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 ユーザのために、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。

- Microsoft Internet Explorer（IE）7（Microsoft Windows XP SP3 で実行されている場合）
- Microsoft Internet Explorer（IE）8（Microsoft Windows XP SP3 または Microsoft Vista SP2 で実行されている場合）
- Firefox 3.x（Microsoft Windows XP SP3、Microsoft Vista SP2、または Apple MAC OS X で実行されている場合）
- Safari 4.x（Apple MAC OS X で実行されている場合）

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

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 Administration Guide*』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
ccmadmin	Cisco Unified Communications Manager の管理
ccmservice	Cisco Unified サービスアビリティ
cmplatform	オペレーティング システムの管理
cmuser	Cisco Personal Assistant
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	障害復旧システム
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。

Cisco Unified IP Phone サービスでの HTTPS

リリース 8.0 よりも前の Cisco Unified Communications Manager では、Cisco Unified IP Phone および Cisco Unified IP Phone サービスで HTTPS 通信がサポートされておらず、ポート 8080 で「クリア テキスト」を使用して通信が行われていました。

Cisco Unified Communications Manager リリース 8.0 では、Cisco Unified IP Phone および Cisco Unified IP Phone サービスで、HTTPS、暗号化、およびポート 8443 によるサーバの安全な識別がサポートされています。

サポートされるデバイス

HTTPS をサポートしている Cisco Unified IP Phone は、次のとおりです。

- 7906
- 7911
- 7931
- 7941
- 7961
- 7970
- 7942
- 7945
- 7962
- 7965
- 7975

サポートされる機能

HTTPS をサポートしている機能は、次のとおりです。

- Cisco Extension Mobility（EM; エクステンション モビリティ）
- Cisco Extension Mobility Cross Cluster（EMCC; クラスタ間のエクステンション モビリティ）
- Cisco Unified Communications Manager の Manager Assistant（IPMA）
- Cisco IP Phone サービス
- パーソナル ディレクトリ
- クレデンシャル変更

IP Phone サービスの設定内容

Cisco Unified Communications Manager リリース 8.0(1) では、HTTPS をサポートするために、電話機の設定内容に表 2-2 に示すセキュア URL パラメータが含まれています。

セキュア URL パラメータを設定するには、Cisco Unified Communications Manager の管理ページから [デバイス (Device)] > [デバイスの設定 (Device Settings)] > [IP Phone サービス (Phone Services)] の順に選択します。詳細については、『*Cisco Unified Communications Manager アドミニストレーション ガイド*』の「IP Phone サービスの設定」の章を参照してください。

表 2-2　セキュア URL 用の電話機の設定内容

フィールド	説明
[セキュア認証 URL (Secure Authentication URL)]	電話機の Web サーバに対する要求を検証するために、この電話機が使用するセキュア URL を入力します。 **（注）** [セキュア認証 URL (Secure Authentication URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルトでは、この URL は、インストール時に設定された [Cisco Unified CM のユーザ オプション (Cisco Unified CM User Options)] ウィンドウにアクセスします。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 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となるサーバのセキュア URL を入力します。このパラメータには、ディレクトリ ボタンを押したときに、セキュリティで保護された Cisco Unified IP Phone が使用する URL を指定します。 **（注）** [セキュアディレクトリ URL (Secure Directory URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255

表 2-2　セキュア URL 用の電話機の設定内容 （続き）

フィールド	説明
[セキュアアイドル URL (Secure Idle URL)]	[アイドルタイマー (Idle Timer、秒)] フィールドの指定に従って電話機がアイドル状態になったときに、Cisco Unified IP Phone のディスプレイに表示する情報のセキュア URL を入力します。たとえば、電話機が 5 分間使用されなかったときに、LCD 上にロゴを表示できます。 **（注）** [セキュアアイドル URL (Secure Idle URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255
[セキュア情報 URL(Secure Information URL)]	Cisco Unified IP Phone がヘルプ テキスト情報を検索できるサーバの場所を示すセキュア URL を入力します。この情報は、ユーザが情報（[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 (Secure Information URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255

表 2-2　セキュア URL 用の電話機の設定内容 （続き）

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。ユーザがメッセージ ボタンを押すと、Cisco Unified IP Phone はこの URL に接続されます。 （注）[セキュアメッセージURL (Secure Messages URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255
[セキュアサービス URL (Secure Services URL)]	Cisco Unified IP Phone サービスのセキュア URL を入力します。これは、ユーザがサービス ボタンを押すと、セキュリティ保護された Cisco Unified IP Phone が接続される場所です。 （注）[セキュアサービス URL (Secure Services URL)] の値を指定しないと、デバイスでは非セキュア URL が使用されます。セキュア URL と非セキュア URL の両方を指定した場合、デバイスではデバイスの持つ機能に応じて適切な URL が選択されます。 デフォルト値を受け入れるには、このフィールドをブランクのままにします。 最大長：255

エンタープライズ パラメータの設定内容

HTTPS をサポートするために、Cisco Unified Communications Manager リリース 8.0(1) では次の新しいエンタープライズ パラメータをサポートしています。

- Secured Authentication URL
- Secured Directory URL
- Secured Idle URL
- Secured Information URL
- Secured Messaged 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方法

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 8 にインポートします。証明書の警告が表示された Web サイトへのアクセスを続行する場合、その証明書が信頼ストアに存在しないときは、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 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。

Internet Explorer 8 のルート証明書信頼ストアに Cisco Unified Communications Manager 証明書をインポートする手順は、次のとおりです。

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ました」というメッセージが表示されます。

ステップ 2　サーバにアクセスするには、[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。

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

「関連項目」（P.2-13）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　[証明書のエラー] ステータス ボックスをクリックします。

ステップ 2　[証明書の表示] をクリックします。

ステップ 3　[詳細設定] タブをクリックします。

ステップ 4　[ファイルにコピー] ボタンをクリックします。

ステップ 5　[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 6　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 7　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 8　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 9　ファイルと設定が表示されます。[終了] をクリックします。

ステップ 10　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

「関連項目」（P.2-13）を参照してください。

Firefox での 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警告の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。

- [危険性を理解した上で接続するには] をクリックして、現在の Web セッションに対してだけ証明書を信頼します。現在のセッションに対してだけ証明書を信頼すると、セキュリティ警告のダイアログボックスは、信頼できるフォルダに証明書をインストールするまで、アプリケーションにアクセスするたびに表示されます。
- [スタートページに戻る] 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、[危険性を理解した上で接続するには] をクリックする必要があります。

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

- 「Firefox 3.x 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.2-9）
- 「証明書のファイルへのコピー」（P.2-10）

Firefox 3.x 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　セキュリティ警告のダイアログボックスが表示されたら、[危険性を理解した上で接続するには] をクリックします。

ステップ 3　[例外を追加] をクリックします。

[セキュリティ例外の追加] ダイアログボックスが表示されます。

ステップ 4　[証明書を取得] をクリックします。

ステップ 5　[次回以降にもこの例外を有効にする] チェックボックスをオンにします。

ステップ 6　[セキュリティ例外を承認] をクリックします。

ステップ 7　証明書の詳細を表示するには、次の手順に従います。

a. Firefox ブラウザから、[ツール] > [オプション] をクリックします。

[オプション] ダイアログボックスが表示されます。

b. [詳細] をクリックします。

c. [証明書を表示] をクリックします。

[証明書マネージャ] 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て、[表示] をクリックします。

[証明書ビューア] ダイアログボックスが表示されます。

e. [詳細] タブをクリックします。

f. [証明書のフィールド] フィールドで、表示するフィールドを強調表示します。

[フィールドの値] フィールドに詳細が表示されます。

g. [証明書ビューア] ダイアログボックスで、[閉じる] をクリックします。

h. [証明書マネージャ] ダイアログボックスで、[OK] をクリックします。

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　Firefox ブラウザから、[ツール] > [オプション] をクリックします。

[オプション] ダイアログボックスが表示されます。

ステップ 2　まだ選択されていない場合は、[詳細] をクリックします。

ステップ 3　[暗号化] タブをクリックして、[証明書を表示] をクリックします。

[証明書マネージャ] ダイアログボックスが表示されます。

ステップ 4　[サーバ証明書] タブをクリックします。

ステップ 5　コピーする証明書を強調表示して、[エクスポート] をクリックします。

[証明書をファイルに保存] ダイアログボックスが表示されます。

ステップ 6　ファイルのコピー先に移動します。

ステップ 7　[ファイルの種類] ドロップダウン リストで、次のオプションからファイル タイプを選択します。

- [X.509 証明書（PEM）] : **PEM** を使用してエンティティ間で情報を転送します。
- [証明書パスを含む X.509 証明書（PEM）] : プライバシー エンハンスト 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 証明書（DER）] : **DER** を使用してエンティティ間で情報を転送します。
- [X.509 証明書（PKCS#7）] : PKCS#7 は、データの署名または暗号化の標準です。署名されたデータの検証に必要になるため、証明書を SignedData 構造に含めることができます。.P7C ファイルは、署名が必要なデータを持たない縮退した SignedData 構造です。
- [証明書パスを含む X.509 証明書（PKCS#7）] : PKCS#7 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。

ステップ 8　[保存] をクリックします。

ステップ 9　[OK] をクリックします。

追加情報

「関連項目」（P.2-13）を参照してください。

Safari での 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対してだけ証明書を信頼すると、[セキュリティの警告] ダイアログボックスは、信頼できるフォルダに証明書をインストールするまで、アプリケーションにアクセスするたびに表示されます。
- [証明書を表示] > [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 [証明書を表示] > [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、Safari で HTTPS を使用する方法について説明します。

- 「Safari 4 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.2-11）
- 「証明書のファイルへのコピー」（P.2-12）

Safari 4 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、[証明書を表示] 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] 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] 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　[完了] 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拇印が表示されます。

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。

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、[証明書を表示] をクリックします。

ヒント　Safari 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、[証明書を表示] オプションを表示します。

ステップ 2　[詳細] 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 証明書 (.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。[終了] 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

「関連項目」（P.2-13）を参照してください。

参考情報

関連項目

「証明書」（P.1-15）

シスコの関連マニュアル

- 『*Cisco Unified Serviceability Administration Guide*』
- 『*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