



【連携機器】Aruba 7005/AP-205 【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、Aruba 社製無線 LAN コントローラ -7005 および無線アクセスポイント AP-205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 7005/AP-205 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6
1-1-1 機器7
1-1-2 認証方式7
1-1-3 ネットワーク設定7
2. NetAttest EPS の設定8
2-1 システム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. Aruba 7005 の設定13
3-1 Aruba 7005 設定の流れ13
Aruba の設定項目14
3-1-1 Controllerの基本設定14
3-1-2 APの基本設定16
3-1-3 SSID の設定19
3-1-4 Control Plane Securityの設定20
3-1-5 AP プロビジョニングの設定20
4. EAP-TLS 認証でのクライアント設定22
4-1 Windows 8.1 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
4-2-1 クライアント証明書のインポート
4-2-2 サプリカント設定26
4-3 Android(Nexus 7)での EAP-TLS 認証
4-3-1 クライアント証明書のインポート
4-3-2 サプリカント設定

5. EAP-PEAP 認証でのクライアント設定	29
5-1 Windows 8.1 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(Nexus 7)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 認証	. 32

<u>S≎liton</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



1-1-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS ST-04	Soliton Systems	RADIUS/CA サーバー	4.8.4
7005	Aruba	RADIUS クライアント (無線 LAN コントローラー)	6.4.2.12
AP-205	Aruba	アクセスポイント	6.4.2.12
Surface	MicroSoft	802.1X クライアント (Client PC)	Windows 8.1 64bit Windows 標準サプリカント
iPhone 6	Apple	802.1X クライアント (Client SmartPhone)	9.2.1
Google Nexus 7	ASUS	802.1X クライアント (Client Tablet)	5.1
NetAttest D3 SX-04	Soliton Systems	DHCP/DNS サーバー	4.2.2

1-1-2 認証方式

IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)

1-1-3 ネットワーク設定

製品名	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS ST-04	192.168.1.2/24	1913	secret
7005	192.168.1.1/24	UDF 1812	secret
AP-205	192.168.1.4/24		
Client PC	DHCP	-	-
Client SmartPhone	DHCP	-	-
Client Tablet	DHCP	-	-

2. NetAttest EPS の設定

2-1 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。

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.local
IP アドレス	デフォルト
ライセンス	なし

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

CA使用语识		
CA種別選択	ル-トCA ¥	
CA秘密線		
● 内部で新しい鍵を生成する		
公開観方式	RSA 🗸	
親長	2048 🗸	
● 外部HSMデバイスの鍵を使	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 イ	
都道府県名	Tokyo	
市区町村名	Shinjuku	
会社名(組織名)	Soliton Systems	
部署名		
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。

verattest	EDO					ログオン中: admin
	EPS			● トップペー	ジ 🕒 🐹	定保存 📵 ログオフ
naeps.local		💄 ユーザーー・覧				
システム設定				コーザーナで、検索		
証明機関	L. Ež	- サー ● 一部 ● 元 細オブションの設定	注 クルーフ 🎽	x (
DHCPサーバー		<u> </u>				
LDAPサーバー						追加
RADIUS ワーハー ユーザー				그는	<u>·ザー削除時の</u>)証明書失効オブ 雪ン
□ユーザー一覧		名前	<u>ユーザーID</u>	日時	証明書	タスク
■ エクスポート		test user	<u>test</u>		発行	変更 削 注
コインボート コマーザーパフロュ	- にまいシュー					
■ エーク <i>ー</i> ハスノー ■ デフォルトユーザ	ープロファイル		🤰 ユーザ-	一設定		V
			編集対象:	新規		
			ユーザー情報	🖁 チェックアイテム リプラ・		
			<u>金本市田和</u>		user01	
			名			
			E-Mail			
			詳細情報			0
			認証情報			
	項目	値	ユーザーm) •	user01	
			パスワード	(1)	•••••	
	姓	user01		明停止		•
		I IISALU I				
	ユーザーID	userui				
	ユーザーID パスワード	password				0K キャンセル 道用
	ユーザーID パスワード	password)K キャンセル 連用
	ユーザーID パスワード	password)K <u>キャンセル</u> 道用
	ユーザーID パスワード	password)K キャンセル 適用
	ユーザーID パスワード	password				ж <u>+</u> +r/eル 適用
at Attact	ユーザーID パスワード	Gran Tutab設定またはデー				ж キャンセル 道用 ログオン中: admin
etAttest	ユーザーID パスワード	user01 password 解存されていない設定またはデー	タがあります!	->50	- - - - - - - - - - - - - - - - - - -)K キャンセル 通用 ログオン中: admin 宦保存 (1) ログオフ
et Attest	ユーザーID パスワード	user01 password 解存されていない認定またロデー シューザーー皆	90%691±7 1	() ->->->->->->->->->->->->->->->->->->->	-y) (a 20	ж キャンセル 通用 ログオン中: admin 宦保存 (1) ログオフ
etAttest aepslocal システム設定	ユーザーID パスワード EPS	dser01 password 解存わていない設定またはデー シューザーー覧	タがあります!	->tei		K キャンセル 適用 □グオン中: admin 2保存 ④ ログオフ
et Attest aepslocal システム設定 システム管理 証明期期	ユーザーID パスワード EPS	user01 password <td>9//減ります! 注 グループ ♥</td> <td>① トップペー 3-ザーまで 検索</td> <td>-y) (a) 201</td> <td>K ‡ャンセル 通用 □グオン中: admin 2保存 ④ ログオフ</td>	9//減ります! 注 グループ ♥	① トップペー 3-ザーまで 検索	-y) (a) 201	K ‡ャンセル 通用 □グオン中: admin 2保存 ④ ログオフ
etAttest æpslocal システム設定 システム管理 証明機関 DHCPサーバー	ユーザーID パスワード EPS	user01 password 家存されていない設定また日子ー シューザーー覧 ・ザー 細オゴションの設定 フェボート	タがあります! 2全 グルーナ ▼	 トップペー ユーザーまで 検索 	「 マ ジ) 白 新)K キャンセル 通用 ログオ*ン中: admin E保存 10 ログオフ
et Attest æps.local 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	ユーザーID パスワード	user01 password 解存されていない設定またはデー シューザー一覧 ニーザー 細オブションの設定 22ボート	タがあります! 注 クルーナ ▼	・ザーまで 検索		K ‡+2/セル 通用 □グオン中: admin 注保存 ● ログオフ
etAttest eeps.local 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 RADUSサーバー	ユーザーID パスワード EPS	はSer 01 password 第幕されていない設定またはずー 2ザーー覧 -ザー 第オブションの設定 2スポート	夕が除り上す! 5全 グループ ♥	 () トップペー ユーザーまで 検索 ユー - ゴーまで (検索) 	-ジ) (D) 読む ゴ ザ - 削除時の	メK キャンセル 漁用 ログオン中: admin 官保存 ① ログオフ 自用書 ① ログオフ
etAttest aepslocal 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 コーザー	ユーザーID パスワード	user 01 password	タが取ります! 会か クルーナ ▼ 三 <u>ユーザーD</u>	 ・ トップペー ユーザーまで 依案 ユニー 最終認証の広功 	-ジ ・ジ ・ジ ・ が ー が い 、 、 、 、 、 、 、 、 、 、 、 、 、	メ キャンセル 通用 ログオン中: admin 定保存 ④ ログオフ 通加 加 ションク タスク
9tAttest 20ps.local 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 覧 エクスポート	ユーザーID パスワード	user 01 password 家存されていれい愛愛また日子ー ショーザーー覧 マーザー「覧 マーザー」 ションの設定 2スポート 名前 test user	タがあります! タがあります! E全 グルーナ ▼ <u>ユーザーID</u> test	 ① トップペー ユーザーまで 検索 ユー 最終認証成功 	ジ) ら 読 ゴリ時時の 記明書 発行	jx キャンセル 通用 口グオン中: admin 定保存 ① ログオフ 注保存 ① ログオフ 追加 追加 注明書失効オブション タスク 変更 剤除



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)

Net Attest EDG	パウカナヤ ブレンドレンジロナナ レナブ・レ			ログオン中: admin
NetAttest EPS)	PRIFCITUUPAGIEDEA/LIAJ :		()トップページ) () 数5	筐保存 📵 ログオフ
 næepslocal システム設定 システム管理 証明機関 DHCPサーバー 	<u> こーザー</u> 覧 ユーザー ご細オブションの設定 エクスポート	全 グループ 💙	ユーザーまで	
■ LDAPサーバー ■ RADIUSサーバー ■ ユーザー	■ 2前	7 – 11 – m	<u>ユーザー削除時の</u> 最終認証成功 _{美田日表}	<u>追加</u> 証明書失効オブション
■ ユーザー一覧 ■ エクフポート	tart upar	tart		亦更別段
■ インポート	user01	user01		変更 削陈 割除
		- mug		
		編集対象: user01 基本情報	V	
		姓	user01	
		名		
		E-Mail		
		言关制情報		0
		認時報		
		ユーザーID 有効明報 ● 日数 365 E ● 日付 2016 ¥ 4 記明書ファイルオプション パスワード	user01 7 V 月 9 V 日 23 V 時 59 V	分 <mark>59 ∨</mark> やまで
項目	値	バスワード(確認)		
	365	※パスワードが空間の場合には	、ユーザーのバスワードを回説します。	
证仍首行 为规议	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・・・ チェック有			発行 キャンセル
	👱 ユーザー証明 ユーザー証明書ダウンズ	書のダウンロード コードの準備ができました。対象	変ファイルに保存して下さい。	ダウンロード

3. Aruba 7005 の設定

3-1 Aruba 7005 設定の流れ

Aruba 社製無線 LAN コントローラーAruba 7005 は、WEBGUI または CLI を用いて設定が行え ます。本書ではより設定の分かりやすい WEBGUI を用いて各種設定を実施する方法を紹介します。 今回設定するのは以下の項目です。

- Contoroller の基本設定
 - IP アドレス、VLAN 等
- AP の基本設定
 - APGroup、認証方式等
- SSID の基本設定
 - SSID 設定、暗号強度設定
- Control Plane security
 - コントローラーAP 間の鍵交換
- AP プロビジョニングの設定
 - AP の IP アドレス指定・Radio 起動



Arubaの設定項目

3-1-1 Controller の基本設定

Controller 側の基本設定を Wizard にて行います。

[Configuration]タブをクリックします。[WIZARDS]メニューから、[Controller]をクリックします。 ウィザードが開始されるので[Basic Info]にて[Name]に Controller の名前を指定します。

[VLANs and IP Interface]にて Named VLANs の[All]選択し、Vlan を[1]、Port を[All]と指定しま す。その他は特に変更の必要はありません。



aruba ma	BILITY CONTROLLER Aruba7005				Log out admin	
Dashboard Monitoring	g Configuration Diagnostics Mainte	nance Save Configuration				
Configure Controller						
Workflow P H	Specify Basic Info Specify the name, timezon Name:	mation for this Control e, date/time, and passwords for t Aruba7005	er his controller. <u>More</u>			
	Password for user "Admin" Retype:	: 6-	32 characters			
VLANs and IP Inte	Dashboard Monitoring Configu	NTROLLER Aruba700	itenance Save Configuration 🍕			
4 Connectivity	Configure Controller					
	Workflow 🛛 Help					
5 Uplink	1 Basic Info Name: Aruba7005	Configure VLANs Configure VLANs for this	and IP Interfaces for Aru	ba7005		
		Named VLANs	All VLAN IDs on This Controller			
6 Ports	2 Licenses	All	ID IP Address/Netmask	IPv6 Address	Enable NAT Port Members	DHCP Settings
	License Installed: 3		1 192.168.1.1/255.255.255.0	-	all	None
7 Finish	3 VLANs and IP Interfaces					
		New Delete	Add Delete			
	Connectivity			R		
	5 Uplink					



最後に設定を確認して[Finish]をクリックします。

		ILITY CONTROL	LLER Arub	a7005				Log out admin
Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration 🧳			
Configure	WLAN							
Workflov	v 📀 i	lelp	Configura	tion of solit	on wlan in Group soliton i	s Complete		
APGroup SSID: s	v soliton oliton_wlan		The settings y	vou have specifie	d are ready to be pushed to the Cont	roller. <u>More</u>		
2 Forwar	rding Mode		Campus V	VLAN Wizard	Configuration Summary	14:54:53,Wed Mar 23 2016		
 3 Radio Radio Ty VLAN: 1 4 Internal Internal 5 Auther WPA-2 if 6 Captive Disabled 	& VLAN (pe: all al/Guest interprise e Portal	incryption	WLAN 1 1. WLAI APGroup: SSID: so 2. Forw Tunnel 3. Radii Sodin Tim Printable con To configur To comfigur	N soliton liton_wian arding Mode o & VLAN box still fig summary re another WLAN ie the Wizard and	(Created) Commands to be pushed click again. d apply the settings you have specifie	d, click the Finish button below		
7 Auther Radius: 8 Role A Pre-auth Post-aut	ntication Serve netattestST04 ssignment entication role: hentication role:	egon authentic					ţ,	
9 WLAN	Configured							Back Finish Cancel

3-1-2 APの基本設定

APの基本設定を Wizard にて行います。

[Configuration]タブをクリックし、[WIZERDS]メニューから[Campus WLAN]を クリックします。ウィザードが開始されるので、以下のように設定します。

ALUDA MOE	ILITY CONTROLLER Aruba7005		Log out admin
Dashboard Monitoring	Configuration Diagnostics Maintenance	Save Configuration 9	
WIZARDS	Network > Controller > System Settings		
AP Controller	System Settings Control Plane Security	Cluster Settings Licenses Centralized Licenses Sync whitelist service	
Caminus WLAN Remote AP	Controller Role Master IP Address	Master V	
AirWave	Authentication	IPSec Key Certificate	
> Controller VLANs	IPSec Key (IKE PSK) Retype IPSec Key (IKE PSK)		
Ports	Uplink		
Cellular Profile IP	Primary Uplink Secondary Uplink	Wired V None V	

arub	O MOB	ILITY CONTRO	LLER Arub	a7005				L
ashboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration 🧳			
onfigure W	VLAN							
Workflow	🛛 н	elp	Specify W	ireless LA	N (WLAN)			
			Specify the W	LAN to edit. <u>Mo</u>	<u>re</u>			
Forwardi	ing Mode		AP Groups default soliton	*	WLANs for soliton soliton_wlan	WLAN Usage		
Radio &	VLAN					R		
Internal/	/Guest		New	*	New Copy Delete	Share		
Authenti	ication and E	ncryption	Click the Nex	t button to edit	soliton_wlan			

項目	設定値
AP Group	soliton
WLANs for	soliton_wlan

arut		LITY CONTROL	LLER Arub	a7005	Log out admin
Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration 9
Configure	WLAN				
Workflow	🛛 He	lp	Specify F	orwarding N	Mode for soliton_wlan in Group soliton
APGroup: SSID: so	soliton liton_wlan		The Forwardin	ng Mode provide	es a range of options for forwarding traffic back to the controller through the IPsec tunnel. More
2 Forward	ding Mode		Forwarding M Decrypt-1 The AP d and send	ode: Funnel ecrypts and deca s the 802.3 fram	capsulates all 802.11 frames from the client mes to the controller through the GRE tunnel.
3 Radio 8	k VLAN		 Tunnel User traff 	fic is forwarded l	I back to the controller through the IPsec tunnel.
4 Interna	l/Guest		 Bridge User traft 	fic is locally rout	uted/switched (no traffic is sent through the IPsec tunnel).
5 Authen	tication and Er	cryption			

4.EAP-TLS 認証でのクライアント設定

ł	arub	O MOB	ILITY CONTRO	LLER Arub	a7005	Log out admin
Da	shboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration 🧳
Co	nfigure V	WLAN				
1	Workflow WLAN APGroup: SSID: soli	I H soliton	elp	Specify R Specify the ra VLAN specifie	a dio Type a adio type on whic d below by confi	nd VLAN for soliton_wlan in Group soliton this WLAN is available, as well as the VLAN in which users connecting to this WLAN are to be placed by default. Note: you can override the giring per-role VLANs in Step 8. <u>More</u>
2	2 Forwarding Mode Tunnel			Radio Type: Broadcast SS	All ▼ ID: Yes ▼	
3	Radio &	VLAN		VLAN:	1	
4	Internal	/Guest				
5	Authenti	ication and E	ncryption			

項目	設定値
Radio Type	All
Broadcast SSID	Yes
VLAN	1

ALLA	O MOB	ILITY CONTRO	LLER Arub	a7005	Log out admin
Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration 🦿
Configure V	WLAN				
Workflow	0 н	elp	Specify U	sage Scena	ario for soliton_wlan in Group soliton
2 Forward Tunnel 3 Radio & Radio Typ VLAN: 1	APGroup: soliton SSID: soliton_vlan 7 Forwarding Mode Tunnel 7 Radio & VLAN Radio Type: all VLAN: 1		Is this WLAN Internal	internal WLAN	is typically employ encryption and stronger layer 2 authentication. <u>More</u>
Internal Authent	/Guest	ncryption			

ATUDO MOBILITY CONTRO	LLER Aruba7005	Log out admin
Dashboard Monitoring Configuration	Diagnostics Maintenance Save Configuration 9	
Configure WLAN		
Workflow Help	Specify Authentication and Encryption for soliton_wlan in Group soliton	
APGroup: soliton SSID: soliton_wlan	The authentication and encryption options below are grouped by the level of security they guarantee. More	
2 Forwarding Mode Tunnel	More Secure	
3 Radio & VLAN Radio Type: all VLAN: 1	 Strong encryption with shared-key authentication. Weak encryption, with optional authentication. 	
4 Internal/Guest Internal	- Open - no authentication or encryption. Less Secure	
Authentication and Encryption Captive Portal	Authentication: WPA-2 Enterprise WPA Enterprise Encryption: aes,tkip	

項目	設定値
Encryption	aes,tkip



外部 Radius サーバを指定します。NetAttestEPS にて設定した値を登録します。

ただし、[Name]については任意の名前を使用できます。

Orubo MOBILITY CONTROL	LLER Aruba7005			Log out admin					
Dashboard Monitoring Configuration	Diagnostics Maintenance	Save Configuration							
Configure WLAN									
Workflow Help	Specify Authentication Server for soliton_wlan in Group soliton								
APGroup: soliton SSID: soliton_wlan	test deployments. More	An enterprise environment typically uses an external RADIUS server for authentication. The controller also has an internal database that can be used for small scale or test deployments. <u>Hore</u>							
2 Forwarding Mode Tunnel	Ordered list of Authentication servers:		項目	設定値					
3 Radio & VLAN Radio Type: all			Name	netattestST04					
VLAN: 1 4 Internal/Guest	 Select from known servers Specify new server 		IP address	192.168.1.2					
5 Authentication and Encryption	Server type: RADIUS Name: netattestST04 IP address: 192.168.1.2		Auth port	1812					
6 Captive Portal	Auth port: 1812 Acct port: 1813 Shared key: ••••••		Acct port	1813					
Disabled	Retype key: •••••• OK Cancel		Shared key	secret					
Authentication Server			Retype key	secret					

MOBILITY CONTROL	LLER Aruba7005	Log out admin
Dashboard Monitoring Configuration	Diagnostics Maintenance	Save Configuration 🧳
Configure WLAN		
Workflow Help WLAN APGroup: soliton SSID: soliton vian	Configure Role Assign After being authenticated, eac or assion server-derived roles	Inment for soliton_wlan in Group soliton ch client is assigned a role, which determines the resources to which the client will have access. You can assign the same role to all clients, based on attributes returned by the authentication server at authentication time. More
2 Forwarding Mode Tunnel	Default role: Server-derived roles:	authenticated •
3 Radio & VLAN Radio Type: all VLAN: 1	Show Roles & Policies	
4 Internal/Guest Internal		
5 Authentication and Encryption WPA-2 Enterprise		
6 Captive Portal Disabled		
7 Authentication Server Radius: netattestST04		
8 Role Assignment		

項目	設定値
Default role	authenticated
Server-derived roles	off

[9 WLAN Configured]にて設定に誤りが無いことを確認して[Finish]をクリックします。

その後の画面で[Close]をクリックしてウィザードを終了します。

3-1-3 SSID の設定

左のメニューから[WIRELESS]の中の、[AP Configuration]をクリックします。 [Wireless LAN]、[Virtual AP]、[soliton_wlan-vap_prof]の順に展開し、[SSID]をクリックします。 [SSID Profile >]の右側に[soliton_wlan-ssid_prof]が選択されていることを確認します。 [Network Name(SSID)]を記入し、[802.11 Security]の WPA2、AES にチェックを入れます。

	BILITY CONTROLLER Aruba7005		Log out adm
Dashboard Monitoring WIZARDS AP	Configuration Diagnostics Mainter Configuration > AP Group > Edit "sol	nance Save Confi	figuration 7
Controller Campus WI AN	Profiles		Profile Details
Remote AP WIP	Virtual AP		SSID Profile > soliton_wlan-ssid_prof Show Reference Save As Reset Racic Advanced
AirWave NETWORK	★ AAA	soliton_wlan- aaa_prof	Network
Controller VLANs	 802.11K Hotspot 2.0 	default	Network Name (SSID) SolitonLab
Ports Cellular Profile	E SSID	soliton_wlan- ssid_prof	Network Authentication
IP SECURITY	EDCA Parameters Station EDCA Parameters AP		Encryption AES
Authentication Access Control	High-throughput SSID	soliton_wlan- htssid_prof	Keys
AP Configuration	802.11r WMM Traffic Management		
MANAGEMENT General Administration Certificates SNMP	 ➡ RF Management ➡ AP ➡ QOS ➡ IDS ➡ Mesh 		
Logging Clock Guest Provisioning			
Captive Portal SMTP Bandwidth Calculator			

項目	設定値
Network Name	SolitonLab



3-1-4 Control Plane Securityの設定

Control PlaneSecurity の設定を行います。

[Configration]タブをクリックします。[NETWORK]メニューを展開し、[Controller]リンクをクリ ックします。[Control Plane Security]タブをクリックして[Disabled]にチェックを入れます。最後 に[Apply]をクリックします。

※デフォルトでは有効になっています。

		BILITY CONTRO	LLER Arı	ıba7005					<u>Log out admin</u>
Dashboard	Monitoring	Configuration	Diagnostics	Maintenance	Save Configuration	2			
WIZARDS	WIZARDS Network > Control Plane Security								
AP Controller		System Setting	s Control	Plane Security	Cluster Settings	Licenses	Centralized Licenses	Sync whitelist service	
Campus W	/LAN	Control Plane Sec	urity		Enabled Disable	d			
Remote AF	P	Auto Cert Provisio	oning						
WIP		Addresses Allowe	d for Auto Cert	:	All Opecified add	lress range			
AirWave NETWORK > Controlle VLANs	er.					•	Delete		Add
Ports		Number of AP Wh	nitelist Entries		1				
Cellular Pro IP	ofile								
SECURITY	ation								Apply
Access Cor	ntrol	Commands							<u>View Commands</u>
WIRELESS									

3-1-5 AP プロビジョニングの設定

AP のプロビジョニングを行います。

[Configration]タブをクリックします。[WIRELESS]メニューを展開し、[AP Installation]リンクを クリックするとコントローラーで確認できる AP が表示されます。対象の AP にチェックを入れて [Provision]をクリックします。

	SILITY CONTROLLER Aruba7005	Log out admin						
Dashboard Monitoring	Configuration Diagnostics Maintenance Save Configuration							
WIZARDS AP	Wireless > AP Installation > Provisioning							
Controller Campus WI AN	Search	Search						
Remote AP	■ AP Name ▲ AP Group ▲ AP IP ▲ AP Type ▲ AP MAC Address ▲ AP Serial Number ▲ F	Flags 🔺 🛛 Status 🔺						
WIP	✓ 84:d4:7e:c1:d3:e8 soliton 192.168.1.4 205 84:d4:7e:c1:d3:e8 CM0550895	Up 2h:22m:47s						
AirWave	1 1-1 of 1 10 v							
NETWORK Controller VLANs Ports Cellular Profile IP	Flags: U = Unprovisioned; N = Duplicate name; G = No such group; L = Unlicensed; I = Inactive; D = Dirty or no config; E = Regulatory Domain Mismatch; X = Maintenance Mode; P = PPPoE AP; B = Built-in AP; s = LACP striping; R = Remote AP; R- = Remote AP requires Auth; C = Cellular RAP;; c = CERT-based RAP; 1 = 802.1x authenticated AP; 2 = Using IKE version 2; u = Custom-Cert RAP; S = Standby-mode AP; J = USB cert at AP; M = Mesh node; Y = Mesh Recovery; ; Port information is available only on 6xx.; Provision							
SECURITY Authentication Access Control WIRELESS AP Configuration AP Installation								

[Provisioning]画面へ遷移します。[IP Setting]にて AP へ指定するアドレスを入力します。 最後に[Apply and Reboot]をクリックします。AP が自動的に再起動します。

	BILITY CONTROLLER Aruba7005			Log out admin
Dashboard Monitoring	Configuration Diagnostics Mainte	nance Save Configuration 🧳		
WIZARDS	Wireless > AP Installation > Provis	ion		
AP	Provisioning Provisioning Profile	Whitelist		
Campus WLAN	AP Parameters			
Remote AP	AP Group	soliton 🔻		
WIP AirWave	AP Installation Mode			
NETWORK	Default	O Indoor	Outdoor	
Controller VLANs	Antenna Parameters			
Ports Cellular Profile	Antenna Selection Internal/Included Antenna	🔘 External Antenna		
IP	Authentication Method			
SECURITY	Remote AP 🕐	🔍 Yes 🖲 No		
Authentication	Remote AP Authentication Method	Pre-shared Key Certificate		
WIDELECC	PKCS12 Passphrase			
AP Configuration	IKE PSK		Confirm IKE PSK	
> AP Installation	User credential assignment 📀			
RA CONTRACTOR CONTRACTOR CONTRACTOR	Use Automatic Generation			

Bandwidth Calculator	802.1x Paramet	ers using PEAP	_						
Threshold	User Name								
ADVANCED SERVICES Redundancy	Password				Confirm Passw	vord			
AirGroup	Master Discovery								
IP Mobility	O Use AP Discover	y Protocol							
Stateful Firewall	Master Controlle	er IP Address/DNS nam	e 🕐 🛙	192.168.1.1	TFTP Server	• (?)			
External Services	O Host Controller	Name 🕐	E		Master Cont	troller IP A <mark>d</mark> dress/D	NS name ?		
Wired Access	IP Settings								
All Profiles	Uplink Vlan		0						
E-mail Support	Obtain IP Address Using DHCP								
	• Use the following	g IP Address							
	IP Address		192.168	8.1.4	Subnet Mask		25	5.255.255.0	
	Gateway IP Ad	dress	192.168	8.1.1					
	DNS IP Addres	s			Domain Name	2			
	IPv6 Address/F	Prefix-length							
	Gateway IPv6	Address							
	DNS IPv6 Add	ress							
	Single Chain Mode								
	Enable for Radio-0				Enable for Rad	dio-1	٥		
	AP List								
	AP IP Address	AP Name		AP Group	SNMP System Location	Mes	h Role	AP Type	Serial Number
	192.168.1.4	84:d4:7e:c1:d3:e8		soliton		none		205	CM0550895

項目	設定値
IP Address	192.168.1.4
Subnet Mask	255.255.255.0
Gateway IP Address	192.168.1.1



4. EAP-TLS 認証でのクライアント設定

4-1 Windows 8.1 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。





● ☞ 証明書のインポート ウィザード	
秘密キーの保護 セキュリティを維持するために、秘密キーはバ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)	
インポート オプション(I):	
○ 秘密キーの保護を描力にする(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)	
キーのパックアッフィドランスパードとり設定します。	
70A (N) = +10° d70.	
④ ジ 証明書のインボート ウィザード	
standard an	
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)	
○ 証明書をすべて次のストアに配置する(P)	
証明書ストア:	
≥ m(N)…	
/だへ(N) キャンパフル	
🔹 🔶	
● ₩ 証明書のインボート ウイザード	
証明書のインボート ウィザードの完了	
[完了] をクリックすると、証明書がインポートされます。	
次の設定が送金されました・	
2000年に2月1日にといるいに、 選択された証明書ストア ウイザードで自動的に決定されます	
内容 PFX ファイル名 C:¥Users¥Soliton¥Downloads¥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



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。

※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。



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	
- このコンピューターの・・・	On
- 単純な証明書の選択を・・・	On
証明書を検証してサーバー・・・	On
信頼されたルート証明機関	TestCA

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

7005/AP-205 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(Nexus 7)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 5.1 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が、本書では無線 LAN 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



4-3-2 サプリカント設定

Seliton

7005/AP-205 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。



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 8.1 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(E): WPA2 - エンタープライズ ~ 助売ーかの種類(A)・ AFS ~	セキュリティの種類	WPA2-エンタープライズ
-81-310x/3500(x). Inc.	暗号化の種類	AES
ネットワークの認証方法の選択(O):	ネットワークの認証・・・	Microsoft:保護された EAP
Microsoft: 保護された EAP (PEAP) ✓ 認定(S)		
詳細設定(D) のK キャンセル	保護された E 接続のための認証方法: ・ 証明書を検証してサーバーの ID を称 次のサーバーに接続する (例: srv: 「価値されたルート証明機関(R): 「Microsoft Root Certificate Ar で TestCA し thawte Primary Root CA し Thawte Timestamping CA	EAP のプロパティ × 触証する(V) 1. srv2*¥.srv3¥.com)(O): uthority 2011 ^
¥ 詳細設定 ★ 1903 1X 050字 100 14 650☆	□ UTN-USEKHIRSC-Object □ VeriSign Class 3 Public Prima く 报続前の通知(T):	ary Certification Authority - G5
OUZ.IX の設定 802.II の設定 「認証モードを指定する(P):	サーバー名またはルート証明書が指定さ 認証方法を選択する(5): セキュリティで保護されたパスワード (EAP マ 高速再接続を有効にする(F) ストリーク アクセス保護を注制する(N サーバーに暗号化パインドの TLV がな ID プライバシーを有効にする(I)	thなかった場合にユーザーに通知します v -MSCHAP v2) v 構成(C) り い場合は切断する(D) OK キャンセル
 ✓ 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) このネットワーケでは、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) OK キャンセル 	EAF 接続のための認証 □ Windows (合はドメイン)	P MSCHAPv2 のプロパティ 方法: のDU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

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

7005/AP-205 で設定した SSID を設定し、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「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	2		@ 8	3% 🔳)	•••• au 4G	13:52	100%
く設定	Wi-Fi				"SolitonL	ab"のパス	マード	を入力			キャンセル	証明書	信頼
			++	ンセル	パ	スワート	ド入力			接続			
Wi-Fi			_							_	naep	s.local	
			<u></u>	ザ名	user	01					発行力	: 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	/01/26 13:46:29	
その他			Ŧ-	ĸ			-	-	白	動う	加美利田		>
				<i>d</i> .					H	342 7			
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 クを選択する必要があり	7が見つからない場合は)ます。	、手動でネットワー											
			a	we	e r	t	vi	1	i o	p			
			4	<u> </u>		Ľ.	, L			٣			
			a	S	d	g	h	j	k	1			
				z	x	v	b	n	m	\otimes			
			.?	123		spac	е		ret	urn			

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



5-3 Android(Nexus 7)のサプリカント設定

7005/AP-205 で設定した SSID を設定し、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。「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。

					78	11:22
÷	Wi-Fi				م	:
	ON					•
•	SolitonLab					
L_						
	/				1	17:15
÷	Wi-Fi				Q	
	SolitonLab					•
	EAP方式 PEAP			~		
	フェーズ2認証 MSCHAPV2			~		
▼ a	CA証明書			_		
	ID			Ť		
	user01					
	匿名ID					
	パスワード					
	·····					
	🗌 パスワードを表示する					
V 8	✔ 詳細設定項目					
▼ ≙	プロキシ			•		
	IP設定			_		
V à	DHCP			Ŧ		
V é			キャンセル	保存		
	4	0				

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	ログ表示例						
NetAttest EPS	naeps radiu RadiusClientC	sd[2540]: nc)1 port 0 cli C0	otice 2016/03/ 0335EDF2A23)	23 16:09:07	Login OK:	[user01]	(from client	
	Dashboard Monitoring NETWORK	LITY CONTROLLER Arul Configuration Diagnostics Network > All WLAN Cli	Maintenance 🦿				Log out admin	
Aruba7005	Network Summary All WLAN Controllers All Access Points All Mesh Nodes All Air Monitors All Routers All WLAN Clients CONTROLLER Controller Summary	Client Selection Phy Type User Name Role AP Name BSSID Query Operator	• • •	NAC 4 IP Add Auth ESSIC Curre Devic Num[]pr of results per page: 10	Address Gress Type nt Controller e Type Search Reset	T	Hide Search	
	Access Points Mesh Nodes Air Mohitors IP Routing IP Mobility IP Multicast Clients Els-telier cliente ログインユーサ	Global Clients(Complet User Name Device T user01	e results.) ype ▲ MAC Address ▲ Clien cb:33:5e:df:2e:22 192.16 AC アドレス、端	IP ▲ User Role ▲ AP Na 5.1.100 authenticated 84:d4:7e 1 1-1 of 1	me▲ Essid▲ Curren Letid3:e8 SolitonLab 192.188 10 ▼ 、認証タイプ等	t Controller▲ Auth T 11 802.1× 等を表示	<u>Hide Search</u> ype ▲ Roaming Status ▲ Wireless	

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	ログ表示例							
NotAttact EDC	naeps radius RadiusClient0	eps radiusd[6923]: notice 2016/03/23 17:09:09 Login OK: [user01] (from client							
Nelallest EPS	naeps radius RadiusClient0	naeps radiusd[6923]: notice 2016/03/23 17:09:09 Login OK: [user01] (from clien RadiusClient01 port 0 cli C0335EDF2A23)							
	Dashboard Monitoring	TY CONTROLLER Aruba Configuration Diagnostics Network > All WLAN Clie	17005 Maintenance 🦿				Lo	g out admin	
	Network Summary	ary Client Selection Hide Search							
	All WLAN Controllers	Phy Type		MAC	Address				
	All Access Points	User Name		IP Ac	dress				
	All Air Monitors	Role		Auth	Auth Type				
	All Routers	AP Name		ESSI	ESSID				
Aruba7005	All WLAN Clients	BSSID		Curre	nt Controller				
Aluba7005	CONTROLLER	Query Operator	•	Devid	е Туре				
	Controller Summary	ller Summary Num ar of results per page: 10 🔻 Search Reset							
	Access Points Mesh Nodes	Global Clients(Complete	results.)				ł	tide Search	
	Air Monitors IP Routing IP Mobility IP Multicast Clients Blacklich Cliente	User Name 🛆 🛛 Device Ty user01	pe ▲ MAC Address ▲ Client IF <u>c0:33:5e:df:2a:23</u> 192.168.1	User Role AP N 100 authenticated 84:d4:76 1 1-1 of 1	ame▲ Essid▲ Curre ::c1:d3:e8 SolitonLab <u>192.15</u> 10 ▼	nt Controller ▲ Auth T 8.1.1 802.1x	ype▲ Roamir Wireless	ng Status 🔺	
	ロクインユーサ	「名、端末の MA	Cアドレス、端末	の IP アドレフ	、、認証タイプ	等を表示			

改訂履歴

日付	版	改訂内容
2016/05/18	1.0	初版作成