

NetAttest EPS

認証連携設定例

【連携機器】 ハンドリームネット SubGate AP WSG-1200C

【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、ハンドリームネット社製無線アクセスポイント SubGate AP WSG-1200C 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 SubGate AP WSG-1200C 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.....	1
1-1 構成図.....	1
1-2 環境.....	2
1-2-1 機器.....	2
1-2-2 認証方式.....	2
1-2-3 ネットワーク設定.....	2
2. NetAttest EPS の設定.....	3
2-1 初期設定ウィザードの実行.....	3
2-2 システム初期設定ウィザードの実行.....	4
2-3 サービス初期設定ウィザードの実行.....	5
2-4 ユーザーの登録.....	6
2-5 クライアント証明書の発行.....	7
3. SubGate AP WSG-1200C の設定.....	8
3-1 IP アドレスおよびネットワークの設定.....	8
3-2 SSID 設定(2.4Ghz 基準).....	9
3-3 WiFi セキュリティ設定.....	10
4. EAP-TLS 認証でのクライアント設定.....	11
4-1 Windows 10 での EAP-TLS 認証.....	11
4-1-1 クライアント証明書のインポート.....	11
4-1-2 サブリカント設定.....	13
4-2 iOS での EAP-TLS 認証.....	14
4-2-1 クライアント証明書のインポート.....	14
4-2-2 サブリカント設定.....	15
4-3 Android での EAP-TLS 認証.....	16
4-3-1 クライアント証明書のインポート.....	16
4-3-2 サブリカント設定.....	17

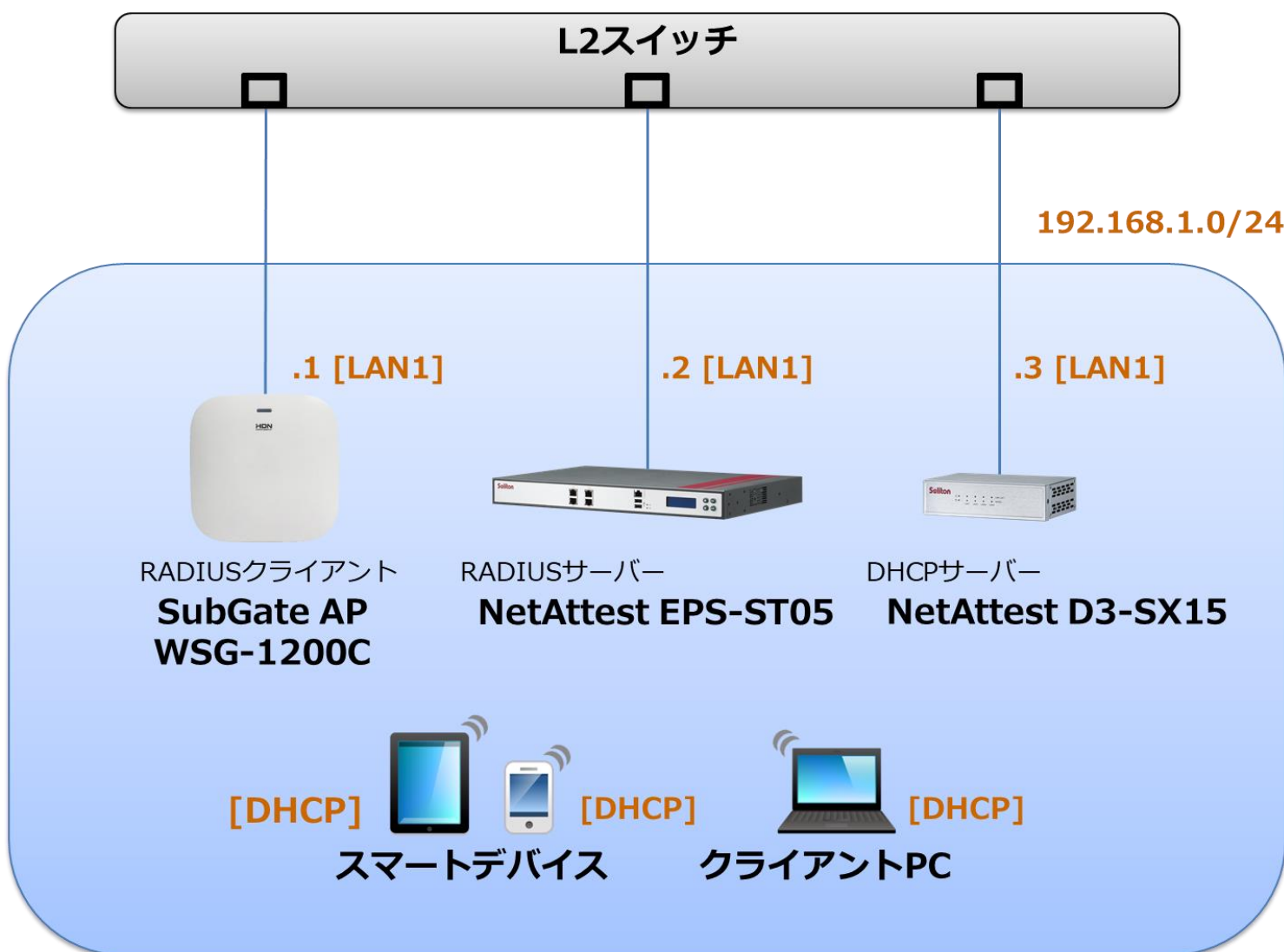
5. EAP-PEAP 認証でのクライアント設定.....	18
5-1 Windows 10 での EAP-PEAP 認証.....	18
5-1-1 Windows 10 のサブリカント設定	18
5-2 iOS での EAP-PEAP 認証.....	19
5-2-1 iOS のサブリカント設定.....	19
5-3 Android での EAP-PEAP 認証	20
5-3-1 Android のサブリカント設定.....	20
6. 動作確認結果	21
6-1 EAP-TLS 認証.....	21
6-2 EAP-PEAP 認証.....	21

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	4.10.5
SubGate AP WSG-1200C	ハンドリームネット	RADIUS クライアント (無線アクセスポイント)	1.0.3.build82
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブクライアント
iPhone 10	Apple	802.1X クライアント (Client SmartPhone)	13.1
Pixel C	Google	802.1X クライアント (Client Tablet)	8.1.0
NetAttest D3-SX15	ソリトンシステムズ	DHCP/DNS サーバー	4.2.19

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
SubGate AP WSG-1200C	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。

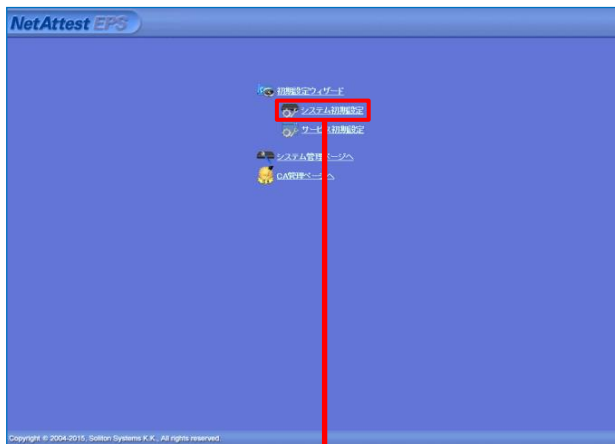
下記のような流れでセットアップを行います。

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

初期設定ウィザードを実行します。

- 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

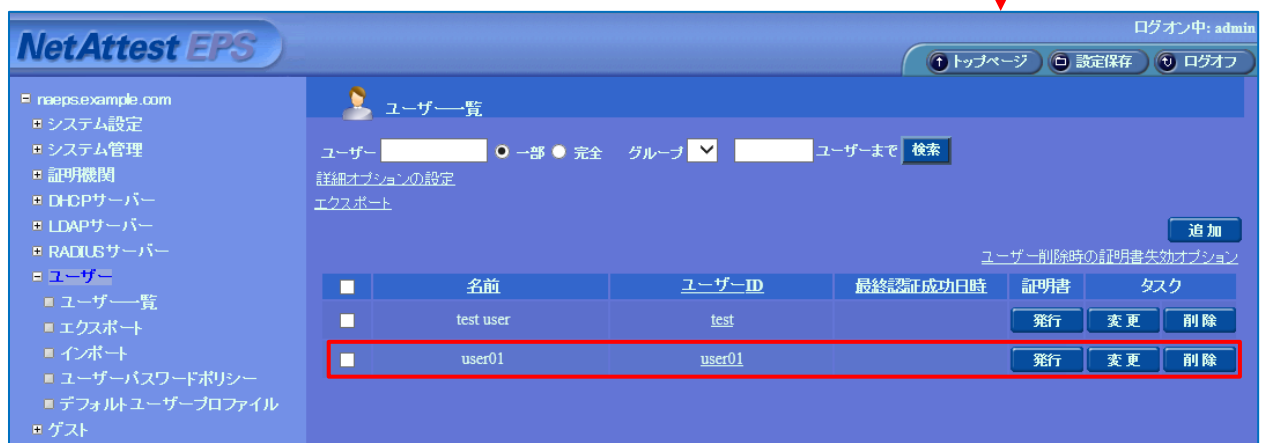
項目	値
NAS/RADIUS クライアント名	RadiusClient01
IP アドレス	192.168.1.1
シークレット	secret

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。



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.p12 という名前で保存)

NetAttest EPS ユーザー一覧画面のスクリーンショット。ユーザー一覧テーブルの「発行」ボタンが赤い枠で囲われ、赤い矢印が右側の詳細設定画面へと指している。

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

ユーザー詳細画面の「認証情報」セクションが黄色い枠で囲われ、有効期限が365日と設定されている。また、「発行」ボタンが赤い枠で囲われ、赤い矢印が右側のダウンロード画面へと指している。


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。ダウンロードボタンが赤い枠で囲われ、赤い矢印が右側のダウンロードボタンへと指している。

3. SubGate AP WSG-1200C の設定

3-1 IP アドレスおよびネットワークの設定

SubGate AP(WSG-1200C)は初期化状態で出荷されます。初期化状態の管理 IP アドレスは、172.31.255.1 です。



Network	
WAN	
<input checked="" type="checkbox"/> WAN Config	
IPアドレス	192.168.1.1
サブネットマスク	255.255.255.0
ゲートウェイ	192.168.1.254
DNSサーバ1	8.8.8.8
DNSサーバ2	8.8.4.4

項目	値
IPアドレス	192.168.1.1
サブネットマスク	255.255.255.0
ゲートウェイ	192.168.1.254

3-2 SSID 設定(2.4Ghz 基準)

SSID の指定を行います。

WiFi 使用	<input checked="" type="radio"/> 使用中 <small>② WiFi を使用中止するには、「使用しない」に設定してください。</small>
ネットワーク名(SSID)	<input type="text" value="solitonlab"/> × <input type="checkbox"/> Isolate <input type="checkbox"/> 隠し <small>② SSID が検索されないように設定するには、「隠し」オプションを設定してください。 ② 無線ユーザー間の通信を禁止するには、「Isolate」オプションを設定してください。</small>
VLAN ID	<input type="text" value="使用しない"/> <small>② Tag VLAN を使用するには、VLAN ID(3-4033)を入力してください。</small>
WiFiモード	<input type="button" value="Auto"/> ▾ <small>② 無線モードを設定してください。(Auto設定時混合モードで動作)</small>

項目	値
WiFi 使用	有効
ネットワーク名(SSID)	solitonlab

3-3 WiFi セキュリティ設定

暗号化方式と RADIUS サーバーを指定します。

WiFi Security

暗号化方式	<div style="border: 1px solid #ccc; padding: 2px;">WPA2-Enterprise ▾</div> <p><small>① 認証方法を選択します。 ② WPA2-Enterpriseを使用するには、RADIUSを追加で設定してください。</small></p>						
RADIUS Server	<p><input checked="" type="radio"/> 外部認証サーバー <input type="radio"/> embedded認証サーバー</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr style="background-color: #f0f0f0;"> <th style="width: 40%;">RADIUS Server IP</th> <th style="width: 15%;">Server Port</th> <th style="width: 45%;">アクセスパスワード</th> </tr> </thead> <tbody> <tr> <td style="padding: 2px;">192.168.1.2</td> <td style="padding: 2px;">1812</td> <td style="padding: 2px;">*****</td> </tr> </tbody> </table> <p><small>① 外部認証サーバーを使用するには、認証サーバーのIPアドレス,Port,アクセスパスワードを入力してください。</small></p>	RADIUS Server IP	Server Port	アクセスパスワード	192.168.1.2	1812	*****
RADIUS Server IP	Server Port	アクセスパスワード					
192.168.1.2	1812	*****					
WPA暗号化	<div style="border: 1px solid #ccc; padding: 2px;">TKIP and CCMP(AES) ▾</div> <p><small>① 暗号化方式を設定してください。</small></p>						
WPA共有キー	<div style="border: 1px solid #ccc; padding: 2px; background-color: #f0f0f0;"> ● </div> <p><small>① WPA共有キーを入力してください。</small></p>						

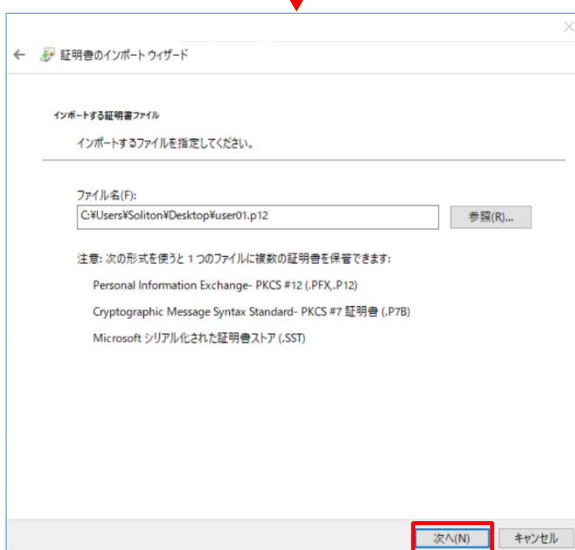
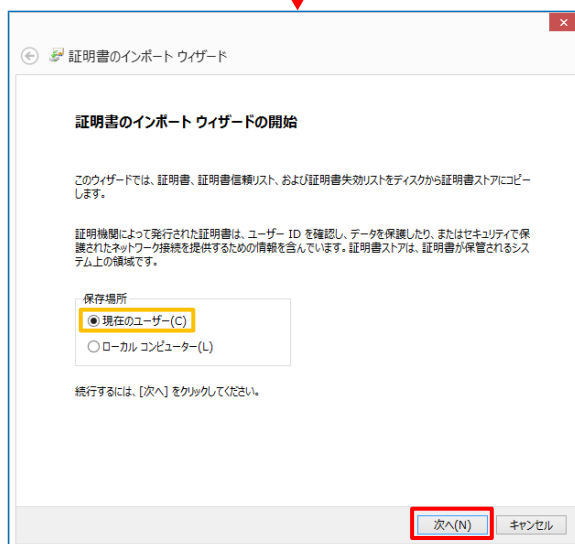
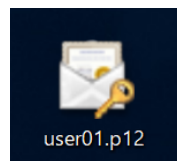
項目	値
暗号化方式	WPA2-Enterprise
RADIUS Server	外部認証サーバー
RADIUS Server IP	192.168.1.2
Server Port	1812
アクセスパスワード	secret

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:

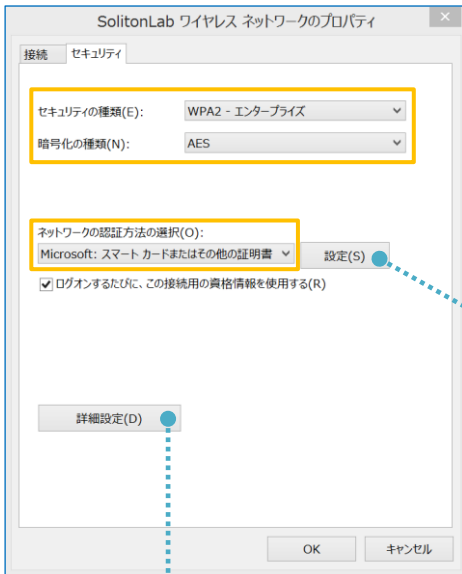
選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\Soliton\Downloads\User01_02.p12

完了(F) キャンセル

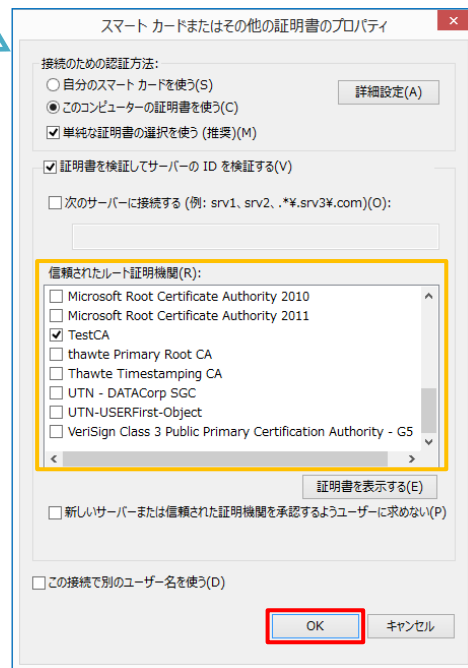
4-1-2 サプリカント設定

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
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

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)

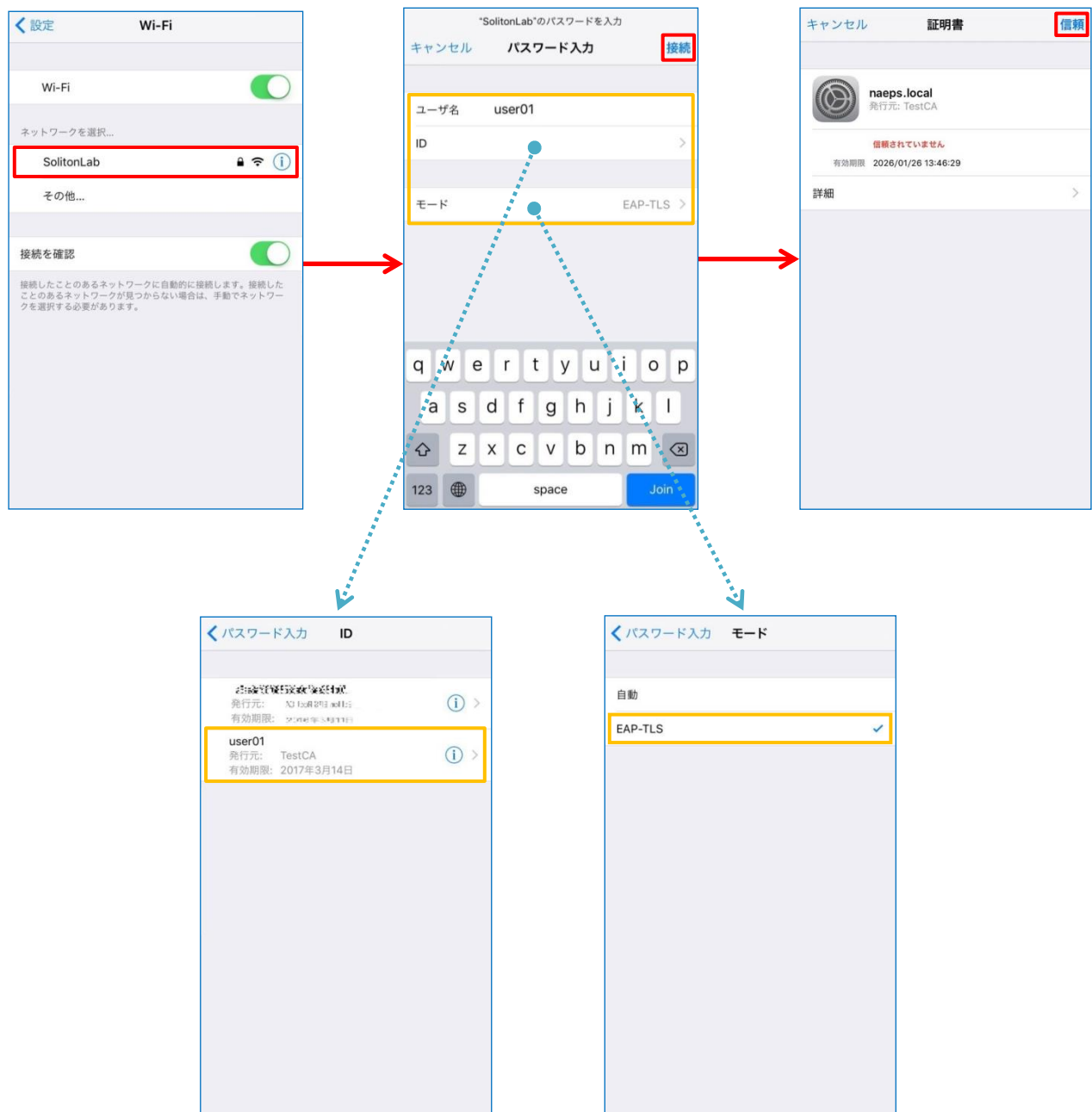
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

SubGate AP WSG-1200C で設定した SSID を選択し、サブ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

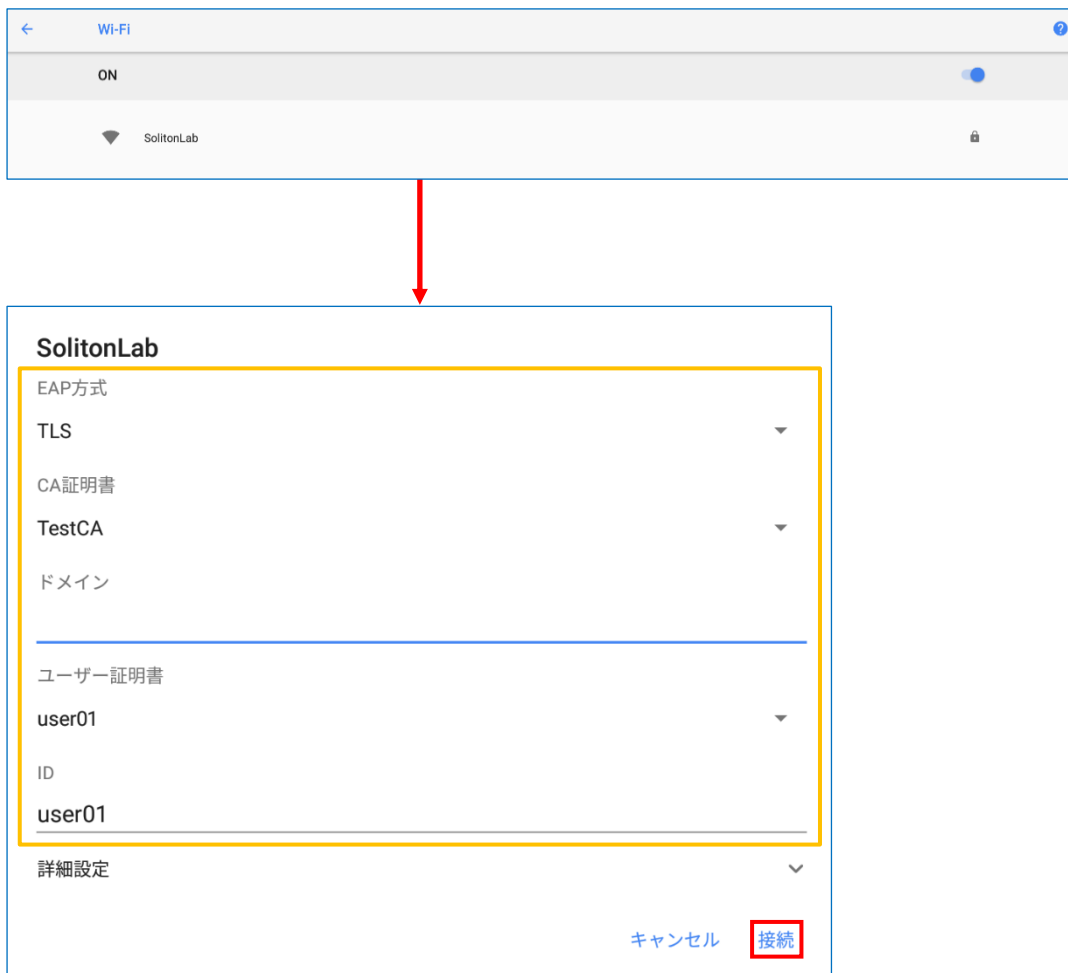
パッケージの内容:
ユーザーキー1個
ユーザー証明書1件
CA証明書1件

キャンセル

4-3-2 サプリカント設定

SubGate AP WSG-1200C 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。



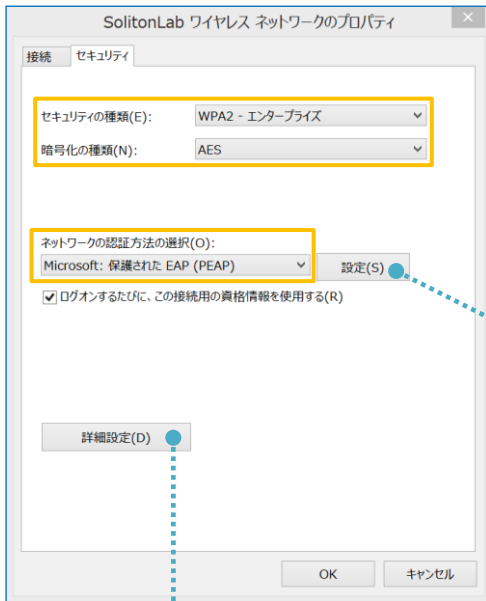
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

5. EAP-PEAP 認証でのクライアント設定

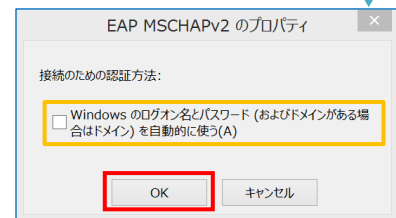
5-1 Windows 10 での EAP-PEAP 認証

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 のサブリカント設定

SubGate AP WSG-1200C 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

5-3 Android での EAP-PEAP 認証

5-3-1 Android のサブリカント設定

SubGate AP WSG-1200C 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。

The screenshot shows the Android Wi-Fi settings for a network named 'SolitonLab'. The configuration is as follows:

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

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 0 cli 40-A3-CC-32-10-A4)

The screenshot shows the 'クライアント情報' (Client Information) page in the Soliton web interface. The page is titled 'クライアント情報' and has a sub-header 'Client Information (2.4GHz)'. Below the header is a table with the following data:

No.	IP	MAC	SSID
1	192.168.1.101	40:A3:CC:32:10:A4	SolitonLab

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 0 cli 40-A3-CC-32-10-A4 via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 0 cli 40-A3-CC-32-10-A4)

The screenshot shows the 'クライアント情報' (Client Information) page in the Soliton web interface. The page is titled 'クライアント情報' and has a sub-header 'Client Information (2.4GHz)'. Below the header is a table with the following data:

No.	IP	MAC	SSID
1	192.168.1.101	40:A3:CC:32:10:A4	SolitonLab

