Cisco Unified Communications Manager, Release 9.0(1) IM and Presence サービスのための Microsoft OCS による Microsoft Office Communicator のコール制御

初版：2012 年 07 月 18 日

最終更新：2012 年 07 月 18 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章

Microsoft OCS を使用した IM and Presence Release 9.0(1) の設定

統合の要件

このドキュメントでは、IM and Presence サービスを Microsoft Office Communications Server または Microsoft Live Communications Server と統合し、Microsoft Office Communicator (MOC) の通話コントロール機能を使用するための設定手順について説明します。

（注） このドキュメントでは、IM and Presence を Microsoft Office Communications Server（OCS）と統合する手順について説明します。 IM and Presence と Microsoft Live Communications Server（LCS）との間で同様の統合を設定する場合にも、この章をガイドとして参照できます。

ソフトウェア要件

- IM and Presence Server Release 9.0
- Cisco Unified Communications Manager Server Release 9.0
- Microsoft Office Communications（OCS）2007 または 2007 R2 Server, Standard または Enterprise
- Microsoft Live Communications（LCS）2005 Server, Standard または Enterprise
- Microsoft Office Communicator（MOC）
- Microsoft Windows Server

- Cisco CSS 11500 Content Services Switch

この統合では、インストールおよび設定を次のように行っていることを前提としています。

- 『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』の中で説明されているように、セットアップおよび設定が済んだ IM and Presence サーバ。
- 『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』の中で説明されているように、IM and Presence サーバを Cisco Unified Communications Manager（CUCM）を使用して正しく導入する必要があります。
- Microsoft 社のマニュアルに定義されている要件に従って、Microsoft OCS サーバまたは LCS サーバをセットアップし、設定していること。

注意 サーバを Microsoft OCS と統合する前に、IM and Presence サブクラスタでハイアベイラビリティを無効にする必要があります。 詳細については、『*Deployment Guide for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

統合の概要

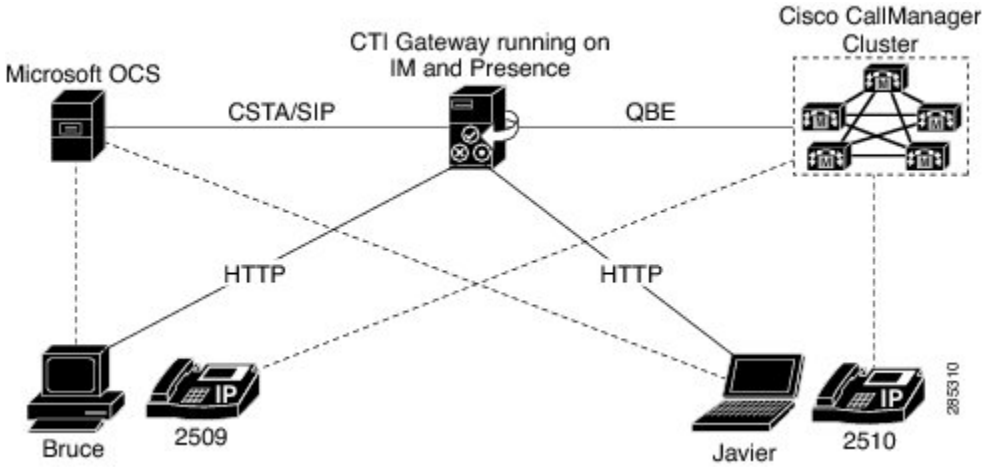
統合の仕組み

IM and Presence を使用すると、企業ユーザが Microsoft Office Communicator（サードパーティ製デスクトップ IM アプリケーション）経由で Cisco Unified IP Phone を制御できるようになります。この統合に使用する Microsoft Office Communicator クライアントは、Microsoft Live Communications Server（LCS）2005 上または Microsoft Office Communications Server（OCS）2007 上で実行できます。

Microsoft Office Communicator は、セッション開始要求を IM and Presence の CTI ゲートウェイに送信し、Cisco Unified Communications Manager に登録された Cisco Unified IP Phone を制御します（次の図を参照）。 CTI ゲートウェイは、要求を Cisco Unified Communications Manager 上の CTI マネー

ジャに転送します。 Cisco Unified Communications Manager は、同じ経路を反対方向に使用して、イベントを Microsoft Office Communicator アプリケーションに返します。

図 *1*：統合の概要



IM and Presence は、最大 8 つの Cisco Unified Communications Manager ノードとの CTI 接続をサポートします。つまり、IM and Presence において最大 8 つの CTI 接続アドレスを設定できます。

Microsoft Office Communicator は、セッション開始要求を IM and Presence に送信します。 これらの要求は、IM and Presence に設定された CTI 接続アドレスへラウンドロビン順でルーティングされます。 たとえば、1 番目の要求は最初の CTI ノードにルーティングされ、2 番目の要求は、次の CTI ノードにルーティングされます。 CTI 接続アドレスにはその設定順にプライオリティが割り当てられます。 デュアル ノードの IM and Presence クラスタが導入される場合、ロード バランサを使用する必要があります。 このシナリオでは、ロードバランサは Microsoft Office Communicator クライアントから IM and Presence パブリッシャ ノードおよびサブスクライバ ノードにラウンドロビン順にセッション開始要求を送信します。 Microsoft Office Communicator リモート コントロール クライアントをサポートするように設定されている場合、IM and Presence クラスタ内には最大 2 つのノードが存在します。

デュアル ノード IM and Presence クラスタでは、ロードバランサを使用することで、Microsoft Office Communicator クライアントからパブリッシャおよびサブスクライバ IM and Presence ノードへのセッション開始要求の送信をラウンドロビンで行うことができます。

IM and Presence 上の CTI ゲートウェイは、起動すると、設定済みリストにあるすべての CTI 接続アドレスに接続し、定期的にハートビート メッセージを送信することでそれぞれの接続をモニタします。 Microsoft Office Communicator ユーザがサイン インすると、Microsoft OCS は、CSTA ボディを含めた SIP INVITE 要求を CTI ゲートウェイに送信してユーザの Cisco Unified IP Phone をモニタします。 CTI ゲートウェイは、その Microsoft Office Communicator ユーザ用のセッションを作成し、ロードバランシング メカニズムを使用して、そのユーザから任意の CTI 接続アドレスへのセッション開始要求の送信を行います。

CSTA アプリケーション セッションが確立されると、デバイスの監視、コールの発信、コールの転送、デバイス制御のステータスの変更など、さまざまなアクティビティのための一連の SIP INFO

メッセージが Microsoft Office Communicator と CTI ゲートウェイの間で交換されます。 このメッセージ交換は、最初のセッション確立に使用したのと同じ CTI 接続アドレスで送信されます。

各 CTI マネージャへの接続がいずれも失敗した場合は、接続が使用可能になるまで、Microsoft Office Communicator からの発信コール要求が返送されます。 Cisco Unified Communications Manager ノードがダウンしている場合は、CTI ゲートウェイが定期的にそのノードとの接続の再確立を試みます。 Cisco Unified Communications Manager ノードが使用可能になると、CTI ゲートウェイがそのノードに再接続し、接続をモニタします。 この場合、Microsoft OCS が（セッション中の）SIP INFO 要求を送信すると、新規接続となるため、CTI ゲートウェイの CTI マネージャ接続 ID は別のものになります。 Microsoft Office Communicator は、新規 SIP INVITE メッセージを送信しますが、Microsoft Office Communicator ユーザは再度サイン インする必要はありません。

関連トピック

ライン アピアランス, （4 ページ）
この統合の冗長性の設定

ライン アピアランス

リモート通話コントロール機能を使用する電話機をユーザが選択すると、IM and Presence では、Microsoft Office Communicator から制御するライン アピアランスも選択されることになります。 ラインアピアランスとは、回線とデバイスとの関連付けのことです。 Cisco Unified Communications Manager では、管理者は、1 つのデバイスを複数の回線に関連付けたり、1 つの回線を複数のデバイスに関連付けたりできます。 一般に、相互に関連付ける回線やデバイスを指定してラインアピアランスを設定するという作業は、Cisco Unified Communications Manager 管理者の役割です。

関連トピック

Cisco Unified Communications Manager でのユーザおよびデバイスの設定, （7 ページ）

ライセンス要件

各 Microsoft Lync RCC ユーザに IM and Presence を割り当てる必要があります。 IM and Presence 機能は、User Connect Licensing（UCL）と Cisco Unified Workspace Licensing（CUWL）の両方に含まれています。 詳細については、『*Cisco Unified Communications Manager Enterprise License Manager User Guide*』を参照してください。

Cisco Unified Communications Manager の [エンド ユーザの設定（End User Configuration）] ウィンドウで IM and Presence をユーザに割り当てることができます。 詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

詳細情報

IM and Presence

IM and Presence の追加マニュアルについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Cisco Unified Communications Manager

Cisco Unified Communications Manager のマニュアルについては、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Microsoft Active Directory

Microsoft Windows Server Active Directory の詳細については、次の URL を参照してください。

http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx

詳細情報

第 2 章

Microsoft OCS との統合のための Cisco Unified Communications Manager の設定

（注） Cisco Unified Communications Manager のリリースによってメニュー オプションおよびパラメータが異なる場合があるため、使用中のリリースに対応した Cisco Unified Communications Manager のマニュアルを参照してください。

Cisco Unified Communications Manager でのユーザおよびデバイスの設定

Microsoft OCS と統合するために Cisco Unified Communications Manager を設定する前に、Cisco Unified Communications Manager でユーザおよびデバイスの設定を完了する必要があります。 電話デバイスを設定し、ユーザを設定し、各ユーザにデバイスを関連付ける必要があります。

回線をデバイスに関連付ける必要もあります。ただし、拡張モビリティ機能のユーザの場合は、回線をデバイスプロファイルに関連付けます。 この関連付けがラインアピアランスとなります。ユーザをデバイスまたはデバイスプロファイルに関連付けると、ラインアピアランスがユーザに関連付けられます。

タスク	メニュー パス
電話デバイスを設定し、プライマリ内線を各デバイスに関連付ける	[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [デバイス（Device）] > [電話（Phone）]
ユーザを設定し、各ユーザにデバイスを関連付ける	[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [ユーザ管理（User Management）] > [エンド ユーザ（End User）].
ユーザをラインアピアランスに関連付ける	[Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [デバイス（Device）] > [電話（Phone）]

（注） IM and Presence Release 9.0 以降のリリースでは、Cisco Unified Communications Manager で各デバイスにプライマリ内線を関連付ける必要がなくなりました。

次の作業

標準 CCM アクセス制御グループへのユーザの追加, （8 ページ）

関連トピック

ライン アピアランス, （4 ページ）

標準 CCM アクセス制御グループへのユーザの追加

はじめる前に

Cisco Unified Communications Manager で、前提条件であるユーザとデバイスの設定を完了しておきます。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [アクセス コントロール グループ（Access Control Group）] を選択します。

ステップ 2 [検索（Find）] を選択します。

ステップ 3 [標準 CCM エンド ユーザ（Standard CCM End Users）] を選択します。

ステップ 4 標準 CCM アクセス コントロール グループに追加するエンド ユーザを選択します。

ステップ 5 [選択項目の追加（Add Selected）] を選択します。

ステップ 6 [保存（Save）] を選択します。

次の作業

CTI ゲートウェイ向けのアプリケーション ユーザの設定, （9 ページ）

関連トピック

Cisco Unified Communications Manager でのユーザおよびデバイスの設定, （7 ページ）

CTI ゲートウェイ向けのアプリケーション ユーザの設定

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [ユーザ管理（User Management）] > [アプリケーション ユーザ（Application User）] を選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [ユーザ ID（User ID）] フィールドに、アプリケーション ユーザ名（「**CtiGW**」など）を入力します。

ステップ 4 このアプリケーション ユーザのパスワードを入力し、パスワードを確認します。

ステップ 5 [保存（Save）] を選択します。

次の作業

CTI 対応のアクセス コントロール グループへのアプリケーション ユーザの追加, （10 ページ）

CTI対応のアクセスコントロールグループへのアプリケーション ユーザの追加

CTI 対応のアクセス コントロール グループにアプリケーション ユーザを追加するには、次の手順を実行します。

はじめる前に

CTI ゲートウェイを使用できるようにアプリケーション ユーザを設定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [ユーザ管理（User Management）] > [User Settings（ユーザ設定）] > [アクセス コントロール グループ（Access Control Group）] を選択します。

ステップ 2 [検索（Find）] を選択します。

ステップ 3 [標準 CTI 対応（Standard CTI Enabled）] を選択します。

ステップ 4 [グループにアプリケーション ユーザを追加（Add App Users to Group）] を選択します。

ステップ 5 CTI ゲートウェイ用に作成したアプリケーション ユーザを選択します。

ステップ 6 [選択項目の追加（Add Selected）] を選択します。

ステップ 7 [保存（Save）] を選択します。

次の作業

アプリケーション ユーザへの CTI デバイス コントロールの割り当て, （10 ページ）

関連トピック

CTI ゲートウェイ向けのアプリケーション ユーザの設定, （9 ページ）

アプリケーション ユーザへの CTI デバイス コントロールの割り当て

アプリケーション ユーザに CTI デバイス コントロールを割り当てるには次の手順を実行します。

はじめる前に

CTI ゲートウェイを使用できるようにアプリケーション ユーザを設定します。

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] > [ユーザ管理（User Management）] > [User Settings（ユーザ設定）] > [アクセス コントロール グループ（Access Control Group）] を選択します。

ステップ 2 [検索（Find）] を選択します。

ステップ 3 [標準 CTI によるすべてのデバイスの制御（Standard CTI Allow Control of All Devices）] を選択します。 Cisco Unified IP Phone の RT モデルを配置している場合は、[標準 CTI による接続時の転送および会議をサポートする電話の制御（Standard CTI Allow Control of Phones supporting Connected Xfer and conf）] を選択します。

ステップ 4 [グループにアプリケーション ユーザを追加（Add App Users to Group）] を選択します。

ステップ 5 CTI ゲートウェイ用に作成したアプリケーション ユーザを選択します。

ステップ 6 [選択項目の追加（Add Selected）] を選択します。

関連トピック

CTI ゲートウェイ向けのアプリケーション ユーザの設定, （9 ページ）
CTI 対応のアクセス コントロール グループへのアプリケーション ユーザの追加, （10 ページ）

第 3 章

Microsoft OCS との統合のための IM and Presence の設定

サービス パラメータの設定

IM and Presence から Microsoft Office Communicator への SIP メッセージ ルーティングは、Microsoft OCS が初期要求に追加したレコードルート ヘッダーに基づいています。 IM and Presence は、レコードルート ヘッダー内のホスト名を IP アドレスに解決し、SIP メッセージを Microsoft Office Communicator クライアントにルーティングします。

また、IM and Presence の転送タイプは、Microsoft OCS に設定された IM and Presence ルートの転送タイプ（TLS または TCP）と同じである必要があります。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [システム パラメータ（Service Parameters）] を選択します。

ステップ 2 IM and Presence サーバを選択します。

ステップ 3 サービス [Cisco SIP プロキシ（Cisco SIP Proxy）] を選択します。

ステップ 4 次のパラメータが正しく設定されていることを確認します。

a) Proxy Domain パラメータ値には、企業の最上位ドメイン名（たとえば「example.com」）を定義する必要があります。 このパラメータでは、この IM and Presence インストールがどの URI をローカルとして扱って処理するかを指定します。 他の SIP 要求はプロキシできます。

b) Add Record-Route Header パラメータを有効にします。

c) Use Transport in Record-Route Header パラメータを有効にします。
d) SIP Route Header Transport Type パラメータ値を、Microsoft OCS から IM and Presence ルート用に Microsoft OCS に設定されたトランスポート パラメータと同じタイプに設定する必要があります。

ステップ 5 [保存（Save）] を選択します。

次の作業

着信アクセス コントロール リストの設定, （14 ページ）

着信アクセス コントロール リストの設定

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [着信 ACL（Incoming ACL）] を選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [説明（Description）] フィールドに説明を入力します。

ステップ 4 [アドレス パターン（Address Pattern）] フィールドに、関連付けられた Microsoft OCS サーバの IP アドレス、ホスト名、または Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を入力します。

ステップ 5 [保存（Save）] を選択します。

次の作業

ルーティング設定の構成, （15 ページ）

ルーティング設定の構成

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ルーティング（Routing）] > [設定（Settings）] を選択します。

ステップ 2 [メソッド/イベント ルーティングのステータス（Method/Event Routing Status）] で [オン（On）] を選択します。

ステップ 3 優先プロキシ サーバに対して、[デフォルト Cisco SIP プロキシ TCP リスナー（Default Cisco SIP Proxy TCP Listener）] を選択します。

ステップ 4 [保存（Save）] を選択します。

次の作業

リモートコール制御の設定, （15 ページ）

リモートコール制御の設定

IM and Presence での CTI 接続の設定

はじめる前に

CTI ゲートウェイに関連付けられた Cisco Unified Communications Manager サーバでアプリケーション ユーザ アカウントに対して設定した、ユーザ名およびパスワードを取得します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [アプリケーション（Application）] > [Microsoft RCC] > [設定（Settings）] を選択します。

ステップ 2 [アプリケーションのステータス（Application Status）] メニューから [オン（On）] を選択します。

ステップ 3 CTI ゲートウェイ アプリケーション ユーザ名とパスワードを入力します。

ヒント ユーザ名およびパスワードは大文字と小文字が区別され、Cisco Unified Communications Manager での設定に一致する必要があります。

ステップ 4 ハートビート間隔の値（秒単位）を入力します。 これは、CTI 接続を監視するために、IM and Presence から Cisco Unified Communications Manager ノードに送信されるハートビート メッセージ間の時間の長さです。

ステップ 5 セッション タイマーの値（秒単位）を入力します。 これは、Microsoft Office Communicator サインイン セッション用のセッション タイマーです。

ステップ 6 [Microsoft サーバ タイプ（Microsoft Server Type）] メニューから、使用している Microsoft サーバのタイプを選択します。

ステップ 7 必要に応じて、CTI 接続を確立する各 Cisco Unified Communications Manager ノードの IP アドレスを入力します。

（注） 最大 8 つの Cisco Unified Communications Manager ノードとの CTI 接続を設定できます。このようなノードはすべて、同じ Cisco Unified Communications Manager クラスタに属している必要があります。

ステップ 8 [保存（Save）] を選択します。

トラブルシューティングのヒント

- [Microsoft サーバ タイプ（Microsoft Server Type）] として [MOC サーバ OCS（MOC server OCS）] を選択した場合は、複数のライン アピアランスを使用してリモート通話コントロールを実施するユーザのために、Microsoft Office Communicator に Phone Selection プラグインをインストールする必要があります。 Phone Selection プラグインをインストールすると、Microsoft Office Communicator クライアントにタブが追加されて、制御するライン アピアランスをユーザが選択できるようになります。
- [Microsoft サーバ タイプ（Microsoft Server Type）] として [MOC サーバ LCS（MOC server LCS）] を選択した場合は、リモート通話コントロール機能によって、IM and Presence の既存のデバイス選択ロジックに基づき制御するデバイスが決定されます。

次の作業

ユーザの機能の割り当て, （17 ページ）

関連トピック

CTI ゲートウェイ向けのアプリケーション ユーザの設定, （9 ページ）
Phone Selection プラグインの導入, （49 ページ）
Microsoft RCC トラブルシュータの実行, （17 ページ）

ユーザの機能の割り当て

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [アプリケーション（Application）] > [Microsoft RCC] > [ユーザ割り当て（User Assignment）] を選択します。

ステップ 2 [検索（Find）] を選択します。

ステップ 3 固定電話機能を割り当てるユーザを確認し、[選択したユーザの割り当て（Assign Selected Users）] を選択します。

ステップ 4 [Microsoft RCC の割り当て（Microsoft RCC Assignment）] ウィンドウで [Microsoft RCC を有効にする（Enable Microsoft RCC）] をオンにし、[保存（Save）] を選択します。

トラブルシューティングのヒント

- リモートコール制御機能を各 Microsoft Office Communicator ユーザに割り当てたことを確認します。
- リモート通話コントロール機能のある LCS を使用している場合は、Cisco Unified Communications Manager でユーザごとに最大 2 つのデバイスを関連付けることができます。 ユーザが Extension Mobility（EM; 拡張モビリティ）デバイスにサイン インしている場合、EM デバイスはユーザに関連付けることができる 2 つのデバイスのうちの 1 つであると見なされます。

次の作業

IM and Presence との統合のための Microsoft コンポーネントの設定, （19 ページ）

関連トピック

IM and Presence での CTI 接続の設定, （15 ページ）
Microsoft RCC トラブルシュータの実行, （17 ページ）

Microsoft RCC トラブルシュータの実行

Microsoft RCC トラブルシュータは、Microsoft Office Communicator クライアントと IM and Presence との統合をサポートする設定を検証します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [診断（Diagnostics）] > [Microsoft RCC トラブルシュータ（Microsoft RCC Troubleshooter）] を選択します。

ステップ 2 有効なユーザ ID を入力します。

ヒント ユーザの ID を検索するには、[検索（Search）] を選択します。

ステップ 3 Microsoft OCS サーバのアドレスを入力します。

ステップ 4 [送信（Submit）] を選択します。

第 4 章

IM and Presence との統合のための Microsoft コンポーネントの設定

Microsoft Active Directory での回線 URI の設定

Microsoft Active Directory で回線 URI パラメータを設定する場合は、次の点に注意してください。

- 回線 URI には、tel:xxxx;phone-context=dialstring の形式を使用することを推奨します。
  - xxxx には、コールの発信時に CTI マネージャが発信番号または着信番号として IM and Presence に報告する、ディレクトリ番号を指定します。
  - phone-context=dialstring を指定すると、Microsoft Office Communicator ディレクトリ番号に関連付けられているデバイスのいずれかをクライアントが制御できるようになります。
- デバイス ID を設定する場合、Microsoft Office Communicator クライアントは最初のサインイン時にその ID に対応するデバイスを制御します。たとえば、tel:xxxx;phone-context=dialstring;device=SEP0002FD3BB5C5 となります。
- パーティションを設定する場合、Microsoft Office Communicator クライアントはディレクトリ番号のパーティションを指定します。たとえば、tel:xxxx;phone-context=dialstring;device=SEP0002FD3BB5C5;partition=myPartition となります。
- 回線 URI は、Microsoft Office Communicator ユーザがサイン インするときだけ有効になります。

- 初回のサイン イン後、Microsoft Office Communicator ユーザは Phone Selection プラグインを使用して、制御するライン アピアランスを変更できます。
- 回線 URI でデバイス ID を設定しないと、CTI ゲートウェイが回線の Directory Number（DN; ディレクトリ番号）に関連付けられるデバイスを決定します。 回線の DN にデバイスが 1 つだけ関連付けられていると、CTI ゲートウェイはそのデバイスを使用します。
- Microsoft LCS を配置し、回線 URI でデバイス ID を設定せず、2 つのデバイスを回線の DN に関連付けている場合（共有回線）、CTI ゲートウェイは次の規則に従ってデバイスを選択します。
  - この 2 つのデバイスのいずれかが Cisco IP Communicator であり、そのステータスが登録されている場合、CTI ゲートウェイはそのデバイスを使用します。
  - この 2 つのデバイスのいずれかが Cisco IP Communicator であるものの、そのステータスが登録されていない場合、CTI ゲートウェイはもう一方のデバイスを使用します。
  - 2 つのデバイスとも Cisco IP Communicator ではない場合、Microsoft Office Communicator ユーザがサイン インすると両方の電話機が鳴ります。 ユーザは、電話機に応答してそのデバイスを制御する必要があります。
  - 3 つ以上のデバイスを回線の DN に関連付けている場合は、回線 URI で目的のデバイスを指定する必要があります。

関連トピック

ライン アピアランス, （4 ページ）
IM and Presence でのユーザ認証, （20 ページ）
Phone Selection プラグインの導入, （49 ページ）

IM and Presence でのユーザ認証

Microsoft Active Directory で SIP URI を設定するときは、IM and Presence がどのようにユーザ認証チェックを実行するかを考慮してください。 ユーザ認証ロジックは次のとおりです。

1. IM and Presence は、Microsoft Office Communicator（サインイン）のユーザ ID がCisco Unified Communications Manager のユーザ ID と一致するかチェックします。 IM and Presence が一致を検出できない場合：
2. IM and Presence は、Microsoft Office Communicator のユーザ電子メール（[発信元（From）]）ヘッダーが Cisco Unified Communications Manager のユーザ電子メールと一致するかチェックします。 IM and Presence が一致を検出できない場合：
3. IM and Presence は、Microsoft Office Communicator のユーザ電子メールが Cisco Unified Communications Manager のユーザの ocsPrimaryAddress 値と一致するかチェックします。

たとえば、ユーザ Joe の Microsoft Office Communicator ユーザ ID が joe@someCompany.com であるとします。 SIP INVITE の発信元ヘッダーは sip:joe@someCompany.com です。

この場合、IM and Presence は次のチェックを実施します。

- Cisco Unified Communications Manager データベース内にユーザ ID が「joe」のユーザが存在するかどうか。 このユーザ ID が存在しない場合：
- Cisco Unified Communications Manager データベース内にメール アドレスが「joe@someCompany.com」のユーザが存在するかどうか。 このメールが存在しない場合：
- Cisco Unified Communications Manager データベース内に ocsPrimaryAddress の値が「sip:joe@someCompany.com」であるユーザが存在するかどうか。

Microsoft Active Directory の設定

はじめる前に

- Microsoft Active Directory での回線 URI 設定に関するトピックに目を通します。
- IM and Presence でのユーザ認証チェックに関するトピックに目を通します。

手順

ステップ 1 Microsoft Active Directory アプリケーション ウィンドウから、各特定のユーザに関連付けるユーザ名および電話番号を追加します。

ステップ 2 追加したユーザごとに、Microsoft Active Directory で [プロパティ（Properties）] ウィンドウを開き、次のパラメータを設定します。

a) Office Communications Server 用のユーザを有効にします。
b) SIP URI を入力します。
c) Microsoft OCS サーバ名またはプールを入力します。
注意 OCS サーバ名またはプール名にはアンダースコア文字が含まれていないことを確認します。
d) [テレフォニー設定（Telephony Settings）] で、[設定（Configure）] を選択します。
e) [リモート通話コントロールを有効にする（Enable Remote call control）] をオンにします。
f) リモート通話コントロール SIP URI を、たとえば sip:8000@my-cups.my-domain.com のように入力します。my-cups.my-domain.com には、この統合のために設定した IM and Presence サーバの FQDN を指定します。
g) 回線 URI 値を入力します。
トラブルシューティングのヒント

Microsoft Active Directory で入力する SIP URI は、Microsoft OCS でスタティック ルートを設定しているときに定義するスタティック ルート URI に一致する必要があります。

次の作業

Microsoft OCS の設定の概要, （22 ページ）

関連トピック

Microsoft Active Directory での回線 URI の設定, （19 ページ）
IM and Presence でのユーザ認証, （20 ページ）
ライン アピアランス, （4 ページ）
http://technet2.microsoft.com/windowsserver/en/technologies/featured/ad/default.mspx

Microsoft OCS の設定の概要

（注） このトピックでは、この統合のために Microsoft OCS で必要になる設定について簡単に説明します。 Microsoft OCS 設定の詳細な説明は、この章では触れません。 Microsoft OCS のマニュアルを参照してください。

Microsoft OCS サーバが正しくインストールされてアクティブになっていることを確認します。Microsoft OCS で次の項目が設定されていることを確認します。

- 証明書設定
- スタティック ルート
- 認証済みホスト
- ドメイン ネーム サーバ
- プール プロパティ
- サーバ プロパティ
- プール ユーザ
- ユーザ設定
- Microsoft Office Communicator（MOC）の設定

関連トピック

Microsoft Active Directory での正規化規則の設定, （23 ページ）
Microsoft OCS に関するセキュリティ証明書の設定, （35 ページ）
Microsoft OCS での IM and Presence のための TLS ルートの設定, （42 ページ）
Microsoft OCS での認証済みホストとしての IM and Presence の設定, （43 ページ）
http://office.microsoft.com/en-us/communicationsserver/FX101729111033.aspx

第 5 章

Microsoft Active Directory での正規化規則

Microsoft Active Directory での正規化規則の設定

ディレクトリ番号からユーザ名への逆ルックアップは、次の条件下では機能しません。

- Microsoft Office Communicator ユーザが Cisco Unified IP Phone を制御している
- そのユーザへの着信音声コールがある
- ユーザのディレクトリ番号が、Active Directory に E.164 として設定されている
- Active Directory 電話番号正規化規則が設定されていない

このような条件下では、アプリケーションはコールを内線番号から発信されたものであると見なし、ユーザ名が Microsoft Office Communicator に表示されません。

このため、コールが発信されると表示されるポップアップ ウィンドウで Microsoft Office Communicator ユーザが発信側の名前を参照できるようにするには、Microsoft Office Communicator サーバに Active Directory アドレス帳の正しい正規化規則を設定する必要があります。

（注） 内線ダイヤリング用の正規化規則ファイルを用意する必要があります。 例については、正規化規則のサンプルを取り上げているトピックを参照してください。

はじめる前に

アドレス帳の同期化のために適切な証明書を配布するには、Microsoft Office Communicator PC に Microsoft OCS の Certificate Authority（CA; 認証局）署名付き証明書が必要です。 Verisign や RSA

など広く普及している CA を証明書の署名に使用している場合は、CA 証明書がすでに PC にインストールされている可能性があります。

手順

ステップ 1 正規化規則をこのファイルに追加するには、ディレクトリ パス C:\Program Files\Microsoft Office Communications Server 2007\Web Components\Address Book Files\Files\Company_Phone_Number_Normalization_Rules.txt を使用します。

ステップ 2 アドレス帳サーバ（ABServer）を実行し、正規化規則を再生成するには、ディレクトリ パス C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>Abserver.exe -regenUR を使用します。

（注） UR の再生成が正常に完了するまで、最大 5 分間待機することになる場合があります。

ステップ 3 ABServer を同期するには、ディレクトリ パス C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>ABServer.exe -syncnow を使用します。

（注） ABServer の同期が正常に完了するまで、最大 5 分間待機することになる場合があります。

ステップ 4 同期化が完了したら、Microsoft OCS サーバのイベント ビューアをチェックして、同期化の完了が示されていることを確認します。

ステップ 5 電話番号 C:\Program Files\Microsoft Office Communications Server 2007\Server\Core>Abserver.exe -testPhoneNorm <E164 phone number> で正規化規則をテストします。

次の作業

Microsoft Office Communicator インターフェイスに表示されたユーザ名の確認, （24 ページ）

関連トピック

正規化規則のサンプル, （25 ページ）

Microsoft Office Communicator インターフェイスに表示されたユーザ名の確認

コールが発信されると表示される Microsoft Office Communicator ポップアップ ウィンドウでユーザが発信側の名前を参照できるということを、確認する必要があります。

はじめる前に

Microsoft Active Directory で正規化規則を設定します。

手順

ステップ 1 Microsoft Office Communicator を終了します。 ただし、サイン アウトしないでください。

ステップ 2 C:\Documents and Settings\<username>\Local Settings\Application Data\Microsoft\Communicator にあるアドレス帳ファイル contacts.db を削除します。

ステップ 3 Microsoft Office Communicator クライアントを開始し、再度サインインします。

ステップ 4 galcontacts.db が作成されていることを確認します。

ステップ 5 再度 Microsoft Office Communicator を終了し、サイン インし、Microsoft Office Communicator にユーザ名が表示されることを確認します。

関連トピック

Microsoft Active Directory での正規化規則の設定, （23 ページ）
正規化規則のサンプル, （25 ページ）

正規化規則のサンプル

```
# ++ test RTP## PSTN:+61262637900, Extension:37XXX # +61262637ddd
[\s()\-\./\+]*(61)?[\s()\-\./]*0?(2)\)?[\s()\-\./]*(6263)[\s()\-\./]*(7\d\d\d)
 3$4;phone-context=dialstring # ++ test1 RTP ## Site:, PSTN:+61388043300,
 Extension:33XXX
[\s()\-\./\+]*(61)?[\s()\-\./]*0?(3)\)?[\s()\-\./]*(8804)[\s()\-\./]*(3\d\d\d)
 3$4;phone-context=dialstring #Test input +61388043187, Test result->
tel:33187;phone-context=dialstring # ++ test2 RTP ## PSTN:+61292929000,
Extension:29XXX
[\s()\-\./\+]*(61)?[\s()\-\./]*0?(2)\)?[\s()\-\./]*(9292)[\s()\-\./]*(9\d\d\d)
 2$4;phone-context=dialstring # Test input +61292929761, test result->
tel:29761;phone-context=dialstring
```

内線ダイヤリング用の正規化規則ファイルを用意する必要があります。 たとえば、3 桁の内線ダイヤリングの正規化規則は次のようになります。

```
^(\d{3}) $1;phone-context=dialstring
```

関連トピック

Microsoft Active Directory での正規化規則の設定, （23 ページ）
Microsoft Office Communicator インターフェイスに表示されたユーザ名の確認, （24 ページ）

第 6 章

IM and Presence に関するセキュリティ証明書の設定

このトピックを適用できるのは、IM and Presence と Microsoft OCS との間にセキュアな接続を必要とする場合だけです。

このトピックでは、スタンドアロン CA を使用してセキュリティ証明書を設定する方法について説明します。 エンタープライズ CA を使用する場合は、エンタープライズ CA を使用した証明書交換手順の例について、『*Interdomain Federation for IM and Presence Service on Cisco Unified Communications Manager*』を参照してください。

（注） SIP プロキシ証明書（所有および信頼）は、X.509 バージョン 3 に準拠する必要があります。

スタンドアロン ルート認証局（CA）の設定

手順

ステップ 1 ドメイン管理者権限で CA サーバにサイン インします。

ステップ 2 Windows Server 2003 CD を挿入します。

ステップ 3 [スタート（Start）] > [設定（Settings）] > [コントロール パネル（Control Panel）] を選択します。

ステップ 4 [プログラムの追加と削除（Add or Remove Programs）] をダブルクリックします。

ステップ 5 [Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

ステップ 6 [アプリケーション サーバ（Application Server）] を選択します。

ステップ 7 [インターネット インフォメーション サービス（IIS）（Internet Information Services (IIS)）] を選択します。

ステップ 8 インストール手順を完了します。

ステップ 9 [Windows コンポーネントの追加と削除（Add/Remove Windows Components）] を選択します。

ステップ 10 [証明書サービス（Certificate Services）] を選択します。

ステップ 11 [次へ（Next）] を選択します。

ステップ 12 [スタンドアロンのルート CA（Standalone root CA）] を選択します。

ステップ 13 [次へ（Next）] を選択します。

ステップ 14 CA ルートの名前を入力します。

（注） この名前は、フォレストルートのCAルートをわかりやすくした名前にすることができます。

ステップ 15 時間をこの証明書に必要な年数に変更します。

ステップ 16 [次へ（Next）] を選択して、インストールを開始します。

ステップ 17 証明書データベースおよび証明書データベース ファイルの場所を選択します。

ステップ 18 [次へ（Next）] を選択します。

ステップ 19 IIS を停止するように求められたら、[はい（Yes）] を選択します。

ステップ 20 Active Server Pages に関するメッセージが表示されたら [はい（Yes）] を選択します。

ステップ 21 [完了（Finish）] を選択します。

次の作業

CA サーバからのルート証明書のダウンロード, （29 ページ）。

CA サーバからのルート証明書のダウンロード

はじめる前に

スタンドアロン ルート Certificate Authority（CA; 認証局）を設定します。

手順

ステップ 1 CA サーバにサイン インし、Web ブラウザを開きます。

ステップ 2 URL **http://<ca_server_IP_address>/certsrv** を開きます。

ステップ 3 [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] を選択します。

ステップ 4 [エンコード方式（Encoding Method）] で [Base 64] を選択します。

ステップ 5 [CA 証明書のダウンロード（Download CA Certificate）] を選択します。

ステップ 6 証明書ファイル certnew.cer をローカル ディスクに保存します。

トラブルシューティングのヒント

ルート証明書のサブジェクトの Common Name（CN; 共通名）がわからない場合は、外部の証明書管理ツールを使用して探すことができます。 Windows オペレーティング システムでは、拡張子が .cer の証明書ファイルを右クリックして、証明書のプロパティを開くことができます。

次の作業

IM and Presence へのルート証明書のアップロード, （29 ページ）

関連トピック

スタンドアロン ルート認証局（CA）の設定, （28 ページ）

IM and Presence へのルート証明書のアップロード

はじめる前に

CA サーバからルート証明書をダウンロードします。

手順

ステップ 1 IM and Presence サーバの管理に使用するローカル コンピュータに certnew.cer ファイルをコピーします。

ステップ 2 [Cisco Unified IM and Presence オペレーティングシステムの管理（Cisco Unified IM and Presence Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 3 [証明書のアップロード（Upload Certificate）] を選択します。

ステップ 4 [証明書の名前（Certificate Name）] メニューから [cup-trust] を選択します。

（注） ルート名のフィールドは空白のままにしておきます。

ステップ 5 [参照（Browse）] を選択します。

ステップ 6 ローカル コンピュータで certnew.cer ファイルがある場所に移動します。

（注） 証明書ファイルの拡張子を .pem に変更することが必要になる場合があります。

ステップ 7 [ファイルのアップロード（Upload File）] を選択します。

ヒント [証明書の管理（Certificate Management）] の検索画面を使用して、cup-trust にアップロードした新規 CA 証明書ファイル名を書き留めます。 この証明書ファイル名（拡張子の .pem または .der 以外）が、CA 署名済み SIP プロキシ証明書をアップロードするときにルート CA のフィールドに入力する値となります。

次の作業

IM and Presence の証明書署名要求の生成, （30 ページ）

関連トピック

CA サーバからのルート証明書のダウンロード, （29 ページ）
IM and Presence への署名付き証明書のアップロード, （33 ページ）

IM and Presence の証明書署名要求の生成

はじめる前に

IM and Presence にルート証明書をアップロードします。

手順

ステップ 1 [Cisco Unified IM and Presence オペレーティングシステムの管理（Cisco Unified IM and Presence Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [CSR の作成（Generate CSR）] を選択します。

ステップ 3 [証明書の名前（Certificate Name）] メニューから [cup] を選択します。

ステップ 4 [CSR の作成（Generate CSR）] を選択します。

次の作業

IM and Presence からの証明書署名要求のダウンロード, （31 ページ）

関連トピック

IM and Presence へのルート証明書のアップロード, （29 ページ）

IM and Presence からの証明書署名要求のダウンロード

はじめる前に

IM and Presence の証明書署名要求を生成します。

手順

ステップ 1 [Cisco Unified IM and Presence オペレーティングシステムの管理（Cisco Unified IM and Presence Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [CSR のダウンロード（Download CSR）] を選択します。

ステップ 3 [証明書の名前（Certificate Name）] メニューから [cup] を選択します。

ステップ 4 [CSR のダウンロード（Download CSR）] を選択します。

ステップ 5 [保存（Save）] を選択して、cup.csr ファイルをローカル コンピュータに保存します。

次の作業

CA サーバでの証明書署名要求の送信, （32 ページ）

関連トピック

IM and Presence の証明書署名要求の生成, （30 ページ）

CA サーバでの証明書署名要求の送信

はじめる前に

IM and Presence から証明書署名要求をダウンロードします。

手順

ステップ 1 証明書要求ファイル cup.csr を CA サーバにコピーします。

ステップ 2 URL **http://local-server/certserv** または **http://127.0.0.1/certsrv** を開きます。

ステップ 3 [証明書の要求（Request a certificate）] を選択します。

ステップ 4 [証明書の要求の詳細設定（Advanced certificate request）] を選択します。

ステップ 5 [ベース 64 エンコード CMC または PKCS #10 ファイルを使用して証明書要求を送信するか、ベース 64 エンコード PKCS #7 ファイルを使用して更新要求を送信する（Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file）] を選択します。

ステップ 6 メモ帳などのテキスト エディタを使用して、生成した cup 自己証明書を開きます。

ステップ 7 次の行から、
-----BEGIN CERTIFICATE REQUEST

次の行までの情報をすべてコピーします。

END CERTIFICATE REQUEST-----

ステップ 8 証明書要求の内容を [証明書要求（Certificate Request）] テキスト ボックスに貼り付けます。

ステップ 9 [送信（Submit）] を選択します。
要求 ID 番号が表示されます。

ステップ 10 [管理ツール（Administrative Tools）] で [証明機関（Certificate Authority）] を開きます。
[認証局（Certificate Authority）] ウィンドウの [保留中の要求（Pending Requests）] の下に、送信したばかりの要求が表示されます。

ステップ 11 その証明書要求を右クリックします。

ステップ 12 [すべてのタスク（All Tasks）] で [発行（Issue）] を選択します。

ステップ 13 [発行した証明書（Issued certificates）] を選択し、証明書が発行されていることを確認します。

次の作業

CA サーバからの署名付き証明書のダウンロード, （33 ページ）

関連トピック

IM and Presence からの証明書署名要求のダウンロード, （31 ページ）

CA サーバからの署名付き証明書のダウンロード

はじめる前に

CA サーバで証明書署名要求を送信します。

手順

ステップ 1 CA が実行されている Windows サーバで **http://<local_server>/certsrv** を開きます。

ステップ 2 [保留中の証明書の要求の状態（View the status of a pending certificate request）] を選択します。

ステップ 3 直前に送信された要求を表示するオプションを選択します。

ステップ 4 [Base 64 エンコード（Base 64 encoded）] を選択します。

ステップ 5 [証明書のダウンロード（Download certificate）] を選択します。

ステップ 6 署名済み証明書をローカル ディスクに保存します。

ステップ 7 証明書 cup.pem の名前を変更します。

ステップ 8 cup.pem ファイルをローカル コンピュータにコピーします。

次の作業

IM and Presence への署名付き証明書のアップロード, （33 ページ）

関連トピック

CA サーバでの証明書署名要求の送信, （32 ページ）

IM and Presence への署名付き証明書のアップロード

はじめる前に

CA サーバから署名済み証明書をダウンロードします。

手順

ステップ 1 [Cisco Unified IM and Presence オペレーティングシステムの管理（Cisco Unified IM and Presence Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択します。

ステップ 2 [証明書のアップロード（Upload Certificate）] を選択します。

ステップ 3 [証明書の名前（Certificate Name）] メニューから [cup] を選択します。

ステップ 4 ルート証明書の名前を指定します。 ルート証明書の名前には、拡張子 .pem または .der が含まれている必要があります。

ステップ 5 [参照（Browse）] を選択します。

ステップ 6 ローカル コンピュータで署名済みの cup.pem 証明書がある場所に移動します。

ステップ 7 [ファイルのアップロード（Upload File）] を選択します。

次の作業

Microsoft OCS に関するセキュリティ証明書の設定, （35 ページ）

関連トピック

CA サーバからの署名付き証明書のダウンロード, （33 ページ）

第 7 章

IM and Presence と Microsoft OCS 間のセキュリティの設定

このトピックを適用できるのは、IM and Presence と Microsoft OCS との間にセキュアな接続を必要とする場合だけです。

Microsoft OCS に関するセキュリティ証明書の設定

CA 証明書チェーンのダウンロード

手順

ステップ 1 [スタート（Start）] > [ファイル名を指定して実行（Run）] を選択します。

ステップ 2 次の操作を実行します。

a) http://<name of your Issuing CA Server>/certsrv と入力します。

b) [OK] を選択します。

ステップ 3 [タスクの選択（Select a task）] から [CA 証明書、証明書チェーン、または CRL のダウンロード（Download a CA certificate, certificate chain, or CRL）] をクリックします。

ステップ 4 [CA 証明書チェーンのダウンロード（Download CA certificate chain）] を選択します。

ステップ 5 [ファイルのダウンロード（File Download）] ダイアログボックスで [保存（Save）] を選択します。

ステップ 6 サーバのハード ディスク ドライブにファイルを保存します。

トラブルシューティングのヒント

証明書ファイルの拡張子は .p7b です。 この .p7b ファイルを開くと、チェーンに次の 2 つの証明書が含まれるようになります。

- スタンドアロンのルート CA 証明書の名前
- スタンドアロンの下位 CA 証明書の名前（ある場合）

次の作業

CA 証明書チェーンのインストール, （36 ページ）

CA 証明書チェーンのインストール

はじめる前に

CA 証明書チェーンをダウンロードします。

手順

ステップ 1 [スタート（Start）] > [ファイル名を指定して実行（Run）] を選択します。

ステップ 2 次の操作を実行します。

a) mmc と入力します。

b) [OK] を選択します。

ステップ 3 [ファイル（File）] > [スナップインの追加と削除（FileAdd/Remove Snap-in）] を選択します。

ステップ 4 [スナップインの追加と削除（Add/Remove Snap-in）] ダイアログボックスで [追加（Add）] を選択します。

ステップ 5 [利用できるスタンドアロン スナップイン（Available Standalone Snap-ins）] のリストで [証明書（Certificates）] を選択します。

ステップ 6 [追加（Add）] を選択します。

ステップ 7 [コンピュータ アカウント（Computer account）] を選択します。

ステップ 8 [次へ（Next）] を選択します。

ステップ 9 [コンピュータの選択（Select Computer）] ダイアログボックスから次の手順を実行します。

a) [ローカル コンピュータ:（このコンソールを実行しているコンピュータ）（Local computer: (the computer this console is running on)）] を選択します。

b) [完了（Finish）] を選択します。

c) [閉じる（Close）] を選択します。

d) [OK] を選択します。

ステップ 10 [証明書（Certificates）] コンソールの左ペインで、[証明書（ローカル コンピュータ）（Certificates (Local Computer)）] を展開します。

ステップ 11 [信頼されたルート証明機関（Trusted Root Certification Authorities）] を展開します。

ステップ 12 [証明書（Certificates）] を右クリックします。

ステップ 13 次の操作を実行します。

a) [すべてのタスク（All Tasks）] をポイントします。

b) [インポート（Import）] を選択します。

ステップ 14 インポート ウィザードで [次へ（Next）] を選択します。

ステップ 15 [参照（Browse）] を選択し、自分のコンピュータ上で証明書チェーンがある場所に移動します。

ステップ 16 [開く（Open）] を選択します。

ステップ 17 [次へ（Next）] を選択します。

ステップ 18 [証明書をすべて次のストアに配置する（Place all certificates in the following store）] をデフォルト値のままオンにしておきます。

ステップ 19 [証明書ストア（Certificate store）] の下に [信頼されたルート証明機関（Trusted Root Certification Authorities）] が表示されていることを確認します。

ステップ 20 [次へ（Next）] を選択します。

ステップ 21 [完了（Finish）] を選択します。

次の作業

CA サーバでの証明書要求の送信, （38 ページ）

関連トピック

CA 証明書チェーンのダウンロード, （36 ページ）

CA サーバでの証明書要求の送信

はじめる前に

CA 証明書チェーンをインストールします。

手順

ステップ 1 証明書を必要とするコンピュータで、Web ブラウザを開きます。

ステップ 2 URL **http://<name of your Issuing CA server>/certsrv** を入力します。

ステップ 3 Enter を押します。

ステップ 4 [証明書の要求（Request a certificate）] を選択します。

ステップ 5 [証明書の要求の詳細設定（Advanced certificate request）] を選択します。

ステップ 6 [この CA への要求を作成し、送信する（Create and submit a request to this CA）] を選択します。

ステップ 7 [必要な証明書の種類（Type of Certificate Needed）] リストで [その他（Other）] を選択します。

ステップ 8 [識別情報（Identifying Information）] セクションの [名前（Name）] フィールドに、FQDN と入力します。 この名前は、Microsoft OCS の名前と一致する必要があります。LCS の名前は通常、FQDN です。

ステップ 9 [OID] フィールドに、OID として **1.3.6.1.5.5.7.3.1,1.3.6.1.5.5.7.3.2** と入力します。

（注） OID の中央にある 2 つの 1 をカンマで区切ります。

ステップ 10 次のいずれかの手順を実行します。

a) Windows Certificate Authority 2003 を使用している場合は、[キーのオプション（Key Options）] の [ローカル コンピュータの証明書ストアに証明書を格納する（Store certificate in the local computer certificate store）] をオンにします。

b) Windows Certificate Authority 2008 を使用している場合は、このトピックの「トラブルシューティングのヒント」で説明している回避策を参照してください。

ステップ 11 わかりやすい名前を入力します。

ステップ 12 [送信（Submit）] を選択します。

ステップ 13 [潜在するスクリプト違反（Potential Scripting Violation）] ダイアログボックスで [はい（Yes）] を選択します。

トラブルシューティングのヒント

Windows Certificate Authority 2008 を使用している場合、証明書登録ページでローカル コンピュータ ストアに証明書を保存するためのオプションがなくなりました。 上記のステップ 10 の代わりに、次の回避策を実行してください。

a) Microsoft OCS サーバからサイン アウトします。

b) ローカル ユーザとして Microsoft OCS サーバにサイン インします。
c) 証明書を作成します。
d) CA サーバから証明書を承認します。
e) 証明書をファイルにエクスポートします。
f) Microsoft OCS サーバからサイン アウトします。
g) ドメイン ユーザとして Microsoft OCS サーバにサイン インします。
h) 証明書ウィザードを使用して、証明書ファイルをインポートします。 証明書が、Microsoft OCS 証明書のタブに表示されます（証明書がローカル コンピュータ ストアにインストールされるためです）。

次の作業

証明書の承認およびインストール, （39 ページ）

関連トピック

CA 証明書チェーンのインストール, （36 ページ）

証明書の承認およびインストール

はじめる前に

CA サーバで証明書要求を送信します。

手順

ステップ 1 ドメイン管理者クレデンシャルで企業の下位 CA サーバにサイン インします。

ステップ 2 [スタート（Start）] > [ファイル名を指定して実行（Run）] を選択します。

ステップ 3 次の操作を実行します。

a) mmc と入力します。

b) Enter を押します。

ステップ 4 [ファイル（File）] > [スナップインの追加と削除（FileAdd/Remove Snap-in）] を選択します。

ステップ 5 [追加（Add）] を選択します。

ステップ 6 [スタンドアロン スナップインの追加（Add Standalone Snap-in）] で [証明機関（Certification Authority）] を選択します。

ステップ 7 [追加（Add）] を選択します。

ステップ 8 [証明機関（Certification Authority）] でデフォルト オプションの [ローカル コンピュータ（このコンソールを実行しているコンピュータ）（Local computer (the computer this console is running on)）] を受け入れます。

ステップ 9 [完了（Finish）] を選択します。

ステップ 10 [閉じる（Close）] を選択します。

ステップ 11 [OK] を選択します。

ステップ 12 MMC で、[証明機関（Certification Authority）] を展開し、発行証明書サーバを展開します。

ステップ 13 [保留中の要求（Pending Requests）] を選択します。

ステップ 14 詳細ウィンドウで、次の手順を実行します。

a) 要求 ID で識別される要求を右クリックします。

b) [すべてのタスク（All Tasks）] をポイントします。

c) [発行（Issue）] を選択します。

ステップ 15 証明書の要求元のサーバで [スタート（Start）] > [ファイル名を指定して実行（Run）] を選択します。

ステップ 16 http://<name of your Issuing CA Server>/certsrv と入力します。

ステップ 17 [OK] を選択します。

ステップ 18 [タスクの選択（Select a task）] から、[保留中の証明書の要求の状態（View the status of a pending certificate request）] を選択します。

ステップ 19 証明書要求を選択します。

ステップ 20 [この証明書のインストール（Install this certificate）] を選択します。

次の作業

インストールされた証明書の設定, （40 ページ）

関連トピック

CA サーバでの証明書要求の送信, （38 ページ）

インストールされた証明書の設定

はじめる前に

証明書を承認し、インストールします。

手順

ステップ 1 [スタート（Start）] > [すべてのプログラム（Programs）] > [管理ツール（Administrative Tools）] > [インターネット インフォメーション サービス (IIS) マネージャ（Internet Information Services (IIS) Manager）] を選択します。

ステップ 2 右側のペインで（ローカル コンピュータ）ツリーを展開します。

ステップ 3 [既定の Web サイト（Default Web Site）] を選択します。

ステップ 4 [プロパティ（Properties）] ダイアログボックスを右クリックして開きます。

ステップ 5 [既定の Web サイトのプロパティ（Default Web Site Properties）] ダイアログボックスから [証明書（Certificate）] タブを選択します。

ステップ 6 証明書がすでに選択されている場合は、[証明書の削除（Delete Certificate）] を選択して、選択を解除します。

ステップ 7 [証明書（Certificate）] を選択して、証明書ウィザードを起動します。

ステップ 8 証明書ウィザードを使用して、Microsoft OCS のためにインストールした証明書を選択します。

ステップ 9 **Microsoft Office Communications Server 2007** アプリケーションを起動します。

ステップ 10 右側のペインで、ローカル マシンを表すサーバを選択します。

ステップ 11 サーバを右クリックします。

ステップ 12 [プロパティ（Properties）] > [フロント エンドのプロパティ（Front End Properties）] を選択します。

ステップ 13 [証明書（Certificate）] タブを選択します。

ステップ 14 [証明書の選択（Select Certificate）] を選択します。

ステップ 15 Microsoft OCS のためにインストールした証明書を検索し、選択します。

（注） Microsoft LCS を使用している場合は、上記のステップ 1 ～ 7 に従って、**Microsoft Live Communications Server 2005** アプリケーションを開きます。 管理ページから、目的のサーバを右クリックして、[プロパティ（Properties）] ダイアログボックスを開きます。[セキュリティ（Security）] タブを選択し、[証明書の選択（Select Certificate）] を選択して、新規にインストールした LCS 証明書を選択します。

次の作業

Microsoft OCS での IM and Presence のための TLS ルートの設定, （42 ページ）

関連トピック

証明書の承認およびインストール, （39 ページ）

Microsoft OCS での IM and Presence のための TLS ルートの設定

手順

ステップ 1 **Microsoft Office Communications Server 2007** アプリケーションを起動します。

ステップ 2 右側のペインで Microsoft OCS サーバ プールを右クリックします。

ステップ 3 [プロパティ（Properties）] > [フロント エンドのプロパティ（Front End Properties）] を選択します。

ステップ 4 [フロント エンド サーバのプロパティ（Front End Server Properties）] ダイアログボックスから、[ルーティング（Routing）] タブを選択します。

ステップ 5 [追加（Add）] を選択します。

ステップ 6 次の手順を実行して、スタティック ルートを追加します。

a) [ドメイン（Domain）] フィールドに IM and Presence のホスト名/FQDN を入力します。
（注） これは、IM and Presence 証明書のサブジェクトの CN と一致する必要があります。一致しない場合、Microsoft OCS は IM and Presence との TLS 接続を確立しません。

b) [転送（Transport）] メニューから [TLS] を選択します。

c) [ポート（Port）] フィールドに 5062 と入力します。 ポート番号 5062 は、IM and Presence がピア認証 TLS 接続をリッスンするデフォルトのポートです。

d) [要求 URI 内のホストを置き換える（Replace host in request URI）] をオンにします。

e) [OK] を選択します。

トラブルシューティングのヒント

[Cisco Unified CM IM and Presence オペレーティングシステムの管理（Cisco Unified CM IM and Presence Operating System Administration）] > [セキュリティ（Security）] > [証明書の管理（Certificate Management）] を選択し、証明書の一覧に登録されている証明書を選択すると、IM and Presence 証明書のサブジェクトの CN を確認できます。

次の作業

Microsoft OCS での認証済みホストとしての IM and Presence の設定, （43 ページ）

MicrosoftOCSでの認証済みホストとしてのIMandPresenceの設定

手順

ステップ 1 **Microsoft Office Communications Server 2007** アプリケーションを起動します。

ステップ 2 右側のペインで Microsoft OCS サーバ プールを右クリックします。

ステップ 3 [プロパティ（Properties）] > [フロント エンドのプロパティ（Front End Properties）] を選択します。

ステップ 4 [ホストの承認（Host Authorization）] タブを選択します。

ステップ 5 [追加（Add）] を選択します。

ステップ 6 FQDN を選択し、証明書の記載どおりに CUP X.509 サブジェクトの共通名を入力します。

ステップ 7 [サーバとして帯域を制限する（Throttle as server）] をオンにします。

ステップ 8 [認証済みとして扱う（Treat as Authenticated）] をオンにします。

ステップ 9 [OK] を選択します。

ステップ 10 Microsoft OCS サーバをリブートします。
サーバが再起動すると、Microsoft OCS サーバ プールに、設定したばかりの発信スタティック ルートが表示されます。

次の作業

TLSv1 を使用するような Microsoft OCS の設定, （43 ページ）

TLSv1 を使用するような Microsoft OCS の設定

IM and Presence は TLSv1 のみをサポートするため、TLSv1 を使用するように Microsoft OCS を設定する必要があります。 この手順では、Microsoft OCS が TLS 暗号 TLS_RSA_WITH_3DES_EDE_CBC_SHA で TLSv1 を送信できるように、Microsoft OCS で FIPS 準拠のアルゴリズムを設定する方法について説明します。 この手順では、Microsoft OCS がドメイン コントローラに設定されています。

手順

ステップ 1 [スタート（Start）] > [管理ツール（Administrative Tools）] > [ローカル セキュリティ ポリシー（Local Security Policy）] を選択します。

ステップ 2 コンソール ツリーで [セキュリティの設定（Security Settings）] を選択します。

ステップ 3 [ローカル ポリシー（Local Policies）] を選択します。

ステップ 4 [セキュリティ オプション（Security Options）] を選択します。

ステップ 5 詳細ウィンドウで FIPS セキュリティ設定をダブルクリックします。

ステップ 6 セキュリティ設定を変更します。

ステップ 7 [OK] を選択します。

ステップ 8 Windows Server を再起動し、FIBS セキュリティ設定を有効にします。

次の作業

IM and Presence での Microsoft OCS の新規 TLS ピア サブジェクトの作成, （44 ページ）

IM and Presence での Microsoft OCS の新規 TLS ピア サブジェクトの作成

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS ピア サブジェクト（TLS Peer Subjects）] を選択します。

ステップ 2 [新規追加（Add New）] を選択します。

ステップ 3 [ピア サブジェクト名（Peer Subject Name）] フィールドに、Microsoft OCS が提示する証明書のサブジェクト CN を入力します。

ステップ 4 [説明（Description）] フィールドに Microsoft OCS サーバの名前を入力します。

ステップ 5 [保存（Save）] を選択します。

次の作業

IM and Presence 上の選択された TLS ピア サブジェクト リストへの TLS ピアの追加, （45 ページ）

IM and Presence 上の選択された TLS ピア サブジェクト リストへの TLS ピアの追加

はじめる前に

IM and Presence で Microsoft OCS の新規 TLS ピア サブジェクトを作成します。

手順

ステップ 1 [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [セキュリティ（Security）] > [TLS コンテキスト設定（TLS Context Configuration）] を選択します。

ステップ 2 [検索（Find）] を選択します。

ステップ 3 [Default_Cisco_UPS_SIP_Proxy_Peer_Auth_TLS_Context] を選択します。
[TLS コンテキスト設定（TLS Context Configuration）] ウィンドウが表示されます。

ステップ 4 使用可能な TLS 暗号のリストから、[TLS_RSA_WITH_3DES_EDE_CBC_SHA] を選択します。

ステップ 5 右矢印を選択して、この暗号を [選択された TLS 暗号（Selected TLS Ciphers）] に移動します。

ステップ 6 [空の TLS フラグメントの無効化（Disable Empty TLS Fragments）] をオンにします。

ステップ 7 使用可能な TLS ピア サブジェクトのリストから、設定した TLS ピア サブジェクトを選択します。

ステップ 8 右矢印を選択して、[選択された TLS ピア サブジェクト（Selected TLS Peer Subjects）] に移動します。

ステップ 9 [保存（Save）] を選択します。

関連トピック

IM and Presence での Microsoft OCS の新規 TLS ピア サブジェクトの作成, （44 ページ）

第 8 章

TCP でのロード バランシング

このトピックでは、着信 CSTA/TCP 接続で使用できるように、IM and Presence デュアル ノード設定でロード バランサを組み込む方法について説明します。 ロード バランサには、Cisco CSS 11501 Content Services Switch を推奨します。

次の表では、この統合に合わせて Cisco CSS 11501 Content Services Switch を設定する際に必要となるタスクの概要を示します。 各タスクの詳細については、次の URL で Cisco CSS 11500 Content Services Switch のマニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/contnetw/ps792/products_installation_and_configuration_guides_list.html

表 *1*：*TCP* でのロード バランシングのための *Cisco CSS 11501* 設定チェックリスト

タスク	追加の注意事項
各 IM and Presence サーバの SIP サービス エントリを作成する。	• キープアライブ ポートは、内容と同じポート（ポート 5060）である必要があります。 • キープアライブ メッセージ タイプの値は「tcp」である必要があります。
SIP 規則を作成して、内容およびこの内容を管理するサービスを定義する。	内容は、ポート 5060 の SIP です。 （各 IM and Presence サーバの）SIP サービス エントリは、規則に関連付ける必要があります。
ロード バランサの仮想 IP アドレスを表示するためのネットワーク アドレス変換（NAT）規則を作成する。	NAT 規則では、IM and Presence サーバから Microsoft OCS に戻るパケットを、（IM and Presence サーバから直接発生したものではなく）ロード バランサから発生したものとして示します。

Microsoft OCS では、次のパラメータを設定する必要があります。

- SIP メッセージのルーティングに使用するロード バランサの仮想 IP アドレスとなるネクスト ホップ アドレス。
- ポート 5060 でのデフォルトの TCP リスナー。

IM and Presence では、ロード バランサの仮想 IP アドレスを設定する必要があります。 これは、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [サービス パラメータ（Service Parameters）] > [Cisco SIP プロキシ（Cisco SIP Proxy）] > [一般的なプロキシ パラメータ（クラスタ全体）（General Proxy Parameters (Clusterwide)）] にある、仮想 IP アドレスのフィールドに設定します。

第 9 章

Phone Selection プラグインの導入

Phone Selection プラグインを導入すると、Microsoft Office Communicator クライアント インターフェイスに [IM and Presence] タブが追加され、制御する電話デバイスをユーザが選択できるようになります。 Microsoft Office Communicator が IM and Presence サーバに接続し、ユーザが選択したデバイスを Cisco Unified IP Phone から Cisco IP Communicator に切り替えられない，（51 ページ）に示すように、Microsoft Office Communicator の連絡先リストの下のペインに [電話の選択（Phone Selection）] タブが表示されます。

次の場合、Phone Selection プラグインをインストールする必要があります。

- IM and Presence で、[Microsoft サーバ タイプ（Microsoft Server Type）] の値が [MOC サーバ OCS（MOC Server OCS）] になっている
- ユーザが複数のデバイス（回線）を保有している
- Microsoft OCS で、ユーザの回線 URI がライン アピアランスを一意に識別しない（たとえば、回線 URI に device= または partition= のいずれか、または両方がない）

（注） Microsoft LCS 2005 でリモート通話コントロール機能を実行している場合には、Phone Selection プラグインを使用できません。Microsoft LCS 2005 は、カスタマイズしたタブをサポートしないためです。 Microsoft LCS 2005 を使用している場合は、リモート通話コントロール機能によって、IM and Presence のデバイス選択ロジックに基づき制御するデバイスが決定されます。[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] の GUI で、[アプリケーション（Application）] > [Microsoft RCC] > [設定（Settings）]を選択し、[Microsoft サーバ タイプ（Microsoft Server Type）] の値として [MOC サーバ LCS（MOC Server LCS）] を選択します。

クライアント PC での Phone Selection プラグインのインストール

はじめる前に

この手順を実行するには、Phone Selection プラグイン インストーラ ファイル **Cisco MOC RCC Plug-in.msi** が必要です。これは、[Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] からダウンロードできます。 [アプリケーション（Application）] > [プラグイン（Plugins）] を選択し、Cisco Unified CM IM and Presence MOC Remote Call Control プラグインをダウンロードします。

手順

ステップ 1 クライアント PC で次のコマンドを実行します。CUPFQDN 値には、IM and Presence サーバの FQDN を指定します。
msiexec /I "<plug_in_filename>.msi" CUPFQDN=my-CUP.cisco.com /L*V install_log.txt

（注） このコマンドで IM and Presence サーバの FQDN を指定しない場合、プラグインのインストールが中断します。

ステップ 2 インストール手順に従ってインストールを進め、Phone Selection プラグインのインストールを完了します。

ステップ 3 Microsoft Office Communicator を起動し、IM and Presence タブが接続されてインターフェイスに表示されることを確認します。

リモート コール制御のトラブルシューティング

Microsoft Office Communicator ユーザに DTMF トーンごとにビープ音が 2 回聞こえる

Microsoft Office Communicator をリモート コール制御とともに使用すると、ユーザは Cisco IP Communicator を電話機として選択できます。

このシナリオでは、ユーザが電話をかけ DTMF トーンを入力すると（たとえば、ボイスメールのパスワードの入力）、ボタンを押すごとに Microsoft Office Communicator から 1 回、Cisco IP Communicator から 1 回、合計 2 回 DTMF トーンが鳴ります。 これは、DTMF をインバンドでネゴシエートする場合は正常で予期される動作です。DTMF をアウトオブバンドでネゴシエートする場合は、発生しません。

ユーザが選択したデバイスを Cisco Unified IP Phone から Cisco IP Communicator に切り替えられない

この問題は、Cisco IP Communicator のデバイス名を Cisco Unified Communications マネージャのユーザ名と同じものに設定すると発生する可能性があります。 これは、サポート対象外の設定なので、Cisco IP Communicator のデバイス名を一意の名前に変更する必要があります。

リモートコール制御が機能しない

リモートコール制御が Microsoft Office Communicator ユーザ向けに動作せず、SIP プロキシ サービスが Microsoft Office Communicator サーバからの着信メッセージを処理していない場合、次のことを確認してください。

これは、Microsoft OCS を再起動したあとに、Microsoft Office Communicator に対するサインインの試行が大量かつ同時に行われていることが原因の可能性があります。

それらの大量の試行が同時に行われると、SIP プロキシ サービスは、INVITES および INFO メッセージであふれてしまいます。

1. サービス停止についてユーザに通知し、この間、Microsoft Office Communicator からサインアウトするように勧告してください。
2. SIP プロキシ サービスを停止します。
3. Microsoft OCS を再起動します。
4. SIP プロキシ サービスを再起動します。
5. リモートコール制御が適切に動作するようにするには、再度サインインする必要があることをユーザに通知します。

Microsoft Office Communicator クライアントが IM and Presence タブに接続できない

Microsoft Office Communicator クライアントが IM and Presence タブに接続できない場合は、次のことを確認してください。

- IM and Presence サーバに対して無効な IP アドレスまたは FQDN を指定した可能性があります。 プラグインのインストール手順を繰り返して、ステップ 1 のコマンドで正しい IM and Presence サーバ アドレスを指定します。
- タブ接続の問題が発生した場合には、次の点に注意してください。
  - クライアント PC でブラウザを開き、信頼される Web アドレスのリストに IM and Presence サーバの Web アドレスを追加することが必要になる場合があります。 Microsoft Internet Explorer で、[インターネットオプション（Internet Options）]>[セキュリティ（Security）]>[信頼済みサイト（Trusted Sites）] を選択し、Web アドレス **https://<***IM and Presence_server_name***>** を信頼される Web アドレスのリストに追加します。
  - IM and Presence サーバのセキュリティ ゾーンにドメインの HTTPS Web アドレスを追加することが必要になる場合があります。 Microsoft Internet Explorer で、[インターネット

オプション（Internet Options）] > [セキュリティ（Security）] > [ローカル イントラネット（Local intranet）] > [サイト（Sites）] > [詳細設定（Advanced）] を選択し、セキュリティ ゾーンの Web アドレスのリストにエントリ **https://*.*your-domain*** を追加します。

- この機能を使用するための権限がないことをユーザに通知するエラー メッセージが表示される場合は、IM and Presence で Microsoft Office Communicator に対してユーザを有効にする必要があります。

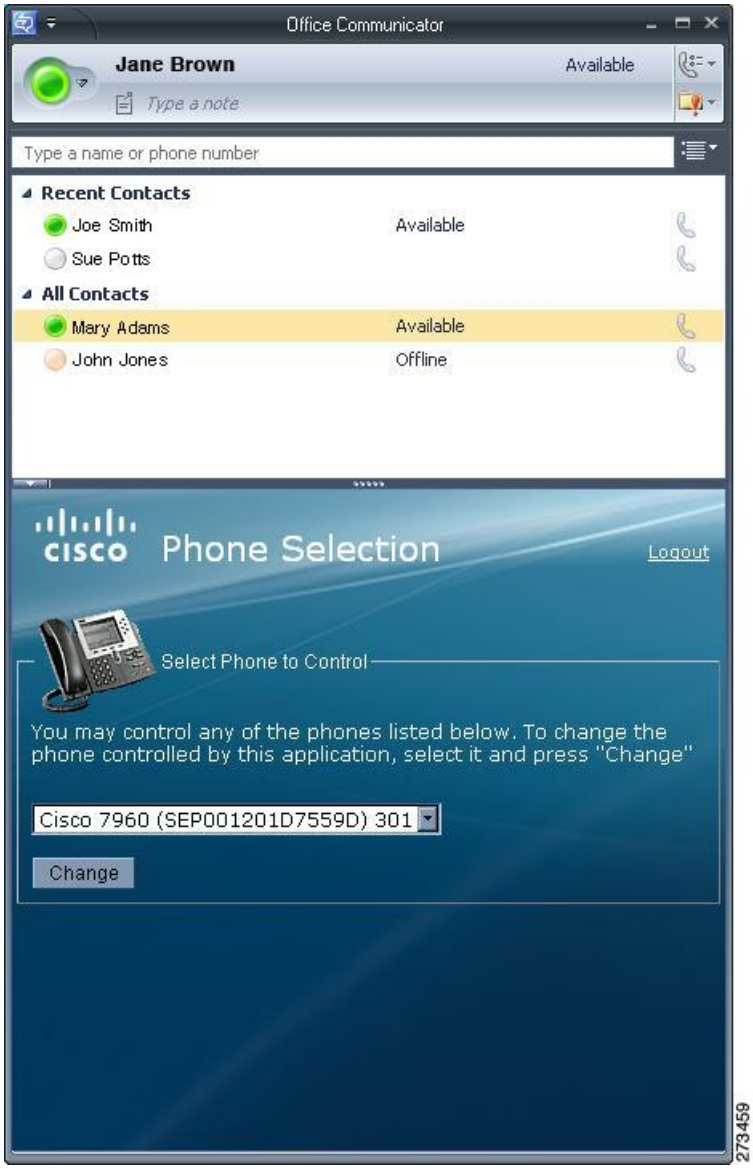
Microsoft Vista にプラグインをインストールする際の問題

Microsoft Vista プラットフォームを実行しているときに、プラグインのインストールで問題が発生した場合は、クライアント PC で User Access Control（UAC; ユーザ アクセス コントロール）を無効にすることが必要になる場合があります。 UAC を無効にするには、次の手順に従います。

1. ローカル管理者グループのメンバーのクレデンシャルでクライアント PC にサイン インします。
2. [スタート（Start）] > [コントロール パネル（Control Panel）] > [ユーザ アカウント（User Accounts）] を選択します。
3. [ユーザ アカウント（User Accounts）] ペインで [ユーザ アカウント（User Accounts）] を選択します。
4. ユーザ アカウントの作業ペインで、[ユーザ アカウント制御の有効化または無効化（Turn User Account Control On or Off）] を選択します。
5. UAC が現時点で管理者承認モードに設定されている場合は、ユーザ アカウント制御メッセージが表示されます。 [続行（Continue）] を選択します。
6. [ユーザ アカウント制御（UAC）を使ってコンピュータの保護に役立たせる（Use User Account Control（UAC）to help protect your computer）] をオフにします。
7. [OK] を選択します。

8 [今すぐ再起動する（Restart Now）] を選択して変更を適用します。

図 *2*：*[*電話の選択（***Phone Selection***）*]* タブのある ***Microsoft Office Communicator*** クライアント



関連トピック

Phone Selection プラグインのアンインストール，（54 ページ）
プラグイン情報の配布，（54 ページ）

Phone Selection プラグインのアンインストール

Phone Selection プラグインをアンインストールするには、クライアント PC で次のコマンドを実行します。

msiexec /x "<plug_in_filename>" /L*V install_log.txt

プラグイン情報の配布

提供する情報	説明
サイン イン情報	IM and Presence インターフェイス用のユーザ名とパスワードが登録されたユーザ ベースを提供します。
Phone Selection プラグインを使用するための手順	『*Quick Start Guide for the Phone Selection Plug-In for the Microsoft Office Communicator Call Control Feature for Cisco Unified Presence Release 7.03*』をユーザに提供します。