NEC

D10-0000021609 1.8 版

QX シリーズ Ethernet スイッチ

Web 認証

オペレーションマニュアル

改版履歴

版数	日付	改版内容
1.0	2011/08	・初版発行
1.1	2011/12	・「本マニュアルについて」の「適用装置」、「関連マニュアル」に QX-S4000 シリーズ Ethernet スイッチ(QX-S4009P、QX-S4020P、QX-S4028P、QX-S4028P-PW)を追加 ・「1.10 ポータル検知機能の設定」「2.8 ローカル RSA 鍵ペアの廃棄」「2.9 証明書の削除」にメモを追記
1.2	2012/02	・「本マニュアルについて」の「適用装置」、「関連マニュアル」に QX-S5300 シリーズ Ethernet スイッチを追加 ・誤記訂正 ・「1.7.2 オンラインポータルユーザの最大数の設定」のデフォルト値を追加、変更
1.3	2012/04	・「本マニュアルについて」の「適用装置」に QX-S4009P-PW に関する記述を追加
1.4	2012/07	・「本マニュアルについて」の「適用装置」に QX-S3800 シリーズ Ethernet スイッチを追加
1.5	2012/12	・「本マニュアルについて」の「適用装置」に QX-S5700 シリーズ Ethernet スイッチを追加
1.6	2015/09/18	・「3 章 SSL 設定」に「3.4 SSL3.0 の無効化機能」を追加 ・誤記訂正
1.7	2016/02/29	・「3 章 SSL 設定」の **ssl version ssl3.0 disable** コマンドに QX-S5700 シリーズのソフトウェアを追加 ・誤記訂正
1.8	2016/12/27	・「3 章 SSL 設定」の **ssl version ssl3.0 disable** コマンドに QX-S4000 シリーズのソフトウェアを追加しました。 ・誤記訂正

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- QX シリーズの Web 認証機能は *QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

適用装置

本マニュアルの適用装置は以下となります。

装置	適用バージョン
QX-S5200 シリーズ Ethernet スイッチ	Version 5.3.1 を含む以降のソフトウェア
QX-S3300TP シリーズ Ethernet スイッチ	Version 5.1.5 を含む以降のソフトウェア
QX-S4000 シリーズ Ethernet スイッチ	Version 5.3.3 を含む以降のソフトウェア (QX-S4009P-PW は Version5.3.5 を含む以降のソフトウェア)
QX-S5300 シリーズ Ethernet スイッチ	Version 5.1.x を含む以降のソフトウェア
QX-S3800 シリーズ Ethernet スイッチ	Version 5.1.x を含む以降のソフトウェア
QX-S5700 シリーズ Ethernet スイッチ	Version 5.1.x を含む以降のソフトウェア

関連マニュアル

マニュアル	内容
QX シリーズ Ethernet スイッチ Web 認証オペレーションマニュアル	Web 認証の設定について記述しています。
QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル	Web 認証に関するコマンドを使用するときの参考になります。
QX-S5200 シリーズ Ethernet スイッチオペレーションマニュアル	QX-S5200 シリーズ Ethernet スイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S5200 シリーズ Ethernet スイッチコマンドマニュアル	QX-S5200 シリーズ Ethernet スイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S3100TP/S3300TP シリーズ Ethernet スイッチオペレーションマニュアル	QX-S3100TP/S3300TP シリーズ Ethernet スイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S3100TP/S3300TP シリーズ Ethernet スイッチコマンドマニュアル	QX-S3100TP/S3300TP シリーズ Ethernet スイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S4000 シリーズ Ethernet スイッチオペレーションマニュアル	QX-S4000 シリーズ Ethernet スイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S4000 シリーズ Ethernet スイッチコマンドマニュアル	QX-S4000 シリーズ Ethernet スイッチのユーザがさまざまなコマンドを使用するときの参考になります。

マニュアル	内容
QX-S5300 シリーズ Ethernet スイッチオペレーションマニュアル	QX-S5300 シリーズ Ethernet スイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S5300 シリーズ Ethernet スイッチコマンドマニュアル	QX-S5300 シリーズ Ethernet スイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S3800 シリーズ Ethernet スイッチオペレーションマニュアル	QX-S3800 シリーズ Ethernet スイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S3800 シリーズ Ethernet スイッチコマンドマニュアル	QX-S3800 シリーズ Ethernet スイッチのユーザがさまざまなコマンドを使用するときの参考になります。
QX-S5700 シリーズ Ethernet スイッチオペレーションマニュアル	QX-S5700 シリーズ Ethernet スイッチのデータ設定や代表的なアプリケーションについて記述しています。
QX-S5700 シリーズ Ethernet スイッチコマンドマニュアル	QX-S5700 シリーズ Ethernet スイッチのユーザがさまざまなコマンドを使用するときの参考になります。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンドの表記規則

表記規則	説明
太字体	コマンド行のキーワードには**太字体**を使用します。
イタリック体	コマンドの引数には*イタリック体*を使用します。
[]	大カッコに囲まれた項目(キーワードまたは引数)はオプションです。
{x|y|…}	選択する項目は中カッコに入れて、縦線で区切ってあります。１つを選択します。
[x|y|…]	オプションの選択項目は大カッコに入れて、縦線で区切ってあります。１つまたは複数を選択します。
{x|y|…}*	選択する項目は中カッコに入れて、縦線で区切ってあります。少なくとも１つ、多い場合はすべてを選択できます。
[x|y|…]*	オプションの選択項目は大カッコに入れて、縦線で区切ってあります。複数選択することも、何も選択しないこともできます。
#	#で始まる行はコメントです。

II. GUI の表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。たとえば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。たとえば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。たとえば、[File/Create/Folder]。

III. キーボード操作

書式	説明
<キー>	三角カッコ内の名前のキーを押します。たとえば、<Enter>、<Tab>、<Backspace>、<A>となります。
<キー1 + キー2>	複数のキーを同時に押します。たとえば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<キー1、キー2>	複数のキーを順番に押します。たとえば、 <Alt、A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

動作	説明
クリック	左ボタンまたは右ボタンを素早く押します(特に記述がない場合は左ボタン)。
ダブルクリック	左ボタンを素早く 2 回続けて押します。
ドラッグ	左ボタンを押したまま、別の位置まで移動します。

V. 記号

本マニュアルでは、以下のような記号も使用して、操作中に特に注意すべき点を強調しています。意味は次のとおりです。

⚠ **注意、警告、危険**：操作中に特に注意すべきことを表します。

🕮 **メモ、コメント、ヒント、ノウハウ、アイデア**：補助的な説明を表します。

VI. 設定例

本マニュアルの設定例の記述は、各機能の設定例です。インタフェース番号、システム名の表記、display コマンドでの情報表示が、ご使用の装置と異なることがあります。

本マニュアルは以下に示す 4 章で構成されています。

01-Web 認証

02-PKI

03-SSL

04-トリプル認証

目次

1章 Web 認証

1.1 Web認証概要

1.1.1 Web 認証の導入

Web 認証を導入することにより、インタネットへのアクセス管理の手助けとなります。Web 認証は、“ポータル認証”とも呼ばれます。

Web 認証では、アクセスデバイスが、Web 認証ページにアクセスするすべてのユーザをリダイレクトさせます。すべてのユーザは、インタネットにアクセスするために Web 認証にパスする必要があります。

1.1.2 ローカルポータルサーバを用いた Web 認証システム

I. システム構成

Web 認証システムは Web ユーザをダイレクトに認証するために、アクセスデバイスのローカルポータルサーバ機能を使用します。図 13-1に示すように Web 認証システムは、認証クライアント(Authentication Client)、アクセスデバイス(Access device with embedded portal server)、認証/アカウンティングサーバ(Authentication/accounting server)の 3 つのコンポーネントから構成されます。

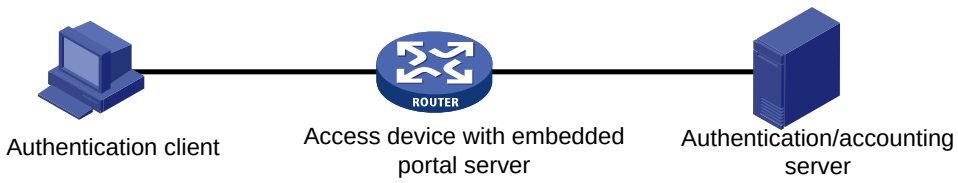

図13-1 ローカルポータルサーバを用いた Web 認証システム

🕮 **メモ：**

Web 認証システム内のリモート認証/アカウンティングサーバとして RADIUS サーバのみを使うことができます。

II. クライアントとローカルポータルサーバ間の相互プロトコル

HTTP と HTTPS がローカルポータルサーバ機能を提供するために、認証クライアントとアクセスデバイス間で使われます。HTTP が使用された場合は、HTTP パケットが平文で転送されるため潜在的にセキュリティの問題があります。HTTPS が使用された場合、

HTTPS パケットが SSL ベースで暗号化されて転送されるため、セキュアなデータ転送を保証します。

III. 認証ページカスタマイズ

ローカルポータルサーバ機能は認証ページをカスタマイズすることができます。対応する HTML ファイルを編集、圧縮し、デバイスのメモリにファイルを保存することで、認証ページをカスタマイズすることができます。カスタマイズされた認証ページは、ログオンページ、ログオン成功ページ、オンラインページ、ログオフ成功ページ、ログオン失敗ページ、システムビジーページの 6 つの認証ページから構成されます。ローカルポータルサーバは各認証フェーズに対応する認証ページを表示させます。認証ページをカスタマイズしない場合、ローカルポータルサーバはデフォルトで保存されている認証ページを表示させます。

1.1.3 Web 認証モード

Web 認証は OSI 参照モデルのレイヤ 2 の Web 認証のみサポートしています。

認証モードにおいて、Web 認証は、認証クライアントが接続するアクセスデバイスのレイヤ 2 ポートが有効になります。送信元 MAC アドレスが認証をパスしたクライアントのみ外部ネットワークにアクセスできます。クライアントが Web 認証を実行するために、アクセスデバイスがローカルポータルサーバとして動作します。

また Web 認証では、アクセスデバイスは、ユーザのリソースへのアクセスを管理できるように、ユーザ認証によって、認証サーバは異なる VLAN を割り当てることができます。

クライアントが認証をパスした後、認証サーバは、VLAN のリソースにユーザがアクセスできるように認可された VLAN を割り当てることができます。クライアントが認証に失敗した場合は、認証サーバは Auth-Fail VLAN を割り当てることができます。

1.1.4 Web 認証プロセス

I. Web 認証プロセス

図 13-2にローカル Web 認証のプロセスを示します。

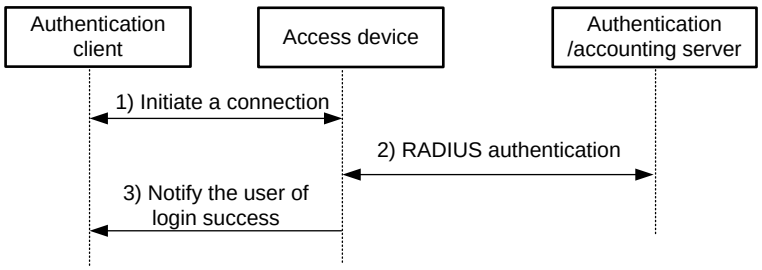

図13-2 ローカル Web 認証プロセス

図 13-2に示すようにローカル Web 認証は次の手順になります。

1) Web 認証クライアントは HTTP あるいは HTTPS リクエストを送信します。アクセスデバイスは、HTTP あるいは HTTPS リクエストを受信するとローカルポータルサーバの IP アドレスをリスニングし、リダイレクトします。そして Web 認証ページを Web 認証クライアントに表示させます。ユーザは Web 認証ページ上でユーザ名とパスワードを入力します。ローカルポータルサーバのリスニング IP アドレスは、Web 認証クライアントがルーティング可能なアクセスデバイスのレイヤ３インタフェースの IP アドレスです。一般的にはループバックインタフェースの IP アドレスとなります。
2) アクセスデバイスと RADIUS サーバはユーザの認証を行うために RADIUS パケットの交換を行います。
3) ユーザが RADIUS 認証をパスした場合、ローカルポータルサーバはログオン成功ページを認証クライアントに表示します。

II. 認可 VLAN

Web 認証は認証サーバによって VLAN を割り当てることができます。ユーザは Web 認証をパスした後、認証サーバにユーザ用の認可 VLAN が設定されている場合、認証サーバはアクセスデバイスに認可 VLAN を割り当てます。そして認可 VLAN にユーザを追加し、MAC VLAN エントリを作成します。

認可 VLAN 割り当て機能を使用することによって、Web 認証をパスしたユーザがアクセスできるネットワークリソースを管理することができます。

III. Auth-Fail VLAN 機能

Auth-Fail VLAN 機能は、認証に失敗したユーザが、クライアントソフトウェアや他のプログラムをアップグレードできるようにパッチサーバ、ウィルス定義サーバ、クライアントソフトウェアサーバ、アンチウィルスソフトウェアサーバのようなネットワークリソースを提供できるようにします。この VLAN は“Auth-Fail VLAN”と呼ばれます。

Web 認証は MAC-based Auth-Fail VLAN(MAFV)をサポートしています。Auth-Fail VLAN がポートに設定されている状態で、ユーザが認証に失敗した場合、アクセスデバイスはユーザの MAC アドレスを元にした MAC VLAN エントリを作成し、ユーザを Auth-Fail VLAN に加えます。ユーザは Auth-Fail VLAN の HTTP 以外のリソースにアクセスすることができますが、ユーザのすべての HTTP リクエストは認証ページにリダイレクトされます。Auth-Fail VLAN に加えられたユーザが認証をパスした場合、アクセスデバイスは認証サーバが VLAN を割り当てていれば、割り当てられた VLAN にユーザを追加し、認証サーバが VLAN を割り当てていなければ、ポートの初期 VLAN にユーザを戻します。ユーザが認証に失敗すると、アクセスデバイスは Auth-Fail VLAN にユーザを保持します。アクセスポートが指定された期間(デフォルトでは 120 秒)、Auth-Fail VLAN のユーザからトラフィックを受信しなかった場合、Auth-Fail VLAN からユーザを削除し、ポートの初期 VLAN にユーザを追加します。

🕮 **メモ：**

ユーザが認可 VLAN あるいは Auth-Fail VLAN に追加された後、クライアントが VLAN のホストと通信できるように、IP アドレスは自動あるいは手動で更新される必要があります。

1.2 Web認証設定作業リスト

Web 認証を設定するために、次の手順を実行します。

表1-1 Web 認証設定作業リスト

作業		補足
Web認証のローカルポータルサーバの指定		必須項目
ローカルポータルサーバの設定	認証ページのカスタマイズ	オプション項目
	ローカルポータルサーバの設定	必須項目
Web認証の有効化		必須項目
ポータルユーザのアクセス管理	ポータルフリールールの設定	オプション項目
	オンラインポータルユーザの最大数の設定	オプション項目
	ポータルユーザの認証ドメインの設定	オプション項目
	Webプロキシサーバポート番号の追加	オプション項目
	移動ポータルユーザ機能の有効化	オプション項目
Web認証のAuth-Fail VLANの設定		オプション項目
認証されたポータルユーザの自動リダイレクションURLの設定		オプション項目
ポータル検知機能の設定		オプション項目
ポータルユーザのログオフ		オプション項目

1.3 設定必要項目

Web 認証はユーザ認証とセキュリティチェックソリューションを提供します。しかし Web 認証それ自体では実現できません。RADIUS 認証は、ユーザ認証を完全なものにするために Web 認証と協力して、アクセスデバイス上に設定される必要があります。

Web 認証を設定する前に、以下の項目を行う必要があります。

- RADIUS サーバが適切に設定されています。
- Web 認証クライアント、アクセスデバイス、サーバが互いにルーティング可能です。
- RADIUS 認証を行うため、ユーザ名、ユーザのパスワードが RADIUS サーバに設定されています。RADIUS クライアント設定がアクセスデバイスに行われています。

1.4 Web認証のローカルポータルサーバの指定

Web 認証はローカルポータルサーバを使用します。デバイスのレイヤ 3 インタフェースの IP アドレスを指定する必要があります。レイヤ 3 インタフェースは、ローカルポータルサーバの IP アドレスをリスニングできるようにポータルクライアントにルーティング可能です。ローカルポータルサーバは物理レイヤ 3 インタフェースよりもループバックインタフェースの IP アドレスを使うことを強く推奨します。

- ループバックインタフェースの状態は安定しています。インタフェースの故障によって認証ページのアクセスが失敗となりません。
- ループバックインタフェースはネットワークから受信したパケットを転送しません。多くのネットワークアクセスリクエストがあったときにシステムパフォーマンスの影響を避けることができます。

Web 認証のローカルポータルサーバを指定するための手順を以下に示します。

表1-2 Web 認証のローカルポータルサーバの指定

操作	コマンド	補足
system viewへ移行する	system-view	–
Web認証のためにローカルポータルサーバのリスニングIPアドレスを指定する	portal local-server ip *ip-address*	必須項目 デフォルト：リスニングIPアドレスの指定はありません。

メモ：

Web 認証がすべてのポートで有効でない場合のみ、指定されたリスニング IP アドレスを変更したり、削除したりできます。

1.5 ローカルポータルサーバの設定

Web 認証が行われる間、ローカルポータルサーバはユーザに認証ページを表示させます。認証ページはカスタマイズすることができます。カスタマイズしない場合、デフォルトの認証ページが認証プロセスの行われている間使われます。

1.5.1 認証ページのカスタマイズ

カスタマイズされた認証ページは HTML ファイル形式で作成します。そのページを圧縮し、アクセスデバイスのメモリに保存します。

認証ページは 6 つのメイン認証ページとそのページ要素があります。メイン認証ページはログオンページ、ログオン成功ページ、ログオン失敗ページ、オンラインページ、システムビジーページ、ログオフ成功ページの 6 つです。ページの要素は認証ページリファレンスのファイルを参照します。たとえば Logon.htm ページの back.jpg です。各メイン認証ページは複数ページの要素を参照することができます。メイン認証ページのいくつかを定義した場合、定義されていない認証ページはデフォルトの認証ページが使われます。

認証ページのカスタマイズを行う際、ローカルポータルサーバを正常に確実に動作させるため、以下のルールに従ってください。

I. ファイル名のルール

メイン認証ページはあらかじめ定義され、変更できないファイル名があります。表 1-3にリストを示します。

表1-3 メイン認証ページのファイル名

メイン認証ページ	ファイル名
ログオンページ	logon.htm
ログオン成功ページ	logonSuccess.htm
ログオン失敗ページ	logonFail.htm

メイン認証ページ	ファイル名
オンラインページ ユーザがオンライン状態で、再び認証動作を行った場合オンライン通知が表示されます。	online.htm
システムビジーページ ログインプロセスにおいてシステムあるいはユーザがビジー状態であることを表示されます。	busy.htm
ログオフ成功ページ	logoffSuccess.htm

🕮 **メモ：**

メイン認証ページファイル以外の他のファイル名を定義することができます。ファイル名とディレクトリ名は大文字と小文字の区別はしません。

II. ページリクエストのルール

ローカルポータルサーバは Post と Get リクエストのみサポートしています。

- Get リクエストは認証ページにある静的なファイルを取得するのに使われます。そして再帰を許可しません。たとえば”Logon.htm ファイルが ca.htm ファイルの Get アクションを実行するコンテンツを含んでいる場合、ca.htm ファイルは Logon.htm に関連しているものを含むことできません。
- Post リクエストは、ユーザがユーザ名とパスワードのセット、システムのログオン、システムのログオフを通知する際に使われます。

III. Post リクエストアトリビュートのルール

1) 認証ページの form を編集する場合、次の必要事項に注意してください。

- 認証ページは複数の form を持つことができますが、アクションの form は logon.cgi のみを用います。複数の form を使用するとユーザ情報がローカルポータルサーバに送信できなくなります。
- ユーザ名アトリビュートは PtUser として固定されています。パスワードアトリビュートは PtPwd として固定されています。
- PtButton アトリビュートはログオンやログオフを行うユーザリクエストのアクションを示すのに必要です。
- ログオン Post リクエストは PtUser、PtPwd、PtButton アトリビュートが必須です。
- ログオフ Post リクエストは PtButton アトリビュートが必須です。

2) 認証ページ logon.htm と logonFail.htm は、ログオン Post リクエストが必須です。

例として以下に logon.htm ページのスクリプトの一部を示します。

```
<form action=logon.cgi method = post >
<p>User name:<input type=“text” name = “PtUser” style=“width:160px;height:22px” maxlength=64>
<p>Password :<input type= “ password ” name = “ PtPwd ” style= “width:160px;height:22px” maxlength=32>
<p><input type=SUBMIT value=“Logon” name = “PtButton” style=“width:60px;” >
</form>
```

3) 認証ページ logonSuccess.htm と online.htm は、ログオフ Post リクエストが必須です。

例として以下に online.htm ページのスクリプトの一部を示します。

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value=“Logoff” name=“PtButton” style=“width:60px;”>
</form>
```

IV. ページのファイル圧縮と保存のルール

- 認証ページファイルのセットは標準 zip ファイルに圧縮しなくてはいけません。zip ファイルの名前は、文字、数字、アンダーラインのみが使えます。デフォルトの認証ページの zip ファイルは、defaultfile.zip という名前で保存しなくてはいけません。
- 認証ページのセットは、zip ファイルのルートディレクトリに格納されなくてはいけません。
- zip ファイルは FTP や TFTP でデバイスに転送され、デバイスの指定されたディレクトリに保存される必要があります。デフォルト認証ページファイルはデバイスのルートディレクトリに保存し、他の認証ファイルはルートディレクトリあるいはデバイスのルートディレクトリの下の portal ディレクトリに保存される必要があります。

デバイスの zip ファイルの例を示します。

<QX > dir

```
Directory of flash:/portal/
   0     -rw-      1405  Feb 28 2008 15:53:31   2.zip
   1     -rw-      1405  Feb 28 2008 15:53:20   1.zip
   2     -rw-      1405  Feb 28 2008 15:53:39   3.zip
   3     -rw-      1405  Feb 28 2008 15:53:44   4.zip
2540 KB total (1319 KB free)
```

V. ファイルサイズとコンテンツのルール

システムにおいて、カスタマイズされた認証ページをスムースに表示させるために、以下の認証ページのサイズとコンテンツの要求事項を満足させる必要があります。

- メイン認証ページとページの要素を含んでいる認証ページの各セットの zip ファイルのサイズは、500KB 以下にする必要があります。
- メインページとそのページ要素を含んだ、ひとつのページサイズは圧縮する前の状態で 50KB 以下にする必要があります。
- ページの要素は HTML、JS、CSS、画像などのような静的なコンテンツのみを含むことができます。

VI. ログオン成功やオンラインページを終了するユーザのログオフ

ユーザが認証をパスした後、システムは logonSuccess.htm という名前のログオン成功ページを表示します。ユーザがログオンページで再び認証を開始した場合、online.htm という名前のオンラインページを表示します。ユーザがこれらの 2 つのページのどちらかを閉じるとき、強制的にログオフするように設定することができます。その設定を行うため、logonSuccess.htm と online.htm に以下のコンテンツを追加する必要があります。

- JS ファイル pt_private.js の参照
- トリガーページを取り除くのに使われる pt_unload()機能
- イベントハンドラー機能の pt_submit()機能
- トリガーページの読み込みを行う pt_init()機能

以下に追加されたコンテンツをグレー表示した例を示します。

```
<html>
<head>
```

```
    <script type=“text/javascript” language=“javascript” src=“pt_private.js”
></script>
    </head>
    <body onload=“pt_init();” onbeforeunload=“return pt_unload();” >
    ... ...
<form action=logon.cgi method = post onsubmit=“pt_submit()” >
    ... ...
    </body>
    </html>
```

VII. 指定された Web ページへの認証されたユーザのリダイレクト

自動的に認証にパスしたユーザを指定された Web ページにリダイレクトするため、logon.htm と logonSuccess.htm に以下のことを行います。

1) logon.htm で空白ページに目的アトリビュートをセットします。コンテンツにグレーで表示したところを確認してください。

```
<form method=post action=logon.cgi target=“blank” >
```

2) logonSuccess.htm に pt_init()アトリビュートを読み込む機能を追加します。コンテンツにグレーで表示したところを確認してください。

```
<html>
<head>
<title>LogonSuccessed</title>
<script type=“text/javascript” language=“javascript” src=“pt_private.js”
></script>
</head>
<body onload=“pt_init();” onbeforeunload=“return pt_unload();” >
... ...
</body>
</html>
```

🕮 **メモ：**

- 認証クライアントに IE6.0 以上のブラウザを使用することを推奨します。
- 認証クライアントのブラウザがポップアップやアクセスデバイスからのポップアップを許可するようにします。ポップアップが許可されていないと、ユーザがログオン成功ページ、オンラインページを閉じるためにログオフできません。またログオン成功やオンラインページに戻るためにキャンセルをクリックすることだけが可能となります。
- ユーザがログオン成功やオンラインページの再読み込みをしたり、ページを別の Web サイトに移動したりする場合、デバイスはユーザのログオフをします。
- ユーザが Chrome ブラウザを使用する場合、ログオン成功やオンラインページを閉じる際、ユーザのログオフができません。

1.5.2 ローカルポータルサーバの設定

ローカルポータルサーバを有効にするため、Web 認証クライアントとローカルポータルサーバの通信用にプロトコルを設定する必要があります。

I. 設定必要項目

HTTPS をサポートするためには、ローカルポータルサーバを設定する前に以下の手順を行う必要があります。

- CA 証明書､ローカル証明書を取得するための PKI ポリシーの設定を行ってください。詳細は"PKI 設定"を参照してください。
- SSL サーバポリシーの設定および､PKI ポリシーで設定される PKI ドメインの指定を行ってください。詳細は"SSL 設定"を参照してください。

ローカルポータルサーバをサポートするため、プロトコルを指定する場合、ローカルポータルサーバはデフォルト認証ページファイルを読み込みます。デフォルト認証ページファイルは、デバイスのルートディレクトリに保存されていると仮定されます。ローカルポータルサーバがユーザ定義のデフォルト認証ページを使用するため､あらかじめ認証ページを編集し、保存しておく必要があります。認証ページが編集、保存されていない場合、デフォルト認証ページが使われます。

II. 設定手順

ローカルポータルサーバを設定するために以下の手順を行います。

表1-4 ローカルポータルサーバの設定

操作	コマンド	補足
system viewへ移行する	system-view	–
デフォルト認証ページファイルのサポートと読み込みを行うローカルポータルサーバのプロトコルタイプを設定する	portal local-server { http | https server-policy *policy-name* }	必須項目 デフォルト：ローカルポータルサーバはプロトコルのサポートはありません。
ローカルポータルサーバのデフォルト認証ページのwelcomeバナーを設定する	portal server banner *banner-string*	オプション項目 デフォルト：welcome バナーなし

1.6 Web認証の有効化

Web 認証を有効にしたアクセスインタフェースに接続されたクライアントのみが Web 認証を実行できます。

Web 認証を有効にする前に、ローカルポータルサーバのリスニング IP アドレスが指定されていることを確認してください。

Web 認証の有効にするために、次の手順を行います。

表1-5 Web 認証の有効化

操作	コマンド	補足
system viewへ移行する	system-view	–
Layer 2 Ethernet interface view へ移行する	interface *interface-type interface-number*	–
ポートのWeb認証の有効にする	portal local-server enable	必須項目 デフォルト：無効

🕮 **メモ：**

- レイヤ2ポートのWeb認証の通常の操作を保証するため、ポートセキュリティ、802.1X のゲスト VLAN を有効にしないことを推奨します。
- 認可 VLAN の割り当てをサポートするには、ポートに MAC ベース VLAN を有効にする必要があります。

1.7 ポータルユーザのアクセス管理

1.7.1 ポータルフリールールの設定

ポータルフリールールは、ユーザが Web 認証なしで指定された外部 Web サイトにアクセスできるよう許可する設定です。

Web 認証では、すべての送信元アドレスから、すべてあるいは指定された宛先アドレス形式のポータルフリールールのみ設定することができます。ポータルフリールールが、指定された宛先アドレスの形式で設定した場合、ユーザは、Web 認証ページにリダイレクトされることなく、直接指定されたアドレスにアクセスすることができます。通常、確実なサービス（たとえばソフトウェアアップグレードサービス）を提供するサーバのポータルフリールールの宛先 IP アドレスを設定できます。これによりポータルユーザは Web 認証なしでサービスをアクセスできるようにします。

以下にポータルフリールールを設定する手順を示します。

表1-6 ポータルフリールールの設定

操作	コマンド	補足
system viewへ移行する	system-view	–
ポータルフリールールを設定する	portal free-rule *rule-number* { destination { any | ip { *ip-address* mask { *mask-length* | *netmask* } | any } } } *	必須項目

🕮 **メモ：**

- 同じルールナンバーで 2 つ以上のポータルフリールールを設定できません。
- Web 認証が有効かどうかにかかわらず、ルールの追加や削除を行うことができます。
- QX-S3300TP シリーズでは、ポータルフリールールで VLAN とインタフェースを両方指定する場合、インタフェースは VLAN に属している必要があります。属していない場合、ポータルフリールールは適用されません。
- QX-S3300TP シリーズでは、アグリゲーショングループのレイヤ 2 インタフェースはポータルフリールールの送信元インタフェースとして指定することはできません。ポータルフリールールの送信元インタフェースはアグリゲーショングループに追加することはできません。

1.7.2 オンラインポータルユーザの最大数の設定

システムでオンラインポータルユーザの最大数を管理することができます。

以下にオンラインポータルのユーザ最大数を設定する手順を示します。

表1-7 オンラインポータルユーザの最大数の設定

操作	コマンド	補足
system viewへ移行する	system-view	–
オンラインポータルユーザの最大数を設定する	portal max-user *max-number*	必須項目 デフォルト： QX-S3300TPシリーズ、QX-S4000シリーズ：512 QX-S3800シリーズ：1024 QX-S5200シリーズ、QX-S5300シリーズ：1000 QX-S5700シリーズ：3000

🕮 **メモ：**

- 正確なオンラインポータルユーザの最大数は、スイッチに設定された ACL に依存します。
- このコマンドで指定されたオンラインポータルユーザの最大数が現在のポータルユーザよりも少ない場合、コマンドは正常に実行され、オンラインポータルユーザに影響を与えません。しかしシステムは、オンラインポータルユーザ数が最大数未満になるまで新しいポータルユーザのログオンを許可しません。

1.7.3 ポータルユーザの認証ドメインの設定

インタフェースにポータルユーザの認証ドメインを指定した場合、デバイスは、ユーザ名のドメイン名を無視して、インタフェースのすべてのポータルユーザの認証、認可、アカウンティング（AAA）の認証ドメインを使用することができます。異なるインタフェースごとに、異なった認証ドメインを指定することができます。

インタフェースにポータルユーザの認証ドメインを設定する項目を以下に示します。

表1-8 ポータルユーザの認証ドメインの設定

操作	コマンド	補足
system viewへ移行する	system-view	–
interface viewへ移行する	interface *interface-type interface-number*	–
インタフェースのポータルユーザの認証ドメインを設定する	portal domain *domain-name*	必須項目 デフォルト：ポータルユーザの認証ドメインは未設定です。

🕮 **メモ：**

装置は、インタフェースに指定された認証ドメイン、ユーザ名にある認証ドメイン、システムデフォルト認証ドメインの順番でインタフェースにポータルユーザの認証ドメインを選択します。デフォルト認証ドメインについては各装置の"AAA"を参照してください。

1.7.4 Web プロキシサーバポート番号の追加

デフォルトで、HTTP リクエストは、認証されていないユーザから、Web 認証にポート番号 80 番が起動できるように使われます。認証されていないユーザが Web プロキシサーバを使います。プロキシサーバのポート番号が 80 でない場合、ユーザの HTTP リクエストは Web 認証に失敗し、廃棄されます。この問題を回避するため、デバイスに Web プロキシサーバのポート番号を設定します。

Web サーバがネットワークでポート番号が 80 でない場合、ユーザは、サーバにアクセスする前に Web 認証をパスする必要があります。HTTP リクエストが Web 認証を起動させることができるようにするため、デバイスのポート番号に Web サーバのプロキシーを追加することができます。

以下に、HTTP リクエストのポート番号が Web 認証で起動できるように、Web プロキシサーバのポート番号を追加する手順を示します。

表1-9 Web プロキシサーバポート番号の追加

操作	コマンド	補足
system viewへ移行する	system-view	–
Webプロキシサーバのポート番号を追加する	portal web-proxy port *port-number*	必須項目 デフォルト：Webプロキシサーバのポート番号は未設定、HTTPリクエストのポート番号は80です。

🕮 **メモ：**

- Web プロキシサーバのポート番号が 80 である場合、デバイスのサーバのポート番号の設定を行う必要はありません。
- ユーザのブラウザが Web プロキシサーバを発見する Web プロキシオートディスカバリー(WPAD)プロトコルを使用している場合、デバイスの Web プロキシサーバのポート番号を追加する必要があります。認証なしでパスするために、WPAD サーバの IP アドレス用のユーザパケットを許可するポータルフリールールを設定する必要があります。
- Web 認証において、デバイスに Web プロキシサーバのポート番号を追加する必要があります。ローカルポータルサーバのリスニング IP アドレスのため、ユーザはプロキシサーバを使わないで、ブラウザが Web プロキシサーバを使うようにする必要があります。これによりポータルユーザがローカルポータルサーバに送信する HTTP パケットは Web プロキシサーバに送信されません。

1.7.5 移動ポータルユーザ機能の有効化

ユーザとアクセスデバイス間に、ハブ、レイヤ 2 スイッチ、アクセスポイント(AP)がある構成において、認証されているユーザが現在のアクセスポートから別の Web 認証が有効なデバイスのポートにログオフなしで移動した場合、元のポートが UP 状態であると、ユーザはオンラインとすることができません。これはデフォルトで、移動前のポートがユーザの認証情報を維持しており、デバイスが別のポートからユーザがオンラインで接続しようとすることを許可しないためです。

この問題を解決するため、デバイスの移動ポータルユーザ機能を有効にします。ユーザがデバイスのポートから別のポートに移動した場合、デバイスは次の 2 つの方法のどちらかでサービスを提供します。

- オリジナルポートが UP 状態で、2 つのポートが同じ VLAN である場合、デバイスは再認証なしでユーザのネットワークのアクセスを許可します。ユーザのアカウンティングは新しいポート情報を使用します。
- オリジナルポートがダウンする、もしくは 2 つのポートが異なった VLAN である場合、デバイスはオリジナルポートからユーザの認証情報を削除し、新しいポートでユーザを認証します。

移動ポータルユーザ機能を有効にする手順を以下に示します。

表1-10 移動ポータルユーザ機能の有効化

操作	コマンド	補足
system viewへ移行する	system-view	–
移動ポータルユーザ機能を有効にする	portal move-mode auto	必須項目 デフォルト：無効

メモ：

設定されたユーザの認証情報(認可 VLAN など)のため、ユーザがポートから別のポートに移動した後、デバイスは新しいポートに認証情報を割り当てることを試みます。割り当てが失敗した場合、デバイスはオリジナルポートからユーザの情報を削除し、新しいポートでユーザの再認証を行います。たとえばオリジナルポートと移動先ポートに MAC 認証の設定もしてある場合がこれにあたります。

1.8 Web認証のAuth-Fail VLANの設定

Web 認証に失敗したユーザに割り当てる Auth-Fail VLAN を設定することができます。

Auth-Fail VLAN を設定する前に、VLAN を作成しておく必要があります。

以下に、Web 認証の Auth-Fail VLAN を設定する項目を示します。

表1-11 Web 認証の Auth-Fail VLAN の設定

操作	コマンド	補足
system viewに移行する	system-view	–
Layer2 Ethernet interface viewに移行する	interface *interface-type interface-number*	–

操作	コマンド	補足
ポートのWeb認証のAuth-Fail VLANの設定	portal auth-fail vlan *authfail-vlan-id*	必須項目 デフォルト：未設定

🕮 **メモ：**

- ポートで Web 認証の Auth-Fail VLAN を有効にするため、ポートで MAC VLAN 機能を有効にする必要があります。
- 異なるポートに Web 認証の異なる Auth-Fail VLAN を設定することができます。ポートは Web 認証のひとつの Auth-Fail VLAN のみ設定することができます。
- Web 認証が失敗したときのために作成された MAC VLAN は、他の認証モードで作成された MAC VLAN エントリを上書きしません。具体的には MAC 認証に失敗して Guest VLAN を割り当てたのち、Web 認証が失敗した場合 Auth-Fail VLAN には変更されません。

1.9 認証されたポータルユーザの自動リダイレクションURLの設定

ユーザが Web 認証をパスした後、アクセスデバイスは自動リダイレクション URL が設定されている場合、ある指定された一定の期間の後、URL にユーザをリダイレクトします。

以下に認証されたポータルユーザの自動リダイレクション URL の設定手順を示します。

操作	コマンド	補足
system viewへ移行する	system-view	–
認証されたポータルユーザの自動リダイレクション URLを設定する	portal redirect-url *url-string* [wait-time *period*]	必須項目 デフォルト：指定なし 認証されたユーザは、リダイレクト先の指定がされていない場合、認証が行われる前に、アドレスバーで入力されたURLにリダイレクトされます。ただし、認証が行われる前にアドレスバーで入力したURLが255文字以上の場合、ユーザが認証にパスした後のURLページへのリダイレクトができません。

🕮 **メモ：**

wait-time オプションはローカル Web 認証のみ適用されます。

1.10 ポータル検知機能の設定

ポータルユーザがオンラインとなった後、デバイスはユーザの検知タイマを開始し、ユーザの MAC アドレスエントリが期限切れになった、あるいはユーザの MAC アドレスエントリが期間の間にマッチ（マッチとは、パケットがユーザから受信したということです）したかどうかをチェックします。ユーザの MAC アドレスエントリがない、もしくは 2 連

続の検知期間中にユーザからのパケットを受信しない場合、デバイスはユーザがオフラインであると認識し、ユーザの認証情報を削除します。

以下にポータルユーザ検知期間の手順を示します。

表1-12 ポータル検知機能の設定

操作	コマンド	補足
system viewへ移行する	system-view	–
Layer 2 Ethernet interface viewへ移行する	interface *interface-type interface-number*	–
ポータルユーザ検知期間を設定する	portal offline-detect interval *offline-detect-interval*	必須項目 デフォルト：300秒

メモ：

QX-S4000 シリーズは、portal offline-detect interval コマンドで指定したタイマによってユーザがオフラインであると検知されるまで、MAC アドレスエントリが保持されます。

1.11 ポータルユーザのログオフ

認証されたユーザリストからユーザをログオフすることができます。

以下にユーザのログオフの手順を示します。

表1-13 ポータルユーザのログオフ

操作	コマンド	補足
system viewへ移行する	system-view	–
ユーザをログオフする	portal delete-user { *ip-address* | all | interface *interface-type interface-number* }	必須項目

1.12 Web認証の表示

表1-14 Web 認証の表示

操作	コマンド	補足
ポータルフリールールあるいはすべてのポータルフリールールの情報を表示する	display portal free-rule [*rule-number*] [| { begin | exclude | include } *regular-expression*]	すべてのviewで有効です。
指定されたインタフェースのWeb認証設定を表示する	display portal interface *interface-type interface-number* [| { begin | exclude | include } *regular-expression*]	すべてのviewで有効です。
ローカルポータルサーバの設定情報を表示する	display portal local-server [| { begin | exclude | include } *regular-expression*]	すべてのviewで有効です。

操作	コマンド	補足
指定されたインタフェースあるいはすべてのインタフェースのポータルユーザの情報を表示する	display portal user { all | interface *interface-type interface-number* } [| { begin | exclude | include } *regular-expression*]	すべてのviewで有効です。

1.13 Web認証設定例

1.13.1 ネットワーク必要条件

図 13-3に示すように、ホストは直接スイッチに接続しています。スイッチはGigabitEthernet 1/0/1 ポートに接続されたユーザに Web 認証を行っています。

- 認証、認可、アカウンティング用にリモート RADIUS サーバを使用します。
- ユーザに IP アドレスを割り当てるためにリモート DHCP サーバを使用します。
- ローカルポータルサーバのリスニング IP アドレスは 4.4.4.4。ローカルポータルサーバはユーザ定義の認証ページをユーザに表示させ、認証データを HTTPS で転送します。
- VLAN3 に認証に成功したユーザを追加します。
- VLAN2 に認証が失敗したユーザを追加し、ユーザはアップデートサーバのリソースにアクセスできるようにします。
- ホストは DHCP を用いて IP アドレスを取得します。認証が行われる前に、DHCP サーバは 192.168.1.0/24 セグメントの IP アドレスをホストに割り当てます。ホストが認証をパスしたとき、DHCP サーバは 3.3.3.0/24 セグメントの IP アドレスをホストに割り当てます。ホストが認証に失敗したとき、DHCP サーバは 2.2.2.0/24 セグメントの IP アドレスをホストに割り当てます。

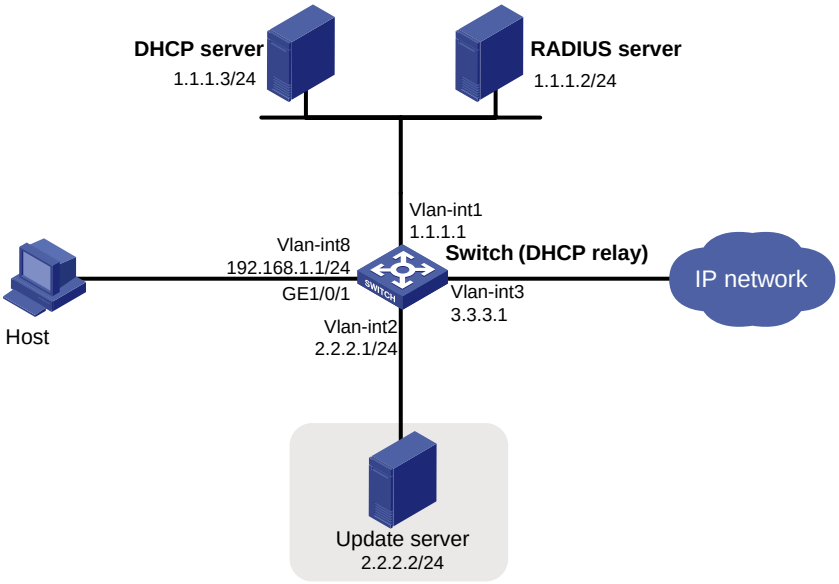

図13-3 Web 認証設定のネットワーク図

1.13.2 設定手順

🕮 **メモ：**

- Web 認証が有効になる前に、スイッチ、サーバが通信可能であることが必要です。
- RADIUS サーバは適切に通常の認証/認可/アカウンティング機能をユーザに提供します。この例ではポータルユーザアカウントを RADIUS サーバ上に userpt で作成し、アカウント用に認可 VLAN を設定します。
- DHCP サーバにおいて、IP アドレス範囲(192.168.1.0/24、3.3.3.0/24、2.2.2.0/24)、デフォルトゲートウェイアドレス(192.168.1.1、3.3.3.1、2.2.2.1) が指定されるように設定します。デバイスは、すべてのホストにアップデートサーバのアドレス 2.2.2.2 を割り当てしないように設定し、割り当てられた IP アドレスのリース時間を設定します(各アドレスのために短いリース期間を設定します。これは認証状態変更に備えて IP アドレスのアップデート時間を短くするためです)。ホストにデフォルトルートが存在することを確認します。
- DHCP サーバと DHCP クライアントは同じサブネットにあり、DHCP リレーエージェントをクライアントのサブネットに設定する必要があります。
- DHCP リレー機能をサポートしていない装置は、DHCP リレーを行う L3 スイッチなどを用意する必要があります。

1) Web 認証の設定

イーサネットポートに関連した VLAN を追加し、VLAN インタフェース用に、IP アドレスを設定します(詳細は省略します) 。

PKI ドメイン pkidm を設定し、ローカル証明書と CA 証明書を適用します。

ユーザ定義の認証ページを編集します。defaultfile という名前で zip ファイルに圧縮します。アクセスデバイスのルートディレクトリに保存します。

SSL サーバポリシーsslsvr を設定し、PKI ドメイン pkidm を使うために指定します。

<QX> system-view

[QX] ssl server-policy sslsvr

[QX-ssl-server-policy-sslsvr] pki pkidm

[QX-ssl-server-policy-sslsvr] quit

ローカルポータルサーバが HTTPS をサポートするように設定し、SSL サーバポリシー sslsvr を参照します。

[QX] portal local-server https server-policy sslsvr

ループバックインタフェース 12 の IP アドレスを 4.4.4.4 に設定します。

[QX] interface loopback 12

[QX-LoopBack12] ip address 4.4.4.4 32

[QX-LoopBack12] quit

Web 認証用のローカルポータルサーバのリスニング IP アドレスとして 4.4.4.4 を指定します。

[QX] portal local-server ip 4.4.4.4

GigabitEthernet 1/0/1 ポートで Web 認証を有効にし、VLAN2 を Auth-Fail VLAN に割り当てます。

[QX] interface gigabitethernet 1/0/1

[QX- GigabitEthernet1/0/1] port link-type hybrid

[QX- GigabitEthernet1/0/1] mac-vlan enable

[QX- GigabitEthernet1/0/1] portal local-server enable

[QX- GigabitEthernet1/0/1] portal auth-fail vlan 2

[QX- GigabitEthernet1/0/1] quit

2) RADIUS スキームの設定

RADIUS スキーム rs1 を作成し、RADIUS view に移行します。

<QX> system-view

[QX] radius scheme rs1

プライマリ認証サーバとプライマリアカウンティングサーバを指定し、サーバの通信を行うためのキーを設定します。

[QX-radius-rs1] primary authentication 1.1.1.2

[QX-radius-rs1] primary accounting 1.1.1.2

[QX-radius-rs1] key accounting radius

[QX-radius-rs1] key authentication radius

[QX-radius-rs1] quit

3) 認証ドメインの設定

ドメイン triple を作成し、ドメインに移行します。

[QX] domain triple

ドメインの AAA 方式を設定します。

[QX-isp-triple] authentication portal radius-scheme rs1

[QX-isp-triple] authorization portal radius-scheme rs1

[QX-isp-triple] accounting portal radius-scheme rs1

[QX-isp-triple] quit

すべてのユーザにデフォルトのドメインとして triple を設定します。ユーザがログイン時、ドメインなしでユーザ名を入力した場合、デフォルトドメインの認証とアカウンティング方式が使用されます。

[QX] domain default enable triple

4) DHCP リレーエージェントの設定

DHCP を有効にします。

[QX] dhcp enable

DHCP サーバグループ 1 を作成し、グループに DHCP サーバ 1.1.1.3 を追加します。

[QX] dhcp relay server-group 1 ip 1.1.1.3

VLAN インタフェース 8 に DHCP リレーエージェントを有効にします。

[QX] interface vlan-interface 8

[QX-Vlan-interface8] dhcp select relay

VLAN インタフェース 8 に DHCP サーバグループ 1 を関連付けます。

[QX-Vlan-interface8] dhcp relay server-select 1

[QX-Vlan-interface8] quit

VLAN インタフェース 2 に DHCP リレーエージェントを有効にします。

[QX] interface vlan-interface 2

[QX-Vlan-interface2] dhcp select relay

VLAN インタフェース 2 に DHCP サーバグループ 1 を関連付けます。

[QX-Vlan-interface2] dhcp relay server-select 1

[QX-Vlan-interface2] quit

VLAN インタフェース 3 に DHCP リレーエージェントを有効にします。

[QX] interface vlan-interface 3

[QX-Vlan-interface3] dhcp select relay

VLAN インタフェース 3 に DHCP サーバグループ 1 を関連付けます。

[QX-Vlan-interface3] dhcp relay server-select 1

[QX-Vlan-interface3] quit

1.13.3 検証

ユーザ userpt が Web ページにアクセスする前、ユーザは、VLAN8(初期 VLAN)に存在し、サブネット 192.168.1.0/24 の IP アドレスに割り当てられています。ユーザが外部ネットワークの Web ページにアクセスするとき、Web リクエストは認証ページ https://4.4.4.4/portal/logon.htm にリダイレクトされます。正しいユーザ名、パスワードが入力された後、ユーザは認証にパスします。デバイスは VLAN8 から VLAN3 の認可 VLAN に移動します。user view の **display connection ucibindex** コマンドでオンラインユーザ情報を見ることができます。

<QX> display connection ucibindex 30

```
Slot:  1
Index=30  , Username=userpt@triple
MAC=0015-e9a6-7cfe
IP=192.168.1.2
IPv6=N/A
Access=PORTAL  ,AuthMethod=PAP
Port Type=Ethernet,Port Name=GigabitEthernet1/0/1
Initial VLAN=8, Authorization VLAN=3
ACL Group=Disable
User Profile=N/A
CAR=Disable
Priority=Disable
Start=2009-11-26 17:40:02 ,Current=2009-11-26 17:48:21 ,Online=00h08m19s
 Total 1 connection matched.
```

作成された MAC VLAN を見るために display mac-vlan all を使用します。認証にパスした MAC アドレスと対応する VLAN が記録されています。

[QX] display mac-vlan all

```
The following MAC VLAN addresses exist:
S:Static  D:Dynamic
MAC ADDR         MASK             VLAN ID   PRIO   STATE
------------------------------------------------------------
0015-e9a6-7cfe   ffff-ffff-ffff   3         0      D
Total MAC VLAN address count:1
```

クライアントが認証に失敗した場合、VLAN2 に追加されます。上記コマンドを使用して、クライアントの割り当てられた IP アドレスと作成された MAC VLAN エントリを調べます。

目次

2章 PKI 設定

2.1 PKIの導入

2.1.1 PKI 概要

Public Key Infrastructure(PKI)は公開鍵技術を用いて、情報セキュリティを提供する一般的なセキュリティ方式です。

PKI は、非対称鍵方式とも呼ばれ、データの暗号化と復号化の鍵ペアを用います。鍵ペアは秘密鍵と公開鍵から構成されます。秘密鍵は秘密を保つ必要がありますが、公開鍵は分配する必要があります。2 つの鍵の 1 つを用いて暗号化されたデータはもう一方の鍵のみによって、復号化されます。

PKI の鍵の問題点は、公開鍵の管理方法です。この問題を解決するため、PKI はデジタル証明書を使用します。デジタル証明書のメカニズムは、公開鍵がオーナのものであることを結びつけ、安全で大規模なネットワークで公開鍵を配布できるようにします。

デジタル証明書において、PKI システムは、ユーザ認証、データ否認拒否、データの機密性、データの完全性のようなセキュリティサービスを行うネットワーク通信と e-コマースを提供します。

PKI システムは、Secure Sockets Layer (SSL)のため、証明書管理を提供します。

2.1.2 PKI 用語

I. デジタル証明書

デジタル証明書は、エンティティのため、認証局(CA)によってファイルの署名が行われます。主に認証情報、エンティティの公開鍵、CA 名、CA の署名、証明書の有効期間が含まれます。CA の署名が、証明書の有効性を保証します。デジタル証明書は、ITU-T X.509 の国際標準に準拠していなくてはいけません。一般的な標準は X.509 v3 です。

本文書で用いるローカル証明書と CA 証明書について説明します。ローカル証明書は、エンティティのため、CA によってデジタル証明書に署名されます。CA 証明書は CA が証明書に署名します。複数の CA が PKI システムの異なるユーザによって信頼されると、CA はトップレベルがルート CA となる CA ツリーの形となります。ルート CA はそれ自体 CA 証明書をもっており、低レベルの CA は次に高いレベルの CA によって、CA 証明書に署名されます。

II. CRL

発行されている証明書は、ユーザ名の変更、秘密鍵の漏洩、ユーザがビジネスを停止するときなどによって、取り消される必要があります。証明書の取り消しは、ユーザが正しいことを示す情報の公開鍵との結合を削除します。PKI において、取り消しは証明書失効リスト(CRL)によって行われます。証明書が取り消されるとき、CA は、すべての証明書が

取り消されたということを示すため、ひとつあるいは複数の CRL を発行します。CRL はすべての取り消された証明書のシリアル番号を含んでおり、証明書が正しいかをチェックするのに効果的です。

CA は取り消された証明書の数が大きく、複数の CRL が配布されると、ネットワークに悪影響が起こる可能性があるときに、1 つのみ CRL が発行されます。CRL の URL を示すために、CRL 配布ポイントを使います。

III. CA ポリシー

CA ポリシーは CA が証明書リクエスト、失効証明書のプロセスや、CRL の配布を行うための基準です。一般的に CA は証明書実行ステート(CPS)の形式でポリシーを配布します。CA ポリシーは電話、ディスク、電子メールなどの通信外の方法を経由して取得できます。エンティティの公開鍵の結合をチェックする際、異なる CA は、異なる方法を使用します。そのため、信頼された CA を選択する前に、証明書リクエスト用の CA ポリシーを理解する必要があります。

2.1.3 PKI のアーキテクチャ

図 2-1に示すように PKI システムは、エンティティ、CA、登録局(RA)、PKI リポジトリ(repository)から構成されます。

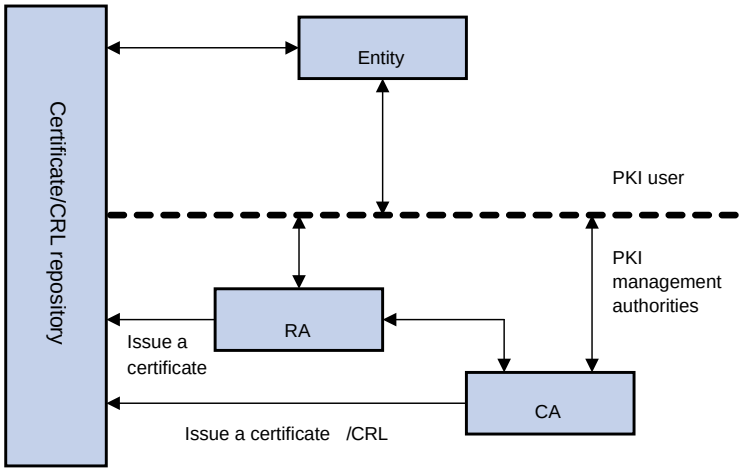

図2-1 PKI アーキテクチャ

I. エンティティ

エンティティは、人や組織、ルータやスイッチやコンピュータで動作するプロセスのようなデバイスなどの PKI の製品やサービスのエンドユーザです。

II. CA

CA はデジタル証明書を発行したり管理したりするための、信頼された機関です。CA は CRL の配布に必要となるため、証明書の発行、証明書の有効期間を指定、失効証明書の取り消しを行います。

III. RA

登録局(RA)は CA の拡張機関、あるいは独立な機関です。CRL 管理、鍵ペア生成、鍵ペアのバックアップを含んだ機能を実装しています。PKI 標準では、アプリケーションシステムの、より高度なセキュリティを実現するため、独立な RA が登録管理されることを推奨しています。

IV. PKI リポジトリ

PKI リポジトリは Lightweight Directory Access Protocol(LDAP)サーバや共通データベースで使われます。単一のクエリ機能を提供している間、証明書リクエスト、証明書、鍵、CRL、ログなどの情報を保存し、管理します。

LDAP は PKI 情報をアクセスし、管理するためのプロトコルです。LDAP サーバは、RA サーバからユーザ情報、デジタル証明書を保存します。ディレクトリナビゲーションサービスを提供します。エンティティは他のエンティティの証明書と同様に、そのローカル証明書と CA 証明書を取得することができます。

2.1.4 PKI のアプリケーション

PKI テクノロジーはオンライン処理のセキュリティ要求事項を満足させます。基盤として PKI は広い範囲のアプリケーションをもっています。ここではいくつかのアプリケーション例をあげます。

I. VPN

仮想プライベートネットワーク(VPN)は、公衆回線網を基にしたプライベートデータ通信ネットワークです。VPN は PKI ベースの暗号化に関連した IPsec や、機密保持のためのデジタル署名技術のような、ネットワークレイヤのセキュリティプロトコルに効果があります。

II. セキュア(安全)な email

Email は機密性、完全性、認証、非拒否性が必要とされます。PKI はこれらのニーズに取り組むことができます。安全な Email プロトコルは、Secure/Multipurpose Internet Mail Extensions (S/MIME)で、急速に発展しています。このプロトコルは PKI ベースを基にしており、署名に暗号化されたメールの転送を行うために使われます。

III. Web セキュリティ

Web セキュリティにおいて、トランスペアレントでセキュアな通信を行うために、アプリケーションレイヤで、最初に 2 つのピアが SSL 通信を確立できます。PKI において、SSL はブラウザとサーバ間で暗号化した通信を有効にします。通信グループの両方は、デジタル証明書を用いて、互いが正しいかアイデンティティを検証することができます。

2.1.5 PKI の動作

PKI が有効であるネットワークにおいて、エンティティは CA からローカル証明書をリクエストできます。デバイスは証明書が正しいかどうかをチェックします。以下に動作を示します。

1) エンティティは RA に証明書リクエストを提出します。
2) RA はエンティティが正しいかアイデンティティを再チェックし、アイデンティティ情報とデジタル署名の公開鍵を CA に送信します。
3) CA はデジタル署名をチェックします。アプリケーションを確認し、証明書を配布します。
4) RA は CA から証明書を受信し、ディレクトリナビゲーションサービスを提供するために LDAP サーバに証明書を送信します。証明書の発行に成功したことをエンティティに通知します。
5) エンティティは証明書を回収します。エンティティは、証明書を使用し、暗号化とデジタル署名によって、安全に他のエンティティと通信することができます。
6) 証明書の取り消しが必要なとき、エンティティは、CA にリクエストします。CA はリクエストを確認します。CRL をアップデートし、LDAP サーバの CRL を公表します。

2.2 PKI 設定手順リスト

以下に PKI を設定する手順を示します。

表2-1 PKI 設定手順リスト

作業		補足
エンティティのDNの設定		必須設定項目
PKIドメインの設定		必須設定項目
PKI証明書リクエストの提出	PKI証明書リクエストの提出	必須設定項目
手動での証明書の取得		オプション設定項目
PKI証明書の確認の設定		オプション設定項目
ローカルRSA鍵ペアの廃棄		オプション設定項目
証明書の削除		オプション設定項目

2.3 エンティティのDNの設定

証明書は、公開鍵とエンティティのアイデンティティ情報を組み合わせます。そしてエンティティ識別名(DN)によって、アイデンティティ情報が、正常かどうか判断します。CA はエンティティ DN によって証明書申請者を独自に識別します。

エンティティ DN は以下のパラメータによって定義されます。

- エンティティの共通名
- 標準 2 文字で表されたエンティティのカントリーコード。たとえば CN は中国、US はアメリカ、JP は日本と表します。
- エンティティの完全修飾ドメイン名(FQDN)、ネットワーク上でエンティティの一意な識別子。ホスト名とドメイン名で構成され、IP アドレスに変換されます。たとえばwww.whatever.comはFQDN、wwwはホスト名、whatever.comはドメイン名です。

- エンティティの IP アドレス
- エンティティがある所在地
- エンティティが所属している組織
- 組織内のエンティティのユニット
- エンティティがある州、県

🕮 **メモ：**

エンティティ DN の設定は、CA 証明書のポリシーに従う必要があります。たとえば、どのエンティティ DN パラメータが必須なのか、オプションなのかを決定する必要があります。そうでないと証明書は拒否されます。

以下にエンティティ DN を設定する手順を示します。

表2-2 エンティティの DN の設定

操作	コマンド	補足
system viewへ移行する	system-view	ー
エンティティを作成し、そのviewに移行する	pki entity *entity-name*	必須設定項目 デフォルト：なし
エンティティの共通名を設定する	common-name *name*	オプション設定項目 デフォルト：なし
エンティティのカントリーコードを設定する	country *country-code-str*	オプション設定項目 デフォルト：なし
エンティティのFQDNを設定する	fqdn *name-str*	オプション設定項目 デフォルト：なし
エンティティのIPアドレスを設定する	ip *ip-address*	オプション設定項目 デフォルト：なし
エンティティの所在地を設定する	locality *locality-name*	オプション設定項目 デフォルト：なし
エンティティの組織を設定する	organization *org-name*	オプション設定項目 デフォルト：なし
エンティティのユニット名を設定する	organization-unit *org-unit-name*	オプション設定項目 デフォルト：なし
エンティティの州あるいは県を設定する	state *state-name*	オプション設定項目 デフォルト：なし

🕮 **メモ：**

- デバイスは 2 つのエンティティを作成することができます。
- Windows 2000 CA サーバは証明書リクエストのデータ長にいくつかの制限があります。もし証明書のエンティティ DN が、証明書のリクエストの制限を越える場合、サーバは証明書のリクエストに応答しません。

2.4 PKIドメインの設定

PKI 証明書のリクエストを行う前に、エンティティは登録情報の設定をする必要があります。登録情報は PKI ドメインとして参照されます。IKE、SSL のような他のアプリケーシ

ョンにとって、PKI ドメインは参照を行う場合に役立ちます。デバイスに設定された PKI ドメインは、CA と他のデバイスには知られません。各 PKI ドメインはそれ自体のパラメータをもちます。

PKI ドメインは以下のパラメータで定義されます。

- trusted CAーエンティティは trusted CA.から証明書をリクエストします。
- エンティティー証明書アプリカント(申請者)は、CA にアイデンティティ情報を提供するためのエンティティを使用します。
- RAーー般的に独立した登録局(RA)は証明書リクエストマネジメントを管理しています。エンティティから登録リクエストを受信し、その資格をチェックします。デジタル証明書に署名するために CA に確認していいかどうかを決めます。RA はエンティティのアプリケーションの資格をチェックするだけで、いかなる証明書も発行しません。独立した RA が必要でない場合、登録の管理は CA が行いますが、独立した RA を配置すべきです。
- 登録サーバの URLーエンティティは、エンティティが CA と通信するために使われる SCEP (Simple Certification Enrollment Protocol)を通して、登録サーバに証明書リクエストを送信します。
- ポーリング間隔と総数ーアプリカントが証明書リクエストを作成した後、手動で証明書リクエストを確認する場合、CA は長い時間かかります。証明書の署名が行われた後、アプリカントができるだけ早く証明書を取得できるように、周期的にリクエストの状態を問い合わせする必要があります。ポーリング間隔と総数を設定することができます。
- LDAP サーバの IP アドレスーLDAP サーバは、普通、証明書と CRL を記録するのに使われます。このため、LDAP サーバの IP アドレスを設定する必要があります。
- ルート証明書が改ざんされていないための証明書データ(フィンガープリント)ーCA のルート証明書を取得した際、エンティティはルート証明書のフィンガープリントを検証する必要があります。これはルート証明書のデータのハッシュ値です。このハッシュ値は、証明書ごとに一意に決まります。ルート証明書のフィンガープリントが PKI ドメイン用に設定されたものと異なる場合、エンティティはルート証明書を拒否します。

PKI ドメインを設定する手順を以下に示します。

表2-3 PKI ドメインの設定

操作	コマンド	補足
system viewへ移行する	system-view	ー
PKIドメインを作成し、そのviewへ移行する	pki domain *domain-name*	必須設定項目 デフォルト：なし
trusted CAを指定する	ca identifier *name*	必須設定項目 デフォルト：なし
証明書リクエスト用のエンティティを指定する	certificate request entity *entity-name*	必須設定項目 デフォルト：なし 指定されたエンティティは必要です。
証明書リクエスト用の機関を指定する	certificate request from { ca | ra }	必須設定項目 デフォルト：なし
証明書リクエスト用のサーバのURLを設定する	certificate request url *url-string*	必須設定項目 デフォルト：なし
証明書リクエスト問い合わせ用のポーリング間隔と総数を設定する	certificate request polling { count *count* | interval *minutes* }	オプション設定項目 デフォルト：ポーリングは20分の間隔で50回です。
LDAPを指定する	ldap-server ip *ip-address* [port *port-number*] [version *version-number*]	オプション設定項目 デフォルト：なし

操作	コマンド	補足
ルート証明書検証のためのフィンガープリントを設定する	root-certificate fingerprint { md5 | sha1 } *string*	証明書リクエストモードが自動の場合は必須設定項目です。 証明書リクエストモードが手動の場合はオプション設定項目。 証明書リクエストモードが手動で、このコマンドが設定されていない場合、ルート証明書のフィンガープリントは手動で検証する必要があります。 デフォルト：なし。

🕮 **メモ：**

- デバイスは 2 つの PKI ドメインを作成できます。
- CA 証明書を取得するときのみ、CA 名が要求されます。ローカル証明書リクエストの時には使われません。
- 証明書リクエスト用のサーバの URL はドメイン名解決をサポートしていません。

2.5 PKI証明書リクエストの提出

証明書を要求する際、エンティティは、アイデンティティ情報と公開鍵を提供することによって、CA に通知します。その情報は証明書の重要な構成要素となります。証明書リクエストは、オンラインモードあるいはオフラインモードでも CA に提出できます。オフラインモードにおいて、証明書リクエストは、電話、ディスク、Email などのような通信外の手段によって、提供されます。

オンライン証明書リクエストは手動モードと自動モードに分けられます。しかし本装置では手動モードのみサポートしています。

2.5.1 証明書リクエストの提出

エンティティ用に、CA 証明書を取得し、ローカル RSA 鍵ペアを作成し、ローカル証明書リクエストを提出する必要があります。

CA 証明書の取得の目的は、ローカル証明書の確実性と妥当性を検証するためです。

RSA 鍵ペアの作成は、証明書リクエストの重要な手順です。鍵ペアは公開鍵と秘密鍵をもっています。秘密鍵はユーザによって保持され、公開鍵は他の情報と一緒に CA に転送されます。

証明書リクエストを提出する手順を以下に示します。

表2-4 証明書リクエストの提出

操作	コマンド	補足
system viewへ移行する	system-view	―
PKI domain viewへ移行する	pki domain *domain-name*	―

操作	コマンド	補足
証明書リクエストモードの手動設定を行う	certificate request mode manual	オプション設定項目 デフォルト：手動
system viewへ戻る	quit	ー
手動でのCA証明書を取得する	手動での証明書の取得を参照	必須設定項目
ローカルRSA鍵ペアを作成する	public-key local create rsa	必須設定項目 デフォルト：なし
手動のローカル証明書リクエストを提出する	pki request-certificate domain *domain-name* [*password*] [pkcs10 [filename *filename*]]	必須設定項目

🕮 **メモ：**

- PKI ドメインがすでにローカル証明書をもっている場合、RSA 鍵ペアの作成は、鍵ペアと証明書が矛盾します。新しい RSA 鍵ペアを作成するため、ローカル証明書を削除した後、**public-key local create** コマンドを実行します。
- 新しく作成された鍵ペアはすでに存在している鍵ペアに上書きされます。もしローカル RSA 鍵ペアを作成する際に、**public-key local create** コマンドを実行する場合、システムは上書きするかどうかの確認メッセージが表示されます。
- もし PKI ドメインがすでにローカル証明書をもっている場合、そのためにまた別の証明書を要求することはできません。これは設定の変更によって証明書と登録情報の間で矛盾が起こらないようにします。
- SCEP を通して、CA から証明書を要求することができないとき、**pki request-certificate domain** コマンドの pkcs10、ファイル名のキーワードを使用することによって、リクエスト情報を保存します。そして通信外の手段によって CA にファイルを送信します。
- エンティティと CA のクロックが同期されていることを確認してください。同期していないと証明書期間が異常となります。
- PKI リクエスト証明書ドメイン設定は、コンフィグファイルに保存されません。

2.6 手動での証明書の取得

CA 証明書とローカル証明書をダウンロードし、それをローカルに保存することができます。オンラインモードやオフラインモードのどちらかで行います。オフラインモードでは FTP、disk、Email のような通信外の手段を用いて証明書を取得する必要があります。ローカル PKI システムに、証明書を取り入れます。

証明書の取得は 2 つの目的に利用されます。

- 取得クエリの効率化とクエリ総数の削減を行うため、ローカルセキュリティドメインに関連した証明書をローカルに保存します。
- 証明書の確認用の準備を行います。

オンラインモードでローカル証明書の取得を行う前に、LDAP サーバの設定を行う必要があります。

手動証明書の取得の手順を以下に示します。

表2-5 手動での証明書の取得

操作		コマンド	補足
system viewへ移行する		system-view	ー
手動証明書を取得する	オンライン	pki retrieval-certificate { ca | local } domain *domain-name*	必須設定項目 どちらかのコマンドを使用します。
	オフライン	pki import-certificate { ca | local } domain *domain-name* { der | p12 | pem } [filename *filename*]	

注意:

- PKI ドメインがすでに CA 証明書をもっている場合、また別の CA 証明書を取得することはできません。これは設定の変更ができないようにすることで証明書と登録情報が矛盾を生じないようにします。
- 新しい CA 証明書を取得するためには、**pki delete-certificate** コマンドを用い、存在する CA 証明書とローカル証明書を最初に削除します。
- PKI の取得と証明書の設定は、コンフィグファイルに保存されません。
- 証明書を有効とさせるため、デバイスのシステム時間が証明書の妥当な期間内にあることを確認してください。

2.7 PKI証明書の確認の設定

証明書は使用する前に確認する必要があります。証明書が CA によって署名されており、証明書の期限が切れていないことや無効でないことを確認します。

証明書の確認を行う前に、CA 証明書を取得する必要があります。

CRL のチェックは、証明書の確認で使うか指定することができます。もし CRL チェックを有効にした場合、CRL は証明書の確認に使われます。

I. CRL チェック機能有効時の PKI 証明書の確認の設定

CRL チェック有効時の PKI 証明書の確認の設定手順を以下に示します。

表2-6 CRL チェック機能有効時の PKI 証明書の確認の設定

操作	コマンド	補足
system viewへ移行する	system-view	ー
PKI domain viewへ移行する	pki domain *domain-name*	ー
CRL発行ポイントのURLを指定する	crl url *url-string*	オプション設定項目 デフォルト：指定なし
CRLアップデート期間を設定する	crl update-period *hours*	オプション設定項目 デフォルト：CRLアップデート期間はCRLファイルのネクストアップデートフィールドに依存します。
CRLチェックを有効にする	crl check enable	オプション設定項目 デフォルト：有効

操作	コマンド	補足
system viewへ戻る	quit	ー
CA証明書を取得する	手動での証明書の取得を参照してください。	必須設定項目
CRLを取得する	pki retrieval-crl domain *domain-name*	必須設定項目
証明書の有効性をチェックする	pki validate-certificate { ca | local } domain *domain-name*	必須設定項目

II. CRL チェック機能無効時の PKI 証明書の確認の設定

CRL チェック無効時の PKI 証明書の確認の設定の手順を以下に示します。

表2-7 CRL チェック機能無効時の PKI 証明書の確認の設定

操作	コマンド	補足
system viewへ移行する	system-view	ー
PKI domain viewへ移行する	pki domain *domain-name*	ー
CRLチェックを無効にする	crl check disable	必須設定項目 デフォルト：有効
system viewへ戻る	quit	ー
CA証明書を取得する	手動での証明書の取得を参照してください。	必須設定項目
証明書の有効性をチェックする	pki validate-certificate { ca | local } domain *domain-name*	必須設定項目

🕮 **メモ：**

- CRL アップデート期間は、エンティティが CRL サーバから CRL をダウンロードする間隔を参考にしています。CRL アップデート期間は、CRL で指定された期間よりも優先して設定されます。
- PKI 取得 CRL ドメインの設定は、設定ファイルに保存されません。
- CRL 発行ポイントの URL はドメイン名解決をサポートしていません。

2.8 ローカルRSA鍵ペアの廃棄

証明書はライフタイムをもっています。ライフタイムは CA によって決められます。秘密鍵が漏洩したり、証明書が期限切れとなったりする場合、古い RSA 鍵ペアの破棄を行います。そして新しい証明書を要求するリクエストのペアを作成します。

ローカル RSA ペアを廃棄する手順を以下に示します。

表2-8 ローカル RSA 鍵ペアの廃棄

操作	コマンド	補足
system viewへの移行する	system-view	ー
ローカルRSA鍵ペアを廃棄する	public-key local destroy rsa	必須設定項目

🕮 **メモ：**

古い RSA 鍵ペアを完全に削除するためには装置の再起動が必要です。新しい RSA 鍵ペアを作成する場合は再起動の必要はありません。

2.9 証明書の削除

手動でリクエストされた証明書が期限切れとなったり、新しい証明をリクエストしたりする場合、現在のローカル証明書あるいは CA 証明書を削除します。

証明書を削除する手順を以下に示します。

表2-9 証明書の削除

操作	コマンド	補足
system viewへ移行する	system-view	―
証明書を削除する	pki delete-certificate { ca | local } domain *domain-name*	必須設定項目

🕮 **メモ：**

証明書を完全に削除するためには装置の再起動が必要です。新しい証明書を取得する場合は再起動の必要はありません。

2.10 PKIの表示

表2-10 PKI の表示

操作	コマンド	補足
証明書のコンテンツやリクエストステータスを表示する	display pki certificate { { ca | local } domain *domain-name* | request-status } [| { begin | exclude | include } *regular-expression*]	すべてのviewで実行可能です。
CRLを表示する	display pki crl domain *domain-name* [| { begin | exclude | include } *regular-expression*]	すべてのviewで実行可能です。

2.11 PKI 設定例

⚠ **注意:**

SCEP アドオンは CA として Windows サーバを使用するときに必要となります。この場合、PKI ドメインの設定を行うとき、エンティティが RA から証明書をリクエストするために、ra コマンドで証明書リクエストを使用する必要があります。

2.11.1 Windows2003 サーバで動作している CA から証明書の要求

🕮 **メモ：**

本章の設定例では、CA サーバは Windows2003 サーバで動作します。

I. ネットワーク要件

CA サーバからローカル証明書をリクエストするスイッチの PKI エンティティを設定します。

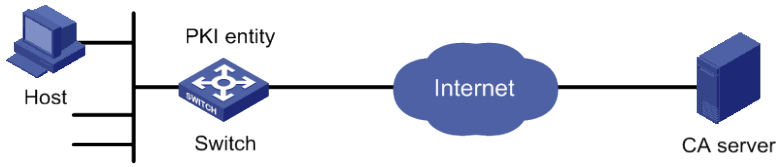

図2-2 Windows 2003 サーバで動作している CA から証明書のリクエスト

II. 設定手順

1) CA サーバの設定

- 証明書サービスセットのインストール

スタートメニューから、コントロールパネルのプログラムの追加と削除を選択します。Add/Remove Windows コンポーネントの証明書サービスを選択します。Next ボタンをクリックし、インストールを開始します。

- SCEP アドオンのインストール

Windows2003 サーバで動作する CA サーバはデフォルトで SCEP をサポートしていません。スイッチが証明書を登録、取得できるようにするため、SCEP アドオンをインストールする必要があります。SCEP アドオンのインストールが完了した後、URL が表示されます。その URL は、証明書の登録を行うため、サーバの URL としてスイッチに設定する必要があります。

- 証明書サービスアトリビュートの取得

スタートメニューから、コントロールパネル＞管理ツール＞証明書機関を選択します。CA サーバと SCEP アドオンが正しくインストールされた場合、CA によって RA に 2 つの証明書が発行されます。ナビゲーションツリーの CA サーバを右クリックし、プロパティ＞ポリシーモジュールを選択します。もし適用できるならば、プロパティをクリックし、証明書テンプレートにある設定の Follow を選択します。適用できなければ、自動的に証明書が発行されます。

- インタネット情報サービス(IIS)アトリビュートの取得

スタートメニューからコントロールパネル＞管理ツール＞インタネット情報サービス(IIS)マネージャを選択し、ナビゲーションツリーから Web サイトを選択します。デフォルト Web サイトを右クリックし、プロパティ＞ホームディレクトリを選択します。ローカルパステキストボックスにある証明書サービスのパスを指定します。加えて、現存するサービスと衝突しないように、デフォルト Web サイトの TCP ポート番号として有効なポート番号を指定します。

設定を行った後、スイッチが正常に証明書をリクエストできるようにするため、スイッチのシステムクロックが CA サーバのシステムクロックと同期しているか確認します。

2) スイッチの設定

- エンティティ DN の設定

エンティティ名を aaa、共通名を switch と設定します。

<QX> system-view

[QX] pki entity aaa

[QX-pki-entity-aaa] common-name switch

[QX-pki-entity-aaa] quit

- PKI ドメインの設定

#PKI ドメイン torsa を作成し、PKI ドメインに移行します。

[QX] pki domain torsa

trusted CA 名 myca を設定します。

[QX-pki-domain-torsa] ca identifier myca

証明書サーバの URL を http://host:port/ certsrv/mscep/mscep.dll の形式で設定します。host:port は CA サーバの IP アドレスとポート番号を示します。

[QX-pki-domain-torsa] certificate request url http://4.4.4.1:8080/certsrv/mscep/mscep.dll

RA に証明書機関を設定します。

[QX-pki-domain-torsa] certificate request from ra

証明書リクエスト用のエンティティ aaa を指定します。

[QX-pki-domain-torsa] certificate request entity aaa

- RSA を使用してローカル鍵ペアを作成します。

[QX] public-key local create rsa

```
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating Keys...
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++
```

- 証明書の適用

#CA 証明書の取得を行い、それをローカルに保存します。

[QX] pki retrieval-certificate ca domain torsa

```
Retrieving CA/RA certificates. Please wait a while......
The trusted CA's finger print is:
    MD5  fingerprint:766C D2C8 9E46 845B 4DCE 439C 1C1F 83AB
    SHA1 fingerprint:97E5 DDED AB39 3141 75FB DB5C E7F8 D7D7 7C9B 97B4

Is the finger print correct?(Y/N):y

Saving CA/RA certificates chain, please wait a moment......
CA certificates retrieval success.
```

手動ローカル証明書をリクエストします。

[QX] pki request-certificate domain torsa challenge-word

```
Certificate is being requested, please wait......
```

[QX]

```
Enrolling the local certificate,please wait a while......
Certificate request Successfully!
Saving the local certificate to device......
Done!
```

3) 設定の確認

#以下のコマンドを用いて、取得されたローカル証明書の情報を表示します。

[QX] display pki certificate local domain torsa

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            48FA0FD9 00000000 000C
        Signature Algorithm: sha1WithRSAEncryption
        Issuer:
            CN=myca
        Validity
            Not Before: Nov 21 12:32:16 2007 GMT
            Not After : Nov 21 12:42:16 2008 GMT
        Subject:
            CN=switch
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00A6637A 8CDEA1AC B2E04A59 F7F6A9FE
                    5AEE52AE 14A392E4 E0E5D458 0D341113
                    0BF91E57 FA8C67AC 6CE8FEBB 5570178B
                    10242FDD D3947F5E 2DA70BD9 1FAF07E5
                    1D167CE1 FC20394F 476F5C08 C5067DF9
                    CB4D05E6 55DC11B6 9F4C014D EA600306
                    81D403CF 2D93BC5A 8AF3224D 1125E439
                    78ECEFE1 7FA9AE7B 877B50B8 3280509F
                    6B
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
            B68E4107 91D7C44C 7ABCE3BA 9BF385F8 A448F4E1
            X509v3 Authority Key Identifier:
            keyid:9D823258 EADFEFA2 4A663E75 F416B6F6 D41EE4FE

            X509v3 CRL Distribution Points:
            URI:http://l00192b/CertEnroll/CA%20server.crl
            URI:file://\\l00192b\CertEnroll\CA server.crl

            Authority Information Access:
            CA Issuers - URI:http://l00192b/CertEnroll/l00192b_CA%20server.crt
            CA Issuers - URI:file://\\l00192b\CertEnroll\l00192b_CA server.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
        81029589 7BFA1CBD 20023136 B068840B
(省略)
```

他の display コマンドー**display pki certificate ca domain** コマンドを使用できます。CA 証明書の詳細な情報を表示します。

2.12 PKIのトラブルシューティング

2.12.1 CA 証明書の取得に失敗

I. 現象

CA 証明書の取得に失敗しました。

II. 解析

以下の原因が考えられます。

- ネットワーク接続が正しくありません。たとえばネットワークケーブルの損傷あるいは切断。
- trusted CA が指定されていません。
- 証明書リクエスト用の証明書サーバの URL が不正あるいは設定されていません。
- 証明書リクエスト用の機関が設定されていません。
- デバイスのシステムクロックが CA のシステムクロックと同期していません。

III. 解決方法

- ネットワーク接続が物理的に正しいか確認します。
- 必要とされるコマンドが正しく設定されたか確認します。
- ping コマンドを用いて、RA サーバに通信可能か確認します。
- 証明書リクエスト用の機関を指定します。
- デバイスのシステムクロックを CA のシステムクロックと同期させます。

2.12.2 ローカル証明書のリクエストに失敗

I. 現象

ローカル証明書のリクエストに失敗しました。

II. 解析

以下の原因が考えられます。

- ネットワーク接続が正しくありません。たとえばネットワークケーブルの損傷あるいは切断。
- CA 証明書が取得されていません。
- 現在の鍵ペアが証明書と関連付けられていません。
- trusted CA が指定されていません。
- 証明書リクエスト用の証明書サーバの URL が不正あるいは設定されていません。
- 証明書リクエスト用の機関が設定されていません。
- エンティティ DN の必要なパラメータが設定されていません。

III. 解決方法

- ネットワーク接続が物理的に正しいか確認します。
- CA 証明書を取得します。
- 鍵ペアを再度作成します。

- trusted CA を指定します。
- ping コマンドを用いて、RA サーバに通信可能か確認します。
- 証明書リクエスト用の機関を指定します。
- エンティティ DN の必要なパラメータを設定します。

2.12.3 CRL の取得に失敗

I. 現象

CRL の取得に失敗しました。

II. 解析

以下の原因が考えられます。

- ネットワーク接続が正しくありません。たとえばネットワークケーブルの損傷あるいは切断。
- CRL の取得をする前に、CA 証明書が取得されていません。
- LDAP サーバの IP アドレスが設定されていません。
- CRL 配布 URL が設定されていません。
- LDAP サーババージョンが間違っています。

III. 解決方法

- ネットワーク接続が物理的に正しいか確認します。
- CA 証明書を取得します。
- LDAP サーバの IP アドレスを指定します。
- CRL 配布 URL を指定します。
- LDAP バージョンの再設定を行います。

目次

3章 SSL 設定

3.1 SSL概要

Secure Sockets Layer (SSL) は、HTTP のような TCP ベースのアプリケーションレイヤプロトコルのセキュアなコネクションサービスを提供するセキュリティプロトコルです。

SSL は、e ビジネスやインタネットでセキュアなデータ通信を保証する必要があるオンライン銀行などに広く使われます。

3.1.1 SSL セキュリティメカニズム

SSL によって提供されるセキュアな通信は以下の特徴があります。

- **機密性**－SSL はデータを暗号化する対称暗号アルゴリズムを使用しています。そして対象暗号アルゴリズムによって作成された鍵を暗号化するために、Rivest, Shamir, and Adelman (RSA)の非対称の鍵アルゴリズムを使用します。
- **認証**－SSL は証明書を基にした、デジタル署名に使われるサーバとクライアントの同一性を示す認証をサポートしています。SSL サーバとクライアントは、公開鍵基盤を用いて、認証局(CA)から証明書を取得します。
- **信頼性**－SSL は、メッセージの完全性をチェックするため、鍵を基にしたメッセージ認証コード(MAC)を使用します。MAC アルゴリズムは、可変長のメッセージを固定長に変更します。図 3-1にメッセージの完全性をチェックする MAC アルゴリズムを使用する SSL について示します。送信元は、鍵のために、メッセージの MAC の値を計算する MAC アルゴリズムを使用します。次に送信元は、MAC の値をメッセージに添付し、結果を宛先に送信します。宛先は同じ鍵を用い、受信したメッセージの MAC の値を計算する MAC アルゴリズムを使用し、受信された MAC の値とローカルに計算された値と比較します。それぞれの MAC の値が同じならば、宛先はメッセージが損なわれていないと判断します。MAC の値が異なる場合、転送中にメッセージが変更されたと認識し、メッセージを廃棄します。

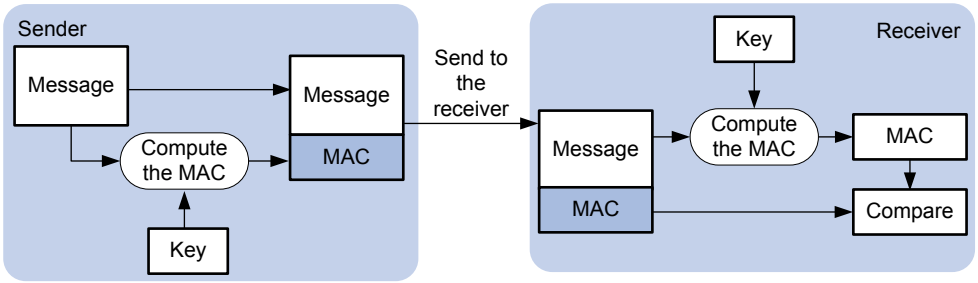

図3-1 MAC アルゴリズムによるメッセージの完全性の検証

3.1.2 SSL プロトコルスタック

図 3-2に示すように、SSL は 2 つのレイヤのプロトコルから構成されます。低いレイヤの SSL レコードプロトコルと、上位の SSL ハンドシェイクプロトコル、SSL change cipher spec プロトコル、SSL alert プロトコルがあります。

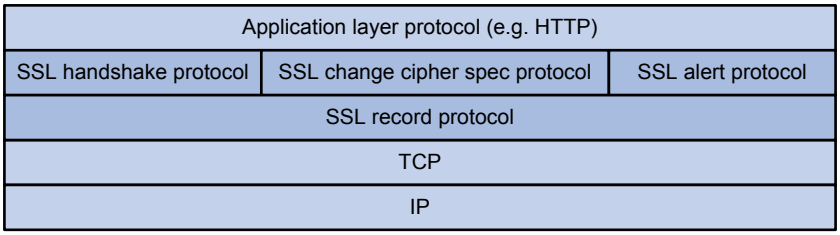

図3-2 SSL プロトコルスタック

- **SSL レコードプロトコル**－転送されたデータをフラグメントし、データに MAC を追加し、計算します。対向先に転送する前にデータを暗号化します。
- **SSL ハンドシェイクプロトコル**－SSL プロトコルスタックの重要な部分です。信頼できるセキュアな通信に使われる暗号方式を決めます（非対称暗号アルゴリズム、鍵交換アルゴリズム、MAC アルゴリズムを含みます）。また、サーバとクライアント間の鍵交換をセキュアに行い、サーバとクライアントが、なりすましなどが行われていないことを示す同一性の認証を提供します。SSL ハンドシェイクプロトコルを通して、セッションがサーバとクライアント間で取得されます。セッションは、セッション ID、ピア証明書、暗号文、master secret を含んだパラメータから構成されます。
- **SSL 変更暗号文スペックプロトコル(SSL change cipher spec protocol)**－連続パケットを保護し、新規にネゴシエートされた暗号方式と鍵を基にして転送するためにクライアントとサーバ間でやりとりされるプロトコルです。
- **SSL 警告プロトコル(SSL alert protocol)**－SSL クライアントとサーバにお互いに警告メッセージを送信するプロトコルです。警告メッセージは、警告シビアリティレベルと説明文を含みます。

3.2 SSL設定手順リスト

以下に SSL 設定手順を示します。

作業	補足
SSLサーバポリシーの設定	必須項目

3.3 SSLサーバポリシーの設定

SSL サーバポリシーは、サーバが立ち上がったときに使われる SSL パラメータです。SSL サーバポリシーは HTTP プロトコルのようなアプリケーションレイヤのプロトコルに関連している場合のみ効果があります。

3.3.1 設定必要条件

SSL サーバポリシーの PKI ドメインを設定します。PKI ドメインは、サーバ側の証明書を取得するのに使われます。

3.3.2 設定手順

以下に SSL サーバポリシーを設定する手順を示します。

操作	コマンド	補足
system viewへ移行する	**system-view**	ー
SSLサーバポリシーの作成とそのviewへ移行する	**ssl server-policy** *policy-name*	必要項目
SSLサーバポリシー用のPKIドメインを指定する	**pki-domain** *domain-name*	必要項目 デフォルト：なし

🕮 **メモ：**

- クライアント認証を有効にした場合、クライアント用にローカル証明書を要求する必要があります。
- SSL は主に SSL2.0、3.0、TLS1.0 のバージョンを使用します。TLS1.0 は SSL3.1 に対応します。装置が SSL サーバとして動作するとき、SSL3.0 や TLS1.0 で動作するクライアントと通信することができます。そしてクライアントからの Hello パケットを識別することで、クライアントが SSL2.0 で動作することを確認することができます。もしクライアントが、SSL2.0 に加えて SSL3.0 あるいは TLS1.0 をサポートする場合、サーバは、クライアントに SSL3.0 あるいは TLS1.0 を使用して通信するということを通知します。サポートされるバージョン情報は、クライアントがサーバに送信するパケットに含まれます。

3.4 SSL3.0の無効化

⚠ **注意:**

SSL Version 3.0 の設定を変更する場合、**ssl version ssl3.0 disable** コマンドあるいは **undo ssl version ssl3.0 disable** コマンドを設定したのち、HTTPS サービスを有効にする必要があります。すでに HTTPS サービスが有効である場合、無効にしたのち、再度有効にしてください。

メモ：

SSL3.0 を無効にする機能は、以下のソフトウェアでサポートしています。

- QX-S4000 シリーズ：Version 5.4.14 を含む以降のソフトウェア
- QX-S5300 シリーズ：Version 5.1.11 を含む以降のソフトウェア
- QX-S5700 シリーズ：Version 5.1.12 を含む以降のソフトウェア

システムセキュリティを拡張するため、装置で SSL3.0 を無効にします。

- SSL3.0 を無効にしたのち、SSL サーバは TLS1.0 のみサポートします。
- SSL3.0 が無効あるいは有効にかかわらず、クライアントポリシーで SSL3.0 を指定している場合、SSL クライアントは常に SSL3.0 を使用します。

SSL 接続を正常に確立するため、対向装置が SSL3.0 のみをサポートしている場合、装置で SSL3.0 を無効にしないでください。セキュリティのために、TLS1.0 をサポートさせるため対向装置のアップグレードを行うことを推奨します。

以下に装置で SSL3.0 を無効にする手順を示します。

操作	コマンド	補足
system viewへ移行する	**system-view**	ー
装置でSSL3.0を無効にする	**ssl version ssl3.0 disable**	デフォルト：有効

3.5 SSLの表示

操作	コマンド	補足
SSLサーバポリシー情報を表示する	**display ssl server-policy** { *policy-name* | **all** } [| { **begin** | **exclude** | **include** } *regular-expression*]	すべてのviewで有効です。

目次

4章　トリプル認証

4.1　トリプル認証の概要

4.1.1　概要

LAN に接続されている端末は、異なる認証方式をサポートしています。図 4-1に示すように、プリンタは MAC アドレス認証のみ、802.1X クライアントでインストールされた PC は 802.1X 認証、他の PC は Web 認証(ポータル認証)をサポートしています。異なる認証方式を満足するため、端末に接続するアクセスデバイスのポートは、これらの 3 つの認証方式をサポートし、端末が 1 つの認証タイプをパスした後、ネットワークにアクセスすることを許可する必要があります。

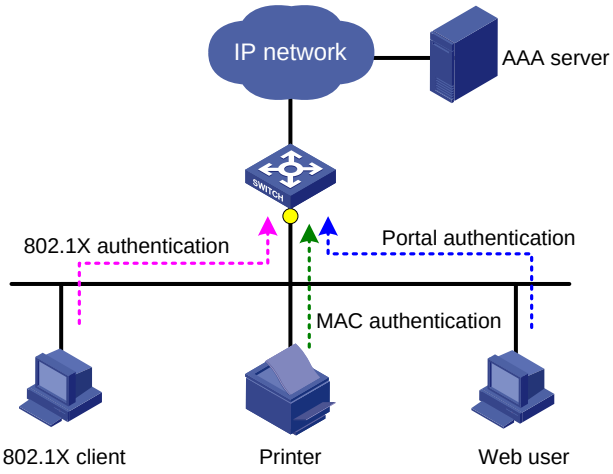

図4-1　トリプル認証ネットワーク図

トリプル認証ソリューションは、上記の必要条件を満足させることができます。トリプル認証は、レイヤ 2 アクセスポートで Web 認証、MAC アドレス認証、802.1X 認証を有効にすることができます。ポートに接続された端末は認証にパスした後、ネットワークにアクセスできます。

4.1.2　トリプル認証メカニズム

アクセスポートで有効になる認証の 3 つのタイプは、トリガーによって、実行される認証タイプが異なります。

- 端末から ARP や DHCP ブロードキャストパケットを受信した場合、アクセスポートは、最初に MAC アドレス認証を実行します。MAC アドレス認証に失敗した場合、802.1X あるいは Web 認証が実行されます。
- 802.1X クライアントやサードパーティのクライアントから EAP パケットを受信した場合、アクセスポートは 802.1X 認証のみを実行します。

- 端末から HTTP パケットを受信した場合、アクセスポートは Web 認証を実行します。

もし端末が複数の認証タイプをサポートしている場合、認証は同時に行われます。1 つの認証タイプに失敗した場合、他の認証に影響しません。認証の 1 つにパスしたとき、他のタイプの認証は終了しますが、その後他の認証タイプがトリガーとなるかは異なります。

- 端末が 802.1X 認証あるいは Web 認証にパスした場合、他の認証タイプはトリガーとなりません。
- 端末が MAC アドレス認証にパスした場合、Web 認証はトリガーとなりませんが、802.1X 認証がトリガーになります。MAC アドレス認証にパスした端末が 802.1X 認証にパスした場合、MAC アドレス認証情報に 802.1X 認証情報を上書きします。

4.1.3 拡張機能

トリプル認証が有効化されたポートは、以下の拡張機能をサポートしています。

I. VLAN 割り当て

端末が認証をパスした後、認証サーバはアクセスポートに VLAN を割り当てます。端末はサーバが割り当てた VLAN 内のネットワークリソースにアクセスすることができます。

🕮 **メモ：**

VLAN 割り当てをサポートするには、ポートで MAC ベース VLAN の有効化が必要です。

II. Auth-Fail VLAN あるいは guest VLAN

端末が認証に失敗した後、アクセスポートは使用する認証サービスによって、端末に追加する VLAN が異なります。

- 802.1X あるいは Web 認証サービスを使用する場合、アクセスポートは端末を Auth-Fail VLAN に追加します。
- MAC アドレス認証サービスを使用する場合、アクセスポートは端末を guest VLAN に追加します。

🕮 **メモ：**

Web 認証の通常の操作を保証するため、802.1X のゲスト VLAN を有効にしないことを推奨します。

III. オンライン端末の検出

- オンラインのポータルクライアントを検出するため、オンライン検出タイマが有効になっています。タイマのデフォルトは、10 分です。タイマ値は変更できますが、無効にすることはできません。
- 設定された間隔で、オンラインの 802.1X クライアントを検出するため、周期的なオンラインユーザの再認証機能を有効にすることができます。
- 設定された間隔で、オンラインの MAC アドレス認証が終了することを検出するため、オフライン検出タイマを有効にすることができます。

4.2 トリプル認証設定手順

作業	補足	
802.1x認証の設定	MACベースのアクセスコントロール(macbased)が必要です。	必要項目 3つのなかで少なくとも1タイプの認証が必要です。
MACアドレス認証の設定	ー	
Web認証の設定	ー	

4.3 トリプル認証設定例

4.3.1 トリプル認証基本機能設定例

I. ネットワーク要件

図 4-2に示すように端末は IP ネットワークにアクセスするスイッチに接続されています。端末に接続しているスイッチのレイヤ 2 インタフェースにトリプル認証を設定する必要があります。802.1X 認証、Web 認証、MAC アドレス認証の 3 つの認証のなかでどれか 1 つの認証がパスしている端末が IP ネットワークにアクセスできるようにします。具体的に以下に示します。

- 端末用に 192.168.1.0/24 のネットワークでスタティック IP アドレスを設定します。
- 認証、認可、アカウンティングを行うためリモート RADIUS サーバを使用します。RADIUS サーバに ISP ドメイン名を保持していないユーザ名を送信するようにスイッチの設定をします。
- スイッチ上のローカル Web 認証サーバはリスニング IP アドレス 4.4.4.4 を使用します。スイッチは、デフォルト認証ページを Web ユーザに送信し、HTTP を使用して認証データを転送します。

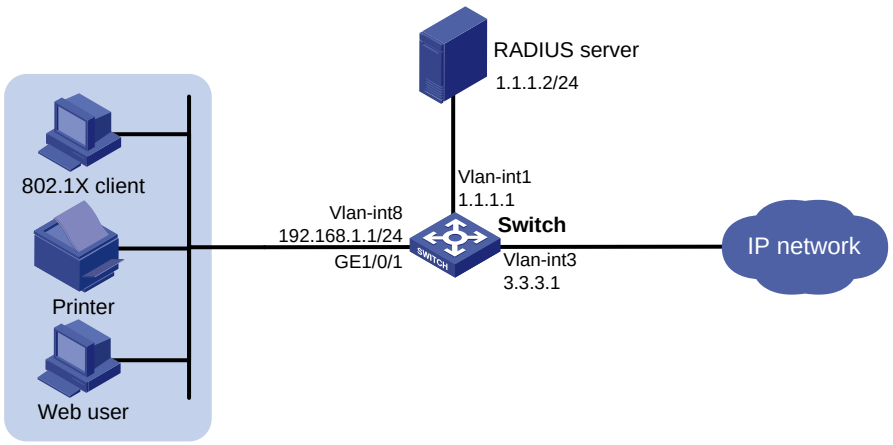

図4-2 トリプル認証基本機能設定例

II. 設定手順

🕮 **メモ：**

- サーバ、スイッチがそれぞれ通信可能であることを確認してください。
- Web ユーザのホストは、ローカルポータルサーバのリスニング IP アドレスへのルートを持つ必要があります。
- RADIUS サーバの設定を行ってください。認証、認可、アカウンティングが正常に動作することを確認してください。この例では RADIUS サーバは、802.1X ユーザ(ユーザ名 userdot)、ポータルユーザ(ユーザ名 userpt)、MAC アドレス認証ユーザ(ユーザ名とパスワードはプリンタの MAC アドレス 001588f80dd7 からなります)を設定します。
- MAC アドレス認証と Web 認証を一緒に設定しているポートでは、移動ポータルユーザ機能は再認証が必要となります。

1)　Web 認証の設定

VLAN インタフェースの VLAN と IP アドレスの設定、VLAN へのポートの追加(省略)

HTTP をサポートするローカルポータルサーバを設定します。

<QX> system-view

[QX] portal local-server http

インタフェース loopback12 の IP アドレスを 4.4.4.4 に設定します。

[QX] interface loopback 12

[QX-LoopBack12] ip address 4.4.4.4 32

[QX-LoopBack12] quit

#Web 認証用のローカルポータルサーバのリスニング IP アドレスを 4.4.4.4 に指定します。

[QX] portal local-server ip 4.4.4.4

GigabitEthernet 1/0/1 で Web 認証を有効化します。

[QX] interface gigabitethernet 1/0/1

[QX–GigabitEthernet1/0/1] portal local-server enable

[QX–GigabitEthernet1/0/1] quit

2)　802.1X 認証の設定

802.1X 認証のグローバル設定

[QX] dot1x

GigabitEthernet 1/0/1 に 802.1X 認証(MAC ベースアクセスコントロールが必要)を有効化します。

[QX] interface gigabitethernet 1/0/1

[QX–GigabitEthernet1/0/1] dot1x port-method macbased

[QX–GigabitEthernet1/0/1] dot1x

[QX–GigabitEthernet1/0/1] quit

3) MAC アドレス認証の設定

MAC アドレス認証のグローバル設定

[QX] mac-authentication

GigabitEthernet 1/0/1 に MAC アドレス認証を有効化します。

[QX] interface gigabitethernet 1/0/1

[QX–GigabitEthernet1/0/1] mac-authentication

[QX–GigabitEthernet1/0/1] quit

4) RADIUS スキームの設定

RADIUS スキーム rs1 を作成します。

[QX] radius scheme rs1

プライマリ認証とアカウンティングサーバとキーを指定します。

[QX-radius-rs1] primary authentication 1.1.1.2

[QX-radius-rs1] primary accounting 1.1.1.2

[QX-radius-rs1] key authentication radius

[QX-radius-rs1] key accounting radius

RADIUS サーバに送信されるユーザ名は、ドメイン名を保持しないことを指定します。

[QX-radius-rs1] user-name-format without-domain

[QX-radius-rs1] quit

5) ドメインの設定

ISP ドメイン triple を作成します。

[QX] domain triple

ドメインで、ユーザのすべてのタイプにデフォルト AAA 方式を設定します。

[QX-isp-triple] authentication default radius-scheme rs1

[QX-isp-triple] authorization default radius-scheme rs1

[QX-isp-triple] accounting default radius-scheme rs1

[QX-isp-triple] quit

デフォルトドメインとしてドメイン triple を設定します。もしユーザ名が ISP ドメイン名を含んでいない場合、デフォルトドメインの認証方式が使われます。

[QX] domain default enable triple

III. 確認

ユーザ userdot は、認証の初期化を行う際 802.1X クライアントを使用します。ユーザは、正しいユーザ名、パスワードを入力した後、802.1X 認証をパスすることができます。Web

ユーザ userpt は外部ネットワークにアクセスするため、Web ブラウザを使用します。Web リクエストは認証ページ http://4.4.4.4/portal/logon.htm にリダイレクトされます。正しいユーザ名とパスワード名を入力した後、Web ユーザは Web 認証をパスすることができます。プリンタはネットワークに接続した後、MAC アドレス認証をパスすることができます。

オンラインユーザの接続情報を見る場合、**display connection** コマンドを使用します。

[QX] display connection

```
Slot:  1
Index=30  , Username=userpt@triple
 IP=192.168.1.2
 IPv6=N/A
 MAC=0015-e9a6-7cfe
Index=31  , Username=userdot@triple
 IP=192.168.1.3
 IPv6=N/A
 MAC=0002-0002-0001
Index=32  , Username=001588f80dd7@triple
 IP=192.168.1.4
 IPv6=N/A
 MAC=0015-88f8-0dd7

 Total 3 connection(s) matched on slot 1.
 Total 3 connection(s) matched.
```

4.3.2 VLAN 割り当てと Auth-Fail VLAN をサポートしたトリプル認証の設定例

I. ネットワーク要件

図 4-3に示すように、端末が IP ネットワークにアクセスするスイッチに接続されています。端末に接続しているスイッチのレイヤ 2 インタフェースのトリプル認証の設定が必要です。端末が 802.1X 認証、Web 認証、MAC アドレス認証の 3 つの認証方式のなかでどれか 1 つの認証にパスし、IP ネットワークに接続できるようにします。

- ポータルクライアントは DHCP を用いて IP アドレスを要求します。認証がパスする前は 192.168.1.0/24 のネットワークアドレスを持ち、認証にパスした後、3.3.3.0/24 のネットワークアドレスに入ります。
- 802.1X 端末は認証が行われる前、192.168.1.0/24 のネットワークアドレスを持ち、認証にパスした後、DHCP を用いて 3.3.3.0/24 のネットワークアドレスを要求します。端末が認証に失敗すると、2.2.2.0/24 のネットワークアドレスに入ります。
- MAC アドレス認証にパスした後、プリンタは 3.3.3.111/24 のアドレスを取得します。このアドレスは DHCP を用いて MAC アドレスと結び付けられたものです。
- 認証、認可、アカウンティングを実行するリモート RADIUS サーバを使用します。スイッチが RADIUS サーバにユーザ名を送信する設定を行います。このユーザ名は ISP ドメイン名が保持されていません。
- スイッチのローカル Web 認証サーバはリスニング IP アドレス 4.4.4.4 を使用します。スイッチは、デフォルト認証ページを Web ユーザに送信し、HTTPS を使用して認証データを転送します。
- RADIUS サーバに認可 VLAN として VLAN3 を設定します。認証にパスしたユーザは、この VLAN に追加されます。
- アクセスデバイスに Auth-Fail VLAN として VLAN2 を設定します。認証に失敗したユーザは、この VLAN に追加され、アップデートサーバのみアクセスできます。

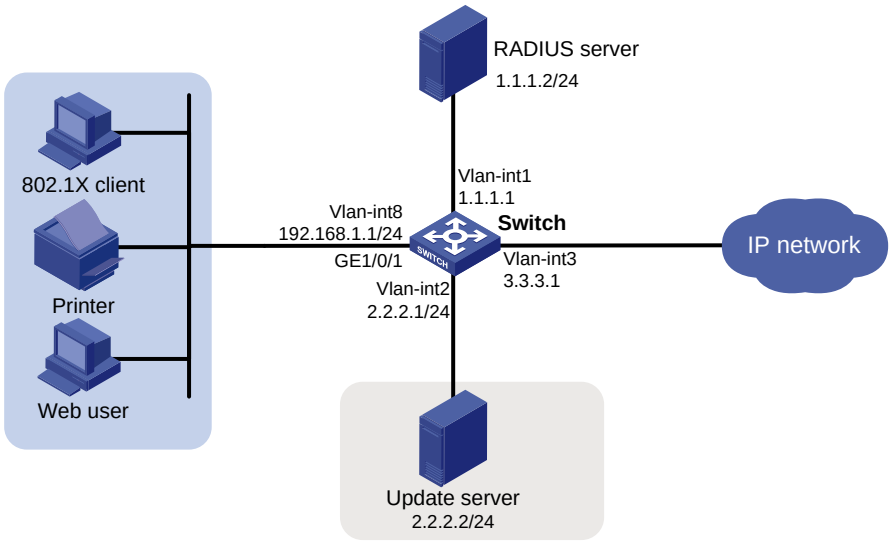

図4-3 VLAN 割り当てと Auth-Fail VLAN をサポートしたトリプル認証のネットワーク図

II. 設定手順

メモ：

- サーバ、スイッチがそれぞれ通信可能であることを確認してください。
- MAC アドレス認証と 802.1X 認証を一緒に設定しているポートでは、ユニキャストトリガ機能は無効となります。
- DHCP サーバ機能をサポートしていない装置は、外部 DHCP サーバを使用してください。
- 外部 DHCP サーバを使用する場合、端末が認証前後にサーバから IP アドレスを確実に取得できるようにしてください。
- RADIUS サーバの設定を行ってください。認証、認可、アカウンティングが正常に動作することを確認してください。この例では RADIUS サーバは、802.1X ユーザ(ユーザ名 userdot)、ポータルユーザ(ユーザ名 userpt)、MAC アドレス認証ユーザ(ユーザ名とパスワードはプリンタの MAC アドレス 001588f80dd7 からなります)、認可 VLAN(VLAN3)を設定します。
- PKI ドメイン pkidm、ローカル証明書の取得、CA 証明書の取得の設定を行ってください。
- 認証ページファイルの編集を行う場合、defaultfile という名前で zip ファイルに圧縮し、ルートディレクトリに zip ファイルを保存してください。
- MAC アドレス認証と Web 認証を一緒に設定しているポートでは、移動ポータルユーザ機能は再認証が必要となります。

1)　DHCP の設定

VLAN インタフェースの VLAN と IP アドレスの設定、VLAN へのポートの追加を行います(詳細は省略します)。

DHCP を有効化します。

<QX> system-view

[QX] dhcp enable

割り当てからアップデートサーバの IP アドレスを除外します。

[QX] dhcp server forbidden-ip 2.2.2.2

アドレス範囲、リース期間、ゲートウェイアドレスを含んだ IP アドレスプール 1 を設定します。

[QX] dhcp server ip-pool 1

[QX-dhcp-pool-1] network 192.168.1.0 mask 255.255.255.0

[QX-dhcp-pool-1] expired day 0 hour 0 minute 1

[QX-dhcp-pool-1] gateway-list 192.168.1.1

[QX-dhcp-pool-1] quit

メモ：

端末が認証にパスしたり、認証に失敗したりした後、端末が IP アドレスを再取得するのに使う時間を短くさせるため、リース期間を短くすることを推奨します。しかしあるアプリケーションでは、端末はリース期間が終了する前に端末が新しい IP アドレスを要求することができます。

アドレス範囲、リース期間、ゲートウェイアドレスを含んだ IP アドレスプール 2 を設定します。

[QX] dhcp server ip-pool 2

[QX-dhcp-pool-2] network 2.2.2.0 mask 255.255.255.0

[QX-dhcp-pool-2] expired day 0 hour 0 minute 1

[QX-dhcp-pool-2] gateway-list 2.2.2.1

[QX-dhcp-pool-2] quit

アドレス範囲、リース期間、ゲートウェイアドレスを含んだ IP アドレスプール 3 を設定します。

[QX] dhcp server ip-pool 3

[QX-dhcp-pool-3] network 3.3.3.0 mask 255.255.255.0

[QX-dhcp-pool-3] expired day 0 hour 0 minute 1

[QX-dhcp-pool-3] gateway-list 3.3.3.1

[QX-dhcp-pool-3] quit

IP アドレスプール 4 を設定します。プリンタの MAC アドレス 0015-e9a6-7cfe をアドレスプールの IP アドレス 3.3.3111/24 に割り当てます。

[QX] dhcp server ip-pool 4

[QX-dhcp-pool-4] static-bind ip-address 3.3.3.111 mask 255.255.255.0

[QX-dhcp-pool-4] static-bind mac-address 0015-e9a6-7cfe

[QX-dhcp-pool-4] quit

2)　Web 認証の設定

SSL サーバポリシーsslsvr を作成し、PKI ドメイン pkidm を使用するように指定します。

[QX] ssl server-policy sslsvr

[QX-ssl-server-policy-sslsvr] pki pkidm

[QX-ssl-server-policy-sslsvr] quit

HTTPS をサポートするローカルポータルサーバを設定し、SSL サーバポリシーsslsvr を使用します。

[QX] portal local-server https server-policy sslsvr

インタフェース loopback12 に IP アドレス 4.4.4.4 を設定します。

[QX] interface loopback 12

[QX-LoopBack12] ip address 4.4.4.4 32

[QX-LoopBack12] quit

ローカルポータルサーバのリスニング IP アドレスを 4.4.4.4 に指定します。

[QX] portal local-server ip 4.4.4.4

GigabitEthernet 1/0/1 の Web 認証を有効化し、Auth-Fail VLAN として VLAN2 を指定します。VLAN2 は端末が認証に失敗した際に追加される VLAN です。

[QX] interface gigabitethernet 1/0/1

[QX–GigabitEthernet1/0/1] port link-type hybrid

[QX–GigabitEthernet1/0/1] mac-vlan enable

[QX–GigabitEthernet1/0/1] portal local-server enable

[QX–GigabitEthernet1/0/1] portal auth-fail vlan 2

[QX–GigabitEthernet1/0/1] quit

3) 802.1X 認証の設定

802.1X 認証をグローバルに設定します。

[QX] dot1x

GigabitEthernet 1/0/1 に 802.1X 認証(MAC ベースアクセスコントロールが必要です)を有効化し、Auth-Fail VLAN として VLAN2 を指定します。

[QX] interface gigabitethernet 1/0/1

[QX–GigabitEthernet1/0/1] dot1x port-method macbased

[QX–GigabitEthernet1/0/1] dot1x

[QX–GigabitEthernet1/0/1] dot1x auth-fail vlan 2

[QX–GigabitEthernet1/0/1] quit

4) MAC アドレス認証の設定

MAC アドレス認証をグローバルに設定します。

[QX] mac-authentication

GigabitEthernet 1/0/1 に MAC アドレス認証を有効化し、Auth-Fail VLAN として VLAN2 を指定します。

[QX] interface gigabitethernet 1/0/1

[QX–GigabitEthernet1/0/1] mac-authentication

[QX–GigabitEthernet1/0/1] mac-authentication guest-vlan 2

[QX–GigabitEthernet1/0/1] quit

5) RADIUS スキームの設定

RADIUS スキーム rs1 を作成します。

[QX] radius scheme rs1

プライマリ認証、アカウンティングサーバ、キーを指定します。

[QX-radius-rs1] primary authentication 1.1.1.2

[QX-radius-rs1] primary accounting 1.1.1.2

[QX-radius-rs1] key authentication radius

[QX-radius-rs1] key accounting radius

RADIUS サーバに送信されるユーザ名は、ドメイン名を保持しないことを指定します。

[QX-radius-rs1] user-name-format without-domain

[QX-radius-rs1] quit

6) ISP ドメインの設定

ISP ドメイン triple を作成します。

[QX] domain triple

ドメインで、ユーザのすべてのタイプ用にデフォルト AAA 方式を設定します。

[QX-isp-triple] authentication default radius-scheme rs1

[QX-isp-triple] authorization default radius-scheme rs1

[QX-isp-triple] accounting default radius-scheme rs1

[QX-isp-triple] quit

デフォルトドメインとしてドメイン triple を設定します。もしユーザ名に ISP ドメイン名が含まれていない場合、デフォルトドメインの認証方式が使われます。

[QX] domain default enable triple

III. 確認

ユーザ userdot は、認証を行うため、802.1X クライアントを使用しています。ユーザは、正しいユーザ名とパスワードを入力した後、802.1X 認証をパスすることができます。Web ユーザ userpt は、外部ネットワークにアクセスするため、Web ブラウザを使用します。Web リクエストは認証ページ https://4.4.4.4/portal/logon.htm にリダイレクトされます。

正しいユーザ名とパスワードを入力した後、Web ユーザは Web 認証をパスすることができます。プリンタはネットワークに接続した後、MAC アドレス認証をパスすることができます。

オンラインユーザの接続情報を見る場合、**display connection** コマンドを使用します。

[QX] display connection

```
Slot:  1
Index=30  , Username=userpt@triple
 IP=192.168.1.2
 IPv6=N/A
 MAC=0015-e9a6-7cfe
Index=31  , Username=userdot@triple
 IP=3.3.3.2
 IPv6=N/A
 MAC=0002-0002-0001
Index=32  , Username=001588f80dd7@triple
 IP=N/A
 IPv6=N/A
 MAC=0015-88f8-0dd7

 Total 3 connection(s) matched on slot 1.
 Total 3 connection(s) matched.
```

オンラインユーザの MAC VLAN エントリを見るために、**display mac-vlan all** コマンドを使用します。

VLAN3 は認可 VLAN です。

[QX] display mac-vlan all

```
  The following MAC VLAN addresses exist:
  S:Static  D:Dynamic
  MAC ADDR         MASK             VLAN ID   PRIO   STATE
  ------------------------------------------------------
  0015-e9a6-7cfe   ffff-ffff-ffff   3         0      D
  0002-0002-0001   ffff-ffff-ffff   3         0      D
  0015-88f8-0dd7   ffff-ffff-ffff   3         0      D
  Total MAC VLAN address count:3
```

オンラインユーザに割り当てられた IP アドレスを見るために、**display dhcp server ip-in-use** コマンドを使用します。

[QX] display dhcp server ip-in-use all

```
Pool utilization: 0.59%
 IP address       Client-identifier/    Lease expiration          Type
                  Hardware address
 3.3.3.111        0015-88f8-0dd7        Dec 15 2009 17:40:52      Auto:COMMITTED
 3.3.3.2          0002-0002-0001        Dec 15 2009 17:41:02      Auto:COMMITTED
 3.3.3.3           0015-e9a6-7cfe        Unlimited                 Manual

 --- total 3 entry ---
```

端末が認証に失敗したとき、VLAN2 に追加されます。display コマンドで端末の MAC VLAN エントリと IP アドレスを見ることができます。