

NetAttest EPS

認証連携設定例

【連携機器】 Riverbed Xirrus XD2-240

【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、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
	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 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。

目次

1. 構成.....	6
1-1 構成図.....	6
1-2 環境.....	7
1-2-1 機器.....	7
1-2-2 認証方式.....	7
1-2-3 ネットワーク設定.....	7
2. NetAttest EPS の設定.....	8
2-1 初期設定ウィザードの実行.....	8
2-2 システム初期設定ウィザードの実行.....	9
2-3 サービス初期設定ウィザードの実行.....	10
2-4 ユーザーの登録.....	11
2-5 クライアント証明書の発行.....	12
3. NetAttest D3 の設定.....	13
3-1 スコープの設定.....	14
3-2 IP アドレスの静的割り当て.....	15
3-3 DHCP サーバーの起動.....	17
4. Xirrus XD2-240 の設定.....	18
4-1 Express Setup.....	19
4-2 External RADIUS サーバーの設定.....	20
4-3 無線の設定.....	21
5. EAP-TLS 認証でのクライアント設定.....	22
5-1 Windows 10 での EAP-TLS 認証.....	22
5-1-1 クライアント証明書のインポート.....	22
5-1-2 サプリカント設定.....	24
5-2 iOS での EAP-TLS 認証.....	25
5-2-1 クライアント証明書のインポート.....	25
5-2-2 サプリカント設定.....	26
5-3 Android での EAP-TLS 認証.....	27
5-3-1 クライアント証明書のインポート.....	27

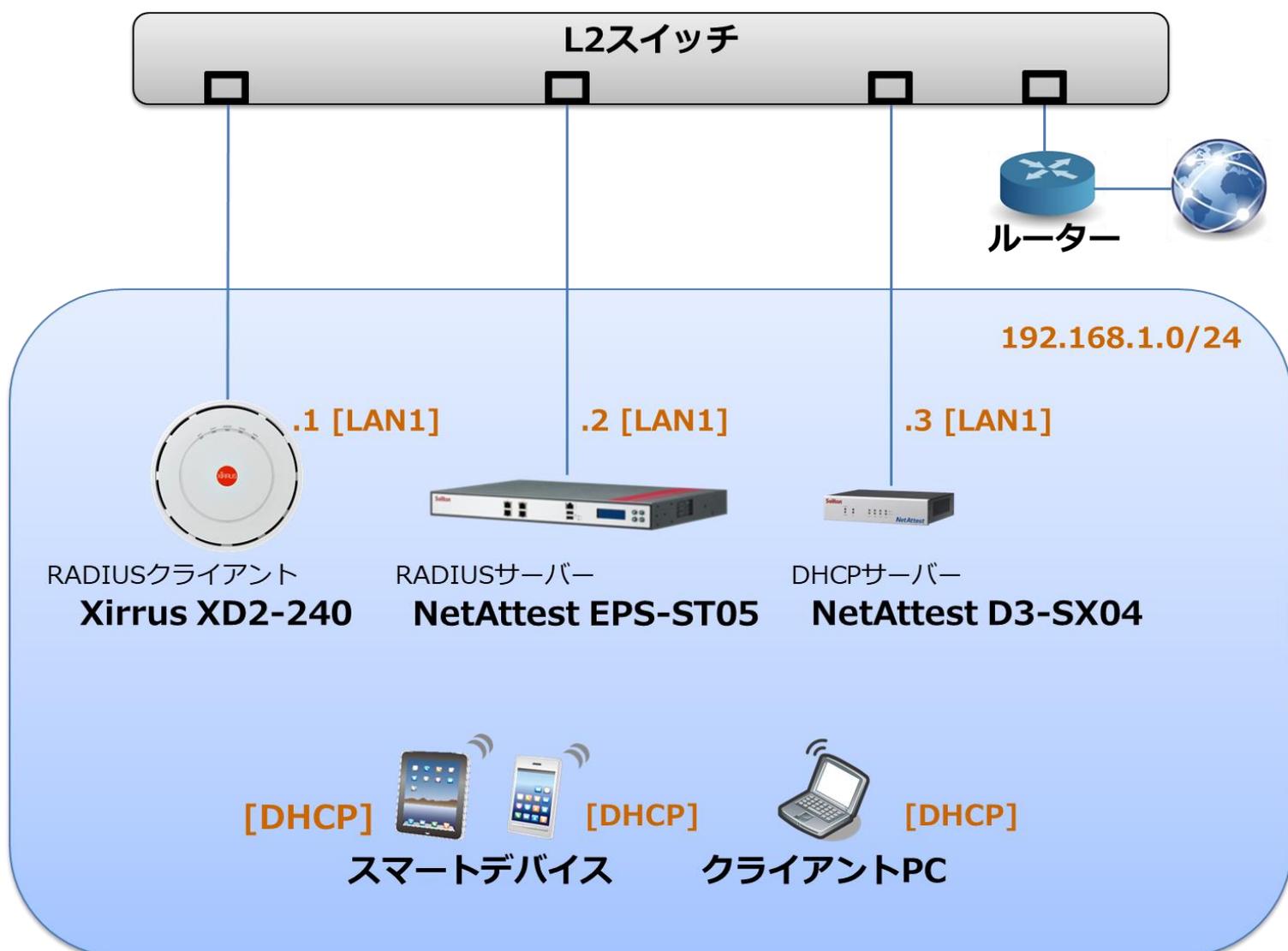
5-3-2 サプリカント設定.....	28
6. EAP-PEAP 認証でのクライアント設定.....	29
6-1 Windows 10 での EAP-PEAP 認証.....	29
6-1-1 Windows 10 のサプリカント設定	29
6-2 iOS での EAP-PEAP 認証.....	30
6-2-1 iOS のサプリカント設定	30
6-3 Android での EAP-PEAP 認証.....	31
6-3-1 Android のサプリカント設定.....	31
7. 動作確認結果	32
7-1 EAP-TLS 認証.....	32
7-2 EAP-PEAP 認証.....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

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



1-2 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 標準サブリカント
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	UDP 1812	secret
Xirrus XD2-240	192.168.1.1/24		secret
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。

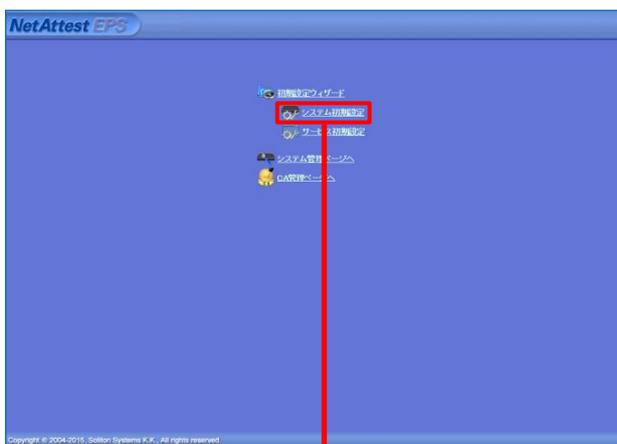
下記のような流れでセットアップを行います。

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)

NetAttest EPS 管理画面の「ユーザー一覧」画面。検索条件は「一部」で「user01」が検索結果として表示されている。右側の「発行」ボタンが赤い枠で囲われ、赤い矢印が下向きに伸びている。

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

編集対象: user01
 基本情報
 姓: user01
 名:
 E-Mail:
 詳細情報
 証明書情報
 ユーザーID: user01
 有効期限: 365 日
 ● 日付: 2016 年 7 月 9 日 23 時 59 分 59 秒まで
 証明書ファイルオプション
 パスワード:
 パスワード(確認):
 ※パスワードが空欄の場合は、ユーザーのパスワードを使用します。
 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

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

ユーザー証明書のダウンロード
 ユーザー証明書ダウンロードの準備ができました。対象をファイルに保存して下さい。
 ダウンロード

3. NetAttest D3 の設定

Xirrus XD2-240 は、デフォルトでは DHCP にて IP アドレスを取得するよう設定されています。しかし、EPS に RADIUS クライアントとして登録するためには IP アドレスを静的に指定する必要があります。今回は Xirrus XD2-240 に静的に IP アドレスを割り当てるために、NetAttest D3 の静的割り当て機能を使用して IP アドレスを払い出すことにします。

NetAttest D3 の初期設定は LAN2(管理インターフェイス)から行います。初期の IP アドレスは、[192.168.2.1/24]です。管理端末に適切な IP アドレスを設定し、Google Chrome から [http://192.168.2.1:2181/]にアクセスしてください。NetAttest D3 では以下の設定を行います。

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

3-1 スコープの設定

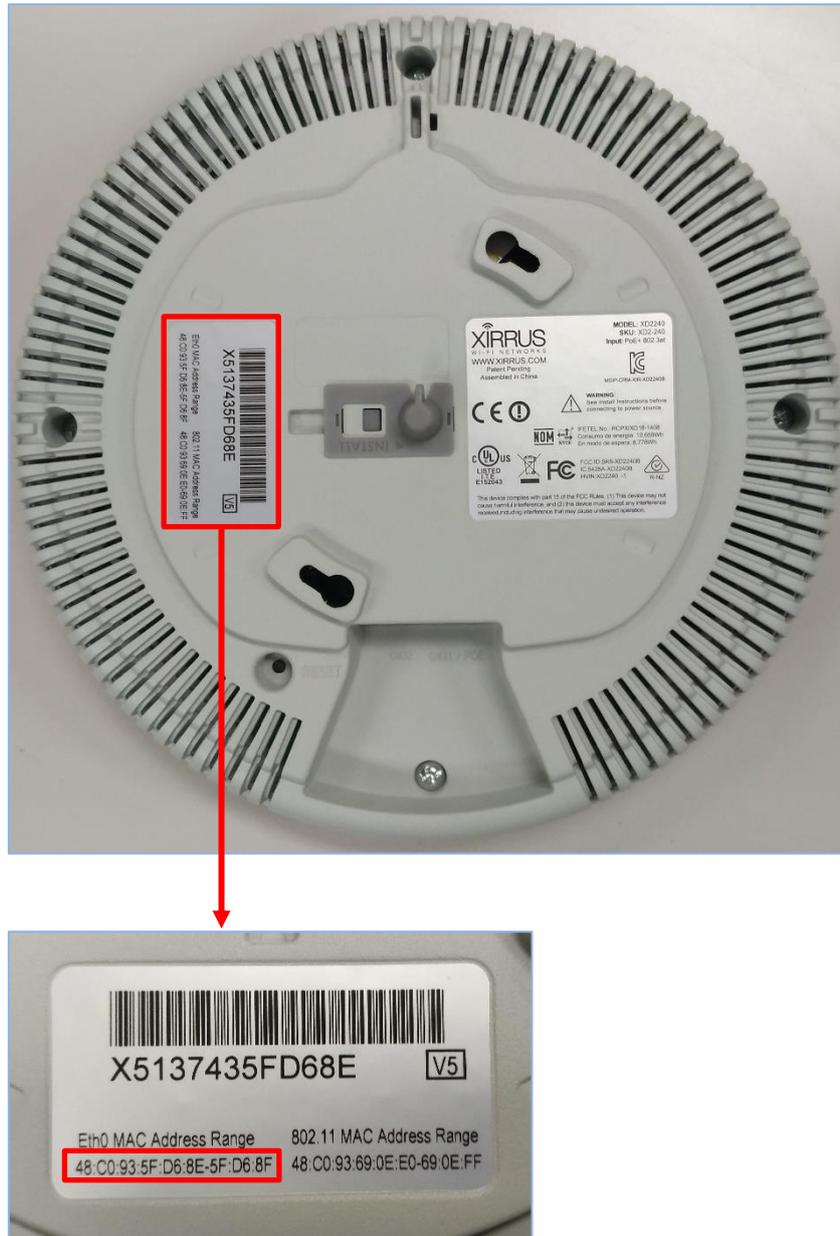
[DHCP サービス]-[スコープ]から[追加]ボタンでスコープを追加します。今回は、端末に払い出す IP アドレスを[192.168.1.100-140]にするため、以下のように設定します。



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

3-2 IP アドレスの静的割り当て

Xirrus XD2-240 の MAC アドレスに IP アドレスを静的に割り当てるため、事前に Xirrus XD2-240 の MAC アドレスを確認します。Xirrus XD2-240 の MAC アドレスは本体裏面に記載されています。



[DHCP サービス]-[静的割り当て]から[追加]ボタンで IP アドレスの静的割り当てを行います。Xirrus XD2-240 の MAC アドレスと、静的に割り当てる IP アドレスを指定します。

NetAttest D3

ホスト名: nad3.example.com | DNS: ✕ | DHCP: ✕

システム設定

システム管理

ドメインネームサービス

DHCPサービス

サーバー状態

サーバー設定

リース情報

スコープ

登録クライアント

静的割り当て

冗長化設定

DHCP - 静的割り当て

ホスト名 IPアドレス MACアドレス 備考1 備考2 備考3 最終リース日時

表示するデータはありません

フィルタ

追加 CSVダウンロード CSVアップロード 付加情報項目名のカスタマイズ

NetAttest D3

ホスト名: nad3.example.com | DNS: ✕ | DHCP: ✕

システム設定

システム管理

ドメインネームサービス

DHCPサービス

サーバー状態

サーバー設定

リース情報

スコープ

登録クライアント

静的割り当て

冗長化設定

認証用NetAttest EPS設定

DHCP - 静的割り当て - 追加/修正

ホスト名 Xirus

IPアドレス 192.168.1.1

MACアドレス 48:c0:93:5f:d6:8e

備考1

備考2

備考3

OK キャンセル

項目	値
ホスト名	Xirus
IP アドレス	192.168.1.1
MAC アドレス	48:c0:93:5f:d6:8e
備考 1	XD2-240 (任意)

NetAttest D3

ホスト名: nad3.example.com | DNS: ✕ | DHCP: ✕

システム設定

システム管理

ドメインネームサービス

DHCPサービス

サーバー状態

サーバー設定

リース情報

スコープ

登録クライアント

静的割り当て

冗長化設定

認証用NetAttest EPS設定

ユーザー定義オプション

DHCP - 静的割り当て

ホスト名	IPアドレス	MACアドレス	備考1	備考2	備考3	最終リース日時
<input checked="" type="checkbox"/> Xirus	192.168.1.1	48:c0:93:5f:d6:8e	XD2-240			

全選択

1

表示する件数 25 (全部: 1ページ, 1件)

1 ページ 移動

フィルタ

追加 削除 全削除 CSVダウンロード CSVアップロード

付加情報項目名のカスタマイズ ゴーストMACアドレスの確認

3-3 DHCP サーバーの起動

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

NetAttest D3

ホスト名: nad3.example.com DNS [×] DHCP [×]

システム設定
システム管理
ドメインネームサービス
DHCPサービス
サーバー状態
サーバー設定
リース情報
スコープ
登録クライアント
静的割り当て
冗長化設定
認証用NetAttest EPS設定

DHCP - サーバー状態

動作状態

サーバー稼働状態: 停止

冗長化状態: 冗長化しない

IP使用率(%)

0%

0 / 0 max

4. Xirrus XD2-240 の設定

Xirrus XD2-240 は PoE 対応のスイッチにケーブルで接続すれば起動します。Xirrus XD2-240 はクラウドからの設定とローカル接続での設定の両方が可能ですが、今回はローカル接続で設定を行います。

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。

アクセスする URL は、`https://<IP_ADDRESS>`

証明書の例外エラーが出るため、例外登録をしたうえで続行

初期 ID/Password は、admin/admin です。

セットアップは下記の流れで行います。

1. Express setup の設定
2. External RADIUS サーバーの設定
3. 無線の設定

4-1 Express Setup

Time Zone の設定は必ず行ってください。ライセンスキーはベンダーから手に入れたものを入力してください。SSID の設定は後で変更しますが、SSID 名だけここで作成してください。

License	
License Key:	1P34Q-B75X6-9UR11-AI <input type="button" value="Apply"/>
Contact Information	
Location:	Anywhere, USA
Contact Name:	J Smith
Contact Email:	jsmith@xyzcorp.com
Contact Phone:	212 555-1212
Network Settings	
Host Name:	factoryap
Address Type:	<input checked="" type="radio"/> DHCP <input type="radio"/> Static
IP Settings:	Address: 192.168.1.84 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.1.254 <input type="button" value="Apply"/>
SSID Settings	
SSID Name (Replaces SSID "xirrus"):	<input type="text"/>
Wireless Security:	Open <input type="button" value="Apply SSID Settings"/>
Current SSIDs	guest honeypot xyzcorp
Admin Settings	
New Admin User (Replaces user "admin"):	<input type="text"/>
New Admin Privilege Level:	1 : read-write <input type="button" value="Apply Admin Settings"/>
New Admin Password:	<input type="text"/>
Confirm Admin Password:	<input type="text"/>
Time and Date Settings	
Time Zone:	(GMT - 08:00) Pacific Time (US & Canada); Tijuana <input type="button" value="Apply"/>
Quick Configuration	
Apply Quick Configuration Template:	Select a Te... <input type="button" value="Apply"/>
IAP Settings	
Enable/Configure All IAPs:	<input type="button" value="Execute"/>

項目	値
License Key	...
SSID	SolitonLab
Timezone	GMT +09:00
admin	任意

4-2 External RADIUS サーバーの設定

RADIUS サーバーの設定を行います。

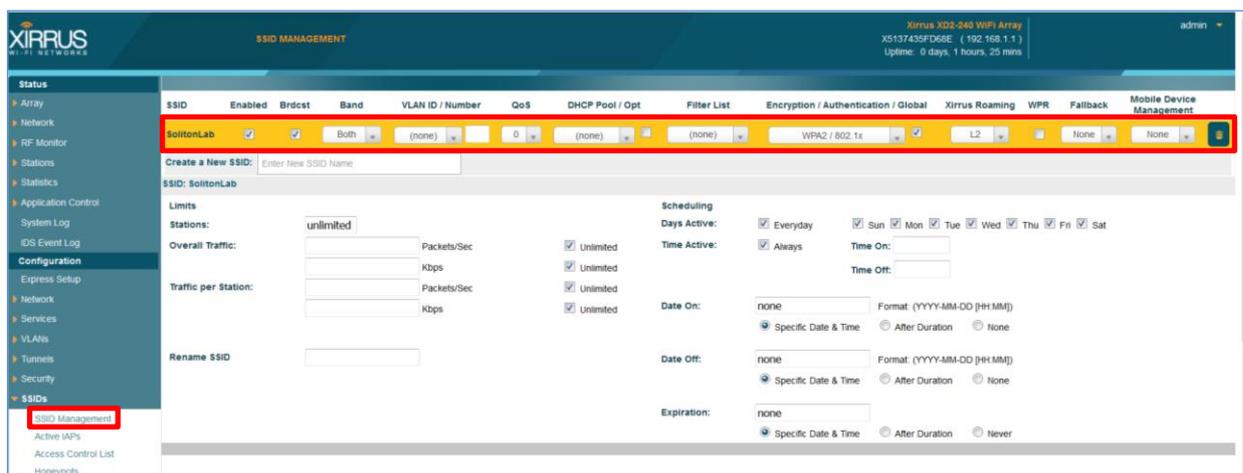
The screenshot displays the configuration page for External RADIUS. The left sidebar shows the navigation menu with 'External Radius' selected. The main content area is divided into several sections:

- Primary Server:** Host Name / IP Address: 192.168.1.2, Port Number: 1812, Shared Secret / Verify Secret: [masked]
- Secondary Server:** Host Name / IP Address: [empty], Port Number: 1812, Shared Secret / Verify Secret: [empty]
- RADIUS Failover Settings:** Timeout (seconds): 600, Failover Timeout (seconds): 10
- RADIUS Dynamic Authorization Settings:** DAS Port: 3799, DAS Event-Timestamp: Optional, Required, DAS Time Window: 300, NAS Identifier: [empty]
- RADIUS Attribute Formatting:** Called-Station-Id Attribute Format: BSSID, BSSID.SSID, Ethernet-MAC, Station MAC Format: lower-case [xxxxxxxxxxxx], UPPER-case [XXXXXXXXXXXX], lc-hyphenated [xx-xx-xx-xx-xx-xx], UC-hyphenated [XX-XX-XX-XX-XX-XX]
- Accounting:** Off, On
- Accounting Interval (seconds):** 300
- Primary Server Host Name / IP Address:** 192.168.1.2
- Primary Server Port Number:** 1813
- Primary Server Shared Secret / Verify Secret:** [masked]
- Secondary Server Host Name / IP Address:** [empty]

項目	値
Host Name/IP Address	192.168.1.2
Port Number	1812
Shared Secret/Verify Secret	secret
Accounting	On
Primary Server Host Name/IP Address	192.168.1.2
Primary Server Port Number	1813
Primary Server Shared Secret/Verify Secret	secret

4-3 無線の設定

無線の設定は SSID の設定で行われます。Express setup で作成した SSID を選択して、設定を変更してください。



項目	値
SSID	SolitonLab
Enabled	Checked
Encryption/Authentication	WPA2/802.1X
Global	Checked

IAP Setting で IAP を Enable にします。Enable all IAPs をクリックしてください。

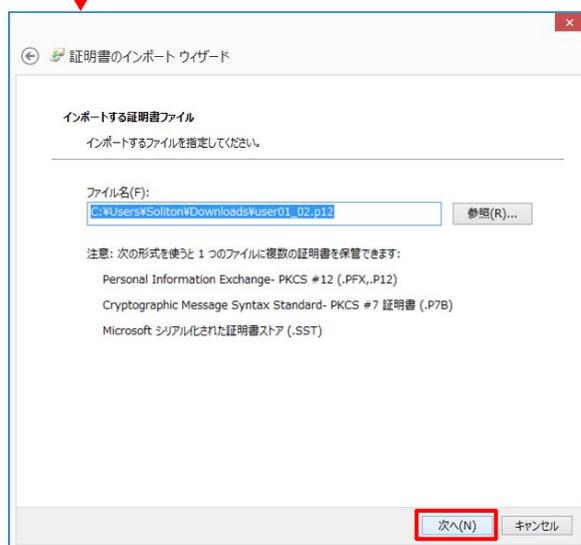
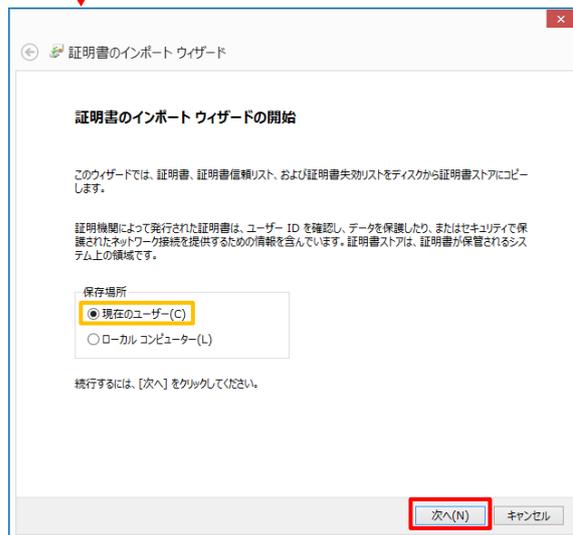
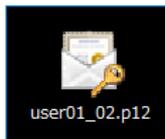


5. EAP-TLS 認証でのクライアント設定

5-1 Windows 10 での EAP-TLS 認証

5-1-1 クライアント証明書のインポート

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



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】
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

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:

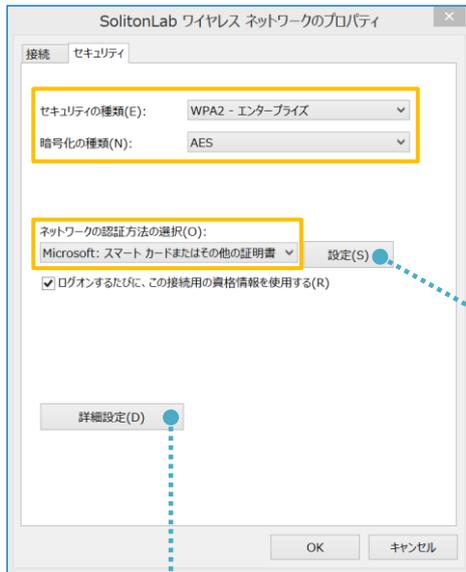
選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\Soliton\Downloads\User01_02.p12

完了(F) キャンセル

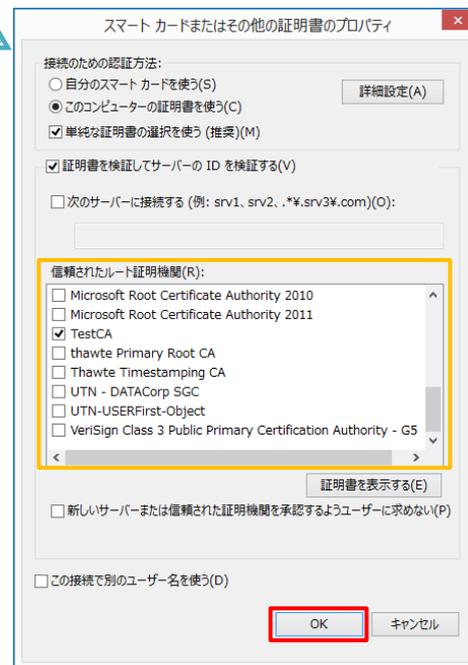
5-1-2 サプリカント設定

Windows 標準サプリカントで TLS の設定を行います。

[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
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

項目	値
認証モードを指定する	ユーザー認証

5-2 iOS での EAP-TLS 認証

5-2-1 クライアント証明書のインポート

NetAttest EPS から発行したクライアント証明書を iOS デバイスにインポートする方法には下記などがあります。

- 1) Mac OS を利用して Apple Configurator を使う方法
- 2) クライアント証明書をメールに添付し iOS デバイスに送り、インポートする方法
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)

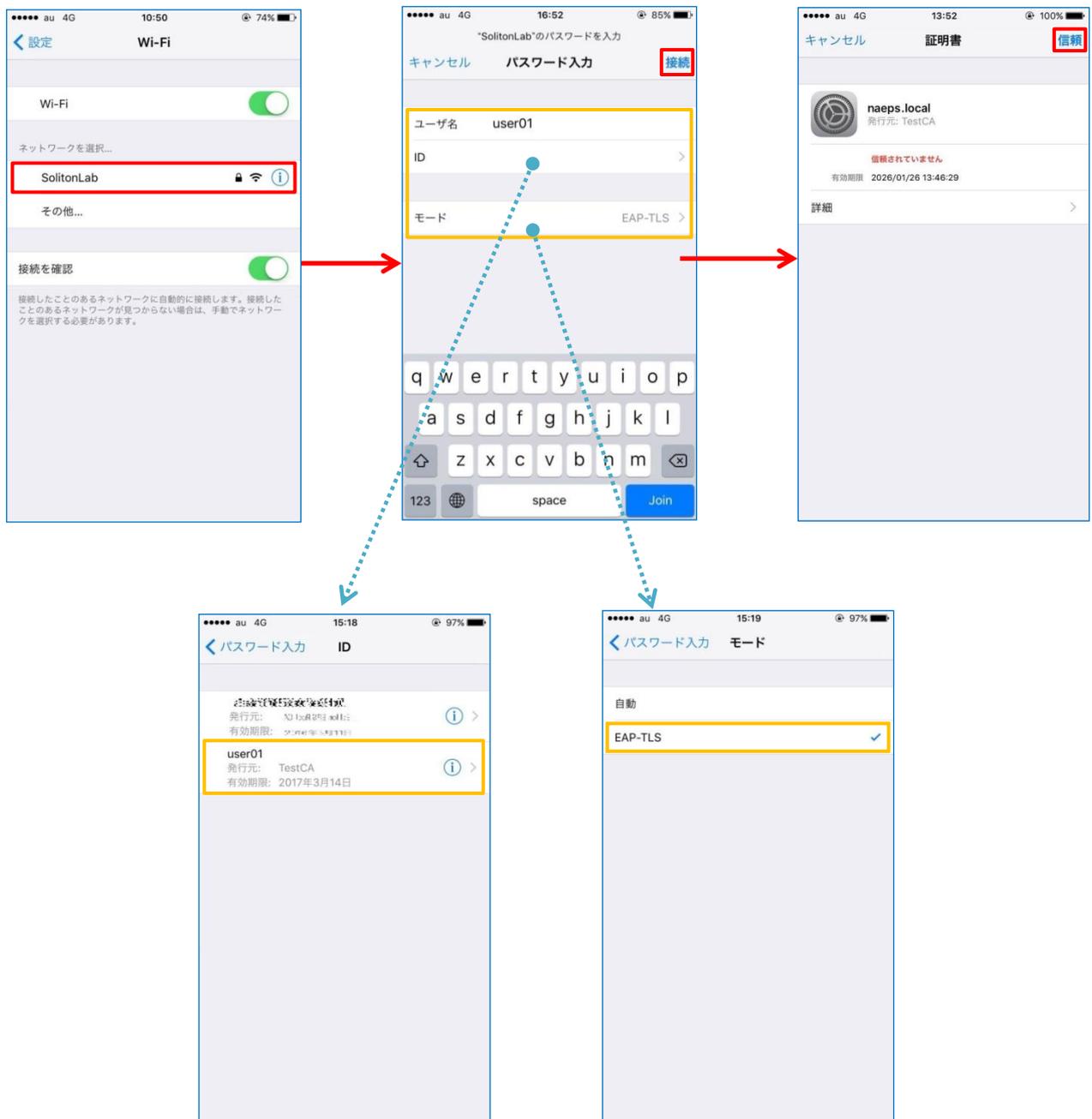
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

5-2-2 サプリカント設定

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。



5-3 Android での EAP-TLS 認証

5-3-1 クライアント証明書のインポート

NetAttest EPS から発行したクライアント証明書を Android デバイスにインポートする方法として、下記 3 つの方法等があります。いずれかの方法で CA 証明書とクライアント証明書をインポートします。手順については、本書では割愛します。

- 1) SD カードにクライアント証明書を保存し、インポートする方法※1
- 2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※2
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※1 メーカーや OS バージョンにより、インポート方法が異なる場合があります。事前にご検証ください。

※2 メーカーや OS バージョン、メーカーにより、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

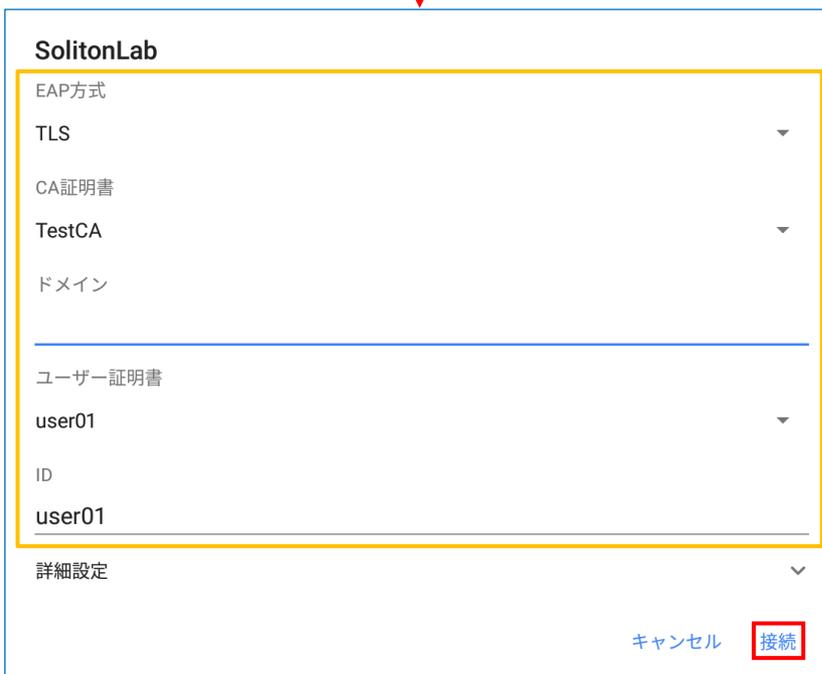
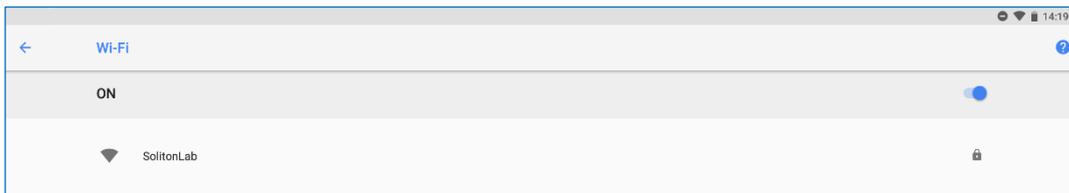
パッケージの内容:
ユーザーキー1個
ユーザー証明書1件
CA証明書1件

キャンセル

5-3-2 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擇して下さい。



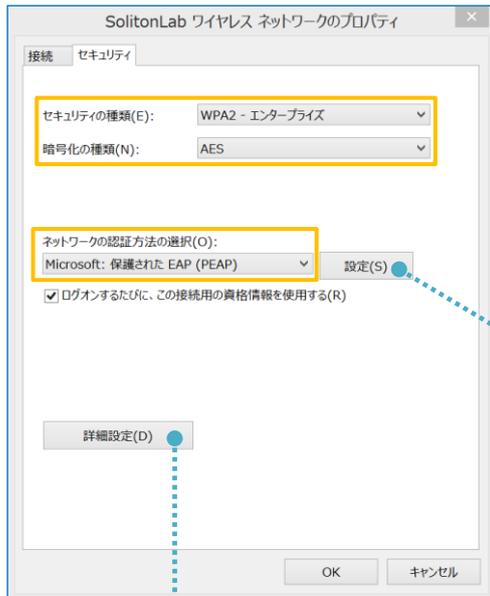
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

6. EAP-PEAP 認証でのクライアント設定

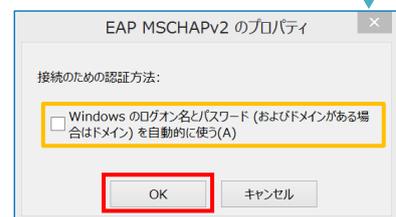
6-1 Windows 10 での EAP-PEAP 認証

6-1-1 Windows 10 のサブリカント設定

[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。



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

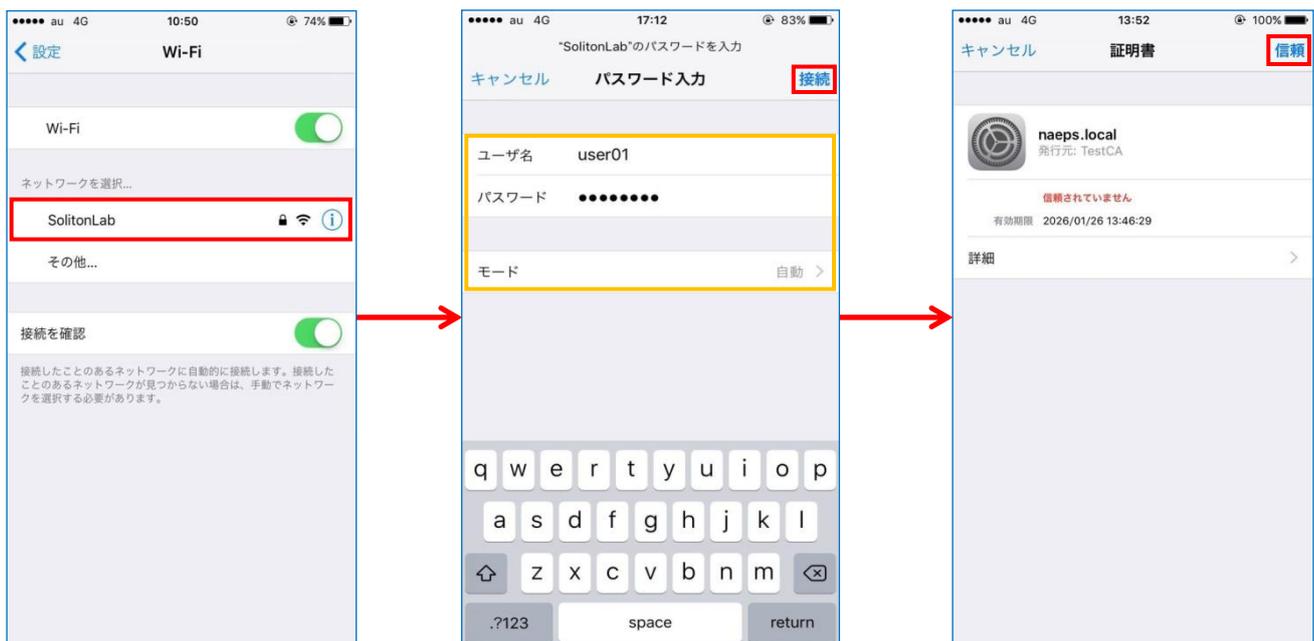
項目	値
接続のための認証方法	
- サーバー証明書の検証をする	On
- 信頼されたルート認証機関	TestCA
- Windows のログオン名と・・・	Off

6-2 iOS での EAP-PEAP 認証

6-2-1 iOS のサブリカント設定

Xirrus XD2-240 で設定した SSID を選択し、サブ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。

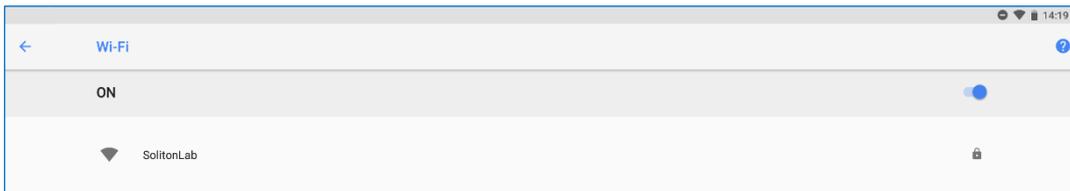


項目	値
ユーザ名	user01
パスワード	password
モード	自動

6-3 Android での EAP-PEAP 認証

6-3-1 Android のサブリカント設定

Xirrus XD2-240 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。



SolitonLab

EAP方式
PEAP ▼

フェーズ2認証
MSCHAPV2 ▼

CA証明書
TestCA ▼

ドメイン

ID
user01

匿名ID

パスワード
.....

パスワードを表示する

詳細設定 ▼

キャンセル 接続

項目	値
EAP 方式	PEAP
フェーズ 2 認証	MSCHAPV2
CA 証明書	TestCA
ID	user01
パスワード	password

7. 動作確認結果

7-1 EAP-TLS 認証

EAP-TLS 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	May 30 14:38:06 naeps radiusd[3094]: notice 2018/05/30 14:38:06 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

7-2 EAP-PEAP 認証

EAP-PEAP 認証が成功した場合のログ表示例

製品名	ログ表示例
NetAttest EPS	May 30 14:53:10 naeps radiusd[3094]: notice 2018/05/30 14:53:10 Login OK: [user01] (from client WirelessAP port 256 cli 40-A3-CC-32-10-A4 via proxy to virtual server) May 30 14:53:10 naeps radiusd[3094]: notice 2018/05/30 14:53:10 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

