



【連携機器】サイレックス・テクノロジー AP-500AC 【Case】IEEE802.1X EAP-TLS/EAP-PEAP 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、サイレックス・テクノロジー社製 無線アクセスポイント AP-500AC の IEEE802.1X EAP-TLS / EAP-PEAP 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、
<u>.</u>	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 AP-500AC 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。

<mark>S≎liton</mark> 目次

1. 構成
1-1 構成図3
1-2 環境
1-2-1 機器
1-2-2 認証方式
1-2-3 ネットワーク設定4
2. NetAttest EPS の設定5
2-1 初期設定ウィザードの実行5
2-2 システム初期設定ウィザードの実行6
2-3 サービス初期設定ウィザードの実行7
2-4 ユーザーの登録8
2-5 クライアント証明書の発行9
3. AP-500AC の設定10
3-1 設定モードの実行10
3-2 Web 設定ページを利用したセットアップ 11
3-2 Web 設定ページを利用したセットアップ11 4. EAP-TLS 認証でのクライアント設定
 3-2 Web 設定ページを利用したセットアップ
 3-2 Web 設定ページを利用したセットアップ 11 4. EAP-TLS 認証でのクライアント設定 13 4-1 Windows 10 での EAP-TLS 認証 13 4-1-1 クライアント証明書のインポート 13 4-1-2 サプリカント設定 15 4-2 iOS での EAP-TLS 認証 16 4-2-1 クライアント証明書のインポート 16 4-2-2 サプリカント設定 17 4-3 Android での EAP-TLS 認証 18 4-3-1 クライアント証明書のインポート 18 4-3-2 サプリカント設定 19
 3-2 Web 設定ページを利用したセットアップ
 3-2 Web 設定ページを利用したセットアップ
 3-2 Web 設定ページを利用したセットアップ

Seliton®

5. EAP-PEAP 認証でのクライアント設定	24
5-1 Windows 10 での EAP-PEAP 認証	24
5-1-1 Windows 10 のサプリカント設定	24
5-2 iOS での EAP-PEAP 認証	25
5-2-1 iOS のサプリカント設定	25
5-3 Android での EAP-PEAP 認証	26
5-3-1 Android のサプリカント設定	26
5-4 BR-300AN での EAP-PEAP 認証	27
5-4-1 BR-300AN のサプリカント設定	27
6. 動作確認結果	29
6-1 EAP-TLS 認証	29
6-2 EAP-PEAP 認証	29
6-3 端末接続状況	29

<u>Seliton</u>

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



S≎liton®

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	4.10.4
AP-500AC	サイレックス・テクノロジー	RADIUS クライアント (無線アクセスポイント)	1.1.3
BR-300AN	サイレックス・テクノロジー	802.1X クライアント (ワイヤレスブリッジ)	1.6.0
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サプリカント
iPad Air 2	Apple	802.1X クライアント (Client SmartPhone)	12.2
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0
NetAttest D3-SX15	ソリトンシステムズ	DHCP/DNS サーバー	4.2.17

1-2-2 認証方式

IEEE802.1X EAP-TLS/EAP-PEAP

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
AP-500AC	192.168.1.1/24	UDF 1612	secret
BR-300AN	DHCP		
VAIO Pro PB	DHCP	-	-
iPad Air 2	DHCP	-	-
Pixel C	DHCP	-	-

Seliton®

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

管理ページにアクセスしたら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
- ドメインネームサーバーの設定

Net Attest EPS		
50 11551224 2,220 3,220 4 2,224 5 2,224 5 5	Ψ-F Inmata S	
Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.		
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	
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	20	
外部サーバー証明書	無効	
RADIUSプロキシ	無効	
Windowsドメイン認識正連携	無効	
グループ	無効	
MACアドレス認証	無効	
ポート制御	無効	
	〒2 五七4	

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

Seliton®

2. NetAttest EPS の設定

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

CAMPBEER			
CAMPORIN	ルートCA ❤		
CARCER			
● 内部で新しい鍵を生成する			
公開職方式	RSA 🗸		
親長	2048 🗸		
○ 外部HSMデバイスの鍵をf	吏用する		
要求の署名			
要求署名アルゴリズム	SHA256 V		
CA情报			
	TestCA		
	日本	~	
都道府県名	Tokyo		
市区町村名	Shinjuku		
会社名(組織名)	Soliton Systems		
部署名			
E-mailアドレス			

項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA

EAP		
EAP語語ウイブ 優先期位 認証シイブ 1 TLS × 2 PEAP × 3 なし × 4 なし × 5 なし ×		Î
EAP-TL&/TTL&PEAPオプション		
	<u>1024 マ</u> バイト	
メッセージの長さ情報	フラジメントされた 最初のパケットにのみ含まれる 🗸	
EAP-TTLS/PEAPオプション		
■ GTC記証を有効にする		
■ TLSセッションキャッシュを有効		
EAP-FASTオブション		~



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

Seliton

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。

						ログオン中・admit
NetAttest EPS				(They they they they they they they they t	-ジ) 🕒 談	ロノオノキ: Aunua を保存 🕦 ログオフ
■ naeps.example.com	2 7_H					
■システム設定		92.		48. +		
■ 証明機関	ユーサー 詳細オブションの話	● →部 ● 完全 註:	クループ 🎽 🗾 ゴ			
■ DHCPサーバー	エクスポート					
■ RADIUSサーバー				<u></u>	-ザー削除時の	道加 証明書失効オブ /ョン
■ ユーザー		名前	<u>ユーザーID</u>	最終認証成功日時	証明書	タスク
■ エクスポート	•	test user	<u>test</u>		発行	変更 削余
■ インボート ■ フーザーパフロードポリシー						
■ エーブーバスフードホリン ■ デフォルトユーザープロファイ	ОV					
■ ゲスト						
						↓
			📃 🔔 ユーザー設定			
			編集対象: 新規			
			ユーザー情報 チェックア 基本情報			
			9±*	user01		
			名			
			E-Mail			
			詳細情報			
па	庙		ユーザーID*	user01		
坝日			パスワード・	•••••		
姓	user01		パスワード(確認)	•••••	<u>م</u>	
7-#-TD	user01		□一時利用停止			
	useroi					
パスワード	password				K = ++>te	ル道用
						ログオン中: admi
NetAttest EPS				() トップペ	-ジ 🕒 読	定保存 📵 ログオフ
■ naeps.example.com	🤶 7+f					
 ■ システム設定 ■ システム管理 		372 0		46. +		
■ 証明機関	ユーサー 詳細オブションの話	● →部 ● 元全 9定	クループ 🎽 🗾 ゴ			
■ DHCPサーバー	エクスポート					
■ RADIUSサーバー					-ザー削 <u>除時</u> σ	追加 証明書失効オブション
		名前	<u>ユーザーID</u>	最終認証成功日時	証明書	タスク
■ エーリーー覧 ■ エクスポート		test user	test		発行	変更 削除
		user01	<u>user01</u>		発行	変更 削除
■ ユーサーバスワードボリシー ■ デフォルトユーザープロファイ	<u>а</u> .					
■ゲスト						



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.p12 という名前で保存)

					ログオン中: ad
NetAttest EPS				۲ ۲ ۲ ۲	ージ 🕒 設定保存 📵 ログオン
= naeps.example.com	N	nr≁.			
■ システム設定		<u>一</u> 宜			
■ システム管理 <u>-</u>	1-4-	● 一部 ● 完全	グループ 🚩 ユ	ーザーまで検索	
■ mynoxは ■ DHCPサーバー T	細 <u>オブションの</u> クァポート	<u>97</u>			
■ LDAPサーバー					追加
■ RADIUSサーバー				<u></u>	- ザー削除時の証明書失効オプション
		名前	<u>ユーザーID</u>	最終認証成功日時	証明書 タスク
<u> </u>		test user	test		発行 変更 削除
■ インボート		user01	<u>user01</u>		発行 変更 削除
■ ユーザーバスワードポリシー ■ ニューリーユーザープロフロ / JI					
■ デフォルトエーリーフロファイル ■ ゲスト					
					•
			編集対象: user01		
			基本情報	ucor01	
			*1		
			та т. мя		
			E-Maii		
			詳細情報		0
			認証情報		
			ユーザーID	user01	
			有効期限		
			● 日付 2016 ♥ 3	目 〒 7 ✔月 9 ✔ 日 23 N	✓ 時 <mark>59 ❤</mark> 分 <mark>59 ❤</mark> 秒まで
			証明書ファイルオプション		
			パスワード		
項目		値	バスワード(確認)		
「田聿右効期限」		365	※パスワードが空間の場合には		
		505	☑ PKCS#12ファイルに証明	機関の証明書を含める	
PKCS#12 ファイルに証明機関の	D · · · 0	チェック有			発行 キャンセル
					Ļ
		@			·
		- ユーザー証明	書のタワンロード		
		ユーザー証明書ダウンロ	コードの準備ができました。対象	をファイルに保存して	ちい。 ダウンロード

Seliton

3. AP-500AC の設定

3-1 設定モードの実行

AP-500ACの初期設定は本体内部のWeb設定ページから行います。

下記手順で本体内部 Web 設定ページにアクセスしてください。

1. 設定用の管理端末と AP-500AC をネットワークケーブルで直接接続。



- 2. AP-500AC に付属の AC アダプタを接続し、AC アダプタのプラグをコンセントに差し込む。
- 3. 電源投入後、筐体上部の「ACTIVE」LED が緑色に点灯したら 「SW2」(プッシュスイッチ)を先の細いもので数秒(約3秒)押し込む。
- 4. 筐体上部の「ACTIVE」LED が橙点滅に変わったらプッシュスイッチを離す。



- 5. 管理端末で Web ブラウザ(Internet Explorer など)を起動すると AP-500AC の Web 設定ページが起動する。
 - ◆ 表示されない場合はアドレスバーに「http://silex」と入力してください。





3-2 Web 設定ページを利用したセットアップ

Web 設定ページが開いたら必要な個所の設定を行います。必要最低限の項目は下記の通りです。 無線 LAN に関連する部分の設定は利用する環境によって異なります。 ご利用環境に併せて設定してください。下記は 2.4GHz で設定した場合の一例です。

1. 「TCP/IP 設定」内の下記項目

項目	値
DHCP クライアント	無効
IP アドレス	192.168.1.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.1.254

2. 「無線 LAN(2.4GHz)設定」-「無線 LAN 共通設定」の下記項目

項目	値
無線モード	802.11n/b/g/
チャネル帯域幅	20MHz
通信チャネル	11

3. 「無線 LAN(2.4GHz)設定」-「無線 LAN 基本設定 1」の下記項目

項目	値
インタフェース	有効
SSID	任意文字列(1-32 文字の文字列)
ステルス	無効
ネットワーク認証	WPA2-Enterprise



4. 「無線 LAN(2.4GHz)設定」-「WPA/WPA2 設定」の下記項目

項目	値
暗号方式	AES
グループ鍵更新間隔	60

5. 「無線 LAN(2.4GHz)設定」-「RADIUS サーバ設定」の下記項目

項目	値
サーバ IP アドレス	192.168.1.2
ポート番号	1812
シークレットキー	secret

6. 設定実施後、画面右下の「更新」ボタンを押下する



7. 再起動を促すメッセージが表示されるので「再起動」ボタンを押下する



8. 再起動後、ネットワークケーブルを管理端末から外し実際の利用環境に接続し直して完了



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.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。





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。

[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。

ユリティの種類(E): WPA2 - エン	タープライズ ~	項目	值
化の種類(N): AES	v	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
-ッーッの認証力法の選択(U): rosoft: スマート カードまたはその他の証明 コグオンオスたびに、アの持续日の違いませい	月書 ✓ 設定(S) ●	ネットワークの認証・・・	Microsoft: スマートカード・
詳細設定(D)	OK キャンセル 上 資格情報の保存(C) 除する(D) (C) 水ンを有効にする(S) (C) る(E) (C) る(F) 10 (アログの表示を許可する(L)) (C) とユーザーの認証に別の仮想 (C)	スマートカー 提続のための認証方法: 自分のスマートカードを ② このンピューターの証明 「単純な証明書の選択を 「証明書を検証してサー/ 次のサーバーに接続する 「「加水セ Primary Ru 「Microsoft Root Cet 「Microsoft Root Cet 「Thawte Primary Ru 「Thawte Primary Ru 「Thawte Primary Ru 「Thawte Timestam UTN - DATACOPS 「WerlSign Class 3P」 「新しいサーバーまたは握 この接続で別のユーザー名	ドまたはその他の証明書のプロバライ 使う(S) 詳細設定(A) 書を使う(C) (法会)(#実)(M) (-の ID を検証する(V) る (例: srv1, srv2, *¥.srv3¥.com)(0): (f(R): ttrificate Authority 2010 ttrificate Authority 2011 oot CA uping CA SGC bject bjilic Primary Certification Authority - CS 正明書を表示する(E) i類された証明機関を承認するようユーザーに求めない(P) (本使う(D) (K) キャンセンレ
		項目	值
	ОК ‡ †>±и		
		- 単純な証明書の選	沢を使う(推奨) On
	值	証明書を検証してサー	バーのIDを・・・ On



4-2 iOS 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には 下記などがあります。

- 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て 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。

S会目までの 4-2-2 サプリカント設定

AP-500AC で設定した SSID を選択し、サプリカントの設定を行います。 まず、「ユーザ名」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 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て 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 8.1.0 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が、

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

AP-500AC 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」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下さい。

÷	Wi-Fi		(
	ON		۰
	SolitonLab		â
	•		
Soli	tonLab		
EAP	式		
TLS		-	
CA証	明書		
Test	CA	~	
ドメー			
7-4			
user)1	-	
ucon			
ID	01		
user			
詳細詞	段定	~	
		キャンセル 接続	
		キャンセル 技統	

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

<u>Seliton</u>

4-4 BR-300AN での EAP-TLS 認証

4-4-1 管理画面へアクセス

BR-300AN に NetAttest EPS から発行したクライアント証明書をインポートするには 本体内部の Web 設定ページを使用します。

下記手順で本体内部 Web 設定ページにアクセスしてください。

1. 設定用の管理端末と BR-300AN を付属のネットワークケーブルで直接接続。



- 2. BR-300AN に付属の AC アダプタを接続し、AC アダプタのプラグをコンセントに差し込む。
- 3. 電源投入後、筐体上部の「POWER」LED が赤色に点灯したらプッシュスイッチを 数秒押し込む。
- 4. 筐体上部の「WLAN」LED と「STATUS」LED が緑色で同時点滅を開始したら

プッシュスイッチを離す。



- 5. 管理端末で Web ブラウザ(Internet Explorer など)を起動すると BR-300AN の Web 設定ページが起動する。
 - ◆ 表示されない場合はアドレスバーに「http://silex」と入力してください。





4-4-2 無線 LAN 設定

Web 設定ページが開いたらサプリカントの設定とクライアント証明書のインポートを行います。 必要最低限の項目は下記の通りです。

1. 「詳細設定」タブに移動

	■ 無線LAN 設定			
言語選択 Japanese ~	簡単設定 詳細設定 スマート無線設定			
 ▼ システム設定 - 無線LAN設定 - 高度な設定 - 証明書設定 - パスロード設定 	無線LANのパラメータを手動で設定します。 パラメータを入力して「設定更新」をクリックしてください。			

2. 「無線 LAN 基本設定」内の下記項目

項目	値
無線モード	Infra
無線規格	AUTO
SSID	AP-500AC に設定した SSID
SSID フィルタ	OFF (※ 環境により ON)
ネットワーク認証	WPA2
IEEE802.1x 認証	ON

3. 「IEEE802.1x 認証設定」内の下記項目

項目	値
IEEE802.1x 認証モード	EAP-TLS

4. 「WPA/WPA2 設定」内の下記項目

項目	値
暗号化方式	AES



5. 「IEEE802.1x 認証ユーザ設定」内の下記項目

項目	値
IEEE802.1x ユーザ名	user01

6. 「IEEE802.1X 接続機器設定」内の下記項目

項目	値
接続機器フィルタ	ON
接続機器アドレス	※ BR-300AN を接続する機器の MAC アドレス

7. 設定実施後、画面右下の「更新」ボタンを押下





4-4-3 クライアント証明書のインポート

1. 「証明書設定」メニューに移動

	■ 証明書設定
言語選択 Japanese ~	証明書設定
▼ システム設定 - 無線LAN設定 高度な設定 - 証明書設定 - パスラード設定	IEEE802.1X認証で使用する証明書を登録します。

- 2. 「クライアント証明書」内の「証明書ファイル」欄を選択後、「参照」ボタンより NetAttest EPS で発行したクライアント証明書ファイルを指定し、「パスワード」を入力
- 3. 「CA 証明書」内の「証明書ファイル」欄を選択後、「参照」ボタンより NetAttest EPS で発行したクライアント証明書ファイルを指定
- 4. 設定実施後、画面右下の「更新」ボタンを押下



5. 再起動を促すメッセージが表示されるので「再起動」ボタンを押下





5. EAP-PEAP 認証でのクライアント設定

5-1 Windows 10 での EAP-PEAP 認証

5-1-1 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 × 接続 セキュリティ		項目		値	
		セキュリティの	D種類	WPA2-エンク	タープライズ
セキュリティの種類(E): WPA2 - エンタープライズ 暗号化の種類(N): AES		暗号化の種類		AES	
		ネットワークの	D認証・・・	Microsoft: 🕯	呆護された EAP
? ? <td?< td=""> <td?< td=""> <td?< td=""></td?<></td?<></td?<>	******			R護された EAP のプロパテ・ パーの ID を検証する(V) する (例: srv1, srv2, .*¥.srv3 購(R): iertificate Authority 2011 Root CA mping CA > SGC Object Public Primary Certification 取得者が指定されなかった場合にこ スワード (EAP-MSCHAP v2) る(F) なのの(N) 水の Tuv がない場合は切断する こする(I) のK EAP MSCHAPv2 の) の認証方法: dows のログオン名とパスワード 「シイン) を自動的に使う(A)	イ × i<
		項目			値
		接続のための語	忍証方法		

- サーバー証明書の検証をする

- Windows のログオン名と・・・

- 信頼されたルート認証機関

項目	値
認証モードを指定する	ユーザー認証

On

Off

TestCA



5-2 iOS での EAP-PEAP 認証

5-2-1 iOS のサプリカント設定

AP-500AC 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。

★ 設定 Wi-Fi	キャンセー	"SolitonLab"のパスワードを入力	接續	キャンセル 証明書	信頼
Wi-Fi	ユーザ名	user01		naeps.local 発行元: TestCA	
ネットワークを選択 SolitonLab	パスワート	•••••		信頼されていません 有効期限 2026/01/26 13:46:29	
その他	モード		自動 >	詳細	>
接続を確認	→			→	
接続したことのあるネットワークに自動的に接続します。接続した ことのあるネットワークが見つからない場合は、手動でネットワー クを選択する必要があります。					
	a w	ertvui			
	as	dfqhj	k I		
	☆ z	xcvbn	m 🗵		
	.?123	space	return		

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

Soliton

5-3 Android での EAP-PEAP 認証

5-3-1 Android のサプリカント設定

AP-500AC 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」にインポ ートした CA 証明書を選択してください。

← Wi-Fi
ON
SolitonLab
SolitonLab
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
□ パスワードを表示する
詳細設定
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

Soliton

5-4 BR-300AN での EAP-PEAP 認証

5-4-1 BR-300AN のサプリカント設定

BR-300AN のサプリカントの設定は本体内部の Web 設定ページより行います。 Web 設定ページへのアクセスは「4-4-1 管理画面へアクセス」をご参照ください。 Web 設定ページが開いたら必要な個所の設定を行います。必要最低限の項目は下記の通りです。

1. 「詳細設定」タブに移動



2. 「無線 LAN 基本設定」内の下記項目

項目	値
無線モード	Infra
無線規格	AUTO
SSID	AP-500AC に設定した SSID
SSID フィルタ	OFF(※ 環境により ON)
ネットワーク認証	WPA2
IEEE802.1x 認証	ON

3. 「IEEE802.1x 認証設定」内の下記項目

項目	値
IEEE802.1x 認証モード	PEAP

4. 「WPA/WPA2 設定」内の下記項目

項目	値
暗号化方式	AES



5. 「内部認証方式設定」内の下記項目

項目	値
内部認証方式	MSCHAPv2

6. 「サーバ証明書検証設定」内の下記項目

項目	値
サーバ証明書の検証	OFF

7. 「IEEE802.1x 認証ユーザ設定」内の下記項目

項目	値
IEEE802.1x ユーザ名	user01
パスワード	secret

8. 「IEEE802.1X 接続機器設定」内の下記項目

項目	値
接続機器フィルタ	ON
接続機器アドレス	※ BR-300AN を接続する機器の MAC アドレス

9. 設定実施後、画面右下の「更新」ボタンを押下



10. 再起動を促すメッセージが表示されるので「再起動」ボタンを押下



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 RadiusClient01 port 0 cli 40-A3-CC-32-10-A4)
AP-500AC	ath0: STA 40:a3:cc:32:10:a4 IEEE 802.1X: authenticated - EAP type: 13 ((null))

6-2 EAP-PEAP 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 RadiusClient01 port 0 cli 40-A3-CC-32-10-A4 via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 0 cli 40-A3-CC-32-10-A4)
AP-500AC	ath0: STA 40:a3:cc:32:10:a4 IEEE 802.1X: authenticated - EAP type: 13 ((null))

6-3 端末接続状況

AP-500AC 管理画面の[ステータス表示]-[無線 LAN]にて確認できます。

■ アクセスポイント		
無線ステーション ステータス		
		🌶 更新 📭 ヘルプ
MACアドレス	電波強度(dBm)	IPアドレス
40:a3:cc:32:10:a4	•••••••••••••••••••••••••••••••••••••••	192.168.1.100
▶ 2.4GHz - 無線LAN 2		
MACアドレス	電波強度(dBm)	IPアドレス

<u>Seliton</u>

改訂履歴

日付	版	改訂内容
2019/11/06	1.0	初版作成