Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）

この章では、セキュアソケットレイヤを介したハイパーテキスト転送プロトコルについて説明します。

HTTPS

HTTPS（Hypertext Transfer Protocol over Secure Sockets Layer（SSL））は、Microsoft Windows ユーザ向けにブラウザと 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、ブラウザ接続をセキュアにします。HTTPS は、インターネット経由の転送時に、公開キーを使用して、ユーザログインやパスワードなどのデータを暗号化します。

Unified Communications Manager は、HTTPS 接続の SSL および Transport Layer Security（TLS）をサポートしています。Web ブラウザのバージョンが TLS をサポートしている場合は、TLS を使用してセキュリティを向上させることを推奨します。セキュアな HTTPS 通信に TLS を使用するには、web ブラウザで SSL を無効にします。

HTTPS を有効にするには、接続プロセス中にサーバ識別用の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にサーバ証明書を使用するか、サーバでの現在のセッションと将来のセッションを保護するために信頼フォルダ（ファイル）に証明書をダウンロードすることができます。信頼フォルダには、すべての信頼済みサイトの証明書が保存されます。

Unified Communications Manager での Cisco Tomcat Web サーバ アプリケーションとの接続について、シスコでは次のブラウザをサポートしています。

- Microsoft Windows XP SP3 上で動作している場合は、Microsoft Internet Explorer（IE）7

- Microsoft Windows XP SP3 または Microsoft Vista SP2 上で動作している場合は、Microsoft Internet Explorer（IE）8
- Microsoft Windows XP SP3、Microsoft Vista SP2 または Apple MAC OS X 上で動作している場合は、Firefox 3.x
- Apple MAC OS X 上で動作している場合は、Safari 4.x

（注） 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）が生成されます。この自己署名証明書は、Unified Communications Manager へのアップグレード時に自動的に移行されます。この証明書のコピーは .DER および .PEM 形式で作成されます。

自己署名証明書は、Cisco Unified Communications Operating System GUI を使用して再生成できます。詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Unified Communications Manager で Cisco Tomcat との間で HTTPS を使用するアプリケーションを次の表に示します。

表 *1 : Unified Communications Manager HTTPS* アプリケーション

Unified Communications Manager HTTPS アプリケーション	**Web アプリケーション（Web Application）**
ccmadmin	Unified Communications Manager Administration
ccmservice	Cisco Unified Serviceability
cmplatform	オペレーティング システムの管理ページ
cmuser	Cisco Personal Assistant [英語]
ast	Real Time Monitoring Tool
RTMTReports	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される TAC トラブルシューティングツール
art	Unified Communications Manager CDR Analysis and Reporting
taps	Unified Communications Manager Auto-Register Phone Tool
DNA {"title": "Japanese"}	Dialed Number Analyzer
drf	Disaster Recovery System

Unified Communications Manager HTTPS アプリケーション	Web アプリケーション（Web Application）
SOAP	Unified Communications Manager データベースの読み取り/書き込み用の Simple Object Access Protocol API （注） セキュリティのために、SOAP を使用しているすべての Web アプリケーションには HTTPS が必要です。シスコでは、SOAP アプリケーションの HTTP をサポートしていません。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 HTTPS に変換することはできません。

Cisco Unified IP 電話 サービスの HTTPS

Unified Communications Manager、Cisco IP 電話、および Cisco Unified IP 電話 の各サービスでは、HTTPS、暗号化、およびポート 8443 を使用したサーバのセキュアな識別がサポートされています。

TV (信頼検証サービス) は、証明書チェーンを検証しません。TV が証明書を確認するには、電話機によって TV に提示されたものと同じ証明書が tomcat 信頼証明書ストアに含まれている必要があります。

TVは、ルート証明書または中間証明書を確認します。アイデンティティ証明書は、データベースに存在しない場合にのみ検証されます。ルート証明書と中間証明書が存在する場合でも、。検証に失敗しました。

HTTPS をサポートする Cisco Unified IP 電話

次の Cisco IP 電話 では、HTTPS がサポートされています。

- 6901、6911、6921、6941、6945、6961
- 7811、7821、7832、7841、7861
- 7906、7911、7925、7925-EX、7926、7931、7941、7941G-GE、7942、7945、7961、7962、7961G-GE、7965、7975
- 8811、8821、8831、8832、8841、8845、8851、8851NR、8861、8865、8865NR
- 8941、8945、8961
- 9951、9971

（注） このリスト内の69xx 電話は、HTTPS クライアントとして機能できますが、HTTPS サーバとして機能することはできません。このリスト内の残りの電話機は、HTTPS クライアントまたはHTTPS サーバとして動作できます。

HTTPS をサポートする機能

次の機能は、HTTPS をサポートしています。

- Cisco Extension Mobility（EM）
- Cisco Extension Mobility Cross Cluster（EMCC）
- Cisco Unified Communications Manager Manager Assistant（IPMA）
- Cisco Unified IP 電話 サービス
- パーソナル ディレクトリ
- クレデンシャルの変更（Change Credentials）

Cisco Unified IP 電話 サービスの設定

Unified Communications Manager リリース 8.0(1) 以降では、HTTPS をサポートするため、次の表に示すセキュア URL パラメータが電話の設定に含まれるようになりました。

セキュア URL の各パラメータを設定するには、[Unified Communications Manager Administration] から **[Device]** > **[Device Settings]** > **[Phone Services]** を選択します。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

（注） Cisco Unified Communications Manager Administration の [エンタープライズパラメータ (Enterprise Parameter)] セクションでセキュアな電話の URL パラメータを削除してから再起動すると、URL パラメータはデフォルトで再入力されます。再起動後に、[セキュアな電話の URL パラメータ (セキュア電話の URL Parameters)] セクションに移動し、URL に対して正しい変更を行い、電話機を再起動します。

表 *2:* セキュア *Url* の電話機の構成時の設定

フィールド	説明
[セキュア認証URL（Secure Authentication URL）]	電話 Web サーバに対する要求を検証するために電話機で使用するセキュア URL を入力します。 （注） セキュア認証 URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 この URL はデフォルトでは、インストール時に設定される Cisco Unified Communications の [セルフケアポータル（Self Care Portal）] ウィンドウにアクセスします。 デフォルトの設定を受け入れるには、このフィールドを空白にします。 最大長：255
[セキュアディレクトリ URL（Secure Directory URL）]	電話機がディレクトリ情報を取得する際の取得元サーバのセキュア URL を入力します。このパラメータには、ユーザが [Directory] ボタンを押したときにセキュアな Cisco IP 電話 が使用する URL を指定します。 （注） セキュア ディレクトリ URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルトの設定を受け入れるには、このフィールドを空白にします。 最大長：255

フィールド	説明
[セキュアアイドルURL（Secure Idle URL）]	電話が [Idle Timer] フィールドで指定された時間アイドルだったときに Cisco IP 電話 に表示される情報のセキュア URL を入力します。たとえば、電話が 5 分間使用されていない場合、LCD にロゴを表示できます。 （注） セキュア アイドル URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[セキュア情報URL（Secure Information URL）]	Cisco IP 電話 がヘルプ テキストの情報を取得するサーバの場所を示す URL を入力します。この情報は、ユーザが電話機の情報（i）ボタンまたは疑問符（?）ボタンを押すと表示されます。 （注） セキュア情報URLを指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

フィールド	説明
[セキュアメッセージURL（Secure Messages URL）]	メッセージ サーバのセキュア URL を入力します。ユーザが [Messages] ボタンを押すと、Cisco IP 電話 はこの URL にアクセスします。 （注） セキュア メッセージ URL を指定しない場合、デバイスは非セキュアなURL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255
[セキュアサービスURL（Secure Services URL）]	Cisco Unified IP 電話 サービスのセキュア URL を入力します。ユーザが [サービス（Services）] ボタンを押すと、Cisco Unified IP 電話 はこのセキュア URL にアクセスします。 （注） セキュア サービス URL を指定しない場合、デバイスは非セキュアな URL を使用します。セキュアな URL と非セキュアな URL の両方を指定した場合、デバイスはその機能に基づいて適切な URL を選択します。 デフォルト設定を受け入れるには、このフィールドを空白のままにします。 最大長：255

HTTPS をサポートするためのエンタープライズ パラメータの設定

HTTPS をサポートするため、Unified Communications Manager リリース 8.0(1) 以降では次の新しいエンタープライズ パラメータがサポートされています。

- [保護された認証URL（Secured Authentication URL）]
- [保護されたディレクトリURL（Secured Directory URL）]
- Secured Idle URL
- [保護された情報URL（Secured Information URL）]
- [Secured Messaged URL]

• [保護されたサービスURL（Secured Services URL）]

Internet Explorer 8 を使用して証明書を信頼できるフォルダに保存する

ブラウザを再起動するたびに証明書をリロードしなくても安全なアクセスが行えるよう、Unified Communications Manager の証明書を Internet Explorer 8 にインポートしてください。Web サイトで証明書に対する警告が表示され、証明書が信頼ストアにない場合、Internet Explorer 8 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た後も、Internet Explorer 8 ではその Web サイトに対する証明書エラーが引き続き表示されます。ブラウザの信頼できるルート認証局信頼ストアにインポートされた証明書が含まれている場合は、セキュリティ警告を無視できます。

次の手順では、Internet Explorer 8 のルート証明書の信頼ストアに Unified Communications Manager の証明書をインポートする方法について説明します。

手順

Step 1 Tomcat サーバのアプリケーションを参照します（たとえば、Unified Communications Manager Administration のホスト名、localhost または IP アドレスをブラウザに入力します）。

ブラウザに証明書エラー: Navigation ブロックメッセージが表示され、この web サイトが信頼できないことを示します。

Step 2 サーバにアクセスするには、[Continue to this website (not recommended)] をクリックします。

[Unified Communications Manager Administration] 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のステータスが赤色で表示されます。

Step 3 サーバ証明書をインポートするには、[Certificate Error] 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。レポートの [View Certificates] リンクをクリックします。

Step 4 証明書の詳細を確認します。

Step 5 [Certificate] ウィンドウで [General] タブを選択し、[Install Certificate] 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。

Step 6 ウィザードを起動するには、[Next] をクリックします。

[Certificate Store] ウィンドウが表示されます。

Step 7 [Automatic] オプションが選択されていることを確認します。これを選択すると、ウィザードでこの証明書タイプの証明書ストアを選択できるようになります。[Next] をクリックします。

Step 8 設定を確認し、[Finish] をクリックします。

インポート操作に対してセキュリティ警告が表示されます。

Step 9 証明書をインストールするには、[**Yes**] をクリックします。

インポート ウィザードに「「The import was successful.」」と表示されます。

Step 10 [OK] をクリックします。**[View Certificates]** リンクを次にクリックしたときには、[Certificate Path] ウィンドウの **[Certification Path]** タブに「「This certificate is OK.」」と表示されます。

Step 11 信頼ストアにインポートした証明書が含まれていることを確認するには、Internet Explorer のツールバーの **[Tools]** > **[Internet Options]** をクリックして、**[Content]** タブを選択します。[Certificates] をクリックして、[Trusted Root Certifications Authorities] タブを選択します。インポートした証明書が見付かるまでリストをスクロールします。

証明書のインポート後、ブラウザには引き続きアドレス バーと証明書エラーのステータスが赤色で表示されます。このステータスは、ホスト名、localhost または IP アドレスを入力したり、ブラウザを更新または再起動した場合でも表示されます。

関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 15

Internet Explorer 8 証明書をファイルにコピーする

証明書をファイルにコピーしてローカルに保存すると、必要な場合は常に証明書を復元できます。

次の手順を実行すると、標準の証明書の保存形式を使用して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

Step 1 [Certificate Error status] ボックスをクリックします。

Step 2 [証明書の表示（View Certificates）] をクリックします。

Step 3 [詳細（Details）] タブをクリックします。

Step 4 **[ファイルにコピー]** ボタンをクリックします。

Step 5 [Certificate Export Wizard] が表示されます。[次へ（Next）] をクリックします。

Step 6 次のリストは、選択可能なファイル形式を定義しています。エクスポートされたファイルに使用するファイル形式を選択します。[**Next**] をクリックします。

a) [DER encoded binary X.509 (.CER)]：エンティティ間の情報転送で DER を使用します。
b) Base-64 encoded x.509 (.CER): インターネットを介して安全なバイナリ添付ファイルを送信します。は 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。
c) [Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)]：証明書自体と、選択した PC の認証パスにあるすべての証明書をエクスポートします。

Step 7 ファイルのコピーをエクスポートする場所を参照し、ファイルに名前を付けます。[保存（Save）] をクリックします。

Step 8 ファイル名とパスが [Certificate Export Wizard] ペインに表示されます。[次へ（Next）] をクリックします。

Step 9 ファイルと設定が表示されます。[Finish] をクリックします。

Step 10 [Successful export] 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。

関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 15

HTTPS を使用した Firefox の初回認証

Unified Communications Manager のインストールまたはアップグレード後に、[Unified Communications Manager Administration] またはその他の Unified Communications Manager SSL 対応仮想ディレクトリにユーザがブラウザ クライアントから初めてアクセスすると、サーバを信頼するかどうかを尋ねる [Security Alert] ダイアログボックスが表示されます。

このダイアログボックスが表示された場合、次のいずれかのタスクを実行する必要があります。

- **[I Understand The Risks]** をクリックすると、現在の Web セッションの間だけ証明書を信頼することになります。現在のセッションの間だけ証明書を信頼する場合は、アプリケーションにアクセスするごとに [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。つまり、信頼できるフォルダに証明書をインストールするまでこのダイアログボックスが表示されることになります。
- **[Get Me Out Of Here]** をクリックすると、操作がキャンセルされます。認証が行われないため、Web アプリケーションにアクセスできません。Web アプリケーションにアクセスするには、**[I Understand The Risks]** をクリックする必要があります。

関連トピック

Internet Explorer 8 証明書をファイルにコピーする, on page 9
Safari 4.x を使用して証明書を信頼できるフォルダに保存する, on page 13

Firefox 3.x を使用して証明書を信頼できるフォルダに保存します。

ブラウザクライアントの信頼できるフォルダに HTTPS 証明書を保存するには、次の手順を実行します。

手順

Step 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 Administration] 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）。

Step 2 [セキュリティ警告 (Security Alert)] ダイアログボックスが表示されたら、[**リスクを理解**する (I)] をクリックします。

Step 3 [Add Exception] をクリックします。

[Add Exception] ダイアログボックスが表示されます。

Step 4 [Get Certificate] をクリックします。

Step 5 [Permanently store this exception] チェックボックスをオンにします。

Step 6 [セキュリティ例外の確認（Confirm Security Exception）] をクリックします。

Step 7 次の手順を実行して証明書の詳細を表示します。

a) Firefox ブラウザで **[Tools]** > **[Options]** をクリックします。

[Options] ダイアログボックスが表示されます。

b) [詳細設定（Advanced）] をクリックします。

c) [証明書の表示（View Certificates）] をクリックします。

[Certificate Manager] ダイアログボックスが表示されます。

d) 表示する証明書を強調表示し、[**表示 (view)**] をクリックします。

[Certificate Viewer] ダイアログボックスが表示されます。

e) [詳細（Details）] タブをクリックします。

f) [Certificate Fields] フィールドで、表示するフィールドを強調表示します。

[フィールド値 (Field Values)] フィールドに詳細が表示されます。

g) [Certificate Viewer] ダイアログボックスで、[**Close**] をクリックします。

h) [Certificate Viewer] ダイアログボックスで [OK] をクリックします。

ファイルに 3. x 証明書をコピー Firefox

証明書をファイルにコピーしてローカルに保存すると、必要な場合は常に証明書を復元できます。

次の手順を実行すると、標準の証明書の保存形式を使用して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

Step 1 Firefox ブラウザで **[Tools]** > **[Options]** をクリックします。

[Options] ダイアログボックスが表示されます。

Step 2 選択されていなければ、[Advanced] をクリックします。

Step 3 [**Encryption**] タブをクリックし、[**View Certificates**] をクリックします。

[Certificate Manager] ダイアログボックスが表示されます。

Step 4 [Servers] タブをクリックします。

Step 5 コピーする証明書を強調表示して [Export] をクリックします。

[Save Certificate to File] ダイアログボックスが表示されます。

Step 6 ファイルをコピーする場所に移動します。

Step 7 [Save as type] ドロップダウン リストで、ファイル タイプを次のオプションから選択します。

a) [X.509 Certificate (PEM)]：エンティティ間の情報転送で **PEM** を使用します。

b) [X.509 Certificate with chain (PEM)]: プライバシー強化メールを使用して、証明書チェーンを検証し、エンティティ間で情報を転送します。

- [X.509 Certificate (DER)]：エンティティ間の情報転送で **DER** を使用します。
- X.509 Certificate (pkcs＃7): pkcs＃7 は、データの署名または暗号化のための標準規格です。署名されたデータを検証するために証明書が必要であるため、これを SignedData 構造に含めることができます。A.P7C ファイルは、署名するデータを持たない、退化した SignedData 構造です。
- [X.509 Certificate with chain (pkcs＃7)]: pkcs＃7 を使用して、証明書チェーンを確認し、エンティティ間で情報を転送します。

Step 8 [保存（Save）] をクリックします。

Step 9 [OK] をクリックします。

関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 15

HTTPS を使用した Safari の初回認証

Unified Communications Manager のインストールまたはアップグレード後に、[Unified Communications Manager Administration] またはその他の Unified Communications Manager SSL 対応仮想ディレクトリにユーザがブラウザ クライアントから初めてアクセスすると、サーバを信頼するかどうかを尋ねる [Security Alert] ダイアログボックスが表示されます。

このダイアログボックスが表示された場合、次のいずれかのタスクを実行する必要があります。

- [Yes] をクリックすると、現在の Web セッションの間だけ証明書を信頼することになります。現在のセッションの間だけ証明書を信頼する場合は、アプリケーションにアクセスするごとに [セキュリティの警告（Security Alert）] ダイアログボックスが表示されます。つまり、信頼できるフォルダに証明書をインストールするまでこのダイアログボックスが表示されることになります。
- **[Show Certificate]** > **[Install Certificate]** をクリックして、証明書のインストール作業を実行し、証明書を常に信頼することを示します。証明書を信頼できるフォルダに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ごとに [セキュリティの警告（Security Alert）] ダイアログボックスが表示されなくなります。
- [No] をクリックすると、操作がキャンセルされます。認証が行われないため、Web アプリケーションにアクセスできません。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 **[Show Certificate]** > **[Install Certificate]** オプションを選択して証明書をインストールする必要があります。

（注） Unified Communications Manager へのアクセスに使用するアドレスは、証明書にあ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その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とアクセスするサイトの名前が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。

関連トピック

Internet Explorer 8 証明書をファイルにコピーする, on page 9
Firefox 3.x を使用して証明書を信頼できるフォルダに保存します。, on page 10

Safari 4.x を使用して証明書を信頼できるフォルダに保存する

ブラウザクライアントの信頼できるフォルダにHTTPS証明書を保存するには、次の手順を実行します。

手順

Step 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 Administration] 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）。

Step 2 [Security Alert] ダイアログボックスが表示されたら、[Show Certificate] をクリックします。

証明書データを確認することを選択した場合は、[**details**] 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)、次のいずれかのオプションを選択します。

a) すべて (all): すべてのオプションが [詳細 (Details)] ペインに表示されます。
b) 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、発行元、有効な From、有効な To、Subject、および公開キーオプションが表示されます。
c) [拡張のみ (Extensions Only)]: サブジェクトキー識別子、キーの使用状況、および拡張キー使用法のオプションが表示されます。
d) [Critical Extensions Only]: 重要な内線番号 (存在する場合) が表示されます。
e) [プロパティのみ (Properties Only)]: サムプリントアルゴリズムとサムプリントオプションが表示されます。

Step 3 [Certificate] ペインの [Install Certificate] をクリックします。

Step 4 [Certificate Import Wizard] が表示されたら、[Next] をクリックします。

Step 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。

Step 6 [Trusted Root Certification Authorities] を参照し、選択して、[OK] をクリックします。

Step 7 [次へ（Next）] をクリックします。

Step 8 [Finish] をクリックします。

セキュリティ警告ボックスには、ユーザの証明書サムプリントが表示されます。

Step 9 証明書をインストールするには、[Yes] をクリックします。

インポートが正常に実行さ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。

Step 10 ダイアログボックスの右下隅にある [OK] をクリックします。

Step 11 証明書を信頼して、ダイアログボックスが今後表示されないようにするには、[Yes] をクリックします。

ヒント 証明書が正常にインストールされたことを確認するには、[Certificate] ペインの [certificate **Path**] タブをクリックします。

Safari 4.x 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てローカルに保存すると、必要な場合は常に証明書を復元できます。

次の手順を実行すると、標準の証明書の保存形式を使用して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

Step 1 [Security Alert] ダイアログボックスで、[Show Certificate] をクリックします。

ヒント Safari で、[Certificate Error] ステータスボックスをクリックして、[Show Certificate] オプションを表示します。

Step 2 [詳細（Details）] タブをクリックします。

Step 3 **[ファイルにコピー]** ボタンをクリックします。

Step 4 [Certificate Export Wizard] が表示されます。[次へ（Next）] をクリックします。

Step 5 次のリストは、選択可能なファイル形式を定義しています。エクスポートされたファイルに使用するファイル形式を選択します。[**Next**] をクリックします。

a) [DER encoded binary X.509 (.CER)]：エンティティ間の情報転送で DER を使用します。
b) Base-64 encoded x.509 (.CER): インターネットを介して安全なバイナリ添付ファイルを送信します。は 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。
c) 暗号化メッセージ構文標準 PKCS #7 証明書 (.P7B): 証明書および証明書のすべての証明書を、選択した PC にエクスポートします。

Step 6 ファイルのコピーをエクスポートする場所を参照し、ファイルに名前を付けます。[保存（Save）] をクリックします。

Step 7 ファイル名とパスが [Certificate Export Wizard] ペインに表示されます。[次へ（Next）] をクリックします。

Step 8 ファイルと設定が表示されます。[Finish] をクリックします。

Step 9 [Successful export] 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。

関連トピック

HTTPS 設定に関する詳細情報の入手先, on page 15

HTTPS 設定に関する詳細情報の入手先

関連するシスコのドキュメント

- 『*Cisco Unified Serviceability Administration Guide*』
- 『*Administration Guide for Cisco Unified Communications Manager*』
- HTTPS で入手可能な Microsoft のドキュメンテーション