



【連携機器】NEC プラットフォームズ NA1500A 【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、NEC プラットフォームズ社製無線 アクセスポイント NA1500A 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
(پ	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 NA1500A 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。

1. 構成1
1-1 構成図 1
1-2 環境2
1-2-1 機器
1-2-2 認証方式 2
1-2-3 ネットワーク設定2
2. NetAttest EPS の設定3
2-1 初期設定ウィザードの実行3
2-2 システム初期設定ウィザードの実行4
2-3 サービス初期設定ウィザードの実行5
2-4 ユーザーの登録6
2-5 クライアント証明書の発行7
2. NA 1500A の訳中
3. NATSOUA の設定
4. EAP-TLS 認証でのクライアント設定11
4. EAP-TLS 認証でのクライアント設定
4. EAP-TLS 認証でのクライアント設定
4. EAP-TLS 認証でのクライアント設定
4. EAP-TLS 認証でのクライアント設定 11 4-1 Windows 10 での EAP-TLS 認証 11 4-1-1 クライアント証明書のインポート 11 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 14
4. EAP-TLS 認証でのクライアント設定 11 4-1 Windows 10 での EAP-TLS 認証 11 4-1-1 クライアント証明書のインポート 11 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 14 4-2-1 クライアント証明書のインポート 14
4. EAP-TLS 認証でのクライアント設定 11 4-1 Windows 10 での EAP-TLS 認証 11 4-1-1 クライアント証明書のインポート 11 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 14 4-2-1 クライアント証明書のインポート 14 4-2-1 クライアント証明書のインポート 14 4-2-2 サプリカント設定 15
4. EAP-TLS 認証でのクライアント設定 11 4-1 Windows 10 での EAP-TLS 認証 11 4-1-1 クライアント証明書のインポート 11 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 14 4-2-1 クライアント証明書のインポート 14 4-2-2 サプリカント設定 15 4-3 Android での EAP-TLS 認証 16
4. EAP-TLS 認証でのクライアント設定 11 4-1 Windows 10 での EAP-TLS 認証 11 4-1-1 クライアント証明書のインポート 11 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 14 4-2-1 クライアント証明書のインポート 14 4-2-2 サプリカント設定 15 4-3 Android での EAP-TLS 認証 16 4-3-1 クライアント証明書のインポート 16
4. EAP-TLS 認証でのクライアント設定 11 4-1 Windows 10 での EAP-TLS 認証 11 4-1-1 クライアント証明書のインポート 11 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 14 4-2-1 クライアント証明書のインポート 14 4-2-2 サプリカント設定 15 4-3 Android での EAP-TLS 認証 16 4-3-1 クライアント証明書のインポート 16 4-3-2 サプリカント設定 17
 4. EAP-TLS 認証でのクライアント設定 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 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 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 14 4-2-2 サプリカント設定 15 4-3 Android での EAP-TLS 認証 16 4-3-1 クライアント証明書のインポート 16 4-3-2 サプリカント設定 17 5. EAP-PEAP 認証でのクライアント設定
 4. EAP-TLS 認証でのクライアント設定
 4. EAP-TLS 認証でのクライアント設定 4. EAP-TLS 認証でのクライアント設定 11 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 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 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 14 4-2-2 サプリカント設定 15 4-3 Android での EAP-TLS 認証 16 4-3-1 クライアント証明書のインポート 16 4-3-2 サプリカント設定 17 5. EAP-PEAP 認証でのクライアント設定 18 5-1 Windows 10 での EAP-PEAP 認証 18 5-1-1 Windows 10 のサプリカント設定
 4. EAP-TLS 認証でのクライアント設定 4. EAP-TLS 認証でのクライアント設定 11 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 4-1-2 サプリカント設定 13 4-2 iOS での EAP-TLS 認証 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 14 4-2-2 サプリカント設定 15 4-3 Android での EAP-TLS 認証 16 4-3-1 クライアント証明書のインポート 16 4-3-2 サプリカント設定 17 5. EAP-PEAP 認証でのクライアント設定 18 5-1 Windows 10 での EAP-PEAP 認証 19



	5-3 Android での EAP-PEAP 認証
	5-3-1 Android のサプリカント設定20
6.	動作確認結果
	6-1 EAP-TLS 認証 21
	6-2 EAP-PEAP 認証



<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-SX04 の
 DHCP サーバーから払い出す



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
NA1500A	NEC プラットフォームズ	RADIUS クライアント (無線アクセスポイント)	1.0.26
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
iPhone 7	Apple	802.1X クライアント (Client Smart Phone)	12.0
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0
NetAttest D3-SX04	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
NA1500A	192.168.1.1/24	UDF 1012	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

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

NetAttest EPS				
K∵ HUBBACA (m. 202) 2-3 Marite - Marite -	V-F Family Family S			
opyright # 2004-2015, Soliton Systems K.K., All rights inserved.				
19月11年2797年~18月1日の電話 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-74222				
	200			
最大NAS/RADIUSクライアント数	20			
外部サーバー証明書	#K501			
RADIUS JUL+ 9	#X0			
Windowsh タイン記法比単語	#50 年か			
	mox/ 新动			
	<u>無効</u> 無効			
194164 T - Tr				
	戻る 再起物			
Copyright © 2004-2015, Soliton Systems K.K., All rights res	erved.			

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. 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

CA框例医訳			
CANDERIN	л−⊦са ∨		
CAREER			
● 内部で新しい鍵を生成する			
公開施方式	RSA 🗸		
親兵	2048 🗸		
○ 外部HSMデバイスの鍵を6	切用する		
要求の署名			
要求署名アルゴリズム	SHA256 V		
CA情報			
	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-mail7HJ-2			
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

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。

						-1
NetAttest EPS			(hu-to		ロク *辛切友)(オン中: admir
■ neeps.example.com	2 ユーザー		T P95A		RJEI#1	
■ システム設定 ■ システム管理		≑¢ би У 7	ーザーまで 検索			
■ 証明機関	ユーリー					
■ DHCPサーバー ■ L DAPサーバー	エクスポート					
■ RADIUSサーバー			<u></u>	- ザー削除時	の証明書失	<u>追加</u> 効オジ <mark>ノ</mark> ョン
	□	<u>ユーザーID</u>	最終認証成功日時	証明書	奴	10
 ■ エーリーー頁 ■ エクスポート 	test user	test		発行	変更	削余
■インボート						
 ■ ユーザーバスワードボリシー ■ デフォルトユーザープロファイル 						
■ゲスト						
						1
		💄 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 リプライアイテム	OTP		
		基本情報	user01			
		名				
		E-Mail				
		言关细情報			\bigcirc	
		認証情報				
項目	値	パスワード*	usero1			
<u>b</u> ‡	user01	バスワード(確認)	•••••	\$		
×1		■ 一時利用停止				
ユーザーID	user01					
パスワード	password			K ++)	セル 🕺	1用
	pubbiliti					
				,		
Not Attact EPC					ログ	オン中: admi
NEIMILESIEFS			(① トップペ	-ジ 🕒 🛙	定保存)(🕑 ログオフ
■ naepsexample.com	💄 ユーザ覧					
 ■ システム設定 ■ システム管理 	ユーザー • 一部 •	完全 グループ 💙 🍡 コ	レーザーまで 検索			
■ 証明機関	詳細オブションの設定					
■ DHCPサーバー ■ I DAPサーバー	<u>エクスポート</u>					AP to
■ RADIUSサーバー			<u></u>	ーザー削除時	の証明書失	<u>き</u> 加 効オブション
 ユーザー ユーザー 	▲ 名前	<u>ユーザーID</u>	最終認証成功日時	証明書	<u>9</u> 5	や
■ エクスポート	test user	test		発行	変更	削除
■ インボート	user01	<u>user01</u>		発行	変更	削除
■ <u>エーリーハスリートホリラー</u> ■ デフォルトユ <u>ーザープロファイル</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]-[ユーザーー 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)

Net Attest FDG					ログオン中: admin
NetAttest EPS				×5 و- ۱	ージ 🕒 設定保存 📵 ログオフ
■ naeps.example.com	ע-ב 🙎	/			
■ システム設定				44 + 7 19 5	
 ■ ンスデム官理 ■ 証明機関 	ユーザー 詳細オゴミュンの言	● 一部 ● 完全 Arc	グループ 💙 ユ	ーザーまで「快楽」	
■ DHCPサーバー	<u>エクスポート</u>	<u>v</u>			
■ LDAPサーバー					追加
RADIUSサーバー				<u>ר</u>	<u>-ザー削除時の証明書失効オプション</u>
- <u>+</u> - 「 ■ ユーザー→覧		名煎	<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	test		発行 変更 削除
		user01	<u>user01</u>		発行 変更 削除
■ エーリーハスワートホリシー ■ デフォルトユーザープロファイル ■ ゲスト					
					Ļ
			編集対象: user01		
			基本情報		
			姓	user01	
			名		
			E-Mail		
			詳細情報		0
			認計報		
			ユーザーID	user01	
			有効期限		
			● 日数 365 日 ● 日付 2016 ▼ 4	В Е 7 V 月 9 V н 23 N	4時 59 ▼ 分 59 ▼ 秒まで
			証明書ファイルオブション		
			パスワード		
項目		値	バスワード(確認)		
		365	※パスワードが空間の場合には	に ユーザーのパスワードを他用	
PKCS#12 ファイルに証明機	問の・・・	チェック有	✓ 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
		📥 ユーザー証明	唐のダウンロード 		
		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つ	きい。 ダウンロード

3. NA1500A の設定

3-1 ローカルコンソールによる設定

- 1) NA1500A の電源を切ります。
- NA1500Aの CONSOLE ポートとパソコンなどの端末を、コンソールケーブル ZB-NA-CON1 (別売)で接続してください。



※パソコンなどの端末側で USB 端子を使用する場合は、市販の USB-RS232C 変換ケーブルを 使用してください。

- 3) パソコンなどの端末の電源を入れてください。
- 4) パソコンなどの端末で、ターミナルソフトを下記のように設定変更します。

通信速度	: 9600 boud
データ長	: 8bit
パリティ	:なし
ストップビット	: 1bit
フロー制御	:なし

※あらかじめ作成したコンフィグの流し込みを行う場合は、取りこぼしを防ぐため、

ターミナルソフトを送信遅延(1ミリ秒/字以上)に設定してください。

- 5) ターミナルソフトから NA1500A にアクセスします。
 ※NA1500A に接続しているシリアルポート番号を指定します。(例) 接続方法: COM1
- 6) NA1500A の電源を入れます。
 ※しばらく待つと、「login:」と表示されます。

7) NA1500A にログインします。

管理者権限ユーザー名(login)と管理者権限パスワード(Password)の初期値は、

管理者権限ユーザー名(login) : config

管理者権限パスワード(Password): config

です。はじめて NA1500A にログインする場合は、管理者権限ユーザー名(login)と

管理者権限パスワード(Password)の変更が必要です。

ログインに成功すると、ターミナルソフト上で、「AP#」と表示されます。

8) 「config」コマンドを入力し、グローバルコンフィグレーションモードに入ります。

グローバルコンフィグレーションモードでは、下記のとおり、プロンプトが変化します

AP# config Enter configuration commands, one per line. End with CTRL+Z. AP(config)#

9) 以下の設定を入力します。

AP(config)# interface vlan u AP(config-vlan u)# ip address 192.168.1.1/24 AP(config-vlan u)# ip route 192.168.1.254 AP(config-vlan u)# vlan enable AP(config-vlan u)# exit AP(config)# ssid SolitonLab AP(config-ssid SolitonLab)# max-associations 50 AP(config-ssid SolitonLab)# vlan u AP(config-ssid SolitonLab)# encryption mode wpa2 aes AP(config-ssid SolitonLab)# authentication type dot1x AP(config-ssid SolitonLab)# radius host ip 192.168.1.2 acct-port 1813 auth-port 1812 retransmit 3 timeout 3 key 0 secret AP(config-ssid SolitonLab)# radio-device both AP(config-ssid SolitonLab)# hide bssid AP(config-ssid SolitonLab)# enable-ssid AP(config-ssid SolitonLab)# exit AP(config)# radio-enable both AP(config)# write memory

10) 「exit」コマンドを入力し、グローバルコンフィグレーションモードに抜け出ます。

その後、再度「exit」コマンドを入力し、NA1500A よりログアウトします。

AP(config)# exit AP#exit

3-2 SSH/Telnet 接続による設定(CLI)

1) NA1500A が有線 LAN 接続している LAN 上にパソコンなどの端末を接続します。



2) パソコンなどの端末で、ターミナルソフトを下記のように設定します。

IP アドレス あらかじめローカルコンソールで設定した固定 IP アドレスまたは DHCP サーバーから割り振られた IP アドレスを指定してください TCP ポート SSH の場合 : 22

telnet の場合 : 23

- 3) ターミナルソフトから NA1500A にアクセスします。
- 4) NA1500A にログインします。

※管理者権限ユーザー名(login)と管理者権限パスワード(Password)の初期値は、

管理者権限ユーザー名(login) : config

管理者権限パスワード(Password): config

です。はじめて NA1500A にログインする場合は、管理者権限ユーザー名(login)と

管理者権限パスワード(Password)の変更が必要です。

ログインに成功すると、ターミナルソフト上で「AP#」と表示されます。

※以降、コマンド入力がないまま約5分(初期値)経過すると強制的にログアウトされます。

5) 以降は、3-1章の8)と同様に設定します。

また、PC上で動くGUI設定ツールもご用意しております。本ツールのダウンロードとご使用方法 については、NECプラットフォームズのNA1500Aホームページまでアクセスしてください。 https://www.necplatforms.co.jp/product/na1500a/



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。



	4.EAP-TLS 認証 Cのクライアント
	7
 ※ 27 証明書のインポートウイザード 	
移営キーの保護 サキュロティタはサオスために 知道キ」(+パフロ」ドア母報キサア()+オ	
秘密キーのパスワードを入力してください。	
ノだスフード(P):	
 パスワードの表示(D) 	
インポート オブション(I):	
○ 秘密キーの保護を増力にする(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め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) キーのバックアップセトランフポートを可能に1.ます。	
マ すべての拡張プロパティを含める(A)	
	[パフロード]
次へ(N) キャンセル	「2-4 ユーザーの登録」で設定したパスワードを)
×	Π
証明書ストア 証明書ストアは 証明書が保管されるシステムトの領域です。	
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)	
 証明書をすべて次のストアに配置する(P) 証明書ストア: 	
参照(R)	
次へ(N) キャンセル	
]
×	1
€ 🖉 証明書のインボート ウィザード	
€ ₽ 証明書のインボート ウィザード	
 ・ ジ 証明書のインボート ウィザード 証明書のインボート ウィザードの完了 	
 	
 	
 ・ ・ ・	
 ・● ジ 証明書のインボート ウィザードの完了 正明書のインボート ウィザードの完了 [完了]をかりかすると、証明書がインボートされます。 次の設定が描述されました: 【読んれた証明書ストア ウィザードで目勤的に決定されます 内容 PX ファイル・名 C:¥Users¥Soliton¥Downloads¥user01_02.p12 	
 ・ ・ ・	
 	
 	

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。





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 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

NA1500A 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 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

NA1500A 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	0
ON	۲
V SolitonLab	â
	_
SolitonLab	
EAP方式	
TLS	
CA証明書	
TestCA	
ドメイン	
ユーザー証明書	
user01	
ID	
user01	
詳細設定	
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 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・	ィの種類	WPA2-エンタープライズ
でキュリテイの種類(E): WPA2 - エンターノフイス > 暗号化の種類(N): AES >		暗号化の種類	Į.	AES
		ネットワー	ウの認証・・・	Microsoft:保護された EAP
ネットワークの認証方法の遵択(O): Microsoft: 保護された EAP (PEAP) ✓ 設定(S) ✓ ログオンするたびに、この接続用の真俗情報を使用する(R)	******	·*****	(保護 接続のための認証方法: ♥証明書を検証してサーバーの □次のサーバーに接続する(4	された EAP のプロバティ × ID を検証する(V) 列: srv1, srv2, .*¥.srv3¥.com)(0):
詳細設定(D) OK キャンセル		······································	信頼されたルート証明機関(R Microsoft Root Certifi ダ TestCA thavte Primary Root してAwte Timestampir UTN - DATACorp SGC UTN - USERFirst-Objee VeriSign Class 3 Publi): cate Authority 2011 CA g CA t t c Primary Certification Authority - G5
<u> </u>	1		接続前の通知(T): サーバー名またはルート証明書	が指定されなかった場合にユーザーに通知します >
詳細設定 ×			認証方注を選択する(C)・	
802.11 の設定 802.11 の設定 図 認証モードを指定する(P): ユーザー認証			セキュリティで保護されたパスワー ▼高速再接続を有効にする(F) □ キットワーク アクセス保護を継げ □ サーバーに暗号化パインドの T □ ID プライパシーを有効にする(ド (EAP-MSCHAP V2) < 構成(C)● 関する(N) LV がない場合は切断する(D) I)
このネットワークに対するシングル サインオンを有効にする(S) アーザー ログオンの直部に書気でする(C)				OK キャンセル
 ● ユーザー ログオンの直接に案行する(E) ● ユーザー ログオンの直接に案行する(F) 母 大待ち時間(秒)(M): 図 シングル サインオン中に追加のダイアログの表示を許可する(L) ■ このネットワークでは、コンビューターとユーザーの認証に別の仮想 LAN を使用する(V) 		L	EA 接続のための認識 □ Windows 合はドメイン	P MSCHAPv2 のプロパティ 正方法: のログオン名とパスワード (およびドメインがある場 ク)を自動的に使う(A) OK キャンセル
OK #7721/		項目		値

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
- Windows のログオン名と・・・	Off

5-2 iOS での EAP-PEAP 認証

5-2-1 iOS のサプリカント設定

NA1500A 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。

く設定 Wi-Fi			"SolitonLab"のパスワードを入力]	キャンセル	証明書	信頼
		キャンセル	パスワード入力	接続				
Wi-Fi		ユーザ名	user01			maeg 発行方	ps.local īt: TestCA	
ネットワークを選択		パスワード	•••••			信頼:	されていません	
SolitonLab 🔒 🗢 🧻						有効期限 2026	5/01/26 13:46:29	
その他		モード		自動 >		詳細		>
接続を確認	\longrightarrow				\rightarrow	•		
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。								
				ion				
		y w e	l i y u					
		a s	d f g h	jkl				
		φz	xcvb	n m 🗵				
		.?123	space	return				

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



5-3 Android での EAP-PEAP 認証

5-3-1 Android のサプリカント設定

NA1500A 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
user01
EQUD
パスワード
□ パスワードを表示する
詳細設定 く
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

NA1500A のログを表示するには、3-1 章、3-2 章と同様に NA1500A にログインし、「config」 コマンドを入力しグローバルコンフィグレーションモードに入ります。このモードで「show associations」を入力します。

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(config)# show associations
	[radio0]
	[radio1]
	association 1
	MAC Address 40:a3:cc:32:10:a4
NA1500A	SSID SolitonLab
	Mode 11NG_HT20
	Security WPA2 (AES)
	RSSI 56
	Associated 00:02:58
	AP(config)#

6-2 EAP-PEAP 認証

EAP-PEAP 認証が成功した場合のログ表示例

NA1500A のログを表示するには、3-1 章、3-2 章と同様に NA1500A にログインし、「config」 コマンドを入力しグローバルコンフィグレーションモードに入ります。このモードで「show associations」を入力します。

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(config)# show associations
	[radio0]
NA1500A	[radio1] association 1 MAC Address 40:a3:cc:32:10:a4 SSID SolitonLab Mode 11NG_HT20 Security WPA2 (AES) RSSI 56 Associated 00:02:58
	AP(config)#

改訂履歴

日付	版	改訂内容
2018/12/11	1.0	初版作成

改訂履歴