Soliton

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。

目次

1. 構成

1-1 構成図

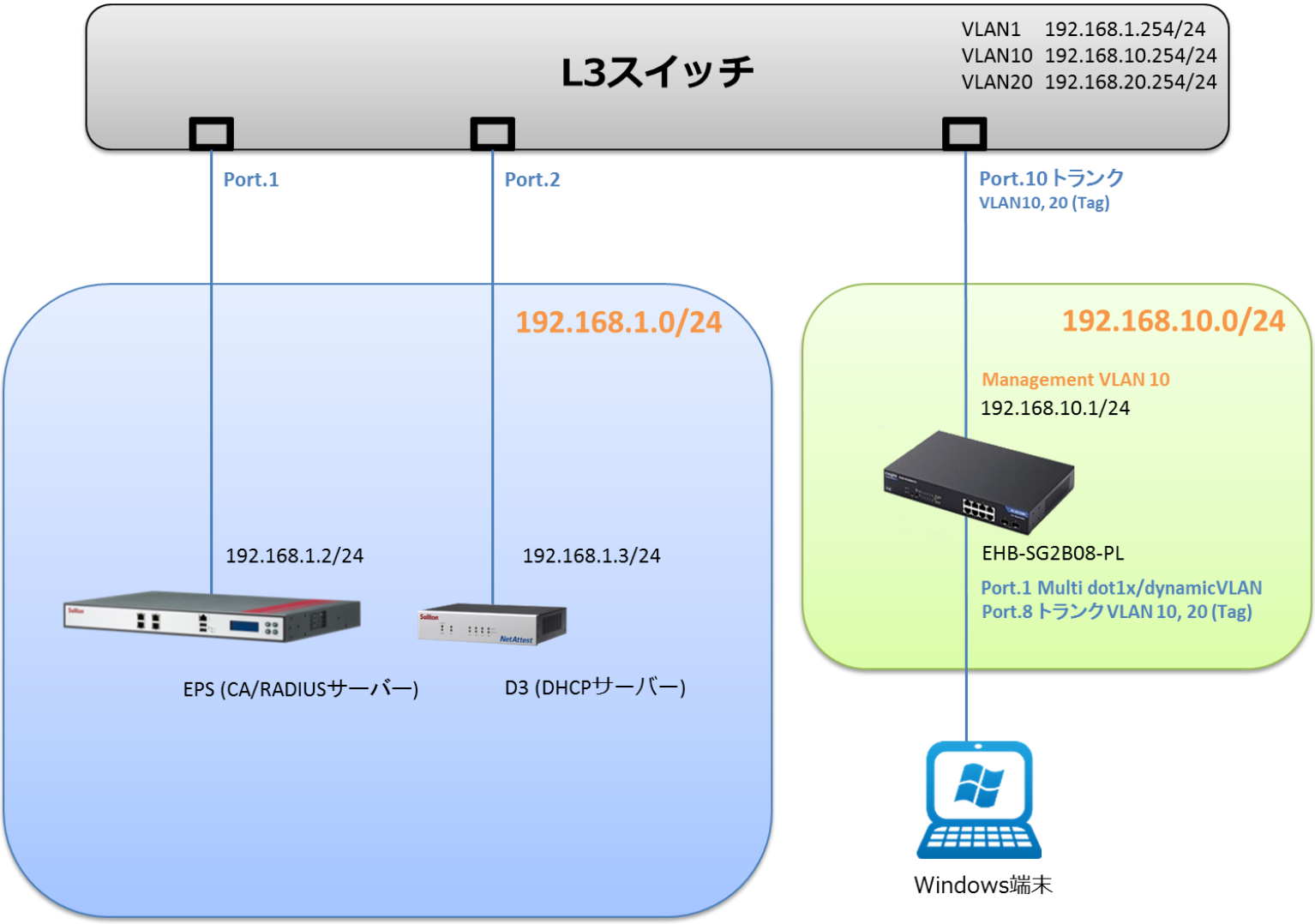
以下の環境を構成します。

・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	4.2.11

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。

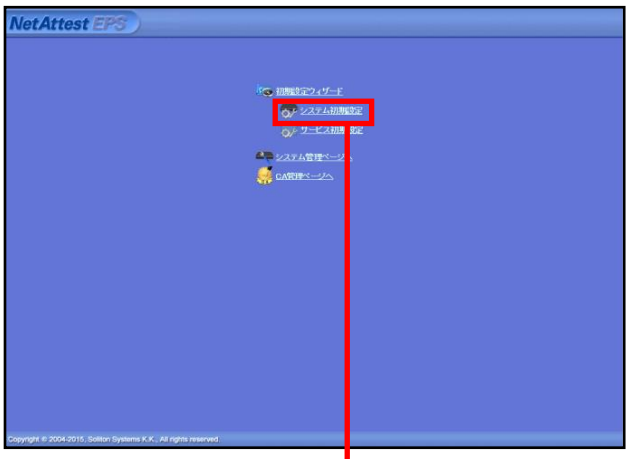
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

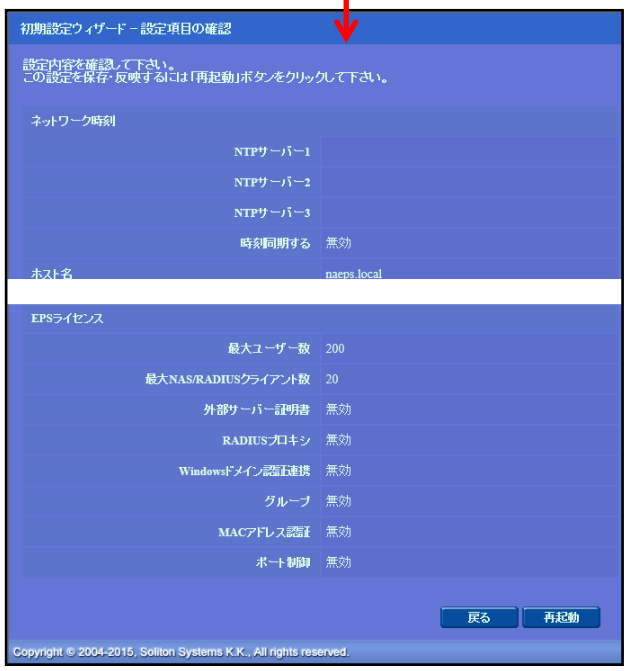
2-2 システム初期設定ウィザードの実行

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



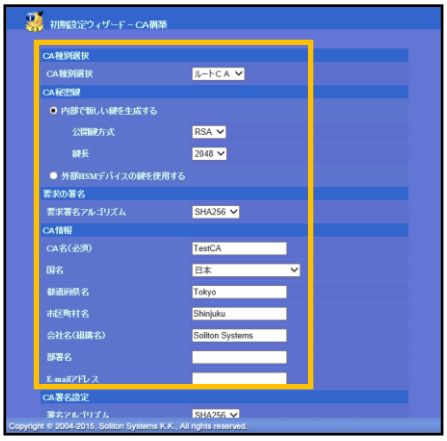


項目	値
ホスト名	naeps.local
IP アドレス	デフォルト
ライセンス	なし

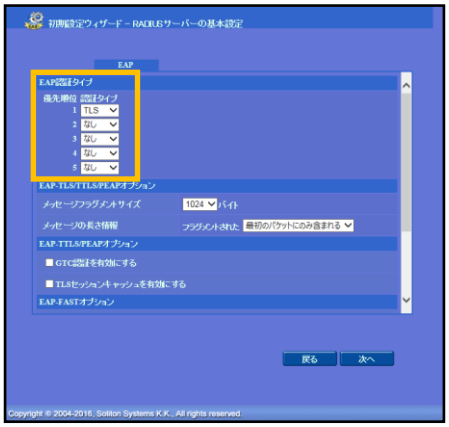
2-3 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

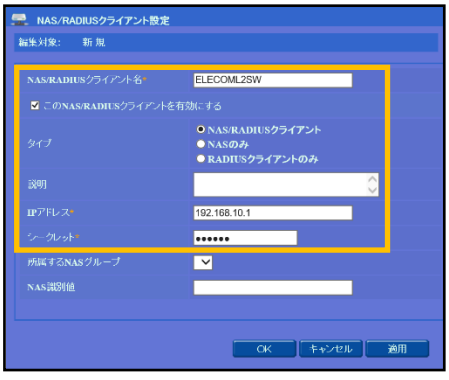
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定



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

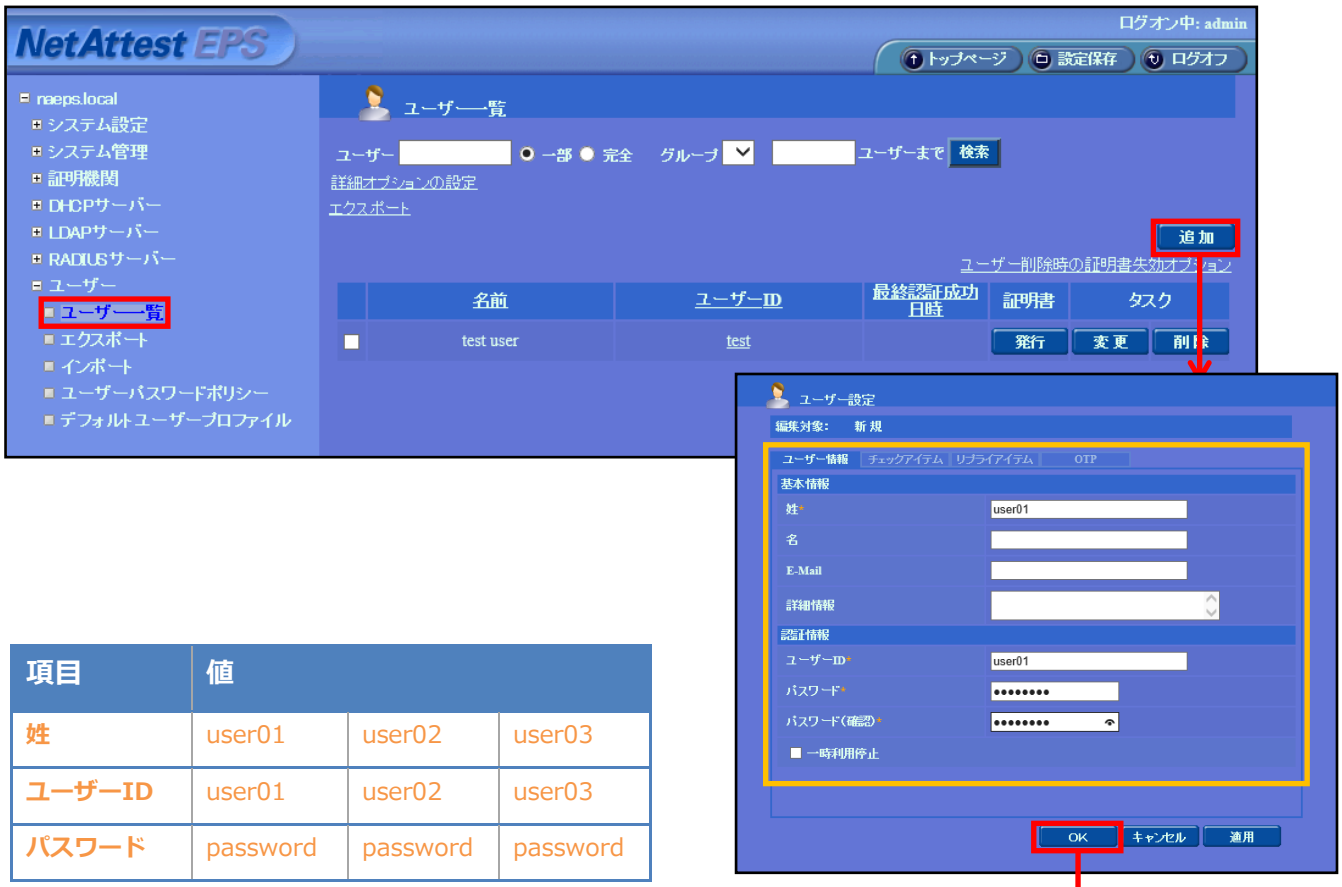


項目	値
NAS/RADIUS クライアント名	ELECOML2SW
IP アドレス	192.168.10.1
シークレット	secret

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。

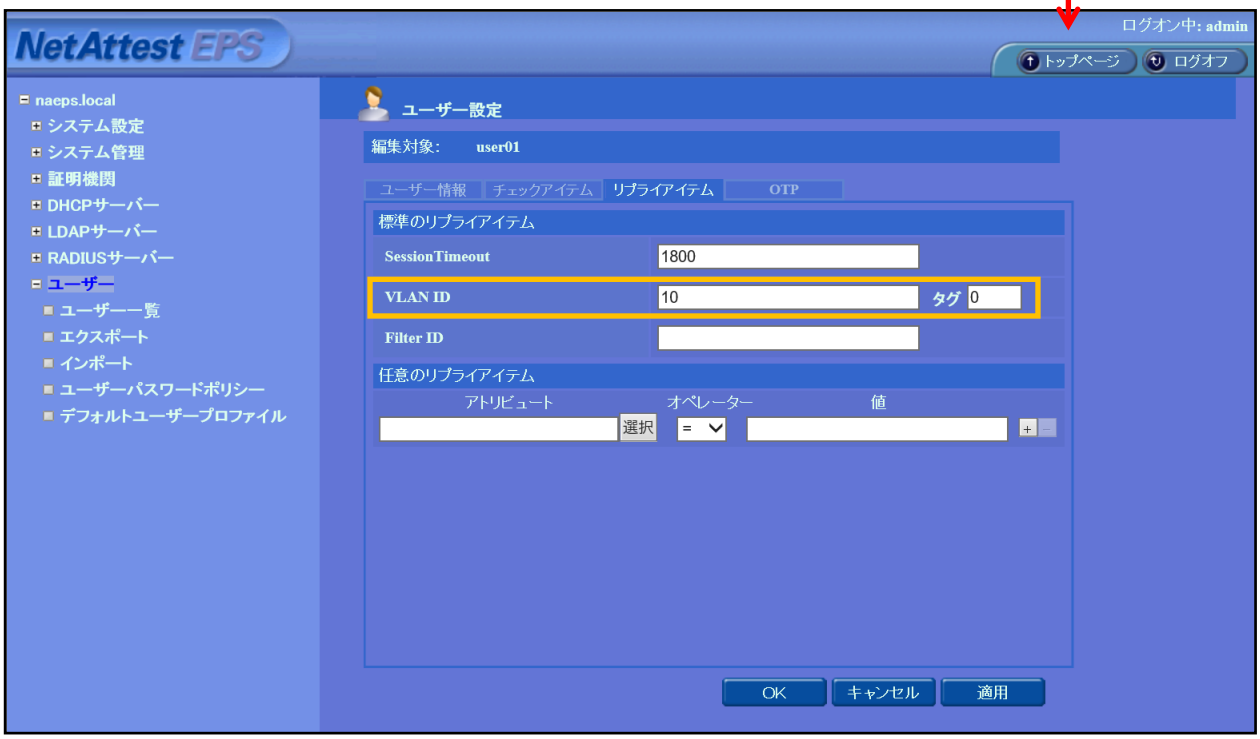


項目	値		
姓	user01	user02	user03
ユーザーID	user01	user02	user03
パスワード	password	password	password

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	-

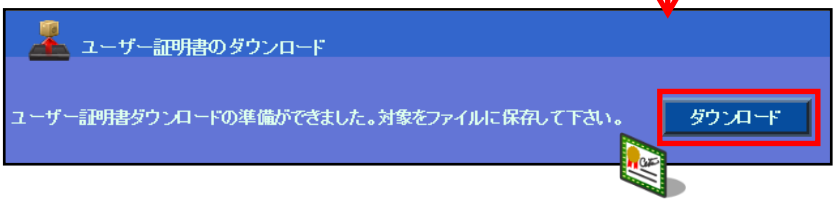
2-6 クライアント証明書の発行

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)

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. 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。

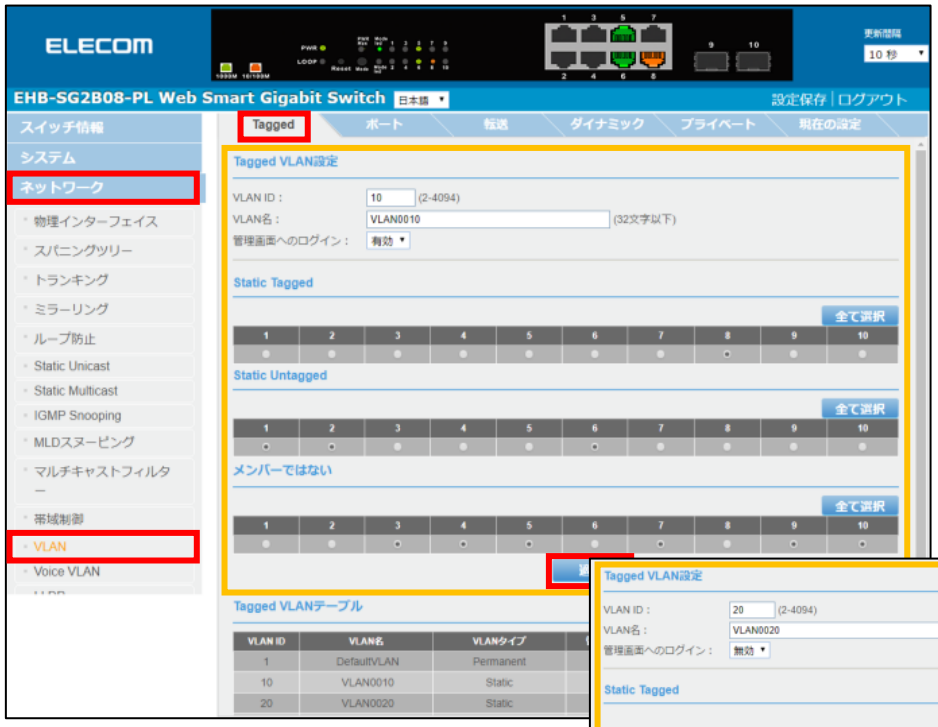
※初期設定では、ユーザー名：admin　パスワード：admin です。

[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。

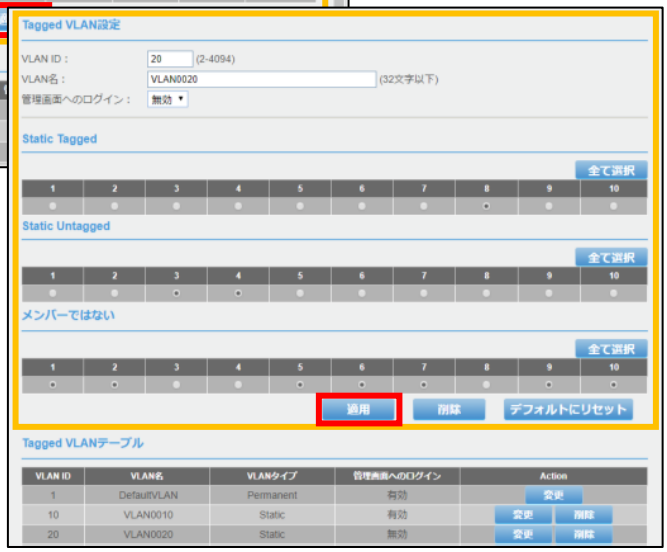
項目	値
IP アドレス	192.168.10.1
サブネットマスク	255.255.255.0
デフォルトゲートウェイ	192.168.10.254

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」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。

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。

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。

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。

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

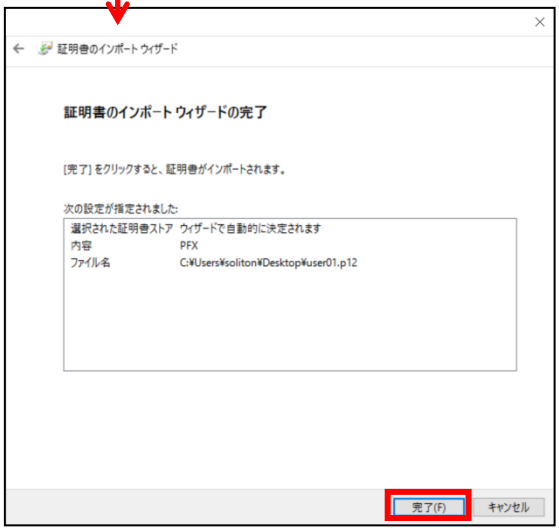
[DHCP サービス] - [サーバー状態] にて「起動」ボタンを押し、DHCP サーバーを起動します。

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。



【パスワード】

NetAttest EPS で証明書を発行した際に

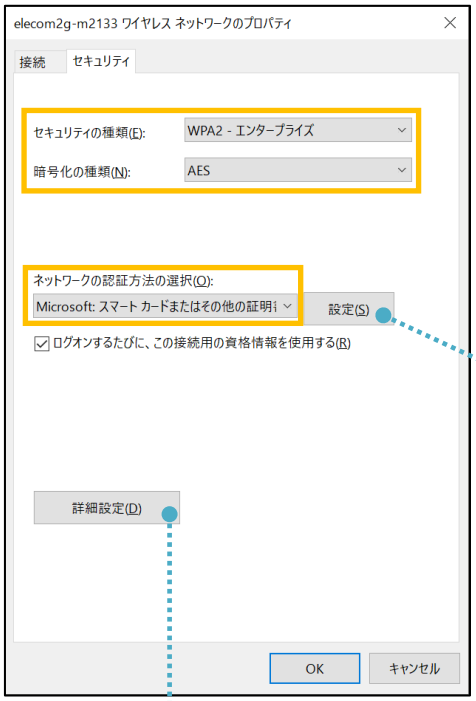
設定したパスワードを入力

5-1-2 サプリカント設定

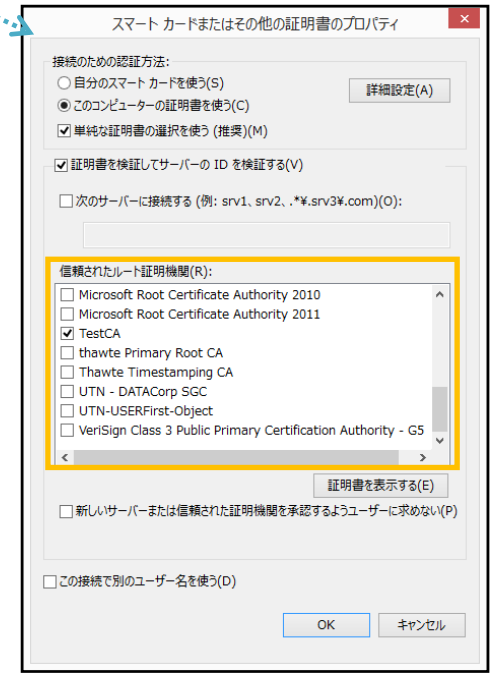
Windows 標準サプリカントで TLS の設定を行います。

※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
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

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

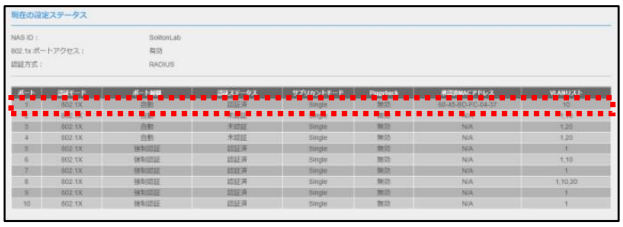
製品名	ログ表示例
NetAttest EPS	Login OK: [user03] (from client ELECOML2SW port 1 cli 60-45-BD-C-04-37)
EHB-SG2B シリーズ EHB-SG2B-PL シリーズ	1 local0/Info Jul 10 16:31:36 802.1x Authentication success from (Username: user03, Port: 1, MAC: 60-45-bd-fc-04-37)

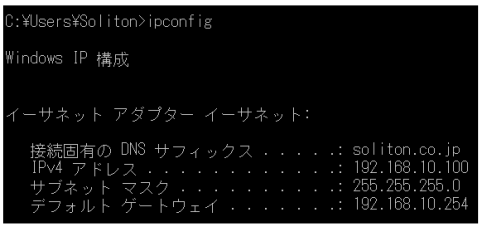
EAP-TLS 認証が成功した場合の EHB-SG2B/EHB-SG2B-PL シリーズ画面表示例

6-2 EAP-TLS+ダイナミック VLAN 認証

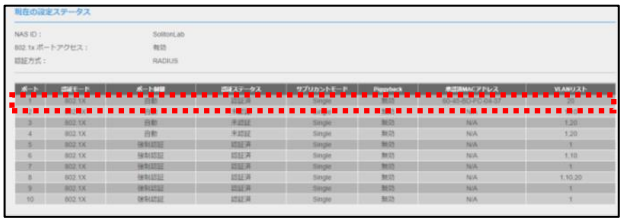
EAP-TLS 認証+ダイナミック VLAN が成功した場合のログ表示例

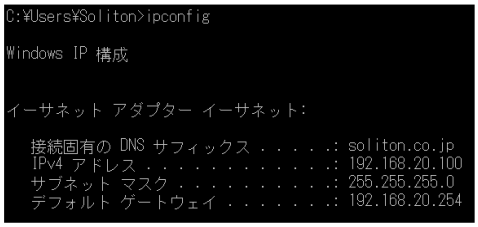
製品名	ログ表示例
NetAttest EPS	Login OK: [user01] (from client ELECOML2SW port 1 cli 60-45-BD-C-04-37) Login OK: [user02] (from client ELECOML2SW port 1 cli 60-45-BD-C-04-37)
EHB-SG2B シリーズ EHB-SG2B-PL シリーズ	34 local0/Info Jul 10 17:20:53 802.1x Authentication success from (Username: user02, Port: 1, MAC: 60-45-bd-fc-04-37) 31 local0/Info Jul 10 17:17:22 802.1x Authentication success from (Username: user01, Port: 1, MAC: 60-45-bd-fc-04-37)





User01 の場合





User02 の場合

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。

改訂履歴

日付	版	改訂内容
2017/07/31	1.0	初版作成