



【連携機器】Hewlett Packard Aruba IAP 305 【Case】IEEE802.1X EAP-TLS/EAP-PEAP Rev2.0

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、Hewlett Packard 社製無線アクセスポイント Aruba IAP 305 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、
	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 Aruba IAP 305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	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 NetAttest D3の設定	13
3-1 スコープの設定	
3-2 IP アドレスの静的割り当て	15
3-3 DHCP サーバーの起動	16
4. Aruba IAP 305の設定	
4-1 WLAN 設定	
4-2 VLAN 設定	
4-3 セキュリティ設定	
4-4 アクセス設定	
5. EAP-ILS 認証でのクライアント設定	
5-1-1 クライアント証明書のインホート	
5-1-2 サノリカント設定	
	25
5-2-1 クライアント証明書のインボート	
5-2-2 サブリカント設定	26
5-3 Android での EAP-TLS 認証	27

Seliton®

5-3-1 クライアント証明書のインポート	27
5-3-2 サプリカント設定	28
6. EAP-PEAP 認証でのクライアント設定	29
6-1 Windows 10 での EAP-PEAP 認証	29
6-1-1 Windows 10 のサプリカント設定	29
6-2 iOS での EAP-PEAP 認証	30
6-2-1 iOS のサプリカント設定	30
6-3 Android での EAP-PEAP 認証	31
6-3-1 Android のサプリカント設定	31
7. 動作確認結果	32
7-1 EAP-TLS 認証	32
7-2 EAP-PEAP 認証	

目次

<u>Saliton</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



Spliton

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	4.10.3
Aruba IAP 305	Hewlett Packard	RADIUS クライアント (無線アクセスポイント)	v6.5x
Surface	Microsoft	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 SmartPhone)	iOS 11.2.6
nova	Huawei	802.1X クライアント (Client Tablet)	Android 7.0
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.15

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
Aruba IAP 305	192.168.1.1/24	0DF 1012	secret
Client PC	DHCP	-	-
Client SmartPhone DHCP		-	-
Client Tablet	DHCP	-	-

<u>Seliton</u>

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

Soliton

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
- ド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

<u>Seliton</u>

2. Net Attest 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







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

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。

et Attest FPS					ログ	オン中: a
CIALLOST EI O			(① トップベ	ページ 🕒 🖥	锭保存)(🔊 ログオ
aeps.example.com システム設定	🤳 ユーザー一覧					
システム管理	ユーザー 🛛 🔿 一部 🔍 完	全 グループ 💙 📃	ユーザーまで 検索			
証明機関 DHCPサーバー	詳細 <u>オプションの設定</u> エクマ ポート					
LDAPサーバー						追加
RADIUSサーバー			<u>_</u>	ーザー削除時(の証明書失う	効オブ /ョ
<u></u> ■ ユーザー一覧		<u>ユーザーID</u>	最終認証成功日時	証明書	رو 	ひ
■ エクスポート	test user	test		発行	変更	削余
■ インホート ■ ユーザーバスワードポリシー						
■ デフォルトユーザープロファイル						
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 基本 情報	アイテム リプライアイテム			
		<u>坐</u> 4 mm	user01			
		名				
		E-Mail				
		詳細情報			\bigcirc	
		認証情報 フーザーme	user01		_	
項目	値	パスワード・	••••••			
<i>b</i> 华	user01	パスワード(確認)	•••••	<u>م</u>		
×1		■ 一時利用停止				
ユーザーID	user01					
)K ± + - ' /	セル 🏾 🗎	I用
パスワード	nassword		C			
パスワード	password					
パスワード	password					
パスワード	password					
パスワード	password		 		口グ	オン中: a
パスワード etAttest EPS)	password		ع بر المراجع ((-Ÿ) (□ ≣	ログ	オン中: a も ログオ
パスワード etAttest EPS) aepsexample.com	password		ילנין ד	·	口グ 定保存)(オン中: a も ログオ
パスワード etAttest EPS) eepsexample.com システム設定 システム管理	password シューザー・覧 フーザー・覧		() トップベ 2-ザーまで 裕奈	······································	ログ 淀保存)(オン中: a ひ ログオ
パスワード etAttest EPS) aepsexample.com システム設定 システム管理 証明機関	password ユーザーー覧 ユーザー 覧 ・デ	全 グループ ▼	 ① トップペ 2-ザーまで <u>検索</u>	x	ログ	オン中: a 1) ログオ
パスワード etAttest EPS eepsexample.com システム設定 システム管理 証明機関 DtPPサーバー Loontt. 15	password <u> こーザーー覧</u> ユーザー <u> </u> ・ ージ ・ 売 詳細オブションの設定 エクスポート	全 グルーナ 💙 💶 二	 ①ザーまで <u>検索</u>		口グ	オン中: a も ログオ
パスワード etAttest EPS aepsexample.com システム設定 システム管理 証明機関 D+CPサーバー LDAPサーバー RADUSサーバー	password <u> こーザー一覧</u> <u> ユーザー一覧</u> <u> ユーザー 一覧</u> <u> ユーザー 一覧</u>	全 グルーナ 💙 💶 ニ	 (・)・ッフベ 2-ザーまで <u>検索</u>	- 17 - 11/15e8t5	口夕 远保存)(オン中: a 1) ログオ 道加 かオ チン・
パスワード etAttest EPS aepsexample.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 LDAPサーバー ユーザー	password <u> こーザー </u> ユーザー ゴンガー	全 グループ ▼ = <u>ユーザー10</u>	1-ザーまで 検索 最終語正成功日時	(一ジー前除時) 証明書	ログ 锭保存)(の証明書失 タフ	オン中: a も ログオ 追加 効オブショ ・ ク
パスワード etAttest EPS aepsezample.com システム設定 システム管理 証明機関 D+D+D+-バー LDAPサーバー LDAPサーバー ユーザー ユーザー エクスポート	password	注 グルーナ ▼ = <u>ユーザーID</u> <u>test</u>	ユーザーまで <u>検索</u> ユーザーまで <u>検索</u> 最終認証成功日時	 マジ) ○ 部 ブー削除時 証明書 発行 	ログ 定保存)(の証明書先 タフ 変更	オン中: a
パスワード CtAttest EPS aepsexample.com システム設定 システム管理 証明機関 D+CPサーバー LDAPサーバー IDAPサーバー RADUSサーバー ユーザー覧 コーザー覧 コンズホート	password <u> こーザー「覧</u> ユーザー「覧 ユーザー」 ● 一部 ● 売 詳細オブションの設定 エクスポート ■ 名前 ■ test user ■ user01	全 グルーナ ▼	2-ザ-まで <u>検索</u> 2-ザ-まで <u>検索</u> 最終認証成功日時	 ニジ (2) 部 ニヴ 一前除時 証明書 発行 	ログ 定保存)(の証明書失) タフ 変更 変更	オン中: a 3) ログオ 道加 効オブショ ク 一 削除 一 削除



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_02.p12 という名前で保存)

Not Attact EPS					ログオン中: admin
NetAllest EFS				(トップページ	
■ naeps.example.com	- 💄 ユーザー	一覧			
 ■システム設定 ■システム管理 	7.46				
■ 証明機関	- ユーター - 詳細 <u>オブションの設</u> 録				
■ DHCPサーバー	エクスポート				
				⊐+ * -	
- ユーザー		名前	ユーザーID		
■ ユーザー一覧		test user	test		発行 変更 削除
■ ±),,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		user01	user01		第二字車 副除
■ ユーザーバスワードポリシー ■ デフォルトユーザープロファイル ■ ゲスト					
			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	
			● 日数 365 日	·	
			● 日付 2016 V 年 新日本ファイルオナション	- <mark>7 ∨ 月 9 ∨ 日</mark> 23 ∨ 時	<mark>59 ></mark> 分 <mark>59 ></mark> 秒まで
			パスワード		
項目		値	バスワード(確認)		
「「「「「「」」」」		365	※ スワードが空間の場合には	、ユーザーのパスワードを使用します。	
		505	✓ PKCS#12ファイルに証明	繊則の証明書を含める	
PKCS#12 ファイルに証明	機関の・・・	チェック有			発行 キャンセル
		초 ユーザー証明	詰 のダウンロード		
	2	ー・ザー証明書ダウンに	コードの準備ができました。対象	ーー をファイルに保存して下さい	- ダウンロード

<u>Seliton</u>

3. NetAttest D3 の設定

Aruba IAP 305 は、デフォルトでは DHCP にて IP アドレスを取得するよう設定されています。 しかし、EPS に RADIUS クライアントとして登録するためには IP アドレスを静的に指定する必要が あります。今回は Aruba IAP 305 に静的に IP アドレスを割り当てるために、NetAttest D3 の静 的割り当て機能を使用して IP アドレスを払い出すことにします。

NetAttest D3 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、Google Chrome から [http://192.168.2.1:2181/]にアクセスしてください。NetAttest D3 では以下の設定を行います。

- DHCP サーバーの起動
- スコープの設定
- IP アドレスの静的割り当て

Seliton®

3-1 スコープの設定

[DHCP サービス]-[スコープ]から[追加]ボタンでスコープを追加します。今回は、端末に払い出す IP アドレスを[192.168.1.100-140]にするため、以下のように設定します。

NetAttest	D <i>3</i>		
 B 	ホスト名 nad3.example.com DNS 🗙	DHCP 🗶	
◆ システム設定			
◆ システム管理	DHCP - スコープ		
✔ ドメインネームサービス	<u>ネットワーク</u>	<u>IP使用率(%)</u>	
✔ DHCPサービス	表示するデーターはありません	<i>A</i>	
サーバー状態	追加 CSVダウンロード CSVアッ	<u>^</u> ド	
リース情報			
スコープ 登録クライアント			
	V		
NetAttest I	03		
	ホスト名 nad3.example.com DNS 🗙	рнср 🗙	
✔ システム設定		⇔±n	
▶ システム管理		旦/川	
✔ ドメインネームサービス	スコープの設定		
✓ DHCPサービス	ネットワーク 🕑	192.168.1.0	
サーバー設定	サブネットマスク	255.255.255.0	
リース情報	ルーター	192.168.1.254	TER
登録クライアント	ドメイン名	solitonlab.com	現日
静的割り当て 冗長化設定	ドメインネームサーバー	192.168.1.3	スコープの影
認証用NetAttest EPS設定 ユーザー定義オプション	レンジの設定		- ネットワ
ペンダー固有オブション	レンジ開始アドレス	192.168.1.1	- サブネッ
	レンジ終了アドレス	192.168.1.140	- ルーター
	除外レンジ開始アドレス	192.168.1.2	- 51/2
	除外レンジ終了アドレス	192.168.1.99	
	OK キャンセル		- ドメイン
			レンジの設定
			- レンジ開

項日	但
スコープの設定	
- ネットワーク	192.168.1.0
- サブネットマスク	255.255.255.0
- ルーター	192.168.1.254
- ドメイン名	solitonlab.com
- ドメインネームサーバー	192.168.1.3
レンジの設定	
- レンジ開始アドレス	192.168.1.1
- レンジ終了アドレス	192.168.1.140
- 除外レンジ開始アドレス	192.168.1.2
- 除外レンジ終了アドレス	192.168.1.99

3-2 IP アドレスの静的割り当て

Aruba IAP 305の MAC アドレスに IP アドレスを静的に割り当てるため、事前に Aruba IAP 305の MAC アドレスを確認してください。

[DHCP サービス]-[静的割り当て]から[追加]ボタンで IP アドレスの静的割り当てを行います。 Aruba IAP 305の MAC アドレスと、静的に割り当てる IP アドレスを指定します。

NetAttest D3							
 Image: Second sec	水スト名 nad3.example.com DNS X DHCP X						
 ✓ システム設定 ✓ システム管理 ✓ ドメインネームサービス 	DHCP - 静的割り当て 水ム上名 IPアドレス MACアドレス 優考1 優考2 優考3 最終リース日時						
▼ DHCPサービス サーバー状態 リーバー設定 リース情報 スコープ	ネ示すらデーターはありません フィルク 通知 CSVダウンバコード CSVアップロード 付加時報源目24のカスタマイズ						
日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日本 日							
NetAttest	D3						
 Image: Second sec	ホスト名 nad3.example.com DNS 🗙 DHCP 🗶						
 ✓ システム設定 ✓ システム管理 	┃ DHCP - 静的割り当て - 追加/修正						
♥ ドメインネームサービス	ホスト名 🕑 Aruba						
✓ DHCPサービス	IPアドレス 🗹 [192.168.1.1						
サーバー状態	MACアドレス 🕑 11:22:33:44:55:66						
リース情報	偏考1 [AP 305						
プーレス	備考2						
登録クライアント 静的割り当て	偏考3						
冗長化設定	OK キャンセル						

項目	値
ホスト名	Aruba
IP アドレス	192.168.1.1
MAC アドレス	11:22:33:44:55:66

	· · · · · · · · · · · · · · · · · · ·					
NetAttest D3						
 Image: Second sec	ホスト名 nad3.axample.com DNS X DHCP X					
 ✓ システム設定 ✓ システム管理 	DHCP - 静的割り当て					
ドメインネームサービス	ホスト名 IPアドレス MACアドレス 備考1 備考2 催考3 最終リース日時					
▼ DHCPサービス	Aruba 192.168.1.1 11:22:33:44:55:66 IAP 305					
サーバー状態	■ 全選択					
サーバー設定						
リース情報	表示すみ作数 25 · (全部・1ページ 1件)					
スコープ						
登録クライアント						
静的割り当て	フィルタ					
冗長化設定	追加 削除 全削除 CSVダウンロード CSVアップロード					
2221/INetAttest EPS822	付加情報項目名のカスタマイズ ゴーストMACアドレスの確認					
ユーザー定義オプション						

3-3 DHCP サーバーの起動

[DHCP サービス]-[サーバー状態]にて[起動]ボタンを押し、DHCP サーバーを起動します。

NetAttest D3								
	ホスト名 nad3.example.com DNS 🗶	DHCP 🗙						
 ◆ システム設定 ◆ システム管理 	┃ DHCP - サーバー状	設						
▶ ドメインネームサービス	動作状態	動作状態						
✓ DHCPサービス	サーバー稼動状態	停止						
サーバー状態 サーバー設定	冗長化状態	冗長化しない						
リース情報 スコープ	IP使用率(%)							
登録クライアント	0%							
静的割り当て	0 / 0 max							
冗長化設定 郑正田NatAttact EDC型字	起動 停止 Active昇格 初期	ル リース情報全消去 MACアド	レス使用履歴全消去 状態の更新					
認証用NetAttest EPS設定								

<u>Seliton</u>

4. Aruba IAP 305 の設定

Aruba IAP 305 は初期値として IP アドレスが設定されていません。管理画面にアクセスするため には、DHCP サーバーが動作している環境で利用するか、またはコンソールケーブルを用いて IP ア ドレスを設定する必要があります。今回は、D3 で静的に割り当てた IP アドレスを仕様し、管理画 面へのアクセスを行います。

アクセスする URL は、http://192.168.1.1、 初期ユーザー名/パスワードは、admin/admin です。

セットアップは下記の流れで行います。

- 1. WLAN 設定
- 2. VLAN 設定
- 3. セキュリティ設定
- 4. アクセス設定

Scliton

4-1 WLAN 設定

「新規」ボタンより、SSID を作成します。デフォルト状態では「instant」という SSID が登録されていますが、新規に SSID を作成すると自動的に消去されます。

								システム R	F セキュリティ メンテナンス 詳細表示・ ヘルプ ログアウト
a Hewlett Packard Enterprise company	VIRTUAL CONTROLLER INS	tant-CA	:F5:A6						食素
⊗ 1 ネットワーク		+	🔊 1 P/2	スポイント		+	📕 0 クライアン	2F	+
名前 → instant → 新規	クライアント 0		名前 。 34:fc:b9:ca:f5	:a6 *	クライアン 0	4	名前	IP アドレス	ESSID アクセスポイント
instant-CA:F	5:A6	DE Church	-#K			0.011001	et to UED Ucan		モニタリング IDS AirGroup 設定 0 アラート ー
▲ 電子: 「国一ド: (双国コントローラ IP: VC DNS: IP Mode: Cluster-Security DTLS: 管理: マスクー: アップリンクのタイブ: アップリンクステータス:	instant-CA:FS:A6 jP3 0.0.0.0 0.0	TAT !	75472F	シグナル !!	進度	アクセスポイント 34:fc:b9:ca:f5:z	使用率 16 <u></u>	/1X I5-	295/72 h 10 10 17:53 2JL-79 h (bps) 10 10 10 10 17:55 2JL-79 h (bps) 10 10 10 17:55 2JL-79 h (bps) 10 10 10 10 10 10 10 10 10 10
日本語 ▼						Aruba Central			一時停止

「名前」欄に SSID を設定します。ここで設定した文字列 SSID 名として出力されます。

新規 WLAN						<u>^///7</u>
1 WLAN 設定	2	VLAN	3	セキュリティ	4	アクセス
WLAN 設定						
名前と用途						
名前:	SolitonLab					
主な用途:	◉ 従業員					
	◎ 音声					
	○ダスト					

項目	値
名前	SolitonLab
主な用途	従業員

- ・ 従業員 → ゲスト、音声以外
- ・ 音声 → Wi-Fiを利用して音声通話が発生する場合
- ・ ゲスト → Web 認証

Seliton

4-2 VLAN 設定

クライアント IP の割り当てが「ネットワーク割り当て」の場合、Instant AP はブリッジとして動作し、SSID と紐付けた VLAN 上にある DHCP サーバーより IP アドレスを取得します。クライアント VLAN の割り当てが「デフォルト」の場合、VLAN との紐付けをせず、Instant AP が所属するネットワークに接続されます。

新規 WLAN				ヘルブ
1 WLAN 設定	2 VLAN	3 セキュリティ	4 アクセス	
クライアント IP と VLAN	の割り当て			
クライアント IP の割り当て:	 ● 仮想コントローラ管理 ● ネットワーク割り当て 			
クライアント VLAN の割り当て	● デフォルト ● スタティック ● ダイナミック			

項目	値
クライアント IP の割り当て	ネットワーク割り当て
クライアント VLAN の割り当て	デフォルト

4-3 セキュリティ設定

セキュリティレベルの設定を行います。外部認証サーバーとして EPS を指定してください。

新規 WLAN						<u> ヘルブ</u>	
1 WLAN	設定	2 VLAN		3 セキュリティ	4 アクセ	ス	
セキュリティ	レベル						
セキュリティ	*	コー管理・		WPA-2 エンタープライブ	•		
強める	-	1 単語:		内部サーバー	- -		
		再認証の間隔:		0 分 ▼			
 エンタ 	ープライズ ――	MAC 認証:		802.1X の前に MAC 認証を	実行		
x-y-	ナル			 ■ MAC 認証フェイルスルー			
<i>t</i> -7	新規 WLAN						<u>^ルブ</u>
	1 WLAN 設	定	2 VLAN	<mark>3</mark> 七キ	ミュリティ	4 アクセス	
8 A 11 A 1	セキュリティレ	ベル					
弱める	بغر العريد		date was				
	モイエリアイを 強める		キー管理:	WPA-2 I	9-7512 •		
	1		認証サーバー 1:	新九見	•		
	⊝- エンターフ	ブライズ ―	タ前・	NetAttestEPS		_	
	バーソナル	,	 IP プドレス:	192.168.1.2			
			RadSec:	無効 ▼			
	オープン		認証ポート:	1812			
	U		アカワンティンクホ 共有キー:	1813			
	セキュリティを 23 4 5		⇒−の再入力:	•••••			
	33000		タイムアウト:	5 t	9		
			再試行回缴:	3			
			RFC 3576:	無効			
			RFC 5997:				
				□ アカウンティング			
			NAS ID:		4 / ンヨノ) オブション)		
			停止時間:	5 5			
			DRP IP:				
			DRP マスク:				
			DRP VLAN:				
			DRP ゲートウェイ:			夏る 次へ	キャンセル
					0K キャンt	2/1	

項目	値
認証サーバー	外部サーバー
- 名前	NetAttestEPS
- IP アドレス	192.168.1.2
- RadSec	無効
- 認証ポート	1812
- アカウンティングポート	1813
- 共有キー/共有キーの再入力	secret



4-4 アクセス設定

セキュリティ画面にて「次へ」を押下するとアクセスルールの設定画面が表示されます。今回は アクセス制限を行いませんので「制限なし」を選択し、終了を押下します。

新規 WLAN				ヘルブ
1 WLAN 設定	2 VLAN	3 セキュリティ	4 アクセス	
アクセスルール				
詳細な制御				
- ロールベース				
- ネットワークベース				
⊖ - 刺限なし	宛先またはトラフィックのタイプに基づく	〈アクセス制限なし		
簡略な制御				
			戻る 終了 キ	ャンセル

以上で Aruba IPA 305の設定は完了です。

<u>Seliton</u>

5. EAP-TLS 認証でのクライアント設定

5-1 Windows 10 での EAP-TLS 認証

5-1-1 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

5-1-2 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。





5-2 iOS での EAP-TLS 認証

5-2-1 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。

5-2-2 サプリカント設定

Soliton

Aruba IAP 305 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。



Seliton

5-3 Android での EAP-TLS 認証

5-3-1 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 7.0 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



5-3-2 サプリカント設定

Aruba IAP 305 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下さい。

			O 🛡 🗎 14:19
← Wi-Fi			0
ON			•
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	妾続	

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



6. EAP-PEAP 認証でのクライアント設定

6-1 Windows 10 での EAP-PEAP 認証

6-1-1 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 ×		項目		値
		セキュリラ	⁼ ィの種類	WPA2-エンタープライズ
セキュリティの連鎖(E): WPA2 - エンターフライズ > 暗号化の種類(N): AES >		暗号化の種	類	AES
		ネットワー	-クの認証・・・	Microsoft:保護された EA
マットワークの認証方法の選択(O): Microsoft:保護された EAP (PEAP) ジログオンするたびに、この接続用の資格情報を使用する(R) 詳細設定(D) び	*******	*****	保護され 接続のための認証方法:	L した EAP のプロパティ × D を検証する(V) : srv1, srv2, .*¥.srv3¥.com)(O): .te Authority 2011 A CA Primary Certification Authority - GS 、 描志されなかった場合にユーザーに通知します ×
B+RulpSAE 802.1X の設定 802.11 の設定 ② 認証モードを指定する(P): ユーザー認証 ③ すべてのユーザーの資格情報を削除する(D) □ 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)			認証方法を選択する(S): セキュリティで保護されたパスワード ● 高速再接続を有効にする(F) ■ ペットワークアクセス保護を強制 ■ サーバーに暗号化パインドの TLL ■ ID プライパシーを有効にする(I)	(EAP-MSCHAP v2) v 構成(C) する(N) v がない場合は切断する(D) OK キャンセル
 ● ユーザー ログオンの直前に実行する(E) ● ユーザー ログオンの直後に実行する(F) 最大符ち時間(彩)(M): 10 ● 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、コンピューターとユーザーの認証に別の仮想 LAN を使用する(V) 			EAF 接続のための認証 〇 台はドメイシン	P MSCHAPv2 のプロパティ ち法: DDグオン名とパスワード (およびドメインがある場 を自動的に使う(A) OK キャンセル
ОК ‡ Р>セル		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

6-2 iOS での EAP-PEAP 認証

6-2-1 iOS のサプリカント設定

Aruba IAP 305 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。

●● au 4G	10:50	74%		••••• au	4G		17:12		83%	Ð	•••• au 4G	13:52
設定	Wi-Fi				"Se	olitonLab	のパスワー	ドを入力	i		キャンセル	証明書
				キャンセ	ル	パス	ワード入	カ	接紙			
Wi-Fi											naer	os local
				ユーザ名		user01					発行す	ī: TestCA
ネットワークを選択				パスワー	۲		•••				信頼さ	きれていません
SolitonLab		€ 중 (j)									有効期限 2026	6/01/26 13:46:29
その他				モード					自動 >		詳細	
									A REEC S			
接続を確認			\rightarrow									
接続したことのあるネ	ットワークに自動的に接続	売します。接続した										
ことのあるネットワー 7を選択する必要があ	クか見つからない場合は、 ります。	手順でネットワー										
				q w	е	r	t y	u	i o p			
				a		d f	a t	i	k I			
							9					
				☆ 2	z	x c	vk	n	m 👁)		

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

6-3 Android での EAP-PEAP 認証

6-3-1 Android のサプリカント設定

Aruba IAP 305 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
一 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

<mark>S≎liton</mark> 7. 動作確認結果

7-1 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	naeps radi port 0 cli 7	usd[115 701ce721	73]: notice f9f54)	2018,	/06/12 16	59:05 L	ogin	OK: [u	iser01] (from client Wire	lessAP
Aruba IAP 305	名前 - IP 7 user01 192	アドレス 2.168.1.100	MAC アドレス 70:1c:e7:2f:9f:54	0S 	ESSID SolitonLab	アクセスポイント 34:fc:b9:ca:f5:a6	チャネル 100E	タイプ AC	ロール SolitonLab	IPv6 Address シグナル fe80::ad1a:257	速度 (mbps) 234

7-2 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	列									
NetAttest EPS	naeps radius port 0 cli 70 naeps radius port 0 cli 70	sd[19514]: n 1ce72f9f54 v sd[19514]: n 1ce72f9f54)	otice 2018 ia proxy t otice 2018	8/06/12 1 :o virtual s 8/06/12 1	7:21:04 L server) 7:21:04 L	ogin (ogin (OK: [u OK: [u	ser01] (ser01] (from clie from clie	nt Wirel nt Wirel	lessAP lessAP
Aruba IAP 305	名前マ IP アドし user01 192.168	レス MAC アドレス i8.1.100 70:1c:e7:2f:9	OS f:54	ESSID SolitonLab	アクセスポイント 34:fc:b9:ca:f5:a6	チャネル 100E	タイプ AC	ロール SolitonLab	IPv6 Address シグ fe80::ad1a:257	ナル	速度 (mbps) 234

<u>Seliton</u>

改訂履歴

日付	版	改訂内容
2019/02/25	1.0	初版作成
2019/03/19	2.0	ロゴ画像差し替え

改訂履歴