

# **NetAttest EPS**

## 認証連携設定例

【連携機器】 アイ・オー・データ機器 BSH-GM シリーズ/BSH-GP08

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

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、アイ・オー・データ機器社製 L2 スイッチ BSH-GM シリーズ/BSH-GP08 の IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS 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 BSH-G08M 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

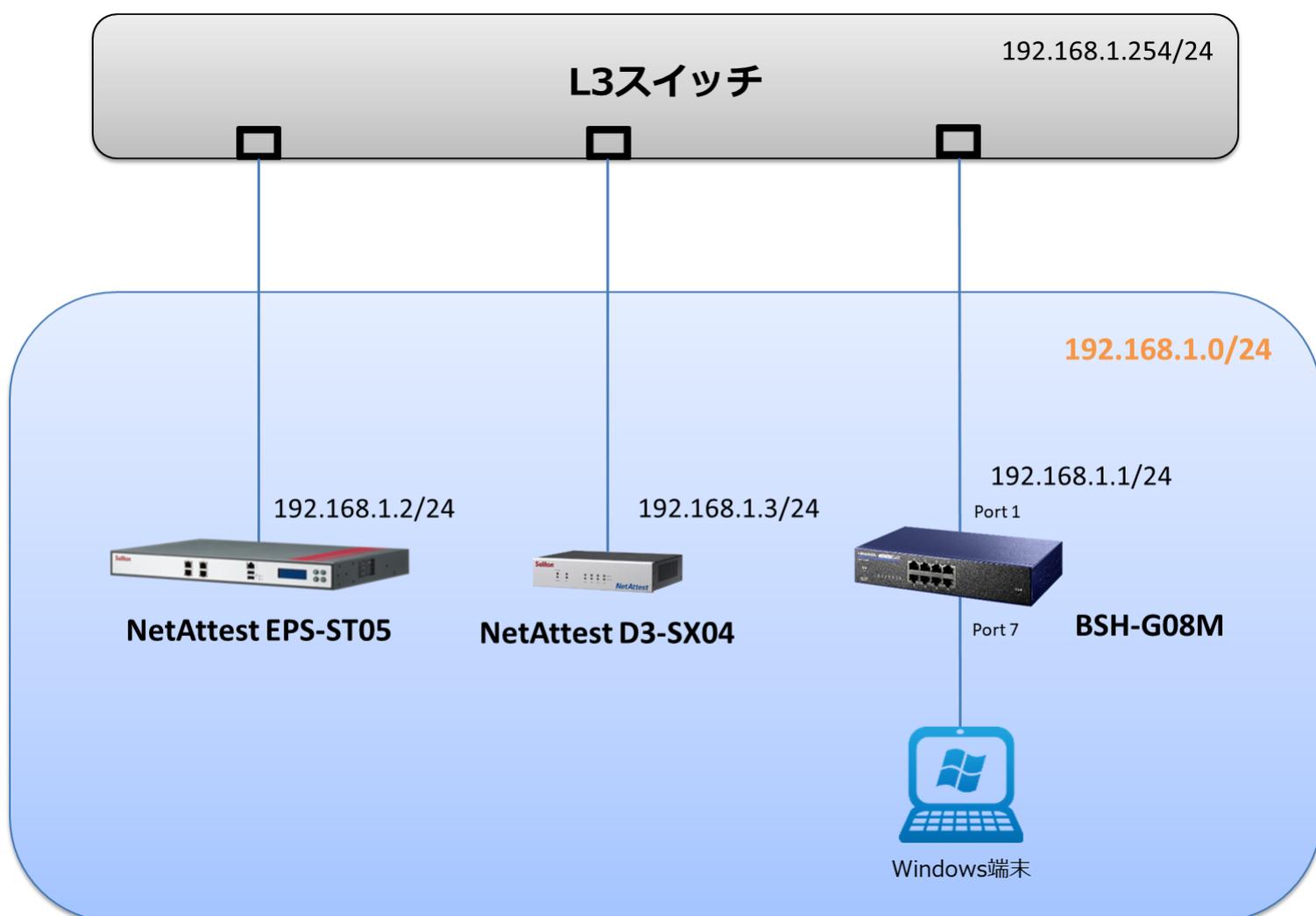
1. 構成.....	1
1-1 構成図.....	1
1-2 環境.....	2
1-2-1 機器.....	2
1-2-2 認証方式.....	2
1-2-3 ネットワーク設定.....	2
2. NetAttest EPS の設定.....	3
2-1 初期設定ウィザードの実行.....	3
2-2 システム初期設定ウィザードの実行.....	4
2-3 サービス初期設定ウィザードの実行.....	5
2-4 ユーザーの登録.....	6
2-5 クライアント証明書の発行.....	7
3. BSH-GM シリーズ/BSH-GP08 の設定.....	8
3-1 IP アドレスの設定.....	9
3-2 RADIUS サーバーの設定.....	10
4. Windows 10 のクライアント設定.....	13
4-1 EAP-PEAP 認証.....	13
4-2 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.....	16
5. 動作確認結果.....	17
5-1 EAP-PEAP 認証.....	17
5-2 EAP-TLS 認証.....	17

# 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 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
BSH-G08M	アイ・オー・データ機器	RADIUS クライアント (L2 スイッチ)	2.1.0
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブプリカント
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.16

### 1-2-2 認証方式

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

### 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
BSH-G08M	192.168.1.1/24		secret
Client PC	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

---

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
優先順位	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	192.168.10.1
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 user registration process in NetAttest EPS. It shows the 'ユーザー一覧' (User List) page with a table containing one user: 'test user' with ID 'test'. A red box highlights the '追加' (Add) button. An arrow points to the 'ユーザー設定' (User Settings) form, which is pre-filled with 'user01' for the name and ID, and 'password' for the password. A red box highlights the 'OK' button. Another arrow points back to the 'ユーザー一覧' page, where the 'user01' entry is now present in the table, highlighted with a red box.

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)

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. BSH-GM シリーズ/BSH-GP08 の設定

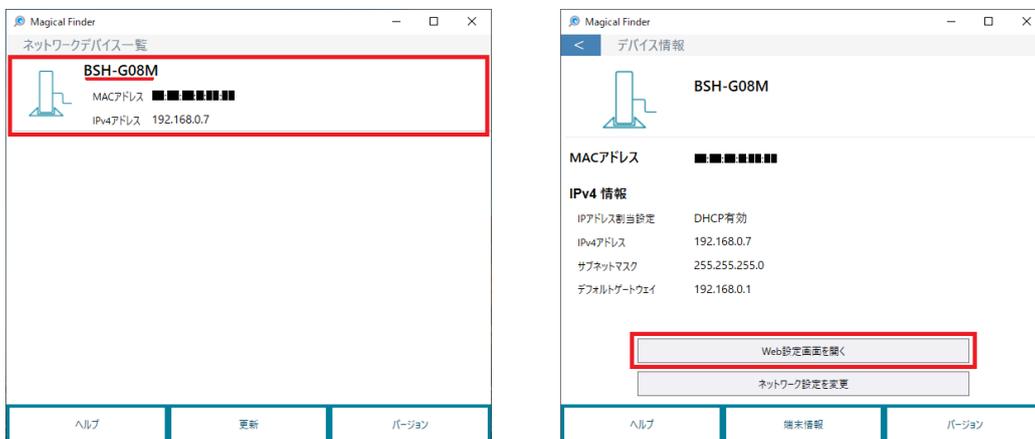
アイ・オー・データ製 L2 インテリジェントスイッチの BSH-GM シリーズおよび BSH-GP08 は同一の方法で設定が可能です。そのため本書では、代表して BSH-G08M を使用して設定を行います。購入時の IP アドレスは DHCP 設定となっていますので、専用ツール「Magical Finder」を使います。

「Magical Finder」は下記 Web ページにアクセスし、お使いの OS を選んでダウンロードします。

<http://www.iodata.jp/r/3022>

Magical Finder を起動すると、下記のように対象製品が表示されます。

設定を行う機器を選択し、「Web 設定画面を開く」をクリックして設定画面を起動します。



設定画面が起動したら、ユーザー名/パスワードを入力しログインします。

初期ユーザー名は admin(小文字)

パスワードは IODATA(大文字)です

ログイン

http://192.168.0.3  
このサイトへの接続ではプライバシーが保護されません

ユーザー名

パスワード

BSH-G08Mのセットアップは下記の流れで行います。

1. IP アドレスの設定
2. RADIUS サーバーの設定

## 3-1 IP アドレスの設定

[ネットワーク]-[IP アドレス]にアクセスし IP アドレスを設定します。

IP アドレス設定画面を開いたら以下の項目を設定します

IPv4アドレス

アドレスタイプ  スタティック  
 ダイナミック

IPv4アドレス 192.168.1.1

サブネットマスク 255.255.255.0

IPv4デフォルトゲートウェイ 192.168.1.254

DNSサーバー1

DNSサーバー2

IPv6アドレス

自動設定  有効

DHCPv6クライアント  有効

IPv6アドレス

プレフィックス長 0 (0 - 128)

IPv6デフォルトゲートウェイ

DNSサーバー1

DNSサーバー2

現在のステータス

IPv4アドレス 192.168.0.3

IPv4デフォルトゲートウェイ 192.168.0.1

IPv6アドレス ::

IPv6デフォルトゲートウェイ ::

リンクローカルアドレス fe80::3676:c5ff:feff:3a1f/64

適用

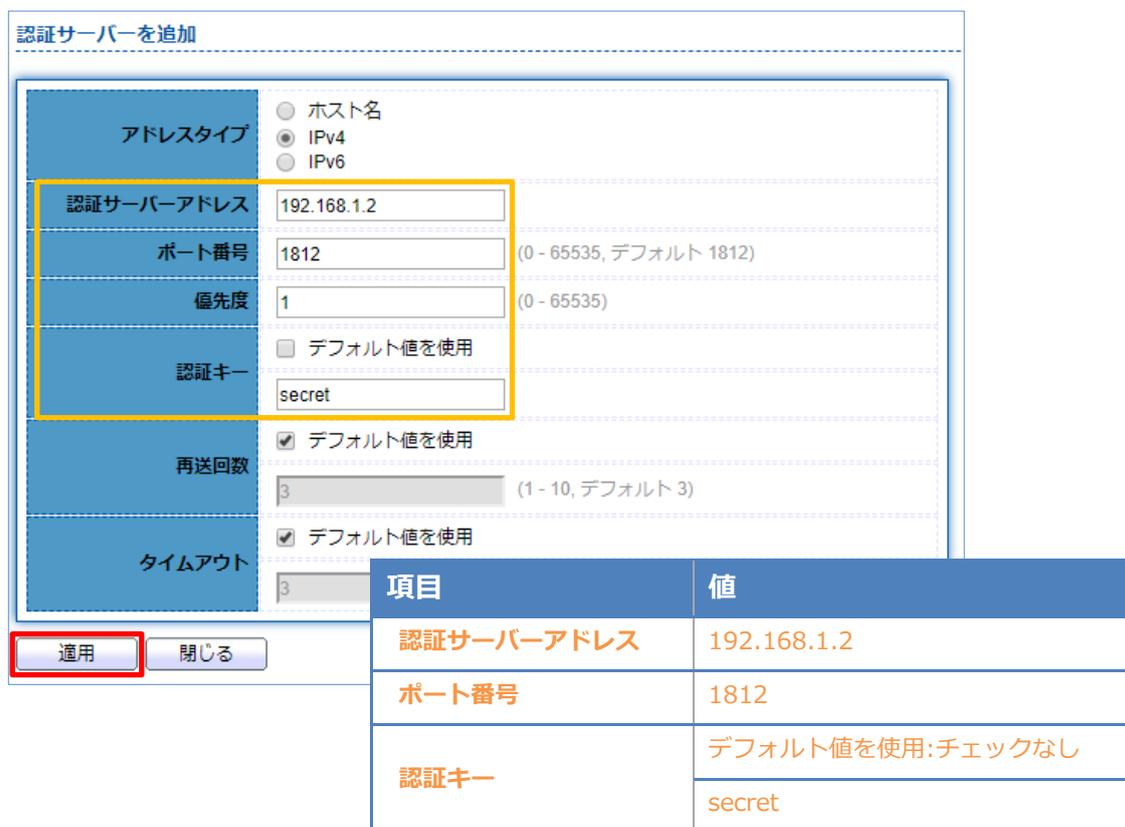
項目	値
アドレスタイプ	スタティック
IPv4 アドレス	192.168.1.1
サブネットマスク	255.255.255.0
IPv4 デフォルトゲートウェイ	192.168.1.254

## 3-2 RADIUS サーバーの設定

認証サーバーの設定をします。設定画面より[RADIUS 認証]-[認証サーバー設定]を選択します。  
 認証サーバーテーブルの設定画面が表示されるので「追加」を選択します。



認証サーバーの追加画面が表示されるので必要項目を入力します。



設定画面より[RADIUS 認証]-[オーセンティケータ設定]-[プロパティ]を選択します。

ポートモードテーブルの設定画面が表示されるので「802.1x 認証」にチェックを付け適用します。

認証対象の端末を接続するポートを選択し、「編集」をクリックします。

The screenshot shows the configuration interface. On the left, a sidebar menu has 'RADIUS認証' (RADIUS authentication), 'オーセンティケータ設定' (Authenticator settings), and 'プロパティ' (Properties) highlighted with red boxes. The main area shows the 'Authenticator settings' for '802.1x authentication'. The 'MAC address format' is set to 'XXXXXXXXXXXX'. Below this is a 'Port Mode Table' with the following data:

No.	ポート	認証方法		ホストモード	優先順位	
		802.1x認証	MAC認証			
<input type="checkbox"/>	1	GE1	無効	無効	マルチ認証	802.1x認証
<input type="checkbox"/>	2	GE2	無効	無効	マルチ認証	802.1x認証
<input type="checkbox"/>	3	GE3	無効	無効	マルチ認証	802.1x認証
<input type="checkbox"/>	4	GE4	無効	無効	マルチ認証	802.1x認証
<input type="checkbox"/>	5	GE5	無効	無効	マルチ認証	802.1x認証
<input type="checkbox"/>	6	GE6	無効	無効	マルチ認証	802.1x認証
<input checked="" type="checkbox"/>	7	GE7	無効	無効	マルチ認証	802.1x認証
<input type="checkbox"/>	8	GE8	無効	無効	マルチ認証	802.1x認証

編集をクリックするとポートモードの編集画面が表示されるので、認証方法の「802.1x 認証」にチェックを付けます。優先順位の適用一覧に「802.1x 認証」が入っていることを確認し、適用します。

The 'Edit Port Mode' dialog box shows the configuration for port GE7. The 'Authenticator method' is set to '802.1x authentication' (checked). The 'Host mode' is set to 'Multi-authentication'. The 'Priority' section shows '802.1x authentication' in the 'Apply list' (高順位) and 'MAC authentication' in the 'Candidate list' (候補一覧). The 'Apply' button is highlighted with a red box.

設定画面より[RADIUS 認証]-[オーセンティケータ設定]-[ポート設定]を選択します。

ポート設定テーブル

No.	ポート	ポート制御	再認証	最大ホスト数	一般タイマー			802.1xパラメーター				
					再認証	非アクティブ	待機時間	TX期間	サブリカントタイムアウト	サーバータイムアウト	最大リクエスト数	
<input type="checkbox"/>	1 GE1	無効	無効	256	3600	60	60	30	30	30	30	2
<input type="checkbox"/>	2 GE2	無効	無効	256	3600	60	60	30	30	30	30	2
<input type="checkbox"/>	3 GE3	無効	無効	256	3600	60	60	30	30	30	30	2
<input type="checkbox"/>	4 GE4	無効	無効	256	3600	60	60	30	30	30	30	2
<input type="checkbox"/>	5 GE5	無効	無効	256	3600	60	60	30	30	30	30	2
<input checked="" type="checkbox"/>	6 GE6	無効	無効	256	3600	60	60	30	30	30	30	2
<input checked="" type="checkbox"/>	7 GE7	無効	無効	256	3600	60	60	30	30	30	30	2
<input type="checkbox"/>	8 GE8	無効	無効	256	3600	60	60	30	30	30	30	2

編集

表示されるポート設定テーブルにて認証対象の端末を接続するポートを選択し、「編集」をクリックします。ポート設定の編集画面が表示されるので、ポート制御の「自動」を選択し適用します。

ポート設定を編集

ポート: GE7

ポート制御:  無効  強制的に認証する  強制的に認証しない  自動

再認証:  有効

最大ホスト数: 256 (1 - 256, デフォルト 256)

一般タイマー

再認証: 3600 秒 (300 - 4294967294, デフォルト 3600)

非アクティブ: 60 秒 (60 - 65535, デフォルト 60)

待機時間: 60 秒 (0 - 65535, デフォルト 60)

802.1xパラメーター

TX期間: 30 秒 (1 - 65535, デフォルト 30)

サブリカントタイムアウト: 30 秒 (1 - 65535, デフォルト 30)

サーバータイムアウト: 30 秒 (1 - 65535, デフォルト 30)

最大リクエスト数: 2 (1 - 10, デフォルト 2)

適用 閉じる

以上で BSH-G08M の設定は完了です。

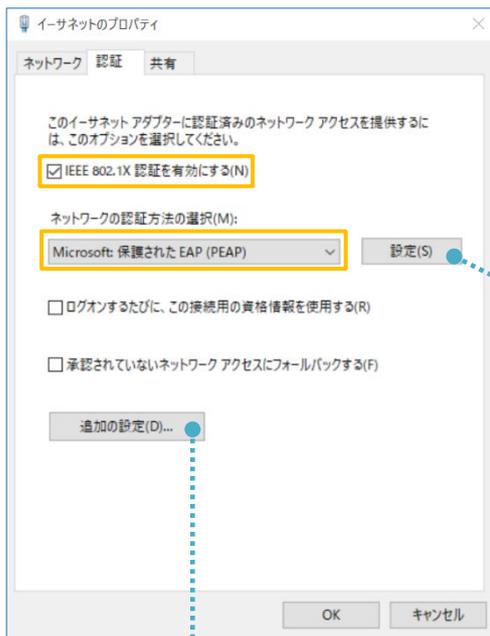
# 4. Windows 10 のクライアント設定

## 4-1 EAP-PEAP 認証

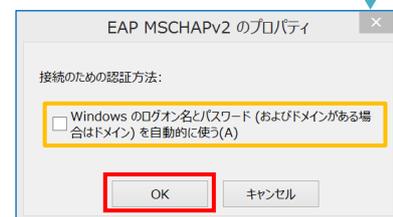
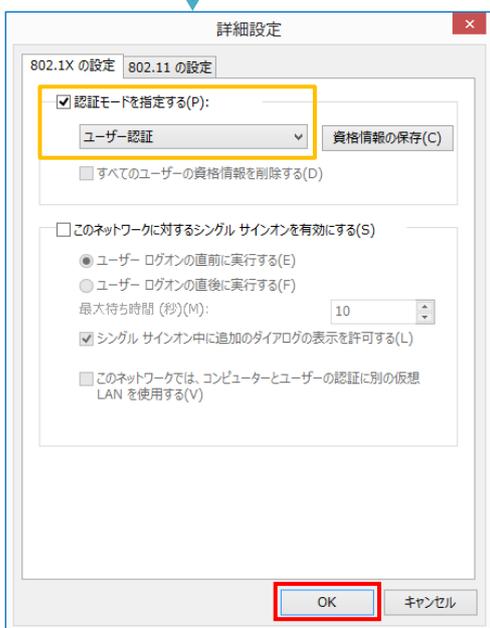
Windows 標準サブリカントで PEAP の設定を行います。

※ 本設定を行う前に「Wired AutoConfig」サービスが起動されていることをご確認ください。

[イーサネットのプロパティ] の [認証] タブから以下の設定を行います。



項目	値
IEEE 802.1X 認証を・・・	有効
ネットワークの認証・・・	Microsoft: 保護された EAP



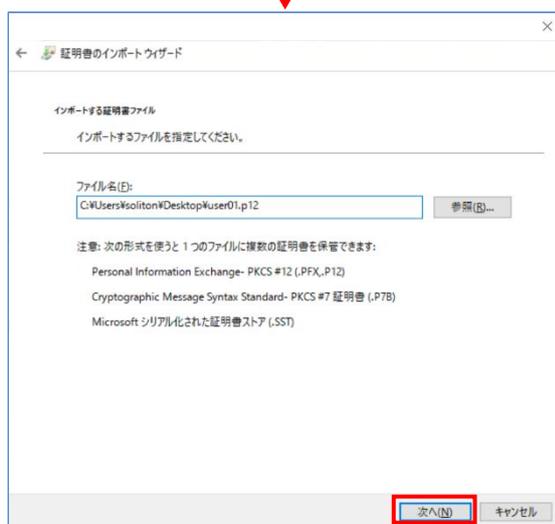
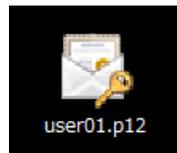
項目	値
認証モードを指定する	ユーザー認証

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

## 4-2 EAP-TLS 認証

### 4-2-1 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.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(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省略する(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	PFK
ファイル名	C:\Users\Soliton\Desktop\User01.p12

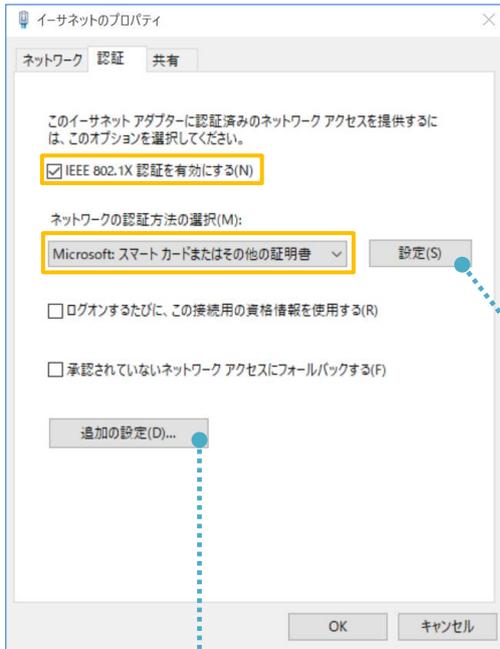
完了(F) キャンセル

## 4-2-2 サプリカント設定

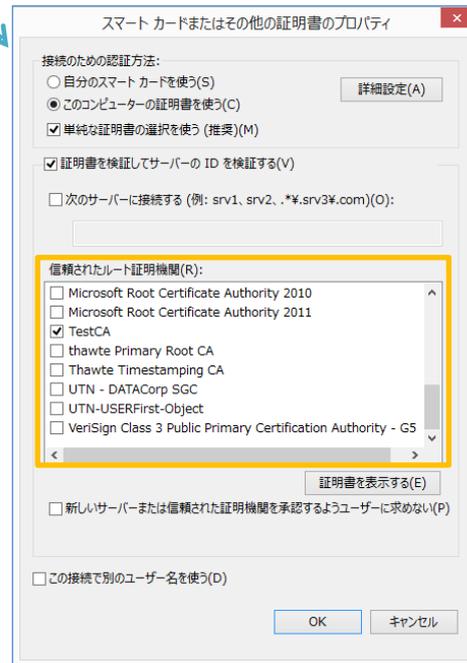
Windows 標準サプリカントで TLS の設定を行います。

※ 本設定を行う前に「Wired AutoConfig」サービスが起動されていることをご確認下さい。

[イーサネットのプロパティ] の [認証] タブから以下の設定を行います。



項目	値
IEEE 802.1X 認証を有効にする	有効
ネットワークの認証方式の選択	Microsoft:スマートカード または他の証明書



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使う	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 を検証する	On
信頼されたルート証明機関	TestCA

## 5. 動作確認結果

### 5-1 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 1 cli CC-30-80-32-8B-AF via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)
BSH-GM シリーズ/ BSH-GP08	802.1x authentication successful for client CC:30:80:32:8B:AF on GigabitEthernet7

### 5-2 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 1 cli CC-30-80-32-8B-AF)
BSH-GM シリーズ/ BSH-GP08	802.1x authentication successful for client CC:30:80:32:8B:AF on GigabitEthernet7

