

NetAttest EPS

認証連携設定例

【連携機器】 Cisco Meraki MR18

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

Rev3.0

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、Cisco Meraki 社製無線アクセスポイント MR18 の IEEE802.1X EAP-TLS/EAP-PEAP(MS-CHAP V2)環境での接続について、設定例を示したものです。設定例は管理者アカウントでログインし、設定可能な状態になっていることを前提として記述します。

アイコンについて

アイコン	説明
	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、NetAttest D3 及び MR18 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
1-1-1 機器.....	7
1-1-2 認証方式.....	7
1-1-3 ネットワーク設定.....	7
2. NetAttest EPS の設定.....	8
2-1 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. MR18 の設定.....	18
4-1 RADIUS 認証設定.....	18
5. EAP-TLS 認証でのクライアント設定.....	20
5-1 Windows 8.1 での EAP-TLS 認証.....	20
5-1-1 クライアント証明書のインポート.....	20
5-1-2 サプリカント設定.....	22
5-2 iOS(iPhone 6)での EAP-TLS 認証.....	23
5-2-1 クライアント証明書のインポート.....	23
5-2-2 サプリカント設定.....	24
5-3 Android(Google Nexus 7)での EAP-TLS 認証.....	25
5-3-1 クライアント証明書のインポート.....	25
5-3-2 サプリカント設定.....	26
6. EAP-PEAP 認証でのクライアント設定.....	27
6-1 Windows 8.1 のサプリカント設定.....	27
6-2 iOS(iPhone 6)のサプリカント設定.....	28

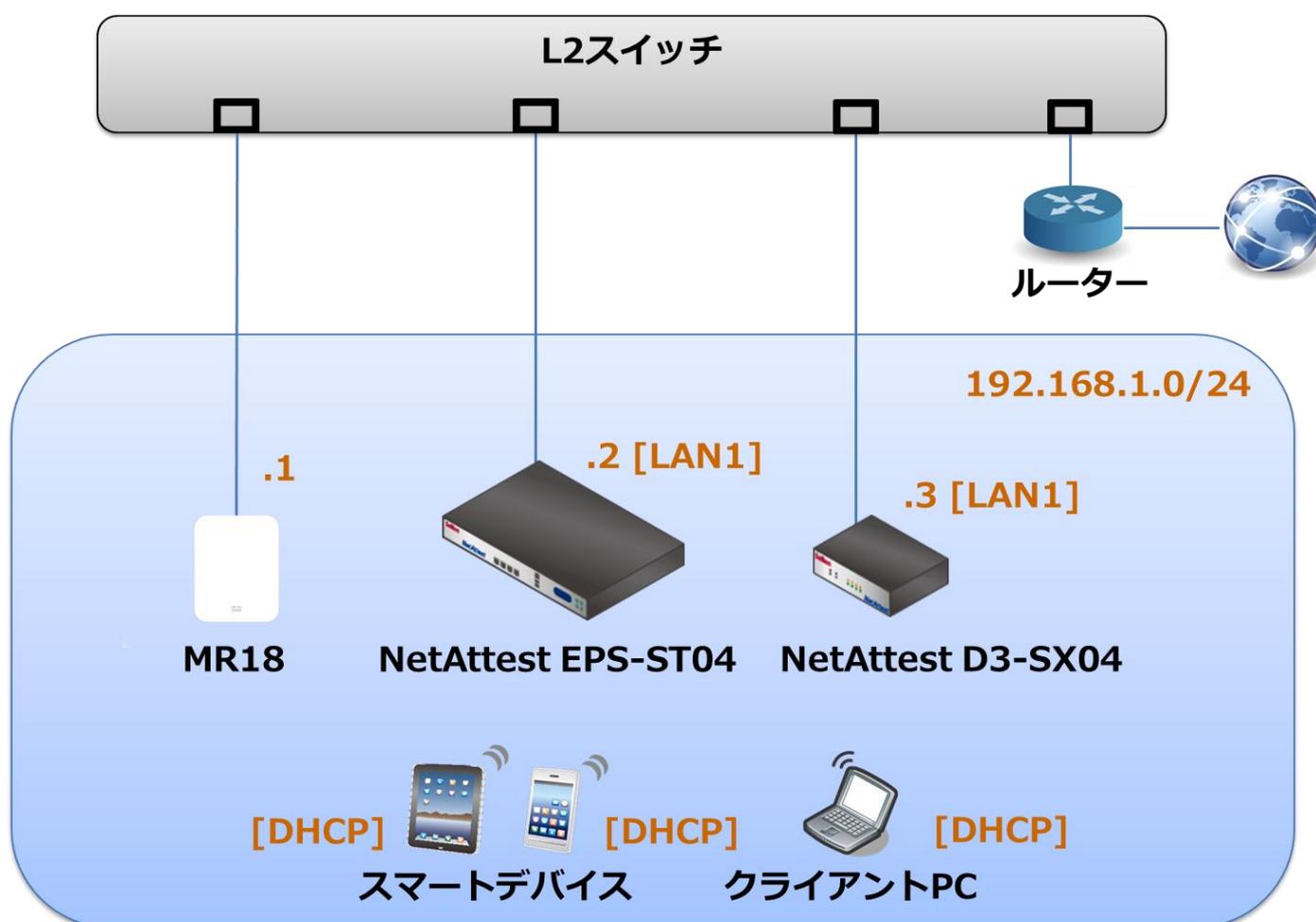
6-3 Android(Google Nexus 7)のサブリカント設定	29
7. 動作確認結果	30
7-1 EAP-TLS 認証.....	30
7-2 EAP-PEAP(MS-CHAP V2)認証	30

1. 構成

1-1 構成図

以下の環境を構成します。

- ・有線 LAN で接続する機器は L2 スイッチに収容
- ・有線 LAN と無線 LAN は同一セグメント
- ・無線 LAN で接続するクライアント PC の IP アドレスは、NetAttest D3-SX04 の DHCP サーバーから払い出す



1-1-1 機器

製品名	メーカー	役割	バージョン
NetAttest EPS ST-04	Soliton Systems	RADIUS/CA サーバー	4.8.4
MR18	Cisco Meraki	RADIUS クライアント (無線アクセスポイント)	—
Surface	Microsoft	802.1X クライアント (Client PC)	Windows 8.1 64bit Windows 標準サブリカント
iPhone 6	Apple	802.1X クライアント (Client SmartPhone)	9.2.1
Google Nexus 7	ASUS	802.1X クライアント (Client Tablet)	5.1
NetAttest D3 SX-04	Soliton Systems	DHCP/DNS サーバー	4.2.2

1-1-2 認証方式

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

1-1-3 ネットワーク設定

製品名	IP アドレス	RADIUS port (Authentication)	RADIUS Secret (Key)
NetAttest EPS ST-04	192.168.1.2/24	UDP 1812	secret
MR18	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。

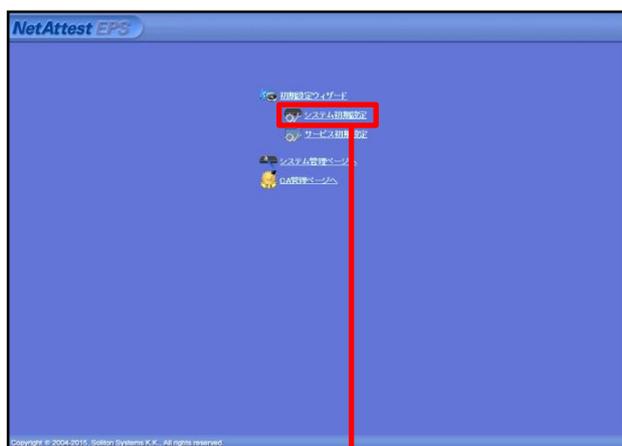
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

2-2 システム初期設定ウィザードの実行

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

その後、システム初期設定ウィザードを使用し、以下の項目を設定します。

- タイムゾーンと日付・時刻の設定
- ホスト名の設定
- サービスインターフェイスの設定
- 管理インターフェイスの設定
- メインネームサーバーの設定



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
ホスト名	naeps.local
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ドメイン機器連携	無効
グループ	無効
MACアドレス認証	無効
ポート制御	無効

戻る 再起動

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

項目	値
ホスト名	naeps.local
IP アドレス	デフォルト
ライセンス	なし

2-3 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

初期設定ウィザード - CA構築

CA種別選択
CA種別選択: ルートCA

CA秘密鍵
 内蔵で新しい鍵を生成する
 公開鍵方式: RSA
 鍵長: 2048
 外部RSM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

CA情報
 CA名(必須): TestCA
 国名: 日本
 郵便局名: Tokyo
 市区町村名: Shirojuku
 会社名(組織名): Soliton Systems
 部署名:
 E-mailアドレス:
 CA署名設定
 署名アルゴリズム: SHA256

項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA

初期設定ウィザード - RADIUSサーバーの基本設定

EAP

EAP認証タイプ
 優先順位: 認証タイプ
 1: TLS
 2: PEAP
 3: なし
 4: なし
 5: なし

EAP-TLS/TLS/PEAPオプション
 メッセージの最大サイズ: 1024 (バイト)
 メッセージの長さ情報: フラグメントなし (最初のフラグメントにのみ含まれる)

EAP-TLS/PEAPオプション
 GTC認証を有効にする
 TLSセッションチャンスを有効にする

EAP-FASTオプション

項目	値
EAP 認証タイプ	
1	TLS
2	PEAP

初期設定ウィザード - NAS/RADIUSクライアント設定

編集対象: 新規

NAS/RADIUSクライアント名: RadiusClient01

このNAS/RADIUSクライアントを有効にする

タイプ
 NAS/RADIUSクライアント
 NASのみ
 RADIUSクライアントのみ

説明: [空欄]

IPアドレス: 192.168.1.1

シークレット: *****

NAS識別値: [空欄]

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。

The screenshot illustrates the steps to add a new user in NetAttest EPS. It shows the navigation from the main menu to the user list, the 'Add' button, the configuration dialog for a new user, and the final state of the user list with the new user added.

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

2-5 クライアント証明書の発行

NetAttest EPS の管理画面より、クライアント証明書の発行を行います。

[ユーザー]→[ユーザー一覧]から、該当するユーザーのクライアント証明書を発行します。

(クライアント証明書は、user01_02.p12 という名前で保存)

NetAttest EPS 管理画面の「ユーザー一覧」タブ。検索条件を設定し、ユーザー一覧を表示。ユーザー「user01」の「発行」ボタンが赤枠で強調されている。

ユーザー「user01」の編集画面。認証情報と証明書ファイルオプションが黄色と赤で強調されている。

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確認画面。「ダウンロード」ボタンが赤枠で強調されている。

3. NetAttest D3 の設定

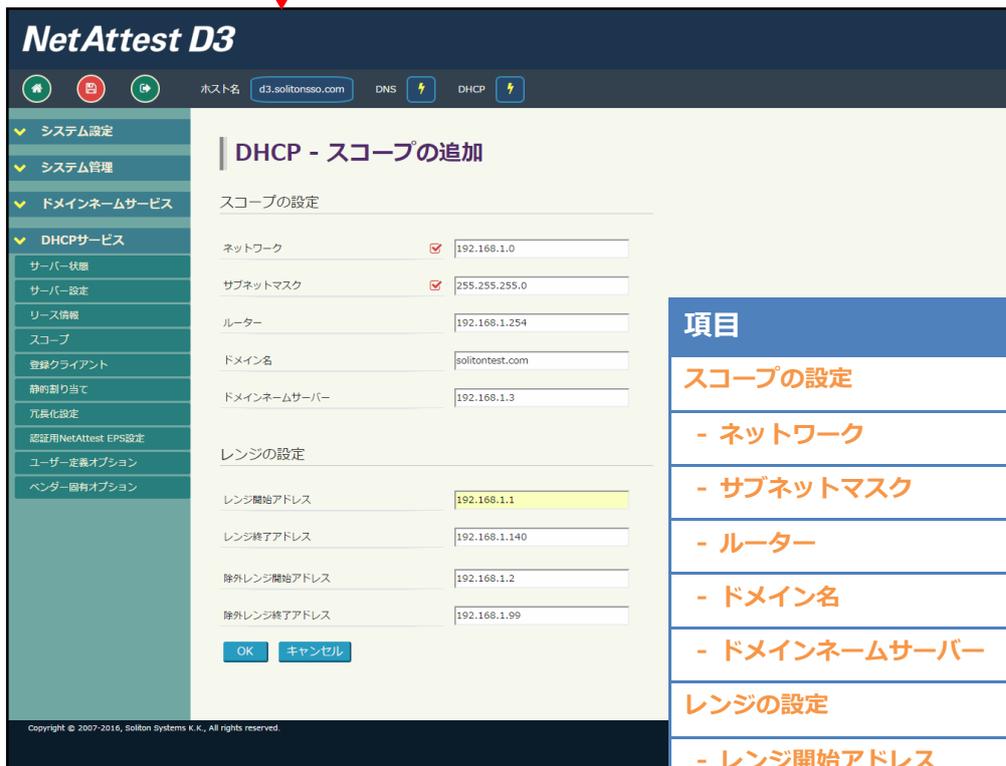
MR18 は、デフォルトでは DHCP から IP アドレスを取得するよう設定されています。しかし、EPS に RADIUS クライアントとして登録するためには IP アドレスを静的に指定する必要があります。今回は MR18 に静的に IP アドレスを割り当てるために、NetAttest D3 の静的割り当て機能を使用して IP アドレスを払い出すことにします。

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	solitontest.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

MR18 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 MR18 の MAC アドレスを確認します。MR18 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。
MR18 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: d3.solitonssso.com | DNS | DHCP

静的割り当て

表示するデータはありません

追加 CSVダウンロード CSVアップロード

NetAttest D3

ホスト名: d3.solitonssso.com | DNS | DHCP

DHCP - 静的割り当て - 追加/修正

ホスト名 m00180a6f2984

IPアドレス 192.168.1.1

MACアドレス 00:18:0A:6F:29:84

OK キャンセル

項目	値
ホスト名	M00180a6f2984 (任意)
IP アドレス	192.168.1.1
MAC アドレス	00:18:0A:6F:29:84

NetAttest D3

ホスト名: d3.solitonssso.com | DNS | DHCP

DHCP - 静的割り当て

	ホスト名	IPアドレス	MACアドレス	最終リリース日時
<input checked="" type="checkbox"/>	m00180a6f2984	192.168.1.1	00:18:0A:6F:29:84	2016-03-29 15:41:11
<input type="checkbox"/>	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

追加 削除 全削除 CSVダウンロード CSVアップロード

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。

The screenshot shows the NetAttest D3 management console. The left sidebar contains a menu with 'DHCPサービス' expanded, and 'サーバー状態' highlighted with a red box. The main content area is titled 'DHCP - サーバー状態' and shows the following information:

- 動作状態: 動作中
- サーバー稼働状態: 動作中
- 冗長化状態: 冗長化しない
- IP使用率(%): 0% (0 / 41 max)

At the bottom of the page, there are several control buttons: '起動' (Start), '停止' (Stop), '初期化' (Reset), 'リース情報全消去' (Clear all lease information), 'MACアドレス使用履歴全消去' (Clear all MAC address usage history), and '状態の更新' (Refresh status). The '起動' button is highlighted with a red box.

4. MR18 の設定

MR18 の設定はクラウド上の管理ページ[<http://dashboard.meraki.com>]から行います。

4-1 RADIUS 認証設定

[Network]に[(該当するネットワーク)]を選択し、[Wireless]-[Access control]より設定する SSID を選択し、RADIUS 認証の設定を行います。ここでは、

- 認証方式
- RADIUS 認証ポート
- アカウンティングポート
- クライアント IP の割当方法

を設定します。

The screenshot shows the Meraki dashboard interface for configuring RADIUS authentication. The left sidebar contains navigation options: Network-wide, Wireless (selected), Organization, and Help. The main content area is titled 'Access control' and shows the following settings:

- SSID:** SoftonLab
- Network access:**
 - Association requirements: WPA2-Enterprise with my RADIUS server (selected)
 - WPA encryption mode: WPA1 and WPA2
 - 802.11r: Disabled
- Splash page:** None (direct access) (selected)
- RADIUS servers:** A table with columns #, Host, Port, Secret, and Actions. One server is listed with Host 192.168.1.2 and Port 1812.
- RADIUS testing:** RADIUS testing disabled
- RADIUS accounting:** RADIUS accounting is enabled
- RADIUS accounting servers:** A table with columns #, Host, Port, Secret, and Actions. One server is listed with Host 192.168.1.2 and Port 1813.
- RADIUS attribute:** Filter-id
- Assign group policies by device type:** Disabled: do not assign group policies automatically

Addressing and traffic

Client IP assignment

- NAT mode: Use Meraki DHCP
Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit.
- Bridge mode: Make clients part of the LAN
Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.
- Layer 3 roaming
Clients receive DHCP leases from the LAN or use static IPs as in bridge mode. If they roam between APs their traffic will be forwarded to an AP on the same subnet they originally joined, so they will keep the same IP address.
- Layer 3 roaming with a concentrator
Clients are tunneled to a specified VLAN at the concentrator. They will keep the same IP address when roaming between APs.
- VPN: tunnel data to a concentrator
Meraki devices send traffic over a secure tunnel to an MX or VM concentrator.

Note: VPN and Layer 3 roaming with concentrator require an MX or VM concentrator. To use them, [add an MX](#), or [create a concentrator](#).

VLAN tagging

RADIUS override

Content filtering

Bonjour forwarding

Wireless options

Band selection

- Dual band operation (2.4 GHz and 5 GHz)
- 5 GHz band only
5 GHz has more capacity and less interference than 2.4 GHz, but legacy clients are not capable of using it.
- Dual band operation with Band Steering
Band Steering detects clients capable of 5 GHz operation and steers them to that frequency, while leaving 2.4 GHz available for legacy clients.

Minimum bitrate (Mbps)

Lower Density Higher Density

1 2 5.5 6 9 11 12 18 24 36 48 54

Maximum device compatibility

or

(Please allow 1-2 minutes for changes to take effect.)

© 2016 Cisco Systems, Inc. [privacy](#) - [terms](#) Last login: 18 days ago from your current IP address. Current session started: 5 minutes ago

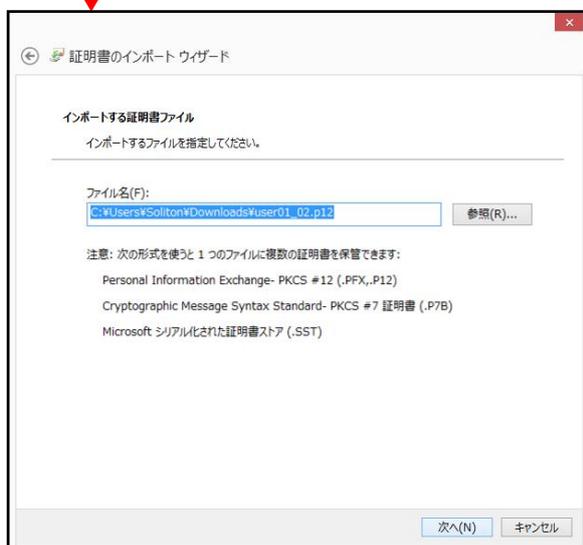
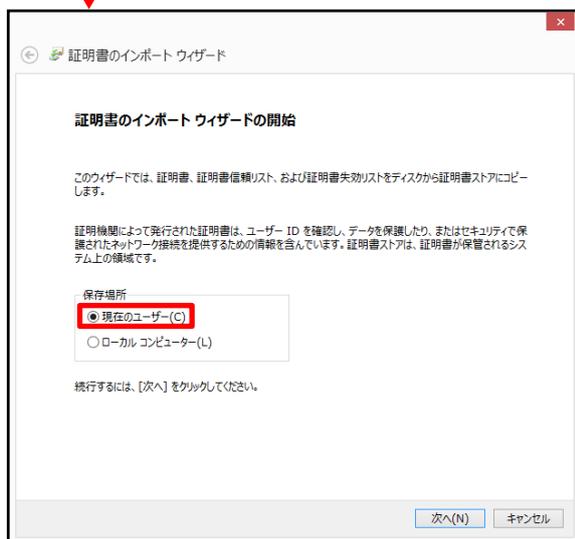
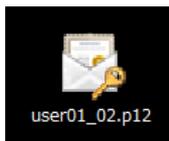
項目	値
Association requirements	WPA2-Enterprise with my RADIUS server
RADIUS server	192.168.1.2:1812 , secret
RADIUS accounting server	192.168.1.2:1813 , secret
Client IP assignment	Bridge mode: Make clients part of the VLAN

5. EAP-TLS 認証でのクライアント設定

5-1 Windows 8.1 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。



証明書のインポート ウィザード

秘密キーの保護
セキュリティを維持するために、秘密キーは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(I):

- 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。
- このキーをエクスポート可能にする(M)
キーの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

証明書のインポート 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

証明書のインポート 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\kuser01_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
認証モードを指定する	ユーザー認証



項目	値
接続のための認証方法	
- このコンピューターの・・・	On
- 単純な証明書の選択を・・・	On
証明書を検証してサーバーの・・・	On
信頼されたルート証明機関	TestCA

5-2 iOS(iPhone 6)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として、下記の方法などがあります。

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

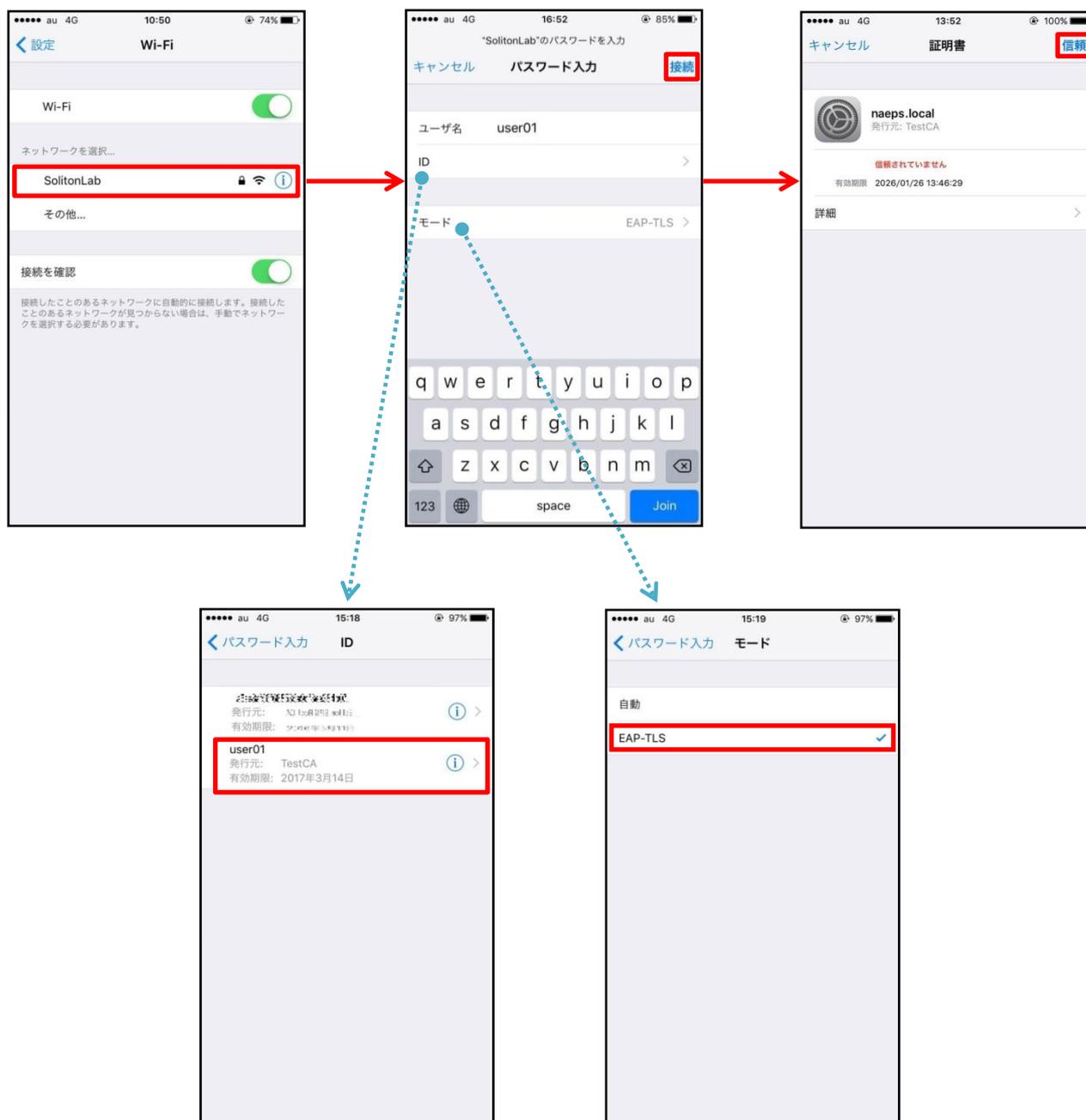
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

5-2-2 サプリカント設定

MR18 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、[ユーザー名]には証明書を発行したユーザーのユーザーID を入力します。次に[モード]より[EAP-TLS]を選択します。その後、[ユーザー名]の下の[ID]よりインポートされたクライアント証明書を選択します。

※初回接続時は「信頼されていません」と警告が出るので、「信頼」を選択し、接続します。



5-3 Android(Google Nexus 7)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。

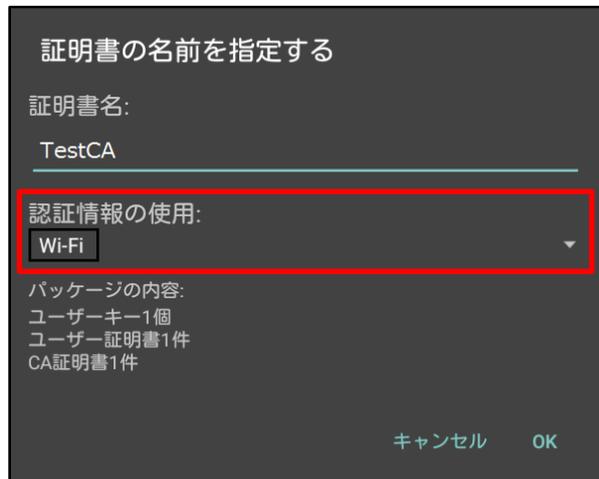
- 1) SD カードにクライアント証明書を保存し、インポートする方法※1
- 2) クライアント証明書をメールに添付し Android デバイスに送り、インポートする方法※2
- 3) SCEP で取得する方法(NetAttest EPS-ap を利用できます)※3

※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。

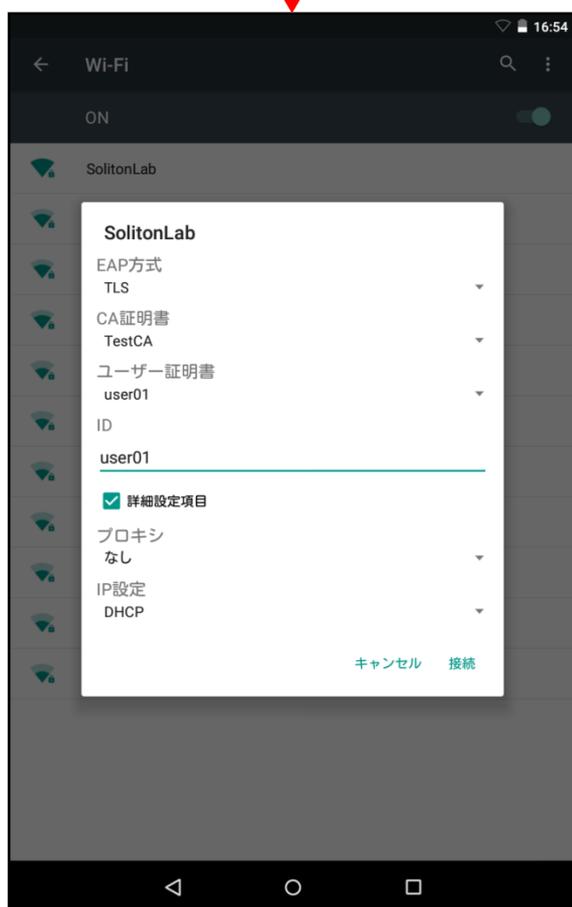
Android 5.1 では証明書インポート時に用途別に証明書ストアが選択できますが、本書では無線 LAN 接続を行うため[Wi-Fi]を選択しています。



5-3-2 サプリカント設定

MR18 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アカウントの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。

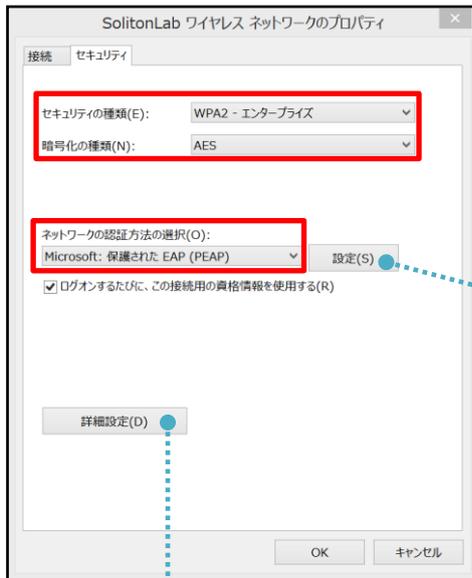


項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

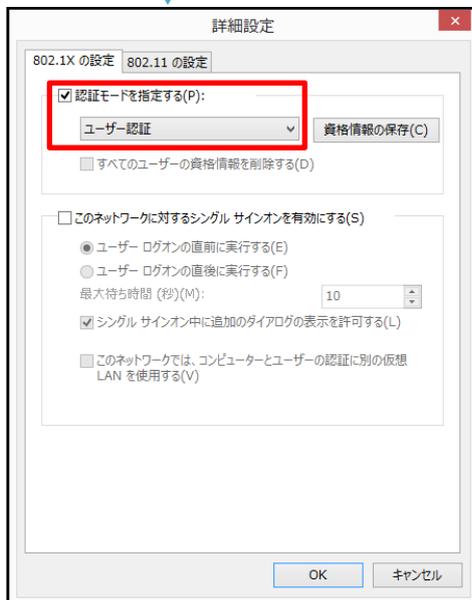
6. EAP-PEAP 認証でのクライアント設定

6-1 Windows 8.1 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	
- サーバ証明書の検証をする	On
- 信頼されたルート認証機関	TestCA

6-2 iOS(iPhone 6)のサブリカント設定

MR18 で設定した SSID を選択し、サブリカントの設定を行います。[ユーザー名]、[パスワード] には「2-4 ユーザー登録」で設定したユーザーID、パスワードを入力してください。

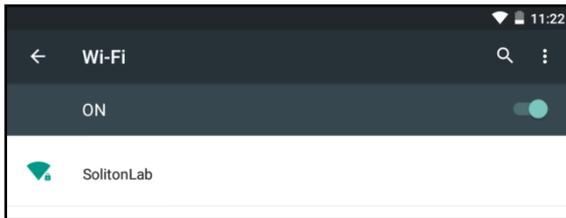
※初回接続時は「証明書が信頼されていません」と警告が出るので、「信頼」を選択し、接続します。



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

6-3 Android(Google Nexus 7)のサブリカント設定

MR18 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]には、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

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	Mar 29 16:27:38 naeps radiusd[2498]: notice 2016/03/29 16:27:38 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23)
MR18	2016/3/29 16:27, 00:18:0a:6f:29:84, SolitonLab, SolitonTestPC, 802.1X EAP success, radio: 1, vap: 2, client_mac: C0:33:5E:DF:2A:23""

7-2 EAP-PEAP(MS-CHAP V2)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	Mar 29 16:48:00 naeps radiusd[2498]: notice 2016/03/29 16:48:00 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23 via proxy to virtual server) Mar 29 16:48:00 naeps radiusd[2498]: notice 2016/03/29 16:48:00 Login OK: [user01] (from client RadiusClient01 port 0 cli C0-33-5E-DF-2A-23)
MR18	2016/3/29 16:48, 00:18:0a:6f:29:84, SolitonLab, SolitonTestPC, 802.1X EAP success, radio: 1, vap: 2, client_mac: C0:33:5E:DF:2A:23""

