概要

Cisco CallManager は、Cisco Communications 製品ファミリのソフトウェア ベースのコール処理コンポーネントです。Cisco Media Convergence Server は広範囲にわたり、Cisco CallManager 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 CallManager 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 CallManager 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 CallManager 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。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 SoftPhone、Cisco IP Interactive Voice Response（IP IVR）、Cisco Personal Assistant、Cisco CallManager Attendant Console 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

主な機能と利点

Cisco CallManager 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、複数回線通話、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 CallManager はソフトウェア アプリケーションなので、実稼働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 CallManager は、すべての Cisco 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 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 QoS が保証され、WAN 帯域幅が十分でないときには別の公衆電話交換網（PSTN）にコールが自動転送されます。

Cisco CallManager の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。

Cisco CallManager Administration の参照

Cisco CallManager Administration プログラムには、Web サーバや Cisco CallManager プログラムがインストールされているマシンとは別の PC からアクセスすることを推奨します。

Web ブラウザ

注意　Web ブラウザは、リソース消費型アプリケーションであるため、システムのメモリと CPU サイクルを大量に消費する場合があります。Web ブラウザが Cisco CallManager に必要なリソースまで消費すると、コール処理に悪影響を与えます。Web サーバや Cisco CallManager と同じマシンでブラウザを使用すると、ダイヤル トーンの遅延やコールの終了を引き起こす可能性があります。

Cisco CallManager Administration プログラムは、次の Microsoft Windows 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。

- Netscape Communicator 4.X
- Microsoft Internet Explorer 5 または 6

ネットワーク内の任意のユーザ PC から、Cisco CallManager Administration 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 CallManager Administration にログインすると、Web ページの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。

手順

次の手順に従って、サーバを参照します。

ステップ 1　適当な Microsoft Windows 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。

https://<*CCM-server-name*>/CCMAdmin/main.asp

ただし、<*CCM-server-name*> はサーバの名前または IP アドレスです。

ステップ 3　割り当てられた管理特権でログインします。

Java ランタイム環境

Cisco CallManager では、Cisco CallManager Administration を参照しているローカル PC に Java ランタイム環境（JRE）がインストールされ、設定されている必要があります。さらに、ブラウザ セキュリティは Java が使用可能になっている必要があります。

ローカル PC に JRE を取得するには、C:\utils\JRE ディレクトリからローカル PC に J2RE_Client.zip ファイルをコピーし、ファイルを解凍して実行可能ファイルを実行します。

（注）　上記のディレクトリ内の JRE を取得するには、Cisco CallManager サーバ上で Microsoft OS バージョン 2000.2.6 以降を実行する必要があります。

Microsoft Internet Explorer を使用する場合、ユーザ ID とパスワードをたずねるウィンドウが表示されます。IE で SUN JRE が使用されている場合は、JRE のユーザ名とパスワードを求める 2 番目のログイン ウィンドウが表示されます。常にそのパスワードを使用する場合は、Remember Password ボタンをクリックします。ただし、パスワードが常に有効であるため、セキュリティの問題が発生する可能性があります。パスワードの記憶を設定しない場合、このウィンドウが表示されるたびにパスワードを入力する必要があります。

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

ブラウザ クライアントと IIS サーバ間の通信を保護する Secure Sockets Layer（SSL）上のハイパーテキスト転送プロトコルは、証明書およびインターネット上で転送されるデータを暗号化する公開鍵を使用します。また、HTTPS は、ユーザのログイン パスワードが Web 経由で安全に転送されるようにします。次の Cisco CallManager アプリケーションは、確実にサーバを識別する HTTPS をサポートしています。Cisco CallManager Administration、Cisco CallManager Serviceability、Cisco IP Phone User Option Pages、Bulk Administration Tool（BAT）、TAPS、Cisco CDR Analysis and Reporting（CAR）、Trace Collection Tool、および Real Time Monitoring Tool。

Cisco CallManager をインストールまたはアップグレードすると、HTTPS 自己署名証明書である httpscert.cer が、Cisco CallManager 仮想ディレクトリをサポートする IIS デフォルト Web サイトに自動的にインストールされます。Cisco CallManager 仮想ディレクトリには、CCMAdmin、CCMService、CCMUser、AST、BAT、RTMTReports、CCMTraceAnalysis、PktCap、ART、および CCMServiceTraceCollectionTool が含まれています。HTTPS 証明書は、C:\Program Files\Cisco\Certificates ディレクトリに保存されます。必要に応じて、認証局からサーバ認証証明書をインストールして、HTTPS 自己署名証明書の代わりに使用することができます。Cisco CallManager のインストールまたはアップグレード後に認証局の証明書を使用する場合は、自己署名証明書を削除する必要があります（『*Cisco CallManager セキュリティ ガイド*』を参照）。次に、認証局によって提供されたサーバ認証証明書をインストールします（認証局のマニュアルを参照）。

（注） ホスト名を使用して Web アプリケーションにアクセスし、信頼できるフォルダ内の証明書をインストールしてから、ローカルホストまたは IP アドレスを使用してアプリケーションにアクセスしようとすると、セキュリティ証明書の名前がサイトの名前と一致しないことを知らせる Security Alert ダイアログボックスが表示されます。

ローカルホスト、IP アドレス、または URL 内のホスト名を使用して HTTPS をサポートしているアプリケーションにアクセスする場合は、URL タイプごとに（ローカル ホスト、IP アドレスなどとともに）信頼できるフォルダ内に証明書を保存する必要があります。URL のタイプごとに証明書を保存しない場合、各タイプに対して Security Alert ダイアログボックスが表示されます。

Cisco CallManager Administration での Internet Explorer および HTTPS の使用方法

Web アプリケーションにアクセスするたびに Security Alert ダイアログボックスが表示されないように、信頼できるフォルダ内に CA ルート証明書を保存する手順は、次のとおりです。ブラウザ クライアントから Cisco CallManager 4.1 をインストールまたはアップグレードした後に、システム管理者（またはユーザ）が最初に Cisco CallManager Administration または他の Cisco CallManager SSL が使用可能になっている仮想ディレクトリにアクセスするとき、サーバを信頼するかどうかをたずねる Security Alert 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。

- Yes をクリックして、現在の Web セッションに対してのみ証明書を信頼する。現在のセッションに対してのみ証明書を信頼すると、Security Alert 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。
- View Certificate > Install Certificate 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する。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 Security Alert ダイアログボックスが表示されることはありません。
- No をクリックして、操作をキャンセルする。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、Yes をクリックするか、View Certificate > Install Certificate オプションで証明書をインストールする必要があります。

Security Alert ダイアログボックスで実行できるその他の作業については、『*Cisco CallManager セキュリティ ガイド 4.1*』を参照してください。

手順

ステップ 1　IIS サーバ上のアプリケーションを参照します。

ステップ 2　Security Alert ダイアログボックスが表示されたら、**View Certificate** をクリックします。

ステップ 3　Certificate ペインで、**Install Certificate** をクリックします。

ステップ 4　**Next** をクリックします。

ステップ 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。

ステップ 6　**Trusted Root Certification Authorities** を参照します。

ステップ 7　**Next** をクリックします。

ステップ 8　**Finish** をクリックします。

ステップ 9　証明書をインストールするために、**Yes** 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、**Yes**　をクリックします。

（注）　ローカルホスト、IP　アドレス、または　URL　内のホスト名を使用して HTTPS をサポートしているアプリケーションにアクセスする場合は、URL タイプごとに（ローカル ホスト、IP アドレスなどとともに）信頼できるフォルダ内に証明書を保存する必要があります。URL のタイプごとに証明書を保存しない場合、各タイプに対して Security Alert ダイアログボックスが表示されます。

関連項目

- Cisco CallManager Administration での Internet Explorer および HTTPS の使用方法（P.1-6）
- 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 CallManager セキュリティ ガイド*

Cisco CallManager Administration での Netscape および HTTPS の使用方法

Netscape で HTTPS を使用する場合、証明書の資格情報を表示し、1 回のセッションに対して証明書を信頼する、期限が切れるまでその証明書を信頼する、または証明書を信頼しない、のいずれかを選択できます。

ヒント　1 回のセッションに対してのみ証明書を信頼する場合は、HTTPS がサポートされているアプリケーションにアクセスするたびに次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。

次の手順を実行して、信頼できるフォルダに証明書を保存します。

手順

ステップ 1　Netscape を使用して、アプリケーション（たとえば、Cisco CallManager Administration）にアクセスします。

ステップ 2　New Site Certificate ウィンドウが表示された後、**Next** をクリックします。

ステップ 3　次の New Site Certificate ウィンドウが表示された後、**Next** をクリックします。

ヒント　Next　をクリックする前に証明書の資格情報を表示する場合は、**More Info** をクリックします。資格情報を確認し、**OK** をクリックします。次に New Site Certificate ウィンドウで **Next** をクリックします。

ステップ 4　次のいずれかのオプション ボタンをクリックします。

- Accept this certificate for this session
- Do not accept this certificate and do not connect
- Accept this certificate forever (until it expires)

ステップ 5　**Next** をクリックします。

ステップ 6　Do not accept this certificate... オプション ボタンをクリックした場合は、ステップ 8 へ進みます。

ステップ 7　Netscape で他のサイトに情報を送信する前に警告を表示する場合は、**Warn me before I send information to this site** チェックボックスをオンにしてから、**Next** をクリックします。

ステップ 8　**Finish** をクリックします。

関連項目

- 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 CallManager Administration での Netscape および HTTPS の使用方法（P.1-8）
- *Cisco CallManager セキュリティ ガイド*

参考情報

- *Cisco CallManager システム ガイド*
- *Cisco IP テレフォニー ソリューション リファレンス ネットワーク デザイン ガイド*
- *Cisco CallManager インストレーション ガイド*
- *Cisco CallManager アップグレード手順*
- *Cisco CallManager セキュリティ ガイド 4.1*