

NetAttest EPS

認証連携設定例

【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
	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 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.....	3
1-2 環境.....	4
1-2-1 機器.....	4
1-2-2 認証方式.....	4
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.....	10
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.....	12
3-2-3 IP 設定.....	12
3-2-4 ワイヤレス LAN.....	13
3-2-5 管理者.....	13
3-2-6 確認.....	14
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 Group.....	19
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

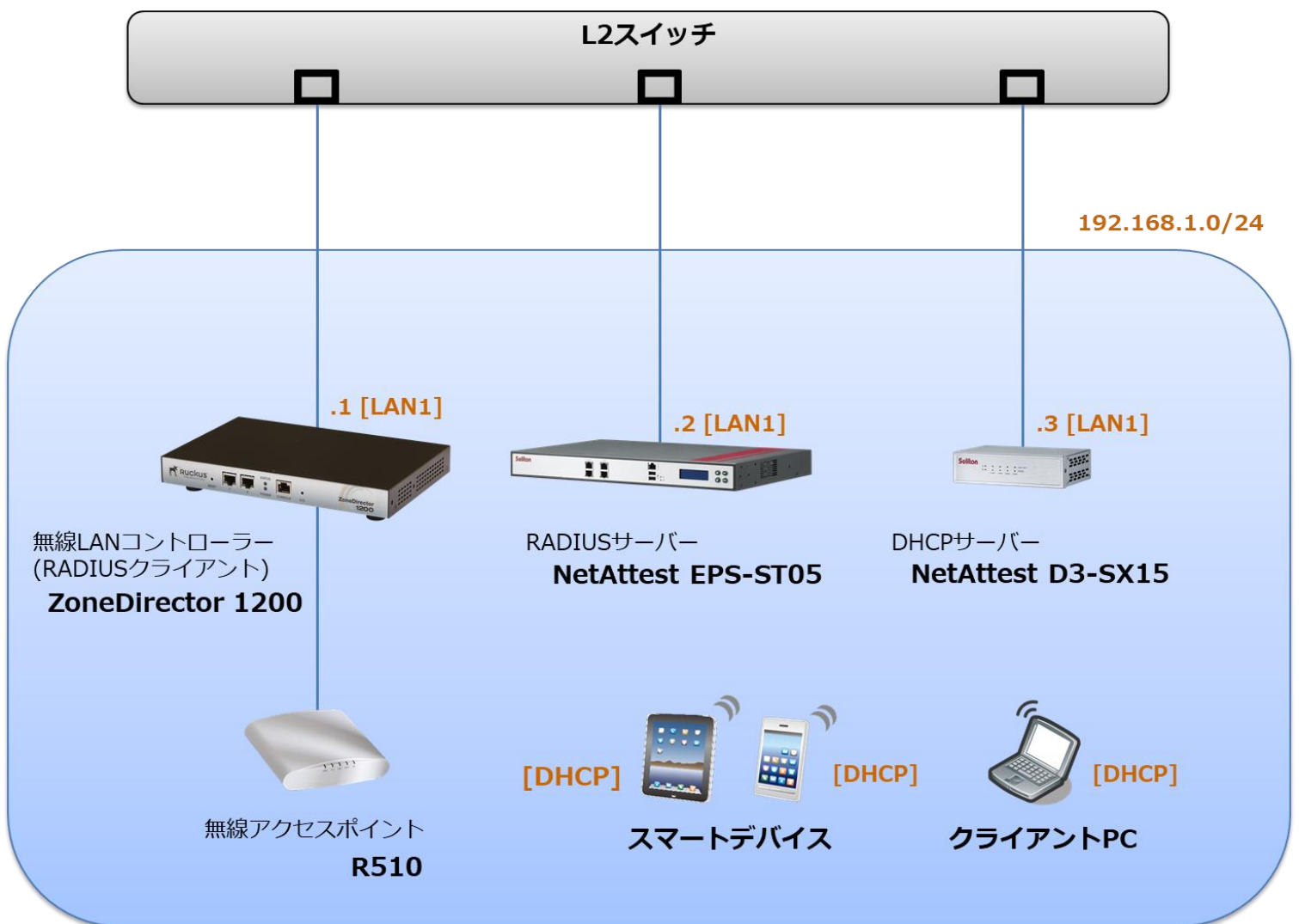
4. EAP-TLS 認証でのクライアント設定	26
4-1 Windows 10 での EAP-TLS 認証	26
4-1-1 クライアント証明書のインポート	26
4-1-2 サプリカント設定	28
4-2 iOS での EAP-TLS 認証	29
4-2-1 クライアント証明書のインポート	29
4-2-2 サプリカント設定	30
4-3 Android での EAP-TLS 認証	31
4-3-1 クライアント証明書のインポート	31
4-3-2 サプリカント設定	32
5. EAP-PEAP 認証でのクライアント設定	33
5-1 Windows 10 での EAP-PEAP 認証	33
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
6-2 EAP-PEAP 認証	36

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



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 標準サブリカント
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	UDP 1812	secret
ZoneDirector 1200	192.168.1.1/24		secret
R510	192.168.1.11/24	-	-
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。

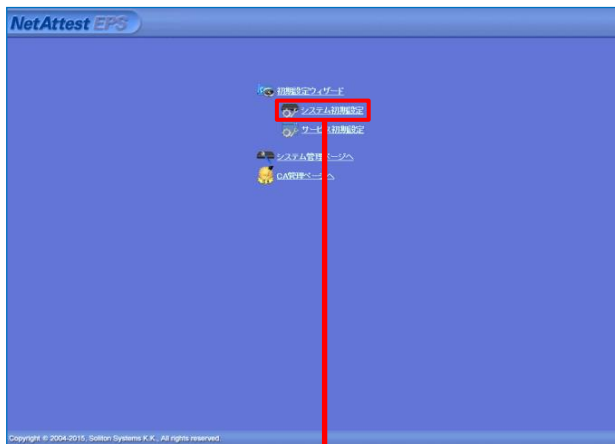
下記のような流れでセットアップを行います。

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



初期設定ウィザード - 設定項目の確認

設定内容を確認して下さい。
この設定を保存・反映するには「再起動」ボタンをクリックして下さい。

ネットワーク時刻	
NTPサーバー1	
NTPサーバー2	
NTPサーバー3	
時刻同期する	無効

EPSライセンス	
最大ユーザー数	200
最大NAS/RADIUSクライアント数	20
外部サーバー証明書	無効
RADIUSプロキシ	無効
Windowsドメイン認証連携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効

Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

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

2-3 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

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。

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test		発行	変更 削除

項目	値
姓	user01
ユーザーID	user01
パスワード	password

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test		発行	変更 削除
user01	user01		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]-[ユーザー一覧]から、該当するユーザーのクライアント証明書を発行します。(クライアント証明書は、user01.p12 という名前で保存)

項目	値
証明書有効期限	365
PKCS#12 ファイルに証明機関の・・・	チェック有

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	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 the display language that you want to use on the Web interface.
Wireless LANs	Language <input type="text" value="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 (الْعَرَبِيَّة)
	<input type="button" value=" < Back"/> <input type="button" value=" 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 * <input type="text" value="ruckus"/>
管理者	国コード <input type="text" value="Japan"/>
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	<input type="checkbox"/> メッシュを有効にする
終了	

< 戻る 次へ >

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。[手動] を選択した場合は、該当する IP アドレス指定情報を入力します。(アスタリスク (*) が付いているフィールドは必須です。)
ワイヤレス LAN	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> IPv4 と IPv6
管理者	<input checked="" type="radio"/> 手動 <input type="radio"/> DHCP
確認	IP アドレス * <input type="text" value="192.168.1.11"/>
サービス条件	ネットマスク * <input type="text" value="255.255.255.0"/>
終了	Gateway * <input type="text" value="192.168.1.254"/>
	プライマリ DNS サーバー <input type="text" value="192.168.1.254"/>
	セカンダリ DNS サーバー <input type="text"/>

< 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 設定を行わず、「次へ>」をクリックします。

言語	<h2>ワイヤレス LAN</h2> <p>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きます。（後で、限定的な用途で、WLAN を追加できます。）</p> <p><input type="checkbox"/> ワイヤレス 1 -- 最初のワイヤレス LAN を作成します</p> <p><input type="checkbox"/> Guest WLAN -- 訪問者用の一時的なアクセス。</p>
一般	
IP 設定	
ワイヤレス LAN	
管理者	
確認	
サービス条件	
終了	
< 戻る 次へ >	

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	<h2>管理者</h2> <p>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 にログインします。）</p> <p>管理者名 * <input type="text" value="admin"/></p> <p>パスワード * <input type="password" value="*****"/></p> <p>パスワードの確認 * <input type="password" value="*****"/></p> <p>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。）</p> <p><input type="checkbox"/> ユーザー アカウントの作成</p>
一般	
IP 設定	
ワイヤレス LAN	
管理者	
確認	
サービス条件	
終了	
< 戻る 次へ >	

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	確認
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	システム名 ruckus IP 設定 192.168.1.11
確認	ワイヤレス LAN 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	管理者 アカウント (admin) が作成されます システム時刻 システム時刻は自動設定されています。 (現在の PC 時刻は 2019/3/4 11:30:05 です)
	*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。
	<input type="button" value="戻る"/> <input type="button" value="次へ>"/>

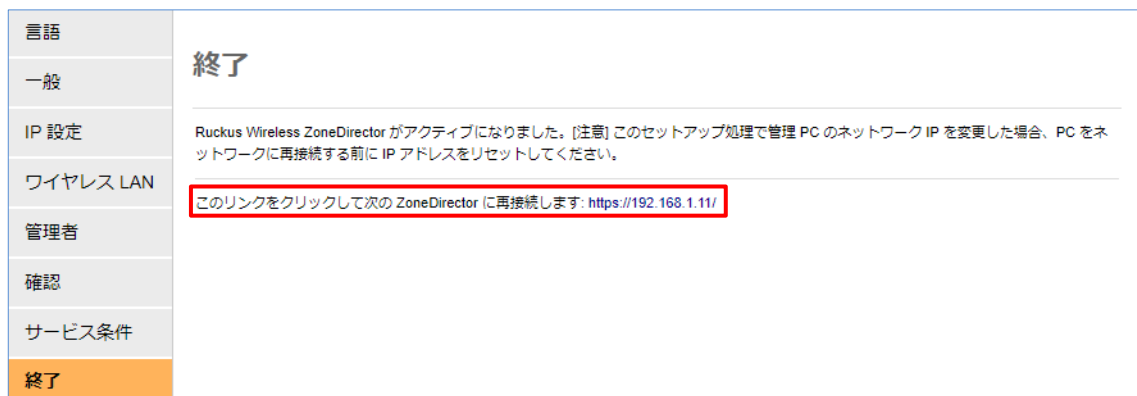
3-2-7 サービス条件

「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ク스에接続され、ラック스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。ラック스는ファイルを ZoneDirector 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、補充されることがあります。
ワイヤレス LAN	
管理者	
確認	
サービス条件	<input checked="" type="checkbox"/> 承認条件
終了	
	<input type="button" value="戻る"/> <input type="button" value="終了"/>

3-2-8 終了

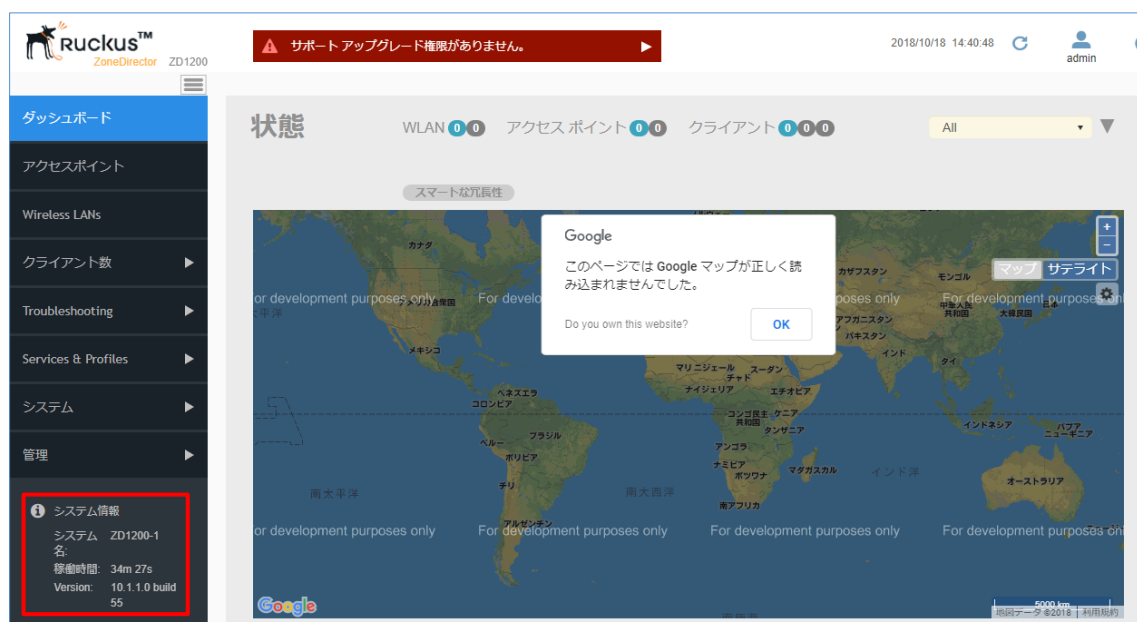
Setup Wizard が終了し、IP アドレスが変更されます。ZoneDirector をネットワークに接続します。



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/アカウントサーバー

この表には、認証が必要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。

<input type="checkbox"/>	名前	タイプ	操作
<input type="button" value="新規作成"/>			<input type="button" value="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
 Type AD for Web Portal LDAP RADIUS RADIUS Accounting TACACS+
 AD for 802.1x
 Encryption TLS
 Auth Method PAP CHAP
 Backup RADIUS Enable Backup RADIUS support
 * IP Address
 * Port
 * Shared Secret
 * Confirm Secret

Retry Policy

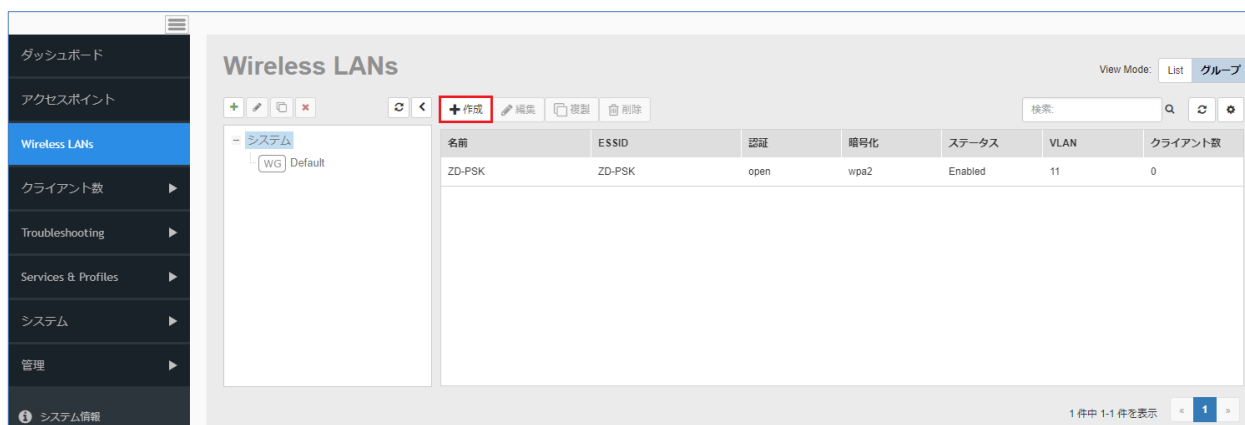
* Request Timeout
 * Max Number of Retries

項目	値
Name	RADIUS
Type	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。



General

Name: SolitonLab

ESSID: SolitonLab

Description:

WLAN Usages

Type: Standard Usage (For most regular wireless network usages.)

Guest Access (Guest access policies and access control will be applied.)

Hotspot Service (WISPr)

Hotspot 2.0

Autonomous

項目	値
General	
- Name	SolitonLab
- ESSID	SolitonLab
WLAN Usages	
- Type	Standard Usage

認証オプション

方式: オープン 802.1x EAP MAC Address 802.1x EAP + MAC Address

高速 BSS 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

認証サーバー:

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 と 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、チャンネル化設定は 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)
チャンネル化:	<input checked="" type="checkbox"/> Override 20	<input checked="" type="checkbox"/> Override 20
チャンネル:	<input checked="" type="checkbox"/> Override Auto	<input checked="" type="checkbox"/> Override 屋内 Auto <input checked="" type="checkbox"/> Override 屋外 Auto
送信電力:	<input type="checkbox"/> Override Auto	<input type="checkbox"/> Override Auto
11n/ac のみのモード:	<input type="checkbox"/> Override Auto	<input type="checkbox"/> Override Auto
WLAN グループ:	<input checked="" type="checkbox"/> Override WLAN Group 1	<input checked="" type="checkbox"/> Override WLAN Group 1
コールドミッション制御:	<input type="checkbox"/> Override OFF	<input type="checkbox"/> Override OFF
WLAN サービス:	<input type="checkbox"/> Override Enable	<input type="checkbox"/> Override Enable
Protection Mode:	<input type="checkbox"/> Override RTS/CTS	

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

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

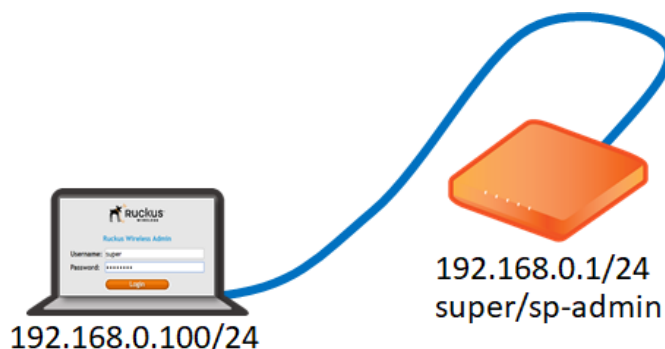
「IP subnet broadcast」は、Ruckus Standalone AP を ZoneDirector 1200 と同じセグメントに接続すると、セグメント内の ZoneDirector 1200 を自動的にディスカバリし、同じバージョンへアップグレードされ、ZoneDirector 1200 の管理下となる方法です。

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 を自身に割り当てて起動します。

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。

The screenshot shows the 'Administration :: Management' page with the following settings:

- Network Profile: 4bss
- Telnet Access?: Enabled Disabled
- Telnet Port: 23
- SSH Access?: Enabled Disabled
- SSH Port: 22
- HTTP Access?: Enabled Disabled
- HTTP Port: 80
- HTTPS Access?: Enabled Disabled
- HTTPS Port: 443
- Certificate Verification: PASSED
- Controller Discovery Agent (LWAPP)? Enabled Disabled
- SmartCellGateway Agent? Enabled Disabled
- Cloud Discovery Agent (FQDN) Enabled Disabled
- Set Controller Address (Reboot to take effect) Enabled Disabled
- Primary Controller Addr: 192.168.1.1
- Secondary Controller Addr: (empty)
- TR069 / SNMP Management Choice:
 - Auto (SNMP and TR069 will work together.)
 - SNMP only
 - FlexMaster only
 - None

Buttons: 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。

項目	値
IPv4 Connection Type	Static IP
IPv4 Address	192.168.1.11
IPv4 Subnet Mask	255.255.255.0
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
OK
rkscli: reboot
OK
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。

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
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
- 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
自動リカバリ	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

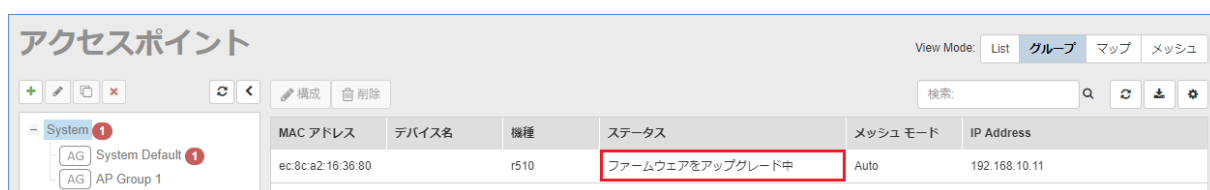
3-8 ディスカバリと AP グループアサイン

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。

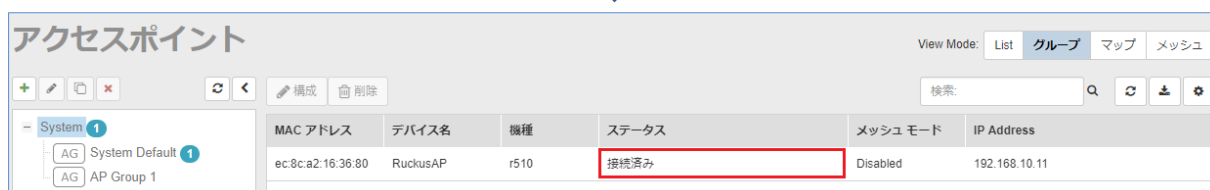


アクセスポイント

View Mode: List **グループ** マップ メッシュ

検索: [検索] [リフレッシュ] [ダウンロード] [設定]

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
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 **グループ** マップ メッシュ

検索: [検索] [リフレッシュ] [ダウンロード] [設定]

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
ec:8c:a2:16:36:80	RuckusAP	r510	接続済み	Disabled	192.168.10.11

「AP Group 1」を選択し、「 (編集)」をクリックします。



アクセスポイント

View Mode: List **グループ** マップ メッシュ

検索: [検索] [リフレッシュ] [ダウンロード] [設定]

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
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 Settings

AP Members:

Move to 検索:

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 < 1 >

Available アクセスポイント:

Add to this group 検索:

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

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	はい

1 件中 1-1 件を表示 < 1 >

Available アクセスポイント:

Add to this group 検索:

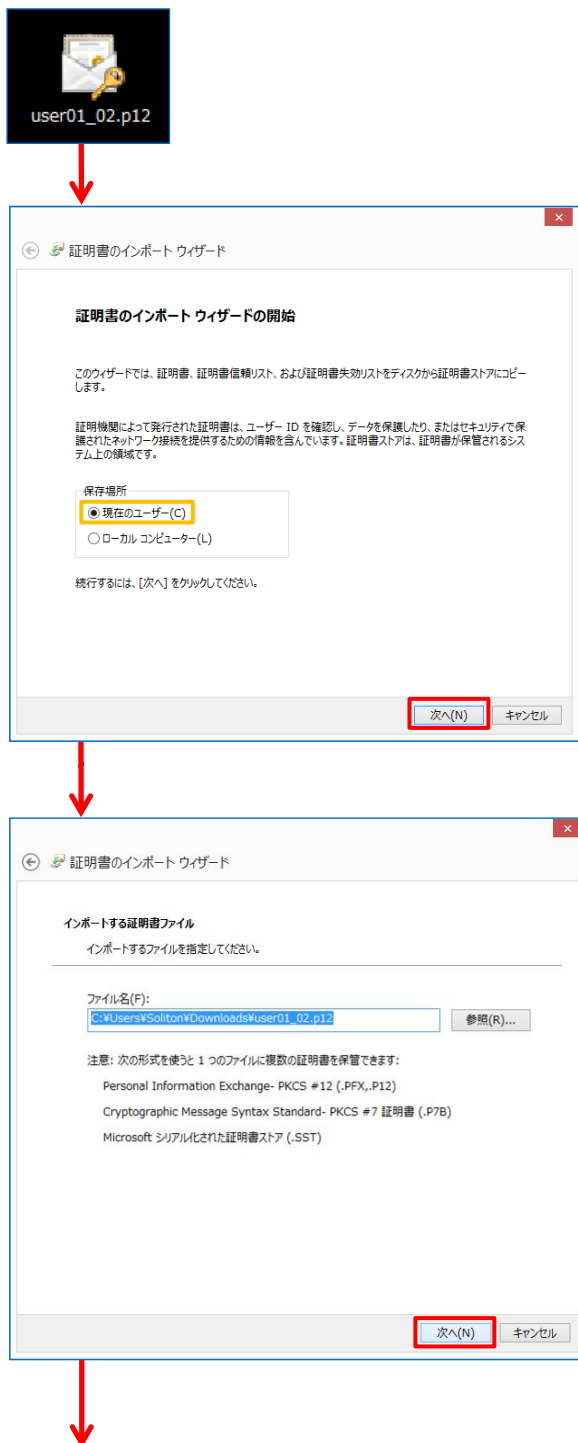
MAC アドレス	デバイス名	説明	機種	承認済み
No data available.				

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。



証明書インポート 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、秘密キーはパ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(O):

秘密キーの保護を強化にする(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)
キーのバックアップやトランスポートを可能にします。

すべての拡張プロパティを含める(A)

次へ(N) キャンセル

【パスワード】

「2-4 ユーザーの登録」で設定したパスワードを入力

証明書インポート ウィザード

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:
参照(R)...

次へ(N) キャンセル

証明書インポート ウィザード

証明書のインポート 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。

次の設定が指定されました:

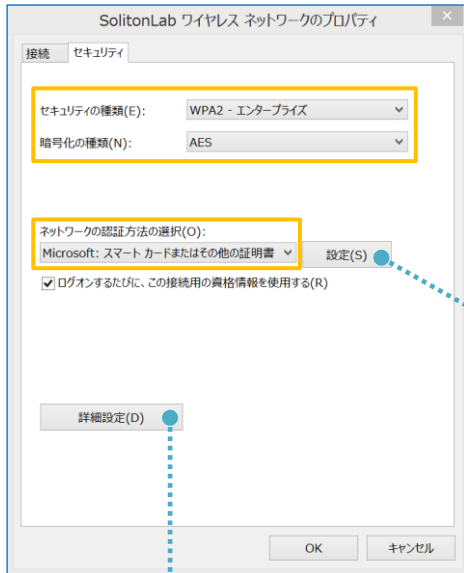
選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\Soliton\Downloads\User01_02.p12

完了(F) キャンセル

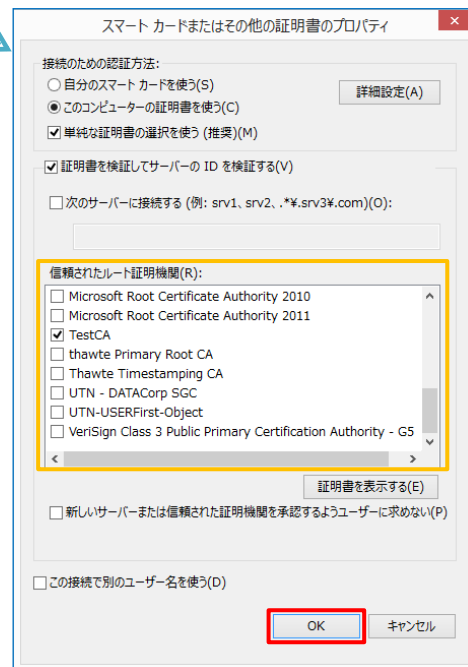
4-1-2 サプリカント設定

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。



項目	値
セキュリティの種類	WPA2-エンタープライズ
暗号化の種類	AES
ネットワークの認証・・・	Microsoft: スマートカード・・・



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証明書を・・・	On
- 単純な証明書の選択を使う (推奨)	On
証明書を検証してサーバーの ID を・・・	On
信頼されたルート証明機関	TestCA

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)

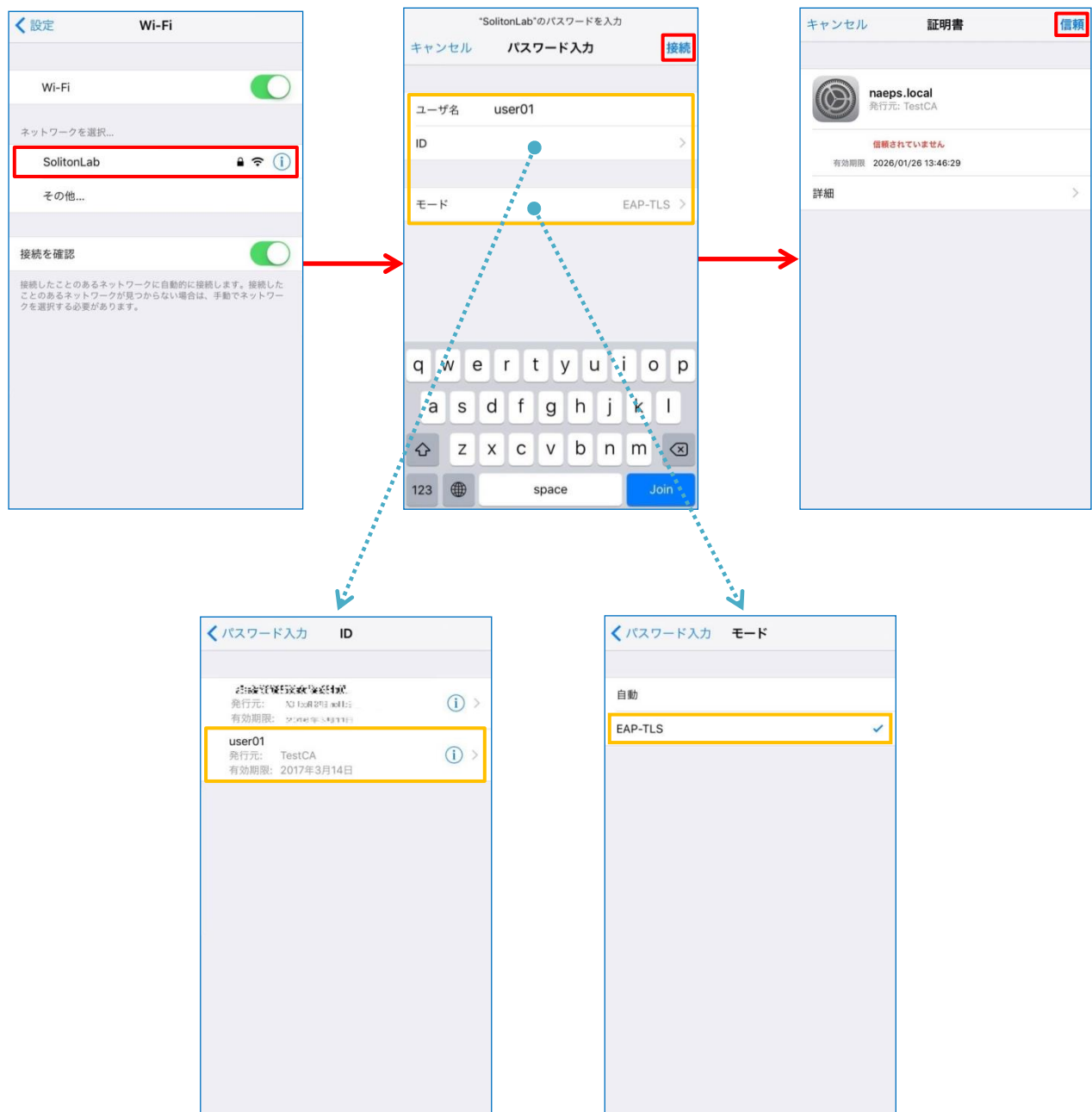
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

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、メーカーにより、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

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

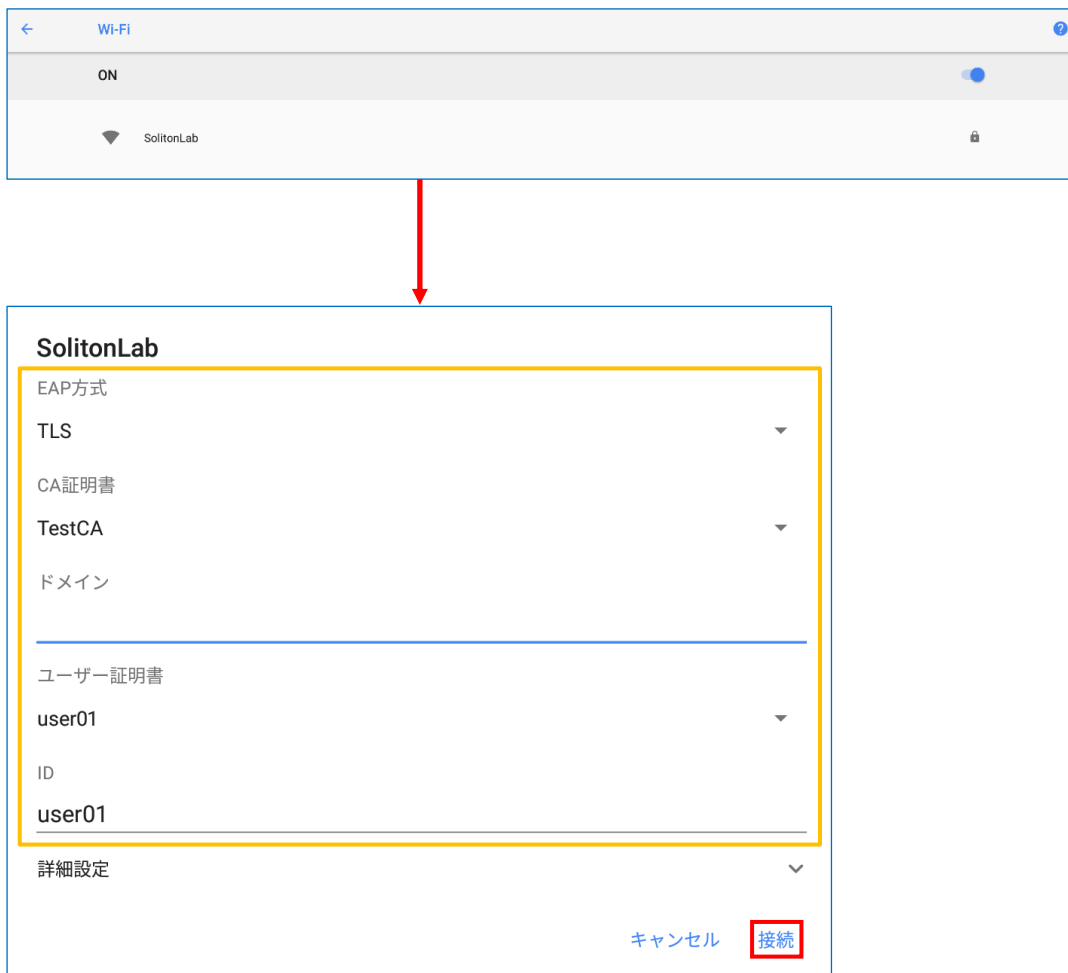
パッケージの内容:
ユーザーキー1個
ユーザー証明書1件
CA証明書1件

キャンセル

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。



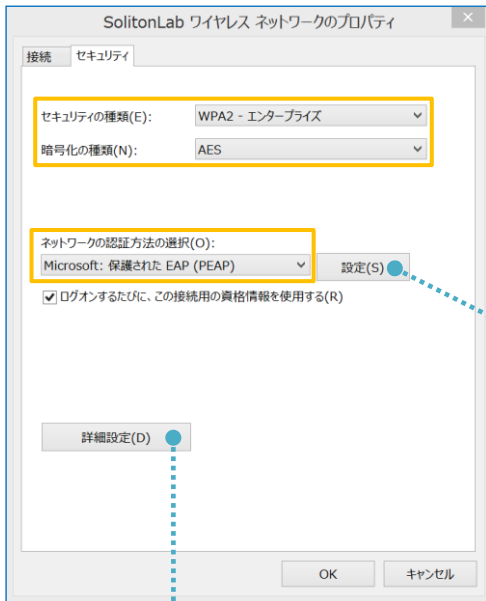
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

5. EAP-PEAP 認証でのクライアント設定

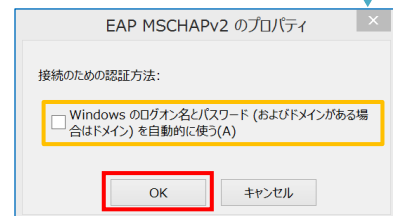
5-1 Windows 10 での EAP-PEAP 認証

5-1-1 Windows 10 のサブクライアント設定

[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。



項目	値
セキュリティの種類	WPA2-エンタープライズ
暗号化の種類	AES
ネットワークの認証・・・	Microsoft: 保護された EAP



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 のサブクライアント設定

ZoneDirector 1200 で設定した SSID を選択し、サブクライア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。



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 のサブリカント設定

ZoneDirector 1200 で設定した SSID を選択し、サブ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。

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
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。

Wireless Clients

This table lists all [1] currently connected and [2] disconnected client devices. Only those connected devices with a status of "authorized" are permitted access to the network. To prevent an "unauthorized" client from attempting to connect to your network, click Block. To troubleshoot a problematic connection, click Delete. (That client can then reconnect to the WLAN.)
To show a list of blocked clients, click [here](#)

Active Clients **Inactive Clients** All Events/Activities

Search

MAC Address	OS/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

1-1 of 1 shown

General Charts

Info

MAC Address	80 a5 89 53 b4 0f
OS Type	Android
Host Name	
Username	user01

