Cisco Meeting Server

Cisco Meeting Server リリース 2.1

Cisco Unified Communications Manager との導入ガイド

2016 年 12 月 23 日

目次

1 はじめに

Cisco Meeting Server は、以前は Acano サーバと呼ばれていました。Cisco Meeting Server は、現在 Cisco UCS サーバの事前設定された新しいバージョン（Cisco Meeting Server 1000）でホストされます。また、Acano X シリーズ ハードウェアでも、仕様ベースの VM サーバでもホストが可能です。

注：このドキュメント内のミーティング サーバという用語は、Cisco Meeting Server 1000、Acano X シリーズ サーバ、または仮想ホストで実行中のソフトウェアのいずれかを意味します。

このドキュメントには、ミーティング サーバを Cisco Unified Communications Manager と併せて使用するための設定例が記載されています。各種の例は、導入状況に合わせて変更が必要な場合もあります。Avaya および Polycom のコール制御デバイスの使用に関する詳細については、『Deployments with Third Party call Control guide』[英語] を参照してください。

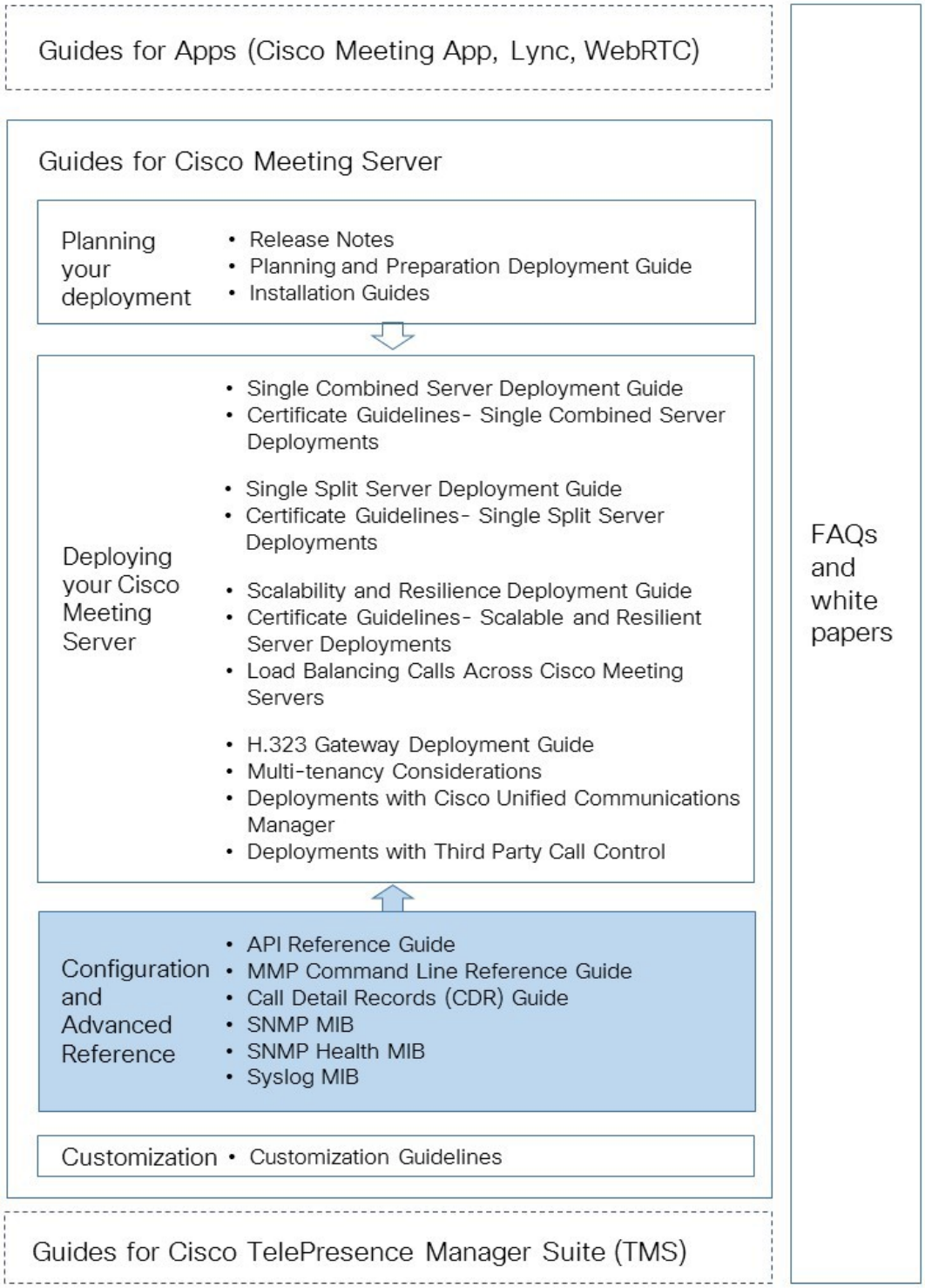
ここに記載されている事項は、ミーティング サーバのすべての導入トポロジ（単一サーバ型導入と拡張性/耐障害性導入）に同様に適用されます。

1.1 本ガイドの使用方法

このガイドは、ミーティング サーバに関するドキュメント セット（図 1 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 に関するドキュメント 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取り上げる会議の種類は表 1 に定義するとおりです。

表 1：会議の種類

会議の種類	説明
ランデブー（パーソナル CMR）	事前に定義された、期限なしで使用可能なアドレス。これにより、事前にスケジュールせずに会議を開催できます。 ホストがアドレスを他のユーザに共有すると、それらのユーザは、いつでもそのアドレスにコールインできるようになります。
アドホック	インスタント会議、またはポイントツーポイント コールから 3 人以上の参加者を伴うマルチパーティ コールなどへと手動でエスカレーションされた会議。
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。

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

この章では、Cisco Unified Communications Manager とミーティング サーバとの間に SIP トランクを設定する方法を説明します。ミーティング サーバは、分割サーバの導入環境におけるコア サーバ、または単一の統合サーバとして設定する必要があります。

シスコではセキュア SIP トランクの設定を推奨しますが、会社のポリシーで社内のトラフィックは非セキュアとしている場合は、非セキュア SIP トランクの設定も可能です。ただし、Cisco Unified Communications Manager での 2 者間コールをミーティング サーバでの会議へとエスカレーションする際には、Cisco Unified Communications Manager が Cisco Meeting Server の API と通信する必要があります。この API には HTTPS 通信が必要です。したがって、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ためには、Cisco Meeting Server と Cisco Unified Communications Manager の両方に証明書を作成してアップロードし、Cisco Unified Communications Manager に Meeting Server の証明書を信頼させる必要があります。

ミーティング サーバと Cisco Unified Communications Manager との間ではスケジュール コールかランデブー コールのみを許可し、SIP トランクを非セキュアに設定する場合は、証明書は不要です。コールの種類の定義は第 1.1.2 項に記載されています。

注： Cisco Unified Communications Manager の社内サーバ管理者ではない場合、同等の設定をサーバの設定に導入する最善の方法をローカル管理者に相談することを強く推奨します。

2.1 セキュア SIP トランクの設定

まず第 2.1.1 項および第 2.1.2 項のステップに従ってセキュア SIP トランクを設定します。次に、第 4 章のステップに従って Cisco Unified Communications Manager での 2 者間コールをミーティング サーバでの会議にエスカレーションできるようにします。

2.1.1 ミーティング サーバで必要な設定

Cisco Meeting Server の各種導入ガイドに従ってミーティング サーバを設定します。設定が完了したら、次の手順を実行します。

1. ミーティング サーバの MMP に SSH でログインします。
2. リスニング インターフェイスが未指定の場合、MMP コマンド **`callbridge listen`** を使用して指定します。
3. Call Bridge の秘密キーと証明書署名要求ファイル（.csr）を作成し、「cucm-trust.csr」という名前を付けます。

   Cisco Unified Communications Manager には、TLS 証明書の許容要件がいくつかあります。「cucm.csr」に SSL クライアントおよび SSL サーバの有効な目的があることを確認してください。この確認は、証明書が署名された段階で行います。

4. 「cucm-trust.csr」を CA（パブリック CA または内部 CA）に送信し、署名を受けます。内部 CA で署名された証明書は許容範囲です。
5. 署名が完了したら、次の OpenSSL を使用して証明書に問題がないことを確認します。

   openssl x509 -in <certificatename> -noout -text –purpose

   例：

   openssl x509 -in cucm-trust.crt -noout -text –purpose

   出力において重要な行は「SSL client」と「SSL server」です。これらの出力内容は、次の例に示すように「Yes」である必要があります。

   ```
   Certificate purposes:
   SSL client : Yes
   SSL client CA : No
   SSL server : Yes
   ```

6. 署名された証明書と中間 CA バンドル（ある場合）を Call Bridge にアップロードします。
   a. MMP に SSH でログインします。
   b. 次のコマンドを使用して、Call Bridge に証明書と秘密キーを指定します。

      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 により証明書バンドルが提供されている場合は、バンドルも個別のファイルとして証明書に含めます。

      次に例を示します。

      callbridge certs cucm-trust.key cucm-trust.crt cucm-trust-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が失敗すると、次のエラー メッセージが表示されます。

      ```
      FAILURE: Key and certificate problem: certificate and key do not match
      ```

注： Call Bridge の証明書と証明書バンドルを Cisco Unified Communications Manager の信頼ストアに追加する必要があります。第 2.1.2 項のステップ 2 を参照してください。

注：証明書の作成とミーティング サーバへのアップロードの詳細については、該当する『Cisco Meeting Server Certificate Guideline』を参照してください。

2.1.2 Cisco Unified Communications Manager で必要な設定

シスコによるテストは、メディア ターミネーション ポイント（MTP）の設定がないトランクで行っています。したがって、次のようにします。

- 導入環境に悪影響が生じることがなければ、MTP を無効化します。SCCP 電話を使用しており、ミーティング サーバに DTMF を送信する必要がある場合は、MTP を無効にすると導入環境に悪影響を与えるおそれがあります。
- 上記の実装が妥当ではない場合、同時コール数によっては Cisco Unified Communications Manager の MTP 容量を増やす必要があります。

1. Cisco Unified Communications Manager の証明書を生成します
   a. [Cisco Unified Communications Manager OS Administration] ページにログインします。
   b. [Security] > [Certificate Management] の順に選択します。[証明書の一覧（Certificate List）] ウィンドウが表示されます。
   c. [Generate CSR] ボタンをクリックし、Cisco Unified Communications Manager の証明書署名要求（CSR）を生成します。
   d. 認証局で CSR に署名します。内部 CA で署名された証明書は許容範囲です。
   e. 署名済みの証明書、秘密キー、中間 CA バンドル（ある場合）を Cisco Unified Communications Manager にアップロードします。
2. 第 2.1.1 項の手順 4 でミーティング サーバの Call Bridge に向けて作成された署名済みの証明書と、認証局からのルート証明書または証明書チェーンを Cisco Unified Communications Manager の信頼ストアにアップロードします。
   a. [Cisco Unified Communications Manager OS Administration] ページにログインします。
   b. [Security] > [Certificate Management] の順に選択します。
   c. [Upload Certificate/Certificate Chain] を選択します。
   d. [Choose File] をクリックして自分の証明書を見つけます。この証明書は、ルート証明書または Call Bridge の証明書と証明書バンドルの場合があります。
   e. [Upload File] をクリックします。
3. SIP トランクのセキュリティ プロファイルを作成します。

   SIP トランクを作成すると、Cisco Unified Communications Manager は **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 用のセキュリティ プロファイルです。TLS または標準以外のセキュリティ プロファイルを使用するには、次のステップに従います。
   a. [Cisco Unified Communications Manager Administration] にログインします。
   b. [System] > [Security] > [SIP Trunk Security Profile] の順に移動します。
   c. [Add New] をクリックします。

d. 次のようにフィールドを設定します。
   - Name：名前（例：CMS_SecureTrunk）を入力します。
   - Device Security Mode：[Encrypted] を選択します。
   - Incoming Transport Type：[TLS] を選択します。
   - Outgoing Transport Type：[TLS] を選択します。
   - X.509 Subject Name：Call Bridge の証明書の CN を入力します。
   - Incoming Port：TLS 要求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。

e. [Save] をクリックします。

4. SIP トランクを作成します。
   a. Cisco Unified Communications Manager で [Device] > [Trunk] の順に移動します。
   b. [Add New] をクリックします。
   c. 次のフィールドを設定します。
      - Trunk Type：[SIP trunk]
      - DeviceProtocol：[SIP]
      - Trunk Service Type ：[None]（デフォルト）
   d. [Next] をクリックします。
   e. SIP トランクの宛先情報を以下の表 2 に従って設定します。

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 [System] > [Device Pool] で設定したもの）
SRTP Allowed	[SRTP Allowed] を選択してメディア暗号化を許可します。
Inbound Calls > Calling Search Space	Cisco Unified Communications Manager での 2 者間のアドホック コールをミーティング サーバでの会議にエスカレーションすることのみを許可する場合、デフォルトの [not required] を選択します。
Outbound Calls > Calling Party Transformation CSS	必要に応じて選択します。
SIP Information > Destination address	ミーティング サーバの FQDN を入力します。ミーティング サーバの証明書の CN に必ず一致させます。
SIP Information > Destination Port	TLS の場合は **5061** と入力します。

フィールド	説明
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。
SIP Profile	[Standard SIP Profile For TelePresence Conferencing] を選択します。
正規化スクリプト	この SIP トランクには **[cisco-telepresence-conductor-interop]** を指定します。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するのが最善です。Conductor がない場合であっても、ミーティング サーバには Conductor が起こしうる相互運用性の問題と同様の問題があるため、コア ミーティング サーバのトランクにはこのスクリプトが適しています。

f. [Save] をクリックします。

2.2 非セキュア SIP トランクの設定

まず第 2.2.1 項および第 2.2.2 項に従って非セキュア SIP トランクを設定します。次に、第 3 章に従って Cisco Unified Communications Manager とミーティング サーバの間でランデブー コールとスケジュール コールができるようにします。

2.2.1 ミーティング サーバで必要な設定

Cisco Meeting Server の各種導入ガイドに従ってミーティング サーバを設定します。設定が完了したら、次の手順を実行します。

1. ミーティング サーバの MMP に SSH でログインします。
2. リスニング インターフェイスが未指定の場合、MMP コマンド **`callbridge listen`** を使用して指定します。

2.2.2 Cisco Unified Communications Manager で必要な設定

シスコによるテストは、メディア ターミネーション ポイント（MTP）の設定がないトランクで行っています。したがって、次のようにします。

- 導入環境に悪影響が生じることがなければ、MTP を無効化します。SCCP 電話を使用しており、ミーティング サーバに DTMF を送信する必要がある場合は、MTP を無効にすると導入環境に悪影響を与えるおそれがあります。
- 上記の実装が妥当ではない場合、同時コール数によっては Cisco Unified Communications Manager の MTP 容量を増やす必要があります。

1. SIP トランクを作成します。
2. a. Cisco Unified Communications Manager で [Device] > [Trunk] の順に移動します。
   b. [Add New] をクリックします。

c. 次のフィールドを設定します。
   - Trunk Type：[SIP trunk]
   - DeviceProtocol：[SIP]
   - Trunk Service Type ：[None]（デフォルト）

d. [Next] をクリックします。

e. SIP トランクの宛先情報を以下の表 3 に従って設定します。

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 [System] > [Device Pool] で設定したもの）
SRTP Allowed	SRTP は許可しません。
Inbound Calls > Calling Search Space	[default] を選択します。
Outbound Calls > Calling Party Transformation CSS	必要に応じて選択します。
SIP Information > Destination address	宛先アドレス（例：ciscomeetingserver.example.com）または IP アドレスを入力します。
SIP Information > Destination Port	TCP の場合は **5060** と入力します。
SIP Trunk Security Profile	非セキュア SIP トランクの場合は不要です。
SIP Profile	[Standard SIP Profile For TelePresence Conferencing] を選択します。
正規化スクリプト	非セキュア SIP トランクの場合は不要です。

f. [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 コールの設定

セキュア SIP トランク（第 2.1 項参照）または非セキュア SIP トランク（第 2.2 項参照）の設定が完了したら、第 3.1 項および第 3.2 項に従ってミーティング サーバから Cisco Unified Communications Manager へのランデブー コールとスケジュール コールができるようにします。

3.1 ミーティング サーバの設定

1. ミーティング サーバから Cisco Unified Communications Manager に送信するコールのアウトバウンド ダイヤル プラン ルールを設定します。
   a. ミーティング サーバの Web 管理画面インターフェイスを使用して [Configuration] > [Outbound Calls] の順に移動します。

      表 4：[Outbound Calls]

   b. 空白行の [Domain] で、Cisco Unified Communications Manager に送信する必要があるコールにあわせたドメインを入力します。
   c. [SIP proxy to use] で、次のいずれかを実行します。
      - このフィールドを空白のままにします。サーバは、**`_sip.tls.<yourcucmdomain>.com`** を使用して呼び出し先ドメインの DNS SRV ルックアップを実行します。これで解決しない場合、ミーティング サーバは、まずは TCP、次に UDP を使用してルックアップを試行します。

        または

      - CUCM FQDN を入力します。サーバは、指定されたドメインの DNS SRV ルックアップを実行します。

        注：これで解決しない場合、ミーティング サーバは、まずは TCP、次に UDP を使用してルックアップを試行します。上記の TLS、TCP、または UDP を使用した SRV ルックアップで解決できなかった場合、サーバは、入力されたホストの DNS A レコード ルックアップを実行します。

        または

      - Cisco Unified Communications Manager の IP アドレスを入力します。
   d. [Local contact domain] フィールドは空白のままにします。このフィールドが必要なのは、Lync への SIP トランクを設定するときのみです。

e. [Local from domain] で、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：[Local from domain] を空白のままにすると、発信者 ID に使用されるドメインは、デフォルトで [Local contact domain] として入力したドメイン（ここでは空白）になります。

---

f. [Trunk type] で、[Standard SIP] を選択します。

g. [Priority] は、必要に応じて設定します。

h. [Encryption] で、導入環境に適した暗号化モードを選択します。たとえば、トラフィックを SIP トランクで暗号化していない場合、[Unencrypted] を選択します。

i. [Add New（新規追加）] を選択します。

3.2 Cisco Unified Communications Manager の設定

1. アウトバウンド コールのダイヤル プランを設定します。
   ミーティング サーバへのルーティングは、番号（例：7xxx）によるルーティングまたはドメイン（例：@mydomain.example.com）によるルーティングのいずれかを設定できます。いずれの場合も、Cisco Unified Communications Manager のインターフェイスを通じて実行されます。次のいずれかの例に従います。

   ドメインによるルーティングの例

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

   a. [Cisco Unified Communications Manager Administration] インターフェイスにログインします。

   b. [Call Routing] > [Sip Route Pattern] の順に移動します。

   c. [Add New] をクリックします。

   d. 次の手順を実行します。

      - Pattern usage：[domain routing]
      - IPv4 pattern：「mydomain.example.com」など
      - Description：任意の内容を入力します
      - Route partition：以下を参照してください
      - SIP trunk / route list：設定済みのトランク

   e. [Save] をクリックします。

番号によるダイヤリングの例

この基本例では、7 で始まるものをすべてミーティング サーバにルーティングします。

a. [Cisco Unified Communications Manager Administration] インターフェイスにログインします。
b. [Call routing] > [Route/Hunt] > [Route Pattern] の順に移動します。
c. [Add New] をクリックします。
d. 次の手順を実行します。
   - Route pattern：7.!（「!」は任意の文字列です。「.」は後述のオプションで役立ちます）。
   - Route partition：ルールを所属させるルート パーティション。以下の注を参照してください。
   - Description：任意のテキスト
   - Gateway/route list：設定済みのトランク
   - Route this pattern：このオプションが選択されていることを確認します。

   ページの下のほうでは、さまざまな変換を設定できます。たとえば [Discard Digits] フィールドで [PreDot] を選択すると、この例でいう先頭の 7 が削除されます。
e. [Save] をクリックします。

注： ルート パーティションにはさまざまなダイヤル プラン ルールが付加されており、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ています。CSS はさまざまな人、電話機、またはトランクに対して個別に設定できます。発信が行われると、Cisco Unified Communications Manager は CSS 内の各ルート パーティションを確認してルールに適合するものを選択します。

---

2. テストをします。

   いくつかのテスト コールを発信します。

4 エスカレーションされたアドホック コールの設定

セキュア SIP トランク（第 2.1 項参照）の設定が完了したら、第 4.1 項および第 4.2 項のステップに従って Cisco Unified Communications Manager での 2 者間コールをミーティング サーバでの会議にエスカレーションできるようにします。

注：SIP トランクを非セキュアに設定する場合でも、証明書を使用する必要があります。これは、Cisco Unified Communications Manager での 2 者間コールをミーティング サーバでの会議にエスカレーションする際には、Cisco Unified Communications Manager が Cisco Meeting Server の API に通信する必要があるためです。API には HTTPS 通信が必要です。したがって、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ためには、Cisco Meeting Server と Cisco Unified Communications Manager の両方に証明書を作成してアップロードし、それぞれに互いの証明書を信用させる必要があります。

4.1 ミーティング サーバの設定

1. 『Cisco Meeting Server Deployment Guide』を参照してミーティング サーバに受信ダイヤル プランを設定します。アドホック コールについては、ルールをスペースに対して一致させる必要があります。
2. 使用する Cisco Unified Communications Manager の「api」許可を持つ管理者ユーザ アカウントを設定します。『Cisco Meeting Server MMP Command Line Reference Guide』を参照してください。

4.2 Cisco Unified Communications Manager の設定

1. 会議ブリッジを作成します。
    a. [Cisco Unified Communications Manager Administration] で、[Media Resources] > [Conference Bridge] の順に選択します。[Find and List Conference Bridges] ウィンドウが表示されます。
    b. [Add New] をクリックします。[Conference Bridge Configuration] ウィンドウが表示されます。
    c. [Conference Bridge Type] ドロップダウン リストから [Cisco TelePresence Conductor] を選択します。
    d. [Device Information] ペインでミーティング サーバの名前と説明を入力します。
    e. [SIP Trunk] ドロップダウン リストから SIP トランクを選択します。
    f. HTTP インターフェイス情報を入力し、[HTTPS] チェックボックスをオンにします。これにより、Cisco Unified Communications Manager と Cisco Meeting Server との間にセキュアな HTTPS 接続が作成されます。
2. Call Bridge の証明書とキーをまだ Cisco Unified Communications Manager の信頼ストアにアップロード（第 2.1.2 項のステップ 2 を参照）していない場合、アップロードします。

5 ActiveControl のサポート

バージョン 2.1 以降のミーティング サーバは、ホストされたコールの ActiveControl をサポートしています。CE 8.3 以降のソフトウェアがインストールされた Cisco SX、MX、または DX のエンドポイントを使用する会議出席者は、ActiveControl により、エンドポイントのインターフェイスを使用して会議中に会議詳細を受け取ることと、いくつかの管理タスクを実行することができます。

5.1 ミーティング サーバの ActiveControl

ミーティング サーバは、ActiveControl に対応するエンドポイントに以下の会議情報を送信できます。

- 参加者リスト（名簿ともいう）。これにより、他のコール参加者の名前と参加者の合計人数がわかります。
- 現在発言中の参加者のオーディオ アクティビティを示すインジケータ
- 現在どの参加者が出席しているかを示すインジケータ
- 会議は録音または配信されているか、コールに非セキュアなエンドポイントはあるかどうかを示すインジケータ
- 全参加者に表示される画面メッセージ。詳細は、第 1.0.1 項を参照してください。

また、ActiveControl に対応するエンドポイントでは、以下の管理タスクを実行することができます。

- エンドポイントで使用するレイアウトの選択
- 他の会議参加者の接続解除。詳細は、第 1.0.4 項を参照してください。

5.2 制限事項

- ActiveControl 対応コールが 9.1(2) より古いバージョンの Unified CM を使用して Unified CM トランクを横断すると、失敗する可能性があります。古いバージョンの Unified CM トランク（Unified CM 8.x 以前）上では、ActiveControl を無効にする必要があります。
- ActiveControl は SIP 専用機能です。H.323 インターワーキング シナリオはサポートされません。

注：Active Control は、特定の機能（エンドポイントへの名簿の送信、会議中のユーザによる他の参加者の接続解除）において UDT 転送を使用します。ミーティング サーバ上で従うべきステップを参照してください。

5.3 ActiveControl と iX プロトコルの概要

ActiveControl 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る iX プロトコルを使用します。ミーティング サーバは自動的に ActiveControl をサポートするため、機能を無効化することはできません。遠端ネットワークで iX をサポートしていないデバイスがあるか不明な状況や、そのようなデバイスがあると判明している状況では、ミーティング サーバと他のコール制御デバイスやビデオ会議デバイスとの間の SIP トランク上で iX を無効化するほうが無難です。たとえば、次のような場合です。

- Unified CM 8.x またはそれより古いシステムとの接続。古い方の Unified CM システムが ActiveControl 対応デバイスからのコールを拒否します。こうした呼損を避けるには、ネットワーク内の Unified CM 8.x デバイスに向かうすべてのトランクで iX を無効のままにします。SIP プロキシ経由で 8.x デバイスに到達する場合は、そのプロキシに向かうトランクで iX を必ず無効にしてください。
- サードパーティ ネットワークへの接続。この場合は、サードパーティ ネットワークが ActiveControl 対応デバイスからのコールをどのように処理するかを知る方法はありませんが、処理メカニズムがそれらのコールを拒否することがあります。こうした呼損を避けるには、サードパーティ ネットワークに向かう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している、または内部で古いバージョンの Unified CM に接続している Cisco VCS 中心の導入環境。Cisco VCS X8.1 以降では、ゾーン フィルタをオンにすることで、外部ネットワークまたは古いバージョンの Unified CM システムに送信される INVITE 要求に対して iX を無効にすることができます（このフィルタは、デフォルトではオフになっています）。

5.4 ミーティング サーバでの ActiveControl の有効化

ミーティング サーバ上で ActiveControl を設定して有効化するには、次のステップに従います。

ミーティング サーバの API を使用して次の手順を実行します。

1. sipUdt パラメータを「true」に設定した互換性プロファイルを作成します。sipUDT=true を **`/compatibilityProfiles`** オブジェクトに POST するか、**`/compatibilityProfiles/<compatibility profile id>`** オブジェクトに PUT します。
2. compatibilityProfile パラメータおよび id（ステップ 1 より）をシステム プロファイルに追加することで、ActiveControl をシステム全体で有効化します。compatibityProfile=<compatibility profile id を **`/system/profiles/`** オブジェクトに PUT します。

5.5 Cisco Unified Communications Manager での iX の有効化

iX プロトコルのサポートは、デフォルトでは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、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 サポートの設定

1. [Device] > [Device Settings] > [SIP Profile] の順に選択します。[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、[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、[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 Profile Configuration] ウィンドウが表示されます。
3. [Allow iX Application Media] チェックボックスをオンにします。
4. 追加の設定変更を加えます。
5. [Save] ボタンをクリックします。

SIP トランクへの SIP プロファイルの適用

1. [Device] > [Trunk] を選択します。

   [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、[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、[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。

   [Trunk Configuration] ウィンドウが表示されます。
3. [SIP Profile] ドロップダウン リストで、該当する SIP プロファイルを選択します。
4. [Save] をクリックします。
5. 既存のトランクを更新するには、[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ていないネイバー ゾーンについては iX アプリケーション回線を除外するように Cisco VCS を設定するには、ゾーン設定により、[SIP UDP/IX filter mode] の詳細設定オプションが [On] のカスタム ゾーン プロファイル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変更するには、以下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（[Configuration] > [Zones] > [Zones]）。
2. [Advanced Parameters] セクションの [Zone profile] で、[Custom] がまだ選択されていなければ、選択します。ゾーン プロファイル詳細設定の各オプションが表示されます。
3. [SIP UDP/IX filter mode] ドロップダウン リストから [On] を選択します。
4. [Save] をクリックします。

5.7 iX 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の概要

シナリオ	結果
Unified CM 8.x 以前のリリース	呼損
9.1(2) より前のバージョンの Unified CM 9.x	コールは正常に処理されるが、ActiveControl なし
Unified CM 9.1(2)	コールは正常に処理されるうえ、ActiveControl あり
エンドポイント：iX に対するサポートなし、SDP 実装なしの場合	エンドポイントのリブートまたは呼損の可能性あり

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 導入環境においてミーティング サーバの拡張性と復元性を高める方法を説明します。

クラスタ化されたすべての Call Bridge にわたってコールのロード バランシングを行うためには、Call Bridge のグループ化を使用します。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転送することです。

注：ロード バランシングの対象は、Call Bridge から Cisco Unified Communications Manager へのアウトバウンド コールです。こうしたアウトバウンド コールを機能させるためには、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。第 3.1 項を参照してください。

6.1 コールのロード バランシングのための Call Bridge の設定

ミーティング サーバ導入環境全体にわたるコールのロード バランシングの設定には、次の 3 つの要素があります。

- Call Bridge グループの作成
- ロード バランシングの有効化
- 任意での各 Call Bridge でのロード バランシングの調整。これは、ほとんどの導入環境で不要です。

6.1.1 Call Bridge グループの作成

1. 各ミーティング サーバ クラスタについて、Call Bridge をグループ化する方法（例：データセンター別、国または地域別など）を決めます。
2. **/callBridgeGroups** に Call Bridge グループの名前で POST を行い、Call Bridge グループを作成します。
3. 戻される GUID を使用して **/callBridges** に **callBridgeGroup=GUID** で PUT を行い、このグループに属する各 Call Bridge を追加していきます。
4. 上記の手順を他のすべての Call Bridge グループにも実行します。

6.1.2 ロード バランシングの有効化

1. 各 Call Bridge について、**/system/configuration/cluster** ノードに **loadLimit** の値で PUT を発行します。これにより、サーバの負荷上限値が設定されます。この値はまだ確定していません。現時点では、次の表を参照してください。

システム	負荷制限値
CMS1000	96000
X3	250000
X2	125000
X1	25000
VM	vCPU ごとに 1250

Call Bridge に負荷制限値を設定すると、その Call Bridge は現在の負荷に基づいてコールを拒否するようになります。

デフォルトでは、負荷制限値の 80% に達すると、コールを分散できるようこの拒否が発生します。この値を調整する場合は、以下の手順を実行します。

2. **/callBridgeGroups/<call bridge group>** に **loadBalancingEnabled=true** で PUT を行います。

6.1.3 ロード バランシングの調整

ロード バランシング のパラメータは調整可能です。調整は、ソリューションの可用性に影響する可能性があるため、注意して行う必要があります。デフォルト値を変更すると、サーバの過負荷やビデオ品質の劣化につながる可能性があります。このようなことが起こるのは、会議が複数の Call Bridge に分散されること、または複数の会議によって 1 つの Call Bridge のリソースが過剰に消費されることが原因です。

Call Bridge に対するコールのロード バランシングは、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 の負荷上限値。
- **newConferenceLoadLimitBasisPoints**：アクティブでない会議への着信が拒否される負荷制限値のベーシスポイント（1 万分の 1）を表す数値。0 から 10000 までで、デフォルト値は 5000（50% の負荷）です。値は **LoadLimit** に応じて増減します。
- **existingConferenceLoadLimitBasisPoints**：当該 Call Bridge への着信が拒否される負荷制限値のベーシスポイントを表す数値。0 から 10000 までで、デフォルト値は 8000（80% の負荷）です。値は **LoadLimit** に応じて増減します。

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

1. **/system/configuration/cluster** ノードに **newConferenceLoadLimitBasisPoints** の値と **existingConferenceLoadLimitBasisPoints** の値で PUT を発行します。

注： 分散されたコールは常に受け入れられるため、リソースはさらに消費されるようになります。ロード バランシングのパラメータを変更する際は、こうしたコールに必要となるオーバーヘッドも必ず計算に含めてください。

6.1.4 ロード バランシングにおける設定の使用

各 Call Bridge グループ内には、Call Bridge の選択に関するスペースごとの優先順位があります。スペース内のコールは、Call Bridge グループのどこかに到達すると、この優先順位に従って Call Bridge にリダイレクトされます。リダイレクトは、既存会議のしきい値と新しい会議のしきい値との 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。

既存会議のしきい値 = existingConferenceLoadLimitBasisPoints / 10000 X loadLimit

新しい会議のしきい値 = newConferenceLoadLimitBasisPoints / 10000 X loadLimit

コールが Call Bridge に到達すると、ローカルの負荷制限値が確認されます。これが既存会議のしきい値を超えている場合、コールは拒否されます。拒否されたコールはコール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。なお、コールはこれ以外の理由でも拒否できます。

負荷がこのしきい値を下回っている場合、コールは応答され、IVR は通過されます。会議が認識されると、グループ内での Call Bridge の優先順位が決定できるようになります。この順位は、選択可能な Call Bridge が複数ある場合にどの Call Bridge を使用するか決定するために使用されます。

グループ内のいくつかの Call Bridge がすでに会議を実行中の場合、これらの Call Bridge に対する負荷が確認されます。これらのいずれかが既存会議のしきい値を下回っている場合、その中の 1 つが使用されます。

会議がどの場所でも実行されていない場合、または現在ある会議を実行中の Call Bridge がすべて既存会議のしきい値を上回っている場合、それら以外の Call Bridge の負荷が確認されます。これらの Call Bridge のいずれかで負荷レベルが新しい会議のしきい値を下回っている場合、その中の 1 つが選択されます。

選択されている Call Bridge がまだ 1 つもない場合、負荷が既存会議のしきい値を下回っている Call Bridge が選択されます。

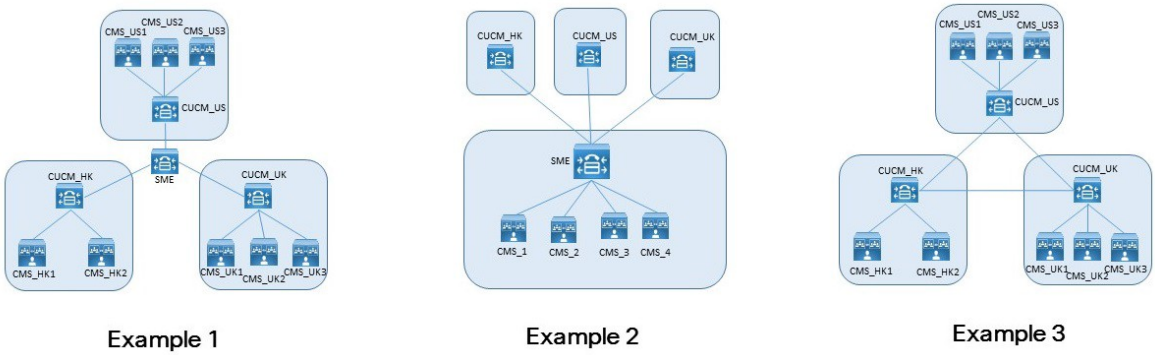
6.2 導入例

ロード バランシングに関するホワイト ペーパーでは、3 つの導入例を説明しています。

- 例 1 では、ミーティング サーバはローカルの Cisco Unified Communications Manager にトランキングされています。Cisco Unified Communications Manager はリーフ ノードとして Cisco Unified Communications Manager Session Management Edition（SME）に接続しています。SME はノード間でコールをルーティングします。
- 例 2 では、一元的な複数のミーティング サーバが SME および世界各地の Cisco Unified Communications Manager 導入環境にトランキングされています。

- 例 3 では、ミーティング サーバはローカルの Cisco Unified Communications Manager にトランキングされています。Cisco Unified Communications Manager 間はトランキングされているのみで、一元的にコールのルーティングを行う SME はありません。

図 2：3 つの導入例



Example 1　　Example 2　　Example 3

どのような導入環境でも、各種デバイスからのコールを各リソースにマッピングする方法には、3 つのオプションがあります。

- コーリング サーチ スペース（正しいパーティションの選択に使用）を持つ複数パーティション
- ローカル ルート グループを持つ単一パーティション。ルートの選択は、複数のデバイス プール経由で行います。
- 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

これらのオプションのいずれも、どのような導入環境でも使用できます。

最後のオプションは番号ダイヤル プランに適していますが、URI ダイヤルに LUA スクリプトが必要となります。これ以外の 2 つのオプションは、番号ダイヤリングでも URI ダイヤリングでも正常に動作します。

ミーティング サーバ全体にわたるロード バランシングのこれらの例の詳細については、ホワイト ペーパー [英語] を参照してください。

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。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. 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、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。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版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、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices/）をご覧ください。

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。

FCC クラス A 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス A デジタル装置の制限に準拠していることが確認済みです。これらの制限は、商業環境で装置を使用したときに、干渉を防止する適切な保護を規定しています。この装置は、無線周波エネルギーを生成、使用、または放射する可能性があり、この装置のマニュアルに記載された指示に従って設置および使用しなかった場合、ラジオおよびテレビの受信障害が起こることがあります。住宅地でこの装置を使用すると、干渉を引き起こす可能性があります。その場合には、ユーザ側の負担で干渉防止措置を講じる必要があります。

FCC クラス B 準拠装置に関する記述：この装置はテスト済みであり、FCC ルール Part 15 に規定された仕様のクラス B デジタル装置の制限に準拠していることが確認済みです。これらの制限は、住宅地で使用したときに、干渉を防止する適切な保護を規定しています。本機器は、無線周波数エネルギーを生成、使用、または放射する可能性があり、指示に従って設置および使用しなかった場合、無線通信障害を引き起こす場合があります。ただし、特定の設置条件において干渉が起きないことを保証するものではありません。装置がラジオまたはテレビ受信に干渉する場合には、次の方法で干渉が起きないようにしてください。干渉しているかどうかは、装置の電源のオン/オフによって判断できます。

- 受信アンテナの向きを変えるか、場所を移動します。
- 機器と受信機との距離を離します。
- 受信機と別の回路にあるコンセントに機器を接続します。
- 販売業者またはラジオやテレビの専門技術者に連絡します。

シスコでは、この製品の変更または改造を認めていません。変更または改造した場合には、FCC 認定が無効になり、さらに製品を操作する権限を失うことになります。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved.

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、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。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版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、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices）をご覧ください。