Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）

この章では、Hypertext Transfer Protocol Over Secure Sockets Layer（HTTPS）について説明します。

HTTPS

Secure Sockets Layer（SSL）での HTTPS または Hypertext Transfer Protocol は、Microsoft Windows ユーザ向けにブラウザと Web サーバの間の通信をセキュアにします。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 では、ユーザ ログインやパスワードなどのインターネット経由での伝送中に、公開キーでデータを暗号化します。

Cisco Unified Communications Manager は、HTTPS 接続の SSL およびトランスポート レイヤ セキュリティ（TLS）をサポートしています。ご使用の Web ブラウザ バージョンが TLS をサポートしている場合、TLS の使用を推奨します。TLS を使用して HTTPS 通信をセキュアにするには、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のセキュリティを確保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を保存します。

Cisco Unified Communications Manager での Cisco Tomcat ウェブ 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 上で実行している場合は、Microsoft Internet Explorer（IE）7
- Microsoft Windows XP SP3 または Microsoft Vista SP2 上で実行している場合は、Microsoft Internet Explorer（IE）8
- Microsoft Windows XP SP3、Microsoft Vista SP2 または Apple MAC OS X 上で実行している場合は、Firefox 3.x
- Apple MAC OS X 上で実行している場合は、Safari 4.x

（注） Cisco Unified Communications Manager をインストール/更新すると、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、Cisco Unified Communications Manager へのアップグレードの間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 フォーマットで作成されます。

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。

Cisco Unified Communications Manager において Cisco Tomcat による 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*：*Cisco Unified Communications Manager HTTPS* アプリケーション

Cisco Unified Communications Manager HTTPS アプリケーション	**Web アプリケーション**
ccmadmin	Cisco Unified CM の管理
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
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	Cisco Unified Communications Manager CDR Analysis and Reporting
taps	Cisco Unified Communications Manager Auto-Register Phone Tool

Cisco Unified Communications Manager HTTPS アプリケーション	Web アプリケーション
dna	Dialed Number Analyzer
drf	Disaster Recovery System
SOAP	Cisco 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、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。HTTP による SOAP アプリケーションの使用はサポートされていません。HTTP を使用する既存アプリケーションは実行に失敗します。ディレクトリ変更によって HTTPS に変換することはできません。

Cisco Unified IP Phone サービスの HTTPS

Cisco Unified Communications Manager、Cisco Unified IP Phone、および Cisco Unified IP Phone 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。

TVS（信頼検証サービス）において、証明書チェーンは確認されません。TVS が証明書を確認するためには、電話によって TVS に提示されるのと同じ証明書が Tomcat 信頼証明書ストア内に存在する必要があります。

TVS では、ルート証明書や中間証明書は確認されません。アイデンティティ証明書のみ、データベースに存在しない場合に確認されます。ルート証明書および中間証明書が提示された場合でも、検証は失敗します。

HTTPS をサポートする Cisco Unified IP Phone

次の Cisco Unified IP Phone 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、7921、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） このリストの 69xx 電話は、HTTPS クライアントとして動作可能ですが、HTTPS サーバとしての動作はできません。このリスト内の残りの電話は、HTTPS クライアントまたは HTTPS サーバとして動作可能です。

HTTPS をサポートする機能

次の機能で HTTPS がサポートされています。

- Cisco Extension Mobility（EM）
- Cisco Extension Mobility Cross Cluster（EMCC）
- Cisco Unified Communications Manager Manager Assistant（IPMA）
- Cisco Unified IP Phone 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 Phone サービス設定

Cisco 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構成時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、Cisco Unified Communications Manager Administration から [Device（デバイス）] > [Device Settings（デバイスの設定）] > [Phone Services（電話サービス）] 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 Parameters）] セクションで Secured Phone URL パラメータを削除してリブートすると、デフォルトで URL パラメータが再度読み込まれます。リブートの後、[セキュア電話の URL パラメータ（Secured Phone URL Parameters）] セクションに移動し、正しい URL に変更して電話を再起動します。

表 *2*：セキュア ***URL*** の電話構成時の設定

フィールド	説明
セキュア認証 URL（Secured 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されるセキュア 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。 デフォルトでは、この URL はインストール中に設定された [Cisco Unified Communications セルフケアポータル（Cisco Unified Communications Self Care Portal）] ウィンドウにアクセスします。 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 ディレクトリ URL（Secured Directory URL）	電話機のディレクトリ情報の取得元となるサーバの URL を入力します。このパラメータには、ユーザが Directory ボタンを押下したときにセキュアな 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 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 アイドル URL（Secured Idle URL）	電話機が [アイドル タイマー（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 Unified IP Phone に表示される情報のセキュア URL を入力します。たとえば、電話機が 5 分間使用されなかったときに、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（Secured Information URL）	Cisco Unified IP Phone 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ボタン（i）またはヘルプ ボタン（?）ボタンを押下したときに表示されます。 （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（Secured 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下すると、Cisco Unified IP Phone 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 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 ボタンを押下したときにセキュア Cisco Unified IP Phone がアクセスする場所になります。 （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、Cisco 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）]
- [セキュア メッセージ URL（Secured Messages 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

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、Cisco 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。このセキュリティの警告は、ブラウザの信頼ルート認証局の信頼できるストアにインポートされた証明書が含まれている場合には無視できます。

次の手順では、Internet Explorer 8 のルート証明書の信頼ストアに Cisco 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

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、Cisco 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：ナビゲーションがブロックされました（Certificate Error: Navigation Blocked）」というメッセージが表示されます。これはこの Web サイトは信頼できないことを示しています。

ステップ 2 サーバにアクセスするには、[この Web サイトへのアクセスを続行(推奨しません)（Continue to this website (not recommended)）] をクリックします。
[Cisco Unified Communications Manager の管理（Cisco 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。

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（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 [証明書の表示（View Certificates）] 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（Certificate）] ウィンドウで [一般（General）] タブを選択し、[証明書のインストール（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。

ステップ 6 ウィザードを起動するには、[次へ（Next）] をクリックします。
[証明書ストア（Certificate Store）] ウィンドウが表示されます。

ステップ 7 [自動（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。[次へ（Next）] をクリックしてください。

ステップ 8 設定を確認し、[完了（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。

ステップ 9 証明書をインストールするには、[はい（Yes）] をクリックします。
インポート ウィザードに「インポートが成功しました。（The import was successful.）」と表示されます。

ステップ 10 [OK] をクリックします。[証明書の表示（View Certificates）] リンクを次にクリックしたときには、[証明書（Certificate）] ウィンドウの [認証パス（Certification Path）] タブに「この証明書は問題ありません。（This certificate is OK.）」と表示されます。

ステップ 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 [ツール（Tools）] > [インターネット オプション（Internet Options）] をクリックして、[コンテンツ（Content）] タブを選択します。[証明書（Certificates）] をクリックして、[信頼されたルート証明機関（Trusted Root Certifications Authorities）] タブを選択します。インポートした証明書が見つ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, （16 ページ）

Internet Explorer 8 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、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。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（Certificate Error）] ステータス ボックスをクリックします。

ステップ 2 [証明書を表示（View Certificate）] をクリックします。

ステップ 3 [詳細（Details）] タブをクリックします。

ステップ 4 [ファイルにコピー（Copy to File）] 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（Certificate Export Wizard）] が表示されます。[Next] をクリックします。

ステップ 6 次のリストに、選択可能なファイル形式を定義しています。エクスポートするファイルに使用するファイル形式を選択し、[次へ（Next）] をクリックします。

a) DER エンコードされたバイナリ X.509（.CER）（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 エンコードされた X.509（.CER）（Base-64 encoded X.509 (.CER)）：バイナリ添付ファイルをインターネット上でセキュアに送信できます。ファイルの文字化けを防ぐため、ASCII テキスト形式を使用します。

c) PKCS #7 証明書（.P7B）（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。

ステップ 7 ファイルのコピーをエクスポートし、ファイル名を設定する場所を参照します。[保存（Save）] をクリックします。

ステップ 8 ファイル名とパスは [証明書エクスポート（Certificate Export）] ウィザードのペインに表示されます。[Next] 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（Finish）] をクリックします。

ステップ 10 エクスポートの成功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。

関連トピック

HTTPS 設定に関する詳細情報の入手先, （16 ページ）

HTTPS による Firefox での初回の認証

Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）や、SSL を使った Cisco Unified Communications Manager の他の仮想ディレクトリ（Cisco Unified Communications Manager のインストール、アップグレード後）をブラウザ クライアントから最初にアクセスした時、サーバを信頼するか尋ねるセキュリティ警告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。

- [リスクを承知の上で信頼（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。

- [ここから出る（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、[リスクを承知の上で信頼（I Understand The Risks）] をクリックします。

関連トピック

Internet Explorer 8 証明書のファイルへのコピー, （9 ページ）
Safari 4.x を使用して証明書を信頼できるフォルダに保存, （14 ページ）

Firefox 3.x を使用して証明書を信頼できるフォルダに保

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、Cisco 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）。

ステップ 2 表示される [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たら、[リスクを承知の上で進む（I Understand The Risks）] をクリックします。

ステップ 3 [例外の追加（Add Exception）] をクリックします。
[例外の追加（Add Exception）] ダイアログボックスが表示されます。

ステップ 4 [証明書の取得（Get Certificate）] 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（Permanently store this exception）] 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（Confirm Security Exception）] をクリックします。

ステップ 7 次の手順を実行して証明書の詳細を表示します。

a) Firefox のブラウザで [ツール（Tools）] > [オプション（Options）] をクリックします。
[オプション（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) [証明書を表示（View Certificate）] をクリックします。
[証明書マネージャ（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て [表示（View）] をクリックします。
[証明書ビューア（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) [証明書のフィールド（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。

詳細は [フィールドの値（Field Values）] フィールドに表示されます。

g) [証明書ビューア（Certificate Viewer ）] ダイアログボックスで [閉じる（Close）] をクリックします。

h) [証明書ビューア（Certificate Viewer ）] ダイアログボックスで [OK] をクリックします。

Firefox 3.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、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。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 のブラウザで [ツール（Tools）] > [オプション（Options）] をクリックします。
[オプション（Options）] ダイアログボックスが表示されます。

ステップ 2 選択されていなければ、[詳細（Advanced）] をクリックします。

ステップ 3 [セキュリティ（Security）] タブをクリックし、[証明書を表示（View Certificates）] をクリックします。
[証明書マネージャ（Certificate Manager）] ダイアログボックスが表示されます。

ステップ 4 [サーバ（Servers）] 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（Export）] をクリックします。
[証明書をファイルに保存（Save Certificate to File）] ダイアログボックスが表示されます。

ステップ 6 ファイルをコピーする場所に移動します。

ステップ 7 [タイプを変更して保存（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 証明書（PEM）（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) チェーンを含む X.509 証明書（PEM）（X.509 Certificate with chain (PEM)）：証明書チェーンを検証し、エンティティ間で情報を転送するために、プライバシー強化メール（Privacy Enhanced Mail）を使用します。

- X.509 証明書（DER）（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 証明書（PKCS#7）（X.509 Certificate (PKCS#7)）：PKCS#7 は署名、データ暗号化のための標準規格です。署名されたデータを確認するには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。

- チェーンを含む X.509 証明書（PKCS#7）（X.509 Certificate with chain (PKCS#7)）：証明書チェーンを検証し、エンティティ間で情報を転送するために、PKCS#7 を使用します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 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, （16 ページ）

HTTPS による Safari での初回の認証

Cisco Unified Communications Manager の管理（Cisco Unified Communications Manager Administration）や、SSL を使った Cisco Unified Communications Manager の他の仮想ディレクトリ（Cisco Unified Communications Manager のインストール、アップグレード後）をブラウザ クライアントから最初にアクセスした時、サーバを信頼するか尋ねるセキュリティ警告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。

- [はい（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。
- [証明書の表示（Show Certificate）] > [証明書のインストール（Install Certificate）] をクリックして、証明書のインストールのタスクを実行し、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。
- [いいえ（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、[はい（Yes）] をクリックするか、または[証明書の表示（Show Certificate）] > [証明書のインストール（Install Certificate）] の順にクリック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ある名前と一致する必要があります。そうでない場合、デフォルトでは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した場合、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 証明書のファイルへのコピー, （9 ページ）
Firefox 3.x を使用して証明書を信頼できるフォルダに保, （11 ページ）

Safari 4.x を使用して証明書を信頼できるフォルダに保存

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（Security Alert）] ダイアログボックスが表示されたら、[証明書を表示（Show Certificate）] 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（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）、次のオプションのいずれか 1 つを選択します。

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（Version 1 Fields Only）]：[バージョン（Version）]、[シリアル番号（Serial Number）]、[署名アルゴリズム（Signature Algorithm）]、[発行者（Issuer）]、[有効期間の開始（Valid From）]、[有効期間の終了（Valid To）]、[サブジェクト（Subject）]、および [公開キー（Public Key）] の各オプションが表示されます。
c) [拡張機能のみ（Extensions Only）]：[サブジェクトキー識別子（Subject Key Identifier）]、[キー使用法（Key Usage）]、および [拡張キー使用法（Enhanced Key Usage）] の各オプションが表示されます。
d) [重要な拡張機能のみ（Critical Extensions Only）]：存在する場合は [重要な拡張機能（Critical Extensions）] が表示されます。
e) [プロパティのみ（Properties Only）]：[拇印アルゴリズム（Thumbprint algorithm）] と [拇印（Thumbprint）] オプションが表示されます。

ステップ 3 [証明書（Certificate）] ペインの [証明書のインストール（Install Certificate）] 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（Certificate Import Wizard）] が表示されたら、[次へ（Next）] 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（Place all certificates in the following store）] オプション ボタンをクリックし、[参照（Browse）] 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（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 [終了（Finish）] をクリックします。

[セキュリティ警告（Security Warning）] ボックスに証明書の拇印が表示されます。

ステップ 9 証明書をインストールするには、[はい（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。

ステップ 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。

ステップ 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、[はい（Yes）] をクリックします。

ヒント [証明書（Certificate）] ペインの [証明のパス（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。

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、ローカルに保存しておけば、必要な時にいつでも証明書を復元できます。

次の手順を実行することで、標準の証明書保管形式で証明書をコピーできます。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 アラート（Security Alert）] ダイアログボックスで、[証明書の表示（Show Certificate）] をクリックします。

ヒント Safari で、[証明書エラー（Certificate Error）] ステータス ボックスをクリックして、[証明書の表示（Show Certificate）] オプションを表示します。

ステップ 2 [詳細（Details）] タブをクリックします。

ステップ 3 [ファイルにコピー（Copy to File）] 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（Certificate Export Wizard）] が表示されます。[Next] をクリックします。

ステップ 5 次のリストに、選択可能なファイル形式を定義しています。エクスポートするファイルに使用するファイル形式を選択し、[次へ（Next）] をクリックします。

a) DER エンコードされたバイナリ X.509（.CER）（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 エンコードされた X.509（.CER）（Base-64 encoded X.509 (.CER)）：バイナリ添付ファイルをインターネット上でセキュアに送信できます。ファイルの文字化けを防ぐため、ASCII テキスト形式を使用します。

c) PKCS #7 証明書（.P7B）（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。

ステップ 6 ファイルのコピーをエクスポートし、ファイル名を設定する場所を参照します。[保存（Save）] をクリックします。

ステップ 7 ファイル名とパスは [証明書エクスポート（Certificate Export）] ウィザードのペインに表示されます。[次へ（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。[終了（Finish）] をクリックします。

ステップ 9 エクスポートの成功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。

関連トピック

HTTPS 設定に関する詳細情報の入手先, （16 ページ）

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 に関して利用可能な Microsoft のドキュメント