NetAttest EPS
認証連携設定例

【連携機器】FXC FXC5200 シリーズ

【Case】IEEE802.1X EAP-TLS 認証/EAP-TLS 認証+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、FXC 社製 L2 スイッチ FXC5200 シリーズの IEEE802.1X EAP-TLS 認証/EAP-TLS 認証+ダイナミック VLAN 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 FXC5224 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 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. FXC5200 シリーズの設定 14
3-1 FXC5200 シリーズの設定について 14
3-2 FXC5200 シリーズの設定項目 15
3-2-1 VLAN 作成の設定 15
3-2-2 VLAN Tagged ポートの設定 15
3-2-3 IP アドレスとデフォルトゲートウェイの設定 15
3-2-3 RADIUS サーバー登録の設定 16
3-2-4 認証方式と Dynamic VLAN ポートの設定 16
4. NetAttest D3 の設定 17
4-1 ネットワーク設定 18
4-2 スコープ・レンジ設定 19
4-3 DHCP サーバーの起動 20
5. EAP-TLS 認証でのクライアント設定 21
5-1 Windows 8.1 での EAP-TLS 認証 21
5-1-1 クライアント証明書のインポート 21
5-1-2 サプリカント設定 23

6. 動作確認結果 24
6-1 EAP-TLS 認証 24
6-2 ダイナミック VLAN 25
付録 L3 スイッチの設定 26
ポート設定、DHCP リレー設定 26

1. 構成

1-1 構成図

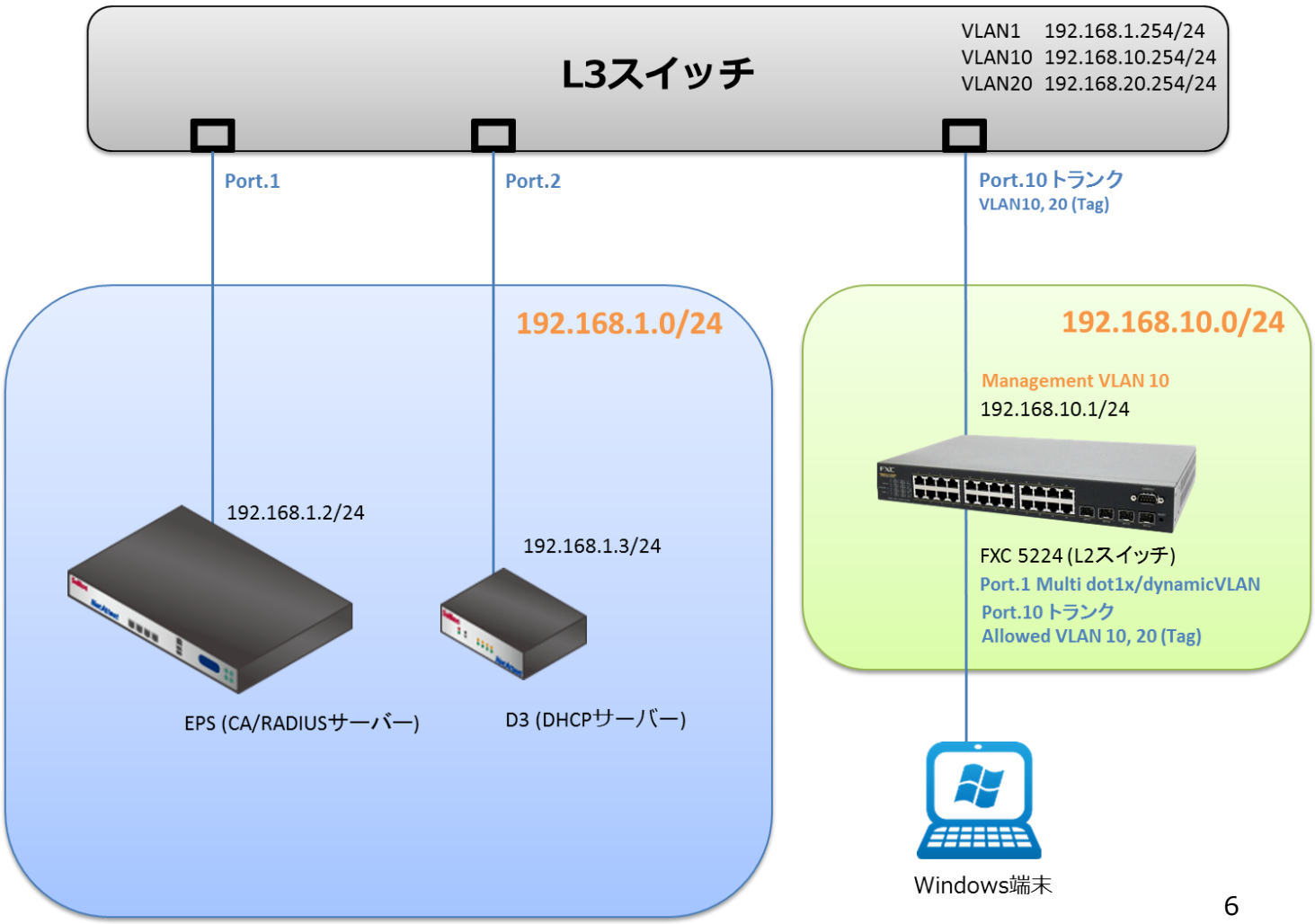
以下の環境を構成します。

・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
(FXC5200 管理、Dynamic VLAN/user01、認証のみ/user03 用)
- VLAN20 : 192.168.20.0/24 (Dynamic 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-ST04	Soliton Systems	RADIUS/CA サーバー	4.8.6
FXC5224	FXC	RADIUS クライアント (L2 スイッチ)	1.00.16
Surface	Microsoft	802.1X クライアント (Client PC)	Windows 8.1 64bit Windows 標準サプリカント
NetAttest D3-SX04	Soliton Systems	DHCP/DNS サーバー	4.2.4

1-2-2 認証方式

IEEE802.1X EAP-TLS 認証

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-ST04	192.168.1.2/24	UDP 1812	secret
FXC5224	192.168.10.1/24		secret
NetAttest D3-SX04	192.168.1.3/24		
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。

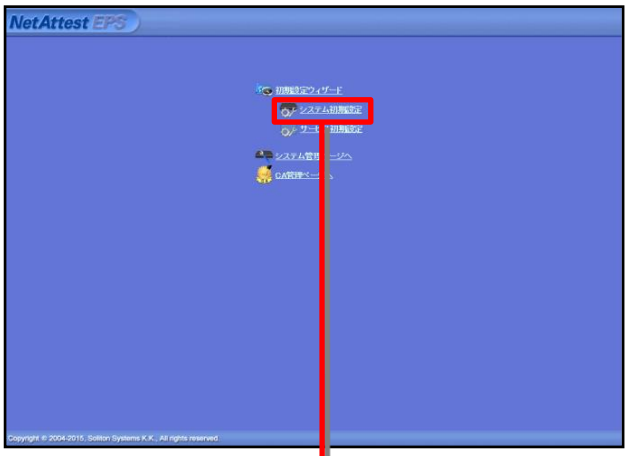
1. システム初期設定ウィザードの実行
2. サービス初期設定ウィザードの実行
3. RADIUS クライアントの登録
4. 認証ユーザーの追加登録
5. 証明書の発行

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

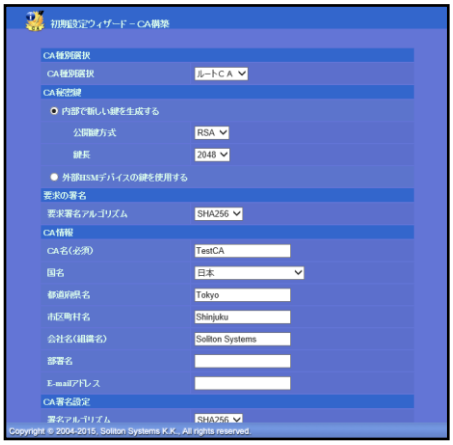


項目	値
ホスト名	naeps.local
IP アドレス	デフォルト
ライセンス	なし

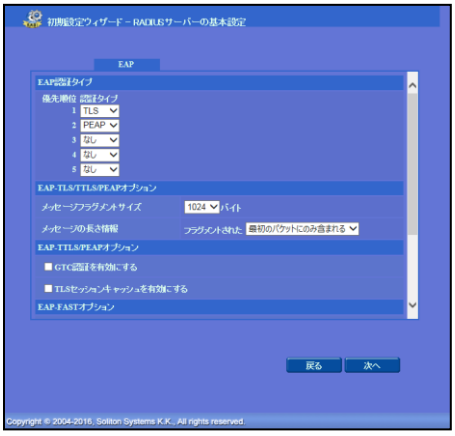
2-3 サービス初期設定ウィザードの実行

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

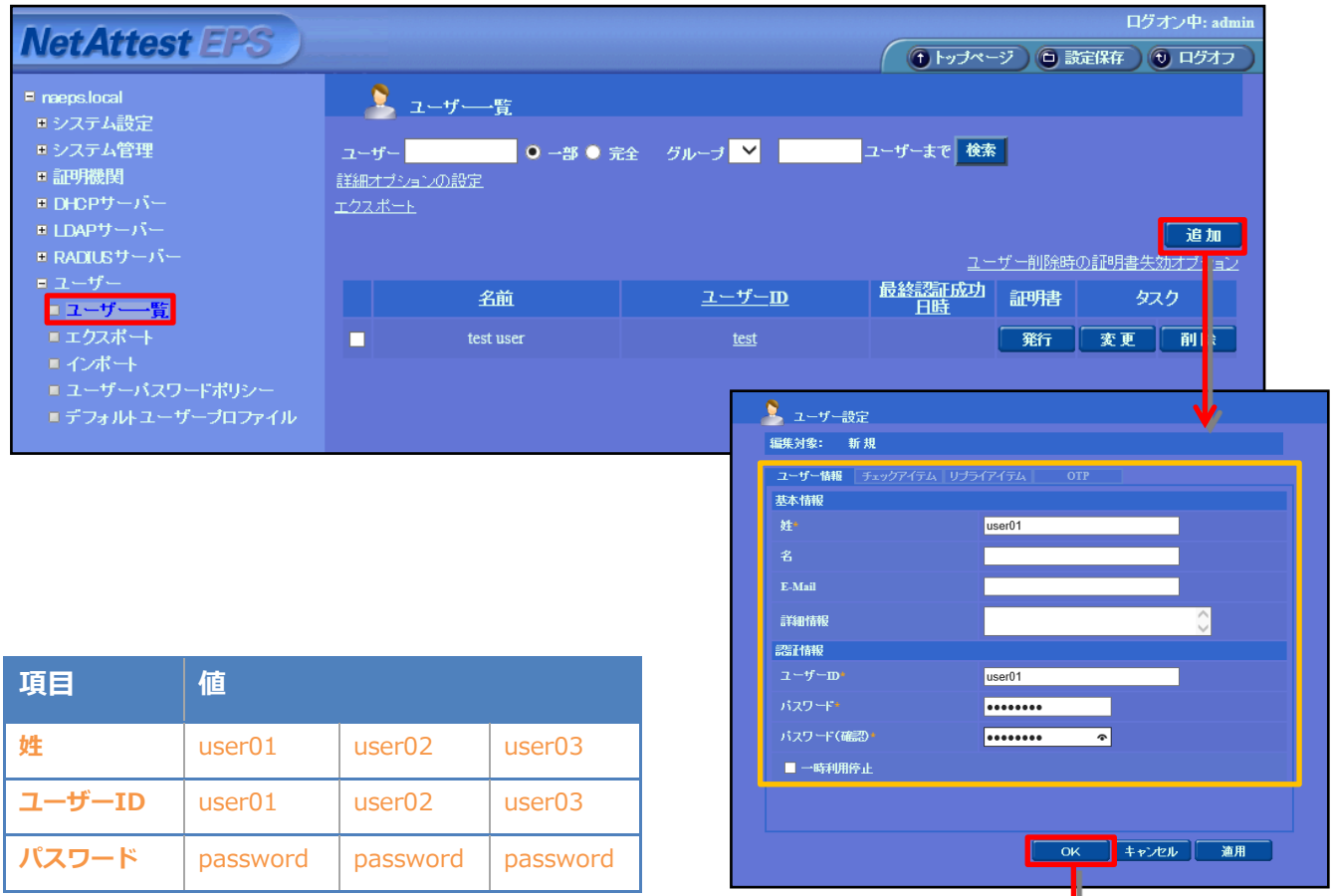


項目	値
EAP 認証タイプ	
1	TLS
2	PEAP

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。ダイナミック VLAN の対象とするユーザーとして user01, user02、認証可否のみを判断するユーザーとして user03 を作成します。

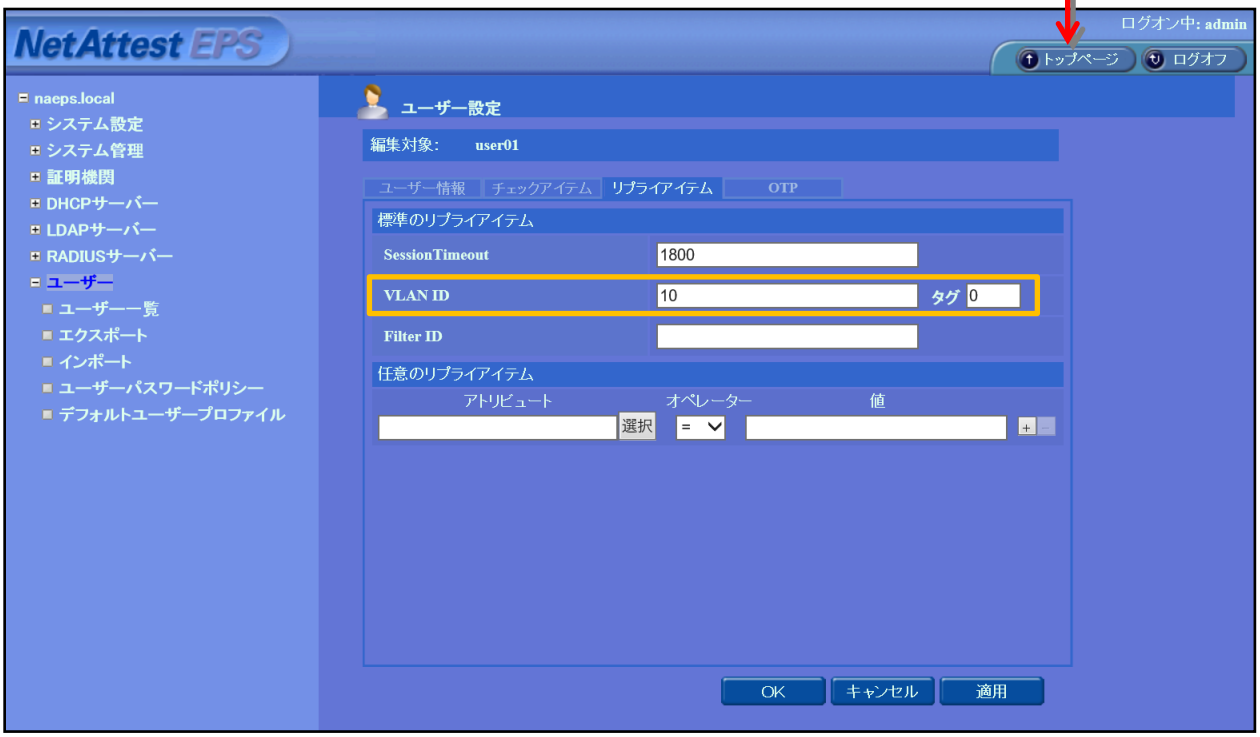


項目	値		
姓	user01	user02	user03
ユーザーID	user01	user02	user03
パスワード	password	password	password

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	-

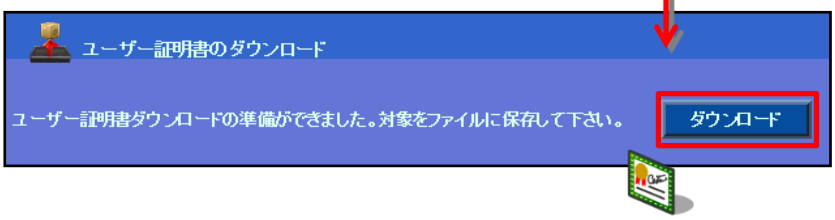
2-6 クライアント証明書の発行

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_02.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. FXC5200 シリーズの設定

3-1 FXC5200 シリーズの設定について

FXC 社製 L2 スイッチ FXC5200 シリーズの設定はシリアルコンソールポート(Baud Rate 115200)、有線接続による Telnet、WebGUI から行います。初期の IP アドレスは「192.168.1.1/24」です。

WebGUI より機器にアクセスする場合は管理端末に適切な IP アドレスを設定し Internet Explorer から「https://192.168.1.1/」にアクセスしてください。本書では CLI による各種設定方法を紹介します。

- 3-2-1　VLAN 作成の設定
- 3-2-2　VLAN Tagged ポートの設定
- 3-2-3　管理用 IP アドレスとデフォルトゲートウェイの設定
- 3-2-4　RADIUS サーバー登録の設定
- 3-2-5　認証方式と Dynamic VLAN ポートの設定

3-2 FXC5200 シリーズの設定項目

3-2-1 VLAN 作成の設定

FXC5200 スイッチ上に VLAN10、VLAN20 を作成します。

【コマンド】

```
FXC5224# configure
FXC5224(config)# vlan database
FXC5224(config-vlan)# vlan 10
FXC5224(config-vlan)# vlan 20
FXC5224#
```

3-2-2 VLAN Tagged ポートの設定

Uplink-port（L3 スイッチ接続）側のポートに vlan10、20 のタグ設定を行う。

【コマンド】

```
FXC5224# configure
FXC5224(config)# interface ethernet 1/10
FXC5224(config-if)# switchport allowed vlan add 10
FXC5224(config-if)# switchport allowed vlan add 20
FXC5224(config-if)# switchport tx_tag tag_all
FXC5224(config-if)# switchport mode c-port
FXC5224#
```

3-2-3 IP アドレスとデフォルトゲートウェイの設定

FXC5200 スイッチの Management VLAN10 に IP アドレスを設定し、サブネットが異なる RADIUS サーバー宛てのゲートウェイ設定を行います。

【コマンド】

```
FXC5224# configure
FXC5224(config)# interface vlan 10
FXC5224(config-if)# ip address 192.168.10.1 255.255.255.0
FXC5224(config-if)# exit
FXC5224(config)# ip default-gateway 192.168.10.254
FXC5224#
```

3-2-3 RADIUS サーバー登録の設定

IEEE802.1x 認証の有効および対象となる RADIUS サーバーの登録を行います。

※accounting、authentication のデフォルト UDP ポート番号は、それぞれ 1813、1812 です。

【コマンド】

```
FXC5224# configure
FXC5224(config)# dot1x mode
FXC5224(config)# radius-accounting-server 1 host 192.168.1.2
FXC5224(config)# radius-accounting-server 1 key secret
FXC5224(config)# radius-accounting-server 1 active
FXC5224(config)# radius-authentication-server 1 host 192.168.1.2
FXC5224(config)# radius-authentication-server 1 key secret
FXC5224(config)# radius-authentication-server 1 active
FXC5224#
```

3-2-4 認証方式と Dynamic VLAN ポートの設定

各インターフェイスにて IEEE802.1x 認証方式および Dynamic VLAN の有効化を行います。

今回は IEEE802.1x 認証方式 Multi 802.1x のポート設定例を紹介します。

※1:1 で FXC5200 シリーズの物理ポートと被認証端末が接続される為、動作としては Single 802.1x 認証方式でも同様の挙動となります。

※FXC5200 シリーズでは 1 つの物理ポートに対して以下の内から一つの認証方式を設定可能です。

- Auto
- Single 802.1x
- Multi 802.1x
- Mac Base

【コマンド】

```
FXC5224# configure
FXC5224(config)# dot1x radius_vlan
FXC5224(config)# interface ethernet 1/1
FXC5224(config-if)# dot1x port-control multi-802.1x
FXC5224(config-if)# dot1x radius-vlan
FXC5224#
```

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、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

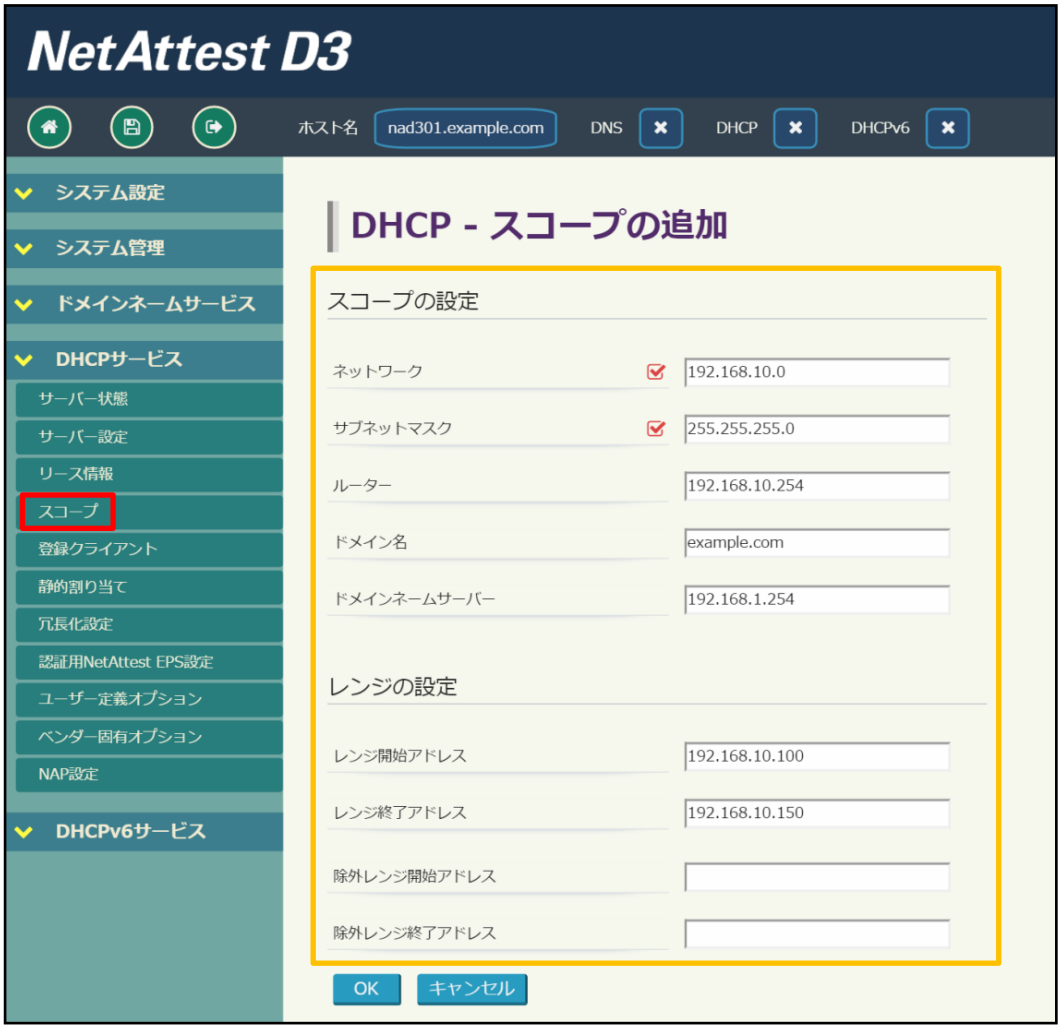
4-1 ネットワーク設定

[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	nad301.example.com

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を、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

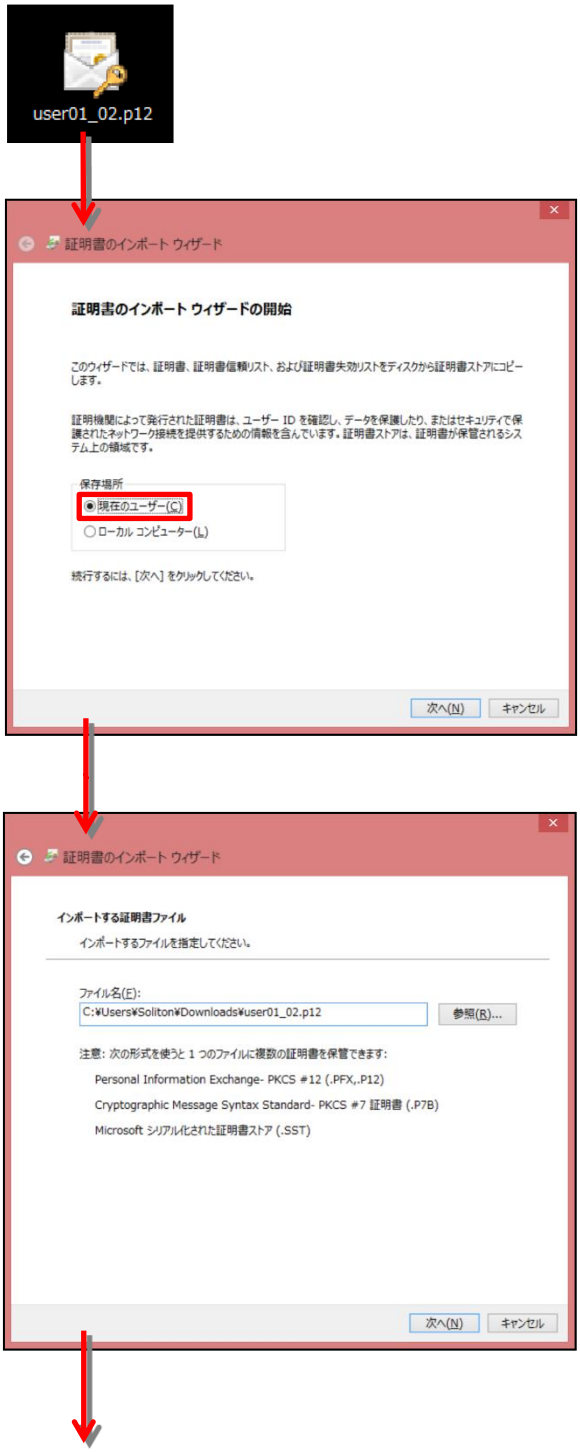
[DHCP サービス] - [サーバー状態] にて [起動] ボタンを押し、DHCP サーバーを起動します。

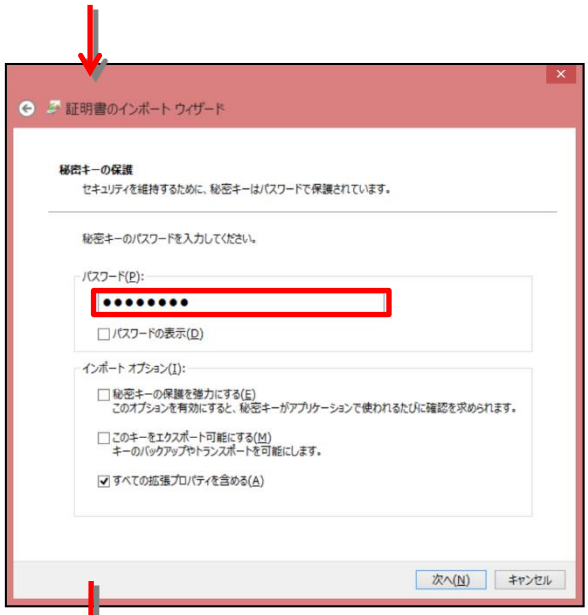
5. EAP-TLS 認証でのクライアント設定

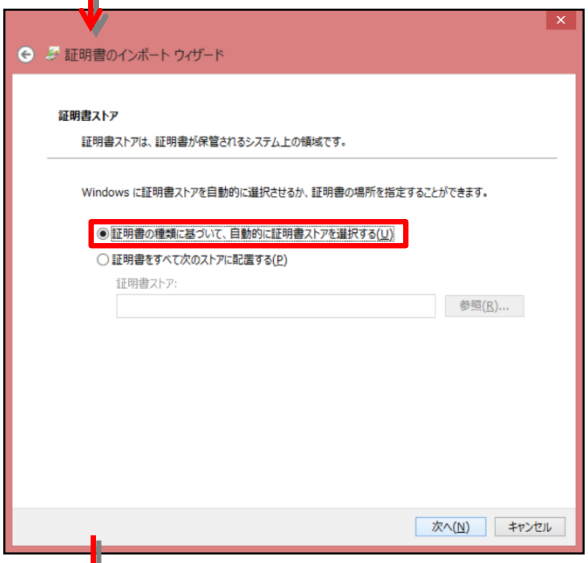
5-1 Windows 8.1 での EAP-TLS 認証

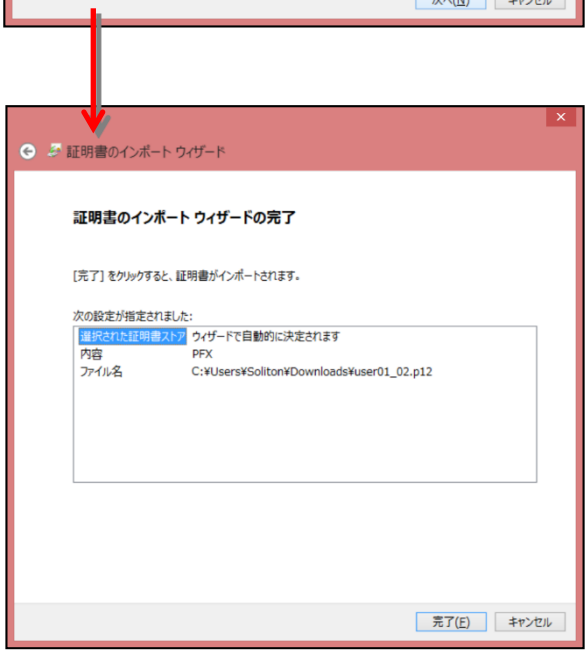
5-1-1 クライアント証明書のインポート

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_02.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】

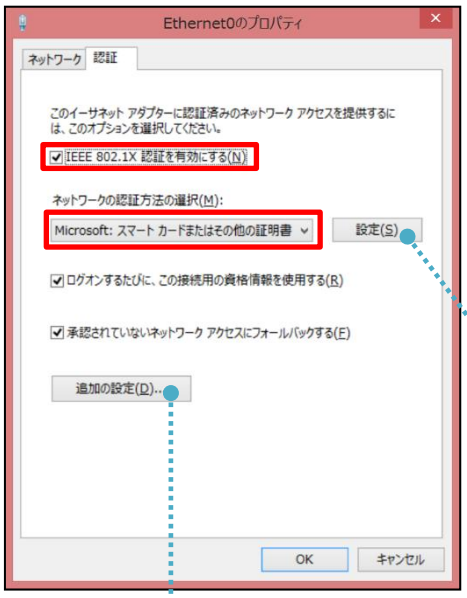
NetAttest EPS で証明書を発行した際に設定したパスワードを入力

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・・・	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・・・	On
- 単純な証明書の選択・・・	On
証明書を検証してサーバー・・・	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

認証結果は EPS の RADIUS 認証ログ、および FXC5224 の情報にて確認可能です。

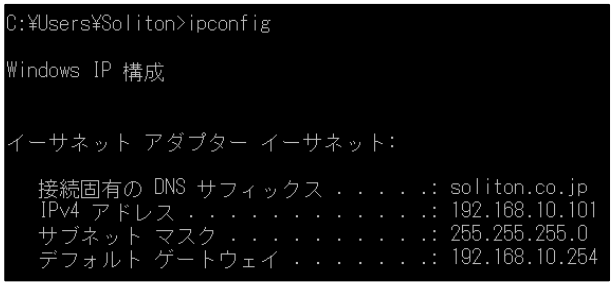
EAP-TLS 認証が成功した場合は以下のように表示されます。

製品名	表示例
NetAttest EPS	2016/07/20 14:06:01 Login OK: [user03] (from client RadiusClient01 port 1 cli 74-03-BD-3D-38-0B)
FXC5224	・各インターフェイスの認証状態の確認 Show dot1x Port Admin State Port State Last Source Last ID ---- ---------- ---------- ---------- ---------- 1 Multi 802.1X 1 Auth/0 Unauth 74-03-BD-3D-38-0B user03 2 Force Authorized Link Down - - 3 Force Authorized Link Down - -

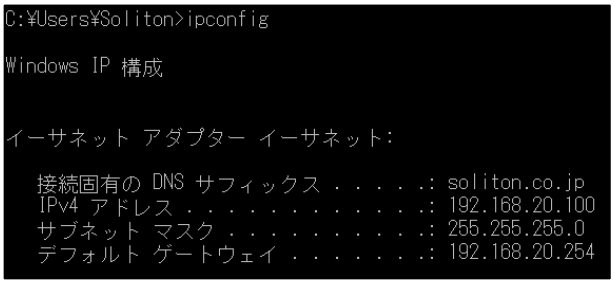
6-2 ダイナミック VLAN

FXC5224 にて表示される情報、およびクライアントに払い出される IP アドレスから、ダイナミック VLAN によって接続先の制御が行われていることが確認可能です。

製品名	表示例
EPS	2016/07/20 14:36:45 Login OK: [user01] (from client RadiusClient01 port 1 cli 74-03-BD-3D-38-0B)
FXC5224	・各インターフェイスの認証状態の確認 Show dot1x Port Admin State Port State Last Source Last ID ---- ---------- ---------- ---------- ---------- 1 Multi 802.1X 1 Auth/0 Unauth 74-03-BD-3D-38-0B user01 2 Force Authorized Link Down - - 3 Force Authorized Link Down - - ・Dynamic-vlan 割り当ての確認 show dot1x radius_vlan RADIUS Port VLAN Current ---- ------- ------- 1 Enabled 10 2 Disabled 3 Disabled



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
2016/10/03	1.0	初版作成