Cisco WebEx Meeting Center with Collaboration Meeting Rooms

エンタープライズ導入ガイド

2015 年 4 月

目次

はじめに

このガイドでは、Cisco WebEx Meeting Center with Collaboration Meeting Rooms（CMR Cloud とも呼ばれる）を使用するようにビデオデバイスおよび TelePresence インフラストラクチャをセットアップする方法を説明します。

導入シナリオ

参加者は、WebEx Web アプリケーション、電話、またはビデオデバイスから CMR Cloud ミーティングに参加できます。ビデオデバイスは WebEx Cloud との間で送受信されるすべてのメディア（メインビデオ、コンテンツ、オーディオ）についてネゴシエートします。このメディアは、SIP または H.323 を使用してネゴシエートされた IP 経由で送受信されます（SIP が推奨されます）。Cisco TelePresence インフラストラクチャを使用すれば、コール制御やファイアウォール トラバーサルが可能になりますが、必須ではありません。

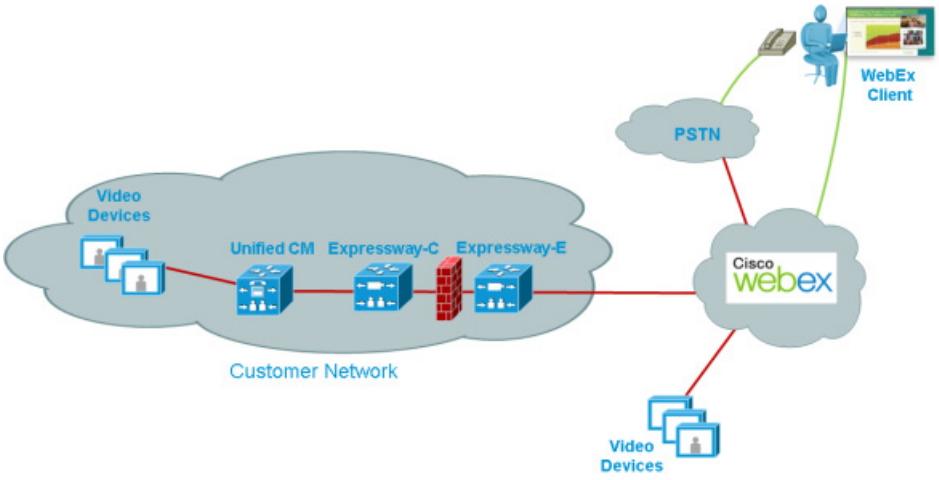
WebEx では、WebEx アプリケーションユーザーおよび電話での参加者に様々な音声ソリューションの選択肢を提供しています。CMR Cloud では、WebEx Audio（Cloud Connected Audio など）や、CMR Hybrid/CMR Cloud との互換性が検証済みの電話会議サービスプロバイダ（TSP）による音声などを利用できます。

WebEx Audio の詳細、および検証済みの TSP 音声プロバイダパートナーの最新の情報については、Cisco Account Manager にご連絡ください。

例：シスコインフラストラクチャを使用した SIP サイト

図 1：Cisco Unified Communications Manager を使用した SIP サイト（4ページ）では、企業のビデオデバイスが Cisco Unified Communications Manager に登録され、通話のセキュリティ保護とファイアウォールトラバーサルを実現するために Cisco Expressway-C と Cisco Expressway-E が使用されています。

図 1：Cisco Unified Communications Manager を使用した SIP サイト



Cisco TelePresence インフラストラクチャでは、以下の導入シナリオも可能です。

- Cisco VCS Control および Cisco VCS Expressway
  ビデオデバイスを Unified CM ではなく Cisco VCS に登録します。
- Cisco VCS Control と Cisco VCS Expressway および Unified CM
  ビデオデバイスを Cisco VCS と Unified CM の両方に登録します（上記の 2 つのモデルを組み合わせたシナリオ）。

前提条件

要件

表 1：CMR Cloud 導入の要件

要件	説明
Cisco WebEx Meeting Center	Cisco WebEx Meeting Center サイトではリリース WBS29 が実行されている必要があります。
Audio	WebEx では、WebEx アプリケーションユーザーおよび電話での参加者に様々な音声ソリューションの選択肢を提供しています。CMR Cloud では、WebEx Audio（Cloud Connected Audio など）や、CMR Hybrid/CMR Cloud との互換性が検証済みの電話会議サービスプロバイダ（TSP）による音声などを利用できます。 WebEx Audio の詳細、および検証済みの TSP 音声プロバイダパートナーの最新の情報については、Cisco Account Manager にご連絡ください。
ネットワーク アクセス	Cisco Expressway-E、Cisco VCS Expressway、その他のエッジトラバーサルデバイスおよびファイアウォールのポート範囲で以下のトラフィックが許可されることを確認してください。 ▪ RTP ポート 36000 ～ 59999：UDP を使用した WebEx クラウドからのインバウンドメディアトラフィック ▪ ポート 5060 および 5061：TCP を使用した WebEx クラウドからのインバウンドシグナリングトラフィック ▪ RTP ポート 36000 ～ 59999：UDP を使用した WebEx クラウドへのアウトバウンドメディアトラフィック ▪ ポート 5060 ～ 5070：TCP を使用した WebEx クラウドへのアウトバウンドシグナリングトラフィック WebEx クラウドで使用する、地理的な場所ごとの IP アドレス範囲については、次の URL にアクセスしてください。 https://kb.webex.com/WBX264 [英語]
ネットワークの帯域幅	必要なネットワーク帯域幅は、求められるビデオ品質とプレゼンテーションデータを提供するための各ビデオデバイスの要件によって異なります。 最適なエクスペリエンスを実現するには、1 画面あたり 1.5 Mbps 以上に設定することを推奨します。一部のビデオデバイスではこれ以上のレートを利用できます。また、デバイスによっては、サービスでこれ以下のレートに対応することも可能です。
Quality of service	出力ゲートウェイでは、次の DSCP マーキングをサポートしている必要があります。 ▪ RFC 2597 準拠の DSCP AF41 でマーキングされたビデオトラフィック ▪ RFC 3246 準拠の DSCP EF でマーキングされた音声トラフィック

ネットワーク インフラストラクチャ

ビデオデバイスには、各種の標準規格に準拠した任意のコール制御システムを使用できます。導入環境にファイアウォールトラバーサルデバイスを含めて、モバイルアクセスおよびリモートアクセスを可能にすることもできます。

以下の表は、該当する機能を提供可能なシスコ製品の推奨バージョンを示したものです。これらのコンポーネントは必須ではありません。

表 2：CMR Cloud 導入環境に推奨されるネットワークインフラストラクチャ

コンポーネント	推奨されるシスコ製品
コール制御、デバイス登録	▪ Cisco Unified Communications Manager（テスト済みリリース：9.1(1)、9.1(2) および 10.5） ▪ Cisco VCS Control と Cisco VCS Expressway（テスト済みリリース：X8.1）
ファイアウォールトラバーサル、モバイルおよびリモートアクセス	▪ Cisco Expressway-C と Cisco Expressway-E（テスト済みリリース：X8.1） ▪ Cisco VCS Control と Cisco VCS Expressway（テスト済みリリース：X8.1）

注：バージョン X8.1/X8.1.1 では、Cisco Expressway-E または Cisco VCS Expressway をスタティック NAT 用に設定してメディア暗号化を有効にした場合、WebEx クラウドへのコールが失敗します（警告：CSCum90139）。スタティック NAT を使用する場合にコールを保護するには、X8.2 にアップグレードすることを推奨します。

ビデオ デバイス

以下の表は、デバイスのタイプごとの一般要件と考慮事項を示したものです。

表 3：CMR Cloud 導入環境のビデオデバイス要件

デバイス/クライアントのタイプ	要件
SIP	▪ 参加者が共有コンテンツを提示または表示するには、デバイスがクラウドサーバーと Binary Floor Control Protocol（BFCP）をネゴシエート可能でなければなりません。BFCP を使用しなければ、コンテンツを共有できません。その場合、コンテンツはメインビデオチャネルに埋め込まれたように表示されます。 ▪ 3 つ以上の画面を持つデバイスで複数の画面にビデオを表示するには、そのデバイスが WebEx クラウドサーバーと TelePresence Interoperability Protocol（TIP）をネゴシエート可能でなければなりません。 **注**：CMR Cloud では、スタンドアロンモードで設定された SIP エンドポイントをサポートしていません。

デバイス/クライアントのタイプ	要件
H.323	▪ H.323 デバイスは、URI ダイヤリング（Annex 0）を使用して WebEx クラウドにコールインする必要があります。URI ダイヤリングのセットアップ方法については、ベンダー提供の資料を参照してください。 ▪ IVR を使用して、主催者として会議を開始したり、主催者より前に会議に参加したりするには、H.323 デバイスが H.245 ユーザー入力方式または RFC 2833 方式の DTMF シグナリングをサポートしている必要があります。この機能を使用せずに会議を開始するには、ユーザーは H.323 デバイスから参加する前に、主催者として WebEx アプリケーションにサインインする必要があります。 ▪ 参加者が共有コンテンツを提示または表示するには、デバイスがクラウドサーバーと H.239 をネゴシエート可能でなければなりません。H.239 を使用しなければ、コンテンツを共有できません。その場合、コンテンツはビデオに埋め込まれたように表示されます。 ▪ 3 つ以上の画面を持つ H.323 デバイスはサポートされていません。3 つ以上の画面を持つデバイスで複数の画面にビデオを表示するには、そのデバイスが WebEx クラウドサーバーと TelePresence Interoperability Protocol（TIP）をネゴシエートするように設定されている必要があります（また、TIP は SIP で実行されるため、H.323 ではなく TIP/SIP を使用するように再設定する必要もあります）。

導入タスク

ここでは、以下の大まかな各ワークフローでの具体的なタスクについて説明します。

1. 準備：提供サービスと前提条件の理解、注文するための準備
2. セットアップ：インフラストラクチャと WebEx クラウドの接続、サービスの設定
3. セキュリティ設定：コールセキュリティの設定（Cisco Expressway シリーズまたは Cisco VCS が必要です）
4. 検証および完了：サービスの動作確認、ユーザーへのサービスの提供

準備

タスク 1：サービスを理解する

はじめに、前提条件（5 ページ）に示されている前提条件を確認します。

ユーザーがサービスに接続してサービスを使用する仕組みについて理解するには、CMR Cloud 会議の開催および参加（17 ページ）を参照してください。

サイトでテレフォニーサービスプロバイダ（TSP）の統合音声を使用する場合は、TSP 音声について（21 ページ）を参照してください。

タスク 2：注文のための準備をする

CMR Cloud の注文に先立って、シスコパートナーまたは Cisco Account Manager は Assessment to Quality（A2Q）を送信して承認を得る必要があります。導入を確実に成功させるために、シスコは A2Q を使用して、お客様の環境を検討します。

注文の処理が完了すると、Cisco WebEx サイトへのアクセス情報の詳細（URL とサイト管理用アカウント）を受け取ります。

セットアップ

タスク 3：WebEx クラウドのポート範囲を開く

手順については、該当する管理者ガイドの「Configuring firewall rules」の項を参照してください。

- 『Cisco Expressway Administrator Guide』
- 『Cisco VCS Administrator Guide』

タスク 4：Cisco Expressway-E で WebEx クラウドの DNS ゾーンおよび検索ルールを作成する

Cisco Expressway-E（または Cisco VCS Expressway）のデフォルト DNS ゾーンの設定を使用して、WebEx クラウドにコールをルーティングできます。ただし、暗号化を適用する場合は特に、以下のゾーン設定を推奨します。（既存の DNS ゾーンの設定を変更したくない場合は、WebEx 専用の DNS ゾーンを別途作成し、以下の推奨に従ってゾーンを設定することもできます）。

	非セキュア	セキュア（サードパーティ CA 署名付き証明書）	セキュア（自己署名付き証明書）
H.323 Mode	*On*（デフォルト）または *OFF*（推奨）	*On*（デフォルト）または *OFF*（推奨）	*On*（デフォルト）または *OFF*（推奨）
SIP Media encryption mode	*Auto*（デフォルト）または *Best Effort*	*Forced Encrypted* または *Best Effort*（[H.323 Mode] を [On] に設定した場合は必須）	*Forced Encrypted* または *Best Effort*（[H.323 Mode] を [On] に設定した場合は必須）
TLS Verify mode	*Off*	*On*	*Off*
[TLS verify subject name] フィールド	N/A	`sip.webex.com`	N/A
Advanced zone profile	*Default* または *Custom*（[H.323 Mode] を [Off] に設定した場合は必須）	*Default* または *Custom*（[H.323 Mode] を [Off] に設定した場合は必須）	*Default* または *Custom*（[H.323 Mode] を [Off] に設定した場合は必須）
Automatically respond to SIP searches	*Off*（デフォルト）または *On*（[H.323 Mode] を [Off] に設定した場合は必須）	*Off*（デフォルト）または *On*（[H.323 Mode] を [Off] に設定した場合は必須）	*Off*（デフォルト）または *On*（[H.323 Mode] を [Off] に設定した場合は必須）
SIP SDP attribute line limit mode	*Off*（[Advanced zone profile] を [Custom] に設定した場合は必須）	*Off*（[Advanced zone profile] を [Custom] に設定した場合は必須）	*Off*（[Advanced zone profile] を [Custom] に設定した場合は必須）

以下のプロパティを使用して WebEx ドメインの検索ルールを作成します。

プライオリティ	既存の DNS ゾーンの検索ルールより小さい値を使用します。
プロトコル	*いずれか（Any）*
ソース	<Admin Defined>（デフォルト：*Any*）
モード	*エイリアスのパターンマッチ*
パターンタイプ	*Regex*
パターン文字列	`(.*)@(.*)(\.webex\.com).*`
パターン動作	*Replace*
置換文字列	`\1@\2\3`
正常に一致する場合	*Stop*
Target	<WebEx Cloud にコールをルーティングするために使用する DNS ゾーン>
状態	*イネーブル*

詳細については、該当する管理者ガイドの「Routing configuration」の章を参照してください。

- 『Cisco Expressway Basic Configuration Deployment Guide』
- 『Cisco VCS Basic Configuration (Control with Expressway) Deployment Guide』

タスク 5：Cisco Expressway C（または Cisco VCS Control）で Unified CM のネイバーゾーンの BFCP を有効にする

注：BFCP では Cisco Unified Communications Manager バージョン 8.6(1) 以降が必要です。BFCP の相互運用性を確保するために、8.6(2a)SU3 以降のバージョンを使用することを強く推奨します。

プレゼンテーション共有を有効にするには、Cisco Expressway C または Cisco VCS Control の Unified CM ネイバーゾーンで BFCP が 有効にされていることを確認します。

X8.1 以降では、Unified CM ネイバーゾーンで Unified CM バージョン 8.6(1) 以降の適切な拡張ゾーンプロファイルを選択すると、BFCP が自動的に有効にされます。

Cisco VCS Control X7.2 および X7.1 では、Unified CM ネイバーゾーンでカスタム拡張ゾーンプロファイルパラメータを明示的に設定します。手順については、該当する導入ガイドの BFCP の有効化に関する付録を参照してください。

- 『Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide (X7.2)』
- 『Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide (X7.1)』

タスク 6：Cisco Expressway への SIP トランクを Unified CM に設定する

Unified CM に登録されたエンドポイントが CMR Cloud 会議に参加したり、Cisco VCS Control に登録されたエンドポイントを呼び出したりできるようにするために、Unified CM に Cisco Expressway-C（または Cisco VCS Control）への SIP プロファイルおよびトランクを設定します。

プレゼンテーション共有を有効にするには、[SIP Profile Configuration] ウィンドウの [Trunk Specific Configuration] セクションで、[Allow Presentation Sharing using BFCP] チェックボックスを必ずオンにしてください。（BFCP をサポートしているサードパーティ製ビデオデバイスの場合は、[Phone Configuration] ウィンドウの [Protocol Specific Information] セクションでも、[Allow Presentation Sharing using BFCP] チェックボックスをオンにする必要があります。

詳細については、該当するマニュアルを参照してください。

- 『Cisco Unified Communications Manager with Cisco Expressway (SIP Trunk) Deployment Guide』
- 『Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide』

タスク 7：Unified CM でルートパターンを追加する

Unified CM で、*.webex.com（または *.*）の SIP ルートパターンを追加し、そのパターンで Cisco Expressway-C（または Cisco VCS Control）への SIP トランクを指します。

ルートパターンの設定手順については、該当するリリースの『Cisco Unified Communications Manager Administration Guide』を参照してください。

タスク 8：帯域幅の制御を設定する

最適なエクスペリエンスを実現するには、1 画面あたり 1.5 Mbps 以上に設定することを推奨します。一部のビデオデバイスではこれ以上のレートを利用できます。また、デバイスによっては、サービスでこれ以下のレートに対応することも可能です。

- Cisco Expressway または Cisco VCS で、必要最小限の帯域幅を使用できるように（ネットワークの要件に応じて）適切にゾーンとパイプを設定します。

手順については、該当する管理者ガイドの「Bandwidth control」の章を参照してください。
- 『Cisco Expressway Administrator Guide』
- 『Cisco VCS Administrator Guide』

- Unified CM と WebEx クラウドのエンドポイント間で最適な SIP 音声およびビデオ接続を確保するため、Unified CM で、最小限必要な帯域幅を使用できるようにリージョンを設定します。
  リージョンの設定手順については、該当するリリースの『Cisco Unified Communications Manager Administration Guide』を参照してください。

タスク 9:ビデオダイヤル文字列を短縮する

スケジュールされた CMR Cloud 会議に参加するためにテレプレゼンスユーザーが通常ダイヤルしなければならない文字列は、9 桁の会議番号の後に @ 記号と WebEx サイトドメインが続く文字列です（たとえば、123456789@customer-a.webex.com）。

パターン置換を使用することで、企業内の SIP および H.323 ビデオデバイスに対してこの文字列を短縮できます。以下の例では、ダイヤルする際にドメインの代わりとして入力できる短いプレフィックスを追加します。この導入環境の例では、企業のビデオデバイスが Unified CM に登録されていて、Cisco Expressway Series（または Cisco VCS）を使用してリモートデバイスおよびファイアウォールトラバーサルに対応しています。この環境で、Unified CM のルートパターンと Cisco Expressway の変換機能を使用して、短縮ダイヤル文字列をルーティングし、それを完全なビデオダイヤル文字列に変換します。

短縮ダイヤルをセットアップするには、以下の手順に従います。

1. ダイヤルプランで頻繁に使用されていない数字で始まるプレフィックスを選択します。プレフィックスには * または # を使用できます。
2. Unified CM で、そのプレフィックスで始まり、その後にドット（ピリオド）文字と会議番号を表す 9 桁の X 文字が続くルートパターンを作成します。

   たとえば、プレフィックスが 7 の場合は、ルートパターンとして **`7.XXXXXXXXX`** を使用します。
3. コールを Cisco Expressway に転送するようにルートパターンを設定します。
4. Cisco Expressway で、7 で始まり 9 桁の数字が続くすべてのダイヤル文字列と一致する変換パターンを作成します。

   たとえば、プレフィックスが 7 の場合は、**`7(\d{9)`** という正規表現のパターン文字列を使用します。
5. プレフィックスの数字（この例では 7）を削除し、ドメイン（@customer- a.webex.com）を末尾に追加するよう変換パターンを設定し、コールが該当する WebEx サイトにルーティングされるようにします。

   たとえば、上記の正規表現パターンの場合、置換文字列として **`1@customer-a.webex.com`** を使用します。

この例で、ユーザーが 7123456789 をダイヤルすると、コールは最終的に 123456789@customer- a.webex.com としてルーティングされます。この置換は、Unified CM に登録されたデバイスと Cisco VCS Expressway に登録されたリモートデバイスの両方に適用されます。

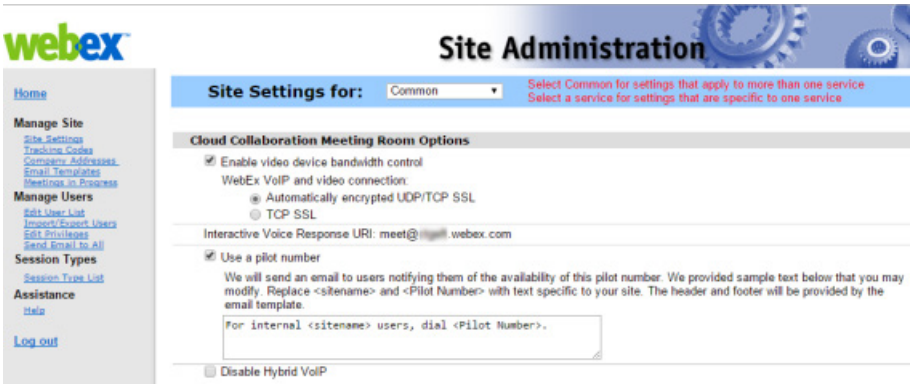
注意する点として、この短縮化が適用されるのは、企業内のデバイスで、その企業で開催されている会議に参加する場合のみです。他の企業で開催されている会議にダイヤルするユーザーや、外部のビデオ参加者は、ドメインを含む完全なビデオダイヤル文字列をダイヤルする必要があります。

タスク 10：CMR Cloud のサイト管理の設定を行う

WebEx アカウントチームを介して Cisco WebEx サイト管理にアクセスするには、固有の WebEx サイト管理 URL とパスワードを使用します。最初のセットアップ時に、サイト管理者としてログインし、アカウントを統合してプロビジョニングする必要があります。最初のセットアップを完了した後は、アカウントを管理したり、WebEx ユーザーガイドや管理ガイドにアクセスして、サイトに設定されたサービスと機能について参照したりできます。

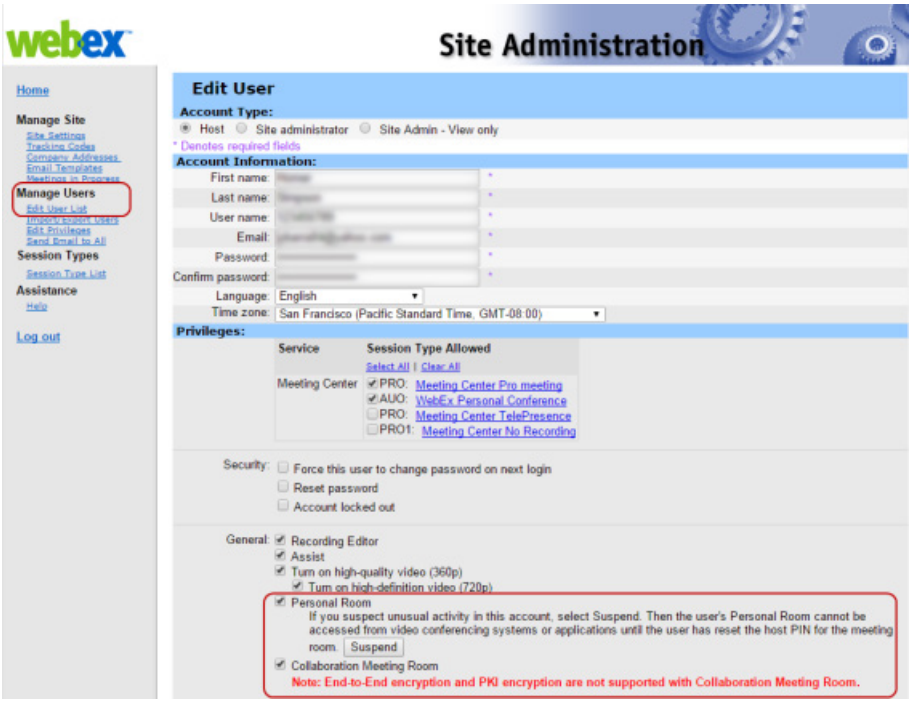
CMR Cloud のサイト全体の設定を行うには、サイト管理の左側にあるナビゲーションバーで、[Manage Site] から[Site Settings] を選択し、[Cloud Collaboration Meeting Room Options] まで下方向にスクロールします。

図 2：CMR Cloud のサイト設定



ユーザーを追加または編集する際に、そのユーザーのクラウド Collaboration Meeting Room オプションを有効/無効にできます。パーソナル Collaboration Meeting Room（「パーソナルルーム」とも呼ばれます）をサイトレベルで有効にすると、個々のユーザーについてパーソナルルームを有効/無効にすることができます。[Edit User] ページでは、パーナル CMR を一時停止することもできます。これにより、所有者が主催者 PIN を変更するまで、主催者とゲストはアクセスできなくなります。

図 3：クラウド Collaboration Meeting Room のユーザー設定



注: [Meeting Center TelePresence] チェックボックスをオンにすると、Cisco Collaboration Meeting Rooms Hybrid が有効になります。このチェックボックスがオンになっていなくても、クラウド Collaboration Meeting Room オプションを有効にできます。この 2 つのサービスを一緒に使用する方法については、Cisco Collaboration Meeting Rooms Hybrid サービスとクラウド Collaboration Meeting Room サービスの共用（20 ページ）を参照してください。

詳細については、WebEx の [Support] > [User Guides] ページにある『Cisco WebEx Site Administration User Guide』を参照してください。

セキュリティ設定

SIP ベースのコールに対して、Cisco WebEx CMR Cloud サービスでは以下の 3 つのレベルのセキュリティをサポートしています（優先順に記載）。

1. CA 署名付き証明書と sRTP メディア暗号化による暗号化 TLS シグナリング、または非セキュア RTP メディア（自動的にメディア暗号化をネゴシエートし、クライアントが sRTP を提供していない場合は RTP にフォールバックします）
2. 自己署名付き証明書と sRTP メディア暗号化による暗号化 TLS シグナリング、または非セキュア RTP メディア（自動的にメディア暗号化をネゴシエートし、クライアントが sRTP を提供していない場合は RTP にフォールバックします）
3. 非セキュア RTP メディアを使用した、非セキュア TCP シグナリング

H.323 ベースのコールに対しては、CMR Cloud サービスは非セキュア H.225/H.245 シグナリング方式と H.235 メディア暗号化方式をサポートしています。

これらの方式は、各コールのシグナリングで自動的にネゴシエートされます。デフォルトでは、Cisco Expressway および Cisco VCS Expressway シリーズは自己署名付き証明書を使用します。したがって、SIP の使用時には WebEx クラウドとセキュリティレベル 2 をネゴシエートします。

WebEx クラウドに対する通話のセキュリティ保護を有効にするには、この項で説明するタスクを行ってください。これらのタスクには、Cisco Expressway シリーズ（Cisco Expressway-C と Cisco Expressway-E）または Cisco VCS（Cisco VCS Control と Cisco VCS Expressway）が必要です。他のベンダー製機器で同様のタスクを行うには、ベンダーの資料を参照してください。

タスク 11：サポートされるルート認証局を選択する

WebEx では、特定のルート認証局から発行された証明証をサポートしています。証明書のプロバイダに複数のルート認証局があり、そのすべてが WebEx でサポートされていない場合もあります。使用する証明書は、以下の認証局のいずれか（またはこれらの中間認証局のいずれか）によって発行されたものでなければなりません。そうでない場合、WebEx は Cisco Expressway-E または Cisco VCS Expressway からのコールを受け入れません。

- 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[1]
- verisign_class_1_public_primary_ca_-_g3
- ca_cert_signing_authority
- geotrust_global_ca
- globalsign_root_ca
- thawte_primary_root_ca
- geotrust_primary_ca
- addtrust_external_ca_root
-

上記のリストは、変更される可能性があります。最新の情報については、WebEx に問い合わせるか、https://kb.webex.com/WBX83490 [英語] で確認してください。

[1]entrust_2048_ca によって生成された証明書を Cisco VCS ExpresswayX7.2（または X7.2 からアップグレードした以降のバージョン）で使用するには、Cisco VCS Expressway の信頼できる CA のリストに含まれている Entrust ルート CA 証明書を、Entrust から入手できる最新バージョンに置き換える必要があります。最新の entrust_2048_ca.cer ファイルは、Entrust Web サイト（https://www.entrust.net/downloads/root_index.cfm [英語]）のルート証明書のリストからダウンロードできます。

タスク 12：Cisco Expressway-E を使用して証明書署名要求を生成する

コールを保護するには、Cisco Expressway-E（または Cisco VCS Expressway）を使用して証明書署名要求（CSR）を生成し、その CSR をダウンロードして対象のルート認証局（CA）に送信する必要があります。ほとんどの認証局では、CSR を PKCS#10 要求フォーマットで提供するよう規定しています。

これに対し、CA からの応答に、サーバー認証鍵とクライアント認証鍵の両方が含まれる SSL サーバー証明書が提供されていることを確認してください。

証明書署名要求プロセスの詳細については、該当するガイドの「Generating a certificate signing request」の項を参照してください。

- 『Cisco Expressway Certificate Creation and Use Deployment Guide』
- 『Cisco VCS Certificate Creation and Use Deployment Guide』

タスク 13：Cisco Expressway-E に署名付き SSL サーバー証明書をインストールする

公式 CA から SSL サーバー証明書を受け取ったら、その証明書を Cisco Expressway-E（または Cisco VCS Expressway）にロードします。

証明書をロードする方法の詳細については、該当するマニュアルの「Loading certificates and keys」で始まるタイトルの項を参照してください。

- 『Cisco Expressway Certificate Creation and Use Deployment Guide』
- 『Cisco VCS Certificate Creation and Use Deployment Guide』

タスク 14：Cisco Expressway-E に信頼できる CA のリストを設定する

セキュアな呼び出しの設定を完了するには、Cisco Expressway-E（または Cisco VCS Expressway）の信頼できる CA のリストに、次の 2 種類の証明書が含まれていなければなりません。

- SSL サーバー証明書に署名を付けるために使用した公的 CA のルート証明書（および該当する場合は中間証明書）。
- WebEx クラウドで使用する公的 CA の証明書。これらの証明書を取得するには、以下のリンクにあるコンテンツをコピーして、拡張子を .PEM に設定した別のテキストファイルに貼り付けます。
  - VeriSign Class 3 Public Primary CA
  - VeriSign Class 3 Primary CA - G5
  - VeriSign Class 3 Public Primary CA - G3
  - QuoVadis Root CA 2

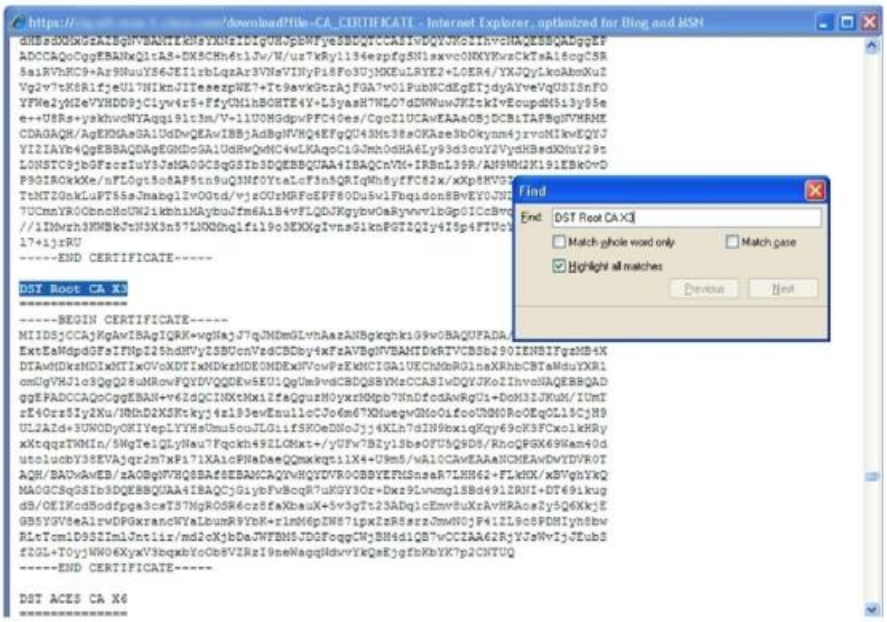
信頼できる CA のリストを設定する方法の詳細については、該当するマニュアルを参照してください。

- 『Cisco Expressway Certificate Creation and Use Deployment Guide』
- 『Cisco VCS Certificate Creation and Use Deployment Guide』

信頼できる CA リストに CA 証明書が含まれているかどうかを判別するには、以下の手順に従います。

1. Cisco Expressway-E または Cisco VCS Expressway で、次の操作を行います。
   - X8.1 以降では、[Maintenance] > [Security certificates] > [Trusted CA certificate] に移動します。
   - X7.2.3 では、[Maintenance] > [Certificate management] > [Trusted CA certificate] に移動します。
2. [Show CA certificate] をクリックします。

   新しいウィンドウに、現行の信頼できる CA リストが表示されます。
3. 該当する証明書を発行した CA の名前（たとえば、**`DST Root CA X3`**）を検索します。



検証および完了

タスク 15：CMR Cloud サービスを検証する

1. テスト用ホストアカウントを作成して、そのアカウントを CMR Cloud（および、該当する場合はパーソナル CMR）に対して有効にします。TSP 音声を使用する場合、TSP の電話会議アクセスパラメーターを使用して主催者アカウントを設定します。
2. テスト用の主催者として WebEx サイトにサインインし、Windows 用生産性ツールをダウンロードして、パーソナル CMR セットアップ（該当する場合）を実行します。
3. Windows 用生産性ツールを使用して、WebEx ミーティングをスケジュールします。
   - スケジュールした会議が予定表に表示されることを確認します。
   - テスト用主催者が WebEx から会議の確認メールを受信することを確認します。
4. パーソナル CMR（該当する場合）またはスケジュールされた会議にコールインします。
   - WebEx ミーティングアプリケーションと、テレプレゼンス、Jabber、またはその他のビデオデバイスとの間の双方向ビデオを確認します。
   - プレゼンテーション共有をサポートしているデバイスがプレゼンテーションを共有できることを確認します。

CMR Cloud 会議の開催および参加

スケジュール済み CMR Cloud 会議の作成

会議の主催者は、Cisco WebEx と TelePresence を Outlook または WebEx Web サイトに統合する機能を使用して、会議をスケジュールできます。

会議は、以下の方法で開始できます。

- 任意の時間に、主催者が参加して会議を開始できます。
- スケジュールされた開始時間に、会議参加者が会議にコールインできます。主催者が必要な会議に主催者が参加していない場合、参加者は、会議がまだ開始されていないことを通知するメッセージを受信します。この場合、参加者は会議に参加できるようになるまで待つ必要があります。
- 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 [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。

パーソナル Collaboration Meeting Room の使用

パーソナル Collaboration Meeting Room（パーソナル CMR、またはパーソナルルーム）は、主催者に集合場所のようなタイプの永続的な会議室を提供します。パーソナルルームが有効になっている場合、主催者は他の参加者を招待して、主催者 PIN を使用して会議を随時開始できます。主催者がプライバシーを必要とする場合や連続して会議を行う場合は、パーソナルルームをロックできます。この場合、ロックが解除されるまで、以降の発信者は会議に参加できません。

主催者は [My WebEx] プロファイルで、主催者 PIN を設定して、パーソナルルームをインスタントミーティングに使用するかどうかを選択できます。パーソナルルームごとに、一定の会議数とデフォルトの Web URL（https://<sitename>.webex.com/meet/<hostID> 形式）が割り当てられます。ユーザーはビデオデバイスまたはアプリケーションから URI <userid>@<sitename>.webex.com にダイヤルすることによっても、主催者のパーソナルルームにアクセスできます。

サイト設定で有効にされている場合、主催者は必要に応じて、パーソナルルームの ID とタイトルを変更できます。ID を変更すると、デスクトップユーザーおよびモバイルユーザー用の Web URL と、SIP および H.323 デバイス用の URI が変更されます。タイトルは、WebEx アプリケーションに表示されるだけでなく、ビデオデバイスまたはアプリケーションから参加したユーザーに表示されるロビー画面にも表示されます。

クラウド Collaboration Meeting Room 会議への参加

WebEx 参加者が CMR に参加するには、会議への招待に記載されているリンクを使用します。また、パーソナル CMR の場合は、https://<sitename>.webex.com/meet/<hostID> にアクセスして参加します。

SIP 標準および H.323 ビデオデバイスを使用している参加者は、以下のいずれかにダイヤルして会議に参加できます。

- 自動音声応答装置（IVR）サーバーのパイロット URI をダイヤルし、9 桁の会議番号と、該当する場合は主催者 PIN を入力します。（IVR を使用するには、H.323 デバイスが H.245 ユーザー入力方式または RFC 2833 方式の DTMF シグナリングをサポートしている必要があります）。

- 9 桁の会議番号の後に @ 記号と WebEx サイトドメインが続くビデオダイヤル文字列（たとえば、**123456789@customer-a.webex.com**）。
- 短縮ダイヤル文字列（企業内のデバイスの場合のみ）。タスク 9:ビデオダイヤル文字列を短縮する（11 ページ）を参照してください。

テレプレゼンス会議エクスペリエンス

会議中、テレプレゼンス参加者には、他のすべてのテレプレゼンス参加者のライブビデオと、最後にアクティブになった WebEx 参加者のビデオが表示されます。WebEx 参加者には、他のすべての WebEx 参加者のビデオと、最後にアクティブになったテレプレゼンス参加者のビデオが表示されます。（WebEx 参加者のカメラがオンになっていない場合、その参加者は黒いシルエットとして表示されます）。

プレゼンテーションを共有する場合、テレプレゼンス参加者はビデオディスプレイのケーブルをコンピュータに接続し、（必要な場合は）ボタンを押して、テレプレゼンス参加者および WebEx 参加者とのプレゼンテーション共有を開始します。アクティブなテレプレゼンスプレゼンタのビデオが、Cisco WebEx Web クライアントにストリーミング配信されます。WebEx からのビデオとプレゼンテーションがテレプレゼンス参加者に表示されます。

Cisco WebEx ミーティングエクスペリエンス

参加者が Cisco WebEx ミーティングに参加するには、Cisco WebEx Meeting Center の Web アプリケーションまたはモバイルアプリケーションにログインします。Meeting Center アプリケーションにはテレプレゼンス参加者が共有するコンテンツが自動的に表示され、WebEx 参加者はデスクトップやアプリケーションをテレプレゼンス参加者と共有できるようになります。デフォルトで WebEx 参加者に表示されるのは、現在プレゼンテーション中のテレプレゼンス参加者または WebEx 参加者のビデオです。

WebEx 参加者には、すべての会議参加者の一覧も表示されます。WebEx アノテーション機能がサポートされています。WebEx 参加者は、Meeting Center アプリケーションに標準装備されているアノテーションツールを使用できます。これらのアノテーションは、WebEx 参加者とテレプレゼンス参加者の両方に表示されます。ただし、テレプレゼンス参加者は、アノテーションツールを使用できません。

WebEx 参加者がテレプレゼンス参加者とプレゼンテーションを共有するには、以下の手順に従う必要があります。

1. コンピュータで Cisco WebEx Meeting Center アプリケーションにログインします。
2. [Quick Start] タブで、[Share Application] をクリックします。
3. 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。

Cisco WebEx ミーティング機能の使用方法の詳細については、Cisco WebEx Meeting Center アカウントにログインして、左側のナビゲーションペインで [Support] をクリックしてください。

Video Quality

テレプレゼンス参加者から WebEx 参加者に送信されるビデオの品質は、帯域幅が最も小さい WebEx クライアントに合わせて設定されます。帯域幅が最も小さい WebEx クライアントが会議から退席すると、すぐに帯域幅が増加する場合があります。たとえば、会議に参加している WebEx クライアントの 1 人が 360p にしか対応していない場合、テレプレゼンス参加者からすべての WebEx 参加者への最大帯域幅は 360p に制限されます。その参加者が会議から退席すると、他のすべてのクライアントがより大きい帯域幅（たとえば、720p）に対応している場合、すべての WebEx 参加者の帯域幅が増加します。

プレゼンタが複数いる場合のプレゼンテーションの表示の詳細

テレプレゼンス参加者がプレゼンタになるには、ビデオディスプレイのケーブルをビデオデバイスに接続し、(必要な場合は)デバイス上のプレゼンテーションボタンを押します。複数のテレプレゼンス参加者が同時にプレゼンテーションを行うと、最後にプレゼンテーションを開始したデバイスのものが表示されます。ケーブルが外されると、次のプレゼンタが再びプレゼンテーションを開始する必要があります。

WebEx 参加者がプレゼンタになる場合は、[Quick Start] タブで [Share Application] をクリックし、プレゼンテーションのコンテンツを選択します。

注:主催者しかプレゼンテーションできないように WebEx サイトがプロビジョニングされている場合、プレゼンテーションを許可されていない出席者がプレゼンテーションを行うには、主催者キーを使用して新しい主催者になる必要があります。

会議参加者リスト

WebEx の会議参加者リストには、WebEx 参加者とテレプレゼンス参加者の両方が含まれます。単一の参加者またはすべての参加者をミュート/ミュート解除する機能は、WebEx 参加者とテレプレゼンス参加者の両方が使用できます。ユーザーが WebEx インターフェイスから会議を終了した場合、すべての参加者が切断されます。

SIP ベースのビデオデバイスを使用しているテレプレゼンス参加者の表示名は、エンドポイントからの再招待メッセージまたは更新メッセージに含まれる多数のフィールドから決定されます。H.323 エンドポイントの表示名は、Q.931 表示名または H323-ID から決定されます。いずれにしても、表示名に複数の候補がある場合には、システムは以下の優先順で表示名を選択します。

表 4:エンドポイントの表示名を選択する際の優先順位

デバイスの種類	Order
SIP	▪ RPID 表示名 ▪ PAI 表示名 ▪ 連絡先表示名 ▪ From/To 表示名 ▪ RPID ユーザー名 ▪ PAI ユーザー名 ▪ From/To ユーザー名 ▪ 連絡先ユーザー名 ▪ 連絡先主催者名
H.323	▪ H323-ID ▪ Q.931 表示名

CMR Cloud 会議のネットワークベースの記録

会議の主催者は、CMR Cloud 会議を記録できます。

- 記録した会議を再生すると、WebEx とテレプレゼンス両方のビデオが表示され、コンテンツの共有、チャット、およびポーリング（有効である場合）を使用できます。
- ユーザー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して、記録を操作できます。
- ユーザーは、記録の中で参加者がいつ通話しているのかを視覚的に確認できます。

注：ネットワークベースの記録は、WebEx クラウドサービスによって有効にされます。

Cisco Collaboration Meeting Rooms Hybrid サービスと Cloud Collaboration Meeting Room サービスの共用

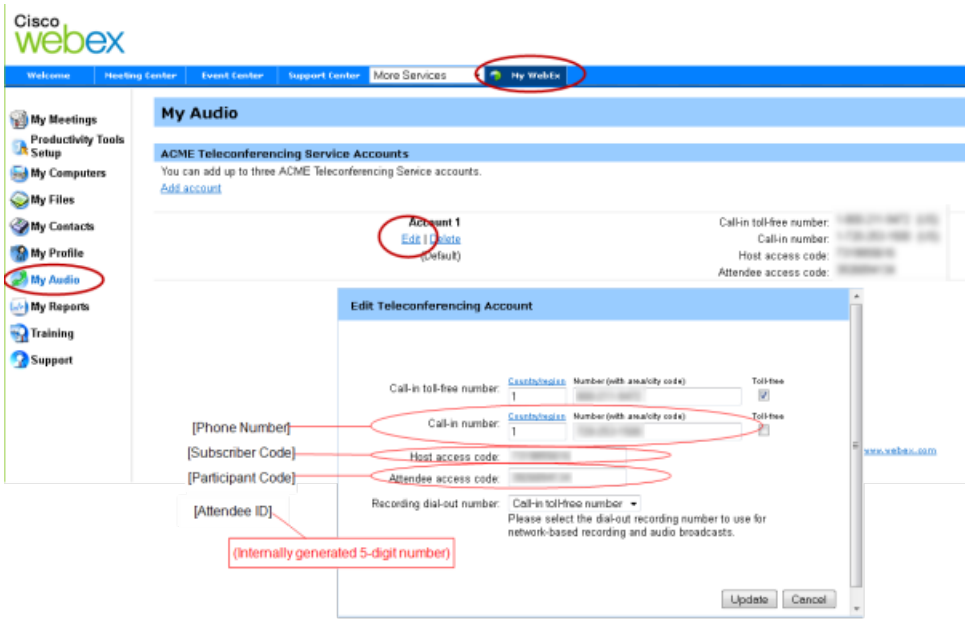
主催者が CMR Hybrid と Cloud Collaboration Meeting Room の両方のオプションを有効にしている場合、Windows 用の生産性ツールで、クラウドリソースを使用して会議を管理できます。

主催者がオンプレミスリソースを使用して会議を管理する必要がある場合は、代わりの手段として Cisco Smart Scheduler や Cisco WebEx Scheduling Mailbox などを使用する必要があります。

TSP 音声について

CMR Cloud を電話会議サービスプロバイダ（TSP）の統合音声と一緒に使用している場合、WebEx は TSP サーバーへの PSTN コールを確立し、DTMF エントリの「スクリプト」を使用して音声会議に参加します。ダイヤルする電話番号と、この DTMF スクリプトに必要なパラメーターは、WebEx の主催者のアカウントに含まれる TSP 音声アカウントから取得されます（図 4：WebEx 主催者アカウント/TSP 音声アカウント（21 ページ）を参照）。

図 4：WebEx 主催者のアカウント/TSP 音声アカウント



WebEx は各 TSP パートナーとともに、使用するダイヤルスクリプトを決定します（ダイヤルスクリプトを表示または変更できるのは WebEx のみです）。

TSP 音声に関する問題のトラブルシューティングを行うには、TSP 音声に関する問題のトラブルシューティング（22 ページ）を参照してください。

トラブルシューティング

Cisco WebEx サイト管理のオンラインヘルプ

Cisco WebEx サイト管理の使用に関する詳細を調べるには、以下のようにして Cisco WebEx サイト管理のヘルプに移動します。

1. WebEx サイトのサイト管理にログインします。

   ログインするには、WebEx サイトの URL の後にスラッシュ(/)と「admin」を続けます。

   例:*https://*customer-a.*webex.com/admin*
2. ページ左側の [Assistance] で、[Help] リンクをクリックします。

TSP 音声に関する問題のトラブルシューティング

表 5:TSP 音声に関する問題

問題またはメッセージ	考えられる原因	推奨処置
テレプレゼンス参加者に WebEx 参加者の音声が聞こえない	WebEx 主催者のアカウントが使用している TSP 音声アカウントが有効でない	音声アカウントが有効であることを確認するために、同じ主催者アカウントを使用して WebEx ミーティング(CMR Cloud 会議ではありません)を開始します。コールバック機能を使用して、テレフォニーが機能することを確認します。コールバックが失敗した場合は、主催者が会議をスケジュールするために使用したのと同じ WebEx サイトにログインし、主催者のアカウントに含まれるデフォルトの TSP 音声アカウントを編集して有効性を確認します([My WebEx] > [My Audio] > [Edit] の順にクリックします)。有効な TSP 音声アカウントを取得するために、TSP サービスプロバイダに連絡しなければならない場合があります。
	PSTN/DTMF ダイヤルスクリプトが TSP 音声会議サービスの IVR にアクセスできない	テクニカル サポートに問い合わせてください。会議に使用する WebEx 主催者のアカウントの TSP 音声アカウントの詳細を提供できるよう準備します。

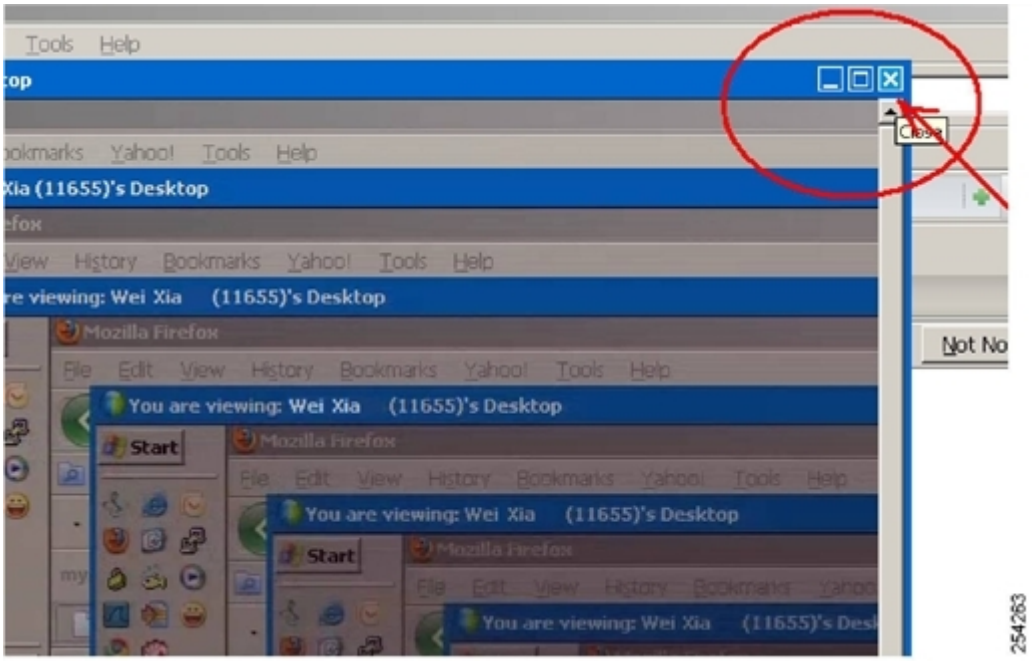
システム動作の管理

Cisco WebEx ビデオ表示ウィンドウの管理

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プレゼンテーションケーブル(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。

画面がカスケード表示されたら(図 5:カスケード表示された Cisco WebEx ビデオ表示ウィンドウ(23 ページ)を参照)、そのままビデオ表示ウィンドウを閉じてください。

図 5:カスケード表示された Cisco WebEx ビデオ表示ウィンドウ



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

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

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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