Cisco Collaboration Meeting Rooms（CMR）Hybrid コンフィギュレーション ガイド（TMS 15.0 - WebEx Meeting Center WBS30）

初版：2016 年 05 月 02 日

最終更新：2017 年 04 月 24 日

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

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

目 次

第 1 章

CMR Hybrid の概要

Cisco TelePresence 会議

Cisco TelePresence 会議で Cisco WebEx ブリッジ機能を設定および管理するには、Cisco TMS を使用します。会議中に、TelePresence 参加者に対し、その他のすべての TelePresence 参加者のライブビデオと、直近のアクティブな WebEx 参加者のビデオが表示されます。WebEx 参加者に対し、その他のすべての WebEx 参加者のビデオと、直近のアクティブな TelePresence 参加者のビデオが表示されます。

Cisco WebEx のブリッジ機能により、Cisco TelePresence MCU シリーズ または Cisco TelePresence Server のマルチポイント会議と、Cisco WebEx 会議サーバが統合されます。Cisco TelePresence 発信者はワンボタン機能（OBTP）または自動接続テクノロジーを使用して会議に接続します。MCU/TelePresence Server は会議の開始時刻に接続し、Cisco WebEx 会議に自動的に接続し、2 つの会議に参加します。Cisco WebEx との接続時に、Cisco TelePresence プレゼンテーション画面にウェルカム ページが表示されます。

プレゼンテーション共有の場合、TelePresence ユーザがビデオ ディスプレイ ケーブルを各自のコンピュータに接続し、（必要に応じて）ボタンを押して TelePresence 参加者および WebEx 参加者とプレゼーテンションを共有開始します。発言中の TelePresence 参加者のビデオが Cisco WebEx Web クライアントにストリーミングされます。WebEx からのビデオとプレゼンテーションは、TelePresence 参加者に対して表示されます。

Cisco WebEx Meetings

リモート参加者は、Cisco WebEx Meeting Center Web および/またはモバイル アプリケーションにログインすることで、Cisco WebEx 会議に参加します。Cisco TelePresence 参加者と共有するコンテンツが Meeting Center アプリケーションに自動的に表示され、WebEx 参加者は各自のデスクトップまたはアプリケーションを Cisco TelePresence 参加者と共有できます。デフォルトでは、WebEx 参加者に対し、現在発言中の Cisco TelePresence 参加者または WebEx 参加者のライブ ビデオが表示されます。

WebEx 参加者には、すべての WebEx 会議参加者の統合リストも表示されます。WebEx 注釈機能がサポートされています。WebEx 参加者は標準 WebEx Meeting Center アプリケーションの注釈ツールを使用して注釈を作成でき、この注釈は WebEx 参加者と TelePresence 参加者の両方に対して表示されます。ただし、TelePresence 参加者は注釈ツールを使用できません。

WebEx の最初の参加者が加わると、「TelePresence systems」が WebEx 参加者リストと全画面ビューの WebEx 参加者の行に表示されます。これは、Cisco CMR Hybrid 会議であることを示します。個々の TelePresence ユーザは WebEx 参加者リストに表示されません。代わりに [TelePresence システム（TelePresence systems）] とだけリストされます。また、TelePresence 参加者が発言中になると、発言中の参加者のウィンドウにこれが表示されます。

サポートされる機能

CMR ハイブリッド の主要な機能を次に示します。

- スケジュール済みの Always-On 個人コラボレーション会議室オプション
- WebEx アプリケーションと TelePresence デバイスの間での最大 1080p 画面解像度での双方向ビデオ共有
- 音声とプレゼンテーションの統合共有（会議に参加するすべてのユーザのアプリケーションおよびデスクトップ コンテンツの共有機能を含む）
- TelePresence デバイスの表示名を含む、WebEx 参加者の統合名簿
- 会議のネットワークベースの録音/録画（コンテンツ共有、チャット、およびポーリングを含む）
- CMR ハイブリッド会議を簡単にスケジュールできるようにする Cisco TelePresence Management Suite（Cisco TMS）を使用した、統合会議スケジューリング
- Cisco Expressway-E または Cisco VCS Expressway が提供するメディア暗号化によって実現される安全なコール制御および接続
- Unified CM および VCS を中心としたコール制御展開オプション
- Cisco TelePresence Conductor により提供される会議ブリッジの会議リソース割り当てと管理
- サードパーティのテレプレゼンス デバイスとの相互運用性
- Microsoft Lync クライアントとの相互運用性

表 *1*：*CMR* ハイブリッドの機能

サポートされる機能	説明
[音声（Audio）]	TelePresence 参加者は、G.711 および G.722 を使用する Cisco WebEx 会議参加者との間で双方向音声機能を使用できます。 （注） Cisco WebEx 側からはプレゼンテーション音声は送信されません。
ホスト	MCU/TS は、すべての TelePresence 参加者を接続するため会議開始時に自動的にダイヤルインします。会議主催者が WebEx で参加していない場合は、MCU/TS がホストになります。会議主催者がスケジュールされた開始時刻よりも前に WebEx で会議に参加すると、その主催者がホストになります。
スケジューリング	Cisco TMS、WebEx と TelePresence の Outlook 連携機能、Smart Scheduler、WebEx Scheduling Mailbox または WebEx Web サイトを使用して、WebEx での Cisco TelePresence 会議をスケジュール設定します。スケジュールされている Cisco TelePresence エンドポイントからワンボタン機能（OBTP）を使用するか、または Cisco TMS の自動接続機能を使用して会議を開始すると、会議の開始時刻にスケジュール済みエンドポイントがすべて接続されます。 WebEx ホストである場合は、Cisco Collaboration Meeting Rooms（CMR）Hybrid 会議の WebEx 部分を予定時刻よりも早く開始できます。WebEx 参加者がホストよりも前に WebEx 会議に参加しようとすると、会議はまだ開始されておらず、スケジュールされている開始時刻または WebEx ホストが参加するまで待機する必要があることを示すメッセージが、この参加者に対して表示されます。 （注） Cisco Collaboration Meeting Rooms（CMR）Hybrid の相互運用性ではスケジュール済みの会議のみサポートされます。スケジュールされていない TelePresence の参加者が Cisco Collaboration Meeting Rooms（CMR）Hybrid 会議に参加するには、会議（MCU/TelePresence Server）ブリッジに手動でダイヤルする必要があります。会議主催者は、会議をスケジュールするときにビデオダイヤル イン参加者のためにポートを予約します。 会議のスケジュールについては、『Cisco TelePresence Management Suite Administrator Guide』を参照してください。

サポートされる機能	説明
共有	Cisco TelePresence ユーザは、TelePresence エンドポイントのビデオ ディスプレイ ケーブルを各自のコンピュータに接続することで、プレゼンテーションを共有できます。サポートされるビデオディスプレイ インターフェイスは、VGA、DVI、HDMI、DisplayPort、および Mini DisplayPort などです。 Cisco WebEx Meeting Center クライアントは、デスクトップまたは選択されたアプリケーションを共有できます。エンドポイントでは、Cisco WebEx プレゼンテーションを解像度 1024 X 768 （XGA）で表示および共有します。 エンドポイントで送信可能な解像度は、エンドポイントのモデルに応じて異なりますが、TS/MCU はプレゼンテーションをトランスコードし、解像度 1024 x 768 で WebEx クラウドに送信します。
双方向ビデオ	Cisco TelePresence エンドポイントからのビデオが Cisco WebEx 参加者に送信され、また Cisco WebEx 参加者からのビデオが Cisco TelePresence エンドポイントに送信されます。 ライブ ビデオは、最低でも Common Intermediate Format（CIF）フォーマット（毎秒 30 フレーム）、約 300-450 kbps（最大 720p）で送信できます。 Cisco WebEx クライアントからのプレゼンテーションは各 TelePresence エンドポイントに表示されます。 （注） すべての CMR ハイブリッド 会議では、Cisco TelePresence Server または MCU を使用する必要があります。

エスカレートされた会議/インスタント会議

プライマリ展開では、Multiway（エスカレートされた会議の Cisco VCS 方式）はサポートされません。

機能の制約事項

CMR ハイブリッド のすべての制約事項と既知の問題のリストについては、CMR ハイブリッド のリリース ノートを参照してください。

関連資料

関連項目	リンク
Cisco TelePresence Conductor	Cisco TelePresence Conductor

関連項目	リンク
Cisco TelePresence Management Suite	Cisco TelePresence Management Suite
（オプション）Cisco Expressway シリーズ	Cisco Expressway シリーズ
Cisco TelePresence Video Communication Server（Cisco VCS）	Cisco TelePresence Video Communication Server
Cisco TelePresence Video Communication Server（Cisco VCS）	Cisco TelePresence Video Communication Server
Cisco Unified Communications Manager（Unified Communications Manager）	Cisco Unified Communications Manager
Cisco TelePresence Server	Cisco TelePresence Server http://www.cisco.com/c/en/us/support/conferencing/telepresence-server-on-multiparty-media-310/model.html http://www.cisco.com/c/en/us/support/conferencing/telepresence-server-on-multiparty-media-320/model.html
Cisco TelePresence MCU シリーズ	• MCU 5300 シリーズ • MCU 4501 シリーズ • MCU 4500 シリーズ • MCU 4200 シリーズ • MCU MSE シリーズ
Cisco WebEx のマニュアル	
Cisco WebEx 会議機能の使用方法に関する情報。	• Cisco WebEx サイト ホームページに移動します。 • Cisco WebEx Meeting Center アカウントにログインし、左側のナビゲーション ペインで [サポート（Support）] > [ユーザ ガイド（User Guides）] の順にクリックします。
Cisco TelePresence Integration オプションの指定と Cisco WebEx サイトの管理。	Cisco WebEx Site Administration アカウントと Cisco TelePresence を統合する，（171 ページ）を参照してください。

関連項目	リンク
Cisco Collaboration Meeting Rooms（CMR）Hybrid のマニュアル	
会議主催者を対象とした CMR Cloud の会議のスケジュール方法に関する情報	http://www.cisco.com/en/US/products/ps11338/products_user_guide_list.html

第 2 章

計画

CMR ハイブリッド の展開方法について

CMR ハイブリッド の中心的な要素は次のとおりです。

- TelePresence Conductor
- TelePresence Server または Cisco TelePresence MCU シリーズ会議ブリッジ（あるいはこの両方）
- Cisco TMS

会議ブリッジは TelePresence Conductor により管理されます。SIP トランクによりブリッジが TelePresence Conductor に接続され、TelePresence Conductor は 1 つ以上のコール コントローラにトランキングされます。すべての XML RPC 接続も、TelePresence Conductor 経由でルーティングされます。Cisco TMS は、会議のスケジュール、プロビジョニング、モニタなどの会議管理機能を提供します。XML RPC 接続により、Cisco TMS が TelePresence Conductor にリンクされます。

このソリューションアーキテクチャはSIP専用です。H.323エンドポイントを使用した会議には、Cisco VCS Control または Cisco Expressway-C によるインターワーキングが必要です。

CMR Hybrid は、次のいずれかのネットワークに展開できます。

- Cisco Unified-CM を中心としたネットワーク
- Cisco VCS を中心としたネットワーク

サポートされる展開モデルは、展開オプション，（29 ページ）のセクションで説明します。

Cisco TMS スケジュール権限

Cisco TMS は Cisco WebEx サイトへのコントロール リンクを提供します。このインターフェイスにより、Cisco TMS は WebEx ホストの代理として WebEx 対応会議を予約し、会議参加者に配布する Cisco WebEx 会議情報を取得することができます。次に Cisco TMS は Cisco WebEx 会議の詳細を TelePresence Server/MCU にプッシュします。

TelePresence Server および MCU の権限

Cisco TelePresence Server/MCU は WebEx Meeting Center クライアントと TelePresence エンドポイント間で最大 720p30 の双方向メイン ビデオを送受信できます。MCU/TS は WebEx Meeting Center クライアントに単一トランスコード ビデオ ストリームを送信します。

MCU/TS は TelePresence 会議参加者の単一の混合音声ストリームを WebEx クラウドに送信します。同様に、MCU/TS はすべての WebEx 参加者（PSTN または VoIP 経由で参加する WebEx Meeting Center 参加者を含む）からの単一の混合音声ストリームを受信します。

TelePresence エンドポイントと WebEx クライアント間での双方向コンテンツ共有の解像度として XGA（1024 X 768）がサポートされています。

各会議では、Transmission Control Protocol（TCP）の輻輳と TCP ウィンドウの問題の発生を回避するため、専用の SIP 接続が作成されます。

MCU/Cisco TelePresence Server は、スケジュールされた会議開始時刻に自動的に接続します。

CMR ハイブリッド で使用するポートとプロトコル

CMR ハイブリッド ソリューションの各種コンポーネント間では次のポートとプロトコルが使用されます。

コンポーネント間の通信	使用するポートとプロトコル
Cisco TMS から WebEx クラウド	TLS.443 を使用するエフェメラル ポート
WebEx and TelePresence Integration to Outlook から Cisco TMSXE	TLS.443 を使用するエフェメラル ポート

コンポーネント間の通信	使用するポートとプロトコル
Cisco VCS Expressway から WebEx クラウド	Expressway に設定されたトラバーサル サブゾーンのメディア ポート範囲に従って設定します。詳細については、『Cisco VCS Basic Configuration Control with Expressway Deployment Guide X8-5』の 52 ページ「*Appendix 3: Firewall and NAT Settings*」の「Inbound (Internet > DMZ)」を参照してください（Expressway 8.5 を使用する場合）。 以前にサポートされていたバージョンの Expressway を使用している場合は、Cisco.com の該当するバージョンの同じ項を参照してください。 （注） 発信については、1024 以降のすべてのポートが開かれている必要があります。
WebEx クライアントから WebEx クラウド	UDP ポート 9000-9001*

*すべての WebEx IP サブネットのリストについては、WebEx Knowledge Base の記事「WBX264」を参照してください。

注：UDP と TCP を使用する WebEx クライアントでは、顧客が各自のファイアウォール設定を確認し、UDP がブロックされないようにする必要があります。

重要 ディープ パケット インスペクションを実行するファイアウォール、ポート、およびプロトコルは使用しないでください。特に、Check Point Software Technologies, Inc. のファイアウォールで使用されているステートフル パケット インスペクションには、Cisco VCS Expressway および Expressway-E との互換性がありません。

スケジューリング フローについて

ここでは、次の機能を使用して CMR ハイブリッド をスケジュールする際の処理について説明します。

- Cisco WebEx and TelePresence Integration to Outlook を使用したスケジュール, （10 ページ）
- Cisco Smart Scheduler を使用したスケジュール, （12 ページ）
- Cisco WebEx Scheduling Mailbox を使用したスケジュール, （14 ページ）

（注） 複数の展開を同時に実行できます。たとえば、Smart Scheduler を使用する場合、TMSXEが展開されていると、会議に予約された会議室のカレンダーが会議の詳細で更新されます。

CiscoWebExandTelePresenceIntegrationtoOutlookを使用したスケジュール

Cisco WebEx and TelePresence Integration to Outlook でのスケジュールの流れ

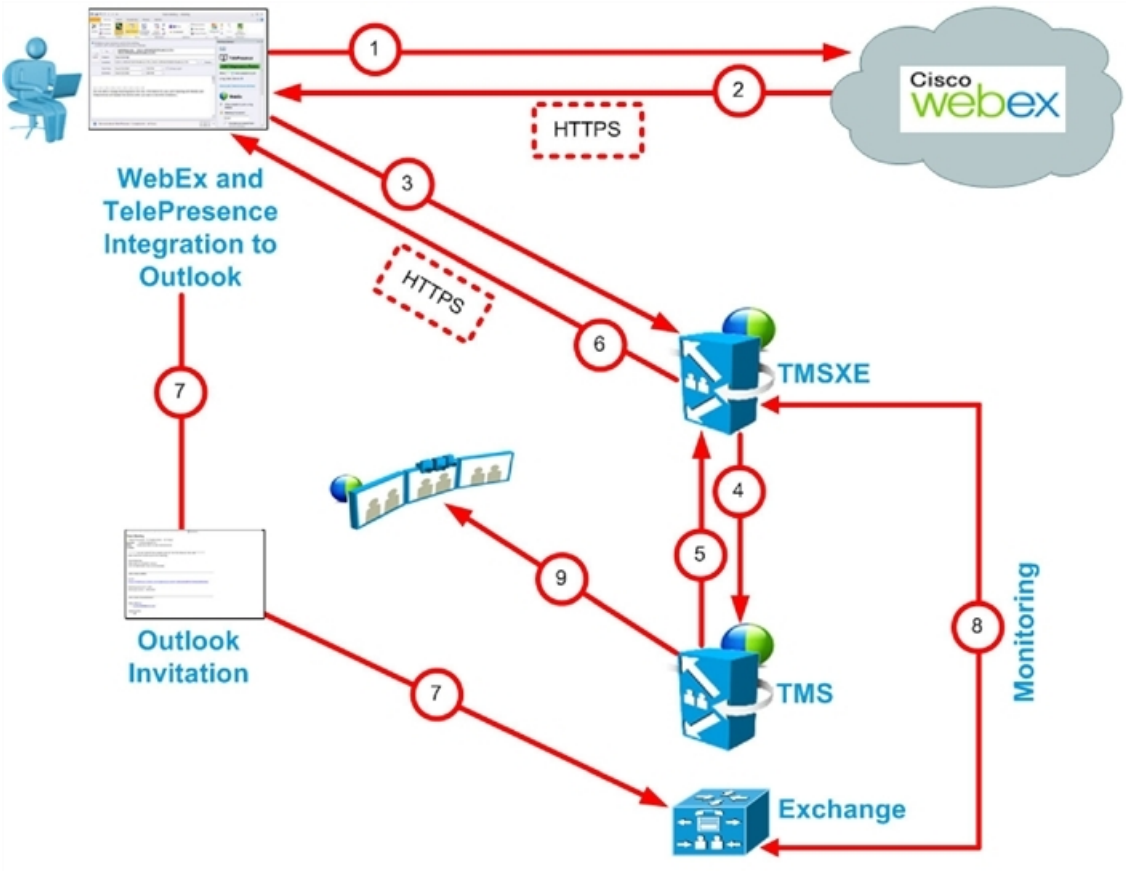


表 *2*：*Cisco WebEx and TelePresence Integration to Outlook* でのスケジュール手順

ステップ番号	説明
1	ユーザが Cisco WebEx and TelePresence Integration to Outlook を使用して会議を予約します。 ユーザを追加します。 会議室を追加します。 会議要求が WebEx に送信され、会議の WebEx 部分が予約されます。
2	WebEx が会議に関する次の情報で応答します。 会議の日時 会議の議題 音声ダイヤルイン情報 TSP 音声の場合、MCU が TSP プロバイダーにダイヤルするための追加情報がこの音声に含まれます。 ブリッジが WebEx にダイヤルインするための SIP ビデオおよび音声（SIP 音声の場合）ダイヤルイン情報 参加者がクリックする会議 URL
3	Cisco WebEx and TelePresence Integration to Outlook が TMSXE にコンタクトし、ステップ 2 の WebEx 情報を含んだ予約要求を行います。
4	TMSXE が同じ情報を含む予約要求を TMS に送信します。
5	TMS が会議を確認し、TMSXE に会議の詳細を返します。
6	TMSXE が Cisco WebEx and TelePresence Integration to Outlook に会議の確認を送信します。
7	Outlook の出席依頼が会議室を予約するために Exchange に送信され、追加された参加者に送信されます。
8	会議室が会議を受け入れることを確認するため、TMSXE が会議室のメールボックスをモニタします。
9	ユーザが TelePresence 会議室を招待すると、TMS のワンボタン機能情報が TelePresence エンドポイントに送信されます。

Cisco Smart Scheduler を使用したスケジュール

Cisco WebEx Smart Scheduler でのスケジュールの流れ

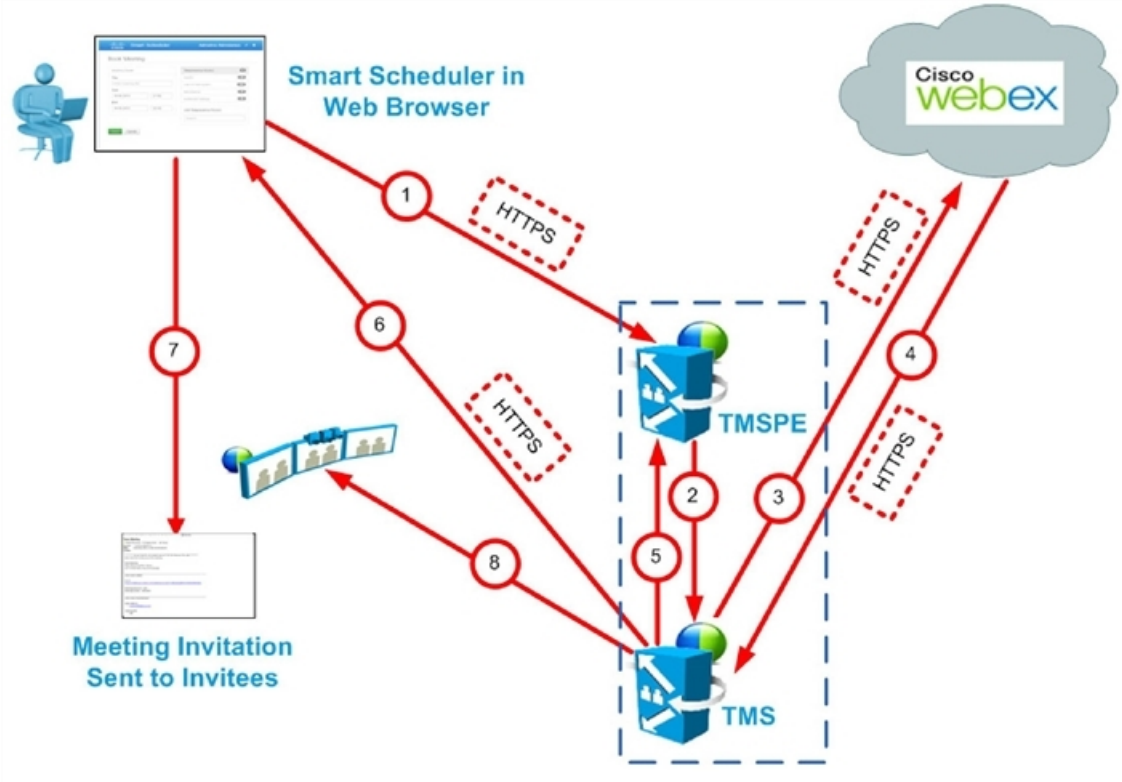


表 *3* : *Cisco Smart Scheduler* でのスケジュール手順

ステップ番号	説明
1	ユーザは Smart Scheduler を使用して会議を予約します。 会議室を追加します。 WebEx を追加します。 [保存（Save）] をクリックします。
2	TMSPE が TMS に予約要求を送信します。
3	TMS が WebEx に予約要求を送信します。 WebEx が会議の WebEx 部分を予約します。

ステップ番号	説明
4	WebEx が、TMS からの予約要求への応答として次に示す会議詳細を送信します。 会議の日時 会議の議題 音声ダイヤルイン情報 TSP 音声の場合、MCU が TSP プロバイダーにダイヤルするための追加情報がこの音声に含まれます。 ブリッジが WebEx にダイヤルインするための SIP ビデオおよび音声（SIP 音声の場合）ダイヤルイン情報 参加者がクリックする会議 URL
5	TMS が、TMSPE に対し予約確認情報で応答します。
6	TMS が確認メールをユーザに送信します。
7	ユーザが、会議の詳細を記載した会議招待状を招待者に送信します。
8	ユーザが TelePresence 会議室を招待すると、TMS のワンボタン機能情報が TelePresence エンドポイントに送信されます。

Cisco WebEx Scheduling Mailbox を使用したスケジュール

Cisco WebEx Scheduling Mailbox を使用したスケジュールの流れ

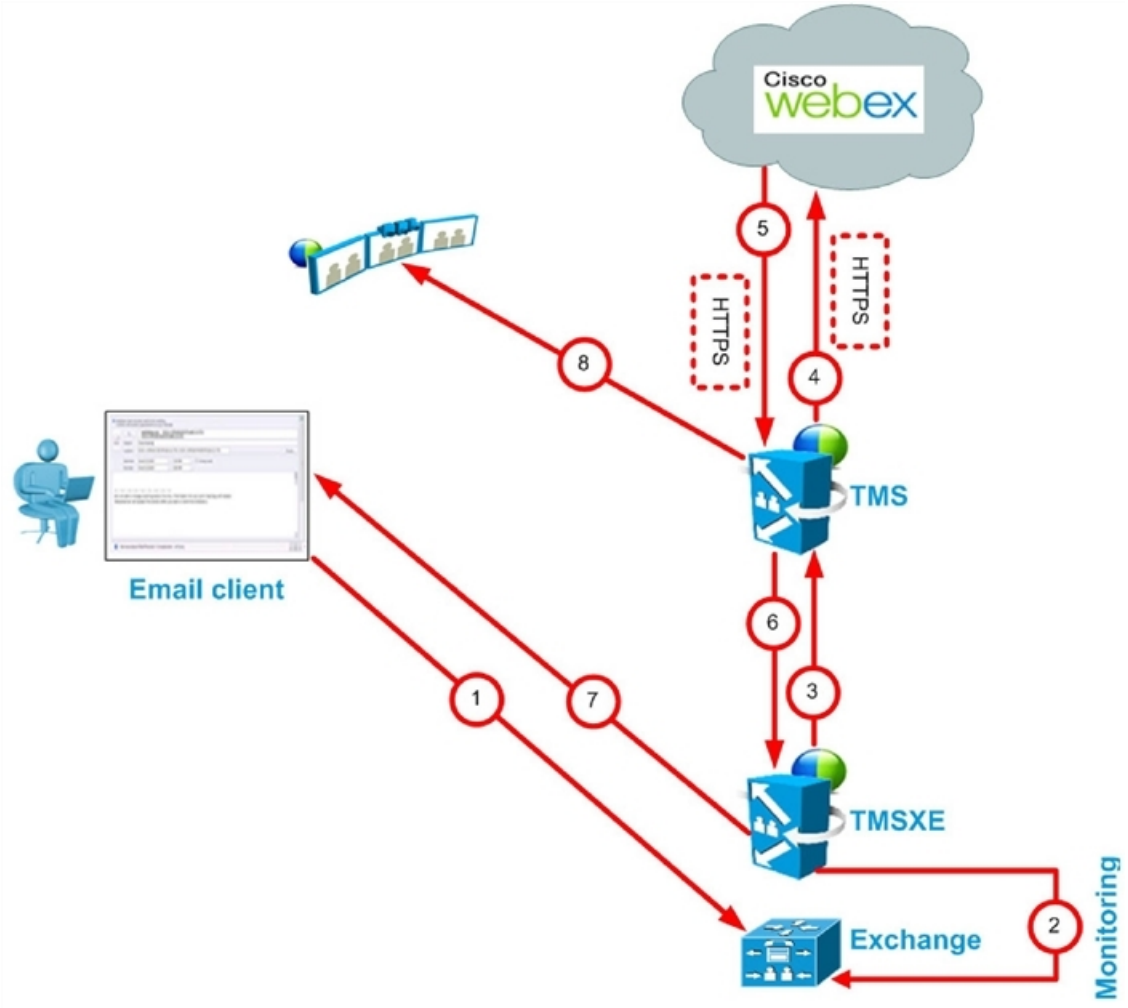


表 *4*：***Cisco WebEx Scheduling Mailbox*** を使用したスケジュール手順

ステップ番号	説明
1	Microsoft Exchange でサポートされる電子メール/カレンダー クライアントで、ユーザが会議を予約します。 会議室を追加します。 WebEx Scheduling Mailbox（例：webex@example.com）を追加します。 参加者を追加します。 [送信（Send）]をクリックします。 会議要求が Exchange に送信されます。
2	TMSXE が会議室のメールボックスと WebEx Scheduling Mailbox をモニタします。
3	TMSXE が TMS の Booking API と通信し、WebEx 対応会議を要求します。
4	TMS が WebEx に対し、会議の WebEx 部分を予約するよう要求します。
5	WebEx が、TMS からの予約要求への応答として次に示す会議詳細を送信します。 会議の日時 会議の議題 音声ダイヤルイン情報 TSP 音声の場合、MCU が TSP プロバイダーにダイヤルするための追加情報がこの音声に含まれます。 ブリッジが WebEx にダイヤルインするための SIP ビデオおよび音声（SIP 音声の場合）ダイヤルイン情報 参加者がクリックする会議 URL。
6	TMS が、TMSXE に対し予約確認情報で応答します。
7	TMSXE が確認メールを会議主催者に送信します。
8	ユーザが TelePresence 会議室を招待すると、TMS のワンボタン機能情報が TelePresence エンドポイントに送信されます。

TelePresence Conductor 管理ブリッジをスケジュールする場合の違い

TelePresence Conductor スケジュール展開環境に移行する前に、直接管理されているブリッジのスケジュールと、TelePresence Conductor により管理されるブリッジのスケジュールの相違点に注意してください。

表 *5*：*TelePresence Conductor* 管理ブリッジのスケジュールにおける相違点

	直接管理	TelePresence Conductor 管理
予約	• 会議ごとに会議設定を行い、デフォルトの会議設定をオーバーライドできます。 • Cisco TMS は会議のダイヤルイン番号を提供するため SIP URI を選択します。 • Cisco TMS参加者テンプレートおよび会議テンプレートに追加できます。 • ブリッジ リソースのオーバーブッキング オプションはありません。	• 一部の会議設定は TelePresence Conductor 会議テンプレートで設定され、予約中に変更できません。 • 会議のダイヤルイン番号を作成するため、ユーザは予約時にエイリアスの変数部分を入力できます。 • Cannot be added to Cisco TMS 参加者テンプレートおよび会議テンプレートに追加できません。 • ブリッジ リソースのオーバーブッキング：サービス設定の容量調整機能を使用して、サービス設定に関連付けられているプール内のブリッジで実際に使用可能なリソースをオーバーブッキングできるように、Cisco TMSを設定できます。このように設定すると、ユーザが会議に必要な数よりも多いポートを不必要に予約することが可能になるため、未使用のリソースをその他のユーザのために解放します。

	直接管理	TelePresence Conductor 管理
カスケード	• TelePresence Server のカスケードはサポートされていません。 • Cisco TMS は、会議のルーティング時に MCU をカスケードするかどうかを決定します。 • Cisco TMS では、会議開始後、ホスティング MCU の容量を超える参加者が参加する場合には、カスケードを作成することはできません。 • たとえば、会議制御センターの多くの機能では、参加者がカスケードしている MCU 間で移動されます。 • カスケードは、会議の予約時に [分散（Distribution）] オプションを使用して選択されます。 • Cisco TMS Booking API（Cisco TMSBA）を使用するクライアント（Microsoft Outlook や Smart Scheduler など）から予約を行う場合、カスケードは実行できません。	• カスケードされた TelePresence Server をサポートします。 • TelePresence Conductor はブリッジをカスケードします。 • TelePresence Conductor は、参加する参加者がホスティング ブリッジの初期容量を超えると、即時にカスケードを実行できます。 • 会議制御センターの機能はありません（参加者が接続しているブリッジを確認できる機能を除く）。 • 会議を予約するときに、カスケードをサポートするエイリアスを選択する必要があります。 • Cisco TMS Booking API（Cisco TMSBA）を使用するクライアント（Microsoft Outlook や Smart Scheduler など）から予約を行う場合、カスケードを実行できます。

	直接管理	TelePresence Conductor 管理
会議制御センター	すべての機能を利用できるかどうかは、会議をホストするブリッジのタイプに依存します。	次の機能は、TelePresence Conductor が管理する TelePresence Server でホストされる会議では使用できません。 • ビデオ プロトコル • 音声プロトコル • 暗号化のステータス（Encryption status） • 番号（Number） • 参加者の音声レベル • ビデオ解像度 • デュアル ビデオ ステータス • スナップショット

	直接管理	TelePresence Conductor 管理
レポート	全機能	• TelePresence Conductor により管理される会議ブリッジからのコール詳細レコード（CDR）には、会議 ID は含まれません。 • TelePresence Conductor 自体は、会議 CDR を Cisco TMS にフィードバックしません。ブリッジ自体は、Cisco TMS. に追加されている場合はフィードバックします。 • コールの方向によっては、不完全な CDR データを受け取る可能性があります。これは、ダイヤルアウトによって誤ったデータが発生する可能性があるためです。 • ブリッジ使用状況レポートは、TelePresence Conductor でホストされる会議ではサポートされません。
ゾーン	Cisco TMS は、IP ゾーンを使用して、システムが地理的に近いブリッジを使用するようにします。	Cisco TMS は、使用する TelePresence Conductor を IP ゾーンに基づいて選択しますが、ブリッジ自体の IP ゾーン情報は無視します。

コール フローについて

ここでは、次の CMR ハイブリッド 会議のコール フローについて説明します。

• SIP 音声コール フロー, （20 ページ）
• 待合室をアンロックする API コマンドを使用した TSP 音声コール フロー, （22 ページ）

- 待合室および MCU/TelePresence Server をホストとして使用する TSP 音声コール フロー, （24 ページ）
- WebEx 音声（PSTN）コール フロー, （25 ページ）

SIP 音声コール フロー

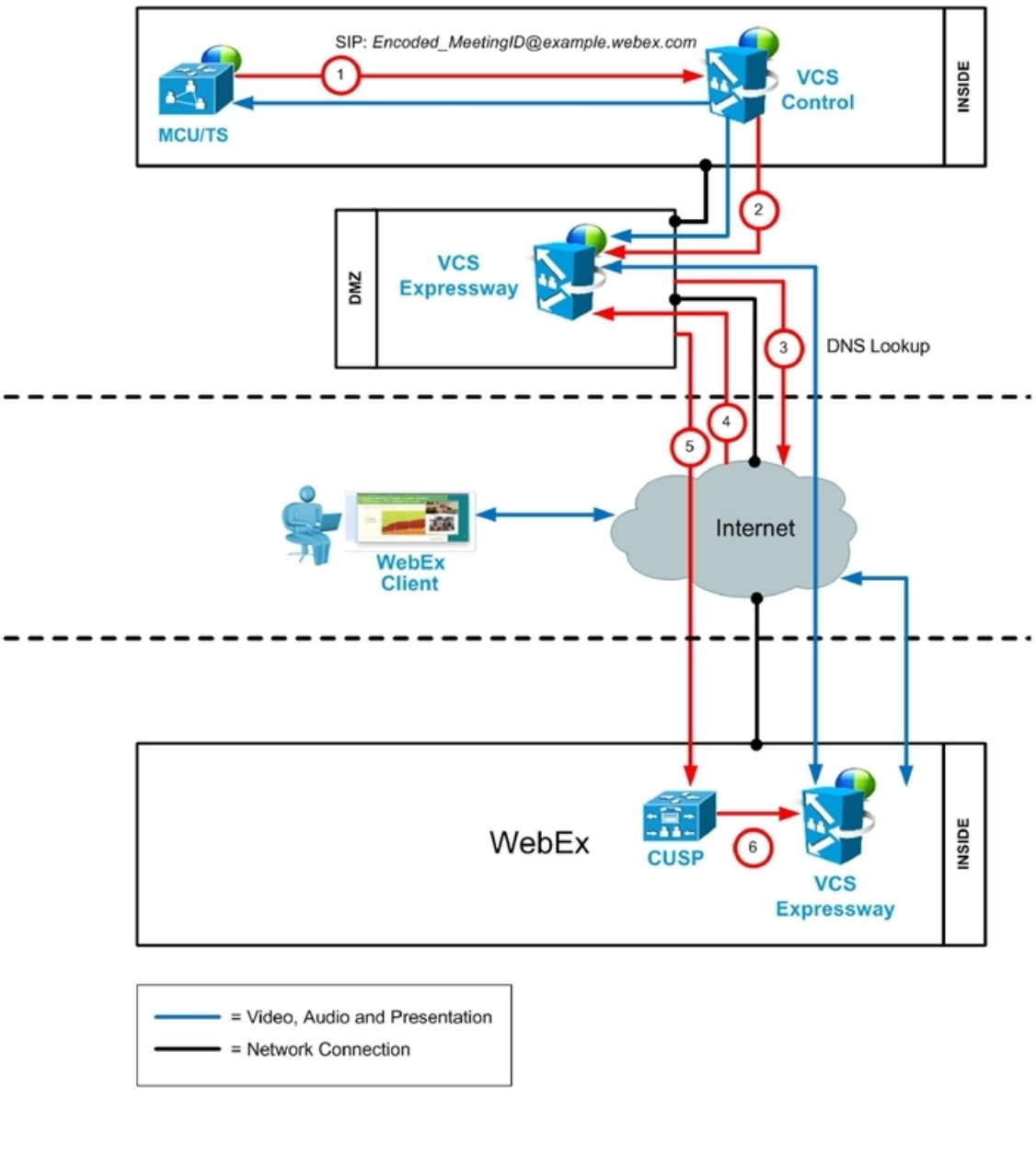


表 *6* : *SIP* 音声コール フローのステップ

ステップ番号	説明
1	MCU が SIP URI を使用して WebEx にコールし、このコールが Cisco VCS Control を介してルーティングされます。
2	Cisco VCS Control は、トラバーサル ゾーンを介して VCS-E にコールを送信します。
3	Cisco VCS Expressway が example.webex.com の DNS ルックアップを実行します。
4	DNS が example.webex.com を CUSP サーバに解決します。
5	Cisco VCS Expressway は CUSP にコールを送信します。このステップは常に暗号化されます（必須）（前のステップでは暗号化はオプションです）。 - Cisco VCS Expressway および CUSP サーバが相互の証明書を確認します。
6	CUSP がコールを WebEx dmz 内の Cisco VCS Expressway に転送します。 - このレッグも暗号化されます（必須）。
7	メディアが接続されます。 - メディアは（インターネット上で）2 つの Cisco VCS Expressway 間で暗号化されます。 - MCU と顧客サイト内の Cisco VCS Expressway の間での暗号化はオプションです。

待合室をアンロックする API コマンドを使用した TSP 音声コール フロー

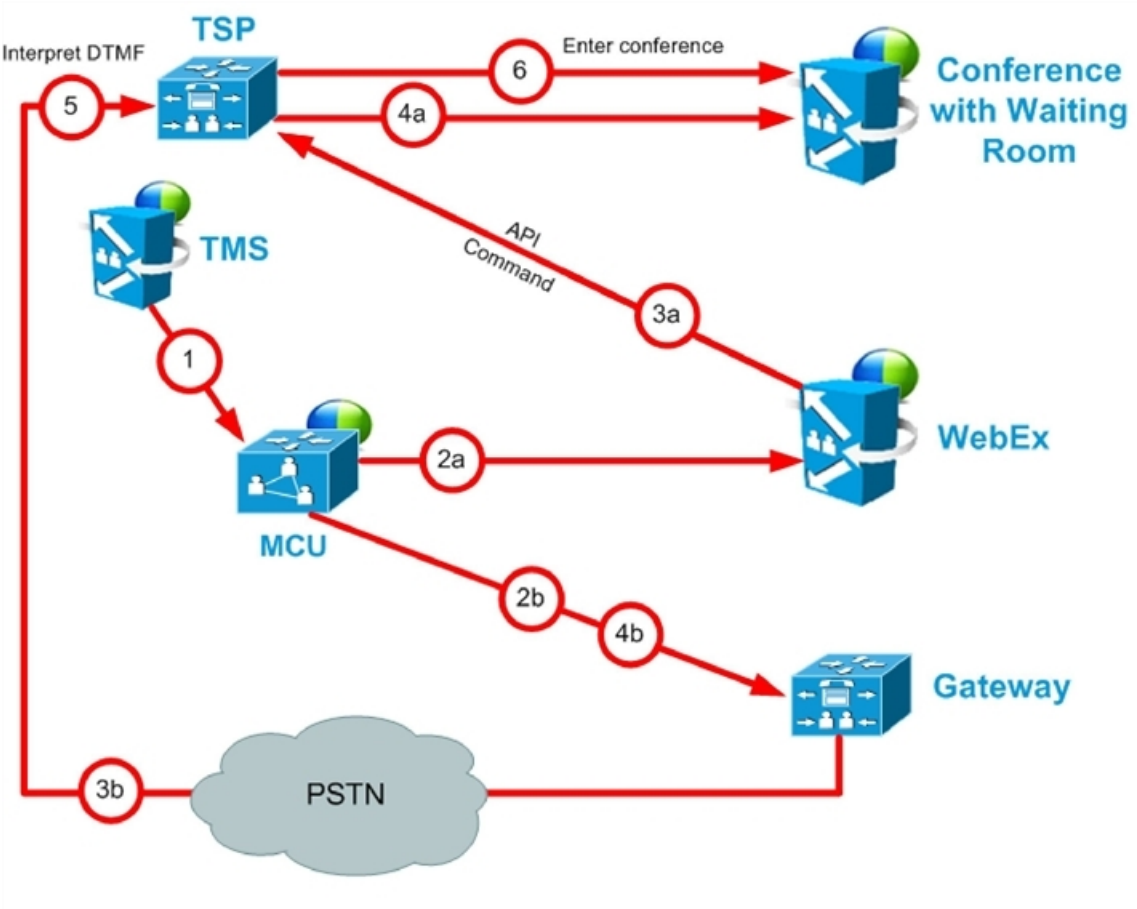


表 *7*：待合室をアンロックする *API* コマンドを使用した *TSP* 音声コール フローのステップ

ステップ番号	説明
1	TMS が MCU/TelePresence Server で会議を開始し、WebEx にダイヤルするための SIP URI、電話番号（PSTN 音声を使用する場合）、および DTMF 文字列（PSTN 音声を使用する場合）を MCU/TelePresence Server に渡します。
2a	MCU/TelePresence Server が SIP を介して WebEx にダイヤルします。（詳細については、「Understanding Cisco CMR Hybrid Call Flow [p.1]」を参照してください）。
2b	ステップ 2a と同時に、MCU/TelePresence Server が WebEx の PSTN コールイン番号にダイヤルします。

ステップ番号	説明
3a	WebEx は API コマンドを使用して、音声会議を開始することを TSP プロバイダーに通知します。WebEx はこの通知の一部として、会議タイプが telepresence であり、これにより待合室がアンロックされることを TSP プロバイダーに通知します。
3b	ステップ 3a と同時に、TSP プロバイダーが MCU/TelePresence Server に対して会議アクセス番号を求めます。
4a	TSP プロバイダーがステップ 3a に対応して待合室をアンロックします。
4b	ステップ 4a と同時に、MCU/TelePresence Server がステップ 3b で求められた DTMF トーンを TSP に送信します。
5	TSP プロバイダーが DTMF トーンを受信します。
6	TSP プロバイダーが MCU/TelePresence Server を音声会議に配置します。

待合室および MCU/TelePresence Server をホストとして使用する TSP 音声コール フロー

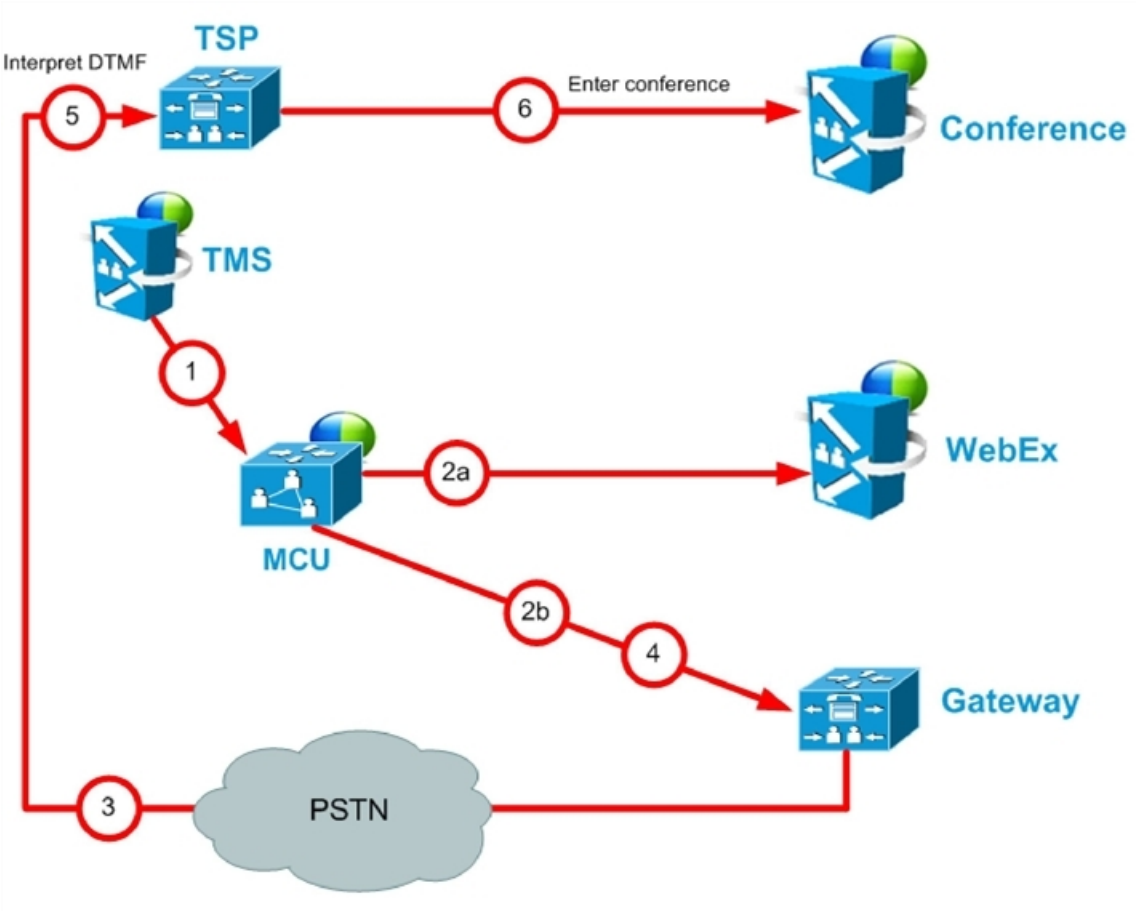


表 *8*：待合室および *MCU/TelePresence Server* をホストとして使用する *TSP* 音声コール フローのステップ

ステップ番号	説明
1	TMS が MCU/TelePresence Server で会議を開始し、WebEx にダイヤルするための SIP URI、電話番号（PSTN 音声を使用する場合）、および DTMF 文字列（PSTN 音声を使用する場合）を MCU/TelePresence Server に渡します。
2a	MCU/TelePresence Server が SIP を介して WebEx にダイヤルします。（詳細については、「Understanding Cisco CMR Hybrid Call Flow [p.1]」を参照してください）。
2b	ステップ 2a と同時に、MCU/TelePresence Server が WebEx の PSTN コールイン番号にダイヤルします。

ステップ番号	説明
3	TSP プロバイダーが MCU/TelePresence Server に対して会議アクセス番号とホスト キーを求めます。
4	MCU/TelePresence Server が、ステップ 3 で求められた DTMF トーンとホスト キーを送信します。
5	TSP プロバイダーが DTMF トーンを受信します。
6	TSP プロバイダーは待合室をアンロックし、MCU/TelePresence Server を音声会議に配置します。

WebEx 音声（PSTN）コール フロー

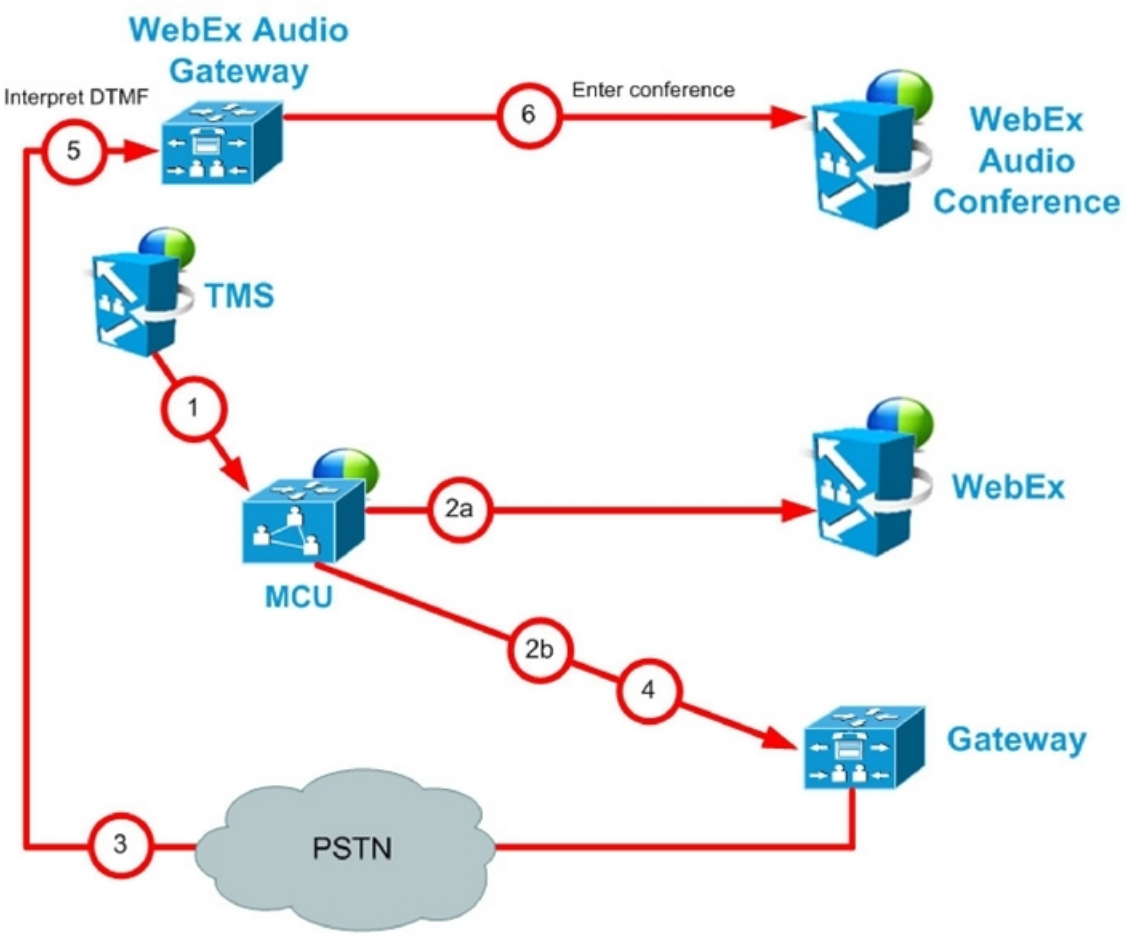


表 *9*：***WebEx*** 音声（***PSTN***）コール フローの手順

ステップ番号	説明
1	TMS が MCU で会議を開始し、WebEx にダイヤルするための SIP URI、電話番号、および DTMF 文字列を MCU に渡します。
2a	MCU が SIP を介して WebEx にダイヤルします。（詳細については、「Understanding Cisco CMR Hybrid Call Flow [p.1]」を参照してください）。
2b	ステップ 2a と同時に、MCU が WebEx の PSTN コールイン番号にダイヤルします。
3	WebEx から MCU に対し、会議のアクセス番号が要求されます。
4	MCU が、ステップ 3 で求められた DTMF トーンを TSP に送信します。
5	WebEx が DTMF トーンを受信します。
6	WebEx が MCU を音声会議に配置します。

サーバおよびサイトのアクセス チェックリスト

表 *10*：初めて ***CMR*** ハイブリッド を設定する前に準備しておく必要がある情報。

必要な情報	説明と入手先	終了（**Done**）
WebEx サイトの URL	Cisco WebEx サイトの URL。 Cisco WebEx アカウント チームから提供されます。 例： https://example.webex.com/example 手順については、Cisco TMS での Cisco WebEx 機能の設定，（120 ページ）を参照してください。	

必要な情報	説明と入手先	終了（Done）
WebEx サイトのホスト名	お客様が使用する WebEx サイトのホスト名。 Cisco WebEx アカウント チームから提供されます。 例：example.webex.com 手順については、Cisco TelePresence Management Suite を設定する，（119 ページ）を参照してください。	
WebEx Site Administration URL	Cisco WebEx Site Administration インターフェイスにアクセスするための一意のアドレス。このインターフェイスでは、Cisco WebEx の初回セットアップ設定を行い、初回セットアップ後にアカウントを管理および保守します。この URL では WebEx 管理サイトに直接移動します。 Cisco WebEx アカウント チームから提供されます。 例：https://example.webex.com/admin 手順については、Cisco WebEx Site Administration アカウントと Cisco TelePresence を統合する，（171 ページ）を参照してください。	
Cisco WebEx 管理者ユーザ名	Cisco WebEx 管理者アカウント ユーザ名。 Cisco WebEx アカウント チームから提供されます。 例：webexAdmin 手順については、Cisco WebEx Site Administration アカウントと Cisco TelePresence を統合する，（171 ページ）を参照してください。	

必要な情報	説明と入手先	終了（Done）
（オプション）証明書のペア（公開証明書と TMS の秘密キーを含む）	シングルサインオン（SSO）が TMS で有効になっている場合は、WebEx アカウントを持つユーザが予約した会議のために、WebEx クラウドに対して Cisco TMS を認証するために使用されます。SSO が設定されており、ユーザが WebEx 対応会議をスケジュールする場合、Cisco TMS ユーザ プロファイルの WebEx ユーザ名が WebEx サイトに渡され、予約が完了します。 手順については、Cisco TMS のシングル サインオンの設定，（132 ページ）を参照してください。	
Cisco VCS Expressway のクライアント/サーバ証明書	Cisco VCS Expressway と WebEx クラウドとの間でコール レッグを暗号化する必要があるためです。 手順については、Cisco Expressway および TelePresence 設定タスク，（90 ページ） および Cisco Expressway-E および Cisco VCS Expressway での証明書を設定する，（105 ページ）を参照してください。	

第 3 章

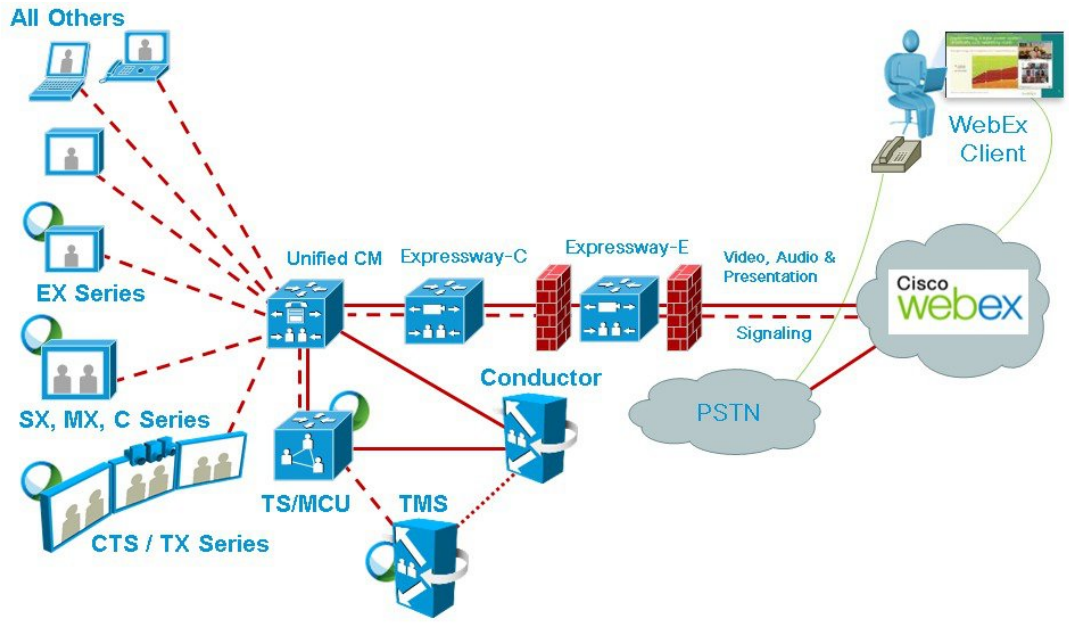
展開オプション

Unified CM を中心とした展開での SIP ビデオ、プレゼンテーション、および音声

WebEx は WebEx Audio を使用して展開されます。WebEx クラウドへの（または WebEx クラウドからの）メイン ビデオ、コンテンツ、音声は、顧客サイトの Cisco Expressway-E と WebEx クラウドの間でネゴシエートされます。IP 経由でのメディア（メイン ビデオ、コンテンツ、および音

声）フローはすべて SIP を使用してネゴシエートされます。青と緑のボールは、WebEx 対応エンドポイントを示します（エンドポイント ディスプレイにボールが表示されます）（OBTP）。

図 *1*：ネットワーク トポロジ：*SIP* ビデオ、音声、プレゼンテーション



Unified CM を中心とした展開での SIP ビデオ、プレゼンテーション、および PSTN 音声

WebEx は、PSTN を使用する WebEx 音声を使用して展開されます。顧客サイトの Cisco Expressway-E と WebEx クラウド（SIP/IP）で、メイン ビデオとコンテンツだけがネゴシエートされます。

スケジュール時に、Cisco TMS から MCU PSTN アクセス情報（ダイヤル番号、会議 ID、出席者 ID）が提供されます。Cisco MCU がコールし、PSTN 経由での WebEx クラウドへの音声のみのコールを設定し、DTMF を使用して会議 ID と参加者 ID を受け渡します。

この展開環境は、次のいずれかの方法でセットアップできます。

- Unified Communications Manager に登録された PSTN ゲートウェイを使用する。
- Cisco Expressway-C に登録された PSTN ゲートウェイを使用する

（注） Codian ISDN ゲートウェイを使用しているお客様は Cisco VCS Control に登録する必要があり、したがって Cisco VCS を使用する必要があります。

図 *2*：ネットワーク トポロジ：***Unified Communications Manager*** を使用した ***PSTN*** 音声の ***SIP*** ビデオおよびプレゼンテーション

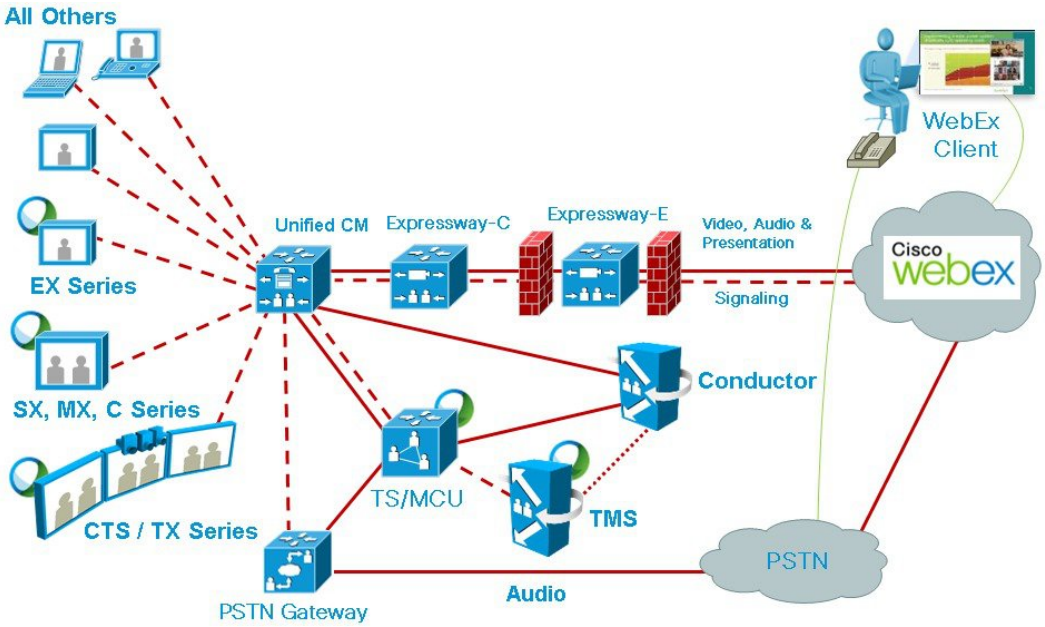
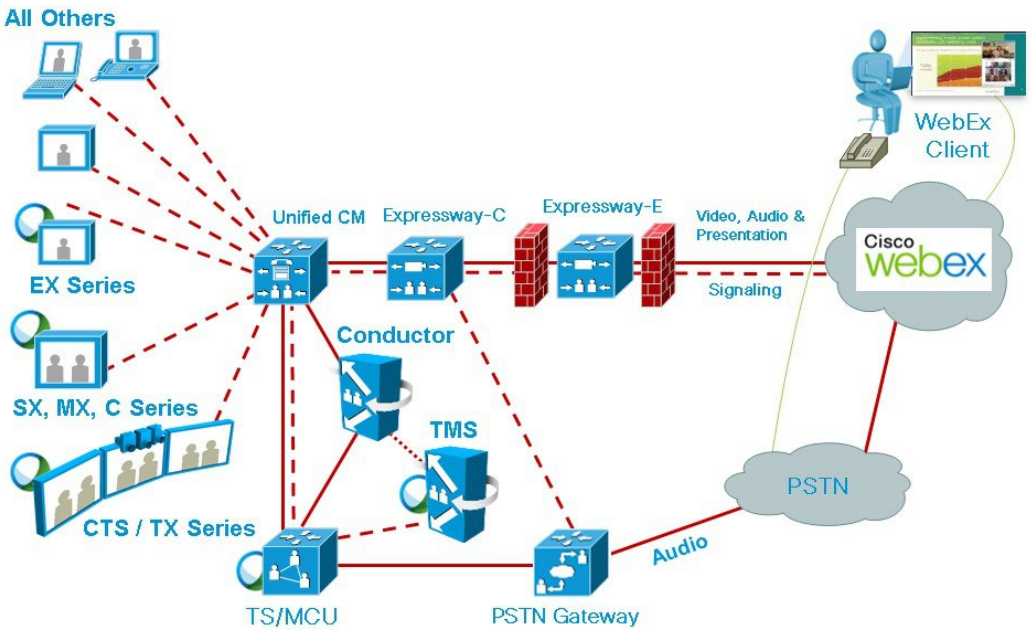


図 *3*：ネットワーク トポロジ：***Cisco Expressway-C*** を使用した ***PSTN*** 音声の ***SIP*** ビデオおよびプレゼンテーション

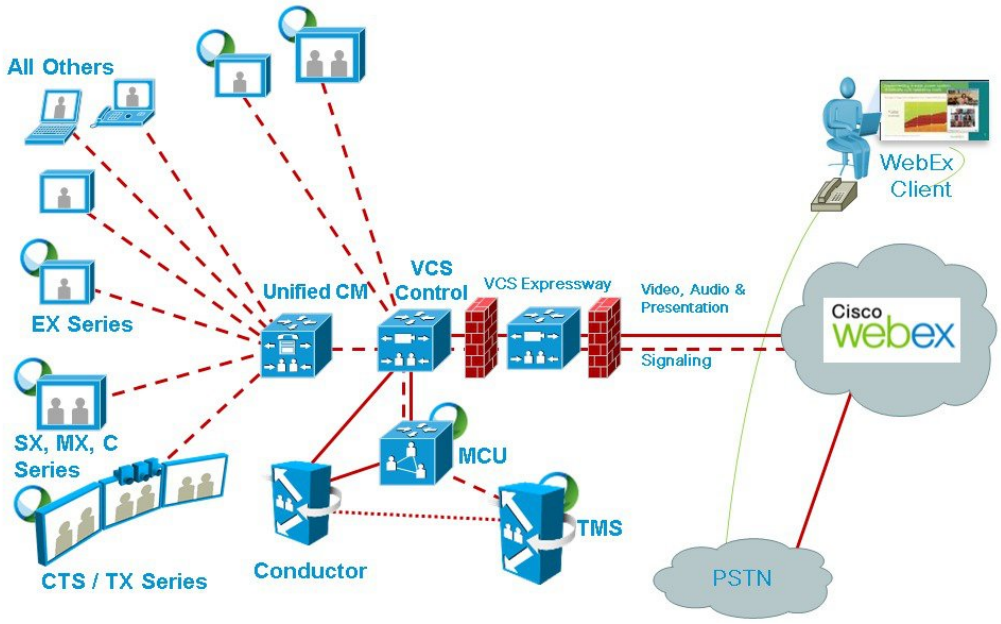


VCSを中心とした展開でのSIPビデオ、プレゼンテーション、および音声

WebEx は WebEx Audio を使用して展開されます。WebEx クラウドへの（または WebEx クラウドからの）メイン ビデオ、コンテンツ、音声は、顧客サイトの Cisco VCS Expressway と WebEx クラウドの間でネゴシエートされます。IP 経由でのメディア（メイン ビデオ、コンテンツ、および

音声）フローはすべて SIP を使用してネゴシエートされます。青と緑のボールは、WebEx 対応エンドポイントを示します（エンドポイント ディスプレイにボールが表示されます）（OBTP）。

図 *4*：ネットワーク トポロジ：*SIP* ビデオ、音声、プレゼンテーション



VCSを中心とした展開でのSIPビデオ、プレゼンテーション、および PSTN 音声

WebEx は、PSTN を使用する WebEx 音声を使用して展開されます。顧客サイトの Cisco VCS Expressway と WebEx クラウド（SIP/IP）で、メイン ビデオとコンテンツだけがネゴシエートされます。

スケジュール時に、Cisco TMS から MCU PSTN アクセス情報（ダイヤル番号、会議 ID、出席者 ID）が提供されます。Cisco MCU がコールし、PSTN 経由での WebEx クラウドへの音声のみのコールを設定し、DTMF を使用して会議 ID と参加者 ID を受け渡します。

この展開環境は、次のいずれかの方法でセットアップできます。

- Unified Communications Manager に登録された PSTN ゲートウェイを使用する。

- VCS に登録された PSTN ゲートウェイを使用する。

図 *5*：ネットワーク トポロジ：***Unified Communications Manager*** を使用した ***PSTN*** 音声の ***SIP*** ビデオおよびプレゼンテーション

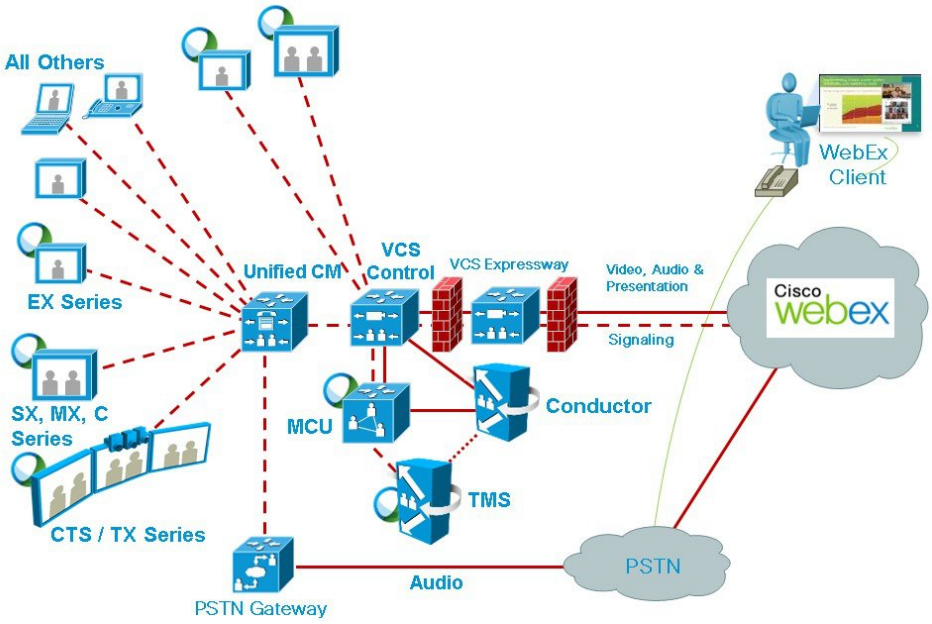
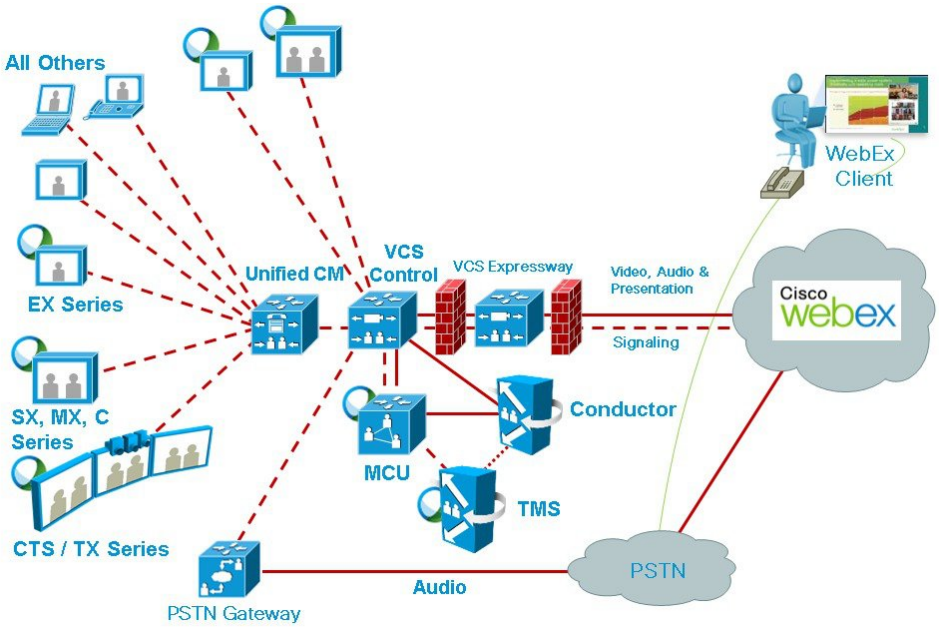


図 *6*：ネットワーク トポロジ：***Cisco VCS Control*** を使用した ***PSTN*** 音声の ***SIP*** ビデオおよびプレゼンテーション



第 4 章

要件

CMR Hybrid の前提条件

CMR ハイブリッド製品とサービスの要件

表 *11*：*CMR* ハイブリッド製品とサービスの要件

要件	説明	最小バージョン	推奨されるバージョン
Cisco TelePresence Conductor	会議リソース割り当ておよび会議ブリッジの管理に TelePresence Conductor が必要です。 特定の TelePresence Server および MCU とともに使用するために必要です。Conductor が必要かどうかを判断するには、使用する予定のブリッジのマニュアルを参照してください。 TelePresence Conductor は、Back-to-Back User Agent（B2BUA）を使用して展開する必要があります。外部ポリシー サーバ インターフェイスはサポートされていません。	XC3.0 TSP 音声には XC3.0.2 が必要です。	XC4.0 以降
Cisco TelePresence Management Suite（Cisco TMS）	Cisco TMS は、CMR Cloud 会議のスケジュールに必要です。	14.6	15.0 以降 TMSXE 5.0 および WebEx Meeting Center WBS30 以降で新しい WebEx 生産性向上ツール機能を取得するために必要です。詳細については、リリース ノートを参照してください。

要件	説明	最小バージョン	推奨されるバージョン
Microsoft SQL Server	Cisco TMS のデータベース	2008 R2 64 ビット	2012 SP2 64 ビット
Cisco TelePresence Management Suite Extension for Microsoft Exchange（Cisco TMSXE）	Cisco TMSXE は、WebEx Productivity Tools プラグインまたは WebEx Scheduling Mailbox を使用して Microsoft Outlook で CMR ハイブリッド会議をスケジュールするために必要です。	4.1	5.0 以降 TMS 15.0 および WebEx Meeting Center WBS30 以降で新しい WebEx 生産性向上ツール機能を取得するために必要です。詳細については、リリース ノートを参照してください。
Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）	Cisco TMSPE は、Smart Scheduler を使用する Cisco Collaboration Meeting Rooms（CMR）Hybrid 会議のスケジュール設定に必要です。 （注） Smart Scheduler を使用する際に、TMS プロビジョニング オプション キーは必要ありません。	1.4	1.5 以降
Cisco Expressway	Cisco Expressway-C と Cisco Expressway-E は、Unified CM を中心とした展開環境に必要です。 （注） 注：Cisco Expressway を購入するには、Unified CM ライセンスが必要です。	X8.5.3	X8.6.1 以降（完全な URI のダイヤルを使用する WebEx への無料トラバーサル/RMS のコール用）

要件	説明	最小バージョン	推奨されるバージョン
Cisco Unified Communications Manager（Unified Communications Manager）	Unified Communications Manager は Unified CM を中心とした展開環境に必要です。また、エンドポイントが Unified Communications Manager に登録されている場合は VCS を中心とした展開環境でも Unified CM を使用できます。	10.5(2) SU1	10.5(2) SU2 以降
Cisco TelePresence Video Communication Server	（オプション）ネットワーク内のレガシー/H.323 エンドポイントからのコールをサポートするには、エンドポイントを Cisco VCS に登録する必要があります。	X8.5.3	X8.6.1 以降（完全な URI のダイヤルを使用する WebEx への無料トラバーサル/RMS のコール用）
Cisco TelePresence Server	TelePresence Server は CMR ハイブリッド会議用の会議ブリッジとして使用できます。 TelePresence Server ブリッジは TelePresence Conductor にトランキングされます。また、TelePresence Conductor によるリモート管理のために TelePresence Server ブリッジを設定する必要があります。	4.1	4.2 以降
Cisco TelePresence MCU シリーズ	Cisco TelePresence MCU シリーズは CMR ハイブリッド会議用の会議ブリッジとして使用できます。	4.4	4.5 以降 Unified Communications Manager を中心とした展開環境に必要です。

要件	説明	最小バージョン	推奨されるバージョン
Cisco WebEx Meeting Center	WebEx Meeting Center サイトは Cisco TelePresence Integration をサポートするように設定する必要があります。詳細については、Cisco WebEx Site Administration アカウントと Cisco TelePresence を統合する，（171 ページ）を参照してください。	最新のサービスパックをインストールした WBS29.11。	最新のサービスパックをインストールした WBS30 以降。 TMS 15.0 および TMSXE 5.0 以降で新しい WebEx 生産性向上ツール機能を取得するために必要です。詳細については、リリースノートを参照してください。
	リソース割り当てのガイドライン（会議あたり） - 最大限のエクスペリエンスを実現するには、WebEx Meeting Center クライアントあたり 1.3 mb/秒以上の帯域幅が必要です。 - TCP 経由で接続する WebEx クライアントは、ネットワーク障害に対する耐性が低くなり、WebEx と UDP からのダウンスピードを要求する可能性が高くなります。WebEx Meeting Center クライアントに対し UDP ポート 9000/9001 を開きます。		

要件	説明	最小バージョン	推奨されるバージョン
	アカウント検証のガイドライン Cisco TMS での Cisco Collaboration Meeting Rooms（CMR）Hybrid会議をスケジュールする各ユーザは、WebEx サイト上のホストアカウントを持っている必要があります。 WebExアカウントのユーザ名とパスワードを、スケジュール設定に使用する WebEx サイトと共に、Cisco TMS の各会議スケジュール担当者のユーザプロファイルに追加する必要があります。 Cisco TMS は、認証済み Cisco WebEx アカウント所有者を検証します。 （注） TMS でシングルサインオン（SSO）が設定されている場合は、WebEx パスワードは必要ありません。詳細については、Cisco TMS のシングル サインオンの設定, （132 ページ）を参照してください。		
サポートされるエンドポイント	TelePresence Server または MCU によってサポートされているどのエンドポイントでも、CMR Cloud 会議に参加できます。 WebEx 参加者に対して表示されるようにするには、エンドポイントで BFCP プロトコルがサポートされている必要があります。	該当なし	

CMR ハイブリッド CPU の要件

表 *12*：*CMR* ハイブリッド *CPU* の要件

要件	説明
CPU 性能：最適なビデオ品質と、Cisco WebEx と Cisco TelePresence ネットワークの統合のための推奨事項。	推奨される CPU 性能（実行するアプリケーションに応じて異なる）は、デュアル コア CPU 2.5 GHz、および 2 GB 以上の実行メモリです。

CMR ハイブリッド ネットワーク要件

表 *13*：*CMR* ハイブリッド ネットワーク要件

要件	説明
ネットワークの要件と推奨事項	CMR ハイブリッド で最適な結果を得るためには、お客様が次のネットワーク要件と推奨事項に従う必要があります。 • 顧客宅内から WebEx への UDP 接続では、パケット損失率が 6 ～ 8 % 未満でなければなりません。WebEx Site Administration 設定で UDP が選択されていることを確認します。詳細については、以下を参照してください Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合，（171 ページ） • 顧客宅内からパブリック インターネット経由での WebEx へのネットワーク接続では、パケット損失率が 1% 未満でなければなりません。満足できるレベルのビデオ画質を得るには、パケット損失率が 0.05 % 未満である必要があります。 • MCU/TelePresence Server と Cisco WebEx の間のネットワーク帯域幅は上り 2 ～ 4 Mbps 以上である必要があります。たとえば、5 つの同時 Cisco WebEx コールが予想される場合は、帯域幅が 2 ～ 4 Mbps のインスタンスが 5 つ必要です。

CMR ハイブリッドで使用されている IP 範囲、プロトコルおよびポート

CMR ハイブリッド で最適な結果を得るためには、お客様が次に示すすべての IP 範囲とポートでの接続を許可することが推奨されます。

IP 範囲

米国/カナダ

- 64.68.96.0/19（CIDR）または 64.68.96.0 - 64.68.127.255（ネット範囲）
- 66.114.160.0/20（CIDR）または 66.114.160.0 - 66.114.175.255（ネット範囲）
- 66.163.32.0/20（CIDR）または 66.163.32.0 - 66.163.47.255（ネット範囲）
- 208.8.81.0/24（CIDR）または 208.8.81.0 - 208.8.81.255（ネット範囲）
- 173.243.0.0/20（CIDR）または 173.243.0.0 - 173.243.15.255（ネット範囲）

APAC

- 210.4.192.0/20（CIDR）または 210.4.192.0 - 210.4.207.255（ネット範囲）
- 114.29.192.0/19（CIDR）または 114.29.192.0 - 114.29.223.255（ネット範囲）

EMEA

- 62.109.192.0/18（CIDR）または 62.109.192.0 - 62.109.255.255（ネット範囲）

表 *14*：*WebEx* クライアントにより発信通信と着信接続で使用されるプロトコルとポート（*Windows* および *MAC*）

プロトコル	ポート番号	アクセス タイプ（Access Type）
[TCP]	80	クライアント アクセス
[TCP]	443	クライアントアクセス - セキュア トラフィック（SSL サイト）
TCP/UDP	1270	クライアントアクセス（非SSL サイト）
TCP/UDP	53	ドメイン ネーム システム（DNS）
TCP/UDP	5101	マルチメディア プロセッサ（MMP）

[TCP]	8554	オーディオ ストリーミング クライアント アクセス
UDP	7500	オーディオ ストリーミング
UDP	7501	オーディオ ストリーミング
UDP	9000	VoIP/ビデオ
UDP	9001	VoIP/ビデオ

表 *15*：*Expressway Edge* または *VCS Expressway* により *TelePresence* エンドポイントからの発信コールで使用されるポート

プロトコル	ポート番号	アクセス タイプ（Access Type）
[TCP]	5060 - 5065	コール シグナリング（プライマリおよびバックアップ）
UDP	36000 - 59999	コール メディア（プライマリおよびバックアップ）

（注） 重要：ディープ パケット インスペクションを実行するファイアウォール、ポート、およびプロトコルは使用しないでください。特に、Check Point Software Technologies, Inc. のファイアウォールで使用されているステートフルパケットインスペクションには、Cisco VCS Expressway および Expressway-E との互換性がありません。

このため、VCS Expressway または Expressway-E との間でネットワーク トラフィックを送受信するルータ/ファイアウォールでは、SIP および H.323 アプリケーション層ゲートウェイを無効にすることを強く推奨します。これは、これらのゲートウェイが有効になっていると、VCS の組み込みファイアウォール/NAT トラバーサル機能に悪影響を及ぼす可能性があるためです。

会議ブリッジ

ソリューションのプライマリ展開アーキテクチャでは、TelePresence Server の会議ブリッジを使用します。（このリリースでは、オプションの追加機能としてMCU もサポートします）会議ブリッジは TelePresence Conductor にトランキングされます。

- Conductor によるリモート管理がオプションで設定可能なモデルの場合は、TelePresence Server を Conductor によるリモート管理用に設定する必要があります。

- Multiparty ライセンスをサポートするには、TelePresence Conductor と会議ブリッジ間の接続で HTTPS を使用する必要があります。
- 会議ブリッジでは H.323 を無効にする必要があります。

Multiparty ライセンス

Multiparty ライセンスでは、Cisco TelePresence Server にスクリーン ライセンスをローカルでロードする代わりに、Cisco TelePresence Conductor 上でライセンスを一元管理することができます。次の 2 種類のライセンスを利用できます。

- Personal Multiparty（PMP）ライセンス：指定された個々のホストに適用されます。

PMP ライセンスは、Cisco Unified Workspace Licensing（CUWL Pro）で購入します。コール制御に Unified CM を利用する場合に使用できます。

- Shared Multiparty（SMP）ライセンス：複数のホストで共有し、会議の間適用されます。

SMP ライセンスは、コール制御に Unified CM または Cisco VCS を利用する場合に使用できます。

各 TelePresence Conductor は、Multiparty ライセンスまたは TelePresence Server スクリーン ライセンスのいずれか一方をサポートできますが、両方を同時にサポートすることはできません。ただし、TelePresence Server と Cisco TelePresence MCU シリーズ会議ブリッジを組み合わせて使用している場合は、同じ Conductor 上で TelePresence Server 用に Multiparty ライセンスを使用し、同時に、MCU 用にポート ライセンスを使用することができます。

TelePresence Conductor

TelePresence Conductor は、Back-to-Back User Agent（B2BUA）を使用して展開する必要があります。外部ポリシー サーバ インターフェイスはサポートされていません。

Multiparty ライセンスを使用する場合は、TelePresence Server のスクリーン ライセンスは必要ありません。代わりに、Multiparty ライセンスが TelePresence Conductor で集中管理されます。

Cisco TelePresence MCU シリーズ ブリッジを使用する場合は、Multiparty ライセンス モードで動作する Conductor にブリッジを追加できますが、個々のブリッジにポート ライセンスをインストールする必要があります。

Cisco Expressway/Cisco VCS のデフォルト SIP TCP タイムアウト

Cisco Expressway/Cisco VCS バージョン X8.5.3 以降では、SIP TCP タイムアウト値が設定可能です。デフォルト値は10秒です。タイムアウトを展開環境に適した最小値に設定することを強く推

奨します。ネットワークの遅延が極端に大きい場合（衛星通信経由のビデオなど）を除き、ほとんどの場合は、値を 1 秒にするのが適切です。

外部の DNS 宛先に対して発信コールが実行され、その宛先にセカンダリ/ターシャリ サーバがあり、プライマリ サーバが停止している場合は、タイムアウトが発生してセカンダリ サーバが試行されるまでにN秒（Nはタイムアウト値）かかり、再度タイムアウトが発生してターシャリ サーバが試行されるまでにN秒かかります（以下同様）。これは、B2B ポイントツーポイント コールやクラウドベースのホステッド サービスへのコールに適用されます。

SIP TCP タイムアウト値を設定するには、次の手順を実行します。

手順

ステップ 1 コマンドライン インターフェイスにアクセスします（Web インターフェイスでこの設定を行うことはできません）。

ステップ 2 次のコマンドを入力し、「n」を必要なタイムアウト値に置き換えます。xConfiguration SIP Advanced SipTcpConnectTimeout: n
例： xConfiguration SIP Advanced SipTcpConnectTimeout: 1

セキュリティと暗号化

シグナリング トラフィック

TelePresence Conductor とブリッジ間の SIP 通信には、TLS 暗号化が必須です。Multiparty ライセンスには、Conductor とブリッジ間の HTTPS 接続が必要です。また、ソリューションの他のすべての SIP（および XML RPC）通信（エンドポイントとコール コントローラ間、およびコール コントローラと TelePresence Conductor 間）には、TLS を推奨します。

メディア トラフィック

メディア トラフィックには、SRTP 暗号化を推奨します。コールが SRTP 暗号化メディアをサポートするためには、次のように、関連付けられている SIP シグナリングがすべてのホップに TLS を使用する必要があります。

1. エンドポイントとコール コントローラ間。
2. コール コントローラと TelePresence Conductor 間。
3. TelePresence Conductor と会議ブリッジ間（どんな場合でも常に必須）。

注意 TLS シグナリングが 3 つすべての要素に適用されていない場合は、コールで SRTP をサポートできません。

設定の概要

会議ブリッジは、TCP ポート 5061 とシグナリング モード TLS を使用するように設定する必要があります（[SIP設定（SIP Settings）] ページ）。TelePresence Server バージョン 4.2 以降では、TLS 経由の HTTPS および SIP シグナリングで会議ブリッジに暗号キーをインストールする必要はありません。メディア暗号化では、メディア暗号キーをインストールする必要があります。ポート 443 が HTTPS のデフォルトであり、ポート 5061 が TLS のデフォルトです。

TelePresence Conductor の [ロケーション（Location）] とコール コントローラ（[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]）で TCP ポート 5061 および TLS シグナリング モードを指定します。詳細については、『Cisco TelePresence Conductor with Unified Communications Manager Deployment Guide』を参照してください。

Cisco Expressway/Cisco VCS からのメディア暗号化

Expressway ソリューションを DNS ゾーンの宛先に向けて出力するコールにメディア暗号化を適用する場合は、この方法を使用することを強く推奨します。

手順

ステップ 1 トラバーサル クライアント ゾーンで Cisco Expressway-C/Cisco VCS Control から Cisco Expressway-E/Cisco VCS Expressway に向けて、メディア暗号化を有効にします。これを行うには、[メディア暗号化モード（Media encryption mode）] をセキュリティ ポリシーに応じて [ベストエフォート（Best effort）] または [強制暗号化（Force encrypted）] に設定します。

ステップ 2 DNS 出力ゾーンで Cisco Expressway-E/Cisco VCS Expressway からインターネットに向けて、その他の不要なメディア暗号化を無効にします。これを行うには、そのゾーンの [メディア暗号化モード（Media encryption mode）] を [自動（Auto）] に設定します。

回復力とクラスタリング

ソリューション コンポーネントをクラスタ構成で展開して障害発生時の冗長性を提供することをお勧めします。TelePresence Conductor と複数のブリッジ プールで構成されるクラスタを導入すると、エスカレートされたパーソナル CMR/ランデブー会議の復元性が確保されます。

復元性は、Cisco TMS でスケジュールされた会議ではサポートされません。Cisco TMS は複数の TelePresence Conductor をサポートしますが、これは復元性ではなく規模が対象です。Cisco TMS で設定された TelePresence Conductor がダウンした場合、管理者は TMS 内の別の TelePresence Conductor クラスタ メンバに手動でフェールオーバーする必要があります。

Conductor のクラスタリングの詳細については、『Cisco TelePresence Conductor Clustering with Cisco Unified Communications Manager Deployment Guide』を参照してください。

SIP Early Offer メッセージング

TelePresence コールを伝送するすべての Unified CM 接続 SIP トランクには、Early Offer メッセージングを使用することが強く推奨されます。また、Early Offer メッセージングは CMR Hybrid 会議と一部のサードパーティ サービスでは必須です。H.323 から SIP へのインターワーキング コールを除き、Cisco VCS を中心とした展開は常に Early Offer モードで実行されます。（H.323 は Cisco VCS と Cisco Expressway では Slow Start シグナリング モードを使用するため、インターワーキング コールの SIP メッセージングは Delayed Offer を使用して実行されます。）

ブリッジ プールとサービス設定

- TelePresence Conductor には 1 つ以上のサービス設定が必要です。必要に応じて、すべての会議ブリッジ プールを 1 つのサービス設定に配置できます。
- すべての会議ブリッジを TelePresence Conductor 内の 1 つの会議ブリッジ プールに割り当てる必要があります。各会議ブリッジは 1 つのプールにしか属することができません。
- TelePresence Conductor プール内のすべての会議ブリッジを同じタイプ（MCU または TelePresence Server）にする必要があります。これは任意であって必須ではありませんが、同じロケーションからのブリッジを使用してプールを構成することをお勧めします。
- プールと同様に、サービス設定内のすべての会議ブリッジを同じタイプ（MCU または TelePresence Server）にする必要があります。
- プール内のすべての会議ブリッジを同一の設定にする必要があります。
- 1 つのプール内のすべての会議ブリッジの容量を同一にすることを強く推奨します。そうすることで、会議ブリッジ間で会議を効率的に分散できます。1 つのプール内に容量が異なる会議ブリッジがあると、会議の配置バランスが悪くなることがあります。
- 帯域幅使用量を制御するために Unified CM コール アドミッション制御が実装されている場合は、それぞれのサービス設定に 1 か所のブリッジのプールだけを含める必要があります。
- スケジュール済み会議の場合は、プールとサービス設定に関して次の 2 つの設定方法が考えられます。

推奨される方法として、すべての会議タイプ間で共有されるリソース（スケジューリングなど）を TelePresence Conductor で管理できるようにします。これにより、リソースの使用率、ユーザ エクスペリエンス、および可用性の間で最適なトレードオフが実現します。ピーク時間の使用量が増加した場合は、ブリッジの追加を検討する必要があります。Cisco TMS の [容量調整（Capacity Adjustment）] 設定を使用して、オーバーサブスクリプションやアンダーサブスクリプションを調整できます（「タスク 8 : Cisco TMS でサービス設定を編集する（オプション）[p.39]」を参照してください）。

- または、スケジュールされていない会議によってリソースがすでに使い果たされたためにスケジュール済み会議に影響が出るような状況を避けるため、会議ブリッジをスケジュール済

み会議専用で使用することもできます。サービス設定ごとに1つのブリッジを使用し、Cisco TMS でそれをスケジューリング用に設定します。

詳細については、スケジュール済み会議の設定，（70 ページ）を参照してください。

- 1 つのプール内のすべての会議ブリッジの容量を同一にすることを強く推奨します。そうすることで、会議ブリッジ間で会議を効率的に分散できます。1 つのプール内に容量が異なる会議ブリッジがあると、会議の配置バランスが悪くなることがあります。
- Unified CM に接続するエンドポイントからダイヤルされたエイリアスが、Unified CM で予期されるロケーションのブリッジだけを使用することを確認してください。異なるロケーションのブリッジが指定および使用されている場合、Unified CM は誤ったロケーションにコールの帯域幅を割り当てます。予期されるロケーションに帯域幅が誤って割り当てられ、実際のロケーションに帯域幅が割り当てられなくなります。

コンテンツ チャネル

ほとんどの TelePresence エンドポイントでは、コンテンツ チャネルと呼ばれる 2 番目のビデオ チャネルを使用できます。通常、これはライブ ビデオと平行して実行されるプレゼンテーションに使用されます。

- MCU 会議ブリッジの場合、TelePresence Conductor の会議テンプレートの [コンテンツ モード（Content mode）] を [トランスコード（Transcoded）]（[拡張パラメータ（Advanced parameters）]）に設定します。TelePresence Conductor テンプレートでこのモードが選択されると、MCU モデルと設定に応じて、専用コンテンツ ポートまたはビデオ ポートが割り当てられます。
- TelePresence Server の会議ブリッジについては、現在コンテンツ モードは常に [トランスコード（Transcoded）] で、設定可能ではありません。

H.323 インターワーキング

CMR Hybrid ネットワークは SIP ベースです。CMR Hybrid ネットワーク内で H.323 エンドポイントを会議に接続するには、TelePresence Conductor に到達する前にコールをインターワーキングする必要があります。このためには、必要な SIP/H.323 インターワーキングを実行するように、Cisco VCS Control または Cisco Expressway-C を設定します。

- ローカルに登録されたエンドポイントに対してだけインターワーキングするには、[H.323 <-> SIP インターワーキングモード（H.323 <-> SIP interworking mode）] を [登録済みのみ（Registered only）] に設定します（[VCS 設定（VCS configuration）] > [プロトコル（Protocols）] > [Interworking（相互接続）] からアクセス）。
- オプションで外部ネットワークと会議の間で Business-to-Business H.323 コールのインターワーキングを許可するには、[H.323 <-> SIP インターワーキング モード（H.323 <-> SIP interworking

mode）] を [オン（On）] に設定します。これにより、すべての着信コールのインターワーキングが行われます。

Microsoft Lync 2013 の相互運用性

CMR Hybrid では、Cisco Expressway-C によるインターワーキングを使用した Microsoft Lync 2013 サービスとの相互運用性がサポートされます（Microsoft の相互運用性キーが必要です）。容量の点から、Lync へのアクセスと、その他のネットワーク要件に対し、それぞれ個別の Cisco Expressway-C デバイスを使用することを推奨します。

プレゼンテーション共有に推奨される画面解像度

プレゼンテーション中に全画面ビューを使用するには、コンピュータを4：3の縦横比の画面解像度に設定することを推奨します。推奨される画面解像度は次のとおりです。

- 1024 X 768
- 1152 X 864
- 1280 X 1024
- 1600 X 1200

WebExクライアントのビデオに影響するネットワークとクライアントの制限

- PC または Mac の WebEx は、PC のビットレートが 500 Kbps 未満の場合、または PC で開いているアプリケーションが多すぎるために、ビデオ パケットの送受信に使用できる十分な PC CPU またはメモリがない場合は、ビデオを受信できません。
- PC または Mac の WebEx クライアントは、UDP が使用できる場合は UDP を使用し、UDP がブロックされている場合は TCP を使用して WebEx データセンターに接続します。最適なビデオ パフォーマンスを得るには UDP が必要です。顧客は各自のセキュリティ チームに確認し、可能な場合はビデオ用に UDP ポートを使用できるようにしてください。多くの場合、特に最適化されていない WiFi ネットワークを使用する場合は、TCP を使用するとビデオが表示されません。
- インターネット プロキシを使用している顧客は、UDP を使用するとビデオ容量が制限されるため、ほとんどの場合 UDP を使用できません。

（注） WebEx PC クライアント内で [会議、音声、およびビデオの統計（Meeting, Voice and Video Stats）] を選択すると、使用中のビット レートと、UDP または TCP ポートのどちらが使用されているかどうかを確認でき、ビデオが失われた場合のトラブルシューティングに役立ちます。

第 5 章

ソリューション コンポーネントをセットアップする

会議ブリッジ、TelePresence Conductor、および Unified Communications Manager の設定

はじめる前に

- 『Cisco TelePresence Conductor Getting Started』または『Cisco TelePresence Conductor Virtual Machine Installation Guide』の手順に従って、Cisco TelePresence Conductor をインストールしておく必要があります。
- Cisco Unified Communications Manager は、基本構成でインストールおよび設定する必要があります。3 つ以上のエンドポイントを登録して接続を確立し、これらのエンドポイントが音声およびビデオ通信で相互にコールできることを確認します。
- 1 つ以上の会議ブリッジの電源をオンにし、Cisco TelePresence Conductor へ HTTP/HTTPS および SIP TLS 経由でアクセスできるようにしておく必要があります。すべての場合に HTTP が推奨されます。また、Multiparty ライセンスが機能するには HTTP が必須です。

手順

	コマンドまたはアクション	目的
ステップ 1	『Cisco TelePresence Conductor with Unified CM Deployment Guide (XC4.0)』の次のタスクを完了します。 • Cisco TelePresence MCU シリーズの設定（該当する場合）。 • TelePresence Server の設定。 • TelePresence Conductor の一般設定。 • Unified CM の一般設定。	CMR Hybrid では、TelePresence Conductor は B2BUA を使用して展開されます。外部ポリシー サービス インターフェイスはサポートされていません。
ステップ 2	個人用 CMR を有効化する, （53 ページ）	これはオプションです。スケジュール済み会議で PMP ライセンスを使用する場合は、ライセンス グループごとにパーソナル CMR を有効にする必要があります。Cisco TMS がスケジュール済み会議を作成すると、TelePresence Conductor はパーソナル CMR のリストを検索します。ユーザに対して PMP ライセンスが定義されたパーソナル CMR がある場合は、PMP ライセンスが使用されます。一致するユーザが存在しない場合は、SMP ライセンスが使用されます。
ステップ 3	Multiparty ライセンスの管理, （58 ページ）	シスコは Multiparty ライセンスを有効にすることをお勧めします。TelePresence Server 会議ブリッジがあり、Multiparty ライセンスを使用している場合、この手順を使用します。この場合は、ブリッジにスクリーン ライセンスをロードする代わりに、Cisco TelePresence Conductor 上でライセンスを一元管理します。
ステップ 4	スケジュール済み会議を有効にします。詳細については、TelePresence Conductor と Cisco TMS でのスケジューリングの有効化, （75 ページ）を参照してください。	

個人用 CMR を有効化する

パーソナル Collaboration Meeting Rooms（CMR）の主な機能は、ユーザが会議を開催して他のユーザと共同作業するための仮想ルームを提供することです。管理者は、Cisco TMSPE を使用して、TelePresence Conductor 上にユーザ グループ用のパーソナル CMR をプロビジョニングします。その後ユーザは、ユーザ ポータルから各自の CMR をアクティブにしてカスタマイズできます。

Multiparty ライセンスでのパーソナル CMR の役割

Multiparty ライセンスを使用する場合、パーソナル CMR には 2 次的な機能があります。Personal Multiparty（PMP）ライセンスと Shared Multiparty（SMP）ライセンスが混在する展開環境では、管理者が特定のユーザ グループ内の各ユーザに PMP または SMP ライセンスを割り当てる必要があるかどうかを定義するためのメカニズムが提供されます。このメカニズムは、スケジュール済み会議を含むすべての会議タイプに使用されます。

- ユーザがパーソナル CMR を持っていない場合、ユーザは自分が開始するすべてのスケジュール済み会議で SMP ライセンスを消費します。
- ユーザがパーソナル CMR を持っていて、CMR テンプレートの [Multiparty ライセンスモード（Multiparty Licensing Mode）] の値がデフォルト（[Personal Multiparty]）のままの場合、ユーザは PMP ライセンスを消費します。ユーザの PMP ライセンスは、そのユーザが開始するすべてのスケジュール済み会議または CMR 会議で使用されます。
- ユーザがパーソナル CMR を持っていて、[Multiparty ライセンスモード（Multiparty Licensing Mode）] の値が [Shared Multiparty] に変更された場合、ユーザは自分の会議の SMP ライセンスを消費します。

ユーザが自分の会議の SMP ライセンスを消費しないようにする必要があり、ユーザがまだパーソナル CMR を持っていない場合は、デフォルトのライセンス モード（[Personal Multiparty]）でパーソナル CMR をプロビジョニングする必要があります。ユーザがパーソナル CMR を持っていない場合は、以前にデフォルトのライセンス モードを変更していないかぎり、何もする必要はありません。

要約	
ユーザがパーソナル CMR を持っているか	**ユーザが消費するライセンス タイプ**
なし	SMP
はい（PMP モード）	PMP
はい（SMP モード）	SMP

マルチパーティ ランセンスの管理者タスクに関する詳細については、Multiparty ライセンスの管理, （58 ページ）を参照してください。

パーソナル CMR テンプレートと Conductor 会議テンプレート

CMR テンプレートは、TelePresence Conductor 上の会議テンプレートと会議エイリアスに対応します。Cisco TMSPE を使用して作成された CMR は、TelePresence Conductor Web ユーザ インターフェイスから変更できません。TelePresence Conductor を使用して作成された会議テンプレートおよびエイリアスは、Cisco TMSPE 経由で変更できません。

パーソナル CMR タスク フローの有効化

はじめる前に

- TelePresence Conductor は、1 つ以上のブリッジ プールとサービス設定を生成する必要があります。
- Cisco TMSPE は Cisco TMS でインストールして有効にする必要があります。
- Cisco TMSPE には、Cisco TMS の [システム（Systems）]>[プロビジョニング（Provisioning）] メニューからアクセスします。
- Cisco TMSPE 用のユーザ ベースが存在する必要があります。ユーザ ベースの設定方法については、『Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM Deployment Guide』の「*Creating groups and adding users*」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	API アクセス権を持つ TelePresence Conductor ユーザの作成, （55 ページ）	各 TelePresence Conductor またはクラスタでパーソナル CMR の API 対応ユーザ アカウントを作成します。
ステップ 2	TelePresence Conductor API ユーザの Cisco TMSPE への追加, （56 ページ）	
ステップ 3	パーソナル CMR の WebEx の有効化, （56 ページ）	これはオプションです。
ステップ 4	CMR テンプレートの作成, （57 ページ）	1 つまたは複数の CMR テンプレートを作成し、CMR URI と数値エイリアスの基本的なダイヤル プランを指定する必要があります。

	コマンドまたはアクション	目的
ステップ 5	グループへの CMR テンプレートの適用，（57 ページ）	Active Directory ユーザ グループにテンプレートを適用します。
ステップ 6	個人用 CMR のモニタリングの有効化，（58 ページ）	これはオプションです。モニタリングを有効にする場合は、TelePresence Conductor を Cisco TMS に追加します。TelePresence Conductor がすでに Cisco TMSPE に追加されている場合でも、この手順を実行する必要があります。
ステップ 7	CMR の同期，（58 ページ）	Active Directory ユーザは Cisco TMS と定期的に同期されます。同期後、CMR の詳細に関する電子メールが TMS から対象ユーザに送信され、ユーザはその CMR をアクティブ化することができます。
ステップ 8	ユーザが CMR をアクティブ化します。	ユーザが CMR をアクティブ化すると、TelePresence Conductor で CMR が作成されます。パーソナル CMR が作成されると、Cisco TMSPE によって、ユーザのグループに関連付けられている CMR テンプレートの設定が適用され、TelePresence Conductor でルームが作成されて、電子メールがユーザに送信されます。これ以上、管理者が実行する必要のある操作はありません。

次の作業

次の会議の方法を使用できるようになりました。

- PMP または SMP ライセンスを使用したスケジュール済み会議
- パーソナル CMR

API アクセス権を持つ TelePresence Conductor ユーザの作成

手順

TelePresence Conductor で、[ユーザ（Users）] > [管理者アカウント（Administrator accounts）] に移動して、次の属性を持つユーザを作成します。

- アクセス レベル：読み取り/書き込み
- Web アクセス：いいえ
- API アクセス：はい

- 状態：有効

TelePresence Conductor API ユーザの Cisco TMSPE への追加

手順

ステップ 1 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動します。

ステップ 2 [TelePresence Conductorの設定（TelePresence Conductor Settings）] をクリックします。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 TelePresence Conductor の設定のダイアログで、TelePresence Conductor の詳細とユーザ クレデンシャルを追加します。[ホスト名/IP（Hostname/IP）]：TelePresence Conductor のホスト名または IP アドレス。

- [ポート（Port）]：接続するためのポート（デフォルトはポート 443 上の HTTPS です）。
- [ユーザ名/パスワード（Username / Password）]：前のステップで作成した Conductor ユーザのクレデンシャル。
- [ドメイン（Domain）]：TelePresence Conductor は、Cisco TMSPE で作成されたすべての数値エイリアスにこのドメインを付加します。
- [保存（Save）] をクリックします。

パーソナル CMR の WebEx の有効化

CMR Hybrid がすでに導入されている場合は、必要に応じてパーソナル CMR で CMR Hybrid を有効にして、Cisco WebEx ユーザと TelePresence ユーザによる共同参加を許可できます。これが初めての CMR Hybrid 展開である場合は、後で別のタスクとしてこの設定を行い（「パーソナル CMR での CMR Hybrid の使用」を参照）、その時点で CMR を再生成できます。または、CMR を定義する前にここでこの設定を行うこともできます。

手順

ステップ 1 Cisco TMS で、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [プロビジョニング拡張機能の設定（Provisioning Extension Settings）] に移動します。

ステップ 2 Collaboration Meeting Room で、[WebEx接続を許可する（Allow WebEx Connections）] を [はい（Yes）] に設定します。

ステップ 3 [保存（Save）] をクリックします。

ここでこの設定を行う場合は、次の手順で CMR のテンプレートを作成するときに必ず [WebExを含める（Include WebEx）] をオンにしてください。

CMR テンプレートの作成

手順

ステップ 1 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動（して、Cisco TMSPE にアクセス）します。

ステップ 2 [Collaboration Meeting Room テンプレート（Collaboration Meeting Room Templates）] で、必要に応じて 1 つ以上のテンプレートを作成します。

- この CMR テンプレートが PMP ライセンスを持つユーザ用である場合は、CMR テンプレートの [Multiparty ライセンスモード（Multiparty License Mode）] を [Personal Multiparty] に設定します。
- [SIP エイリアス パターン（SIP Alias Pattern）] は、ユーザが CMR に接続するためにダイヤルする URI パターンを指定します。[数値 エイリアス パターン（Numeric Alias Pattern）] は、オプションで追加する数字ダイヤルを指定します。これは、番号範囲または正規表現パターン（Active Directory の [会社電話（Office Phone）] または [携帯電話（Mobile Phone）]）に基づいて指定できます。
- CMR Hybrid を使用しており、WebEx ユーザが会議室にアクセスできるようにする場合は、[WebEx を含める（Include WebEx）] をオンにします。

グループへの CMR テンプレートの適用

手順

ステップ 1 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動します。

ステップ 2 関連するグループを選択して、[アクティブ（Active）]列で必要なテンプレート用のボタンを選択します。

個人用 CMR のモニタリングの有効化

これはオプションです。モニタリングを有効にするには、TelePresence Conductor が Cisco TMSPE に追加されていても、この手順を完了する必要があります。

手順

TelePresence Conductor を Cisco TMS に追加します。Cisco TMS の状況依存ヘルプまたは『Cisco TelePresence Management Suite Administrator Guide』を参照し（http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html）、「Adding systems」を検索してください。

CMR の同期

Cisco TMSPE は、すべてのパーソナル CMR を 1 日に 1 回自動的に同期します。同期が発生するまで待つか、（パーソナル CMR または PMP ライセンスを使用する場合は）手動で CMR を同期できます。

手順

ステップ 1 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動します。

ステップ 2 [Collaboration Meeting Roomテンプレート（Collaboration Meeting Room Templates）] で、[TelePresence Conductor の設定（TelePresence Conductor Settings）] をクリックします。

ステップ 3 開いたダイアログ ウィンドウで、関連する TelePresence Conductor を見つけ、そのアイコンをクリックします。このアイコンは右側にあります（[TelePresence Conductor Multiparty ライセンス（TelePresence Conductor Multiparty Licensing）] というツールチップが表示されます）。

ステップ 4 開いたダイアログ ウィンドウで、[今すぐ同期（Synchronize Now）] をクリックします。
同期が完了すると、Cisco TMS は影響を受けるユーザに各自のパーソナル CMR が使用可能になったことを電子メールで通知します。これで、ユーザは Cisco TMSPE ユーザ ポータルから各自の CMR をアクティブにしてカスタマイズできます。ユーザが各自の CMR をアクティブにすると、TelePresence Conductor でその CMR が作成されます。

Multiparty ライセンスの管理

TelePresence Server 会議ブリッジがあり、Multiparty ランセンスを使用している場合、この項の手順を使用します。この場合は、ブリッジにスクリーン ライセンスをロードする代わりに、Cisco TelePresence Conductor 上でライセンスを一元管理します。

手順

	コマンドまたはアクション	目的
ステップ 1	Multiparty ライセンスの有効化, （59 ページ）	シスコは Multiparty ライセンスを有効にすることをお勧めします。
ステップ 2	ユーザへのライセンスの適用, （60 ページ）	Shared Multiparty（SMP）ライセンスと Personal Multiparty（PMP）ライセンスが混在する場合は、特定のユーザ グループ内の各ユーザに PMP または SMP ライセンスを割り当てる必要があるかどうかを定義できます。特定のユーザ グループに対してどのライセンス タイプが使用されているかを確認するには、次の手順を実行します。
ステップ 3	ライセンス モードの変更, （61 ページ）	特定のユーザ グループのライセンス モードを変更するには、次の手順を実行します。
ステップ 4	ライセンスの手動同期, （61 ページ）	自動同期を待たずに PMP ライセンスをすぐに使用する場合は、次の手順を使用します。
ステップ 5	ライセンスの使用状況のモニタ, （62 ページ）	インストールされているライセンスの数、ユーザに割り当てられた PMP ライセンスの数、および最近 60 日間の SMP ライセンスのピーク時使用状況を確認するには、次の手順を実行します。

Multiparty ライセンスの有効化

シスコは Multiparty ライセンスを有効にすることをお勧めします。

手順

ステップ 1 TelePresence Conductor にログインします。

ステップ 2 TelePresence Conductor にアクティブなコールがないことを確認します。Multiparty ライセンスを有効にすると、現在アクティブなコールが終了します。

ステップ 3 [メンテナンス（Maintenance）] > [オプション キー（Option keys）] に移動します。

ステップ 4 [ソフトウェアオプション（Software option）] の [オプションキーの追加（Add option key）] フィールドに、購入した Personal Multiparty（PMP）または Shared Multiparty（SMP）ライセンスのオプション キーを入力します。

ステップ 5 [オプションの追加（Add option）] をクリックします。

ステップ 6 購入した他の PMP および SMP ライセンス キーについて、この手順を繰り返します。ライセンス キーは追加式になっているため、たとえば、100 個の Personal Multiparty ライセンス用のオプション キーを 2 つ追加した場合は、200 個の Personal Multiparty ライセンスを使用できます。

ステップ 7 同じページで、[Multiparty ライセンス（Multiparty Licensing）] の [TelePresence Server の Multiparty ライセンス（Multiparty licensing for TelePresence Servers）] を [有効（Enabled）] に設定します。

ユーザへのライセンスの適用

Shared Multiparty（SMP）ライセンスと Personal Multiparty（PMP）ライセンスが混在する場合は、特定のユーザ グループ内の各ユーザに PMP または SMP ライセンスを割り当てる必要があるかどうかを定義できます。ユーザにパーソナル CMR がプロビジョニングされていて、そのパーソナル CMR が Personal Multiparty（PMP）ライセンス モード（デフォルト）に指定されている場合を除き、ユーザは自分の会議の Shared Multiparty（SMP）ライセンスを消費します。この指定は、パーソナル CMR を設定するときに行う必要があります。個人用 CMR を有効化する，（53 ページ）を参照してください。

特定のユーザ グループに対してどのライセンス タイプが使用されているかを確認するには、次の手順を実行します。

手順

ステップ 1 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] > [Collaboration Meeting Room テンプレート（Collaboration Meeting Room Templates）] に移動します。

ステップ 2 該当するテンプレートを選択します。

ステップ 3 [Multiparty ライセンスモード（Multiparty License Mode）] ドロップダウンで、このテンプレートが割り当てられたユーザ グループに対してどのライセンス タイプが使用されているかを確認します。

ライセンス モードの変更

注意 このプロセスは、ライセンス モードの変更に関連しています。テンプレートに対するその他の変更は、混乱を招く可能性があるため、事前の計画が必要です。詳細については、http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/solutions/cmrpremises/cmr-premises-deployment-guide-r5-0.pdfの「Managing Administration Changes to personal CMRs」を参照してください。

特定のユーザ グループのライセンス モードを変更するには、次の手順を実行します。

手順

ステップ 1 変更をサポートするのに十分な数の PMP ライセンスまたは SMP ライセンス（必要に応じて）が使用できることを確認します。

ステップ 2 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] > [Collaboration Meeting Room テンプレート（Collaboration Meeting Room Templates）] に移動します。

ステップ 3 該当するテンプレートを選択します。

ステップ 4 必要に応じて、[Multiparty ライセンスモード（Multiparty License Mode）] ドロップダウンを設定します。PMP ライセンスをユーザに適用するには、[Personal Multiparty] を選択します。

ステップ 5 [保存（Save）] をクリックします。

ステップ 6 [同期ステータスの確認（Check sync status）] の横にあるカウンタは、変更されたテンプレートと同期していない CMR の数を示しています。TelePresence Conductor 上の変更を同期させる場合は [CMRの再生成（Regenerate CMRs）] をクリックします。

ライセンスの手動同期

Personal Multiparty（PMP）ライセンスは、Cisco TMSPE による関連するパーソナル CMR の日次同期によって自動的に同期されます。自動同期を待たずに PMP ライセンスをすぐに使用する場合は、次のようにして手動で同期できます。

はじめる前に

同期は、メンテナンス ウィンドウ中に行うか、少なくともピーク時間を避けて行うことを推奨します。

手順

ステップ 1 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動します。

ステップ 2 [Collaboration Meeting Room テンプレート（Collaboration Meeting Room Templates）] で、[TelePresence Conductor の設定（TelePresence Conductor Settings）] をクリックします。

ステップ 3 関連する TelePresence Conductor を見つけ、そのアイコンをクリックします。このアイコンは右側にあります（[TelePresence Conductor Multipartyライセンス（TelePresence Conductor Multiparty Licensing）] というツールチップが表示されます）。

ステップ 4 [今すぐ同期（Synchronize Now）] をクリックします。

ライセンスの使用状況のモニタ

インストールされているライセンスの数、ユーザに割り当てられたPMPライセンスの数、および最近 60 日間の SMP ライセンスのピーク時使用状況を確認できます。

手順

TelePresence Conductor で、[ステータス（Status）] > [Multiparty ライセンス（Multiparty licenses）] に移動します。

第 6 章

コール コントロールへ Cisco TelePresence Conductor を接続する

TelePresence Conductor の Cisco Unified Communications Manager への接続

ここでは、Unified Communications Manager を中心とした展開で CMR ハイブリッド の TelePresence Conductor を設定するのに完了する必要がある手順の概要を示します。詳細な手順については、『Cisco TelePresence Conductor with Unified CM Deployment Guide (XC3.0)』を参照してください。

（注） CMR ハイブリッド では、TelePresence Conductor は B2BUA を使用して導入されます。外部ポリシー サービス インターフェイスはサポートされていません。

はじめる前に

- 『Cisco TelePresence Conductor Virtual Machine Installation Guide』の手順に従って、Cisco TelePresence Conductor をインストールしておく必要があります。
- Cisco Unified Communications Manager は、基本構成でインストールおよび設定する必要があります。3 つ以上のエンドポイントを登録して接続を確立し、これらのエンドポイントが音声およびビデオ通信で相互にコールできることを確認します。
- 1 つ以上の会議ブリッジの電源をオンにし、Cisco TelePresence Conductor へ HTTP/HTTPS および SIP TLS 経由でアクセスできるようにしておく必要があります。すべての場合に HTTP が推奨されます。また、Multiparty ライセンスが機能するには HTTP が必須です。

手順

TelePresence 管理インターフェイスを使用して、次の作業を実行します。

- Cisco MCU TelePresence シリーズの設定。
- TelePresence Server の設定。
- TelePresence Conductor の一般設定と、アドホック会議およびランデブー会議向けの設定
- Unified CM の一般設定と、アドホック会議およびランデブー会議向けの設定

Cisco VCS への TelePresence Conductor の接続

ここでは、Cisco VCS を中心とした展開で CMR ハイブリッド の TelePresence Conductor を設定するのに完了する必要がある手順の概要を示します。手順の詳細については、『Cisco TelePresence Conductor with Cisco VCS (B2BUA) Deployment Guide (XC3.0)』を参照してください。

はじめる前に

- 『Cisco TelePresence Conductor Getting Started』または『Cisco TelePresence Conductor Virtual Machine Installation Guide』の手順に従って、Cisco TelePresence Conductor をインストールしておく必要があります。
- Cisco TelePresence Video Communication Server をインストールし、SIP レジストラおよびプロキシとして機能するように設定する必要があります。
- 1 つ以上の会議ブリッジの電源をオンにし、Cisco TelePresence Conductor へ HTTP/HTTPS および SIP TLS 経由でアクセスできるようにしておく必要があります。
- Cisco VCS Control と TelePresence Conductor 間のトランクの VCS [ゾーンプロファイル（Zone profile）] を [カスタム（Custom）] に設定し、[SIP 検索に対する自動応答（Automatically respond to SIP searches）] を [オン（On）] に設定する必要があります。詳細については、『*Cisco TelePresence Conductor with Cisco TelePresence VCS（B2BUA）Deployment Guide XC3.0*』の「Adding the TelePresence Conductor as a neighbor zone」を参照してください。

手順

TelePresence 管理インターフェイスを使用して、次の作業を実行します。

- ダイヤル プランの設計。
- Cisco MCU TelePresence シリーズの設定。
- TelePresence Server の設定。
- TelePresence Conductor のネイバー ゾーンと検索ルールを使用した Cisco VCS の設定。

- B2BUA モードでの TelePresence Conductor の設定（Cisco VCS 外部ポリシー サービスを使用した展開はサポートされていません）

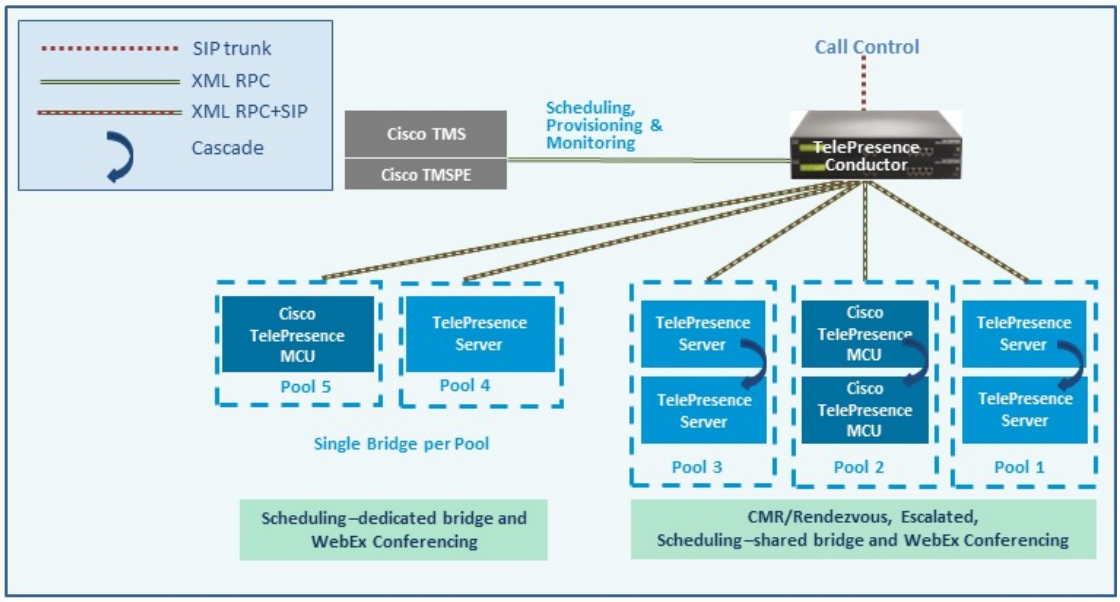
第 7 章

ブリッジ スケジュールを設定する

CMR Hybrid でのブリッジのスケジュール方法

CMR ハイブリッド では次の 2 つの方法でブリッジをスケジュールできます。

- スケジューリング：専用ブリッジ。スケジュール済み会議専用のブリッジを 1 つ以上展開します。各ブリッジはそれぞれの専用プール内にあります。オプションで、2番目の専用ブリッジとプールの組み合わせをバックアップとして使用することもできます。
- スケジューリング：共有ブリッジ。スケジュール済み会議およびスケジュールされない会議にブリッジを使用できます。この場合、必要となるリソースがスケジュールされない会議によってすでに使用されることがあるため、スケジュール済み会議のリソースの可用性は保証できません。



設定シナリオの例と、それぞれの長所と短所については、『Cisco Collaboration Meeting Rooms (CMR) Premises Solution Guide』を参照してください。

下記に記載されている制限と前提条件がこのリリースのスケジュール済み会議に適用されます。

- 制限事項, （68 ページ）
- 要件, （69 ページ）

制限事項

（注） クラスタ化 TelePresence Conductor を使用する場合は、Cisco TMS は 1 つの TelePresence Conductor ノードだけを認識する点に注意してください。そのクラスタ ノードで障害が発生すると、Cisco TMS スケジューリング サービスと CMR プロビジョニング サービスは（TelePresence Conductor が再び稼働状態になるか、または Cisco TMS が更新されクラスタ内の別の TelePresence Conductor と通信できる状態になるまで）停止状態になります。

Cisco TMSPE によりプロビジョニングされた CMR をスケジュールすることはできません。

以前のスケジュール済み会議と同じブリッジを使用するように設定されている TSP が提供する TSP 音声を使用する場合は、Cisco TMS の自動拡張機能をオフにしておくことを推奨します。

TelePresence Conductor と Cisco TMS を使用したスケジューリング ソリューションには、現時点では顕著な制限があり、リリース 3.0 での以前の手法（直接管理ブリッジのスケジュール）と大きく異なる点があります。スケジューリングを有効にする前に、次のマニュアルを確認することを強く推奨します。

- 以前のソリューションでの直接管理ブリッジのスケジューリング方式（旧リリース）と、TelePresence Conductor によって管理されるブリッジのスケジューリング方式（現リリース）の相違点をまとめた表が、『Cisco TelePresence Conductor with Cisco TelePresence Management Suite Deployment Guide』に記載されています。
- Cisco TMS の最新のリリース ノートの「Limitations」の項。
- TelePresence Conductor の最新のリリース ノートの「Limitations」の項。

要件

- CMR ハイブリッドでは、スケジューリングのために Cisco TMS 管理ツールが必要です。TelePresence Conductor で会議が直接スケジュールされることはありません。
- CMR ハイブリッドのソリューション レベルの前提条件が満たされており、設定プロセスが完了していることを確認します。特に、次の点に注意してください。
- スケジューリング専用ブリッジケースでは、いくつかの追加の設定要件が適用されます（下記参照）。
- スケジュール済み会議の参加者は、アドホック/インスタント会議にエスカレートしないようにする必要があります。その場合は、参加者が会議の品質が低下したと感じることになります。

専用ブリッジ スケジューリングに関する要件

スケジューリングに専用会議ブリッジを使用する場合は、次のポイントが適用されます。

- ブリッジ リソースが会議にしか使用されません（正しい設定に依存します）。Cisco TMS への Capacity API 応答では、TelePresence Conductor はサービス設定（[スケジューリングに使用するプール（Pools to use for scheduling）] オプション）でスケジューリング用として「マーク」されているプールだけを返します。
- 回復力を高めるために、1 つ以上の追加のブリッジ/プールを、スケジューリングに使用されるサービス設定に含めることができます。これらのプールはスケジューリング用としてマークされず（そのため、Cisco TMS に報告されない）、プライマリ ブリッジが使用できなくなった場合にのみ追加のブリッジが使用されます。
- リソースの浪費を避けるために、カスケードを無効にすることをお勧めします。カスケードが物理的に実行できない場合でも、カスケードが有効になっていると、リソースが予約されます。
- TelePresence Server リソースの最適化が実施されますが、プライマリ会議ブリッジの使用中はそのメリットが得られません。Cisco TMS は事前にブリッジ使用量を計画するため、最適化によって回復されたリソースは実際には再利用されません。未スケジュール会議とリソースが共有されるバックアップブリッジを使用している場合は、最適化によって共有バックアップ ブリッジに必要な容量が削減されます。

スケジュール専用の会議ブリッジ プールを設定する場合は、次の事項が推奨されます。

- 会議ブリッジ プールに、スケジュール済み会議専用であることを示す名前を付けます。
- プールが単一のサービス設定にだけ使用されることを確認します。
- サービス設定が CMR またはアドホック会議に使用されないことを確認します。

スケジュール済み会議の設定

このソリューションでスケジュール済み会議をサポートするため、さまざまな設定が可能です。これらは、TelePresence Conductor のブリッジ プールと [サービス設定（Service Preference）] の設定値によって制御します。

共有ブリッジ

通常は、この共有ブリッジのアプローチを使用してください。これにより、スケジュール済み会議に加えて他のタイプの会議も会議ブリッジで実行できるようになります。

表 *16*：スケジューリング用の共有ブリッジの展開

	サービス設定の内容	設定（**Configuration**）	利点	欠点
例 1	スケジュール済み会議とスケジュールされない会議のための共用ブリッジ	スケジュール済み会議とスケジュールされない会議で共有される 1 つ以上のプール。 すべてのプールは TelePresence Conductor サービス設定でスケジューリング用としてマークされ、Cisco TMS に報告されます。	会議のカスケードが可能（有効にされている場合）。 対象を絞ったブリッジリソース管理。時間をかけて使用パターンのモニタリングを行うことによって、最適なプール設定を識別できます。	スケジュール済み会議に対してリソースが使用可能であることは保証されません（スケジュールされない会議によりリソースがすべて使用される可能性があります）。このリスクは、Cisco TMS の [容量調整（Capacity Adjustment）] 設定を使用して容量を少なく（100% 未満に）割り当てることによって減らすことができます。実際の容量ではなく、この設定によって減少したパーセンテージだけが TMS で会議をスケジュールするときに使用できるようになります。

代替オプション（専用ブリッジ）

次の表に、スケジュール済み会議専用のブリッジを予約する場合の、可能なアプローチの例とそれらの利点および欠点を示します。

表 *17*：スケジューリング用の専用ブリッジの展開

	サービス設定の内容	設定（**Configuration**）	利点	欠点
例 2	スケジュール済み会議の専用ブリッジ。	1 つの会議ブリッジが含まれている 1 つのプール。 プールは TelePresence Conductor サービス設定でスケジュールに使用されるとマークが付けられます。プールは、容量情報要求で Cisco TMS にレポートされます。	会議が利用可能であることが保証されます（ただしブリッジでの障害（または容量がいっぱいになること）が発生する場合はその限りではありません）。 Cisco TMS はブリッジがいっぱいになるまでポートを予約するため、リソースを最大限に使用できます。	スケジューリング専用に 1 つの会議ブリッジが使用されます。 会議のカスケードは発生しません。リソースを無駄に使用しないように、カスケードを無効にする必要があります。
例 3	• スケジュール済み会議の専用ブリッジ • 専用バックアップ ブリッジ	2 つのプール。 両方のプールに 1 つの会議ブリッジが含まれます。優先度が最も高いプールのブリッジで障害が発生すると、2 番目のプールがバックアップとして使用されます。 1 番目のプールだけが TelePresence Conductor サービス設定でスケジューリング用としてマークされ、Cisco TMS に報告されます。	例 2 と同様、ブリッジで障害が発生した場合のフォールバックのメリットがあります。	スケジューリング専用に 2 つの会議ブリッジを使用します。 バックアップ リソースを消費します。 リソースを無駄に使用しないように、カスケードを無効にする必要があります。

	サービス設定の内容	設定（Configuration）	利点	欠点
例 4	• スケジュール済み会議の専用ブリッジ • スケジュール済み会議とスケジュールされない会議の両方のための共用バックアップ ブリッジ。	2 つ以上のプール。 優先度が最も高いプールに、スケジュール済み会議に使用される 1 つのブリッジのみが含まれています。 その他のプールには、スケジュール済み会議とスケジュールされない会議の両方に使用されるブリッジ（スケジュール済み会議にはバックアップとして使用される）が含まれています。 1 番目のプールだけが TelePresence Conductor サービス設定でスケジューリング用としてマークされ、Cisco TMS に報告されます。	例 2 と同様、ブリッジでの障害発生時に他のプールに予備の容量があれば、フォールバックのメリットが得られる可能性があります。	スケジューリング専用に 1 つの会議ブリッジが使用されます。 専用ブリッジでリソースを無駄に使用しないように、カスケードを無効にする必要があります。

	サービス設定の内容	設定（Configuration）	利点	欠点
例 5	• スケジュール済み会議の専用ブリッジ • スケジュール済み会議とスケジュールされない会議の両方のための共用バックアップ ブリッジ。	2 つ以上のプール。 優先度が最も高いプールに、スケジュール済み会議に使用される 2 つ以上のブリッジが含まれています。関連付けられている会議テンプレートでカスケードが有効に設定されます。 その他のプールには、スケジュール済み会議とスケジュールされない会議の両方に使用されるブリッジ（スケジュール済み会議にはバックアップおよびオーバーフロー用として使用される）が含まれています。 1 番目のプールだけが TelePresence Conductor サービス設定でスケジューリング用としてマークされ、Cisco TMS に報告されます。	例 2 と同様、ブリッジでの障害発生時にフォールバックのメリットが得られる可能性があり、スケジュール済み会議でカスケードを使用している場合はリソースオーバーフローが発生します。 次の状況では、バックアッププールのブリッジがスケジューリングに使用されます。 • プール 1 ブリッジで障害が発生した。 • プール 1 のカスケードで、Cisco TMS がスケジュール用であると認識しているブリッジ リソースすべてが使用された。	スケジューリング専用の会議ブリッジを使用します。 スケジュール済み会議がカスケードされている場合、これらの会議では共用プールのリソースが必要となることがあります。

TelePresence Conductor と Cisco TMS でのスケジューリングの有効化

はじめる前に

- 制限事項, （68 ページ）と要件, （69 ページ）のタスクが完了していることを確認します。
- ブリッジ プールとサービス設定, （47 ページ）で「ブリッジ プールとサービス設定」のベスト プラクティスのガイドラインを確認します。

手順

ステップ 1 **TelePresence Conductor を Cisco TMS に追加する**：
まだ行っていない場合、スケジューリングに使用する予定の TelePresence Conductor を Cisco TMS 内のシステムとして追加し、それぞれのシステムと該当するゾーンを関連付けます。Cisco TMS のヘルプまたは次の Cisco.com の URL で『Cisco TMS Administrator Guide』を参照（「Adding Systems」を検索）してください。
http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html

（注） クラスタ化された TelePresence Conductor を使用している場合は、Cisco TMS に対してクラスタあたり 1 つずつのノードを定義します。

ステップ 2 **Cisco TMS での TelePresence Conductor の IP ゾーンの定義**：
まだ行っていない場合、Cisco TMS で、[管理ツール（Administrative Tools）] > [ロケーション（Locations）] > [IP ゾーン（IP Zones）]に移動して、TelePresence Conductor ごとまたは TelePresence Conductor クラスタごとに 1 つずつの IP ゾーンを定義します。

ステップ 3 **TelePresence Conductor での会議ブリッジ リソースの設定**：
TelePresence Conductor で、スケジュール済み会議に使用する会議ブリッジの 1 つ以上の会議ブリッジ プールとサービス設定を設定します。
プールとサービス設定には、同じ物理ロケーション内のブリッジだけが含まれている必要があります。

組織の要件に応じてさまざまな設定が可能です。具体的には、スケジュール済み会議専用のリソースを割り当てる必要があるかどうかや未スケジュール会議とのリソースの共有を許可するかどうかなどがあります。後者のケースでは、未スケジュール会議ですでに使用可能なリソースが使い果たされている場合は、スケジュール済み会議を開始できない可能性があります。

設定例については、Cisco.com（http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/solutions/cmrpremises/cmr-premises-solution-guide-r5-0.pdf）で『Cisco Collaboration Meeting Rooms (CMR) Premises 5.0 Solution Guide』を参照してください。

オプションで「スケジューリング：専用ブリッジ」ケースを導入するには、該当する会議ブリッジ プールをスケジューリング用として「マーク」する必要があります。これは、TelePresence Conductor の [サービス設定（Service Preference）] ページで行います。

（注） スケジュール専用の会議ブリッジ プールを設定する場合は、次の事項が推奨されます。

- 会議ブリッジ プールに、スケジュール済み会議専用であることを示す名前を付けます。
- プールが単一のサービス設定にだけ使用されることを確認します
- サービス設定が CMR またはアドホック会議に使用されないことを確認します。

ステップ 4 **TelePresence Conductor の場所の割り当て**：
以前のタスクで定義した会議ブリッジ プールごとに適切なロケーションを割り当てます。スケジュール済み会議には専用ロケーションが必要ありません。ランデブー会議に割り当てられたものと同じロケーションを使用します。

ステップ 5 **TelePresence Conductor での会議テンプレートの設定**：
適切な会議テンプレートが TelePresence Conductor 内に存在しない場合は、スケジュール済み会議の要件を反映した 1 つ以上のテンプレートを定義します。
TelePresence Conductor で、[会議設定（Conference configuration）] > [会議テンプレート（Conference templates）] に移動します。[スケジュール済み会議（Scheduled conference）] を [はい（Yes）] に設定します。

ステップ 6 **TelePresence Conductor での会議エイリアスの設定**：
スケジュール済み会議の要件を反映した 1 つ以上の TelePresence Conductor エイリアスを定義します。
TelePresence Conductor で、[会議設定（Conference configuration）] > [会議エイリアス（Conference aliases）] に移動します。

次の設定要件が適用されます。

- Cisco TMSPE 経由でプロビジョニングされた個人用 CMR は、スケジュール済み会議に使用できません。
- スケジュール済み会議には専用会議エイリアスが必要です。未スケジュール会議にすでに割り当てられている会議エイリアスを使用しないでください。
- [会議の作成を許可する（Allow conference to be created）] を [いいえ（No）] に設定します。

ステップ 7 **Cisco TMS での会議エイリアスの設定**：
Cisco TMS で、[システム（Systems）] > [ナビゲータ（Navigator）] に進み、[TelePresence Conductor エイリアス（TelePresence Conductor Aliases）] を選択し、[エイリアス（Aliases）] を選択して、[新規（New）] を選択します。
エイリアス名は TelePresence Conductor 内の対応する会議エイリアスと一致させる必要はありませんが、同じ名前を使用すると管理しやすい場合もあります。

TelePresence Conductor 内の対応する会議エイリアスの [入力エイリアス（Incoming alias）] 設定と一致するように [エイリアスパターン（Alias Pattern）] 設定を指定します（TelePresence Conductor とは異なり、パターンは正規表現として指定されません。）

（注） Cisco TMS エイリアスは、TMS により会議作成時に動的に割り当てられ、手動での変更が可能です。

ステップ 8 **（オプション）Cisco TMS のサービス設定の編集**：
会議エイリアスと違って、Cisco TMS が自動的にサービス設定を作成します。値は、関連するエイリアス パターンに関連付けられた TelePresence Conductor 内のサービス設定から生成されます。オプションでサービス設定の設定値を変更するには、Cisco TMS で、[システム（Systems）] > [ナビゲータ（Navigator）] > [コンダクタ（Conductor）] > [サービス設定（Service Preferences）] に移動して、[編集（Edit）] を選択します。

TelePresence Conductor は、サービス設定の総容量を Cisco TMS にレポートします。スケジューリングに単一の専用ブリッジを使用しない場合は、[容量調整（Capacity Adjustment）] の設定値をデフォルトの 100% から変更して、その効果をモニタすることもできます。この設定値は、Cisco TMS がこのサービス設定を使用して会議をスケジュールするときに使用できる総容量のパーセンテージを指定します。

次の場合は、[容量調整（Capacity Adjustment）] を 100 より大きい値に設定できます。

- カスケードを使用しているが、会議があまり頻繁にカスケードされない傾向がある場合。これにより、予約されたカスケードのリソースが実際には使用されない可能性を相殺できます。
- ブリッジのリソース最適化を使用する場合。Cisco TMS は、スケジュール済み会議専用のリソースに関して最適化を考慮しません。関与するエンドポイントの組み合わせによっては、エンドポイントが Conductor テンプレート設定によって割り当てられているすべてのリソースを実際には使用しない可能性があります。容量を過大に割り当てることにより、TMS によって最初に予約された容量が、最適化によって最初のリソースが解放された後で実際に使用されるリソースより多い場合に、予約されたリソースが実際には使用されない可能性を相殺できます。

容量を過大に（100% より大きく）割り当てると、当然ながらすべての参加者をサポートするのに十分なリソースがなくなるリスクが高まります。そのリスクを最小限に抑えるため、スケジューリング用にマークされていない予約ブリッジ プールを使用して、そこにオーバーサブスクライブされた会議を流し込むこともできます。

次の場合は、[容量調整（Capacity Adjustment）] を 100 より小さい値に設定できます。

- 一般に、スケジュール済み会議とスケジュールされない会議の共有ブリッジを使用する場合（容量を少なく割り当てることで、リソース不足のためにユーザが会議に参加できなくなるリスクを最小限に抑えることができるため）。
- 会議の規模が予想よりも大きくなる（招待状が転送されたり、招待されていない参加者が参加しようとしたりする）傾向がある場合。

ステップ 9 **（オプション）Cisco TMS の会議ブリッジの追加**：
必要な場合は、TelePresence Conductor によって管理される会議ブリッジを Cisco TMS でオプションとして設定することにより、いくつかのメリットが得られます。

ステップ 10 **TMS での TelePresence Conductor の設定**：

Cisco TMS で、[システム（Systems）] > [ナビゲータ（Navigator）] に進み、[TelePresence Conductor] を選択し、[設定（Settings）] > [設定の編集（Edit Settings）] に移動します。

[TMS スケジューリング設定（TMS Scheduling Settings）] で、TelePresence Conductor の予約オプションと発信オプションを選択します。

1. H.323 ダイヤルはいずれの方向でも有効にしないでください。
2. SIP URI ダイヤルを有効にしてください。
3. オプションで [拡張設定（Extended Settings）] に進み、特定の番号範囲とステップ値を使用して、カスタマイズ会議 ID 範囲を設定します。

ステップ 11　会議のスケジュール設定：

注：このガイドでは、[Cisco TMS 予約（Cisco TMS Booking）] > [新しい会議（New Conference）] を使用した会議のスケジュール方法を説明します。他に、Cisco TMSPE での Smart Scheduler、Cisco TMSXE での Microsoft Outlook、Cisco TMSBA Booking API などの方法も使用できます。

Cisco TMS で、[予約（Booking）] > [新しい会議（New Conference）] に移動して、会議に適切な設定を定義します。

1. [基本設定（Basic Settings）] を使用して、会議タイトル、接続方法、会議所有者、開始時刻と終了時刻、Cisco WebEx オプション、および繰り返し用のオプションを定義します。
2. その他のオプションは、[詳細設定（Advanced Settings）] 領域で利用できます。
3. [参加者（Participants）] タブを使用して、ユーザとエンドポイントを会議に追加します。

会議を保存すると、会議のダイヤルイン番号が主催者や参加者に電子メール経由で配信されます。会議を更新するたびに新しい番号が配信されます。

第 8 章

Cisco MCU および TelePresence Server を設定する

MCU および TelePresence Server の概要

この章では、MCU と TelePresence Server の両方で、CMR ハイブリッド 会議で使用する必要がある設定と使用が推奨される設定について説明します。

MCU および TelePresence Server には 2 つの展開オプションがあります。

- Cisco Unified Communications Manager への MCU と TelePresence Server のトランキング
- Cisco Expressway-C または Cisco VCS Control への MCU と TelePresence Server の登録

ユーザ エクスペリエンスの観点では、TelePresence から MCU または TelePresence Server への発言中の参加者は、WebEx ユーザに対して表示され、WebEx から MCU または TelePresence Server への発言中の参加者は、TelePresence に対して表示されます。TelePresence Server は、デフォルトでは ActivePresence という機能を使用して、発言中の参加者を全画面ビューで表示し、画面下部に最大 9 人までの他の TelePresence 参加者を横並べに表示できます。MCU は、デフォルトでは発言中の参加者を全画面ビューで表示します。使用可能な画面レイアウト オプションの詳細については、TelePresence Server および MCU のマニュアルを参照してください。

（注） CMR ハイブリッド では、シスコのマルチパーティ ブリッジ（Cisco TelePresence Server、Cisco TelePresence MCU など）だけがサポートされます。

MCU 設定タスク フロー

はじめる前に

MCU から WebEx へのコールでは SIP だけがサポートされています。MCU で SIP が正しく設定されていることを確認します。MCU/TS、Cisco Unified Communications Manager、Cisco Expressway-C、Cisco VCS Control、Cisco Expressway-E、Cisco VCS Expressway および WebEx クラウド間のコールレッグをインターワーキングすることはできません。

（注） SIP の設定方法の詳細については、MCU のヘルプを参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	MCU のコンテンツ モードの設定, （81 ページ）	必須作業です。ハイブリッド モードを使用するには、入力コンテンツ ストリームを設定します。この設定は Cisco TMS を使用して行うことをお勧めします。
ステップ 2	ビデオ コーデックとオーディオ コーデックの設定, （81 ページ）	必須作業です。WebEx では、ビデオとコンテンツに H.264、音声に G.711 および G 722 が必要です。
ステップ 3	自動コンテンツ ハンドオーバーの設定, （82 ページ）	必須作業です。TelePresence エンドポイントのこの機能を有効にして CMR ハイブリッド 会議中に共有できるようにする必要があります。
ステップ 4	TSP 音声のデフォルト SIP ドメインの設定, （82 ページ）	必須作業です。MCU リリース 4.5 にこの手順を使用します。
ステップ 5	自動的にコンテンツ チャネルを重要として設定, （83 ページ）	推奨。
ステップ 6	発信トランスコード コーデックの設定, （83 ページ）	推奨。
ステップ 7	適応型ゲイン制御の設定, （84 ページ）	推奨。
ステップ 8	通知音の設定, （84 ページ）	推奨。
ステップ 9	暗号化の設定, （85 ページ）	推奨。

MCU のコンテンツ モードの設定

ハイブリッド モードでは、受信コンテンツ ストリームがパススルーされ、HD エンドポイントに可能な最高品質が提供されます。また、受信コンテンツ ストリームがデコードされ、これを使用して、パススルー ストリームを受信できないすべてのユーザ（SD エンドポイント）を対象とした 2 番目の解像度が低いストリームが作成されます。このためビデオ ポートが使用されますが、ユーザはトランスコードとパススルーの両方のメリットを得ることができます。

コンテンツ モードが [パススルー（Passthrough）] に設定されている場合、会議のすべての参加者に 1 つのビデオ ストリームが送信されます。すべての参加者が HD エンドポイントの場合、可能な最高品質で受信します。受信できるビデオが SD ビデオのみの参加者が 1 人以上いる場合、すべての参加者が SD ビデオを受信します。

MCU でコンテンツ モードを設定できますが、Cisco TMS を使用して設定することを推奨します。

手順

ステップ 1 [システム（Systems）] > [ナビゲータ（Navigator）] に移動します。

ステップ 2 MCU を選択し、[システム設定の編集（Edit system settings）] をクリックします。

ステップ 3 [設定（Settings）] タブで [拡張設定（Extended Settings）] をクリックします。

ステップ 4 [コンテンツモード（Content Mode）] で [ハイブリッド（Hybrid）] を選択し、[保存（Save）] をクリックします。

ビデオ コーデックとオーディオ コーデックの設定

WebEx では、ビデオとコンテンツに H.264、音声に G.711 および G 722 が必要です。

MCU でビデオ コーデックとオーディオ コーデックを設定するには、次の手順を実行します。

手順

ステップ 1 MCU にログインします。

ステップ 2 [設定（Settings）] をクリックします。
[設定（Settings）] ページが表示され、[会議（Conferences）] タブが表示されます。

ステップ 3 [詳細設定（Advanced Settings）] セクションの次の項目で [H.264] がオンになっていることを確認します。

- [MCU からのビデオコーデック（Video codecs from MCU）]

- [MCU へのビデオコーデック（Video codecs to MCU）]

ステップ 4 [詳細設定（Advanced Settings）] セクションの次の項目で [G.711] および [G.722] がオンになっていることを確認します。

- [MCU からのオーディオコーデック（Audio codecs from MCU）]
- [MCU へのオーディオコーデック（Audio codecs to MCU）]

ステップ 5 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

自動コンテンツ ハンドオーバーの設定

CMR ハイブリッド会議中に TelePresence エンドポイントが共有できるようにするためには、この機能を有効にする必要があります。

手順

ステップ 1 MCU にログインします。

ステップ 2 [設定（Settings）] をクリックします。
[設定（Settings）] ページが表示され、[会議（Conferences）] タブが表示されます。

ステップ 3 [コンテンツ（Content）] タブをクリックします。

ステップ 4 [自動コンテンツハンドオーバー（Automatic content handover）] の [有効（Enabled）] を選択します。

ステップ 5 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

TSP 音声のデフォルト SIP ドメインの設定

MCU リリース 4.5 では、TSP 音声を使用する展開の場合、デフォルト SIP ドメインを設定する必要があります。これは、TSP 音声でのみ必要です。

TMS は MCU に対して番号をダイヤルするよう指示するときに、@domain 部分がない番号を提供します。コールが正常に実行されるためにはドメインが必要であるため、MCUはダイヤルする番号にドメインを自動的に追加する必要があります。

詳細については、MCU のオンライン ヘルプを参照してください。

MCU リリース 4.5 でデフォルト SIP ドメインを設定するには、次の手順を実行します。

手順

ステップ 1 MCU にログインします。

ステップ 2 [設定（Settings）] をクリックします。
[設定（Settings）] ページが表示されます。

ステップ 3 [SIP] タブをクリックします。

ステップ 4 [発信コール設定（Outbound call configuration）] に、[トランクを使用する（Use Trunk）] を選択します。

ステップ 5 [発信先アドレス（Outbound address）] として、トランク接続先のホスト名または IP アドレスを入力します。

ステップ 6 [発信先ドメイン（Outbound domain）] として、トランク接続先のドメインを入力します。

自動的にコンテンツ チャネルを重要として設定

コンテンツ チャネルを自動的に重要として扱うように会議を設定することを推奨します。会議の新しいコンテンツ チャネルはすべて重要として扱われ、会議レイアウトにコンテンツ チャネルが表示されるすべての参加者に対し、すぐわかるように表示されます。

コンテンツ チャネルを自動的に重要として設定する機能を有効にするには、次の手順を実行します。

手順

ステップ 1 MCU にログインします。

ステップ 2 [設定（Settings）] をクリックします。
[設定（Settings）] ページが表示され、[会議（Conferences）] タブが表示されます。

ステップ 3 [詳細設定（Advanced Settings）] セクションで、[自動的にコンテンツ チャネルを重要として設定する（Automatically make content channel important）] をオンにします。

ステップ 4 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

発信トランスコード コーデックの設定

発信トランスコード コーデックを H.264 に設定することを推奨します。これにより、MCU は発信トランスコード コンテンツ チャネルに H.264 ビデオ コーデックを使用するようになります。

手順

1. MCU にログインします。
2. ページの上部にある [会議（Conferences）] をクリックします。
   [会議（Conferences）] ページが表示され、[会議リスト（Conference list）] タブが表示されます。
3. [テンプレート（Templates）] タブをクリックします。
   [会議テンプレート（Conference Templates）] ページが表示されます。
4. [トップレベル（Top level）] のリンクをクリックします。
   [トップレベルのテンプレートの設定（Top level template configuration）] ページが表示されます。
5. [コンテンツ（Content）] セクションで、[発信トランスコードコーデック（Outgoing transcoded codec）] メニューを使用して、[H.264] を選択します。
6. ページの下部にある [変更を適用する（Apply changes）] をクリックします。

適応型ゲイン制御の設定

参加時の適応型ゲイン制御を有効に設定することを推奨します。適応型ゲイン制御（ACG）では、すべての参加者の音量レベルを統一するため、各参加者の音声のゲインが変更されます。

手順

1. MCU にログインします。
2. ページの上部にある [会議（Conferences）] をクリックします。
   [会議（Conferences）] ページが表示され、[会議リスト（Conference list）] タブが表示されます。
3. [テンプレート（Templates）] タブをクリックします。
   [会議テンプレート（Conference Templates）] ページが表示されます。
4. [トップレベル（Top level）] のリンクをクリックします。
   [トップレベルのテンプレートの設定（Top level template configuration）] ページが表示されます。
5. [パラメータ（Parameters）] セクションで [参加時の適応型ゲイン制御（Adaptive Gain Control on join）] メニューを使用して、[有効（Enabled）] を選択します。
6. ページの下部にある [変更を適用する（Apply changes）] をクリックします。

通知音の設定

この設定は、会議中に発生するさまざまな音を制御します。CMR ハイブリッド 会議で特に注意する設定として、参加と退席の通知があります。これは、他の参加者が会議に参加したことと、会議から退席したことを通知するメッセージ音です。デフォルトでは、有効（オン）です。

WebEx にも参加と退席の通知がありますが、これは MCU の設定からは独立しています。MCU と WebEx の両方でこの通知が有効になっている場合、MCU 側と WebEx 側で参加者が会議に参加または退席するたびに通知が聞こえます。このため、MCU または WebEx のいずれかまたは両方で、参加と退席の通知を無効にすることがあります。

MCU で参加と退席の通知音を無効にするには、次の手順を実行します。

手順

ステップ 1 MCU にログインします。

ステップ 2 [設定（Settings）] をクリックします。
[設定（Settings）] ページが表示され、[会議（Conferences）] タブが表示されます。

ステップ 3 [会議設定（Conference Settings）] セクションの [通知音（Audio Notifications）] で、[参加と退席の通知（Join and leave indications）] をオフにします。

ステップ 4 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

暗号化の設定

暗号キーを使用する MCU では、会議設定でメディアの暗号化をオプションとして設定することを推奨します。すべてのメディアで暗号化を必須に設定すると、WebEx に送信されるメイン ビデオとコンテンツ ビデオが 1 つのストリームにマージされ、1 人の参加者として扱われます。

暗号化をオプションとして設定するには、次の手順を実行します。

手順

ステップ 1 MCU にログインします。

ステップ 2 ページの上部にある [会議（Conferences）] をクリックします。
[会議（Conferences）] ページが表示され、[会議リスト（Conference list）] タブが表示されます。

ステップ 3 [テンプレート（Templates）] タブをクリックします。
[会議テンプレート（Conference Templates）] ページが表示されます。

ステップ 4 [トップレベル（Top level）] のリンクをクリックします。
[トップレベルのテンプレートの設定（Top level template configuration）] ページが表示されます。

ステップ 5 [パラメータ（Parameters）] セクションで、[暗号化（Encryption）] メニューを使用して [オプション（Optional）] を選択します。

ステップ 6 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

TelePresence Server 設定タスク フロー

はじめる前に

TelePresence Server から WebEx へのコールでは SIP だけがサポートされています。TelePresence Server で SIP が正しく設定されていることを確認します。SIP の設定方法の詳細については、TelePresence Server のヘルプを参照してください。

TelePresence Server ソフトウェアの詳細については、次のリンクを参照してください。

http://www.cisco.com/en/US/products/ps11339/prod_release_notes_list.html

手順

	コマンドまたはアクション	目的
ステップ 1	ローカル管理モードを設定する，（87 ページ）	必須作業です。TMS で TelePresence Server を制御するには、TelePresence Server をローカル管理モードに設定する必要があります。 これは、ハードウェア ベースの TelePresence Server にのみ適用されます。仮想マシン上の TelePresence Server は、Conductor から制御できるようにリモート管理モードにする必要があります。
ステップ 2	自動コンテンツ ハンドオーバーの設定，（87 ページ）	必須作業です。TelePresence エンドポイントの自動コンテンツ ハンドオーバーを有効にして CMR ハイブリッド会議中に共有できるようにする必要があります。 これは、ハードウェア ベースの TelePresence Server にのみ適用されます。リモート管理モードになっている仮想マシン上の TelePresence Server については、Conductor API で自動的に有効化されます。
ステップ 3	表示設定の設定，（88 ページ）	推奨。WebEx ビデオがマルチスクリーンのエンドポイントでフルサイズで表示されるように表示設定を設定します。 これは、ハードウェア ベースの TelePresence Server にのみ適用されます。リモート管理モードになっている仮想マシン上の TelePresence Server については、Conductor API で自動的に有効化されます。

ローカル管理モードを設定する

TMS で TelePresence Server を制御するには、TelePresence Server をローカル管理モードに設定する必要があります。

（注） これは、ハードウェア ベースの TelePresence Server にのみ適用されます。仮想マシン上の TelePresence Server は、Conductor から制御できるようにリモート管理モードにする必要があります。

手順

ステップ 1 TelePresence Server にログインします。

ステップ 2 [設定（Configuration）] > [動作モード（Operation mode）] の順に移動します。
[動作モード（Operation mode）] ページが表示されます。

ステップ 3 [動作モード（Operation mode）] メニューを使用して、[ローカル管理（Locally managed）] を選択します。

ステップ 4 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

自動コンテンツ ハンドオーバーの設定

CMR ハイブリッド会議中に TelePresence エンドポイントが共有できるようにするためには、この機能を有効にする必要があります。

（注） これは、ハードウェア ベースの TelePresence Server にのみ適用されます。リモート管理モードになっている仮想マシン上の TelePresence Server については、Conductor API で自動的に有効化されます。

手順

ステップ 1 TelePresence Server にログインします。

ステップ 2 [設定（Configuration）] > [システム設定（System Settings）] に進みます。
[システム設定（System Settings）] ページが表示されます。

ステップ 3 [自動コンテンツハンドオーバー（Automatic content handover）] がオンになっていることを確認します。

ステップ 4 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

表示設定の設定

TelePresence Server の表示設定を全画面に設定することを推奨します。これにより、マルチスクリーン エンドポイントで WebEx ビデオを全画面で表示できます。

（注） これは、ハードウェア ベースの TelePresence Server にのみ適用されます。リモート管理モードになっている仮想マシン上の TelePresence Server については、Conductor API で自動的に有効化されます。

手順

ステップ 1 TelePresence Server にログインします。

ステップ 2 [設定（Configuration）]>[デフォルトのエンドポイント設定（Default Endpoint Settings）] の順に進みます。

ステップ 3 [表示（Display）] セクションで、シングルスクリーン エンドポイントの全画面ビューの [許可（Allowed）] を選択します。

ステップ 4 ページの下部にある [変更を適用する（Apply changes）] をクリックします。

第 9 章

コール コントロールを設定する

コール制御の概要

CMR ハイブリッド の使用を開始するには、ビデオ ネットワークで使用されるコール制御製品を設定する必要があります。

4 通りのコール制御シナリオが考えられます。

- Cisco Cisco Unified Communications Manager と、Cisco Expressway-C および Cisco Expressway-E。

  エンドポイントが登録され、ブリッジは Unified Communications Manager だけにトランキングされます。

- Cisco VCS Control および Cisco VCS Expressway

  エンドポイントは、Cisco VCS Control または Cisco VCS Expressway、あるいはこの両方だけに登録され、ブリッジは Cisco VCS Control だけに登録されます。

- Cisco Unified Communications Manager と、Cisco Expressway-C および Cisco Expressway-E、または Cisco VCS Control と Cisco VCS Expressway

  エンドポイントは Unified Communications Manager だけに登録され、ブリッジは Cisco VCS Control だけに登録されます。

- Cisco VCS Control および Cisco VCS Expressway と Unified Communications Manager

  エンドポイントは、Cisco VCS Control/Expressway と Unified Communications Manager だけに登録され、ブリッジは Cisco VCS Control だけに登録されます。

（注） Unified Communications Manager をコール制御ソリューションとして使用すると、エンドポイントが Unified Communications Manager または Cisco VCS に登録されているかどうかにかかわらず、WebEx と通信するために、Cisco Expressway-C と Cisco Expressway-E、または Cisco VCS Control と Cisco VCS Expressway のいずれかを導入する必要があります。

Cisco Expressway および TelePresence 設定タスク

次に示す手順は VCS 製品と Expressway 製品の両方に適用されます。VCS Control を参照するステップはすべて Expressway-C にも適用されます。同様に、VCS Expressway を参照するステップはすべて Expressway-E にも適用されます。

はじめる前に

Cisco VCS または Expressway で WebEx を設定するには、次のコンポーネントが必要です。

- Cisco TelePresence Video Communication Server（Cisco VCS）または Expressway では、ファームウェア リリース X8.5 以降が稼動している必要があります。
- Cisco VCS Expressway または Expressway は、静的 IP アドレス、DNS、および NTP 情報が割り当てられ、その Web インターフェイス経由で管理用にアクセスできる必要があります。
- Cisco Expressway シリーズにリッチ メディア ライセンスがインストールされている必要があります。
- ソフトウェア バージョン X8.5.3 以降では、要件, （35 ページ）の「Cisco Expressway/Cisco VCS のデフォルト SIP TCP タイムアウトの短縮」の説明に従って、Cisco Expressway/Cisco VCS にデフォルトの SIP TCP タイムアウト値を設定することを推奨します。
- ネットワークのエンドポイントが、Cisco VCS Control または Expressway、あるいは Unified Communications Manager に登録されています。

  （注） エンドポイントが Unified Communications Manager に登録されている場合、Unified Communications Manager と VCS Control 間に SIP トランクを設定する必要があります。詳細については、Cisco Unified Communications Manager の設定, （94 ページ）を参照してください。

- Cisco VCS Expressway にアクセスできるように、ファイアウォールでポート 5061 が開いている必要があります。

  このポートが正しく設定されていない場合、コールは正しく実行されません。

（注） 重要：Check Point Software Technologies, Inc. のファイアウォールで使用されているステートフル パケット インスペクションには、Cisco VCS Expressway および Expressway-E との互換性がありません。

- このため、VCS Expressway または Expressway-E との間でネットワーク トラフィックを送受信するルータ/ファイアウォールでは、SIP および H.323 アプリケーション層ゲートウェイを無効にすることを強く推奨します。これは、これらのゲートウェイが有効になっていると、VCS の組み込みファイアウォール/NAT トラバーサル機能に悪影響を及ぼす可能性があるためです。

- 使用する会議ブリッジ（MCU または TelePresence Server）がネットワーク上ですでに稼働しています。
- Cisco VCS Control または Expressway-C がプライベート ネットワーク上にあります。
- Cisco VCS Expressway または Expressway-E が DMZ にあり、インターネットにアクセスできます。
- WebEx コールに 2 ～ 4 Mbps 以上の帯域幅を許可するため、（ネットワークの要件に基づいて）ゾーンとパイプを適切に設定します。帯域幅制御の詳細については、次の URL にある『Cisco VCS Administrator Guide』を参照してください。

  http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-maintenance-guides-list.html

  または、次の URL にある『Cisco Expressway Administrator Guide』を参照してください。

  http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html

- Cisco VCS Control に登録されているエンドポイントは、SIP レジストラ/H.323 ゲートキーパーとして設定する必要があります。

  CMR ハイブリッド が Cisco VCS Control に登録されているエンドポイントと連携できるようにするには、Cisco VCS Control を SIP レジストラとして設定し、Cisco VCS Control が SIP デバイスを登録してコールをこれらのデバイスにルーティングできるようにします。Cisco VCS Control は H.323 ゲートキーパーと SIP レジストラの両方として機能します。

  Cisco VCS Control を SIP レジストラとして設定するには、1 つ以上の SIP ドメインを設定します。Cisco VCS Control はこれらのドメインの SIP レジストラおよびプレゼンス サーバとして機能し、これらのドメインを含むエイリアスの登録を試みるすべての SIP エンドポイントの登録要求を受け入れます。

  Cisco VCS Control の SIP ドメインを設定する方法の詳細については、次の URL にある『Cisco VCS and CUCM Deployment Guide』を参照してください。

  http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

または、次の URL にある『Cisco Expressway and CUCM via SIP Trunk Deployment Guide』を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.html

- 企業間 TelePresence 参加者：他の企業の参加者が TelePresence を介して参加できるようにするには、設定した SIP ドメインの Cisco VCS Expressway に解決される有効な SIP SRV（セキュア SIP）、非セキュア SIP SRV、または複数の SIP および H.323 SRV レコードが必要です。これにより、TelePresence 参加者は Cisco VCS Expressway にルーティングできます。

手順

	コマンドまたはアクション	目的
ステップ 1	新しい DNS ゾーンの作成，（92 ページ）	必須作業です。WebEx クラウドへ接続するために Cisco VCS Expressway に DNS ゾーンを設定します。
ステップ 2	MCU のトラバーサル ゾーンの設定，（93 ページ）	暗号化が有効な MCU をサポートするトラバーサル ゾーンを設定します（デフォルト設定）。

新しい DNS ゾーンの作成

WebEx クラウドへの接続では新しい DNS ゾーンを使用します。この DNS ゾーンを Cisco VCS Expressway で設定する必要があります。

CMR ハイブリッド 向けに Expressway-E または Cisco VCS Expressway を設定するには、次の手順を実行します。

手順

ステップ 1 新しい DNS ゾーンを作成します。[H.323] を [オフ（Off）] に設定します。

a) [SIP メディア暗号化モード（SIP Media encryption mode）] を [強制暗号化（Force encrypted）] に設定します。
b) [TLS 検証モード（TLS Verify mode）] を有効にします。
c) [TLS 検証サブジェクト名（TLS verify subject name）] フィールドに、sip.webex.com と入力します。
d) [ゾーンの作成（Create Zone）] をクリックします。

ステップ 2 WebEx のドメイン内の既存の DNS ゾーン（低い優先度）の検索ルールよりも高い優先度の検索ルールを設定します。次のように設定する必要があります。

- プロトコル：SIP
- [ソース（Source）]：<管理者定義>、デフォルトは [いずれか（Any）]
- [モード（Mode）]：[エイリアスのパターン マッチ（Alias Pattern Match）]
- [パターン タイプ（Pattern Type）]：[正規表現（Regex）]
- [パターン文字列（Pattern String）]：(.*)@(.*)(\.webex\.com).*
- [パターン動作（Pattern Behavior）]：[置換（Replace）]
- [置換文字列（Replace String）]：\1@\2\3
- [正常に一致する場合（On Successful Match）]：[停止（Stop）]
- [ターゲット（Target）]：<WebEx 向けに作成した DNS ゾーン>
- [状態（State）]：[有効（Enabled）]

DNS ゾーンの検索ルールの作成および設定方法の詳細については、次の『Cisco TelePresence Video Communication Server Basic Configuration（Control with Expressway）Deployment Guide』を参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf

ステップ 3 企業の有効なクライアント/サーバ証明書を設定します。通常、証明書の CName は社内の Cisco VCS Expressway へのルーティング可能なドメインです。これは、WebEx によってサポートされる公開 CA が発行した CA レベルの証明書名でなければなりません。

（注） 自己署名証明書はサポートされません。

サポートされる証明書と VCS Expressway で証明書を設定する方法の詳細については、Cisco Expressway-E および Cisco VCS Expressway での証明書を設定する，（105 ページ）を参照してください。

MCU のトラバーサル ゾーンの設定

この手順では、暗号化が有効な（デフォルト設定）MCU をサポートするために VCS で必要な設定について詳しく説明します。

注意 次の設定を行わない場合、暗号化が有効な MCU では、プレゼンテーション コンテンツが個々のストリームではなくメイン ビデオ チャネルで配信されます。

（注） 次の手順では、VCS Control のタスクは Expressway-C と同じであり、Expressway-E のタスクは VCS Expressway と同じです。

暗号化が有効な MCU をサポートするには、次の手順を実行します。

手順

ステップ 1 新しいトラバーサル クライアント ゾーンを Cisco VCS Control から Cisco VCS Expressway に設定します。
（注） 新しいゾーンでは異なるポート番号が使用されることを確認してください。

ステップ 2 トラバーサル クライアントのメディア暗号化設定を [強制暗号化解除（Force unencrypted）] または [ベストエフォート（Best effort）] に設定します。

ステップ 3 Cisco VCS Expressway で、前のステップで設定した Cisco VCS Control トラバーサル ゾーンに接続する新しいトラバーサル サーバ ゾーンを設定します。

ステップ 4 この新しい Cisco VCS Expressway トラバーサル サーバ ゾーンで、メディア暗号化を [強制暗号化解除（Force unencrypted）] に設定します。

ステップ 5 Cisco VCS Control で、WebEx トラフィックに一致する検索ルール（例：match = .*@example.webex.com）を、デフォルトのトラバーサル ゾーンを使用する検索ルールよりも高い優先度で設定します。
（注） 上記の設定では、MCU暗号化が有効であるかどうかに関係なく、ビデオとプレゼンテーションが個別のチャネルで配信されます。また、WebEx からのコンテンツは、MCU に送信される場合は（インターネット上で暗号化されても）暗号化されません。

Cisco Unified Communications Manager の設定

ここでは、CMR ハイブリッド用の Cisco Unified Communications Manager（Unified Communications Manager）を設定するために必要な手順を説明します。この設定では、エンドポイントが Unified Communications Manager だけに登録されている展開と、Unified Communications Manager と Cisco VCS Control/Cisco VCS Expressway の両方に登録されている展開もサポートされます。

ここでは、次の作業について説明します。

- Cisco Unified Communications Manager の設定, （94 ページ）
- Cisco Unified Communications Manager と Cisco Expressway-C または Cisco VCS Control 間の SIP トランク, （95 ページ）
- SIP メッセージングの Early Offer の設定, （95 ページ）
- Unified Communications Manager にトランキングされているブリッジのルーティング ルールの設定, （98 ページ）

Cisco Unified Communications Manager 設定の前提条件

Cisco Unified Communications Manager（Unified Communications Manager）で WebEx を設定するには、次のコンポーネントが必要です。

- Unified Communications Manager 10.5(2)SU1 または SU2
- ネットワーク上のエンドポイントは Unified Communications Manager に登録されています
- 使用する会議ブリッジ（MCU または Cisco TelePresence Server）はすでにネットワーク内で稼働しており、Unified Communications Manager にトランキングされているかまたは VCS に登録されています
- Cisco Expressway-C または Cisco VCS Control がプライベート ネットワークに配備されています
- Unified Communications Manager 上の MCU および TelePresence Server エンドポイントと WebEx クラウド間で最適な SIP 音声およびビデオ接続を実現するため、2 ～ 4 Mbps 以上を許可するようにリージョンを設定することを推奨します。
- Cisco Expressway-E または Cisco VCS Expressway は DNS ゾーンが設定されています。

Cisco Unified Communications Manager と Cisco Expressway-C または Cisco VCS Control 間の SIP トランク

このセクションでは、SIP トランク経由でインターワークするために Cisco Expressway シリーズ X8.5 以降と Cisco Unified Communications Manager（Unified Communications Manager バージョン 10.5(2)SU1 以降）を設定する方法について説明します。

これは、Unified Communications Manager に登録されているエンドポイントが Cisco Collaboration Meeting Rooms Hybrid 会議に参加し、Cisco VCS Control に登録されているエンドポイントにコールするために必要です。また Cisco VCS の Unified Communications Manager ネイバー ゾーンが BFCP 対応に設定されていることを確認します。

設定手順は、次の場所の『Cisco Unified Communications Manager with Cisco VCS Deployment Guides』で説明されています。

http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-installation-and-configuration-guides-list.html

SIP メッセージングの Early Offer の設定

Early Offer の設定は、ブリッジが Unified CM にトランキングされ、エンドポイントが Unified CM に登録されている Unified CM を中心とした展開でのみ必要です。

Early Offer により、セッションの開始側が SIP INVITE でその機能を送信し、呼び出されたデバイスが優先コーデックを選択します。TelePresence コールを伝送するすべての SIP トランクを Early Offer に対応して設定することを推奨します。

また、CMR ハイブリッド コールをサポートするため、直接スケジュール済みブリッジから Cisco Expressway または Cisco VCS への Early Offer が必要です。発信側デバイスからサービスへのパス全体で Early Offer をサポートするように設定する必要があります。

Cisco VCS を中心とした展開は常に Early Offer モードで稼働するため、この項の内容は Unified CM を中心とした展開のみに関連します。発信トランクを Early Offer として設定する場合の推奨される方法を説明します。

（注） Unified CM トランクのデフォルト設定は Delayed Offer（ディレイド オファー）です。

次の Optimized Conferencing 要素間のトランクはすべて、Early Offer に対応している必要があります。次に示すトランクに対し、メディア ターミネーション ポイント（MTP）リソースを直接または間接的に使用可能にしないでください。

- Unified CM から Cisco Expressway-C
- Unified CM から Cisco VCS Control
- Unified CM から TelePresence Server
- Unified CM から MCU
- TelePresence エンドポイントと前述のネットワーク要素からのトラフィックを伝送する Unified CM 間トランクも、Early Offer 対応（メディア ターミネーション ポイント（MTP）リソースなし）にする必要があります。たとえば、EX90 >> UCM1 >> UCM2 >> Conductor >> TelePresence Server というコール フローのシナリオでは、UCM1 >> UCM2 間のトランクと UCM2 >> Conductor 間のトランクを Early Offer 対応にする必要があります。

MTP の使用を制限するには、すべての Session Management Edition（SME）クラスタからすべての MTP リソースを削除し、Unified CM クラスタのすべての MTP リソースを、TelePresence トラフィックを伝送する SIP トランクと TelePresence エンドポイントの両方からアクセスできないメディア リソース グループに配置する必要があります。

さまざまな展開シナリオに適用される事項があります。

シナリオ 1.単一 Unified CM システム設定での Early Offer の設定

会議ブリッジは Cisco Unified Communications Manager へ接続され、Unified Communications Manager は Cisco Expressway にトランキングされています。エンドポイントは Unified Communications Manager に登録されます。このシナリオでは、次のトランクが Early Offer 対応に設定されている必要があります。

- Unified Communications Manager から Cisco Expressway-C
- Unified Communications Manager から TelePresence Conductor

シナリオ2.マルチクラスタシステム（TelePresenceConductorがUnifiedCommunications Manager SME に接続されている）での Early Offer の設定

リーフ Unified CM クラスタが接続されている 1 つ以上の Unified Communications Manager SME クラスタ。TelePresence Conductor と会議ブリッジは Unified Communications Manager SME に接続されます。Unified Communications Manager SME は Cisco Expressway-C にトランキングされます。このシナリオでは、次のトランクが Early Offer 対応に設定されている必要があります。

- Unified Communications Manager SME から Cisco Expressway-C
- Unified Communications Manager SME から TelePresence Conductor

（注） 3 つ以上のクラスタからなるマルチクラスタ システム（そのうち 1 つの Unified CM クラスタが専用 Unified Communications Manager SME）では、エンドポイントが Unified Communications Manager SME に登録されることはなく、常にリーフ Unified CM SME に登録されます。

シナリオ3.マルチクラスタシステム（TelePresenceConductorがUnifiedCommunications Manager SME に接続されている）での Early Offer の設定

リーフ Unified Communications Manager クラスタが接続されている 1 つ以上の SME クラスタ。会議ブリッジはリーフ クラスタに接続されます。1 つのトランクによって SME が Cisco Expressway-C に接続されます。このシナリオでは、次のトランクが Early Offer 対応に設定されている必要があります。

- Unified Communications Manager SME から Cisco Expressway-C
- リーフ Unified Communications Manager クラスタから TelePresence Conductor
- リーフ Unified CM クラスタから Unified Communications Manager SME

SIP トランクでの Early Offer（およびディレイド オファーへのフォールバック）の設定

手順

ステップ 1 トランクごとに、ご使用の Unified CM バージョンに応じて次のいずれかを実行します。

- Unified CM バージョン 10.5(2) システムでは、[音声コールとビデオコールに対する Early Offer サポート（Early Offer support for voice and video calls）] ドロップダウンで [ベストエフォート (MTPの挿入なし)（Best Effort (no MTP inserted)）] を選択します。

ステップ 2 次の要素からすべての MTP リソースを削除します。

- SME クラスタ（Unified Communications Manager SME 展開環境の場合）。
- すべての Unified CM クラスタのすべての TelePresence エンドポイントと SIP トランク。

ステップ 3 [SIP トランク DTMF シグナリング方式（SIP Trunk DTMF Signaling Method）] を [RFC 2833]（デフォルト）に設定します。

ステップ 4 次の要素に対して [受信オファーのオーディオコーデック初期設定を承認（Accept Audio Codec Preference in Received Offer）] を有効にします。

- すべての SME SIP トランク（Unified Communications Manager SME 展開環境の場合）。
- すべての Unified CM クラスタで TelePresence コールを伝送するすべての SIP トランク。

ディレイド オファーへのフォールバック

発信コールでは、MTP リソースが存在しない場合に備えて、デフォルト設定はディレイドオファーへの自動フォールバックです。フォールバックなしの場合、ネットワークの Optimized Conferencing 以外の領域で問題が発生する可能性があります。着信コールでは、MTP リソースに関する要件なしで Early Offer がサポートされます。

エンドポイント

Unified CM に登録された TelePresence エンドポイントを設定するときには、MTP リソースが含まれないメディア リソース グループ リスト（MRGL）を使用してください。このため、エンドポイントが前述のいずれかのタイプのトランクを通過するコールを発信するときに、エンドポイントの MRGL 内には使用できる MTP がありません。

Unified Communications Manager にトランキングされているブリッジのルーティング ルールの設定

Unified Communications Manager を中心とした展開環境では、Unified Communications Manager にトランキングされているすべての MCU または TelePresence Server のルーティング ルールを設定する必要があります。

MCU または TelePresence Server が Unified CM にトランキングされている場合、MCU または TelePresence Server が CMR ハイブリッド サイトで長い文字列（例：yoursite.webex.com）をダイヤルします。

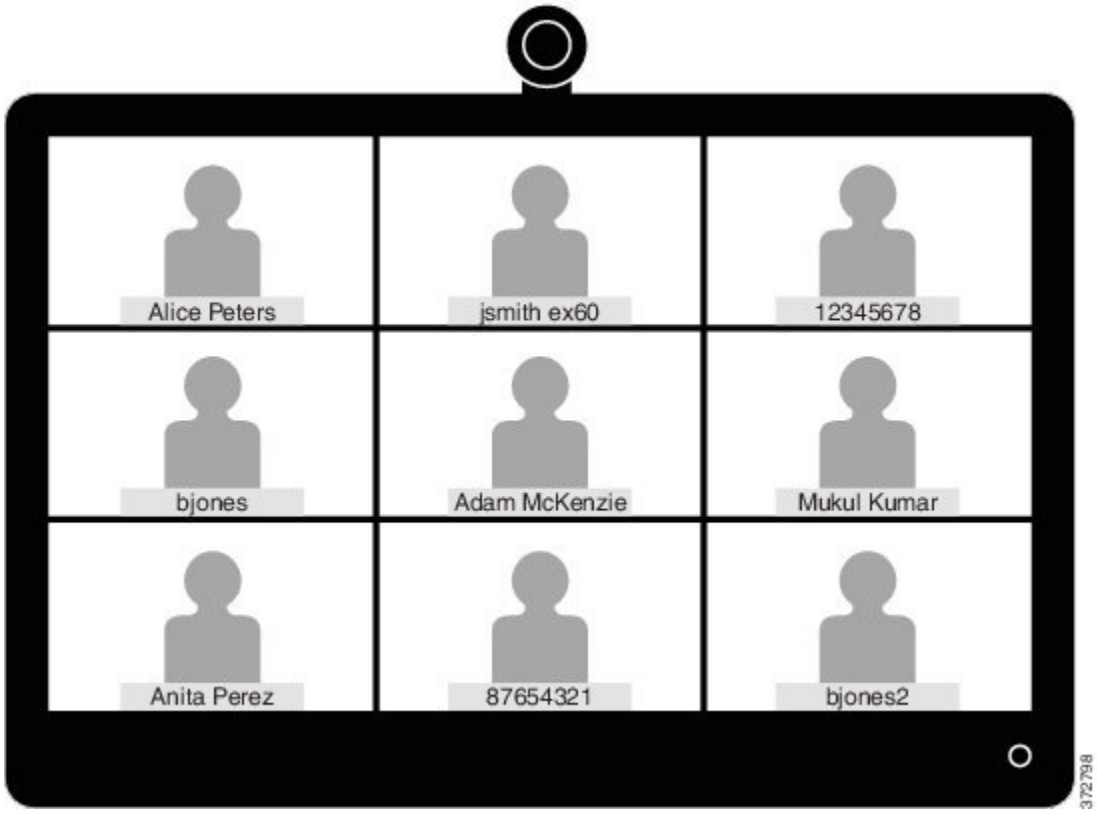
コールが正しくルーティングされるようにするため、ご使用のサイトの Unified CM で Expressway-C の SIP トランクへのルーティングのための SIP ルーティング パターンを設定します。詳細については、Unified CM のマニュアルを参照してください。

また、SIP メッセージングの Early Offer の設定, （95 ページ） で説明されているように、Unified CM にトランキングされている各 MCU または TelePresence Server に有効な Early Offer があることを確認します。

エンドポイントの表示名のプロビジョニング

TelePresence などのエンドポイントでは、その他の参加者に対してユーザを識別するために表示名が使用されます。

図 7：表示名の例



この名前の形式として、ユーザの名と姓（例：Alice Peters）、またはエンドポイントが設置されている会議室の正規名（例：MDR21-3-#120（Madrid のビル 21、3 階、部屋番号 120））を使用することを推奨します。ただし、この名前が明示的にプロビジョニングされていない場合、システ

ムはエンドポイントの SIP URI またはデバイス番号に基づいて表示名を選択します。表示される結果は、特定のユーザと会議室がどのようにプロビジョニングされているかによって異なります。これが原因で、上記の例に示すように、会議コールに表示される名前と、さまざまな形式で表示される個人ユーザ情報に整合性がないことがあります。

整合性のある名前が表示されるようにするため、Unified CM または Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）で、Cisco VCS 登録エンドポイントのこれらの設定をプロビジョニングする必要があります。

プロビジョニングするエンドポイントが Unified CM 登録されている場合は、Unified CM での表示名のプロビジョニング, （100 ページ） を参照します。プロビジョニングするエンドポイントが Cisco VCS 登録されている場合は、Cisco VCS での表示名のプロビジョニング, （102 ページ） を参照します。

Unified CM での表示名のプロビジョニング

ここでは、Cisco Unified CM Administration ユーザ インターフェイスで表示名を更新する方法について説明します。管理者がこの更新を行う正しいフィールドとロケーションを確認できるようにするために、ユーザ、デバイス、および回線を設定する方法を説明します。この更新により、名前が正しく表示されます。「トランク, （102 ページ）」というタイトルの項では、一部のユーザに役立つ詳細設定（オプション）について説明します。

ユーザとデバイス

Cisco Unified CM Administration ユーザ インターフェイスでは、[ユーザ管理（User Management）] > [エンドユーザ（End User）] ウィンドウで新しいユーザを設定します。新しいユーザの作成と、Active Directory（AD）または LDAP を使用したユーザのインポートの両方を実行できます。

新しいデバイスは、[デバイス（Device）] > [電話機（Phone）] ウィンドウで設定します。その後ユーザがデバイスに関連付けられます。この設定中に指定される詳細情報は、表示名には使用されません。表示名は [コールルーティング（Call routing）] > [電話番号（Directory Number）] の下の回線に手動で設定するか、または [デバイス（Device）] > [電話（Phone）] > [回線番号（Line#）] の下でエンドポイントに対して設定されている回線を選択して設定します。

回線（Line）

デバイスに関連付けられている回線で表示名が設定されます。このため、そのユーザが関連付けられている特定のデバイスに対して表示名が設定されます。共有回線の場合、共有回線の各アピアランスに異なる表示名を設定できます。ただし、すべてのデバイスで、ユーザの氏名または会議室の名前を使用した同一の表示名を使用することを推奨します。

一括管理を使用した Unified CM 登録エンドポイントの表示名の設定

一括管理を使用して、多数のユーザの Unified Communications Manager 登録エンドポイントの表示名を設定できます。

はじめる前に

ユーザを設定し、デバイスに関連付けていることを確認します。ユーザのプロビジョニング方法については、『Cisco Unified Communications Manager Administration Guide, Release 10.0(1)』を参照してください。

手順

ステップ 1 ユーザ レコードをエクスポートするには、『Cisco Unified Communications Manager Cisco Unified Communications Manager Administration Guide, Release 10.0(1)』を参照してください。

ステップ 2 ダウンロードした CSV ファイルの名と姓の列を、新しい CSV ファイルにコピーします。

ステップ 3 この CSV ファイルを正しいデバイスにアップロードするには、『Cisco Unified Communications Manager Administration Guide, Release 10.0(1)』の「Update phones using custom file」を参照してください。

Unified CM 登録エンドポイントの表示名の手動設定

この手順では、Unified Communications Manager 登録デバイスの表示名を設定する方法を説明します。このデバイスが、他のデバイスに関連付けられているユーザに割り当てられているかどうか、またはデバイスが共有会議室のデバイスであるかどうかは関係ありません。

はじめる前に

ユーザを設定し、デバイスに関連付けていることを確認します。ユーザのプロビジョニング方法については、『Cisco Unified Communications Manager Administration Guide, Release 10.0(1)』を参照してください。

手順

ステップ 1 Cisco Unified CM の管理ユーザ インターフェイスにログインして、[デバイス（Device）] > [電話機（Phone）] の順に選択し、[電話の検索/一覧表示（Find and List Phone）] ウィンドウに移動します。

ステップ 2 [電話の設定（Phone Configuration）] ウィンドウに到達できるように設定するデバイスの [デバイス名(回線)（Device Name(Line)）] を選択します。

ステップ 3 ウィンドウの左側の [関連付け（Association）] 領域からデバイスの回線を選択します。これにより、[電話番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

ステップ 4 [電話番号情報（Directory Number Information）] 領域の [呼び出し表示（Alerting name）] フィールドと [ASCII(発信者ID)（ASCII (Caller ID)）] フィールドに、表示名を入力します。注：これは、

Unified Communications Manager クラスタに存在しないデバイスと通信する場合に、ユーザ名を表示するために使用されます。

ステップ 5 [デバイスの回線1（Line 1 on Device）] 領域の [表示(発信者ID)（Display (Caller ID)）] フィールドと [ASCII表示(発信者ID)（ASCII Display (Caller ID)）] フィールドに、表示名を入力します。注：これは Cisco Unified CM と同じクラスタ内にあるデバイスに表示されます。

ステップ 6 共有回線の場合は、すべてのデバイスに変更が表示されるようにするため、[共有デバイス設定の更新（Update Shared Device Settings）] チェック ボックスをオンにし、[選択対象を反映（Propagate selected）] をクリックします。注：[呼び出し表示（Alerting Name）]、[ASCII呼び出し表示（ASCII Alerting Name）]、[表示(発信者ID)（Display (Caller ID)）]、および [ASCII(発信者ID)（ASCII (Caller ID)）] フィールドに、ユーザに関連付けられているデバイスの場合は表示名を設定し、共有会議室スペース内にあるエンドポイントの場合は会議室名を設定することが推奨されます。

ステップ 7 [保存（Save）] をクリックします。
エンドポイントがアクティブ コール中でない場合は、変更が自動的に反映され、即時に有効になります。エンドポイントがアクティブ コール中の場合は、アクティブ コールの終了後即時に有効になります。

トランク

必要に応じて、表示名の動作をさらに制御するために次の機能を設定できます。これらの設定は、[トランク設定（Trunk Configuration）] ウィンドウにあります。

- [デバイス情報（Device Information）] 領域で、[発信側名にUTF-8を転送（Transmit UTF-8 for Calling Party Name）] チェックボックスをオンにすると、UTF-8 をサポートするデバイス上で ASCII 呼び出し表示が送信されます。
- トランク単位で表示名を非表示にできます。このためには、[インバウンドコール（Inbound Calls）] 領域で、[接続名の表示（Connected Name Presentation）] ドロップダウン リストから [非許可（Restricted）] を選択します。
- [発信者情報（Caller Information）] 領域の [発信者名（Caller Name）] フィールドを設定すると、個々のデバイスの表示名がオーバーライドされます。

Cisco VCS での表示名のプロビジョニング

Cisco VCS で表示名をプロビジョニングする方法は 2 通りあります。

1 番目の方法では、FindMe テンプレートを使用して表示名をプロビジョニングします。この方法は、個々のユーザをプロビジョニングする場合に使用されます。各テンプレートには、個々のユーザの詳細情報（表示面など）が含まれています。

2 番目の方法では、直接管理方式で表示名をプロビジョニングします。この方法は、会議室エンドポイントをプロビジョニングする場合に使用されます。つまり、各会議室エンドポイントの表示名は、エンドポイント自体で個々にプロビジョニングされます。

FindMe

FindMe とは、ユーザが各自のユーザ ID に対するコールを受信したときに、どのビデオ/音声デバイスが呼出音を鳴らすかを指定できるようにする Cisco TMSPE 機能です。このため、1 つの ID を使用して、その ID に関連付けられている複数デバイスに到達することができます。

FindMe では、管理者は FindMe アカウントとプロビジョニング テンプレートを使用してユーザをプロビジョニングします。プロビジョニング テンプレートには表示名などの属性が含まれています。ユーザの新規追加またはインポートを、AD または LDAP を使用して実行できます。

FindMe の詳細については、『Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide』の「Deploying FindMe」を参照してください。

Cisco VCS ユーザの発信者 ID 表示名の設定

ここでは、Cisco VCS FindMe ユーザの表示名を手動で設定する方法を説明します。

（注） 多数のユーザを処理する場合、Active Directory または LDAP を使用してユーザの詳細情報をインポートすることを推奨します。この方法では、ユーザの表示名が自動的にインポートおよび設定されます。

はじめる前に

Cisco TMSPE をインストールしてプロビジョニングしていることを確認します。『Cisco TelePresence Management Suite Provisioning Extension with Cisco VCS Deployment Guide』の「Configuring Cisco VCS for provisioning」、「Installing Cisco TMSPE」および「Setting up users and provisioning」を参照してください。

手順

ステップ 1 Cisco TMS にログインして、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動します。

ステップ 2 [ユーザ設定（User Settings）] ペインで [編集（Edit）] をクリックします。[ユーザ設定（User Settings）] ダイアログボックスが開きます。
[表示名（Display Name）] フィールドに、ユーザの名と姓を入力します。注：LDAP を使用してユーザがインポートされている場合、表示名はすでにユーザに関連付けられています。

会議室の発信者 ID 表示名の設定

手順

ステップ 1 Cisco TMS にログインして、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動します。

ステップ 2 ナビゲータで、ウィンドウの左側にあるパネルから更新する会議室を選択します。

ステップ 3 設定するエンドポイントのアドレスを選択します。これにより、選択したエンドポイントのユーザ インターフェイスが表示されます。

ステップ 4 [設定（Configuration）] > [システム設定（System Configuration）] を選択し、ウィンドウの左側にある検索フィールドを使用して「display」という単語を検索します。

ステップ 5 [プロファイル1表示名（Profile 1 DisplayName）] フィールドに、表示名を入力します。注：ステップ 4 と 5 は、選択したエンドポイントのモデルによって異なる場合があります。

ステップ 6 [保存（Save）] をクリックします。

第 10 章

Cisco Expressway-E および Cisco VCS Expressway での証明書を設定する

サポートされる証明書

WebEx でサポートされる証明書を発行する公開認証局に対し、証明書署名要求を送信してください。

（注） 自己署名証明書はサポートされません。

WebEx は、特定のルート認証局が発行した証明書をサポートします。証明書プロバイダーに複数のルート認証局があり、その一部が WebEx ではサポートされていないことがあります。次のいずれかのルート認証局（またはその中間認証局のいずれか）から発行される証明書を使用する必要があります。これ以外の場合、Cisco Expressway-E または Cisco VCS Expressway からのコールが WebEx で受け入れられません。

- entrust_ev_ca
- digicert_global_root_ca
- verisign_class_2_public_primary_ca_-_g3
- godaddy_class_2_ca_root_certificate
- Go Daddy Root Certification Authority - G2
- verisign_class_3_public_primary_ca_-_g5
- verisign_class_3_public_primary_ca_-_g3
- dst_root_ca_x3

- verisign_class_3_public_primary_ca_-_g2
- equifax_secure_ca
- entrust_2048_ca

  X7.2 からアップグレードした Cisco VCS Expressway で、entrust_2048_ca により生成される証明書を使用するには、Cisco VCS Expressway の信頼された CA のリストで、Entrust ルート CA 証明書を Entrust から入手可能な最新バージョンに置き換える必要があります。新しい entrust_2048_ca.cer ファイルは、https://www.entrust.net/downloads/root_index.cfm の Entrust Web サイトのルート証明書リストからダウンロードできます。
- verisign_class_1_public_primary_ca_-_g3
- ca_cert_signing_authority
- geotrust_global_ca
- GlobalSign Root R1

（注） GlobalSign Root 証明書には、R2 または R3 が（将来的にはその他も）割り当てられている可能性があります。これらのいずれかが割り当てられている場合は、証明書のキーを R1 に更新する必要があります。支援が必要な場合は、GlobalSign に連絡してください。

- thawte_primary_root_ca
- geotrust_primary_ca
- addtrust_external_ca_root

このリストは、時間の経過に伴い変更されることがあります。最新の情報については、WebEx に問い合わせるか、または次のリンク先の情報を確認してください。 https://cisco-support.webex.com/guest/articles/en_US/Usability_FAQs/WBX83490/myr=false

注意 Cisco VCS Expressway ではワイルドカード証明書はサポートされていません。

証明書設定タスク

ご使用の Cisco VCS Expressway または Cisco Expressway-E のバージョンによって、信頼された CA 証明書リストの設定方法が決定します。

手順

	コマンドまたはアクション	目的
ステップ 1	証明書署名要求（CSR）の生成, （107 ページ）	
ステップ 2	SSL サーバ証明書のインストール, （108 ページ）	SSL サーバの証明書を Cisco Expressway-E または Cisco VCS Expressway にインストールするには、次の手順を使用します。
ステップ 3	信頼された CA リストの設定, （109 ページ）	ご使用の Cisco VCS Expressway または Cisco Expressway-E のバージョンによって、信頼された CA 証明書リストの設定方法が決定します。このセクションでは、Cisco VCS Expressway をアップグレードした場合、または新たに Cisco VCS Expressway または Cisco Expressway-E をインストールした場合の手順を提供します。

証明書署名要求（CSR）の生成

証明書署名要求を生成するには、次の手順を実行します。

手順

ステップ 1 Cisco Expressway-E または Cisco VCS Expressway で、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] に移動します。

ステップ 2 [CSR の作成（Generate CSR）] をクリックします。

ステップ 3 CSR に関する必須情報を入力し、[CSR の作成（Generate CSR）] をクリックします。[CSRの作成（Generate CSR）] ボタンをクリックすると、[サーバ証明書（Server Certificate）] ページに、CSR の作成が成功したことを示すメッセージが表示されます。

（注） 秘密キーは CSR 作成プロセスで自動的に生成されます。CSR を破棄するオプションはクリックしないでください。このオプションを使用すると CSR を再生成する必要が生じ、以前に生成された秘密キーが破棄されます。

ステップ 4 CSRプロセスを完了し、サポートされる公開認証局（CA）から署名付き証明書を受信するには、[ダウンロード（Download）] をクリックして CSR をダウンロードする必要があります。

（注） ほとんどの認証局は、PKCS#10 要求形式の CSR を提供するよう要求します。

ステップ 5 公開 CA に CSR を送信します。

（注） 公開 CA から提供される SSL サーバ証明書に、サーバとクライアントの両方の認証キーが含まれていることを確認してください。

公開 CA から SSL サーバ証明書を受け取ったら、Cisco Expressway-E または Cisco VCS Expressway にその証明書をインストールできます。

SSL サーバ証明書のインストール

SSL サーバの証明書を Cisco Expressway-E または Cisco VCS Expressway にインストールするには、次の手順を使用します。

はじめる前に

Cisco Expressway-E または Cisco VCS Expressway にサーバ証明書をインストールする前に、証明書が .PEM 形式であることを確認してください。ユーザが受信した証明書が .CER 形式の場合、この証明書を .PEM ファイルに変換するには、ファイル拡張子を .PEM に変更するだけです。

注意 サーバ証明書は、ルート CA 証明書または中間 CA 証明書とともにスタックすることはできません。

手順

ステップ 1 （推奨）メモ帳などのテキスト エディタ アプリケーションでサーバ証明書を開き、1 つの証明書が表示されること（Begin Certificate と End Certificate で囲まれていること）を確認します。
また、サーバ証明書を .CER ファイルとして開き、この証明書の有効性を確認することもできます。[発行先（Issued to）] フィールドが Cisco Expressway-E または Cisco VCS Expressway サーバのものであることを確認する必要があります。

ヒント 証明書の発行元 CA が中間 CA を使用しているか、またはルート CA からの証明書を発行および署名しているかを書きとめておくと役立ちます。中間 CA が関連している場合は、信頼された CA 証明書に中間 CA 証明書を「スタック」するか、追加する必要があります。

ステップ 2 Cisco Expressway-E または Cisco VCS Expressway で、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] に移動します。

ステップ 3 [参照（Browse）] をクリックし、公開 CA から受信したサーバ証明書を選択し、[開く（Open）] をクリックします。

（注） サーバ証明書は、.PEM 証明書形式で Expressway にロードする必要があります。

ステップ 4 [サーバ証明書データをアップロード（Upload server certificate data）] をクリックします。
サーバ証明書をアップロードすると、ファイルがアップロードされたことを通知するメッセージがページ上部に表示されます。

信頼された CA リストの設定

ご使用の Cisco VCS Expressway または Cisco Expressway-E のバージョンによって、信頼された CA 証明書リストの設定方法が決定します。

手順

	コマンドまたはアクション	目的
ステップ 1	中間 CA 証明書のスタック，（109 ページ）	場合によっては、ルート CA が中間 CA を使用して証明書を発行することがあります。サーバ証明書が中間 CA によって発行される場合、中間 CA 証明書をデフォルトの信頼された CA リストに追加する必要があります。 この手順は、Cisco VCS Expressway X7.2.3 だけに適用されます。
ステップ 2	アップグレードでの信頼された CA 証明書リストの設定タスク，（111 ページ）	X7.2.3 から X8.5 にアップグレードした Cisco VCS Expressway では、X7.2.3 の信頼された CA 証明書リストが維持されます。この項の手順を使用して、信頼された証明書のリストをリセットするか、または、中間 CA 証明書を追加します。
ステップ 3	新規インストールでの信頼された CA 証明書リストの設定タスク，（114 ページ）	新規にインストールした Cisco Expressway-E または Cisco VCS Expressway X8.5 を使用する場合は、各自の信頼された CA 証明書リストをロードする必要があります。デフォルトでは、デフォルトの信頼された CA 証明書リストには証明書が含まれていないためです。 また、WebEx クラウドが使用するルート証明書（DST Root CA X3）を、Cisco Expressway-E または Cisco VCS Expressway X8.5 のデフォルトの信頼された CA 証明書リストに追加する必要があります。

中間 CA 証明書のスタック

Cisco VCS Expressway X7.2.3 で次の手順を使用します。

場合によっては、ルート CA が中間 CA を使用して証明書を発行することがあります。サーバ証明書が中間 CA によって発行される場合、中間 CA 証明書をデフォルトの信頼された CA リストに追加する必要があります。

ロードする必要がある中間証明書とルート証明書が公開 CA から提供されない場合、これらの証明書をサーバ証明書から取得できます。場合によっては、これは確実に正しい中間 CA 証明書をスタックできるより適切な方法です。

手順

ステップ 1 サーバ証明書を .CER ファイルとして開きます。

ステップ 2 [証明のパス（Certification Path）] タブをクリックし、[中間証明書（Intermediate Certificate）] をダブルクリックします。
これにより、別の証明書ビューアが開き、中間 CA 証明書が表示されます。

ステップ 3 [発行先（Issued to）] フィールドに、中間 CA の名前が表示されていることを確認します。

ステップ 4 [詳細（Details）] タブをクリックし、次に [ファイルにコピー...（Copy to File…）] をクリックします。
[証明書のエクスポートウィザードの開始（Welcome to the Certificate Export Wizard）] が表示されます。

ステップ 5 [Next] をクリックします。

ステップ 6 [エクスポート ファイルの形式（Export File Format）] として [Base 64 encoded X.509 (.CER)（Base-64 encoded X.509 (.CER)）] を選択し、[次へ（Next）] をクリックします。

ステップ 7 ファイルの名前を指定し、[次へ（Next）] をクリックし、[完了（Finish）] をクリックします。

ステップ 8 Cisco VCS Expressway からデフォルトの信頼された CA リストをコピーするため、[メンテナンス（Maintenance）] > [証明書の管理（Certificate management）] > [信頼されたCA証明書（Trusted CA certificate）] に進み、[CA証明書を表示（Show CA Certificate）] をクリックします。ウィンドウが開いたら、すべての内容を選択します。

ステップ 9 メモ帳などのテキスト編集アプリケーションに、この内容を貼り付けます。

ステップ 10 テキスト編集アプリケーションの新しいウィンドウで intermediate.cer ファイルを開き、その内容をクリップボードにコピーします。

ステップ 11 デフォルトの信頼された CA リストの内容が含まれているテキスト ファイル内で、既存のルート CA 証明書を検索します。

ステップ 12 ルート証明書の上に中間 CA 証明書を貼り付けます。

ステップ 13 このテキスト ファイルを .PEM ファイル（例：NewDefaultCA.pem）として保存します。
（注） ルート CA がデフォルトの信頼された CA リストにない場合は、中間 CA 証明書のスタック手順に従ってください。

ステップ 14 [参照（Browse）] をクリックし、新しく作成/スタックされた信頼された CA のリストを見つけ、[開く（Open）] をクリックします。

ステップ 15 [CA 証明書のアップロード（Upload CA certificate）] をクリックします。
これで Cisco VCS Expressway X7.2.3 での証明書の設定が完了しました。

次の作業

クライアント/サーバ証明書の設定方法の詳細（セキュリティ用語や定義の情報を含む）については、次の URL にある『*Certificate creation and use with Cisco VCS Deployment Guide*』を参照してください。

https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Certificate_Creation_and_Use_Deployment_Guide_X7-2.pdf

アップグレードでの信頼された CA 証明書リストの設定タスク

X7.2.3 から X8.5 にアップグレードした Cisco VCS Expressway では、X7.2.3 の信頼された CA 証明書リストが維持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	信頼された CA 証明書リストのリセット，（111 ページ）	デフォルトの信頼された CA 証明書リストが現在使用されていない場合は、これをデフォルトの CA 証明書にリセットすることを推奨します。これにより、必要な証明書があることを確認する作業が容易になります。
ステップ 2	Cisco Expressway-E または VCS Expressway X8.5 における証明書の更新，（112 ページ）	
ステップ 3	中間証明書の CA 証明書を追加する，（113 ページ）	場合によっては、ルート CA が中間 CA を使用して証明書を発行することがあります。サーバ証明書が中間 CA によって発行される場合、中間 CA 証明書をデフォルトの信頼された CA リストに追加する必要があります。

信頼された CA 証明書リストのリセット

X7.2.3 から X8.15 にアップグレードした Cisco VCS Expressway で次の手順を使用します。

デフォルトの信頼された CA 証明書リストが現在使用されていない場合は、これをデフォルトの CA 証明書にリセットすることを推奨します。これにより、必要な証明書があることを確認する作業が容易になります。

Cisco VCS Expressway X8.5 で信頼された CA 証明書リストをリセットするには、次の手順を実行します。

手順

ステップ 1 [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] に進み、[デフォルト CA 証明書にリセットする（Reset to default CA certificate）] をクリックします。

（注） Cisco VCS Expressway では、クライアント/サーバ SSL ハンドシェイク時にサーバから渡されるサーバ証明書の証明書発行元を信頼する必要があります（この場合、サーバは WebEx クラウドの SIP プロキシです）。

Cisco VCS Expressway のデフォルトの信頼された CA 証明書リストには、クラウドが示すサーバ証明書のパブリック ルート CA 証明書がすでに含まれています。WebEx クラウドのルート CA は、Cisco SSCA2 の中間 CA を含む DST ルート CA X3 です。

サーバ証明書の発行元が（中間 CA ではなく）ルート CA である場合、ルート証明書はデフォルトの信頼された CA リストに含まれている可能性があります。

ステップ 2 ベスト プラクティスは、適切なルート証明書が存在していることを確認することです。これを確認するには、[すべて表示（PEM ファイル）（Show all (PEM file)）] をクリックします。
この操作により、現在 Cisco VCS Expressway にロードされているデフォルトの信頼された CA 証明書リストが、新しいウィンドウに表示されます。

ステップ 3 サーバ証明書の発行元ルート CA を見つけます。
サーバ証明書の発行元が中間 CA ではなく最上位ルート CA である場合、デフォルトの信頼された CA 証明書リストに有効な CA 証明書が含まれているため、Cisco VCS Expressway での証明書の設定はこれで完了です。

サーバ証明書の発行元が中間 CA である場合、またはサーバ証明書の発行元である最上位ルート CA の証明書が信頼された証明書リストに含まれていない場合は、その証明書をリストに追加します。この手順については次の項で説明します。

Cisco Expressway-E または VCS Expressway X8.5 における証明書の更新

Cisco Expressway-E または Cisco VCS Expressway では、WebEx クラウドとのクライアント/サーバ SSL ハンドシェイク時にサーバから渡されたサーバ証明書の発行元を信頼する必要があります。このためには、Cisco Expressway-E または Cisco VCS Expressway で、信頼された CA のリストにこれらの証明書を追加する必要があります。信頼された CA 証明書リストにこれらの証明書を追加するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのリンクに移動し、表示される証明書の内容をコピーし、個々のテキスト ファイルに貼り付け、各テキスト ファイルをファイル拡張子 .PEM で保存します。

a) VeriSign Class 3 Public Primary CA
b) VeriSign Class 3 Primary CA - G5
c) VeriSign Class 3 Public Primary CA - G3
d) QuoVadis Root CA 2

たとえば、1 番目の CA の場合は次のようになります。
Class-3-Public-Primary-Certification-Authority.pem

注：証明書失効を使用していないか、または VCS-Expressway または Expressway-E で証明書失効ポリシーがアクティブではない場合は、ステップ 3 にスキップします。

ステップ 2 「自動」証明書失効を使用している場合は、この機能を一時的に無効にします。

a) VCS/Expressway で、[メンテナンス（Maintenance）]>[セキュリティ証明書（Security certificates）] > [CRL 管理（CRL Management）] に進みます。

b) [自動 CRL 更新（automatic CRL updates）] を [無効（disabled）] に設定します。

注：失効した証明書のリストを手動でアップロードすることで、証明書失効を「手動」で行う場合は、次のステップ 3 を完了するまでは、認証局からの 2015 年 2 月 1 日以降の日付の新しいリストをインストールしないでください。

ステップ 3 Cisco Expressway-E または Cisco VCS Expressway X8.5 で、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] に進みます。

ステップ 4 [参照（Browse）] をクリックし、ステップ a で保存した最初の証明書を選択し、[開く（Open）] をクリックします。

ステップ 5 [CA 証明書の追加（Append CA certificate）] をクリックします。

ステップ 6 ステップ 1 で保存した他の証明書に対してステップ 4 と 5 を繰り返します。

ステップ 7 ステップ 2 で「自動」証明書失効を無効にした場合は、これを再び有効にします。

VeriSign および *QuoVadis* の証明書の有効期限

証明書	期限日（**Expiration Date**）
VeriSign Class 3 Public Primary CA	水曜日、2028 年 8 年 02 日 3:59:59 PM
VeriSign Class 3 Primary CA - G5	水曜日、2036年7月16日
VeriSign Class 3 Public Primary CA - G3	水曜日、2036 年 7 年 16 日 3:59:59 PM
QuoVadis Root CA 2	2031年11月24日

中間証明書の CA 証明書を追加する

Cisco VCS Expressway X8.15 以降に、中間証明書の CA 証明書を追加するには、次の手順を使用します。

場合によっては、ルート CA が中間 CA を使用して証明書を発行することがあります。

サーバ証明書が中間 CA によって発行される場合、中間 CA 証明書をデフォルトの信頼された CA リストに追加する必要があります。

ロードする必要がある中間証明書とルート証明書が公開 CA から提供されない場合、これらの証明書をサーバ証明書から取得できます。場合によっては、これは確実に正しい中間 CA 証明書をスタックできるより適切な方法です。

手順

ステップ 1 サーバ証明書を .CER ファイルとして開きます。

ステップ 2 [証明のパス（Certification Path）] タブをクリックします。

ステップ 3 [中間証明書（Intermediate Certificate）] をダブルクリックします。
これにより、別の証明書ビューアが開き、中間 CA 証明書が表示されます。

ステップ 4 [発行先（Issued to）] フィールドに、中間 CA の名前が表示されていることを確認します。

ステップ 5 [詳細（Details）] タブをクリックし、次に [ファイルにコピー...（Copy to File…）] をクリックします。
[証明書のエクスポートウィザードの開始（Welcome to the Certificate Export Wizard）] が表示されます。

ステップ 6 [Next] をクリックします。

ステップ 7 [エクスポート ファイル形式（Export File Format）] として [Base-64 エンコード X.509（.CER）（Base-64 encoded X.509 (.CER)）] を選択し、[次へ（Next）] をクリックします。

ステップ 8 ファイルの名前を指定し、[次へ（Next）] をクリックし、[完了（Finish）] をクリックします。

ステップ 9 中間 CA 証明書の拡張子を、.cer から .pem に変更します。例：intermediate.pem

ステップ 10 Cisco VCS Expressway X8.5 で、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] の順に進みます。

ステップ 11 [参照（Browse）] をクリックし、中間 CA 証明書を見つけ、[開く（Open）] をクリックします。

ステップ 12 [CA証明書の追加（Append CA certificate）] をクリックします。
これで Cisco VCS Expressway X8.5 での証明書の設定が完了しました。

次の作業

クライアント/サーバ証明書の設定方法の詳細（セキュリティ用語や定義の情報を含む）については、次の URL にある『*Cisco VCS Certificate Creation and Use Deployment Guide（X8.1）*』を参照してください。

- http://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/X8-1/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-1.pdf
- http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-5.pdf

新規インストールでの信頼された CA 証明書リストの設定タスク

新規にインストールした Cisco Expressway-E または Cisco VCS Expressway X8.5 を使用する場合は、各自の信頼された CA 証明書リストをロードする必要があります。デフォルトでは、デフォルトの信頼された CA 証明書リストには証明書が含まれていないためです。

また、WebEx クラウドが使用するルート証明書（DST Root CA X3）を、Cisco Expressway-E または Cisco VCS Expressway X8.5 のデフォルトの信頼された CA 証明書リストに追加する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	DST ルート証明書を追加する，（115 ページ）	Cisco Expressway-E または Cisco VCS Expressway では、クライアント/サーバ SSL ハンドシェイク時にサーバから渡されるサーバ証明書の証明書発行元（DST Root CA）を信頼する必要があります（この場合、サーバは WebEx クラウドの SIP プロキシです）。
ステップ 2	Cisco Expressway-E または VCS Expressway X8.5 における証明書の更新，（112 ページ）	
ステップ 3	ルート証明書または中間 CA 証明書の追加，（117 ページ）	WebEx クラウドが Cisco Expressway-E または Cisco VCS Expressway サーバ証明書を信頼するためには、サーバ証明書の発行元 CA のルート CA 証明書または中間 CA 証明書を追加する必要があります。

DST ルート証明書を追加する

Cisco Expressway-E または Cisco VCS Expressway では、クライアント/サーバ SSL ハンドシェイク時にサーバから渡されるサーバ証明書の証明書発行元（DST Root CA）を信頼する必要があります（この場合、サーバは WebEx クラウドの SIP プロキシです）。

Cisco Expressway-E または Cisco VCS Expressway X8.1 で信頼された CA 証明書リストに DST ルート証明書を追加するには、次の手順を実行します。

手順

ステップ 1 http://www.identrust.com/doc/SSLTrustIDCAA5_DSTCAX3.p7b にアクセスします。

DST Root 証明書の内容を示すページが表示されます。ページの先頭は「-----Begin Certificate-----」です。

ステップ 2 ページの内容全体を選択してコピーします。

ステップ 3 コンピュータのメモ帳などのテキストエディタを開き、DST Root 証明書の内容を貼り付けます。

ステップ 4 拡張子が .PEM のテキスト ファイルに保存します。例：dst_root_ca.pem.

ステップ 5 Cisco Expressway-E または Cisco VCS Expressway X8.5 で、[メンテナンス（Maintenance）]>[セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] の順に進みます。

ステップ 6 [参照（Browse）]をクリックし、ステップ 4 で保存した DST ルート証明書を選択し、[開く（Open）]をクリックします。

ステップ 7 [CA証明書の追加（Append CA certificate）] をクリックします。

Cisco Expressway-E または VCS Expressway X8.5 における証明書の更新

Cisco Expressway-E または Cisco VCS Expressway では、WebEx クラウドとのクライアント/サーバ SSL ハンドシェイク時にサーバから渡されたサーバ証明書の発行元を信頼する必要があります。このためには、Cisco Expressway-E または Cisco VCS Expressway で、信頼された CA のリストにこれらの証明書を追加する必要があります。信頼された CA 証明書リストにこれらの証明書を追加するには、次の手順を実行します。

手順

ステップ 1 次のいずれかのリンクに移動し、表示される証明書の内容をコピーし、個々のテキスト ファイルに貼り付け、各テキスト ファイルをファイル拡張子 .PEM で保存します。

a) VeriSign Class 3 Public Primary CA
b) VeriSign Class 3 Primary CA - G5
c) VeriSign Class 3 Public Primary CA - G3
d) QuoVadis Root CA 2

たとえば、1 番目の CA の場合は次のようになります。
Class-3-Public-Primary-Certification-Authority.pem

注：証明書失効を使用していないか、または VCS-Expressway または Expressway-E で証明書失効ポリシーがアクティブではない場合は、ステップ 3 にスキップします。

ステップ 2 「自動」証明書失効を使用している場合は、この機能を一時的に無効にします。

a) VCS/Expressway で、[メンテナンス（Maintenance）]>[セキュリティ証明書（Security certificates）] > [CRL 管理（CRL Management）] に進みます。
b) [自動 CRL 更新（automatic CRL updates）] を [無効（disabled）] に設定します。

注：失効した証明書のリストを手動でアップロードすることで、証明書失効を「手動」で行う場合は、次のステップ 3 を完了するまでは、認証局からの 2015 年 2 月 1 日以降の日付の新しいリストをインストールしないでください。

ステップ 3 Cisco Expressway-E または Cisco VCS Expressway X8.5 で、[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] に進みます。

ステップ 4 [参照（Browse）] をクリックし、ステップ a で保存した最初の証明書を選択し、[開く（Open）] をクリックします。

ステップ 5 [CA 証明書の追加（Append CA certificate）] をクリックします。

ステップ 6 ステップ 1 で保存した他の証明書に対してステップ 4 と 5 を繰り返します。

ステップ 7 ステップ 2 で「自動」証明書失効を無効にした場合は、これを再び有効にします。

VeriSign および *QuoVadis* の証明書の有効期限

証明書	期限日（**Expiration Date**）
VeriSign Class 3 Public Primary CA	水曜日、2028 年 8 年 02 日 3:59:59 PM
VeriSign Class 3 Primary CA - G5	水曜日、2036年7月16日
VeriSign Class 3 Public Primary CA - G3	水曜日、2036 年 7 年 16 日 3:59:59 PM
QuoVadis Root CA 2	2031年11月24日

ルート証明書または中間 CA 証明書の追加

WebEx クラウドが Cisco Expressway-E または Cisco VCS Expressway サーバ証明書を信頼するためには、サーバ証明書の発行元 CA のルート CA 証明書または中間 CA 証明書を追加する必要があります。

ロードする必要がある中間証明書またはルート証明書が公開 CA から提供されない場合、これらの証明書をサーバ証明書から取得できます。場合によっては、これは確実に正しい中間 CA 証明書をスタックできるより適切な方法です。

Cisco Expressway-E または Cisco VCS Expressway X8.5 にルート CA または中間 CA を追加するには、次の手順を実行します。

ロードする必要がある中間証明書とルート証明書が公開 CA から提供されない場合、これらの証明書をサーバ証明書から取得できます。場合によっては、これは確実に正しい中間 CA 証明書をスタックできるより適切な方法です。

手順

ステップ 1 サーバ証明書を .CER ファイルとして開きます。

ステップ 2 [証明のパス（Certification Path）] タブをクリックします。

（注） ここに示すサーバ証明書の例は、中間CAにより発行されたものです。証明書の発行元がルート CA の場合、2 つの証明書（ルート証明書とサーバ証明書）だけが表示されます。

ステップ 3 CA 証明書を開きます。

- 証明書の発行元がルート CA の場合は、[ルート CA 証明書（Root CA Certificate）] をダブルクリックします。
- 証明書の発行元が中間 CA の場合は、[中間証明書（Intermediate Certificate）] をダブルクリックします。

これにより、別の証明書ビューアが開き、CA 証明書が表示されます。

ステップ 4 [発行先（Issued to）] フィールドに、ルート CA または中間 CA の名前が表示されていることを確認します。

ステップ 5 [詳細（Details）] タブをクリックし、次に [ファイルにコピー...（Copy to File…）] をクリックします。
[証明書のエクスポートウィザードの開始（Welcome to the Certificate Export Wizard）] が表示されます。

ステップ 6 [Next] をクリックします。

ステップ 7 [エクスポート ファイルの形式（Export File Format）] として [Base 64 encoded X.509 (.CER)（Base-64 encoded X.509 (.CER)）] を選択し、[次へ（Next）] をクリックします。

ステップ 8 ファイルの名前を指定し、[次へ（Next）] をクリックし、[完了（Finish）] をクリックします。

ステップ 9 ルート CA 証明書または中間 CA 証明書の拡張子を、.cer から .pem に変更します。例：root.pm または intermediate.pem

ステップ 10 Cisco Expressway-E または Cisco VCS Expressway X8.1 で、[メンテナンス（Maintenance）]>[セキュリティ証明書（Security certificates）] > [信頼された CA 証明書（Trusted CA certificate）] の順に進みます。

ステップ 11 [参照（Browse）] をクリックし、ルートまたは中間CA証明書を見つけ、[開く（Open）] をクリックします。

ステップ 12 [CA証明書の追加（Append CA certificate）] をクリックします。
Cisco Expressway-E または Cisco VCS Expressway X8.5 での証明書設定が完了します。

次の作業

クライアント/サーバ証明書の設定方法の詳細（セキュリティ用語や定義の情報を含む）については、次の URL にある『*Cisco VCS Certificate Creation and Use Deployment Guide*（*X8.5*）』を参照してください。

- http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Certificate-Creation-and-Use-Deployment-Guide-X8-5.pdf

第 11 章

Cisco TelePresence Management Suite を設定する

前提条件

- Cisco TMS ソフトウェア リリース 14.6 が必要です（15.0 を推奨します）。
- Microsoft Outlook を使用して会議をスケジュールする場合は、Cisco TMSXE ソフトウェア リリース 4.1 以降が必要です（5.0 を推奨します）。

Microsoft Outlook を使用したスケジュールの場合、2 つのオプションがあります。

- Microsoft Outlook 用の WebEx 生産性向上ツール プラグイン
- WebEx Scheduling Mailbox の使用

- Smart Scheduler を使用して会議をスケジュールする場合は、Cisco TMSPE ソフトウェア リリース 1.4 以降が必要です（1.5 を推奨します）
- MCU から WebEx へのコールでは SIP だけがサポートされています。SIP に対して次の設定を行う必要があります。

- Cisco TMS：CMR ハイブリッド会議に使用する各 MCU で、[Cisco TMS スケジュール設定（Cisco TMS Scheduling Settings）] の [着信および発信 SIP URI ダイヤルを許可する（Allow Incoming and Outgoing SIP URI Dialing）] を [はい（Yes）] に設定する必要があります。
- MCU および TelePresence Server についての詳細は、Cisco MCU および TelePresence Server を設定する，（79 ページ） を参照してください。

- WebEx Meeting Center WBS30 で新しい WebEx 生産性向上ツール機能を取得するには、次のコンポーネントが必要です：TMS 15.0
  - TMSXE 5.0

詳細については、最新の CMR Hybrid リリース ノートを参照してください。

Cisco TMS での Cisco WebEx 機能の設定

Cisco TMS で Cisco WebEx 機能を設定するには、次の手順を実行します。

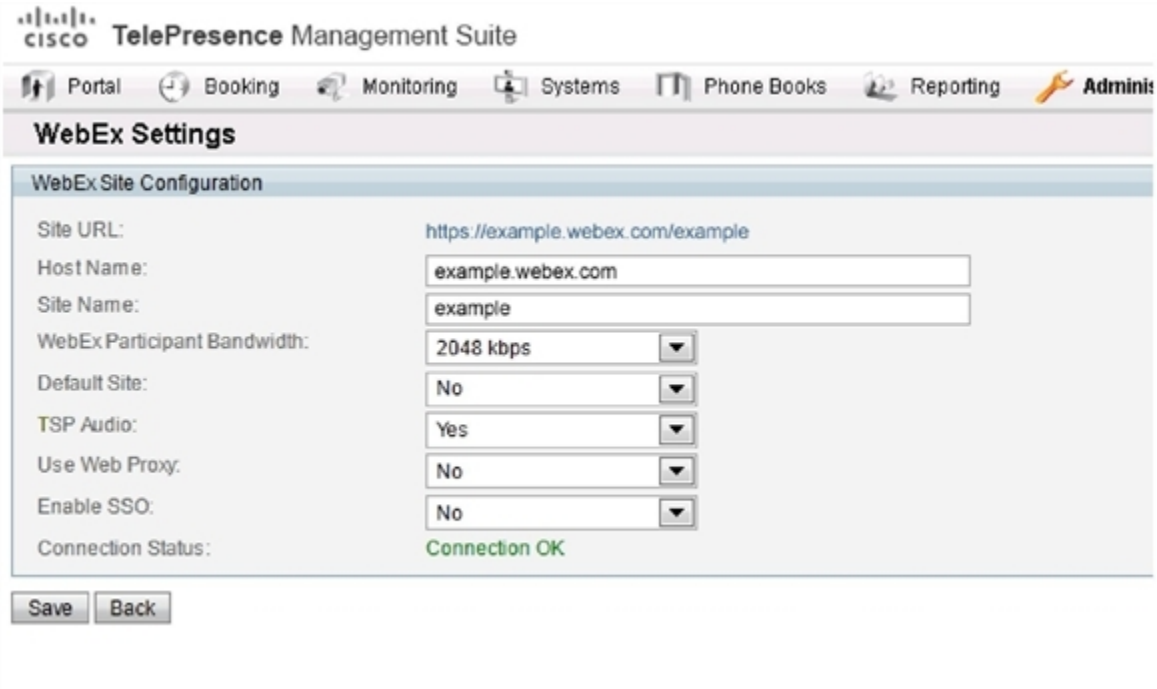
手順

ステップ 1 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [WebEx の設定（WebEx Settings）] に進みます。
[WebEx の設定（WebEx Settings）] ページが表示されます。

ステップ 2 [サイトの追加（Add Site）] をクリックします。

[WebEx サイトの設定（WebEx Site Configuration）] ページが表示されます。

図 *8*：*WebEx* サイトの設定



ステップ 3 [ホスト名（Host Name）] フィールドに、WebEx サイトのホスト名を入力します。

ステップ 4 [サイト名（Site Name）] フィールドに、WebEx サイト名を作成します。

（注） サイト URL の形式は `https://[HostName]/[SiteName]` でなければなりません。たとえば、https://example.webex.com/example などです。

ステップ 5 [WebEx 参加者の帯域幅（WebEx Participant Bandwidth）] で、MCU から WebEx への会議あたりの許容最大帯域幅を選択します。

（注） MCU と VCS では帯域幅が制限されていることがあります。

ステップ 6 （オプション）デフォルト サイト。1 つ以上の WebEx サイトがすでに存在している場合は、[はい（Yes）] を選択してこのサイトをデフォルト WebEx サイトとして選択できます。

（注） 新しいユーザは、WebEx を使用した会議を初めてスケジュールするときにデフォルト サイトを使用するように、自動的に設定されます。

ステップ 7 TSP または PSTN 音声を使用する場合は、[TSP音声（TSP Audio）] で [はい（Yes）] を選択します。

（注） [TSP 音声（TSP Audio）] で [はい（Yes）] を選択すると、Cisco TMS では TSP 音声だけが使用されます。SIP 音声は機能しません。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 [WebEx 構成（WebEx Configuration）] セクションで、次の手順を実行します：[Webex 有効（WebEx Enabled）] で [はい（Yes）] を選択します。

a) [WebExをすべての会議に追加する（Add WebEx To All Conferences）] で [はい（Yes）] を選択します。
b) [保存（Save）] をクリックします。

Cisco TMS の WebEx ユーザの設定

Cisco TMS を使用して会議をスケジュールするには、サーバが信頼するように設定したユーザ名とパスワードが必要になります。

Cisco TMS は次のアカウントを認証します。

- Cisco TMS がインストールされている Windows Server のローカル アカウント
- サーバがドメイン メンバーシップと Active Directory（AD）を介して信頼しているアカウント

Cisco TMS に正常にログインした各ユーザに対し、ユーザ名に基づいて新しいユーザ プロファイルが作成され、各自のプロファイルに情報を入力するように促されます。既存の Windows または AD のユーザ パスワードが使用されますが、これらのパスワードは Cisco TMS には保存されません。ユーザの Windows または AD のパスワードが変更された場合は、ユーザは Cisco TMS にログインするときに、変更後のパスワードを使用する必要があります。

WebEx 対応会議のスケジュールに関するユーザ要件

Cisco TMS を使用して WebEx 対応会議をスケジュールするには、Cisco TMSユーザは Cisco TMS ユーザ プロファイルに保存された次のものが必要です。

- WebEx ユーザ名
- WebEx パスワード（シングル サインオンが有効ではない場合）
- アカウントを持っている WebEx サイト

（注） この WebEx サイトは、Cisco TMS での Cisco WebEx 機能の設定, （120 ページ）で説明するように、Cisco TMS にも追加する必要があります。

WebEx スケジュール用に Cisco TMS ユーザ アカウントを有効にする方法は 3 通りあります。

- 管理者が Cisco TMS ユーザ プロファイルを編集する。

詳細については、次を参照してください。Cisco TMS での Cisco CMR Hybrid ユーザの設定, （124 ページ）

- Cisco TMS ユーザが Cisco TMS にログインし、Cisco TMS Web UI の左下隅に表示される各自のユーザ名をクリックして、プロファイルを編集する。
- 管理者が [Active Directoryのユーザ情報の参照（Lookup User Information from Active Directory）] と [Active DirectoryからWebExユーザ名を取得（Get WebEx Username from Active Directory）]、およびオプションで [シングルサインオン(SSO)（Single Sign On (SSO)）] を有効にする。

Active Directory 参照機能を有効にするメリットとして、WebEx ユーザ名を含むユーザ アカウント情報が、各新規 Cisco TMS ユーザに自動的に追加される点があります。管理者またはユーザが WebExパスワードを追加する必要がありますが、シングル サインオンを有効にする場合は、WebExパスワードは不要です。Active Directory 機能とシングル サインオン機能が有効であり、Cisco TMS で複数の WebEx サイトが有効になっている場合は、ユーザに対してその WebEx サイトだけを選択する必要があります。WebExサイトが 1 つだけの場合、Cisco TMS はそのサイトを使用します。複数のサイトが設定されている場合は、ユーザの Cisco TMS プロファイルが編集されてデフォルト以外の WebEx サイトが指定されている場合を除き、Cisco TMS では、「デフォルト」として指定されている WebEx サイトが自動的に選択されます。

詳細については、Active Directory からの自動ユーザ参照の設定, （123 ページ）および次を参照してください。 Cisco TMS のシングル サインオンの設定, （132 ページ）

Active Directory からの自動ユーザ参照の設定

Active Directory（AD）を使用する場合は、ユーザ プロファイル情報が自動的に入力されるように Cisco TMS を設定できます。この機能を有効にすると、ユーザが初めて Cisco TMS にアクセスするときにユーザの詳細情報が自動的にインポートされ、定期的に同期されます。WebEx ユーザ名に Active Directory のフィールド（AD ユーザ名または電子メール アドレスなど）を使用する場合、[WebEx の設定（WebEx Settings）] ページで [Active Directory から WebEx ユーザ名を取得する（Get WebEx Username from Active Directory）] 機能を有効にして、Cisco TMS が WebEx ユーザ名をインポートするように設定できます。

Cisco TMS での Active Directory 参照

Active Directory 参照により、Cisco TMS にユーザ情報が自動的にインポートされ、更新されます。オプションで、Cisco TMS では WebEx ユーザ名もインポートできます。

AD 参照を有効にすることで、WebEx と Cisco TMS ではユーザ情報が一定間隔で同期されます。これにより、各 WebExユーザが会議の予約または会議への参加時に入力する必要があるのはパスワードだけになり、ユーザ名の入力は必要なくなります。

AD 参照を設定しない場合、ユーザは Cisco TMS と WebEx 間の通信でユーザとパスワードを入力する必要があります。

Active Directory 参照を設定するには、次の手順を実行します。

手順

ステップ 1 [管理ツール（Administrative Tools）] > [構成（Configuration）] > [ネットワーク設定（Network Settings）] に進みます。

ステップ 2 [Active Directory] ペインで、[Active Directoryのユーザ情報の参照（Lookup User Information from Active Directory）] を [はい（Yes）] に設定します。

ステップ 3 [Active Directory] ペインのその他のフィールドに情報を入力し、[保存（Save）] をクリックします。

ステップ 4 各フィールドの詳細については、Cisco TMS ヘルプを参照してください。

ステップ 5 [Active DirectoryからWebExユーザ名を取得（Get WebEx Username from Active Directory）] を設定するには、次の手順に従います。

ステップ 6 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [WebEx の設定（WebEx Settings）] に進みます。

ステップ 7 [WebEx設定（WebEx Configuration）] ペインで、[Active DirectoryからWebExユーザ名を取得（Get WebEx Username from Active Directory）] メニューを使用して、WebEx ユーザ名を保存する AD のフィールドを選択します。

ステップ 8 [保存（Save）] をクリックします。
詳細については、Cisco TMS ヘルプを参照してください。

WebEx 予約の仕組み

WebEx 予約が機能するには、予約を実行するユーザの WebEx ユーザ名とパスワードが、そのユーザの Cisco TMS プロファイルで WebEx ユーザ名および WebEx パスワードとして定義されている必要があります。これにより、正しいユーザが WebEx で会議を「所有」しており、ログインして、WebEx 会議を開催できることが保証されます。

WebEx サイトでシングル サインオン（SSO）が有効な場合、WebEx アカウントを持つユーザは Cisco TMS で WebEx 対応会議を予約できます。このとき WebEx パスワードが Cisco TMS ユーザ プロファイルに保存されている必要はありません。SSO が設定されている場合、ユーザが会議を予約すると、Cisco TMS ユーザ プロファイルの WebEx ユーザ名が WebEx サイトに渡され、予約が完了します。SSO の設定方法の詳細については、Cisco TMS のシングル サインオンの設定, （132 ページ）を参照してください。

残りのフィールドへの入力は必須ではありませんが、他の Cisco TMS 機能で使用されます。Active Directory を使用している場合、新規ユーザのこれらのフィールドに自動的に値を取り込むように Cisco TMS を設定できます。

Cisco TMS での Cisco CMR Hybrid ユーザの設定

次の 3 つの条件に該当する場合は、この設定は不要です。

- 「Active Directory からの自動ユーザ参照の設定」（ページ 6-5）の説明に従って、[Active Directory のユーザ情報の参照（Lookup User Information from Active Directory）] と [Active Directory から WebEx ユーザ名を取得（Get WebEx Username from Active Directory）] を有効にしている場合
- シングル サインオンを有効にしている場合（詳細についてはCisco TMS のシングル サインオンの設定, （132 ページ）を参照）。
- ユーザが WebEx 会議のスケジュールにデフォルト WebEx サイトを使用する場合。

Cisco TMS で Cisco CMR Hybrid ユーザを設定するには、次の手順を実行します。

手順

ステップ 1 [管理ツール（Administrative Tools）] > [ユーザ管理（User Administration）] > [ユーザ（Users）] に進みます

ステップ 2 [新規（New）] をクリックして新しいユーザを追加するか、または既存のユーザ名をクリックしてそのユーザのプロファイルに WebEx スケジュール機能を追加し、[編集（Edit）] をクリックします。

ステップ 3 Windows/AD ユーザ名、姓、名、および電子メール アドレスを入力します。

（注） 既存のユーザまたは AD 参照が有効な場合、一部のフィールドにはすでに情報が取り込まれていることがあります。

ステップ 4 [WebExユーザ名（WebEx Username）] に、ユーザの WebEx アカウントのユーザ名を入力します。

ステップ 5 [WebExパスワード（WebEx Password）] に、ユーザの WebEx アカウントのパスワードを入力します。

（注） WebEx サイトが選択されていない場合、デフォルトとして設定されている WebEx サイトが使用されます。

ステップ 6 [WebEx サイト（WebEx Site）] で、ユーザが登録されている WebEx サイトを選択します。

ステップ 7 Cisco TMS ユーザ プロファイルの他の設定を行い、[保存（Save）] をクリックします。

Cisco TMS の MCU および TelePresence Server のポート予約の設定

各スケジュール済み会議のポートを予約するように MCU と TelePresence Server を設定することを推奨します。

この設定を有効にすると、会議に予約されているポートの数が適用されます。この会議の TelePresence 部分で、5 つのポートと 5 人の参加者が TelePresence に接続している場合、会議への招待状が 6 番目の参加者に転送されると、これらの参加者は TelePresense で会議に参加できなくなります。

ポート予約が有効に設定されていない場合、5 つの TelePresence ポートが予約されている会議において、招待状が転送されると、その時点で使用可能なポートの最大数まで追加ユーザが TelePresence で参加できます。これが原因で、別のスケジュール済み会議が失敗することがあります。このため、MCU と TelePresence Server では常にポート予約を有効にしておくことを推奨します。

MCU のポート予約の有効化

MCU のポート予約を有効にするには、Cisco TMS で次の手順を実行します。

手順

ステップ 1 [システム（Systems）] > [ナビゲータ（Navigator）] に移動します。
ステップ 2 MCU を選択します。
ステップ 3 [設定（Settings）] タブをクリックします。
ステップ 4 [拡張設定（Extended Setting）] をクリックします。
ステップ 5 [ポート数を予定参加者の数に制限する（Limit Ports to Number of Scheduled Participants）] メニューを [オン（On）] に設定します。
ステップ 6 [保存（Save）] をクリックします。
ステップ 7 すべての MCU に対してステップ 2 ～ 6 を繰り返します。

TelePresence Server のポート予約の有効化

TelePresence Server のポート予約を有効にするには、Cisco TMS で次の手順を実行します。

手順

ステップ 1 [システム（Systems）] > [ナビゲータ（Navigator）] に移動します。
ステップ 2 TelePresence Server システムを選択します。
ステップ 3 [設定（Settings）] タブをクリックします。
ステップ 4 [拡張設定（Extended Setting）] をクリックします。
ステップ 5 [ポート予約（Port Reservation）] を [オン（On）] に設定します。
ステップ 6 [保存（Save）] をクリックします。
ステップ 7 各 TelePresence Server について、ステップ 2 から 6 を繰り返します。

Cisco TMS での MCU のハイブリッド コンテンツ モードの設定

WebEx を使用した CMR ハイブリッド 会議に使用する MCU が、ハイブリッド コンテンツ モードを使用するように設定する必要があります。ハイブリッドモードでは、受信コンテンツ ストリームがパススルーされ、最高品質が提供されます。また、受信コンテンツ ストリームがデコードされ、これを使用して、パススルー ストリームを受信できないすべてのユーザ（SD エンドポイント）を対象とした 2 番目の解像度が低いストリームが作成されます。このためビデオ ポートが使用されますが、ユーザはトランスコードとパススルーの両方のメリットを得ることができます。

Cisco TMS で MCU のハイブリッド コンテンツ モードを設定するには、次の手順を実行します。

手順

ステップ 1 [システム（Systems）] > [ナビゲータ（Navigator）] に進みます。
ステップ 2 MCU を選択し、[システム設定の編集（Edit system settings）] をクリックします。
ステップ 3 [設定（Settings）] タブで [拡張設定（Extended Settings）] をクリックします。
ステップ 4 [コンテンツモード（Content Mode）] で [ハイブリッド（Hybrid）] を選択し、[保存（Save）] をクリックします。

Cisco TMS でのロビー画面の設定

WebEx を使用した CMR ハイブリッド 会議に使用するすべての TelePresence Server で、ロビー画面を「オン（On）」に設定する必要があります。

Cisco TMS の TelePresence Server でロビー画面を設定するには、次の手順を実行します。

手順

ステップ 1 [システム（Systems）] > [ナビゲータ（Navigator）] に進みます。
ステップ 2 TelePresence Server の名前をクリックします。
ステップ 3 [設定（Settings）] タブをクリックし、[拡張設定（Extended Settings）] をクリックします。
ステップ 4 [会議にロビー画面を使用する（Use Lobby Screen for conferences）] を [オン（On）] に設定し、[保存（Save）] をクリックします。

WebEx Welcome 画面が無効な場合の会議における最初の TelePresence 参加者へのロビー画面の表示

WebEx Welcome 画面が無効な場合、TelePresence Server を使用して会議に最初に参加する TelePresence Server 参加者のユーザ エクスペリエンスは、Cisco TMS での TelePresence Server の [会議にロビー画面を使用する（Use Lobby Screen for conferences）] 設定に応じて異なります。 表 18：WebEx Welcome 画面が無効な場合の最初の TelePresence 参加者に対するロビー画面の表示, （128 ページ）に、さまざまなシナリオで、会議の最初の TelePresence 参加者に表示される内容を示します。最初の TelePresence 参加者に対して黒色の画面が表示されないようにするため、前述の項で説明したとおり、CMR Cloud 会議に使用するすべての TelePresence Server で [会議にロビー画面を使用する（Use Lobby Screen for conferences）] を [はい（Yes）] に設定してください。

表 *18*：*WebEx Welcome* 画面が無効な場合の最初の *TelePresence* 参加者に対するロビー画面の表示

TelePresence Server のロビー画面の設定	CMR ハイブリッド会議か	1 人以上の WebEx 参加者がいるかどうか	WebEx 参加者がカメラに対応しているかどうか	最初の TelePresence 参加者に対して表示される内容
なし	×（TelePresence のみ）	該当なし	該当なし	黒色の画面（1 人以上の他の TelePresence 参加者が参加するまで）
なし	[はい（Yes）]	[いいえ（No）]	該当なし	黒色の画面（1 人以上の他の TelePresence または WebEx 参加者が参加するまで）
なし	[はい（Yes）]	[はい（Yes）]	[いいえ（No）]	WebEx 参加者のシルエットイメージ
なし	[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	WebEx 会議参加者のビデオ
[はい（Yes）]	[いいえ（No）]（TelePresence のみ）	該当なし	該当なし	ロビー画面（1 人以上の他の TelePresence 参加者が参加するまで）

TelePresence Server のロビー画面の設定	CMR ハイブリッド会議か	1 人以上の WebEx 参加者がいるかどうか	WebEx 参加者がカメラに対応しているかどうか	最初の TelePresence 参加者に対して表示される内容
[はい（Yes）]	[はい（Yes）]	[いいえ（No）]	該当なし	ロビー画面（1 人以上の他の TelePresence または WebEx 参加者が参加するまで）
[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	[いいえ（No）]	WebEx 参加者のシルエット
[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	[はい（Yes）]	WebEx 会議参加者のビデオ

Cisco TMS での電話会議設定の設定

ここでは、Cisco TMS で設定できる CMR ハイブリッド 会議の推奨会議設定とオプションの会議設定について説明します。

デフォルト画像モード

[デフォルト画像モード（Default Picture Mode）] を [分割表示（Continuous Presence）] に設定することを推奨します。これにより、MCU を使用する会議で、複数の参加者を同時に画面に表示できます。TelePresence Server は、常に複数の参加者を表示するように設定されています（TelePresence Server の ActivePresence）。

Cisco TMS でデフォルト画像モードを設定するには、次の手順を実行します。

手順

ステップ 1 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] の順に移動します。

ステップ 2 [会議作成オプション（Conference Create Options）] セクションで、[デフォルト画像モード（Default Picture Mode）] を [継続表示（Continuous Presence）] に設定します。

ステップ 3 [保存（Save）] をクリックします。

会議接続/切断オプション

スケジュールされている終了時刻を越えて会議を延長する際に、会議を延長できる十分なリソースがない場合に警告が表示されるようにするため、TMS で [会議接続/切断オプション（Conference Connection/Ending Options）] を設定することを推奨します。

手順

ステップ 1 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] の順に移動します。

ステップ 2 [会議接続/会議延長（Conference Connection/Conference Extension）] セクションで次のオプションを設定します。

a) [会議延長のスケジュールで競合が発生した場合の連絡先を指定する（Supply Contact Information on Extend Meeting Scheduling Conflict）] で、[はい（Yes）] を選択します。
これにより、予約の競合が原因で会議の延長が不可能な場合に、参加者が連絡先情報を確認できます。

注：このオプションは、CTS、Jabber Video など、TMS からの直接メッセージングをサポートしないエンドポイントではサポートされません。

b) [会議終了に関する警告をビデオ内に表示する（Show In-Video Warnings About Conference Ending）] で [はい（Yes）] を選択します。
これにより、TelePresence 参加者に対し、会議が終了することを通知するテキスト メッセージが、ブリッジによりビデオに表示されます。

この機能は、次のブリッジとの互換性があります。

- MCU 42xx、45xx、84xx、85xx、5xxx
- TelePresence Server 70xx、87xx

注：WebEx は MCU/TelePresence Server への単一参加者接続であるため、TelePresence ユーザが現在発言中の参加者である場合は、ビデオ内テキスト メッセージは WebEx 参加者に対してのみ表示されます。

c) [会議延長のための連絡先（Contact Information to Extend Meetings）] では、会議終了通知の後に続いて表示する内容をカスタマイズできます。ユーザの代わりに会議を延長できる担当者の電話番号または名前などの連絡先情報を入力できます。
ここで設定されたテキストは、ブリッジから会議の全参加者に送信される会議終了に関するビデオ内警告と、Cisco TMS から個々の参加者に送信される会議終了通知の両方に適用します。

ステップ 3 （オプション）次のオプションを設定することで、ビデオ内の警告の長さ、タイミング、内容を設定できます。

a) [メッセージのタイムアウト（秒）（Message Timeout (in seconds)）] は警告メッセージが表示される秒数です。（デフォルトの設定は 10）

b) [終了 X 分前にメッセージを表示する（Show Message X Minutes Before End）] は警告メッセージを表示する時点から会議終了までの間の分数です。

このメッセージは、カンマで分を分割して複数回示すことができます。たとえば、1,5は会議終了の 1 分前と 5 分前に警告メッセージを表示します。デフォルト設定：1,5（1 分と 5 分）。

（注） TelePresence MPS ブリッジの場合、10、5 および 1 のみをここに入力することができ、画面に数字アイコンとして表示されます。その他すべてのシステムは、任意の数の間隔に設定でき、[会議延長のための連絡先（Contact Information to Extend Meetings）] に入力されたテキスト文字列に続いて会議終了通知を表示します。

ステップ 4 [保存（Save）] をクリックします。

早期参加許可の設定

TelePresence参加者は、スケジュールされた会議開始時刻の最大5分前から参加できるようになりました。これにより、Cisco TMS はメイン参加者（MCU または TS）に対し会議開始時刻の 5 分前に会議を割り当てます。これは、ベストエフォート機能です。したがってメイン参加者に使用可能なリソースがない場合は、一部またはすべての参加者が 5 分以内に会議に参加できないことがあります。

（注） Cisco TMS は、スケジュールされた開始時刻までは WebEx にダイヤルアウトしません。

Cisco TMS で早期参加許可を設定するには、次の手順を実行します。

手順

ステップ 1 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議の設定（Conference Settings）] > [参加者に対し 5 分前の参加を許可する（Allow Participants to Join 5 Minutes Early）] に進みます。

ステップ 2 [保存（Save）] をクリックします。
最適な結果を得るため、TMS が、会議のスケジュール時点で選択された数を超えて、会議のポート数を動的に増加できるようにしてください。

延長時のリソース可用性の設定

延長時のリソース可用性確認を有効にすると、すべてのリソースが使用可能な場合は会議が15分間延長され、延長された会議が完了するまでリソースが予約されます。

Cisco TMS で [延長時のリソース可用性確認（Resource Availability Check on Extension）] を設定するには、以下の手順を実行します。

手順

ステップ 1 [管理ツール（Administrative Tools）] > [構成（Configuration）] > [会議設定（Conference Settings）] > [延長時のリソース可用性確認（Resource Availability Check on Extension）] に進みます。

ステップ 2 [保存（Save）] をクリックします。
この設定は [会議延長モード（Extend Conference Mode）] と連動して、[自動ベストエフォート（Automatic Best Effort）] または [エンドポイントプロンプト（Endpoint Prompt）] に適用されます。次のオプションがあります。

- [ベストエフォート（Best Effort）]：今後 15 分間にわたりすべてのリソースが使用可能な場合に、ベスト エフォート ベースでスケジュールされている終了時刻から会議を自動的に延長します。
- [無視（Ignore）]：Cisco TMS は、リソース可用性チェックを無視し、すべてのリソースが使用可能であるかどうかにかかわらず、スケジュールされている終了時間から会議を自動的に延長します。唯一の例外は、メイン参加者で使用されているポートが別の会議と競合する場合です。

Cisco TMS のシングル サインオンの設定

Cisco TMS では、WebEx アカウントのユーザが予約した会議のシングル サインオン（SSO）を有効にするオプションがあります。SSO が設定されており、ユーザが WebEx 対応会議をスケジュールする場合、Cisco TMS ユーザ プロファイルの WebEx ユーザ名が WebEx サイトに渡され、予約が完了します。

SSO が設定されている場合に必要な操作は、ユーザの WebEx ユーザ名をそのユーザの Cisco TMS ユーザ プロファイルに保存することだけです。ユーザの WebEx パスワードは不要です。

Cisco TMS ユーザ プロファイルにユーザの WebEx ユーザ名を追加する方法は 2 通りあります。

- TMS サイト管理者が、ユーザ プロファイルに WebEx ユーザ名を手動で入力する。

  主催者が WebEx を使用した会議を Cisco TMS でスケジュールすると、Cisco TMS から、その Webex ユーザ名が WebEx ホストとして指定されている WebEx サイトに、会議情報が送信されます。

  （注） ユーザが選択した WebEx サイトに対し、TMS で SSO が有効になっている場合、[WebEx ユーザ名（WebEx Username）] フィールドを編集するにはサイト管理者特権が必要です。ユーザは各自の WebEx ユーザ名を編集できません。

- Cisco TMS が Active Directory（AD）から WebEx ユーザ名をインポートできるようにする

（注） ADの任意のフィールドを使用できます。最もよく使用されるフィールドは、電子メール アドレスとユーザ名です。

主催者が WebEx を使用した会議を Cisco TMS でスケジュールすると、Cisco TMS はADに対し、Cisco TMS管理者がAD参照の[ネットワーク設定（Network Settings）]ページで入力したユーザ名とパスワードを使用して、会議主催者の WebEx ユーザ名を要求します。

AD から Cisco TMS に主催者の WebEx ユーザ名が提供されると、Cisco TMS はその WebEx ユーザ名が WebEx ホストとして指定されている WebEx サイトに、会議情報を送信します。

前提条件

Cisco TMS で SSO を設定する前に、WebEx Cloud Services チームと協力して、Cisco TMS と WebEx クラウドの両方で設定する必要がある次の情報を決定する必要があります。

- パートナー名

  この値は、すべての WebEx 顧客において固有でなければならないため、WebEx チームが決定する必要があります。この情報については、WebEx アカウント チームにお問い合わせください。

  例：examplesso.webex.com

- パートナーの発行元（IdP ID）

  これはアイデンティティ プロバイダー（使用する TMS）です。WebEx チームがこの値を決定する必要があります。この情報については、WebEx アカウント チームにお問い合わせください。

  社内の TMS を示す名前を使用することを推奨します。

  例：exampletms

- SAML 発行元（SP ID）

  これはサービス プロバイダー（つまり WebEx）を示します。WebEx チームがこの値を決定する必要があります。この情報については、WebEx アカウント チームにお問い合わせください。

  例：https://examplesso.webex.com/examplesso

- AuthnContextClassRef

  これは、認証コンテキストです。IdP は、X509 証明書、スマート カード、IWA、ユーザ名/パスワードなど、異なるコンテキストのユーザを認証します。

  TMS により自動的に指定されるデフォルト値を使用します。

Cisco TMS での SSO の設定

Cisco TMS で SSO を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	SSO を有効にする WebEx サイトが、Cisco TMS で作成されていることを確認します。	詳細については、Cisco TMS での Cisco WebEx 機能の設定, （120 ページ）を参照してください。
ステップ 2	Cisco TMS と WebEx サイト間の接続を保護するための証明書を生成します。	詳細については、WebEx の証明書の生成, （134 ページ）を参照してください。
ステップ 3	WebEx サイトでパートナー委任認証を有効にします。	詳細については、WebEx サイトでのパートナー委任認証の有効化, （138 ページ）を参照してください。
ステップ 4	Cisco TMS で SSO を有効にします。	詳細については、Cisco TMS での SSO の有効化, （139 ページ）を参照してください。

WebEx の証明書の生成

WebEx では、WebEx クラウドに対して Cisco TMS を認証するときに証明書ペア（公開証明書と秘密キー）を使用する必要があります。

証明書ペアの要件：

- 公開証明書は WebEx Cloud Services チームに送信されるため、.cer または .crt 形式でなければなりません。
- 証明書と秘密キーは、Cisco TMS にアップロードするため PKCS12 形式のファイルにバンドルされています。

新規証明書を生成するか、または既存の証明書（Cisco TMS サーバで HTTPS を有効にするときに使用する証明書など）を使用できます。

信頼された機関によって署名された既存の証明書の使用

信頼された機関によって署名された証明書を現在使用している場合は、WebEx 設定に既存の証明書とキーのペアを使用することを推奨します。手順は、秘密キーがエクスポート可能であるかどうか、および使用可能であるかどうかに応じて異なります。

秘密キーがエクスポート可能な場合

秘密キーがエクスポート可能な場合は、次の手順を実行します。

手順

ステップ 1 Windows 証明書マネージャ スナップインを使用して、既存のキーと証明書のペアを PKCS#12 ファイルとしてエクスポートします。

ステップ 2 Windows 証明書マネージャ スナップインを使用して、既存の証明書を Base 64 PEM エンコード .CER ファイルとしてエクスポートします。

ステップ 3 ファイル拡張子が .cer または .crt であることを確認して、WebEx Cloud Services チームにこのファイルを提供します。

ステップ 4 ステップ 2 で作成した PKCS#12 ファイルは、「Cisco TMS での SSO の有効化」で TMS にアップロードするために使用します。

秘密キーをエクスポートできないが、キー/証明書ペアが使用可能な場合

秘密キーをエクスポートできないが、キーと証明書のペアが使用可能な場合は、次の手順を実行します。

手順

ステップ 1 Windows 証明書マネージャ スナップインを使用して Base 64 PEM ファイルに既存の証明書をエクスポートします。

ステップ 2 ファイル拡張子を .cer または .crt に変更し、WebEx Cloud Services チームにこの Base 64 PEM ファイルを提供します。

ステップ 3 「OpenSSL を使用した証明書の生成」のステップ 10 のコマンドを使用して、PKCS#12 キー/証明書のペアを作成します。

ステップ 4 この PKCS#12 ファイルは、「Cisco TMS での SSO の有効化」で TMS にアップロードするために使用します。

秘密キーがエクスポートできず、使用可能ではない場合

秘密キーをエクスポートできず、使用可能ではない場合は、新しい証明書を作成する必要があります。

新しい証明書を作成するには、「OpenSSL を使用した証明書の生成」のすべての手順に従います。

認証局によって署名されるキーと証明書のペアの作成

キーと証明書のペアがないが、使用する認証局がある場合は、次の手順を実行します。

手順

ステップ 1 「OpenSSL を使用した証明書の生成」のステップに従って、OpenSSL を使用して WebEx SSO 設定に使用する新しいキー/証明書のペアを作成します。

ステップ 2 「OpenSSL を使用した証明書の生成」のステップ 8 を使用して、署名証明書の Base64 PEM エンコード バージョンを作成します。

ステップ 3 ファイル拡張子を .cer または .crt に変更し、WebEx Cloud Services チームに証明書のこのバージョンを提供します。

ステップ 4 「OpenSSL を使用した証明書の生成」のステップ 10 のコマンドを使用して、PKCS#12 キー/証明書のペアを作成します。

ステップ 5 この PKCS#12 ファイルは、「Cisco TMS での SSO の有効化」で TMS にアップロードするために使用します。

自己署名キー/証明書のペアの作成

キーと証明書のペアがなく、使用する認証局がない場合は、自己署名証明書を作成する必要があります。

自己署名キーを作成するには、次の手順を実行します。

手順

ステップ 1 「OpenSSL を使用した証明書の生成」の手順に従います。

ステップ 2 ステップ 6 の手順に従い、自己署名証明書署名要求を作成します。

ステップ 3 ステップ 7 から 9 に従い、自己署名証明書の Base 64 PEM ファイルを WebEx Cloud Services チームに提供します。

ステップ 4 ステップ 10 に従い、PKCS#12 PFX ファイルを作成します。

ステップ 5 「Cisco TMS での SSO の有効化」で、TMS へアップロードします。

OpenSSL を使用した証明書の生成

OpenSSL は、UNIX および Linux で動作するように設計されているオープン ソース プロジェクトです。Shining Light Productions から Windows バージョンを入手できます（http://slproweb.com/

products/Win32OpenSSL.html）。OpenSSL を使用して証明書を生成する前に、OpenSSL をインストールしておく必要があります。

詳細については、http://www.openssl.org/ を参照してください。

WebEx および TMS に必要な TMS 証明書を生成するには、次の手順を実行します。

手順

ステップ 1 秘密キーを生成します。

ステップ 2 証明書署名要求（CSR）を生成します。

ステップ 3 認証局により CSR に署名してもらいます。

ステップ 4 署名付き証明書の拡張子が .cer または .crt であることを確認し、それを WebEx チームに提供します。

ステップ 5 署名証明書と秘密キーを PKCS#12 形式ファイルに変換します。

ステップ 6 変換後の証明書と秘密キーを TMS にアップロードします。

ステップ 7 Windows でコマンド プロンプトを開きます。

ステップ 8 openssl\bin インストール ディレクトリに移動します。

ステップ 9 コマンド openssl genrsa -out tms-privatekey.pem 2048 を使用して秘密キーを生成します。

ステップ 10 上記の秘密キー（openssl req -new -key tms-privatekey.pem -config openssl.cfg -out tms-certcsr.pem）を使用して、証明書署名要求（CSR）を生成します。

ステップ 11 次の項目を含む、要求されたデータを入力します。

a) 国（Country）
b) 州または地域
c) 組織名
d) 組織ユニット（Organization unit）
e) 共通名（これは Cisco TMS の FQDN です）
f) （任意）電子メール アドレス、パスワード、会社名

ステップ 12 Cisco TMS 証明書署名要求ファイル `tms-certcsr.pem` を信頼された認証局（CA）による署名を受けるために送信するか、または OpenSSL または Windows CA を使用して証明書署名要求に自己署名します。
信頼された認証局への証明書要求の送信方法の詳細については、当該認証局にお問い合わせください。

ステップ 13 OpenSSL または Windows CA を使用して、証明書に自己署名します。

a) OpenSSL を使用して、証明書署名要求に自己署名するには、次のコマンドを使用します。tms-certcsr.pem は PEM 形式の証明書署名要求です。tms-privatekey.pem は PEM 形式の秘密キーです。days は、証明書を有効にする日数です。**openssl x509 -req -days 360 -in tms-certcsr.pem -signkey** tms-privatekey.pem **-out tms-cert.pem**
作成される tms-cert.pem は、自己署名証明書です。

b) Windows CA を使用して証明書署名要求に自己署名するには、Windows 証明書マネージャ スナップインを使用します。Windows 証明書マネージャ スナップインを使用して証明書要求を

送信する方法の詳細については、Windows 証明書マネージャ スナップインのドキュメントを参照してください。

ステップ 14 認証局は、証明書要求に署名すると、署名した証明書をユーザに送信します。ユーザは、CA から署名証明書 tms-cert.der を受信します。

ステップ 15 この証明書が電子メールまたは Web ページで提供され、ファイルとして提供されない場合は、そのファイルを開き、-----BEGIN CERTIFICATE----- 行から -----END CERTIFICATE----- 行までの内容をコピーします。コピーした内容をテキスト ファイルに保存し、このファイルに **tms-cert.der** という名前を付けます。

ステップ 16 （証明書が .pem 形式であればこのステップをスキップします）OpenSSL コマンド **openssl x509 -inform der -in tms-cert.cer -out tms-cert.pem** を使用して署名付き証明書を .der から .pem に変換します。

ステップ 17 拡張子を .cer または .crt に変更し、WebEx Cloud Services チームにこの署名証明書を提供します。

ステップ 18 OpenSSL コマンド **openssl pkcs12 -export -inkey tms-privatekey.pem -in tms-cert.pem -out tms-cert-key.p12 -name tms-cert-key** を使用して、署名付き証明書 .pem とステップ 3 で作成した秘密キーを結合します。
これで、SSO 設定の秘密キーが含まれている Cisco TMS 証明書が作成されました。この証明書は Cisco TMS にアップロードされます。

（注） TMS にこの証明書をアップロードする前に、WebEx サイトのパートナー委任認証を有効にする必要があります。詳細については、次の項の「WebEx サイトでのパートナー委任認証の有効化」を参照してください。パートナー委任認証を有効にしたら、前述のステップ 10 で生成した証明書と秘密キーの組み合わせを、「Cisco TMS での SSO の有効化」のステップ 4 で Cisco TMS にアップロードし、SSO 設定を行います。

WebEx サイトでのパートナー委任認証の有効化

この手順は、WebEx サイトでパートナー委任認証を有効にするために必要です。

はじめる前に

WebEx サイトでパートナー委任認証を有効にする前に、WebEx Cloud Services チームが、TMS を委任パートナーとして設定するため、サイト プロビジョニングを変更する必要があります。

手順

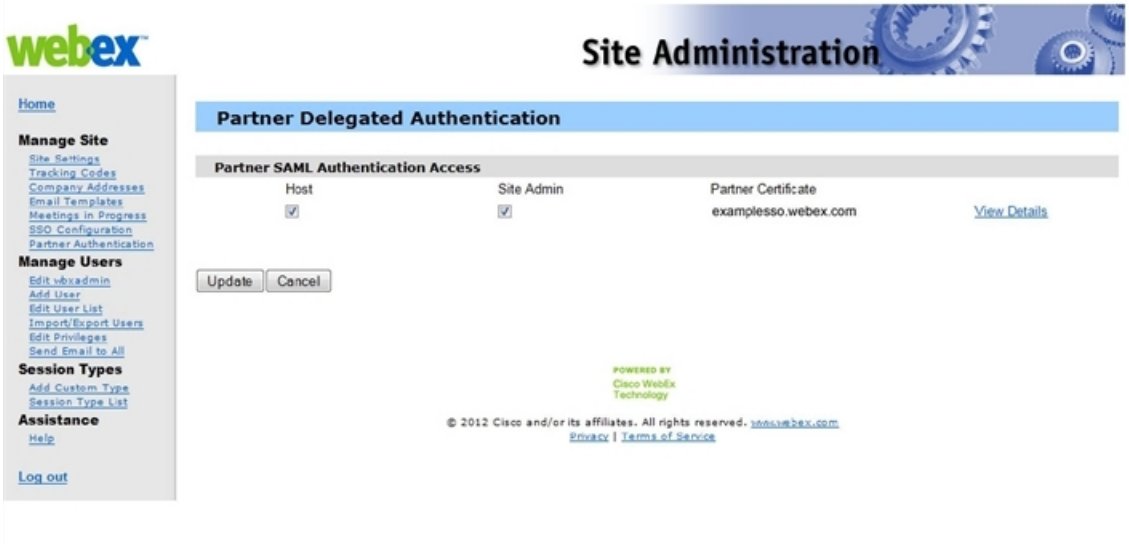
ステップ 1 WebEx Cloud Services チームに対し、SAML 2.0 フェデレーション プロトコルに合わせて設定された TMS のパートナー証明書を追加すること要求します。

ステップ 2 TMS の公開証明書を WebEx Cloud Services チームに提供します。証明書の作成方法の詳細については、「WebEx の証明書の生成」を参照してください。

ステップ 3 WebEx Cloud Services チームから、このステップを完了したことが通知されたら、次の説明に従い、WebEx サイトの Site Administration のホスト アカウントと管理者アカウントの両方で、パートナー委任認証を有効にします。

ステップ 4 「Cisco TMS での SSO の有効化」に進みます。

ステップ 5 WebEx 管理サイトにログインし、[サイトの管理（Manage Site）] > [パートナー認証（Partner Authentication）] に進みます。
[パートナー委任認証（Partner Delegated Authentication）] ページが表示されます。



ステップ 6 [パートナー SAML 認証アクセス（Partner SAML Authentication Access）] セクションで、[ホスト（Host）] と [サイト管理（Site Admin）] の両方がオンであることを確認し、[更新（Update）] をクリックします。

Cisco TMS での SSO の有効化

Cisco TMS で SSO を有効にするには、次の手順を実行します。

はじめる前に

手順を実行する前に、次の情報について確認してください。

- 証明書のパスワード（必要な場合）

- パートナー名
- パートナーの発行元（IdP ID）
- SAML 発行元（SP ID）
- AuthnContextClassRef

（注） SSO を有効にする前に、WebEx サイトでパートナー委任認証を有効にする必要があります。詳細については、「WebEx サイトでのパートナー委任認証の有効化」を参照してください。

手順

ステップ 1 Cisco TMS にログインし、[管理ツール（Administrative Tools）] > [構成（Configuration）] > [WebEx の設定（WebEx Settings）] に進みます。

ステップ 2 [WebEx サイト（WebEx Sites）] ペインで、SSO を有効にする WebEx サイトの名前をクリックします。
[WebEx サイトの設定（WebEx Site Configuration）] ペインが表示されます。

ステップ 3 [SSO を有効にする（Enable SSO）] で [はい（Yes）] を選択します。

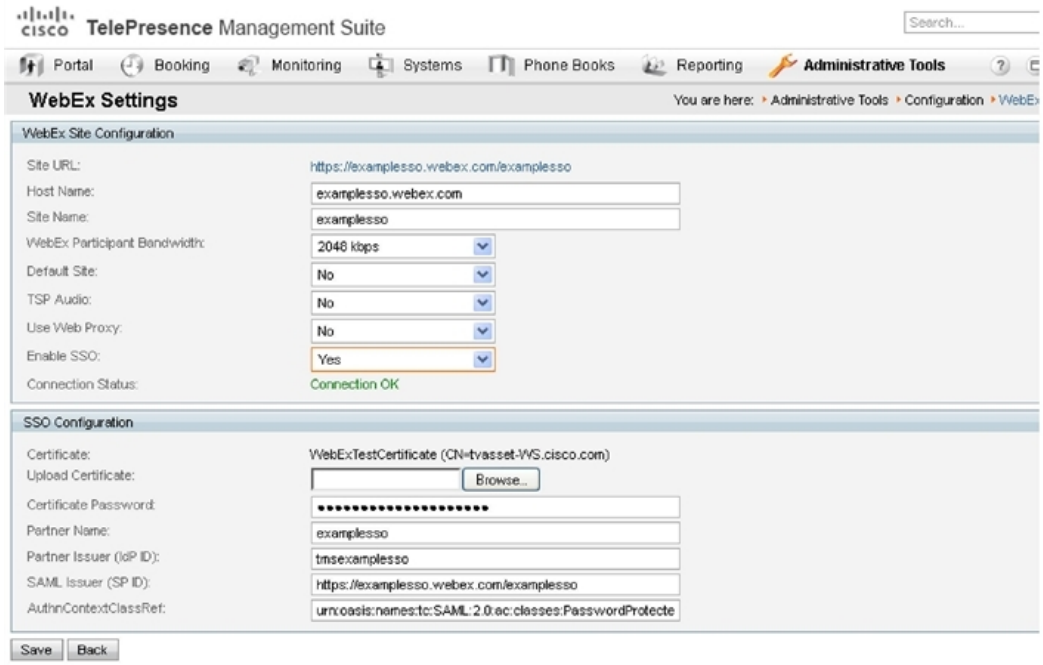
[SSO 設定（SSO Configuration）] ペインが表示されます。

ステップ 4 [参照（Browse）] をクリックし、「WebEx の証明書の生成」で生成した PKS #12 秘密キー証明書（.PFX）をアップロードします。

ステップ 5 証明書の生成時に選択したパスワードおよびその他の情報を使用して、残りの SSO 設定フィールドに入力します。

ステップ 6 [保存（Save）] をクリックします。

図 *9*：*Cisco TMS* の *[WebEx* の設定（*WebEx Settings*）*]* の *[SSO* 設定（*SSO Configuration*）*]*



WebEx ホスト代理としてスケジュールできる設定

前の項では TMS での SSO の設定方法を中心に説明しましたが、WebEx サイト自体で SSO を設定することもできます。このため、CMR ハイブリッド会議のスケジュールでサポートされているすべての設定を理解しておくと便利です。

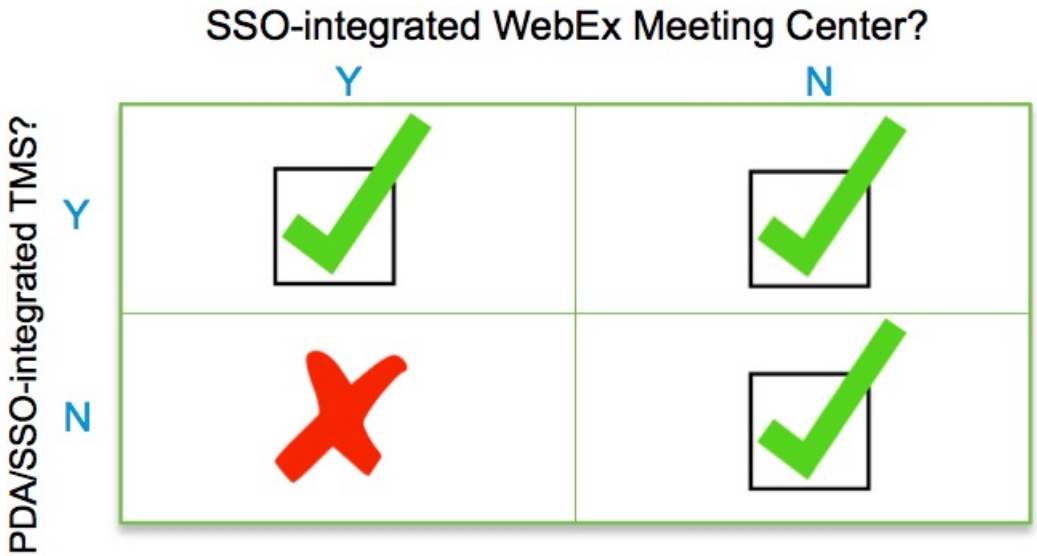
TMS が WebEx ホストの代理としてスケジュールできるようにする 3 つの構成があります。

- WebEx サイトが SSO を使用せず、TMS で SSO が設定されていない。WebEx サイトとのパートナー委任認証（PDA）関係がない。WebEx ホスト ログイン：WebEx ユーザ名とパスワードは WebEx に保存され、ユーザは WebEx サイトに対して直接認証します。
  - TMS スケジューリング：ホストの WebEx ユーザ名およびパスワードは、TMS 個人プロファイルに保存されます。ユーザが TMS にアクセスできる場合はユーザが管理する必

要があります。それ以外の場合は TMS 管理者が管理する必要があります。TMS は、スケジュール時点でユーザ名とパスワードの両方を WebEx に渡します。

- WebEx サイトが SSO を使用しないが、TMS で SSO が設定されている。WebEx サイトとの PDA 関係がある。WebEx ホスト ログイン：WebEx ユーザ名とパスワードは WebEx に保存され、ユーザは WebEx サイトに対して直接認証します。
  - TMS スケジューリング：ホストの WebEx ユーザ名は TMS 個人プロファイル（TMS 管理タスク）に保存されますが、WebEx パスワードは TMS に保存されません。TMS は信頼されており、そのユーザをスケジュールできます。
- WebEx サイトが SSO を使用し、TMS で SSO が設定されている。WebEx サイトとの PDA 関係がある。WebEx ホスト ログイン：WebEx ユーザは SSO アイデンティティ サービス プロバイダーを介してログインします。
  - TMS スケジューリング：ホストの WebEx ユーザ名は TMS 個人プロファイル（TMS 管理タスク）に保存されますが、WebEx パスワードは Cisco TMS に保存されません。Cisco TMS は信頼されており、そのユーザをスケジュールできます。

図 *10*：*CMR Hybrid* のサイト レベルでの *WebEx SSO* と *TMS PDA/SSO* のサポート マトリクス



PDA/SSO の更新のガイドライン

期限がもうすぐ切れるパブリック CA によって署名された証明書を使用している場合は、更新を行う必要があります。期限切れの証明書を使用すると、CMR Hybrid 会議のスケジューリングを試みる代わりに TMS によって示される期限切れの証明書を WebEx が拒否するため、CMR Hybrid 会議のスケジューリングの失敗が発生します。

ここでは、期限切れになった証明書に対処する方法のガイドラインを示します。

- WebEx サイトの代理パートナー証明書は、いつでも複数持つことができます。

  したがって、バックアップ TMS と、一意の証明書付きのオンライン/アクティブ TMS をそれぞれ持つことができます。または、もっと良い方法として、それらの TMS インスタンスのいずれかから同じ証明書と秘密キーを代替にエクスポートしておき、それらで FQDN/ホスト名を共有することができます。[これをコールドスタンバイと呼びます]。または、冗長 TMS 環境を展開し、NLB/フロントエンド TMS 名に対してそれぞれの一意な TMS FQDN と共有 CN を含む複数の SAN で単一の証明書を使用します。

- 特定の [発行先（Issued to）] または [CN]（CommonName）フィールドを参照するときに保留できるのは 1 つの証明書のみであるため、[発行先（Issued to）] または [CN] フィールドは一意にする必要があることに留意してください。

  これは、シスコがサイトの証明書を [発行先（Issued to）] ソート順序を使用して保存するためです。既存の証明書と同じ [発行先（Issued to）] 名の証明書が見つかった場合、シスコは、既存の証明書を新しい証明書に置き換えるかどうかを問い合わせて明らかにする必要があります。このケースの可能性はありますが、証明書 [CN] の同じ [発行先（Issued to）] 名で WebEx サイトに [2] つの証明書を保存することはできません。これが発生すると、シスコが古い証明書を削除するまでまたは古い証明書を新しい証明書で置き換えるまで、新しい証明書は実際にはロードされず機能しません。このため、この問題を回避するために、古い証明書を新しい証明書で置き換えることをシスコにお知らせいただくか、または新しい証明書の [発行先（Issued to）] または [CN] フィールドの情報が異なっていることを確認してください。これは、たとえば TMS に別の FQDN [たとえば TMS1.company.com と TMS2.company.com] を付けた場合は可能です。

第 12 章

Cisco TelePresence Management Suite Extension for Microsoft Exchange を設定する

前提条件

- Cisco TMSXE ソフトウェア リリース 5.2 以降が必要です。
- Cisco TMS ソフトウェア リリース 15.2 以降が必要です。
- ビデオ会議で予約用のメールボックスとして使用できるエンドポイントを、Exchange で AutoAccept に設定する必要があります。
- 会議主催者が、TMSXE がホストされているドメインとは別のドメインで会議をスケジュールしている場合、TMSXE がインストールされているドメインを、会議主催者のコンピュータで「ローカル イントラネット」ゾーンのサイト リストに追加する必要があります。これにより、TMSXE サーバが信頼されるようになります。多数のユーザまたはすべてのユーザが存在するドメインの外部にあるドメインで TMSXE がホストされている場合は、社内 IT グループが、グループ ポリシーまたはログイン スクリプトを使用してすべてのユーザに対してこの作業を行うとより効率的です。この作業を行わない場合、ユーザが会議をスケジュールしようとするたびに、TMSXE のユーザ名とパスワードを入力する必要が生じます。
- TMSXE には、組織内で信頼される署名証明書が必要です。このためには、IIS から証明書署名要求（CSR）を生成し、認証局（CA）に提出します。この証明書には、自己署名証明書を使用するか、または信頼された内部認証局または公開認証局の証明書を使用することができます。

展開のベスト プラクティス

Cisco TMSXE をスタンドアロン サーバにインストールすることを推奨します。

小規模な展開環境では Cisco TMSXE を Cisco TMS と同じ場所に導入できますが、次の前提条件があります。

- サーバには 4 GB 以上の RAM が必要です。
- Cisco TMS と Cisco TMSXE での予約のために最大 50 の TelePresence エンドポイントが使用可能です。

TMSXE のインストールおよび設定の詳細については、次のマニュアルを参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/tmsxe/install_guide/Cisco-TMSXE-deployment-guide-4-1.pdf

Cisco TMSXE のスケジュール オプション

- Microsoft Outlook の WebEx 生産性向上ツール プラグインを使用して、Microsoft Outlook の会議に WebEx を追加します。

WebEx and TelePresence Integration to Outlook のための Cisco TMSXE の設定

WebEx and TelePresence Integration to Outlook を使用して、Cisco TMSXE をスケジューリング用に設定するには、次の作業を行う必要があります。

- Cisco TMS Booking Service のインストール
- WebEx サイトと TMSXE 間の通信をセットアップします。

Booking Service のインストール

はじめる前に

TelePresence の WebEx 生産性向上ツールが Cisco TMSXE と通信できるようにするには、Booking Service がインストールされている必要があります。

初回インストール中にプロキシを追加していない場合は、次の手順を実行します。

手順

ステップ 1 Cisco TMSXE サーバで [コントロール パネル（Control Panel）] に進みます。

ステップ 2 [Cisco TelePresence Management Suite Extension for Microsoft Exchange] を右クリックして、[変更（Change）] を選択します。
これによりインストーラが開始され、インストール内容を変更できます。

ステップ 3 インストーラで表示されるすべての指示に従い、Cisco TMS Booking Service の追加を選択します。
Booking Service をインストールすると、IIS が強制的に再起動されます。

HTTPS に対応した IIS の設定

Booking Service を使用するには、IIS で DefaultSite に HTTPS が設定されている必要があります。

Cisco TMSXE をインストールする前に IIS がサーバに存在していない場合、Booking Service と共に自動的にインストールされます。インストールが完了したら、Booking Service が機能できるようにするため、HTTPS を設定する必要があります。

詳細については、Microsoft サポートの記事「How To Set Up an HTTPS Service in IIS」を参照してください。

（注） 上記のリンクで説明する IIS 構成では、ユーザが Microsoft Outlook 向けの WebEx and TelePresence Integration to Outlook プラグインを使用して会議をスケジュールできるようにするため、[クライアント証明書（Client certificates）] の [SSL 設定（SSL Settings）] で [無視（Ignore）] を選択する必要があります。このようにしないと、Microsoft Outlook 向けの WebEx and TelePresence Integration to Outlook プラグインを使用して会議をスケジュールするときに、「予期しない問題が発生した（hit a glitch）」ことを示すメッセージがユーザに対して表示されます。

サーバ証明書の設定

TMSXE が実行されている Windows サーバで、IIS 内にサーバ証明書をロードする必要があります。

この処理では、証明書署名要求（CSR）を生成し、この CSR が認証局（CA）に送信され、CA から受信した署名証明書をインストールします。

IIS 7（Windows Server 2008）に対応した CSR の生成

手順

ステップ 1 サーバー マネージャ コンソール（[スタート（Start）] > [すべてのプログラム（All Programs）] > [管理ツール（Administrative Tools）] > [サーバー マネージャ（Server Manager）]）を開きます。

ステップ 2 [役割（Role）] ビューで [IIS マネージャ（IIS Manager）] を選択します（[サーバー マネージャ（Server Manager）] > [役割（Roles）] > [Web サーバー（Web Server）] > [IIS マネージャ（IIS Manager）]）。

ステップ 3 [サーバ証明書（Server Certificates）] をダブルクリックします。

ステップ 4 右側の [操作（Actions）] ペインで [証明書の要求の作成（Create Certificate Request）] をクリックします。

ステップ 5 （重要）[一般名:（Common Name:）] フィールドには、ユーザが Web サイトにアクセスするためにブラウザのアドレス バーに入力する DNS 名の完全修飾ドメイン名（site ではなく site.cisco.com）を入力します。ユーザがサイトにアクセスするためにブラウザに入力する名前とは異なる物理ホスト名がある場合は、必ずユーザが使用する名前を入力してください。

ステップ 6 [組織（Organization）] フィールドに、組織名を入力します。

ステップ 7 [組織単位（Organizational Unit）] フィールドに組織名を入力し、[次へ（Next）] をクリックします。

ステップ 8 [市区町村（City/locality）] フィールドに、サーバ所在地の市区町村名を入力し、[次へ（Next）] をクリックします。

ステップ 9 [都道府県（State/province）] フィールドに、サーバ所在地の都道府県を入力します。

ステップ 10 [国/地域（Country/Region）] フィールドで [US（米国）（US (United States)）] を選択し、[次へ（Next）] をクリックします。

ステップ 11 [CSP] はデフォルト値のままにします。

ステップ 12 [ビット長（Bit Length）] で [2048] を選択します。

ステップ 13 証明書要求（CSR）を保存するファイル名を入力（または参照して選択）して、[完了（Finish）] をクリックします。

ステップ 14 保存した CSR ファイルの内容全体をコピーして貼り付けます。
デフォルトの保存場所は C:\ です。

ステップ 15 CSR ファイルを CA に提出し、署名証明書が送られてくるまで待ちます。

IIS 7（Windows Server 2008）への公開ルート証明書のインストール

手順

ステップ 1 ルート CA 証明書ファイルをダブルクリックし、[証明書のインストール（Install Certificate）] をクリックします。

ステップ 2 [次へ（Next）] をクリックし、[証明書をすべて次のストアに配置する（Place all certificates in the following store）] オプション ボタンを選択し、[参照（Browse）] をクリックします。

ステップ 3 [物理ストアを表示する（Show Physical Stores）] をオンにします。

ステップ 4 [信頼されたルート証明機関（Trusted Root Certification Authorities）] フォルダを展開し、[ローカル コンピュータ（Local Computer）] フォルダを選択して [OK] をクリックします。

ステップ 5 [次へ（Next）] をクリックし、次に [完了（Finish）] をクリックします。「正しくインポートされました（The import was successful）」というメッセージが表示されます。

中間 CA 証明書のインストール（該当する場合）

手順

ステップ 1 中間 CA 証明書ファイルをダブルクリックし、[証明書のインストール（Install Certificate）] をクリックします。

ステップ 2 [次へ（Next）] をクリックし、[証明書をすべて次のストアに配置する（Place all certificates in the following store）] オプション ボタンを選択し、[参照（Browse）] をクリックします。

ステップ 3 [物理ストアを表示する（Show Physical Stores）] をオンにします。
[中間証明機関（Intermediate Certification Authorities）] フォルダを展開し、[ローカル コンピュータ（Local Computer）] フォルダを選択して [OK] をクリックします。

ステップ 4 [次へ（Next）] をクリックし、次に [完了（Finish）] をクリックします。「正しくインポートされました（The import was successful）」というメッセージが表示されます。

SSL サーバ証明書のインストール

手順

ステップ 1 IIS マネージャ コンソールで [サーバー証明書（Server Certificates）] 操作ウィンドウに移動し、[証明書の要求の完了（Complete Certificate Request）] をクリックします。[証明書要求を完了する（Complete Certificate Request）] ウィザードが表示されます。

ステップ 2 SSL サーバ証明書を保存した場所を探してこの場所を選択し、[開く（Open）] をクリックします。

ステップ 3 証明書のフレンドリ名を入力します（分からない場合は証明書のホスト名を使用します）。次に、[OK] をクリックします。
この時点で、TMSXE に対して SSL が使用可能になります。SSL を使用するように TMSXE または個別のディレクトリを設定する必要があります。IIS サイトを選択します。

ステップ 4 右側の操作ウィンドウで、サイトを、[サイトの編集（Edit Site）] の下の [結合（バインド）] をクリックします。

ステップ 5 [追加（Add）] ボタンをクリックします。

ステップ 6 [種類（Type）] メニューで [https] を選択します。

ステップ 7 [SSL 証明書（SSL certificate）] メニューで、SSL 証明書を選択します。

ステップ 8 [OK] をクリックします。

WebEx サイトと Cisco TMSXE 間の通信の設定

Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合, （171 ページ）の手順に従ってください。

Outlook で TelePresence 会議室に表示されるロケーションの設定

Outlook で CMR Hybrid 会議をスケジュールする際にテレプレゼンス会議室を選択すると、[出席者とリソースの選択（Select Attendees and Resources）] - [アドレス帳（Address Book）] ウィンドウ（Outlook の一部）と、[テレプレゼンス会議室の選択（Select Telepresence Rooms）] ウィンドウ（WebEx and TelePresence Integration to Outlook を使用する場合に表示されるウィンドウ）の両方に会議室の場所が表示されます。

手順

ステップ 1 [出席者とリソースの選択（Select Attendees and Resources）] - [アドレス帳（Address Book）] ウィンドウを表示するには、[会議（Meeting）] ウィンドウで [宛先...（To...）] ボタンをクリックします。

ステップ 2 [テレプレゼンス会議室の追加（Add Telepresence Rooms）] ウィンドウを表示するには、[会議オプション（Meeting Options）] ペインの [テレプレゼンス会議室の追加（Add Telepresence Rooms）] ボタンをクリックします。
[テレプレゼンス会議室の選択（Select Telepresence Rooms）] ウィンドウのロケーションは、TMSXE 起動時に、有効なメール ボックスの Active Directory アカウントの Active Directory から読み取られ、WebEx and TelePresence Integration to Outlook に提供されます。これは構造化データではなく、単純なテキスト フィールドです。ロケーション情報に表示される内容は、次に示す、Microsoft Exchange の [アドレス帳（Address Book）] の [場所（Location）] カラムと同じです。 WebEx and TelePresence Integration to Outlook のための Cisco TMSXE の設定, （146 ページ）

Exchange の [アドレス帳（Address Book）] のドロップダウン メニューに表示される構造と階層（WebEx and TelePresence Integration to Outlook のための Cisco TMSXE の設定, （146 ページ））は、Exchange管理者によって手動で作成されます。このためには、ノードを作成し、それらのノードに名前と検索フィルタを指定します。（地域的な使用以外の）一般的な用途は、部署、グループ、または事業部門を使用したリストを作成することです。詳細については、Microsoft Exchange のマニュアルを参照してください。

WebEx and TelePresence Integration to Outlook のインストール

WebEx and TelePresence Integration to Outlook プラグインを使用して会議をスケジュールする会議主催者は、WebEx 生産性向上ツールを WebEx サイトからダウンロードして TelePresence にインストールする必要があります。詳細については、以下を参照してください。 Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合, （171 ページ）

WebEx Scheduling Mailbox のための Cisco TMSXE の設定

手順

ステップ 1 Microsoft Exchange で WebEx メールボックスを設定します。

ステップ 2 WebEx メールボックスを Cisco TMSXE に追加します。

Microsoft Exchange での WebEx Scheduling Mailbox の設定

Microsoft Exchange で WebEx メールボックスを設定するには、Exchange 管理コンソールまたは Powershell を次のように使用します。

手順

ステップ 1 WebEx Scheduling Mailbox の新しいユーザ メールボックス（例：webex@example.com）を作成します。
詳細については、「Create a Mailbox（Exchange 2010 Help）」または「How to Create a Mailbox for a New User（Exchange 2007 Help）」を参照してください。

ステップ 2 このメールボックスに、EWS サービス アカウント フル メールボックス アクセス権を付与します。
詳細については、「Allow Mailbox Access（Exchange 2010 Help）」または「How to Allow Mailbox Access（Exchange 2007 Help）」を参照してください。

ステップ 3 メールボックスのプロパティを次のように変更します。

a) メールボックスの [カレンダー アテンダント（Calendar Attendant）] をオフにします。
詳細については、「Configure User and Resource Mailbox Properties（Exchange 2010 Help）」または「How to Disable the Auto-Processing of Meeting Messages（Exchange 2007 Help）」を参照してください。

b) メールボックスの [カレンダー設定（Calendar Settings）] タブを使用している場合は、[AddNewRequestsTentatively（新規会議要求を仮要求としてマーク）（AddNewRequestsTentatively (Mark new meeting requests as Tentative)）] を無効にして、新しい要求が仮要求として自動的にマークされないようにしてください。

Cisco TMSXE への WebEx メールボックスの追加

手順

ステップ 1 TMSXE がインストールされているサーバにログインします。

ステップ 2 Windows のタスク バーから、[スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco] > [TMSXE 設定（TMSXE Configuration）] を選択します。

ステップ 3 Cisco TMSXE がすでに実行中の場合、設定ツールを開始するために Cisco TMSXE サービスを停止する必要があることを示すメッセージが表示されます。[サービスの停止（Stop Service）] をクリックします。
[Cisco TMSXE の設定（Cisco TMSXE Configuration）] ウィンドウが表示されます。

ステップ 4 [Exchange Web サービス（Exchange Web Services）] タブをクリックします。

ステップ 5 このウィンドウの下部にある [WebEx Scheduling Mailbox] フィールドに、Microsoft Exchange で作成した WebEx メールボックスの電子メール アドレスを入力します。

ステップ 6 [保存（Save）] をクリックします。
TMSXE が、指定された電子メールアドレスを検証します。設定が保存されたことを示すメッセージが表示されます。

ステップ 7 [終了（Exit）] をクリックします。

その他の推奨事項

WebEx Scheduling メールボックスで次のように設定することを推奨します。

- Exchange 管理コンソールの [メールフローの設定（Mail Flow Settings）] または Powershell を使用して、必要に応じてメッセージ配信制限を強化します。

たとえば、送信元の認証を義務付けて、特定のグループのユーザからの送信だけを許可します。

詳細については、「Configure Message Delivery Restrictions (Exchange 2010 Help)」または「How to Configure Message Delivery Restrictions (Exchange 2007 Help)」を参照してください。

- AD ユーザとコンピュータまたは Powershell を使用して、Active Directory ユーザ アカウントを無効に設定します。

詳細については、「Disable or Enable a User Account」を参照してください。

第 13 章

TelePresence Management Suite Provisioning Extension を設定する

前提条件

- Cisco TMS ソフトウェア リリース 15.0 以降がインストールされている必要があります。
- Cisco TMSPE ソフトウェア リリース 1.5 以降が Cisco TMS にインストールされ、有効に設定されている必要があります。
- Cisco TMS で WebEx が設定されている必要があります。
  - Cisco WebEx オプション キー
  - 1 つ以上の WebEx サイト

各ユーザのシングル サインオンまたは指定の WebEx クレデンシャル

ユーザの追加と管理を容易にするために、Cisco TMS と WebEx でシングル サインオンを設定することを強く推奨します。

（注） Cisco TMS でシングル サインオンが設定されていない場合は、WebEx で会議をスケジュールする各 Cisco TMS Smart Scheduler ユーザの WebEx ユーザ名とパスワードを手動で追加する必要があります。

Cisco TMS の設定方法については、Cisco TMS のシングル サインオンの設定, （132 ページ）を参照してください。

- Smart Scheduler を使用するには、次のいずれかのブラウザが必要です。
  - Microsoft Internet Explorer バージョン 10 以降
  - Mozilla Firefox バージョン 29 以降
  - Apple Safari バージョン 7 以降（Mac OS X およびiPad）
  - Google Chrome バージョン 34 以降

はじめに

Smart Scheduler は Cisco WebEx および TelePresence ソリューションの一部であり、これによりユーザは WebEx を使用したテレプレゼンス会議をスケジュールできます。

Smart Scheduler では、ユーザは WebEx を使用する Cisco TelePresence 会議または WebEx を使用しない会議をスケジュールできます。

Cisco TMS 内の予約可能なシステムはすべて直接スケジュールできます。Cisco TMS 予約でサポートされていないシステム（Cisco TMSPE によりプロビジョニングされるデバイスを含む）を、コールイン参加者としてスケジュールすることができます。

Cisco TMS を使用して Cisco WebEx がすでにセットアップされている場合は、Smart Scheduler 予約フォームで、会議に WebEx を含めるオプションを使用できます。

（注） 新規会議のデフォルト日時形式は dd.mm.yyyy および 24 時間形式です。各ユーザはこのデフォルト設定を変更できます。変更するにはその名前をクリックするか、Smart Scheduler ウィンドウの右上にあるレンチ アイコンをクリックします。この設定は、使用する各ブラウザでクッキーとして保存されます。

Cisco TMSPE へのユーザ アクセス

必要なクレデンシャルがあるユーザは、次の URL を使用して Smart Scheduler にアクセスできます。

http://<Cisco TMS サーバ ホスト名>/tms/booking/

```
Example: http://example-tms.example.com/tms/booking/
```

Cisco TMS をすでに使用しているユーザは、右上隅のポータル アイコンをクリックして、Smart Scheduler と FindMe に移動することもできます。

Smart Scheduler へのリダイレクトの作成

次の HTML コードを使用して HTTP リダイレクトを作成することもできます。

```
<html> <head> <META HTTP-EQUIV="Refresh" CONTENT="0; URL= https://<Cisco TMS Server
Hostname>/tmsagent/tmsportal/#scheduler"> <title>Cisco TelePresence Management Suite Smart
 Scheduler</title> </head> <body> </body> </html>
```

アクセス権と権限

Smart Scheduler へのアクセスと Cisco TMS へのアクセスは同様に動作します。

ユーザには次のいずれか 1 つのアカウントが必要です。

- Cisco TMS Windows Server のローカル アカウント
- サーバが Active Directory を介して信頼するドメイン アカウント。サーバをドメインのメンバーにすることによって、信頼されるすべてのドメイン ユーザが、既存の Windows クレデンシャルを自動的に使用できます。

Cisco TMS ユーザ アカウントがまだ存在しない場合は、これらのユーザがサイトにアクセスするときに自動的に作成されます。

（注） 実際の予約は個々のユーザによって直接作成されるのではなく、これらのユーザの代わりに、インストール時に追加された Cisco TMSPE サービス ユーザによって作成されます。このため、予約の権限はすべてのユーザで同一です。

タイム ゾーンの表示

予約の作成時には、ユーザの Web ブラウザのタイム ゾーン（ユーザのオペレーティング システムのタイム ゾーンにより決定される）が使用されます。

スケジューラ内部では、Web ブラウザとオペレーティング システムのタイム ゾーンが表示されます。

Smart Scheduler のしくみ

手順

	コマンドまたはアクション	目的
ステップ 1	ドメイン ユーザが Smart Scheduler にログインし、会議を予約すると、要求が Cisco TMS に渡されます。	
ステップ 2	このやり取りは、Cisco TelePresence Management Suite Extension Booking API（Cisco TMSBA）経由で行われます。	
ステップ 3	Cisco TMSPE のインストール中に入力される Cisco TMS ユーザは、Smart Scheduler のサービス ユーザです。このユーザは、Cisco TMSPE ユーザに代わって Cisco TMS で予約を作成します。	
ステップ 4	Cisco TMSPE ユーザが Cisco TMS にまだ存在しない場合は、予約と同時にそれが作成されます。	
ステップ 5	予約が完了すると、Cisco TMS は会議を予約したユーザに対して確認メールを送信します。その後、ルート、スケジュールされたシステム、WebEx 情報などの会議の詳細を含むメッセージを、他の会議参加者に転送できます。	

制限事項

Cisco TMS でスケジュールされた会議を、Smart Scheduler を使って変更しないことを強く推奨します。これは、Cisco TMS で会議に関して選択されたすべての機能とオプションがこのインターフェイスでサポートされるわけではないためです。

- 一連の定例会議の例外は、Smart Scheduler ではサポートされません。変更した場合、すべてのインスタンスにそれが適用されます。
- Smart Scheduler は、Cisco TMS から追加されたコールイン参加者の名前を変更します。

第 14 章

音声を設定する

前提条件

SIP または PSTN 音声を設定するための要件は次のとおりです。

- Cisco VCS Control/Cisco VCS Expressway を設定する必要があります。

詳細については、Cisco Expressway および TelePresence 設定タスク，（90 ページ）を参照してください。

- Unified Communications Manager を使用しているときは、次を確認してください。
  - Unified Communications Manager と Cisco VCS Control の間の SIP トランクが設定されています。

詳細の参照先： Cisco Unified Communications Manager の設定，（94 ページ）

- リージョンが G.711 および G.722 に対応して設定されている。
- PSTN 音声を設定する場合は、Cisco VCS または Unified Communications Manager にゲートウェイが登録されている必要があります。
- MCU/TelePresence Server が VCS に登録されている必要があります。
  - Unified Communications Manager にトランキングされている MCU/TelePresence Server はサポートされません。

- VCS または Unified Communications Manager に登録されているエンドポイントは、MCU/TelePresence Server にコールできます
- 必要なすべての製品について理解していること
- TSP プロバイダーから待合室機能が提供される状況で TSP 音声を設定する場合には、複数のホストが音声会議にログインできるよう TSP プロバイダーが設定を行う必要があります。あるいは、ホストとしてログインしないようホストユーザに指示する必要があります。複数のホストが有効になっていない場合、あるホストがダイヤルインすると、それより前にダイヤルインしていたホストが切断されます。たとえば、MCU が最初にダイヤルインし、その後でホスト ユーザがダイヤルインすると、MCU が切断されます。

ホスト ユーザは WebEx クライアントでホスト特権を維持し、必要に応じてそのユーザ インターフェイスを使って参加者をミュートまたはミュート解除できます。

- TSP 音声を設定する場合は、TSP プロバイダーでコールイン ユーザ マージ機能がサポートされている必要があります。コールイン ユーザ マージを使用すると、ユーザに音声で求める代わりに、DTMF コードを介して TSP パートナーが参加者 ID を渡すことができます。WebEx Meeting Manager は、DTMF コードの後に参加者 ID を入力するようユーザに求めます。

CMR ハイブリッド 用の SIP 音声の設定

ここでは、CMR ハイブリッド で SIP 音声を設定するために必要な手順を説明します。

ここでは、次の内容について説明します。

- SIP 音声を使用するように Cisco TMS で WebEx サイトを設定する, （160 ページ）
- WebEx サイトでのハイブリッド音声の有効化, （161 ページ）

（注） SIP 音声では、WebEx 音声だけがサポートされます（TSP 音声はサポートされていません）。

SIP 音声を使用するように Cisco TMS で WebEx サイトを設定する

WebEx サイトで SIP を使用するように Cisco TMS を設定するには、以下の手順を実行します。

手順

ステップ 1 Cisco TMS にログインします。

ステップ 2 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [WebEx の設定（WebEx Settings）] に進みます。

ステップ 3 [WebEx の設定（WebEx Settings）] ページが表示されます。

ステップ 4 設定する WebEx サイトの名前をクリックします。

ステップ 5 [WebEx サイトの設定（WebEx Site Configuration）] ページが表示されます。

ステップ 6 新規サイトの場合は、[サイト名（Site Name）]、[ホスト名（Host Name）]、およびその他の必須フィールドに情報を入力します。

ステップ 7 [TSP 音声（TSP Audio）] で [いいえ（No）] を選択します。

ステップ 8 [保存（Save）] をクリックします。

WebEx サイトでのハイブリッド音声の有効化

SIP 音声を使用するには、WebEx サイトをハイブリッド音声対応にする必要があります。また、自分のコンピュータを使って会議の音声部分に接続できるオプションを WebEx 参加者に提供するためにも、ハイブリッド音声が必要です。

WebEx チームがこの設定を行う必要があります。サポートが必要な場合は WebEx チームにお問い合わせいただくか、または次のサイトでオンライン チケットを送信してください。

https://cisco-support.secure.force.com/WebEx_GPL_WebForm

ハイブリッド音声は、会議の会議ブリッジとして TelePresence Server を使用する場合に必要となります（現時点では SIP 音声だけがサポートされるためです）。

CMR ハイブリッド 用の PSTN 音声の設定

ここでは、CMR ハイブリッド で PSTN 音声を設定するために必要な手順を説明します。

ここでは、次の内容について説明します。

- PSTN 音声を使用するように Cisco TMS で WebEx サイトを設定する, （162 ページ）
- WebEx サイトでのハイブリッド モードの有効化, （162 ページ）
- PSTN コールが PSTN ゲートウェイをパススルーして WebEx に着信するための設定, （163 ページ）

（注） Cisco CMR ハイブリッドは常に、国際番号用のエスケープ文字（+）で始まる完全修飾 E.164 番号をダイヤルします。例：+14085551212。VCS および/または Unified Communications Manager コール ルーティングが適切に設定されていることを確認します。

PSTN 音声を使用するように Cisco TMS で WebEx サイトを設定する

WebEx サイトで PSTN を使用するように Cisco TMS を設定するには、以下の手順を実行します。

手順

ステップ 1 Cisco TMS にログインします。

ステップ 2 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [WebEx の設定（WebEx Settings）] に進みます。

ステップ 3 [WebEx の設定（WebEx Settings）] ページが表示されます。

ステップ 4 設定する WebEx サイトの名前をクリックします。

ステップ 5 [WebEx サイトの設定（WebEx Site Configuration）] ページが表示されます。

ステップ 6 新規サイトの場合は、[サイト名（Site Name）]、[ホスト名（Host Name）]、その他の必須フィールドに情報を入力します。

ステップ 7 [TSP 音声（TSP Audio）] で [はい（Yes）] を選択します。

ステップ 8 [保存（Save）] をクリックします。
注意：会議主催者が会議のスケジュール時に TelePresence Server を選択すると、Cisco TMS は自動的に MCU を使用してその会議をスケジュールしようとします。MCU が使用可能でない場合は、会議が正しくスケジュールされません。

WebEx サイトでのハイブリッド モードの有効化

WebEx 参加者が自分のコンピュータから会議の音声部分に接続できるオプションを提供するためには、WebEx サイトをハイブリッド モードに設定する必要があります。WebEx チームがこの設定を行う必要があります。WebEx チームに連絡してアドバイスを受けてください。

PSTN コールが PSTN ゲートウェイをパススルーして WebEx に着信するための設定

WebEx は常に、国際番号用のエスケープ文字（+）で始まる完全修飾 E.164 番号を提供します。例：+14085551212。PSTN コールが正しくルーティングされるようにするには、VCS または Unified Communications Manager コール ルーティングを正しく設定する必要があります。

PSTN ゲートウェイをパススルーして PSTN コールを WebEx にルーティングするために、2 つの展開モデルがサポートされています。

- Cisco VCS 登録 PSTN ゲートウェイをパススルーする PSTN コールの設定，（163 ページ）
- Cisco Unified Communications Manager 登録 PSTN ゲートウェイをパススルーする PSTN コールの設定，（164 ページ）

Cisco VCS 登録 PSTN ゲートウェイをパススルーする PSTN コールの設定

VCS に登録された PSTN ゲートウェイをパススルーするよう PSTN コールを設定するには、次の手順を実行します。

VCS で、WebEx が提供するグローバルにルーティング可能な番号（例：+14085551212）を、VCS 登録ゲートウェイのテクノロジープレフィックス付き番号（例：9#14085551212）に変換する検索ルールまたはトランスフォームを作成します。

次の例では、+14085551212@example.webex.com が、正規表現パターン タイプを使用して 9#14085551212@example.webex.com に変換されます。

- パターン文字列：`\+(\d+@.*)`
- 置換文字列：`9#\1`

VCS でのトラバーサル ゾーン、検索ルール、およびトランスフォームの設定の詳細については、『*Cisco TelePresence Video Communication Server Basic Configuration（Control with Expressway）Deployment Guide*』を参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf

ISDN ゲートウェイの設定

ISDN ゲートウェイを使用して PSTN コールを WebEx にパススルーする場合、Cisco VCS Control でインターワーキング設定を行う必要があります。

（注） このステップは、ISDN ゲートウェイでのみ必要です。

ISDN ゲートウェイ用に Cisco VCS Control を設定するには、次の手順を実行します。

1. Cisco VCS Control にログインします。
2. [VCS 設定（VCS Configuration）] > [プロトコル（Protocols）] > [相互接続（Interworking）] の順に進みます。
3. [H.323 <- SIP インターワーキング モード（H.323 <- SIP interworking mode）] で [オン（On）] を選択し、[保存（Save）] をクリックします。

（注） この設定を保存するには、オプション キーが必要です。

Cisco Unified Communications Manager 登録 PSTN ゲートウェイをパススルーする PSTN コールの設定

Unified Communications Manager に登録された PSTN ゲートウェイをパススルーするよう PSTN コールを設定するには、次の手順を実行します。

手順

ステップ 1 VCS で、WebEx 提供の国際番号用のエスケープ文字（+）が付いたグローバルにルーティング可能な番号（例：+14085551212）を Unified Communications Manager にルーティングする検索ルールを作成します。

ステップ 2 Unified Communications Manager で、Unified Communications Manager 登録済みの適切な PSTN ゲートウェイにこのタイプのコールをルーティングするために、ダイヤル プランに基づくルート パターンを作成します。
VCS での検索ルールの設定の詳細については、『*Cisco TelePresence Video Communication Server Basic Configuration*（*Control with Expressway*）*Deployment Guide*』を参照してください。

http://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-5/Cisco-VCS-Basic-Configuration-Control-with-Expressway-Deployment-Guide-X8-5.pdf

Unified Communications Manager でのルート パターンの設定の詳細については、ご使用の Unified Communications Manager バージョンのマニュアルを参照してください。

https://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

CMR ハイブリッド の TSP 音声の設定

TSP Audio を使用する WebEx サイトを含む CMR Hybrid の概要

Telephony Service Provider（TSP）音声を使用する WebEx サイトを含む CMR Hybrid を使用する場合は、2 つの別個の音声会議に参加するために、TelePresence ブリッジ（MCU/TelePresence Server）と TSP 会議サービスの間で音声カスケードを確立する必要があります。TelePresence ブリッジは、ダイヤルイン ユーザのように音声会議に参加するために、TSP 音声サービスへの発信 PSTN コールを行い、「CMR Hybrid ダイヤル スクリプト」に従って DTMF トーンのシーケンスを入力します。

WebEx は、異なる TSP パートナーごとに一意のダイヤル スクリプトを決定して設定します。

（注） TSP Audio を使用するには、TelePresence と TSP パートナー音声ブリッジの間で音声カスケードを確立するために、顧客の TelePresence ブリッジが発信 PSTN コールを実行できる必要があります。ブリッジがコールを発信できることを確認するには、CMR ハイブリッド 用の PSTN 音声の設定, （161 ページ） を参照してください。

会議がスケジュールされた時間になると、電話番号と DTMF スクリプトが WebEx から TelePresence ブリッジ（MCU/TelePresence Server）に渡されます。

会議が開始されると、ブリッジは TSP 音声サービスに対して自動的に発信 PSTN コールを行い、DTMF スクリプトに従ってコールを音声会議に配置します。この音声カスケード接続が確立されると、WebEx ユーザと TelePresence ユーザが互いに会話できるようになります。

（注） この発信コールは、個々の TelePresence エンドポイントによって行われるものではありません。このコールはブリッジ自体によって行われます。会議に複数の TelePresence エンドポイントが存在する場合でも、行われる音声カスケード コールは 1 つだけです。

Telephony Service Provider（TSP）音声機能を展開するには、PSTN 音声が必要です。「CMR ハイブリッド 用の PSTN 音声の設定, （161 ページ）」のステップに従った後で、TSP 設定をサポートする WebEx クラウド サービスにお問い合わせください。

前提条件

TSP 音声を使用する WebEx サイトを含む CMR Hybrid の前提条件は次のとおりです。

- WebEx サイトが特に次の機能に関して CMR Hybrid なしで（TSP 音声を使用して）正常に機能すること。

WebEx 参加者が音声会議に正常にダイヤルインできること。

ダイヤルイン参加者が自分の参加者 ID を入力できること（したがって、「コールイン ユーザ 1」が WebEx 参加者リストのエントリに「マージ」されること）。

発言中の参加者の通知機能が正常に動作し、ビデオが発言中の参加者に切り替わること。

- TSP パートナーが CMR Hybrid と互換性があるかどうかは、WebEx によって確認されます。これは、事前に WebEx と TSP パートナーの間で直接手配されます。WebEx は確認された TSP パートナーのリストを管理します。そのリストが A2Q プロセスでチェックされた後、CMR Hybrid で TSP サイトが有効になります。

この WebEx と TSP パートナー間の手配/検証には、次の処理が含まれます。

TelePresence ブリッジが特定の TSP パートナーの音声会議に正常にダイヤルインするために必要な DTMF スクリプトを決定し、さまざまな条件でテストします。

DTMF スクリプトがホストとしてダイヤルインするか、または参加者としてダイヤルインするかを決定します（後者の方法では、WebEx から TSP パートナーに対してホストが存在しなくても音声会議を開く必要があることを示すシグナルを使用します）。

- 顧客の TelePresence ブリッジが発信 PSTN コールを確立し、応答後にコールを介して DTMF を入力できること。
- CMR Hybrid 会議で使用される WebEx ホスト アカウントが最初の（上記の）要件に従ってすでに正常に機能しており、WebEx ホスト アカウントの TSP 音声アカウント設定で市外局番が設定されていること。

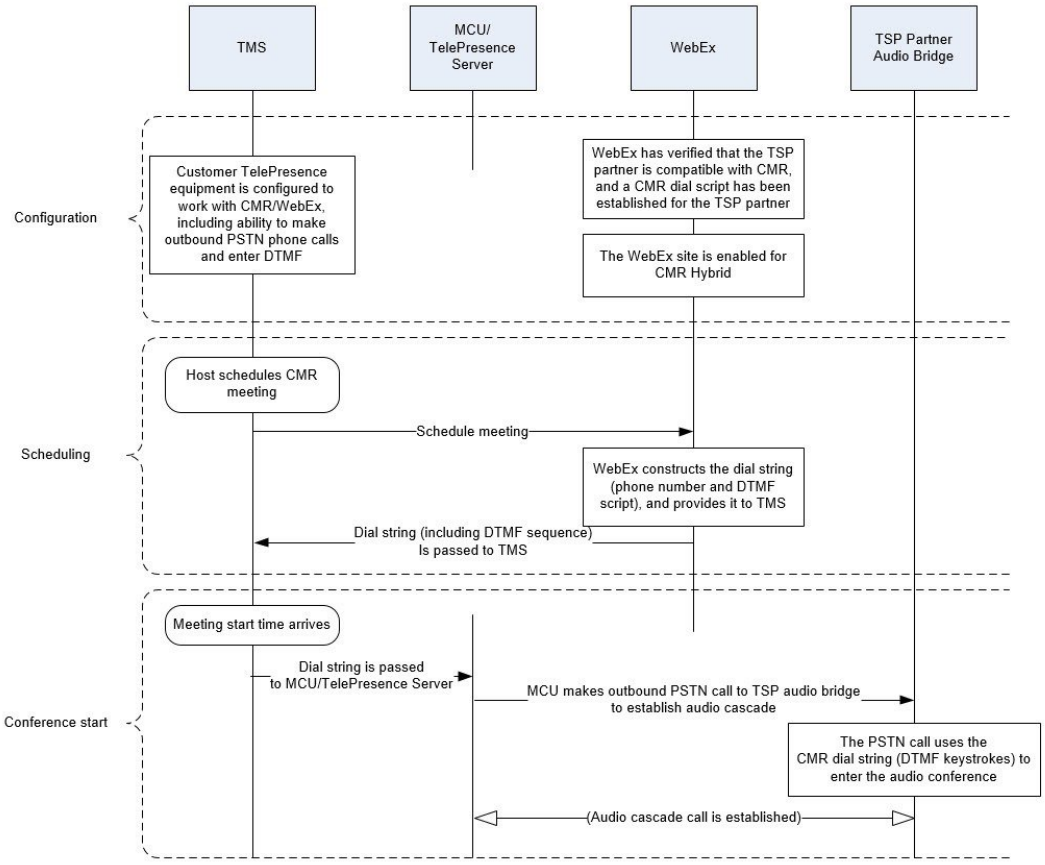
TSP 会議のしくみ

TSP 音声を使用する会議は、次のように実行されます。

1. 会議がスケジュールされます。
2. ダイヤル文字列が MCU/TelePresence Server に渡されます。
3. 最初の TelePresence 参加者がダイヤルインしたときに、MCU/TelePresence Server が会議を開始します。
4. TelePresence が SIP 経由で WebEx に接続します。
5. TSP パートナーが各自のブリッジで音声会議を開始し、会議を開きます。
6. TelePresence は、SIP 経由で WebEx に接続するのと同時に、DTMF ダイヤル文字列を使用して TSP パートナー ブリッジに PSTN 経由でダイヤルインします。

詳細な視覚的表現については、次の図を参照してください。

図 *11*：*TSP* 音声の設定、スケジュール、および会議開始の流れ



会議主催者の TSP 音声の設定

TSP 音声を使用する WebEx サイトでは、各 WebEx ホストの WebEx ホスト アカウントに TSP 音声アカウントが設定されている必要があります。これは、CMR Hybrid に限定された要件ではありません。CMR Hybrid が関与する会議を使用するかどうかに関係なく、TSP 統合音声を使用する WebEx 会議をホストでスケジュールできるようにする場合に必要です。

CMR Hybrid 会議で使用される WebEx ホスト アカウントがすでに正常に機能しており、WebEx ホスト アカウントの TSP 音声アカウント設定で市外局番が設定されていれば、これはすでに完了しています。しかし、ここでは TSP 音声アカウント設定について簡単に説明します。詳細については、TSP パートナーにお問い合わせください。

TSP 音声アカウントの前提条件

各 WebEx ホストには、TSP 音声サービス プロバイダーから提供される固有の TSP 音声アカウントが必要です。TSP 音声アカウントは次の情報で構成されます。

- コールイン番号（フリーダイヤル）
- コールイン番号（Call-in number）
- ホスト アクセス コード
- 参加者アクセス コード

WebEx ホスト アカウントの TSP 音声アカウントの設定

WebEx ホスト アカウントの TSP 音声アカウントを設定するには、次の手順を実行します。

手順

ステップ 1 ブラウザを開き、WebEx サイトに移動します。（例：http://example.webex.com）

ステップ 2 WebEx ホスト アカウントのクレデンシャルを使用してサイトにログインします。

ステップ 3 ページ上部の [My WebEx] をクリックします。

ステップ 4 ページ左側の [設定（Preferences）] をクリックします。

ステップ 5 [音声（Audio）] セクションの横にある [設定（Set up）] リンクをクリックします。

ステップ 6 [電話会議（Teleconference）] セクションまでスクロールします。（これにより、このホスト アカウント用にすでに設定されている既存の TSP 音声アカウントを確認できます）。

ステップ 7 [アカウントの追加（Add account）] をクリックします。これにより、[電話会議アカウントの追加（Add Teleconferencing Account）] ウィンドウが表示されます。

ステップ 8 [電話会議アカウントの追加（Add Teleconferencing Account）] ウィンドウで、TSP 音声サービス プロバイダーから提供された適切な電話番号とアクセス コードを入力します。

ステップ 9 [OK] をクリックします。

（注） WebEx ホスト アカウントの内部には、最大 3 つの別個の TSP 音声アカウントを設定できます。複数のアカウントが設定されている場合は、デフォルトとしてマークされたアカウントが CMR 会議に使用されます。

TSP サイトで使用される CMR Hybrid ダイヤル文字列に関する情報

ここでは、CMR Hybrid ソリューションの全体を理解するのに役立つ背景説明のみを提供します。顧客または CMR Hybrid 展開パートナーがダイヤル文字列を設定する必要はありません。

ここで説明した設定は、CMR Hybrid との互換性が確認されている TSP パートナーの一部として、WebEx と TSP パートナーの間で直接決定されます。

TSP 音声を使用する会議に接続するために、TelePresence ブリッジは TSP パートナーの音声ブリッジにダイヤルインし、事前に定義された DTMF トーンのスクリプトを使用して音声自動応答（IVR）の音声プロンプト フローをナビゲートします。各 TSP パートナーが使用する IVR メニュー プロンプトのセットは異なるため、各 TSP パートナーには固有の CMR Hybrid ダイヤル スクリプトがあります。

DTMF ダイヤル文字列の例

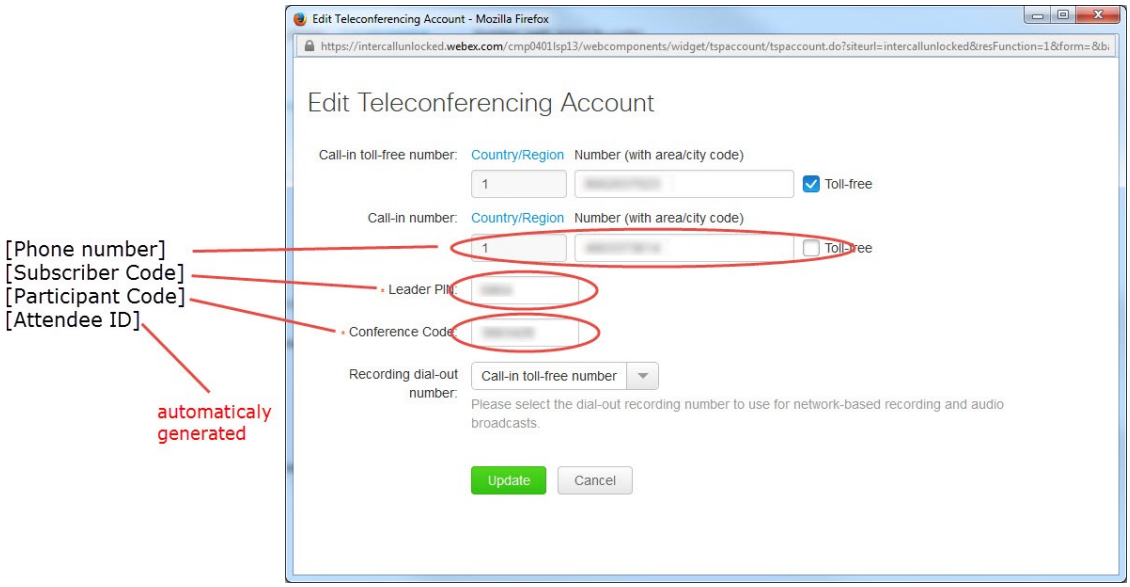
次に、TSP プロバイダーが DTMF ダイヤル文字列の生成に使用するシーケンスの例を示します。

1. 電話番号をダイヤルします（これは、会議開催者の WebEx ホスト アカウント内で設定されたデフォルト TSP 音声アカウントの市外局番です）。
2. 2 秒間、休止します
3. [参加者コード] DTMF 値を入力します。
4. # を入力します。
5. 6 秒間、休止します
6. # を入力します。
7. 20 秒間、休止します
8. #1 を入力します。
9. 0 秒間、休止します
10. [参加者 ID] DTMF 値を入力します。
11. # を入力します。

ダイヤル文字列の決定方法

TSP パートナーの CMR Hybrid ダイヤル スクリプトには、会議開催者の WebEx ホスト アカウント内のデフォルト TSP 音声アカウントのデータを使用して入力された変数が含まれます。

図 *12* : ***WebEx*** ホスト アカウント***/TSP*** 音声アカウント



第 15 章

Cisco WebEx Site Administration アカウントと Cisco TelePresence を統合する

Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合

固有の WebEx Site Administration URL とパスワードを使用して、WebEx Account Team 経由で Cisco WebEx Site Administration インターフェイスにアクセスできます。サイト管理者としてにログインし、初期設定時にアカウントを統合およびプロビジョニングする必要があります。初期設定が完了したら、アカウントを管理できます。また、Cisco TelePresence システムで設定されているサービスと機能に関して WebEx ユーザ ガイドと管理者ガイドを参照できます。

次の項に進み、初期設定を完了します。

- CMR ハイブリッド 用の Cisco WebEx Site Administration の設定，（172 ページ）
- Meeting Center TelePresence セッション タイプの割り当て，（173 ページ）

CMR ハイブリッド 用の Cisco WebEx Site Administration の設定

Cisco TelePresence を Cisco WebEx に統合するには、次の手順を実行します。

手順

ステップ 1 WebEx Site Administration URL のユーザ名とパスワードを使用して、WebEx Site Administration インターフェイスにログインします。
これは、WebEx サイトの URL の後にスラッシュ（/）と単語「admin」が付加されたものです。

例：https://example.webex.com/admin

ステップ 2 左側のナビゲーション バーの [サイトの管理（Manage Site）] で、[サイト設定（Site Settings）] を選択します。[サイト設定（Site Settings）] 画面が表示されます。

ステップ 3 [OneTouch TelePresence オプション（OneTouch TelePresence Options）] にスクロールします。

ステップ 4 [Cisco WebEx OneTouch 会議を許可する（MC のみ）（Allow Cisco WebEx OneTouch meetings (MC only)）] をクリックして選択します。
これを選択しないと、このサイトで Cisco WebEx が無効になり、残りの Cisco TelePresence Integration オプションがグレー表示になります。

ステップ 5 WebEx and TelePresence Integration to Microsoft Outlook を使って会議をスケジュールするオプションと共に CMR ハイブリッド ソリューションを展開する場合は、[Cisco TMS Booking Service の URL（Cisco TMS booking service URL）] フィールドに、TelePresence Management Suite Extension for Microsoft Exchange（TMSXE）のホスト アドレスを入力する必要があります。（例：https://tmsxe.example.com/TMSService/Booking.svc）
Cisco TMSXE の設定の詳細については、次を参照してください Cisco TelePresence Management Suite Extension for Microsoft Exchange を設定する，（145 ページ）

ステップ 6 [カレンダー上に Cisco TelePresence 会議をリストする（List Cisco TelePresence meetings on calendar）] をクリックして選択します。これにより、各ユーザによってホストされるスケジュール済み会議が WebEx サイトの [My WebEx 会議（My WebEx Meetings）] の下に表示されます。

（注） このオプションは、WebEx Meeting Center WBS29.13 では削除されています。TelePresence 会議は、ユーザが WebEx サイトでホストしている会議のリストに自動的に表示されます。ユーザが招待されている TelePresence 会議は、[My WebEx 会議（My WebEx Meetings）] の下に表示されません。

ステップ 7 [会議ホストへの招待メールの送信（Send invitation email to meeting host）] をクリックして選択します。これにより、会議のスケジュール後に、会議情報を記載した電子メールが Cisco WebEx ホストに送信されます。

ステップ 8 [参加者へのフリーダイヤル電話番号の表示（Display toll-free number to attendees）] をクリックして選択します。これにより、システムが参加者が会議参加のためにコールできるフリーダイヤル番号を表示できます。

ステップ 9 （オプション）TelePresence Welcome 画面を表示するには、[TelePresence Welcome 画面を表示する（Display TelePresence welcome screen）] をクリックして選択します。Welcome 画面には、会議に

接続中の参加者とその他の会議情報が表示されます。これは、参加者が共有しているコンテンツがない場合に表示されます。デフォルトでは Welcome 画面はオフです。

ステップ 10 （TSP 音声のみ）TSP 音声を展開する場合は、[TSP アイデンティティ コード（TSP identity code）] をクリックして選択し、TSP に関連付けられているコードを入力します（TSP に連絡して、この作業を行う必要があるかどうか、どんなコードを入力する必要があるか確認してください）。

（注） サイトで CMR ハイブリッド を設定する前に、TSP コールイン ユーザ マージ機能がすでに設定され、標準の WebEx 会議で機能している必要があります。

ステップ 11 [WebEx VoIP およびビデオ接続（WebEx VOIP and video connection）] セクションで、WebEx 会議アプリケーションとマルチメディア サーバ（VoIP およびビデオ）の間の接続方法を次のように選択します。

- [自動暗号化 UDP/TCP SSL（Automatically encrypted UDP/TCP SSL）]：（推奨）WebEx 会議アプリケーションで暗号化 UDP を使用してマルチメディア サーバに接続できるようにします。UDP 接続が許可されない場合、アプリケーションは SSL にフォールバックします。これは特に、WebEx アプリケーションとテレプレゼンス デバイスの間のトラフィックの輻輳を最小限に抑える必要がある場合に、最も柔軟性が高いオプションです。
- [TCP SSL]：WebEx 会議アプリケーションで SSL を使用してマルチメディア サーバに接続できるようにします。重要：TCP/SSL は、Cisco TAC から推奨される場合にのみ選択してください。それ以外の場合は、UDP を選択してください。

ステップ 12 （オプション）ユーザがこの WebEx サイトで VoIP 音声を使用できないようにするには、[ハイブリッド VOIP を無効にする（Disable Hybrid VOIP）] をオンにします。
これにより、CMR ハイブリッド 会議だけでなく、このサイトのすべての会議で VoIP が無効になります。

ステップ 13 ページの一番下までスクロールし、[保存（Save）] をクリックして設定を保存します。

次の作業

Meeting Center TelePresence セッション タイプの割り当て, （173 ページ） に進んで、設定を完了させてください。

Meeting Center TelePresence セッション タイプの割り当て

セットアップを完了するには、WebEx Site Administration インターフェイスでホストアカウントに Meeting Center TelePresence セッション タイプを割り当てる必要があります。それを行うには、個々のユーザの [ユーザの編集（Edit User）] 画面を開くか、[ユーザリストの編集（Edit User List）] 画面から各ユーザの適切なセッション タイプを選択します。新しいユーザを追加すると、デフォルトでこのセッションタイプが割り当てられます。次の項の手順に従い、このセッションタイプを確認または設定します。

- ユーザ リストでの Cisco TelePresence セッション タイプの追加, （174 ページ）

• [ユーザの編集（Edit User）] 画面での Cisco TelePresence セッション タイプの追加, （175 ページ）

カスタム セッション タイプのサポート

ユーザの特定のグループの WebEx 機能を制限できるカスタム セッション タイプを作成できます。たとえば、特定のユーザ グループに対して録画、チャット、および注釈を無効にするためのカスタム セッション タイプを作成できます。会議主催者が会議をスケジュールするときには、デフォルトの TelePresence セッション タイプが使用されます（これをカスタム セッション タイプに設定できます）。会議主催者が WebEx and TelePresence Integration to Outlook プラグインを使用して会議をスケジュールする場合、Site Administration レベルで設定されている他のカスタム セッション タイプを選択できます。WebEx サイト管理者は、特定のカスタム セッション タイプにアクセスできるユーザを決定できます。会議主催者が Cisco TMS、Smart Scheduler、または WebEx Scheduling Mailbox を使用してスケジュールを設定する場合、常にデフォルトの TelePresence セッション タイプが使用されます。WebEx サイトでカスタム セッション タイプを有効にするには、WebEx Cloud Services にお問い合わせください。有効になったら、左側のナビゲーション バーに移動し、[セッション タイプ（Session Types）] で [カスタム タイプの追加（Add Custom Type）] を選択して、カスタム セッション タイプを作成できます。カスタム セッション タイプの作成方法の詳細については、WebEx Site Administration のヘルプを参照してください。

ユーザ リストでの Cisco TelePresence セッション タイプの追加

手順

ステップ 1 左側のナビゲーション バーで、[ユーザの管理（Manage User）] の [ユーザリストの編集（Edit User List）] を選択します。[ユーザリストの編集（Edit User List）] 画面が表示されます。

ステップ 2 Meeting Center TelePresence セッション タイプを表す PRO 列を見つけます。
各 Cisco WebEx ユーザ アカウントには一連のセッション タイプ チェックボックスがあります。これは、そのユーザに対して有効にされている Cisco WebEx セッション タイプを示します。「Meeting Center TelePresence」は、「PRO」セッション タイプの 1 つです。（Meeting Center Pro 会議などの他のセッション タイプの見出しにも、「PRO」が含まれることがあります）Meeting Center TelePresence セッション タイプを示す列を判別するには、任意の「PRO」セッション タイプの見出しをクリックします。該当するセッション タイプの詳細を示す別ウィンドウが表示されます。[TelePresence でサポートされる機能（Supported Features in TelePresence）] というタイトルのセッション タイプ機能リストを示す列を見つけます。これが Meeting Center TelePresence セッション タイプです。

（注） セッション タイプの列の数は、WebEx サイトでサポートされるセッション タイプの数に基づいて決まります。

ステップ 3 ユーザに Meeting Center TelePresence セッション タイプが割り当てられていることを確認するには、[ユーザ編集（Edit User）] リストでそのユーザのエントリを見つけ、ステップ 2 で確認した適切な PRO セッション タイプのチェックボックスをオンにします。

ステップ 4 ページの一番下までスクロールし、[送信（Submit）] をクリックします。
Meeting Center TelePresence セッション タイプが見つからない場合、またはすべての「PRO」セッション タイプをクリックしても [TelePresence でサポートされている機能（Supported Features in TelePresence）] ウィンドウが表示されない場合は、このサイトはCMR Cloud 向けに正しく設定されていません。

（注） TelePresence 対応 WebEx サイトで [ユーザの追加（Add User）] リンクを使用して新しいホスト アカウントを作成すると、このセッション タイプがデフォルトで割り当てられます。CMR ハイブリッド会議をスケジュールするには、ユーザにこのセッション タイプが割り当てられている必要があります。このサイトが CMR Cloud に更新された既存のサイトである場合、既存のユーザに Meeting Center TelePresence セッション タイプを追加する必要があります。

[ユーザの編集（Edit User）] 画面での Cisco TelePresence セッション タイプの追加

また、個々のユーザのアカウント設定でも Meeting Center TelePresence セッション タイプを設定できます。[ユーザの管理（Manage Users）] > [ユーザリストの編集（Edit User List）] ページで、次の操作を実行します。

手順

ステップ 1 ユーザ エントリを見つけてクリックします。そのアカウントの [ユーザの編集（Edit User）] ウィンドウが開きます。

ステップ 2 [特権（Privileges）] セクションにスクロールします。割り当てられているセッション タイプが、[許可されているセッション タイプ（Session Type Allowed）] ボックスに表示されます。

ステップ 3 必須作業です。[許可されているセッション タイプ（Session Type Allowed）] [p.1] の赤色で囲んだ部分に示すように、[PRO: Meeting Center TelePresence] ボックスをオンにします。

ステップ 4 ウィンドウ下部にある [更新（Update）] ボタンをクリックして、PRO: Meeting Center TelePresence セッション タイプの設定を保存します。
これで、Cisco WebEx Site Administration での Meeting Center の Cisco TelePresence セッション タイプ特権の設定が完了しました。Cisco WebEx アカウントが完全に統合およびプロビジョニングされました。

（注） 機能をアップグレードする場合は、Cisco WebEx の営業担当者にお知らせください。

CMR ハイブリッド 会議のネットワーク ベースの録画

会議主催者は、CMR ハイブリッド 会議を録画できます。

会議主催者は、CMR ハイブリッド 会議を録画できます。

- WebEx and TelePresence Integration to Outlook および WebEx Meeting Center クライアントは、録画が有効であるかどうかを自動的に検出し、該当するメッセージを表示します。
- 録画された会議を再生すると、WebEx と TelePresence の両方のビデオが、コンテンツ共有、チャット、およびポーリング（有効な場合）と共に表示されます。
- ユーザは、再生コントロールを使用するかビデオのサムネイルをクリックすることで、録画内を移動できます。
- 参加者の発言時には、録画の中で視覚的表現がユーザに表示されます。

（注） ネットワーク ベースの録画は WebEx Cloud Services によって有効にされます。

WebEx and TelePresence Integration to Outlook のインストール

はじめる前に

インストールする前に、WebEx サイトと TMSXE に関する次の情報がわかっていることを確認してください。

- WebEx サイトの URL
- WebEx ユーザ名
- WebEx パスワード
- TMSXE ユーザ名
- TMSXE パスワード

（注） この情報については、WebEx または IT 管理者にお問い合わせください。

手順

ステップ 1 ブラウザを開き、WebEx サイトに移動します。

ステップ 2 [My WebEx] をクリックします。

ステップ 3 アカウントにログインします。

ステップ 4 ユーザに対して WebEx 生産性向上ツールのダウンロードを自動的に促すようにサイトが設定されている場合は、そのオプションが表示されます。その場合は [はい（Yes）] をクリックしてダウンロードを開始した後、ステップ 7 に進みます。それ以外の場合は次のステップに進みます。

ステップ 5 左側のナビゲーション バーで、[生産性向上ツールの設定（Productivity Tools Setup）] をクリックします。

ステップ 6 `ptools.msi` ファイルがコンピュータにダウンロードされます。

ステップ 7 ダウンロードが完了したら、ptools.msi を開き、画面に表示される指示に従って WebEx 生産性向上ツールをインストールします。

ステップ 8 インストール中に、WebEx サイトにログインする必要があります。

ステップ 9 WebEx サイトの URL、ユーザ名、パスワードを入力し、[ログイン（Login）] をクリックします。

ステップ 10 ログイン後、WebEx 生産性向上ツールがサーバと通信して、Cisco TelePresence Management Suite Extension for Microsoft Exchange（Cisco TMSXE）にログインするように求められます。

ステップ 11 TMSXE のユーザ名とパスワードを入力し、[OK] をクリックします。

ステップ 12 「WebEx 生産性向上ツールがインストールされました（WebEx Productivity Tools are installed）」というメッセージが表示されたら、[OK] をクリックします。

ステップ 13 [生産性向上ツール（Productivity Tools）] ウィンドウを閉じます。
これで、Microsoft Outlook を開き、WebEx and TelePresence Integration to Outlook を使用して CMR Cloud 会議をスケジュールできます。

ユーザの WebEx アカウントのタイム ゾーンと言語の設定

最適な結果を得るには、Outlook を使用してスケジュールを設定する会議主催者が次の手順を実行する必要があります。

- WebEx と Outlook のタイム ゾーンを同じタイム ゾーンに設定します。会議主催者の WebEx と Outlook のタイム ゾーンが一致しない場合は、WebEx と Outlook で同じ時刻に会議がスケジュールされません。
- WebEx アカウントで優先言語が選択されていることを確認します。選択した言語は、会議への招待状ですべての招待者に対して表示される言語です。

手順

ステップ 1 ブラウザを開き、WebEx サイトに移動します。

ステップ 2 [My WebEx] をクリックします。

ステップ 3 WebEx ユーザ名とパスワードを入力して、[ログイン（Log In）] をクリックします。

ステップ 4 WebEx 生産性向上ツールをダウンロードするオプションが表示される場合、すでにダウンロード済みであれば [後で（Later）] をクリックします。このツールをダウンロードして今すぐインストールする場合は、「WebEx and TelePresence Integration to Outlook のインストール」のステップ 4 を参照してください。
[My WebEx 会議（My WebEx Meetings）] ページが表示され、ページの右隅に、現在の言語とタイム ゾーンの設定が表示されます。

ステップ 5 言語とタイムゾーンを変更するには、現在の言語またはタイムゾーンのいずれかを示すリンクをクリックします。
[設定（Preferences）] ページが表示されます。

ステップ 6 [タイムゾーン（Time zone）] メニューと [言語（Language）] メニューを使用して、CMR Hybrid 会議に使用するタイム ゾーンと言語を選択します。

ステップ 7 [OK] をクリックします。

ユーザの WebEx アカウントの TSP 音声の設定

TSP Audio を使用する CMR ハイブリッド会議をスケジュールする必要がある会議主催者は、自分のアカウントに TSP Audio プロバイダー情報を追加する必要があります。

詳細については、「CMR ハイブリッドの TSP Audio の設定」を参照してください。

次の作業

Cisco WebEx 管理サイト アカウントの管理の詳細については、WebEx サイトのヘルプを参照してください。https://go.webex.com/docs/T27LB/common_docs/en_US/siteadmin/help/wwhelp/wwhimpl/js/html/wwhelp.htm

第 16 章

CMR Hybrid 会議を管理する

はじめに

この章では、TMS を使用して CMR ハイブリッド 会議をスケジュールする方法の概要と、CMR ハイブリッド 会議に関する役立つ情報、ヒント、既知の問題について説明します。

CMR ハイブリッド 会議をスケジュールする方法としては、TMS を使用したスケジュールの他に 3 つの方法があります。

- Cisco WebEx and TelePresence Integration to Outlook の使用

WebEx and TelePresence Integration to Outlook を使用すると、ユーザは Windows で Microsoft Outlook から CMR ハイブリッド 会議を直接スケジュールできます。外部のビデオおよび音声ダイヤルイン参加者の追加など、詳細オプションも使用できます。

スケジュールについては、『WebEx and TelePresence Integration to Outlook Quick Reference Guide』を参照してください。

他のユーザの代理として会議をスケジュールする方法、会議をスケジュールする代理人を割り当てる方法などの追加情報については、WebEx and TelePresence Integration to Outlook のヘルプ（Outlook で利用可能）、またはユーザ ガイド（WebEx サイトで利用可能）を参照してください。

- Cisco Smart Scheduler の使用

Cisco Smart Scheduler を使用すると、Macintosh、モバイル、その他の非 Windows ユーザが、タッチスクリーンに対応したシンプルな Web ベースのインターフェイスを使用して CMR ハイブリッド 会議をスケジュールできます。

スケジュールについては、『Cisco Smart Scheduler and WebEx Scheduling Mailbox Quick Reference Guide』を参照してください。

サポートされるブラウザとモバイル プラットフォームなどの詳細については、Cisco TelePresence Management Suite Provisioning Extension（TMSPE）のリリース ノートを参照してください。

- Cisco WebEx Scheduling Mailbox の使用

Cisco WebEx Scheduling Mailbox を使用すると、WebEx and TelePresence Integration to Outlook を使用しないユーザが、Outlook で TelePresence 対応 WebEx 会議を作成できます。そうするには TelePresence 会議室を招待し、特別な招待先として WebEx Scheduling Mailbox を組み込むことで会議に WebEx を追加します。

このメールボックスは単に「webex」などと呼ばれることがあります。これは管理者により設定され、ユーザに提供されます。

詳細については、『Cisco TelePresence Management Suite Extension for Microsoft Outlook（TMSXE）Installation Guide』と TMSXE のリリース ノートを参照してください。

スケジュールについては、『Cisco Smart Scheduler and WebEx Scheduling Mailbox Quick Reference Guide』を参照してください。

CMR Hybrid 会議のスケジュール

手順

ステップ 1 Cisco TMS にログインします。

ステップ 2 [予約（Booking）] > [新しい会議（New Conference）] に進みます。

ステップ 3 [タイトル（Title）]に、会議のタイトルを入力します。これは、すべての Cisco TMS インターフェイスと会議に関する電子メール通知に表示されます。

ステップ 4 [タイプ（Type）] で [自動接続（Automatic Connect）] または [ワンボタン機能（One Button to Push）] を選択します。[自動接続（Automatic Connect）]：会議の開始時に、Cisco TMS がすべての参加者を自動的に接続します。

（注） [ワンボタン機能（One Button to Push）]：ワンボタン機能に対応したエンドポイントに、会議ダイヤルイン情報が自動的に表示されます。これらのエンドポイントの参加者は、ボタンを押して会議に参加します。ワンボタン機能に対応していないエンドポイントでは、会議主催者がビデオ ダイヤルイン番号を追加します。その他のタイプについては、TMS のヘルプを参照してください。

ステップ 5 会議の [開始時刻（Start Time）] と [終了時刻（End Time）]、または [期間（Duration）] を設定します。

ステップ 6 [WebEx 会議を含める（Include WebEx Conference）] がオンであることを確認します。

ステップ 7 オプションで、[WebEx 会議のパスワード（WebEx Meeting Password）] を入力します。
パスワードを入力しない場合、WebEx によって自動的にパスワードが生成されます。会議のスケジュールが正常に完了すると、パスワードが [確認（Confirmation）] ページに表示されます。

ステップ 8 オプションで、毎週または毎日の会議など、一連の関連する会議を作成するには[定例会議の設定（Recurrence Settings）] をクリックします。
詳細設定はオプションです。ほとんどの設定のデフォルト値には、管理ツールで設定された会議デフォルト値が使用されます。使用可能なすべての設定の概要については、ヘルプを参照してください。[詳細設定（Advanced Settings）] の詳細については、Cisco TMS の [ヘルプ（Help）] ボタンをクリックしてください。
[セキュア（Secure）] が [はい（Yes）] に設定されている場合、Cisco TMS では、暗号化をサポートするシステムだけが会議に参加できます。

ステップ 9 オプションで、会議の招待状に表示される [会議情報（Conference Information）] に、会議に関するメモを追加します。

ステップ 10 [参加者（Participant）] タブで [参加者の追加（Add Participant）] をクリックします。新しいウィンドウが表示されます。

ステップ 11 既存のスケジュール済み会議およびアドホック会議に基づいて、選択可能な参加者と、参加者の可用性を示すプランナー ビューが表示されます。カラーの縦線は、スケジュール済み会議に対する現在の要求時間を表しています。

ステップ 12 参加者をタイプ別に表示するには、各タブをクリックします。以前にスケジュールを使用したことがある場合、デフォルトのタブは、最近使用したシステムにすばやくアクセスできる [前回の使用（Last Used）] になります。

ステップ 13 システムまたはスケジュール済み会議の詳細を確認するには、プランナー ビューでシステムまたはブロック上にカーソルを合わせます。

ステップ 14 会議に参加者を追加します。そうするには、参加者のチェックボックスをオンにし、ボタンをクリックして、ウィンドウ右側の選択された参加者のリストに参加者を追加します。MCUやゲートウェイなどのネットワークインフラストラクチャコンポーネントの追加は、オプションです（Cisco TMS によってこの操作が自動的に行われます）。

ステップ 15 Cisco TMS によって管理されないシステム（他の組織のエンドポイントや電話参加者など）を追加するには、[外部（External）] タブを使用します。

ステップ 16 ダイヤルアウト参加者の場合、その連絡先情報を入力します。Cisco TMS は、スケジュールされた時間に参加者を会議に自動的に接続します。

ステップ 17 ダイヤルイン参加者（ワンボタン機能をサポートしないエンドポイントを含む）の場合、Cisco TMS は会議でサイトをホストするために必要な容量を予約し、参加者に転送する正確なダイヤルイン情報を提供します。

ステップ 18 すべての参加者を追加したら、[OK] をクリックします。
会議ページが再び表示されます。このページの参加者セクションには、選択した参加者といくつかの追加タブが表示されます。これらの追加タブでは、コール接続方法の変更、会議の特定の MCU 会議設定などの拡張スケジュール作業を実行できます。

ステップ 19 [ビデオ会議マスター（Video Conference Master）] ドロップダウン リストを使用して、どのシステムを会議主催者とみなすかを決定します。一部のテレプレゼンス システムは、この機能に必要な要件を満たしません。要件を満たすシステムだけがこのリストに表示されます。これは、自動化

されたコールの開始がスケジュールされていない場合、会議を接続するようプロンプトが表示されるシステムです。

ステップ 20 [会議の保存と有効化（Save Conference）] をクリックします。会議が保存されると、Cisco TMS はすべてのルーティング計算を実行し、選択された参加者を接続する最適な方法を判別します。Cisco TMS が要求を完了できる場合、確認画面が表示されます。ここには会議が保存されたことが示され、会議の詳細情報（参加者リスト、各参加者の会議への接続がどのようにスケジュールされているか、参加者がダイヤルする必要のある正確なダイヤル文字列など）が表示されます。確認電子メールを送信するように WebEx サイトが設定されている場合、WebEx からさらに 2 つの追加電子メール通知を受け取ります。1.「会議がスケジュールされました（Meeting Scheduled）」という件名の電子メール。これには、ホストキーと会議の WebEx 情報が含まれています。2.「（参加者へ転送）会議の招待状（(Forward to attendees) Meeting Invitation）」という件名の電子メール。これには参加者の WebEx 情報だけが含まれています。

Cisco TMS が予約要求を完了できない場合は、[新しい会議（New Conference）] ページに戻ります。メッセージ バナーに、会議を保存できなかった理由が示されます。可用性の欠落、ネットワーク リソースの不足、またはすべての参加者を接続するためのルートが不明なことなどが原因である可能性があります。

この場合、次のチェックを実施します。

1. 会議の設定を編集して、問題を解決し、会議を再度保存してください。
2. 会議のスケジュールが正常に完了したら、カレンダーアプリケーションを使用して会議に参加者を招待します。

会議の開始/会議への参加

会議は次の手順で開始できます。

- 任意の時間に、主催者が参加して会議を開始できます。
- 会議のスケジュールされた開始時刻に、MCU/TelePresence Server が WebEx にコールします。
  - WebEx ホストが会議に参加していない場合、MCU/TelePresence Server がデフォルトの WebEx ホストになります。
  - WebEx ホストが会議のスケジュールされた開始時刻よりも前に参加する場合、そのホストが WebEx ホストになります。
- サイトで「Join Before Host」機能が有効になっている場合、主催者が WebEx と TelePresence の Outlook への統合機能を使用して会議をスケジュールする際に [出席者は開始時間より前に会議に参加可能（Attendees Can Join Meeting Before Starting Time）] を設定していれば、参加者は（主催者の設定に応じて）スケジュールされた時間の 5 分、10 分、または 15 分前から会議に参加できます。これが設定されていない場合、主催者が会議を開始するまで、参加者は会議に参加できません。

- TelePresence 参加者が会議に参加します。
  - 自動接続を使用してスケジュールされた会議の場合、Cisco TMS はサポートされている各エンドポイントにダイヤルして接続します。
  - ワンボタン機能（OBTP）を使用してスケジュールされた会議の場合、OBTP に対応したエンドポイントを使用する参加者が、エンドポイントのボタンを押して会議に参加します。
  - 自動接続と OBTP のいずれもサポートされていないエンドポイントを使用する参加者は、会議への招待状にリストされているビデオ ダイヤルイン番号をダイヤルして会議に参加します。
- WebEx 参加者は、会議への招待状にあるリンクを使用して会議に参加します。

Cisco WebEx プレゼンテーションの共有

次に、WebEx の参加者がプレゼンテーションを TelePresence およびそのほかの WebEx 参加者と共有する方法を示します。

手順

ステップ 1 コンピュータの Cisco WebEx Meeting Center アプリケーションにログインします。

ステップ 2 ボールを取得するか、WebEx ホストからプレゼンターとして指定されるようにします。

ステップ 3 [クイック スタート（Quick Start）] タブで、[アプリケーションの共有（Share Application）] をクリックします。

ステップ 4 アプリケーションまたはデスクトップの共有を開始します。

（注） サポートされるモバイル クライアントの一覧については、CMR ハイブリッド のリリース ノートを参照してください。

会議についての情報、ヒント、既知の問題

ここでは、CMR ハイブリッド 会議に関する役立つ情報（ヒントと既知の問題など）を説明します。CMR ハイブリッド Solution に含まれる各製品に対応する項に分かれています。

Cisco TMS

- 予約の前に Cisco TMS 管理者による会議の承認を義務付けるよう、Cisco TMS を設定できます。ポートの使用を制限/調整する必要がある企業では、この機能を使用してポートの使用を調整できます。

- Cisco TMS は、ポートの数を、スケジュール時に Cisco TMS 会議の [外部（External）] タブで選択された数に制限します。
- TelePresence および WebEx の両方では、会議のスケジュール時に [延長モード（Extend Mode）] 設定を使用することで、会議の延長がサポートされます。会議の延長は保証されていません。スケジュールされた会議終了時刻の時点でリソース（ポート）がすべて予約されている場合は、会議が終了します。
- WebEx and TelePresence Integration to Outlook を使用して会議をスケジュールする会議主催者は、その後 Cisco TMS でその会議を変更してはなりません。

後で Cisco TMS で元の会議を変更すると、Cisco TMS でのその会議の情報が、会議主催者の Outlook カレンダーと同期していない状態になります。その理由は、Cisco TMSXE には会議主催者のカレンダーへの書き込みアクセス権がないので、カレンダーを変更できないためです。

MCU および TelePresence Server

- TelePresence Conductor を使用すると、最初のテレプレゼンス参加者が会議に参加した後で、MCU/TelePresence Server が WebEx を呼び出します。
- TelePresence Conductor を使用しない場合、MCU/TelePresence Server は、テレプレゼンスまたは WebEx の参加者がいなくても、会議の開始時に WebEx を呼び出します。
- MCU/TelePresence Server の役割は、通常の WebEx 参加者とは異なります。会議に参加した時点で、その会議に会議ホストがいない場合、MCU がデフォルトのホストとなって会議を開始します。
- WebEx ホストがすでに存在する場合は、MCU/TelePresence Server はホストになりません。
- WebEx ホストが会議を退席すると、MCU/TelePresence Server がホストになり、会議は継続されます。
- WebEx ホストが会議を退席する前に MCU/TelePresence Server が会議を退席した場合、会議は継続されます。
- WebEx ホストが退席した後で MCU/TelePresence Server が会議を退席した場合、会議は終了します。
- MCU/TelePresence Server が退席した後で WebEx ホストが会議を退席した場合、会議は終了します。
- MCU/TelePresence Server が退席した後で WebEx ホストが引き続き会議にとどまる場合、WebEx 会議は継続されます。
- デフォルトでは、TelePresence Server が ActivePresence 画面レイアウトでビデオを送信します。このレイアウトでは、発言中の参加者が全画面ペインに表示され、その他の参加者が画面下部の最大 6 つの同一サイズのオーバーレイ ペインに表示されます（2 画面エンドポイントと 4 画面エンドポイントの場合は最大 4 つのペイン）。WebEx の全画面モードでは、WebEx 参加者がウィンドウ下部の TelePresence ビデオの下の、同一サイズのペインに表示されます。デフォルトでは、MCU はビデオを全画面レイアウトで送信します。

エンドポイント

- 任意の TelePresence エンドポイントから会議に参加する参加者が、エンドポイントをコンピュータ モニタとして使用している場合は、これらの参加者に WebEx からのプレゼンテーションが表示されないことがあります。
- EX60 から提供されるコンテンツが表示されるまでに時間がかかることがあります。エンドポイントが Unified Communications Manager に登録されている場合、Unified Communications Manager で User-Agent パススルーを有効にすることで、これを解決できます。

Cisco TMSXE

Web Scheduling Mailbox を使用して会議を予約するときに、TMSXE がエラー状態（WebEx サーバに接続できないなど）を検出すると、エラーを通知する電子メールがプレーン テキスト形式で会議主催者に送信されます。

WebEx

- WebEx Meeting Center では、TelePresence ユーザが発言中である場合および参加者リストの両方で、すべての TelePresence エンドポイントが「TelePresence システム（TelePresence systems）」という 1 つの WebEx 参加者として表示されます。
- Meeting Center の全画面ビューでは、「TelePresence システム（TelePresence systems）」参加者は、黒色のシルエットとして表示されます。
- WebEx ホストは、参加者が会議に参加した後で、参加者全員または個別の参加者をミュートにできます。WebEx クライアントで TelePresence 参加者をミュートにすることはできません。TelePresence 参加者は、自分自身をミュートにする必要があります。
- WebEx 参加者をミュートにするには、WebEx ホストでなければなりません。

ホストの役割を再度取得するには、WebEx ホスト キーを取得する必要があります。

- 会議は、その会議の最初の参加者（ホストまたは他の WebEx 参加者）によって開始されます。他の参加者は会議に「参加」します。
- WebEx の音声のみの参加者が発言する場合、次のビデオ参加者が発言するまでは、直前に発言したビデオ参加者が表示されます。
- Outlook と WebEx の両方で会議を正しい時刻にスケジュールするには、ユーザの Outlook タイム ゾーンと WebEx アカウントのタイム ゾーンが同一でなければなりません。
- 会議の WebEx 部分が終了すると、音声も終了します。

第 17 章

CMR Hybrid をトラブルシュートする

検証とテスト

Cisco WebEx Site Administration オンライン ヘルプ

Cisco WebEx Site Administration の使用に関する詳細については、次のように Cisco WebEx Site Administration のヘルプを参照してください。

手順

ステップ 1 WebEx サイトの Site Administration にログインします。これは、WebEx サイトの URL の後にスラッシュ（/）と単語「admin」が付加されたものです。
例：https://example.customer-a.webex.com/admin

ステップ 2 ページ左側の [アシスタンス（Assistance）] の下の [ヘルプ（Help）] リンクをクリックします。

トラブルシューティングのヒント

ここでは、CMR ハイブリッド 会議の次のような問題に関するトラブルシューティングのヒントを説明します。

- 会議の開始または参加に関する問題, （190 ページ）
- 会議の進行中に発生する問題, （192 ページ）
- TSP 音声会議に関する問題, （199 ページ）
- TelePresence Server および MCU に関する問題, （203 ページ）

会議のスケジュールに関する問題

ここでは、会議主催者が Cisco TMS を使って会議をスケジュールする際に発生する可能性のある問題について説明します。

次の表で、会議を正しくスケジュールできない原因となる一般的な問題の解決方法を示すトラブルシューティング情報を確認できます。

表 *19*：会議のスケジュールに関する問題

問題またはメッセージ	考えられる原因	推奨処置
会議主催者が、会議がスケジュールされたことを確認する電子メールを Cisco TMS から受信しません。	Cisco TMS が、確認電子メールを送信するように設定されている。	Cisco TMS 設定を確認します。 Cisco TMS 設定が正しい場合は、アンチウイルス/ファイアウォールプログラムを調べて、Cisco TMS からの送信がブロックされているかどうか確認します。
会議主催者が TMS を使用して会議をスケジュールした後、「WebEx との通信中に予期しないエラーが発生しました。（An unexpected error occurred while communicating with WebEx.）」というエラーが表示されます。会議は作成されましたが、WebEx の設定に問題があります。会議確認メールを受信しますが、WebEx の情報がそれに含まれていません。	会議主催者の WebEx ホスト アカウントが、Meeting Center TelePresenceセッション タイプでプロビジョニングされていない。	WebEx サイトの WebEx Site Administration にログインし、会議主催者のホスト アカウントで [Meeting Center TelePresence] セッション タイプが有効になっていることを確認します。詳細については、Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合, （171 ページ）を参照してください。

問題またはメッセージ	考えられる原因	推奨処置
会議がエンドポイントのディスプレイにリストされません。	複数のスケジューリング サーバがそのエンドポイントを管理している（例：Cisco TMS と CTS-Manager が同時に管理している場合など）。 その他の原因： • スケジュール済み会議のタイプがワンボタン（OBTP）でない。エンドポイントには OBTP 会議だけが表示されます。 • エンドポイントと Cisco TMS の間のネットワーク接続で障害が発生している。	1 つのエンドポイントを除くすべてのエンドポイントにプッシュされる場合は、ネットワーク接続を確認します。 どのエンドポイントにもプッシュされない場合は、Cisco TMS がダウンしているかどうかを確認します。 [管理ツール（Administrative Tools）] > [設定（Configuration）] > [WebEx設定（WebEx Settings）] で、WebEx サイトを選択し、[接続ステータス（Connection Status）] が [接続OK（Connection OK）] であることを確認します。
（[保存（Save）]をクリックすると）Cisco TMS で WebEx スケジュール エラーが発生します。 症状：Cisco TMS に「WebEx 会議を含めることができません」と表示される。WebEx ユーザ名またはパスワードが正しくありません。	WebEx サイトでネットワークの問題が発生している。 WebEx ユーザが WebEx サイトに存在しない。 原因：この主催者に関して設定されている WebEx サイトが、会議主催者に関して設定されている WebEx ユーザ名とパスワードを認識しない。	WebEx アカウント ユーザ プロファイルを確認します。 推奨処置：ユーザ個人情報ページで WebEx サイトの WebEx ユーザ名/パスワードを確認します。また、WebEx サイト ユーザ クレデンシャル情報が変更されている可能性もあります。この場合は、WebEx サイト管理者にお問い合わせください。 Cisco TMS トラブルシューティング情報を参照してください。この問題は Cisco CMR Hybrid に限定されていません。
WebEx から確認電子メールが送信されません	WebEx サイトで電子メールが有効になっていない	WebEx サイト管理者にお問い合わせください。
会議が TMS で予約されていますが、WebEx が存在しません。	会議に予約されているエンドポイントが Exchange でメールボックスとして設定されているが、招待状の AutoAccept が設定されていない。	CMR Hybrid 会議で予約用のメールボックスとして使用できるすべてのエンドポイントを、Exchange で AutoAccept に設定する必要があります。

問題またはメッセージ	考えられる原因	推奨処置
「TelePresence スケジューリング システムで問題が発生しました。しばらくしてから再試行してください。（We've hit a glitch in connecting to the telepresence scheduling system.）」	TMSXE	TMSXE 管理者にお問い合わせください。
TMS での会議のスケジュール設定時に WebEx オプションが表示されません。	WebEx ユーザ名とパスワードが TMS ユーザ プロファイルにまだ追加されていない。	TMS ユーザを編集し、WebEx ユーザ名とパスワードを入力して保存します。これで、WebEx オプションが TMS スケジューリング UI に表示されます。

会議の開始または参加に関する問題

ここでは、会議参加者が会議を開始したり会議に参加したりするとき発生する可能性のある問題について説明します。

参加者による会議の開始または参加を妨げる一般的な問題を解決する方法については、次の表のトラブルシューティング情報を参照してください。

表 *20*：会議の開始または参加に関する問題

問題またはメッセージ	考えられる原因	推奨処置
WebEx 会議に参加できません	会議がまだ開始されていない	会議の開始を待機します
どのエンドポイントも TelePresence 会議に参加できません。	TelePresence 会議が存在しない。 コールを正しくルーティングできなかった。	1.MCU/TelePresence Server を調べて、会議が作成されたことを確認します。 2.MCU/TelePresence Server のイベント ログを調べます。 3.VCS 検索履歴を調べます。
TelePresence 会議が早期に開始しませんでした。「会議の早期開始」が機能しませんでした。	Cisco TMS スケジュール済み会議では、早期開始がサポートされていません。エンドポイントは、会議が開始するまで待ってダイヤルインする必要があります。	セットアップ バッファとティア ダウン バッファの設定を調べます。

問題またはメッセージ	考えられる原因	推奨処置
1 人の TelePresence 参加者が会議に参加できません。	ビデオ ポートと音声ポートが不足している。 エンドポイントから MCU または TelePresence Server へのコール ルーティングの問題	会議のイベント ログを調べます。さらに、TelePresence Server または MCU で会議を調べます。 管理者は [TelePresence Server 会議（TelePresence Server Conferences）] ページでポート値を変更することで、この制限を取り除くことができます。
TelePresence 参加者が音声でしか参加できません。	ビデオポートが不足している。	Cisco TMS、TelePresence Server または MCU のビデオ ポートを増やします。
すべての TelePresence 参加者が会議に参加できません	会議がまだ開始されていない。Cisco TMS スケジュール済み会議では、早期開始がサポートされていません。エンドポイントは、会議が開始するまで待ってダイヤルインする必要があります。 MCU/TelePresence Server の音声ポートおよびビデオ ポートがすべて使用中。もう 1 つの原因は、会議のポートのビデオ/音声制限に達したことです。	MCU/TelePresence Server のポート合計容量に達した場合、必要な操作はありません。 会議の制限に達した場合は、管理者が [TelePresence Server 会議（TelePresence Server Conferences）] ページでこの制限を取り除くことができます。
WebEx ホストが会議に参加した後で、MCU/TelePresence Server が切断します。	WebEx ホストが現在、別の会議に参加しており、その会議でもホストになっている。	同じ WebEx ホスト ID を使用して複数の会議に同時に参加しないでください。 1 つのホストが一度に実行できる CMR Hybrid 会議は 1 つだけです。
自分が招待された CMR Hybrid 会議が、自分の WebEx サイトの [My WebEx 会議（My WebEx Meetings）] の下に表示されません。	ユーザが招待されている CMR Hybrid 会議は、[My WebEx 会議（My WebEx Meetings）] の下に表示されません。	なし。[My WebEx 会議（My WebEx Meetings）] の下に表示されるのは、ユーザがホストする CMR Hybrid 会議だけです。

会議の進行中に発生する問題

ここでは、会議の進行中に会議参加者に発生する可能性のある問題について説明します。

会議の進行中に発生する一般的な問題を解決する方法については、次の表のトラブルシューティング情報を参照してください。

表 *21*：会議の進行中に発生する問題

問題またはメッセージ	考えられる原因	推奨処置
WebEx Welcome 画面が表示されません	MCU でコンテンツが無効になっている。 MCU/TelePresence Server から WebEx へのビデオ コールが失敗した。接続はさまざまな原因で失敗することがあります。 • 解決不能な SIP URI が原因で、WebEx SIP ダイヤルが接続先に到達できない • WebEx サーバがダウンしている • VCS の検索ルールの問題 • VCS でのメディア暗号化設定	• MCU の設定および会議ステータスを確認します。 • 検索ルールを検証し、SIP URI が WebEx サイトに正しくルーティングされることを確認します。 • VCS でこのゾーンの暗号化設定を確認します。 • 上記の操作を行ってもエラーが解決しない場合は、WebEx サイト管理者にお問い合わせください。
TelePresence が WebEx にリンクされません	MCU/TelePresence Server から WebEx へのビデオ コールが失敗した。接続はさまざまな原因で失敗することがあります。 • 解決不能な SIP URI が原因で、WebEx SIP ダイヤルが接続先に到達できない • WebEx サーバがダウンしている • VCS の検索ルールの問題 • VCS でのメディア暗号化設定	-

問題またはメッセージ	考えられる原因	推奨処置
WebEx でビデオが表示されません	WebEx 参加者がビデオを有効にしていない。 WebEx 参加者のカメラに問題がある。	• TelePresence および WebEx コールが接続されていることを確認します。 • TelePresence に接続した参加者がビデオを送信しているかどうかを確認します。

問題またはメッセージ	考えられる原因	推奨処置
Windows または Mac の WebEx Meeting Center クライアントで低帯域幅の警告が表示されます 「現在、帯域幅が低いため、TelePresence ビデオを表示できません（Due to low bandwidth, we are not able to show TelePresence video at the moment）」	• WebEx Meeting Center クライアントに使用可能な帯域幅が不足している。 • ダウンスピードがビデオ解像度 180p を下回っている。	

問題またはメッセージ	考えられる原因	推奨処置
		• WebEx Meeting Center クライアント用に十分な帯域幅があることを確認します。データ共有が有効な場合に低帯域幅警告を回避するには、継続的なスループットとして 1.3 mb/s が必要です。 • 会議から切断して再接続し、メイン ビデオに再度参加します。 • レビュー Windows または Mac の WebEx Meeting Center クライアントでの低帯域幅のトラブルシューティングに関するヒント, （199 ページ） • CMR ハイブリッド の Meeting Center クライアントの要件の詳細については、次を参照してください。 CMR Hybrid の前提条件, （36 ページ） • サポートに連絡する前に、会議から音声とビデオの統計情報を取得してください。Meeting Center クライアントで会議中に、[会議（Meeting）] > [音声とビデオの統計情報...（Audio & Video Statistics...）] を選択します。 ◦ あるいは全画面ビューで、発言中の参加者のビデオを右クリックし、[音声とビデオの統計情報...（Audio & Video Statistics...）] を選択

問題またはメッセージ	考えられる原因	推奨処置
		します。
TelePresence でビデオが表示されません	-	• WebEx ユーザがすでに参加済みで、ビデオを送信しているかどうかを確認します。
WebEx で音声が聞こえません	-	• TelePresence コール統計情報を調べて、TelePresence エンドポイントがミュートになっていないことを確認します。 • WebEx ユーザの間で相互に聞こえることを確認します。
TelePresence で音声が聞こえません	-	• TelePresence の統計情報を調べて、WebEx 側から音声を受信しているかどうかを確認します。PSTN/TSP 音声の場合は、音声コールが接続されていることを確認します。
TelePresence 側で、WebEx 側から共有されるプレゼンテーションが表示されません	-	• TelePresence の統計情報を調べて、コンテンツ チャネルの状況を確認します。 • WebEx ユーザ間で相互にコンテンツが表示されるかどうかを確認します。

問題またはメッセージ	考えられる原因	推奨処置
WebEx 側で、TelePresence 側からのプレゼンテーションが表示されません	-	• TelePresence の統計情報を調べて、コンテンツ チャネルの状況を確認します。 • WebEx ユーザ間で相互にコンテンツが表示されるかどうかを確認します。
WebEx 側で、WebEx からのプレゼンテーションが表示されません	-	• WebEx 管理者に連絡してアドバイスを受けてください。
TelePresence 側で、TelePresence 側からのプレゼンテーションが表示されません	-	• TelePresence の統計情報を調べて、コンテンツ チャネルが確立しているかどうかを確認します。 • コンテンツ送信を停止してから再開してみます。
プレゼンテーションがメイン ビデオに表示されます	-	• コンテンツ チャネルの現在のコール統計情報を調べます。 • SIP コールが暗号化されているかどうかを確認します。
TelePresence 側で表示される WebEx 参加者からのビデオが低品質です	-	• ネットワークの帯域幅を調べて、ネットワーク接続不良が発生しているかどうかを確認します。
TelePresence 側での WebEx 参加者からの音声が低品質です	TBD	• TBD
WebEx 側で表示される TelePresence 参加者からのビデオが低品質です	ネットワーク接続不良	• TelePresence 参加者のコール統計情報を確認します。

問題またはメッセージ	考えられる原因	推奨処置
WebEx 側での TelePresence 参加者からの音声が低品質です。	TBD	• TBD
ビデオで音声が遅れます（リップ シンクの問題）	PSTN/TSP 音声では、リップ シンクは保証されません	-
発言中の参加者が切り替わりません	-	• PSTN/TSP の場合、音声コールとビデオ コールがリンクされていることを確認します。
発言中のコールイン参加者のビデオが切り替わらず、これらの参加者に電話アイコンが関連付けられていません。	1.WebEx サイト管理者が正しく設定されていない。 2.音声コールが失敗した。 3.MCU が誤った参加者 ID を送信する。	• Cisco TMS CCC または MCU で、音声コールが失敗したかどうかを確認します。 • コールイン ユーザをマージするには、サイトで WebEx サイト管理者の「TSP アイデンティティ コード」が有効になっている必要があります。無効になっていると、コールイン マージは機能しません（たとえ正しい値をダイヤルし、InterCall で #1 が正しい場合でも）。
WebEx 側での TelePresence 参加者からのプレセンテーションが低品質です。	ネットワークの問題が発生している可能性があります。	• TelePresence と WebEx の間の帯域幅を調べます。
WebEx 参加者からのビデオがフリーズします。	ネットワークの問題が発生している可能性があります。	• TelePresence と WebEx の間の帯域幅を調べます。
会議が予期しない状況で終了します	-	• TelePresence ログを調べ、コール終了の理由を確認します。

問題またはメッセージ	考えられる原因	推奨処置
会議が自動的に延長されませんでした	現在の会議が終了した時点で始まる別の会議に TelePresence が予約されている。	• Cisco TMS 予約リストを調べて確認します。

Windows または Mac の WebEx Meeting Center クライアントでの低帯域幅のトラブルシューティングに関するヒント

WebEx Meeting Center クライアントの低帯域幅をトラブルシューティングするには、以下の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	WebEx 遅延のトラブルシューティングに関するヒントを http://kb.webex.com/WBX28297 で確認してください。	
ステップ 2	プロキシとファイアウォールで指定されるすべての WebEx ポートを許可していることを確認してください。詳細については、「How Do I Allow WebEx Traffic on My Network?」（https://kb.webex.com/WBX264）を参照してください。	
ステップ 3	『VCS Basic Configuration（Control with Expressway）x8.2 Deployment Guide』の「Appendix 3: Firewall and NAT settings」を参照して、VCS-Expressway または Expressway-E で正しいポートが有効になっていることを確認します。	
ステップ 4	TMS で次の操作を実行して、WebEx 参加者の帯域幅の TMS 設定を確認してください：[管理ツール（Administrative Tools）] > [設定（Configuration）] > [WebEx の設定（WebEx Settings）]	
ステップ 5	次を実行して、WebEx サイトのサイト管理設定を確認してください。WebEx サイトの [WebEx Site Administration] にログインします。	

TSP 音声会議に関する問題

ここでは、TSP 音声を使用する会議で発生する可能性のある問題について説明します。

TSP 音声会議で発生する一般的な問題を解決する方法については、次の表のトラブルシューティング情報を参照してください。

表 *22*：*TSP* 会議に関する問題

問題またはメッセージ	考えられる原因	推奨処置
ホストで以前にスケジュールされ、スケジュールの終了時刻を過ぎて延長された会議の音声に、TelePresence が参加します。	TelePresence システムは、スケジュールされた時間にホスト音声会議にダイヤルインします。延長中の以前の音声会議にホストが参加している可能性があります。 例： TelePresence によって使用されるホスト アカウントが、実際の WebEx ホストのアカウントです。このホスト アカウントが 2 つの連続する会議をスケジュールします（最初の会議は WebEx 会議、2 番目は TP+WebEx）。ホストが最初の会議を開始し、この会議が延長します。TelePresence+WebEx の会議の開始時点で、TelePresence はダムダイヤル文字列を使用して TSP 会議にダイヤルし、この会議に接続します。結果：TelePresence 参加者には、以前の会議の音声が聞こえます。 これは TSP 音声のしくみが原因であり、顧客に十分に理解される可能性があります。	• TSP 音声への参加後に TelePresence 音声プロンプトを再生するように設定します。「Cisco TelePresence が音声会議に参加しました（Cisco TelePresence is now in the audio conference）」（あるいは類似のメッセージ）。 （注） API を使用する方法ではこれは解決できません。
ホストが 「音声会議を継続する（keep audio conference running）」オプションを指定して退席した、以前のスケジュール済み会議の音声に TelePresence が参加します。	前述のシナリオに似ており、ホストは最初の会議を退席しますが、退席時に「音声会議を継続する（keep audio conference running）」を選択しています。したがって、最初の会議の音声会議が継続され、やがて TelePresence がダイヤルインします。 これは TSP 音声のしくみが原因であり、顧客に十分に理解される可能性があります。	• TSP 音声への参加後に TelePresence 音声プロンプトを再生するように設定します。「Cisco TelePresence が音声会議に参加しました（Cisco TelePresence is now in the audio conference）」（あるいは類似のメッセージ）。 （注） API を使用する方法ではこれは解決できません。

問題またはメッセージ	考えられる原因	推奨処置
「ホストプライベート会議コード」のために DTMF ダムダイヤル入力方式を使用できないことがあります（ホストとしてダイヤルイン+ホストがすでにダイヤルイン済み）。	TSP が「ホスト プライベート会議コード」を導入した場合、ホストが使用する会議コードは参加者が使用するコードと異なるため、ホストが PIN 番号を入力する必要がありません。この場合、ホストがすでに会議にダイヤルしていると、音声プロンプト コール フローによって MCU のダムダイヤルが使用できなくなることがあります。（当社のテストでは、この時点で TSP ブリッジからすべての外国語プロンプトが聞こえました。これはホスト会議コードがすでに使用中であるというブリッジ警告です。）	• API 方式を使用します。または、 • TSP パートナーへのアドバイス：「ホスト プライベート会議コード」を使用する場合は、2 番目のユーザがホスト プライベート会議コードを使用してダイヤルインすることを TSP 音声ブリッジで許容することを検討してください。

問題またはメッセージ	考えられる原因	推奨処置
（NBR とは異なり）ダイヤル シーケンスを TSP API 経由で即時に発行できません。	サイトのテレフォニー ドメインでは、OT 2.0 と TSP の統合のためのダイヤル シーケンスを静的に設定する操作だけが可能です。これにより、TSP がある程度制限されます（異なる音声ブリッジ インフラストラクチャや異なるダイヤルイン番号ある場合）。 対照的に NBR では静的設定と動的設定が可能です。動的設定を行うには、会議開始時にパートナー TSP アダプタが、次を使用して NBR ダイヤル文字列を WebEx に送信するように設定します：`A2W_RspCreateConference[NBRPhoneNumber]`。	• MCU ロジックが WebEx 会議を開始し、その時点で WebEx からダイヤルイン文字列を収集するように、ロジックを変更します。このシーケンスにより、WebEx は TSP からダイヤル文字列を次のように動的に収集できるようになります。 1 TelePresence が TelePresence 会議を開始する。 2 TelePresence が WebEx 会議を開始する。 3 WebEx が TSP に W2A_CreateConference を送信する。 4 TSP が WebEx に A2W_RspCreateConference を送信する（これに TP ダイヤル文字列が含まれます）。 5 WebEx が MCU にダイヤル文字列を送信する。 6 MCU が TSP ブリッジにダイヤルインする。 （他のコンポーネントを変更するとともに）TSP API と TSP Server も変更する必要があります。

問題またはメッセージ	考えられる原因	推奨処置
MCU ダイヤル文字列により使用される TSP 音声アカウント情報が古い情報です。	MCU は、会議開始（数週間後としてスケジュールされることもある）の時点で使われる TSP ダイヤル文字列を、会議スケジュール時点で収集して保存しているため、ダイヤル文字列が古くなって TSP 会議へのコールが失敗することがあります。TelePresence 会議のスケジュール時点から TelePresence 会議の開始までの間にデフォルト（最初の）TSP 音声アカウントが変更された場合に、この状況が発生します。	• 前述の推奨事項に従うことで、この問題が解決します（TelePresence 機器が会議のスケジュール時点ではなく会議の開始時に WebEx から TelePresence ダイヤル文字列を収集するように設定する）。

TelePresence Server および MCU に関する問題

ここでは、TelePresence Server および MCU が原因で会議で発生する可能性のある問題について説明します。

TelePresence Server と MCU で発生する一般的な問題を解決する方法については、次の表のトラブルシューティング情報を参照してください。

表 *23*：*TelePresence Server* および *MCU* に関する問題

問題またはメッセージ	考えられる原因	推奨処置
MCU/TelePresence が、WebEx に接続した直後に切断されます。SIP Bye メッセージを WebEx クラウドから受信します。	WebEx ホストが、すでにホストとして会議に参加している状態で会議に参加しようとした。	• 同じ WebEx ホスト ID を使用して複数の会議に同時に参加しないでください。 （注） 1 つのホストが一度に実行できる CMR Hybrid 会議は 1 つだけです。

システム動作の管理

[Cisco WebExビデオ表示（Cisco WebEx Video View）] ウィンドウの管理

Cisco WebEx ビデオ表示パネルが開いている状態で、PC とテレプレゼンスビデオデバイスをビデオ（VGA）ケーブル（VGA、DVI、HDMI）で接続すると、ウィンドウがカスケード表示される場合があります。WebEx アプリケーションは、テレプレゼンスビデオデバイスが接続されたことを検出し、テレプレゼンスを介して画面を共有するかどうかを尋ねるプロンプトを出します。共有することを確認することで、カスケード表示の問題を回避できます。 この問題を防ぐには、プレゼンテーションを行うラップトップにプレゼンテーション ケーブルを接続する前に、Cisco WebEx ビデオ表示アプリケーションを閉じてください。

カスケード画面が表示されたら、ビデオ表示ウィンドウを閉じます。

付 録 A

Cisco Unified Communications Manager の正規化スクリプトを追加する

正規化スクリプトの概要

TelePresence 用に SIP トランクの暗号化と TLS を使用する展開環境では、Cisco Unified Communications Manager に 1 つ以上の TelePresence 正規化スクリプトを追加する必要があります。

注意 このリリースでは新しいバージョンのスクリプトが必要です。予期しないコールの切断を防ぐため、最新バージョンがインストールされていることを確認する必要があります。

Cisco Unified Communications Manager バージョン 10.5(2) 以降では、スクリプトがソフトウェアと共に自動的にインストールされます。以前のバージョンでは、最新スクリプトを https://software.cisco.com/download/navigator.html?mdfid=268439621&flowid=45900 の Cisco Web サイトからダウンロードしてインストールする必要がありました。

使用可能な正規化スクリプトを次に示します。

表 *24*：正規化スクリプト

スクリプト	インストール ...
telepresence-conductorinterop	ネクスト ホップ ピアとして TelePresence Conductor と直接連動する SIP トランク
vcs-interop	ネクスト ホップ ピアとして Cisco VCS Control または Cisco Expressway-C と直接連動する SIP トランク

スクリプト	インストール ...
telepresence-mcu-ts-directinterop	ネクスト ホップ ピアとして TelePresence Server または MCU と直接連動する SIP トランク

スクリプトの追加

手順

ステップ 1 Cisco ウェブサイトから必要なスクリプトをダウンロードします（関連する Unified CM ソフトウェア バージョンに移動して、[SIP 正規化および透過性スクリプト（SIP Normalization and Transparency Scripts）] > [スクリプト（Scripts）] の順に選択します）。

（注） Cisco Unified Communications Manager バージョン 10.5(2) 以降を使用している場合は、スクリプトがソフトウェアとともに自動的にインストールされるため、このステップをスキップしてください。

ステップ 2 Unified CM で、[デバイス（Device）] > [デバイスの設定（Device Settings）] > [SIP 正規化スクリプト（SIP Normalization Script）] に移動します。

ステップ 3 [新規追加（Add New）] をクリックします。

ステップ 4 [ファイルのインポート（Import File）] をクリックします。

ステップ 5 ダウンロードしたスクリプトを選択します。

ステップ 6 [ファイルのインポート（Import File）] をクリックします。

ステップ 7 次の詳細情報を入力または変更します。

[名前（Name）]	スクリプト名を入力します。例：telepresence-conductor-interop
説明	説明を入力します。たとえば、「TelePresence Conductor 経由でコールの相互運用性を提供」と入力します
メモリしきい値（Memory Threshold）	「1000」と入力します。
Lua 命令しきい値（Lua Instruction Threshold）	「2000」と入力します。

ステップ 8 [保存（Save）] をクリックします。

ステップ 9 必要なすべてのスクリプトが追加されるまで、上記の手順を繰り返します。

ステップ 10 SIP トランクにスクリプトをインストールするには、次の手順を実行します。

a) Unified CM で、[デバイス（Device）] > [トランク（Trunk）] または [メディアリソース（Media Resources）] > [会議ブリッジ（Conference Bridge）]（Unified CM バージョン 9.1（2）SU2 のアドホック会議ブリッジの場合）に移動して、関連するトランク/ブリッジを選択します。
b) [SIP 情報（SIP Information）] セクションの [正規化スクリプト（Normalization script）] エリアで、該当するトランクまたはブリッジ用のスクリプトを選択します。
c) [保存（Save）] をクリックします。
d) [リセット（Reset）] をクリックします。

付 録 B

移行パス

移行の概要

優先するアーキテクチャに、以前のソリューションの展開環境を移行できます。この CMR Hybrid リリースで使用される CMR Premises リリース 5.0 アーキテクチャでは、会議インフラストラクチャとして 2 つの推奨展開アーキテクチャが使用されています。

- Unified CM に接続する会議インフラストラクチャ。これは推奨されるアーキテクチャです。
- Cisco VCS に接続する会議インフラストラクチャ。

新規（初回）展開では、Unified CM に接続する展開環境を実装する必要があります。

この 2 つのシナリオのいずれにも該当しない既存の音声とビデオの展開環境では、5.0 推奨コードレベルを使用して展開環境を CMR Premises 5.0 展開環境に移行することを推奨します。このアーキテクチャはテスト済みであり、このアーキテクチャに基づいて新機能の開発が予定されているためです。

CMR Hybrid 展開環境に移行するには、次の手順を実行します。

- 最初に、インフラストラクチャを CMR Premises 5.0 標準に移行します。
- 次に、エンドポイントが Cisco VCS に現在登録されている場合、Unified CM に登録可能なエンドポイントを Unified CM に移行します。

移行の前提条件

CMR Premises リリース 5.0 では、エンドポイント発信者 ID を使用して、参加者リストにこの ID が表示されます。また、（有効になっている場合には）TelePresence Server ActivePresence モードの会議の画面にも表示されます。ダイヤル プランを調べて、表示される発信者 ID がわかりやすいものであることを確認するよう推奨します。詳細については、「エンドポイントの表示名のプロビジョニング」のソリューションでの表示名のプロビジョニングに関する情報を参照してください。

移行でサポートされるソフトウェアのバージョン

表 *25*：サポートされるソフトウェアのバージョン

製品	推奨	最小ハードウェア	注記（**Notes**）
TelePresence Server	4.2	4.1	TelePresence Conductor によるリモート管理用に TelePresence Server ブリッジを設定する必要があります。
TelePresence Conductor	XC4.0	XC3.0 TSP 音声には XC3.0.2 が必要です	
MCU	4.5	4.5	
Cisco VCS	X8.5.3	X8.5	
Cisco VCS：H.323 登録用に	X8.5.3	X8.5	
Cisco Expressway	X8.5.3	X8.5	
Cisco TMS	15.0	14.6	
Cisco TMSPE	1.5	1.4	
Unified CM	10.5(2)SU2	10.5(2)SU1	

Cisco Unified Communications Manager のみのシステムの CMR Hybrid への移行

手順

ステップ 1 Unified CM を、CMR Hybrid で推奨されるバージョンにアップグレードします。

ステップ 2 TelePresence Conductor を Unified CM に追加し、TelePresence Conductor にトランキングされたブリッジを展開します。これらのコンポーネントはすべての会議タイプをサポートします。

ステップ 3 エンドポイント ソフトウェアを、Unified CM で提供されるバージョンにアップグレードします。

ステップ 4 パーソナル CMR / ランデブーおよびスケジュールをサポートするために、Cisco TMS/Cisco TMSPE をアップグレードします。

ステップ 5 WebEx 参加者がコールに追加される場合は、実行中の Unified CM がコード バージョン 9.1(2)SU2 以上であることを確認し、Early Offer をサポートするように Unified CM 設定を更新します。

ステップ 6 企業ネットワーク外部の参加者が会議に参加できるようにするには、ファイアウォール トラバーサル用に Cisco Expressway-C および Cisco Expressway-E を展開します。

ステップ 7 Lync との相互運用性が必要な場合は、Cisco Expressway-C または Cisco VCS Control を、Microsoft Lync インフラストラクチャにゲートウェイとして追加します。バージョン X8.5 以降が必要です。（Cisco VCS Control と Cisco Expressway-C のどちらがニーズに最適かを判断するには、Cisco VCS / Cisco Expressway 展開ガイドを参照してください）。

ステップ 8 ソリューションにレガシー エンドポイントと H.323 エンドポイントを追加する場合は、それらのエンドポイントを登録できる Cisco VCS Control を追加します。

個別の音声およびビデオ エンドポイント

一部の Unified CM 展開環境では、音声専用エンドポイントとビデオ エンドポイントそれぞれに個別の Unified CM が使用されます。理想的なソリューションは、同じ Unified CM バージョンで両方のシステムを動作させることです。その場合は、前述した「Cisco Unified Communications Manager のみのシステムの CMR Hybrid への移行, （211 ページ）」の手順に従う必要があります。

音声エンドポイントとビデオ エンドポイントをそれぞれ別個の Unified CM に登録して異なるバージョンで実行しなければならない理由がある場合は、作業を進める前に、展開環境で 2 つの Unified CM バージョンが許容されるかどうかアカウント管理者に確認する必要があります。この場合は、ビデオ Unified CM 上で、前述した「Cisco Unified Communications Manager のみのシステムの CMR Hybrid への移行, （211 ページ）」の手順を実行します。

Cisco Unified Communications Manager および Cisco VCS の CMR Hybrid への移行

手順

ステップ 1 Cisco VCS を、CMR Hybrid で推奨されるバージョンにアップグレードします。

ステップ 2 Unified CM を、CMR Hybrid で推奨されるバージョンにアップグレードします。

ステップ 3 TelePresence Conductor にトランキングしているブリッジを使用する Unified CM に接続している TelePresence Conductor を移行または維持します。

ステップ 4 TelePresence Conductor を Cisco VCS から移動する場合、Cisco VCS で TelePresence Conductor にコールを送信するのに使用した検索ルールによって、コールが Unified CM に送信され、Unified CM がこれらのコールを TelePresence Conductor に転送することを確認します。

ステップ 5 Cisco VCS アーキテクチャは、ファイアウォール トラバーサル、Lync 相互運用性、およびレガシー/H.323 エンドポイント登録向けに設定された状態を維持することができます。

ステップ 6 Unified CM に登録可能なエンドポイントを Unified CM に移行し、このソリューション リリースで必要なバージョンにソフトウェアをアップグレードします。

エンドポイント機能の比較

次の表で Unified CM に登録されたエンドポイントと Cisco VCS に登録されたエンドポイントの機能を比較します。

表 *26*：エンドポイント機能

機能（Capability）	Unified CM 登録	Cisco VCS 登録
電話帳	TMS 電話帳の階層ディレクトリ	TMS 電話帳の階層ディレクトリ
管理	Unified CM と Prime Collaboration スイートによる管理、Unified CM によるプロビジョニング	Cisco TMS による管理 Cisco TMS によるプロビジョニング
会議のスケジュール	Cisco TMS による管理	Cisco TMS による管理
ファイアウォール トラバーサル	Cisco Expressway-C および Cisco Expressway-E の使用	Cisco VCS Expressway の使用

機能（Capability）	Unified CM 登録	Cisco VCS 登録
会議のエスカレーション	アドホック	Multiway

機能とバージョンの依存関係

表 *27*：機能とバージョンの依存関係

機能	必要なバージョン
CMR のプロビジョニングとユーザ ポータル	XC 3.0、TMS 14.6、TMSPE 1.4
TelePresence Server スケーラビリティの強化	TS 4.1
基本的な TelePresence Server カスケード	TS 4.1、XC 3.0、TMSPE 1.4
TelePresence のユーザ エクスペリエンスの強化	TS 4.1
TelePresence Server のサービサビリティの強化	TS 4.1
ホスト/ゲスト会議の 1 つのエイリアス（役割は PIN により決定）	TS 4.1、XC 3.0、TMS 14.6、TMSPE 1.4

関連製品、バージョン、および機能

表 *28*：関連製品、バージョン、および機能

製品	バージョン	機能
MCU	4.5	4.0 運用のための最小バージョン。次の機能を追加します。 • ClearPath（Flux 1） • 暗号化 SIP 参加者用の個別のコンテンツ チャネル • ドメインなしでのアウトダイヤル要求のために追加されるドメイン：MCU が Unified CM にトランキングされている場合に、WebEx アウトダイヤル（TSP会議音声）用に必要です。

製品	バージョン	機能
Unified CM	10.5(2)SU1	サポートされている最小バージョン データ接続および明示的 SIP トランクとしてアドホック ブリッジが設定されるようになりました。
Cisco VCS	X8.5	この CMR Hybrid リリースで Lync ゲートウェイが動作するための最小バージョン
Cisco TMS	14.6	CMR Hybrid およびホスト/ゲスト PIN での WebEx の最小バージョン

CMR Premises ソリューションと展開の詳細については、次のガイドを参照してください。

- Cisco Collaboration Meeting Rooms（CMR）Premises Solutions Guide： http://www.cisco.com/c/en/us/support/conferencing/collaboration-meeting-rooms-premises/model.html
- Cisco Collaboration Meeting Rooms（CMR）Premises Deployment Guide： http://www.cisco.com/c/en/us/support/conferencing/collaboration-meeting-rooms-premises/model.html

付 録 C

大規模なまたは重大なミーティングのカスケードをセットアップする

カスケードの概要

ローカル CMR Premises 企業ネットワーク内では、1 つの会議ブリッジの容量を超える大規模な会議を、1 つ以上の追加ブリッジ間でカスケード（分散）できます。ブリッジは相互ルーティングおよび Cisco TelePresence Conductor とルーティング可能でなければなりません。

（注） 1 つの会議ブリッジから、ローカル エンタープライズ ネットワークの境界外のブリッジへのカスケードはサポートされていません。

- カスケード リンクは、TelePresence Server との間で 1 つのビデオ画面だけを共有します。
- TelePresence Server ブリッジから MCU へのカスケード、および MCU から TelePresence Server へのカスケードはサポートされていません。
- カスケードに対応した会議では、会議の開始時から、設定されている最大数のカスケードのためのカスケードリソースが予約されます（実際に使用されるかどうかに関係なく）。このため、大規模な会議や、VIP ユーザが使用するランデブー会議 / パーソナル CMR では特に、カスケード オプションを控えめに使用することを推奨します。
- 専用ブリッジをスケジュールする場合（スケジュール用に専用プール内の 1 つのブリッジを予約する場合）など、リソースが利用可能であることが重要な状況では、カスケードを有効にしないでください。
- TelePresence Server の ActiveControl 機能では、最大 500 人の参加者がサポートされます。

CMR の会議のプロセス

このプロセスは、Cisco TMS の Cisco TMSPE のプロビジョニング拡張機能を使用して、カスケード対応 CMR のテンプレートを作成し、グループに適用します。ご使用の展開環境で Cisco TMSPE を使用していない場合は、TelePresence Conductor のマニュアルの説明に従い、TelePresence Conductor を使用してカスケードを設定できます。

手順

ステップ 1 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] > [Collaboration Meeting Room テンプレート（Collaboration Meeting Room Templates）] に移動し、必要に応じて 1 つ以上のテンプレートを作成します。

ステップ 2 [カスケードを許可する（Allow Cascading）] チェックボックスをオンにします。

ステップ 3 会議に関して許可する最大カスケード数を指定します。

ステップ 4 Cisco TMS で、[システム（Systems）] > [プロビジョニング（Provisioning）] > [ユーザ（Users）] に移動します。関連するグループを選択して、[アクティブ（Active）]列で必要なテンプレート用のボタンを選択します。

スケジュール済み会議のプロセス

はじめる前に

スケジュール用に専用ブリッジを使用する展開環境では、カスケードは推奨されません（単一ブリッジからなる単一プールの場合は可能です）。スケジュール済み会議とスケジュールされない会議の両方をサポートする、共用ブリッジを使用する展開環境の場合、ソリューションでは TelePresence Conductor により管理される TelePresence Server または MCU 会議ブリッジで、スケジュール済み会議のカスケードがサポートされます。

参加者数が 1 つのブリッジの容量を超えている場合、Cisco TMS は予約時にそのことを通知します。

手順

ステップ 1 **Cisco TMS の標準としてのスケジュール済み会議の予約**：会議に TelePresence Conductor を追加します（デフォルト MCU として定義されている場合を除く）。

ステップ 2 **会議の配信の有効化**：前のステップで作成した会議の設定で、[配信（Distribution）] チェックボックスをオンにします。

詳細情報

詳細については、次の Cisco Web サイトで『Cisco TelePresence Conductor with Cisco TMS Deployment』ガイドを参照してください。
http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html