# NetAttest EPS
## 認証連携設定例

【連携機器】NEC QX-S3109TP/QX-S4009P/QX-S5224GT-4X-PW

【Case】IEEE802.1x EAP-TLS 認証

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 CA 内蔵 RADIUS サーバーアプライアンス NetAttest EPS と NEC 社製有線 LAN スイッチ QX-S3109TP/QX-S4009P/QX-S5224GT-4X-PW の IEEE802.1x EAP-TLS 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 QX-S3109TP/QX-S4009P/QX-S5224GT-4X-PW 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。

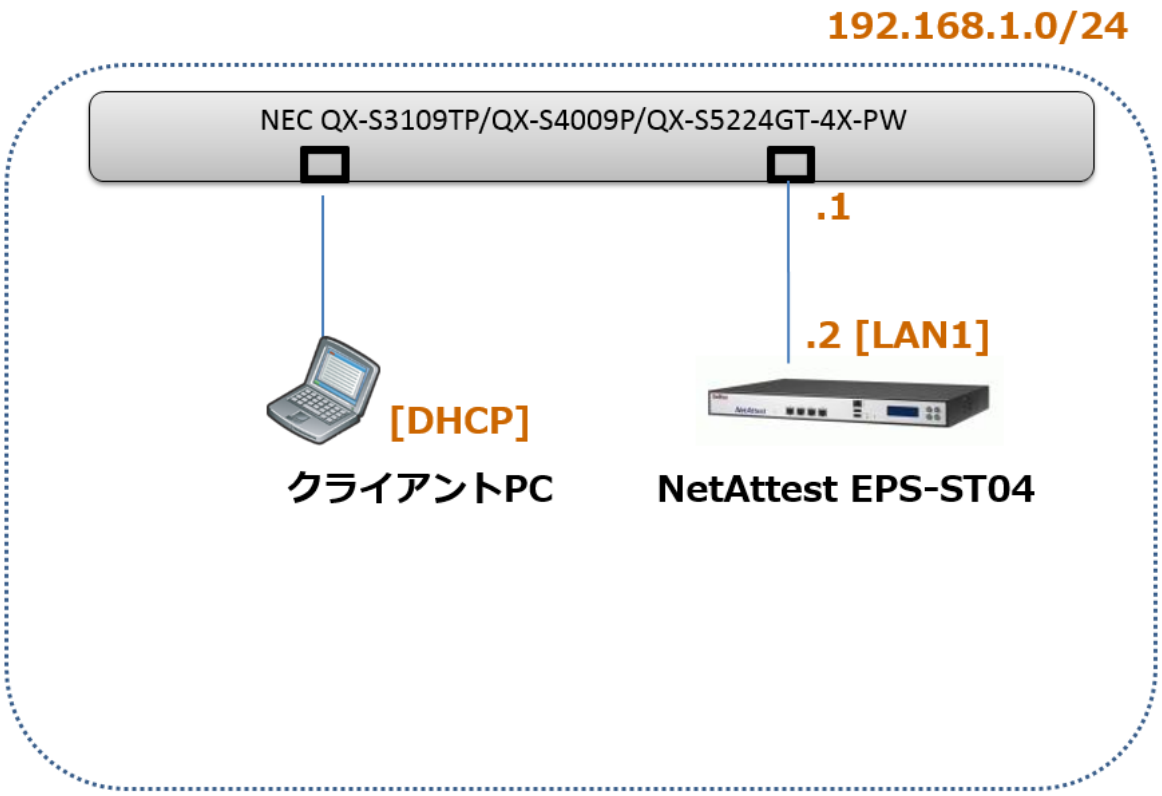
# 目次

# 1. 構成

## 1-1 構成図

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。

- 有線 LAN で接続する機器は L2 スイッチに収容
- クライアント PC の IP アドレスは、
  NetAttest EPS-ST04 の DHCP サーバーから払い出す



# 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 | Ver. 4.8.4 |
| QX-S3109TP | NEC | RADIUS クライアント | Ver. 5.2.26 |
| QX-S4009P | NEC | RADIUS クライアント | Ver. 5.4.12 |
| QX-S5224GT-4X-PW | NEC | RADIUS クライアント | Ver. 7.1.12 |
| Surface Pro | Microsoft | Client PC<br>(802.1x クライアント) | Windows 8.1 64bit<br>Windows 標準サプリカント |

## 1-2-2 認証方式

IEEE802.1x EAP-TLS 認証

## 1-2-3 ネットワーク設定

| | IP アドレス | RADIUS port<br>(Authentication) | RADIUS Secret<br>(Key) |
|---|---|---|---|
| NetAttest EPS-ST04 | 192.168.1.2/24 | UDP 1812 | secret |
| QX-S3109TP | 192.168.1.4/24 | | |
| QX-S4009P | 192.168.1.1/24 | | |
| QX-S5224GT-4X-PW | 192.168.1.3/24 | | |
| Client PC | DHCP | - | - |

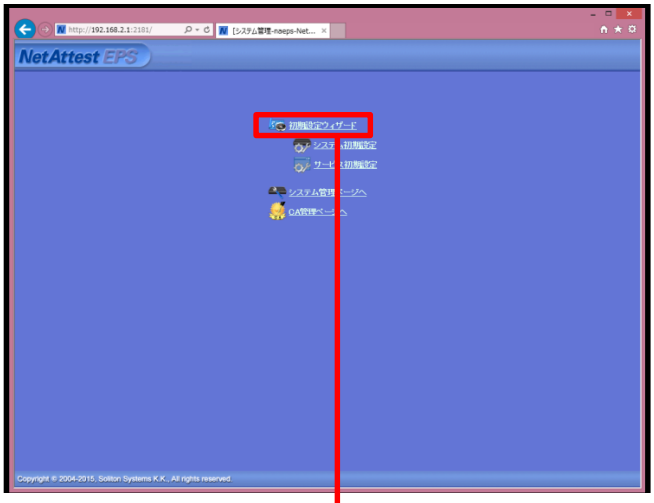
# 2. NetAttest EPS の設定

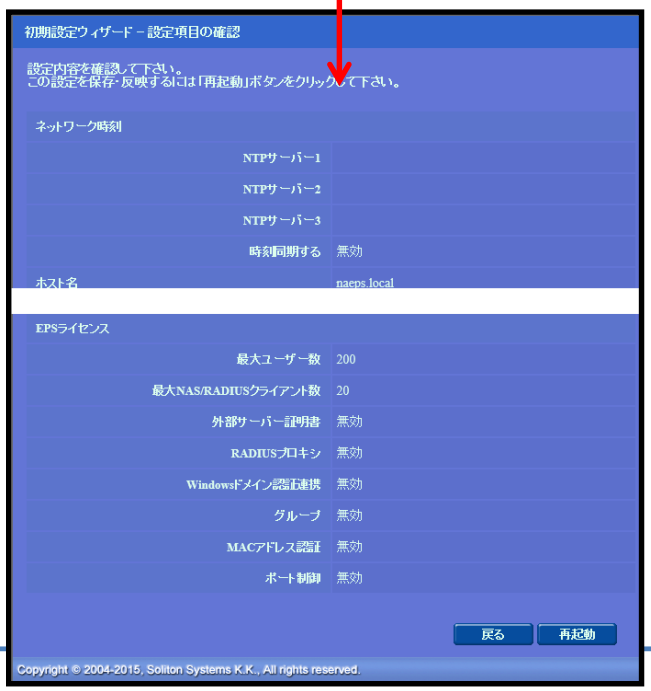
## 2-1 システム初期設定ウィザードの実行

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、インターネットエクスプローラーから「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



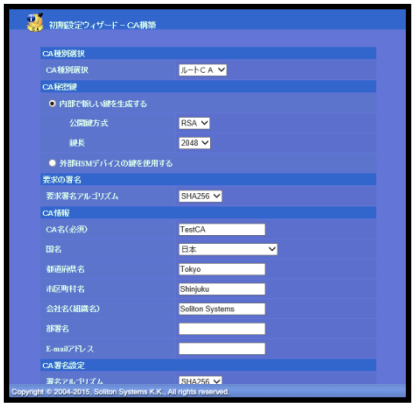




| 項目 | 値 |
|---|---|
| ホスト名 | naeps.local |
| IP アドレス | デフォルト |
| ライセンス | なし |

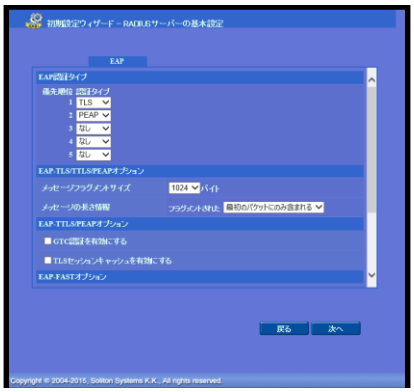
# 2-2 サービス初期設定ウィザードの実行

サービス初期設定ウィザードを実行します。

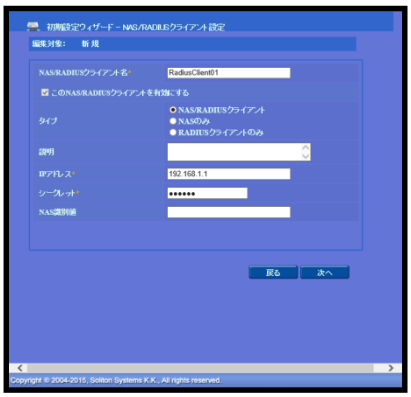
- CA 構築
- LDAP データベースの設定
- RADIUS サーバーの基本設定（全般）
- RADIUS サーバーの基本設定（EAP）
- RADIUS サーバーの基本設定（証明書検証）
- NAS/RADIUS クライアント設定




| 項目 | 値 |
|---|---|
| CA 種別選択 | ルート CA |
| 公開鍵方式 | RSA |
| 鍵長 | 2048 |
| CA 名 | TestCA |
| 署名アルゴリズム | SHA256 |




| 項目 | 値 |
|---|---|
| EAP 認証タイプ | |
| 1 | TLS |




| 項目 | 値 |
|---|---|
| NAS/RADIUS クライアント名 | RadiusClient |
| IP アドレス | 192.168.1.1 |
| シークレット | secret |

## 2-3 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。

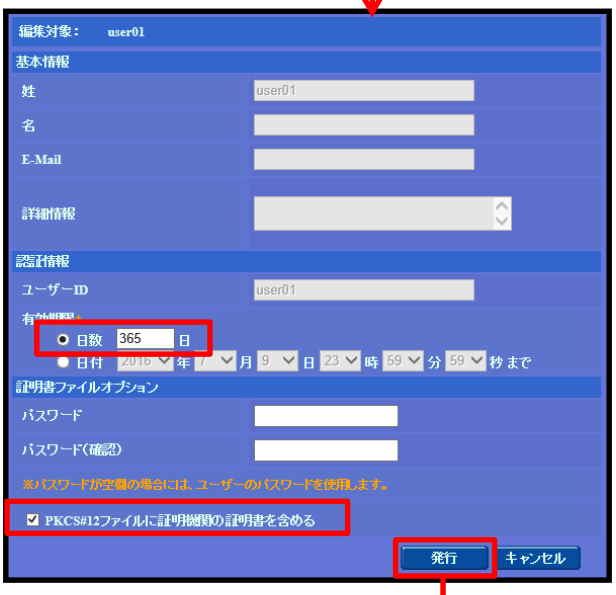

| 項目 | 値 |
|---|---|
| 姓 | user01 |
| ユーザーID | user01 |
| パスワード | password |

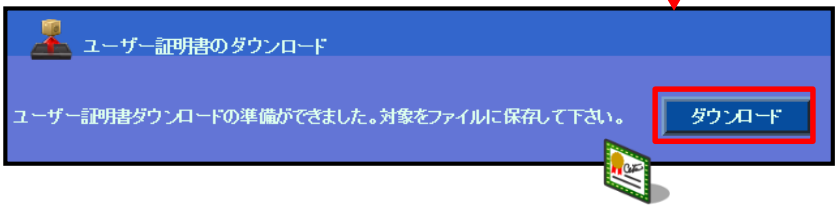
# 2-4 クライアント証明書の発行

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. NEC QX-S3109TP/QX-S4009P/QX-S5224GT-4X-PW

## 3-1 NEC QX-S3109TP/QX-S4009P/QX-S5224GT-4X-PW 設定の流れ

NEC 社製有線 LAN スイッチ QX-S3109TP/QX-S4009P/QX-S5224GT-4X-PW を設定するためには CLI を用います。本書では CLI を用いて各種設定を実施する方法を紹介します。

## 3-2 NEC QX スイッチ側設定項目

### 3-2-1 Radius サーバーの登録

QX スイッチに IP アドレスを設定し、RADIUS サーバーとして NetAttest EPS を登録します。

(QX-S3109TP/QX-S4009P/QX-S5224GT-4X-PW 共通)

**[入力値]**

```
interface Vlan-interface1
 ip address 192.168.1.1 24
 quit

radius scheme rs1
 primary authentication 192.168.1.2
 primary accounting 192.168.1.2
 key authentication simple secret
 key accounting simple secret
 quit

domain local.com
 authentication default radius-scheme rs1
 authorization default radius-scheme rs1
 accounting default radius-scheme rs1
 quit

domain default enable local.com
# デフォルトの認証先として RADIUS サーバーを指定します。
```

### 3-2-2 IEEE802.1x の設定

IEEE802.1x 認証を有効にし、インターフェイスに認証ポートを設定します。

(QX-S3109TP:Ethernet1/0/1, QX-S4009P/QX-S5224GT-4X-PW:GigabitEthernet1/0/1)

**[入力値]**

```
dot1x
dot1x authentication-method eap

# QX-S3109TP の場合
interface Ethernet1/0/1
# QX-S4009P/QX-S5224GT-4X-PW の場合
interface GigabitEthernet1/0/1
```

**dot1x**
**dot1x unicast-trigger**
**undo dot1x handshake**
**undo dot1x multicast-trigger**
**quit**

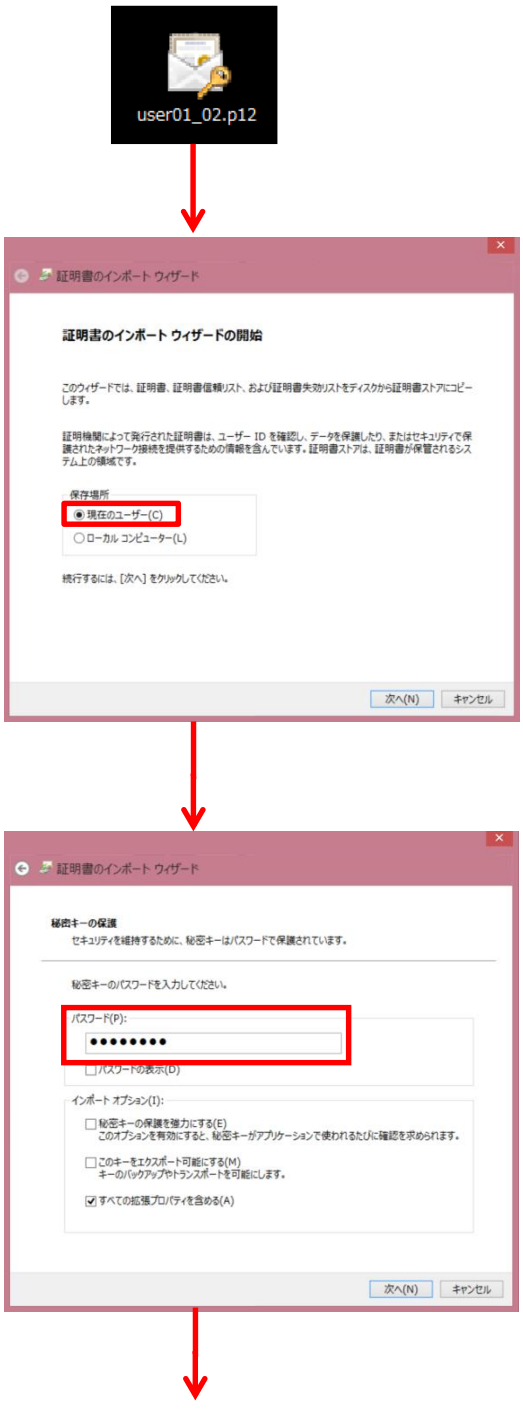
各スイッチの設定後のコンフィグイメージは巻末の(付録)をご参照ください。

# 4. EAP-TLS 認証でのクライアント設定

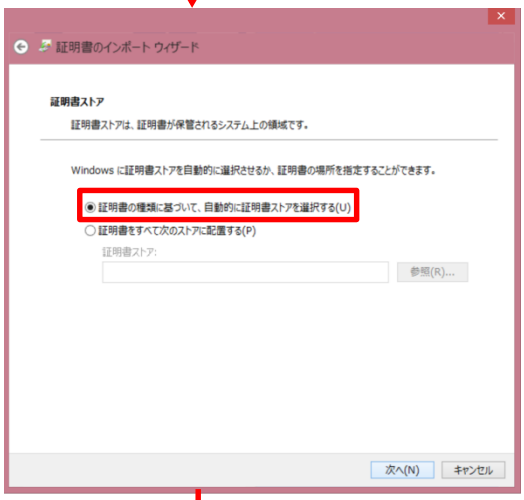
## 4-1 Windows 8.1 での EAP-TLS 認証

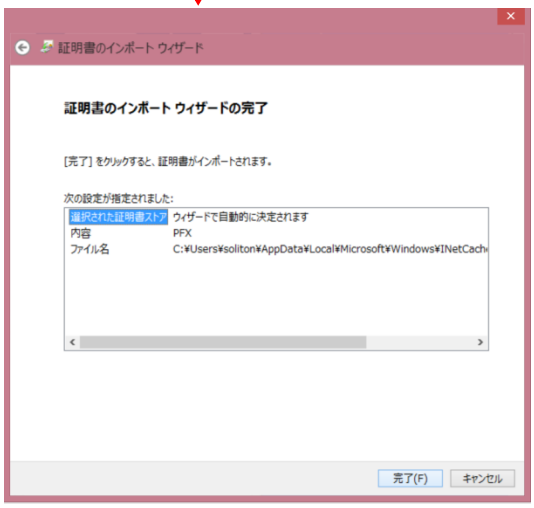
### 4-1-1 デジタル証明書のインポート

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


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)
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

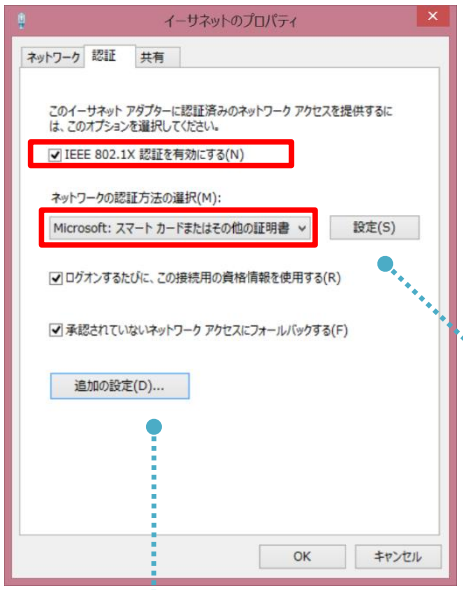

証明書のインポート ウィザード
証明書のインポート ウィザードの完了
[完了] をクリックすると、証明書がインポートされます。
次の設定が指定されました:
選択された証明書ストア
ウィザードで自動的に決定されます
内容
PFX
ファイル名
C:¥Users¥soliton¥AppData¥Local¥Microsoft¥Windows¥INetCach
完了(F)
キャンセル

## 4-1-2サプリカント設定

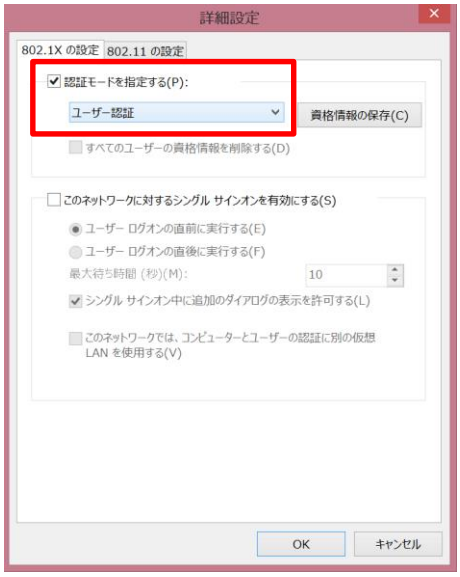
Windows 標準サプリカントで TLS の設定を行います。

※ 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 |

# 5. 動作確認結果

認証結果は EPS の RADIUS 認証ログ、および各 QX スイッチのログで確認可能です。

## 5-1 EAP-TLS 認証

・EAP-TLS 認証が成功した場合、ログ表示例

| 製品名 | ログ表示例 |
|---|---|
| EPS | naeps radiusd[8354]: notice 2016/03/02 13:47:28 Login OK: [user01] (from client RadiusClient port 16781313 cli CC-E1-D5-0D-D6-90) |
| QX-S3109TP<br>QX-S4009P | RDS/6/RDS_SUCC:-IfName=GigabitEthernet1/0/1-VlanId=1-MACAddr=CC:E1:D5:0D:D6:90-IPAddr=N/A-IPv6Addr=N/A-UserName=user01@local.com; User got online successfully. |
| QX-S5224GT-4X-PW | DOT1X/6/DOT1X_LOGIN_SUCC: -IfName=GigabitEthernet1/0/1-MACAddr=cce1-d50d-d690-VLANID=1-Username=user01;<br>User passed 802.1X authentication and came online. |

# 6.(付録) NEC QX スイッチの設定後のコンフィグ

## 6-1 NEC QX-S3109TP Switch の設定完了後のイメージ

QX-S3109TP の設定完了後の設定イメージを以下に示します。

RADIUS サーバーとの間の共有シークレット等は、暗号化されて表示されます。

```
[QX-S3109TP]display current-configuration
#
 version 5.2.26
#
 sysname QX-S3109TP
#
 domain default enable local.com
#
 telnet server enable
#
 dot1x
 dot1x authentication-method eap
#
 password-recovery enable
#
vlan 1
#
radius scheme system
 primary authentication 127.0.0.1 1645
 primary accounting 127.0.0.1 1646
 user-name-format without-domain
radius scheme rs1
 primary authentication 192.168.1.2
 primary accounting 192.168.1.2
 key authentication cipher $c$3$HOAg6eTbPy9qtgS9XjjhBOAVMYjdyvHoOw==
 key accounting cipher $c$3$6gFaixC+X2Zfm4bpD9IHXSEfR1XRPsfMRA==
#
domain local.com
 authentication default radius-scheme rs1
 authorization default radius-scheme rs1
 accounting default radius-scheme rs1
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
 group-attribute allow-guest
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet1/0/1
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x
```

```
 dot1x unicast-trigger
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface Ethernet1/0/8
#
interface GigabitEthernet1/0/9
#
 undo info-center logfile enable
#
 load xml-configuration
#
 load tr069-configuration
#
user-interface aux 0
user-interface vty 0 15
#
return
```

## 6-2 NEC QX-S4009P Switch の設定完了後のイメージ

QX-S4009P の設定完了後の設定イメージを以下に示します。

RADIUS サーバーとの間の共有シークレット等は、暗号化されて表示されます。

```
[QX-S4009P]display current-configuration
#
 version 5.4.12
#
 sysname QX-S4009P
#
 irf mac-address persistent timer
 irf auto-update enable
 irf link-delay 250
#
 domain default enable local.com
#
 telnet server enable
#
 dot1x
 dot1x authentication-method eap
#
 password-recovery enable
#
vlan 1
#
radius scheme rs1
 primary authentication 192.168.1.2
 primary accounting 192.168.1.2
 key authentication cipher $c$3$xOYZJFDbxjdbRlKOKyrg4u9+5LNsZEL9iA==
 key accounting cipher $c$3$2uiPdvgfjTLs4kck5sQyVlw0qNMvN+8jEg==
```

```
#
domain local.com
 authentication default radius-scheme rs1
 authorization default radius-scheme rs1
 accounting default radius-scheme rs1
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
domain system
 access-limit disable
 state active
 idle-cut disable
 self-service-url disable
#
user-group system
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/2
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/3
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/4
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/5
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/6
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/7
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/8
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/9
#
 load tr069-configuration
```

```
#
user-interface aux 0
user-interface vty 0 15
#
return
```

## 6-3 NEC QX-S5224GT-4X-PW の設定完了後のイメージ

QX-S5224GT-4X-PW の設定完了後の設定イメージを以下に示します。

RADIUS サーバーとの間の共有シークレット等は、暗号化されて表示されます。

```
[QX-S5224GT-4X-PW]display current-configuration
#
 version 7.1.12
#
 sysname QX-S5224GT-4X-PW
#
 undo copyright-info enable
#
 irf mac-address persistent timer
 irf auto-update enable
 irf link-delay 500
 irf member 1 priority 1
#
 dot1x
 dot1x authentication-method eap
#
 loopback-detection global enable vlan 1 to 4094
#
 password-recovery enable
#
vlan 1
#
interface NULL0
#
interface Vlan-interface1
 ip address 192.168.1.1 255.255.255.0
#
interface GigabitEthernet1/0/1
 poe enable
 dot1x
 undo dot1x handshake
 undo dot1x multicast-trigger
 dot1x unicast-trigger
#
interface GigabitEthernet1/0/2
 poe enable
#
interface GigabitEthernet1/0/3
 poe enable
#
interface GigabitEthernet1/0/4
 poe enable
#
interface GigabitEthernet1/0/5
 poe enable
#
interface GigabitEthernet1/0/6
 poe enable
#
```

```
interface GigabitEthernet1/0/7
 poe enable
#
interface GigabitEthernet1/0/8
 poe enable
#
interface GigabitEthernet1/0/9
 poe enable
#
interface GigabitEthernet1/0/10
 poe enable
#
interface GigabitEthernet1/0/11
 poe enable
#
interface GigabitEthernet1/0/12
 poe enable
#
interface GigabitEthernet1/0/13
 poe enable
#
interface GigabitEthernet1/0/14
 poe enable
#
interface GigabitEthernet1/0/15
 poe enable
#
interface GigabitEthernet1/0/16
 poe enable
#
interface GigabitEthernet1/0/17
 poe enable
#
interface GigabitEthernet1/0/18
 poe enable
#
interface GigabitEthernet1/0/19
 poe enable
#
interface GigabitEthernet1/0/20
 poe enable
#
interface GigabitEthernet1/0/21
 poe enable
#
interface GigabitEthernet1/0/22
 poe enable
#
interface GigabitEthernet1/0/23
 poe enable
#
interface GigabitEthernet1/0/24
 poe enable
#
interface Ten-GigabitEthernet1/0/25
#
interface Ten-GigabitEthernet1/0/26
#
interface Ten-GigabitEthernet1/0/27
#
interface Ten-GigabitEthernet1/0/28
#
 scheduler logfile size 16
#
line class aux
 user-role network-admin
```

```
#
line class vty
 user-role network-operator
#
line aux 0
 user-role network-admin
#
line vty 0 63
 user-role network-operator
#
radius scheme rs1
 primary authentication 192.168.1.2
 primary accounting 192.168.1.2
 key authentication cipher $c$3$0vLd3EffbIH2jq959l9v9y08uSBtqz2ztw==
 key accounting cipher $c$3$9V/1k9aTKYf61ioRV8ePQ1MYzkZ9xE+a1Q==
#
radius scheme system
 user-name-format without-domain
#
domain local.com
 authentication default radius-scheme rs1
 authorization default radius-scheme rs1
 accounting default radius-scheme rs1
#
domain system
#
 domain default enable local.com
#
role name level-0
 description Predefined level-0 role
#
role name level-1
 description Predefined level-1 role
#
role name level-2
 description Predefined level-2 role
#
role name level-3
 description Predefined level-3 role
#
role name level-4
 description Predefined level-4 role
#
role name level-5
 description Predefined level-5 role
#
role name level-6
 description Predefined level-6 role
#
role name level-7
 description Predefined level-7 role
#
role name level-8
 description Predefined level-8 role
#
role name level-9
 description Predefined level-9 role
#
role name level-10
 description Predefined level-10 role
#
role name level-11
 description Predefined level-11 role
#
role name level-12
 description Predefined level-12 role
```

```
#
role name level-13
  description Predefined level-13 role
#
role name level-14
  description Predefined level-14 role
#
user-group system
#
return
```

改訂履歴

| 日付 | 版 | 改訂内容 |
|---|---|---|
| 2016/03/11 | 1.0 | 初版作成 |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |