Cisco Meeting Server

Cisco Meeting Server 3.8

Cisco Unified Communications Manager を使用した展開

2023 年 9 月 7 日

目次

変更履歴

日付	変更点
2023 年 9 月 7 日	バージョン 3.8 用に更新。 IMPS/CUCM での CMS 証明書の検証に関する情報を更新。
2023 年 3 月 16 日	バージョン 3.7 用に更新。 AXL ユーザーとプレゼンスユーザーを作成する手順を追加。
2022 年 11 月 4 日	軽微な修正。
2021 年 4 月 8 日	バージョン 3.2 用に更新。 Cisco Meeting Server プラットフォームの負荷制限を更新。
2020 年 12 月 2 日	セクション 4.2 の冒頭の注記を修正。
2020 年 10 月 20 日	マイナーアップデート。
2020 年 9 月 11 日	バージョン 3.0 用に更新。
2020 年 4 月 8 日	バージョン 2.9 用に更新。API メソッドの使用に関する情報を、Web 管理インターフェースを介した API へのアクセスに置き換え。
2019 年 9 月 26 日	軽微な修正。
2019 年 5 月 31 日	軽微な修正。
2019 年 2 月 27 日	セクション 2.1.2 のステップ 4 の前に注記を追加。
2019 年 1 月 2 日	バージョン 2.5 の変更はなし。
2018 年 10 月 2 日	バージョン 2.4 のドキュメンテーションマップへのマイナーな変更。
2018 年 5 月 10 日	最小 TLS バージョンの変更について、相互参照を追加。
2018 年 2 月 1 日	バージョン 2.3 用に更新。第 4 章の冒頭に、デフォルトとして TLS 1.2 に関する注記を追加。
2018 年 1 月 23 日	全般的なマイナーな編集と改善。
2017 年 11 月 8 日	付録 A：複数のクラスタを使用したアドホックエスカレーションを追加、その他の軽微な修正。
2017 年 7 月 14 日	第 3 章に追加情報を追加。
2017 年 5 月 9 日	バージョン 2.2 用に更新。発信コールのロードバランシングに関するセクションを追加。
2016 年 12 月 20 日	バージョン 2.1 用に更新。着信コールのロードバランシングコールに関する章を追加。
2016 年 8 月 3 日	Cisco Meeting Server 2.0 用にブランドを変更。

1 はじめに

Cisco Meeting Server ソフトウェアは、シスコ ユニファイド コンピューティング サーバー（UCS）技術に基づく特定のサーバー、または仕様に基づく VM サーバーでホストできます。このマニュアルでは、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 以降では、X シリーズサーバーをサポートしません。

注：このマニュアルでの Meeting Server という用語は、Cisco Meeting Server 2000、Cisco Meeting Server 1000、または仮想ホストで実行されるソフトウェアのいずれかを意味します。

このガイドには、Cisco Unified Communications Manager と連携するために Meeting Server を設定する方法の例が記載されています。例は、特定の展開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 の呼制御デバイスの使用の詳細については、『Deployments with Third Party Call Control Guide』を参照してください。Cisco Expressway をご利用の場合は、Expressway のマニュアルを参照してください。

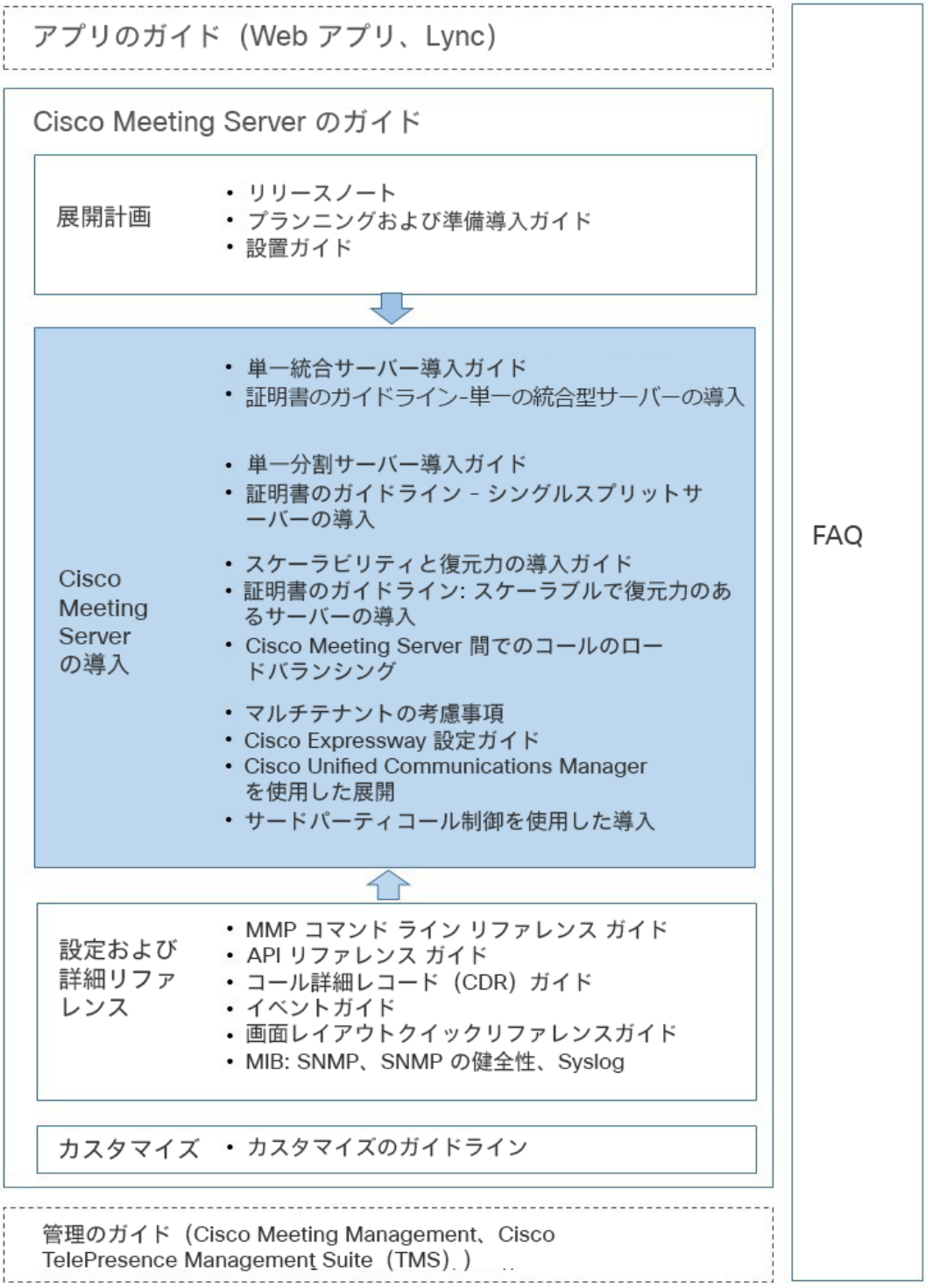
これらの手順は、すべての Meeting Server 展開トポロジ（単一サーバーおよび拡張/復元力のある展開）に等しく適用されます。

注：Meeting Server は、DTMF インバンドトーンのみを転送できます（RFC 2833）。たとえば、エンドポイントが DTMF をアウトオブバンドで Cisco Unified Communications Manager に送信し、それを Meeting Server に転送する場合、Meeting Server は DTMF を別のエンドポイントに転送しません。

1.1 このガイドの使い方

このガイドは、Meeting Server のドキュメントセット（ 図 1 を参照）の一部です。これらのドキュメントは、cisco.com から入手できます。

図 1：Cisco Meeting Server のドキュメントセット



1.1.1 コマンド

本書では、コマンドは黒文字 で**示されており、表示どおりに入力する必要があります。ただし、山括弧 <> で囲まれているパラメータについては、適切な値に置き換えてください。サンプルは青文字 で示されており、**導入環境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会議タイプは、表 1 で定義されているものです。

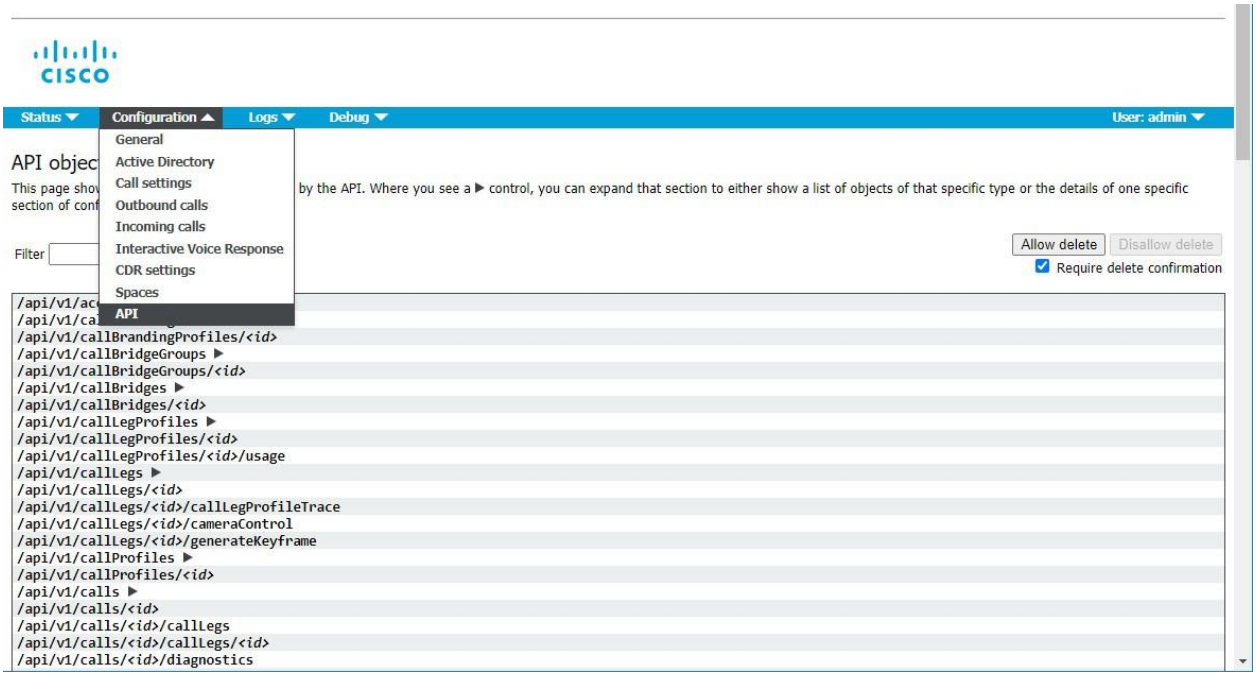
表 1：会議の種類

会議タイプ	説明
ランデブー（別名は、パーソナル CMR または VMR）	事前に定義された永続的に利用可能なアドレスであり、会議を事前スケジューリングなしで実施できます。 ホストはその他のユーザーとアドレスを共有します。共有されたユーザーは、いつでもそのアドレスにコールインできます。
アドホック	インスタントまたはエスカレートされた会議。たとえば、ポイントツーポイントコールから 3 人以上の参加者によるマルチパーティーコールに手動でエスカレートされます。
スケジュール済み	開始時間と終了時間が設定された事前予約会議。

1.2 Meeting Server API の使用方法を簡素化する

バージョン 2.9 以降、API メソッドやサードパーティ製アプリケーションではなく、Meeting Server Web 管理インターフェイスを使用して API にアクセスできます。Web 管理インターフェイスにログインした後、[**設定**（Configuration）] タブに移動し、プルダウンリストから [API] を選択します（図 2 参照）。

図 2：Meeting Server Web 管理インターフェイスを介した API へのアクセス



注：Web インターフェイスから API にアクセスするには、サードパーティ製アプリケーションを使用する場合のように、MMP を使用して Meeting Server の構成設定および認証を実行する必要があります。

2 Cisco Unified Communications Manager で SIP トランクを設定する

この章では、Cisco Unified Communications Manager と Meeting Server の間に SIP トランクを設定する方法について説明します。Meeting Server は次のように設定できます。

- 単一の結合サーバー、または
- 分割サーバー展開またはスケーラブルで復元力のある展開のコアサーバー。

注：スケーラブルで復元力のある展開では、各 Cisco Unified Communications Manager と各 Meeting Server の間に SIP トランクを設定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、Call Bridge ノードごとに個別のトランクを設定する必要があります。

シスコでは、セキュアな SIP トランクを設定することを推奨していますが、組織内のトラフィックを非セキュアにするという会社のポリシーがある場合は、非セキュアな SIP トランクを設定できます。
ただし、Cisco Unified Communications Manager の双方向コールを Meeting Server の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 には HTTPS 通信が必要であるため、エスカレート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し、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 間のスケジュールコールまたはランデブーコールを許可するだけで、SIP トランクを非セキュアに設定している場合、証明書は必要ありません。呼び出しタイプの定義は、セクション 1.1.2 に示されています。

注：組織の Cisco Unified Communications Manager サーバーの管理者ではない場合、シスコでは、サーバーの設定に同等の情報を導入する最良の方法について、現場の管理者に助言を求めるよう、強く推奨します。

セキュアな 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。非セキュア SIP トランクを設定する場合は、セクション 2.2 に直接進んでください。

2.1 SIP トランクセキュリティを設定する

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 トランクを設定し、第 4 章に従って、Cisco Unified Communications Manager での双方向コールを Meeting Server での会議にエスカレーションできるようにします。

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 Web Admin に異なる証明書がある場合は、Meeting Server Web Admin 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 を介して 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について説明しています。

2.1.1 Meeting Server で必要な設定

『Cisco Meeting Server 導入ガイド』に従って、Meeting Server を設定します。設定したら、Call Bridge ごとに次の手順を実行します。

1. Meeting Server の MMP に SSH で接続します。
2. まだ行っていない場合は、次の MMP コマンドを活用してリッスンインターフェイスを指定します：
   ```
   callbridge listen
   ```
3. Call Bridge の秘密キーと証明書署名要求（.csr）ファイルを生成します。秘密キーと証明書署名要求（.csr）ファイルを作成する方法の詳細については、該当する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 が必要です。

   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 サーバーの目的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. 署名のために CA（パブリック CA または内部 CA）に Call Bridge 証明書を送信します。内部 CA 署名付き証明書は受け入れられます。ただし、自己署名証明書はサポートされません。
5. 署名したら、openSSL または **pki inspect**コマンドを使用して証明書に問題がないことを確認します。

   - 入力 **pki inspect <certificatename>x509v3 拡張鍵用途：TLS Web サーバー認証、TLS Web クライアント認証を確認します。**
   または
   - **openssl x509 -in <certificatename> -noout -text -purpose** を入力します
   例：
   openssl x509 -in callBridge1.crt -noout -text -purpose

   出力の重要な回線は、**SSL クライアント**と **SSL サーバー**で、
   [はい（Yes）] **になっている必要があります。たとえば：**

   証明書の目的：

   SSL クライアント：はい（Yes）

   SSL クライアント CA：いいえ（No）

   SSL サーバー：はい（Yes）

6. 署名付き証明書と中間 CA バンドル（存在する場合）を SFTP を使用して Call Bridge にアップロードします。
7. 証明書と秘密キーを Call Bridge に割り当てます。
   a. MMP に SSH でログインします。
   b. 次のコマンドを入力します。

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

      ここで、 **keyfile**と **certificatefile**は、それぞれ対応する秘密キーと証明書のファイル名です。CA によって証明書バンドルが提供された場合は、バンドルも個別のファイルとして証明書に含めます。

      例：

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

   c. 変更を適用するには、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、次のように表示されます。

```
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。

FAILURE：キーと証明書に問題があります：証明書とキーが一致しません

注：Cisco Unified Communications Manager は、CA と、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。これは、上記のステップ 4 で作成した Call Bridge 証明書を、CallManager-trust を介して Cisco Unified Communications Manager の信頼ストアにアップロードすることによって実現されます。
セクション 2.1.2 のステップ 2 を参照してください。

注：Meeting Server への証明書の作成とアップロードについて詳しくは、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 ターミネーション ポイント（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

- これが展開に悪影響を与えない場合は、MTP を無効にします。SCCP 電話機を使用していて、DTMF を Meeting Server に送信する必要がある場合、MTP をオフにすると、展開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ない場合は、同時コールの数に応じて、Cisco Unified Communications Manager の MTP キャパシティを増やす必要があります。

1. まだ行っていない場合は、CallManager サービスがアクティブになっている各 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します。注：Meeting Server はデフォルトでは受信した証明書を検証せず、すべての有効な証明書を受け入れ、Call Manager の自己署名証明書を受け入れるため、これは推奨事項であり、必須ではありません。
    a. Cisco Unified Communications Manager で [OS **の管理**（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**（Certificate List）] ウィンドウで、[CSR **の作成**（Generate CSR）] をクリックします。

c. [**証明書の名前**（Certificate Name）] ドロップダウンリストで、[CallManager] を選択します。

d. [CSR **の作成**（Generate CSR）] をクリックして、証明書署名要求を生成します。

e. CSR が正常に生成されたら、[CSR **のダウンロード**（Download CSR）] をクリックします。[署名要求のダウンロード（Download Signing Request）] ダイアログボックスから [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 署名付き証明書は受け入れられます。

g. CA から証明書が返されたら、[**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）] ドロップダウンリストで、[CallManager-trust] を選択します。最初にルート証明書を参照してアップロードし、次に中間証明書をアップロードします。[**証明書目的**（Certificate Purpose）] ドロップダウンリストで、[CallManager] を選択します。CallManager サービスの証明書を参照して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証明書と中間証明書を Cisco Unified Communications Manager 信頼ストアにアップロードします。

a. Cisco Unified Communications Manager で [OS **の管理**（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/証明書チェーンのアップロード**（Upload Certificate/Certificate Chain）] をクリックします。[証明書/証明書チェーンのアップロード（Upload Certificate/Certificate Chain）] 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）] ドロップダウンリストで、[CallManager **信頼**（CallManager-trust）] を選択します。

d. 最初にルート証明書を参照してアップロードし、続いて中間証明書を 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する

Cisco Unified Communications Manager は、**非セキュア** SIP **トランク**（No Secure SIP Trunk）と呼ばれるデフォルト セキュリティ プロファイルを適用します。TLS、または標準セキュリティ プロファイル以外のものを使用するには、以下の手順を実行します。

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）] **の順に移動します。**

c. [**新規追加**（Add New）] をクリックします。

d. 次のようにフィールドに入力します。

- [**名前**（Name）] = 名前を入力します（例：「CMS_SecureTrunk」）
- [**デバイスセキュリティモード**（Device Security Mode）]= [**暗号化**（Encrypted）] **を選択**
- [**着信転送タイプ**（Incoming Transport Type）] = [TLS] **を選択**
- [発信転送タイプ（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 を入力します。
- [**着信ポート**（Incoming Port）] = TLS リクエストを受信するポートを入力します。TLS のデフォルトは 5061 です。
- [**ヘッダー置き換えの許可**（Accept Replaces Header）] = Call Bridge Grouping を使用する場合は、このボックスをオンにします（セクション 6 を参照）。

e. [**保存**（Save）] をクリックします。

注：ビデオ機能を使用した最低 2 人の会議参加者とのアドホック会議の場合、Cisco Unified Communications Manager は、[**デバイスセキュリティモード**（Device Security Mode）] が [**暗号化**（Encrypted）] に設定されているときや、サービスパラメータが [**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 true（デフォルト）に設定されている場合、暗号化オーディオ会議ブリッジに割り当てます。このパラメータが false に設定されている場合、暗号化されたビデオ会議ブリッジは Cisco Unified Communications Manager で現在サポートされていないため、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。サービスパラメータをリセットするには、[**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）] から [**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 - 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 TelePresence Conferencing **のデフォルトの標準** SIP **プロファイル**を使用する場合は、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）。チェックされていることを確認するキー値は、次のとおりです：[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共有の許可**（Allow Presentation Sharing using BFCP）]。
5. SIP トランクの作成

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

b. [**新規追加**（Add New）] をクリックします。

c. 次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**（SIP Trunk）]
- DeviceProtocol =SIP
- トランクサービスのタイプ（Trunk Service Type） = なし（None）**（デフォルト）**

d. [**次へ**（Next）] をクリックします。

e. SIP トランクの接続先情報を設定します。以下の 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	デバイスを所属させるプール（Cisco Unified Communications Manager の [**システム**（System）] > [**デバイスプール**（Device Pool）] で設定）
SRTP の許可（SRTP Allowed）	メディア暗号化を許可するには、[SRTP **を許可**（SRTP Allowed）] を選択します。
[インバウンドコール（Inbound Calls）] > [コーリングサーチスペース（Calling Search Space）]	Cisco Unified Communications Manager から Meeting Server の会議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は、デフォルトを選択します。
[アウトバウンドコール（Outbound Calls）] > [発信側変換 CSS（Calling Party Transformation CSS）]	適宜選択してください。
[SIP 情報（SIP information）] > [接続先アドレス（Destination Address）]	単一の Meeting Server の FQDN を入力します。これは、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（SIP Information）] > [宛先ポート（Destination port）]	TLS の場合は、5061 を入力します
[SIP トランクセキュリティプロファイル（SIP Trunk Security Profile）]	手順 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 グループ化を行うときは、これを、発呼側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 プロファイル（SIP Profile）]	[TelePresence **会議用標準** SIP **プロファイル**（Standard SIP Profile For TelePresence Conferencing）]を選択します
正規化スクリプト（Normalization Script）	この SIP トランクに cisco-telepresence-conductor-interop を割り当てます。注：シスコの Web 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いただくことが理想的です。Conductor がない場合でも、Meeting Server には Conductor と同じ相互運用性の問題があるため、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 ノードへのコールも出力する場合は、このチェックボックスをオンにします。

6. [**保存**（Save）] をクリックし、設定を適用します。
   [トランクリスト（Trunk List）] を使用して、数分後、トランクがサービス中であることを確認します。

2.2 非セキュア SIP トランクを設定する

セクション 2.2.1 およびセクション 2.2.2 の手順に従って非セキュア SIP トランクを設定し、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コールを有効にします。

2.2.1 Meeting Server で必要な設定

設定したら、『Cisco Meeting Server 導入ガイド』に従って、Meeting Server を設定します。

1. Meeting Server の MMP に SSH で接続します。
2. まだ行っていない場合は、次の MMP コマンドを活用してリッスンインターフェイスを指定します：
   ```
   callbridge listen
   ```

2.2.2 Cisco Unified Communications Manager で必要な設定

テストは、メディア ターミネーション ポイント（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

- これが展開に悪影響を与えない場合は、MTP を無効にします。SCCP 電話機を使用していて、DTMF を Meeting Server に送信する必要がある場合、MTP をオフにすると、展開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ない場合は、同時コールの数に応じて、Cisco Unified Communications Manager の MTP キャパシティ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**（No Secure SIP Trunk）と呼ばれるデフォルト セキュリティ プロファイルを適用します。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ことも、名前を付けて他のオプションをデフォルトのままにして新しいプロファイルを作成することもできます。デフォルト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）] **の順に移動します。**

   c. [**新規追加**（Add New）] をクリックします。

   d. [名前（Name）] フィールドに次のように入力します。

      - Name =「CMS_SecureTrunk」**などの名前を入力し、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）]= [**非セキュア**（Non Secure）] **を選択**
      - [**着信転送タイプ**（Incoming Transport Type）] = [TCP+UDP] **を選択**
      - [発信転送タイプ（Outgoing Transport Type）] = [TCP] **を選択**
      - [**着信ポート**（Incoming Port）]。TCP のデフォルトは 5060 です
      - [**ヘッダー置き換えの許可**（Accept Replaces Header）] = Call Bridge Grouping を使用する場合は、このボックスをオンにします（セクション 6 を参照）。

   e. [保存（Save）] をクリックします。

2. SIP トランクの作成

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

   b. [**新規追加**（Add New）] をクリックします。

   c. 次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**（SIP Trunk）]

- DeviceProtocol =SIP
- トランクサービスのタイプ（Trunk Service Type） = なし（None）**（デフォルト）**

d. [**次へ**（Next）] をクリックします。

e. SIP トランクの接続先情報を設定します。以下の 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るプール（Cisco Unified Communications Manager の [**システム**（System）] > [**デバイスプール**（Device Pool）] で設定）
SRTP の許可（SRTP Allowed）	SRTP を許可しない
[インバウンドコール（Inbound Calls）] > [コーリングサーチスペース（Calling Search Space）]	デフォルトを選択します。
[アウトバウンドコール（Outbound Calls）] > [発信側変換 CSS（Calling Party Transformation CSS）]	適宜選択してください。
[SIP 情報（SIP information）] > [接続先アドレス（Destination Address）]	Meeting Server FQDN を入力することをお勧めします（または DNS ルックアップに依存します）。
[SIP 情報（SIP Information）] > [宛先ポート（Destination port）]	TCP には 5060 を入力します
[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 グループ化を行うときは、これを、発呼側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。
[SIP プロファイル（SIP Profile）]	[TelePresence **会議用標準** SIP **プロファイル**（Standard SIP Profile For TelePresence Conferencing）]を選択します
正規化スクリプト（Normalization Script）	非セキュア SIP トランクには必要ありません。

f. [**保存**（Save）] をクリックします。

3 スケジュールコールとランデブーコールを設定する

セキュア SIP トランク（セクション 1.1）または非セキュア SIP トランク（セクション 1.2 を参照）を設定した後、セクション 3.1 およびセクション 3.2 の手順に従って、Meeting Server から Cisco Unified Communications Manager へのランデブーコールおよびスケジュールされたコールの発信を有効にします。

3.1 Meeting Server を設定する

1. Meeting Server から Cisco Unified Communications Manager に送信される コール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するには、[**設定**（Configuration）] > [API] を選択します。
   a. API オブジェクトのリストから、/outboundDialPlanRules の後ろにある ► をタップします
   b. [**新規作成**（Create new）] をクリックします。
   c. 以下の表 4 にパラメータを入力します

表 4：アウトバウンド ダイヤル プラン ルールの設定

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一致するドメインを入力します
使用する SIP **プロキシ**	確認内容： このフィールドを空白のままにします。サーバーは、_sips.tcp.**を使用して、**手順 b に入力したドメインの DNS SRV ルックアップを実行します。<yourcucmdomain>。これで解決できない場合、サーバーは **の** DNS A **ルックアップを試みます。**<yourcucmdomain>。これに失敗すると、_sip._tcp **の** SRV ルックアップが試行されます。<yourcucmdomain>これが失敗すると、_sips.udp **が試行されます。**<yourcucmdomain>。 または、使用するサーバーの SIP プロキシ（Cisco Unified Communications Manager の FQDN など）を入力します。このドメインは、上記の箇条書きで説明されている内容で解決します。 または、Cisco Unified Communications Manager 用の IP アドレスを入力します。
ローカルコンタクトドメイン	このフィールドは空白のままにします。Lync または Skype for Business への SIP トランクを設定する場合にのみ必要です。

ドメインからのローカル	コールの発信元（発信者 ID）にするドメインを入力します。 注 : [**ドメインからのローカル**（Local from domain）] **を**空白のままにした場合、発信者 ID で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）] **として入力された**ドメインになります。
トランクタイプ	標準 SIP（Standard SIP）を選択します。
優先対応	必要に応じて設定してください。
暗号化	展開に適したモードを選択します。たとえば、トラフィックが SIP トランクで暗号化されていない場合は、[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、コールを正しい場所に転送します。

ルートグループを使用すると、トランクが選択される順序を指定できます。たとえば、2 つの長距離通信会社を使用する場合、長距離コールで、費用がより低い通信会社の優先度が高くなるよう、ルートグループを追加できます。最初のトランクが利用できない場合でのみ、コールはより費用の高い通信会社をルーティングします。

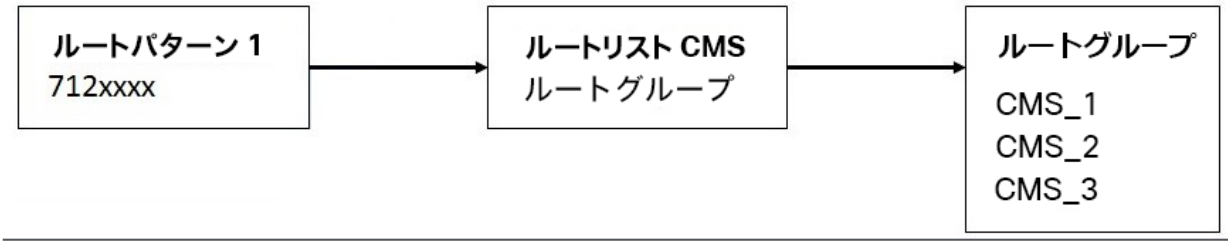
ルートリストによって、指定された優先順位で一連のルートグループを関連付けます。そのルートリストを 1 つ以上のルートパターンに関連付けることで、それらのルートグループにアクセスする順序が決まります。この順序により、発信コールに使用可能なデバイスの検索の進行が制御されます。ルートリストにはルートグループだけを含めることができます。各ルートリストには、少なくとも 1 つのルートグループが必要です。1 つのルートグループを任意の数のルートリストに追加することができます。

ルートパターンは、数字列（アドレス）とルートリストへのコールまたはゲートウェイへのコールを指定するディジット操作セットから構成されます。また、ルートフィルタおよびルートリストと連動して、特定のデバイスにコールを直接転送したり、特定の数字パターンを包含、除外、変更したりします。

メディアリソースグループでは、メディアサーバーの論理的なグループ化が定義されます。必要に応じて、メディアリソースグループを地理上の場所またはサイトと関連付けることができます。さらに、サーバーの使用または目的のサービスのタイプ（ユニキャストまたはマルチキャスト）を制御するメディアリソースグループを形成することもできます。

ルートグループ、ルートリスト、およびリソースグループの詳細については、使用している Cisco Unified Communications Manager 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：通話を正しい場所に転送する



注：スケーラブルで復元力のある Meeting Server 展開を設定していない場合は、Cisco Unified Communications Manager でルートグループまたはルートリストを設定する必要はありません。Cisco Unified Communications Manager からのアウトバウンドコールのダイヤルプランを設定するときは、ルートパターンを作成するだけです。 ドメインベースのルーティングの場合は、SIP **トランク/ルートリスト**を以前に設定した SIP トランクにポイントし、数字ダイヤルの場合は**ゲートウェイ/ルートリスト**を以前に設定した SIP トランクを選択し、[**ルートオプション**（Route Option）] を [**このパターンをルーティング**（Route this pattern）] として選択します。

3.2.1 ルートグループを設定する

1. 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一覧が表示されます。
3. 適切なものがない場合は、[**新規追加**（Add New）] をクリックします。
4. 次の手順を実行します。
   - 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分散アルゴリズムを選択します（例：**トップダウン**）
   - [**利用可能デバイス**（Available Devices）] 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**（Add to Route Group）] ボタンをクリックします
   - このルートグループに該当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して、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 ルートリストを設定する

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. 適切なものがない場合は、[**新規追加**（Add New）] をクリックします。
3. 次の手順を実行します。
   - Name = 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）] セクションから、[**ルートグループの追加**（Add Route Group）] を選択し、**選択したグループ**のリストに追加するルートグループを選択します。
   - 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（Route Lists）] のリストを確認して、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（アウトバウンドコールのダイヤルプラン）

@mydomain.example.com などのドメインベースのルーティングまたは、7XXX などの番号ベースのルーティングを設定して、Cisco Unified Communications Manager インターフェイスを介して Meeting Server に送信します。たとえば次のようなものです。

ドメインベースのルーティングの例

すべてのドメインベースのコールを Cisco Unified Communications Manager から Meeting Server にルーティングするには、次の手順を実行します。

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. 適切なものがない場合は、[**新規追加**（Add New）] をクリックします。
3. 次の手順を実行します。
   - パターン使用法（Pattern Usage） = ドメインルーティング（Domain Routing）
   - mydomain.example.com のような IPv4 のパターン
   - 説明（Description） = 任意のテキスト
   - 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付加され、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設定されます。人、電話、トランクごとに異なる CSS を使用できます。コールが発信されると、Cisco Unified Communications Manager は、一致するルールがあ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. 適切なものがない場合は、[**新規追加**（Add New）] をクリックします。
3. 次の手順を実行します。
   - ルートパターン = 703777XXX（ページのさらに下でさまざまな変換を設定できます。たとえば、[数字の破棄（Discard Digits）] フィールドで PreDot を選択して、この例では先頭の 7 を削除できます）
   - 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付加され、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設定されます。人、電話、トランクごとに異なる CSS を使用できます。コールが発信されると、Cisco Unified Communications Manager は、一致するルールがあ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） = 適切な任意のテキスト
   - [**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. テストコールを複数回行います。Cisco Unified Communications Manager に登録されたエンドポイントが必要です。また、Meeting Server で、Cisco Unified Communications Manager からのコールを受け入れるためのスペースと着信ダイヤルプランルールを作成する必要があります。これを行う方法については、該当する『Cisco Meeting Server 導入ガイド』を参照してください。

3.3 Jabber プレゼンスを更新する（ベータ機能）

Meeting Server は、Jabber ユーザーが Cisco Meeting Server Web アプリミーティングに参加しているときに、そのプレゼンスステータス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、以下のとおりです。

- Meeting Server のログイン ID は E メールである必要があり、AD の $mail$ 属性にマップする必要があります。
- Cisco Unified Communications Manager では、同じユーザーが $mail$ 属性をディレクトリ URI フィールドにマップする必要があります。
- Jabber ログインは、Cisco Unified Communications Manager のディレクトリ URI またはユーザー ID フィールドのいずれかを介して行うことができます。

注：シスコでは、ベータ機能が将来完全にサポートされる機能になることを保証しません。ベータ機能はフィードバックに基づいて変更される可能性があり、機能は将来変更または削除される可能性があります。

Jabber ユーザーが Web アプリにサインインしてミーティングに参加すると、ミーティングサーバーは Jabber ステータスを「ミーティング中、通話中」に更新し、ユーザーがミーティングを終了すると、以前のステータスに戻ります。

Meeting Server は、次の場合、Jabber ステータスを更新しません。

- Web アプリケーション会議に参加中に、Jabber ユーザーが別の会議または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 Web アプリミーティングに参加する前にステータスを [**サイレント**-**応答不可**（DND-Do not disturb）] に設定している場合、ミーティングサーバーは Jabber ステータスを更新しません。
- ユーザーが Web アプリケーション会議中にいつでも手動で Jabber ステータスを更新できる場合、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 Web アプリ参加者、または SIP エンドポイント、Lync、または Skype を介して参加する参加者をサポートしません。
- Meeting Server は、コンテンツ共有のプレゼンスを更新しません。

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 ノードで Meeting Server を設定します。これは、IMP サーバーの単一クラスター、つまり、6 つの IMPS ノードの 3 つのプレゼンス冗長グループのみをサポートします。Meeting Server で設定できる Cisco Unified Communications Manager は 1 つだけです。Meeting Server は、IMP サーバーをユーザーのプレゼンスステータスで更新します。次に、Jabber は IMP サーバーからこれらの詳細を取得し、それに応じてユーザープレゼンスを更新します。

注：Meeting Server は、TCP ポート 8083 を使用して IMP サーバーに接続します。IMP サーバーと Meeting Server Call Bridge の間にファイアウォールがある場合は、このポートを開いて通信を許可することをお勧めします。

3.3.1 Cisco Unified Communications Manager を設定する

Jabber の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、標準 AXL API アクセスのロール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、**事前定義グループ** 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。

3.3.1.1 ユーザーグループの作成とロールの割り当て

以下の手順に従って、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 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 Management）] > [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**（Add New）] をクリックします。
4. [**アクセス制御グループ情報**（Access Control Group Information）] **セクションで、次の情報を入力します。**
   - **名前** = アクセルグループの名前を入力します。例: CUCM_AXL_Group
5. 右上隅で、[**関連リンク**（Related Links）] > [**アクセス制御グループへのロールの割り当て**（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）] チェックボックスを選択し、[**選択したものを追加**（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 ユーザーの作成とロールの割り当て

以下の手順に従って、AXL およびプレゼンスユーザーを作成し、適切なグループをそれらに割り当てます。

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）]**を選択します。**
2. [**新しいユーザーの追加**（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**（Permissions Information）] セクションで、[**アクセス制御グループに追加**（Add to Access Control Group）] を選択します。
4. **利用可能な**アクセス制御グループ**のリストから**:
   a. AXL ユーザーの場合：セクション 3.3.1.1 で説明されている手順に従って作成されたグループを選択します。
   b. present_user の場合：グループ 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**（Save）] をクリックします。

3.3.2 Meeting Server と Cisco Unified Communications Manager/IMP サーバー間のセキュアな通信を実現

Callbridge 証明書バンドルは、IMP サーバーの場合は CUPS トラストストアに、Cisco Unified Communications Manager の場合は Tomcat トラストストアにアップロードする必要があります。

同様に、IMP サーバーの CUPS 証明書と Cisco Unified Communications Manager の Tomcat 証明書は、ミーティングサーバーにアップロードして検証する必要があります。証明書の検証の詳細については、MMP ユーザー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。これは、IMP サーバーの単一クラスター、つまり、6 つの IMPS ノードの 3 つのプレゼンス冗長グループのみをサポートします。

6 IMPS ノードの割合です。Meeting Server で設定できる CUCM は 1 つだけです。

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 ログイン情報を提供します。コマンドのリストの詳細については、『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。

4 エスカレート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 およびセクション 4.2 の手順に従って、Cisco Unified Communications Manager での双方向コールを Meeting Server での会議にエスカレーションできるようにします。

注：非セキュアで SIP トランクを設定する場合でも、Cisco Unified Communications Manager の双方向コールを Meeting Server の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るため、証明書が必要になります。API には HTTPS 通信が必要であるため、エスカレート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し、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 ゲートウェイコール間のカスケードがサポートされています。ただし、スペースにダイヤルし、アドホックコールを追加して同じ Meeting Server にエスカレートすること（つまり、2 つのスペース間のカスケード）はサポートされていません。異なる Meeting Server 上の 2 つのスペース間でカスケードすることは可能ですが、ユーザーエクスペリエンスが低下する可能性があるためお勧めしません。

4.1 Meeting Server を設定する

1. Meeting Server で着信ダイヤルプランを設定します。該当する『Cisco Meeting Server 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は着信コールのルールに含まれている必要があります。つまり、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設定します。詳細については、『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。

4.2 Cisco Unified Communications Manager を設定する

Cisco Unified Communications Manager と Meeting Server 間の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 Web Admin に異なる証明書がある場合は、Meeting Server Web Admin 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進める前に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 を介して 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について説明しています。

Meeting Server は、Unified Communications Manager の会議ブリッジとして処理されます。

1. Meeting Server ごとに、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**（Add New）] 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. [Cisco Meeting Server] **を** [会議ブリッジのタイプ（Conference bridge type）] **ドロップダウンリストから選択します。**（オプションとして Cisco Meeting Server が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 を選択します）
    d. [デバイス情報（Device Information）] **ペインで、**Meeting Server **の名前と説明を入力します。**
    e. Meeting Server がこの Cisco Unified Communications Manager クラスタに直接接続されていない集中型展開にアドホック会議を展開する場合は、**会議ブリッジプレフィックス**を入力します。これについては、付録 A で詳しく説明します。

    注：展開内の Meeting Server ノードと Cisco Unified Communications Manager クラスタのペアごとに、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）]のドロップダウンリストから、[SIP トランク（SIP Trunk）] を選択します。

g. HTTP **インターフェイス情報**を入力して、Cisco Unified Communications Manager と Cisco Meeting Server の間にセキュアな HTTPS 接続を作成します。注：

   i. これには、Web 管理インターフェイスとポートが一致している必要があります。

   ii. Web **管理者が** SIP **トランクへの別のアドレスでリッスンしている場合は、**[SIP トランク接続先を HTTP アドレスとして上書き（Override SIP Trunk Destination as HTTP Address）] **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は、Web 管理にロードされた証明書と一致する必要があります。

h. [**保存**（Save）] をクリック後、[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、展開のトポロジによって異なります。

   a. [**メディアリソース**（Media Resources）] > [**メディアリソースグループ**（Media Resource Group）] に移動します。

   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を作成し、名前を入力します。

   c. 手順 1 で作成した 1 つ以上の会議ブリッジを [**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、展開のトポロジによって異なります。

   各 MRGL については次のように操作します。

   a. [メディアリソース（Media Resources）] > [メディアリソースグループ（Media Resource Group）] **に移動します。**

   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 を選択してクリックして編集します。

c. **手順 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、デバイスプールを設定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（つまり、エンドポイント）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ている場合は、エンドポイントの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 マニュアル』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リストを作成し、名前を入力するか、既存のデバイスプールを選択して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、適切な Cisco Unified Communications Manager グループをドロップダウンリストから選択します。

   d. [**ローミングセンシティブ設定**（Roaming Sensitive Settings）] セクションで、ドロップダウンリストを使用して、上記の手順 2f で作成した**日付/時刻**グループ、**リージョン**、および**メディア リソース グループ リスト**を選択します。その他のフィールドは、そのデフォルト値（または以前に設定した値）のままにします。

   e. [**保存**（Save）] と [**リセット**（Reset）] 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たデバイスがある場合は、[リセット（Reset）] をクリックすると再起動します。

      新しいデバイスプールが作成されている場合。

   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、デバイスプールの設定を変更するデバイスを選択します。

   h. ドロップダウンリストから、上記手順 3b で作成され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. 変更を有効にするには、[**リセット**（Reset）] をクリックします。これにより、適用時にエンドポイントが再起動されます

5. Cisco Unified Communications Manager Session Management Edition で展開する場合はいずれかを実行します。

   a. 適切な Meeting Server ノードを指すカンファレンス ブリッジ プレフィックス セット（手順 1e）を持つコールのダイヤルプランルールを設定する。

   b. コール情報ヘッダーを削除する 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 ノードを指す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 の間でアドホックコール エスカレーションを設定する手順については、付録 A を参照してください。付録には、コール情報ヘッダーを削除する LUA スクリプトの例も含まれています。

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. その objectGUID を持つユーザーは、Meeting Server にインポートされている必要があります。
3. ユーザーは、関連付けられた 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のみ objectGUID 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、ホストされたコールに対して 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している参加者に対して、ActiveControl では、会議の参加者が会議の詳細を受信し、エンドポイントインターフェイスを使用して会議中にいくつかの管理タスクを実行できます。

5.1 Meeting Server 上の ActiveControl

Meeting Server は、ActiveControl が有効なエンドポイントに次のミーティング情報を送信サポートしています。

- 参加者リスト（名簿リストとも呼ばれます）。コールに参加している他の参加者の名前と参加者の総数を確認できるようになります。
- 現在話している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している参加者を示すインジケータ。
- 会議が録画またはストリーミングされているかどうかを示すインジケータ、および通話中にセキュアでないエンドポイントがあ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画面メッセージ。

また、ActiveControl が有効なエンドポイントで以下の管理タスクをサポートします。

- エンドポイントに使用するレイアウトを選択します。
- ミーティングの他の参加者の接続を解除します。

5.2 制限事項

- ActiveControl が有効になったコールが、Unified CM バージョンが 9.1（2）未満の Unified CM トランクを通過した場合、コールが失敗する可能性があります。古い Unified CM トランク（Unified CM 8.x 以前）で ActiveControl を有効にすべきではありません。
- 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 iX プロトコルを使用します。このプロトコルは、SIP Session Description Protocol（SDP）でアプリケーション回線としてアドバタイズされます。Meeting Server は ActiveControl を自動的にサポートしますが、この機能は無効にすることができます。セクション 5.4 を参照してください。遠端ネットワークが不明な場合、または iX プロトコルをサポートしていないことが明らかになっているデバイスの場合は、Meeting Server と他の通話制御デバイスまたはビデオ会議デバイスの間の SIP トランクで iX を無効にすることが最も安全な場合があります。例えば、次のような場合です。

- Unified CM 8.x 以前のシステムへの接続の場合、古い Unified CM システムは ActiveControl 対応デバイスからのコールを拒否します。これらのコールの失敗を回避するために、ネットワーク内の Unified CM 8.x デバイス宛てのトランクでは iX を無効にしてください。SIP プロキシ経由で 8.x デバイスに到達する場合は、そのプロキシのトランク上で iX が無効にされていることを確認します。
- サードパーティ製ネットワークへの接続の場合。このような場合、ActiveControl 対応のデバイスからのコールをサードパーティ製ネットワークが処理する方法を知る方法はありません。処理メカニズムが拒否する場合があります。このようなコールの失敗を回避するために、サードパーティ製ネットワークへのすべてのトランクで iX を無効にしたままにしてください。
- Cisco VCS を中心とした展開で、外部ネットワークに接続するか、古い Unified CM バージョンに内部で接続する場合。Cisco VCS X8.1 以降、ゾーンフィルタをオンにして、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 を無効にできます（デフォルトでは、フィルタはオフになっています。）

5.4 SIP コール内で UDT を無効にする

ActiveControl は、特定の機能に対して、UDT トランスポートプロトコルを使用します。たとえば、名簿リストをエンドポイントに送信することで、ユーザーが通話中に他の参加者との接続を解除し、さらに展開間の参加リストを接続解除できるようにするなどです。UDT は、デフォルトで有効になっています。診断の目的で、UDT を無効にできます。たとえば、コール制御が Meeting Server から着信を受信しない理由が、そのコール制御が UDT を使用していないことが理由であると考えられる場合などです。

Meeting Server の Web 管理インターフェイスを使用するには、[**設定**（Configuration）] > [API] を選択します。

1. API オブジェクトのリストから、/compatibilityProfiles の後ろにある ► 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、新しい互換性プロファイルを作成します。
3. パラメータ sip-UDT = false に設定します。[**変更**（Modify）] をクリックします。
4. API オブジェクトのリストから、/system/profiles の後ろにある ► をタップします。
5. [**表示**（View）] **または** [**編集**（Edit）] ボタンをクリックします。

6. パラメータ compatiilityProfile の右側にある [**選択**（Choose）] をクリックします。
   上記の手順 3 で作成した compatibilityProfile の object id を選択します。
7. [**変更**（Modify）] をクリックします。

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

一部の SIP プロファイルでは、Cisco Unified Communications Manager で iX プロトコルのサポートが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 プロファイルでサポートを設定してから、その SIP プロファイルを SIP トランクに適用する必要があります。

SIP プロファイルでの iX サポートを設定する

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（Find and List SIP Profiles）] 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**（Add New）] 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 プロファイルの設定（SIP Profile Configuration）] 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）] チェックボックスをオンにします。
4. 追加の設定変更があれば加えます。
5. [保存（Save）] 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**（Device）] > [**トランク**（Trunk）] の順に選択します。

   [トランクの検索と一覧表示（Find and List Trunks）] 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**（Add New）] 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**（Find）] 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。

   [トランクの設定（Trunk Configuration）] ウィンドウが表示されます。
3. [SIP プロファイル（SIP Profile）] 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 での iX のフィルタリング

プロトコルをサポートしないネイバーゾーンの iX アプリケーション回線をフィルタ処理するように Cisco VCS を設定するには、SIP UDP/IX フィルタモードの詳細設定オプションが [オン（On）] 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。

詳細ゾーンプロファイルのオプション設定を更新するには、次の手順を実行します。

1. 新しいネイバーゾーンを作成するか、既存のゾーンを選択します（[**設定**（Configuration）] > [**ゾーン**（Zones）] > [**ゾーン**（Zones）]）を選択します。
2. まだ選択されていない場合、[詳細パラメータ（Advanced parameters）] セクションの [**ゾーンプロファイル**（Zone profile）] で、[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**（SIP UDP/IX filter mode）] ドロップダウンリストから、[**オン**（On）] 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 ヘッダーを含むコールのコール処理概要

シナリオ	結果
Unified CM 8.x 以前	コールが失敗します
9.1(2) 以前の Unified CM 9.x	コールは通常処理されますが、ActiveControl は処理されません
Unified CM 9.1(2)	コールと ActiveControl は通常処理されます
エンドポイント：iX および SDP 実装はサポートされていません	エンドポイントが再起動、またはコールが失敗する可能性があります

6 コールのロードバランシングの概要

この章では、Cisco Unified Communications Manager 展開内の Meeting Server のスケーラビリティと復元力を向上させる方法について説明します。

Call Bridge グループ化は、クラスタ化された Call Bridge 間でコールを負荷分散するために使用されます。Cisco Unified Communications Manager の主な役割は、Cisco Meeting Server の指示に従って、Call Bridge グループ間でコールを移動することです。ローカル Call Bridge への各トランクは、[Replaces ヘッダーの許可（Accept Replaces Header）]チェックボックスがオンになっている 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。

ローカル Call Bridge を介した着信コールのバランシングは、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によって実現されます。ルートグループには、そのロケーションのローカル会議リソースへのリンクが含まれています。ルートグループは、Meeting Server 間でのコールのロードバランシングのために循環分散を設定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 を介した発信コールのバランシングは、スペースからのアウトバウンド SIP コールのロードバランシングを有効にし、アウトバウンド SIP コールをロードバランシングするためのアウトバウンド ダイヤル プラン ルールを設定することによって実現されます。セクション 6.2 を参照してください。

Meeting Server 間のロードバランシングコールのバックグラウンド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：着信コールのロードバランシングには、Call Bridge から Cisco Unified Communications Manager へのアウトバウンドコールが含まれます。これらのアウトバウンドコールを機能させるには、アウトバウンド 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）。

6.1 着信コールをロードバランシングするための Call Bridge を設定する

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、次の 3 つの側面があります。

- Call Bridge グループの作成
- ロード バランシングの有効化
- 各 Call Bridge のロードバランシングの微調整（オプション）。ほとんどの展開では、これは必要ありません。

さらに、着信コールのロードバランシングには、Call Bridge から Cisco Unified Communications Manager または Cisco Expressway へのアウトバウンドコールが含まれます。これらのアウトバウンドコールを機能させるには、アウトバウンド ダイヤルプランルールを設定する必要があります（『アウトバウンド SIP コールのロードバランシング』を参照）。

注：着信コールのロードバランシングに、Call Bridge から Cisco Expressway ではなく Cisco VCS への発信コールが含まれる場合は、VCS にトラバーサルライセンスが必要です。注文品の仕向国が、ロードバランシングされた Meeting Server の展開では、Cisco Expressway でのリッチ メディア セッション ライセンスの要件はありません。

注：Call Bridge グループでロードバランシングを使用していない場合は、コールは拒否されませんが、負荷制限に到達したときにすべてのコールの品質が低下します。この現象が頻繁に起きる場合は、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 グループを作成する

1. Meeting Server クラスタごとに、Call Bridge をグループ化する方法を決定します（データセンター、国または地域ごとなど）。
2. クラスタ内のサーバーの Web 管理インターフェイスを使用するには、[**設定**（Configuration）] > [API] を選択します
3. Call Bridge グループの新規作成
   a. API オブジェクトのリストから、/api/v1/callBridgeGroups の後ろにある ▶ をタップします

b. [Create new（**新規作成**）] ボタンを選択し、新しい callBridgeGroup の名前を入力して、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. 新しいグループは、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から、/api/v1/callBridges の後ろにある ► 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] フィールドの横にある [**選択**（Choose）] ボタンをクリックし、手順 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 Call Bridge ごとにステップ 4b を繰り返します。

5. 他のすべての Call Bridge グループについて繰り返します。

6.1.2 クラスタの負荷制限の指定とロードバランシングの有効化

1. クラスタ内の各 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から、/system/configuration/cluster の後ろにある ► をタップします

b. [**表示**（View）] または [**編集**（Edit）] ボタンを選択し、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に対する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：サーバープラットフォームの負荷制限

システム	負荷制限
Meeting Server 2000 M5v2	875,000
Meeting Server 2000	700,000
Meeting Server 1000 M5v2	120,000
Meeting Server 1000	96,000
VM	vCPU あたり 1250

注：Meeting Server 1000 M5v2 および Meeting Server 2000 M5v2 の負荷制限を増やすには、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コールが拒否されます。デフォルトでは、新しい参加者からのコールの拒否は、コールの分散を可能にするために負荷制限の 80% で発生します。この値は微調整できます。以下を参照してください。

2. クラスタ内の各サーバーでロードバランシングを有効にします。

   Cisco Unified Communications Manager の展開の場合：

   a. API オブジェクトのリストから、/callBridgeGroups の後ろにある ► をタップします
   b. Cisco Unified Communications Manager にトランクされた Call Bridge グループの object 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 展開の場合：

   a. API オブジェクトのリストから、/callBridgeGroups の後ろにある ► 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 object id をクリックします
   c. loadBalancingEnabled=true **に設定し、**loadBalanceIndirectCalls=true に設定します。

      [**変更**（Modify）] をクリックします。

   Cisco Unified Communications Manager 展開の場合：

   a. API **オブジェクトのリストから、**callBridgeGroup **の後にある ► をタップします**<call bridge group>
   b. [**表示または編集**（View or edit）] ボタンを選択し、loadBalancingEnabled = true を設定します。[**変更**（Modify）] ボタンをクリックします。

ヒント：Call Bridge が 1 つだけで、通話の品質を下げるのではなく通話を拒否する場合は、単一の Call Bridge で Call Bridge グループを作成し、ロードバランシングを有効にします。

6.1.3 ロードバランシングの微調整

ロードバランシング 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、サーバーが過負荷になり、ビデオ品質が低下する可能性があります。これは、複数の Call Bridge で会議がフラグメント化するか、単一の Call Bridge で使用するリソースが多すぎるために発生する可能性があります。

Call Bridge でのロードバランシングコールは、次の 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 – 非アクティブな会議への着信コールが優先されなくなる負荷制限の基準点（10,000 分の 1）の数値。範囲は 0 から 10000 で、デフォルトは 5000（50% の負荷）です。値は、LoadLimit を基準に拡張します。
- existingConferenceLoadLimitBasisPoints – この Call Bridge への着信コールが拒否される負荷制限の基準点の数値。範囲は 0 ～ 10,000 で、デフォルトは 8,000（80% 負荷）です。値は、LoadLimit **を基準に拡張します**。

Call Bridge のデフォルトのしきい値を変更するには、次のステップを実行します。

1. API オブジェクトのリストから、/system/configuration/cluster の後ろにある ► をタップします
2. [**表示**（View）] **または** [**編集**（Edit）] ボタンを選択し、newConferenceLoadLimitBasisPoints および existingConferenceLoadLimitBasisPoints の値を設定します。[**変更**（Modify）] をクリックします。

注：分配コールは常に受け入れられ、追加でリソースを消費します。ロードバランシング パラメータを変更する場合は、これらのコール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 ロードバランシングによる設定の使用方法

各 Call Bridge グループ内には、各スペースに対して Call Bridge が選択される特定の優先順位があります。Call Bridge グループ内の任意の場所にランディングするスペースへのコールは、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。リダイレクトは、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います。

しきい値は次のように定義されます。

existing conference threshold = existingConferenceLoadLimitBasisPoints/10000×loadLimit
new conference threshold = newConferenceLoadLimitBasisPoints/10000×loadLimit

コールが Call Bridge にランディングすると、負荷制限がチェックされ、負荷制限が既存の会議のしきい値を超える場合、コールが拒否されます。他の理由でコールが拒否される場合もあります。拒否されたコールは、呼制御デバイスによってリダイレクトする必要があります。

負荷制限が既存の会議しきい値を下回っている場合、コールに応答し、すべての IVR を通過させます。会議が認識されると、グループ内の Call Bridge の優先順位を決定できます。この順序は、選択できる Call Bridge が複数ある場合に、Call Bridge を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 がすでに会議を実行している場合、これらの Call Bridge の負荷制限がチェックされます。これらのいずれかが既存の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、既存の会議のしきい値よりも負荷制限が小さい Call Bridge の 1 つが選択されます。

6.2 アウトバウンド SIP コールのロードバランシング

Call Bridge グループは、インバウンド SIP コールに加えて、アウトバウンド SIP コールのロードバランシングをサポートします。

アウトバウンド SIP コールをロードバランシングするには、次の手順を実行します。

- スペースからのアウトバウンド SIP コールのロードバランシングを有効にします。
- 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アウトバウンド ダイヤルプランルールを設定します。
- アウトバウンド SIP コールに Call Bridge グループまたは特定の Call Bridge を指定します。

ロードバランシングが有効になると、アウトバウンド SIP コールは次のロジックに従います。

- ドメインに一致する最も優先順位の高いアウトバウンド ダイヤルプランルールを見つけます。
  - これがローカルの Call Bridge に適用される場合は、ローカルの Call Bridge グループ内でコールをバランシングします。
  - これがリモート Call Bridge にのみ適用される場合は、Call Bridge がメンバーである Call Bridge グループ内でコールをロードバランシングします。

Call Bridge グループ間での SIP コール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「Cisco Meeting Server 間でのコールのロードバランシング （Load Balancing Calls Across Cisco Meeting Servers）」を参照してください。

注：Lync クライアントとの間のコールのロードバランシングは、現在、Call Bridge グループではサポートされていません。

6.2.1 アウトバウンド SIP コールのロードバランシングを有効にする方法

特定の Call Bridge グループで Call Bridge を設定して、スペースからのアウトバウンド SIP コールのロードバランシングを試行するには、次の手順を実行します。

1. API オブジェクトのリストから、/callBridgeGroups の後ろにある ► をタップします
2. 選択した Call Bridge グループの object id をクリックするか、[New（**新規**）] 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**。

アウトバウンド コールのロードバランシングでは、グループ内の各 Call Bridge に同じダイヤルプランルールが必要です。

6.2.2 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アウトバウンド ダイヤル プラン ルールを設定する方法

アウトバウンド SIP コールをロードバランシングするためのアウトバウンド ダイヤルプランルールを設定するには、次の 3 つの方法があります。

1. すべてのアウトバウンド ダイヤルプランルールで scope パラメータを [global（**グローバル**）] に設定します。 これにより、すべての Call Bridge がすべてのアウトバウンド 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 に同一のアウトバウンド ダイヤルプランルールを作成します。scope パラメータを callBridge に設定します。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 グループのアウトバウンド 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 Call Bridge グループの ID に設定します。

アウトバウンドコールのロードバランシングを使用する前に、Call Bridge グループの各 Call Bridge の既存のアウトバウンド 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から、/outboundDialPlanRules の後ろにある ► をタップします
2. 新しいアウトバウンド ダイヤルプランルールを作成するか、アウトバウンド SIP コールのロードバランシングに使用する予定の既存のアウトバウンド ダイヤルプランの object id をクリックします。
3. ダイヤルプランの使用方法に応じて、scope、callBridge、および 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 参加者へのアウトバウンド SIP コールに使用する Call Bridge グループまたは特定の Call Bridge を提供する方法

特定の Call Bridge グループからコールするには

1. API オブジェクトのリストから、/calls の後にある ► をタップします
2. 個別のコールの object id をクリックします。
3. ページ上部の**関連オブジェクト**からの api/v1/calls/<call id>/participants を選択します。
4. パラメータ callBridgeGroup まで下にスクロールし、[**選択**（Choose）] をクリックします。このコールに使用する Call Bridge グループの object id を選択します。[**作成**（Create）] をクリックします。

6.2.4 アクティブな空の会議のロードバランシングの処理

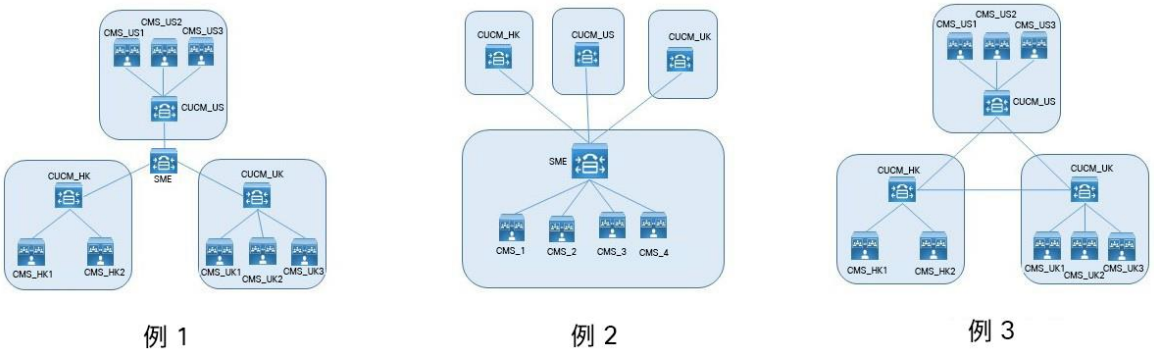
ロードバランシング アルゴリズムでは、会議がすでにアクティブになっている Call Bridge に新しいコールを優先的に配置します。Call Bridge で空の会議を開始するには、
API オブジェクトリストから /calls を選択し、[**新規作成**（Create new）] をクリックします。デフォルトでは、これらの空の会議はアクティブとして扱われます。つまり、空の会議への最初のコールは、優先的にこの Call Bridge にロードバランシングされます。新しいコールを作成する際にパラメータ activeWhenEmpty を false に設定することにより、空の会議を優先的に使用するロードバランシングを回避できます。

6.3 Cisco Unified Communications Manager を使用した着信コールのロードバランシングの導入例

ロードバランシングに関するホワイトペーパーでは、呼制御デバイスとして Cisco Unified Communications Manager を使用してコールをロードバランシングする 3 つの配置例について説明しています。

- 例 1 では、Meeting Server がローカルの Cisco Unified Communications Manager にトランクされています。Cisco Unified Communications Managers をリーフノードとして Cisco Unified Communications Manager Session Management Edition（SME）に接続します。SME は、ノード間のコールをルーティングします。
- 例 2 では、SME にトランクされた集中型の Meeting Server と、グローバルな Cisco Unified Communications Manager の展開があります。
- 例 3 では、Meeting Server がローカルの Cisco Unified Communications Manager にトランクされています。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 はありません。

図 4：着信コールのロードバランシングの 3 つの導入例



例 1　　例 2　　例 3

どのような展開でも、さまざまなデバイスからのコールを特定のリソースにマップする方法には 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使用されるコーリングサーチスペースを持つ複数のパーティション。
- ローカルルートグループを持つ単一のパーティション。ルートの選択は、複数のデバイスプールを介して行われます。
- クラスタごとの単一パーティション内でのダイヤル文字列操作。

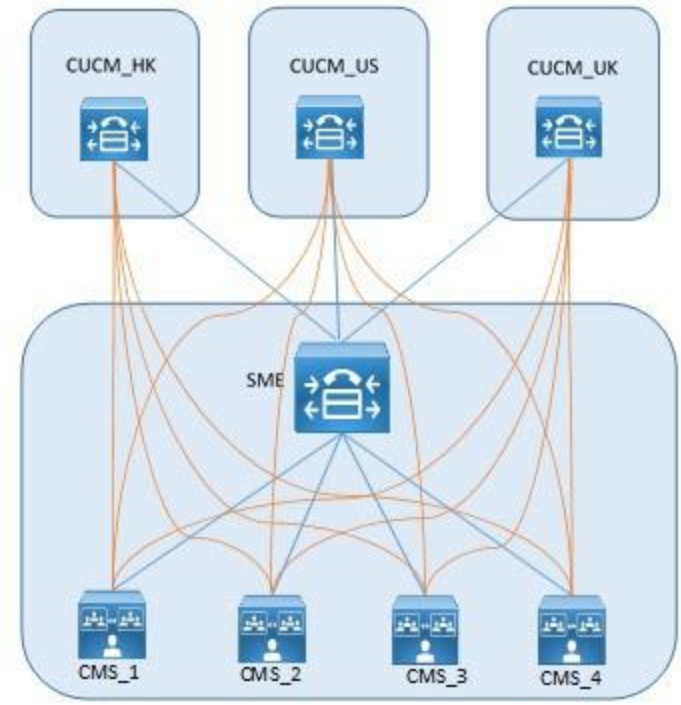
これらの各オプションは、どの展開でも使用できます。

最後のオプションは、数字のダイヤルプランでは簡単に実行できますが、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、数字ダイヤルと URI ダイヤルで同様に機能します。

Meeting Server 間でのインバウンドコールのロードバランシングのこれらの例、およびアウトバウンドコールのロードバランシングの例の詳細については、ホワイトペーパーを参照してください。

付録 A 複数のクラスタを使用したアドホックのエスカレーション

アドホックリソースが複数の Cisco Unified Communications Manager クラスタ間で共有される場合は、その他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、集中型展開を Cisco Unified Communications Manager Session Management Edition（SME）と共に使用している場合です。



たとえば、上の図で、オレンジ色の線は https Meeting Server ノードに対応し、青い線は使用中の SIP トランクです。

2 つのその他の考慮事項は以下のとおりです。

1. 独自の会議ブリッジプレフィックスの使用
2. コールが正しい Call Bridge に到達することを確認する。

A.1 独自の会議ブリッジプレフィックスの使用

各 Cisco Unified Communications Manager クラスタは独立して動作するため、2 つのクラスタが同時に同じ会議 ID を使用しようとする可能性があります。これは、Cisco Unified Communications Manager で設定するときに各会議ブリッジに一意の会議ブリッジ 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 Cluster	Meeting Server ノード	**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 コールが適切な Call Bridge に届くようにする

複数の Meeting Server ノードを使用する場合は、ダイヤルプランまたは Call Bridge グループを使用して、1 つの会議のすべてのコールが同じ Call Bridge に到達するようにすることをお勧めします。

コールに一意のプレフィックスを使用すると、コールを正しいリソースに送信でき、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。たとえば次のようなものです。

プレフィックス	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、代わりに SME で LUA スクリプトを使用して Cisco Unified Communications Manager ヘッダーを削除します。このヘッダーが削除されていない場合、コールのロードバランシングの試みは失敗します。

```
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_INV
ITE***")
msg:removeHeaderValue("Call-Info", "<urn:x-cisco-remotecc:conference>")
end return M
```

シスコの法的情報

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表現、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、すべてユーザー側の責任となります。

対象製品のソフトウェア ライセンスと限定保証は、製品に添付された『Information Packet』に記載されています。ソフトウェアライセンスまたは限定保証書が見つからない場合は、シスコの代理店に連絡してコピーを入手してください。

シスコが採用している 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。All rights reserved. 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。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

いかなる場合においても、シスコ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。

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。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などの図は、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 IP 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。最新バージョンについては、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（http://www.cisco.com/jp/go/offices）をご覧ください。

シスコの商標