モバイルおよびリモートアクセスの設定

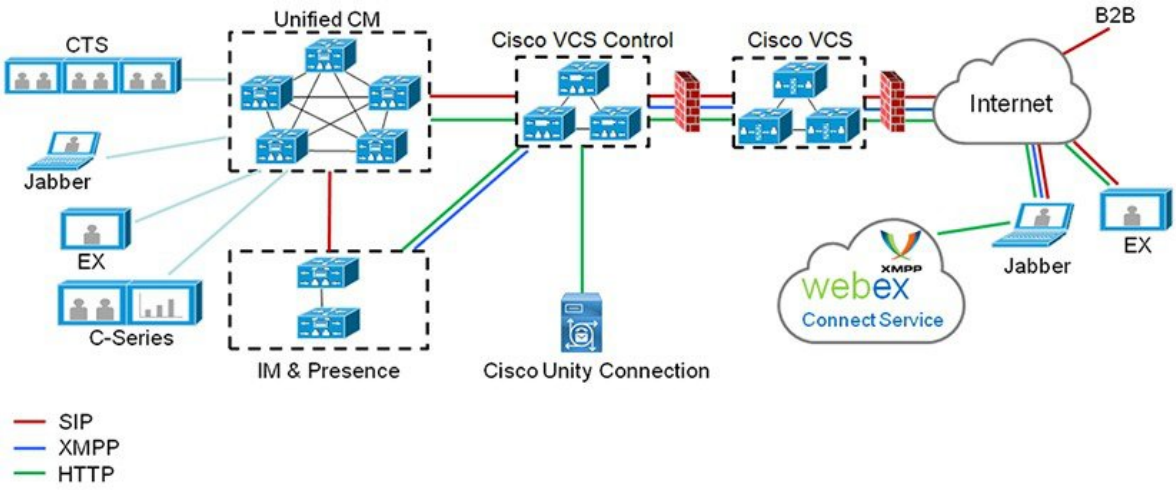
モバイルおよびリモート アクセスの概要

Unified Communications Managerモバイルおよびリモートアクセスは、Cisco Collaboration Edge アーキテクチャの中核となります。これにより、エンタープライズ ネットワーク内にエンドポイントが無い場合、Cisco Jabber などのエンドポイントで、Unified Communications Manager が提供した登録、コール制御、プロビジョニング、メッセージングそしてプレゼンス サービスを保持することができます。Cisco Expresswayは、モバイル エンドポイントをオンプレミス ネットワークに接続し、Unified CM 登録に対して、安全なファイアウォール トラバースと回線側のサポートを提供します。

ソリューションによって以下が実現します。

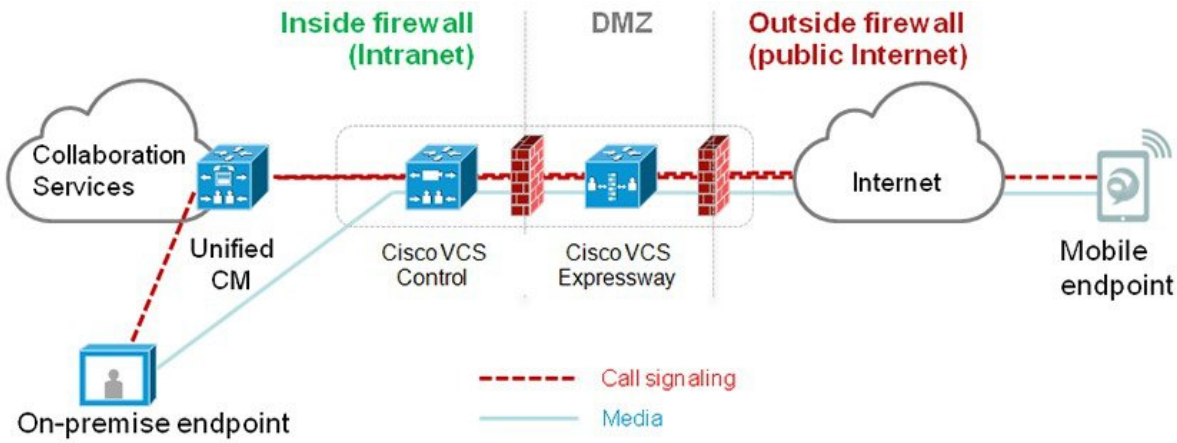
- オフプレミス アクセス：ネットワーク外で、Jabber および EX/MX/SX シリーズ クライアントに一貫性のあるエクスペリエンスを提供
- セキュリティ：セキュアな Business-to-Business（B2B）コミュニケーション
- [クラウド サービス（Cloud services）]：豊富な Cisco Webex 統合とサービス プロバイダ製品を提供するエンタープライズ グレードの柔軟性かつ拡張可能なソリューション
- ゲートウェイと相互運用性サービス：メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

図 *1:* ユニファイド コミュニケーション：モバイルおよびリモート アクセス



サードパーティの SIP または H.323 デバイスを Expressway-C に登録でき、必要に応じて SIP トランクを介して Unified CM に登録されたデバイスと相互運用できます。

図 *2:* 一般的なコール フロー：シグナリングとメディア パス



- Unified CM は、モバイルとオンプレミスの両方のエンドポイントにコール制御を提供します。
- シグナリングは、モバイル エンドポイントと Unified CM の間で Expressway ソリューションを横断します。
- メディアは Expressway ソリューションを横断し、エンドポイント間で直接リレーされます。すべてのメディアが Expressway-C とモバイル エンドポイント間で暗号化されます。

モバイルおよびリモート アクセスの設定

Cisco Jabber ユーザに MRA 機能を有効にするには、Unified Communications Manager の **[ユーザプロファイル構成（User Profile Configuration）]** ウィンドウで、MRA ユーザ ポリシーを設定します。MRA ユーザ ポリシーは、Jabber 以外のエンドポイントでは必要ありません。

また、モバイルおよびリモート アクセスで Cisco Expressway を設定する必要もあります。詳細については、『Cisco Expressway を介したモバイルおよびリモートアクセスの導入ガイド』を参照してください。

モバイルおよびリモートアクセスの前提条件

Cisco Unified Communications Manager の要件

以下の要件が適用されます。

- 複数の Unified Communications Manager クラスタを導入する場合は、ILS ネットワークをセットアップします。
- モバイルおよびリモートアクセスでは、展開用の NTP サーバを設定する必要があります。ネットワーク用の NTP サーバが導入されていて、SIP エンドポイントの電話機 NTP リファレンスであることを確認してください。
- メディア パスを最適化するために ICE を導入する場合は、TURN および STUN サービスを提供できるサーバを導入する必要があります。

DNS の要件

Cisco Expressway への内部接続には、次の Unified Communications Manager を指すローカルで解決可能なDNS SRV を設定します。

```
_cisco-uds._tcp<domain>
```

モバイルおよびリモートアクセスで使用するすべての Unified Communications ノードに対して、転送および逆引き参照用の内部 DNS レコードを作成する必要があります。これにより、IPアドレスまたはホスト名が FQDNの代わりに使用されている場合に、Expressway-C がノードを検索することができます。SRV レコードは、ローカル ネットワークの外部で解決できないことを確認します。

Cisco Expressway の要件

この機能を使用するには、Unified Communications Manager と Cisco Expressway を統合する必要があります。移動とリモートアクセスの Cisco Expressway 構成の詳細については、『Cisco Expressway 導入ガイド』の「モバイルおよびリモートアクセス」を参照してください。

Cisco Jabber を使用して MRA アクセス ポリシーをサポートする一番低い Expressway リリース バージョンは X8.10 です。

証明書の前提条件

Unified Communications Manager、IM and Presence サービスおよび Cisco Expressway-C 間で証明書を交換する必要があります。シスコの推奨は、各システムで同じ CA で CA 署名された証明書を使うことです。この場合、次のように計算します。

- 各システムに CA ルート証明書 チェーンをインストールします（Unified Communications Manager の場合。そして インスタント メッセージおよびプレゼンス サービスは、tomcat 信頼ストアに証明書チェーンをインストールします）。
- Unified Communications Manager の場合は、CA 署名済み tomcat（AXL および UDS トラフィック向け）と Cisco CallManager（SIP 向け）証明書を要求するように CSR を発行します。
- インスタント メッセージおよびプレゼンス の場合は、CSR を発行して CA 署名付き tomcat 証明書を要求します。

（注） 別の CA を使用している場合は、各 CA のルート証明書チェーンを Unified Communications Manager、インスタント メッセージおよびプレゼンス サービスおよび Expressway-C でかならずインストールします。

（注） また、Unified Communications Manager および インスタント メッセージおよびプレゼンス サービスの両方に対しては、自己署名付き証明書を使用することもできます。この場合は、Unified Communications Manager には、tomcat 証明書と Cisco CallManager 証明書を、インスタント メッセージおよびプレゼンス サービスでは tomcat 証明書を Expressway-C にアップロードする必要があります。

モバイルおよびリモート アクセス構成タスク フロー

モバイルおよびリモート アクセス エンドポイントを展開するには、これらのタスクを Unified Communications Manager で実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco AXL Web サービスの有効化 （6 ページ）	パブリッシャ ノードで Cisco AXL Web サービスが有効になっていることを確認します。
ステップ 2	ビデオの最大セッション BitRate の設定 （6 ページ）	**オプション**MRA エンドポイントの地域固有の設定を構成します。例えば、MRA エンドポイントでビデオを使用する場合

	コマンドまたはアクション	目的
		は、**ビデオコールの最大セッションビットレートの設定**を増やす必要があります。これは、ビデオ エンドポイントによっては、デフォルトの設定で384 kbpsが低すぎる可能性があるためです。
ステップ3	デバイス プール MRA の設定 （7 ページ）	MRA エンドポイントが使用するデバイス プールに [日時グループ（Date/Time Group）] と [リージョンの設定（Region configuration）] を割り当てます。
ステップ4	ICE の設定 （7 ページ）	**オプション**ICEはオプションの導入であり、STUN および TURN サービスを使用して、MRA コールの利用可能なメディア パスを分析し、最適なパスを選択します。ICE は、コール セットアップ時間に追加する場合がありますが、これにより MRA コールの信頼性が向上します。
ステップ5	MRA に電話機のセキュリティ プロファイルを設定 （9 ページ）	電話機のセキュリティ プロファイルを設定して、MRA エンドポイントで使用するには、次の手順を実行します。
ステップ6	Cisco Jabber ユーザの MRA アクセス ポリシーの設定 （9 ページ）	Cisco Jabber のみ。Cisco Jabber のユーザに MRA アクセス ポリシーをセットアップします。Cisco Jabber のユーザは、MRA の機能を使用するためにユーザ プロファイル内で MRA アクセスが有効になっている必要があります。
ステップ7	MRA ユーザの設定 （11 ページ）	Cisco Jabber のユーザに対しては、セットアップするユーザ ポリシーをエンドユーザの設定に適用する必要があります。
ステップ8	MRA のエンドポイントの設定 （11 ページ）	MRA 機能を使用するエンドポイントを設定およびプロビジョニングします。
ステップ9	モバイルおよびリモート アクセスに対して Cisco Expressway を設定 （12 ページ）	モバイルおよびリモート アクセスに対して Cisco Expressway を設定します。

Cisco AXL Web サービスの有効化

パブリッシャ ノードで Cisco AXL Web サービスが有効になっていることを確認します。

手順

ステップ 1 [Cisco Unified 有用性（Cisco Unified Serviceability）] から、以下を選択します。 **[Tools（ツール）] > [サービスのアクティブ化（Service Activation）]**

ステップ 2 **[サーバ（Server）]** ドロップダウン リストからパブリッシャ ノードを選択し、**[移動（Go）]** をクリックします。

ステップ 3 **[データベースと管理サービス（Database and Admin Services）]** で、**[Cisco AXL Web サービス（Cisco AXL Web Service）]** が **[有効（Activated）]** になっていることを確認します。

ステップ 4 サービスがアクティブ化されていない場合は、対応するチェックボックスをオンにし、**[保存（Save）]** をクリックしてサービスをアクティブにします。

ビデオの最大セッション BitRate の設定

MRA エンドポイントの地域の設定を構成します。多くの場合、デフォルト設定で十分な場合がありますが、MRAエンドポイントでビデオを使用する場合は、[地域設定（Region Configuration）] で **[ビデオコールの最大セッションレート（Maximum Session Bit Rate for Video Calls）]** を上げる必要があります。DX シリーズなどの一部のビデオ エンドポイントでは、デフォルト設定で 384 kbps が低すぎる場合があります。

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[システム（System）] > [リージョン情報（Region Information）] > [リージョン（Region）]**。

ステップ 2 次のいずれかの操作を行います。

- **[検索（Find）]** をクリックして、既存の地域内のビット レートを編集する地域を選択します。
- **[新規追加（Add New）]** をクリックして新しいパーティションを作成します。

ステップ 3 **[他のリージョンへの関連付けの変更（Modify Relationship to other Regions）]** 領域で、**[ビデオコールのセッション ビット レート（Maximum Session Bit Rate for Video Calls）]** の新規設定を構成します。たとえば、6000 kbps のようになります。

ステップ 4 **[リージョンの設定（Region Configuration）]** ウィンドウでフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンラインヘルプを参照してください。。

ステップ 5 **[保存 (Save)]** をクリックします。

デバイス プール MRA の設定

新しいリージョンを作成した場合は、MRA エンドポイントが使用するデバイス プールに地域を割り当てます。

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[システム（System）] > [デバイス プール（Device Pool）]**。

ステップ 2 次のいずれかを実行します。

- **[検索（Find）]** をクリックし、既存のデバイス グループを選択します。
- [新規追加（Add New）] をクリックして新しいデバイス プールを作成します。

ステップ 3 **デバイス プール名**を入力します。

ステップ 4 冗長する **Cisco Unified Communications Manager グループ**を選択します。

ステップ 5 設定した**日付と時刻グループ**を割り当てます。このグループには、MRA エンドポイント用に設定した電話用 NTP 参照が含まれています。

ステップ 6 **[地域（Region）]** ドロップダウン リストから、MRA に対して設定した地域を選択します。

ステップ 7 **[デバイス プール構成（Device Pool Configuration）]** ウィンドウで、残りのフィールドを入力します。 フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 8 **[保存 (Save)]** をクリックします。

ICE の設定

MRA コールの設定を処理するために ICE を導入する場合は、この手順を使用します。ICE はオプションの導入であり、MRA および TURN サービスを使用して、MRA コールの利用可能なメディア パスを分析し、最適なパスを選択します。ICE は、コール セットアップ時間に追加する場合がありますが、これにより MRA コールの信頼性が向上します。

始める前に

ICE を導入する方法を決定します。電話機グループの ICE は、一般的な電話プロファイル設定、個々の Cisco Jabber デスクトップデバイス、またはすべての電話機に適用されるシステム規模のデフォルト経由で設定できます。

フォールバック メカニズムとして、ICE は、TURN サーバを使用してメディアをリレーできます。TURN サーバが導入されていることを確認してください。

手順

ステップ 1 [Cisco Unified CM Administration] から：

- **[システム（System）]** > **[エンタープライズの電話（Enterprise Phone）]** の順に選択し、ICE に対してシステム デフォルトを設定します。
- **[デバイス（Device）]** > **[デバイスの設定（Device Settings）]** > **[共通電話プロファイル（Common Phone Profile）]** の順に選択し。エンドポイントの グループに対する ICE を設定し、編集するプロファイルを選択します。
- **[デバイス（Device）]** > **[電話機（Phone）]** の順に選択し、個々の Cisco Jabber デスクトップ エンドポイントの ICE を設定し、編集するエンドポイントを選択します。

ステップ 2 **インタラクティブ接続確立（ICE）** セクションまでスクロール ダウンします。

ステップ 3 **[ICE]** ドロップダウン リストを **[有効（Enabled）]** に設定します。

ステップ 4 **[デフォルトの候補タイプ（Default Candidate Type）]**を設定する：

- **[ホスト（Host）]**：ホストデバイスの IP アドレスを選択することによって得られる候補。これはデフォルトです。
- **[サーバ再帰（Server Reflexive）]**：STUN 要求の送信によって取得される IP アドレスとポートの候補。多くの場合、これは NAT のパブリック IP アドレスを表す場合があります。
- **[中継（Relayed）]**：TURN サーバから取得した IP アドレスとポートの候補。IP アドレスとポートは、TURN サーバによってメディアが中継されるように、TURN サーバに常駐しています。

ステップ 5 **[サーバの再帰アドレス（Server Reflexive Address）]** ドロップダウン リストから、このフィールドを **[有効（Enabled）]** または **[無効（Disabled）]** に設定することで、STUN のようなサービスを有効にするか選択します。デフォルトの候補として Server Relexive を設定した場合は、このフィールドを有効に設定する必要があります。

ステップ 6 プライマリ サーバとセカンダリ サーバの IP アドレスまたはホスト名を入力します。

ステップ 7 **[TURN Server のトランスポートタイプ（TURN Server Transport Type）]** を、**[自動（Auto）]**（デフォルト）、**[UDP]**、**[TCP]** または **[TLS]** に設定します。

ステップ 8 TURN Server に**ユーザ名**と**パスワード**を入力します。

ステップ 9 **[保存 (Save)]** をクリックします。

（注） 共通の電話プロファイル用に ICE を設定した場合は、電話機を使用して、そのプロファイルを使用するには共通の電話プロファイルに電話機を関連付ける必要があります。**[電話の設定（Phone Configuration）]** ウィンドウから、プロファイルを電話に適用できます。

MRA に電話機のセキュリティ プロファイルを設定

電話機のセキュリティ プロファイルを設定して、MRA エンドポイントで使用するには、次の手順を実行します。

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。 **[システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）]**

ステップ 2 [Add New] をクリックします。

ステップ 3 **[電話機のセキュリティ プロファイル タイプ（Phone Security Profile Type）]** ドロップダウン リストから、デバイス タイプを選択します。たとえば、Jabber アプリケーションには、**Cisco Unified クライアント サービス フレームワーク** を選択できます。

ステップ 4 **[次へ (Next)]** をクリックします。

ステップ 5 プロファイルの**名前**を入力します。MRA の場合、名前は FQDN 形式である必要があり、エンタープライズ ドメインを含める必要があります。

ステップ 6 **[デバイス セキュリティ モード（Device Security Mode）]** ドロップダウン リストから、**[暗号化（Encrypted）]** を選択します。

（注） このフィールドは、**[暗号化（Encrypted）]** に設定する必要があります。そうでない場合、Expressway が通信を拒否します。

ステップ 7 **[トランスポートタイプ（Transport Type）]** を **[TLS]** に設定します。

ステップ 8 **[TFTP 暗号化設定（TFTP Encrypted Config）]** チェックボックスはオフにします。このチェックボックスをオンにすると、MRA は DX シリーズ、IP 電話7800、IP 電話8811、8841、8845、8861、8865などの電話で起動しなくなるからです。

ステップ 9 **[電話のセキュリティ プロファイルの設定（Phone Security Profile Configuration）]** ウィンドウで、残りのフィールドを設定します。フィールドと設定オプションの詳細については、システムのオンライン ヘルプを参照してください。

ステップ 10 **[保存 (Save)]** をクリックします。

（注） 各 MRA エンドポイントの電話機の設定にこのプロファイルを適用する必要があります。

Cisco Jabber ユーザの MRA アクセス ポリシーの設定

Cisco Jabber のユーザに MRA アクセスポリシーを設定するには、次の手順を使用します。Cisco Jabber のユーザは、MRA の機能を使用するためにユーザ プロファイル内で MRA アクセスが有効になっている必要があります。Cisco Jabber を使用して MRA アクセス ポリシーをサポートする一番低い Expressway リリース バージョンは X8.10 です。

（注） 非 Jabber のユーザには、MRA アクセス ポリシーは不要です。

ユーザ プロファイルの詳細については、『『System Configuration Guide for Cisco Unified Communications Manager』』の「ユーザ プロファイルの概要」章を参照してください。

手順

ステップ 1 [Cisco Unified CM Administration] から、以下を選択します。**[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [ユーザ プロファイル （User Profile）]**。

ステップ 2 [新規追加（Add New）] をクリックします。

ステップ 3 ユーザ プロファイルの [名前（Name）] および [説明（Description）] を入力します。

ステップ 4 [ユニバーサル デバイス テンプレート（Universal Device Template）] を、ユーザの [デスク フォン（Desk Phones）]、[モバイルおよびデスクトップ デバイス（Mobile and Desktop Devices）]、および [リモート接続先/デバイス プロファイル（Remote Destination/Device Profiles）] に割り当てます。

ステップ 5 [ユニバーサル回線テンプレート（Universal Line Template）] をこのユーザ プロファイルのユーザの電話回線に適用するために割り当てます。

ステップ 6 このユーザプロファイルのユーザに自分の電話をプロビジョニングするセルフプロビジョニング機能の使用を許可するには、次の手順を実行します

a) **[エンド ユーザの電話機のプロビジョニングを許可（Allow End User to Provision their own phones）]**のチェックボックスをオンにします。

b) [エンド ユーザのプロビジョニングする電話数を制限（Limit Provisioning once End User has this many phones）] フィールドに、ユーザがプロビジョニングできる電話の最大数を入力します。最大値は 20 です。

ステップ 7 このユーザ プロファイルに関連付けられた Cisco Jabber ユーザがモバイルおよびリモート アクセス（MRA）機能を使用できるようにするには、[モバイルおよびリモート アクセスの有効化（Enable Mobile and Remote Access）] チェック ボックスをオンにします。

（注）
1. デフォルトでは、このチェックボックスはオンになっています。このチェックボックスをオフにすると、[Jabber ポリシー（Jabber Policies）] セクションが無効になり、サービス クライアント ポリシー オプションは、デフォルトで選択されません。
2. この設定は、Cisco Jabber ユーザの場合にのみ必須です。非 Jabber ユーザは、この設定がなくても MRA を使用できます。MRA 機能は、Jabber MRA ユーザにのみ適用され、他のエンドポイントまたはクライアントには適用されません。

ステップ 8 このユーザ プロファイルに Jabber ポリシーを割り当てます。**[Jabber デスクトップ クライアント ポリシー（Jabber Desktop Client Policy）]** と **[Jabber モバイル クライアント ポリシー（Jabber Mobile Client Policy）]** のドロップダウン リストから、次のオプションのいずれかを選択します。

- [サービスなし（No Service）]：このポリシーは、すべての Cisco Jabber サービスへのアクセスを禁止します。
- [IM & Presence のみ（IM & Presence only）]：このポリシーは、インスタント メッセージとプレゼンス機能だけを有効にします。
- [IM とプレゼンス、音声とビデオ コール（IM & Presence, Voice and Video calls）]：このポリシーは音声やビデオ デバイスを使うすべてのユーザに対して、インスタント メッセージ、プレゼンス、ボイスメールと会議機能を有効化します。これがデフォルトのオプションです。

（注） Jabber デスクトップ クライアントには Windows ユーザ用 Cisco Jabber および Mac ユーザ用 Cisco Jabber が含まれています。Jabber モバイル クライアントには、iPad および iPhone ユーザ用 Cisco Jabber および Android ユーザ用 Cisco Jabber が含まれています。

ステップ 9 このユーザ プロファイルのユーザが Cisco Unified Communications セルフケア ポータルで Extension Mobility または Extension Mobility Cross Cluster の最大ログイン時間を設定するには、**[エンド ユーザにエクステンション モビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]** チェックボックスをオンにします。

（注） デフォルトでは **[エンド ユーザにエクステンション モビリティの最大ログイン時間の設定を許可する（Allow End User to set their Extension Mobility maximum login time）]** チェックボックスはオフになっています。

ステップ 10 **[保存 (Save)]** をクリックします。

MRA ユーザの設定

Cisco Jabber のユーザの場合、設定した MRA アクセスポリシーは、LDAP 同期中に Cisco Jabber ユーザに関連付ける必要があります。エンドユーザをプロビジョニングする方法の詳細については、『System Configuration Guide for Cisco Unified Communications Manager』の「エンドユーザの設定」項を参照してください。

MRA のエンドポイントの設定

モバイルおよびリモートアクセス用のエンドポイントをプロビジョニングし、設定します。

- Cisco Jabber クライアントについては、『System Configuration Guide for Cisco Unified Communications Manager』の「*Cisco Jabber* 構成タスク フロー」項を参照してください。
- その他のエンドポイントについては、『System Configuration Guide for Cisco Unified Communications Manager』の「エンドポイントデバイスの設定」項を参照してください。

モバイルおよびリモート アクセスに対して Cisco Expressway を設定

モバイルおよびリモートアクセス用の Cisco Expressway の設定方法に関しては、『Cisco Expressway 導入ガイド』の「モバイルおよびリモートアクセス」を参照してください。