



【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
(پ	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。 .

# <mark>S≎liton</mark> 目次

1. 構成6	Ì
1-1 構成図6	5
1-2 環境7	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	7
2. NetAttest EPSの設定8	3
2-1 初期設定ウィザードの実行8	3
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	ł
3-1 IP アドレスの設定14	ŀ
3-2 VLAN の設定 15	5
3-3 RADIUSの設定16	5
3-4 ポートアクセス制御の設定17	7
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	3
5-1 Windows 10 での EAP-TLS 認証23	3
5-1-1 クライアント証明書のインポート23	3
5-1-2 サプリカント設定25	5
6. 動作確認結果	5

6-1 EAP-TLS 認証2	6
6-2 EAP-TLS+ダイナミック VLAN 認証 2	7
付録 L3 スイッチの設定2	8
ポート設定、DHCP リレー設定	8

## <u>Saliton</u> 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		secret
EHB-SG2B シリーズ EHB-SG2B-PL シリーズ	192.168.10.1/24	UDP 1812	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.NetAttest EPS の設定

#### 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

CA種別選択			
CAMEDERIR	"⊢⊦са ∨		
CA NOTINE			
● 内部で新しい鍵を生成する			
公開總方式	RSA 🗸		
鍵長	2048 🗸		
◎ 外部HSMデバイスの鍵を使	Ulliga		
要求の署名			
要求署名アルゴリズム	SHA256 V		
CA情報			
	TestCA		
	日本	~	
都道府県名	Tokyo		
市区町村名	Shinjuku		
会社名(組織名)	Soliton Systems		
部署名			
E-mailアドレス			
CA署名設定			



	ELECOML2SW
	を有効にする
	● NAS/RADIUSクライアント ● NASのみ ● RADIUSクライアントのみ
	192.168.10.1
シークレット・	•••••
所属するNASグループ	✓
NAS識別値	

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。

Not Attact	EDC							ログ	オン中: admin
NetAttest	EFS					() トップペー	ジ 🕒 🖥	定保存)(	も ログオフ
■ naeps.local ■ システム設定		ユーザ	覧						
■ システム管理		ユーザー	● 一部 ● 完全	グループ 💙		ユーザーまで 検索			
■ 証明機関 ■ DHCPサーバー		詳細 <u>オブションの設定</u> エクスポート							
■ LDAPサーバー									追加
■ RADIUSサーバー ■ ユーザー						<u></u>	ザー削除時	の証明書失	効オブ: 雪ン
□ ユーザー一覧		名	<b></b> 前	<u>ユーザー</u> I	<u>D</u>	版設設計成初 <u>日時</u>	証明書	欠	スク
■エクスポート		test	user	<u>test</u>			発行	変更	削除
■ 1 ンホート ■ ユーザーパスワー	ードポリシー				🤰 ユーザー設	定			
■ デフォルトユーザ	ープロファイル				編集対象: 非	ŕ規			
					ユーザー情報	チェックアイテム リプラ・	(7754	OTP	
					<u>建</u> 44 mm		user01		
					E-Mail				<u>^</u>
					詳細情報				<u> </u>
項目	値						user01		
			, ,		パスワード・		•••••		
姓	user01	user02	user03		バスワード(確	없)* 동나	•••••	•	
フーザーロ	user01	user02	user03						
				-					a alguli Witte
パスワード	password	password	password						
NetAttest	EPS	保存されている	い優定またはデータ床	あります!			- 27	口グ	オン中: admin 11 ログオコ
reens local		<u> </u>							
■ システム設定		<u> ユーザー・</u>	ĺ.						
■ システム管理 ■ 証明機関			● 一部 ● 完全	グループ 💙		ユーザーまで 検索			
■ DHCPサーバー		詳細 <u>イノンヨンの設定</u> エクスポート							
■ LDAPサーバー									追加
■ RADIOS ワーバー ■ ユーザー			×.	7.15		<u>ユー</u> 最終認証成功	ザー削除時	の証明書失	効オブション
■ ユーザー一覧				<u></u> _	<u>v</u>	日時	副明書	9. 	
■エクスホート ■インポート		test	iser	test			発行	変更	削除
■ ユーザーパ <u>スワ</u> ー	ードポリシー	user	r01	user01			発行	変更	削除

#### 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。

NetAttest EPS					↑ トップページ	ログオン中:	admin オフ
■ nacps.local ■ システム設定 ■ システム管理 ■ 証明機関 ■ DHCPサーパー	ユーザー <u></u> 注細オブションの設定 エクスポート	完全 グルーナ 💙	ユーザーまで	検索			
■ LDAPサーバー ■ RADIUSサーバー ■ ユーザー	■名前	<u>ユーザーID</u>	<u>最終認証成功</u>	<u>ユーザー</u> 証明書	<u>削除時の証明</u> タス	追り 唐夫効オプジ <b>ク</b>	加 ション
■ ユーザー一覧 ■ エクスポート ■ <i>とい</i> ポート	test user	test	<b>上時</b> 2016/06/17 16:	証明書	変更	削除	
■ ユーザーパスワードポリシー	user01	user01		発行	変更	削除	
NetAttest EPS					♥ ● トップページ	ログオン中: ジ 📵 ログ	: admin iオフ
<ul> <li>■ naeps.local</li> <li>● システム設定</li> <li>● システム管理</li> <li>● 証明機関</li> <li>■ DHCPサーバー</li> <li>■ LDAPサーバー</li> <li>■ LDAPサーバー</li> <li>■ ユーザーバー</li> <li>■ ユーザー一覧</li> <li>■ エクスポート</li> <li>■ インポート</li> <li>■ ユーザーパスワードポリシー</li> <li>■ デフォルトユーザープロファイル</li> </ul>	<ul> <li>ユーザー設定</li> <li>編集対象: user01</li> <li>ユーザー情報 チェックアイテム</li> <li>標準のリプライアイテム</li> <li>SessionTimeout</li> <li>VLAN ID</li> <li>Filter ID</li> <li>任意のリプライアイテム</li> <li>アトリビュート</li> </ul>	リナナ・イテム OTP 1800	値 ( ) ( キャンセル)	グ 0 適用			

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				() ->> ->> ->> ->> ->> ->> ->> ->	-ジ) 🕞 🖁	ログ 定保存 ) (	オン中: admi む ログオフ
<ul> <li>næpslocal</li> <li>システム設定</li> <li>システム管理</li> <li>証明機関</li> <li>DHCPサーバー</li> <li>LDAPサーバー</li> </ul>	<u>。</u> ユー ユーザー 詳細オブション/ エクスポート	ザ覧 <u></u>	完全 グルーナ 💙	ユーザーまで「検索	1		追加
・ MALIGS 7-7-7- = ユーザー = ユーザー 重 クスポート ■ アクポート		名前 test user	<u>ユーザーID</u> <u>test</u>	ユニ 最終認証成功 日時		の証明書失 タン 変更	効オブション <b>スク</b> <u> 削除</u>
<ul> <li>■ ユーザーバスワードボリシー</li> </ul>		user01	<u>user01</u>		発行	変更	削除

編集対象: user01	
基本情報	
姓	user01
E-Mail	
詳細情報	0
認時報	
ユーザーID	user01
有効期報 ● 日数 <mark>365</mark> 日 ● 日付 2016 ✔ 年	7 >月 9 > 日 23 > 時 59 > 分 59 > 秒まで
証明書ファイルオプション	
パスワード	
パスワード(確認)	
▼ PKCS#12ファイルして評理目機	関の証明見まな今める
	発行 キャンセル

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。

E	_ECOM
ユーザー名:	admin
パスワード:	•••••
言語:	日本語
	ログイン

[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。

ELECOM			
EHB-SG2B08-PL Web	Smart Gigabit Switch 🛛 🗮 🔹	設定保存 ログアウト	
スイッチ情報	設定		
5274	IPv4 設定		
・ システム管理	MACアドレス: BC:5C:4C:48:C1:59		
* iPv4 設定	IPアドレス: 192 168 10 1		
· IPv6 設定	サブネットマスク: 255 255 0 デフォルトゲートウェイ: 192 168 10 254		
・IPv6ネイバー	IPE-N: Static •		
· DNS			
・ IPアクセスリスト		逾用	
* 管理者			
・ユーザーインターフェイ ス			
・システム時間			
· SSL			
* DHCP自動設定			
・システムログ		TO	/+
- SNMP		現日	10000000000000000000000000000000000000
RMON		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。

ELECOM	
EHB-SG2B08-PL Web	Smart Gigabit Switch 📪 認定保存 ログアウト
スイッチ情報	Tagged ポート 転送 ダイナミック プライベート 現在の設定
システム	Tagged VLAN設定
ネットワーク	VI AN ID : 10 (2-4094)
・物理インターフェイス	VLAN名: VLAN0010 (32文字以下)
・スパニングツリー	管理画画へのログイン: 有効 •
・ トランキング	Static Tagged
* ミラーリング	全て選択
・ループ防止	1 2 3 4 5 6 7 8 9 10
<ul> <li>Static Unicast</li> </ul>	Static Untagged
Static Multicast	全て選択
· IGMP Shooping	1 2 3 4 5 6 7 8 9 10
・マルチキャストフィルタ	メンバーではない
-	A730
- 帯域制御	1 2 3 4 5 6 7 8 9 10
<ul> <li>VLAN</li> </ul>	
- Voice VLAN	Tagged VLANiBite
	Tagged VLANテーブル         VLAN ID :         20         (2-4094)
	VLAN ID         VLAN9-4プ         VLAN2 :         VLAN020         (32文字以下)           管理画面へのログイン:         無効・
	1 Default/UAN Permanent 10 VLAN0010 Static
	20 VLAN0020 Static Static
	1 2 3 4 5 6 7 8 9 10
	VLAN10 Static Untagged
	全て選択
	1 2 3 4 5 6 7 8 9 10
	メンバーではない

 VLANF
 VLANダイブ
 管理相応のログイン
 Active

 1
 Default/VLAN
 Permanent
 有効
 愛愛

 10
 VLAN010
 Static
 有効
 愛愛

 20
 VLAN020
 Static
 第約
 愛愛

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。

ELECOM	PWR 0 2 2 2 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	7 9 10 10 秒 × 6
EHB-SG2B08-PL Web S	mart Gigabit Switch 日本語 •	設定保存 ログアウト
スイッチ情報	設定	
システム	RADIUS設定	
ネットワーク	サーバープライオリティ: 1 ▼ (最高:1、最低:5)	
QoS	192 . 168 . 1 . 2 • IPV4	
PoE		IPv6
セキュリティ	Accounting Port : 1813 (1-65535)	
* ポートセキュリティ	Shared Secret : Secret (32文字以下)	
* ポートアクセス制御		20.40
ダイヤルインユーザ		
RADIUS	RADIUSテーブル	
TACACS+	サーバープライオ サーバーIPアドレス サーバーボート Accounting Po	ort Shared Secret Action
* 送信先MACフィルター	1 192.168.1.2 1812 1813	secret <b>资更 削除</b>
- ARPスプーフィング防止		
* サービス拒否		
<ul> <li>DHCP Snooping</li> </ul>		
- ACL		

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。

ELECOM		Prot 6 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0		天动的局 10 秒
EHB-SG2B08-PL Web S	Smart Gigabit Switch 🖪	本語 ・		設定保存 ログアウト
システム	設定			
ネットワーク	ボートアクセス制御設定			
QoS	NAS ID :	SolitonLab	16文字以下)	
PoE	ポートアクセス制御ステータス:	有効 •		
***		RADIUS •		
				適用 設定 設定ステータス
・ポートアクセフ制剤	ポートアクセス設定			
・ボードアクセス制御				
RADIUS	ボート: 認証モード:	1 • Initialize		
· TACACS+	ポート制御:	自動・		
・送信先MACフィルター	再認証ステータス:	無効・	項目	値
・ARPスプーフィング防止	サプリカントモート: Piggybackモード:	Single *		
・ サービス拒否	VLAN割り当て:	有効 *	NAS ID	Soliton ab
DHCP Snooping	Qos割り当て:	無効・		Sontoniedb
- ACL	ジストVLAN ID:	(1-4094)	ポートアクセフ制御	<b>17テータ7</b> 有効
ツール				
	送信間隔:	30 秒 (1-65535)	=ਲ਼=ਜ਼-++	DADILLE
		- BR IS PEPPER	前的正力式	KADIUS

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。

ELECOM		MAR 0 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			表新聞端 10 秒 ·	
EHB-SG2B08-PL Web S	6mart Gigabit Switch 🔳	本語 *		ž	定保存 ログアウト	
システム ネットワーク	設定			適用 設定	設定ステータス	
QoS PoE セキュリティ ・ボートセキュリティ ・ボートアクセス制御 ・ダイヤルインユーザ ・RADIUS ・TACACS+ ・送信先MACフィルター	ボートアクセス設定           ボート:           助臣モード:           ボート制節:           周辺正ステータス:           サブリカントモード:           Plogybackモード:           VLAN間の当て:           Oon割の登て:           セドニアVLAN:	Imitialize           802.1X         *           普致・         *           并つ・         *				
<ul> <li>ARPスプーフィング防止</li> <li>サービス拒否</li> <li>DHCP Snooping</li> </ul>	送信間隔: Quiet Period:	30 F9 (1-65535) 60 F9 (1-65535)	項目		値	
・ACL ツール	サブリカントタイムアウト: 	30 杉 (1-65535) 再認証ステータスはデフォルト期間600秒で常に	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。

ELECOM			Pwet 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	: 8		<b>3</b> 10		更新開展 10 秒
EHB-SG2B08-PL Web S	mart Gig	abit Switch	日本語・					設定保存ログアウト
システム		設定						
ネットワーク	NAS ID :		SolitonLab	(16文字	以下)			
QoS	ポートアク <sup>+</sup> 認証方式:	セス制御ステータス	t: 有効 T RADIUS	•				
PoE								
セキュリティ							適用 設定	設定ステータス
・ボートセキュリティ	現在の設定	ミステータス						
・ポートアクセス制御	NAS ID :		SolitonLab					
・ダイヤルインユーザ	802.1x ボー	トアクセス:	有効					
· RADIUS	認証方式:		RADIUS					
- TACACS+								
・送信先MACフィルター		802.1X	白動	実際店	Single	Piggyback.	N/A	1.10
	2	802.1X	自動	未認証	Single	無効	N/A	1.10
・ARPスプーフィング防止	3	802.1X	自動	未認証	Single	無効	N/A	1,20
・サービス拒否	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
DHCP Snooping	6	802.1X	強制認証	認証済	Single	無効	N/A	1,10
- ACL	7	802.1X	強制認証	即証済	Single	無効	N/A	1
	8	802.1X	強制認証	認証済	Single	無効	N/A	1,10,20
ツール	9	802.1X	強制認証	認証済	Single	無効	N/A	1
	10	802.1X	强制熔脏	認証満	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	NetAttest D3						
	ホスト名 nad3.local DNS 🗶 DHCP 🗶 DHCPv6 🗶						
<ul> <li>◆ システム設定</li> <li>ネットワーク設定</li> <li>ホスト</li> <li>スタティックルート</li> </ul>	<b>システム設定 - ネットワーク設定</b> LAN1(サービスインターフェイス)						
IPv6スタティックルート 日付と時刻	IPアドレス 🗹 192.168.1.3						
SNMP設定 ログ設定	サブネットマスク 🕑 255.255.255.0						
証明書	MACアドレス 00:0C:29:5E:12:8B						
管理者アカウント設定	IPv6アドレスの使用 ● 使用しない ● 自動設定のみ ● 手動設定						
セキュリティポリシー設定							
自動バックアップ設定 NetAttest D3Manager設定	IPv6ア デフォルトゲートウェイ						
◆ システム管理	デフォルトゲートウェイ 192.168.1.254						
✔ ドメインネームサービス	LAN2 IPv6デフォルトゲートウェイ						
✔ DHCPサービス	IPアドL						
✓ DHCPv6サービス	サブネッ ホスト名						
	ホスト名 S 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。

NetAttest D3								
	ホスト名 nad3.local DNS 🗙 DHCP	DHCPv6 🗶						
<ul> <li>✓ システム設定</li> <li>✓ システム管理</li> </ul>	DHCP - スコープのi	自加						
✔ ドメインネームサービス	スコープの設定							
◆ DHCPサービス	ネットワーク 🕑	192.168.10.0						
サーバー設定	サブネットマスク	255.255.255.0						
リース情報	ルーター	192.168.10.254						
<ul> <li>スコーノ</li> <li>登録クライアント</li> </ul>	ドメイン名	example.com						
静的割り当て	ドメインネームサーバー	192.168.1.254						
認証用NetAttest EPS設定 ユーザー定義オプション	レンジの設定							
ベンダー固有オプション NAP設定	レンジ開始アドレス	192.168.10.100						
✓ DHCPv6サービス	レンジ終了アドレス	192.168.10.150						
	除外レンジ開始アドレス							
	除外レンジ終了アドレス							
	OKキャンセル							

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。

NetAttest D3							
<ul> <li> (a) </li> </ul>	ホスト名 nad3.local DNS 3	K DHCP X DHCPv6 X					
<ul> <li>✓ システム設定</li> <li>✓ システム管理</li> </ul>	DHCP - サーノ	<b>ビー状態</b>					
✔ ドメインネームサービス	動作状態						
✓ DHCPサービス	サーバー稼動状態	動作中					
サーバー状態 サーバー設定	冗長化状態	冗長化しない					
リース情報 スコープ	IP使用率(%)						
登録クライアント	0%	2					
静的割り当て	0 / 41 max						
冗長化設定	起動 停止 初期化	リース情報全消去 MACアドレス使用履歴全消去	状態の更新				
認証用NetAttest EPS設定							



## 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。

	user01.p12	
₽ E	明書のインボート ウィザード	X 500000 84 0000 8 8
1	証明書のインポート ウィザードの開始	
c L	このウィザードでは、証明書、証明書信頼リスト、および証明書失効リスド します。	をディスクから証明書ストアにコピー
10 TO 1	E明機関によって発行された証明書は、ユーザー ID を確認し、データを保 されたネットワーク接続を提供するための情報を含んでいます。証明書スト 上の領域です。	護したり、またはセキュリティで保護 アは、証明書が保管されるシステム
	保存場所 ③ 現在のユーザー(○) ○ ローカル コンピューター(□)	
5	徳行するには、[次へ]をクリックしてください。	
		×
4 H	1. 2.K. 1. W. L. BER.	
174	ポートする証明書ファイル インボートするファイルを指定してください。	
	ファイル名(E): C#UsersHsoliton#DesktopHuse01.p12 注意:次の形式を使うと1つのファイルに複数の証明書を保管できます Personal Information Exchange- PKCS #12 (.PFX,P12) Cryptographic Message Syntax Standard- PKCS #7 証明書 (. Microsoft シリブル化された証明書ストア (.SST)	参照(B) : P7B)



#### 5.EAP-TLS 認証でのクライアント設定

← <i> </i>		×
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):		
•••••		
- 1ノルード オノジョン(): □ 秘密キーの保護を強力にする(E) このオナ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	1.20
□ 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。		
<ul> <li>マすべての拡張プロパティを含める(A)</li> </ul>		
	175 A /AD	العلم وحمد فأن
	次八(N)	キャンセル
		×
← 🔗 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)		
<ul> <li>証明書をすべて次のストアに配置する(P)</li> <li>応印曲コトア:</li> </ul>		
MC71ELATZ :	参照(	R)
	次へ(N)	キャンセル
← 27 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。		
<ul> <li>         選択された証明母ストア ウイザードで自動的に決定されます         内容         PFX     </li> </ul>		
ファイル名 C:\Users\U		
	完了(F)	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



#### 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。



## 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: [use	er03] (from client ELECOML2SW port 1 cli 60-45-BD-C-04-37)
EHB-SG2B シリーズ	1 local0/Info	Jul 10 16:31:36 802.1x Authentication success from (Username: user03,
EHB-SG2B-PL シリーズ	Port: 1, MAC: 6	0-45-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

ELECOM		1000M 10/100M	PWR 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			9 10		更新聞編 10 秒 🔹
EHB-SG2B08-PL Web Si	mart Gig	abit Switch	日本語 🔻					設定保存ログアウト
		設定						
システム								
ネットワーク	ポートアク	フセス制御設定						
QoS	NAS ID :		SolitonLab	(16文字」	以下)			
	ポートアク	セス制御ステータス	(: 有効 *					
PoE	認証方式:		RADIUS	·				
セキュリティ								
* ポートセキュリティ							適用設定	設定ステータス
* ポートアクセス制御	現在の設定	ミステータス						
・ダイヤルインユーザ	NAS ID :		SolitonLab					
- RADIUS	802.1x ポー	トアクセス:	有効					
- TACACS+	認証方式:		RADIUS					
区1876WAC 24769-	ボート	認証モード	ポート制御	認証ステータス	サプリカントモード	Piggyback	承認済MACアドレス	VLANUZE
* ARPスプーフィング防止	1	802.1X	自動	認証済	Single	無効	60-45-BD-FC-04-37	1,10
・サービス拒否	2	802.1X	自動	末認証	Single	無効	N/A	1,10
	3	802.1X	自動	未認証	Single	無効	N/A	1,20
<ul> <li>DHCP Snooping</li> </ul>	4	802.1X	目動	未認証	Single	無効	N/A	1,20
- ACL	5	802.1X	5虫市(総計) 2公共(1727元	単語目に)件 中和日本10文	Single	無効	N/A	1 10
	5	002.1X	りまゆりならる正 アムキリモの手に	AGAE2月 中辺中市2次	Single	無知	N/A	1,10
<u> </u>	8	802.1X	23(中)AcibLE 2会生15万5正	AUALL/M SZIERS	Single	無効	N/A N/A	1 10 20
	9	802.1X	強制認証	認証済	Single	無効	N/A	1



#### 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)
	34 local0/Info Jul 10 17:20:53 802.1x Authentication success from (Username:
EHB-SG2B シリーズ	user02, Port: 1, MAC: 60-45-bd-fc-04-37)
EHB-SG2B-PL シリーズ	31 local0/Info Jul 10 17:17:22 802.1x Authentication success from (Username:
	user01, Port: 1, MAC: 60-45-bd-fc-04-37)

現在の設定ステータス							
NAS ID: 802.1x ポートアクセス: 問題方式:		SolitonLab					
		有助					
		RADIUS					
#-1	245-1	A-1488	コンステータス	リプリカントモード	Pageback	REDWACT PL/2	VEANUXE
1.	802.1X	88	112.9	Single	1972	50-45-80-PC-04-37	10
	2000 C. C.		1.000				
4	802.1X	0.8	+ 1217	Sinte	10.00	NA	1.20
3	802.1X	WEINTE	1112 A	Sinde	#25	NA	1
6	802.1X	(WROLDLE	加延期	Single	10.05	NA	1,10
7	802.1X	IN ROUTER	結訂再	Single	8.5	NCA	f
	802.1X	強制認証	幼狂界	Single	無効	NA	1,10,20
3	802.130	被制度	助証滞	Single	10.0	NA	1
. 10	802.1X	WAILINE.	1012.00	Single	推动	NA	1

C:¥Users¥Soliton≻ipconfig	
₩indows IP 構成	
イーサネット アダプター イーサネット: 接続固有の DNS サフィックス IPv4 アドレス サブネット マスク デフォルト ゲートウェイ	.: soliton.co.jp .: 192.168.10.100 .: 255.255.255.0 .: 192.168.10.254



(III C) IZ Z	47-92						
NAS ID :		SolitonLab					
12 ta 25-	トアクセス:	812					
能力式:		RACIUS					
#->	34t-1	K-140	目前ステータス	サプリカントモード	Papeters	#EBMACPPUZ	VLABUZE
201	802.1X	1940	1012.9	Single	8.0	60-45-80-PC-04-37	20
3	802.1X	80	7.010	Single	863	NA	1.20
4	802.1X	88	未請試	Sinple	31(2)	NA	1,20
5	802 YK	1811111	ISTE A	Single	\$1.05	N/A	1
6	802 1X	Heat 1512	ISTER .	Single	31(2)	N/A.	1.10
7.	802.DE	(#\$(131))	出日来	Single	9115	N/A	1
8	802.5X	使利益证	LULE W	Single	無助	NA	1.10.20
2	802.5X	(#\$1252)	出日方	5494	3635	N/A	1
0.0	802.1X	085(121)	1212.00	Sitole	8423	NA	1

C:¥Users¥Soliton>ipconfig	
₩indows IP 構成	
イーサネット アダプター イーサネット:	
接続固有の DNS サフィックス ・・・・ IPv4 アドレス ・・・・・・・・・・	.: soliton.co.jp .: 192.168.20.100
サブネット マスク ・・・・・・・ デフォルト ゲートウェイ ・・・・・	.: 255.255.255.0 .: 192.168.20.254

User02の場合

## Seliton 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