

NetAttest EPS

認証連携設定例

【連携機器】 ハンドリームネット SubGate(SG2220G)

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

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、ハンドリームネット社製 L2 スイッチ SubGate(SG2220G)の IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN 認証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 SubGate 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

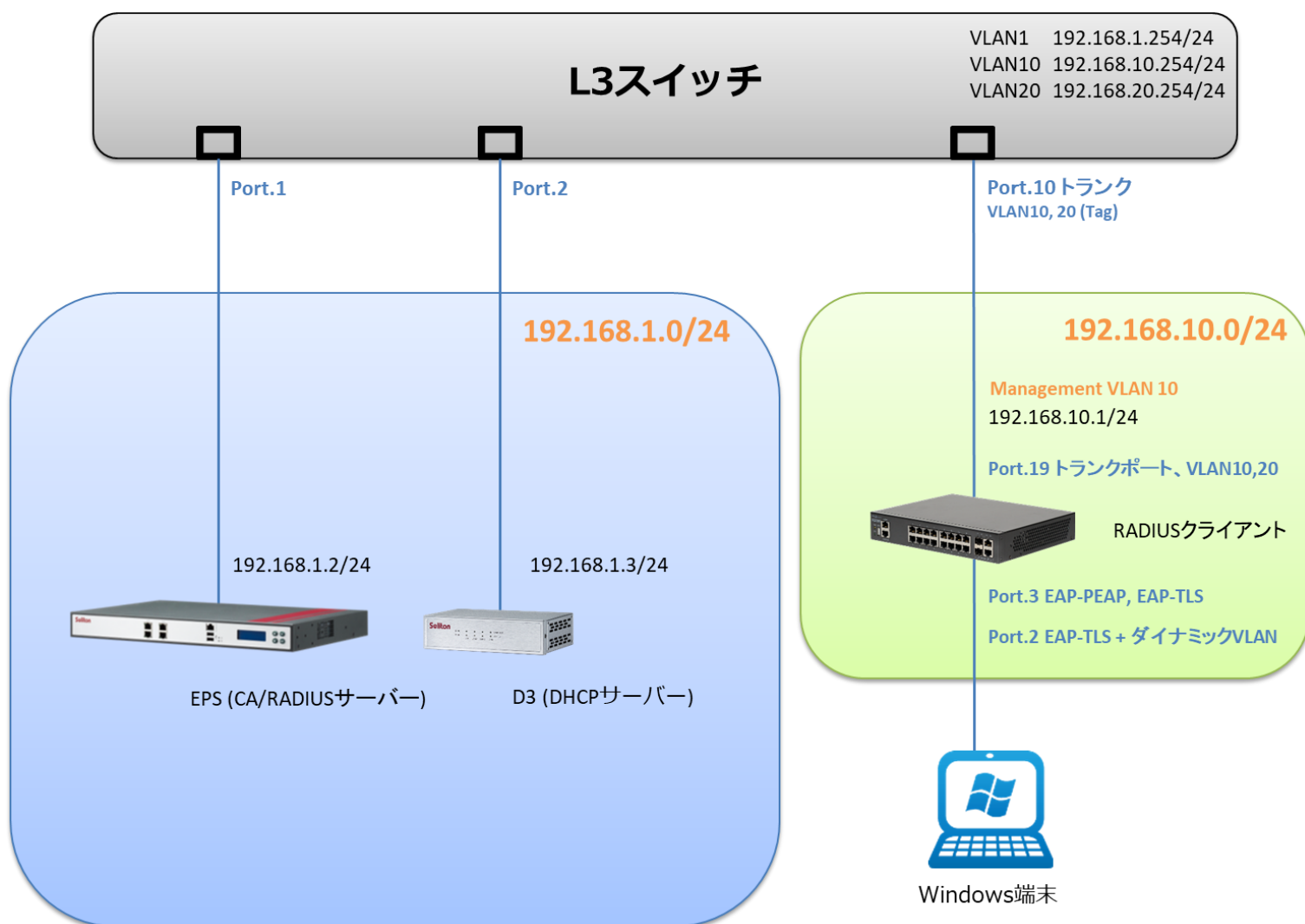
1. 構成.....	2
1-1 構成図	2
1-2 環境.....	3
1-2-1 機器	3
1-2-2 認証方式	3
1-2-3 ネットワーク設定.....	3
2. NetAttest EPS の設定	4
2-1 初期設定ウィザードの実行	4
2-2 システム初期設定ウィザードの実行.....	5
2-3 サービス初期設定ウィザードの実行.....	6
2-4 ユーザーの登録.....	7
2-5 ユーザーのリプライアイテムの設定.....	8
2-6 クライアント証明書の発行	9
3. SubGate(SG2220G)の設定	10
3-1 VLAN の作成	11
3-2 ネットワーク設定.....	12
3-3 dot1x 関連設定(global)	12
3-4 RADIUS サーバー設定	13
3-5 認証端末の Interface 設定(dot1x)	13
4. Windows 10 のクライアント設定.....	14
4-1 EAP-PEAP 認証.....	14
4-2 EAP-TLS 認証	15
4-2-1 クライアント証明書のインポート.....	15
4-2-2 サブリカント設定	17
5. 動作確認結果	18
5-1 EAP-PEAP 認証.....	18
5-2 EAP-TLS 認証	19
5-3 EAP-TLS+ダイナミック VLAN 認証	20
付録 L3 スイッチの設定	22
ポート設定、DHCP リレー設定.....	22

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-SX15 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/user01 用)
 - ・ VLAN10 : 192.168.10.0/24 (ダイナミック VLAN/user02 用)
 - ・ VLAN20 : 192.168.20.0/24 (ダイナミック VLAN/user03 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 = authentication server	4.10.5
SubGate(SG2220G)	ハンドリームネット	RADIUS クライアント = authenticator (L2 スイッチ)	2.2.8.9
VAIO Pro PB	VAIO	802.1X クライアント = Supplicant (Client PC)	Windows 10 64bit Windows 標準サブリカント
NetAttest D3-SX15	ソリトンシステムズ	DHCP/DNS サーバー	4.2.19

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#01
SubGate(SG2220G)	192.168.10.1/24		Secret#01
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。

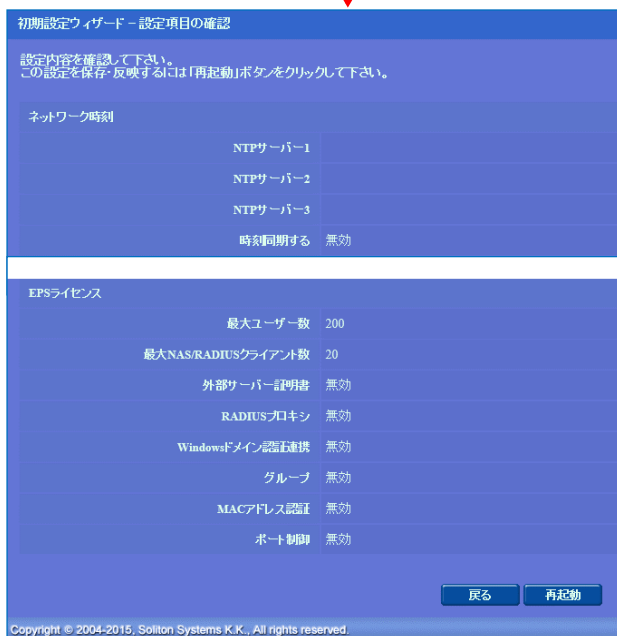
下記のような流れでセットアップを行います。

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

システム初期設定ウィザードを実行します。

- 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.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

初期設定ウィザード - CA構築

CA種別選択
CA種別選択: ルートCA

CA秘密鍵
 内部で新しい鍵を生成する
 公開鍵方式: RSA
 鍵長: 2048
 外部PKMFデバイスの鍵を使用する

署名の署名
署名アルゴリズム: SHA256

CA情報
CA名(必須): TestCA
 国名: 日本
 都道府県名: Tokyo
 市区町村名: Shinyuku
 会社名(組織名): Soliton Systems
 部署名:
 Eメールアドレス:

CA署名設定
署名アルゴリズム: SHA256

Copyright © 2004-2016, Soliton Systems K.K. All rights reserved.

項目	値
CA 種別選択	ルート CA
公開鍵方式	RSA
鍵長	2048
CA 名	TestCA

初期設定ウィザード - RADIUSサーバーの基本設定

EAP
EAP認証タイプ
優先順位: 認証タイプ
1: TLS
2: PEAP
3: TLS
4: EAP-FAST

EAP-TLS/TLS/PEAPオプション
メッセージングボディサイズ: 1024 バイト
メッセージの長さ情報: フラグメントなし 最初のボディのみ含まれる

EAP-TLS/PEAPオプション
 GTC認証を有効にする
 TLSセッションキャッシュを有効にする

EAP-FASTオプション

戻る 次へ

Copyright © 2004-2016, Soliton Systems K.K. All rights reserved.

項目	値
優先順位	EAP 認証タイプ
1	TLS
2	PEAP

初期設定ウィザード - NAS/RADIUSクライアント設定

編集対象: 新規

NAS/RADIUSクライアント名: RadiusClient01

このNAS/RADIUSクライアントを有効にする

モデル名:
タイプ:
 NAS/RADIUSクライアント
 NASのみ
 RADIUSクライアントのみ

説明:
IPアドレス: 192.168.1.1
シークレット: Secret#01

所属するNASグループ:

戻る 次へ

項目	値
NAS/RADIUS クライアント名	RadiusClient01
IP アドレス	192.168.1.1
シークレット	Secret#01

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。

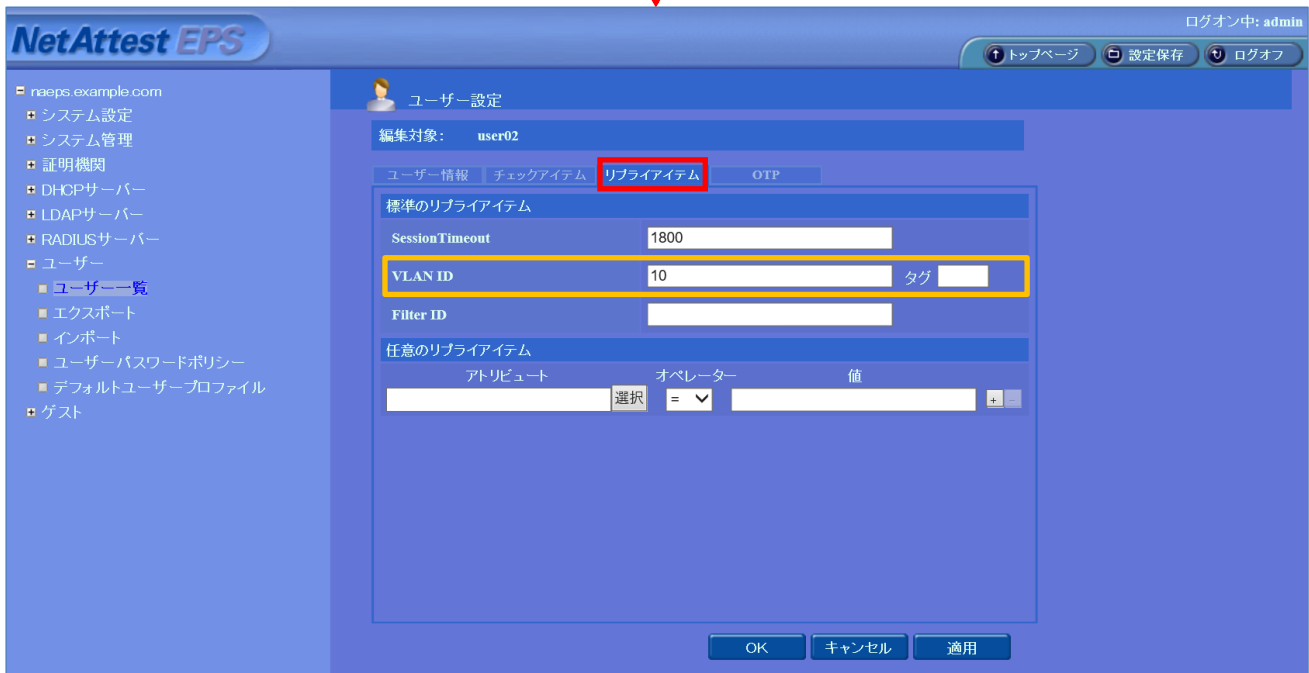
The screenshot shows the NetAttest EPS user management interface. The 'ユーザー一覧' (User List) table contains one entry: 'test user' with ID 'test'. A red box highlights the '追加' (Add) button. An arrow points to the 'ユーザー設定' (User Settings) form, which is pre-filled with 'user01' for the name and ID, and 'password' for the password. The 'OK' button is also highlighted with a red box. A red arrow points from the 'OK' button to the updated 'ユーザー一覧' table below.

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

名前	ユーザーID	最終認証成功日時	証明書	タスク
test user	test		発行	変更 削除
user01	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」を指定します。



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

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、赤い矢印が右側の詳細画面へと指している。

ユーザー「user01」の編集画面。証明書情報欄で有効期限を365日とし、「PKCS#12ファイルに証明機関の証明書を含める」がチェックされている。発行ボタンが赤い枠で囲われ、赤い矢印が下のダウンロード画面へと指している。

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：ユーザー証明書ダウンロードの準備ができました。対象をファイルに保存して下さい。ダウンロードボタンが赤い枠で囲われ、赤い矢印が下のダウンロード画面へと指している。

3. SubGate(SG2220G)の設定

SubGate(SG2220G)は初期化状態で出荷されます。管理 IP アドレスは設定されていないため、最初の設定は CONSOLE から行います。

1. VLAN の作成
2. IP アドレスなどネットワーク設定
3. dot1x 関連設定(global)
4. radius server 設定
5. 認証端末の Interface 設定(dot1x)
 - ・ IEEE802.1X EAP-PEAP(MS-CHAP V2)/EAP-TLS/EAP-TLS+ダイナミック VLAN

3-1 VLAN の作成

- vlan range <VLAN-ID#1, VLAN-ID#2, VLAN-ID… > bridge 1
//VLAN 作成。VLAN 10 は認証用の設定、20 は dynamic-vlan 割り当て用
- switchport trunk allowed vlan add <VLAN-ID>
//L3 スイッチと接続するため、ge19 に trunk port 設定変更と 10,20 を tag vlan で追加

※ 基礎的な操作やモード移行などコマンドについては説明を割愛させていただきます。

詳細は SubGate の use manual をご参照ください。

```
SG2220G>enable
SG2220G#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SG2220G(config)#
SG2220G(config)#vlan database
SG2220G(config-vlan)#
SG2220G(config-vlan)#vlan range 10,20 bridge 1
SG2220G(config-vlan)#exit
SG2220G(config)#
SG2220G(config)#interface ge19
SG2220G(config-if)#
SG2220G(config-if)#switchport trunk allowed vlan add 10,20
SG2220G(config-if)#
```

3-2 ネットワーク設定

- ip address <IP アドレス/Subnet>
//SubGate の IP アドレスを設定
- ip route 0.0.0.0/0 <default gateway IP アドレス>
//default route 指定

```
SG2220G#configure terminal
SG2220G(config)#
SG2220G(config)#interface vlan1.10
SG2220G(config-if)#
SG2220G(config-if)#ip address 192.168.10.1/24
SG2220G(config-if)#
SG2220G(config-if)#exit
SG2220G(config)#
SG2220G(config)#ip route 0.0.0.0/0 192.168.10.254
SG2220G(config)#
```

3-3 dot1x 関連設定(global)

- dot1x system-auth-ctrl
//SubGate で dot1x 認証機能を有効化
- dot1x vlan-notification
//dot1x 認証を行う場合、該当 VLAN 情報も転送

```
SG2220G(config)#
SG2220G(config)#dot1x system-auth-ctrl
SG2220G(config)#
SG2220G(config)#dot1x vlan-notification
SG2220G(config)#
```

3-4 RADIUS サーバー設定

- radius-server host 192.168.1.2 auth-port 1812 key ***** timeout 1 retransmit 3 mode dot1x

//radius サーバー(192.168.1.2)へ dot1x 認証の問い合わせを secret key(Secret#01)で行う

//timeout は失敗までの判断時間(1 秒)、問い合わせは 3 回まで

```
SG2220G(config)#
SG2220G(config)#radius-server host 192.168.1.2 auth-port 1812 key ***** timeout
1 retransmit 3 mode dot1x
SG2220G(config)#
```

3-5 認証端末の Interface 設定(dot1x)

- interface モードで dot1x port-control auto を設定(EAP-PEAP、EAP-TLS など対応)

```
SG2220G(config)#interface range ge1-16
% ge1-16 Selected
SG2220G(config-if-range)#dot1x port-control auto
% ge1-16 Selected
SG2220G(config-if-range)#exit
SG2220G(config)#
```

- ダイナミック VLAN 設定(認証成功によるポート開放と同時に指定した VLAN に割り当てる)

```
SG2220G(config)#interface ge1
SG2220G(config-if)#
SG2220G(config-if)#dot1x extension dynamic-vlan
SG2220G(config-if)#
SG2220G(config-if)#exit
SG2220G(config)#
```

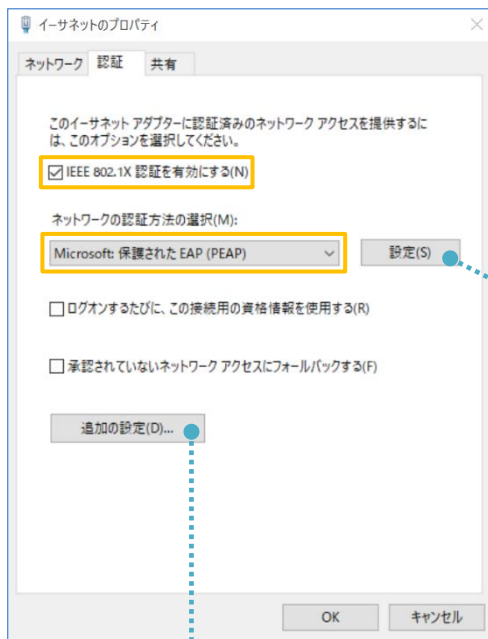

4. Windows 10 のクライアント設定

4-1 EAP-PEAP 認証

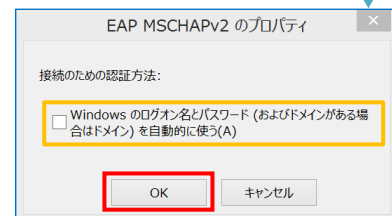
Windows 標準サブリカントで PEAP の設定を行います。

※ 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



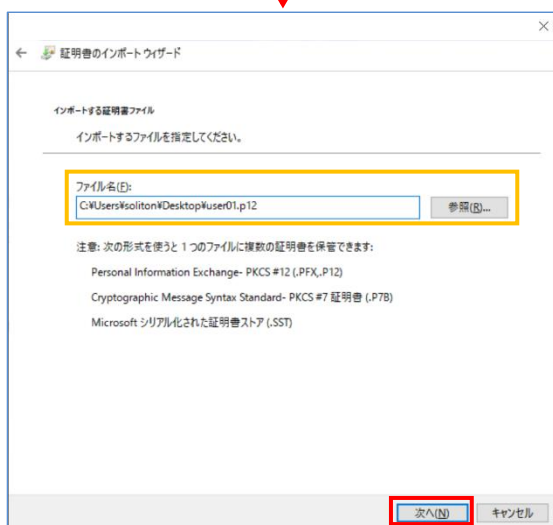
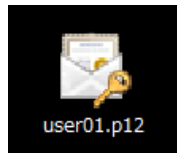
項目	値
認証モードを指定する	ユーザー認証

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
- 信頼されたルート証明機関	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コピーする(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(L)
 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

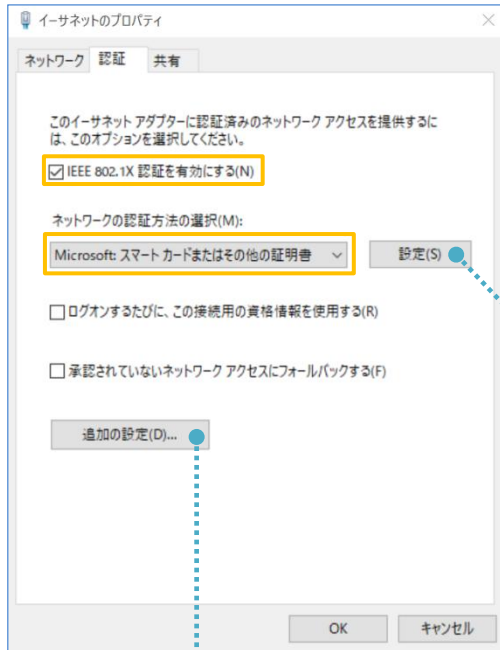
完了(F) キャンセル

4-2-2 サプリカント設定

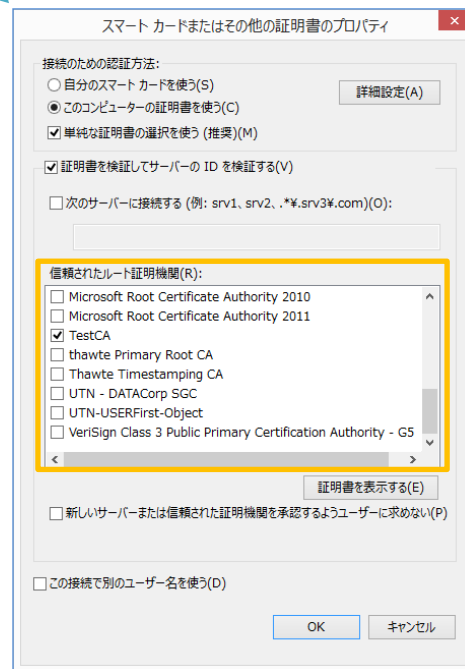
Windows 標準サプリカントで TLS の設定を行います。

※ 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

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: [user01] (from client RadiusClient01 port 5003 cli cc-30-80-32-8b-af via proxy to virtual server) Login OK: [user01] (from client RadiusClient01 port 5003 cli cc-30-80-32-8b-af)
SubGate(SG2220G)	802.1X: Authentication OK from ge3 mac(cc30.8032.8baf) username(user01)

```
SG2220G#show dot1x brief
port   instance  port-status  auth      supplicant  supplicant  successful
        type      address      name      auth-Type
-----
ge1    Master    Unauthorized Port
ge2    Master    Unauthorized Port
ge3    Master    Authorized   Port    cc30.8032.8baf  user01
ge4    Master    Unauthorized Port
ge5    Master    Unauthorized Port
ge6    Master    Unauthorized Port
ge7    Master    Unauthorized Port
ge8    Master    Unauthorized Port
ge9    Master    Unauthorized Port
ge10   Master    Unauthorized Port
--以下省略--
```

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: [user02] (from client RadiusClient01 port 5003 cli cc-30-80-32-8b-af)
SubGate(SG2220G)	802.1X: Authentication OK from ge3 mac(cc30.8032.8baf) username(user01)

```
SG2220G#show dot1x brief
port  instance  port-status  auth      supplicant  supplicant  successful
                                type      address      name      auth-Type
=====
ge1    Master    Unauthor ized  Port
ge2    Master    Unauthor ized  Port
ge3    Master    Author ized  Port  cc30.8032.8baf  user01
ge4    Master    Unauthor ized  Port
ge5    Master    Unauthor ized  Port
ge6    Master    Unauthor ized  Port
ge7    Master    Unauthor ized  Port
ge8    Master    Unauthor ized  Port
ge9    Master    Unauthor ized  Port
ge10   Master    Unauthor ized  Port
--以下省略--
```

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: [user02] (from client RadiusClient01 port 5002 cli cc-30-80-32-8b-af)
SubGate(SG2220G)	802.1X: Authentication OK from ge2 mac(cc30.8032.8baf) username(user02)

user02 の場合

```
SG2220G#show dot1x brief
```

port	instance	port-status	auth type	supplicant address	supplicant name	successful auth-Type
ge1	Master	Unauthorized	Port			
ge2	Master	Authorized	Port	cc30.8032.8baf	user02	
ge3	Master	Unauthorized	Port			
ge4	Master	Unauthorized	Port			
ge5	Master	Unauthorized	Port			
ge6	Master	Unauthorized	Port			
ge7	Master	Unauthorized	Port			
ge8	Master	Unauthorized	Port			
ge9	Master	Unauthorized	Port			
ge10	Master	Unauthorized	Port			

--以下省略--

```
C:¥WINDOWS¥System32>ipconfig
```

```
Windows IP 構成
```

```
イーサネット アダプター イーサネット1:
```

```
接続固有の DNS サフィックス . . . . . : example.com
IPv4 アドレス . . . . . : 192.168.10.100
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
```

user03 の場合

```
SG2220G#show dot1x brief
```

port	instance	port-status	auth type	supplicant address	supplicant name	successful auth-Type
ge1	Master	Unauthorized	Port			
ge2	Master	Authorized	Port	cc30.8032.8baf	user03	
ge3	Master	Unauthorized	Port			
ge4	Master	Unauthorized	Port			
ge5	Master	Unauthorized	Port			
ge6	Master	Unauthorized	Port			
ge7	Master	Unauthorized	Port			
ge8	Master	Unauthorized	Port			
ge9	Master	Unauthorized	Port			
ge10	Master	Unauthorized	Port			

--以下省略--

```
C:\WINDOWS\System32>ipconfig
```

Windows IP 構成

イーサネット アダプター イーサネット1:

```

接続固有の DNS サフィックス . . . . . : example.com
IPv4 アドレス . . . . . : 192.168.20.100
サブネット マスク . . . . . : 255.255.255.0
デフォルト ゲートウェイ . . . . . : 192.168.20.254

```


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。

