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 tomcat サーバとの間の通信を保護し、証明書および公開鍵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、TAPS、Cisco CDR Analysis and Reporting（CAR）、Cisco Dialed Number Analyzer、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と、HTTPS 自己署名証明書（tomcat_cert）がプラットフォームで生成されます。自己署名証明書は、アップグレード中に移行されます。.DER 形式および .PEM 形式で、証明書のコピーが作成されます。表 2-1 に、仮想ディレクトリを示します。

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 Personal Communications Assistant
AST	Real-Time Monitoring Tool （RTMT）
RTMTReports	RTMT レポート アーカイブ
CCMTraceAnalysis	Trace Analysis Tool
PktCap	パケット キャプチャに使用する TAC トラブルシューティング ツール
ART	Cisco CDR Analysis and Reporting （CAR）
TAPS	Tool for Auto-Registration Phone Support（TAPS）
dna	Cisco Dialed Number Analyzer
drf	Cisco IP Telephony Disaster Recovery System

（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。

Internet Explorer による HTTPS の使用方法

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

Cisco CallManager 5.0(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。

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　tomcat サーバのアプリケーション（Cisco CallManager Administration など）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　Certificate Import Wizard が表示されたら、**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** を参照し、選択して、**OK** をクリックします。

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　Security Warning Box に証明書のサムプリントが表示されます。

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** をクリックして続行します。

（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。

ヒント　Certificate ペインの Certification Path タブをクリックして、証明書が正常にインストールされたことを確認できます。

追加情報

詳細については、P.2-8 の「関連項目」を参照してください。

証明書の詳細表示

Security Alert ダイアログボックスが表示されたら、**View Certificate** ボタンをクリックし、**Details** タブをクリックして、証明書の詳細を表示します。

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。

（注）　自己署名証明書は、Cisco IPT Platform Administration GUI で再生成できます。

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し、ローカルに保管することによって、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。

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　Certificate Export 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。エクスポート ファイル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で情報を転送します。
- **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　ファイルのコピーをエクスポートする場所に移動して、ファイルの名前を指定します。**Save**　をクリックします。

ステップ 7　ファイル名とパスが Certificate Export Wizard ペインに表示されます。**Next** をクリックします。

ステップ 8　ファイルと設定が表示されます。**Finish** をクリックします。

ステップ 9　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。

追加情報

詳細については、P.2-8 の「関連項目」を参照してください。

Netscape による HTTPS の使用方法

この項では、Netscape での HTTPS の使用について取り上げます。

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。

Netscape には、証明書をファイルにコピーするための証明書エクスポート ユーティリティがありません。

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。

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 でアクセスします。

証明書認証のダイアログボックスが表示されます。

ステップ 2　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)

（注）　Do not accept を選択すると、アプリケーションは表示されません。

（注）　続行する前に証明書のクレデンシャルを表示するには、**Examine Certificate** をクリックします。クレデンシャルを確認し、**Close** をクリックします。

ステップ 3　**OK** をクリックします。

Security Warning ダイアログボックスが表示されます。

ステップ 4　**OK** をクリックします。

（注）　自己署名証明書は、Cisco IPT Platform Administration GUI で再生成できます。

追加情報

詳細については、P.2-8 の「関連項目」を参照してください。

その他の情報

関連項目

証明書の種類（P.1-13）

シスコの関連マニュアル

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager アドミニストレーション ガイド*
- 入手可能な HTTPS 関連の Microsoft の資料