

NetAttest EPS

認証連携設定例

【連携機器】 シャープ株式会社 QX-C300 シリーズ

【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、シャープ社製無線アクセスポイント QX-C300 シリーズの 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 QX-C300 シリーズ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. QX-C300 の設定.....	10
3-1 QX-C300 へのログイン.....	10
3-2 IP アドレス設定.....	12
3-3 SSID の設定、Radius サーバーの設定.....	13
4. EAP-TLS 認証でのクライアント設定.....	16
4-1 Windows 10 での EAP-TLS 認証.....	16
4-1-1 クライアント証明書のインポート.....	16
4-1-2 サブリカント設定.....	18
4-2 iOS での EAP-TLS 認証.....	19
4-2-1 クライアント証明書のインポート.....	19
4-2-2 サブリカント設定.....	20
4-3 Android での EAP-TLS 認証.....	21
4-3-1 クライアント証明書のインポート.....	21
4-3-2 サブリカント設定.....	22
5. EAP-PEAP 認証でのクライアント設定.....	23
5-1 Windows 10 での EAP-PEAP 認証.....	23
5-1-1 Windows 10 のサブリカント設定.....	23
5-2 iOS での EAP-PEAP 認証.....	24

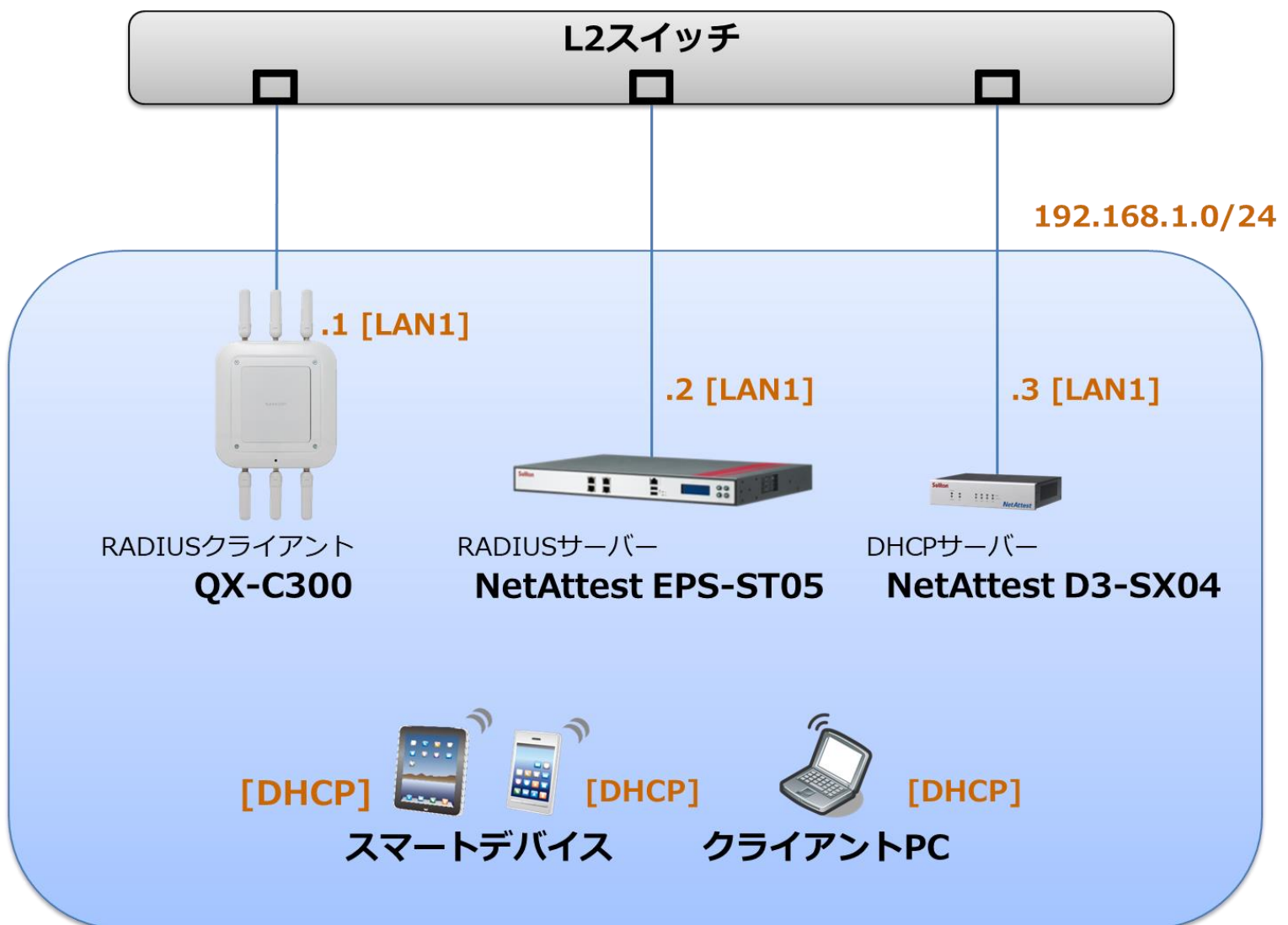
5-2-1 iOS のサブリカント設定	24
5-3 Android での EAP-PEAP 認証	25
5-3-1 Android のサブリカント設定	25
6. 動作確認結果	26
6-1 EAP-TLS 認証	26
6-2 EAP-PEAP 認証	26
6-3 端末接続情報	26

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	4.10.4
QX-C300	シャープ	RADIUS クライアント (無線アクセスポイント)	3.19.4.0
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 12.0
Pixel C	Google	802.1X クライアント (Client Tablet)	Android 8.1.0
NetAttest D3-SX04	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
QX-C300	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。

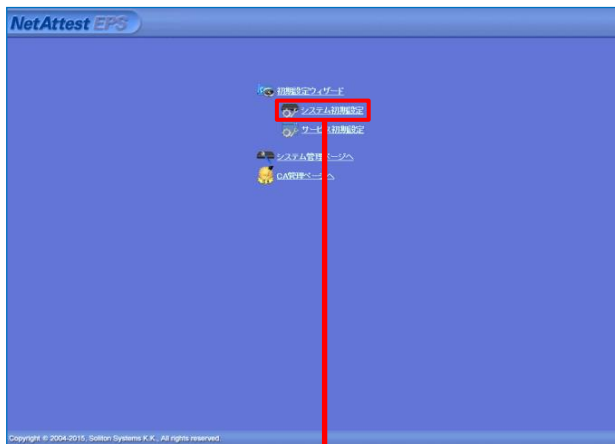
下記のような流れでセットアップを行います。

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

戻る 再起動

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

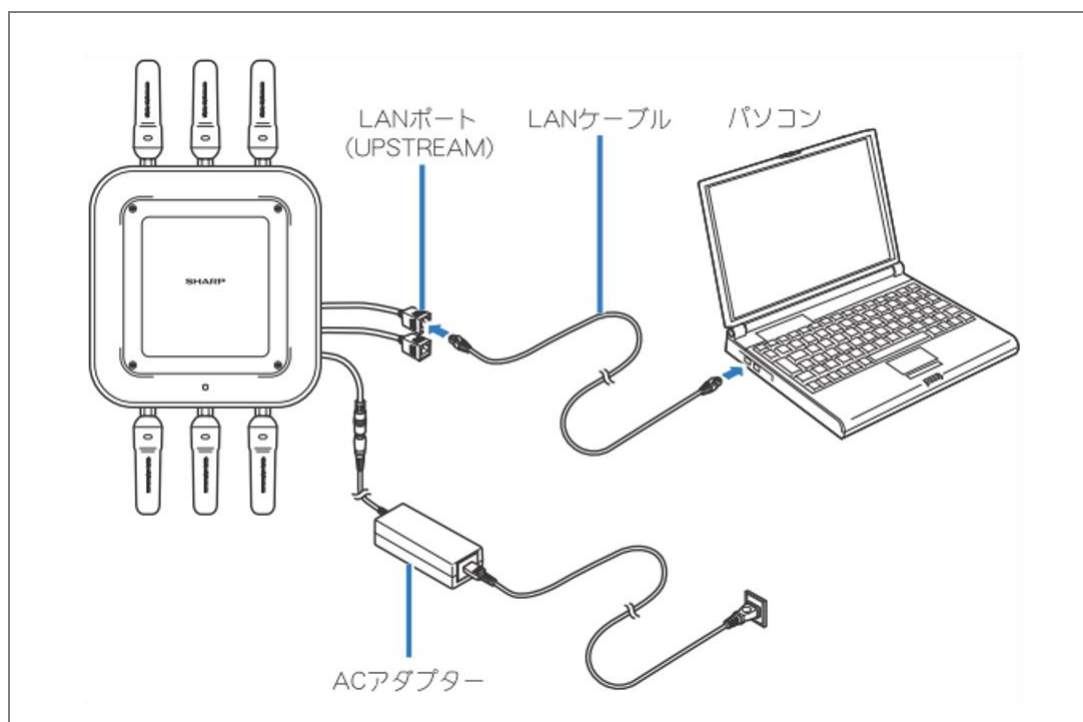
3. QX-C300 の設定

3-1 QX-C300 へのログイン

シャープの無線 LAN アクセスポイント、QX-C300 シリーズ (QX-C300、QX-C300J、QX-C300H、QX-C300JH) の設定は設定用 PC と有線 LAN で接続し、WebUI (設定画面) を利用して行います。本資料では代表して QX-C300 を使用し、設定を行います。

はじめに、設定用 PC に適切な IP を設定してください。購入時の QX-C300 の初期 IP アドレスは「192.168.0.10」、サブネットマスクは「255.255.255.0」に設定されています。

次に、QX-C300 の UPSTREAM 側の LAN ポートと設定用 PC を LAN ケーブルで接続し (下図)、その後 QX-C300 の電源を投入してください。QX-C300 の起動時に UPSTREAM 側がリンクアップするよう、あらかじめ設定用 PC を起動しておいてください。



本体前面のメインインジケータが青色になると起動が完了です。起動完了後、設定用 PC の Internet ブラウザから「http://192.168.0.10/」にアクセスしてください。

ログイン画面が表示されたら、アカウントを入力し、ログインをクリックしてください。

項目	値
アカウント	admin
パスワード	なし

ログインが成功すると以下の WebUI が表示されますので、以降の設定を行ってください。

3-2 IP アドレス設定

WebUI より IP アドレス設定を行います。

画面左側の [端末設定] をクリックし、[IP アドレス設定] にて設定を入力してください。

設定完了後、[保存] をクリックします。

SHARP WebUI IP アドレス設定画面のスクリーンショット。DHCP が OFF に設定されています。IP アドレス、サブネットマスク、デフォルトゲートウェイの入力欄が赤い枠で囲まれています。

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

確認ダイアログが表示されたら [OK] をクリックします。

確認ダイアログボックスのスクリーンショット。内容は「IPアドレス設定を変更すると、Webページを表示できない可能性があります。その場合は、設定したIPアドレスに接続してください。保存しますか？」。OK ボタンが赤い枠で囲まれています。

下記メッセージが表示されれば、IP アドレス設定は完了です。

通知メッセージボックスのスクリーンショット。内容は「保存しました」。OK ボタンが赤い枠で囲まれています。

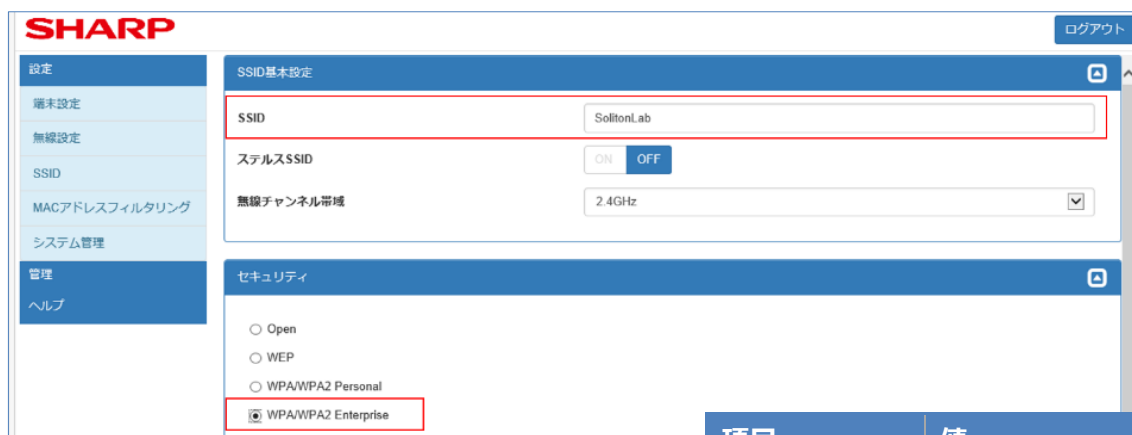
設定用 PC の IP アドレスを変更の上、Internet ブラウザから「<http://192.168.1.1/>」へアクセスし、再度ログインしてから以降の設定を行ってください。

3-3 SSID の設定、Radius サーバーの設定

WebUI より SSID を設定します。Radius サーバーは SSID 毎に設定することができます。
画面左側の[SSID]を選択し、[新規作成]をクリックします。



SSID の新規作成画面から、SSID 名、暗号化方式、RADIUS サーバーを設定します。
[SSID 基本設定]、[セキュリティ] にて以下を設定します。



項目	値
SSID	SolitonLab
セキュリティ	WPA/WPA2 Enterprise

[RADIUS サーバー] にて以下を設定します。



項目	値
IP アドレス	192.168.1.2
ポート番号	1812
共有鍵	secret

[RADIUS アカウンティングサーバー] にて以下を設定し、画面右下の [保存] をクリックします。



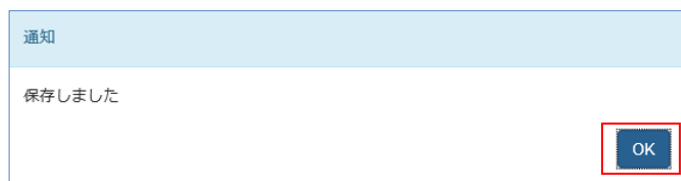
項目	値
IP アドレス	192.168.1.2
ポート番号	1813
共有鍵	secret

確認ダイアログが表示されたら [OK] をクリックします。

確認

保存しますか？

下記、通知ダイアログが表示されれば、SSID の設定は完了です。[OK] をクリックしてください。



上記設定は、EAP-TLS, EAP-PEAP 認証を行う場合の設定の一例です。

RADIUS サーバーによる MAC アドレス認証を行う場合は、[セキュリティ] の設定で、WPA/WPA2 Personal を選択し、[RADIUS サーバー] の設定で、[MAC ベース認証] を ON に設定してください。
(WPA/WPA2 Personal 設定が別途必要です。)

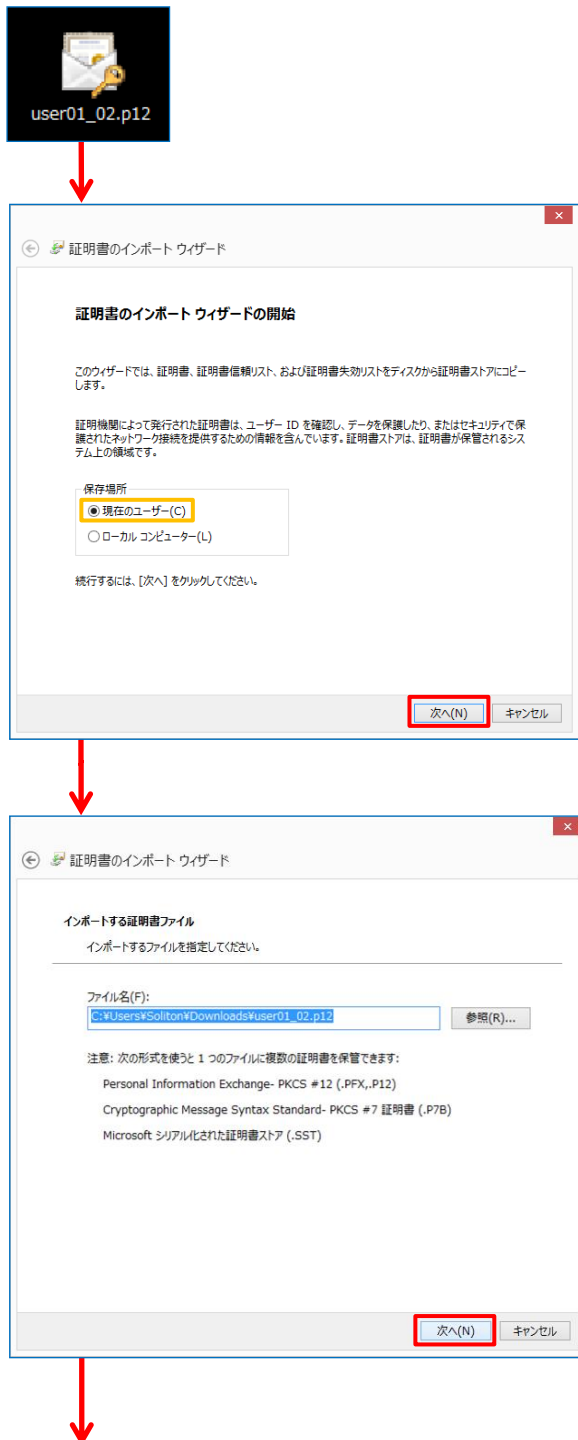
QX-C300 の設定は以上です。

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:

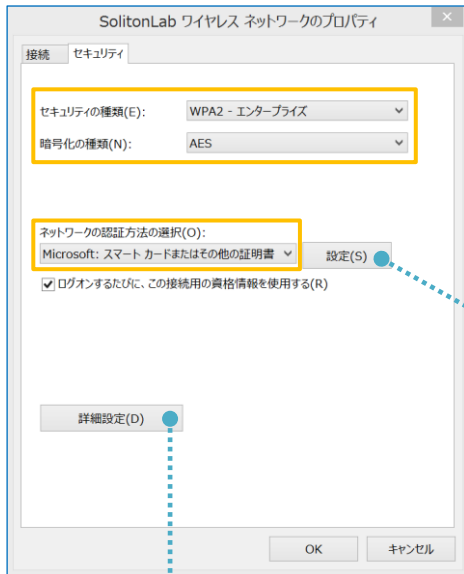
選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\Soliton\Downloads\User01_02.p12

完了(F) キャンセル

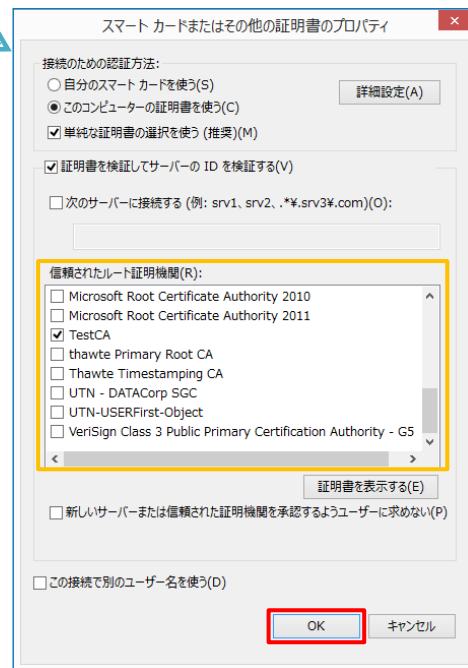
4-1-2 サプリカント設定

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)

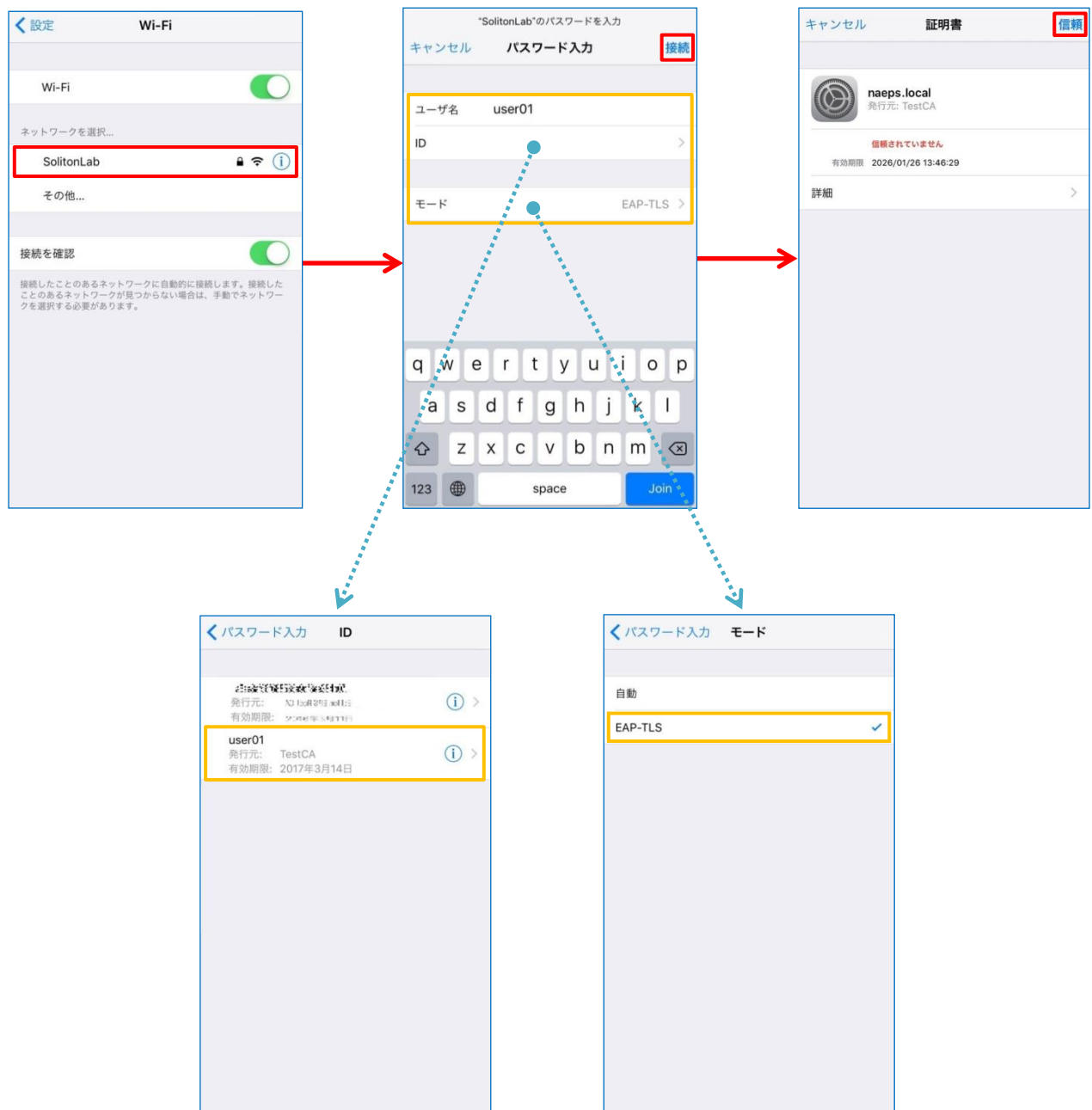
いずれかの方法で CA 証明書とクライアント証明書をインポートします。本書では割愛します。

4-2-2 サプリカント設定

QX-C300 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

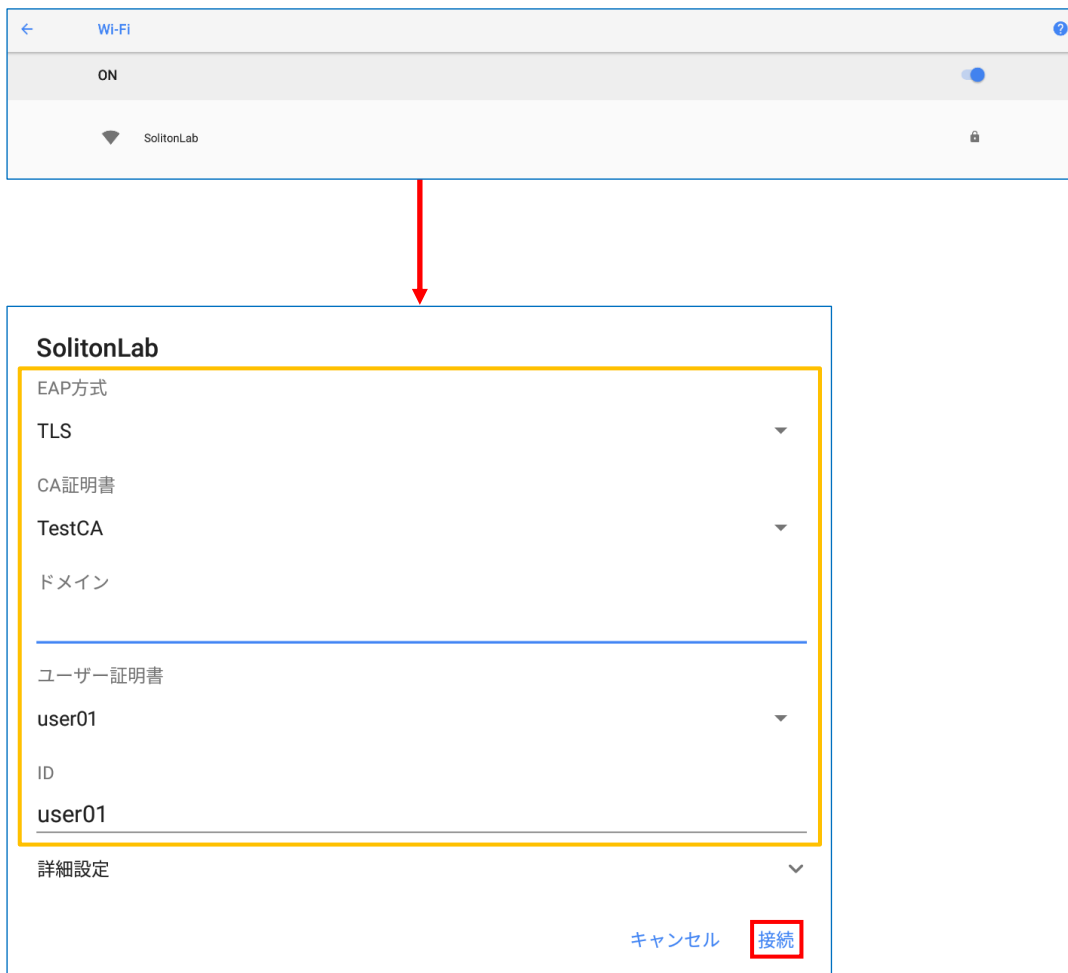
パッケージの内容:
ユーザーキー1個
ユーザー証明書1件
CA証明書1件

キャンセル

4-3-2 サプリカント設定

QX-C300 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」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。



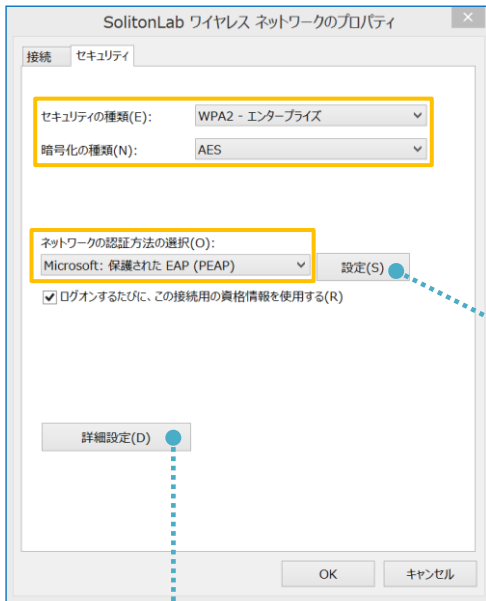
項目	値
EAP 方式	TLS
CA 証明書	TestCA
ユーザー証明書	user01
ID	user01

5. EAP-PEAP 認証でのクライアント設定

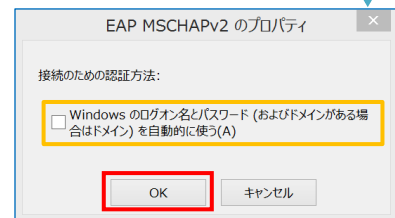
5-1 Windows 10 での EAP-PEAP 認証

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

QX-C300 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。

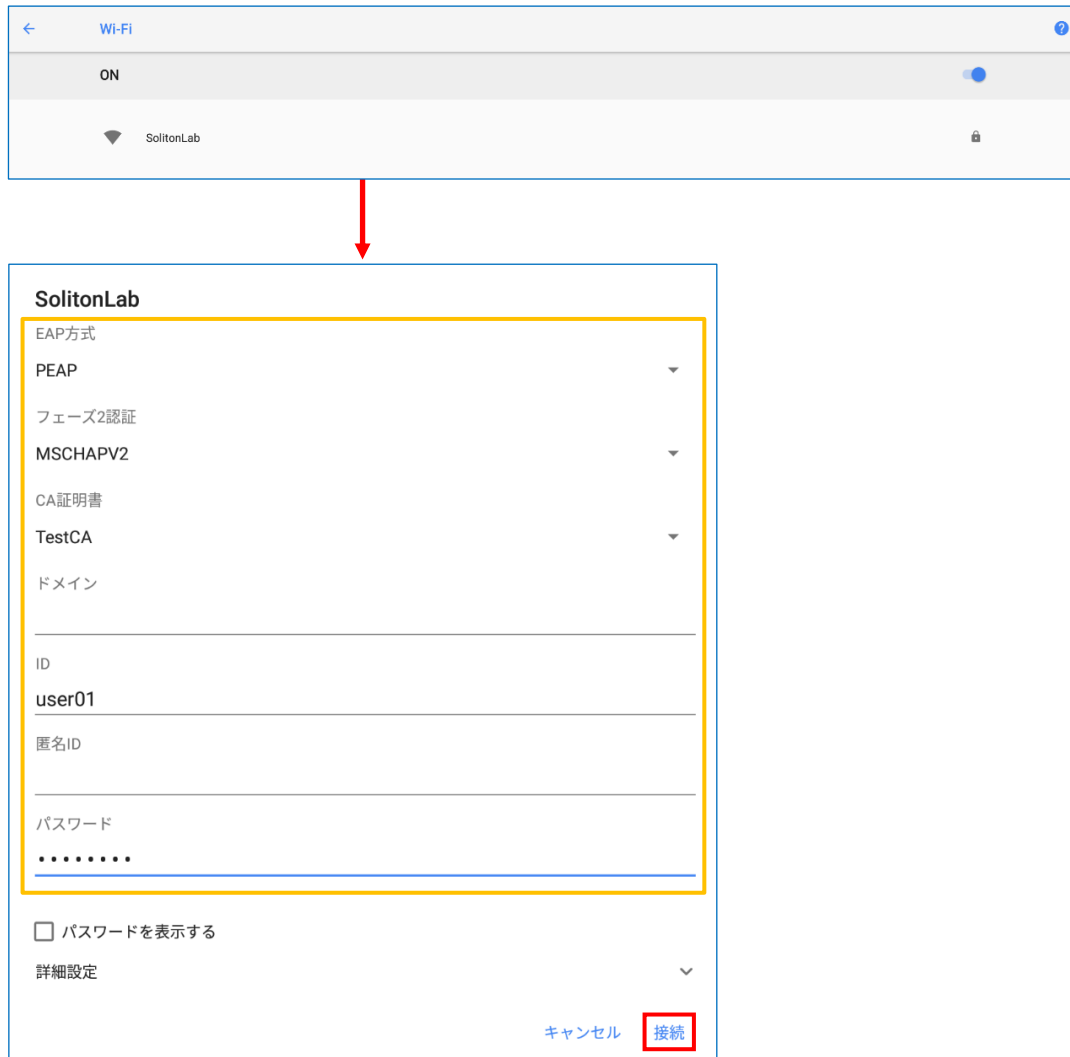


項目	値
ユーザ名	user01
パスワード	password
モード	自動

5-3 Android での EAP-PEAP 認証

5-3-1 Android のサブリカント設定

QX-C300 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 0 cli 40-A3-CC-32-10-A4)

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)

6-3 端末接続情報

QX-C300 で表示される接続情報



