NEC

GVT-018494-001-00 1.16

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

(V7)

改版履歴

版数	日付	改版内容
1.0	2016/10	初版発行
1.1	2017/05/18	・「本マニュアルについて」の「適用装置」に QX-S5500G シリーズ Ethernet スイッチを追加しました。 ・誤記訂正
1.2	2017/06/26	・「本マニュアルについて」の「適用装置」に QX-S4100G シリーズ Ethernet スイッチを追加しました。 ・誤記訂正
1.3	2017/10/06	・「本マニュアルについて」の「適用装置」に QX-S3400F シリーズ Ethernet スイッチを追加しました。 ・「2 章 PKI」の **display pki certificate** コマンドを 2 つのコマンドに分割しました。 ・「2 章 PKI」の **pki delete-certificate** コマンドの Syntax を変更しました。 ・「2 章 PKI」の **pki retrieval-certificate** コマンド名を **pki retrieve-certificate** に変更し、Syntax を変更しました。 ・「2 章 PKI」の **pki retrieval-crl domain** コマンド名を **pki retrieve-crl domain** に変更し、Syntax を変更しました。 ・「2 章 PKI」の **pki validate-certificate** コマンドの Syntax を変更しました。 ・「4 章 トリプル認証」にトリプル認証を使用する際のメモを追加しました。 ・誤記訂正
1.4	2018/06/07	・誤記訂正 （「2 章 PKI」の PKI ドメインの設定手順修正、PKI 証明書の確認の設定修正、証明書の削除コマンドの修正）
1.5	2018/10/15	・「本マニュアルについて」の「適用装置」に QX-S5300G シリーズ、Ethernet スイッチを追加しました。
1.6	2018/10/25	・「本マニュアルについて」の「適用装置」に QX-S5600G シリーズ Ethernet スイッチを追加しました。
1.7	2018/11/09	・「3 章 SSL」に「SSL ネゴシエーション実行中における SSL サーバの完全な証明書チェーンのクライアントへの送信」を追加しました。
1.8	2018/11/22	・「3 章 SSL」に QX-S3400F シリーズのサポートを追加しました。 ・誤記訂正

1.9	2019/02/15	・QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I、QX-S4508GT-4G-I をサポートしました。「本マニュアルについて」の「適用装置」に記載を追加しました（QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I は QX-S4100G シリーズに含みます）。 ・「関連マニュアル」に QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチの記載を追加しました。 ・「関連マニュアル」から QX-S3400F シリーズ、QX-S4100G シリーズの記載を削除しました。 ・「2 章 PKI」のメモ誤記訂正（QX-S3400F シリーズの削除） ・**certificate-chain-sending enable** コマンドの QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I、QX-S4508GT-4G-I のサポートバージョンを追加しました。
1.10	2020/02/04	・QX-S5824XP-2Q2C をサポートしました。
1.11	2020/09/01	・QX-S4300X シリーズをサポートしました。 ・「1 章 Web 認証」に「1.4 認証ページのカスタマイズ」を追加しました。 ・誤記訂正
1.12	2021/03/16	・QX-S5100G シリーズをサポートしました。 ・誤記訂正
1.13	2021/07/02	・QX-S4800X シリーズをサポートしました。
1.14	2022/05	・「1 章 WebAuth」に「Web 認証用の一時タイマアドレスエントリ用のエージング MAC の設定」を追加しました。
1.15	2025/04	・QX-S4200G シリーズをサポートしました。
1.16	2026/11	・QX-S4800X シリーズを適用装置と関連マニュアルに記載しました。 ・certificate-chain-sending enable コマンドのメモに QX-S5500G を追記しました。

Copyright © NEC Corporation 2016-2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

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

- 本装置は *QX シリーズ Ethernet スイッチ Web 認証コマンドマニュアル*に記載されている機能の操作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機能の操作に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。

マニュアル	内容
QX-S3400F シリーズ Ethernet スイッチ	Version 7.2.X を含む以降のソフトウェア
QX-S4100G シリーズ Ethernet スイッチ	Version 7.2.X を含む以降のソフトウェア (QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I は Version7.2.30 を含む以降のソフトウェア)
QX-S4200G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S4300X シリーズ Ethernet スイッチ	Version 7.1.6 を含む以降のソフトウェア
QX-S4508GT-4G-I Ethernet スイッチ	Version 7.2.30 を含む以降のソフトウェア
QX-S4800X シリーズ Ethernet スイッチ	Version 7.3.X を含む以降のソフトウェア
QX-S5100G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S5200G シリーズ Ethernet スイッチ	Version 7.1.12 を含む以降のソフトウェア
QX-S5300G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S5500G シリーズ Ethernet スイッチ	Version 7.2.11 を含む以降のソフトウェア
QX-S5600G シリーズ Ethernet スイッチ	Version 7.1.X を含む以降のソフトウェア
QX-S5800X シリーズ Ethernet スイッチ	Version 7.2.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説明しています。
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について説明しています。
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。

マニュアル	内容
QX-S3400F/S4100G/S4500G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S3400F/S4100G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S4200G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S4200G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S4200G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S4200G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S4300X シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S4300X シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S4300X シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S4800X シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S4800X シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S4800X シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5100G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5100G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S5200G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5200G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5200G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5200G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。

マニュアル	内容
QX-S5300G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5300G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5300G シリーズ Series Ethernet Switches Command References	機能に関するコマンドについて説明しています。
QX-S5300G シリーズ Ethernet スイッチ Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-S5500G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5500G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5500G シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。
QX-S5600G シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5600G シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5600G シリーズ Series Ethernet Switches Command References	機能に関するコマンドについて説明しています。
QX-S5800X シリーズ Ethernet スイッチ インスタレーションマニュアル	システムのインストールについて説明しています。
QX-S5800X シリーズ Ethernet スイッチ オペレーションマニュアル	機能の設定について説明しています。
QX-S5800X シリーズ Ethernet スイッチ コマンドマニュアル	機能に関するコマンドについて説明しています。

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。

表記規則	説明
[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

表記規則	説明
⚠ **警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある情報を示します。
⚠ **注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある情報を示します。
⚠ **重要**	表示を無視したり指示に従わない場合、装置が正しく動作しない恐れのある情報を示します。
🕮 **メモ**	追加または補足となる情報を示します。
🕮 **ポイント**	参考となる情報を示します。

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セクションで構成されています。

01-WebAuth

02-PKI 設定

03-SSL 設定

04-トリプル認証

目次

1章 WebAuth 1-1
1.1 Web認証(WebAuth)の概要 1-1
1.2 Web認証機能のプロセス 1-1
1.2.1 許可VLAN 1-2
1.2.2 制限VLAN 1-2
1.2.3 許可ACL 1-2
1.3 Web認証サーバの設定 1-2
1.4 認証ページのカスタマイズ 1-3
1.5 Web認証の有効化 1-5
1.6 ユーザアクセス制御の設定 1-6
1.6.1 Web認証freeサブネットの設定 1-6
1.6.2 Web認証ドメインの設定 1-6
1.6.3 IPv4 Web認証ユーザの最大数の設定 1-6
1.6.4 オンラインWeb認証ユーザの検出の設定 1-7
1.6.5 Web認証用の一時タイマアドレスエントリ用のエージングMACの設定 1-7
1.7 制限VLANの設定 1-8
1.8 Web認証の表示と維持 1-8
1.9 Web認証の設定例 1-9
1.9.1 ネットワーク要件 1-9
1.9.2 設定手順 1-9
1.9.3 設定の確認 1-11

1章 WebAuth

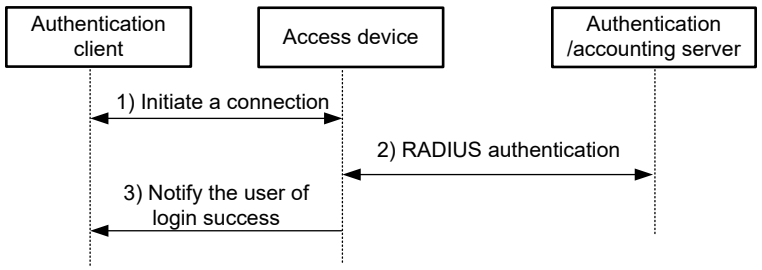
1.1 Web認証(WebAuth)の概要

Web 認証(WebAuth)機能はレイヤ 2 ポータル認証とも呼ばれます。MAC アドレスが認証にパスしたクライアントのみネットワークにアクセスできるように、アクセス装置でポータル認証を実行します。Web 認証はローカル認証です。Web 認証サーバが Web 認証サービスをユーザに提供させるため、アクセス装置がローカル Web 認証サーバとして動作します。

Web 認証は許可 VLAN、制限 VLAN 機能をサポートします。

1.2 Web認証機能のプロセス

図 1-1 Web 認証機能のプロセス



以下に Web 認証のプロセスを示します。

1) 認証クライアントが HTTP 要求を初期化します。
2) HTTP 要求を受信すると、アクセス装置はローカル Web 認証サーバの IP アドレスに要求をリダイレクトします。ローカル Web 認証サーバは認証クライアントに Web 認証ページを送信します。ユーザは Web 認証ページでユーザ名、パスワードを入力します。

   Web 認証サーバの IP アドレスは Web 認証サーバと通信可能なアクセス装置のレイヤ 3 インタフェースの IP アドレスです。通常ループバックインタフェースの IP アドレスです。
3) アクセス装置と RADIUS サーバはユーザを認証するため RADIUS パケットの交換を行います。
4) ユーザが RADIUS 認証にパスした場合、ローカル Web 認証サーバは認証クライアントにログイン成功画面を表示します。

1.2.1 許可 VLAN

Web 認証は、ユーザがネットワークリソースにアクセスすることを制御するため、認証サーバによって許可された VLAN を使用します。認証にパスしたのち、ユーザは許可 VLAN に割り当てられ、VLAN のリソースにアクセスすることができます。

1.2.2 制限 VLAN

制限 VLAN（Auth-Fail VLAN）は認証に失敗したユーザに割り当てられた VLAN です。制限 VLAN は、アンチウィルスソフトウェアやシステムパッチをダウンロードするためにソフトウェアサーバなどの制限されたネットワークリソースを提供します。ユーザはクライアントソフトウェアやほかのプログラムをアップグレードするため、これらのネットワークリソースを使用することができます。

1.2.3 許可 ACL

Web 認証は、ユーザがネットワークリソースにアクセスし、アクセス権限を制限するため、認証サーバによって許可された ACL を使用します。ユーザが認証にパスした場合、認証サーバはユーザのアクセスインタフェースに許可 ACL を割り当てます。アクセス装置は許可 ACL に従ってアクセスインタフェースのユーザからトラフィックをフィルタします。

ユーザのアクセス制御条件を変更する場合、認証サーバで異なる許可 ACL を指定する、あるいはアクセス装置の許可 ACL のルールを変更することができます。

1.3 Web認証サーバの設定

I. 制限とガイドライン

Web 認証サーバを設定するとき、以下の制限とガイドラインに従ってください。

- 使用中の Web 認証サーバを削除することはできません。削除した場合、オンラインユーザは正常にログアウトすることができません。
- リダイレクトを行う URL の先頭は“http://”あるいは“https://”にする必要があります。URL で“http://”あるいは“https://”を指定しない場合、システムは文字列の先頭が“http://”であると認識します。
- Web 認証サーバの IP アドレス、ポート番号はリダイレクトを行う URL で使用する IP アドレスとポート番号と同一にする必要があります。また Web 認証サーバのポート番号はローカルポータル Web サーバで使用するポート番号と同一にする必要があります。
- Web 認証サーバのリダイレクトを行う URL を複数回設定した場合、最後に入力した設定が適用されます。
- Web 認証サーバの IP アドレス、ポート番号を複数回設定した場合、最後に入力した設定が適用されます。

II. Web サーバの設定

以下に Web サーバの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Web サーバを作成し、その view に移行する	**web-auth server** *server-name*	デフォルト：設定なし
3. Web 認証サーバのリダイレクトを行う URL を設定する	**url** *url-string*	デフォルト：設定なし
4. Web 認証サーバの IP アドレス、ポート番号を設定する	**ip** *ipv4-address* **port** *port-number*	デフォルト：設定なし

1.4 認証ページのカスタマイズ

認証ページは HTML ファイルです。ローカル Web 認証には、次のメイン認証ページが必要です。

- 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

認証ページが使用するページ要素を含めて、認証ページをカスタマイズする必要があります。たとえば、back.jpg は認証ページ Logon.htm に使用します。

認証ページファイルを編集するときは、認証ページのカスタマイズ規則に従ってください。

I. ファイル名の規則

メイン認証ページファイルは表 1-1に示す名前に定義されています。メイン認証ページファイル以外の名前を定義できます。ファイル名とディレクトリ名では、大文字と小文字は区別されません

表 1-1 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
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

II. ページリクエストのルール

ローカル Web 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 1 つの logon.cgi 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 Web 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;"
onclick="form.action=form.action+location.search;">
</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は標準 zip ファイルに圧縮します。

- 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ます。
- 認証ページは、zip ファイルのルートディレクトリに格納します。
- zip ファイルは FTP や TFTP で装置に転送でき、装置のルートディレクトリに保存します。

以下に装置の 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. 認証されたユーザの指定 Web ページへのリダイレクト

認証にパスしたユーザを指定する Web ページに自動的にリダイレクトするため、logon.htm と logonSuccess.htm に以下の設定を行います。

1) logon.htm で、Form の target 属性を_blank に設定します。

```
<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関数を追加します。

```
<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>
```

1.5 Web認証の有効化

Web 認証を適用するため、レイヤ 2 Ethernet インタフェースで Web 認証を有効にする必要があります。

Web 認証を有効にする場合、既存の Web 認証サーバを指定する必要があります。存在しない Web 認証サーバを指定した場合、以下のことが発生します。

- Web 認証が適用しません。
- すべてのオンラインユーザが強制的にログアウトします。
- すべての新規ユーザがログインできません。

以下に Web 認証を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3. Web 認証を有効にする	**web-auth enable apply server** *server-name*	デフォルト：無効

1.6 ユーザアクセス制御の設定

1.6.1 Web 認証 free サブネットの設定

ユーザが認証を行うことなく自由にネットワークリソースにアクセスできるように Web 認証 free サブネットを設定することができます。

Web 認証 free サブネットの設定を複数回実行することで、複数の Web 認証 free サブネットを設定することができます。

以下に Web 認証-free サブネットの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Web 認証 free サブネットを設定する	**web-auth free-ip** *ip-address* { *mask-length* | *mask* }	デフォルト：設定なし

1.6.2 Web 認証ドメインの設定

インタフェースで Web 認証ドメインを指定したのち、インタフェースに接続されたすべてのユーザは認証ドメインを使用します。

Web 認証ドメインを指定する場合、以下の制限とガイドラインに従ってください。

- 1 つの Web 認証ドメインのみ指定することができます。複数の Web 認証ドメインを指定した場合、最後に入力した設定が適用されます。
- 実際に Web 認証ドメインとして既存の ISP ドメインを指定してください。そうでない場合 Web 認証ドメインは適用されません。

以下に Web 認証ドメインの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
3. Web 認証ドメインを設定する	**web-auth domain** *domain-name*	デフォルト：設定なし

1.6.3 IPv4 Web 認証ユーザの最大数の設定

インタフェースで IPv4 Web 認証ユーザの最大数を管理することができます。

以下に IPv4 Web 認証ユーザの最大数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
3． IPv4 Web 認証ユーザの最大数を設定する	**web-auth max-user** *max-number*	デフォルト：1024

🕮 **メモ：**

- QX-S3400F シリーズ/S4100G シリーズ/S4200G シリーズ/S4508GT-4G-I/S5100G シリーズはポート当たり 512、装置当たり 512 まで認証動作が可能です。
- QX-S5200G シリーズはポート当たり 448、装置当たり 448 まで認証動作が可能です。
- QX-S5300G シリーズ/S5500G シリーズ/S5600G シリーズ/S4300X シリーズ/ S4800X シリーズ/S5800X シリーズはポート当たり 512、装置当たり 1024 まで認証動作が可能です。

1.6.4 オンライン Web 認証ユーザの検出の設定

この機能は、インタフェースのオンラインユーザの MAC アドレスエントリを定期的に検出します。ユーザの MAC アドレスエントリが更新されていない、あるいはエージアウトした場合、ユーザの検出に失敗します。ユーザが 2 回連続で検出に失敗した場合、装置は強制的にユーザをログオフします。

以下にオンライン Web 認証ユーザの検出の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Ethernet interface view に移行する	**interface** *interface-type interface-number*	—
3． オンライン Web 認証ユーザの検出を有効にし、検出間隔を設定する	**web-auth offline-detect interval** *interval*	デフォルト：無効

1.6.5 Web 認証用の一時タイマアドレスエントリ用のエージング MAC の設定

🕮 **メモ：**

- Web 認証用の一時タイマアドレスエントリ用のエージング MAC の設定は、QX-S5100G の Version 7.1.8 を含むそれ以降のバージョンでサポートしています。

概要

Web 認証を有効にした場合、スイッチはユーザからトラフィックを検出すると、一時的なエントリアドレスを生成します。エントリは、ユーザのアドレス、アクセスインタフェース、VLAN ID、およびエントリのエージングタイムを記録します。

タイマは次のように機能します。

- エージングタイマの期限が切れたときにユーザが認証を開始しない場合、デバイスは一時エントリを削除します。

- エージングタイマが期限切れになる前にユーザが認証をパスした場合、デバイスはエージングタイマを削除し、Web 認証ユーザのオンライン情報を記録します。
- エージングタイマの期限が切れる前にユーザが認証に失敗し、Web 認証に制限 VLAN が指定されている場合、デバイスはユーザのアドレスを Auth-fail VLAN (認証失敗 VLAN) にバインドし、エージングタイマをリセットします。エージングタイマが期限切れになってもユーザが認証に失敗する場合、デバイスはユーザの一時エントリを削除します。

制約事項およびガイドライン

次の場合は、タイマ値を拡大することをお勧めします。

- アクセス権のない Web 認証ユーザは、短時間でトラフィックを送信することがよくあります。その結果、アクセスデバイスは Web 認証プロセスを継続的に開始し、スイッチの負荷が増加します。
- ユーザが認証に失敗すると、ユーザには制限 VLAN からリソースを取得するための十分な時間がありません。たとえば、ウイルスパッチをダウンロードできませんでした。

設定手順

操作	コマンド	補足
4. system view に移行する	**system-view**	ー
5. 一時アドレスエントリのエージングタイマを設定する	web-auth timer temp-entry-aging *aging-time-value*	デフォルト：60秒

1.7 制限VLANの設定

制限 VLAN を適用するため、インタフェースで MAC ベース VLAN 機能を有効にする必要があります。

以下に制限 VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. Ethernet interface view に移行する	**interface** *interface-type interface-number*	ー
3. 制限 VLAN を設定する	**web-auth auth-fail vlan** *authfail-vlan-id*	デフォルト：設定なし

1.8 Web認証の表示と維持

すべての view で display コマンドを実行できます。

操作	コマンド
Web認証の設定を表示する	**display web-auth** [**interface** *interface-type interface-name*]
Web認証-freeサブネットを表示する	**display web-auth free-ip**
Web認証サーバの情報を表示する	**display web-auth server** [*server-name*]

操作	コマンド
Web認証ユーザの情報とユーザの総数を表示する	**display web-auth user** [**interface** *interface-type interface-name* | **slot** *slot-number*]

1.9 Web認証の設定例

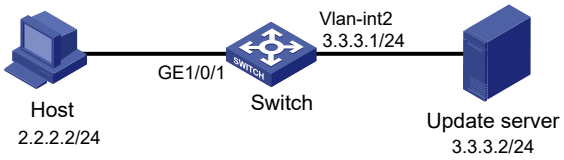
1.9.1 ネットワーク要件

図 1-2に示すように、ホストは装置（アクセス装置）に直接接続されています。

以下の要件を適用するため装置でローカル Web 認証を設定します。

- すべてのユーザは ISP ドメイン bbb に所属しています。
- すべてのユーザはデフォルトで VLAN1 に所属しています。Web 認証の認証に失敗したユーザは VLAN に割り当てられます。
- HTTP でクライアントと認証情報を交換するため、ローカル Web 認証サーバを設定します。
- ホストと通信ができるアクセス装置のレイヤ 3 インタフェースの IP アドレスとしてローカル Web 認証サーバの IP アドレスを設定します。

図 1-2 ネットワーク図



1.9.2 設定手順

1)　ネットワークアクセスユーザを設定します。

ローカルネットワークアクセスユーザ 123 を作成します。

<Switch>system-view

[Switch] local-user 123 class network

ユーザのパスワード 123 を設定します。

[Switch-luser-network-123] password simple 123

LAN アクセスサービスを使用するユーザを許可します。

[Switch-luser-network-123] service-type lan-access

ユーザのユーザロールとして network-admin、network-operator を指定します。

[Switch-luser-network-123] authorization-attribute user-role network-admin

[Switch-luser-network-123] authorization-attribute user-role network-operator

[Switch-luser-network-123] quit

2) ローカルポータル Web サーバを設定します。

HTTP でクライアントと認証情報を交換するため、ローカルポートの Web サーバを設定します。

[Switch] portal local-web-server http

ローカルポータル認証としてデフォルトの認証ページファイル web.zip を指定します。

[Switch-portal-local-websvr-http] default-logon-page web.zip

[Switch-portal-local-websvr-http] quit

3) Web 認証サーバを設定します。

Web 認証サーバ wbs を作成します。

[Switch] web-auth server wbs

Web 認証サーバ wbs のリダイレクトを行う URL として http://20.20.0.1/portal/を指定します。

[Switch-Web 認証-server-wbs] url http://20.20.0.1/portal/

Web 認証サーバ wbs の IP アドレス 20.20.0.1、ポート番号 80 を指定します。

[Switch-web-auth-server-wbs] ip 20.20.0.1 port 80

[Switch-web-auth-server-wbs] quit

4) ISP ドメインを設定します。

ISP ドメイン bbb を作成します。

[Switch] domain bbb

LAN ユーザのローカル認証、許可、アカウンティングを実行する ISP ドメインを設定します。

[Switch-isp-bbb] authentication lan-access local

[Switch-isp-bbb] authorization lan-access local

[Switch-isp-bbb] accounting lan-access local

[Switch-isp-bbb] quit

5) ループバック 0 の IP アドレスを割り当てます。IP アドレスは Web 認証サーバ wbs の IP アドレスと同一にする必要があります。

[Switch] interface loopback 0

[Switch-LoopBack0] ip address 20.20.0.1 255.255.0.0

[Switch-LoopBack0] quit

6) Web 認証を設定します。

GigabitEthernet 1/0/1 をハイブリッドポートとして設定し、タグなしメンバとして VLAN 1 を割り当てます。

[Switch] interface gigabitethernet 1/0/1

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

[Switch-GigabitEthernet1/0/1] port hybrid vlan 1 untagged

GigabitEthernet 1/0/1 で MAC ベース VLAN を有効にします。

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

GigabitEthernet 1/0/1 で Web 認証サーバ wbs を有効にします。

[Switch-GigabitEthernet1/0/1] web-auth enable apply server wbs

制限 VLAN として VLAN 2 を指定します。

[Switch-GigabitEthernet1/0/1] web-auth auth-fail vlan 2

[Switch-GigabitEthernet1/0/1] quit

Web 認証ドメインとして ISP ドメイン bbb を指定します。

[Switch-GigabitEthernet1/0/1] web-auth domain bbb

[Switch-GigabitEthernet1/0/1] quit

1.9.3 設定の確認

GigabitEthernet 1/0/1 で現在の設定を表示します。

[Switch-GigabitEthernet1/0/1] display this

```
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 untagged
mac-vlan enable
web-auth enable apply server wbs
web-auth auth-fail vlan 2
#
```

GigabitEthernet 1/0/1 の Web 認証ユーザの情報と Web 認証ユーザの総数を表示します。

[Switch-GigabitEthernet1/0/1] display web-auth user

```
User Name: 123
  MAC address: acf1-df6c-f9a
  IPv4 address: 2.2.2.2
  Access interface: GigabitEthernet1/0/1
  Initial VLAN: 1
  Authorization VLAN: N/A
  Authorization ACL ID: N/A
  Authorization user profile: N/A

Total 1 users matched.
```

目次

2 章 PKI 設定 2-1
2.1 概要 2-1
2.1.1 PKI 用語 2-1
2.1.2 PKI のアーキテクチャ 2-2
2.1.3 PKI のアプリケーション 2-3
2.1.4 PKI の動作 2-4
2.2 PKI 設定手順リスト 2-4
2.3 エンティティの DN の設定 2-4
2.4 PKI ドメインの設定 2-6
2.5 PKI 証明書リクエストの提出 2-8
2.5.1 証明書リクエストの提出 2-8
2.6 手動での証明書の取得 2-9
2.7 PKI 証明書の確認の設定 2-10
2.8 ローカル RSA 鍵ペアの廃棄 2-12
2.9 証明書の削除 2-12
2.10 PKI の表示 2-13
2.11 PKI 設定例 2-13
2.11.1 Windows2003 サーバで動作している CA から証明書の要求 2-13
2.12 PKI のトラブルシューティング 2-16
2.12.1 CA 証明書の取得に失敗 2-16
2.12.2 ローカル証明書のリクエストに失敗 2-17
2.12.3 CRL の取得に失敗 2-17

2章 PKI 設定

🕮 **メモ：**
PKI は QX-S5500G シリーズではサポートしていません。

2.1 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。

2.1.1 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。

2.1.2 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。

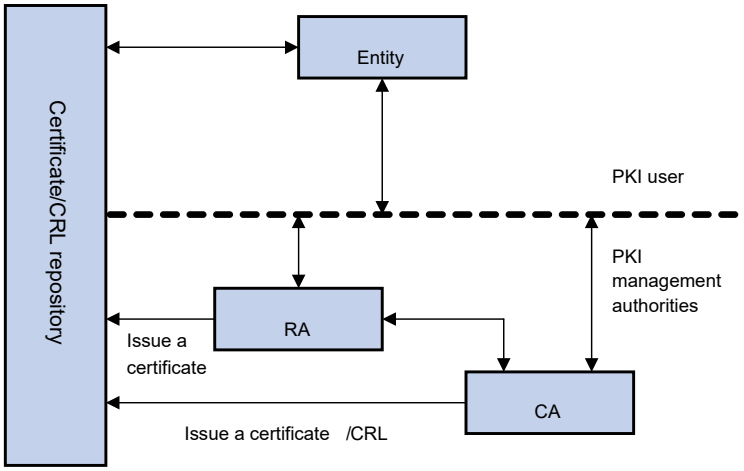


図2-1 PKI アーキテクチャ

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。

2.1.3 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。

2.1.4 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
1. system view へ移行する	**system-view**	—
2. エンティティを作成し、その view に移行する	**pki entity** *entity-name*	デフォルト：なし
3. （オプション設定項目）エンティティの共通名を設定する	**common-name** *name*	デフォルト：なし
4. （オプション設定項目）エンティティのカントリーコードを設定する	**country** *country-code-str*	デフォルト：なし
5. （オプション設定項目）エンティティの FQDN を設定する	**fqdn** *name-str*	デフォルト：なし
6. （オプション設定項目）エンティティの IP アドレスを設定する	**ip** *ip-address*	デフォルト：なし
7. （オプション設定項目）エンティティの所在地を設定する	**locality** *locality-name*	デフォルト：なし
8. （オプション設定項目）エンティティの組織を設定する	**organization** *org-name*	デフォルト：なし

操作	コマンド	補足
9.　（オプション設定項目）エンティティのユニット名を設定する	**organization-unit** *org-unit-name*	デフォルト：なし
10.　（オプション設定項目）エンティティの州あるいは県を設定する	**state** *state-name*	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－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－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－一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－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－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－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)－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
1. system view へ移行する	**system-view**	―
2. PKI ドメインを作成し、その view へ移行する	**pki domain** *domain-name*	デフォルト：なし
3. trusted CA を指定する	**ca identifier** *name*	デフォルト：なし
4. 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*	デフォルト：なし 指定されたエンティティは必要です。
5. 証明書リクエスト用の機関を指定する	**certificate request from** { **ca** | **ra** }	デフォルト：なし
6. 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*	デフォルト：なし
7. （オプション設定項目）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* }	デフォルト：ポーリングは20分の間隔で50回です。
8. 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。

操作	コマンド	補足
9. 証明書要求のためにキーペアを指定する	• RSAキーペア： **public-key rsa** { { **encryption name** *encryption-key-name* [**length** *key-length*] | **signature name** *signature-key-name* [**length** *key-length*] } * | **general name** *key-name* [**length** *key-length*] } • ECDSAキーペア： **public-key ecdsa name** *key-name* [**secp192r1 | secp256r1 | secp384r1 | secp521r1**] • DSAキーペア **public-key dsa name** *key-name* [**length** *key-length*]	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
1. system view へ移行する	**system-view**	―
2. PKI domain view へ移行する	**pki domain** *domain-name*	―
3. （オプション設定項目）証明書リクエストモードの手動設定を行う	**certificate request mode manual**	デフォルト：手動
4. system view へ戻る	**quit**	―
5. 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してください。	―
6. ローカル RSA 鍵ペアを作成する	**public-key local create rsa**	デフォルト：なし
7. 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*]]	―

🕮 **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
1. system view へ移行する		**system-view**	―
2. 手動証明書を取得する	オンライン	**pki retrieve-certificate domain** *domain-name* { **ca** | **local** }	どちらかのコマンドを使用します。
	オフライン	**pki import domain** *domain-name* { **der** { **ca** | **local** | **peer** } **filename** *filename* | **p12 local filename** *filename* | **pem** { **ca** | **local** | **peer** } [**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
1. system view へ移行する	**system-view**	―
2. PKI domain view へ移行する	**pki domain** *domain-name*	―
3. （オプション設定項目）CRL 発行ポイントの URL を指定する	**crl url** *url-string*	デフォルト：指定なし
4. （オプション設定項目）CRL チェックを有効にする	**crl check enable**	デフォルト：有効
5. system view へ戻る	**quit**	―
6. 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。	―
7. CRL を取得する	**pki retrieve-crl domain** *domain-name*	―
8. 証明書の有効性をチェックする	**pki validate-certificate domain** *domain-name* { **ca** | **local** }	―

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
1. system view へ移行する	**system-view**	―
2. PKI domain view へ移行する	**pki domain** *domain-name*	―
3. CRL チェックを無効にする	**undo crl check enable**	デフォルト：有効
4. system view へ戻る	**quit**	―
5. 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。	―
6. 証明書の有効性をチェックする	**pki validate-certificate domain** *domain-name* { **ca** | **local** }	―

🕮 **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
1. system view への移行する	**system-view**	—
2. ローカル RSA 鍵ペアを廃棄する	**public-key local destroy rsa**	—

🕮 **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
1. system view へ移行する	**system-view**	—
2. 証明書を削除する	**pki delete-certificatedomain** *domain-name* { **ca** | **local** }	—

🕮 **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を表示する	**display pki certificate domain** *domain-name* { **ca** | **local** }	すべてのviewで実行可能です。
証明書リクエストステータスを表示する	**display pki certificate request-status**	すべてのviewで実行可能です。
CRLを表示する	**display pki crl domain** *domain-name*	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。

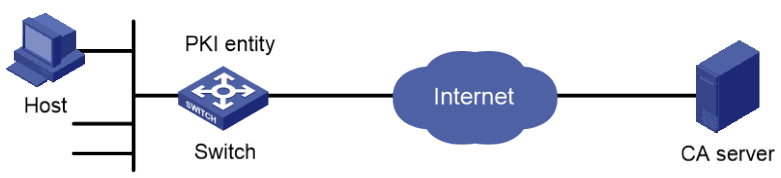


図2-2 Windows 2003 サーバで動作している CA から証明書のリクエスト

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。

<Switch> system-view

[Switch] pki entity aaa

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

[Switch-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。

[Switch] pki domain torsa

trusted CA 名 myca を設定します。

[Switch-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。

[Switch-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。

[Switch-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。

[Switch-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。

[Switch] 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。

[Switch] pki retrieve-certificate domain torsa ca

```
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。

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

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

[Switch]

```
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。

[Switch] display pki certificate domain torsa local

```
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 domain ca** 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
3.1 SSL概要 3-1
3.1.1 SSLセキュリティメカニズム 3-1
3.1.2 SSLプロトコルスタック 3-2
3.2 SSL設定手順リスト 3-2
3.3 SSLサーバポリシーの設定 3-3
3.3.1 設定必要条件 3-3
3.3.2 設定手順 3-3
3.4 SSL3.0の無効化 3-4
3.5 SSLネゴシエーション実行中におけるSSLサーバの完全な証明書チェーンのクライアントへの送信 3-4
3.6 SSLの表示 3-5

3章 SSL 設定

> 🕮 **メモ：**
> SSL は QX-S5500G シリーズではサポートしていません。

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。そして対称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。

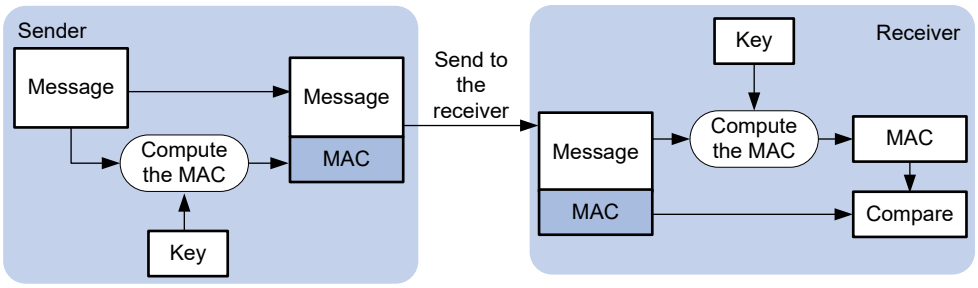


図3-1 MAC アルゴリズムによるメッセージの完全性の検証

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。

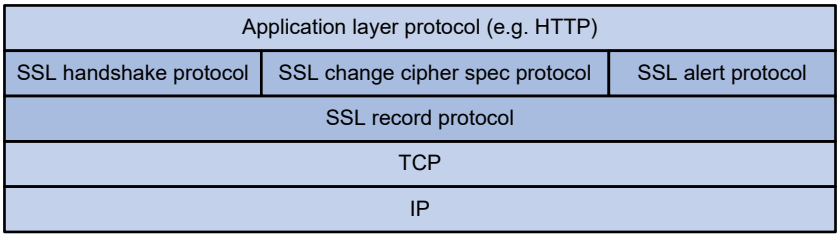


図3-2 SSL プロトコルスタック

- **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	必須設定項目

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
1. system view へ移行する	**system-view**	―
2. 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*	―
3. SSL サーバポリシー用の PKI ドメインを指定する	**pki-domain** *domain-name*	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

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
1. system view へ移行する	**system-view**	―
2. 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ネゴシエーション実行中におけるSSLサーバの完全な証明書チェーンのクライアントへの送信

クライアントがサーバ証明書を確認するための完全な証明書チェーンを持っていない場合、SSL セッションが正常に確立されるようにするためにこの機能を設定します。

以下に SSL ネゴシエーションの実行中に SSL サーバが完全な証明書チェーンをクライアントに送信することを有効にする手順を示します。

操作	コマンド	補足
1. system view へ移行する	**system-view**	―
2. 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*	―
3. SSL ネゴシエーションの実行中に SSL サーバが完全な証明書チェーンをクライアントに送信することを有効にする	**certificate-chain-sending enable**	デフォルト：SSLネゴシエーションの実行中、SSLサーバは、完全な証明書チェーンではなくサーバ証明書をクライアントに送信します

🕮 **メモ：**

- QX-S3400F シリーズ、QX-S4100G シリーズでは Version 7.2.26 を含む以降のソフトウェアからサポートしています（QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I を除く）。
- QX-S4108GT-2G-I、QX-S4108GT-2G-PW-I、QX-S4508GT-4G-I では Version 7.2.30 を含む以降のソフトウェアからサポートしています。
- QX-S5200G シリーズ、QX-S5300G シリーズ、QX-S5500G シリーズ、QX-S5600G シリーズでは **certificate-chain-sending enable** コマンドをサポートしていません。

3.6 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
4.1 トリプル認証の概要.....4-1
4.1.1 概要.....4-1
4.1.2 トリプル認証メカニズム.....4-2
4.1.3 拡張機能.....4-2
4.2 トリプル認証設定手順.....4-3
4.3 トリプル認証設定例.....4-3
4.3.1 トリプル認証基本機能設定例.....4-3

4章　トリプル認証

🕮 メモ：

- QX-S5500G シリーズのトリプル認証は Version 7.2.11 を含む以降のソフトウェアからサポートしています。
- QX-S5800X シリーズはトリプル認証をサポートしていません。
- QX-S4300X シリーズはトリプル認証をサポートしていません。
- QX-S4800X シリーズはトリプル認証をサポートしていません。

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。

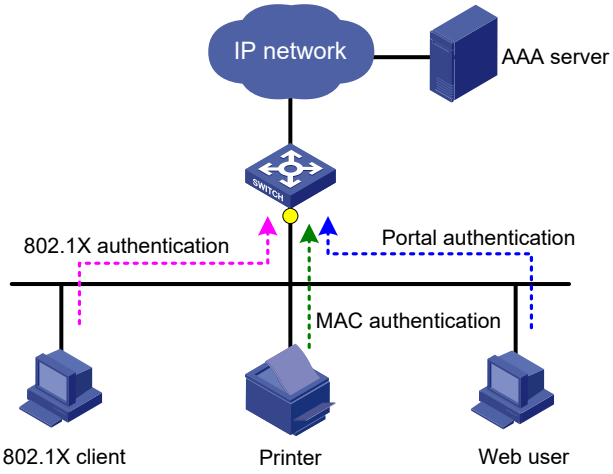


図4-1　トリプル認証ネットワーク図

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

3つの認証機能ではトリガーとなるパケットが異なります。また、接続する端末によって、実行される認証機能が異なります。

I. トリガーパケット

- 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。

II. 複数の認証実行時の動作

- 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。
- 802.1X 認証あるいは Web 認証にパスした場合、認証処理は終了して他の認証タイプは実行されません。
- MAC アドレス認証にパスした場合、Web 認証は実行されませんが、802.1X 認証のトリガーとなるパケットを受信すると 802.1X 認証が実行されます。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	

🕮 **メモ：**

QX-S3400F シリーズと QX-S4100G シリーズでトリプル認証を使用する場合は、認証ポートに **mac-authentication parallel-with-dot1x** コマンドを設定してください。

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。

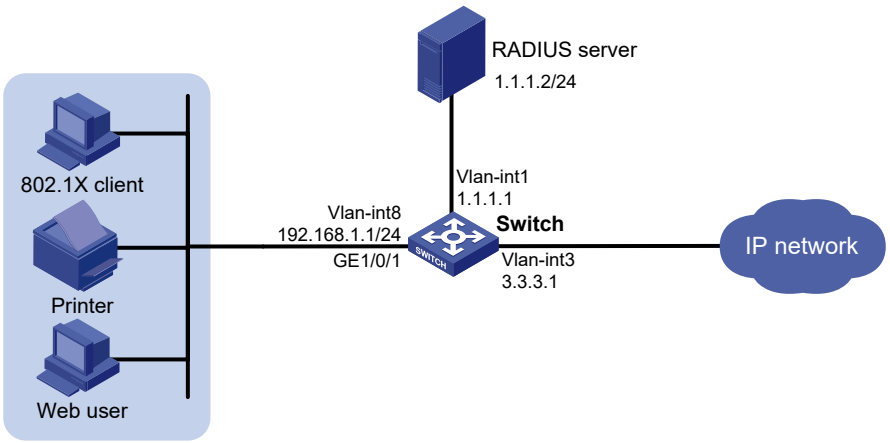


図4-2 トリプル認証基本機能設定例

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。

<Switch> system-view

[Switch] 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。

[Switch] interface loopback 12

[Switch-LoopBack12] ip address 4.4.4.4 32

[Switch-LoopBack12] quit

[Switch] portal local-web-server http

ローカルポータル認証としてデフォルトの認証ページファイル web.zip を指定します。

[Switch-portal-local-websvr-http] default-logon-page web.zip

[Switch-portal-local-websvr-http] quit

WebAuth サーバ wbs を作成します。

[Switch] web-auth server wbs

WebAuth サーバ wbs のリダイレクトを行う URL として http://20.20.0.1/portal/を指定します。

[Switch-web-auth-server-wbs] url http://20.20.0.1/portal/

WebAuth サーバ wbs の IP アドレス 20.20.0.1、ポート番号 80 を指定します。

[Switch-web-auth-server-wbs] ip 20.20.0.1 port 80

[Switch-web-auth-server-wbs] quit

GigabitEthernet 1/0/1 で WebAuth サーバ wbs を有効にします。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] web-auth enable apply server wbs

[Switch-GigabitEthernet1/0/1] quit

WebAuth ドメインとして ISP ドメイン bbb を指定します。

[Switch-GigabitEthernet1/0/1] web-auth domain triple

[Switch-GigabitEthernet1/0/1] quit

2)　802.1X 認証の設定

802.1X 認証のグローバル設定

[Switch] 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。

[Switch] interface gigabitethernet 1/0/1

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

[Switch–GigabitEthernet1/0/1] dot1x

[Switch–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

[Switch] mac-authentication

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

[Switch] interface gigabitethernet 1/0/1

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

[Switch–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。

[Switch] 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。

[Switch-radius-rs1] primary authentication 1.1.1.2

[Switch-radius-rs1] primary accounting 1.1.1.2

[Switch-radius-rs1] key authentication radius

[Switch-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。

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

[Switch-radius-rs1] quit

5)　ドメインの設定

ISP ドメイン triple を作成します。

[Switch] 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。

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

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

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

[Switch-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。

[Switch] 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。