CHAPTER 1

概要

Cisco Unified Communications Manager（以前は Cisco Unified CallManager）は、コールを処理するためのソフトウェア ベースのコンポーネントであり、Cisco Unified Communications ファミリの製品です。さまざまなタイプの Cisco Media Convergence Server が、Cisco Unified Communications Manager のコール処理、サービス、およびアプリケーションに対して可用性の高いサーバ プラットフォームを提供します。

Cisco Unified Communications Manager システムは、企業のテレフォニー機能をパケット テレフォニー デバイスまで拡張して、たとえば、IP Phone、メディア処理デバイス、Voice-over-IP（VoIP）ゲートウェイ、マルチメディア アプリケーションなどを提供します。その他にも、統合メッセージング、マルチメディア会議、コラボレーション連絡センター、対話型マルチメディア応答システムなどで使用されるデータ、音声、ビデオの各サービスでは、オープン型の Cisco Unified Communications Manager テレフォニー API を利用してサービス間の情報を交換することが可能になります。

Cisco Unified Communications Manager は、Cisco 統合テレフォニー アプリケーションおよびサードパーティ アプリケーションに対して、シグナリングとコール制御のサービスを提供します。Cisco Unified Communications Manager の主な機能は、次のとおりです。

- コール処理
- シグナリングとデバイス制御
- ダイヤル プランの管理
- 電話機能の管理
- ディレクトリ サービス
- Operations, administration, management, and provisioning（OAM&P; 操作、アドミニストレーション、管理、およびプロビジョニング）
- Cisco IP Communicator や Cisco Unified IP Interactive Voice Response（IP IVR）などの外部音声処理アプリケーションに対するプログラミング インターフェイス

追加情報

「関連項目」（P.1-17）を参照してください。

主な機能と利点

Cisco Unified Communications Manager システムには、音声会議と WebAttendant 機能を利用するのに必要な一連の統合音声アプリケーションが組み込まれています。音声アプリケーションが組み込まれているため、音声処理用に特別のハードウェアは必要ありません。保留、任意転送、自動転送、会議、複数ライン アピアランス、自動ルート選択、スピード ダイヤル、前回かけた番号のリダイヤルなどの補助的な拡張サービスが、IP Phone とゲートウェイに付加されます。Cisco Unified Communications Manager はソフトウェア アプリケーションなので、実稼動環境で機能を拡張するには、サーバ プラットフォーム上でソフトウェアをアップグレードするだけで済み、高価なハードウェアのアップグレード費用が不要になります。

Cisco Unified Communications Manager は、すべての Cisco Unified IP Phone、ゲートウェイ、アプリケーションと IP ネットワーク全体に配備が可能なため、分散型のバーチャル テレフォニー ネットワークを構築することができます。このアーキテクチャにより、システムのアベイラビリティとスケーラビリティが向上します。コール アドミッション制御により、帯域幅に制約のある WAN リンク内での音声 Quality of Service（QoS; サービス品質）が保証され、WAN 帯域幅が十分でないときには別の Public Switched Telephone Network（PSTN; 公衆電話交換網）にコールが自動転送されます。

Cisco Unified Communications Manager 設定データベースへのインターフェイスは通常の Web ブラウザを使用しているので、リモート デバイスとリモート システムの設定機能も提供しています。ユーザおよび管理者は、このインターフェイスを使用して HTML ベースのオンライン ヘルプにアクセスすることができます。

アプライアンスと同様に動作するように設計された Cisco Unified Communications Manager は、次の機能を備えています。

- Cisco Unified Communications Manager サーバは、お客様やパートナーがサーバを配置しやすいように、ソフトウェアと共に事前にインストールされた状態で入手できます。このサーバはアップデートを自動的に検索し、システムに対する重要なセキュリティ修正やソフトウェア アップグレードが使用可能になると、管理者に自動的に通知することができます。このプロセスは、Electronic Software Upgrade Notification と呼ばれます。
- Cisco Unified Communications Manager サーバは、コールの処理を続けたままアップグレードすることができるため、アップグレードは最小限のダウンタイムで完了します。
- Cisco Unified Communications Manager は高解像度の電話ディスプレイ上で Unicode をサポートしているため、アジアおよび中東地域での使用をサポートしています。
- Cisco Unified Communications Manager は、Fault, Configuration, Accounting, Performance, and Security（FCAPS; 障害、構成、課金、パフォーマンス、およびセキュリティ）を提供します。

追加情報

「関連項目」（P.1-17）を参照してください。

Cisco Unified Communications Manager の管理ページの参照

Cisco Unified Communications Manager の管理プログラムには、Web サーバとなっていない PC、または Cisco Unified Communications Manager がインストールされていない PC からアクセスします。Cisco Unified Communications Manager の管理ページのサーバ上には、ブラウザ ソフトウェアはありません。サーバの参照の詳細については、「Web ブラウザ」（P.1-3）を参照してください。

追加情報

「関連項目」（P.1-17）を参照してください。

Web ブラウザ

Cisco Unified Communications Manager の管理は、次のオペレーティング システム ブラウザをサポートしています。

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

ネットワーク内の任意のユーザ PC から、Cisco Unified Communications Manager の管理ページを実行しているサーバを参照し、管理特権でログインします。

（注） 多数のユーザが同時に Cisco Unified Communications Manager の管理ページにログインすると、パフォーマンスが低下する場合があります。同時にログインするユーザおよび管理者の数は制限してください。

（注） Cisco Unified Communications Manager の管理ページは、ブラウザのボタンをサポートしていません。設定作業を行うときは、ブラウザ ボタン（[戻る] ボタンなど）を使用しないでください。

追加情報

「関連項目」（P.1-17）を参照してください。

Cisco Unified Communications Manager の管理ページへのログイン

Cisco Unified Communications Manager の管理ページにログインする手順を下記に示します。Cisco Unified Communications Manager の管理ページにログインすると、Cisco Unified Communications Manager 用ライセンスの現在の状態を示すメッセージがメイン ウィンドウに表示されることがあります。たとえば、Cisco Unified Communications Manager は次のような状況を識別します。

- Cisco Unified Communications Manager は現在、スターター（デモ）ライセンスで動作しているので、適切なライセンス ファイルをアップロードしてください。
- Cisco Unified Communications Manager は現在、不十分なライセンス数で動作しているので、追加のライセンス ファイルをアップロードしてください。
- Cisco Unified Communications Manager は現在、正しいソフトウェア機能ライセンスを使用していません。この場合、Cisco CallManager サービスは停止し、適切なソフトウェア バージョン ライセンスをアップロードして Cisco CallManager サービスを再起動するまで開始しません。

手順

サーバを参照して Cisco Unified Communications Manager の管理ページにログインする手順は、次のとおりです。

ステップ 1　適当なオペレーティング システム ブラウザを起動します。

ステップ 2　Web ブラウザのアドレスバーに次の URL を入力します。大文字と小文字は区別してください。

https://<*Unified CM-server-name*>:{8443}/ccmadmin/showHome.do

<*Unified CM-server-name*> はサーバの名前または IP アドレスです。

（注）　ポート番号を指定することもできます。

ステップ 3　[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。適切なボタンをクリックします。

ステップ 4　Cisco Unified Communications Manager の管理ページのメイン ウィンドウで、Cisco Unified Communications Manager のインストール時に指定したユーザ名とパスワードを入力し、[ログイン(Login)] をクリックします。

（注）　セキュリティを維持するために、非アクティビティ状態が 30 分続くと、ユーザは Cisco Unified Communications Manager の管理ページからログアウトされます。この場合、もう一度ログインする必要があります。

追加情報

「関連項目」（P.1-17）を参照してください。

Cisco Unified Communications Manager の管理ページからのログオフ

手順

Cisco Unified Communications Manager の管理ページからログオフする手順は、次のとおりです。

ステップ 1　Cisco Unified Communications Manager の管理ページのメイン ウィンドウで、右上にある [ログアウト(Logout)] ボタンをクリックします。

ステップ 2　ログイン フィールドのあるウィンドウが再表示されます。

追加情報

「関連項目」（P.1-17）を参照してください。

Secure Sockets Layer 上のハイパーテキスト転送プロトコル（HTTPS）

Hypertext Transfer Protocol over Secure Sockets Layer（HTTPS; HTTP over SSL）は、Microsoft Windows ユーザのブラウザと Web サーバ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。また、インターネット上でデータ（ユーザ ログインとパスワードなど）を転送する際には、公開鍵を使用してデータを暗号化します。

HTTPS を有効にするには、接続の処理中に、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。サーバ証明書は、現在のセッションに対してだけ受け入れるか、または信頼できるフォルダ（ファイル）にダウンロードして当該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ことができます。信頼できるフォルダには、信頼できるすべてのサイトの証明書が格納されます。

Cisco Unified Communications Manager の管理ページ、Cisco Unity Connection の管理、Cisco Unified サービスアビリティ、Cisco Unified CM のユーザ オプション ページ、トレース収集ツール、Real-Time Monitoring Tool（RTMT）、および XML（AXL）アプリケーション プログラミング インターフェイスの各 Cisco Unified Communications Manager アプリケーションは、HTTPS をサポートしています。

自己署名証明書は、インストール時に Web サーバ上で生成されます（この証明書は、アップグレード時にも移行されます）。

追加情報

「関連項目」（P.1-17）を参照してください。

Internet Explorer 7、HTTPS と Cisco Unified Communications Manager の管理の使用

Internet Explorer（IE）7 では、追加されたセキュリティ機能により、ブラウザで Web サイトへのアクセス時にシスコ証明書を処理する方法を変更できます。シスコでは Cisco Unified Communications Manager サーバ向けに自己署名証明書を提供しているため、Internet Explorer 7 は、Cisco Unified Communications Manager の管理ページ Web サイトを信頼されていないものとしてフラグ設定し、証明書エラーを表示します。この処理は、信頼ストアにサーバ証明書が格納されている場合でも行われます。

（注）　Cisco Unified Communications Manager の管理は、Microsoft Windows XP SP3 で実行されている場合には IE 7 をサポートします。

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アクセスが保護されるようにするために、必ず Cisco Unified Communications Manager 証明書を Internet Explorer 7 にインポートしてください。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 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た後も、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の証明書が表示される場合は、セキュリティの警告を無視できます。

Internet Explorer 7 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 サーバ上のアプリケーションを参照します（たとえば、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 アドレスをブラウザに入力します）。

[証明書エラー : ナビゲーションはブロックされました] ページがブラウザに表示され、この Web サイトが信頼されていないことが示されます。

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 (Cisco Unified Communications Manager Administration)] ウィンドウが表示され、ブラウザのアドレスバーと [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。レポート内の [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 CA ルート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] ウィンドウの [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　ウィザードを開始するには、[次へ] をクリックします。

[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（ウィザードにこの証明書の種類に基づいて証明書ストアを選択させる）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の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] をクリックします。

インポート ウィザードに「正しくインポートされました」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] リンクを次にクリックすると、[証明書] ウィンドウの [証明のパス] 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　信頼ストアにインポート済みの証明書が含まれていることを確認するには、Internet Explorer のツールバーで [ツール] > [インターネット オプション] の順にクリックし、[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、インポート済みの証明書を探します。

証明書をインポートした後も、引き続き、ブラウザのアドレスバーと [証明書のエラー] ステータスは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たり、ブラウザを更新または再起動したりしても、この状態は続きます。

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　次のリストからファイル形式を選択できます。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、[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、証明書の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。[完了] 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.1-17）を参照してください。

Internet Explorer 8、HTTPS と Cisco Unified Communications Manager の管理の使用

（注） Cisco Unified Communications Manager の管理は、Microsoft Windows XP SP3 または Microsoft Vista SP2 で実行されている場合には IE 8 をサポートします。

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アクセスが保護されるようにするために、必ず Cisco Unified Communications Manager 証明書を Internet Explorer 8 にインポートしてください。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の証明書が表示される場合は、セキュリティの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 (Cisco Unified Communications Manager Administration)] ウィンドウが表示され、ブラウザのアドレスバーと [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。レポート内の [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] ウィンドウの [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　ウィザードを開始するには、[次へ] をクリックします。

[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の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] をクリックします。

「正しくインポートされました」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、インポート済みの証明書を探します。

証明書をインポートした後も、引き続き、ブラウザのアドレスバーと [証明書のエラー] ステータスは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たり、ブラウザを更新または再起動したりしても、この状態は続きます。

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　次のリストからファイル形式を選択できます。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、[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、証明書の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。[完了] 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.1-17）を参照してください。

Firefox 3.x、HTTPS と Cisco Unified Communications Manager の管理の使用

（注） Cisco Unified Communications Manager の管理は、Microsoft Windows XP SP3、Microsoft Vista SP2、または Apple MAC OS X で実行されている場合には Firefox 3.x をサポートします。

（Cisco Unified Communications Manager のインストールまたはアップグレード後に）ブラウザ クライアントからシステム管理者（またはユーザ）が Cisco Unified Communications Manager の管理ページまたは他の Cisco Unified Communications Manager SSL が使用可能になっている仮想ディレクトリに初めてアクセスするときは、サーバを信頼するかどうかをたずね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を実行します。

- [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、アクションをキャンセルします。認証は行われず、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、[リスクがあることを理解しています] をクリックする必要があります。

Firefox 3.x 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 サーバにアクセスします（たとえば、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 アドレスをブラウザに入力します）。

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、[リスクがあることを理解しています] 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。

[例外を追加] 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、次の手順を実行します。

a. Firefox ブラウザで、[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、[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 ブラウザで、[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　まだ選択していない場合は、[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、[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、[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　ファイルをコピーする場所を参照します。

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の種類を選択します。

- [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、証明書チェーンを確認し、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 はデータに署名または暗号化するための標準です。署名入りデータの検証には証明書が必要になるため、SignedData 構造に証明書を含めることができます。.P7C ファイルは SignedData 構造を簡素化したもので、データへの署名が必要ありません。
- [証明書パスを含む X.509 証明書 (PKCS#7)] : PKCS#7 を使用して、証明書チェーンを確認し、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.1-17）を参照してください。

Safari 4.x、HTTPS と Cisco Unified Communications Manager の管理の使用

（注） Cisco Unified Communications Manager の管理は、Apple MAC OS X で実行されている場合には Safari 4.x をサポートします。

（Cisco Unified Communications Manager のインストールまたはアップグレード後に）ブラウザ クライアントからシステム管理者（またはユーザ）が Cisco Unified Communications Manager の管理ページまたは他の Cisco Unified Communications Manager SSL が使用可能になっている仮想ディレクトリに初めてアクセスするときは、サーバを信頼するかどうかをたずね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を実行します。

- [はい] 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。
- [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を実行し、その証明書を常に信頼します。信頼できるフォルダ内に証明書をインストールした場合、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、操作をキャンセルします。認証は行われず、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] 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で、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した場合は、セキュリティの警告が表示され、セキュリティ証明書の名前がアクセス先のサイトの名前と一致しないことが示されます。

Safari 4.x 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 サーバにアクセスします（たとえば、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 アドレスをブラウザに入力します）。

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] 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]、[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]、[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] : 重要な拡張機能が表示されます（存在する場合）。
- [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] ペインで、[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、選択してから [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] ダイアログボックスに、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] をクリックします。

インポートが正常に行われたことを知らせる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ある [OK] をクリックします。

ステップ 11　証明書を信頼し、このダイアログボックスを再び表示しない場合は、[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] タブをクリックすると、証明書が正しく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 で、[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] 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　次のリストからファイル形式を選択できます。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、[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、証明書の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

「関連項目」（P.1-17）を参照してください。

Cisco Unified Communications Manager の管理アプリケーションでの操作

ログインすると、Cisco Unified Communications Manager の管理ページのメイン ウィンドウが再表示されます。このウィンドウの右上には、[ナビゲーション (Navigation)] と呼ばれるドロップダウン リスト ボックスがあります。このドロップダウン リスト ボックスにあるアプリケーションにアクセスするには、必要なプログラムを選択し、[移動 (Go)] をクリックします。

（注）　サポートされている最小の画面解像度は 1024x768 です。これよりも画面解像度を小さくすると、デバイスにアプリケーションが正しく表示されない場合があります。

ドロップダウン リスト ボックスに表示されるオプションは、次の Cisco Unified Communications Manager アプリケーションです。

- [Cisco Unified Communications Manager の管理 (Cisco Unified Communications Manager Administration)]：Cisco Unified Communications Manager にアクセスしたときに、デフォルトとして表示されます。システム パラメータ、ルート プラン、デバイスなどを設定するには、Cisco Unified Communications Manager の管理ページを使用します。
- [Cisco Unified サービスアビリティ (Cisco Unified Serviceability)]：Cisco Unified サービスアビリティのメイン ウィンドウが表示されます。このアプリケーションは、トレース ファイルとアラームを設定し、サービスをアクティブまたは非アクティブにするために使用します。
- [Cisco Unified OS の管理 (Cisco Unified OS Administration)]：Cisco Unified OS の管理のメイン ウィンドウが表示され、Cisco Unified Communications Manager プラットフォームの設定と管理を行うことができます。このアプリケーションにログインするには、その前に他のすべてのアプリケーションからログオフする必要があります。
- [障害復旧システム (Disaster Recovery System)]：Cisco 障害復旧システムが表示されます。このプログラムは、Cisco Unified Communications Manager クラスタ内のすべてのサーバに対して、データの完全バックアップおよび復元機能を提供します。このアプリケーションにログインするには、その前に他のすべてのアプリケーションからログオフする必要があります。

Cisco Unified Communications Manager の管理ページにログインすると、各アプリケーションにログインすることなく、[ナビゲーション (Navigation)] ドロップダウン リスト ボックスに表示されるすべてのアプリケーションにアクセスできます。ただし、Cisco Unified オペレーティング システムの管理ページおよび障害復旧システムを除きます。Cisco Unified オペレーティング システムの管理ページまたは障害復旧システムの GUI には、Cisco Unified Communications Manager の管理ページへのアクセスに使用したものと同じユーザ名とパスワードではアクセスできません。これらのアプリケーションに Cisco Unified Communications Manager の管理ページからアクセスするには、[Cisco Unified Communications Manager の管理 (Cisco Unified Communications Manager Administration)] ウィンドウの右上にある [ログアウト (Logout)] ボタンをクリックしてから [ナビゲーション (Navigation)] ドロップダウン リスト ボックスでアプリケーションを選択し、[移動 (Go)] をクリックします。

[ナビゲーション (Navigation)] ドロップダウン リスト ボックスに表示されるいずれかのアプリケーション（Cisco Unified オペレーティング システムの管理ページまたは障害復旧システムを除く）にログイン済みの場合は、ログインすることなく Cisco Unified Communications Manager の管理ページにアクセスできます。それには、[ナビゲーション (Navigation)] ドロップダウン リスト ボックスから [Cisco Unified Communications Manager の管理 (Cisco Unified Communications Manager Administration)] を選択し、[移動 (Go)] をクリックします。

追加情報

「関連項目」（P.1-17）を参照してください。

Cisco Unified Presence サーバ リンク

Cisco Unified Presence サーバを設定した場合、Cisco Unified Communications Manager の管理ページのメイン ウィンドウには、関連付けられた Cisco Unified Presence サーバへの直接的なリンクが表示されます。Cisco Unified Presence の管理ページにアクセスするには、Cisco Unified Presence のアドレス リンクをクリックします。

追加情報

「関連項目」（P.1-17）を参照してください。

Cisco Unified Presence サーバへのリンク

Cisco Unified Presence サーバを Cisco Unified Communications Manager クラスタの一部として設定した場合、Cisco Unified Communications Manager の管理ページのメイン ウィンドウには Cisco Unified Presence パブリッシャ サーバへのリンクが表示されます。

Cisco Unified Presence の管理ページにアクセスするには、Cisco Unified Presence パブリッシャ サーバへのリンクをクリックします。

追加情報

「関連項目」（P.1-17）を参照してください。

カスタム ログイン メッセージ

Cisco Unified Communications Manager の管理ページのメイン ウィンドウに表示されるカスタム ログイン メッセージを含むテキスト ファイルをアップロードすることができます。

カスタム ログイン メッセージのアップロードの詳細と手順については、『*Cisco Unified Communications Operating System Administration Guide*』を参照してください。

追加情報

「関連項目」（P.1-17）を参照してください。

最後に成功したログインに関するメッセージ

Cisco Unified Communications Manager の管理ページにログインすると、システム ログインが最後に成功した日付と時刻が Cisco Unified Communications Manager の管理ページのメイン ウィンドウに表示されます。

Cisco Unified Communications Manager への最初のログイン時には、最後に成功したログイン時刻として現在の時刻が表示されます。

追加情報

「関連項目」（P.1-17）を参照してください。

アクセシビリティ

Cisco Unified Communications Manager の管理ページおよび Cisco Unified CM のユーザ オプション ページは、マウスを使用しなくてもウィンドウ上のボタンにアクセスできる機能を備えています。ウィンドウ上のどの位置でも次の手順を実行できるため、さまざまなフィールドを移動するときに、スクロールしたり Tab キーを押したりする必要はありません。

ウィンドウにあるアイコンへのアクセス

Cisco Unified Communications Manager の多くのウィンドウには、ウィンドウの一番上にアイコンがあります。たとえば、保存を実行するためのディスクのアイコン、追加を実行するためのプラス記号（+）のアイコンなどです。これらのアイコンにアクセスする手順は、次のとおりです。

1. **Alt** キーを押し、**1** キーを押して、**Tab** キーを押します。左側の最初のアイコンが強調表示されます。次のアイコンに移動するには、もう一度 **Tab** キーを押します。
2. **Enter** キーを押します。アイコンが表している機能（追加など）が実行されます。

ウィンドウにあるボタンへのアクセス

Cisco Unified Communications Manager と Cisco PCA の多くのウィンドウには、ウィンドウの一番下にボタンがあります。たとえば、保存のボタンや追加のボタンなどです。これらのボタンにアクセスする手順は、次のとおりです。

1. **Alt** キーを押し、**2** キーを押して、**Tab** キーを押します。左側の最初のボタンが強調表示されます。次のボタンに移動するには、もう一度 **Tab** キーを押します。
2. **Enter** キーを押します。ボタンが表している機能（保存など）が実行されます。

追加情報

「関連項目」（P.1-17）を参照してください。

参考情報

- 『*Cisco Unified Communications Manager システム ガイド*』
- 『*Cisco Unified Communications Manager 機能およびサービス ガイド*』
- 『*Cisco Unified Serviceability Administration Guide*』
- 『*Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide*』
- 『*Installing Cisco Unified Communications Manager Release 8.0(2)*』
- 『*Upgrading Cisco Unified Communications Manager Release 8.0(2)*』
- 『*Cisco Unified Communications Manager セキュリティ ガイド*』
- 『*Cisco Unified Communications Operating System Administration Guide*』
- 『*Disaster Recovery System Administration Guide*』
- 『*Cisco Unified Communications Solution Reference Network Design (SRND)*』

関連項目

- 「概要」（P.1-1）
- 「主な機能と利点」（P.1-2）
- 「Cisco Unified Communications Manager の管理ページの参照」（P.1-3）
  - 「Web ブラウザ」（P.1-3）
  - 「Cisco Unified Communications Manager の管理ページへのログイン」（P.1-4）
  - 「Cisco Unified Communications Manager の管理ページからのログオフ」（P.1-5）
  - 「Secure Sockets Layer 上のハイパーテキスト転送プロトコル（HTTPS）」（P.1-5）
- 「Cisco Unified Communications Manager の管理アプリケーションでの操作」（P.1-14）
  - 「Cisco Unified Presence サーバ リンク」（P.1-15）
  - 「Cisco Unified Presence サーバへのリンク」（P.1-15）
  - 「カスタム ログイン メッセージ」（P.1-16）
  - 「最後に成功したログインに関するメッセージ」（P.1-16）
- 「アクセシビリティ」（P.1-16）
- 「参考情報」（P.1-17）