Cisco Meeting Server

クイック リファレンス ガイド

Meeting Server 会議での ActiveControl の使用

2023 年 3 月 3 日

目次

変更事項

バージョン	変更
2021 年 5 月 10 日	軽微な編集。
2020 年 8 月 21 日	3.0 および Web アプリケーション用に更新されました。

1 はじめに

Cisco Meeting Server は、ActiveControl と呼ばれる機能によって、会議の参加者が、会議エンドポイントから会議エクスペリエンスを直接制御する機能を提供します。

ActiveControl は、会議名簿（参加者リスト）、参加者のミュートや削除、ビデオレイアウトの変更など、ユーザーによるランタイム会議機能をエンドポイントから直接有効にします。

ActiveControl を使用するには、お客様の展開に次のものが必要です。

- エンドポイントが ActiveControl をサポートしていること
- エンドポイントと Meeting Server 間のコールパスは、iX メディアをエンドツーエンドでサポートしていること
- Meeting Server で有効化な適切なアクセス権限

このガイドでは、Cisco Meeting Server での ActiveControl の設定とご利用条件について説明します。

ActiveControl に加えて、Cisco Meeting Server の Web アプリケーションには、Meeting Server の ActiveControl 機能と似ていますが、異なる会議およびスペース制御が複数あります。
Web アプリケーション制御については、このガイドの「 Cisco Meeting Server Web アプリケーションのコントロール」（14 ページ）のセクションで説明しています。

1.1 ActiveControl 機能について

ActiveControl は、Call Bridge と Cisco エンドポイント間でネゴシエートされた一連の機能で、ユーザーは外部アプリケーションやオペレーターを必要とせずに、会議エクスペリエンスを制御できるようにします。ActiveControl は Cisco デバイスの iX メディアプロトコルを利用し、コールの SIP メッセージングの一部としてネゴシエートされます。

ActiveControl は、当初は Cisco TelePresence Server 向けにリリースされましたが、その後、Cisco Meeting Server（Meeting Server）や Webex Meetings などの新しいプラットフォーム向けに変更されました。具体的な機能と構成は、使用しているミーティングサービスによって異なります。このガイドでは、Meeting Server の ActiveControl 実装のみに焦点を当てています。Webex Meetings での ActiveControl の使用については、この記事を参照してください。

Meeting Server で ActiveControl によって実現する主な機能は次のとおりです。

- 会議に接続中のすべての参加者のリスト（会議名簿または参加者リストと呼ばれます）の表示
- その他の参加者のミュートまたはミュート解除
- 会議への参加者の追加または削除
- 会議の録音の開始または停止
- 重要な参加者の指定
- 会議中にアクティブスピーカーである参加者を示す指標
- 会議で現在コンテンツまたはプレゼンテーションを共有している参加者の指標
- 会議のロックまたはロック解除
- レイアウト制御

注：展開で使用できる実際の機能は、使用しているエンドポイントの種類とソフトウェアのバージョンによって異なる場合があります。

注：参加者リストは、会議名簿とも呼ばれます。これにより、通話中のすべての参加者の名前が表示されます。

---

2 サポートされるエンドポイント

Cisco Meeting Server の ActiveControl は、次のエンドポイントでサポートされています。

- Cisco DX シリーズ、SX シリーズ、Room Kit、Room Kit Pro、これらのコーデックをベースにソフトウェア CE8.3 以降が動作するすべてのエンドポイント。
- Cisco Jabber リリース 12.5 以降。

Cisco Meeting Server Web アプリケーションには、ActiveControl とは異なる会議制御が複数あります。詳細については、19 ページの「Cisco Meeting Server Web アプリケーションの制御」を参照してください。

次のセクションでは、さまざまなエンドポイントの機能サポートと要件について詳しく説明します。

2.1 Cisco エンドポイント

このセクションは、DX シリーズ、SX シリーズ、Room Kit、Room Kit Pro、およびこれらのコーデックをベースにした、Touch10 コントローラを使用するすべてのエンドポイントを含む、CE ソフトウェアバージョン 9.6.2 が動作するすべての Cisco エンドポイントに適用されます。デフォルトでは、これらのエンドポイントで ActiveControl が有効になっています。

エンドポイントからこの設定を構成するには、[**設定**（Configuration）] > [**会議**（Conference）] > [ActiveControl **モード**（ActiveControl Mode）]を開きます。

ActiveControl 機能には、Touch10 コントローラまたは DX タッチスクリーン インターフェイスを介してアクセスします。

注：さまざまなバージョンのエンドポイントソフトウェアでサポートされる機能は若干異なる場合があります。Cisco では、最高のエクスペリエンスを得るために、最新バージョンのエンドポイントソフトウェアを使用することを推奨しています。

2.1.1 ソフトウェアバージョン CE9.6.2 でサポートされる機能のリスト

機能	サポート	注意
会議名簿（参加者リスト）	Yes	
相手側の音声のミュート	Yes	DTMF オプションが利用可能
相手側の音声のミュート解除	Yes	DTMF オプションが利用可能
ビデオレイアウト制御	Yes	DTMF オプションが利用可能
参加者の追加	いいえ	実験的な機能として利用可能
参加者を削除する	Yes	
会議の記録制御	Yes	DTMF オプションが利用可能
会議のストリーミング制御	いいえ	DTMF オプションが利用可能

機能	サポート	注意
録画/ストリームの指標	Yes	画面にアイコンが表示されます。
会議のロック/ロック解除	いいえ	DTMF オプションが利用可能
重要度の設定/設定解除	いいえ	
Roster Show Speaker Indicator（アクティブスピーカーの指標）	Yes	
Roster Show Content Contributor（誰がコンテンツを共有しているかを示す指標）	Yes	
参加者数	Yes	
ActiveControl によるローカルミュート	Yes	サーバーとローカルミュートは連動しており、相互に追従します。
ActiveControl によるローカルミュート解除	いいえ	ユーザーがリモートでミュートされなくなると、画面に通知が表示されます。
暗号化された iX メディアのサポート	Yes	TLS で保護された登録とエンドツーエンドのコールパスが必要
メッセージ テキスト	Yes	画面上にメッセージ通知が表示されます

個別の機能の利用は、参加者に対する Meeting Server の設定によって制限される場合があります。詳細については、14 ページの「Cisco Meeting Server の設定」を参照してください。

2.2 Cisco Jabber

Jabber での ActiveControl のサポートは、サポートされているすべてのプラットフォームの Jabber バージョン 12.5 で導入されました。Jabber では、ActiveControl をサポートするために Cisco Unified Communications Manager バージョン 10.5 以降が必要です。

Jabber では、ActiveControl を有効にするためにクライアント側での構成は必要ありませんが、iX メディアは、Unified CM のユーザーのデバイスに割り当てられた SIP プロファイルで有効にする必要があります。

2.3 Jabber 12.5 でサポートされる機能

表 1：Jabber 12.5 でサポートされる機能のリスト

機能	サポート	注意
会議名簿（参加者リスト）	Yes	
相手側の音声のミュート/ミュート解除	Yes	DTMF オプションが利用可能
ビデオレイアウト制御	Yes	DTMF オプションが利用可能
参加者の追加	Yes	
参加者を削除する	Yes	
会議の記録制御	Yes	DTMF オプションが利用可能
会議のストリーミング制御	いいえ	DTMF オプションが利用可能
録画/ストリームの指標	Yes	
会議のロック/ロック解除	Yes	DTMF オプションが利用可能
重要度の設定/設定解除	いいえ	
Roster Show Speaker Indicator（アクティブスピーカーの指標）	Yes	
Roster Show Content Contributor（誰がコンテンツを共有しているかを示す指標）	Yes	
参加者数	Yes	
ActiveControl によるローカルミュート	Yes	サーバーとローカルミュートは連動しており、相互に追従します。
ActiveControl によるローカルミュート解除	Yes	サーバーとローカルミュートは連動しており、相互に追従します。
暗号化された iX メディアのサポート	Yes	
メッセージ テキスト	いいえ	ビデオストリームの一部としての Meeting Server の埋め込み

個別の機能の利用は、参加者に対する Meeting Server の設定によって制限される場合があります。詳細については、14 ページの「Cisco Meeting Server の設定」を参照してください。

3 呼制御とトランク

ActiveControl を使用するには、Meeting Server とエンドポイント間のフルコールパスが SIP メッセージの iX メディアをサポートしている必要があります。iX メッセージングをブロックまたは妨害するプロキシ、ファイアウォール、またはバックツーバック ユーザーエージェント（B2BUA）がパス内にあると、ActiveControl によってネゴシエートされません。

展開で ActiveControl を有効にする場合は、Meeting Server とエンドポイント間のトランクで iX プロトコルがサポートされていることを確認します。

次のセクションでは、Cisco Expressway、Cisco VCS、および Cisco Unified Communications Manager の ActiveControl を有効にする手順について詳しく説明します。展開に適したセクションを参照してください。

3.1 Cisco Unified Communications Manager

ActiveControl は Cisco Unified Communications Manager（Unified CM）バージョン 9.1.2 以降と互換性があります。サポートされているバージョンよりも古いバージョンを実行しているインスタンスにルーティングするトランクでは、iX プロトコルをフィルタリングするか無効化する必要があります。

Unified CM では、使用中の SIP プロファイルと Unified CM のバージョンによっては、iX プロトコルがデフォルトで無効化されている場合があります。より新しい Unified CM バージョンでは、TelePresence で使用するラベルが付いた SIP プロファイルで、iX プロトコルがデフォルトで有効になっています。Jabber に使用される共通プロファイルでは、デフォルトで設定が無効化されている場合があります。デバイスで使用される各 SIP プロファイルと、Telepresence コールが通過するすべてのトランクで iX メディアを有効にする必要があります。

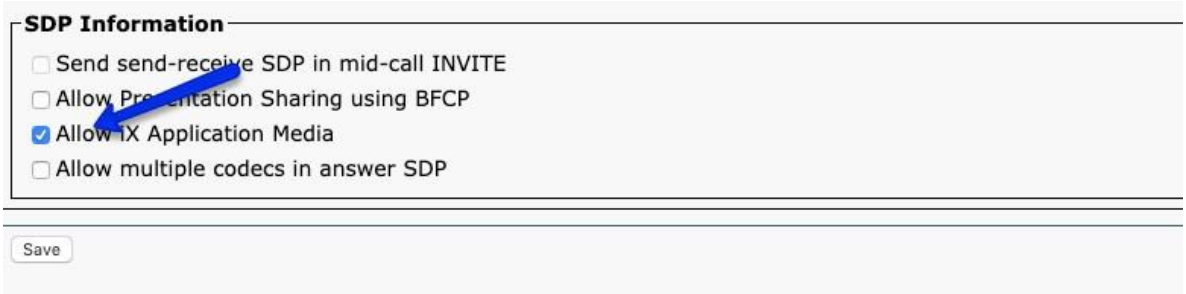
TelePresence エンドポイント、Jabber デバイス、および SIP トランクで使用されるすべての SIP プロファイルを確認します。

3.1.1 SIP プロファイル iX メディア設定の有効化または確認

iX メディア設定を有効にするには、次の手順を実行します。

1. Unified CM Administration Web インターフェイスで、[**デバイス**（Device）] > [**デバイスの設定**（Device Settings）] > [SIP **プロファイル**（SIP Profile）]を選択します。[SIP **プロファイルの検索と一覧表示**（Find and List SIP Profiles）]ウィンドウが表示されます。
2. 問題のトランクまたはデバイスに使用されている既存の SIP プロファイルを見つけ、検索条件を入力して[**検索**（Find）]をクリックします。
3. その結果から、編集する SIP プロファイルの名前をクリックします。[SIP **プロファイルの設定**（SIP Profile Configuration）]ウィンドウが表示されます。

4. [SDP **情報**（SDP Information）]で[iX **アプリケーションメディアを許可**（Allow iX Application Media）]設定を見つけ、チェックボックスがマーク/有効になっていることを確認します。



5. [**構成の適用**（Apply Config）]をクリックして、変更を保存します。

SIP プロファイルに変更が加えられた場合は、必要に応じてトランクまたはデバイスを再起動します

トランクの iX メディアをフィルタ処理または無効化するには、トランクに関連付けられた SIP プロファイルを編集し、[iX **アプリケーションメディアを許可**（Allow iX Application Media）]設定がオフになっていることを確認します。

3.1.2 暗号化の考慮事項

エンドポイントでは、セキュアな SIP セキュリティプロファイルを使用して、暗号化された iX for Call をネゴシエートする必要があります。暗号化された iX をネゴシエートするために、コールパスは TLS エンドツーエンドを使用する必要があります。使用できない場合は、暗号化されていない iX メディアをネゴシエートできます。

3.1.3 MRA 考慮事項

モバイルリモートアクセス（MRA）で接続されたエンドポイントは、Unified CM が混合モードセキュリティであり、Unified CM が Expressway への TLS 接続を使用しない限り、iX メディアと ActiveControl をサポートしません。

この制限事項は、Unified CM および Cisco Expressway の今後のリリースで対応する予定です。

3.2 Cisco Expressway および Cisco Video Communication Server

ActiveControl は、Cisco Expressway（Expressway）および Cisco Video Communication Server（Cisco VCS）バージョン X7.2.3 以降と互換性があります。iX のサポートは、Cisco VCS と Expressway の両方の製品バリエーションで共通です。簡略化するため、このドキュメントでは、Cisco VCS という用語は Expressway と Cisco VCS の両方を指します。サポートされているバージョンより古いリリースを実行しているインスタンスにルーティングするトランクでは、iX プロトコルをフィルタ処理/無効化する必要があります。

Cisco VCS では、ゾーンの SIP UDP/IX フィルタ設定でフィルタ処理するように明示的に設定されていない限り、iX プロトコルはデフォルトでネイバーゾーンを通過できます。

3.2.1 Expressway の iX フィルタ設定の確認

プロトコルをサポートしないネイバーゾーンの iX アプリケーション回線をフィルタ処理するように Cisco VCS を構成するには、SIP

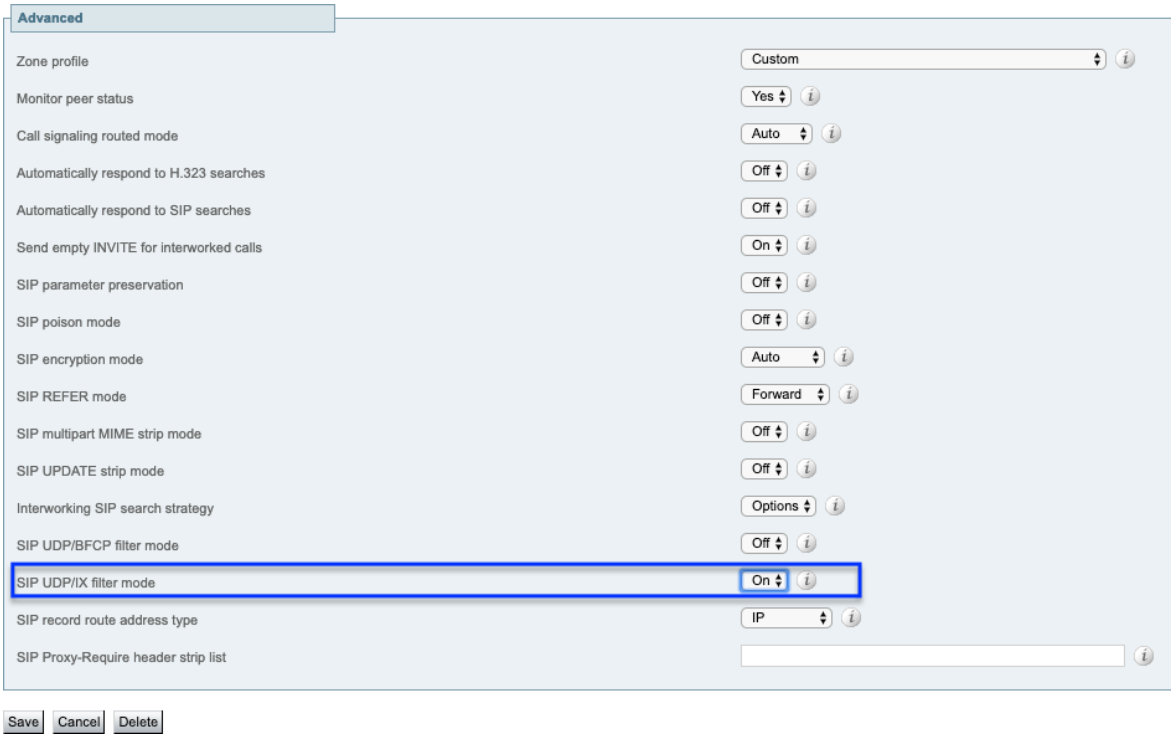
UDP/IX フィルタモードの詳細設定オプションが[オン（On）]

に設定されているカスタムゾーンプロファイルでゾーンを構

成する必要があります。詳細ゾーンプロファイルのオプショ

ン設定を更新するには、次の手順を実行します。

1. Expressway Web インターフェイスで、[**設定**（Configuration）] > [**ゾーン**（Zones）] > [**ゾーン**（Zones）]に移動します。
2. 表示または編集するゾーンの名前をクリックします。
3. [**詳細**（Advanced）]パネルで、[**ゾーンプロファイル**（Zone Profile）]が[**デフォルト**（Default）]または[Cisco Unified Communications Manager]に設定されている場合、SIP UDP/IX フィルタモードはオフと見なされ、表示されません。
4. フィルタを有効にするには、[**ゾーンプロファイル**（Zone Profile）]を[**カスタム**（Custom）]に変更して[詳細設定（Advanced settings）]を表示します。
5. SIP UDP/IX フィルタモードは、このゾーンの iX メディアのフィルタ処理を制御します。ActiveControl を許可するには、[**オフ**（Off）]に設定されていることを確認します。互換性のないネイバーに iX をフィルタ処理する場合は、[**オン**（On）]に設定します。



プロファイルをカスタムに変更し、変更を保存している場合は、編集中のゾーンに適用される他の詳細設定を確認してください。

6. [**保存**（Save）] をクリックして、変更内容を保存します。

3.2.2 暗号化の考慮事項

エンドポイントは TLS に登録し、暗号化された iX を通話にネゴシエートする必要があります。コールパスは、暗号化された iX の TLS エンドツーエンドを使用する必要があります。使用できない場合は、暗号化されていない iX メディアをネゴシエートできます。

3.3 Cisco Meeting Server の設定

ActiveControl は Cisco Meeting Server でサポートされ、デフォルトで有効になっています。ActiveControl とネゴシエーションは自動です。エンドポイントで使用できる機能は、Meeting Server のプロファイルで構成された設定によって制御されます。ActiveControl 機能を使用する前に、Meeting Server のプロファイルを設定する必要があります。

3.3.1 Meeting Server の ActiveControl 機能

表 2：Cisco Meeting Server の ActiveControl 機能のリスト

機能	サポート	注意
会議名簿（参加者リスト）	Yes	
相手側の音声のミュート/ミュート解除	Yes	DTMF オプションが利用可能
ビデオレイアウト制御	Yes	DTMF オプションが利用可能
参加者の追加	Yes	
参加者を削除する	Yes	
会議の記録制御	Yes	DTMF オプションが利用可能
会議のストリーミング制御	Yes	DTMF オプションが利用可能
録画/ストリームの指標	Yes	サポートされている場合はエンドポイントに表示され、サポートされていない場合は Cisco Meeting Server によってビデオストリームに表示されます。
会議のロック/ロック解除	Yes	DTMF オプションが利用可能
重要度の設定/設定解除	Yes	
Roster Show Speaker Indicator（アクティブスピーカーの指標）	Yes	
Roster Show Content Contributor（誰がコンテンツを共有しているかを示す指標）	Yes	
参加者数	Yes	
ActiveControl によるローカルミュート	Yes	
ActiveControl によるローカルミュート解除	Yes	エンドポイント制御機能
暗号化された iX メディアのサポート	Yes	
メッセージ テキスト	Yes	サポートされている場合はエンドポイントに表示され、サポートされていない場合は Cisco Meeting Server によってビデオストリームに表示されます。

3.4 Cisco Meeting Server プロファイル

デフォルトでは、参加者の権限は通常、Meeting Server で無効化されています。参加者が ActiveControl 機能を使用できるようにするには、管理者は Meeting Server の API を介してこの機能を有効にする必要があります。

SIP 接続エンドポイントの場合、アクセス許可は API の callLegProfiles 設定によって制御されます。callLegProfile は、システム全体のレベル、テナントレベル、スペースレベル、メンバー、または accessMethod レベルで適用できます。推奨するベストプラクティスは、システムレベルでの展開の基準として、必要な参加者のアクセス許可を設定することです。Meeting Server API およびオブジェクト階層の使用方法の詳細については、『Cisco Meeting Server API リファレンスガイド』を参照してください。

以下に、SIP 接続エンドポイントに対し、すべての ActiveControl 機能を有効にするために関連する callLegProfile 設定を示します。機能を使用するには、参加者に対して設定を有効にする必要があります。または、設定をシステムレベルの callLegProfile に適用して、デフォルトですべての参加者に設定を適用することもできます。

表 3：SIP 参加者の ActiveControl callLegProfile 設定

callLegProfile 設定	設定する値	注意
changeLayoutAllowed	正しい	参加者自身のレイアウトを変更する権限を付与します
disconnectOthersAllowed	正しい	会議名簿（参加者リスト）から参加者を削除する権限を付与します
addParticipantAllowed	正しい	進行中の通話に参加者を追加する権限を付与します
muteOthersAllowed	正しい	会議名簿（参加者リスト）の音声をミュート/ミュート解除する権限を付与します
muteSelfAllowed	正しい	自分自身にサーバー側のミュートのアクセス許可を付与します
callLockAllowed	正しい	進行中の通話をロック/ロック解除するアクセス許可を付与します
setImportanceAllowed	正しい	会議名簿（参加者リスト）の参加者に重要度を設定/解除する権限を付与します
recordingControlAllowed	正しい	通話で録音が可能な場合、録音制御のアクセス許可を付与します
streamingControlAllowed	正しい	通話でストリーミングが利用可能な場合、ストリーミング制御のアクセス許可を付与します

3.5 その他の関連する依存関係

3.5.1 録音とストリーミング

参加者が録音またはストリーミング制御を使用できるようにするには、次の前提条件を満たす必要があります。

- 録音またはストリーミングは、Call Bridge 用に設定する必要があります。
- スペースには、 **`recordingMode`** が[手動（**`manual`**）]に設定された callProfile が関連付けられている必要があります。

3.5.2 参加者の追加

ActiveControl は、参加者による通話中の新しい参加者へのダイヤルアウトを有効化できますが、その通話を正常に行うためには、要求された URI に正常に接続できる呼制御を使用して Meeting Server のアウトバウンド コールテーブルを正しく設定する必要があります。

3.5.3 暗号化された iX

暗号化された iX メディアをネゴシエートするには、Meeting Server で参加者に対して SIP メディア暗号化を有効にする必要があります。使用できない場合、Meeting Server は暗号化されていない iX メディアをネゴシエートしようとします。これは、参加者、または会議についてレポートされるセキュリティステータスに影響を与える可能性があります。

SIP Media Encryption は、Web 管理インターフェイスの Call Bridge 設定（[**設定**（Configuration）] > [**通話設定**（Call Settings）]）、または参加者に適用される callLeg 設定から無効化することができます。
暗号化された iX が必要な場合は、参加者に対して SIP メディア暗号化が無効化されていないことを確認してください。

4 ActiveControl 機能マトリックス

表 4 に、デバイスタイプごとの ActiveControl 機能の概要を示します。デバイスタイプの詳細については、このガイドの対応するセクションを参照してください。

表 4：ActiveControl 機能のマトリックス

	DX、SX、RK **エンドポイント** CE9.6.2	Cisco Jabber 12.5	ActiveControl **の** Meeting Server **設定**	**注意**
会議名簿（参加者リスト）	はい	はい	該当なし - 自動	
相手側の音声のミュート/ミュート解除	はい	はい	muteOthersAllowed	DTMF 利用可能なオプション
ビデオレイアウト制御	はい	はい	changeLayoutAllowed	DTMF 利用可能なオプション
参加者の追加	いいえ	はい	addParticipantAllowed	
参加者を削除する	はい	はい	disconnectOthersAllowed	
会議の記録制御	はい	はい	recordingControlAllowed	DTMF 利用可能なオプション
会議のストリーミング制御	いいえ	いいえ	streamingControlAllowed	DTMF 利用可能なオプション
録画/ストリームの指標	はい	はい	該当なし - 自動	
会議のロック/ロック解除	いいえ	はい	callLockAllowed	DTMF 利用可能なオプション
重要度の設定/設定解除	いいえ	いいえ	setImportance	
Roster Show Speaker Indicator	はい	はい	該当なし - 自動	
Roster Show Content Contributor	はい	はい	該当なし - 自動	
参加者数	はい	はい	該当なし - 自動	

	DX、SX、RK エンドポイント CE9.6.2	Cisco Jabber 12.5	ActiveControl の Meeting Server 設定	注意
ActiveControl によるローカルミュート	はい	はい	muteSelfAllowed	
ActiveControl によるローカルミュート解除	いいえ	はい	該当なし - 自動	
暗号化された iX メディアのサポート	はい	はい	該当なし - 自動	
メッセージ テキスト	はい	いいえ	該当なし - 自動	

5 Cisco Meeting Server Web アプリケーションの制御

Cisco Meeting Server Web アプリケーションによって会議中の制御を行うことにより、参加者が会議を管理できます。会議制御オプションによっては、SIP 向けの ActiveControl が提供する機能に似ています。主な違いは次のとおりです。

- Web アプリケーションの機能と制御は、SIP 参加者の ActiveControl と同じ方法では管理しません。
- Web アプリケーションは、会議の制御に iX メディアを使用しません。

Web アプリケーションの会議機能を管理する権限は、次の組み合わせです。

- userProfile 設定 – より一般的なユーザーの動作を制御するユーザーに割り当てられたプロファイル。
- スペースメンバーのアクセス許可 – 特定のスペース内でユーザーに割り当てられたアクセス許可。
- callLegProfiles – メンバー、スペース、テナント、またはシステムプロファイルの組み合わせとして参加者に適用される権限。

5.1 会議制御の比較

表 5 では、ActiveControl のオプションと設定を、Web アプリケーションで使用できる会議制御機能と比較しています。この表には、会議機能に関連する Meeting Server の callLegProfile 設定の列と、ゲストユーザーとして参加する Web アプリケーションユーザー（認証されていない、またはメンバーではないスペースに参加する）の違いを示す列も含まれています。

表 5：会議制御の比較

機能	Meeting Server の ActiveControl 設定	Web アプリケーションと同等	Web アプリケーションの動作を制御する設定	Web アプリケーションのゲスト ユーザー エクスペリエンス
会議名簿（参加者リスト）	該当なし - 自動	Yes	自動	
相手側の音声のミュート/ミュート解除	muteOthersAllowed	Yes	muteOthersAllowed	
相手側のビデオのミュート/ミュート解除	使用不可（Not Available）	Yes	videoMuteOthersAllowed	
ビデオレイアウト制御	changeLayoutAllowed	Yes	レイアウト設定はミーティング アプリケーションのローカル設定です	
参加者の追加	addParticipantAllowed	Yes	addParticipantAllowed	ゲストユーザーは利用できません
参加者を削除する	disconnectOthersAllowed	Yes	disconnectOthersAllowed	ゲストは利用できません
会議の記録制御	recordingControlAllowed	Yes	recordingControlAllowed	
会議のストリーミング制御	streamingControlAllowed	Yes	streamingControlAllowed	
会議録画の指標	該当なし - 自動	Yes	該当なし - 自動	
会議のロック/ロック解除	callLockAllowed	Yes	callLockAllowed	
重要度の設定/設定解除	setImportance	Yes	setImportance	

機能	Meeting Server の ActiveControl 設定	Web アプリケーションと同等	Web アプリケーションの動作を制御する設定	Web アプリケーションのゲストユーザーエクスペリエンス
アクティブスピーカー（Roster Show Speaker）の指標	該当なし - 自動	Yes	該当なし - 自動	
Roster Show Content Contributor	該当なし - 自動	Yes	該当なし - 自動	
参加者数	該当なし - 自動	Yes	該当なし - 自動	
ActiveControl によるローカルミュート	muteSelfAllowed	Yes	該当なし - 自動	
ActiveControl によるローカルミュート解除	該当なし - 自動	いいえ	N/A – クライアントのみによって制御されるローカルミュート解除	
暗号化された iX メディアのサポート	該当なし - 自動	なし	なし	
メッセージテキスト	該当なし - 自動	いいえ	該当なし – Web アプリケーションはメッセージテキスト機能をサポートしていません	
スペースへのゲストアクセスを管理する	該当なし – ActiveControl ではサポートされていません	Yes	スペースへのゲストアクセスは、ユーザーポータルを通じて管理できます	ゲストは利用できません

6 設定例

6.1 Meeting Server で ActiveControl 権限を有効にする

このセクションでは、参加者に対してすべての ActiveControl 機能を有効にするために Meeting Server でシステム全体のプロファイルを設定する方法の例を示します。

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

1. システムレベルで適用されている既存の callLegProfiles があるかどうかを確認します – API オブジェクトのリストから、/api/v1/system/profiles の後にある[▶]をタップします

   出力例：

   この出力例では、callLegProfile が一覧にないことが示されているため、新しい callLegProfile を作成して適用できます。

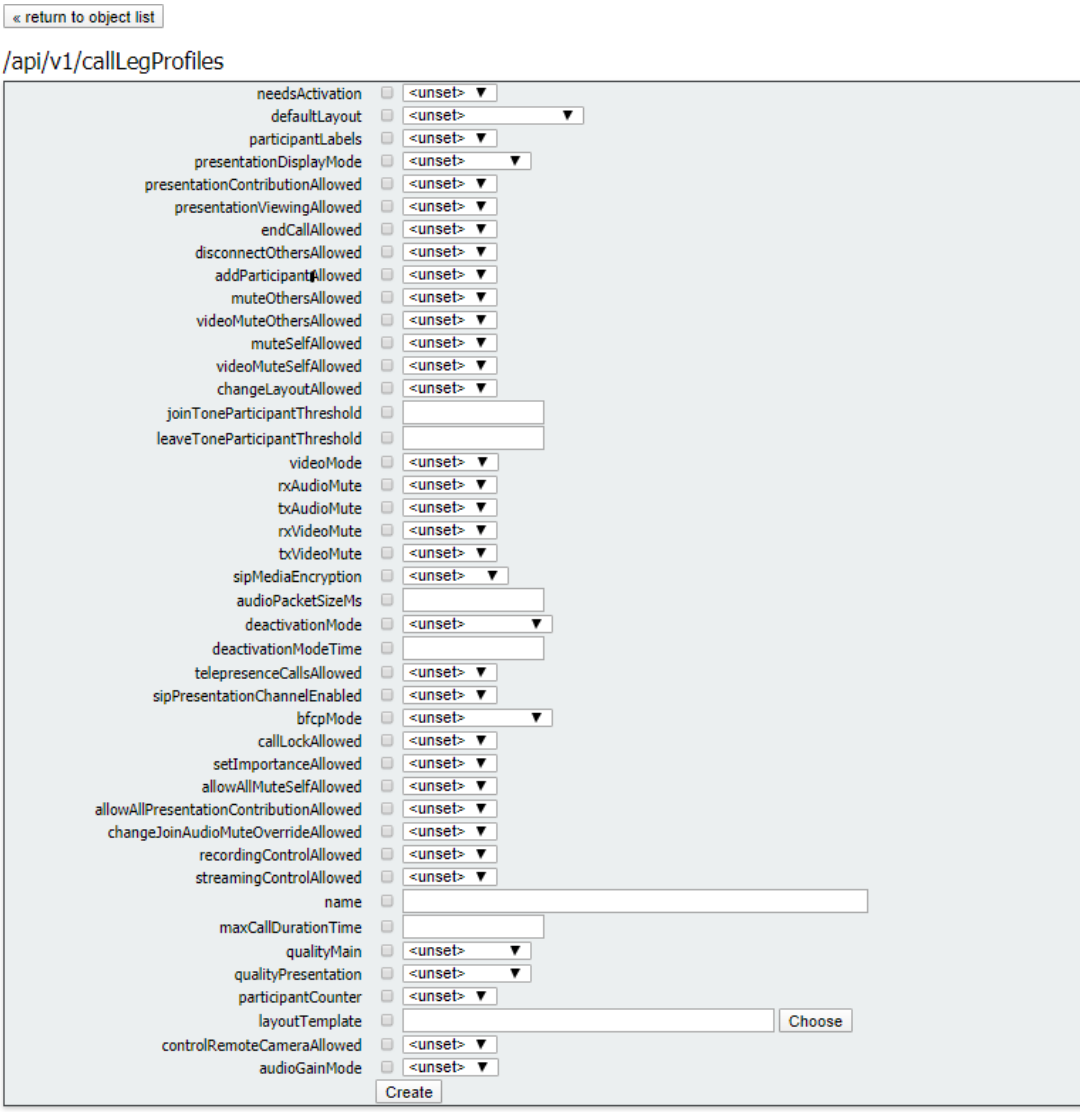
2. API オブジェクトのリストに戻り、リストから、/callLegProfiles の後ろにある[▶]をタップします。

   a. callLegProfile を作成します。

      i. [新規作成（Create new）] ボタンをクリックします。

      ii. 次のパラメータを true に設定します（第 3.4 章 で概説されているように、SIP 参加者の callLegProfile 設定で ActiveControl を有効にするためのすべての権限を含みます）。

- changeLayoutAllowed
- disconnectOthersAllowed
- addParticipantAllowed
- muteOthersAllowed
- muteSelfAllowed
- callLockAllowed
- setImportanceAllowed
- recordingControlAllowed
- streamingControlAllowed

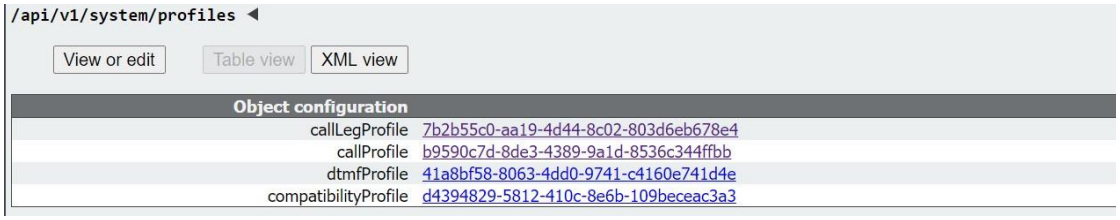


iii. [作成（Create）] をクリックします。

システムプロファイルレベルで適用する必要がある、新しく作成された callLegProfile の**オブジェクト** ID をメモしておきます。

3. API オブジェクトのリストに戻り、リストから、/api/v1/system/profiles の後ろにある[▶]をタップします。
4. [**表示**（View）]**または**[**編集**（edit）]をクリックして、パラメータ callLegProfile まで下にスクロールし、[**選択**（Choose）]をクリックします。
5. 表示されるダイアログから、使用する新しい callLegProfile の**オブジェクト** ID を選択します。
6. [Web 管理（Web Admin）]ページに戻り、[**変更**（Modify）]をクリックします。
7. 新しく作成された callLegProfile は、システム/プロファイルレベルで適用されます。確認するには、API オブジェクトのリストから、/api/v1/system/profiles の後ろにある[▶]をタップします

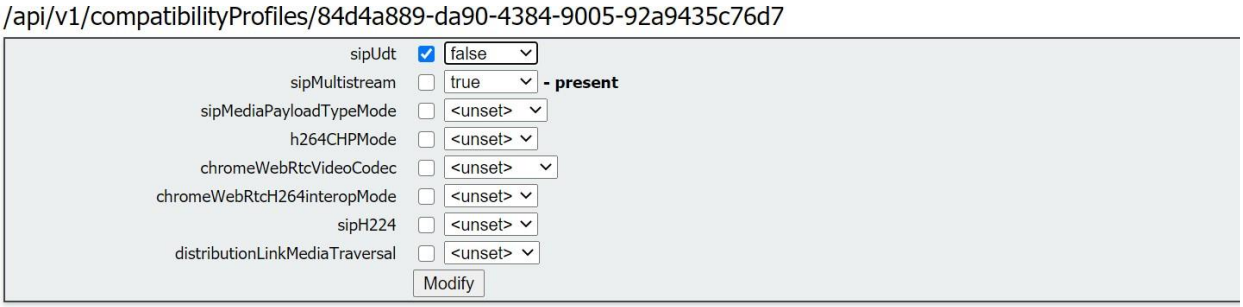
出力例：



6.2 Meeting Server で ActiveControl をオフにする

アクティブコントロールを完全にオフにするには、アクティブな CompatibilityProfile で sipUdt パラメータを false に設定します。

1. API オブジェクトのリストから、/api/v1/compatibilityProfiles の後ろにある[▶]をタップします
2. 有効な compatibilityProfile の**オブジェクト** ID を選択します。
3. sipUdt パラメータを false に設定し、[**変更**（Modify）]をクリックします。



7 ActiveControl のトラブルシューティング

7.1 一般的な ActiveControl の制限事項

以下に、ActiveControl の制限事項を何点か示します。

- ActiveControl は SIP のみのプロトコルであり、相互作用シナリオではサポートされていません。
- 古い SIP デバイスは、iX SIP メッセージを適切に処理できず、表示された場合に通話が失敗する可能性があります。相互運用性の問題を回避するために、次へのトランクでは iX を無効化する必要があります。
  - バージョン 9.1.2 より前のリリースを実行している Unified CM サーバーへのトランク
  - X7.2.3 より前のリリースを実行している VCS/Expressway サーバーへのトランク
  - iX プロトコル処理に起因する通話の失敗が発生した外部ネットワークまたはサードパーティの呼制御デバイスへのトランク

7.2 Meeting Server での ActiveControl ネゴシエーションの確認

ネゴシエートされた場合、ActiveControl は次の場所に表示されます。

- 参加者のステータス/通話の詳細
- 参加者の callLeg API オブジェクト

7.2.1 会議暗号化ステータス

参加者が ActiveControl をネゴシエートすると、iX が暗号化されていない場合、Meeting Server は参加者を暗号化されていないとレポートします。この暗号化されていないユーザーは、他のエンドポイントから表示できるように、会議の暗号化ステータスを下げることができます。

7.3 Meeting Server での iX の無効化

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

必要に応じて、API を介して Meeting Server の UDT を無効にすることで、Meeting Server の ActiveControl を無効化できます。UDT を無効化する手順は次のとおりです。

1. POST メソッドを使用して **`sipUdt`** パラメータを false に設定して互換性プロファイルを作成します（または PUT メソッドで既存のものを変更します）。**`/api/v1/compatibilityProfiles setting sipUdt=false.`**
2. 新しく作成した互換性プロファイルをシステムレベルで設定して、新しく作成した互換性プロファイルを適用します。**`/api/v1/system/profiles`** には、**`compatibilityProfile=<compatibility profile id>`** で PUT メソッドを使用します。

7.4 iX のトラブルシューティング

表 6：iX ヘッダーを含むコールのコール処理概要

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

Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。All rights reserved. Copyright © 1981, Regents of the University of California.
ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよび上記代理店は、商品性、特定目的適合、および非侵害の保証、もしくは取り引き、使用、または商慣行から発生する保証を含み、これらに限定することなく、明示または暗黙のすべての保証を放棄します。

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

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

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

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

Cisco の商標または登録商標