



【連携機器】 ラッカスネットワークス ZoneDirector 1200 【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、ラッカスネットワークス社製無線 LAN コントローラーZoneDirector 1200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 ZoneDirector 1200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3
	1-1 構成図
	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.	ZoneDirector 1200の設定10
	3-1 ZoneDirector 1200 の初期化
	3-2 初期設定ウィザードの実行11
	3-2-1 Language 11
	3-2-2 一般
	3-2-3 IP 設定12
	3-2-4 ワイヤレス LAN13
	3-2-5 管理者13
	3-2-6 確認
	3-2-7 サービス条件 14
	3-2-8 終了15
	3-3 AAA 設定16
	3-4 WLAN 設定 17
	3-5 WLAN Groupと AP Group19
	3-6 AP セットアップ20
	3-7 アクセスポイント ポリシー23
	3-8 ディスカバリと AP グループアサイン24

4. EAP-TLS 認証でのクライアント設定26
4-1 Windows 10 での EAP-TLS 認証26
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28
4-2 iOS での EAP-TLS 認証 29
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
4-3 Android での EAP-TLS 認証 31
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 32
5. EAP-PEAP 認証でのクライアント設定33
5. EAP-PEAP 認証でのクライアント設定
5. EAP-PEAP 認証でのクライアント設定
<ol> <li>5. EAP-PEAP 認証でのクライアント設定</li></ol>
5. EAP-PEAP 認証でのクライアント設定       33         5-1 Windows 10 での EAP-PEAP 認証       33         5-1-1 Windows 10 のサプリカント設定       33         5-2 iOS での EAP-PEAP 認証       34         5-2-1 iOS のサプリカント設定       34
5. EAP-PEAP 認証でのクライアント設定       33         5-1 Windows 10 での EAP-PEAP 認証       33         5-1-1 Windows 10 のサプリカント設定       33         5-2 iOS での EAP-PEAP 認証       34         5-2-1 iOS のサプリカント設定       34         5-3 Android での EAP-PEAP 認証       35
5. EAP-PEAP 認証でのクライアント設定       33         5-1 Windows 10 での EAP-PEAP 認証       33         5-1-1 Windows 10 のサプリカント設定       33         5-2 iOS での EAP-PEAP 認証       34         5-2-1 iOS のサプリカント設定       34         5-3 Android での EAP-PEAP 認証       35         5-3-1 Android のサプリカント設定       35
5. EAP-PEAP 認証でのクライアント設定       33         5-1 Windows 10 での EAP-PEAP 認証       33         5-1-1 Windows 10 のサプリカント設定       33         5-2 iOS での EAP-PEAP 認証       34         5-2-1 iOS のサプリカント設定       34         5-3 Android での EAP-PEAP 認証       35         5-3-1 Android のサプリカント設定       35         6. 動作確認結果       36
5. EAP-PEAP 認証でのクライアント設定       33         5-1 Windows 10 での EAP-PEAP 認証       33         5-1-1 Windows 10 のサプリカント設定       33         5-2 iOS での EAP-PEAP 認証       34         5-2-1 iOS のサプリカント設定       34         5-3 Android での EAP-PEAP 認証       35         5-3-1 Android のサプリカント設定       35         6. 動作確認結果       36         6-1 EAP-TLS 認証       36

## **Seliton** 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



## **Seliton**®

## 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
ZoneDirector 1200	ラッカスネットワークス	RADIUS クライアント (無線 LAN コントローラー)	ver. 10.2.1.0 build 75
R510	ラッカスネットワークス	無線アクセスポイント	ver. 10.2.1.0 build 75
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 SmartPhone)	iOS 12.1.4
Pixel C	Google	802.1X クライアント (Client Tablet)	Android 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	
ZoneDirector 1200	192.168.1.1/24	UDF 1612	secret	
R510	192.168.1.11/24	-	-	
Client PC DHCP		-	-	
Client SmartPhone	DHCP	-	-	
Client Tablet	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

NetAttest EPS			
See Hindoria (a) 222 (a) 7-2 222 Artin (a) 222 Artin (a) 0 Artin	U-F ZAUNEZ IMMEZ ≥Z S		
ogygtt F 2004-2011, Solitor Systems K.K., Al rights travened			
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	りして下さい。		
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			
RADIUSプロキシ			
Windowsドメイン記憶力連携	<u>無</u> 30		
グループ	#KX0		
	#XX0 ## 2h		
	戻る 再起動		
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

CANDER			
CANDERIN	л−⊦са ∨		
CA REESR			
● 内部で新しい鍵を生成する			
公開施方式	RSA 🗸		
親兵	2048 🗸		
● 外部HSMデバイスの鍵を使	し用する		
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		
<b>部署名</b>			
E-mailアドレス			
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

## **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。

Net Attest EDC					ログオン	/中: adn
NetAttest EPS)			① トップへ	(-ジ) 🖸 🖁	定保存) 📵 🛛	ログオフ
■ naeps.example.com	📃 💄 ユーザー一覧					
■ システム設定 ■ システム管理	<b>ザ</b> −●	→部 ○ 完全 グループ 💙	ユーザーまで 検索			
■ 証明機関	詳細オブションの設定					
■ DHCPサーハー ■ LDAPサーバー	エクスポート					ie to
■ RADIUSサーバー			<u>_</u>	ーザー削除時(	し の証明書失効オ	ノロ //1 ブ /ヨン
	□ 名前	<u>ユーザーID</u>	最終認証成功日時	証明書	タスク	
■ <u>エーリーー頁</u> ■ エクスポート	test use	test		発行	変更 育	削余
■ インポート						
■ 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
		8				
			E			
		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				
		<u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	user01			
		E Mail				
		言关和《华帝昌			^	
		認正情報			$\sim$	
<b>酒日</b>	値	ユーザーID・	user01			
<b>7</b> , 1		パスワード	••••••			
姓	user01	バスワード(確認	••••••	<u>~</u>		
	user01		Ш.			
<u></u>	useroi					
パスワード	password			)К ++У	セル 道用	
			•	♥		
Net Attest EPS			Com		ログオン	·中: adı
			( (1 トップ^	・ージ ) (ロ 誘		ログオフ
■ naeps.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	詳細オプションの設定					
■ DHCPサーバー ■ LDAPサーバー	エクスボート					追加
■ RADIUSサーバー			<u>_</u>		の証明書失効オ	<u>通加</u> ブション
■ ユーザー ■ ユーザー・監	□	<u>ユーザー</u> ID	最終認証成功日時	証明書	タスク	
	test use	test		発行	変更	削除
■ エクスポート						-
■ エクスポート ■ インポート	user01	<u>user01</u>		発行	変更 前	削除
■ エクスボート ■ インボート ■ ユーザーバスワードボリシー ■ デフォルトフ <del>ーザーブロファイル</del>	user01	<u>user01</u>		発行	変更	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.p12 という名前で保存)

					ログオン中: admi
NetAttest EPS				<b>()</b> トッラベ	ージ 🕒 設定保存 😢 ログオフ
■ naeps.example.com	🙎 ユーザ・	─ <b>─</b> 覧			
■ システム設定 ■ システム管理	7-#-	<ul> <li>····································</li></ul>	<i>芍</i> ルーナ ▼	ユーザーまで 検索	
■ 証明機関	詳細オブションの設	定 。 。 。 。 。 。 。 。 。 。 。 。 。 、 、 、 、 、 、			
■ DHCPサーバー ■ LDAP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
■ エクスポート		test user	test		発行 変更 削除
■ インボート ■ ユーザーパラロー !!!!!!!		user01	<u>user01</u>		発行 変更 削除
■ エーリーハスリートホリシー ■ 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	userU1	
			fa F. Mail		
			≣¥¥ærinn freg		0
			認計報		
			ユーザーID	user01	
			● 日数 365		
			<ul> <li>● 日付 2016 ∨</li> <li>証明書ファイルオプション</li> </ul>	年 7 ~月 9 ~日 23、	✓ 時 <mark>59 ▼</mark> 分 <mark>59 ▼</mark> 秒まで
		1	パスワード		
頁目		値	バスワード(確認)		
正明書有効期限		365	※パスワードが空間の場合に		
	関の・・・	 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
		1			Ţ
		🧸 ユーザー証	1書のダウンロード		•
		ューザー証明書ダウン	コードの準備ができました。対 	象をファイルに保存して	Fat. ダウンロード



## 3. ZoneDirector 1200の設定

## 3-1 ZoneDirector 1200の初期化

工場出荷状態の ZoneDirector 1200 は、起動時に DHCP サーバーからアドレスを取得します。取 得できない場合には、IP アドレス 192.168.0.2/24 を自身に割り当てて起動します。必要な場合に は、本体起動後、正面 F/D ボタンを 5 秒以上押下して工場出荷時の設定に戻してください。



## 3-2 初期設定ウィザードの実行

設定 PC に適切な IP アドレス (192.168.0.100/24 等) を設定した後、Web ブラウザから接続 すると Setup Wizard が開始します。



#### 3-2-1 Language

Languageの選択を行います。デフォルトは英語ですが必要に応じて変更して下さい。本資料では「Japanese(日本語)」を選択し、「Next>」をクリックします。

Language							
General	Language						
IP setting	Welcome to the Ruckus Wireless ZoneDirector Setup Wizard. Use this wizard to prepare ZoneDirector to run your wireless network. To start, select						
Wireless LANs							
A designation to a	Language English						
Administrator	English						
Confirmation	Chinese Traditional(繁體中文)						
Service Terms	Chinese Simplified(简体中文)						
Finish	Dutch (Nederlands)						
	French (Français)						
	German (Deutsch)						
	Japanese (日本語)						
	Spanish (Español)						
	Swedish (Svenska)						
	Arabic (الْعَرَيْبَةِ)  Back Next >						



### 3-2-2 一般

システム名を入力し、国コード「Japan」を選択し、「次へ>」をクリックします。

言語	
一般	一般
IP 設定	ZoneDirector のシステム名を入力します。名を入力してください。名前には 1 ~ 32 の半角英数字を使用し、空白を入れないでください。
ワイヤレス LAN	システム名 * ruckus
管理者	IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
確認	ZoneDirector では、メッシュ機能を使用できます。ZoneDirector でメッシュを有効にするには、それぞれの ZoneDirector に、バックボーン トラ フィックのメッシュ WLAN に一意の名前 (SSID) を指定する必要があります。
サービス条件	メッシュを有効にする
終了	
	< 戻る <b>次へ &gt;</b>

### 3-2-3 IP 設定

ZoneDirector にアサインする IP 情報を入力し、「次へ>」をクリックします。

言語					
一般	IP 設定				
IP 設定	ネットワークのアドレス指定モードとして、[手動] または [DHCP] を選択します。[DHCP] を選択した場合は、追加の設定は必要ありません。[手 Ma を習知」を得合け、 ないまえ いったい つけぞうけがおう セーキネー(マスクリスク)の「がけいているスマン」にドけいですよう				
ワイヤレス LAN					
管理者					
確認	● 手動 ● DHCP IP アドレス *				
サービス条件	ネットマスク* 255.255.25.0				
終了	Gateway * <sup>192.168.1.254</sup> プライマリ DNS サーバー <sup>192.168.1.254</sup>				
	セカンダリ DNS サーバー				
	<戻る 次へ>				

項目	値
IPアドレス	192.168.1.11
ネットマスク	255.255.255.0
Gateway	192.168.1.254
プライマリ DNS サーバー	192.168.1.254



### 3-2-4 ワイヤレス LAN

ワイヤレス LAN の設定が可能ですが、セットアップウィザード終了後に追加することができるので、ここではチェックボックス内の√を外し、ワイヤレス LAN 設定を行なわず、「次へ>」をクリックします。

言語	
一般	ワイヤレス LAN
IP 設定	既定の設定を変更しない場合は、既定の WLAN である「ワイヤレス 1」がオープン認証で作成されます。WPA_PSK 認証を選択し、パスフレーズ を指定することで、セキュリティをセキュア WLAN に変更できます。また、一時的なゲストアクセス用に「ゲスト」WLAN を作成することもで
ワイヤレス LAN	きます。(後で、限定的な用途で、WLAN を追加できます。)
管理者	□ ワイヤレス 1 最初のワイヤレス LAN を作成します □ Guest WLAN 訪問者用の一時的なアクセス。
確認	
サービス条件	
終了	

### 3-2-5 管理者

ZoneDirector の管理者 (admin) のパスワードを変更し、「次へ>」をクリックします。

言語 一般	管理者
IP 設定	ー 管理者のユーザー名とパスワードを入力してください。このユーザー名を使用して、Web UI 管理アプリケーションに管理者としてアクセスする ことができます。 (新しいワイヤレス ネットワークをより詳細に構成するには、セットアップの完了後、この情報を使用して Web UI にログイン
ワイヤレス LAN	します。) 
管理者	管理者名 * admin
確認	
サービス条件	
終了	これらの機能を使用して、ここでネットワーク ユーザー アカウントを 1 つ作成することができます。(この処理は省略可能であり、後から Web UI を使用して必要なすべてのユーザー アカウントを作成することができます。) ユーザー アカウントの作成
	< 戻る <b>次へ &gt;</b>



### 3-2-6 確認

実施したセットアップウィザードの内容を確認し、「次へ>」をクリックします。

言語	
一般	价值言必
IP設定	次の設定を確認してください。変更する場合は、 [戻る] をクリックして、設定を編集します。この設定を使用する場合は、[完了] をクリックしま す。
ワイヤレス LAN	
管理者	ジステム名 ruckus IP 設定 192.168.1.11
確認	<b>ワイヤレス LAN</b> ワイヤレス LAN は作成されません
サービス条件	メッシュ メッシュ機能は無効になっています
終了	<ul> <li>管理者 アカウント (admin) が作成されます</li> <li>システム時刻は自動設定されています。</li> <li>(現在の PC 時刻は 2019/3/4 11:30:05 です)</li> </ul>
	* セットアップ ウィザードの完了後、Ruckus Wireless サポート Web サイトで最新のソフトウェア更新を確認してください。
	< 戻る <b>次へ &gt;</b>

### 3-2-7 サービス条件

「承認条件」のチェックボックスに√を入れて、「終了」をクリックします。

言語	
一般	サービス条件
IP 設定	ZoneDirector 製品は定期的にラッカスに接続され、ラッカスでは ZoneDirector のシリアル番号、ソフトウェア バージョン、ビルド番号を収集します、ラッカスはファイルを ZoneDirector
ワイヤレス LAN	に送信し、これは、ZoneDirector サポート契約の現在のステータスを表示するために使用され ます。 この情報は、データの保護基準が異なる外国に転送され、補完されることがありま
管理者	व.
確認	
サービス条件	
終了	
	✓ 承認条件
	<戻る <b>終了</b>



### 3-2-8 終了

Setup Wizard が終了し、IP アドレスが変更されます。ZoneDirector をネットワークに接続します。

言語	
一般	終了
IP 設定	Ruckus Wireless ZoneDirector がアクティブになりました。[注意] このセットアップ処理で管理 PC のネットワーク IP を変更した場合、PC をネットワークに再接続する前に IP アドレスをリヤットしてください。
ワイヤレス LAN	アのリングをクリック」。ア次の Zone Director に面接続します。https://192.168.1.11/
管理者	
確認	
サービス条件	
終了	

設定 PC の IP アドレスを変更しネットワークへ接続した後、画面の指示通りリンクをクリックして ZoneDirector へ接続し、先に設定した管理者パスワードでログインします。



ログイン後、ダッシュボード左下に記載されているバージョンを確認し、必要な場合にはアップ グレードを行ってください。





## 3-3 AAA 設定

802.1x 認証を行うために、NetAttest EPS (RADIUS サーバー)の登録を行います。

WebUI より、[Services & Profiles]-[AAA サーバー]を選択し、「認証/アカウントサーバー」セクションにて「新規作成」をクリックします。

認証/ア	認証/アカウント サーバー					
この表(	この表には、認証が必要なときに使用可能なすべての認証方法の一覧が表示されます。					
	名前	タイプ	操作			
新規	削除		⊜ 0-0 (0) ⊖			

新規作成画面にて、RADIUS サーバー名、認証方式、RADIUS サーバーの IP Address と共有シー クレットを入力し、「OK」をクリックします。

* Name	RADIUS		
Туре	<ul> <li>AD for Web Portal</li> <li>LI</li> <li>AD for 802.1x</li> </ul>	DAP <ul> <li>RADIUS  </li></ul> <li>RADIUS Accounting  </li> <li>TAGE</li>	CACS+
Encryptior	TLS		
Auth Method	• PAP 🔾 CHAP		
Backup RADIUS	; 📄 Enable Backup RADIUS	support	
* IP Address	192.168.1.2		
* Por	1812		
* Shared Secre		Ø	
* Confirm Secre		Ø	
Retry Policy			
* Request Timeou	it 3	項目	値
* Max Number of Retrie	<b>s</b> 2	Name	RADIUS
		Туре	RADIUS
		Auth Method	PAP
		IP Address	192.168.1.2
		Port	1812
		Shared Secret / Confirm Secret	secret

必要に応じて、同様の手順で RADIUS Accounting サーバーの設定を行います。



## 3-4 WLAN 設定

WLAN 設定では、「SolitonLab」という WPA2-EAP-AES の SSID を新規作成します。 WebUI より、Wireless LANs を選択し、「+作成」をクリックして WLAN の新規作成を行います。 各パラメータは以下を参考にして入力してください。

ダッシュボード	Wireless I AN	e				
アクセスポイント						
Wireless LANs	- システム	▲ 4 (FR) ● 46% 名前	ESSID	認証 暗号	化ステータス	(秋米. く 3 く 1) (秋米. クライアント数
カライマント教	WG Default	ZD-PSK	ZD-PSK	open wpa	2 Enabled	11 0
Troubleshooting						
Services & Profiles						
システム ト						
管理 🕨						
システム情報						1 件中 1-1 件を表示 🤍 1 🔉
General						-
		litani ah				
	Name: 30	lite-Leb				
	*ESSID: SO	nitonitad				
	Description:					
						•
MEAN OSuges						
	Туре: 💿	Standard Usage (For mo	ost regular wireless networ	(usages.)		
	$\bigcirc$	Guest Access (Guest ac	cess policies and access c	ontrol will be applied.)		
	0	Hotspot Service (WISPr	)			
	0	Hotspot 2.0		項目	値	1
	0	Autonomous		Concural		
				General		
				- Name	S	olitonLab
				- ESSID	S	olitonLab
				WLAN Usag	es	
				- Туре	St	tandard Usage



認証オプション		•
高速 BSS	方式:   オープン   802.1x EAP   MAC Address  802.1x EAP + MAC Address トランジション:  802.11r FT ローミングを有効にする (サポートのために、802.11k 近隣リスト レポートを有効にすることを推奨します。)	
暗号化オプション		•
	方式: ● WPA2 ○ WPA-Mixed ○ WEP-64 (40 ビット) ○ WEP-128 (104 ビット) ○ なし アルゴリズム: ● AES ○ 自動 (TKIP+AES) 802.11w MFP: ● 無効 ○ Optional ○ Required	
オプション		•
	認証サーパー: RADIUS ▼ 新規作成	

項目	値
認証オプション	
- 方式	802.1x EAP
暗号化オプション	
- 方式	WPA2
- アルゴリズム	AES
オプション	
- 認証サーバー	RADIUS



### 3-5 WLAN Group ≿ AP Group

先に作成した WLAN グループ (Default) を、AP グループに割り当てます。工場出荷時の設定では、Default の AP グループが準備されており、この例では Default のグループを利用します。但し、 チャネル化設定は 20MHz を設定します。

WebUIより、「アクセスポイント」を選択し、「+」をクリックして AP グループの新規作成を行います。各パラメータは以下を参考にして入力してください。



#### 無線設定

無線設定	無線 B/G/N (2.4GHz)	無線 A/N/AC (5.0GHz) 🔻
チャネル化:	✓ Override 20 ▼	✓ Override 20 ▼
チャンネル:	✓ Override Auto ▼	Override 屋内 Auto▼     Override 屋内 Auto▼
举后于九		
111/ac 00001:		auto Vernide Auto
WLAN グループ:	Override     WLAN Group 1	Override WLAN Group 1
コールアドミッション制御:	OFF V	OFF T
WLAN サービス:	Override Enable T	Override Enable T
Protection Mode:	Override RTS/CTS T	

項目	値
無線 2.4GHz/5.0GHz	
- チャネル化	Override, 20
- チャンネル	Override, Auto
- WLAN グループ	Override, WLAN Group 1

# **Seliton**

## 3-6 AP セットアップ

Ruckus AP が ZoneDirector 1200 を発見するには、以下の方法があり、一般的には「IP subnet broadcast」又は「AP Static Configuration」のいずれかが用いられることが多いです。

- IP subnet broadcast
- DHCP Option 43 sub-option 3
- DHCPv6 Option 17 sub-option 3
- DHCPv6 Option 52
- DNS entry named "zonedirector. <local domain>"
- AP Static Configuration

「IP subnet broadcast」は、Ruckus Standalone AP を ZoneDirector 1200 と同じセグメント に接続すると、セグメント内の ZoneDirector 1200 を自動的にディスカバリし、同じバージョンへ アップグレードされ、ZoneDirector 1200 の管理下となる方法です。 このドキュメントでは、「AP Static Configuration」の方法にて進めます。

Standalone AP の工場出荷時は管理 IP を DHCP で取得しますが、取得できなかった場合には自動的に IP アドレス 192.168.0.1/24 を自身に割当てて起動します。

設定を行う PC に適切な IP アドレスを設定 (例: 192.168.0.100/24) し、Web ブラウザから 192.168.0.1 へ接続します。ログインユーザーID/パスワードは下記の通りです。

- User Name: super
- Password: sp-admin



WebUIより、[Administration]-[Management]を選択し、コントローラーを指定します。各パラメー タは以下を参考にし、「Update Settings」をクリックしてください。

\_\_\_\_\_

Status	Administration :: Management							
Internet Local Subnets Radio 2.4G Radio 5G	Network Profile: Telnet Access? Telnet Port:	4bss Enabled  Disabled 23						
Configuration Device Internet Local Subnets	SSH Access? SSH Port:	Enabled      Disabled 22						
Radio 2.4G Radio 5G Ethernet Ports Hotspot	HTTP Access? HTTP Port:	Enabled Disabled						
Maintenance Upgrade	HTTPS Access? HTTPS Port:	Enabled Disabled						
Reboot / Reset Support Info	Certificate Verification	PASSED						
Administration	Controller Discovery Agent (LWAPP)?	Foshed     Dicabled						
Diagnostics Log	SmartCellGateway Agent? Cloud Discovery Agent (FQDN)	Enabled      Disabled     Enabled      Disabled						
	Set Controller Address (Reboot to take effect)	Enabled     Disabled						
	Primary Controller Addr:	192.168.1.1						
	Secondary Controller Addr:							
	TR069 / SNMP Management Choice							
	Auto (SNMP and TR069 will work together	.)						
	SNMP only							
	<ul> <li>None</li> </ul>							
	Update Settings Restore previous settings							

項目	値
Set Controller Address (Reboot to take effect)	Enabled
Primary Controller Address	192.168.1.1

AP の管理 IP Address を設定するには、WebUI より、[Configuration]-[Internet]を選択し、IP 情報 を指定します。設定後に「Update Settings」をクリックしてください。クリック後すぐに反映される ので、AP を AP セグメントに接続してください。

Status	Configuration :: In	ternet								
Internet Local Subnets Radio 2.4G Radio 5G	NTP Server:       ntp.ruckuswireless.com         Management VLAN:       1       ( Need to reboot for change to take effect )         IPv4 Connection Type:       DHCP       Static IP       PPPoE         Internet Connection Setting       Setting       PPPoE									
Configuration Device Internet Local Subnets Radio 2.4G Radio 5G Ethernet Ports Hotspot	Infiguration         vice         ernet         cal Subnets         dio 2.4G         dio 5G         hernet Ports         tspot         IPv4 DNS Mode :         Auto         Manual									
Maintenance Upgrade Reboot / Reset Support Info	IPv4 Primary DNS Server: 192.168.1.254 IPv4 Secondary DNS Server: 8.8.8.8									
Administration	IPv6 Connection Type:	項目	値							
Diagnostics	IPv6 Secondary DNS Server:	IPv4 Connection Type	Static IP							
		IPv4 Address	192.168.1.11							
	L2TP Connection L2TP Connection: O Enable	IPv4 Subnet Mask 255	255.255.255.0							
	Update Settings Restore pre	IPv4 Gateway	192.168.10.254							
	IPv4 DNS Mode Manual									
		IPv4 Primary DNS Server	192.168.1.254							
		IPv4 Secondary DNS Server	8.8.8.8							

なお、設定 PC から Standalone AP へ SSH 接続し、CLI にて設定することも可能です。

rkscli: set director ip 192.168.1.1 \*\* Please reboot for this change to take effect 0K rkscli: reboot 0K Rkscli:

AP の管理 IP Address を Static で指定するには、以下のコマンドで IP Address、Subnet Mask、 Gateway を設定します。

```
rkscli:
rkscli: set ipaddr wan 192.168.1.11 255.255.255.0 192.168.1.254
```



## 3-7 アクセスポイント ポリシー

ZoneDirector 1200 の WebUI より「アクセスポイント」を選択すると、画面下部に「アクセスポイントポリシー」タブがあります。ここでは、ZoneDirector への帰属に関するポリシーを設定することができます。

クセスポイントボリシー AP1	Configuration AP US8 イベンドアクティビティ
アクセス ポイント ポリシー	
来認	※ アクセスボイントからのすべての参加要求を自動的に承認する。(最大用のセキュリティを提保するには、このオブションをオフにしてください、その場合、新しく検出されたアクセスボイントをそれぞれ手動で許可する必要があります。)
限定 ZoneDirector 検出	🛃 次の ZoneDirector にのみ接続
	★ プライマリとセカンダリの ZoneDirector 設定をアクセス ポイントに構成する (IP アドレスまたはドメイン名を使用可能)
	プライマリ ZoneDirector アドレス: 192.168.1.1
	セカンダリ ZoneDirector アドレス
	個先されるプライマリ ZoneDirector
	アクセスポイントのプライマリおよびセカンダリの ZoneDirector 設定を保持する
<b>毀禮 VLAN</b>	※ アクセスポイントの設定を保持 ◎ VLAN ID
MTU をトンネル	1500 (ZoneDirector とアクセスボイントの層の最大送港ユニット サイズを次の範疇に制用するに(よ 850 = 1500)
自動リカバリ	GeneDirector から次の時間以上切断された状態が続くと、アクセスポイントは再起動します。 30 分。

承認: AP の自動承認の有効化/無効化(無効時は管理者による手動による承認が必要)
限定 ZoneDirector 検出:ディスカバー後の接続コントローラーの指定
管理 VLAN: AP の管理 VLAN の設定
MTU をトンネル: MTU サイズの調整 (VPN 接続環境下等)
自動リカバリ: ZoneDirector と切断された場合、再起動のタイミングを設定

項目	値
承認	アクセスポイントからのすべての参加要求を自動的に承認する
	次の ZoneDirector にのみ接続
限定 ZoneDirector 検出	プライマリとセカンダリの ZoneDirector 設定をアクセスポイントに
	構成する
- プライマリ ZoneDirector アドレス	192.168.1.1
管理 VLAN	アクセスポイントの設定を保持
MTU をトンネル	1500
白動しっパリ	ZoneDirector から次の時間以上切断された状態が続くと、アクセスポ
	イントは再起動します: 30分



## 3-8 ディスカバリと AP グループアサイン

AP が ZoneDirector 1200 をディスカバリすると、ZoneDirector 1200 と同じバージョンへアッ プグレードされ、自動的に ZoneDirector の管理下となります。

(前章のアクセスポイント ポリシー設定の「承認」が「自動承認」の場合)

WebUI より「アクセスポイント」を選択すると、ディスカバリの状態が確認できます。

以下は、AP が ZoneDirector に帰属し、ファームウェアのアップグレードを実施後、AP グループは 「System Default」へ割り当てられています。

アクセスポイント					View	Mode: List <b>グループ</b> マップ メッシュ
+ / C × C <	✔ 構成 🍵 削除				検索	e Q 🗸 🕹
- System 1	MAC アドレス	デバイス名	機種	ステータス	メッシュ モード	IP Address
AG System Default 1	ec:8c:a2:16:36:80		r510	ファームウェアをアップグレード中	Auto	192.168.10.11
アクセスポイント					View	Mode: List <b>グループ</b> マップ メッシュ
+ / C × 2 <	✔ 構成				検	R: Q 2 4 0
- System 1	MAC アドレス	デバイス名	機種	ステータス	メッシュ モード	IP Address
AG System Default 1	ec:8c:a2:16:36:80	RuckusAP	r510	接続済み	Disabled	192.168.10.11

「AP Group 1」を選択し、「ℕ(編集)」をクリックします。

<b>アクセスポイント</b> View Mode: List <b>グループ</b> マップ メッシ								בלעא
+ / C × 2 <	✔構成 前除				検索:		۹ ۵	* •
System 1	MAC アドレス	デバイス名	機種	ステータス	メッシュ モード	IP Address		
AG System Default 1	No data available.							



下段の「Available アクセスポイント:」からアサインする AP を選択し、「Add to this group」をクリ

#### ックしてグループに入れます。

Group Settin	roup Settings				
	AP Members: Move to			検索:	۵ ک
	メンバー	デバイス名	説明	機種	承認済み
	No data available.				
				0 件中 0-0 件を表	示 <b>《 1 》</b>
	Available アクセス ポ Add to this group	イント:		検索:	۵ و
	MAC アドレス	デバイス名	説明	機種	承認済み
	ec:8c:a2:16:36:80	RuckusAP		r510	はい

グループに入れると以下のように「AP Members:」に登録されるので、「OK」をクリックして設定 を終了します。

Group Settings					
	AP Members: Move to	System Default 🔻		検索:	۹ و
	メンバー	デバイス名	説明	機種	承認済み
	ec:8c:a2:16:36:80	RuckusAP		r510	(まし)
				1 件中 1-1 件を表	示 <b>《 1 》</b>
	Available アクセス ポ Add to this group	オント・		検索:	۹ و
	MAC アドレス	デバイス名	説明	機種	承認済み
	No data available.				

## 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。





## **S**oliton

### 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

ZoneDirector 1200 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

ZoneDirector 1200 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。

★ Wifi (0)          0N       ●         N       ●         * SolitonLab       ●         EAP方式       TLS         TLS       *         CA証明書       ●         TestCA       *         ドメイン       ●         Juer01       *         ID       □         User01       *         詳細設定       *         エナマンセル           近       ●			
N       ●         ●       Submuk       ●         SolitonLab       ●       ●         EAP5元、 TLS       ●       ●         CA証明書       ●       ●         TestCA       ●       ●         F×イン       ●       ●         コーザー証明書       ●       ●         User01       ●       ●         評細設定       ●       ●         Exervtu        ●         近       ●       ●         正       ●       ●         User01       ●       ●         近       ●       ●       ●         近       ●       ●       ●         近       ●       ●       ●         日       ●       ●       ●         回       ●       ●       ●         ●       ●       ●       ●       ●         ●       ●       ●       ●       ●         ●       ●       ●       ●       ●         ●       ●       ●       ●       ●         ●       ●       ●       ●       ●         ●       ●       ●	← Wi-Fi		0
Exited Soliton Lab Foliton Lab Fund CAE明書 TestCA For CA For	ON		۰
SolitonLab         EAP方式         TLS       ・         CA証明書         TestCA       ・         ドメイン         ユーザー証明書         user01       ・         財棚設定       ・         詳細設定       ・	SolitonLab		â
SolitonLab         EAP方式         TLS       ・         CA証明書         TestCA       ・         ドメイン         コーザー証明書         user01       ・         ID         user01       ・         JTmage       ・			-
EAP方式         TLS       ・         CA証明書       ・         TestCA       ・         ドメイン       ・         ユーザー証明書       ・         user01       ・         ID       ・         IB       ・         IB       ・         ID       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・         I       ・	SolitonLab		
TLS       ・         CA証明書       ・         TestCA       ・         ドメイン       ・         ユーザー証明書       ・         user01       ・         D       ・         ID       ・         調定       ・         詳細設定       ・         チャンセル       接続	EAP方式		
CA証明書 TestCA ・ ドメイン ユーザー証明書 user01 ・ U user01 ・ 新細設定 ・	TLS	-	
TestCA       ▼         ドメイン       □         ユーザー証明書       ■         user01       ▼         ID       ■         user01       ▼         詳細設定       ✓	CA証明書		
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	TestCA	-	
ユーザー証明書 user01 ・ user01 詳細設定 ・ キャンセル 接続	ドメイン		
ユーザー証明書 user01			
user01 ・ ID user01 詳細設定 ・ キャンセル 接続	ユーザー証明書		
ID user01 詳細設定 ~ キャンセル 接続	user01	•	
<u>user01</u> 詳細設定 ・ キャンセル 接続	D		
詳細設定 キャンセル 接続	user01		
キャンセル 接続	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



## 5-1 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バティ × 接続 セキュリティ	項目		値	
	セキュリティ	の種類	WPA2-エンタ	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 × 誇号作の種類(N): AES ×	暗号化の種類	Į.	AES	
an a state free de 21.	ネットワーク	の認証・・・	Microsoft: f	呆護された EAP
アットワークの認認証方法の選択(O):       設定(S)         Microsoft: 保護された EAP (PEAP)       設定(S)         ・       ・          ・       ・	 ネットワーク	(保護)         「銀桃のための認証方法:         「山明書を検証してサーバー         「次のサーバーに接続する         「広のサーバーに接続する         「個にrosoft Root Cert         「日本地社を Primary Root         「日本の社を Primary Root         「日本の社を Primary Root         「日本の社を Primary Root         「日本の社会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会会	Microsoft: 分 Lithた EAP のプロパティ の ID を検証する(V) (例: srv1, srv2, *¥.srv3¥.4 R): ificate Authority 2011 bt CA ing CA 3C ect blic Primary Certification Al 書が指定されなかった場合にユー -F (EAP-MSCHAP v2) :) 歯削する(N) TLV がない場合は切断する(D) 5(1) OK EAP MSCHAPv2 のプロ	R護された EAP
			vs のロクオン名とバスリート (ま (ン) を自動的に使う(A) OK キャン	このトメインのある場
ОК зеуни.	項目			値
	接続のための	認証方法		

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

## **So**liton

### 5-2 iOS での EAP-PEAP 認証

5-2-1 iOS のサプリカント設定

ZoneDirector 1200 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	"SolitonLab"のパスワードを入力 キャンセル パスワード入力 接続	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 🔒 🗢 (j)	パスワード・・・・・・・	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。		
	qwertyuiop	
	asdfghjkl	
	☆ z x c v b 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

ZoneDirector 1200 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		â
SolitonLab		
EAP方式		
PEAP	-	
フェーズ2認証		
MSCHAPV2	-	
CA証明書		
TestCA	*	
10.4.45		
FX12		
ID		
useron		
匿名ID		
バスワード		
□ パスワードを表示する		
	~	
	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

## Seliton 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 14 cli 80-A5-89-53-B4-0F)
ZoneDirector 1200	WebUI より、Clients > Wireless Clients を選択し、「Active Client」を確認します。 下図をご参照ください。

## 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 14 cli 80-A5-89-53-B4-0F via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 14 cli 80-A5-89-53-B4-0F)
ZoneDirector 1200 WebUI より、Clients > Wireless Clients を選択し、「Active Client」を確認します。 下図をご参照ください。	

Dashboard	Wireless Clier	nts					
Access Points	This table lists all [1] currently conn connect to your network, click Block	ected and [2] disconnected clie k. To troubleshoot a problematic	nt devices. Only those connec connection, click Delete. (TF	ted devices with a status of "authoriz nat client can then reconnect to the W	ed" are permitted access t LAN.)	o the network. To prevent an "unautho	rized" client from attemptin
Wireless LANs	To show a list of blocked clients, cli Active Clients Inactive Clients	All Events/Activities					
Clients 🔻						Search	Q C 0
Wireless Clients	MAC Address +	O S/Type	Host Name	User/IP	Role	Access Point	WLAN
	80:a5:89:53:b4:0f	Android		user01/192.168.1.100		ec.8c.a2.16.63:00	SolitonLab
Generated PSK	General Charts					1-1 of 1 st	nown e <b>1</b> a
Generated Guest Passes							
Applications	Info						•
	MAC Address	80:a5:89:53:b4:0f					
Troubleshooting	OS Type	Android					
Services & Profiles 🔹 🕨	Username	user01					

#### 改訂履歴

日付	版	改訂内容
2019/03/28	1.0	初版作成
1		