NEC

GVT-187323-001-00 1.7

QX-W シリーズ

Web 認証(ポータル認証)

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	2021/11	初版発行
1.1	2022/03	・「1 章 Web 認証(ポータル認証)」に、” 1.8.1 ポータルフリールールの設定”を追加しました。 ・「1 章 Web 認証(ポータル認証)」に、”1.11.2 ローカルポータル Web サーバ＋ローカル認証の設定例” を追加しました。 誤記修正
1.2	2022/09	・「1 章 Web 認証(ポータル認証)」の、「1.4 ポータル Web サーバの設定”に、url-parameter の設定を追加しました。 ・「1 章 Web 認証(ポータル認証)」の、「1.5 認証ページのカスタマイズ」の「 V. 認証されたユーザの指定 Web ページへのリダイレクト」の設定手順を修正しました。 ・「1 章 Web 認証(ポータル認証)」に、「1.6 ワイヤレスクライアントの有効性チェックの有効化」を追加しました。
1.3	2023/05	・「3 章 SSL」の TLS のサポートバージョンを修正しました。
1.4	2023/09	・対象バージョンに QX-W610 を追加しました。
1.5	2023/12	・対象バージョンに、QX-W1240、QX-W2120AC、QX-W2230AC を追加しました。 ・関連マニュアルに QX-W1240，QX-W2120AC、QX-W2230AC の情報を追加しました。 ・誤記訂正
1.6	2024/01	・「1 章 Web 認証(ポータル認証)」の「1.7 ローカルポータル Web サーバの設定」に、login success-url の設定と login failed-url を追加しました。
1.7	2024/02	・対象バージョンに、QX-W2330AC を追加しました。 ・「1.9.3 IPv4 ポータル認証ユーザの最大数の設定」のメモに QX-W2330AC を追加しました。

Copyright © NEC Corporation 2019 – 2024

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-W シリーズ Web 認証 (ポータル認証)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-W シリーズ Web 認証 (ポータル認証) 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

バージョン

本マニュアルに対応する製品バージョンは以下の通りです。

製品	バージョン
QX-W1000 シリーズ	Version 7.2.47 を含む以降
QX-W1100 シリーズ	Version 7.2.47 を含む以降
QX-W610	初版より
QX-W1240	初版より
QX-W2120AC	Version 7.2.47 を含む以降
QX-W2230AC	Version 7.2.47 を含む以降
QX-W2330AC	初版より

関連マニュアル

マニュアル	内容
QX-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント 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-W1000/W1100 シリーズアクセスポイント Anchor-AC オペレーションマニュアル	Anchor-AC として動作させる場合の機能設定について説明しています。
QX-W1000/W1100 シリーズアクセスポイント Anchor-AC コマンドマニュアル	Anchor-AC として動作させる場合の機能に関するコマンドについて説明しています。
QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC Web コンソール操作マニュアル	Anchor-AC として動作させる場合の 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-W610 シリーズアクセスポイント 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-W610 シリーズアクセスポイント 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-W610 シリーズアクセスポイント 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-W1240 アクセスポイント 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-W1240 アクセスポイント 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-W1240 アクセスポイント 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-W2120AC アクセスコントローラ 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-W2120AC アクセスコントローラ 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-W2120AC アクセスコントローラ 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-W2120AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W2230AC アクセスコントローラ 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-W シリーズ Web 認証 (ポータル認証) 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-W シリーズ Web 認証 (ポータル認証) 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。

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. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**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、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。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 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。例えば、<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。例えば、[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。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <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

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

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重要な情報を示します。
⚠ **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重要な情報を示します。
⚠ **重要**	注意を払う必要が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. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 3 個のセクションで構成されています。

01-Web 認証(ポータル認証)

02-PKI 設定

03-SSL 設定

目次

1章 Web認証(ポータル認証) 1-1
1.1 Web認証(ポータル認証)の概要 1-1
1.2 ポータル認証プロセス 1-1
1.3 ワイヤレスネットワークでのポータル認証設定 1-2
1.4 ポータルWebサーバの設定 1-2
1.5 認証ページのカスタマイズ 1-3
1.6 ワイヤレスクライアントの有効性チェックの有効化 1-5
1.7 ローカルポータルWebサーバの設定 1-6
1.8 ポータル認証の有効化 1-6
1.9 ユーザアクセス制御の設定 1-7
1.9.1 ポータルフリールールの設定 1-7
1.9.2 ポータル認証ドメインの設定 1-8
1.9.3 IPv4 ポータル認証ユーザの最大数の設定 1-9
1.10 HTTPSリダイレクトの設定 1-10
1.11 ポータル認証の表示と維持 1-10
1.12 ポータル認証の設定例 1-11
1.12.1 ローカルポータルWebサーバ＋RADIUSサーバの設定例 1-11
1.12.2 ローカルポータルWebサーバ＋ローカル認証の設定例 1-14

1章 Web 認証(ポータル認証)

1.1 Web認証(ポータル認証)の概要

ポータル認証は、ユーザのインターネットへのアクセスを制御します。ポータルは、ユーザがポータル認証ページに入力するユーザ名とパスワードによって、ユーザを認証します。したがって、ポータル認証は Web 認証とも呼ばれます。ポータル認証がネットワークに展開されると、アクセスデバイスは、認証されていないユーザをポータル Web サーバによって提供される Web サイトにリダイレクトします。ユーザは認証なしで Web サイト上のリソースにアクセスできます。ユーザがインターネットにアクセスするには、Web サイトでの認証をパスする必要があります。

1.2 ポータル認証プロセス

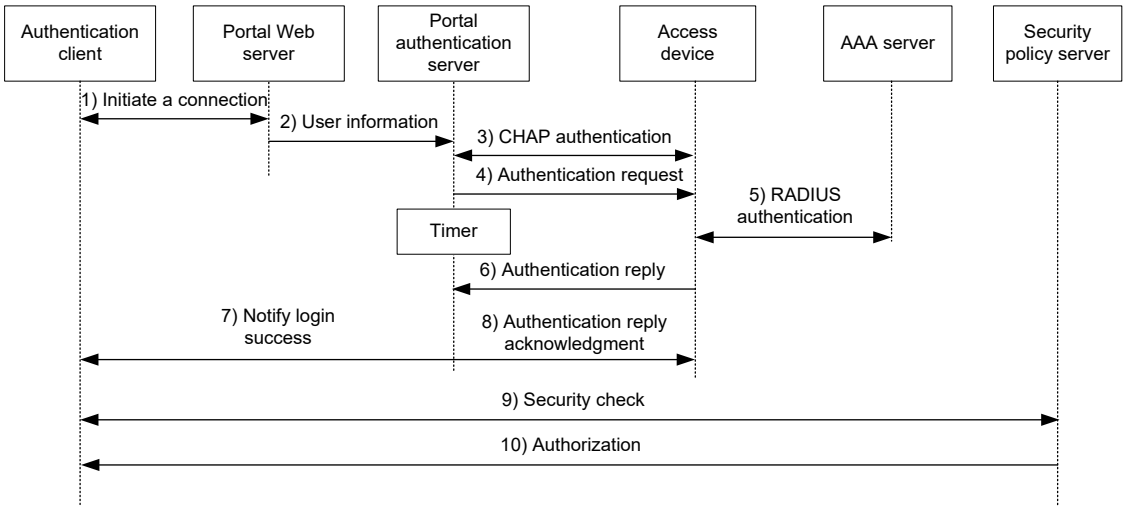

図 1-1 ポータル認証機能のプロセス

以下に、ポータル認証機能のプロセスを示します。

1) ポータルユーザは HTTP を介してインターネットにアクセスし、HTTP パケットがアクセスデバイスに到着します。
- パケットがポータルフリールールに一致する場合、アクセスデバイスはパケットの通過を許可します。
- パケットがポータルフリールールに一致しない場合、アクセスデバイスはパケットをポータル Web サーバにリダイレクトします。ポータル Web サーバは、ユーザ名とパスワードを入力するために Web 認証ページをユーザにプッシュします。

2) ポータル Web サーバは、ポータル認証サーバにユーザ認証情報をサブミットします。
3) ポータル認証サーバとアクセスデバイスは CHAP メッセージを交換します。PAP 認証の場合、この手順は省略されます。ポータル認証サーバは、使用する方式 (CHAP または PAP) を決定します。

4) ポータル認証サーバは、ユーザ名とパスワードを認証要求パケットに追加し、アクセスデバイスに送信します。一方、ポータル認証サーバは、認証応答パケットを待つためにタイマを起動します。
5) アクセスデバイスと RADIUS サーバは、RADIUS パケットを交換します。
6) アクセスデバイスは、認証の成功または失敗を通知するために、認証応答パケットをポータル認証サーバに送信します。
7) ポータル認証サーバは、認証の成功または失敗のパケットをクライアントに送信します。
8) 認証が成功すると、ポータル認証サーバは認証応答確認応答パケットをアクセスデバイスに送信します。
9) ユーザ認証プロセスが完了し、ポータルがオンラインになります。

1.3 ワイヤレスネットワークでのポータル認証設定

FIT AP+AC ネットワークのクライアントデータには、次の 2 つの転送モードがあります。

- 集中型転送:AP は CAPWAP トンネルを介してクライアントから AC にデータフレームを送信し、AC はすべてのデータフレームを転送します。
- ローカル転送:AP は、パケット転送のためにデータフレームを AC に送信するのではなく、クライアントからのデータフレームを直接転送します。

AC では、クライアントデータ転送モードに応じて、VLAN インタフェースまたはサービステンプレートにポータル認証を設定できます。

- VLAN インタフェースでのポータル認証は、集中型転送モードでのみ適用できます。AC は、VLAN ユーザから受信したインタフェースパケットだけを認証します。ローカル転送モードでは、AC はクライアントデータを受信できないため、クライアントのポータル認証を実行できません。

- サービステンプレートのポータル認証は、集中型転送モードとローカル転送モードの両方で適用できます。AC は、集中型転送モードではこの AC 上の BSS に、ローカル転送モードでは AP 上の BSS に、ポータルパケットフィルタリングルールを導入します。AC は、サービステンプレートにバインドされているすべての AP からユーザを認証できます。

クライアントのトラフィック転送の詳細については、QX-W シリーズ アクセスコントローラのオペレーションマニュアル *“WLAN アクセスの設定 － クライアントトラフィック転送モードの指定”* を参照してください。

1.4 ポータルWebサーバの設定

I. 制限とガイドライン

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**	－

操作	コマンド	補足
2. ポータル Web サーバを作成し、その view に移行する	**portal web-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. デバイスが URL をユーザーにリダイレクトするときに、URL で伝達されるパラメーターを設定する	**url-parameter** *param-name* **{ nas-id | nas-port-id | original-url | source-address | ssid | { ap-mac | source-mac } [encryption { aes | des } key { cipher | simple }** *string* **] | value** *expression* **| vlan }**	デフォルト：設定なし

1.5 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。ローカルポータル認証には、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のポータル 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;">
```

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 という名前で保存されています。
- 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、logonSuccess.htm に以下の設定を行います。

1) logonSuccess.htm に pt_init1()アトリビュートを読み込む関数を追加します。

```
<html filename=logonSuccess.htm>
<head>
<title>Logon success</title>
<meta http-equiv=Content-Type content="text/html; charset=GBK">
<link type="text/css" href="common.css" rel=stylesheet>
<meta name="viewport" content="width=device-width,initial-scale=1.0">
<script src="js/jquery.min.js" type="text/javascript"></script>
<script type="text/javascript" language="javascript"
src="logonSuccess.js"></script>
<script type="text/javascript" language="javascript"
src="pt_private.js"></script>
</head>
 <body class="bg" onload="pt_init1()">
```

2) ポータル Web サーバに、認証されたユーザのリダイレクト先 URL を設定します。

以下に、認証されたユーザのリダイレクト先 URL 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. ポータル Web サーバを作成し、その view に移行する	**portal web-server** *server-name*	デフォルト：設定なし
3. 認証されたユーザのリダイレクト先 URL を設定する	**url-parameter** *param-name* **value** *expression*	デフォルト：設定なし *param-name*のパラメータには"userurl"を指定します。 *expression*のパラメータには認証されたユーザのリダイレクト先URLを指定します。

1.6 ワイヤレスクライアントの有効性チェックの有効化

この機能は、サービステンプレートでポータル認証が有効になっている場合に有効にします。ローカル転送モードの AP で構成されたワイヤレスネットワークでは、AC にクライアントの ARP エントリはありません。したがって、AC は ARP エントリを使用してポータルクライアントの有効性をチェックできません。ユーザがポータル認証を実行できるようにするには、AC でワイヤレスクライアントの有効性チェックを有効にする必要があります。

この機能により、AC は WLAN スヌーピングテーブル、DHCP スヌーピングテーブル、および ARP テーブル内のクライアント情報を検索することで、クライアントを検証できます。クライアント情報が存在する場合、AC はそのクライアントのポータル認証が有効であると判断します。

以下に、ワイヤレスクライアントの有効性チェックの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． ワイヤレスクライアントの有効性チェックを設定する	**portal host-check enable**	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.47を含む以前のソフトウェアでは無効です。 ソフトウェアバージョン 7.2.49を含む以降のソフトウェアでは有効です。

1.7 ローカルポータルWebサーバの設定

I. 制限とガイドライン

ローカルポータル Web サーバで HTTPS を使用する場合は、以下のガイドラインに従ってください。

- PKI ポリシーの設定、CA 証明書の取得、およびローカル証明書の要求を行います。詳細は、 *"PKI 設定"* を参照してください。
- SSL サーバポリシーを設定認証し、PKI ポリシーで設定する PKI ドメインを指定します。詳細は、 *"SSL 設定"* を参照してください。

以下に、ローカルポータル 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． ポータル Web サーバを作成し、その view に移行する	**portal local-web-server { http | https ssl-server-policy** *policy-name***}**	デフォルト：設定なし
3． ローカルポータル Web サーバの既定の認証ページファイルを指定する	**default-logon-page** *file-name*	デフォルト：設定なし
4． ローカルポータル Web サーバのポート番号を設定する	**tcp-port** *port-number*	デフォルト： HTTP 80 HTTPS 443
5． 認証成功時のリダイレクト URL を設定する	**login success-url** *url-string*	デフォルト：設定なし
6． 認証失敗時のリダイレクト URL を設定する	**login failed-url** *url-string*	デフォルト：設定なし

1.8 ポータル認証の有効化

VLAN インタフェース上で指定されたポータル Web サーバを使用して、デバイスは VLAN インタフェース上のポータルユーザの HTTP または HTTPS 要求をポータル Web サーバにリダイレクトします。

サービステンプレートでポータル Web サーバが指定されている場合、デバイスは、サービステンプレートにバインドされている WLAN-BSS インタフェース上のポータルユーザの HTTP または HTTPS 要求をポータル Web サーバにリダイレクトします。

ポータル認証は、いずれも VLAN インタフェースまたはサービステンプレートで有効にできます。

I. VLAN インタフェースでのポータル認証設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	ー
3. ポータル Web サーバを設定する	**portal apply web-server** *server-name*	デフォルト：無効
4. ポータル認証を有効にする	**portal enable method direct**	デフォルト：無効

II. サービステンプレートでのポータル認証設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. service-template view に移行する	**wlan service-template** *service-template-name*	ー
3. ポータル Web サーバを設定する	**portal apply web-server** *server-name*	デフォルト：
4. ポータル認証を有効にする	**portal enable method direct**	デフォルト：無効

1.9 ユーザアクセス制御の設定

1.9.1 ポータルフリールールの設定

ポータルフリールールを使用すると、指定したユーザは、ポータル認証なしで指定した外部 Web サイトにアクセスできます。インタフェースフリールールの一致項目には、ホスト名、送信元/宛先 IP アドレス、TCP/UDP ポート番号、送信元 MAC アドレス、アクセス MAC、および VLAN が含まれます。ポータルフリー規則に一致するパケットはポータル認証をトリガーしないため、パケットを送信するユーザは指定された外部サイトに直接アクセスできます。

🕮 **メモ：**

認証前の無線端末は、ポータル Web サーバとだけ通信可能です。認証前の無線端末で DNS サーバ等と通信させる場合は、ポータルフリールールを設定してください。

ポータルフリールールを設定する場合は、次の制約事項および注意事項に従ってください。

- 同じフィルタリング基準で複数のポータルフリールールを設定することはできません。それ以外の場合は、ルールがすでに存在していることを示すプロンプトが表示されます。
- ポータル認証が有効になっているかどうかにかかわらず、ポータルフリールールは追加または削除のみ可能です。変更はできません。
- 送信元ベースのトラフィックフリールールが設定される前にポータルユーザがオンラインになった場合、デバイスはこれらの規則が一致していても、ポータル認証でのユーザのアカウンティングを継続します。

以下にポータルフリールールの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. ポータルフリールールを設定する。	**portal free-rule** *rule-number* **{ destination ip {** *ip-address* **{** *mask-length* **|** *mask* **}	any } [tcp** *tcp-port-number* **| udp** *udp-port-number* **]	source ip {** *ip-address* **{** *mask-length* **|** *mask* **}	any } [tcp** *tcp-port-number* **| udp** *udp-port-number* **] } * [interface** *interface-type interface-number* **]**	デフォルト：設定なし

1.9.2 ポータル認証ドメインの設定

インタフェース、または service-template でポータル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 つのポータル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。
- 実際にポータル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。そうでない場合ポータル認証ドメインは適用されません。

I. VLAN インタフェースでのポータル認証ドメイン指定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	ー
3. ポータル認証ドメインを設定する	**portal domain** *domain-name*	デフォルト：設定なし

II. サービステンプレートでのポータル認証ドメイン指定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー

操作	コマンド	補足
2． service-template view に移行する	**wlan service-template** *service-template-name*	―
3． ポータル認証ドメインを設定する	**portal domain** *domain-name*	デフォルト：設定なし

1.9.3 IPv4 ポータル認証ユーザの最大数の設定

システム内のポータルユーザの総数、および VLAN インタフェースまたはサービステンプレート上の IPv4 ポータルユーザの最大数を管理することができます。

ポータルユーザの最大数を設定する場合は、次の制約事項およびガイドラインに従ってください。

- ポータルユーザ最大数の設定を、デバイス上の現在のオンラインユーザ数合計より小さくしても、この設定は有効です。オンラインユーザは影響を受けませんが、システムは新しいポータルユーザのログインを禁止します。
- VLAN インタフェースまたはサービステンプレート上の現在の設定ユーザ数よりも小さい最大数を設定しても、ポータルは有効です。オンラインユーザは影響を受けませんが、システムは新しいインタフェースユーザがポータルまたはサービステンプレートからログインすることを禁止します。
- すべての VLAN インタフェースまたはサービステンプレートで指定されている IPv4 ポータルユーザの最大合計数が、システムで許可されている最大数を超えていないことを確認します。そうしないと、ポータルユーザの数を超えた場合にデバイスにログインできなくなります。
-

I. システム内のポータル認証ユーザの最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． システム内のポータル認証ユーザの最大数を設定する	**portal max-user** *max-number*	デフォルト：設定なし

II. VLAN インタフェース上の IPv4 ポータル認証ユーザ最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． VLAN interface view に移行する	**interface vlan-interface** *vlan-interface-id*	―
3． IPv4 ポータル認証ユーザ最大数を設定する	**portal ipv4-max-user** *max-number*	デフォルト：設定なし

III. サービステンプレート上の IPv4 ポータル認証ユーザ最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service-template view に移行する	**wlan service-template** *service-template-name*	―

操作	コマンド	補足
3. ポータル認証ドメインを設定する	**portal ipv4-max-user** *max-number*	デフォルト：設定なし

🕮 **メモ：**

- QX-W2120AC は、装置当たり 1024 まで認証動作が可能です。
- QX-W2230AC は、装置当たり 20480 まで認証動作が可能です。
- QX-W2330AC は、装置当たり 30720 まで認証動作が可能です。
- QX-W1000 シリーズ(FAT/ANCHOR-AC)は、装置当たり 512 まで認証動作が可能です。
- QX-W1100 シリーズ(ANCHOR-AC)は、装置辺り 2048 まで認証動作が可能です。
- QX-W1100 シリーズ(FAT)は、装置辺り 1200 まで認証動作が可能です。

1.10 HTTPSリダイレクトの設定

デバイスは、ポータル認証のために HTTPS 要求をポータル Web サーバにリダイレクトできます。SSL 接続の確立中に、ユーザブラウザが証明書によってサーバ ID を確認できないというメッセージを表示する場合があります。ユーザがこのようなメッセージをチェックせずにポータル認証を実行するには、SSL サーバポリシーを設定して、デバイスでクライアントが信頼する証明書を要求します。ポリシーの名前は https_redirect である必要があります。SSL サーバポリシー設定の詳細については、“*SSL 設定*“を参照してください。証明書リクエストの詳細は、”*PKI 設定*“を参照してください。

以下に、HTTPS リダイレク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**	ー
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*	HTTPSリダイレクトのSSLサーバポリシーの名前はhttps_redirectである必要があります。

1.11 ポータル認証の表示と維持

すべての view で display コマンドを実行できます。

操作	コマンド
ポータル認証の設定を表示する	**display portal { ap** *ap-name* **[radio** *radio-id* **] |** *interface interface-type interface-number* **}**
ポータルWeb認証サーバの情報を表示する	**display portal web-server** [*server-name*]
Web認証ユーザの情報とユーザの総数を表示する	**display portal user { all | ap** *ap-name* **[radio** *radio-id* **] | interface** *interface-type interface-number* **| ip ip-address | mac** *mac-address* **| username** *username* **} [brief | verbose]**

1.12　ポータル認証の設定例

1.12.1　ローカルポータル Web サーバ＋RADIUS サーバの設定例

I. ネットワーク要件

図 1-2に示すように、クライアントは AP を介して AC に接続されています。クライアントには、手動または DHCP によってパブリック IP アドレスが割り当てられます。AC は、ポータル認証サーバとポータルWebサーバの両方として機能します。RADIUSサーバは、認証/アカウンティングサーバとして機能します。

ユーザはポータル認証にパスするまで、ローカルのポータル Web サーバにしかアクセスできません。ポータル認証を通過すると、ユーザは他のネットワークリソースにアクセスできます。

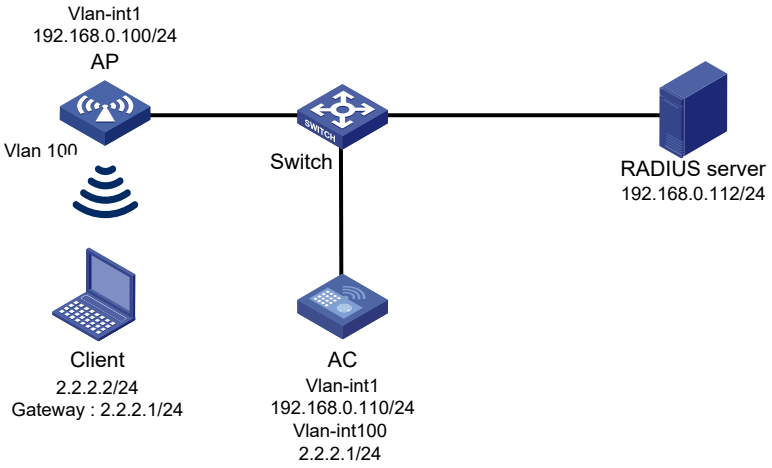

図 1-2 ネットワーク図

II. 設定手順

1)　RADIUS スキームの設定:

#RADIUS スキーム rs1 を作成します。

```
<AC> system-view
[AC] 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とキーを指定します。

```
[AC-radius-rs1] primary authentication 192.168.0.112
[AC-radius-rs1] primary accounting 192.168.0.112
[AC-radius-rs1] key authentication simple radius
[AC-radius-rs1] key accounting simple radius
```

#RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[AC-radius-rs1] user-name-format without-domain
[AC-radius-rs1] quit
```

#RADIUS セッションコントロールを有効にします。

```
[AC] radius session-control enable
```

2) ISP ドメインを設定します。

ISP ドメイン dm1 を作成します。

```
[AC] domain dm1
```

#ポータルユーザの認証､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。

```
[AC-isp-dm1] authentication portal radius-scheme rs1
[AC-isp-dm1] authorization portal radius-scheme rs1
[AC-isp-dm1] accounting portal radius-scheme rs1
[AC-isp-dm1] quit
```

3) ローカルポータル Web サーバを設定します。

#ローカルポータル Web サーバを作成します。HTTP を使用して、クライアントと認証情報を交換します。

```
[AC] 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 abc.zip を指定します。

```
[AC–portal-local-websvr-http] default-logon-page abc.zip
```

#ローカルポータル Web サーバの HTTP サービス受信ポート番号を 2331 に設定します。

```
[AC–portal-local-webserver-http] tcp-port 2331
[AC–portal-local-websvr-http] quit
```

#Web 認証サーバ newpt を作成します。

```
[AC] portal web-server newpt
```

#Web 認証サーバ newpt のリダイレクトを行う URL として http://2.2.2.1:2331/portal/を指定します。

```
[AC-portal-websvr-newpt] url http://2.2.2.1:2331/portal
[AC-portal-websvr-newpt] quit
```

#VLAN Interface 100 でポータル認証を有効にします。

```
[AC] interface vlan-interface 100
[AC–Vlan-interface100] portal enable method direct
```

#ポータル認証の ISP ドメインとして、ドメイン dm1 を設定します。

```
[AC–Vlan-interface100] portal domain dm 1
```

#VLAN Interface 100 でポータル Web サーバ newpt を有効にします。

```
[AC–Vlan-interface100] portal apply web-server newpt
```

```
[AC–Vlan-interface100] quit
```

#認証前端末が DNS サーバと通信することを許可します。

```
[AC] portal free-rule 0 source ip any destination ip any tcp 53
[AC] portal free-rule 1 source ip any destination ip any udp 53
```

III. 設定の確認

#VLAN Interface 100 でポータル認証が有効になっていることを確認します。

```
[AC] display portal interface vlan-interface 100
 Portal information of Vlan-interface 100
     VSRP instance: --
     VSRP state: N/A
     Authorization                   Strict checking
     ACL                             Disabled
     User profile                    Disabled
 IPv4:
     Portal status: Enabled
     Portal authentication method: Direct
     Portal Web server: newpt(active)
     Secondary portal Web server: Not configured
     Authentication domain: Not configured
     Pre-auth domain: Not configured
     User-dhcp-only: Disabled
     Pre-auth IP pool: Not configured
     Max portal users: Not configured
     Bas-ip: Not configured
     User Detection:  Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address               Mask
     Destination authenticate subnet:
         IP address               Mask
IPv6:
     Portal status: Disabled
     Portal authentication method: Disabled
     Portal Web server: Not configured
     Secondary portal Web server: Not configured
     Authentication domain: Not configured
     Pre-auth domain: Not configured
     User-dhcp-only: Disabled
     Pre-auth IP pool: Not configured
     Max portal users: Not configured
     Bas-ipv6: Not configured
     User detection: Not configured
     Action for server detection:
         Server type    Server name                          Action
         --             --                                   --
     Layer3 source network:
         IP address                                          Prefix length
     Destination authenticate subnet:
         IP address                                          Prefix length
```

#VLAN Interface 100 のポータル認証ユーザの情報とポータル認証ユーザの総数を表示します。

```
[AC] display portal user interface vlan-interface 100
Total portal users: 1
```

```
Username: abc
  Portal server: newpt
  State: Online
  VPN instance: --
  MAC                 IP                  VLAN    Interface
  0afb-42a6-7cfe      2.2.2.2             --      Vlan-interface100
  Authorization information:
    IP pool: N/A
    User profile: N/A
    ACL: N/A
```

1.12.2 ローカルポータル Web サーバ＋ローカル認証の設定例

I. ネットワーク要件

図 1-3に示すように、クライアントは AP を介してネットワークに接続されています。クライアントには､手動または DHCP によってパブリック IP アドレスが割り当てられます。AP は、ポータル認証サーバとポータル Web サーバの両方として機能します。Web 認証ユーザは AP のローカル認証で認証します。

Web 認証ページでユーザ名/パスワード入力することなく、ログインボタンを押すだけで Web 認証が行われるように、認証ページをカスタマイズします。

ユーザはポータル認証にパスするまで、ローカルのポータル Web サーバにしかアクセスできません。ポータル認証を通過すると、ユーザは他のネットワークリソースにアクセスできます。

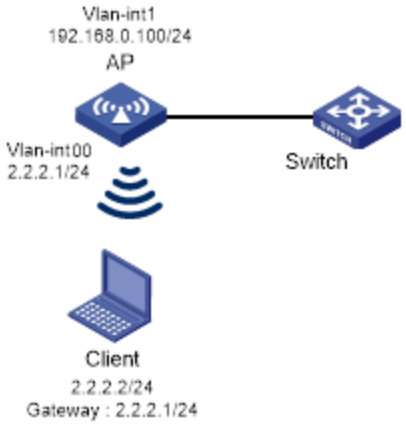

図 1-3 ネットワーク図

II. 設定手順

1) ユーザ名 web､プレーンテキストでパスワード 12345678 のローカルネットワークアクセスユーザを追加します。

```
[AP] local-user web class network
[AP-luser-network-web] password simple 12345678
```

#サービスタイプを portal に設定します。

```
 [AP-luser-network-web] service-type portal
```

2) ISP ドメインを設定します。

ISP ドメイン dm1 を作成します。

```
[AP] domain dm1
```

#ポータル認証で、ローカル認証、ローカル許可、ローカルアカウンティングを使用する ISP ドメインを設定します。

```
[AP-isp-dm1] authentication portal local
[AP-isp-dm1] authorization portal local
[AP-isp-dm1] accounting portal local
[AP-isp-dm1] quit
```

3) 認証ページをカスタマイズします。

#AP のルートディレクトリ上から、FTP/TFTP を使用して defaultfile.zip を取得します。

(詳細は省略します)

#defaultfile.zip を解凍します。(詳細は省略します)

#logon.htm を編集します。認証ユーザ名 **web**、認証パスワード **12345678** を埋め込みます。

```
<td class="input-group td2">
     <input type="text" id="PtUser" value="web" name="PtUser"/>
</td>
</tr>
<tr class="form-group">
   <td class="input-group td1" onclick="onPwClick()">
       <span class="text-title"><nobr>Password</nobr></span>
    </td>
    <td class="input-group td2">
        <input  type="password"  maxLength=320  id="PtPwd"  value="12345678"
name="PtPwd"/>
     </td>
```

#abc.zip というファイル名で圧縮します。(詳細は省略します)

#AP のルートディレクトリ上に FTP/TFTP を使用して abc.zip を保存します。(詳細は省略します)

4) ローカルポータル Web サーバを設定します。

#ローカルポータル Web サーバを作成します。HTTP を使用して、クライアントと認証情報を交換します。

```
[AP] 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 abc.zip を指定します。

```
[AP–portal-local-websvr-http] default-logon-page abc.zip
```

#ローカルポータル Web サーバの HTTP サービス受信ポート番号を 2331 に設定します。

```
[AP–portal-local-webserver-http] tcp-port 2331
[AP–portal-local-websvr-http] quit
```

#Web 認証サーバ newpt を作成します。

```
[AP] portal web-server newpt
```

#Web 認証サーバ newpt のリダイレクトを行う URL として http://2.2.2.1:2331/portal/を指定します。

```
[AP-portal-websvr-newpt] url http://2.2.2.1:2331/portal
[AP-portal-websvr-newpt] quit
```

5) サービステンプレート service1 を作成します。

```
[AP] wlan service-template service1
```

6) サービステンプレートの SSID サービスを指定します。

```
[AP-wlan-st-service1] ssid web_auth
```

7) ポータル認証の ISP ドメインとして、ドメイン dm1 を設定します。

```
[AP-wlan-st-service1] portal domain dm1
```

8) サービステンプレート service1 でポータル認証を有効にします。

```
[AP-wlan-st-service1] portal enable method direct
```

9) サービステンプレート service1 でポータル Web サーバ newpt を有効にします。

```
[AP-wlan-st-service1] portal apply web-server newpt
```

10) サービステンプレート service1 を有効化します。

```
[AP-wlan-st-service1] service-template enable
[AP-wlan-st-service1] quit
```

11) サービステンプレート service1 を AP の WLAN-Radio 1/0/1 に割り当てます。

```
[AP] interface WLAN-Radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service1
[AP-WLAN-Radio1/0/1] quit
```

#認証前端末が DNS サーバと通信することを許可します。

```
[AC] portal free-rule 0 source ip any destination ip any tcp 53
[AC] portal free-rule 1 source ip any destination ip any udp 53
```

III. 設定の確認

#SSID web-auth でポータル認証が有効になっていることを確認します。

```
[AC] display portal ap fatap radio 1
 Portal information of fatap
 Radio ID: 1
 SSID: web_auth
     Authorization : Strict checking
     ACL           : Disable
     User profile  : Disable
     Dual stack    : Disable
     Dual traffic-separate: Disabled
     Dual IP       : Disable
 IPv4:
     Portal status: Enabled
     Portal authentication method: Direct
     Portal Web server: newpt(active)
     Secondary portal Web server: Not configured
     Portal mac-trigger server: Not configured
     Authentication domain: dm1
     Extend-auth domain: Not configured
     User-dhcp-only: Disabled
```

```
    Max portal users: Not configured
    Bas-ip: Not configured
    Portal temp-pass: Disabled
    Portal authenticated-kick: Disabled
    Action for server detection:
        Server type    Server name                          Action
        --             --                                   --
    Destination authentication subnet:
        IP address              Mask
IPv6:
    Portal status: Disabled
    Portal authentication method: Disabled
    Portal Web server: Not configured
    Secondary portal Web server: Not configured
    Portal mac-trigger server: Not configured
    Authentication domain: Not configured
    Extend-auth domain: Not configured
    User-dhcp-only: Disabled
    Max portal users: Not configured
    Bas-ipv6: Not configured
    Portal temp-pass: Disabled
    Portal ipv6 authenticated-kick: Disabled
    Action for server detection:
        Server type    Server name                          Action
        --             --                                   --
    Destination authentication subnet:
        IP address                                          Prefix length
```

#SSID web_auth のポータル認証ユーザの情報とポータル認証ユーザの総数を表示します。

```
[AC] display portal user ap fatap radio 1
Total portal users: 1
Username: web
  AP name: fatap
  Radio ID: 1
  SSID: web_auth
  Portal server: N/A
  State: Online
  VPN instance: N/A
  MAC             IP                   VLAN    Interface
  0103-01af-8cc3  192.168.1.20        1       WLAN-BSS1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A
    Web URL: N/A
```

目次

2 章 PKI 設定 1
2.1 概要 1
2.1.1 PKI 用語 1
2.1.2 PKI のアーキテクチャ 2
2.1.3 PKI のアプリケーション 3
2.1.4 PKI の動作 3
2.2 PKI 設定手順リスト 4
2.3 エンティティの DN の設定 4
2.4 PKI ドメインの設定 5
2.5 PKI 証明書リクエストの提出 7
2.5.1 証明書リクエストの提出 8
2.6 手動での証明書の取得 9
2.7 PKI 証明書の確認の設定 9
2.8 ローカル RSA 鍵ペアの廃棄 11
2.9 証明書の削除 11
2.10 PKI の表示 12
2.11 PKI 設定例 12
2.11.1 Windows2003 サーバで動作している CA から証明書の要求 12
2.12 PKI のトラブルシューティング 16
2.12.1 CA 証明書の取得に失敗 16
2.12.2 ローカル証明書のリクエストに失敗 16
2.12.3 CRL の取得に失敗 17

2章 PKI 設定

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。

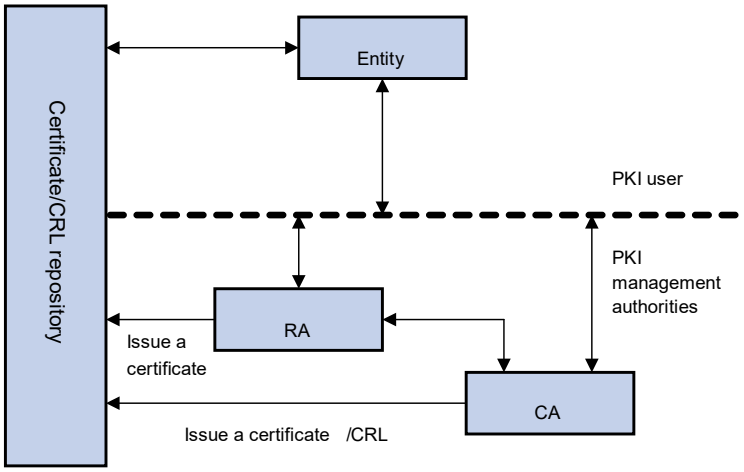

図 2-1 PKI アーキテクチャ

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. 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。

II. 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	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
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：**

- 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
1. system view へ移行する	**system-view**	ー
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。

操作	コマンド	補足
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。
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：**

- 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。

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**	ー
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。

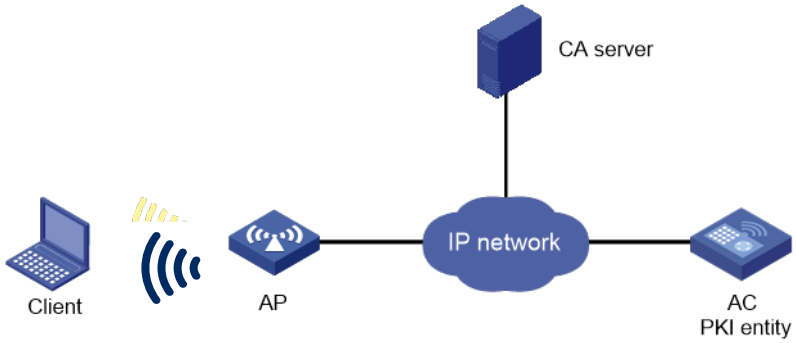

図 2-2 Windows 2003 サーバで動作している CA から証明書のリクエスト

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 AC と設定します。

<AC> system-view

[AC] pki entity aaa

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

[AC-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。

[AC] pki domain torsa

trusted CA 名 myca を設定します。

[AC-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。

[AC-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。

[AC-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。

[AC-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。

[AC] 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。

[AC] 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。

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

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

[AC]

```
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。

[AC] 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=AC
        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 3-2
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 3-3
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 3-4

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。

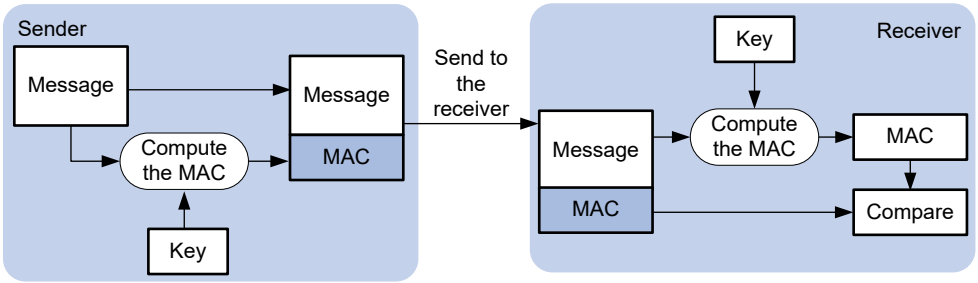

図 3-1 MAC アルゴリズムによるメッセージの完全性の検証

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。

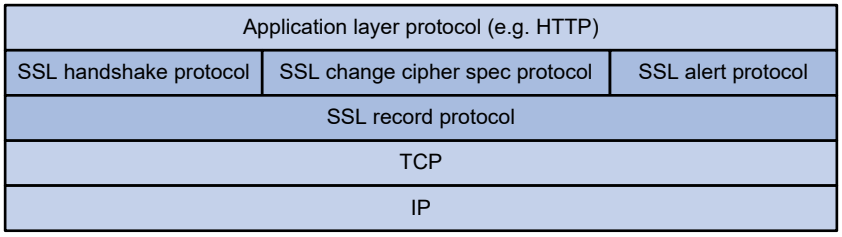

図 3-2 SSL プロトコルスタック

- **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、1.1、1.2 のバージョンを使用します。TLS1.0、1.1、1.2 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、1.1、1.2 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、1.1、1.2 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、1.1、1.2 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、1.1、1.2 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、1.1、1.2 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**	―

操作	コマンド	補足
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

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。