Cisco Meeting Server

シスコ ミーティング サーバ 3.12

Cisco Unified Communications Manager を使用した導入

2025 年 10 月 31 日

コンテンツ

変更履歴 5

1 はじめに 6

1.1 このガイドの使用方法 6

1.1.1 コマンド 8

1.1.2 用語 8

1.2 Meeting Server API の使用方法を簡素化する 8

2 Cisco Unified Communications Manager への SIP トランクの設定 10

2.1 セキュア SIP トランクの設定 11

2.1.1 Meeting Server で必要な設定 11

2.1.2 Cisco Unified Communications Manager で必要な設定 13

2.2 ノンセキュア SIP トランクの設定 18

2.2.1 Meeting Server で必要な設定 18

2.2.2 Cisco Unified Communications Manager で必要な設定 19

3 スケジュールされた通話とランデブー通話を設定する 22

3.1 Meeting Server を設定する 22

3.2 Cisco Unified Communications Manager を設定する 23

3.2.1 ルート グループの設定 24

3.2.2 ルート リストの設定 25

3.2.3 ルートパターンを設定する（発信コールのダイヤルプラン） 26

3.3 Cisco Jabber プレゼンスの更新 28

3.3.1 Cisco Unified Communications Manager を設定する 29

3.3.2 Meeting Server と Cisco Unified Communications Manager/IMP Server 間の安全な通信を有効にする 31

3.3.3 Meeting Server を設定する 31

4 エスカレーションされたアドホックコールを設定する 32
4.1 Meeting Server を設定する 32
4.2 Cisco Unified Communications Manager を設定する 33
4.3 エスカレートされたアドホック コールとライセンス 37

5 ActiveControl のサポート 38
5.1 Meeting Server の ActiveControl 38
5.2 制約事項 38
5.3 ActiveControl と iX プロトコルの概要 39
5.4 SIP 通話内の UDT を無効にする 39
5.5 Cisco Unified Communications Manager で iX サポートを有効にする 40
5.6 Cisco VCS で iX をフィルタリングする 41
5.7 iX のトラブルシューティング 42

6 ロードバランシング通話の概要 43
6.1 着信通話を負荷分散するための Call Bridge の設定 44
6.1.1 Call Bridge グループの作成 44
6.1.2 クラスタの負荷制限を指定し、ロードバランシングを有効にする 45
6.1.3 ロードバランシングを微調整する 47
6.1.4 設定がロードバランシングにどのように使用されるか 47
6.2 発信 SIP 通話の負荷分散 48
6.2.1 発信 SIP 通話のロードバランシングを有効にする方法 49
6.2.2 発信 SIP 通話をロードバランシングするための発信ダイヤルプランルールをセットアップする方法 49
6.2.3 参加者への発信 SIP 通話に使用する Call Bridge グループまたは特定の Call Bridge の提供方法 50
6.2.4 アクティブな空の電話会議のロードバランシングを処理する 50
6.3 Cisco Unified Communications Manager を使用した着信コールの負荷分散の導入例 51

付録 A 複数クラスタを使用するアドホックなエスカレーション 53
A.1 固有の会議ブリッジプレフィックスの使用 54
A.2 通話が適切な Call Bridge に到達することを確認する 54

Cisco の法的情報 56

Cisco の商標または登録商標 57

変更履歴

日付	変更の概要
2025 年 10 月 31 日	3.12 に更新

1 はじめに

Cisco Meeting Server ソフトウェアは、Cisco Unified Computing Server (UCS) テクノロジに基づく特定のサーバ、または仕様ベースの VM サーバでホストできます。 本ドキュメントでは、Cisco Meeting Server を Meeting Server と呼びます。

注：Cisco Meeting Server ソフトウェアバージョン 3.0 以降は X シリーズサーバーをサポートしていません。

注: このドキュメントの「ミーティング サーバ」という用語は、Cisco Meeting Server 2000、Cisco Meeting Server 1000/Small、または仮想ホスト上で実行されているソフトウェアのいずれかを意味します。

このガイドでは、Meeting Server を Cisco Unified Communications Manager と連携させるための設定方法の例を記載しています。 例は、特定の導入に応じて調整する必要がある場合があります。 Avaya および Polycom のコール制御デバイスの使用の詳細については、『サードパーティのコール制御との導入ガイド』を参照してください。 Cisco Expressway を使用している場合、詳細について Expressway のドキュメント を参照してください。

これらの手順は、すべての Meeting Server 導入トポロジ（単一サーバーおよびスケール/レジリエントな導入）に同様に適用されます。

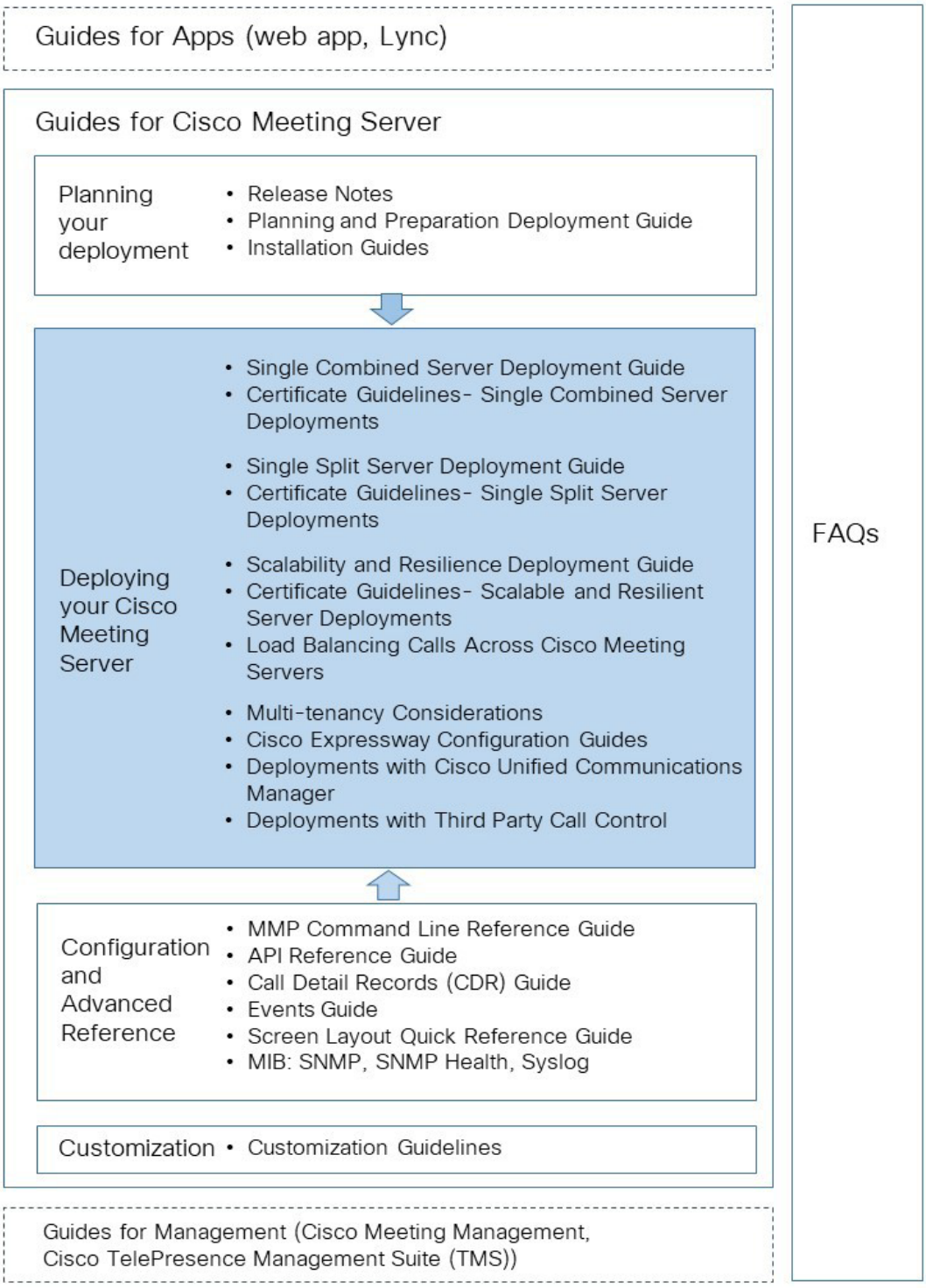
注：Meeting Server は DTMF インバンドトーン（RFC 2833）のみ転送できます。 例えば、エンドポイントが Cisco Unified Communications Manager に帯域外の DTMF を送信し、それが Meeting Server に転送される場合、Meeting Server は DTMF を別のエンドポイントに転送しません。

1.1 このガイドの使用方法

このガイドは、Meeting Server 用のドキュメントセット（図 1 に示されています）

の一部です。 これらのドキュメントは cisco.com で見つけることができます。

図 1：Cisco Meeting Server のドキュメントセット



1.1.1 コマンド

このドキュメントでは、コマンドは**黒**で表示され、指定どおりに入力する必要があります。<> 括弧内に適切な値を入力します。 **青** で例を参照できます。これらは実際の導入に合わせて変更する必要があります。

1.1.2 用語

このドキュメント全体で言及されている電話会議タイプは、表 1 で定義されているものです。

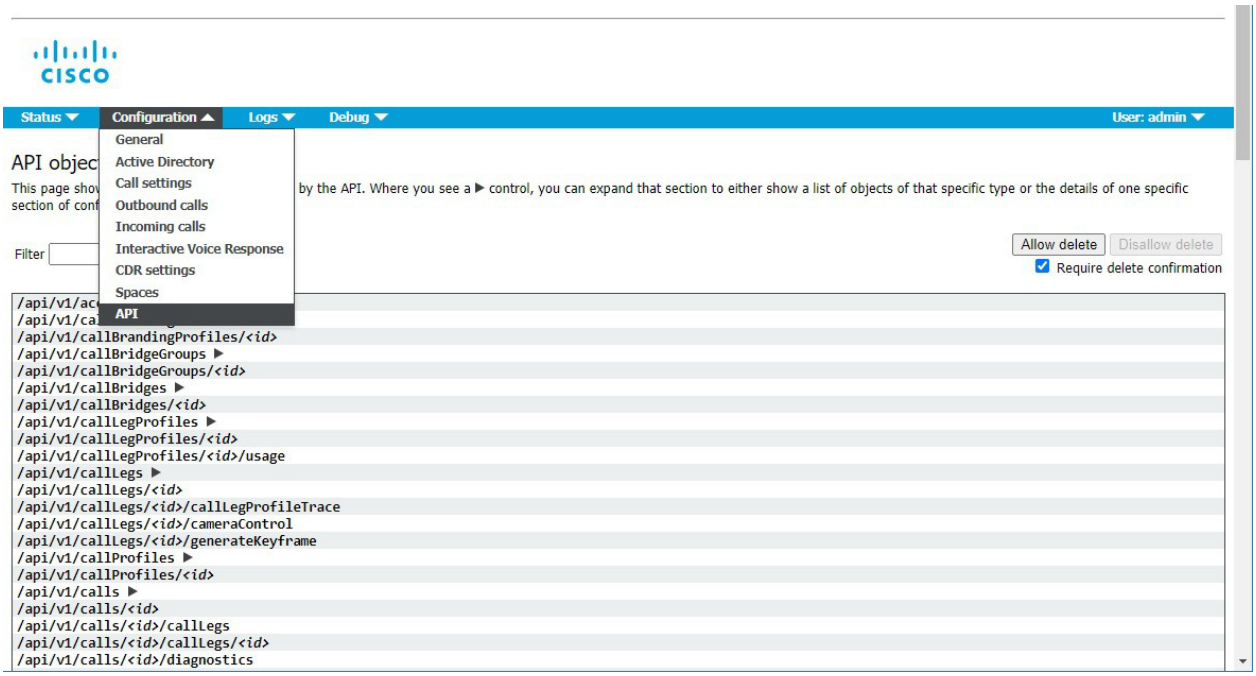
表 1: 電話会議タイプ

電話会議タイプ	説明
ランデブー（別名 パーソナル CMR または VMR）	事前に定義された、常時利用可能なアドレスで、事前のスケジューリングなしに電話会議を可能にします。 主催者はアドレスを他のユーザーと共有します。そのアドレスには他のユーザーがいつでもコールインできます。
アドホック	例えば、ポイントツーポイントコールを手動で 3 人以上の参加者がいるマルチパーティコールにエスカレートする、インスタントまたはエスカレート型の電話会議。
スケジュール	開始時刻と終了時刻がある事前予約済みの電話会議。

1.2 Meeting Server API の使用方法を簡素化する

バージョン 2.9 から、API には API メソッドおよびサードパーティアプリケーションではなく、Meeting Server のWeb 管理インターフェースを使用してアクセスできます。 ウェブ管理インターフェイスにログインした後、**[設定（Configuration）]** タブを選択し、**[API]** プルダウンリストから選択します。 図 2 を参照してください。

図 2: Meeting Serverのウェブ管理インターフェイス経由で API にアクセス



注：Web インターフェイスから API にアクセスするには、サードパーティアプリケーションを使用する場合と同様に、Meeting Server の初期設定と MMP を使用した認証を行う必要があります。

2 Cisco Unified Communications Manager への SIP トランクの設定

この章では、Cisco Unified Communications Manager と Meeting Server 間の SIP トランクのセットアップ方法について説明します。 Meeting Server は次のように設定することができます。

- 単一の統合サーバ、または
- 分割サーバー導入またはスケーラブルでレジリエントな導入のコアサーバー。

注：スケーラブルでレジリエントな導入では、各 Cisco Unified Communications Manager と各 Meeting Server の間に SIP トランクをセットアップする必要があります。 複数の Call Bridge に単一のトランクを使用することはお勧めできません。 アドホック コールの場合、各 Call Bridge ノードにセットアップされた個別のトランクを持つ必要があります。

Cisco はセキュアな SIP トランクをセットアップすることを推奨します。しかし、会社のポリシーにより組織内のトラフィックをノンセキュアなものにしている場合は、ノンセキュアな SIP トランクを設定することができます。
しかし、Cisco Unified Communications Manager での双方向コールを Meeting Server での電話会議にエスカレーションするには、Cisco Unified Communications Manager が Cisco Meeting Server の API と通信する必要があります。 API は HTTPS 通信を必要とします。そのため、エスカレーションされたアドホックコールを機能させるには、証明書を作成して Cisco Meeting Server と Cisco Unified Communications Manager の両方にアップロードする必要があります。また、Cisco Unified Communications Manager は Meeting Server の証明書を信頼する必要があります。

Meeting Server と Cisco Unified Communications Manager の間のスケジュールコールまたはランデブーを許可するだけで、SIP トランクをノンセキュアとして設定している場合、証明書は必要ありません。 コールタイプの定義は、セクション 1.1.2 にあります。

注：お客様が組織の Cisco Unified Communications Manager のサーバー管理者ではない場合、Cisco は強く、ローカル管理者に問い合わせて、サーバー設定に同等の機能を実装する最善の方法をご確認することをお勧めします。

安全な SIP トランクを設定する場合は、 セクション 2.1 を参照してください。 ノンセキュア SIP トランクを設定する場合は、そのまま セクション 2.2 に進んでください。

注：Meeting Server と Cisco Unified Communications Manager（CUCM）との統合の一環として、Jabber 通話用の SIP トランクを設定する際に、[発信側および接続側情報形式（Calling and Connected Party Info Format）] を [接続された第三者の URI と DN を提供する（Deliver URI and DN in connected party）] に設定する場合は、結合された SIP URI（ディレクトリ URI）とディレクトリ番号（DN）の合計を 64 バイト未満に抑えることを強く推奨します。これは、Jabber が参加者リストを正確に表示し、通話エクスペリエンスを向上させるために重要です。

2.1 セキュア SIP トランクの設定

セクション 2.1.1 およびセクション 2.1.2 の手順に従ってセキュアな SIP トランクをセットアップしてから、第 4 章で Cisco Unified Communications Manager 上の双方向通話を Meeting Server 上の電話会議にエスカレートするための設定を行います。

注：アドホックコールの場合、Cisco Unified Communications Manager は HTTPS 接続を介して Meeting Server の API にアクセスする必要があります。 Call Bridge とウェブ管理で異なる証明書を持っている場合、Meeting Server ウェブ管理の証明書に署名したルートおよび中間 CA 証明書を Cisco Unified Communications Manager の信頼ストアにアップロードする必要があります。

セクション 2.1.2 のステップ 2 では、**CallManager-trust** を通じて Cisco Unified Communications Manager の信頼ストアに証明書をアップロードする方法を説明しています。

2.1.1 Meeting Server で必要な設定

Cisco Meeting Server 導入ガイドに従い、Meeting Server を設定します。設定したら、各 Call Bridge で次の手順に従います。

1. ミーティングサーバの MMP に SSH で接続します。
2. MMP コマンドを使ってリスニングインターフェイスを指定します（まだ指定していない場合）。

   ```
   callbridge listen
   ```

3. Call Bridge の秘密鍵と証明書署名リクエスト (.csr) ファイルを生成します。 秘密キーと証明書署名リクエスト（.csr）ファイルの作成方法の詳細については、該当する『Meeting Server の導入の証明書ガイドライン』を参照してください。

   注： Call Bridge 証明書には、Call Bridge がリッスンしているネットワーク インターフェイスの FQDN と一致する CN が含まれている必要があります。

   Cisco Unified Communications Manager には、受け入れる TLS 証明書に関するいくつかの要件があります。 Call Bridge 証明書で SSL クライアントと SSL サーバーが有効になっていることを確認する必要があります。 これは証明書の署名段階で行われます。

4. CA (パブリック CA または内部 CA) に署名のために Call Bridge 証明書を提出します。 内部 CA の署名付き証明書は受け入れ可能です。 ただし、自己署名証明書はサポートされていません。

5. 署名したら、openSSL または **pki inspect** コマンドを使用して証明書が OK であることを確認します。

   - **pki Inspect <certificatename>** を入力し、**[X509v3 拡張キー使用：TLS ウェブサーバー認証、TLS ウェブクライアント認証（X509v3 Extended Key Usage: TLS Web Server Authentication, TLS Web Client Authentication）]** をオンにします。または
   - **openssl x509 -in <certificatename> -noout -text -purpose** と入力します。
   例えば
   openssl x509 -in callBridge1.crt -noout -text -purpose

   出力で重要な行は、**SSL client** と **SSL server** で、それらに対して必ず **Yes** が必要です。例えば、

   証明書の目的:

   SSL クライアント：はい

   SSL クライアント CA：いいえ

   SSL サーバ：はい

6. SFTP を使用して、署名済み証明書、および中間 CA バンドル (ある場合) を Call Bridge にアップロードします。

7. 証明書と秘密鍵を Call Bridge に割り当てます。

a. MMP に SSH で接続する

b. 次のコマンドを入力します:

```
callbridge certs <keyfile> <certificatefile>[<cert-bundle>]
```

keyfile と **certificatefile** は、一致する秘密キーと証明書のファイル名です。 CA が証明書バンドルを提供している場合は、バンドルも証明書とは別のファイルとして含めます。

次に例を示します。

```
callbridge certs callBridge1.key callBridge1.crt callBridge1-bundle.crt
```

c. 変更を適用するために、Call Bridge インターフェイスを再起動します。

```
callbridge restart
```

証明書が Call Bridge に正常にインストールされると、次のメッセージが表示されます。

```
SUCCESS: listen interface configured
SUCCESS: Key and certificate pair match
```

証明書のインストールに失敗すると、次のエラーメッセージが表示されます。

失敗：キーと証明書の問題：証明書とキーが一致しません

注：Cisco Unified Communications Manager は、CA および Call Bridge の証明書に署名したすべての中間 CA を信頼する必要があります。 これを行うには、ステップ 4 で作成した Call Bridge 証明書を、**CallManager-trust** を介して Cisco Unified Communications Manager のトラストストアにアップロードします。セクション 2.1.2 のステップ 2 を参照してください。

注：証明書の作成と Meeting Server へのアップロードの詳細については、該当する『Cisco Meeting Server 証明書ガイドライン』を参照してください。

2.1.2 Cisco Unified Communications Manager で必要な設定

テストは、メディアの終了点（MTP）が設定されていないトランクで行われました。 したがって、

- 導入に悪影響を及ぼさない場合は、MTP を無効にすることができます。 SCCP 電話を使用していて、Meeting Server に DTMF を送信する必要がある場合、MTP をオフにすると、導入に悪影響を与える可能性があります。

- 上記が有効な実装ではない場合、同時コールの数に応じて、Cisco Unified Communications Manager で MTP 容量を増やす必要があります。

1. CallManager サービスが有効になっている各 Cisco Unified Communications Manager に、CallManager サービスの CA 署名付き証明書をインストールすることができます。
   注：Meeting Server はデフォルトでは受け取った証明書を検証せず、すべての有効な証明書を受け入れ、通話マネージャの自己署名証明書も受け入れるため、これは推奨であり、必須ではありません。
   a. Cisco Unified Communications Manager **[OS 管理（OS Administration）]** ページにログインし、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
   b. **証明書リスト** ウィンドウで、 **CSR の生成**をクリックします。
   c. **[証明書名（Certificate Name）]** ドロップダウンメニューから **[CallManager]** を選択します。
   d. [**CSR の生成**] をクリックして証明書署名リクエストを生成します。
   e. CSR が正常に生成されたら、[**CSR のダウンロード**] をクリックします。 [署名リクエストのダウンロード（署名リクエストのダウンロード）] ダイアログボックスで、**[CallManager]** を選択し、**[CSR のダウンロード（Download CSR）]** をクリックします。
   f. 認証局によって署名されたこの CSR を取得します。 内部 CA の署名付き証明書は受け入れ可能です。
   g. CA から証明書が返却されたら、**[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate chain）]** ウィンドウに移動します。 **[証明書目的（Certificate Purpose）]** ドロップダウンメニューで、**[CallManager-trust]** を選択します。 最初にルート証明書、次に中間証明書を参照してアップロードします。 **[証明書目的（Certificate Purpose）]** ドロップダウンメニューで、**[CallManager]** を選択します。 CallManager サービスの証明書を参照し、アップロードします。
   h. 新しい証明書を有効にするには、メンテナンス期間中に **[Cisco Unified Serviceability]** で CallManager サービスを再起動する必要があります。

2. セクション 2.1.1 のステップ 4 で生成した証明書のルートおよび中間証明書を Cisco Unified Communications Manager トラストストアにアップロードします。
   a. Cisco Unified Communications Manager **[OS 管理（OS Administration）]** ページから、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
   b. **[証明書のアップロード/証明書チェーン]** をクリックします。 [証明書のアップロード/証明書チェーン] ポップアップ ウィンドウが表示されます。
   c. **[証明書目的（Certificate Purpose）]** ドロップダウンメニューで、**[CallManager-trust]** を選択します。
   d. 参照して、まずルート証明書をアップロードし、次に中間証明書を **CallManager-trust にアップロードします**。
3. SIP トランク セキュリティ プロファイルを作成します。

   Cisco Unified Communications Manager は、**[非セキュア SIP トランク（Non Secure SIP Trunk）]** というデフォルトのセキュリティプロファイルを適用します。これは TCP 用の SIP トランクを作成する場合です。 TLS、または標準のセキュリティプロファイル以外のものを使用するには、これらの手順に従ってください:
   a. Cisco Unified Communications Manager Administration にログインします。
   b. **[システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** に移動します。
   c. **[新規追加]** をクリックします。
   d. 以下のようにフィールドに入力します。
      - **[名前（Name）]** = 名前を入力（例：CMS_SecureTrunk）
      - **[端末セキュリティモード（Device Security Mode）]** = **[暗号化済み（Encrypted）]** を選択
      - **[受信トランスポートタイプ（Incoming Transport Type）]** = **[TLS]** を選択
      - **[発信トランスポートタイプ（Outgoing Transport Type）]** = **TLS** を選択
      - **[X.509 サブジェクト名（X.509 Subject Name）]** = Call Bridge 証明書の CN を入力。

- **[受信ポート（Incoming Port）]** = TLS リクエストを受信するポートを入力 TLS のデフォルトは 5061
- **[Replaces ヘッダーを受け入れる（Accept Replaces Header）]** = Call Bridge のグループ化を使用する場合は、このボックスにチェックを入れます（セクション 6 を参照）。

e. [保存] **をクリックします。**

注: ビデオに対応した会議参加者が 2 人以上いるアドホック会議の場合、**[デバイス セキュリティ モード]** が **[暗号化]** に設定され、サービス パラメータ **[ビデオ会議ではなく暗号化された音声会議を選択]**が **[true]** (デフォルト) に設定されていると、Cisco Unified Communications Manager は暗号化された音声会議ブリッジを割り当てます。 このパラメータが **false** に設定されている場合、Cisco Unified Communications Manager は暗号化されていないビデオ会議ブリッジを割り当てます。これは、Cisco Unified Communications Manager は現在暗号化されたビデオ会議ブリッジをサポートしていないためです。 サービスパラメータ **[ビデオ会議の代わりに暗号化音声会議を選択する（Choose Encrypted Audio Conference Instead Of Video Conference）]** をリセットするには **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** > **[クラスタ全体のパラメータ（機能 - 電話会議）（Clusterwide Parameters (Feature - Conference)）]** に移動します。

---

4. SIP プロファイルが正しく設定されていることを確認してください。 Cisco Unified Communications Manager バージョン 10.5.2 以降でデフォルトの **[TelePresence 電話会議の標準 SIP プロファイル（Standard SIP Profile For TelePresence Conferencing）]** を使用している場合は、これで十分です。 (古いバージョンの Cisco Unified Communications Manager を使用している場合は、 セクション 5.5 を参照してください。) **[iX アプリケーションメディアを許可（Allow iX Application Media）]**、**[SIP リクエストで完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）]**、**[BFCP を使用するプレゼンテーションの共有を許可（Allow Presentation Sharing using BFCP）]** のキー値がオンになっていることを確認します。
5. SIP トランクを作成する

a. Cisco Unified Communications Manager で、**[デバイス（Device）] > [トランク（Trunk）]** に移動します。

b. **[新規追加]** をクリックします。

c. これらのフィールドを設定します。

- **[トランクタイプ（Trunk Type）]** = **SIP トランク**
- **[デバイスプロトコル（DeviceProtocol）]** = **SIP**
- **[トランクサービスタイプ（Trunk Service Type ）]** = **[なし（None）]**（デフォルト）

d. **[次へ] をクリックします**

e. SIP トランクの宛先情報を設定します。 表 2 を参照してください。

表 2: SIP トランクの宛先情報

フィールド	説明
デバイス名	名前を入力します（例」CiscoMeetingServer（スペースは使用できません））
デバイス プール	お使いのデバイスを所属させたいプール（Cisco Unified Communications Manager の **[システム（System）] > [デバイスプール（Device Pool）]** で設定されたとおり）
[SRTPを許可(SRTP Allowed)]	**[SRTP を許可（SRTP Allowed）]** を選択してメディア暗号化を許可します
[着信] >コーリングサーチスペース	Cisco Unified Communications Manager から Meeting Server 上のミーティングへのエスカレートされた双方向アドホックコールのみを許可する場合、デフォルトを選択する必要はありません。
[アウトバウンドコール（Outbound Calls）] > [発信側トランスフォーメーション CSS（Calling Party Transformation CSS）]	必要に応じて選択します。
[SIP 情報] >宛先アドレス	単一の Meeting Server の FQDN を入力します。Meeting Server 証明書の CN と一致する必要があります。 注：クラスタの場合、単一の Meeting Server の FQDN を入力します
[SIP 情報] >宛先ポート	TLS に **5061** を入力

[SIPトランクセキュリティプロファイル(SIP Trunk Security Profile)]	ステップ 3 で作成したセキュリティ プロファイルを選択します。
再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）	Call Bridge グループを実行するとき、これを、発呼者のパーティションを含むコーリングサーチスペースに設定します。
[CTIプロファイル(SIP Profile)]	**[TelePresence 電話会議の標準 SIP プロファイル（Standard SIP Profile For TelePresence Conferencing）]** を選択
正規化スクリプト	**cisco-telepresence-conductor-interop** をこの SIP トランクに割り当てます。 注：理想的には、Cisco のウェブサイトから最新の正規化スクリプトをダウンロードしてください。 Conductor がいない場合でも、Meeting Server には Conductor と同じ相互接続性の問題があります。そのため、このスクリプトはコア Meeting Server へのトランクに適しています。
すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）	他の CUCM ノードへの発信通話も希望する場合、このチェックボックスを選択します。

6. [**保存**] をクリックして設定を適用します。
   トランクリストを使用して、数分後にトランクが稼働状態になることを確認します。

2.2 ノンセキュア SIP トランクの設定

セクション 2.2.1 およびセクション 2.2.2 の手順に従い、ノンセキュア SIP トランクをセットアップします。その後、第 3 章に従って、Cisco Unified Communications Manager と Meeting Server 間のランデブーおよびスケジュールされたコールを有効にします。

2.2.1 Meeting Server で必要な設定

Cisco Meeting Server 導入ガイドに従い、Meeting Server を設定します。設定ができたら、以下を行います。

1. Meeting Server の MMP に SSH で接続します
2. MMP コマンドを使ってリスニングインターフェイスを指定します（まだ指定していない場合）。

```
callbridge listen
```

2.2.2 Cisco Unified Communications Manager で必要な設定

テストは、メディアの終了点（MTP）が設定されていないトランクで行わ
れました。 したがって、

- 導入に悪影響を及ぼさない場合は、MTP を無効にすることができます。 SCCP 電話を使用していて、Meeting Server に DTMF を送信する必要がある場合、MTP をオフにすると、導入に悪影響を与える可能性があります。
- 上記が有効な実装ではない場合、同時コールの数に応じて、Cisco Unified Communications Manager で MTP 容量を増やす必要があります。

1. SIP トランク セキュリティ プロファイルを作成する

   Cisco Unified Communications Manager は、**[非セキュア SIP トランク（Non Secure SIP Trunk）]** というデフォルトのセキュリティプロファイルを適用します。これは TCP 用の SIP トランクを作成する場合です。 このデフォルトのセキュリティプロファイルを使用するか、名前を付けて新しいプロファイルを作成し、他のオプションはデフォルトのままにしておくことができます。 既定のプロファイル設定を確認するか、新しいプロファイルを作成するには、次の手順に従います:

   a. Cisco Unified Communications Manager Administration にログインします。

   b. **[システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** に移動します。

   c. [**新規追加**] をクリックします。

   d. [名前] フィールドに次のように入力します。

      - **[名前（Name）]** = 名前を入力します。例えば「CMS_SecureTrunk」と入力し、

      デフォルトのフィールドが次のようになっていることを確認します。

      - **[デバイスセキュリティモード（Device Security Mode）]** = **[保護なし（Non Secure）]** を選択
      - **[受信トランスポートタイプ（Incoming Transport Type）]** = [TCP+UDP] を選択
      - **[発信トランスポートタイプ（Outgoing Transport Type）]** = TCP を選択

- **[受信ポート（Incoming Port）]**。 TCP のデフォルトは 5060
- **[Replaces ヘッダーを受け入れる（Accept Replaces Header）]** = Call Bridge のグループ化を使用する場合は、このボックスにチェックを入れます（セクション 6 を参照）。

e. [保存] **をクリックします。**

2. SIP トランクを作成する

a. Cisco Unified Communications Manager で、**[デバイス（Device）] > [トランク（Trunk）]** に移動します。

b. [**新規追加**] をクリックします。

c. これらのフィールドを設定します。

- **[トランクタイプ（Trunk Type）]** = **SIP トランク**
- **[デバイスプロトコル（DeviceProtocol）]** = **SIP**
- **[トランクサービスタイプ（Trunk Service Type ）]** = **[なし（None）]**（デフォルト）

d. [**次へ**] **をクリックします**

e. SIP トランクの宛先情報を設定します。 表 3 を参照してください。

表 3: SIP トランクの宛先情報

フィールド	説明
デバイス名	名前を入力します（例」CiscoMeetingServer（スペースは使用できません））
デバイス プール	デバイスを所属させたいプール（Cisco Unified Communications Manager の [システム（System）] > [デバイスプール（Device Pool）] **で設定）**
[SRTPを許可(SRTP Allowed)]	SRTP を許可しない
[着信] >コーリングサーチスペース	デフォルトを選択します。
[アウトバウンドコール（Outbound Calls）] > [発信側トランスフォーメーション CSS（Calling Party Transformation CSS）]	必要に応じて選択します。

[SIP 情報] >宛先アドレス	Meeting Server の FQDN を入力することをお勧めします（または DNS ルックアップを利用します）。
[SIP 情報] >宛先ポート	TCP に **5060** を入力
再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）	Call Bridge グループを実行するとき、これを、発呼者のパーティションを含むコーリングサーチスペースに設定します。
[SIPトランクセキュリティプロファイル(SIP Trunk Security Profile)]	手順 1 で作成したセキュリティ プロファイルを選択します。
[CTIプロファイル(SIP Profile)]	**[TelePresence 電話会議の標準 SIP プロファイル（Standard SIP Profile For TelePresence Conferencing）]** を選択
正規化スクリプト	ノンセキュア SIP トランクでは必要ありません。

f. **[保存（Save）]** をクリックします。

3 スケジュールされた通話とランデブー通話を設定する

セキュア SIP トランク（セクション 1.1）またはノンセキュア SIP トランク（セクション 1.2 を参照）のセットアップ後、セクション 3.1 およびセクション 3.2 の手順に従い、Meeting Server から Cisco Unified Communications Manager へのランデブーとスケジュールされた通話を有効にします。

3.1 Meeting Server を設定する

1. Meeting Server から Cisco Unified Communications Manager に送信される通話の発信ダイヤルプランルールを設定します。
2. Meeting Server の Web 管理インターフェイスを使用して、**[設定（Configuration）]**>API の順に選択します。
   a. API オブジェクトのリストで、**/outboundDialPlanRuless** の後 の ▶ をタップします
   b. [新規作成] **をクリックします。**
   c. 以下の表 4 のパラメータを入力します

表 4: 発信ダイヤルプランルールを設定する

パラメータ	説明
ドメイン	Cisco Unified Communications Manager に送信する必要があるコールにマッチさせるドメインを入力します
使用する SIP プロキシ（SIP proxy to use）	いずれかについて確認します。 このフィールドを空にしておくと、サーバーは**_sips.tcp.<yourcucmdomain>** を使ってステップ b で入力したドメインに対して DNS SRV 検索を実行します。 これを解決できない場合、サーバーは **<yourcucmdomain>** の DNS A 検索を試みます。 これに失敗すると、**_sip.tcp.<yourcucmdomain>** の SRV 検索を試みます。それでも失敗する場合は、**sips.udp.<yourcucmdomain>** の検索を試みます。 または、サーバーが使用する SIP プロキシを入力します。例えば、Cisco Unified Communications Manager の FQDN です。 このドメインは上記の箇条書きに従って解決されます。

	または、Cisco Unified Communications Manager の IP アドレスを入力します。
ローカル連絡先ドメイン（Local contact domain）	このフィールドは空白にしてください。Lync または Skype for Business への SIP トランクをセットアップする場合にのみ必要です。
ローカルからのドメイン（Local from domain）	通話を発信者として認識させるドメイン（発信者 ID）を入力します。 **注：[ローカルからのドメイン（Local from domain）]** を空のままにしておくと、発信者番号 ID に使用されるドメインは、デフォルトで **[ローカル連絡先ドメイン（Local contact domain）]** になります。この場合は空白です。
トランクタイプ（Trunk type）	[標準 SIP（Standard SIP）] を選択します。
Priority	必要に応じて設定します。
暗号化	導入に適したモードを選択します。 例えば、トラフィックが SIP トランクで暗号化されない場合、[非暗号化（Unencrypted）] を選択します。

d. [作成（Create）] **をクリックします。**

3.2 Cisco Unified Communications Manager を設定する

Cisco Unified Communications Manager は、ルートパターン、ルートグループ、およびルートリストを使用して、コールを正しいロケーションに転送します。

ルートグループでは、トランクが選択される順序を指定することができます。 例えば、2 つの長距離電話通信事業者を使用する場合、ルートグループを追加して、より安価な通信事業者への長距離コールが優先されるようにすることができます。最初のトランクが利用できない場合に限り、通話はより高額な通信事業者にルートされます。

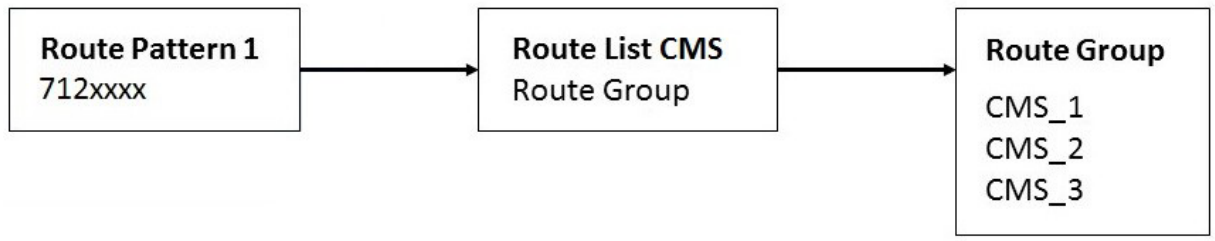
ルート リストは、優先順位が指定されている 1 組のルート グループに関連付けられます。また、ルート リストは、1 つ以上のルート パターンに関連付けられ、そのルート グループがアクセスされる順位を決定します。 この順位は、発信コールに使用可能なデバイスを検索するときの進行を制御します。 ルート リストには、ルート グループだけを入れることができます。 各ルート リストには、少なくとも 1 つのルート グループを入れる必要があります。 ルート グループは、任意の数のルート リストに追加できます。

ルート パターンは、アドレスを表す数字のストリングと、ルート リストまたはゲートウェイにコールをルート指定するように関連付けられた数字操作のセットから構成されています。 ルートパターンは、ルートフィルタおよびルートリストと連動して、コールを特定のデバイスに誘導し、特定の数字パターンの組み込み、除外、または変更を行います。

メディアリソースグループはメディアサーバーの論理的なグループを定義します。 必要に応じて、メディアリソースグループを地理的な場所またはサイトに関連付けることができます。 また、サーバーの使用方法やサービスのタイプ（ユニキャストまたはマルチキャスト）を制御するためのメディアリソースグループも必要に応じて作成できます。

ルートグループ、ルートリスト、リソースグループの詳細については、お使いの Cisco Unified Communications Manager のバージョンの『Cisco Unified Communications Manager システムガイド』を参照してください。

図 3: 通話を正しいロケーションに転送する



注：スケーラブルでレジリエントな Meeting Server の導入を設定しない場合は、Cisco Unified Communications Manager でルートグループやルートリストをセットアップする必要はありません。 Cisco Unified Communications Manager から発信コールのダイヤルプランを設定する場合、まずルートパターンを作成します。ドメインベースのルーティング の場合は、**設定した SIP トランクへの SIP トランク/ルートリスト**を指定し、数字ダイヤル の場合は、 **設定した SIP トランクへのゲートウェイ/ルートリスト**を指定し、その後**ルートオプション**で**このパターンをルートする**を選択します。

3.2.1 ルート グループの設定

1. [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] インターフェイスにログインします。
2. **[コールルーティング（Call Routing）] > [ルート/ハント（Route/Hunt）] > [ルートグループ（Route Group）]** に移動します。 既存のルートグループのリストが表示されます。

3. 適切でない場合は、**[新規追加（Add New）]** をクリックします。
4. 以下を完了します。
   - [ルートグループ名（Route Group Name）] = ルートグループの目的を反映する名前を入力します。例：CMS_1
   - ドロップダウンから配信アルゴリズムを選択します。例：**[上から（Top Down）]**
   - **利用可能なデバイス** リストから適切な SIP トランクを選択し、**[ルートグループに追加する]** ボタンをクリックします。
   - このルートグループに関連する他のフィールド
5. **[保存（Save）]** をクリックします。
6. ルート グループのリストをチェックすることで、新しいルート グループが作成されたことを確認します。

3.2.2 ルート リストの設定

1. **[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ルートリスト（Route List）]** に移動します。 既存のルートリストの一覧が表示されます。
2. 適切でない場合は、**[新規追加（Add New）]** をクリックします。
3. 以下を完了します。
   - [名前] = ルートリストの目的を反映する名前を入力します。例: Route List US
   - **[Cisco Unified Communications Manager グループ（Cisco Unified Communications Manager Group）]** ドロップダウンリから、**[デフォルト（Default）]** を選択します。
   - **[保存（Save）]** をクリックします。
   - **[ルートリストメンバー情報（Route List Member Information）]** セクションで、**[ルートグループの追加（Add Route Group）]** を選択し、リストに追加するルートグループを **[選択したグループ（Selected Groups）]** に選択します。
   - このルートリストに該当する他のフィールド
4. **[保存（Save）]** をクリックします。
5. ルートリストのリストをチェックすることで、新しいルートリストが作成されたことを確認します。

3.2.3 ルートパターンを設定する（発信コールのダイヤルプラン）

ドメインベースのルーティングを Cisco Unified Communications Manager インターフェース経由で Meeting Server に設定できます。例：@mydomain.example.com または番号ベースのルーティング（例：7XXX） 次に例を示します。

ドメインベースのルーティングの例

Cisco Unified Communications Manager から Meeting Server へのすべてのドメインベースの通話をルーティングするには、以下を行います。

1. **[コールルーティング（Call Routing）]** > **[SIP ルートパターン（Sip Route Pattern）]** に移動します。
2. 適切でない場合は、**[新規追加（Add New）]** をクリックします。
3. 以下を完了します。
   - [パターンの用途（Pattern Usage）] = ドメインルーティング
   - IPv4 パターンのような **mydomain.example.com**
   - [説明（Description）] = 任意の内容
   - ルートパーティション = このルールが属するルートパーティション

   注： さまざまなダイヤルプランルールがルートパーティションに添付され、コーリングサーチスペース（CSS）はルートパーティションのリストで構成されます。 ユーザごと、電話ごと、またはトランクごとに、異なる CSS を設定できます。 発信が行われると、Cisco Unified Communications Manager は、ルールに一致するものが見つかるまで、CSS の各ルート パーティションを調べます。
4. **[保存（Save）]** をクリックします。

数字ダイヤルの例

この基本的な例では、7 で始まるすべてのものを Meeting Server にルーティングします。

1. **[コールルーティング（Call Routing）]** > **[ルート/ハント（Route/Hunt）]** > **[ルートパターン（Route Pattern）]** に移動します。 既存のルートパターンのリストが表示されます。
2. 適切でない場合は、**[新規追加（Add New）]** をクリックします。
3. 以下を完了します。
   - ルートパターン = 703777XXX (ページの下の方で様々な変換を設定できます。例えば、桁破棄フィールドで、PreDot を選択して、この例の先頭の 7 を削除します。)
   - [ルートパーティション（Route Partition）] = このルールが属するルートパーティション

     注： さまざまなダイヤルプランルールがルートパーティションに添付され、コーリングサーチスペース（CSS）はルートパーティションのリストで構成されます。 ユーザごと、電話ごと、またはトランクごとに、異なる CSS を設定できます。 発信が行われると、Cisco Unified Communications Manager は、ルールに一致するものが見つかるまで、CSS の各ルート パーティションを調べます。
   - [説明（Description）] = 適切なテキスト
   - **[ゲートウェイ/ルートリスト（Gateway/Route List）]** ドロップダウンから、ルートパターンに追加するルートリストを選択します。
4. **[保存（Save）]** をクリックします。
5. テストコールをいくつか行います。 エンドポイントを Cisco Unified Communications Manager に登録し、Meeting Server 上でスペースを作成し、Cisco Unified Communications Manager からのコールを受け入れるための着信ダイヤルプランルールを作成する必要があります。 設定方法については、適切な『Cisco Meeting Server 導入ガイド』を参照してください。

3.3 Cisco Jabber プレゼンスの更新

Meeting Server は、Cisco Meeting Server ウェブアプリミーティングにいる間、Cisco Jabber（Jabber）ユーザーのプレゼンス状況を更新するように設定できます。

Jabber でプレゼンスを更新するには:

- Meeting Server のログイン ID はメールである必要があり、AD の $mail$ 属性にマッピングされる必要があります。
- Cisco Unified Communications Manager では、同じユーザーの $mail$ 属性がディレクトリ URI フィールドにマッピングされている必要があります。
- Jabber ログインは、Cisco Unified Communications Manager のディレクトリ URI またはユーザ ID フィールドのいずれかを介して行うことができます。

Jabber ユーザーがウェブアプリにサインインしてミーティングに参加すると、Meeting Server は Jabber 状況を「通話中」に更新し、ユーザーがミーティングを終了すると以前の状況に戻ります。

ミーティング サーバは、会議中に最大 8 時間、ユーザのセッション状態とプレゼンス情報をサポートします。

Meeting Server は、以下の場合には Jabber 状況を更新しません。

- Jabber ユーザーがウェブアプリミーティングに参加中に、別のミーティング/通話に参加している場合、Meeting Server は Jabber ステータスを更新しません。
- Jabber ユーザーがウェブアプリミーティングに参加する前に、ステータスを **[DND - サイレント]** に設定している場合、Meeting Server は Jabber のステータスを更新しません。
- ユーザーがウェブアプリミーティング中の任意の時点で Jabber ステータスを手動で更新した場合、Meeting Server は手動で更新されたユーザーステータスを上書きしません。

注：

- この機能は、ゲストとして参加するウェブアプリの参加者または参加者をサポートしていません。SIP エンドポイント、Lync、または Skype を通じて参加することはサポートされていません。
- Meeting Server はコンテンツ共有の在席情報を更新しません。

ユーザープレゼンスを更新するには、AXL サービスを提供する Cisco Unified Communications Manager のノードで Meeting Server を設定します。 Meeting Server は、各々が最大で 5 つの Cisco Unified Communications Manager のクラスタと、Cisco Unified Communications Manager のクラスタごとに 6 つの Cisco Unified Communications Manager IM & Presence ノードを持つ、複数のクラスタで設定することができます。 ユーザーが割り当てられている Cisco Unified Communications Manager/Cisco Unified Communications Manager IM & Presence ノードに関係なく、ユーザーのプレゼンスは更新されます。

注：Meeting Server は、TCP ポート 8083 を使用して Cisco Unified Communications Manager IM & Presence サーバーと接続します。Cisco Unified Communications Manager IM & Presence サーバーと Meeting Server のコールブリッジの間にファイアウォールがある場合は、通信を許可するためにこのポートを開くことを推奨します。

3.3.1 Cisco Unified Communications Manager を設定する

Jabber でプレゼンスを更新するには、Cisco Unified Communications Manager ノードで次のユーザーを作成する必要があります。

- **AXL ユーザー - `<axl_user>`** - このユーザーは、ロール**標準 AXL API アクセス**を持つアプリケーションユーザーです。 管理者は、**標準 AXL API アクセス**のロールを持つ新しいユーザーグループを作成し、それをユーザーに割り当てる必要があります。
- **プレゼンスユーザー** - **`<presence_user>`** - このユーザーは、事前に定義されたグループ **[Admin-サードパーティ API（Admin-3rd Party Api）]** に割り当てられたアプリケーションユーザーです。

注：

- すべてのクラスタの導入で ILS が実行されている必要があります。
- クラスタ間ピアリングは、すべての Cisco Unified Communications Manager IM & Presence ノードで有効にする必要があります。

3.3.1.1 ユーザーグループを作成し、ロールを割り当てる

以下のステップに従い、**標準 AXL API アクセス**のロールを持つ新しいグループを作成します。

1. [Cisco Unified CM の管理（Cisco Unified Communications Manager Administration）] インターフェイスにログインします。

2. **[ユーザー管理（User Mnagement）]** > **[ユーザー設定（User Settings）]** > **[アクセス制御グループ（Access Control Group）]** に移動します。
3. [**新規追加**] をクリックします。
4. [**アクセスコントロールグループ情報**] セクションで次の情報を入力します:
   - **[名前（Name）]** = AXL グループの名前を入力します。例：CUCM_AXL_Group
5. 右上隅から、**[関連リンク（Related Links）]** > **[アクセス制御グループへの権限の割り当て（Assign Role to Access Control Group）]** に移動します。
6. **[標準 AXL API ユーザー（Standard AXL API Users）]** を選択し、**[選択項目の追加（Add selected）]** をクリックします。
7. **[保存（Save）]** をクリックします。

3.3.1.2 ユーザーを作成し、ユーザーグループを割り当てる

以下のステップに従い、AXL およびプレゼンスのユーザーを作成し、適切なグループを割り当てます。

1. **[ユーザー管理（User Management）]** > **[アプリケーションユーザー（Application User）]** > **[新規追加（Add New）]** に移動します。
2. **[新規ユーザーの追加（Add New user）]** ページで必要なすべての情報を入力します。
3. **権限情報**セクションで、**[アクセスコントロールグループに追加する] を選択します。**
4. 利用可能な **アクセスコントロールグループ**のリストから:
   a. AXL ユーザーの場合：セクション 3.3.1.1 に記載されているステップで作成したグループを選択します。
   b. Presence_user の場合：**[Admin-サードパーティ API（Admin-3rd Party API）]** を選択します。
5. **[選択項目の追加（Add Selected）]** をクリックします。
6. **[保存]** をクリックします。

3.3.2 Meeting Server と Cisco Unified Communications Manager/IMP Server 間の安全な通信を有効にする

callbridge 証明書バンドルは、Cisco Unified Communications Manager IM & Presence サーバの CUPS 信頼ストアと、Cisco Unified Communications Manager の Tomcat 信頼ストアにアップロードする必要があります。

同様に、Cisco Unified Communications Manager IM & Presence サーバー用の CUPS 証明書と Cisco Unified Communications Manager 用の Tomcat 証明書を Meeting Server にアップロードし、確認する必要があります。 証明書の検証の詳細は、 MMP ユーザガイド を参照してください。

3.3.3 Meeting Server を設定する

AXL サービスを提供する Cisco Unified Communications Manager ノードで Meeting Server を設定します。 Meeting Server は、各々が最大で 5 つの Cisco Unified Communications Manager のクラスタと、Cisco Unified Communications Manager のクラスタごとに 6 つの Cisco Unified Communications Manager IM & Presence ノードを持つ、複数のクラスタで設定することができます。

MMP コマンド **`callbridge ucm add <hostname/IP> <axl_user> <presence_user>`** を使用して、Cisco Unified Communications Manager のホスト名/IP アドレスと、AXL および IMP サーバーのアプリケーションユーザーの資格情報を提供します。 コマンドの一覧は、Cisco Meeting Server MMP 『コマンドラインリファレンスガイド』を参照してください。 コマンドは、各 Cisco Unified Communications Manager のクラスタに対して個別に実行する必要があります。

4 エスカレーションされたアドホックコールを設定する

セキュア SIP トランクを設定した後（セクション 1.1 を参照）、セクション 4.1 と セクション 4.2 のステップに従って、Cisco Unified Communications Manager の双方向通話を Meeting Server の電話会議にエスカレーションできるようにします。

注：SIP トランクをノンセキュアとしてセットアップすることにした場合でも、Cisco Unified Communications Manager での双方向通話を電話会議にエスカレートする際に証明書を使用する必要があります。Meeting Server は、Cisco Unified Communications Manager が Cisco Meeting Server の API と通信することを必要とします。 API は HTTPS 通信を必要とするため、エスカレートされたアドホックコールが機能するには、証明書を作成し、Cisco Meeting Server と Cisco Unified Communications Manager の両方にアップロードする必要があり、それぞれが互いの証明書を信頼する必要があります。

注：スペースと S4B ゲートウェイ通話間のカスケードに対応しています。 ただし、スペースにダイヤルし、同じ Meeting Server でアドホックコールを拡大すること（つまり、2 つのスペース間でカスケードすること）はサポートされていません。 異なる Meeting Server 上の 2 つのスペース間でのカスケード接続は可能ですが、ユーザーエクスペリエンスが低下するため推奨できません。

4.1 Meeting Server を設定する

1. Meeting Server で着信ダイヤルプランをセットアップします。 該当する『Cisco ミーティング 導入ガイド』を参照してください。 （注：アドホックコールの場合、Cisco Unified Communications Manager で定義されたトランクアドレスが着信コールルールに含まれている必要があります。トランクアドレスは、Cisco Unified Communications Manager からの着信 URI が使用するものです。）
2. Cisco Unified Communications Manager が使用する「api」権限を持つ管理者ユーザーアカウントをセットアップします。 「Cisco Meeting Server MMP コマンドライン リファレンスガイド」を参照してください。

4.2 Cisco Unified Communications Manager を設定する

Cisco Unified Communications Manager と Meeting Server 間の臨時呼び出しでは、Cisco Unified Communications Manager は HTTPS 接続を通じて Meeting Server の API にアクセスする必要があります。 Call Bridge とウェブ管理で異なる証明書を持っている場合、Meeting Server ウェブ管理の証明書に署名したルートおよび中間 CA 証明書を Cisco Unified Communications Manager の信頼ストアにアップロードする必要があります。
これは、セキュアまたは非セキュア SIP トランクを設定したかどうかに関係なく、実行する必要があります。 このセクションの手順を実行する前に、これが完了していることを確認してください。

注：セクション 4 のステップ 2 では、**CallManager-trust** を通じて Cisco Unified Communications Manager の信頼ストアに証明書をアップロードする方法を説明しています。

Meeting Server は、Cisco Unified Communications Manager で電話会議ブリッジとして扱われます。

1. 各 Meeting Server について、会議ブリッジを作成します
    a. Cisco Unified Communications Manager Administration で、**[メディアリソース（Media Resources）] > [会議ブリッジ（Conference Bridge）]** を選択します。 **[会議ブリッジの検索/一覧表示（Find and List Conference Bridges）]** ウィンドウが表示されます。
    b. **[新規追加]** をクリックします。 **[会議ブリッジの設定（Conference Bridge Configuration）]** ウィンドウが表示されます。
    c. **[会議ブリッジタイプ（Conference Bridge Type）]** ドロップダウンメニューから、**[Cisco Meeting Server]** を選択します。（オプションとして **Cisco Meeting Server** を持たない古いバージョンの Cisco Unified Communications Manager ソフトウェアを使用している場合は、 **Cisco TelePresence Conductor を選択してください。**.）
    d. **[デバイス情報（Device Information）]** ペインに Meeting Server の名前と説明を入力します。

e. Meeting Server がこの Cisco Unified Communications Manager のクラスタに直接接続されていない一元化された導入のためのアドホック電話会議を導入する場合、**[会議ブリッジプレフィックス（Conference Bridge Prefix）]** を入力します。 詳細については 付録 Aを参照してください。

注：導入内の Meeting Server ノードと Cisco Unified Communications Manager のクラスタの各ペアに、一意の会議ブリッジプレフィックスを設定します。

---

f. **[SIP トランク（SIP Trunk）]** ドロップダウンメニューから SIP トランクを選択します。

g. **[HTTP インターフェイス情報（HTTP interface information）]** を入力して、Cisco Unified Communications Manager と Cisco Meeting Server の間に安全な HTTPS 接続を作成します。 注：

   i. これはお使いの Web 管理者インターフェースおよびポートと一致している必要があります。

   ii. Web 管理者が SIP トランクとは別のアドレスでリッスンしている場合、**[HTTP アドレスとしての SIP トランク宛先の上書き（Override SIP Trunk Destination）]** チェックボックスをオンにします。

   iii. アドレスフィールドが Web 管理者にロードされた証明書と一致している必要があります。

h. **[保存（Save）]** をクリックしてから、**[リセット（Reset）]** をクリックします。

i. Meeting Server が Cisco Unified Communications Manager に登録されていることを確認します。

2. Meeting Server をメディアリソースグループ（MRG）に追加します。

   MRG の数は、導入のトポロジによって異なります。

   a. **メディアリソース** > **メディアリソースグループ**に移動してください。

   b. **[新規追加]** をクリックして新しいメディアリソースグループを作成し、名前を入力します。

c. ステップ 1 で作成した 1 つ以上の電話会議ブリッジを、**[使用可能なメディアリソース（Available Media Resources）]** ボックスから **[選択されたメディアリソース（Selected Media Resources）]** ボックスに移動します。

d. **[保存（Save）]** をクリックします。

3. メディア リソース グループ (MRG) をメディア リソース グループ リスト (MRGL) に追加します。 MRGL の数は、導入のトポロジによって異なります。

   各 MRGL について、

   a. **メディアリソース** > **メディア リソース グループ リスト**に移動してください。

   b. **[新規追加（Add New）]** をクリックして新しいメディア リソース グループ リストを作成し、名前を入力するか、既存の MRGL を選択し、それをクリックして編集します。

   c. ステップ 2 で作成した 1 つ以上のメディアリソースグループを、**[使用可能なメディアリソースグループ（Available Media Resource Groups）]** ボックスから、**[選択されたメディアリソースグループ（Selected Media Resource Groups）]** ボックスに移動します。

   d. **[保存（Save）]** をクリックします。

4. MRGL をデバイス プールまたはデバイスに追加します。

   実装に応じて、デバイス プールを構成してすべてのエンドポイントに適用するか、個々のデバイス (エンドポイントなど) を特定の MRGL に割り当てることができます。 MRGL がデバイス プールとエンドポイントの両方に適用される場合、エンドポイント設定が使用されます。 デバイスプールまたはデバイスの詳細については、Cisco Unified Communications Manager のドキュメントを参照してください。

   a. **[システム（System）]** > **[デバイスプール（Device Pool）]** に移動します。

   b. **[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、名前を入力するか、既存のデバイスプールを選択し、それをクリックして編集します。

   c. **[デバイスプール設定（Device Pool Settings）]** セクションで、ドロップダウンメニューから適切な Cisco Unified Communications Manager グループを選択します。

d. **[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]** セクションで、ドロップダウンメニューを使用して、**[日時グループ（Date/Time Group）]**、**[地域（Region）]**、および上のステップ 2f で作成した **[メディア リソース グループ リスト（Media Resource Group List）]**を選択します。 他のフィールドはデフォルトの (または以前に設定した) 値のままにします。

e. **[保存]** と [**リセット**] をクリックして変更を有効にします。 プールに関連付けられているデバイスがある場合、[リセット] をクリックすると、デバイスが再起動されます。

新しいデバイス プールが作成された場合:

f. **[デバイス（Device）]** > **[電話（Phones）]** に移動します。

g. **[検索（Find）]** をクリックして、デバイスプール設定を変更するデバイスを選択します。

h. ドロップダウンメニューから、上記のステップ 3b で作成したデバイスプールを選択します。

i. **[保存（Save）]** をクリックします。

j. **[設定の適用（Apply Config）]** をクリックします。

k. **[リセット（Reset）]** をクリックして、変更内容を有効にします。 これにより、適用されるとエンドポイントが再起動します。

5. Cisco Unified Communications Manager Session Management Edition を導入する場合は、次のいずれかを実行します。

a. 適切な Meeting Server ノードをポイントする電話会議プレフィックスセット（ステップ 1e）を持つ通話のダイヤルプランルールをセットアップする。

b. コール情報ヘッダーを取り除く LUA スクリプトを使用してリーフノードからトランクを設定し、すべての Meeting Server ノードをポイントするようにダイヤルプランルールを設定する。

注：Meeting Server ノードと Cisco Unified Communications Manager 間のアド ホック コール エスカレーションの設定ステップについては、付録 A を参照してください。 付録では、通話情報ヘッダーを取り除くサンプル LUA スクリプトも提供します。

4.3 エスカレートされたアドホック コールとライセンス

エスカレートされたアドホック コールは、PMP Plus または SMP Plus ライセンスのいずれかを使用します。 PMP Plus ライセンスを使用する場合:

1. Cisco Unified Communications Manager は、コールをエスカレートするユーザーの objectGUID を提供する必要があります。
2. この objectGUID を持つユーザーは、Meeting Server にインポートされる必要があります。
3. ユーザーは関連する PMP Plus ライセンスを持っている必要があります。

注：Cisco Unified Communications Manager は現在、Active Directory からインポートされたユーザーに objectGUID のみを提供します。 別の LDAP ソースを使用している場合、Cisco Unified Communications Manager は必要な情報を Meeting Server に渡しません。

---

5 ActiveControl のサポート

Meeting Serverは、主催された通話に対して ActiveControl をサポートしています。 CE 8.3+ ソフトウェアがインストールされた Cisco SX、MX または DX エンドポイントを使用する参加者の場合、ActiveControl によりミーティングの詳細を受け取り、ミーティング中にエンドポイント インターフェイスを使用していくつかの管理タスクを実行することができます。

5.1 Meeting Server の ActiveControl

Meeting Server は、ActiveControl が有効なエンドポイントへの次のミーティング情報の送信をサポートしています。

- 参加者リスト (参加者リストとも呼ばれます): 通話の参加者の名前と参加者の合計数を確認することができます。
- 発言中の参加者の音声アクティビティのインジケータ、
- 現在プレゼンテーションを行っている参加者を示すインジケータ、
- ミーティングが録画されているか、ストリーミングされているか、および通話中にセキュアではないエンドポイントが含まれているかどうかを示すインジケータ、
- すべての参加者に表示されるオンスクリーンメッセージ、

また、ActiveControl が有効なエンドポイントでこれらの管理タスクをサポートしています。

- エンドポイントに使用するレイアウトを選択し、
- ミーティングの他の参加者を切断します。

5.2 制約事項

- ActiveControl が有効な通話が、9.1 (2) より古い Unified CM バージョンの Unified CM トランクを通過する場合、通話は失敗する場合があります。 ActiveControl は、古い Unified CM トランク (Unified CM 8.x 以前) では有効にしないでください。
- ActiveControl は SIP のみの機能です。 H.323 インターワーキングシナリオはサポートされていません。

5.3 ActiveControl と iX プロトコルの概要

ActiveControl は、SIP セッション記述プロトコル (SDP) のアプリケーション回線として通知される iX プロトコルを使用します。 Meeting Server 自動的に ActiveControl をサポートしますが、この機能は無効にできます。セクション第 5.4 項を参照してください。 遠端ネットワークが不明であるか、iX プロトコルをサポートしないデバイスがあることがわかっている状況では、Meeting Server と他のコール制御またはビデオ会議デバイス間の SIP トランクで iX を無効にするのが最も安全です。 例:

- Unified CM 8.x 以前のシステムへの接続では、古い Unified CM システムは ActiveControl 対応デバイスからの発信を拒否します。 これらの通話の失敗を回避するには、ネットワーク内の Unified CM 8.x デバイスに向かうトランクで iX を無効のままにしておきます。 SIP プロキシ経由で 8.x デバイスに到達する場合、iX がプロキシへのトランクで無効になっていることを確認します。
- サードパーティネットワークへの接続用。 このような場合、サードパーティのネットワークが ActiveControl 対応デバイスからの呼び出しをどのように処理するかはわからず、処理システムによっては拒否される場合があります。 このような通話の失敗を避けるには、サードパーティネットワークへのすべてのトランクで iX を無効のままにします。
- 外部ネットワークに接続する、または内部で古い Unified CM バージョンに接続する、Cisco VCS 中心の導入用。 Cisco VCS X8.1 から、ゾーン フィルターをオンにして、外部ネットワークまたは古い Unified CM システムに送信される INVITE 要求の iX を無効にすることができます。 (既定では、このフィルターはオフになっています。)

5.4 SIP 通話内の UDT を無効にする

ActiveControl は、エンドポイントへの参加者リストの送信、通話中の他の参加者の切断、導入間の参加者リストなど、特定の機能に UDT トランスポートプロトコルを使用します。 UDT はデフォルトで有効になっています。 診断の目的で UDT を無効にすることができます。例えば、コールコントロールが UDT を使用しない場合で、これがコールコントロールがMeeting Serverからのコールを受けない原因であると考えられる場合です。

Meeting Server の Web 管理インターフェイスを使用して、**[設定（Configuration）]>API** の順に選択します。

1. API オブジェクトのリストで、**/compatibilityProfiles** の後の ► をタップします。
2. 既存の互換性プロファイルの **object id** をクリックするか、または新しい互換性プロファイルを作成します
3. パラメータ **sipUDT** = **false** を設定します。 **[変更（Modify）]** をクリックします。
4. API オブジェクトのリストで、**/system/profiles** の後の ► をタップします。
5. [**表示または編集**] ボタンをクリックします
6. **[選択（Choose）]** をクリックし、パラメータ **compatibilityProfile** の右側を選択します。上記のステップ 3 で作成した互換性プロファイルの **オブジェクト ID** を選択します。
7. [**変更**] をクリックします。

5.5 Cisco Unified Communications Manager で iX サポートを有効にする

iX プロトコルのサポートは、Cisco Unified Communications Manager で一部の SIP プロファイルに対してデフォルトで無効になっています。 Unified CM で iX サポートを有効にするには、まず SIP プロファイルのサポートを設定し、それから SIP プロファイルを SIP トランクに適用します。

SIP プロファイルでの iX サポートの設定

1. **[デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** を選択します。 [SIP プロファイルの検索と一覧表示] ウィンドウが表示されます。
2. 次のいずれかを実行します。
   a. 新しい SIP プロファイルを追加するには、 **新規追加**をクリックします。
   b. 既存の SIP プロファイルを変更するには、検索条件を入力して **[検索（Find）]** をクリックします。 更新する SIP プロファイルの名前をクリックします。

   [SIP プロファイル設定] ウィンドウが表示されます。
3. **[iX アプリケーションメディアを許可（Allow iX Application Media）]** のチェックボックスを選択します
4. 追加の設定変更を加えます。
5. [保存] **をクリックします。**

SIP トランクへの SIP プロファイルの適用

1. **[デバイス（Devce）] > [トランク（Trunk）]** を選択します。

   [トランクの検索と一覧表示] ウィンドウが表示されます。

2. 次のいずれかを実行します。

   a. 新しいトランクを追加するには、**[新規追加]** をクリックします。

   b. トランクを変更するには、検索条件を入力して、**[検索] をクリックします。**
   更新するトランクの名前をクリックします。

   [トランク設定] ウィンドウが表示されます。

3. [SIP プロファイル] ドロップダウンリストから、適切な SIP プロファイルを選択します。

4. **[保存（Save）]** をクリックします。

5. 既存のトランクを更新するには、**[設定の適用（Apply Config）]** をクリックして新しい設定を適用します。

5.6 Cisco VCS で iX をフィルタリングする

プロトコルをサポートしない近隣ゾーンの iX アプリケーション回線をフィルタリングするように Cisco VCS を設定するには、SIP UDP/IX フィルターモードの詳細設定オプションがオンに設定されているカスタムゾーンプロファイルでゾーンを設定する必要があります。

アドバンストゾーンプロファイルのオプション設定を更新するには:

1. 新しい近隣ゾーンを作成するか、既存のゾーンを選択します (**設定 > ゾーン > ゾーン**)。

2. **[ゾーンプロファイル（Zone profile）]**の詳細設定のパラメータ項で、まだ選択されていない場合は、*[カスタム（Custom）]* を選択します。 ゾーンプロファイルの詳細設定オプションが表示されます。

3. **SIP UDP/IX フィルタモード** ドロップダウンリストから **オン**を選択します。

4. **[保存（Save）]** をクリックします。

5.7 iX のトラブルシューティング

表 5: iX ヘッダーを含む通話の通話処理の概要

シナリオ	結果
Unified CM 8.x またはそれ以前	通話が失敗する
Unified CM 9.x 9.1(2) 以前	通話は正常に処理されるが、ActiveControl はなし
Unified CM 9.1(2)	通話は正常に処理され、ActiveControl もある
エンドポイント - iX および SDP 実装のサポートなし	エンドポイントが再起動する可能性があるか、通話が失敗する可能性がある

6 ロードバランシング通話の概要

この章では、Cisco Unified Communications Manager 導入内のMeeting Serverのスケーラビリティとレジリエンスを向上させる方法について説明します。

Call Bridge のグループは、クラスター化された Call Bridge 間で通話の負荷を分散するために使用されます。 Cisco Unified Communications Manager の主なロールは、Cisco Meeting Server の指示に従って、Call Bridge グループ間で通話を転送することです。 ローカル Call Bridge への各トランクは、[ヘッダーの置換を承認] チェックボックスが選択された SIP トランク セキュリティ プロファイルを使用するように設定する必要があります。 詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。

Cisco Unified Communications Manager でロケーションごとにルートグループを設定することで、ローカル Call Bridge を介した着信通話のバランシングを行います。ルートグループには、そのロケーションのローカル電話会議リソースへのリンクが含まれます。 ルートグループは循環配信でセットアップされ、Meeting Server 間でコールの負荷を分散する必要があります。 セクション 6.1 を参照してください。

ローカル Call Bridge を介した発信通話の分散は、スペースからの発信 SIP 通話のロードバランシングを有効にし、発信 SIP 通話の負荷を分散するための発信ダイヤルプランルールを設定することで実現します。 セクション 6.2 を参照してください。

Meeting Servers 間でのロードバランシング通話の背景情報と例については、ホワイトペーパーを参照してください。

注：着信のロードバランシングには、Call Bridge から Cisco Unified Communications Manager への発信が含まれます。 これらの発信コールを機能させるには、発信ダイヤルプランルールを設定する必要があります。セクション 3.1 を参照してください。

6.1 着信通話を負荷分散するための Call Bridge の設定

Meeting Serverクラスタ全体でのコールのロードバランシングの設定には、3 つの側面があります。

- Call Bridge グループを作成する
- ロードバランシングを有効にする
- オプションで、各 Call Bridge のロード バランシングを微調整します。 ほとんどのデプロイメントでは、これは必要ありません。

さらに、着信通話の負荷分散には、Call Bridge から Cisco Unified Communications Manager または Cisco Expressway への発信通話が含まれます。 これらの発信通話を機能させるには、発信ダイヤル プラン ルールを構成する必要があります。次を参照してください。 発信 SIP 通話の負荷分散。

注： Call Bridge から Cisco VCS への着信通話の負荷分散が、Cisco Expressway ではなく、Cisco VCS で行われる場合、VCS にトラバーサルライセンスが必要です。 Meeting Server の負荷分散を行う場合、Cisco Expressway でのリッチメディアセッションライセンスは必要ありません。

注： Call Bridge グループで負荷分散を使用していない場合、通話は拒否されませんが、負荷制限に達したときにすべての通話の品質が低下します。 これが頻繁に発生する場合は、追加のハードウェアを購入することをお勧めします。

6.1.1 Call Bridge グループの作成

1. 各 Meeting Server クラスターについて、例えばデータセンター、国や地域など、Call Bridge をグループ化する方法を決定します。
2. クラスタ内のいずれかのサーバーのウェブ管理インタフェースを使用して、**[設定>API] を選択します。**
3. 新しい Call Bridge グループの作成
   a. API オブジェクトのリストで、**/api/v1/callBridgeGroups** の後ろの ▶ をタップします。
   b. **[新規作成]** ボタンを選択し、新しい callBridgeGroup の名前を入力し、Call Bridge グループのパラメータを設定します。 **[作成（Create）]** を選択します。

c. 新しいグループが callBridgeGroups のリストに表示されます。

4. グループ化する Call Bridge を特定する

a. API オブジェクトのリストで、**/api/v1/callBridges** の後ろの ► をタップします。

b. [callBridge id] をクリックして、グループに追加する各 Call Bridge を選択します

i. [**callBridgeGroup**] フィールドの隣にある [**Choose**] ボタンをクリックし、ステップ 3b で作成した callBridgeGroup を選択します。

ii. [変更（Modify）] **をクリックします。**

c. Call Bridge グループに追加する必要がある各 Call Bridge に対して、ステップ 4b を繰り返します。

5. 他のすべての Call Bridge グループについても繰り返します。

6.1.2 クラスタの負荷制限を指定し、ロードバランシングを有効にする

1. クラスターの各 Call Bridge で、そのサーバーの負荷制限を指定します

a. API オブジェクトのリストで、**/system/configuration/cluster** の後の ► をタップします。

b. **[View or edit (表示または編集)]**ボタンを選択して **loadLimit**の値を入力します。 **[変更（Modify）]** ボタンをクリックします。 これにより、サーバーの最大負荷制限が設定されます。負荷制限については、表 6 を参照してください。

表 6: サーバプラットフォームの負荷制限

システム	負荷制限
ミーティングサーバ 2000 M5v2	875,000
ミーティングサーバ 2000 M6	1,296,000
ミーティングサーバ 1000 M5v2	120,000
ミーティングサーバ 1000 M6	160,000
VM	vCPU ごとに 1250

注： Meeting Server 1000 M5v2 およびMeeting Server 2000 M5v2 の負荷制限の増加には、Meeting Serverソフトウェアバージョン 3.2 が必要です。

Call Bridge に負荷制限を設定すると、現在の負荷に基づいて通話を拒否するようになります。 デフォルトでは、新しい参加者からの通話の拒否は、通話を分配するための負荷制限の 80% で発生します。 この値は微調整することができます。以下を参照してください。

2. クラスター内の各サーバーで負荷分散を有効にします。

   Cisco Unified Communications Manager 展開の場合:

   a. API オブジェクトのリストで、**/callBridgeGroups** の後ろの ► をタップします。

   b. Cisco Unified Communications Manager にトランキングされた Call Bridge グループの **オブジェクト ID** をクリックします

   c. **loadBalancingEnabled=true** に設定します。 **[変更（Modify）]**

   をクリックします。Cisco Expressway 導入の場合：

   a. API オブジェクトのリストで、**/callBridgeGroups** の後ろの ► をタップします。

   b. Cisco Expressway にトランキングされた Call Bridge グループの **オブジェクト ID** をクリックします

   c. **loadBalancingEnabled=true** および **loadBalanceIndirectCalls= true**を設定します。

   Cisco Unified Communications Manager 導入の場合、**[変更（Modify）]**をクリックします。

   a. API オブジェクトのリストで、**/callBridgeGroups/<call bridge group>** の後の ► をタップします。

   b. **[表示または編集（View or edit）]** ボタンを選択して、**loadBalancingEnabled = true** に設定します。 [**変更**] ボタンをクリックします

ヒント: Call Bridge が 1 つしかなく、通話の品質を落とさずに拒否する場合は、単一の Call Bridge で Call Bridge グループを作成し、負荷分散を有効にします。

6.1.3 ロードバランシングを微調整する

負荷分散パラメータを微調整することは可能ですが、ソリューションの可用性に影響を与える可能性があるので注意してください。 デフォルト値を変更すると、サーバーに負荷がかかり、ビデオ品質が低下する場合があります。 これは、電話会議が複数の Call Bridge に断片化しているか、または電話会議が単一の Call Bridge で使用するリソースが多すぎることが原因で発生する可能性があります。

Call Bridge の負荷分散通話は、3 つのパラメータによって制御されます。

- **loadLimit** – 上記で設定した Call Bridge の最大負荷の数値。
- **newConferenceLoadLimitBasisPoints** – 負荷制限の基準点（10,000 分の 1）の数値で、この数値に達すると、アクティブでない会議への着信が不利になります。範囲は 0 から 10000 で、デフォルトは 5000（50% の負荷）です。 値は **LoadLimit**を基準に調整されます。
- **既存の ConferenceLoadLimitBasisPoints** – この Call Bridge への着信を拒否する負荷制限のベーシスポイントの数値です。範囲は 0 から 10000 までで、デフォルトは 8000 (80% の負荷) です。 値は **LoadLimit**を基準に調整されます。

Call Bridge のデフォルトのしきい値を変更するには、次の手順を実行します。

1. API オブジェクトのリストで、**/system/configuration/cluster** の後の ▶ をタップします。
2. **[表示または編集（View or edit）]** ボタンを選択して、**newConferenceLoadLimitBasisPoints** と **existingConferenceLoadLimitBasisPoints** の値を設定します。 **[変更（Modify）]** をクリックします。

注： ディストリビューションの呼び出しは常に受け付けられ、追加のリソースを消費します。 負荷分散パラメータを変更する場合、これらの呼び出しに必要なオーバーヘッドが計算に含まれていることを確認してください。

6.1.4 設定がロードバランシングにどのように使用されるか

各 Call Bridge グループ内では、各スペースに選択される Call Bridge の特定の優先順位があります。 Call Bridge グループ内のスペースへの着信は、この順序に基づいて優先的に Call Bridge にリダイレクトされます。 リダイレクションは、既存の会議のしきい値と新しい会議のしきい値の 2 つのしきい値に基づいて行われます。

しきい値は次のように定義されます。

既存の会議しきい値 = existingConferenceLoadLimitBasisPoints/10000×loadLimit の新しい会議しきい値 = newConferenceLoadLimitBasisPoints/10000×負荷制限

通話が Call Bridge に到達すると、負荷制限が確認され、負荷制限が既存の会議のしきい値を上回る場合、通話は拒否されます。 通話は他の理由でも拒否されることに注意してください。 拒否された通話は、通話制御デバイスによってリダイレクトされる必要があります。

負荷制限が既存の会議のしきい値を下回っている場合、通話に応答があり、IVR は通過します。 電話会議が認識されると、グループ内の Call Bridge の優先順位が決定されます。 この順序は、選択できる Call Bridge が複数ある場合に、Call Bridge 間で決定するために使用されます。

グループ内のいずれかの Call Bridge がすでに電話会議を実行している場合、これらの Call Bridge の負荷制限が確認されます。 これらのいずれかが既存の電話会議のしきい値を下回っている場合、これらのいずれかが使用されます。

Call Bridge がまだ選択されていない場合は、負荷制限が既存の電話会議のしきい値よりも小さい Call Bridge の 1 つが選択されます。

6.2 発信 SIP 通話の負荷分散

Call Bridge グループは、着信 SIP 通話に加えて、発信 SIP 通話の負荷分散をサポートします。

アウトバウンド SIP コールの負荷を分散するには、次の操作を行います。

- スペースからの発信 SIP コールのロードバランシングを有効にする
- アウトバウンド SIP コールのロードバランシングのための発信ダイヤルプランルールをセットアップする。
- 発信 SIP 通話に Call Bridge グループまたは特定の Call Bridge を提供します。

ロードバランシングが有効になると、発信 SIP 通話は次のロジックに従います。

- ドメインに一致する最も高い優先順位の発信ダイヤル プラン ルールを見つけ、
  - これがローカル Call Bridge に適用される場合、ローカル Call Bridge グループ内で通話を分散します。

- これがリモート Call Bridge にのみ適用される場合、Call Bridge がメンバーである Call Bridge グループ内で通話の負荷分散を行います。

Call Bridge グループ全体での SIP 通話のロードバランシングの例については、『Cisco Meeting Server 間でのロードバランシング通話』のホワイトペーパーを参照してください。

注： Lync クライアントからの、または Lync クライアントへの通話の負荷分散は、現在 Call Bridge グループではサポートされていません。

6.2.1 発信 SIP 通話のロードバランシングを有効にする方法

スペースからのアウトバウンド SIP コールをロードバランシングしようとする特定の Call Bridge グループでの Call Bridge の設定方法は次のとおりです。

1. API オブジェクトのリストで、[**/callBridgeGroups** の後ろの ► をタップします。
2. 選択した Call Bridge グループの **オブジェクト ID** をクリックするか、[**new (新規作成)**] をクリックして、新しい Call Bridge グループを作成します。
3. **loadBalanceOutgoingCalls** = **true** に設定します。 **[変更（Modify）]** をクリックします。

発信通話の負荷分散の場合、グループ内の各 Call Bridge は、同じダイヤル プラン ルールを持つ必要があります。

6.2.2 発信 SIP 通話をロードバランシングするための発信ダイヤルプランルールをセットアップする方法

発信 SIP コールを負荷分散するための発信ダイヤル プラン ルールをセットアップするには、3 つの方法があります。

1. すべての発信ダイヤルプランルールで **スコープ** パラメータを **global** に設定します。 これにより、すべての Call Bridge がすべての発信ダイヤル プラン ルールを使用して、一致するドメインに到達できるようになります。
2. Call Bridge グループの各 Call Bridge に同一の発信ダイヤルプランルールを作成します。 **Scope** パラメータを **callBridge** に設定してください。 **callBridge** パラメータを使用して、Call Bridge の **ID** を設定します。

3. 特定の Call Bridge グループの発信ダイヤルプランルールを作成します。 **Scope**パラメータを **callBridgeGroup** に設定し、**callBridgeGroup** パラメータを**IDの** Call Bridge グループに変更します。

発信コールの負荷分散を使用する前に、Call Bridge グループの各 Call Bridge について、既存の発信ダイヤル プラン ルールを確認します。

1. API オブジェクトのリストで、**/outboundDialPlanRuless** の後 の ▶ をタップします
2. 新しい発信ダイヤルプランルールを作成するか、または発信 SIP 通話の負荷分散に使用する既存の発信ダイヤルプランの **オブジェクト ID をクリックします**。
3. ダイヤルプランの使用計画に応じて、**scope**、**callBridge**、**callBridgeGroup** の設定を選択します（上記の 3 つの代替方法を参照）。

6.2.3 参加者への発信 SIP 通話に使用する Call Bridge グループまたは特定の Call Bridge の提供方法

特定の Call Bridge グループから発信するには、

1. API オブジェクトのリストで、**/calls** の後ろの ▶ をタップします。
2. 個々の通話の **オブジェクト ID** をクリックします
3. ページの上部にある**関連オブジェクト**から **api/v1/calls/<call id>/participants** を選択します。
4. パラメータを下にスクロールして **callBridgeGroup** に移動し、ボックスにチェックを入れ、**[Choose (選択)] をクリックします**。 この通話に使用する Call Bridge グループの **オブジェクト ID** を選択します。 **[作成（Create）]** をクリックします。

6.2.4 アクティブな空の電話会議のロードバランシングを処理する

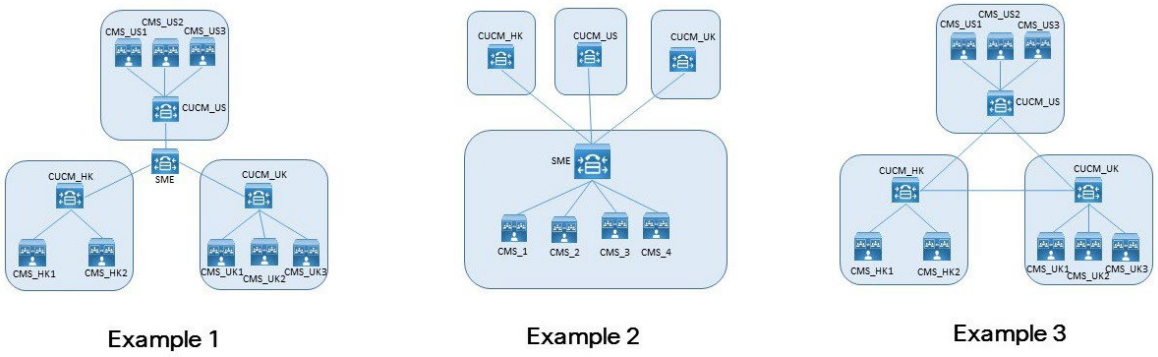
ロード バランシング アルゴリズムは、電話会議がすでにアクティブになっている Call Bridge に新しい通話を優先的に発信します。 空の電話会議を Call Bridge で開始するには、次を選択します: **/calls** を API オブジェクトリストから選択して、**[新規作成]** をクリックします。 既定では、これらの空の電話会議はアクティブとして扱われます。 つまり、空の電話会議への最初の通話は、優先的にこの Call Bridge にロード バランシングされます。 ロードバランシングを防ぐことができます新しい通話を作成するときに、パラメータ **activeWhenEmpty** を **false** に設定して、空の会議を優先的に使用します。

6.3 Cisco Unified Communications Manager を使用した着信コールの負荷分散の導入例

ロードバランシングに関するホワイトペーパーでは、Cisco Unified Communications Manager をコール制御デバイスとして使用して、コールのロードバランシングを行う 3 つの導入例について説明しています。

- 例 1 では、ローカル Cisco Unified Communications Manager にトランク接続された Meeting Server があります。 Cisco Unified Communications Manager がリーフノードとして Cisco Unified Communications Manager Session Management Edition (SME) に接続します。 SME がノード間の通話をルーティングします。
- 例 2 では、SME にトランク接続された一元化された Meeting Server と Cisco Unified Communications Manager のグローバル展開があります。
- 例 3 では、ローカル Cisco Unified Communications Manager にトランク接続された Meeting Server があります。 Cisco Unified Communications Manager は単純にトランク接続されており、コールを一元的にルーティングする SME はいません。

図 4：着信呼び出しをロードバランシングするための 3 つの導入例



どの展開でも、異なるデバイスからの通話を特定のリソースにマッピングする方法について、3 つのオプションがあります。

- 正しいパーティションを選択するためにコーリングサーチスペースが使用される複数のパーティション。
- ローカル ルート グループの単一パーティション。 ルートの選択は、複数のデバイスプール経由で行われます。
- クラスターごとの単一パーティション内でのダイヤル文字列の操作。

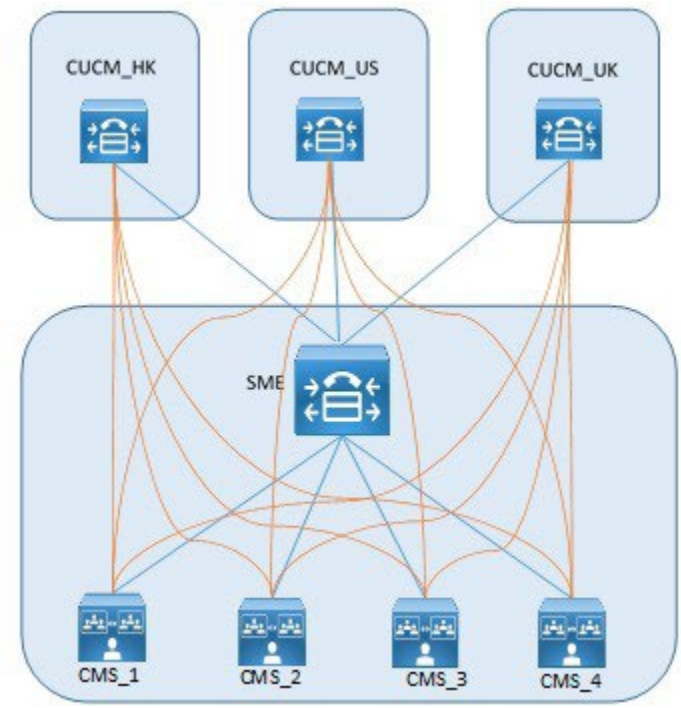
これらの各オプションは、任意の展開で使用できます。

最後のオプションは、数値ダイヤルプランでは簡単ですが、URI ダイヤルでは、LUA スクリプトが必要になります。 他の 2 つのオプションは、数値および URI ダイヤルに対して同様に機能します。

Meeting Server 間での着信通話のロードバランシングの例、および発信通話のロードバランシングの例については、ホワイトペーパーを参照してください。

付録 A 複数クラスタを使用するアドホックなエスカレーション

アドホックリソースが複数の Cisco Unified Communications Manager のクラスタ間で共有される場合、追加の考慮事項が適用されます。 これが発生する最も一般的なケースは、Cisco Unified Communications Manager Session Management Edition（SME）と共に集中型デプロイメントを使用している場合です。



例えば、上の図でオレンジ色の線が https Meeting Server ノードに対応し、青色の線が使用中の SIP トランクを示します。

2 つの追加の考慮事項は次のとおりです。

1. 固有の会議ブリッジプレフィックスの使用
2. 通話が正しい Call Bridge に正確に到達することを確認します。

A.1 固有の会議ブリッジプレフィックスの使用

各 Cisco Unified Communications Manager のクラスタは独立して機能するため、2 つのクラスタが同時に 1 つの電話会議に同じ電話会議 ID を使用する可能性があります。 これは、Cisco Unified Communications Manager でセットアップするときに、各電話会議ブリッジに一意の電話会議ブリッジ ID を割り当てることで解決できます（セクション 4.2 のステップ 1e を参照）

例

Cisco Unified Communications Manager のクラスタ	Meeting Server ノード	電話会議ブリッジのプレフィックス
CUCM_HK	CMS_1	888101
CUCM_HK	CMS_2	888201
CUCM_HK	CMS_3	888301
CUCM_HK	CMS_4	888401
CUCM_US	CMS_1	888102
CUCM_US	CMS_2	888202
CUCM_US	CMS_3	888302
CUCM_US	CMS_4	888402
CUCM_UK	CMS_1	888103
CUCM_UK	CMS_2	888203
CUCM_UK	CMS_3	888303
CUCM_UK	CMS_4	888403

A.2 通話が適切な Call Bridge に到達することを確認する

複数の Meeting Server ノードを使用する場合、ダイヤルプランまたは Call Bridge グループのいずれかを使用して、単一の電話会議のすべての通話が同じ Call Bridge に到達するようにすることをお勧めします。

通話に固有のプレフィックスを使用することで、通話を適切なリソースに転送できます。プレフィックスを慎重に選択することで、ルールの数を最小限に抑えることができます。 次に例を示します。

Prefix	Meeting Server ノード
88810	CMS_1
88820	CMS_2
88830	CMS_3
88840	CMS_4

Call Bridge グループを使用する場合、代替方法は、SME で LUA スクリプトを使用して、Cisco Unified Communications Manager ヘッダーを取り除くことです。 このヘッダーが取り除かれない場合、呼び出しによる負荷分散の試みが失敗します。

```
M = {}
trace.enable()
trace.format("***Remove_Call_Info_header_with_conference_tag***")
function M.inbound_INVITE(msg)
trace.format("***Remove_Call_Info_header_with_conference_tag_Inside_
INVITE***")
msg:removeHeaderValue("Call-Info", "<urn:x-cisco-remotecc:conference>")
end
return M
```

Cisco の法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている式、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 全著作権所有。 Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 CISCO およびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコシステムズおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコシステムズまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

★定型★このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。 ★定型★マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。 説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

この文書の印刷されたハード コピーおよび複製されたソフト コピーは、すべて管理対象外と見なされます。 最新版については、現在のオンライン バージョンを参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。 各オフィスの住所と電話番号は、当社の Web サイト www.cisco.com/go/offices. をご覧ください。

Cisco の商標または登録商標