CHAPTER 2

HTTP over SSL（HTTPS）の使用方法

この章は、次の内容で構成されています。

HTTPS の概要

Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS; HTTP over SSL）は、ブラウザ クライアントと IIS サーバとの間の通信を保護し、証明書および公開キーを使用してインターネット経由で転送されるデータを暗号化します。また、HTTPS によってユーザのログイン パスワードも Web で安全に転送されるようになります。サーバの識別情報を保護する HTTPS をサポートする Cisco CallManager アプリケーションには、Cisco CallManager Administration、Cisco CallManager Serviceability、Cisco IP Phone User Option Pages、Bulk Administration Tool （BAT）、TAPS、Cisco CDR Analysis and Reporting （CAR）、Trace Collection Tool、Real Time Monitoring Tool があります。

Cisco CallManager をインストールまたはアップグレードする場合、HTTPS 自己署名証明書である httpscert.cer は、表 2-1 の Cisco CallManager 仮想ディレクトリをホスティングする IIS のデフォルト Web サイトに自動的にインストールされます。

表 2-1　Cisco CallManager 仮想ディレクトリ

Cisco CallManager 仮想ディレクトリ	対応するアプリケーション
CCMAdmin	Cisco CallManager Administration
CCMService	Cisco CallManager Serviceability
CCMUser	Cisco IP Phone User Option Pages
AST	Real-Time Monitoring Tool （RTMT）
RTMTReports	RTMT レポート アーカイブ
CCMTraceAnalysis	Trace Analysis Tool
PktCap	TAC トラブルシューティング ツール **（注）** これらのトラブルシューティング ツールは、仮想ディレクトリを使用して、SCCP メッセージ（電話機）または UDP および TCP バックホール メッセージ（ゲートウェイ）のトレースを含むトレース ファイルを取得します。

表 2-1　Cisco CallManager 仮想ディレクトリ（続き）

Cisco CallManager 仮想ディレクトリ	対応するアプリケーション
ART	Cisco CDR Analysis and Reporting （CAR）
CCMServiceTraceCollectionTool	Trace Collection Tool
BAT	Bulk Administration Tool（BAT）
TAPS	Tool for Auto-Registration Phone Support（TAPS）

HTTPS 証明書は、C:\Program Files\Cisco\Certificates ディレクトリに格納されます。必要に応じて、認証局からサーバ認証証明書をインストールし、HTTPS 自己署名証明書の代わりに使用することができます。Cisco CallManager のインストールまたはアップグレード後に認証局の証明書を使用するには、P.9-1 の「トラブルシューティング」で説明するように、自己署名証明書を削除する必要があります。次に、認証局の資料で説明されているように、認証局から提供されたサーバ認証証明書をインストールします。

（注）　ホスト名を使用して Web アプリケーションにアクセスし、信頼できるフォルダに証明書をインストールした後、ローカルホストか IP アドレスを使用してそのアプリケーションへのアクセスを試みた場合、セキュリティ証明書の名前がサイトの名前と一致しないことを示す Security Alert ダイアログボックスが表示されます。

URL にローカルホスト、IP アドレス、またはホスト名を使用して HTTPS をサポートするアプリケーションにアクセスする場合、URL の種類別（ローカルホスト、IP アドレスなど）の信頼できるフォルダに証明書を保存する必要があります。保存しないと、Security Alert ダイアログボックスはそれぞれの種類について表示されます。

関連項目

- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager システム ガイド*

- *Bulk Administration Tool ユーザ ガイド*
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*
- *Web での Cisco IP Phone のカスタマイズ*
- Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法（P.2-6）
- 証明書の詳細表示（P.2-7）
- 証明書のファイルへのコピー（P.2-9）

Internet Explorer による HTTPS の使用方法

この項では、Internet Explorer での HTTPS 使用に関連した次のトピックについて取り上げます。

- Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法（P.2-6）
- 証明書の詳細表示（P.2-7）
- 証明書のファイルへのコピー（P.2-9）

Cisco CallManager 4.1 をインストールまたはアップグレードした後に、初めて Cisco CallManager Administration または他の Cisco CallManager SSL 対応仮想ディレクトリにブラウザ クライアントからアクセスすると、サーバを信頼するかどうかを確認する Security Alert ダイアログボックスが表示されます。ダイアログボックスが表示されたら、次の作業のいずれか 1 つを実行する必要があります。

- Yes をクリックして、現在の Web セッションについてだけ証明書を信頼するように選択します。現在のセッションについてだけ証明書を信頼する場合、Security Alert ダイアログボックスはアプリケーションにアクセスするたびに表示されます。つまり、証明書を信頼できるフォルダにインストールしない限り、ダイアログボックスは表示されます。
- View Certificate > Install Certificate の順にクリックして、証明書のインストール作業を実行します。この場合、常に証明書を信頼することになります。信頼できるフォルダに証明書をインストールすると、Web アプリケーションにアクセスするたびに Security Alert ダイアログボックスが表示されることはありません。
- No をクリックして、操作を取り消します。認証は行われず、Web アプリケーションにアクセスすることはできません。Web アプリケーションにアクセスするには、Yes をクリックするか、または View Certificate > Install Certificate オプションを使用して証明書をインストールする必要があります。

関連項目

- HTTPS の概要（P.2-2）
- Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法（P.2-6）
- 証明書の詳細表示（P.2-7）
- 証明書のファイルへのコピー（P.2-9）
- HTTPS のトラブルシューティング（P.9-5）

Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法

ブラウザ クライアントで信頼できるフォルダに HTTPS 証明書を保存して、Web アプリケーションにアクセスするたびに Security Alert ダイアログボックスが表示されないようにするには、次の手順を実行します。

手順

ステップ 1　IIS サーバでアプリケーションを参照します。

ステップ 2　Security Alert ダイアログボックスが表示されたら、**View Certificate** をクリックします。

ステップ 3　Certificate ペインの **Install Certificate** をクリックします。

ステップ 4　**Next** をクリックします。

ステップ 5　**Place all certificates in the following store** オプション ボタンをクリックし、**Browse** をクリックします。

ステップ 6　**Trusted Root Certification Authorities** に移動します。

ステップ 7　**Next** をクリックします。

ステップ 8　**Finish** をクリックします。

ステップ 9　**Yes** をクリックして、証明書をインストールします。

インポートが正常に行われたことを示すメッセージが表示されます。**OK** をクリックします。

ステップ 10　ダイアログボックスの右下に表示される **OK** をクリックします。

ステップ 11　証明書を信頼して、今後このダイアログボックスを表示しないようにするには、**Yes** をクリックします。

（注）　URL にローカルホスト、IP アドレス、またはホスト名を使用して HTTPS をサポートするアプリケーションにアクセスする場合、URL の種類別（ローカルホスト、IP アドレスなど）の信頼できるフォルダに証明書を保存する必要があります。保存しないと、Security Alert ダイアログボックスはそれぞれの種類について表示されます。

関連項目

- HTTPS の概要（P.2-2）
- 証明書の詳細表示（P.2-7）
- 証明書のファイルへのコピー（P.2-9）

証明書の詳細表示

証明書の詳細を表示するには、次の作業のどちらかを実行します。

- **View Certificate** ボタンをクリックしてから、**Details** タブをクリックします。
- 証明書が存在するサーバの **C:\Program Files\Cisco\Certificates\httpscert.cer** で証明書を右クリックし、**Open** をクリックします。

ヒント　このペインの設定に表示されているデータは一切変更できません。次の設定の説明については、Microsoft の資料を参照してください。

次の証明書設定が表示されます。

- Version
- Serial Number
- Signature Algorithm
- Issuer
- Valid From

- Valid To
- Subject
- Public key
- Subject Key Installer
- Key Usage
- Enhanced Key Usage
- Thumbprint Algorithm
- Thumbprint

設定のサブセットを表示するには（使用可能な場合）、次のオプションのいずれか 1 つを選択します。

- All：すべてのオプションが Details ペインに表示されます。
- Version 1 Fields Only : Version、Serial Number、Signature Algorithm、Issuer、Valid From、Valid To、Subject、および Public Key オプションが表示されます。
- Extensions Only : Subject Key Identifier、Key Usage、および Enhanced Key Usage オプションが表示されます。
- Critical Extensions Only：存在する場合は Critical Extensions が表示されます。
- Properties Only : Thumbprint Algorithm と Thumbprint オプションが表示されます。

関連項目

- HTTPS の概要（P.2-2）
- Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法（P.2-6）
- 証明書のファイルへのコピー（P.2-9）

証明書のファイルへのコピー

証明書をファイルにコピーすることによって、必要なときにいつでも証明書を復元することができます。また、次の手順を実行して、別のユーザから受信した証明書ファイルをインストールすることができます。

次の手順を実行すると、標準の証明書保管形式で証明書がコピーされます。証明書の内容をファイルにコピーするには、次の手順を実行します。

手順

ステップ 1　Security Alert ダイアログボックスで、**View Certificate** をクリックします。

ステップ 2　**Details** タブをクリックします。

ステップ 3　**Copy to File** ボタンをクリックします。

ステップ 4　Welcome Wizard が表示されます。**Next** をクリックします。

ステップ 5　ファイル形式を定義する次のリストから選択することができます。ファイルのエクスポートに使用するファイル形式を選択して、**Next** をクリックします。

- **DER encoded binary X.509 (.CER)**：DER を使用してエンティティ間の情報で転送します。
- **Base-64 encoded X.509 (.CER)**：保護されたバイナリ添付ファイルをインターネット経由で送信します。ASCII テキスト形式を使用してファイルの破損を防止します。
- **Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)**：証明書と、認証パス内のすべての証明書を選択した PC にエクスポートします。

ステップ 6　エクスポートするファイルに移動します。

ステップ 7　**Finish** をクリックします。

ステップ 8　エクスポートが正常に行われたことを示すダイアログボックスが表示されたら、**OK** をクリックします。

関連項目

- HTTPS の概要（P.2-2）
- Internet Explorer を使用して証明書を信頼できるフォルダに保存する方法（P.2-6）
- 証明書の詳細表示（P.2-7）

Netscape による HTTPS の使用方法

Netscape で HTTPS を使用する場合、証明書のクレデンシャルを表示する、あるセッションで証明書を信頼する、証明書を期限切れまで信頼する、あるいは証明書をまったく信頼しない、という作業が行えます。

ヒント　あるセッションだけで証明書を信頼する場合、HTTPSをサポートするアプリケーションにアクセスするたびに「Netscape を使用して証明書を信頼できるフォルダに保存する方法」の手順を繰り返す必要があります。証明書を信頼しない場合は、アプリケーションにアクセスできません。

関連項目

- HTTPS の概要（P.2-2）
- Netscape を使用して証明書を信頼できるフォルダに保存する方法（P.2-12）
- HTTPS のトラブルシューティング（P.9-5）

Netscape を使用して証明書を信頼できるフォルダに保存する方法

証明書を信頼できるフォルダに保存するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration などのアプリケーションに Netscape からアクセスします。

ステップ 2　New Site Certificate ウィンドウが表示されたら、**Next** をクリックします。

ステップ 3　次の New Site Certificate ウィンドウが表示されたら、**Next** をクリックします。

ヒント　Next をクリックする前に証明書のクレデンシャルを表示するには、**More Info** をクリックします。クレデンシャルを確認して **OK** をクリックした後、New Site Certificate ウィンドウで **Next** をクリックします。

ステップ 4　次のオプション ボタンのいずれか 1 つをクリックします。

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

ステップ 5　**Next** をクリックします。

ステップ 6　Do not accept this certificate... オプション ボタンをクリックした場合は、ステップ 8 に進みます。

ステップ 7　情報が他のサイトへ送信される前に Netscape で警告を表示する場合は、**Warn me before I send information to this site** チェックボックスをオンにし、**Next** をクリックします。

ステップ 8　**Finish** をクリックします。

関連項目

- HTTPS の概要（P.2-2）
- Netscape による HTTPS の使用方法（P.2-11）
- HTTPS のトラブルシューティング（P.9-5）

サードパーティの認証局によるサーバ認証証明書の使用方法

Cisco CallManager 提供の証明書ではなく、サードパーティの認証局によるサーバ認証証明書を使用するには、次の手順を実行します。

手順

ステップ 1　P.9-9 の「HTTPS 証明書の削除」の説明に従って、HTTPS 証明書を削除します。

ステップ 2　使用する証明書をインストールします。

ステップ 3　証明書ファイルを右クリックします。

ステップ 4　**Install Certificate** オプションを選択します。

ヒント　インストールは、デフォルト設定を使用して実行できます。

ステップ 5　次の手順を実行して、IIS のデフォルト Web サイトに証明書をインストールします。

a. **Start > Programs > Administrative Tools > Internet Service Manager** の順に選択します。
b. 証明書をインストールするサーバの名前をクリックします。
c. **Directory Security** タブをクリックします。
d. Secure Communications で **Server Certificate** ボタンをクリックします。
e. **Next** をクリックします。
f. **Assign an Existing Certificate** オプションを選択します。
g. ステップ 2 の証明書を選択します。
h. **Next** をクリックします。
i. **Finish** をクリックします。

ステップ 6　Root CA 証明書の名前を **httpscert.cer** に変更します。

ステップ 7　証明書を DER 形式で **C:\program files\cisco\certificates** にコピーします。

関連項目

- トラブルシューティング（P.9-1）
- HTTPS の概要（P.2-2）