

NetAttest EPS

認証連携設定例

【連携機器】 パナソニック ES ネットワークス Switch-M24eG

【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、パナソニック ES ネットワークス社製 L2 スイッチ Switch-M24eG 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 Switch-M24eG 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

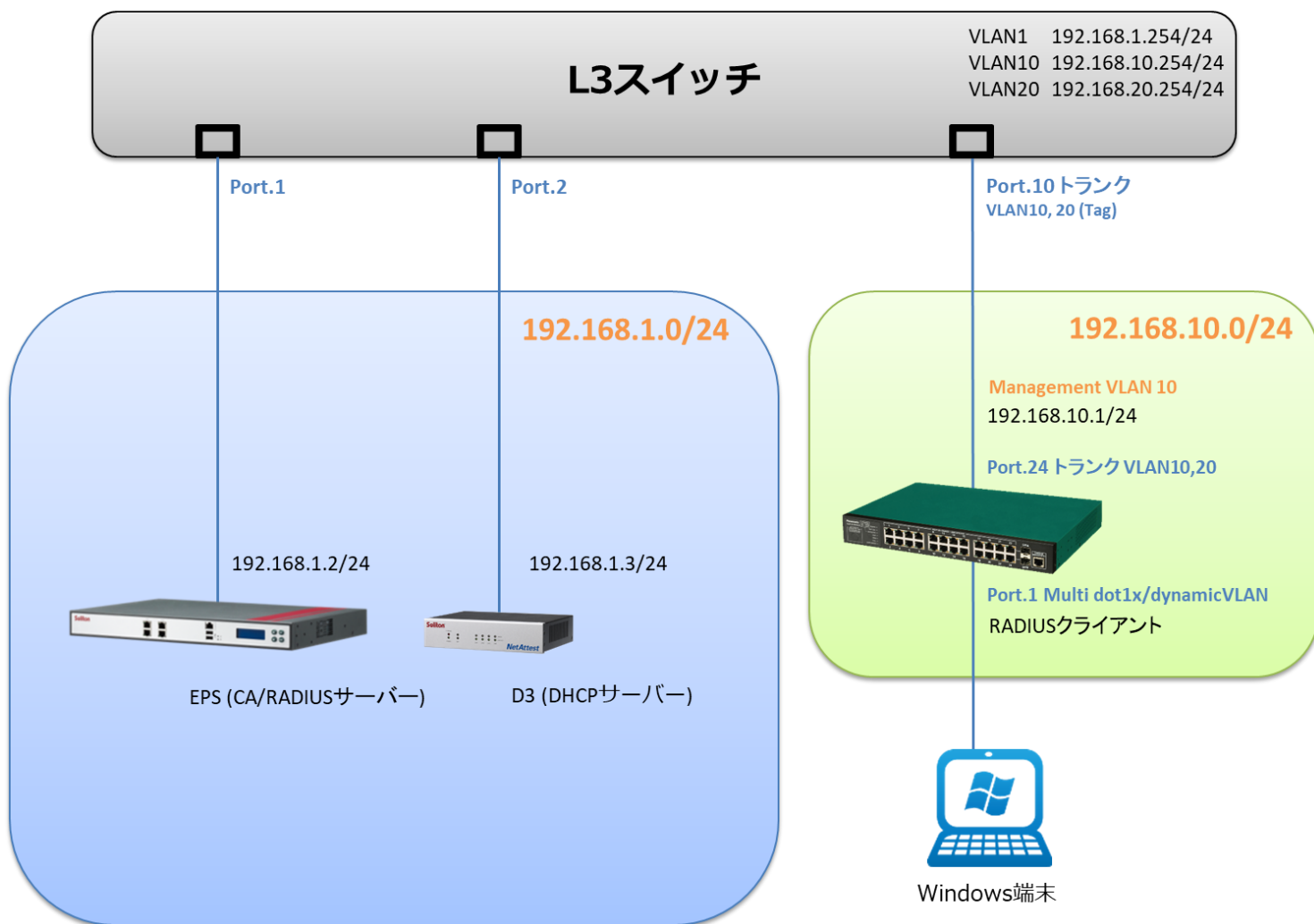
1. 構成.....	1
1-1 構成図	1
1-2 環境.....	2
1-2-1 機器	2
1-2-2 認証方式	2
1-2-3 ネットワーク設定.....	2
2. NetAttest EPS の設定	3
2-1 初期設定ウィザードの実行	3
2-2 システム初期設定ウィザードの実行.....	4
2-3 サービス初期設定ウィザードの実行.....	5
2-4 ユーザーの登録.....	6
2-5 ユーザーのリプライアイテムの設定.....	7
2-6 クライアント証明書の発行	8
3. Switch-M24eG の設定	9
3-1 ネットワーク設定.....	10
3-2 RADIUS サーバー設定	12
3-3 認証ポート設定.....	13
3-4 Config 設定情報確認	14
4. Windows 10 のクライアント設定.....	15
4-1 EAP-PEAP 認証.....	15
4-2 EAP-TLS 認証.....	16
4-2-1 クライアント証明書のインポート.....	16
4-2-2 サプリカント設定.....	18
5. 動作確認結果	19
5-1 EAP-PEAP 認証.....	19
5-2 EAP-TLS 認証.....	20
5-3 EAP-TLS+ダイナミック VLAN 認証	21
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-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	4.10.3
Switch-M24eG	パナソニック ES ネットワークス	RADIUS クライアント (L2 スイッチ)	2.0.1.08
VAIO Pro PB	VAIO	802.1X クライアント (Client PC)	Windows 10 64bit Windows 標準サブプリカント
NetAttest D3-SX04	ソリトンシステムズ	DHCP/DNS サーバー	4.2.16

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
Switch-M24eG	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。

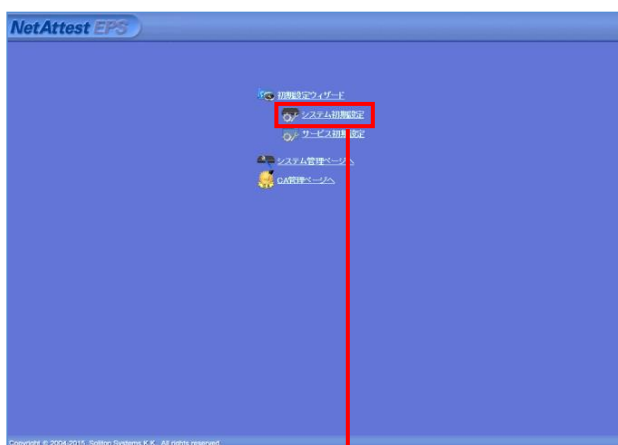
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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) table contains one entry: 'test user' with ID 'test'. A red box highlights the '追加' (Add) button. An inset window shows the 'ユーザー設定' (User Settings) form for a new user. The form fields are as follows:

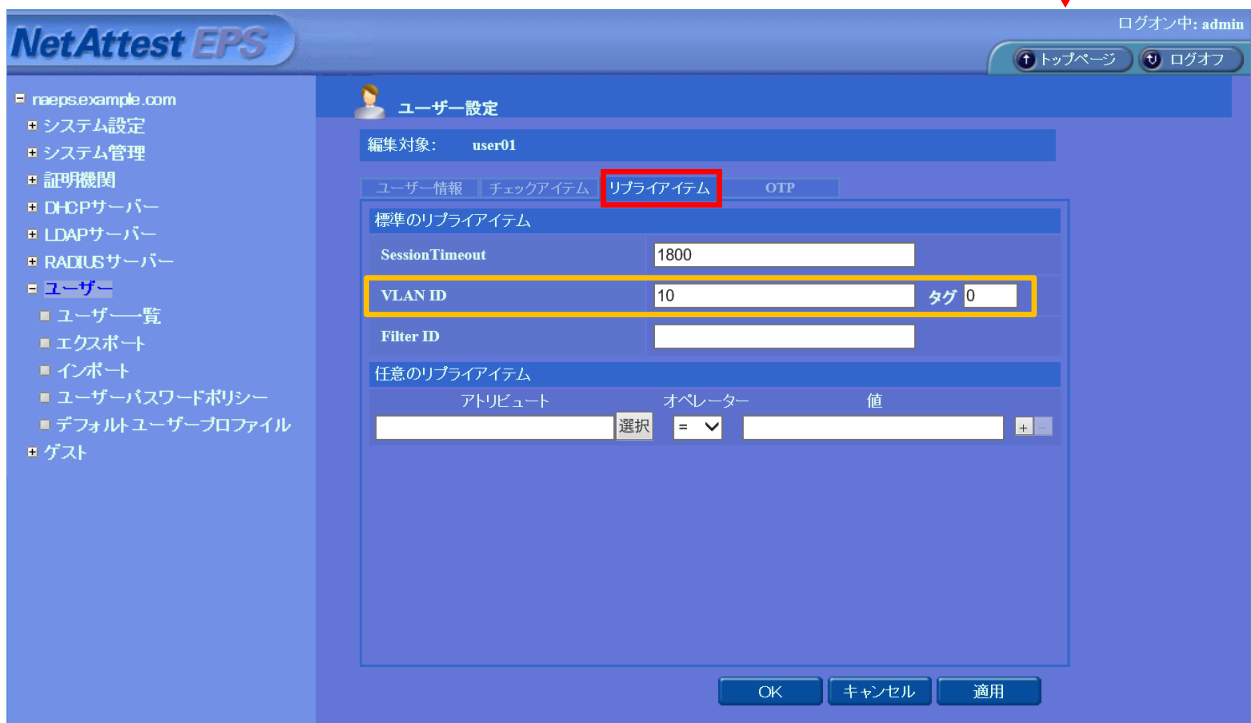
項目	値
姓	user01, user02, user03
ユーザーID	user01, user02, user03
パスワード	password, password, password

The 'ユーザー設定' form includes fields for: 姓 (Last Name), 名 (First Name), E-Mail, 詳細情報 (Detailed Information), 認証情報 (Authentication Information), ユーザーID (User ID), パスワード (Password), パスワード(確認) (Confirm Password), and a checkbox for 一時利用停止 (Temporary Suspension). The 'OK' button is highlighted with a red box.

The final screenshot shows the 'ユーザー一覧' table with two entries: 'test user' and 'user01'. The 'user01' entry is highlighted with a red box, indicating successful registration.

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伸びています。

ユーザー「user01」の編集画面。黄色い枠で「証明書情報」の「有効期限」が365日と設定されていることが確認できます。また、「証明書ファイルオプション」で「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ます。赤い「発行」ボタンが下部に配置されています。

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。」が表示されています。赤い「ダウンロード」ボタンが下部に配置されています。

3. Switch-M24eG の設定

工場出荷状態の Switch-M24eG は、コンソールポートにコンソールケーブル(RJ45-DSub9 ピン)を接続し、ターミナルソフトを用いて以下の通り設定します。

※Switch-M24eG は、Web 設定、メニュー設定、CLI 設定の 3 つの設定方法があります。

本書では CLI での設定方法について記載します。

【ターミナルソフトの設定例】

Tera Term: シリアルポート 設定

ポート(P): COM1

ボー・レート(B): 9600

データ(D): 8 bit

パリティ(A): none

ストップ(S): 1 bit

フロー制御(F): none

送信遅延

0 ミリ秒/字(C) 0 ミリ秒/行(L)

OK

キャンセル

ヘルプ(H)

項目	値
ボー・レート(B)	9600
データ(D)	8bit
パリティ(A)	none
ストップ(S)	1bit
フロー制御(F)	none

3-1 ネットワーク設定

Switch-M24eG を起動させた状態で、ターミナルソフトを起動し、Switch-M24eG にログインします。

※初期設定は、ユーザー名 : manager パスワード : manager です。

```
=====
PN28240K Local Management System Version 2.0.1.04
MAC Address: 00:50:40:3A:0D:7E
=====

Login Menu

Login: manager
Password: *****
```

メニューの設定画面が表示されるため、“c”を入力し、CLIモードに移行します。

```
PN28240K Local Management System

Main Menu

[G]eneral Information
[B]asic Switch Configuration...
[A]dvanced Switch Configuration...
[S]tatistics
Switch [T]ools Configuration...
Save Configuration to [F]lash
Run [C]LI
[Q]uit
Command>
Enter the character in square brackets to select option
```

“enable” ⇒ “configure” の順にコマンドを実行し、コンフィグレーションモードに移行します。

“interface vlan10” コマンドにて VLAN10 を作成+VLAN モードに移行後、メンバーの追加コマンド “member 24” 並びに “management” コマンドにて管理ポートとして設定を実行します。

“interface vlan20” コマンドにて VLAN20 を作成+VLAN モードに移行後、メンバーの追加コマンド “member 24” を実行します。

“interface vlan1” のモードに移行し、管理ポートの設定を“no management” コマンドで無効にします。

※VLAN1 はデフォルト設定で 1-24 がメンバーポートに設定されています。

“exit” にてコンフィグレーションモードに移行後、

“ip address 192.168.10.1 255.255.255.0 192.168.10.254” を実行し、Switch-M24eG の IP アドレスを設定します。

```
M24eG> enable
M24eG# configure
M24eG(config)# interface vlan10
M24eG(config-if)# member 24
M24eG(config-if)# management
M24eG(config-if)# interface vlan20
M24eG(config-if)# member 24
M24eG(config-if)# interface vlan1
M24eG(config-if)# no management
M24eG(config-if)# exit
M24eG(config)# ip address 192.168.10.1 255.255.255.0 192.168.10.254
Interface vlan1
  my HWaddr: 00:50:40:3a:0d:7e
  my IPaddr: 192.168.10.1
Options:
  subnet mask: 255.255.255.0
  IP broadcast: 192.168.10.255
  gateway: 192.168.10.254
M24eG(config)# █
```

項目	値		
VLAN ID	1	10	20
管理 VLAN	-	-	○
メンバー	1-24	24	24
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 RADIUS サーバー設定

コンフィグレーションモードにて “radius-server host 1 ip 192.168.1.2 key secret” コマンドを実行し、ホスト 1 に RADIUS サーバーの IP アドレス「192.168.1.2」と認証キー「secret」を設定します。

“aaa authentication mac primary radius secondary none” コマンドを実行し、MAC ベース認証のプライマリ DB を「radius」、セカンダリ DB を「none」に設定します。

```
M24eG(config)# radius-server host 1 ip 192.168.1.2 key secret
M24eG(config)# aaa authentication mac primary radius secondary none
M24eG(config)#
M24eG(config)#
```

項目	値
RADIUS サーバーホスト	1
ホスト 1# IP アドレス	192.168.1.2
ホスト 1# 認証キー	secret
AAA MAC ベース認証# プライマリ DB	radius
AAA MAC ベース認証# セカンダリ DB	none

3-3 認証ポート設定

“interface GigabitEthernet0/1” コマンドにてインターフェースモードに移行し、“dot1x port-auth-mode mac-based” コマンドにて対象のポートをデフォルト設定のポートベース認証から MAC ベース認証に変更します。

```
M24eG(config)# interface GigabitEthernet0/1
M24eG(config-if)# dot1x port-auth-mode mac-based
M24eG(config-if)#
M24eG(config-if)#
```

項目	値
MAC ベース認証ポート	0/1
ダイナミック VLAN	有効

※ダイナミック VLAN はデフォルト設定で有効となります。無効にしたい場合は、“no authentication dynamic-vlan radius-attribute”コマンドをコンフィグレーションモードにて実行します。

3-4 Config 設定情報確認

“end” コマンドにて enable モードに移行し、“show run” コマンドにて設定変更後の Config を確認します。

```
M24eG# show run
Building configuration...

Current configuration : 1460 bytes
! -- M24eG start of config file --
! -- Software Version : 2.0.1.08 --
!

enable
configure

radius-server host 1 ip 192.168.1.2 key secret
aaa authentication mac primary radius secondary none
password manager:KCsNFkTCsINy1ab4iil6+g==:0BArD1EK0C7ncCf27Ju9Ug==
!
interface GigabitEthernet0/1
 dot1x port-auth-mode mac-based
!
interface GigabitEthernet0/2
!
~以下中略~

interface GigabitEthernet0/24
exit
interface vlan1
 member 1-24
 no management
exit
interface vlan10
 member 24
 management
exit
interface vlan20
 member 24
exit
no watchdog timer
led base-mode status
telnet-server enable
ip address 192.168.10.1 255.255.255.0 192.168.10.254
snmp timezone 51
ip setup interface
!
exit
!
end
! -- end of configuration --
```

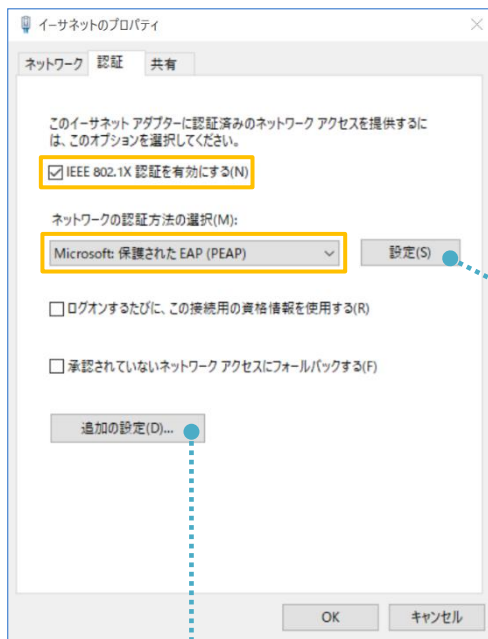
4. Windows 10 のクライアント設定

4-1 EAP-PEAP 認証

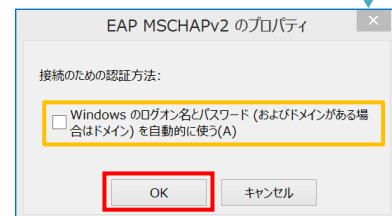
Windows 標準サブリカントで PEAP の設定を行います。

※ 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



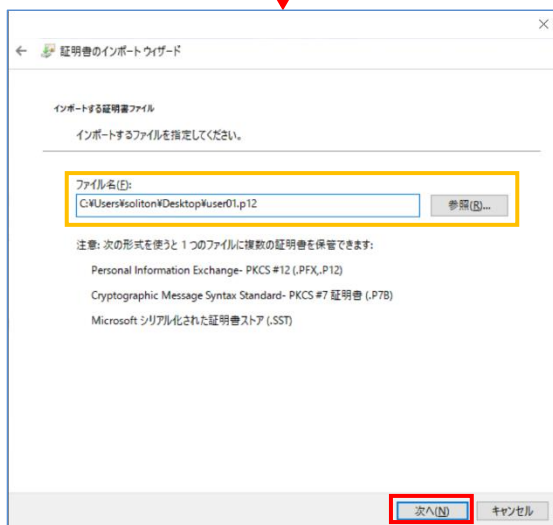
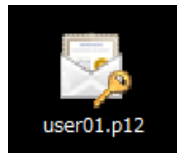
項目	値
認証モードを指定する	ユーザー認証

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(I):

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(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

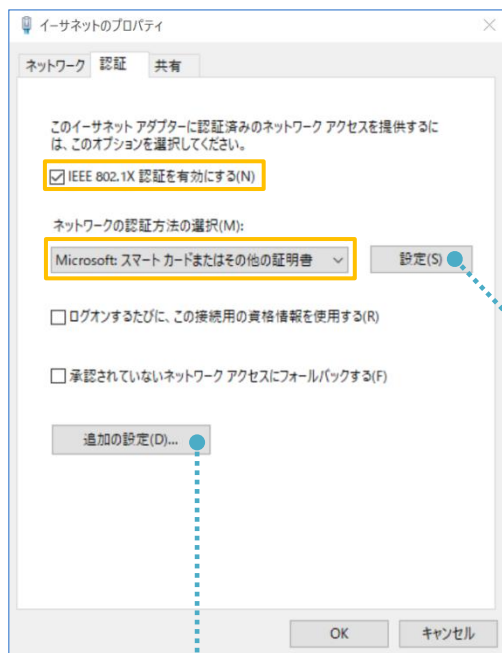
完了(F) キャンセル

4-2-2 サプリカント設定

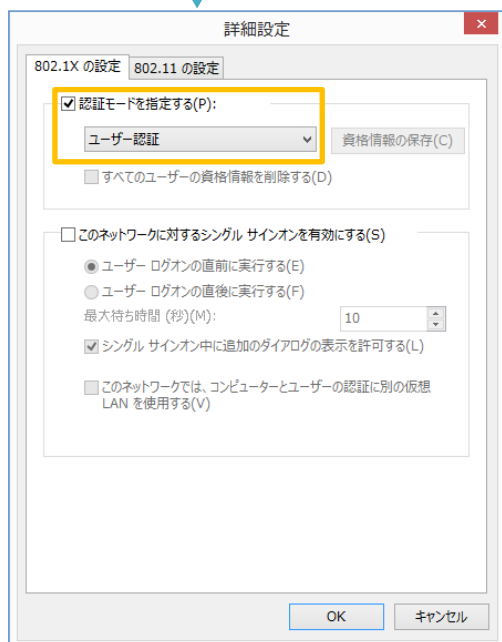
Windows 標準サプリカントで TLS の設定を行います。

※ 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
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

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)
Switch-M24eG	# show syslog authentication [802.1X](RADIUS)Authorized user user03 (CC:30:80:32:8B:AF) on Port 1 to VLAN 1

EAP-PEAP 認証が成功した場合の Switch-M24eG 認証状態のログ表示例

“show authentication sort mac” コマンドにて Auth Status “Authorized”を確認します。

```
M24eG# show authentication sort mac

Total Hosts    :1
Authorized Hosts :1
Auth Aging Time :1440 minutes

MAC Address    Port    Auth Type  Auth Status  Remaining Aging Time
-----
CC:30:80:32:8B:AF 1      802.1X    Authorized  ---
```

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)
Switch-M24eG	# show syslog authentication [802.1X](RADIUS)Authorized user user03 (CC:30:80:32:8B:AF) on Port 1 to VLAN 1

EAP-TLS 認証が成功した場合の Switch-M24eG 認証状態のログ表示例

“show authentication sort mac” コマンドにて Auth Status “Authorized”を確認します。

```
M24eG# show authentication sort mac

Total Hosts      :1
Authorized Hosts :1
Auth Aging Time :1440 minutes

MAC Address      Port   Auth Type  Auth Status  Remaining Aging Time
-----
CC:30:80:32:8B:AF 1      802.1X    Authorized   ---
```


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) Login OK: [user02] (from client RadiusClient01 port 1 cli CC-30-80-32-8B-AF)
Switch-M24eG	# show syslog authentication [802.1X](RADIUS)Authorized user user01 (CC:30:80:32:8B:AF) on Port 1 to VLAN 10 [802.1X](RADIUS)Authorized user user02 (CC:30:80:32:8B:AF) on Port 1 to VLAN 20

EAP-TLS 認証が成功した場合の Switch-M24eG 認証後 VLAN 割当状態のログ表示例

”show mac-address-table interface gi0/1” コマンドにて VLAN“(VLAN-ID)”を確認します。

User01(VLAN10)の場合

Switch-M24eG 側の VLAN 割り当て確認画面

```
M24eG# sh mac-address-table interface gi0/1

MAC Address      Address Type  VLAN  Port
-----
CC:30:80:32:8B:AF Dynamic      10   gi0/1
```

認証端末側の IP アドレス確認画面

```
C:\>ipconfig

Windows IP 構成

イーサネット アダプター Local:

    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
```

User02(VLAN20)の場合

Switch-M24eG 側の VLAN 割り当て確認画面

```
M24eG# sh mac-address-table interface gi0/1

MAC Address      Address Type  VLAN  Port
-----
CC:30:80:32:8B:AF Dynamic      20   gi0/1
```

認証端末側の IP アドレス確認画面

```
C:\>ipconfig

Windows IP 構成

イーサネット アダプター Local:

    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。

