

# ***NetAttest EPS***

## 認証連携設定例

【連携機器】 ELECOM EHB-SG2B/EHB-SG2B-PL シリーズ

【Case】 IEEE802.1X EAP-TLS/EAP-TLS+ダイナミック VLAN

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、ELECOM 社製 L2 スイッチ EHB-SG2B シリーズおよび EHB-SG2B-PL シリーズの IEEE802.1X 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 EHB-SG2B/EHB-SG2B-PL 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.....	6
1-1 構成図.....	6
1-2 環境.....	7
1-2-1 機器.....	7
1-2-2 認証方式.....	7
1-2-3 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 ユーザーのリプライアイテムの設定.....	12
2-6 クライアント証明書の発行.....	13
3. EHB-SG2B/EHB-SG2B-PL シリーズの設定.....	14
3-1 IP アドレスの設定.....	14
3-2 VLAN の設定.....	15
3-3 RADIUS の設定.....	16
3-4 ポートアクセス制御の設定.....	17
3-5 ポートアクセス制御ステータスの確認.....	18
4. NetAttest D3 の設定.....	19
4-1 ネットワーク設定.....	20
4-2 スコープ・レンジ設定.....	21
4-3 DHCP サーバーの起動.....	22
5. EAP-TLS 認証でのクライアント設定.....	23
5-1 Windows 10 での EAP-TLS 認証.....	23
5-1-1 クライアント証明書のインポート.....	23
5-1-2 サブリカント設定.....	25
6. 動作確認結果.....	26

---

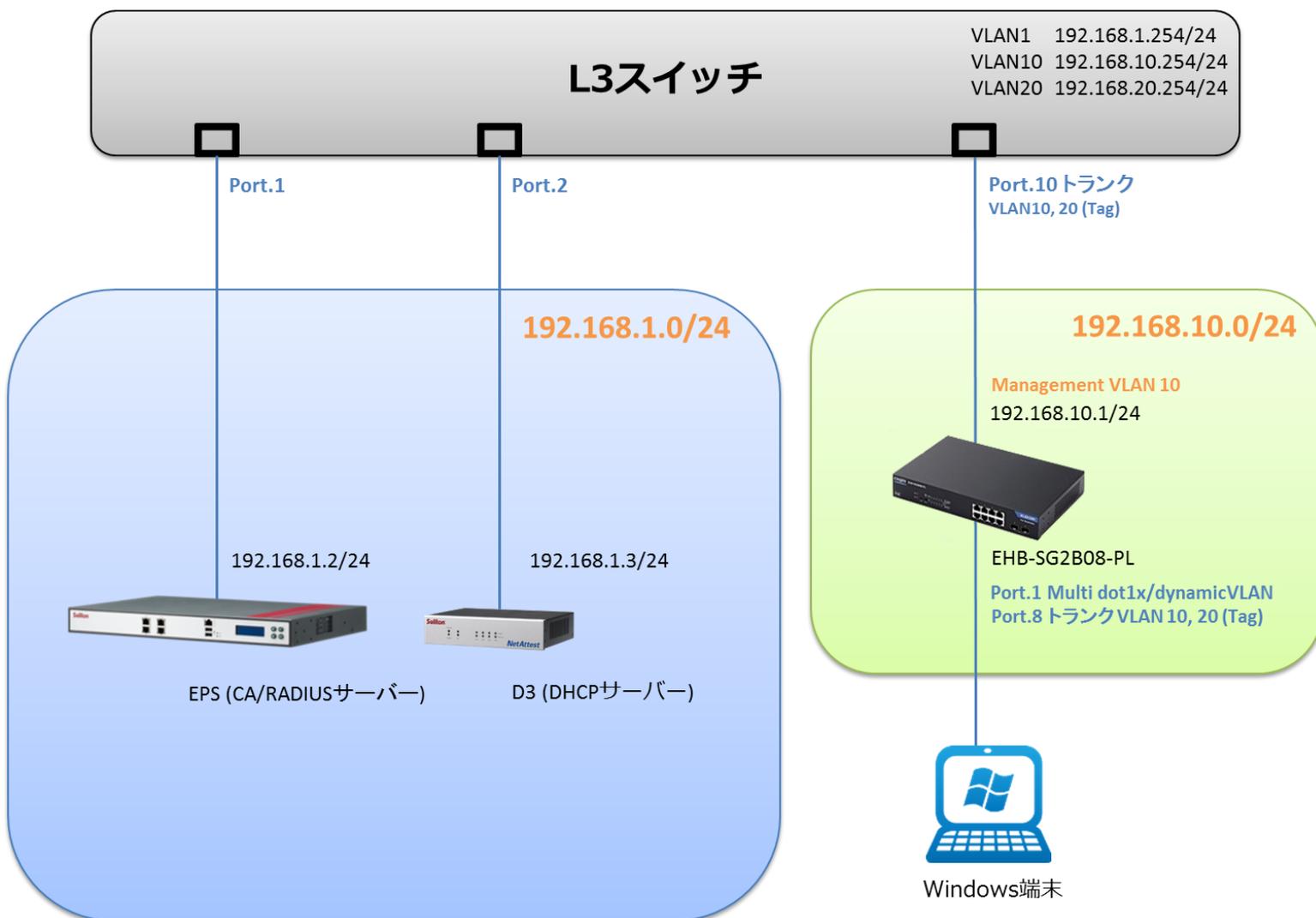
6-1 EAP-TLS 認証.....	26
6-2 EAP-TLS+ダイナミック VLAN 認証.....	27
付録 L3 スイッチの設定 .....	28
ポート設定、DHCP リレー設定.....	28

# 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 用)
  - VLAN10 : 192.168.10.0/24 (EHB-SG2B08-PL 管理、ダイナミック VLAN/user01、認証のみ/user03 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	4.8.11
EHB-SG2B シリーズ EHB-SG2B-PL シリーズ	ELECOM	RADIUS クライアント (L2 スイッチ)	1.00.018
XPS 13	Dell	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブリカント
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.11

### 1-2-2 認証方式

IEEE802.1X 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
EHB-SG2B シリーズ EHB-SG2B-PL シリーズ	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。

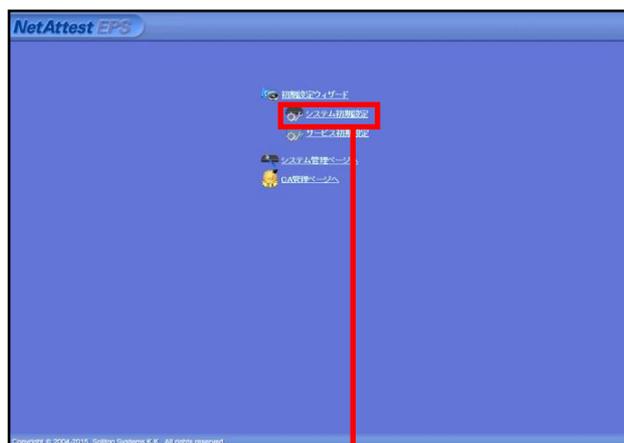
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

## 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
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/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.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

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

項目	値
NAS/RADIUS クライアント名	ELECOML2SW
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。

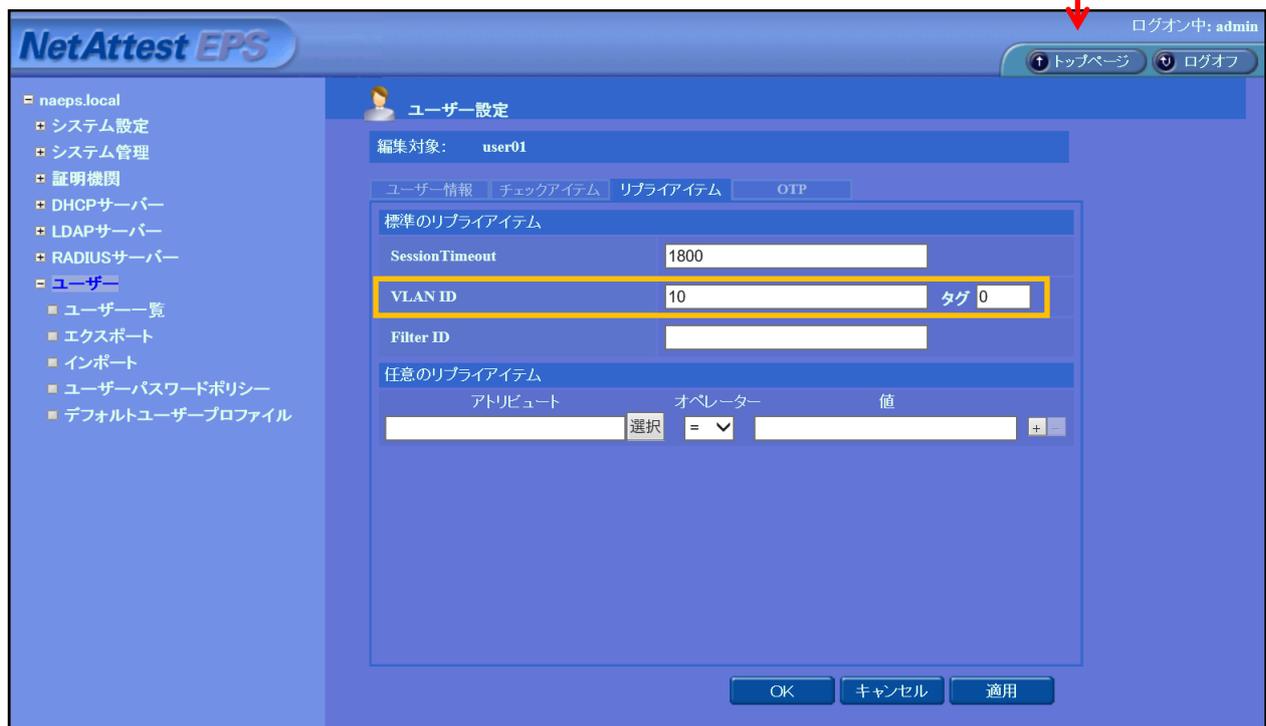
[ユーザー] - [ユーザー一覧]から、「追加」ボタンでユーザー登録を行います。

The screenshot shows the NetAttest EPS management interface. On the left is a sidebar menu with 'ユーザー一覧' (User List) highlighted. The main area shows a table of users with columns for '名前' (Name), 'ユーザーID' (User ID), '最終認証成功日時' (Last successful authentication date), '証明書' (Certificate), and 'タスク' (Tasks). A red box highlights the '追加' (Add) button in the top right of the table. Below the table is a 'ユーザー設定' (User Settings) form. The form has tabs for 'ユーザー情報' (User Information), 'チェックアイテム' (Check Items), 'リプライアイテム' (Reply Items), and 'OTP'. The 'ユーザー情報' tab is active, showing fields for '姓' (Surname), '名' (Name), 'E-Mail', 'ユーザーID', 'パスワード', and 'パスワード(確認)'. A red box highlights the 'OK' button at the bottom of the form. A red arrow points from the 'OK' button back to the '追加' button in the user list.

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	20	-

## 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」タブ。検索条件は「一部」で「user01」が検索結果として表示されている。右側の「発行」ボタンが赤い枠で囲われている。

ユーザー「user01」の編集画面。有効期限が365日、PKCS#12ファイルに証明機関の証明書を含めるにチェックが入っている。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。メッセージが表示され、ダウンロードボタンが赤い枠で囲われている。

## 3. EHB-SG2B/EHB-SG2B-PL シリーズの設定

### 3-1 IP アドレスの設定

工場出荷状態の EHB-SG2B/EHB-SG2B-PL シリーズの初期 IP アドレスは「192.168.3.1/24」です。管理端末に適切な IP アドレスを設定し、Internet Explorer から「http://192.168.3.1/」にアクセスしてください。設定を行う PC に適切な IP アドレスを設定した後、Web ブラウザを起動し、アドレスバーに IP アドレスを入力し、設定を開始します。

Web 管理画面にログインし、設定を開始します。

※初期設定では、ユーザー名 : admin パスワード : admin です。

The image shows the ELECOM login interface. It features the ELECOM logo at the top. Below it, there are three input fields: 'ユーザー名:' with 'admin' entered, 'パスワード:' with masked characters '.....', and '言語:' with '日本語' selected in a dropdown menu. A blue 'ログイン' button is positioned at the bottom right of the form.

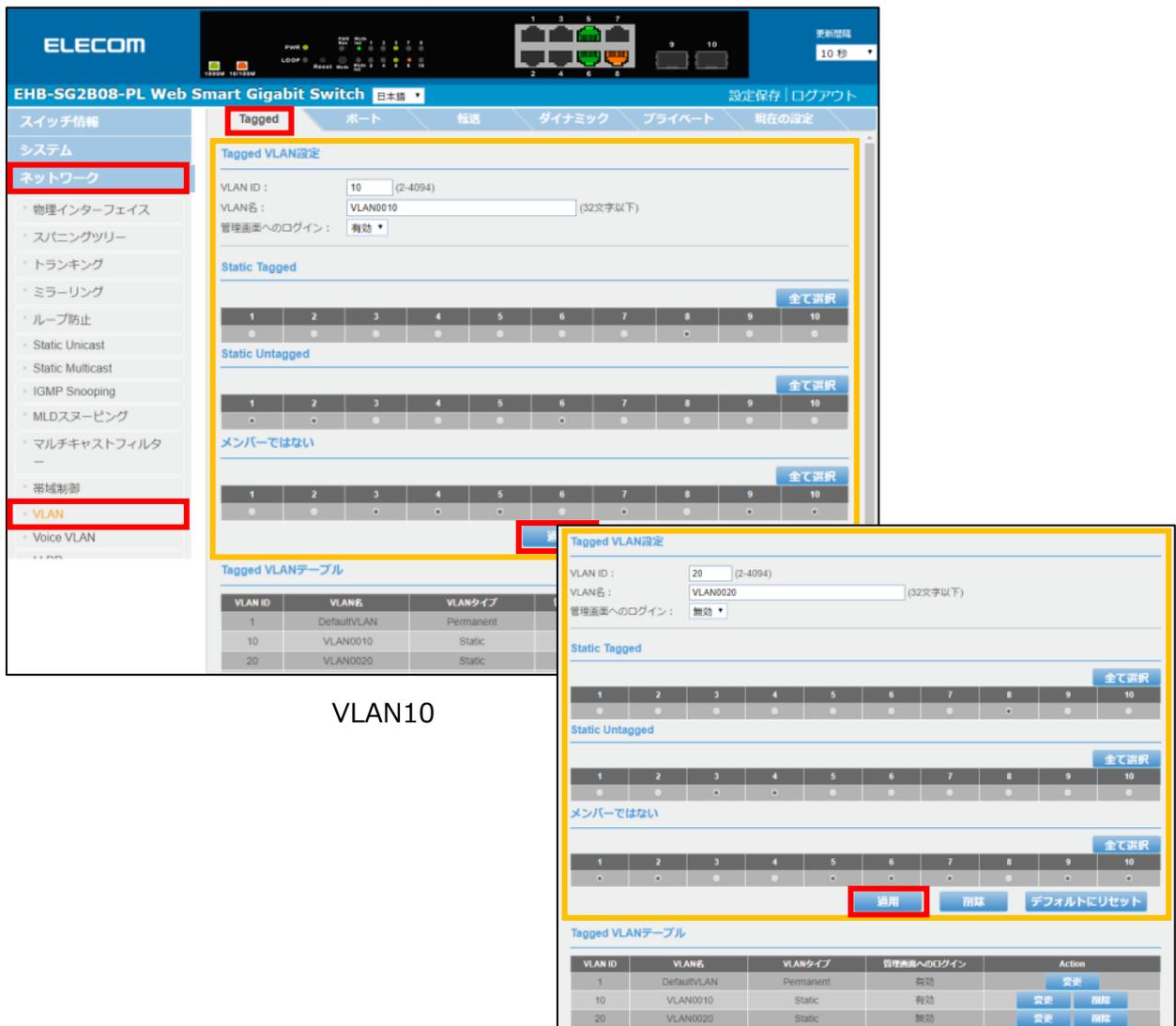
[システム] - [IPv4 設定]をクリックし、IP アドレスに「192.168.10.1」、サブネットマスクに「255.255.255.0」、デフォルトゲートウェイに「192.168.10.254」を入力し、「適用」をクリックします。

The screenshot displays the 'IPv4 設定' (IPv4 Settings) page in the ELECOM management interface. The left sidebar shows the 'システム' (System) menu with 'IPv4 設定' highlighted. The main content area shows the following configuration: MACアドレス: BC:5C:4C:48:C1:59; IP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; IPモード: Static. A red box highlights the '適用' (Apply) button at the bottom right.

項目	値
IP 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

### 3-2 VLAN の設定

VLAN の設定を行います。[ネットワーク] - [VLAN] - [Tagged]をクリックします。  
 VLAN ID(VLAN10 では 10、VLAN20 では 20)、VLAN 名(VLAN10 では VLAN0010、VLAN20 では VLAN0020)、管理画面へのログイン(VLAN10 では有効、VLAN20 では無効)を設定し、Static Tagged、Static Untagged にそれぞれ割り当てるポートを選択して「適用」をクリックします。



VLAN10

VLAN20

項目	値	
VLAN ID	10	20
VLAN 名	VLAN0010	VLAN0020
管理画面へのログイン	有効	無効
Static Tagged	1,2	3,4
Static Untagged	8	8

### 3-3 RADIUS の設定

RADIUS サーバーの登録を行います。[セキュリティ] - [RADIUS]をクリックします。

RADIUS サーバーIP アドレス(NetAttest EPS の IP アドレス)、Shared Secret(共通シークレット)を入力し、「追加」をクリックします。

The screenshot shows the configuration page for the RADIUS server. The 'Security' menu is highlighted in red, and the 'RADIUS' sub-menu is also highlighted in red. The 'RADIUS Settings' form is highlighted in yellow, showing the following fields:

- サーバープライオリティ: 1 (最高: 1、最低: 5)
- サーバーIPアドレス: 192.168.1.2 (IPv4 selected)
- サーバーポート: 1812 (1-65535)
- Accounting Port: 1813 (1-65535)
- Shared Secret: secret (32文字以下)

A red box highlights the '追加' (Add) button. Below the form is a 'RADIUSテーブル' (RADIUS Table) with one entry:

サーバープライオリティ	サーバーIPアドレス	サーバーポート	Accounting Port	Shared Secret	Action
1	192.168.1.2	1812	1813	secret	変更 削除

項目	値
RADIUS サーバー	192.168.1.2
サーバーポート	1812
Accounting Port	1813
Shared Secret	secret

### 3-4 ポートアクセス制御の設定

ポートアクセス制御を有効にし、インターフェイスに認証モードを設定します。

[セキュリティ] - [ポートアクセス制御]をクリックします。

NAS ID(SolitonLab)を入力し、ポートアクセス制御ステータスを「有効」、認証方式に「RADIUS」を選択して「適用」をクリックします。

項目	値
NAS ID	SolitonLab
ポートアクセス制御ステータス	有効
認証方式	RADIUS

ポートを 1、認証モードを「802.1X」、ポート制御を「自動」、VLAN 割り当てに「有効」を選択し、「適用」をクリックします。

項目	値
ポート	1
認証モード	802.1X
ポート制御	自動
VLAN 割り当て	有効

## 3-5 ポートアクセス制御ステータスの確認

現在の設定ステータスを確認します。[セキュリティ] - [ポートアクセス設定]をクリックします。  
「設定ステータス」をクリックします。

The screenshot shows the configuration page for the ELECOM EHB-SG2B08-PL Web Smart Gigabit Switch. The '設定' (Settings) section is active, and the '現在の設定ステータス' (Current Setting Status) section is highlighted with a red dashed border. The table below shows the status of 10 ports.

ポート	認証モード	ポート制御	認証ステータス	サブリカントモード	Piggyback	承認済MACアドレス	VLANリスト
1	802.1X	自動	未認証	Single	無効	N/A	1,10
2	802.1X	自動	未認証	Single	無効	N/A	1,10
3	802.1X	自動	未認証	Single	無効	N/A	1,20
4	802.1X	自動	未認証	Single	無効	N/A	1,20
5	802.1X	強制認証	認証済	Single	無効	N/A	1
6	802.1X	強制認証	認証済	Single	無効	N/A	1,10
7	802.1X	強制認証	認証済	Single	無効	N/A	1
8	802.1X	強制認証	認証済	Single	無効	N/A	1,10,20
9	802.1X	強制認証	認証済	Single	無効	N/A	1
10	802.1X	強制認証	認証済	Single	無効	N/A	1

## 4. NetAttest D3 の設定

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、Internet Explorer または Google Chrome から「<http://192.168.2.1:2181/>」にアクセスしてください。NetAttest D3 では下記設定を行います。

- ネットワーク設定
- スコープ・レンジの設定
- DHCP サーバーの起動

## 4-1 ネットワーク設定

[システム設定] - [ネットワーク設定] からネットワークの設定を行います。

**NetAttest D3**

ホスト名: nad3.local    DNS: ✕    DHCP: ✕    DHCPv6: ✕

システム設定 - ネットワーク設定

LAN1(サービスインターフェイス)

IPアドレス  192.168.1.3

サブネットマスク  255.255.255.0

MACアドレス 00:0C:29:5E:12:8B

IPv6アドレスの使用  使用しない  自動設定のみ  手動設定

IPv6アドレス

サブネットマスク

デフォルトゲートウェイ

デフォルトゲートウェイ 192.168.1.254

IPv6デフォルトゲートウェイ

LAN2

IPアドレス

サブネットマスク

ホスト名

ホスト名  nad3.local

項目	値
IPアドレス	192.168.1.3
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
ホスト名	nad3.local

## 4-2 スコープ・レンジ設定

[DHCP サービス] - [スコープ] から [追加] ボタンでスコープを作成します。

VLAN10 用に「192.168.10.0」のネットワークのスコープ、VLAN20 用に「192.168.20.0」のネットワークのスコープを追加します。

The screenshot shows the NetAttest D3 web interface. The left sidebar has a menu with 'DHCPサービス' expanded and 'スコープ' highlighted. The main area is titled 'DHCP - スコープの追加'. It contains two sections: 'スコープの設定' and 'レンジの設定'. The 'スコープの設定' section has fields for 'ネットワーク' (192.168.10.0), 'サブネットマスク' (255.255.255.0), 'ルーター' (192.168.10.254), 'ドメイン名' (example.com), and 'ドメインネームサーバー' (192.168.1.254). The 'レンジの設定' section has fields for 'レンジ開始アドレス' (192.168.10.100), 'レンジ終了アドレス' (192.168.10.150), '除外レンジ開始アドレス', and '除外レンジ終了アドレス'. At the bottom are 'OK' and 'キャンセル' buttons.

項目	VLAN10	VLAN20
ネットワーク	192.168.10.0	192.168.20.0
サブネットマスク	255.255.255.0	255.255.255.0
ルーター	192.168.10.254	192.168.20.254
ドメイン名	example.com	example.com
ドメインネームサーバー	192.168.1.254	192.168.1.254
レンジ開始アドレス	192.168.10.100	192.168.20.100
レンジ終了アドレス	192.168.10.150	192.168.20.150

## 4-3 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 displays the NetAttest D3 web interface for DHCP server management. The left sidebar contains a menu with 'サーバー状態' (Server Status) highlighted in red. 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 (Running)
- サーバー稼働状態: 動作中
- 冗長化状態: 冗長化しない (Not redundant)
- IP使用率(%): 0% (0 / 41 max)

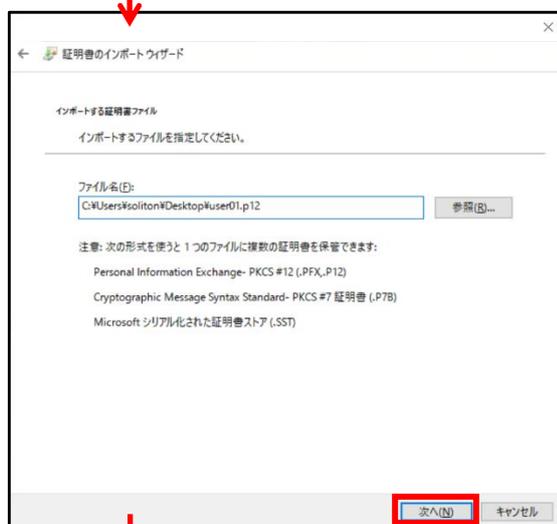
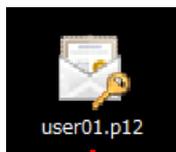
At the bottom of the page, there are several control buttons: '起動' (Start), '停止' (Stop), '初期化' (Reset), 'リース情報全消去' (Clear all lease information), 'MACアドレス使用履歴全消去' (Clear all MAC address usage history), and '状態の更新' (Refresh status). The '起動' button is highlighted with a red box.

## 5. EAP-TLS 認証でのクライアント設定

### 5-1 Windows 10 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.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\Desktop\User01.p12

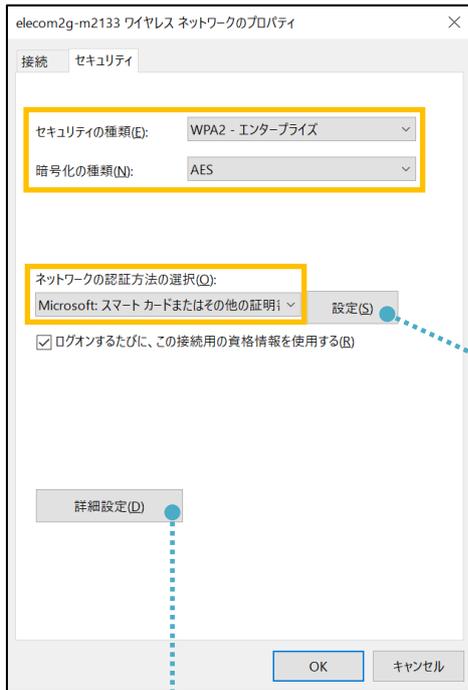
完了(F) キャンセル

## 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。

※本項では TLS の設定のみ記載します。その他の認証方式の設定に関しては付録をご参照ください。

[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

## 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: [user03] (from client ELECOML2SW port 1 cli 60-45-BD-C-04-37)
EHB-SG2B シリーズ EHB-SG2B-PL シリーズ	1 local0/Info Jul 10 16:31:36 802.1x Authentication success from (Username: user03, Port: 1, MAC: 60-45-bd-fc-04-37)

EAP-TLS 認証が成功した場合の EHB-SG2B/EHB-SG2B-PL シリーズ画面表示例

The screenshot displays the configuration page for 'EHB-SG2B08-PL Web Smart Gigabit Switch'. The left sidebar shows the 'Security' menu with 'Port Access Control' selected. The main content area shows 'Port Access Control Settings' with the following configuration:

- NAS ID: SolitonLab (16 characters or less)
- Port Access Control Status: 有効 (Enabled)
- Authentication Method: RADIUS

Buttons for '適用' (Apply), '設定' (Settings), and '設定ステータス' (Configuration Status) are visible. Below, the '現在の設定ステータス' (Current Configuration Status) table is shown:

ポート	認証モード	ポート制御	認証ステータス	サブリカントモード	Piggyback	承認済MACアドレス	VLANリスト
1	802.1X	自動	認証済	Single	無効	60-45-BD-FC-04-37	1,10
2	802.1X	自動	未認証	Single	無効	N/A	1,10
3	802.1X	自動	未認証	Single	無効	N/A	1,20
4	802.1X	自動	未認証	Single	無効	N/A	1,20
5	802.1X	強制認証	認証済	Single	無効	N/A	1
6	802.1X	強制認証	認証済	Single	無効	N/A	1,10
7	802.1X	強制認証	認証済	Single	無効	N/A	1
8	802.1X	強制認証	認証済	Single	無効	N/A	1,10,20
9	802.1X	強制認証	認証済	Single	無効	N/A	1



## 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。

