

【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	説明
•	利用の参考となる補足的な情報をまとめています。
<u>.</u>	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
2 405月4 1010/405月4 1020 の設宁	10
3.1 ACERA 1010/ACERA 1020 の設定	13
3-2 ACERA ヘログイン	14
3-3 ID アドレフ設定	15
3.4 毎娘設定	17
3-4 無縁設定	10
5-5 ESSID 設定	10
3-6 設定反映	
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 サプリカント設定	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 サプリカント設定	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 サプリカント設定	28
5. EAP-PEAP 認証でのクライアント設定	29

	5-1 Windows 10 のサプリカント設定	29
	5-2 iOS(iPhone 6)のサプリカント設定	30
	5-3 Android(Pixel C)のサプリカント設定	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
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使知道把		
CANDERIN	"−hca ¥	
CA REEM		
● 内部で新しい鍵を生成する		
公開減方式	RSA 🗸	
親長	2048 🗸	
○ 外部HSMデバイスの鍵を6	用する	
要求の署名		
要求署名アルゴリズム	SHA256 V	
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	
878-C		
CA署名設定		



NAS/RADIUSクライアント名	RadiusClient01	
	を有効にする	
	● NAS/RADIUSクライアント ● NASのみ ● RADIUSクライアントのみ	
1899)	0	
	192.168.1.1	
シークレット・		
NAS調別値		
	灰石	次へ

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。

NetAttest EPS				(hyt	ログオン中: admin
 naeps.example.com システム設定 システム管理 証明機関 DHCPサーバー LDAPサーバー RADIUSサーバー ユーザー ユーザー エクブート エンボート エンボート エーザーパスワードポリシー 	<u>・</u> ユーザー一覧 ユーザー <u>単細オブションの陸定</u> エクスポート	● 一部 ● 完全 グループ <u>名前</u> test user	✓ ユーザーまで 検索 ユーザーⅡ Lesi	<u>ユーザー副時時の</u> 最終認証成功日時 第明書 発行	道加 2011月また3002 2020 タスク 変更 刊 E
<i>■ 〒</i> フォルトユーザーブロファイル					
			ユーザー設定 編集対象: 新規 ユーザー機能 ユーザー機能 ユーザー機能 チェッグアイテム し ユナ 4582	リライアイテム ロゼ	•
750			姓	user01	
現日			E-Mail		
姓	user01		詳細情報		0
ユーザーID	user01		認証情報 ユーザーID	user01	
パスワード	password	1	パスワード・	•••••	
			「 」 「 「 (4篇2) ●	••••••	
				ОК ++>>tell	通用
Net Attest EPS				¥	ログオン中: admi
NotAttest Ero	N 100			(1 २७७)	ページ 📵 ログオフ
 nacps.cxample.com システム設定 	📥 ユーザー一覧				
■ システム官理 ■ 証明機関	ユーザー <u>詳細オプションの設定</u>	 ● 一部 ● 完全 グループ 			
■ DHCPサーバー ■ LDAPサーバー					追加
■ RADIUSサーバー = ユーザー		夕前	⊐_ +f_m	<u>ユーザー削除時の</u> 品数物転成れた中央 数回会	D証明書失効オプション
■ ユーザー一覧 ■ エクスポート		test user	test	<u>最終設計成功自時</u> 並明書 発行	変更 削除
		user01	user01	発行	変更削除
■ エーサーバスワートホリンー ■ デフォルトユーザープロファイル					

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の設定

3-1 ACERA 1010/ACERA 1020 設定の流れ

- 1. ACERA ヘログイン
- 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。

ユーザ名とパスワードを入力してください	J		
http://192.168.1.10 がユーザ名とパスワードを要求しています。サイトからのメッセージ:	Ι.		
-Access Point Configuration		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。



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。

基本設定 ・ 一般設定	▲ 保存 変更を適用して再起動
・無線LAN設定 ・ MORS設定	一般設定

IP アドレス等、有線 LAN 側の設定を行います。

動作モード	AP 🚽	0				
ユーザID	user	0	無線 IPマスカレード設	定		
パスワード		0	IPマスカレード	◎ 有効 ◎ 無効		
AP名	WN0209	0	無線側IPアドレス			
/F		0	サフネットマスク			
	さむ(用)	0	1目級LAN/11/3	◎ 有効 □ 無効		
	nn () (43) 🔶		DHCPサーバ設定			
专编工业和现实			DHCPサーバ機能	○ 古持 ◎ 新持		
ᆂᇃ	WN0209		プライマリDNS	- 11741 - 11-741		
• AP &	VVIN0209		セカンダリDNS			
LPアトレス設定	◎ 固定 ◎ DHCP		DHCPプール範囲		~	
IPアF レス	192.168.1.1		DHCPリース時間	60	分	
サブ ネットマスク	255.255.255.0	0				
ゲートウェイ		0	管理設定			
ブライマリDNS		0	NTP設定	◎ 有热 ◎ 無効		
セカンダリDNS		0	NTPサーバアドレス			
VLAN ID		0	NTP同期周期 CVCLOCH	1時間 🚽	0	
通信速度	AUTO 🚽	Ø	SYSLUG9 - APP VX	• • • • • • •	0	
DUPLEX	AUTO 🚽	Ø	SNMDTRAC	● 無効 ● 有効	0	
リンク監視	(a) 27.84 (b) 48.84	0	30011444-2716			
	0.041 0 100 100	-				
			SNMPマネージャ			
			SNMPv3設定	◎ 使用しない ── 使用する		
			SNMPv3ユーザ名			
			SNMPv3認証パスワード		0	

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おりません。

3-4 無線設定

「基本設定」の「無線 LAN 設定」を選択します。



チャネル等、必要に応じて設定してください。

Sンド Fャネル	802.11ac 🚽		
チャネル		802.11b/g 🚽	0
	5.20 GHz (40) 🖕	2.412 GHz (1) 🚽	0
かめチャネル切り替え	◎ 無劫 ◎ 有劫	◎ 無劾 ◎ 有劾	0
l1ac/11nモ∽F	VHT40 🗸	HT20 🗸	0
進信出力	5 👻	5 🕌	0
ミーコンインターバル	100 🖵	100 🗸	0
ゴードインター バル	Short O Long	Short O Long	0
Fragmentation Threshold	2346	2346	0
RTS Threshold	2347	2347	0
Protection Mode	淋し -	CTS to self 🚽	0
『ケット集約モード	AMPDU/AMSDU 🚽	AMPDU/AMSDU 👻	0
票稳通信公平化 機能	◎ 無劾 ◎ 有劾	◎ 無热 ◎ 有効	Ø
■線 AN共诵設定			

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。

保存します	
よろしし rで:	ອໍ້ກາ?
ОК	キャンセル

※この時点ではまだ設定は反映されておりません。

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

基本設定 ・一般設定 ・無線LAN設定 ・MORS設定	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
無線LAN1 セキュリティ設 定	設定のコピー ESSID 1 ✓ へ下記設定内容を コピー ●
• ESSID 1	設定 ④ 有效 〇 無效 😢

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)

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			
設定のコピー	ESSID 1 🗸 へ下記設定内容を 🛛 🖵 ビ	@	
設定	◎ 有劾 ◎ 無効	0	
ESSID	SolitonLab	ø	
VLAN ID		0	
QoSブライオリティ	3 👻	ø	
接統制限	◎ 有劫 ◎ 無劫	0	
制限台数	127	0	
DTIMインターバル	1 👻	0	
ステルスモード	◎ 有劾 ◎ 無効	0	
無線リンク監視レベル	無効 🚽	e	
再接続待ち時間	0	0	
any拒否	◎ 有劫 ◎ 無劫	0	
無線セパレータ	◎ 有劾	0	
無線 セパレータポリシー	通遇 这所	0	
無線セパレータ例外アドレス		0	
		÷:	

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	0	
対象MACアドレス		•	
MACアド レスフィルタリン	グレベル 🔘 高 🕘 課準	Ø	
暗号化設定			
暗号方式	WPA2-Enterprise		0
WEP設定			-
	オーチ	Open Shared	0
	キー		0
WPA固有設定			-
	暗号化方式	🔵 TKIP 🖲 AES 🔘 AES/TKIP(自動)	0
	パスフレーズ	TESTSAMPLE	0
	GTK更新聞開	7200	0
	事前認証	◎ 有效 ◎ 無效	0
	PMF	◎ 無效 🔘 有效(自動選択) 🔘 有效(必须	i) 🐵

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	0
	プライマリ認証サーバボート	1812	0
	ブライマリ認証サーバクレデンシャル	secret	0
	セカンダリ認証サーバ		0
	セカンダリ認証サーバボート	1812	0
	セカンダリ認証サーバクレデンシャル		0
	デリミタ		0
アカウンティング設定			—
	ブライマリアカウンティングサーバ		0
	ブライマリアカウンティングサーバポート	1813	0
	ブライマリアカウンティングサーバクレデンシャル		0
	セカンダリアカウンティングサーバ		0
	セカンダリアカウンティングサーバボート	1813	0
	セカンダリアカウンティングサーバクレデンシャル		0
	デリミタ	- 🗸	0

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		
プライマリ想証サーバ	192.168.1.2	Ø
プライマリ想証サーバポート	1812	0
プライマリ想証サーバクレデンシャ	PJb secret	0
セカンダリ問題サーバ		0
セカンダリ問証サーバボート	1812	0
セカンダリ問題サーバクレデンシー	419	Ø

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。

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LAN	l1 セキュリティ設定 ESSID 1
設定を保存	乳しました。

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。



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。

userol	
🛃 証明書のイン	ポート ウィザード
証明書の	ラインボート ウィザードの開始
このウィザード します。	では、証明書、証明書信頼リスト、および証明書夫効リストをディスクから証明書ストアにコピー
証明機関に されたネット 上の領域で	よって発行された証明會は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護 フーク提供を提供するための诸範を合んでいます。証明者ストアは、証明者が保管されるシステム す。
保存場所 ・現在()	ת וµ שילק=ש-(ו)
() = ///	t (26A) 8-7(19-7(17/42))
	次へ(N) キャンセル
ジ 証明書のイン	夜へ(N) キャンセル ボート シィブード
- - - - - - - - - -	次へ(N) キャンセル ボート ウィザード
ジ 証明書のイン インポートする証明 インポート	次へ(N) キャンセル ボート ウィザード ぽファイル きるファイルを指定してください。
ジョ 登明書のイン インポートする証明 インパート ファイル条 ファイル条	次へ(N) キャンセル ボート ウイザード ほファイル Fo ファイルを指定してください。
 ジジ 証明者のイン インボートする証明 インボート インボート ファイル名 C:¥Usert 	次へ(N) キャンセル ボート ウィザード ■ファイル P3ファイルを指定してください。 (P): ※Koliton¥Desktop¥user01_02.p12 参照(R)
ジ 証明書のイン インポートする証明 インポート インポート インポート インポート インポート インポート ファイル名 こ :¥Usen 注意:次の	次へ(N) キャンセル ボート ウイザード ■ファイル # 20アイルを指定してください。 [5]: #voliton¥Desktop¥user01_02:p12 参照(R) D形式を使うと 1 つのファイルに複数の証明巻を保管できます:
ジ 証明書のイン インポートする証明 インポート ファイルを C:ギUseri 注意:次C Perso Cret	次へ(N) キャンセル ボート ウィザード ■ファイル キョファイル ドゥンアノルを指定してください。 (P): ※koliton WDesktop¥user01_02_p12 参照(R) D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: nal Information Exchange - PKCS #12 (.PFX, P12) comparishic Messaes Syntax Standard - PKCS #12 (P78)
 ジ 証明書のイン インボートする証明 インボート ファイル名 C:¥Useri 注意:次(Perso Crypt Micro 	次へ(N) キャンセル ボート ウィザード ************************************
 ジ 証明書のイン インボートする証明 インボート ファイルを C:FUSen 注意:次位 Perso Crypt Micret 	次へ(N) キャンセル ボート ウィザード ************************************
ジ 証明書のイン インポートする証明 インポート ファイル名 C:¥Usen 注意:次の Perso Crypt Micre	次へ(N) キャンセル ボート ウィザード ************************************
 ジ 証明書の1ン インポートする証明 インポート ファイル名 C: USen C: USen 注意: 次(Perso C: ypt Micro 	次へ(N) キャンセル ボート ウィザード オコアイル すっファイルモ指定してださい。 (F): #Soliton WDesktop¥user01_02.p12 参照(R) り形式を使うと 1 つのファイルに複数の証明書を保筆できます: nal Information Exchange- PKCS #12 (.PFX, P12) ographic Message Syntax Standard - PKCS #7 証明書 (.P78) soft シリアル化された証明書ストア (.SST)
ジ 証明書のイン インボートする証明 インボート C:¥Usen 注意:次C Perso Crypt Micre	次へ(N) キャンセル ボート ウィザード ************************************

ᢧ

← </td <td>×</td>	×
税営キーの保護 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。	
- /(スワ−ト ⁽ P): ●●●●●●●●●	
□ パスワードの表示(D) インボート オプション(I):	
□ 秘密キーの保護を強力にする(E) このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。 □ このキーをエクスポート可能(にする(M)	
 □ ビップ モンスパート すいにします。 ■ オーのパッグアップやトランスポートを可能にします。 ☑ すべての拡張プロパティを含める(A) 	
次へ(N) キャンオ	elli
← ● 証明書のインポート ウィザード	×
証得書ストア	
証明書ストアは、証明書が保留されるシステム上の領域です。 	
Windowsに証明巻ストアを自動的に選択させるか、証明巻の場所を指定することができます。	
 ● 星が苦切(塗剤) を Jいて、目前に) 星が長くアを溜がす G(U) ○ 延明巻きすべい次の入りに記載する(P) 	
延明但入下7: 参照(向	
ンアイ/NI キャンチ	711.
◆ 愛 証明書のインボートウバザード	×
証明書のインボートウィザードの完了	
[売了]をクリックすると、証明書がインボートされます。	
次の設定が指定されました 選択された証明巻ストア ウィザードで自動的に決定されます	
アメロードアネ ファイル-名 CiVUsersVsolitonVDesktopVuser01_02.p12	
完了(り) キャンセ	eJl

【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。



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

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。

÷	Wi-Fi		
	ON		
•	SolitonLab		
Solito	onLab		
EAP方示	ť		
TLS			•
CA証明	書		
TestC/	A		•
ドメイ	2		
ユーザ・	-証明書		
user01			-
ID			
user0	1		
詳細設	定項目		^
プロキョ	2		
なし			*
IP設定			
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。

まました100m またしまたの またの またの またの またの またの またの またの またの またの
世界シックの部長が1002 AES オック・クの部長が1002 アンク・クの部長が1002 Macrosofte SRGを死したAPPのFAM WICCOSOfte / CAPA () ワバナダムじた、この時時用の食物像産を使用する() WICCOSOfte / CAPAのの認証・・・ () ワバナダムじた、この時時用の食物像産を使用する() WICCOSOfte / CAPAのの認証・・・ () ビバナダムじた、この時時用の食物像産を使用する() WICCOSOfte / CAPAのの認証・・ () ビバナダムじた、この時時用の食物像産を使用する() WICCOSOfte / CAPAのの認証・ () ビバナ () ビージーの食物像産を使用する() WICCOSOfte / CAPAのの() () ビビビー WICCOSOfte / CAPAのの() () ビビビー WICCOSOfte / CAPAのの() () ビビビー WICCOSOfte / CAPAのの() () ビビー WICCOSOfte / CAPAのADCOSOfte / CAPAのADCO
第年のの構成が MS 2×ウケークの認知たあの変化の: Monosoft: 環境になどの(FAM) 設またの。 (日クオンダムクに、この読み用の食情構成を使用する(D) (日クオンダムクに、この読み用の食情構成を使用する(D) (日クオンダムクに、この読み用の食情構成を使用する(D) (日日本) (日日本) (日日本) (日本) (日日本) (日本) (日本) (日日本) (日本) (日本) (日日本) (日本) (日本) (日本) (日日本) (日本) (日本) (日本) (日日本) (日本) (日本) (日本) (日日本) (日本) (日本) (日本)
ネッチック-の総選方法の選択(): ままの 「日ブオッチなんびに、この接続用の貴格確範を使用する()) 「日本のなんびに、この接続用の貴格確範を使用する()) 「日本のなんびに、この接続用の貴格確範を使用する()) 「日本のなんびに、この接続用の貴格確範を使用する()) 「日本のなんびに、この接続用の貴格確範を使用する()) 「日本のなんびに、この接続用の貴格確範を使用する()) 「日本のなんびに、この接続用の貴格確範を使用する()) 「日本のなんびに、このは読用の貴格確範を使用する()) 「日本のなんびに、この接続用の貴格確範を使用する()) 「日本のなんの認証方法: 「日本のなんびに、」のし、キャンをあん 「日本のなんのびご方法」 「日本のなんびに、コッシューナーの日を読証する()] 「日本のなんのびご方法 「日本のなんびに、コッシューナーの貴格信範を使用する()] 「日本のなんのびご方法」 「日本のなんのびご方法」 「日本のなんのびご方法」 「日本のなんのびごうた」 「日本のなんのびご方法」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんのびごう」 「日本のなんののびごう」 「日本のなんのびごう」 「日本のなんののびごう」 「日本のなんのでのびごう」 「日本のなんののびごう」 「日本のなんののびごう」 「日本のなんののびごう」 「日本のなんののびごうる」 「日本のなんののびごうる」 「日本のなんののびごうる」 「日本のなんののびごうる」 「日本のなんののびごう」 「日本のなんののびごうる」 「日本のなんののびごう」 「日本のなんののびごう」 「日本のなんののびごうる」 「日本のなんののびごう」 「日本のなんののびごう」 「日本のなんのびごうったいのなんののびごろ」 <td< td=""></td<>
「Windows od J-J-742 (ス) 「 (as of ス) J の of 場合はドメイン)を自動的に使う(Δ)

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

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。「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。「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		
ON		
SolitonLab		
Solitonl ab		
EAP方式		
PEAP		~
フェーズ2認証		
MSCHAPV2		.
CA証明書		
TestCA		-
ドメイン		
ID		
user01		
匿名ID		
パスワード		
·····		
□ ハスワートを表示する 詳細設定項目		^
T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 client RadiusClient port 0 cli 34-F3-9A-1E-4F-CE)
ACREA 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

改訂履歴

日付	版	改訂内容
2017/02/16	1.0	初版作成