



【連携機器】Riverbed Xirrus XD2-240 【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、Riverbed 社製無線アクセスポイン ト Xirrus XD2-240 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 Xirrus XD2-240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>Seliton</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
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. Xirrus XD2-240 の設定
3-1 ノロノアイルの作成14
3-2 無線の設定15
3-3 External RADIUS サーバーの設定16
4. EAP-TLS 認証でのクライアント設定18
4-1 Windows 10 での EAP-TLS 認証18
4-1-1 クライアント証明書のインポート18
4-1-2 サプリカント設定
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
4-2-2 サプリカント設定22
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
4-3-2 サプリカント設定24
5. EAP-PEAP 認証でのクライアント設定
5-1 Windows 10 での EAP-PEAP 認証
5-1-1 Windows 10 のサプリカント設定

<u>Seliton</u>

	5-2 iOS での EAP-PEAP 認証	26
	5-2-1 iOS のサプリカント設定	26
	5-3 Android での EAP-PEAP 認証	27
	5-3-1 Android のサプリカント設定	27
6.	動作確認結果	.28
	6-1 EAP-TLS 認証	28
	6-2 EAP-PEAP 認証	28



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



<u>Seliton</u>

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
Xirrus XD2-240	Riverbed	RADIUS クライアント (無線アクセスポイント)	AOS 8.4
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)	11.3.1
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.15

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
Xirrus XD2-240	192.168.1.1/24	001 1012	secret
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	
्राह्मस्य २ ⁹ २०२७ २ २७२४ इ स्रि	4 7-± 12-109002 12-125 12-125 12-125
Copyright & 2004/2015. (Boltor Systems K.K., All right) reserved.	
加期設守立って、「シンプロ日の確認	
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?	かて下さい。
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
FPS=/////	
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ドメイン認識し重携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効
	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

Seliton

2. NetAttest EPS の設定

2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定(全般)
- RADIUS サーバーの基本設定(EAP)
- RADIUS サーバーの基本設定(証明書検証)
- NAS/RADIUS クライアント設定

CA種別選択		
CATERING	"и−нса м	
CANER		
● 内部で新しい鍵を生成する		
公開鞭方式	RSA 🛩	
網長	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	
国名	日本 🗸	
都道府県名	Tokyo	
市区町村名	Shinjuku	
会社名(組織名)	Soliton Systems	
部署名		
E-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



	Radiuschenton	
CONAS/RADIUS/954774	を有効にする	
4711-13 947	● NAS/RADIUSクライアント ● NAS/Dみ ● RADIUSクライアントのみ	
1989))	0	
IP7FL-ス*	192.168.1.1	
シークレット*		
所属するNASグループ	✓	
	Ro x	^

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。

let Attest EDC						Ц2	J.77.
ICTATION LID					トップページ) 🕒	設定保存)(🔁 ログ:
naeps.example.com ■ システム設定	ユーザー	→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>オブションの設</u> 定 エクスポート	定					
∃ LDAPサーバー	<u>+ 2 A 20 11</u>						追り
■ RADIUSサーバー = ユニザニ					<u>ユーザー削除</u> 時	時の証明書失:	劾オブ
■ ユーザー一覧		名前	<u>ユーザー</u> ID	最終認証成功	日時 証明書	\$7	2ク
■ エクスポート		test user	test		発行	変更	削
■ 1 ノホート ■ 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4	()L						
ゲスト							
			📃 🔔 ユーザー設定				
			編集対象: 新 #	規			
			ユーザー情報				
			姓	user01			
			名				
			名 E-Mail				
			名 E-Mail 詳細情報			0	
_			名 E-Mail 詳細情報 読証情報 ユーザーID*	user01		0	
∃	値		名 E-Mail 詳細情報 読計情報 ユーザーD [*] バスワード	user01		0	
目	值 user01		名 E-Mail 詳細情報 <u>読評情報</u> ユーザー D・ パスワード(確認)	user01	•••		
E	值 user01		名 E-Mail 詳細情報 認証情報 ユーザーD・ パスワード パスワード(確認 ■ 一時利用件)	user01	••• •	0	
目 ーザーID	値 user01 user01		名 E.Mail 詳細情報 読証情報 ユーザーID・ パスワード パスワード パスワード(確認 ■ 一時利用件)	user01	•••• ••••	0	
目 ーザーID スワード	値 user01 user01 password		名 E-Mail 詳細情報 ユーザーD・ パスワード パスワード(確認) ■ 一時利用停」	user01	0K ‡≠	С. С. С. 221 () ж	ăЯ
目 ーザーID スワード	値 user01 user01 password		名 E-Mail 詳細情報 ごけ情報 ユーザーD・ バスワード・ パスワード(確認 ■ 一時利用作」	user01	••• ••• •• •• •• •• •• •• •• •• ••	Stern 1	۵ 用
目 ーザーID スワード	値 user01 user01 password		名 E-Mail 詳細情報 二・ザーD・ パスワード パスワード(確認 ■ 一時利用件」	user01		слея ж	ă.Ħ
目 ーザーID スワード	値 user01 user01 password		名 E-Mail 詳細情報 ユーザーD・ パスワード パスワード(確認) ■ 一時利用停止	user01	ок + т) 2011 - January 2011	〕 〕 〕
目 ーザーID スワード let Attest FPS	値 user01 user01 password		名 E-Mail 詳細情報 ユーザーD・ パスワード パスワード パスワード(確認 ■ 一時利用件)	user01	ок + т	Слен П	加用
ヨ ーザーID スワード letAttest EPS	値 user01 user01 password		名 E-Mail 詳細情報 ユーザーD・ パスワード パスワード(確認 - 一時利用件)	L seril L seril L	ок ‡т	ی تورید (ایسی) تورید (ایسی)	M用 オン中 も ログ
目 ーザーID スワード	値 user01 user01 password	覧	名 E-Mail 詳細情報 ユーザーD パスワード パスワード(確認 ■ 一時利用停)	Luser01	••• ••• ••• ••• ••• ••• ••• •••	ンセル 第 記 記 定保存) (■用 「オン中 ② 日グ
目 ザーID スワード //etAttest EPS reepsexample.com : システム設定 : システム管理	値 user01 user01 password		 名 E.Mail 詳細情報 二・ザ・□・ パスワード パスワード パスワード(確認) ■ 一時利用停」 	user01 	··· •·· • •·· •	ンセル 記定保存 ()	M用 オン中 後 ログ
目 -ザーID スワード	値 user01 user01 password	覧 定	 名 E.Mail 詳細情報 読証情報 ユーザーD・ パスワード パスワード パスワード(確認) ■ 一時利用停」 	user01 	 ОК ≠т ↓ уј~-ў) а	シセル 設定保存) (第 用 〕 オン中 3 ○ 口 3
目 -ザーID スワード	値 user01 user01 password		 名 E.M.al 詳細情報 二·丁·□□ パスワード パスワード パスワード(確認) ■ 一時利用停」 	user01 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	ок +т	ことセル ↓ 1000 2010日 3010日 3010日<	第 周
目 -ザーID スワード	値 user01 user01 password	覧 定	 名 E.Mail 詳細情報 二·ザーロ・ パスワード パスワード パスワード(確認) ■ 一時利用停止 	user01	・・・ ・・・ ・・・ ・・・ ・・・ ・・・ ・・・ ・・・	ンセル ゴグ 設定保存) (50証明書失:	■用 「オン中 で 」 は 3 3 3 3 3 3 3 3 3 3 3 3 3
目 -ザーID スワード Vet Attest EPS i システム設定 : システム設定 : システム管理 : 副明機関 : DHDPサーバー : IDAPサーバー : IDAPサーバー : IDAPサーバー : スーザー	値 user01 user01 password	覧 定 名 前	 2ザーID 2ザーID 	useの1 いいのの に し し し し し し し し し し し し し し し し の の の し し の	・・・ ・・・ ・・・ ・・・ ・・・ ・・・ ・・・ ・・・	ンセル 第 設定保存 第 の証明書失: タフ	■用 オン中 ② ログ 道 効オブ・ スク
 ・ザーID スワード ・グーID スワード ・クワード ・システム管理 ・システム管理 ・システム管理 ・辺研機関 ・DtPサーバー ・IDAPサーバー ・コーザー ・ゴー覧 ・エクスボート 	値 user01 user01 password	→覧 定 名前 test user	そ E-Mail 詳細情報 E-THW ユーザーID 生生	User01 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	 シセル ログ 読定保存 ((すの証明書失: タブ 変更 	オン中 道 ジ ログ ジ レク



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)

Not Attact EDC					ログオン中: admin
NetAllest EFS	-			(1トップへ	ニージ 🕒 設定保存 🔞 ログオフ
■ naeps.example.com	-ב 🔔	ザ──覧			
■ システム設定 ■ システム管理	7-11-	● →部 ● 完全	<i>ち</i> ルーナ	ーザーまで 検索	
■ 証明機関	ユー ジ 詳細オプション0		- у у <u>-</u>		
■ DHCPサーバー	エクスポート				
■ LDAPサーハー ■ RADIUSサーバー					
= <u>ユーザー</u>		名前	ユーザーID	 最終認証成功日時	
■ ユーザー→覧		test user	test		発行 変更 削除
■ エンスホート ■ インポート		user()1	user01		一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
■ ユーザーバスワードポリシー			<u></u>		
■ デフォルトユーザープロファイル ■ ゲフト					
- 7 A					
					•
			編集対象: user01		
			基本情報	10000	
			<u>姓</u>	usero i	
			E-Mail		
			言祥細情報		0
			認計報		
			ユーザーID	user01	
			有効期限	-	
			● 日付 2016 ♥ 4	■ 7 ✔月9 ✔日 23	✔ 時 <mark>59 ✔</mark> 分 <mark>59 ✔</mark> 秒 まで
			証明書ファイルオブション		
西日		<i>1</i> 5	パスワード		_
現日			パスワード(確認)		
証明書有効期限		365	※パスワードが空間の場合に1	1、ユーザーのパスワードを使用	
 PKCS#12 ファイルに証明	機関の・・	 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 キャンクル
		🚨 ユーザー証明	詰 のダウンロ <u>ード</u>		•
		ユーザー証明書ダウンロ	コードの準備ができました。対象 	ーー 家をファイルに保存して	Fさい。 ダウンロード

Seliton

3. Xirrus XD2-240の設定

Xirrus XD2-240 は、AC アダプタの PoE 対応スイッチにケーブルで接続すると起動します。本資料では Xirrus XD2-240 の XMS-Cloud による設定を記載します。

デフォルトでは DHCP で IP アドレスが取得されるようになっているため、別途設置された DHCP サーバーから払い出された IP アドレスに対して、Firefox でアクセスします。Xirrus が DHCP で受 け取った IP アドレスは、XMS-Cloud か DHCP サーバー側で確認する必要があります。

セットアップは下記の流れで行います。

- 1. プロファイルの作成
- 2. 無線の設定
- 3. External RADIUS サーバーの設定



3-1 プロファイルの作成

始めにプロファイルを作成します。トップページより[PROFILES]-[+ NEW PROFILE]を選択し、 設定します。プロファイルの Locale の Country、Time Zone は日本の物を選択してください。

riverbed Xirrus	MY NETWORK PROFILES - EASYPASS	▼ REPORTS ▼	
My Network	Profile for Netattest created by Shin Kusanagi Profile for NetattestCloud View All Profiles + NEW PROFILE		
Dashboard 3 High 0 Medium 1 Low 0 24 Hours 0 Tota	iients 4 Ghz Ghz Ø24 Hours 0 2 Total Ø24 Hours	Devices Applicati	ons 3 High 0 Medium 1 Low Ø24 Hours
Dashboard Restore D	vfaults Usage y Do ▼ ☰ ▼ C	ients (over Time)	🚍 👻 Top Clients (by Usage) Total Usage 💌 🚍 👻
New Profile	×		
Profile Name *: EPS Cloud Description:			
Show Advanced	CREATE NEW PROFILE	項目 Profile Name	值 EPS Cloud(任意)
EPS Cloud 🔹 💿	•	s 🕫 🔒	Configuration* Access Points Clients
General ③ Show Advanced Give your profile a name and descriptio Profile Name: Description:		US Network Pailcles I	Songour Director Admin
Locale Country:	• Japan •	項目	値
Time Zone:	(GMT + 09:00) Osaka, Sapporo, Tok 🔻	Locale	lanan
		- Time Zone	(GMT + 09:00) Osaka, Sapporo, Tokyo



3-2 無線の設定

[SSIDs]タブに移動し、[+NEW SSID]より SSID を追加します。

'S CIOUA 🔍 🕲											Configuration Access Points
			G eneral	SSIDa	Network	Policies	CO Bonjour Director	Admin			SAVE CONFIGURA
SIDs @											Show Advanced
w Advanced t or view an existing SSID, assign SSID?	s, and create new SSIDs here.										
											+ NEV
SSID Name	Band	VLAN			Encryption/Auth	entication		Enabled	Bro	idcast	Access Control
SSID Name Soliton Lab	Band 2.4GHz & 5GHz	VLAN			Encryption/Auth WPA2/802.1x	entication		Enabled Yes	Bro- Yes	ədcəst	Access Control None

項目	値
SSID Name	SolitonLab(任意)
Band	2.4GHz & 5GHz
Encryption/Authentication	WPA2/802.1x
Enabled	Yes
Broadcast	Yes
Access Control	None



3-3 External RADIUS サーバーの設定

追加した SSID に暗号化と認証の設定を行います。

created by J Smith										Cutumber Anna Com
			General	55104	Neswork	Policies	Sonjour Director	Admin		SAVE CONFIGURATION
SSIDs () Rear Advanced Edit or view an existing SSID, assign SSIDs, and create new	v SSIDs here.				_					Show Advanced
SSID Name	Band	VLAN Primany			Encryption/Auth	entication		Enabled	Broadcast	+ NEW SSID
		EDIT VLANS)		Configure					Disable VIANs
ncryption & Authentication mfgure the WPA and RADIUS settings What encryption type would you AES (recomme Trup AES & Trup	Ike to use?	Authentication				Encry Configure	rption & A the WPA and RAD ch authentico gure External RA Prim Sh Confirm Sh	Uthentication US settings ation method wou EAP DIUS Server ary Hosz/IP: 192.166 Port: 1812 ared Secret:	Encryption Id you like to use?	Authentication
										Encountion Authentication
		Cancel							Accounting: Yes 🌒 No	move Alternate Accounting Server

項目	値
What encryption type would you like to use?	AES (recommended stronger than TKIP)
Which authentication method would you like to use?	EAP
Configuration External RADIUS Server	
- Primary Host/IP	192.168.1.2
- Port	1812
- Shared Secret/Confirm Shared Secret	secret
- Accounting	Yes
- Primary Host/IP	192.168.1.2
- Port	1813
- Shared Secret/Confirm Shared Secret	secret



EPS Cloud • • ③ created by J Smith										Configuration A	ccess Points Clients
			General	SSIDx	Network	Policies	O Bonjour Director	Admin		SAVE	CONFIGURATION
SSIDs () Snow Advanced Edit or view an existing SSID, assign SSIDs, a	nd create new SSIDs here.									Show Advan	+ NEW SSID
SSID Name	Band	VLAN			Encryption/Aut	hentication		Enabled	Broadcast	Access Control	
Soliton Lab	2.4GHz & 5GHz				WPA2/802.1x			Yes	Yes	None	
											Enable VLANs

以上でクラウドでの Xirrus XD2-240 の設定は完了です。

「SAVE CONFIGURATION」を押下し設定を保存してください。





4. EAP-TLS 認証でのクライアント設定

4-1 Windows 10 での EAP-TLS 認証

4-1-1 クライアント証明書のインポート

PC にクライアント証明書をインポートします。ダウンロードしておいたクライアント証明書 (user01_02.p12)をダブルクリックすると、証明書インポートウィザードが実行されます。





4.EAP-TLS 認証でのクライアント設定



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。

マキュリティの種類(E): WPA2 - エンタープライズ v	項目	値
号化の種類(N): AES ~	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
+>>>→の50-50-50-50-50-50-50-50-50-50-50-50-50-5	ネットワークの認証・・・	Microsoft: スマートカード
詳細設定(0) OK キャンセル 0K キャンセル シンゴス の設定 シンゴス の設定 シンゴス の設定 シンゴス の設定 シンゴス の設定 シンゴス の設定 シンゴス の設定 ● 居信線の保存(C) ・ マイのユーザーの資格情報を削除する(D) ● 日ガインの直線に実行する(E) ・ コーザー ロガインの直線に実行する(F) ● コーザー ロガインの直線に実行する(F) ・ コーザー ロガインの直線に実行する(F) ● コーザー ロジェーターとコーザーの認証に別の仮想	スマートカードまたはその 思想のための認証方法: 自分のスマートカードを使う(S) ① Cのコンビューターの証明書を使う(C) 単純や証明書の選択を使う(推奨)(I) ジ 証明書を検証してサーバーの ID を検 ① 次のサーバーに接続する(例: srv1.) ご 確頼されたルート証明機関(R): 1 Microsoft Root Certificate Auti 〇 竹あいた Primany Root CA 1 Thavke Primary Root CA ○ ThavtACorp SGC ○ UTN - DATACorp SGC ○ TIN - DATACorp SGC ○ TIN - DATACorp SGC ○ TIN - DATACorp SGC ○ UTN - JSERFirst-Object ○ Corp接花で別のユーザー名を使う(D)	/他の証明書のプロ/(ティ ぼ相設定(A) My Eff る(V) srv2, *¥.srv3¥.com)(0): hority 2010 hority 2010 hority 2011
	項日 接続のための認証方法	1進
OK キャンセル	- 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
间值	証明書を検証してサーバー	のIDを・・・ On



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

Xirrus XD2-240 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。



Seliton

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



<u>Seliton</u>

4-3-2 サプリカント設定

Xirrus XD2-240 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。

				O 💎 🗎 14:19
÷	Wi-Fi			0
	ON			۲
	SolitonLab			ŵ
	1			
Soli	onLab			
EAP	式			
TLS			-	
CA証	月書			
Test	A		-	
ドメー	シ			
ユー!	*一証明書			
user	1		•	
ID				
user	01			
詳細語	定		~	
		キャンセル	接続	

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



5. EAP-PEAP 認証でのクライアント設定

5-1 Windows 10 での EAP-PEAP 認証

5-1-1 Windows 10 のサプリカント設定

[ワイヤレスネットワークのプロパティ]の「セキュリティ」タブから以下の設定を行います。

SolitonLab ワイヤレス ネットワークのプロパティ ×	項目		値
	セキュリテ	ィの種類	WPA2-エンタープライズ
セキュリティの種類(E): WPA2 - エンターブライズ v 路号化の種類(N): AES v	暗号化の種	類	AES
	ネットワー	クの認証・・・	Microsoft: 保護された EAP
ネットワークの認証方法の遵択(O): Microsoft:保護された EAP (PEAP) ・	**************** <u>*</u>	保護され 接続のための認証方法: ・ 証明書を検証してサーバーの II 二次のサーバーに接続する(例: 「Microsoft Root Certifica マ TestCA し thavite Primary Root Ci し Thavite Timestamping UTN - DATACorp SGC UTN-USERFirst-Object し VeriSign Class 3 Public R く 接続前の通知(T):	Uた EAP のプロパティ 2 登梯証する(V) srv1、srv2、*¥.srv3¥.com)(0): te Authority 2011 A CA Primary Certification Authority - G5 ×
议 詳細設定 ×		サーバー名またはルート証明書が	指定されなかった場合にユーザーに通知します >
802.1X の設定 802.11 の設定		セキュリティで保護されたパスワード((EAP-MSCHAP v2) × 構成(C)
 ✓ 認証モードを指定する(P): ユーザー認証 すべてのユーザーの資格情報を削除する(D) 		 ✓ 高速再接続を有効にする(F) □ネットワークアクセス保護を溢割 □サーバーに暗号化パインドのTLX □ ID プライパシーを有効にする(I) 	する(N) / がない場合は切断する(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) ④ 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) 最大待ち時間 (秒)(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)		EAP 接続のための認証7 □ Windows d 合はドメイン)	UK キャラビル MSCHAPv2のプロパティ × 方法: ション 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
 のK キャンセル	項目 接続のたる	めの認証方法	値

項目	値
認証モードを指定する	ユーザー認証

項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA
- Windows のログオン名と・・・	Off



5-2 iOS での EAP-PEAP 認証

5-2-1 iOS のサプリカント設定

Xirrus XD2-240 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% = D	•••• au 4G	13:52	۲
く設定	Wi-Fi		"Soli	tonLab"のパスワードを入:	љ	キャンセル	証明書	
			キャンセル	パスワード入力	接続			
Wi-Fi							aeps.local	
			ユーザ名 U	ser01		9	行元: TestCA	
ネットワークを選択.			パスワード・	•••••		1	言頼されていません	
SolitonLab		ê ╤ (j)				有効期限	026/01/26 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 ことのあるネットワー	ットワークに自動的に接続 クが見つからない場合は、	売します。接続した 手動でネットワー						
クを選択する必要があ	ります。							
			q w e	r t y u	о р			
			a s d	fghj	k I			
			☆ 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

Xirrus XD2-240 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。

WiFl (1) (1) (1) (1) (1) (1) (1) (1) (1) (1)			O 🛡 🗎 14:19
N ● ● Situral ● EAP5ボ ● PEAP ● フェーズ2認証 ● MSCHAPV2 ● CA証明書 ● TetCA ● ドメイン ● ID ● user01 ● 暦名印 ● パスワード ● 「パスワードを表示する ● 詳細定 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	← Wi-Fi		0
• botton Lab Биѓол Lab Галба Галба Талба Оханива По User01 По Изаго1 По Изаго1 По Шако1 По По	ON		
SolitonLab EAP5式 PEAP ・ フェース2窓証 ・ MSCHAPV2 ・ CA証明書 ・ TestCA ・ ドメイン ・ ID ・ user01 ・ IZヘフード ・ パスワード ・ 「パスワードを表示する ・ 評細図定 ・	SolitonLab		â
SolitonLab EAP方式 PEAP ・ フェーズ2認証 ・ MSCHAPV2 ・ CA証明書 ・ TestCA ・ ドメイン ・ ID ・ user01 ・ バスワード ・ ・・・・・・ ・			
EAP方式 PEAP ・ フェーズ2認証 MSCHAPV2 ・ CA証明書 TestCA ・ ドメイン ID user01 置名ID パスワードを表示する 詳細設定 ・	SolitonLab		
PEAP ・ フェーズ20部正 ・ MSCHAPV2 ・ CA証明書 ・ TestCA ・ ドメイン ・ ID ・ user01 ・ 原名ID ・ パスワード ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	EAP方式		
フェーズ2認証 ・ MSCHAPV2 ・ CA証明書 ・ TestCA ・ ドメイン ・ ID ・ user01 ・ 度名ID ・ パスワード ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	PEAP	*	
MSCHAPV2 ・ CA証明書 ・ TestCA ・ ドメイン ・ ID ・ user01 ・ 暦名ID ・ パスワード ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	フェーズ2認証		
CA証明書 TestCA ・ ドメイン ID user01 匿名ID パスワード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	MSCHAPV2	-	
TestCA ・ ドメイン ・ ID ・ user01 ・ 匿名ID ・ パスワード ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	CA証明書		
ドメイン ID user01 置名ID パスワード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	TestCA	-	
ID user01 匿名ID パスワード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	ドメイン		
ID user01 匿名ID パスワード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・			
user01 匿名ID パスワード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	ID		
匿名ID パスワード ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・	user01		
バスワード ・・・・・・	匿名ID		
バスワード ・・・・・・			
	パスワード		
□ パスワードを表示する 詳細設定 ~			
 」 パスワードを表示する 詳細設定 キャンセル 接続 			
詳細設定	└┘ パスワードを表示する		
キャンセル 接続	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

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 WirelessAP port 256 cli 40-A3-CC-32-10-A4)
Xirrus XD2-240	Station 40:a3:cc:32:10:a4 (192.168.1.106, S18205, Intel Notebook), IAP iap2: IPv4 address available, IPv4: 192.168.1.106, SSID: SolitonLab, Username: user01

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 WirelessAP port 256 cli 40-A3-CC-32-10-A4 via proxy to virtual server) Login OK: [user01] (from client WirelessAP port 256 cli 40-A3-CC-32-10-A4)
Xirrus XD2-240	Station 40:a3:cc:32:10:a4 (192.168.1.106, S18205, Intel Notebook), IAP iap2: IPv4 address available, IPv4: 192.168.1.106, SSID: SolitonLab, Username: user01

Seliton

改訂履歴

日付	版	改訂内容
2018/06/13	1.0	初版作成
2018/12/25	2.0	Xirrus の設定を XMS-Cloud からに変更