

# ***NetAttest EPS***

## 認証連携設定例

【連携機器】 BUFFALO BS-GS2016

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

EAP-TLS/EAP-TLS+ダイナミックVLAN

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、BUFFALO 社製 L2 スイッチ BS-GS2016 の IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN 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 BS-GS2016 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.....	2
1-1 構成図 .....	2
1-2 環境.....	3
1-2-1 機器 .....	3
1-2-2 認証方式 .....	3
1-2-3 ネットワーク設定.....	3
2. NetAttest EPS の設定 .....	4
2-1 初期設定ウィザードの実行 .....	4
2-2 システム初期設定ウィザードの実行.....	5
2-3 サービス初期設定ウィザードの実行.....	6
2-4 ユーザーの登録.....	7
2-5 ユーザーのリプライアイテムの設定.....	8
2-6 クライアント証明書の発行 .....	9
3. BS-GS2016 の設定 .....	10
3-1 IP アドレスの設定 .....	11
3-2 VLAN の設定 .....	12
3-2-1 VLAN10 の作成.....	12
3-2-2 VLAN20 の作成.....	13
3-2-3 PVID の設定 .....	14
3-2-4 VLAN 1 を修正 .....	14
3-3 RADIUS サーバーの設定 .....	15
3-3-1 RADIUS サーバーの IP アドレス設定 .....	15
3-3-2 認証ポートの設定.....	16
4. Windows 10 のクライアント設定.....	17
4-1 EAP-PEAP 認証.....	17
4-2 EAP-TLS 認証 .....	18
4-2-1 クライアント証明書のインポート.....	18
4-2-2 サブリカント設定.....	20
5. 動作確認結果 .....	21
5-1 EAP-PEAP 認証.....	21

---

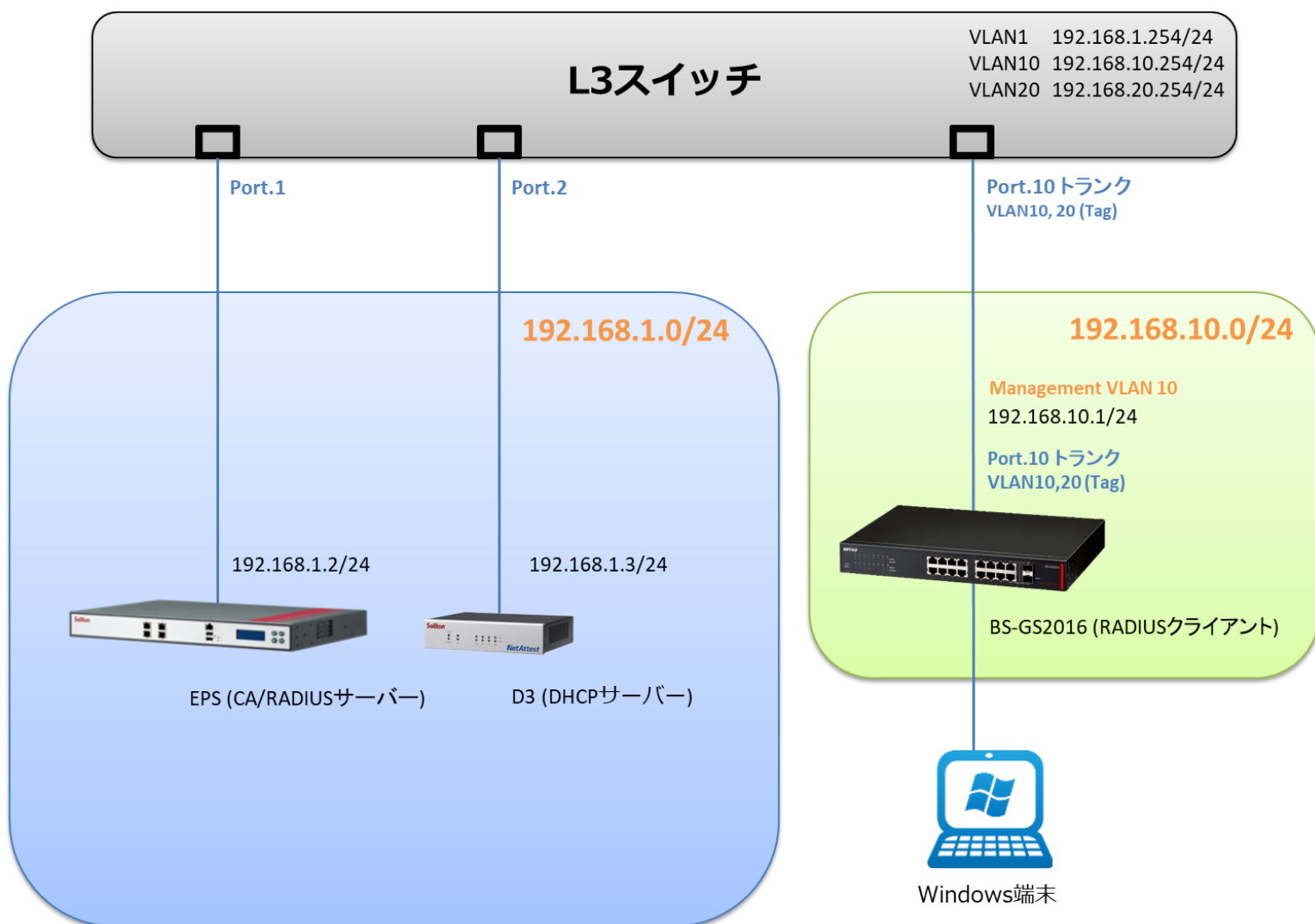
5-2 EAP-TLS 認証 .....	21
5-3 EAP-TLS+ダイナミック VLAN 認証 .....	22
付録 L3 スイッチの設定 .....	24
ポート設定、DHCP リレー設定 .....	24

# 1. 構成

## 1-1 構成図

以下の環境を構成します。

- ・ L3 スイッチには VLAN1、VLAN10、VLAN20 の 3 つの VLAN を作成する
- ・ 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
- ・ 各 VLAN の設計および用途は以下とする。
  - VLAN1 : 192.168.1.0/24 (EPS、D3、認証のみ/user03 用)
  - VLAN10 : 192.168.10.0/24 (ダイナミック VLAN/user01 用)
  - VLAN20 : 192.168.20.0/24 (ダイナミック VLAN/user02 用)



## 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
BS-GS2016	BUFFALO	RADIUS クライアント (L2 スイッチ)	1.0.3.43
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブライアント
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-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN

### 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
BS-GS2016	192.168.10.1/24		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

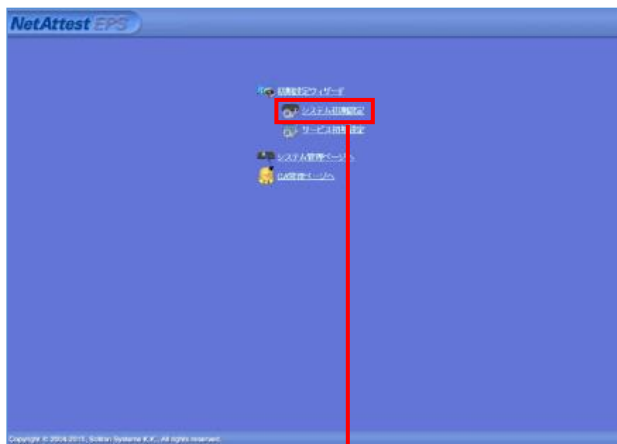


## 2-2 システム初期設定ウィザードの実行

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

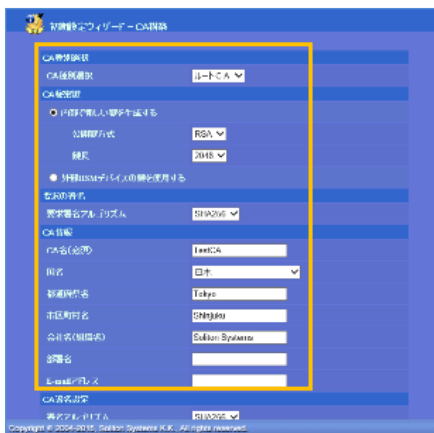
Copyright © 2004-2015, Soliton Systems K.K., All rights reserved.

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

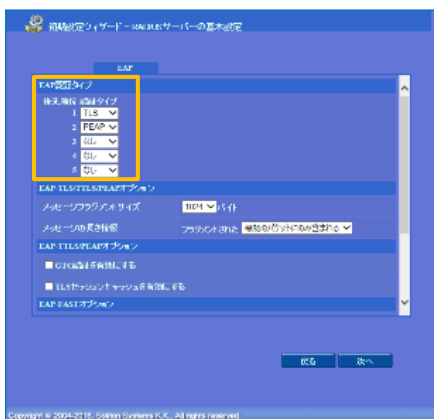
## 2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

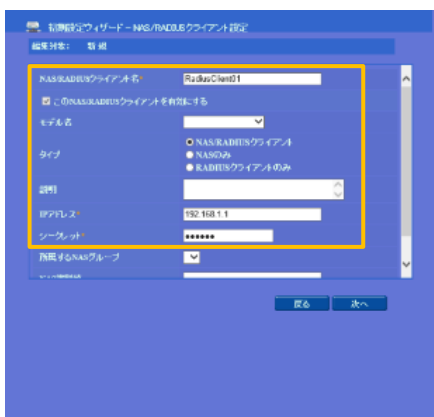
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定



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。

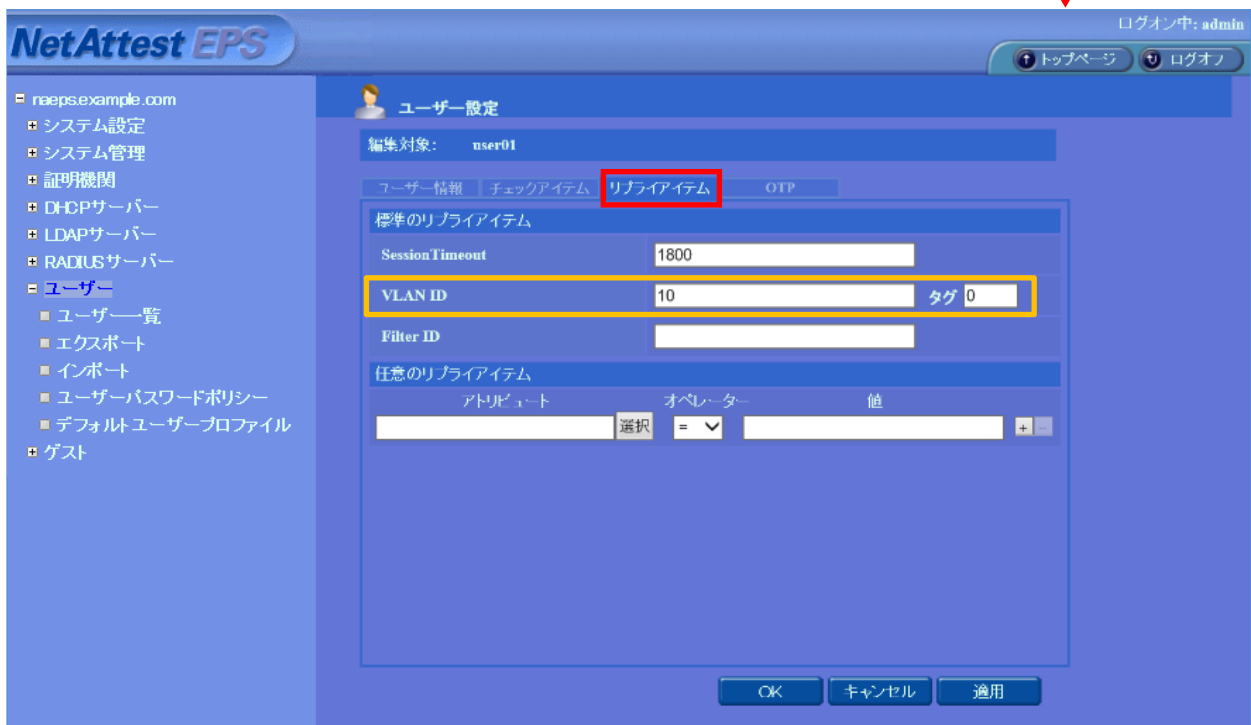
[ユーザー] - [ユーザー一覧]から、「追加」ボタンでユーザー登録を行います。

The screenshot shows the NetAttest EPS user management interface. The 'ユーザー一覧' (User List) page is active, showing a table with one user: 'test user' with ID 'test'. A red box highlights the '追加' (Add) button. A red arrow points from this button to the 'ユーザー設定' (User Registration) form. The form is titled '新規' (New) and contains fields for '姓' (Last Name), '名' (First Name), 'E-Mail', 'ユーザーID' (User ID), 'パスワード' (Password), and 'パスワード(確認)' (Confirm Password). A red box highlights the 'OK' button at the bottom of the form. A red arrow points from the 'OK' button to the updated 'ユーザー一覧' page, which now shows two users: 'test user' and 'user01'.

項目	値
姓	user01    user02    user03
ユーザーID	user01    user02    user03
パスワード	password    password    password

## 2-5 ユーザーのリプライアイテムの設定

ダイナミック VLAN で接続先を制御したいユーザーにリプライアイテムを設定します。  
 対象のユーザーの「変更」ボタンよりユーザー設定画面に進み、「リプライアイテム」タブにて「VLAN ID」と「タグ」を指定します。



項目	値		
ユーザーID	user01	user02	user03
VLAN ID	10	20	-
タグ	0	0	-

## 2-6 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。ユーザー名「user01」の「発行」ボタンが赤い枠で囲われ、赤い矢印が次の画面へと指している。

ユーザー「user01」の編集画面。証明書情報と証明書ファイルオプションの項目が黄色い枠で囲われ、発行ボタンが赤い枠で囲われている。

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

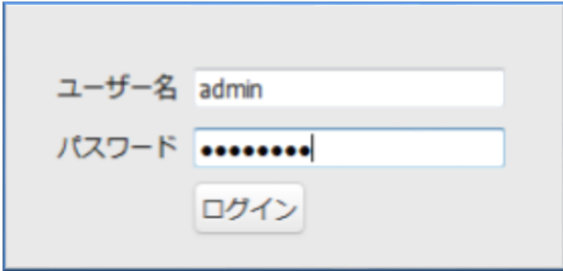
ユーザー証明書のダウンロード画面。メッセージとダウンロードボタンが赤い枠で囲われている。

## 3. BS-GS2016 の設定

BUFFALO 社製レイヤー2 スマートスイッチ BS-GS20 シリーズ (BS-GS20, BS-GS20P) 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 BS-GS2016 を使用し、WebGUI から各種設定を実施する方法を紹介します。

購入時の BS-GS2016 は、IP アドレスが 192.168.1.254 に設定されています。端末に適切な IP アドレスを設定して Web ブラウザより管理画面にアクセスし、設定を開始します。

初期のユーザー名/パスワードは admin/password です。



The image shows a login form with two input fields and a button. The first field is labeled 'ユーザー名' (Username) and contains the text 'admin'. The second field is labeled 'パスワード' (Password) and contains a series of dots. Below the fields is a button labeled 'ログイン' (Login).

セットアップは以下の流れで行います。

1. IP アドレスの設定
2. VLAN の設定
3. RADIUS サーバーの設定

ここでは、

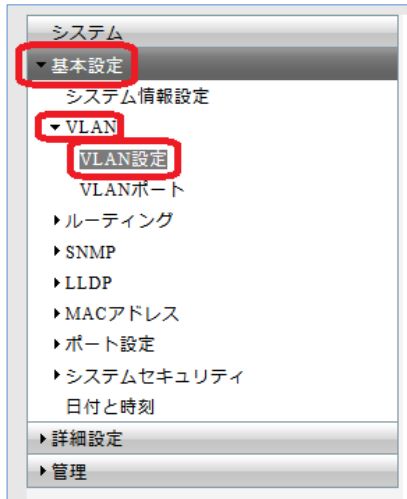
Port 1, 4 を VLAN10

Port2 を VLAN20

に設定します。

### 3-1 IP アドレスの設定

トップページより[基本設定]-[VLAN]-[VLAN 設定]をクリックします。



VLAN1 を選択し、「編集」ボタンをクリックします。



以下の画面から IPv4 アドレス、デフォルトゲートウェイを設定します。

IPv4アドレス設定	
IPv4アドレス	192.168.10.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.254

項目	値
IPv 4アドレス	192.168.10.1
デフォルトゲートウェイ	192.168.10.254

一番下にある「適用」ボタンをクリックします。



## 3-2 VLAN の設定

### 3-2-1 VLAN10 の作成

[基本設定]-[VLAN]-[VLAN 設定]をクリックし VLAN の追加を行います。

「VLAN の追加/編集」の VLAN ID に「10」を入力し、VLAN 名に「VLAN10」を入力します。管理 VLAN の欄にチェックを入れます。

VLANの追加/編集	
VLAN ID	10 (2-4094)
VLAN名	VLAN10
管理VLAN	<input checked="" type="checkbox"/>

項目	値
VLAN ID	10
VLAN 名	VLAN10
管理 VLAN	チェックあり

各ポートの設定を行います。

例：ポート 1 番と 4 番を Untagged に選択。

ポート 10 番を Tagged に選択

最後に「適用」ボタンをクリックします。

ポート		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Tagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untagged	All	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Not Member	All	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>





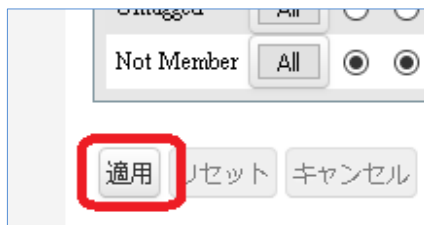
## 3-2-3 PVID の設定

[基本設定]-[VLAN]-[VLAN ポート]をクリックし、各ポートの PVID を変更します。

ポート	PVID	受信するフレームの種類
1	10	すべて
2	20	すべて
3	1	すべて
4	10	すべて
5	1	すべて

項目	値
ポート 1 の PVID	10
ポート 2 の PVID	20
ポート 3 の PVID	1
ポート 4 の PVID	10

「適用」をクリックします。



## 3-2-4 VLAN1を修正

必要に応じて VLAN 1 を修正してください。[基本設定]-[VLAN]-[VLAN 設定]をクリックします。

「VLAN ステータス」の VLAN ID 1 を選択し、「編集」ボタンをクリックします。

<input type="checkbox"/>	VLAN ID	IPv4アドレス
<input checked="" type="checkbox"/>	1	192.168.10.1
<input type="checkbox"/>	10	-
<input type="checkbox"/>	20	-

PVID

プロテクトポート

T:Static Tagged U:Static Untagged -:Not

**編集** 削除

各ポートの設定を行って、最後に「適用」ボタンをクリックします。

ポート	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Tagged	All	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Untagged	All	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Not Member	All	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**適用** リセット キャンセル

## 3-3 RADIUS サーバーの設定

### 3-3-1 RADIUS サーバーの IP アドレス設定

[詳細設定]-[認証]-[RADIUS]をクリックし、認証サーバーを指定します。

認証サーバーIPv4 アドレスに EPS の IP アドレスを指定し、共通暗号化キーに EPS で設定したキー(シークレット)を入力します。

ダイナミック VLAN を行う場合は、詳細設定のダイナミック VLAN にチェックを入れます。

最後に「適用」ボタンをクリックし、設定を保存します。

項目	値
認証	有効
認証サーバーIPv4 アドレス	192.168.1.2
共通暗号化キー	secret
ダイナミック VLAN	有効



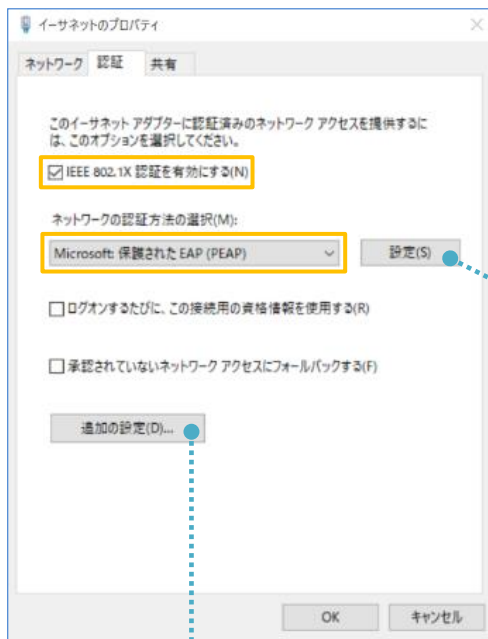
# 4. Windows 10 のクライアント設定

## 4-1 EAP-PEAP 認証

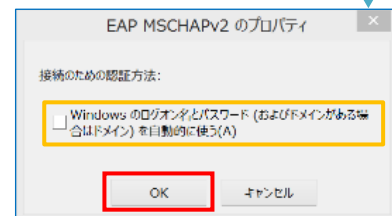
Windows 標準サブリカントで PEAP の設定を行います。

※ 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



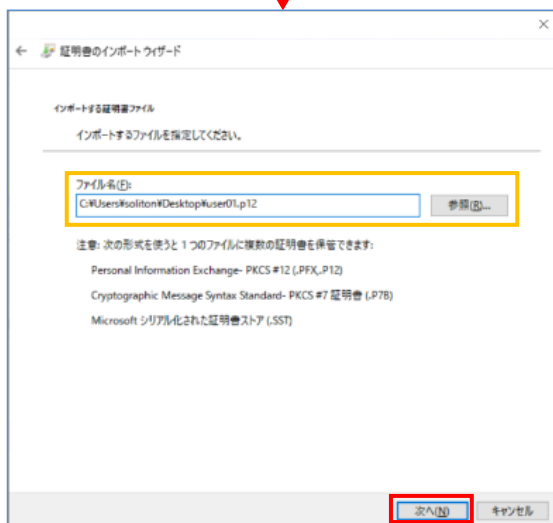
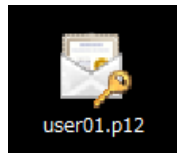
項目	値
認証モードを指定する	ユーザー認証

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省略する(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(S)

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\Desktop\User01.p12

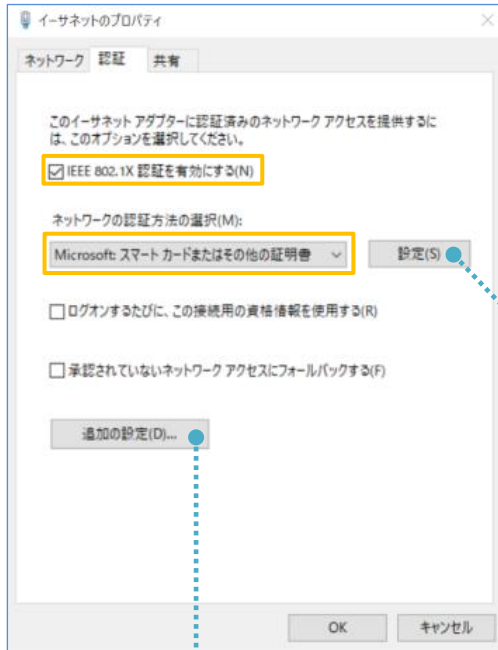
完了(O) キャンセル

## 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その他の証明書



項目	値
接続のための認証方法	
- このコンピュータの証明書を使う	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

項目	値
認証モードを指定する	ユーザー認証



## 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: [user03] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF via proxy to virtual server) Login OK: [user03] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)
BS-GS2016	Port authentication is passed on port 1

BS-GS2016 の設定画面でも確認ができます。

[詳細設定]-[認証]-[ステータス]の画面で「認証済み」と表示されていれば認証成功です。

認証状態		
ポート	認証設定	認証状態
1	802.1Xポート	認証済み
2	802.1Xポート	無効
3	802.1Xポート	無効
4	802.1Xポート	無効

### 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: [user03] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)
BS-GS2016	Port authentication is passed on port 1

BS-GS2016 の設定画面でも確認ができます。

[詳細設定]-[認証]-[ステータス]の画面で「認証済み」と表示されていれば認証成功です。

認証状態		
ポート	認証設定	認証状態
1	802.1Xポート	認証済み
2	802.1Xポート	無効
3	802.1Xポート	無効
4	802.1Xポート	無効

### 5-3 EAP-TLS+ダイナミック VLAN 認証

EAP-TLS 認証+ダイナミック VLAN 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)
BS-GS2016	Port authentication is passed on port 3

ダイナミック VLAN が成功した場合の BS-GS2016 の VLAN 割当状態の表示例

# [基本設定]-[VLAN]-[VLAN 設定]を参照

**VLANステータス**

VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN名	管理VLAN
1	192.168.10.1	-	-	U	-	U	U	U	U	U	U	U	U	U	U	U	U	VLNA10	Up
10	-	U	-	-	U	-	-	-	-	-	T	-	-	-	-	-	-	VLNA10	Up
20	-	-	U	-	-	-	-	-	-	-	T	-	-	-	-	-	-	VLNA20	Down
PVID		10	20	1	10	1	1	1	1	1	1	1	1	1	1	1	1		
プロテクトポート		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		

T:Static Tagged U:Static Untagged -:Not Member X:有効

編集 削除

VLAN10 が割り当てられた場合

**VLANステータス**

VLAN ID	IPv4アドレス	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	VLAN名	管理VLAN
1	192.168.10.1	-	-	U	-	U	U	U	U	U	U	U	U	U	U	U	U	VLNA10	Up
10	-	U	-	-	U	-	-	-	-	-	T	-	-	-	-	-	-	VLNA10	Up
20	-	-	U	-	-	-	-	-	-	-	T	-	-	-	-	-	-	VLNA20	Down
PVID		10	20	1	10	1	1	1	1	1	1	1	1	1	1	1	1		
プロテクトポート		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		

T:Static Tagged U:Static Untagged -:Not Member X:有効

編集 削除

VLAN20 が割り当てられた場合

BS-GS2016 の設定画面でも確認ができます。

[詳細設定]-[認証]-[ステータス]の画面で「動的 VLAN」と表示されていれば認証成功です。

認証状態		
ポート	認証設定	認証状態
1	802.1Xポート	無効
2	802.1Xポート	無効
3	802.1Xポート	動的VLAN
4	802.1Xポート	無効

## 付録 L3 スイッチの設定

### ポート設定、DHCP リレー設定

---

下記のようにポートの設定をします。

ポート	VLAN ID	ネットワーク	スイッチ IP アドレス	備考
1-5	1	192.168.1.0/255.255.255.0	192.168.1.254	
6-9	10	192.168.10.0/255.255.255.0	192.168.10.254	
10	10,20			VLAN10 と VLAN20 の トランクポート
11-14	20	192.168.20.0/255.255.255.0	192.168.20.254	

DHCP リレー設定にて、「192.168.1.3」を指定します。

