

【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	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 ヘ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)のサプリカント設定	37
6.	動作確認結果	.38
	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		secret
ACERA 1010/ ACERA 1020	192.168.1.1/24	UDP 1812	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

CA植物医祝			
CANDERIN	<b>ル−トca</b> ∨		
CARCER			
● 内部で新しい鍵を生成する			
公開施方式	RSA 🗸		
親長	2048 🗸		
● 外部HSMデバイスの鍵を得	用する		
要求の署名			
要求署名アルゴリズム	SHA256 ¥		
CA情報			
CA名(必须)	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		
<b>\$78</b> %			
CA署名設定			





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

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。

<ul> <li>aceps.example.com</li> <li>システム設定</li> <li>システム管理</li> <li>Edf機関</li> <li>DHCPサーバー</li> <li>LDAPサーバー</li> <li>RADIUSサーバー</li> <li>コーザー</li> <li>ユーザー</li> <li>ユーザー</li> <li>ユーゲー</li> <li>コーボート</li> <li>キクスポート</li> <li>コーザーバスワードポリシー</li> <li>デフォルトユーザープロファイル</li> </ul>	<u>シューザー</u> ユーザー <u>詳細オプションの短 エクスポート</u>	覧 ● 一部 ● 完全 グループ 差 <u>名節</u> test user	✓ ユーザーまで 検索 ユーザーID ISSI	□ <u>□</u> <u>□</u> <u>■</u> <u>■</u> <u>#</u> <u>#</u> <u>#</u> <u>#</u> <u>#</u> <u>#</u> <u>#</u> <u>#</u>
			🙎 ユーザー設定	•
			編集対象: 新規	
			ユーザー情報 チェックアイテム 基本情報	
			姓	user01
項目	値		名	
姓	user01		E-Miail	
			認証情報	✓
ユーサーID	user01		ユーザーD	user01
パスワード	password		バスワード・ バスワード(研究)・	
パスワード	password		パスワード* パスワード(確認)* ■ 一時利用停止	······
パスワード	password		パスワード パスワード(確認) ■ 一時利用停止	•••••••• •
パスワード	password		パスワード・ パスワード (確認)・ ■ 一時利用停止	······· 个
パスワード	password		パスワード・ パスワード(編約)・ ■ 一時利用停止	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
パスワード	password		パスワード・ パスワード(確認)・ ■ 一時利用停止	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
パスワード	password		パスワード・ パスワード(確認)・ ■ 一時利用停止	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
パスワード	password		パスワード・ パスワード(確認)・ ■ 一時利用停止	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
パスワード	password		パスワー <b>ド・</b> パスワード(確認)・ ■ 一時利用停止	・・・・・・・
パスワード NetAttest EPS	password		パスワード・ パスワード(確認)・ ■ 一時利用停止	・・・・・・・
パスワード NetAttest EPS	password	%	バスワー <b>ド</b> ・ バスワード(確認)・ ■ 一時利用停止	ок ‡+>/t// шД
パスワード VetAttest EPS naeps.example.com ・システム設定 ・システム管理 ・SKITHMI	password	覧 ○ 一部 ● 完全 グループ	<ul> <li>パスワード・</li> <li>パスワード(確認)・</li> <li>一時利用停止</li> </ul>	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
パスワード <b>VetAttest EPS</b> naeps.example.com ・システム設定 ・システム設定 ・システム設定 ・システム設定 ・システム設定 ・システム設定 ・システム設定	password ユーザー エーザー エクスポート	覧 ● 一部 ● 完全 グループ E	<ul> <li>パスワード・ パスワード(確認)・</li> <li>■ 一時利用停止</li> </ul>	ок <b>‡</b> +>/z/ν Ш ОК <b>‡</b> +>/z/ν Ш ОГ/т/~Э́ № п
パスワード NetAttest EPS naeps.example.com * システム設定 * ジステム管理 * 証明機関 * DHOPサーバー * LDAPサーバー * RADIUSサーバー	password	覧 ● 一部 ● 完全 グループ 室	<ul> <li>パスワード・</li> <li>パスワード(確認)・</li> <li>■ 一時利用停止</li> </ul>	
パスワード <b>VetAttest EPS</b> Pacps.example.com * システム設定 * システム管理 * 証明機関 * DHCPサーバー * DHCPサーバー	password	覧 覧 定 部●完全 グルーブ  名前	バスワード・ バスワード(確認)・ ■ 一時利用停止	
パスワード         VetAttest EPS         * naeps.example.com         * システム設定         * システム設定         * システム管理         * E明機関         DHCPサーバー         * EDAPサーバー         * RADIUSサーバー         = ユーザー         = ユーザー         = ユーザー         = エーガー         = エーブー	password         ・      <	覧 ■ ● 完全 グルーブ 産 <u>名前</u> test user	✓ ユーザーまで 検索 ユーザーまで 検索	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

## 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)



# 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 ヘ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。

UNFAS Managed Server ログイン	UNIFAS
管理サイト名	
ログインD ログインパスワード ログイン リゼット	

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。

UNFAS Managed Server(HELP) ログイン完了		UNIF	AS
		トップサイト管理へ戻る	ログアウト
	<u>管理/二ュー</u>		
ログインしました。			
※本管理画面ではブラウザの「戻る」操作を行わないように注意してください。			
	c	Convright (C) FURUNO SYSTE	MSCOLTD

「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。

UNIFAS Managed Server( <u>HELP</u> ) 管理者メニュー	UNIFAS
Soliton.FURUNOSYSTEMS	トップサイト管理へ戻る ログアウト
マイアカウント	
<ul> <li> <u>             日子石山(取) 冬季</u> </li> <li> <u>             ロクインバスワードの変更</u> </li> <li> <b>サイト管理</b> </li> </ul>	
· 福子         · 福子         · · ·	
	Copyright (C) FURUNO SYSTEMS C O, LTD.

# 3-3 UNIFAS Managed Server ヘ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。

UNIFAS Managed Server (HELP) セキュリティグループ管理 Soliton.FURUNOSYSTEMS			<b>UNIFAS</b> 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	福集
グループの追加		(**** <b>1</b>	<u></u>
			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 FURUNDSYSTEMS 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) 💌 (最大 40 桁) SolitonLeb 🔘 VLANを使用する。VLAN No.[ (1~4092) VLAN 😣 ◎ Dynamic VLANを使用する。 ◎ VLANを使用しない。 QoS プライオリティ 😣 3 ◎ 制限しない。 接統制限 💌 🔘 制限する。制限台数: 🗌 (1~127) ステルスモード 💌 🧿 無効 🔘 有効 💿 無効 無線リンク監視 🔘 有効 (監視レベル: 1 🔔 再接続待ち時間: 💿 秒)) 💿 無効 無線セパレータ💌 🔘 有効 (例外アドレス 🗍 b. 🧿 通常 動作モード 💌 ◎ MORSモード (MORSフィルタ しない \_\_\_ ) ◎ 無効 MACフィルタ 💌 ◎ 有効 (M40グループ: ------ しベル: ◎ 標準 ◎ 高) RADIUS認証 (WPA2-Enterprise / AES) 認証方式 💌 なし / UNIFAS認証B、RADIUS認証で指定 暗号方式 💌 WEP設定 ※暗号方式にWEPを選択時に必須です。 暗号化キー (64bitは10桁、128bitは26桁の16進数を入力) 自動生成 64bit(10桁), 128bit(26桁) 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) (8~63桁の英数記号パスフレーズを入力) 自動生成 <u>63桁</u> キー更新間隔 1800 🚯 (1~9999) PMF. 🧕 無効 🔘 有効(自動選択) 🔘 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

77489					
ホスト名	192.168.1.2				
ボート番号	1812				
クレデンシャル	secret	(最大 16 桁)			
セカンダリ ※任意					
ホスト名					
ボート番号	1812				
クレデンシャル		(最大 16 桁)			
共通設定					
デリ民タ	-				
アカウンティンクサーバー					
- / /1 Y /) ホントター					
	Into				
か 11留写 力し手であみし		(書士 18 55)			
シレテンシャル わつがけ ※#=	L				
メード報告	1813				
கா⊞ு திட≓ுகைய		(長大 16 折)			
- ジレブジン イル		(182) (10 1117			
デルミタ	-				
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。		
ケジュール ※スケシュールを 既定モード (*)	遵訳した場合、スケジュー	ル期間は既定モードと反対	ゆ妖鬱となります。 カ		
ケジュール ※スケジュールを 既定モード ※ スケジュール	連択した場合、スケジュー -	ル期間は既足モードと反対 部部 ● 非稼重	!の妖謡となります。 カ		
ケジュール ※スケジュールを 既定モード® スケジュール	連訳した場合、スケジュー	ル期間は既足モードと反対 ③ 稼動 ○ 非稼重 - 未設足 - ▲	!の妖感となります。 カ		
ケジュール ※スケジュールを 既定モード ⊛ スケジュール 認証A オプション	連択した場合、スケジュー -	ル期間は既足モードと反対 ③ 稼動 ○ 非稼種 - 本設足 - ▲ 本	!の妖器となります。 カ		
ケジュール ※スケジュールを 既定モード (*) スケジュール 認証A オブション 認証画面設定	遵訳した場合、スケジュー	ル期間は既足モードと反対 ● 稼動 ● 非稼種 - 木酸定 - ▲ ▼	いの妖器となります。 カ		
ケジュール ※スケジュールを 既定モード ∞ スケジュール 認証Aオプション 認証画面設定 使用画面 ∞	連択した場合、スケジュー -	ル期間は既足モードと反対	© カスタム画面		
ケジュール ※スケジュールを 既定モード ∞ スケジュール 認証A オプション 認証画面設定 使用画面 ∞ カスタム画面アーカイブフ:	連訳した場合、スケジュー アイル	ル期間は既足モードと反対 ● 稼動 ● 非稼種 - 未設足 - ▲ ・ ・ ・ ・ ・ ・ ・ ・ ・	1の妖器となります。 カ ◎ カスタム画面 が選択されていません。(未アップロー)	F)	
ケジュール ※スケジュールを 既定モード ∞ スケジュール 認証A オブション 認証画面設定 使用画面 ∞ カスタム画面アーカイブフ: 高速認証機能	連択した場合、スケジュー アイル	ル期間は既足モードと反対 ● 稼動 ● 非稼種 - 未設足 - ▲ ・ ・ ・ ・ ・ ・ ・ ・ ・	の妖器となります。 カ ◎ カスタム画面 が選択されていません。(未アップロー)	۴)	
ケジュール ※スケジュールを 戻定モード (*) スケジュール 認証A オブション 認証画面設定 使用画面 (*) カスタム画面アーカイブフ: 高速認証機能 機能利用 (*)	連択した場合、スケジュー アイル	ル期間は既足モードと反対 ● 稼動 ● 非稼種 - 未設足 - ▲ ・ ・ ・ ・ ・ ・ ・ ・ ・	ため妖器となります。 カ ● カスタム画面 が選択されていません。(未アップロー)	F)	
<ul> <li>ケジュール ※スケジュールを</li> <li>戻定モード (*)</li> <li>スケジュール</li> <li>認証A オプション</li> <li>認証画面設定</li> <li>使用画面 (*)</li> <li>カスタム画面アーカイブフ:</li> <li>高速認証機能</li> <li>機能利用 (*)</li> <li>Managed Server不在時認認</li> </ul>	連択した場合、スケジュー アイル 証ポリシー(w)	ル期間は既足モードと反対 ● 容動 ● 非容型 - 未設定 - ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	1の妖器となります。 カ の カ カ カスタム画面 が選択されていません。(未アップロー) 可効 日本	F)	
ケジュール ※スケジュールを 既定モード ∞ スケジュール 認証A オブション 認証画面設定 使用画面 ∞ カスタム画面アーカイブフ: 高速認証機能 機能利用 ∞ Managed Server不在時認認 メールアドレス認証	連択した場合、スケジュー アイル 証ポリシー(*)	ル期間は既足モードと反対 ● 稼動 ● 非稼重 - 未設足 - ▲ ● 共通画面 参見 77イル ● 無効 ● 有 ● 通過 ● 打	1の妖器となります。 カ か カスタム画面 が選択されていません。(未アップロー) 前効 巨否	F)	
ケジュール ※スケジュールを 既定モード (*) スケジュール 認証A オプション 認証画面設定 使用画面 (*) カスタム画面アーカイブフ: 高速認証機能 機能利用 (*) Managed Server不在時認認 メールアドレス認証 機能利用 (*)	連択した場合、スケジュー アイル 証ポリシー(#)	ル期間は既足モードと反対 ● 稼動 ● 非稼重 - 未設足 - ▲ - 東 ● 共通画面 参見 77イル ● 無効 ● 有 ● 通過 ● 打 ● 通過 ● 打	1の妖器となります。 カ ク カスタム画面 が選択されていません。(未アップロー) 言効 巨否 言効	۲) ۲)	
<ul> <li>ケジュール ※スケジュールを</li> <li>既定モード (*)</li> <li>スケジュール</li> <li>認証A オプション</li> <li>認証画面設定</li> <li>使用画面 (*)</li> <li>カスタム画面アーカイブフ:</li> <li>高速認証機能</li> <li>機能利用 (*)</li> <li>Managed Server不在時認認 メールアドレス認証</li> <li>機能利用 (*)</li> <li>D互効期間</li> </ul>	連択した場合、スケジュー アイル 証ポリシー(*)	ル期間は既足モードと反対 ● 稼動 ● 非稼種 - 未設足 - ▲ - 「 ● 共通画面 ● 二 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一 一	1の状態となります。 カ の状態となります。 カ カ カフタム画面 が選択されていません。(未アップロー) 有効 日 百効	F)	
<ul> <li>ケジュール ※スケジュールを</li> <li>既定モード (*)</li> <li>スケジュール</li> <li>認証A オブション</li> <li>認証画面設定</li> <li>使用画面 (*)</li> <li>カスタム画面アーカイブフ:</li> <li>高速認証機能</li> <li>機能利用 (*)</li> <li>Managed Server不在時認認 メールアドレス認証</li> <li>機能利用 (*)</li> <li>D有効期間</li> <li>10口 #### 7#5 4#59</li> </ul>	連択した場合、スケジュー ァイル 証ポリシー(*)	ル期間は既足モードと反対 ● 稼動 ● 非稼種 - 未設足 - ▲ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	1の妖器となります。 カ の カスタム画面 が選択されていません。(未アップロー) 可効 P否 可効 ) 200	F)	
<ul> <li>ケジュール ※スケジュールを</li> <li>既定モード (*)</li> <li>スケジュール</li> <li>認証Aオブション</li> <li>認証画面設定</li> <li>使用画面 (*)</li> <li>カスタム画面アーカイブフ:</li> <li>高速認証機能</li> <li>機能利用 (*)</li> <li>Managed Server不在時認認 メールアドレス認証</li> <li>機能利用 (*)</li> <li>ID有効期間</li> <li>1回に接続できる時間</li> <li>1日の説用の特徴</li> </ul>	連択した場合、スケジュー アイル 証ポリシー(*)	ル期間は既足モードと反対 ● 稼動 ● 非稼重 - 未設足 - ▲ ● 共通画面 ● 共通画面 ● 知勤 ● 有 ● 通過 ● 打 1 日 (1 - 385) 15 分 (1 - 433)	Iの状態となります。 カ カ スタム画面 が選択されていません。(未アップロー) 可効 E否 可効 20) (の)	۶)	

#### [ESSID]

ESSID を入力してください。

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

### 【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。

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 / TKIP) RADIUS認証 (WPA2-Enterprise / AES)
RADIUS認証 (WPA2-Enterprise / TKIP) RADIUS認証 (WPA2-Enterprise / AES) RADIUS認証 (WPA2-Enterprise / Auto)
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 (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 (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(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(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(WPA2-Enterprise / TKIP) RADIUS認証(WPA2-Enterprise / AES) RADIUS認証(WPA2-Enterprise / Auto) RADIUS認証(WPA-Enterprise / Auto) 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認証 (WPA2-Enterprise / TKIP) RADIUS認証 (WPA2-Enterprise / AES) RADIUS認証 (WPA2-Enterprise / Auto) RADIUS認証 (WPA-Enterprise / Auto) 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 / AES) RADIUS認証 (WPA-Mixed Ent / Auto) RADIUS認証 (WPA-Mixed Ent / Auto) RADIUS認証 (WPA-Mixed Ent / Auto) RADIUS認証 (WPA-Mixed Ent / Auto)

#### 【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。

UNIFAS Managed Server セキュリティグル soliton.FURUNCSYS	( <u>HELP</u> ) ー <b>ブ管理</b> ITEMS		<b>UNIFAS</b> 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
SolitonLab	SolitonLab	non	更新・削除
グループの追加			
			Copyright (C) FURUNO SYSTEMS CO.,LTD.

[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。

UNFAS Managed Server (HELP) 管理者メニュー	UNIFAS
Soliton.FURUNOSYSTEMS	トップサイト管理へ戻る ログアウト
マイアカウント	
<ul> <li>管理者情報の変更</li> <li>ログインバスワードの変更</li> </ul>	
サイト管理	
整動スケジュール管理         Macクループ管理         マクセスポイント管理         アクセスポイント管理         固定ユープ管理         固定ユープ管理         ヴスト車音管理         グストローザ管理         ゲストコーザ管理         グストローザ管理         グストローザ管理         ゲストローザ管理         ゲストロンーザ管理         ゲストロンーザ管理         ゲストロンーザ管理         サインス・マント検出管理         サイト設定         通知設定         MORS設定         インボート/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。



「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( <u>HELP</u> ) アクセスポイント設定 Soliton.FURUNOSYSTEMS					<b>М</b> уЛ	UNIFAS <sup>附介管理へ戻る</sup> ログアウト
			管理者上ユーアクセスボイ	<u> </u>		
アクセスポイントの追加	機種	Version	最終起動時刻	稼動状況	情報表示	福集
アクセスポイントの追加					,	
					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	選択
	ACERA1020	4
	ACERA950	
	ACERA850M	
	ACERA850F	
	ACERA810	
	ACERA800/WN-802	
	WN-801	
	ACERA800/WN-802 WN-801	

ACERA 1010 または ACERA 1020 を選択します。

UNIFAS Managed Server( <u>HELP</u> ) アクセスポイント機種選択 soliton.FURUNOSYSTEMS	<b>UNIFAS</b> トップサイト管理へ戻る ログアウト
<u>管理者メニュー</u> アクセスポイント管理 アクセン	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( <u>HELP</u> ) アクセスポイント更新・削除 soliton.FURUNOSYSTEMS	<b>しいしていたい しのしていたい しいしてい し</b> びアウト
管理者メニュー アクセ	2スポイント管理 アクセスポイント設定
機種名 アクセスポイント名	ACERA1020 APO1@soliton_FURUNOSYSTEMS
メモ 利用場所 有線LANES字	(最大40文字) 屋内 →
「用いた」でなえた 	■使用する
IPアドレス (*) サブネットマスク (*) デフェルトゲートウェイ	192.168.1.1 24 bit (0~32)
テノオルトウート ジェ1 DNSサーバ (*)	192.168.1254 プライマリ (*) 8.8.8.8 セカンダリ 8.8.4.4
VLAN (*) Managed Server URL (*)	□ 使用する VLAN Nb. (1~4092) https://UNIFAS.co.jp/UNIFAS/MS/ (最大128文 字)
PROXY Server PROXY Server ボート番号	(最大128文 字) 8080 (0~65535)
VLANハイブリッド ステーション設定	無効 ▼
 ステーション機能の利用	<ul> <li>● 使用しない</li> <li>● 無線LAN1を使用する</li> <li>● 無線LAN2を使用する</li> </ul>
無線バンドステアリング機能 無線LAN 1 設定	無効 -
バンド 11 n/ac 機能 11 n/ac モード 11 n/ac モード	802.11a
11n/acパケット集約 チャネル	A-MPDU/A-MSDU → 36 (802.11a 屋内専用) → 回動的切替を有効にする
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。	4 ▼ 無効 ▼ オンラインモード オフラインモード(任意) SolitonLab

無線LAN 2 設定	
リバンド	802.11b/g =
11n 機能	有効 -
11nモード	20MHz -
<u>11nショートG</u> 設定	
<u>11nパケット集約</u>	
チャネル	動的切替を有効にする
送信出力	
	無如 一
ヤキュリティグループ	オンラインチード オフラインチード(任意)
※使用する場合に1つ以上選択して下さい。	SolitonLab
無線LAN IPマスカレード設定	
IPマスカレードの利用	同使田する
※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。	
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(*)	☑ 使用する
DHCPサーバ機能の利用 	ス 🗇 使用する
DHCP使用時のDNSサーバ	
※IPマスカレード使用時、DNSサーバの設定がはい場合、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 サーパ設定)で動作します。	>ライマリ S セカンダリ
DHCPブールIP開始アドレス (*)	
DHCPプールIP終了アドレス (*)	
DHCPリース時間 (*)	60 分(1~720)
オフラインモード切替	□自動
監視機器IPアドレス	
検出インタフェイス	無線LAN1 ▼
更新 リセット このアクセスポイントを削除	
このアクセスポイントを削除	

### 【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。

UNFAS Maraged Server(HELE) 新規アクセスポイント Soliton FURUNOSYSTEMS		<b>UNIFAS</b> 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ボイント管理アクセスボイノト設定	
アクセスボ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 アクセスポイント soliton.FURUNCSYST	(HELP) 役定 FEMS					<b>しいこちんち</b>
			<u>管理者メニュー フ</u>	ックセスポイン	<u>卜管理</u>	
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	稼動状況	情報表示	編集
AP01	ACERA1020				イベントログ 🚽 一覧	更新·削除
アクセスポイントの追加						
					Copyria	tht (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。

	u	ser01_	_02.p12					
広期書のインボート・ウィザーでの開始   このパゲードでは、証明書、証明書信頼リスト、および証明書たかリストモデイスクから証明書ストアにごすたまっていた。   正明書によって会行された証明書は、ユーゲーID を確認し、ゲークを確認したり、またはた中JJFY でで構成されまったのです。   「「「「」」」」」」   「「」」」」」   「」」「」」」」」」   一 の力、コンビューター(1)   」 の力、リンプレーター(1)   」 の力、リングレーター(1)   」 の力、リングレーター(1)   」 しつか、コンビューター(1)   」 のう、ロングレーター(1)   」 のう、ロングレーター(1)   」 しつか、コンビューター(1)   」 ひつい、ロングレーター(1)   」 のう、ロングレーター(1)   」 ひつい、ロングレーター(1)   」 のう、ロングレーター(1)   」 ひつい、ロングレーター(1)   」 ひつい、ロングレークー(1)   」 ひつい・ロングレークー(1)   」 ひつい、ロングレーク	- 🛃 証明	月書のインボ	ペート ウィザード					×
こからや-やな 転 時 ● 、 転 時 ● 低 戦 り へ か ひ び び 戦 労 大 か い か び か か ひ か ひ か ひ か ひ か ひ か ひ か ひ か ひ か	12	E明書の	インポートウィ	ィザードの開始	1			
田田県観によって条行された延明豊さ、ユーザーID を程度し、ゲーダを得種したり、まだけセキJUFYで存着目 されたさットワープ理解を提供するための信頼をもんでいます。証明豊久トアは、証明豊か併留されるシスタム とい現まです。         東京電加         ● 東京ロノブー(C)         ● つ カル コンビューター(L)         現行するには、(次へ) をクリックしてください。         ● 水ードるに有きフィル         インパート ライザード         ● 小川 コンビューター(L)         ● 小川 コンビューター(L)         ● 使用豊のインパート ウイザード         ● 使用豊のインパート ウイザード         ● 小川 ードラングルを指定してください。         ● プリート ラクライルを指定してください。         ● プリート ラクライルを指定してください。         ● 「ビビショー>>>シューション         ● 「ビビショー>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	20 La	のウィザードで ます。	は、証明書、証	明書信頼リスト、	および証明書失効り	ストをディスクから	5証明書ストアにコピー	
単な世形           ● 現在のユーザー(C)           ● ローカル コンピューター(L)           味行す あには、(次へ) ゼクリックしてください。           (アノー・ドラ カンド)           ● 愛 短明色のインボート ウィザード           インボート サ カファイル ビ インボート サ カファイル ビ インボート サ カファイル ビ オンボート サ カファイル ビ オンボート ジョ コン ワノイル ビ 雑変の 延明 音 年 保 で き ま ?:           ア・パル 名(F):           「CVU Servi % coll in 10 marking か 延明 音 年 保 で き ま 5:           Personal Information Exchange - PKCS #12 (.PFX, P12)           Cyptographic Message Syntax Standard: PKCS #7 延 顧 母 (.P78)           Microsoft シリアリル し された 延 母 母 ストア (.S51)	証 され 上	明機関によ れたネットワー の領域です	って発行された国 - ク接続を提供す -	E明書は、ユーザー するための情報をき	IDを確認し、データ ちんでいます。証明者	を保護したり、また マトアは、証明者	とはセキュリティで保護 きが保管されるシステム	
根行するには、[次へ] モクリックしてください、	Ľ	保存場所 ・現在の:	ユーザー(C) - コンピューター(L)					
次ハN         キャンセル           スハN         キャンセル           インボートウイブード         インボートウイブード           インボートする互相書ファイル インボートするファイルを指定してください。         インボートするファイルを推定してください。           アイル全(F):         「クリレムビートウトガード」           CMUSersFacilitation WDesktop Muser01_02.p.12         参照(R)           注意: 次の形式を使うと 1 つのファイルに複数の証明書を保留できます:         Personal Information Exchange- PKCS #12 (.PFX, P12)           Cyptographic Message Syntax Standard・ PKCS #7 証明書 (.P78) Microsoft シリブルルとされた証明書ストア (.SST)         Microsoft シリブルルとされた証明書ストア (.SST)	続	行するには、	. [次へ] をクリック	7してください。				
次へN         キャンセル           なへN         キャンセル								
次へ(N)         キャンセル           インボートライブード         インボートライブード           インボートラる証明書フィル         インボートラる正常書ファイル           インボートラコフィイルを指定してください。         アーイル名(F):           ごぞしたersiteointon*Desktop#user01_02.p12         参照(R)           注意: 次の形式を使うと1 つのファイルに複数の証明書を供管できます:         Personal Information Exchange- PKCS #12 (.PFX, P12)           Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P78)         Microsoft シリアル化された証明書ストア (.SST)							-	
インボートする証明書ファイル インボートするファイルを指定してください。 ファイル名(F): CMUsers¥solitonMDesktop¥user01_02.p12 参照(R) 注意: 次の形式を使うと1つのファイルに被数の証明音を保管できます: Personal Information Exchange- PKCS #12 (.PFX, P12) Cryptographic Message Syntax Standard- PKCS #7 証明音 (.P78) Microsoft シリアル化された証明音ストア (.SST)	- 29 証明	明書のインボ						×
マンポードするマアイルを指定してください。          アンイル名(F):       「ごべしSersWsolitonWDesktopHuser01_02.p12       学習(R)         注意:次の形式を使うと1つのファイルに複数の証明書を保留できます:       Personal Information Exchange- PKCS #12 (JPFX, P12)         Cryptographic Message Syntax Standard・ PKCS #7 証明書 (JP78)         Microsoft シリアル化された証明書ストア (SST)								
ファイル名(F):       CNUsersWsolitonNDesktop¥user01_02.p12       参照(R)         注意:次の形式を使うと1つのファイルに複数の証明書を保管できます:       Personal Information Exchange- PKCS #12 (PFX, P12)         Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P78)         Microsoft シリフル化された証明書ストア (.SST)	インボ	ートする証明 インポートす	ラァイル るファイルを指定	してください。				
CWUsers¥solitonWDesktop¥user01_02.p12 参照(R) 注意:次の形式を使うと1つのファイルに複数の証明音を保管できます: Personal Information Exchange- PKCS #12 (.PFX,P12) Cryptographic Message Syntax Standard- PKCS #7 証明音 (.P78) Microsoft シリプルにされた証明音ストア (.SST) 文へ(N) キャンセル		ファイル名(F	·);					
注意: 次の形式を使うと 1つのファイルに複数の証明書を保管できます: Personal Information Exchange- PKCS #12 (PFX, P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P78) Microsoft シリアル化された証明書ストア (.SST) 文へ(N) 本ャンセル		C:¥Users¥	soliton¥Deskto	p¥user01_02.p1	2		参照(R)	
Pessonal Information Exchange- PKCS #12 (.PFX, P12) Cryptographic Message Syntax Standard- PKCS #7 証明會 (.P78) Microsoft シリアル化された証明會ストア (.SST) 文へ(N) キャンセル		注意: 次の	形式を使うと1つ	のファイルに複数	の証明書を保管でき	ます:		
Clypudgapute message synak sandadur PKC * 2 55 (P-16) Microsoft シリアル化された証明書ストア (.SST) 文へ(N) キャンセル		Person	al Information	Exchange- PKC	\$#12 (.PFX,.P12)	( 07P)		
次へ(N) キャンセル		Micros	oft シリアル化され	ge syntax stand れた証明書ストア	(.SST)	8 (.F/b)		
次へ(N) キャンセル								
						3	Rへ(N) キャンセル	

← ● 証明書のインボート ウィザード	×
税書キーの保護 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)	
インボートオブション(り: □ 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が	さびに確認を求められます。
<ul> <li>このキーをエクスポート可能にする(M)</li> <li>キーのバックアップやトランスポートを可能にします。</li> </ul>	
✓ すべての拡張プロパティを含める(A)	
	次へ(N) キャンセル
•	×
← 参 証明者のインボートウィザード	
証明書ストァ 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、かのフトアに配置する(0)	
び 単分音をすべてくのストアト 単星 9 (F) 証明書ストア:	参照(R)
	The start of an
	次へ(N) キャンセル
← ● 証明者のインポート ウィザード	×
証明書のインボートウィザードの完了	
[兜了]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。 確認された証明書フトア ウムザードで自動的に注意されます。	
内容 PFX ファイル名 Ci¥Users¥soliton¥Desktop¥user01_02.p12	
	完了(F) 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 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。



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。

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	ок

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	ок

### 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。

÷	Wi-Fi		
	ON		
•	SolitonLab		
Solito	nLab		
EAP方式	ţ		
TLS			•
CA証明	書		
TestC4	λ.		•
ドメイン	2		
ユーザ-	-証明書		
user01			•
ID Waar <b>O</b>			
usero			
詳細設の			^
レ フロキ: なし			~
101000			
DHCP			-
		キャンセル	接続

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。

SolitonLab ワイヤレス ネットワークのプロパティ X	項目	値	
接続 セキュリティ			
セキュリティの種類(E): WPA2 - エンタープライズ ~	ビイエリティル		42-1-2-9-2-2-2-1-A
暗号化の種類( <u>M</u> ): AES ~	喧亏化の裡類	AES	
	ネットワークの	D認証・・・ Micr	osoft:保護された EAP
ネットワークの認証方法の選択((2)): Microsoft: 保護された EAP (PEAP)       設定(2)         〇 ログオンするたびに、この接続用の資格情報を使用する(2)         詳細設定(2)         0K       キャンセル	保護された EAP のプロパラ 接続のための認証方法: ② 証明書を検証してり ③ 次のサーバーに接続 ■ Microsoft Root ( ③ Microsoft Root ( ④ TestCA ■ thawte Primary □ Thawte Timest □ UTN - DATACOT □ UTN - USERFIRSt ○ Asign Bákset addr □ サーバーに暗号化パイ □ ID プライパシーを有効 □ UTN - DATACOT □ UTN -	デイ         サーバーの ID を検証する(少)         焼する (例: srv1, srv2, .*¥.srv3¥.com)         機關(R):         Certificate Authority 2010         Certificate Authority 2011         y Root CA         tamping CA         rp SGC         t-Object         3 Public Primary Certification Authority 2011         gtanta         (ご切えつード (EAP-MSCHAP v2) ~         こする(E)         (ンドの TLV がない場合は切断する(D)         hにする(I)         OK         AP MSCHAPv2 のプロパティ         接続のための認証方法:         Windows のログオン名とパスワード         OK         OK	X N(O): Nority - G5 を表示する(E) -ザーに求めない(P) 構成(C) キャンセル × (およびドメインがある ンゼル
ОК <b>キャンセル</b>	項目		值
	接続のため	の認証方法	

- サーバー証明書の検証をする

- 信頼されたルート認証機関

On

TestCA

項目	値
認証モードを指定する	ユーザー認証

## 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。

← WI-FI		
ΟΝ		
SolitonLab		
4		
SolitonLab		
PEAP		•
MSCHAPV2		<b>.</b>
CA証明書		
TestCA		<b>.</b>
ドメイン		
ID		
user01		
匿名ID		
パスワード		
······		
□ ハスリートを表示する 詳細設定値日		^
プロキシ プロキシ		
なし		-
IP設定		
DHCP		*
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

# 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 cli	ent RadiusClient port 0 cli 34-F3-9A-1E-4F-CE)	
	種別	āZā正	
	日時	2017-01-12 14:27:45	
ACERA 1010/	アクセスポイント	AP01	
	ESSID	SolitonLab	
ACERA 1020/	BSSID	00:D0:1 D:1 A:93:19	
UNIFAS Managed Server	MAC Address	34:F3:9A:1 E:4F:CE	
	ID		
	発生場所	authinfo	
	発生理由	Radius_Authticated(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 clien server) Login OK: [user01] (from clien	t RadiusClient port 0 cli 34-F3-9A-1E-4F-CE via pro t RadiusClient port 0 cli 34-F3-9A-1E-4F-CE)	oxy to virtual
	種別	言恐言正	
	日時	2017-01-12 14:46:36	
ACERA 1010/	アクセスポイント	APO1	
ACERA 1010/	ESSID	SolitonLab	
ACERA 1020/	BSSID	00:D0:1 D:1 A:93:19	
UNIFAS Managed Server	MAC Address	34:F3:9A:1E:4F:CE	
	ID		
	発生場所	authinfo	
	発生理由	Radius_Authticated(192.168.1.2)	

#### 改訂履歴

日付	版	改訂内容
2017/02/16	1.0	初版作成