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 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 Unified Communications Manager アプリケーションには、Cisco Unified Communications Manager の管理ページ、Cisco Unified Serviceability、Cisco Unified IP Phone ユーザ オプション ページ、Cisco Unified Communications Manager Auto-Register Phone Tool、Cisco Unified Communications Manager CDR Analysis and Reporting、Dialed Number Analyzer、および Cisco Unified Real-Time Monitoring Tool があります。

Cisco Unified Communications Manager 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、Cisco Unified Communications Manager 内の HTTPS を使用するアプリケーションを示します。

表 2-1　Cisco Unified Communications Manager の HTTPS アプリケーション

Cisco Unified Communications Manager の HTTPS アプリケーション	Web アプリケーション
CMAdmin	Cisco Unified Communications Manager の管理ページ
CMService	Cisco Unified Serviceability
CMUser	Cisco Personal Assistant
AST	Cisco Unified Real-Time Monitoring Tool
RTMTReports	Cisco Unified Real-Time Monitoring Tool レポート アーカイブ
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 Unified Communications Manager CDR Analysis and Reporting
TAPS	Cisco Unified Communications Manager Auto-Register Phone Tool
dna	Dialed Number Analyzer
drf	Disaster Recovery System
SOAP	Cisco Unified Communications Manager データベースに対して読み書きを行うための Simple Object Access Protocol API **（注）** セキュリティのために、SOAP を使用するすべての Web アプリケーションで HTTPS が必要です。SOAP アプリケーションでは、HTTP はサポートされていません。HTTP を使用する既存のアプリケーションは失敗します。ディレクトリを変更することによって、このようなアプリケーションを HTTPS に変換することはできません。

（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［セキュリティの警告］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、［セキュリティの警告］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。

- 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.2-3）
- 証明書の詳細表示（P.2-4）
- 証明書のファイルへのコピー（P.2-5）

Cisco Unified Communications Manager 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 Unified Communications Manager の管理ページまたは他の Cisco Unified Communications Manager 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［セキュリティの警告］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。

- ［はい］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、［セキュリティの警告］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。
- **［証明書の表示］>［証明書のインストール］**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［セキュリティの警告］ダイアログボックスが表示されることはありません。
- ［いいえ］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、［はい］をクリックするか、または**［証明書の表示］>［証明書のインストール］**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［セキュリティの警告］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 Unified Communications Manager の管理ページなど）を参照します。

ステップ 2　［セキュリティの警告］ダイアログボックスが表示されたら、**［証明書の表示］**をクリックします。

ステップ 3　［証明書］ペインの［**証明書のインストール**］をクリックします。

ステップ 4　［証明書のインポート ウィザード］が表示されたら、［**次へ**］をクリックします。

ステップ 5　［**証明書をすべて次のストアに配置する**］オプション ボタンをクリックし、［**参照**］をクリックします。

ステップ 6　［**信頼されたルート証明機関**］を参照し、選択して、［**OK**］をクリックします。

ステップ 7　［**次へ**］をクリックします。

ステップ 8　［**完了**］をクリックします。

ステップ 9　［セキュリティ警告］ボックスに証明書のサムプリントが表示されます。

［**はい**］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、［**はい**］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、［セキュリティの警告］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　［証明書］ペインの［証明書のパス］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

［セキュリティの警告］ダイアログボックスが表示されたら、［**証明書の表示**］ボタンをクリックし、［**詳細設定**］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。

- バージョン
- シリアル番号
- 署名アルゴリズム
- 発行者
- 有効期間の開始
- 有効期間の終了
- サブジェクト
- 公開キー
- サブジェクト キー識別子
- キー使用法
- 拡張キー使用法
- 拇印アルゴリズム
- 拇印

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。

- ［すべて］: すべてのオプションが［詳細設定］ペインに表示されます。
- ［バージョン 1 のフィールドのみ］:［バージョン］、［シリアル番号］、［署名アルゴリズム］、［発行者］、［有効期間の開始］、［有効期間の終了］、［サブジェクト］、および［公開キー］の各オプションが表示されます。
- ［拡張機能のみ］:［サブジェクト キー識別子］、［キー使用法］、および［拡張キー使用法］の各オプションが表示されます。
- ［重要な拡張機能のみ］: 存在する場合は［重要な拡張機能］が表示されます。
- ［プロパティのみ］:［拇印アルゴリズム］と［拇印］オプションが表示されます。

（注） 自己署名証明書は、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を使用して再生成できます。

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　［セキュリティの警告］ダイアログボックスで、**［証明書の表示］**をクリックします。

ステップ 2　**［詳細設定］**タブをクリックします。

ステップ 3　**［ファイルにコピー］**ボタンをクリックします。

ステップ 4　［証明書のエクスポート ウィザード］が表示されます。**［次へ］**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、［次へ］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。［保存］をクリックします。

ステップ 7　ファイル名とパスが［証明書のエクスポート ウィザード］ペインに表示されます。［次へ］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。［完了］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 Unified Communications Manager の管理ページ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。

- ［この証明書のこのセッションのために一時的に受け入れる］
- ［この証明書を受け入れない / この Web サイトに接続しない］
- ［この証明書を永続的に受け入れる］

（注）　［この証明書を受け入れない / この Web サイトに接続しない］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、**［証明書を調査］**をクリックします。クレデンシャルを確認し、**［閉じる］**をクリックします。

ステップ 3　**［OK］**をクリックします。

［セキュリティに関する報告］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 Unified Communications オペレーティング システムの GUI を使用して再生成できます。

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（P.1-15）

シスコの関連マニュアル

- *Cisco Unified Communications Manager Serviceability アドミニストレーション ガイド*
- *Cisco Unified Communications Manager 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