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、Microsoft Windows ユーザに対して、ブラウザと Web サーバの間の通信を保護します。HTTPS は証明書を使用して、サーバの ID を保証し、ブラウザ接続を保護します。HTTPS は公開鍵を使用して、インターネット経由で転送されるデータ（ユーザのログインやパスワードを含む）を暗号化します。

HTTPS を有効にするには、接続プロセス中にサーバを識別する証明書をダウンロードする必要があります。現在のセッションだけでサーバ証明書を受け入れることができます。また、信頼できるフォルダ（ファイル）に証明書をダウンロードすると、そのサーバとの現在のセッションおよび将来のセッションを保護することができます。信頼できるフォルダには、すべての信頼できるサイトの証明書が格納されています。

シスコは、Cisco Unified Communications Manager 内の Cisco Tomcat Web サーバ アプリケーションへの接続で次のブラウザをサポートしています。

- Internet Explorer 6
- Internet Explorer 7
- Netscape 7.1

（注）　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。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。詳細については、『*Cisco Unified Communications Operating System アドミニストレーション ガイド*』を参照してください。

表 2-1 に、Cisco Unified Communications Manager 内の、Cisco Tomcat で 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

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

Cisco Unified Communications Manager の HTTPS アプリケーション	Web アプリケーション
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。シスコは、SOAP アプリケーションで HTTP をサポートしません。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。

Internet Explorer による HTTPS の使用方法

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。

（注）　Cisco Unified Communications Manager へのアクセスに使用するアドレスは、証明書に記載されている名前と一致する必要があります。一致しない場合は、デフォルトでエラー メッセージが表示されます。信頼できるフォルダに証明書をインストールした後、ローカルホストまたは IP アドレスを使用して Web アプリケーションにアクセスすると、セキュリティ証明書の名前が、アクセスしている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が表示されます。

次の各項では、Internet Explorer で HTTPS を使用する方法について説明します。

- Internet Explorer 6 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.2-4）
- Internet Explorer 7 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.2-5）
- 証明書のファイルへのコピー（P.2-7）

Internet Explorer 6 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 HTTPS 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　Tomcat サーバにアクセスします（たとえば、ブラウザに Cisco Unified Communications Manager の管理ページのホスト名、ローカルホスト、または IP アドレスを入力します）。

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。

証明書のデータを確認する場合は、**［詳細設定］**タブをクリックして、証明書の詳細を表示できます。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。

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　**［Finish］**をクリックします。

［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。

ステップ 9　**［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.2-10 の「関連項目」を参照してください。

Internet Explorer 7 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

Internet Explorer 7 では、セキュリティ機能が追加され、ブラウザが Web サイトにアクセスするためにシスコ証明書を処理する方法が変更されています。シスコは Cisco Unified Communications Manager サーバに自己署名証明書を提供するため、信頼ストアにそのサーバ証明書が含まれていても、Internet Explorer 7 は Cisco Unified Communications Manager の管理機能の Web サイトに、信頼できないというフラグを付け、証明書エラーを発生させます。

（注）　Internet Explorer 7（Windows Vista の機能）は、Windows XP Service Pack 2（SP2）、Windows XP Professional x64 Edition、および Windows Server 2003 Service Pack 1（SP1）上でも動作します。IE に Java 関連のブラウザ サポートを提供するには、Java Runtime Environment（JRE; Java ランタイム環境）が必要です。

ブラウザを再起動するたびに証明書をリロードせずに、アクセスを保護するには、必ず Cisco Unified Communications Manager の証明書を Internet Explorer 7 にインポートします。証明書の警告が表示されている Web サイトの閲覧を続行し、証明書が信頼ストアに存在しない場合、Internet Explorer 7 は現在のセッションの間だけ証明書を記憶します。

サーバ証明書をダウンロードしても、Internet Explorer 7 は引き続き Web サイトの証明書エラーを表示します。ブラウザの［信頼されたルート証明機関］信頼ストアにインポート済み証明書が含まれている場合は、このセキュリティ警告を無視できます。

次の手順は、Cisco Unified Communications Manager の証明書を Internet Explorer 7 のルート証明書信頼ストアにインポートする方法を示しています。

手順

ステップ 1　Tomcat サーバのアプリケーションを参照します（たとえば、ブラウザに Cisco Unified Communications Manager の管理ページのホスト名、ローカルホスト、または IP アドレスを入力します）。

ブラウザに、この Web サイトが信頼されていないことを示す「証明書のエラー：ナビゲーションはブロックされたました。」というメッセージが表示されます。

ステップ 2　**［このサイトの閲覧を続行する（推奨されません）。］**をクリックして、サーバにアクセスします。

［Cisco Unified Communications Manager の管理］ウィンドウが表示され、ブラウザにアドレス バーと［証明書のエラー］ステータスが赤色で表示されます。

ステップ 3　サーバ証明書をインポートするには、［証明書のエラー］ステータス ボックスをクリックして、ステータス レポートを表示します。レポートで［**証明書の表示**］リンクをクリックします。

ステップ 4　証明書の詳細を確認します。

［証明書のパス］タブに、「信頼されたルート証明機関のストアに存在しないためこのルート CA 証明書は信頼されていません。」と表示されます。

ステップ 5　［証明書］ウィンドウで［全般］タブを選択し、［**証明書のインストール**］をクリックします。

［証明書のインポート ウィザード］が起動します。

ステップ 6　［**次へ**］をクリックして、ウィザードを開始します。

［証明書ストア］ウィンドウが表示されます。

ステップ 7　［自動］オプション（ウィザードがこの証明書タイプの証明書ストアを選択できる）が選択されていることを確認し、［**次へ**］をクリックします。

ステップ 8　設定を確認し、［**完了**］をクリックします。

インポート操作に関するセキュリティ警告が表示されます。

ステップ 9　［**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 ウィザードに「インポートに成功しました。」と表示されます。

ステップ 10　［**OK**］をクリックします。次回［証明書の表示］リンクをクリックすると、［証明書］ウィンドウの［証明書のパス］タブに「この証明書は問題ありません。」と表示されます。

ステップ 11　インポートした証明書が信頼ストアにあることを確認するには、Internet Explorer のツールバーで［**ツール**］>［**インターネット オプション**］をクリックし、［コンテンツ］タブを選択します。［**証明書**］をクリックし、［信頼されたルート証明機関］タブを選択します。リストをスクロールして、インポートした証明書を見つけます。

証明書のインポート後も引き続き、ブラウザにアドレス バーと［証明書のエラー］ステータスが赤色で表示されます。ホスト名、ローカルホスト、または IP アドレスを再入力しても、ブラウザをリフレッシュまたは再起動しても、このステータスは変わりません。

追加情報

詳細については、P.2-10 の「関連項目」を参照してください。

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。

ヒント　IE 7 の場合は、［証明書のエラー］ステータス ボックスをクリックして、［証明書の表示］オプションを表示します。

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。**［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.2-10 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。

（注）　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 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。

（注）　Cisco Unified Communications Manager へのアクセスに使用するアドレスは、証明書に記載されている名前と一致する必要があります。一致しない場合は、デフォルトでエラー メッセージが表示されます。信頼できるフォルダに証明書をインストールした後、IP アドレスを使用して Web アプリケーションにアクセスすると、セキュリティ証明書の名前が、アクセスしている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が表示されます。

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　Tomcat サーバのアプリケーションを参照します（たとえば、ブラウザに Cisco Unified Communications Manager の管理ページのホスト名、ローカルホスト、または IP アドレスを入力します）。

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。

追加情報

詳細については、P.2-10 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.1-16）

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