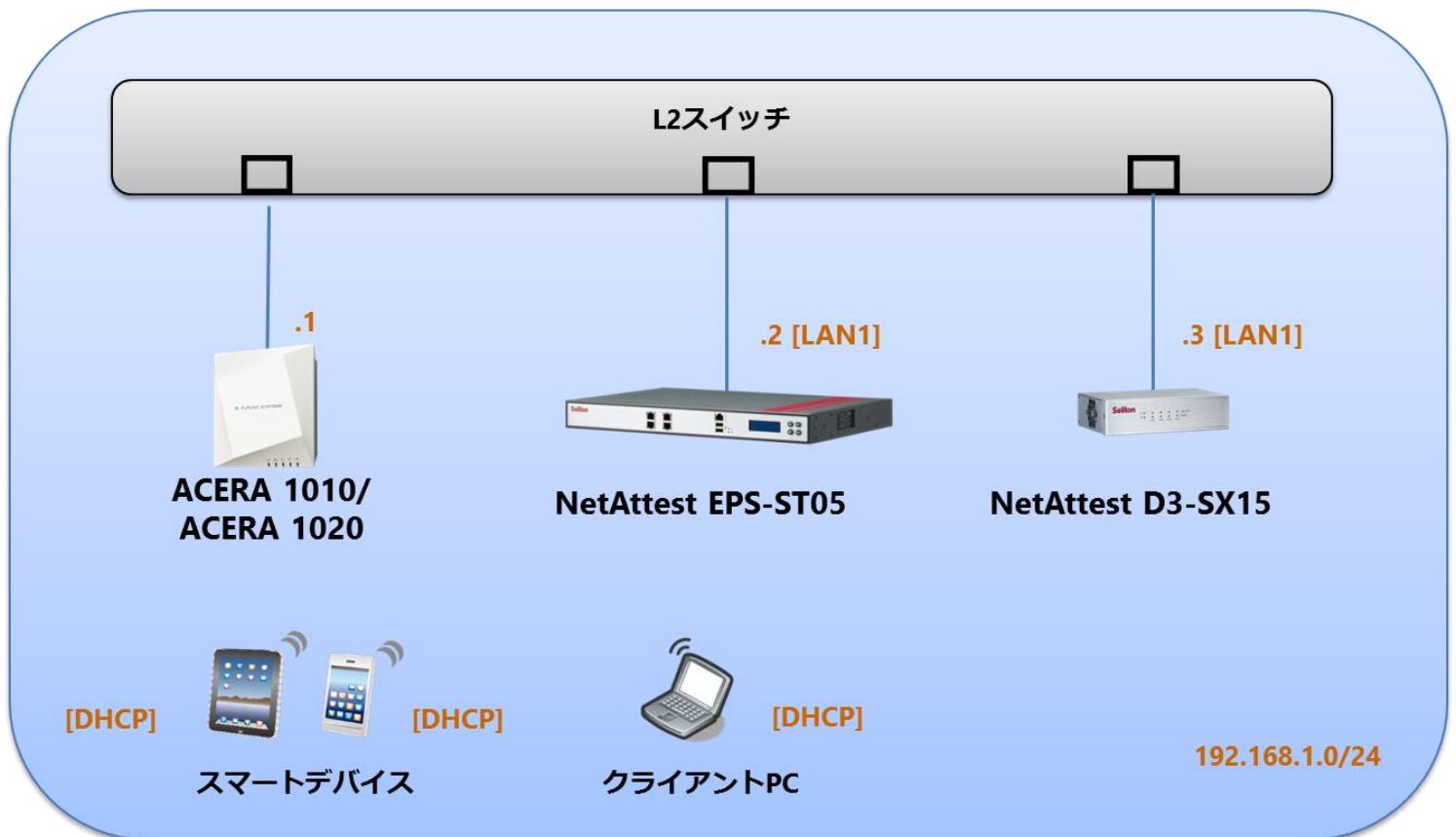
5-1 Windows 10 のサブリカント設定	29
5-2 iOS(iPhone 6)のサブリカント設定	30
5-3 Android(Pixel C)のサブリカント設定.....	31
6. 動作確認結果	32
6-1 EAP-TLS 認証.....	32
6-2 EAP-PEAP(MS-CHAP V2)認証	32

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-SX15 の DHCP サーバーから払い出す
- 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
Let's note	Panasonic	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブリカント
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
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。

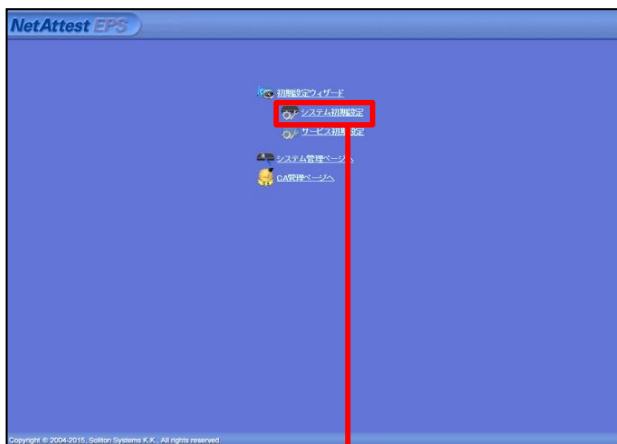
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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

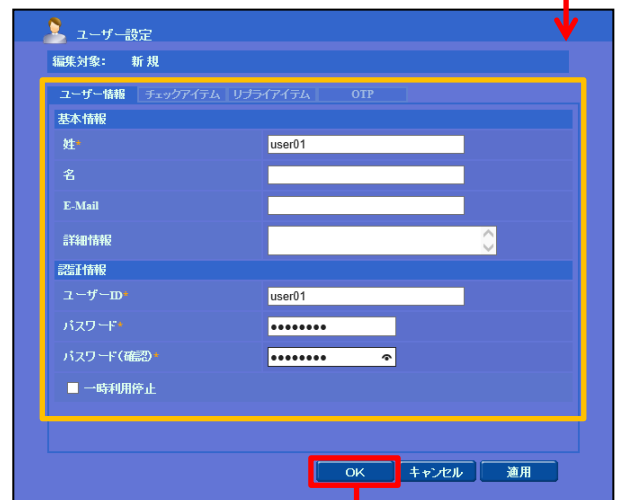
2-4 ユーザーの登録

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)

NetAttest EPS 管理画面の「ユーザー一覧」ページ。ユーザー一覧の表で「user01」の「発行」ボタンが赤枠で囲われ、赤い矢印が右側の詳細画面へと伸びています。

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

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
● 日数 365 日
● 日付 2016 年 7 月 9 日 23 時 59 分 59 秒まで
証明書ファイルオプション
パスワード:
パスワード(確認):
※パスワードが空欄の場合は、ユーザーのパスワードを使用します。
 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. ACERA 1010/ACERA 1020 の設定

3-1 ACERA 1010/ACERA 1020 設定の流れ

1. ACERA へログイン
2. IP アドレス設定
3. 無線設定
4. ESSID 設定
5. 設定反映

3-2 ACERA ヘログイン

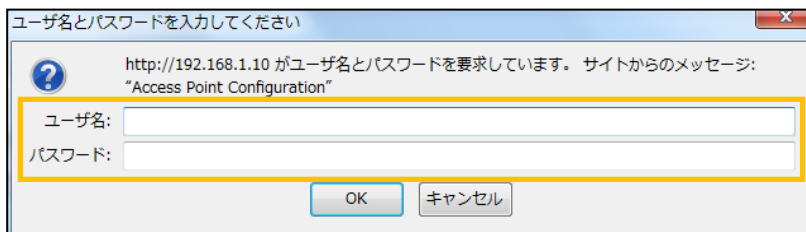
ACERA 1010/ACERA 1020 の初期設定は LAN1 から行います。初期の IP アドレスは「192.168.1.10/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.1.10/」にアクセスしてください。

その後、以下の項目を設定します。

- ACERA IP アドレスの設定
- 無線の設定
- ESSID の設定

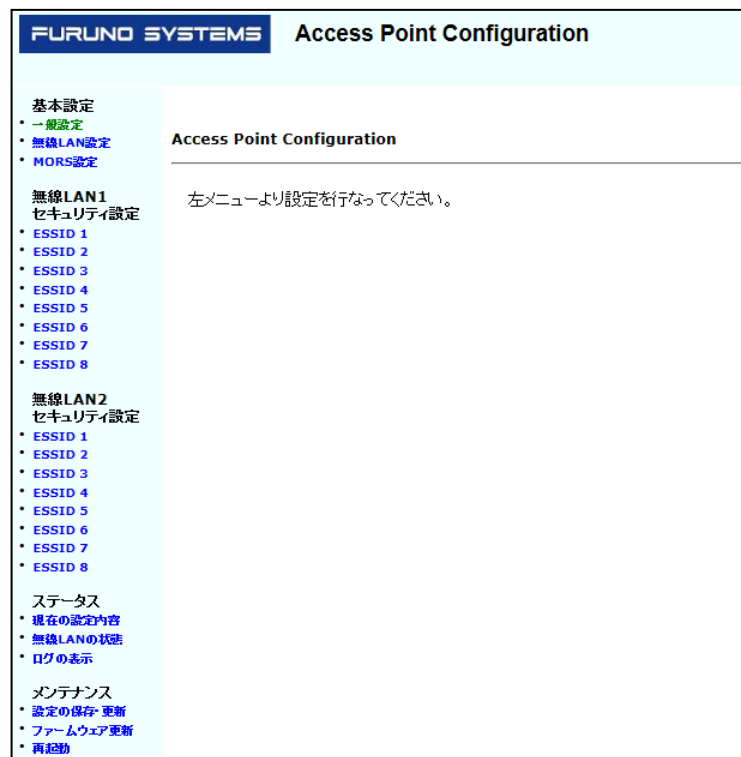
アクセスすると下記のログイン画面が表示されます。

各項目に値を入力しログインしてください。



項目	値
ユーザ名	user
パスワード	user

ログインすると、下記画面が表示されます。



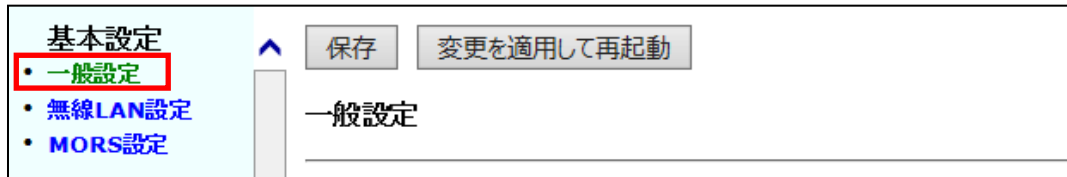
3-3 IP アドレス設定

一般設定より IP アドレス・サブネットマスクなど必要なパラメータを設定してください。

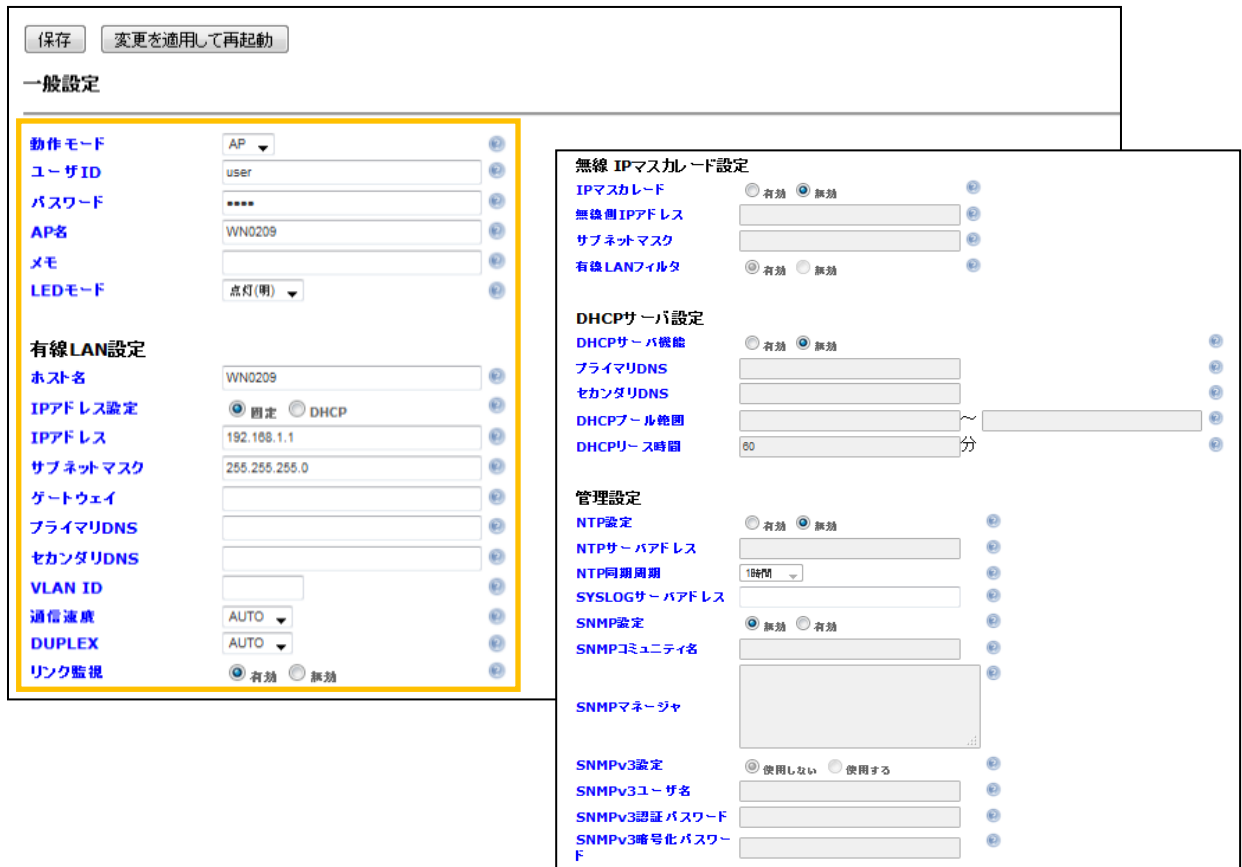
※NetAttest EPS に IP 通信できる IP 設定が必要です。

※ACERA の IP アドレスが RADIUS クライアントの IP アドレスになります。

「基本設定」の「一般設定」を選択します。



IP アドレス等、有線 LAN 側の設定を行います。

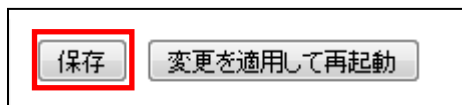


項目	値
動作モード	AP
ユーザ ID	user
パスワード	user
AP 名	WN0209

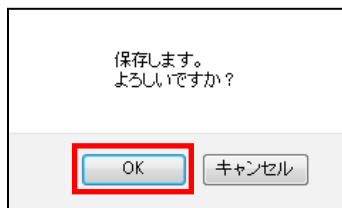
項目	値
ホスト名	WN0209
IP アドレス設定	固定
IP アドレス	192.168.1.1
サブネットマスク	255.255.255.0

設定が完了したら画面ごとに変更した設定内容を保存してください。

画面上部の「保存」ボタンを押下します。



下記メッセージが表示されますので「OK」ボタンを押下します。



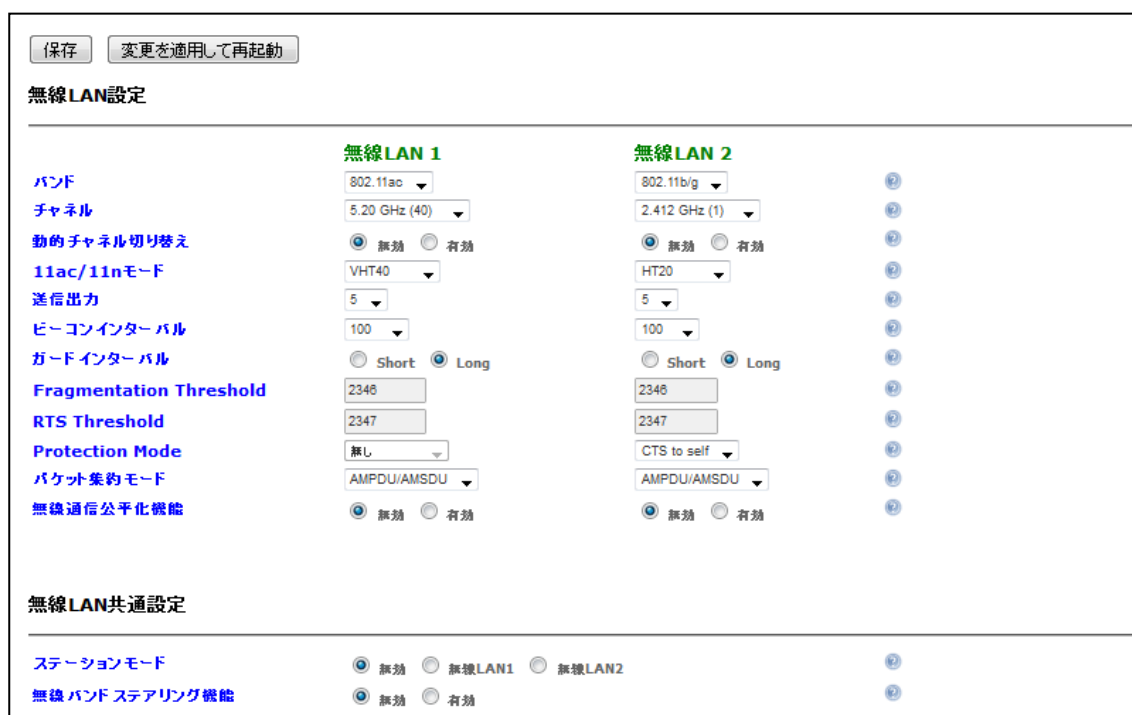
※この時点ではまだ設定は反映されていません。

3-4 無線設定

「基本設定」の「無線 LAN 設定」を選択します。

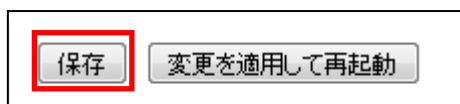


チャンネル等、必要に応じて設定してください。

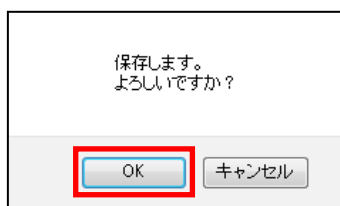


設定が完了したら、画面ごとに変更した設定内容を保存してください。

画面上部の「保存」ボタンを押下します。



下記メッセージが表示されますので「OK」ボタンを押下します。

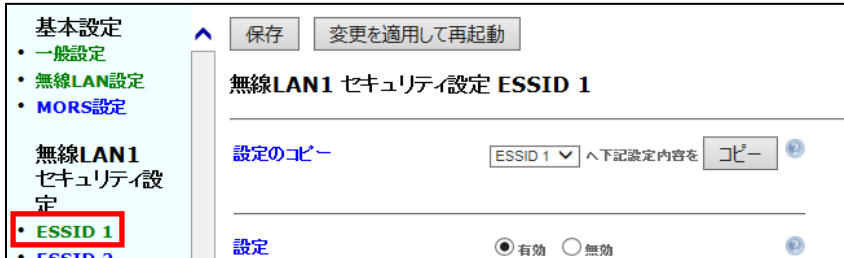


※この時点ではまだ設定は反映されていません。

3-5 ESSID 設定

ESSIDを設定します。

「無線LAN1 セキュリティ設定」の「ESSID 1」を選択します

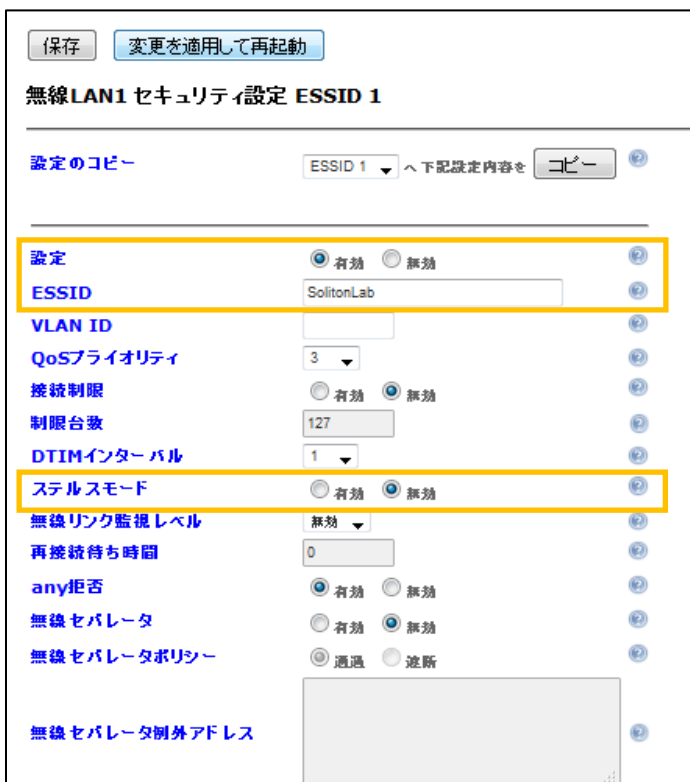


ACERAでは複数ESSIDを設定でき、ESSID毎にセキュリティを変更できます。

RADIUSサーバーを登録する場合もESSID毎に登録します。ここでは以下のパラメータを設定しています。

※必要に応じて「無線LAN2 セキュリティ設定」でも同様の設定を行ってください。

- ESSIDの有効/無効
- ESSID
- ステルスモードの有効/無効
- 暗号方式
- WPA、802.1x 共通設定（RADIUS サーバーの登録）



項目	値
設定	有効
ESSID	SolitonLab
ステルスモード	無効

MACアドレスフィルタリング 有効 無効

対象MACアドレス

MACアドレスフィルタリングレベル 画 標準

暗号化設定

暗号方式 WPA2-Enterprise

WEP設定

モード: Open Shared

キー

WPA固有設定

暗号化方式 TKIP AES AES/TKIP(自動)

パスフレーズ TESTSAMPLE

GTK更新間隔 7200

事前認証 有効 無効

PMF 無効 有効(自動選択) 有効(必須)

項目	値
暗号方式	WPA2-Enterprise
暗号化方式	AES

WPA, 802.1x共通設定

プライマリ認証サーバ 192.168.1.2

プライマリ認証サーバポート 1812

プライマリ認証サーバクレデンシャル secret

セカンダリ認証サーバ

セカンダリ認証サーバポート 1812

セカンダリ認証サーバクレデンシャル

デリミタ -

アカウント設定

プライマリアカウントサーバ

プライマリアカウントサーバポート 1813

プライマリアカウントサーバクレデンシャル

セカンダリアカウントサーバ

セカンダリアカウントサーバポート 1813

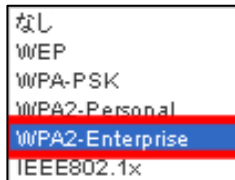
セカンダリアカウントサーバクレデンシャル

デリミタ -

項目	値
プライマリ認証サーバ	192.168.1.2
プライマリ認証サーバポート	1812
プライマリ認証サーバクレデンシャル	secret

【暗号方式】

暗号方式には以下の方式を選択できますが、RADIUS サーバーを利用する場合は WPA2-Enterprise (暗号化が TKIP/AES の場合) もしくは IEEE802.1x (暗号化が WEP の場合) を選択してください。ここでは WPA2-Enterprise を選択しています。



【WPA、802.1x共通設定 (RADIUSサーバーの登録)】

RADIUSサーバーは、プライマリ・セカンダリを登録可能です。

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

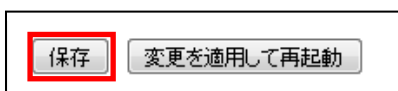
【ポート番号】 1812 (RADIUS サーバーで利用する認証ポート番号)

【クレデンシャル(Secret)】 最大 16 桁

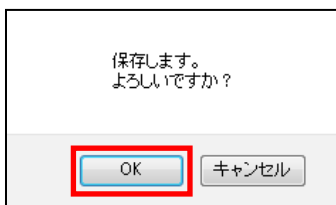
WPA, 802.1x共通設定	
プライマリ認証サーバ	192.168.1.2
プライマリ認証サーバポート	1812
プライマリ認証サーバクレデンシャル	secret
セカンダリ認証サーバ	
セカンダリ認証サーバポート	1812
セカンダリ認証サーバクレデンシャル	

設定が完了したら画面ごとに変更した設定内容を保存してください。

画面上部の「保存」ボタンを押下します。



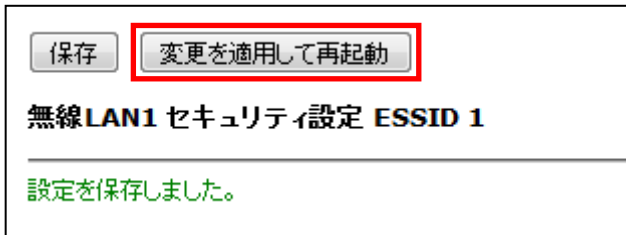
下記メッセージが表示されますので「OK」ボタンを押下します。



※この時点ではまだ設定は反映されておりません。

3-6 設定反映

すべての項目を設定後、変更を適用するために「変更を適用して再起動」ボタンを押下し、再起動を行います。

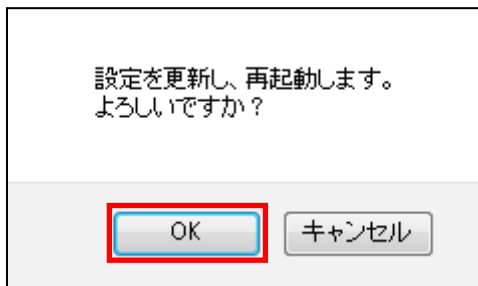


保存 変更を適用して再起動

無線LAN1 セキュリティ設定 ESSID 1

設定を保存しました。

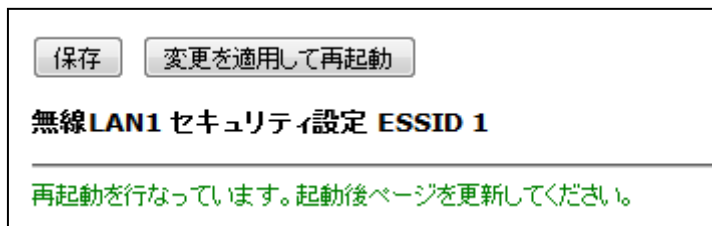
下記メッセージが表示されますので「OK」ボタンを押下します。



設定を更新し、再起動します。
よろしいですか？

OK キャンセル

下記メッセージが表示され、ACERA が再起動されます。



保存 変更を適用して再起動

無線LAN1 セキュリティ設定 ESSID 1

再起動を行なっています。起動後ページを更新してください。

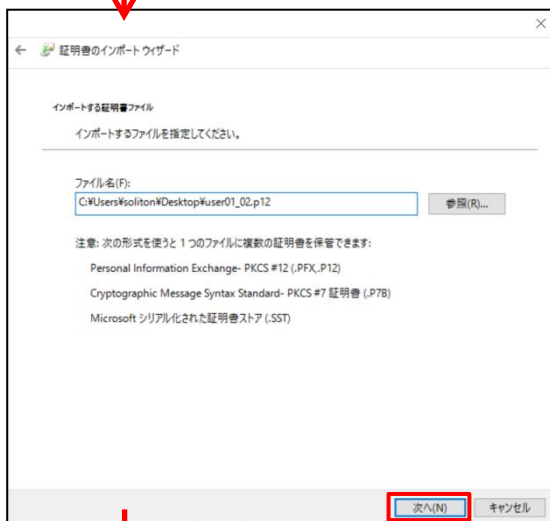
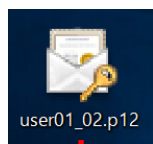
ACERA 1010/ACERA 1020 の設定は以上です。

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

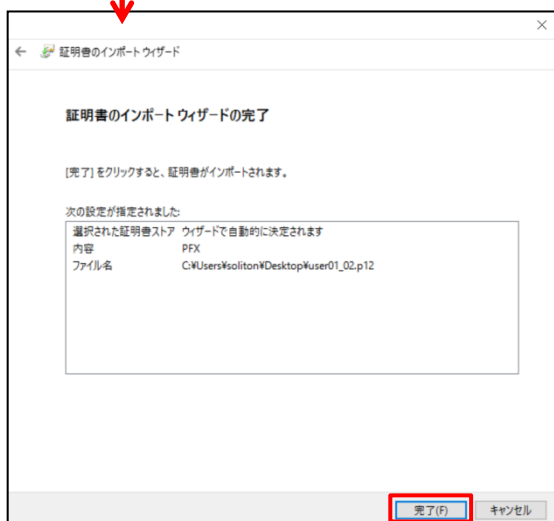
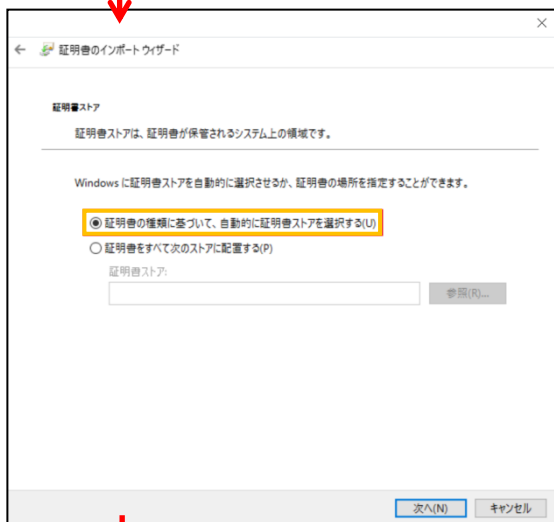
4-1-1 クライアント証明書のインポート

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

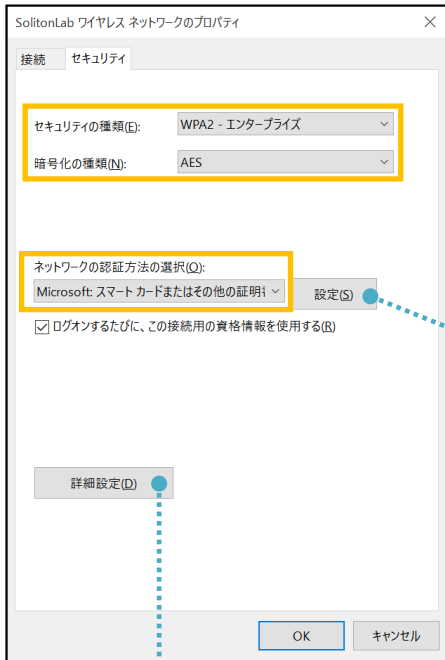


4-1-2 サプリカント設定

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)

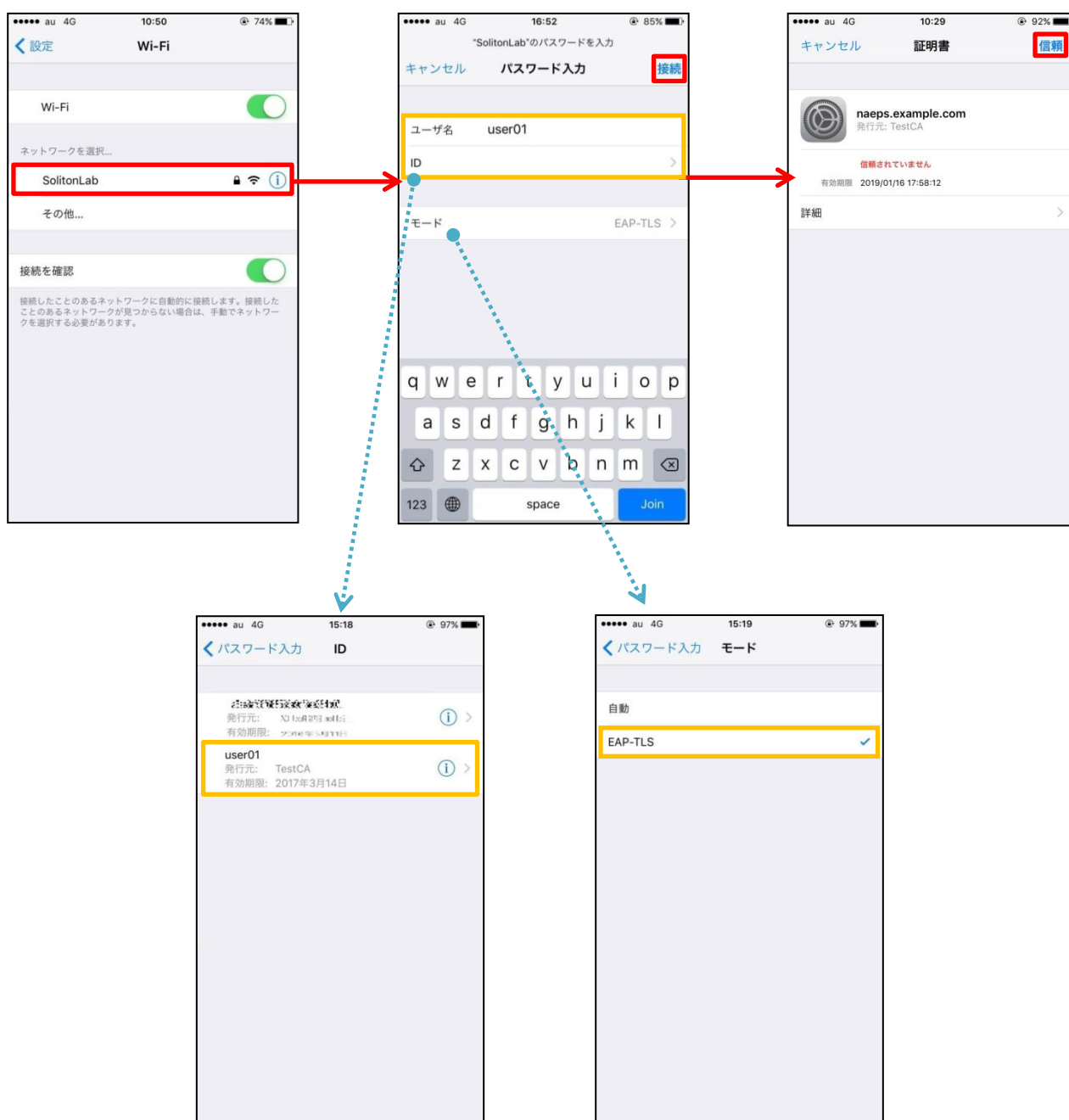
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

ACERA 1010/ACERA 1020 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

ACERA 1010/ACERA 1020 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。

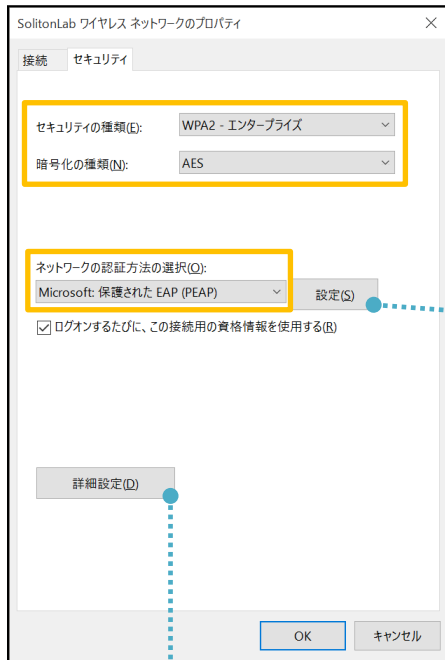


項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

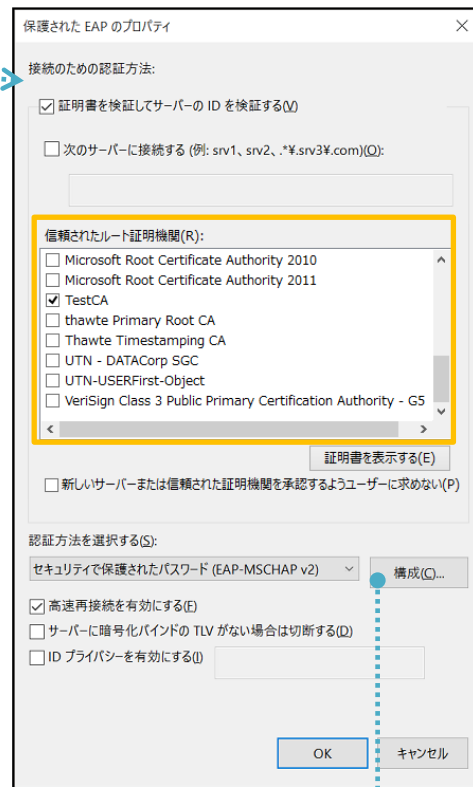
5. EAP-PEAP 認証でのクライアント設定

5-1 Windows 10 のサブリカント設定

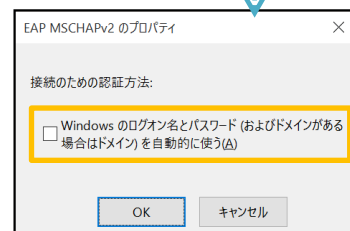
[ワイヤレスネットワークのプロパティ] の「セキュリティ」タブから以下の設定を行います。



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

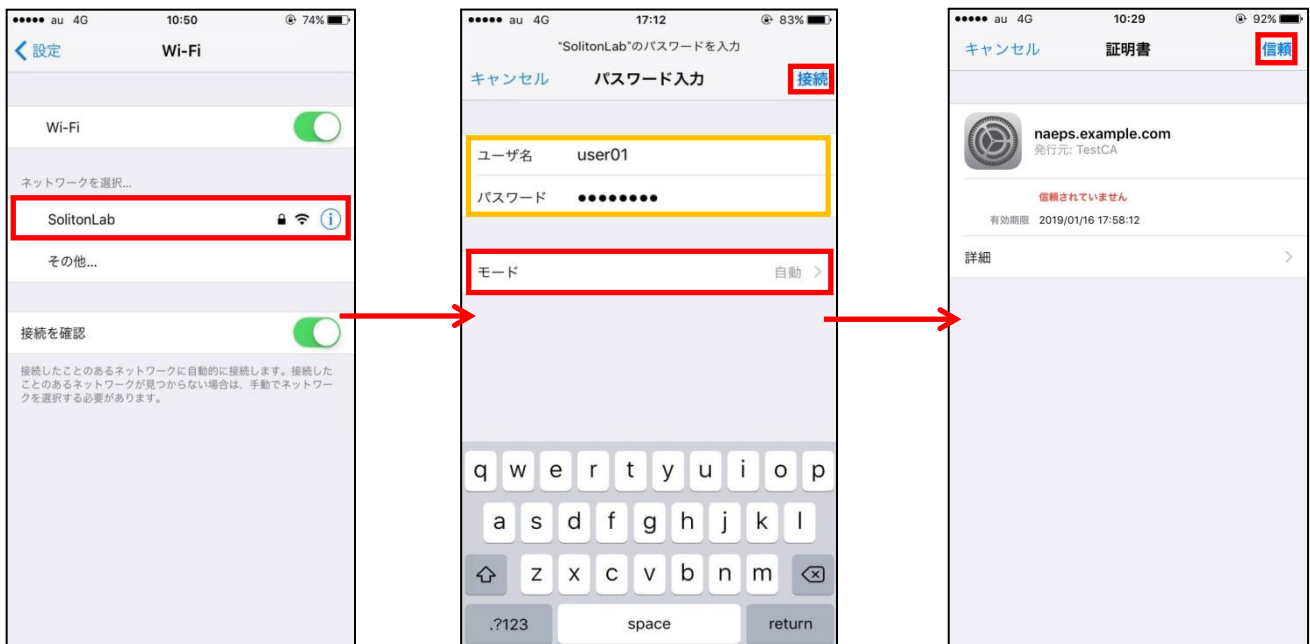


項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA

5-2 iOS(iPhone 6)のサブリカント設定

ACERA 1010/ACERA 1020 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。

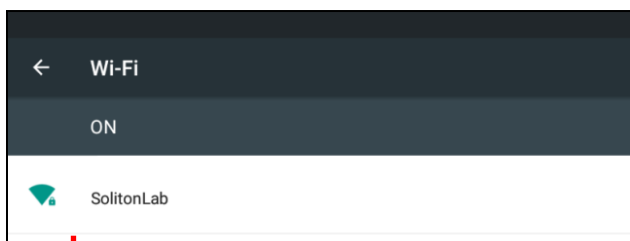
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。



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

5-3 Android(Pixel C)のサブリカント設定

ACERA 1010/ACERA 1020 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	daemon.info hostapd: (WLAN1 SolitonLab)[ACERA BSSID]IEEE 802.11 associated daemon.info authinfo: (WLAN1 SolitonLab)[ACERA BSSID]connect daemon.info authinfo: (WLAN1 SolitonLab)[ACERA BSSID]8021x authenticated

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	daemon.info hostapd: (WLAN1 SolitonLab)[ACERA BSSID]IEEE 802.11 associated daemon.info authinfo: (WLAN1 SolitonLab)[ACERA BSSID]connect daemon.info authinfo: (WLAN1 SolitonLab)[ACERA BSSID]8021x authenticated

