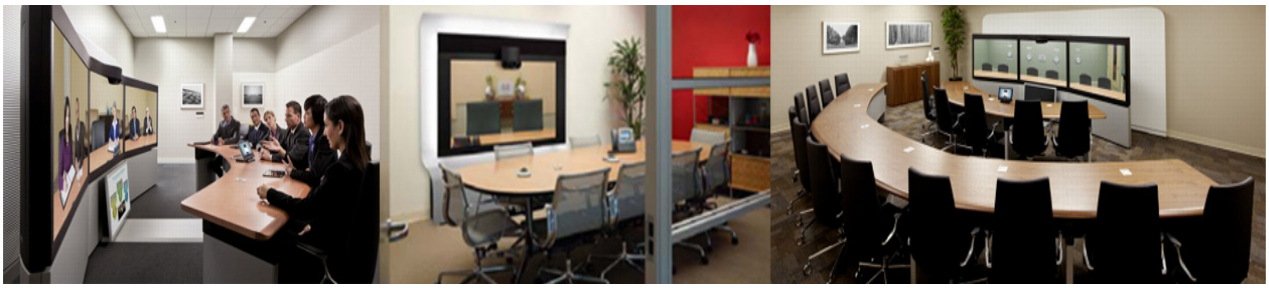


Cisco WebEx Enabled TelePresence 構成ガイド

2013 年 4 月 30 日

Cisco TelePresence Management Suite（TMS）14.3.1
Cisco WebEx Meeting Center WBS29

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/

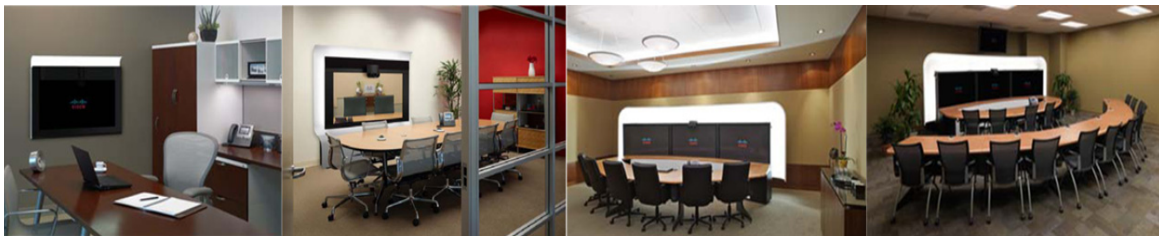
Text Part Number: OL-21352-02-J

【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、米国シスコシステムズ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。

Cisco WebEx Enabled TelePresence 構成ガイド



CONTENTS

はじめに 1

全般的な機能 1

対象読者と用途 1

Cisco WebEx の機能と重要事項 2

サポートされる機能 2

機能の制約事項 4

前提条件 4

ガイドの構成 5

関連資料 6

マニュアルの入手方法およびテクニカル サポート 7

Cisco WebEx Enabled TelePresence 機能について 1-1

目次 1-1

Cisco WebEx Enabled TelePresence エクスペリエンス 1-1

会議のスケジュール 1-1

会議の開始 / 会議への参加 1-2

Cisco TelePresence 会議エクスペリエンス 1-2

Cisco WebEx 会議エクスペリエンス 1-2

Cisco WebEx Enabled TelePresence の展開方法について 1-6

SIP ビデオ、プレゼンテーション、音声 1-6

SIP ビデオ、プレゼンテーション、PSTN 音声 1-7

Cisco TMS スケジュール権限 1-9

TelePresence Server および MCU の権限 1-9

プレゼンターが複数いる場合のプレゼンテーションの表示の詳細 1-9

会議参加者リスト 1-9

WebEx Enabled TelePresence で使用されるポートとプロトコル 1-10

Cisco WebEx Enabled TelePresence スケジュールの流れについて 1-10

Cisco WebEx and TelePresence Integration to Outlook を使用したスケジュール 1-11

Cisco Smart Scheduler を使用したスケジュール 1-13

Cisco WebEx Scheduling Mailbox を使用したスケジュール 1-15

Cisco WebEx Enabled TelePresence コール フローについて 1-16

SIP 音声コール フロー 1-17

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 1-19

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 1-21
WebEx 音声（PSTN）コール フロー 1-23

初回設定チェックリスト 2-1

目次 2-1
サーバおよびサイトのアクセス チェックリスト 2-1
設定作業チェックリスト 2-3
Cisco MCU 2-3
Cisco TelePresence Server 2-4
Cisco Video Communications Server 2-5
Cisco Unified Communications Manager 2-5
Cisco TelePresence Management Suite 2-6
Cisco TelePresence Management Suite Extension for Microsoft Exchange 2-7
Cisco TelePresence Management Suite Provisioning Extension 2-7
Cisco WebEx Enabled TelePresence の音声の設定 2-8
Cisco WebEx Site Administration 2-9

Cisco MCU および TelePresence Server の設定 3-1

目次 3-1
はじめに 3-1
MCU の必須設定 3-2
SIP 3-2
コンテンツ モード 3-2
ビデオ コーデックとオーディオ コーデック 3-2
自動コンテンツ ハンドオーバー 3-3
MCU の推奨設定 3-3
自動的にコンテンツ チャネルを重要として設定 3-4
発信トランスコード コーデック 3-4
適応型ゲイン制御 3-4
参加と退席の通知音 3-5
暗号化 3-5
TelePresence Server の必須設定 3-6
SIP 3-6
ローカル管理モード 3-6
自動コンテンツ ハンドオーバー 3-7
TelePresence Server の推奨設定 3-7
表示設定 3-7

コール制御の設定　4-1

はじめに　4-1

Cisco TelePresence Video Communication Server Control と Expressway の設定　4-1

前提条件　4-2

VCS Expressway での WebEx 向けの新しい DNS ゾーンの作成　4-3

暗号化が有効な MCU でのトラバーサル ゾーンの設定　4-4

Cisco Unified Communications Manager の設定　4-4

前提条件　4-4

Unified CM と VCS Control 間の SIP トランクの設定　4-5

Cisco VCS Expressway の証明書の設定　5-1

はじめに　5-1

VCS Expressway X8.1 の暗号化の問題と回避策　5-1

使用可能なビデオ　5-2

サポートされる証明書　5-2

証明書署名要求（CSR）の生成　5-3

VCS Expressway への SSL サーバ証明書のインストール　5-7

VCS Expressway での信頼された CA 証明書リストの設定　5-12

VCS Expressway X7.2.2 での信頼された CA 証明書リストの設定　5-13

X7.2.2 から X8.1 にアップグレードした VCS Expressway での信頼された CA 証明書リストの設定　5-19

VCS Expressway X8.1 での信頼された CA 証明書リストの設定　5-23

Cisco TelePresence Management Suite の設定　6-1

目次　6-1

前提条件　6-1

Cisco TMS での Cisco WebEx 機能の設定　6-2

Cisco TMS での WebEx ユーザの設定　6-4

WebEx 対応会議のスケジュールに関するユーザ要件　6-4

Active Directory からの自動ユーザ参照の設定　6-5

WebEx 予約の仕組み　6-6

Cisco TMS での Cisco WebEx Enabled TelePresence ユーザの設定　6-6

Cisco TMS での MCU および TelePresence Server のポート予約の設定　6-7

MCU のポート予約の有効化　6-7

TelePresence Server のポート予約の有効化　6-7

Cisco TMS での MCU のハイブリッド コンテンツ モードの設定　6-8

Cisco TMS でのロビー画面の TelePresence Server の設定　6-8

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　6-9

Cisco TMS での会議の設定 6-9
デフォルトのセットアップ バッファとティアダウン バッファ 6-9
デフォルト画像モード 6-10
会議接続 / 切断オプション 6-10
Cisco TMS でのシングル サインオンの設定 6-12
前提条件 6-12
Cisco TMS での SSO の設定 6-13
WebEx の証明書の生成 6-13
WebEx サイトでのパートナー委任認証の有効化 6-17
Cisco TMS での SSO の有効化 6-18
TMS が WebEx ホスト代理としてスケジュールできる設定 6-19

Cisco TelePresence Management Suite Extension for Microsoft Exchange の設定 7-1
目次 7-1
前提条件 7-1
展開のベスト プラクティス 7-2
TMSXE のスケジュール オプション 7-2
WebEx and TelePresence Integration to Outlook のための Cisco TMSXE の設定 7-2
Cisco TMS Booking Service のインストール 7-2
WebEx サイトと TMSXE 間の通信の設定 7-5
WebEx Scheduling Mailbox のための Cisco TMSXE の設定 7-7
Microsoft Exchange で WebEx Scheduling Mailbox を設定します。 7-7
Cisco TMSXE への WebEx メールボックスの追加 7-7
その他の推奨事項 7-8

Cisco TelePresence Management Suite Provisioning Extension の設定 8-1
目次 8-1
前提条件 8-1
はじめに 8-2
Cisco TMSPE へのユーザ アクセス 8-2
Smart Scheduler へのリダイレクトの作成 8-3
アクセス権と権限 8-3
タイム ゾーンの表示 8-3
Smart Scheduler のしくみ 8-3
制限事項 8-4

音声の設定 9-1
目次 9-1
前提条件 9-1

Cisco WebEx Enabled TelePresence の SIP 音声の設定 9-2
SIP 音声を使用するように Cisco TMS で WebEx サイトを設定する 9-2
WebEx サイトでのハイブリッド音声の有効化 9-3
Cisco WebEx Enabled TelePresence の PSTN 音声の設定 9-3
PSTN 音声を使用するように Cisco TMS で WebEx サイトを設定する 9-4
WebEx サイトでのハイブリッド モードの有効化 9-4
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 9-4
Cisco WebEx Enabled TelePresence の TSP 音声の設定 9-8
MACC ドメイン インデックスおよびオープン TSP 会議室の WebEx の設定 9-9
TSP ダイヤル文字列の設定 9-9
電話会議の開始方法の設定 9-10
会議主催者の TSP 音声の設定 9-12
TSP 音声の設定と会議の概要 9-13

Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合 10-1

目次 10-1
Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合 10-1
Meeting Center TelePresence セッション タイプの割り当て 10-3
ネットワーク ベースの WebEx Enabled TelePresence 会議の録画 10-6
WebEx and TelePresence Integration to Outlook のインストール 10-6
ユーザの WebEx アカウントのタイム ゾーンと言語の設定 10-8
ユーザの WebEx アカウントの TSP 音声の設定 10-9
次の作業 10-9

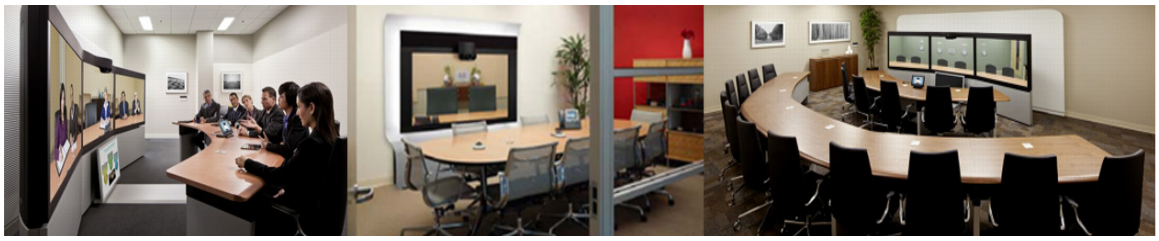
Cisco WebEx Enabled TelePresence 会議のスケジュール 11-1

目次 11-1
はじめに 11-2
Cisco TMS での WebEx Enabled TelePresence 会議のスケジュール 11-3
WebEx Enabled TelePresence 会議についての情報、ヒント、既知の問題 11-5
Cisco TMS 11-6
MCU および TelePresence Server 11-6
エンドポイント 11-7
TMSXE 11-7
WebEx 11-7

トラブルシューティング 12-1

目次 12-1
検証とテスト 12-1
Cisco WebEx サイト管理のオンラインヘルプ 12-1

トラブルシューティングのヒント 12-1
会議のスケジュールに関する問題 12-2
会議の開始または参加に関する問題 12-3
会議の進行中に発生する問題 12-4
TSP 音声会議に関する問題 12-7
TelePresence Server および MCU に関する問題 12-10
システム動作の管理 12-10
Cisco WebEx ビデオ表示ウィンドウの管理 12-10



はじめに

改訂日：2014 年 4 月

ここでは、『Cisco WebEx Enabled TelePresence 構成ガイド - TMS 14.3.1 - WebEx Meeting Center WBS29』の目的、対象読者、組織、および表記法について説明し、また、新機能と関連資料の取得方法について説明します。

ここでは、次の内容について説明します。

- 全般的な機能（1 ページ）
- 対象読者と用途（1 ページ）
- Cisco WebEx の機能と重要事項（2 ページ）
- 前提条件（4 ページ）
- ガイドの構成（5 ページ）
- 関連資料（6 ページ）
- マニュアルの入手方法およびテクニカル サポート（7 ページ）

全般的な機能

このマニュアルでは、Cisco WebEx と Cisco TelePresence の相互運用性を実現する Cisco TelePresence アプリケーションの設定方法について説明します。『Cisco WebEx Enabled TelePresence 構成ガイド - TMS 14.3.1 - WebEx Meeting Center WBS29』では、Cisco TelePresence System（CTS）、Cisco TelePresence Server または MCU マルチポイント会議、Cisco TMS、Cisco Unified Communications Manager（Cisco Unified CM）、Cisco Video Communication Server（VCS）、および Cisco WebEx Meeting Center. 間でスケジュールされた会議の相互運用性を管理および監視する方法について説明します。

対象読者と用途

『*Cisco WebEx Enabled TelePresence 構成ガイド - TMS 14.3.1 - WebEx Meeting Center WBS29*』は、TelePresence Server、MCU、Cisco TMS、Cisco VCS、または Cisco Unified CM を設定して Cisco TelePresence 会議で Cisco WebEx 機能を使用する管理者を対象としています。

Cisco WebEx の機能と重要事項

ここでは、次の機能情報について説明します。

- サポートされる機能（2 ページ）
- 機能の制約事項（4 ページ）

サポートされる機能

Cisco WebEx Enabled TelePresence は次の主要な機能を提供します。

- WebEx クライアントと TelePresence エンドポイントの間の最大 720p 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 Management Suite（Cisco TMS）を使用した統合会議スケジュール（これにより、ユーザは Cisco WebEx Enabled TelePresence 会議を容易にスケジュールできます）
- 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
- サードパーティの TelePresence エンドポイントとの相互運用性

表 1 に、Cisco WebEx Enabled TelePresence の機能を示します。

表 1　　Cisco WebEx Enabled TelePresence の機能

サポートされる機能	説明
音声	CTS 参加者は、G.711 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。 **コメント**　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	すべての Cisco TelePresence の参加者と会議の主催者はデフォルトのホストになることができます。MCU/TelePresence Server 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/TelePresence Server 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会議に参加すると、その主催者がホストになります。

表 1　　Cisco WebEx Enabled TelePresence の機能

サポートされる機能	説明
スケジューリング	Cisco TMS、WebEx and TelePresence Integration to Outlook、Smart Scheduler、または WebEx Scheduling Mailbox を使用して、WebEx での Cisco TelePresence 会議をスケジュールします。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 WebEx Enabled TelePresence 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。 **コメント**　Cisco WebEx Enabled TelePresence の相互運用性は、スケジュール済み会議でのみサポートされています。スケジュールされていない TelePresence 参加者は、Cisco WebEx Enabled TelePresence 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イン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できます。 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。
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、TelePresence Server/MCU はプレゼンテーションをトランスコードし、解像度 1024x768 で WebEx クラウドに送信します。 **コメント**　ビデオ ディスプレイ ケーブルを共有している Cisco TelePresence ユーザはビデオ ディスプレイ ケーブルを接続する前に、ラップトップの Cisco WebEx Meeting Center クライアントを終了する必要があります。終了しない場合は、ウィンドウのカスケード効果が発生する可能性があります。詳細については、第 12 章「Cisco WebEx ビデオ表示ウィンドウの管理」を参照してください。
双方向ビデオ	ビデオ品質は、Cisco TelePresence エンドポイントから Cisco WebEx と、Cisco WebEx から Cisco TelePresence エンドポイントの送信ベスト エフォートです。 会議の CTS 参加者のビデオは、Cisco WebEx ネットワークに転送され、そこで他の Cisco WebEx 参加者とともに Cisco WebEx 参加者に表示されます。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 クライアントのプレゼンテーションは、CTS の機能に応じて、ローカルの CTS プロジェクタ、プレゼンテーション ディスプレイ、または Presentation-In-Picture（PiP）に表示されます。 **コメント**　すべての Cisco WebEx Enabled TelePresence 会議では、Cisco TelePresence Server または MCU を使用する必要があります。

機能の制約事項

Cisco WebEx Enabled TelePresence のすべての制約事項と既知の問題のリストについては、Cisco WebEx Enabled TelePresence のリリース ノートを参照してください。

前提条件

表 2 に、Cisco WebEx Enabled TelePresence 機能の前提条件を示します。

表 2　　Cisco WebEx と Cisco TelePresence System の前提条件

要件	説明
Cisco TelePresence Management Suite（Cisco TMS）	Cisco TMS は、Cisco WebEx Enabled TelePresence 会議をスケジュールするために必要です。 リリース 14.3.1 以降が必要です（リリース 14.3 以降は、Cisco TelePresence Server による TSP 音声のサポートにも必要です）。
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 Cisco WebEx Enabled TelePresence 会議をスケジュールするために必要です。 リリース 3.1 以降が必要です。
Cisco TelePresence Management Suite Provisioning Extension（Cisco TMSPE）	Cisco TMSPE は、Smart Scheduler を使用して Cisco WebEx Enabled TelePresence 会議をスケジュールするために必要です。 リリース 1.1 以降が必要です。 **コメント**　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。
Cisco TelePresence Video Communication Server（VCS）	コール制御ソリューションとして VCS Control および Expressway が必要です。 リリース X7.2.2 以降が必要です。 ⚠ **注意**　VCS Expressway X7.2.2 のスタティック NAT を使用しているお客様は、X8.1 にアップグレードしないことを強く推奨します。VCS Expressway X8.1 が SDP のメディア パーツにイーサネット 2 IP アドレスを使用するため、コールのメディア パーツが失敗します。すでに X8.1 でスタティック NAT を使用している場合は、第 5 章「VCS Expressway X8.1 の暗号化の問題と回避策」の推奨回避策を参照してください。
Cisco Unified Communications Manager（Unified CM）	Unified CM は、Unified CM に登録されているエンドポイントと合わせて展開する場合に VCS とともに使用可能な、オプションのコール制御ソリューションです。 リリース 8.6.2 以降が必要です9.1.1 が推奨されています。
Cisco TelePresence Server	TelePresence Server は、Cisco WebEx Enabled TelePresence 会議の会議ブリッジとして使用できます。 リリース 3.0 以降が必要です。サードパーティの相互運用キーを持つリリース 3.1 以降は、TSP 音声のサポートに必要です。

表 2　　Cisco WebEx と Cisco TelePresence System の前提条件

要件	説明
Cisco TelePresence MCU	Cisco TelePresence MCU は、Cisco WebEx Enabled TelePresence 会議の会議ブリッジとして使用できます。 リリース 4.4 以降が必要です。
プロビジョニング：Cisco TelePresence と Cisco WebEx	1. Cisco WebEx Meeting Center サイトは、最新サービス パックが適用された T28.10 以降のリリースで稼働している必要があります。 2. Cisco WebEx 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、第 10 章「Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合」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 や MCU でサポートされるエンドポイントは、Cisco WebEx Enabled TelePresence 会議に参加できます。
アカウントの検証：会議のスケジュール担当者の Cisco WebEx アカウント。	Cisco TMS での Cisco WebEx Enabled TelePresence 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。 1. 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。 2. Cisco TMS は、認証済み Cisco WebEx アカウント所有者を検証します。 **コメント**　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、第 6 章「Cisco TelePresence Management Suite の設定」を参照してください。
帯域幅と 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。	MCU/TelePresence Server と WebEx の間のネットワーク帯域幅は上り 1.1 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 1.1 Mbps のインスタンスが 5 つ必要です。 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。
Cisco WebEx クライアントのリソース要件：会議ごとに必要なリソースの割り当て	詳細な要件については、『Cisco WebEx Enabled TelePresence release notes』を参照してください。

ガイドの構成

Cisco WebEx Enabled TelePresence の設定と使用法に関する情報は、次の章に記載されています。

- 第 1 章「Cisco WebEx Enabled TelePresence 機能について」
- 第 2 章「初回設定チェックリスト」
- 第 3 章「Cisco MCU および TelePresence Server の設定」
- 第 4 章「コール制御の設定」
- 第 5 章「Cisco VCS Expressway の証明書の設定」
- 第 6 章「Cisco TelePresence Management Suite の設定」
- 第 7 章「Cisco TelePresence Management Suite Extension for Microsoft Exchange の設定」
- 第 8 章「Cisco TelePresence Management Suite Provisioning Extension の設定」
- 第 9 章「音声の設定」

- 第 10 章「Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合」
- 第 11 章「Cisco WebEx Enabled TelePresence 会議のスケジュール」
- 第 12 章「トラブルシューティング」

関連資料

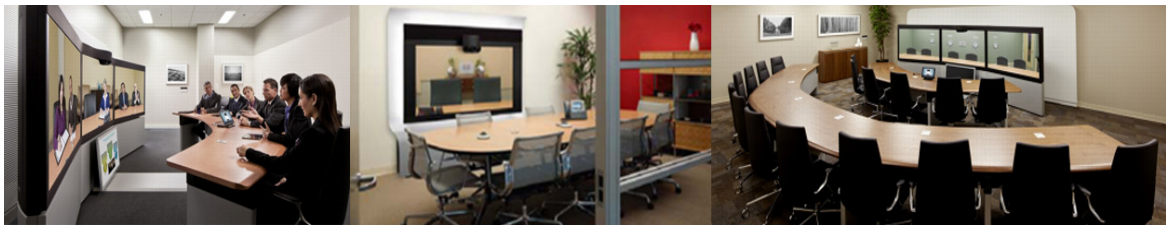
関連項目	ドキュメント リンク
Cisco TelePresence のマニュアル	
Cisco TelePresence Management Suite	• *Cisco TelePresence Management Suite*
Cisco TelePresence Video Communication Server（VCS）	• *Cisco TelePresence Video Communication Server*
Cisco Unified Communications Manager（Unified CM）	• *Cisco Unified Communications Manager*
Cisco TelePresence Server	• *Cisco TelePresence Server*
Cisco TelePresence MCU	• MCU 5300 Series • MCU 4501 Series • MCU 4500 Series • MCU 4200 Series • MCU MSE Series
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 の統合 を参照してください。
Cisco WebEx Enabled TelePresence のマニュアル	
会議主催者を対象とした WebEx Enabled TelePresence 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

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



CHAPTER 1

Cisco WebEx Enabled TelePresence 機能について

改訂日：2014 年 8 月

目次

この章では、Cisco WebEx Enabled TelePresence ソリューションの概要を示します。次のような構成になっています。

- Cisco WebEx Enabled TelePresence エクスペリエンス（1-1 ページ）
- Cisco WebEx Enabled TelePresence の展開方法について（1-6 ページ）
- Cisco WebEx Enabled TelePresence スケジュールの流れについて（1-10 ページ）
- Cisco WebEx Enabled TelePresence コール フローについて（1-16 ページ）

Cisco WebEx Enabled TelePresence エクスペリエンス

ここでは、Cisco WebEx Enabled TelePresence 会議エクスペリエンスに関する次の情報を説明します。

- 会議のスケジュール（1-1 ページ）
- 会議の開始/会議への参加（1-2 ページ）
- Cisco TelePresence 会議エクスペリエンス（1-2 ページ）
- Cisco WebEx 会議エクスペリエンス（1-2 ページ）

会議のスケジュール

会議主催者は、Cisco WebEx and TelePresence Integration to Outlook、Cisco Smart Scheduler、Cisco TelePresence Management Suite（Cisco TMS）、または Cisco WebEx Scheduling Mailbox を使用して会議をスケジュールできます。

さまざまなスケジュール オプションを使用した会議のスケジューリング方法の詳細については、第 11 章「Cisco WebEx Enabled TelePresence 会議のスケジュール」を参照してください。

会議の開始/会議への参加

会議は、以下の方法で開始されます。

- 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。
- 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 TelePresence 会議エクスペリエンス

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、TelePresence 参加者には WebEx 参加者と TelePresence 参加者の両方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 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を共有する場合、TelePresence ユーザはビデオ 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、TelePresence 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。Cisco TelePresence システムで現在発言中の参加者のビデオが、Cisco WebEx Web クライアントにストリーミング配信されます。

Cisco WebEx 会議エクスペリエンス

リモート参加者は Cisco WebEx Meeting Center の Web やモバイル クライアント* にログインすることで、Cisco WebEx ミーティングに参加します。Cisco TelePresence エンドポイントと共有するコンテンツが Cisco WebEx Meeting Center クライアントに自動的に表示され、Cisco 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 エンドポイントと共有できます。Cisco WebEx ユーザに対し、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 参加者は全画面ビューにして、WebEx と TelePresence の他のすべての会議参加者を見ることができます。全画面モードのとき、WebEx 参加者は、ビデオをオンにしているすべての WebEx 参加者を確認できます。全画面モード中、参加者は、TelePresence 参加者が発言者のときに TelePresence から送信されたビデオを視聴できます。Cisco WebEx ユーザには、すべての Cisco 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 参加者は標準的な WebEx Meeting Center クライアント注釈ツールを使って注釈を付けることができ、WebEx 参加者と TelePresence 参加者はどちらも注釈を見ることができます。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 システム（TelePresence systems）」が WebEx 参加者リスト（図 1-1（1-4 ページ））と全画面ビューの WebEx 参加者の行（図 1-2（1-5 ページ））に表示されます。これは、Cisco WebEx Enabled TelePresence 会議であることを示します。個々の TelePresence ユーザは、WebEx 参加者リストには表示されません。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。

Cisco WebEx 参加者がプレゼンテーションを TelePresence 参加者と共有するには、以下の操作を行う必要があります。

1. Cisco WebEx Web クライアントにラップトップからログインします。
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。
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。

* サポートされているモバイル クライアントのリストについては、Cisco WebEx Enabled TelePresence リリースノートを参照してください。

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

ボールの受け渡し

WebEx ユーザは、ボールを受け取り、プレゼンテーションする内容を選択することで、プレゼンテーションを共有します。WebEx サイトで参加者がボールを受け取ることができないように設定されている場合、WebEx ホストが WebEx 参加者にボールを渡す必要があります。あるいは、参加者がホスト キーを使用して新しいホストになることができます。新しいホストは、プレゼンテーションを行うためにプレゼンター ボールを自分自身に割り当てることができます。
Cisco WebEx 会議機能の使用の詳細については、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）] をクリックしてください。

WebEx での会議の表示

WebEx Meeting Center Web クライアント（Windows または Mac）を使用して会議に参加する際に、会議を体験する方法として 2 つの基本的な方法があります。

- デフォルト ビュー（1-4 ページ）
- 全画面ビュー（1-4 ページ）

デフォルト ビュー

会議にログインすると、WebEx クライアントにデフォルト ビューが表示されます（図 1-1 を参照）。デフォルト ビューでは、ビデオ ウィンドウと参加者リストが右側に表示され、共有するプレゼンテーションが左側に表示されます。ビデオ ウィンドウには、現在発言中の参加者（TelePresence または WebEx）が表示されます。

図 1-1　Cisco WebEx 会議：デフォルト ビュー

全画面ビュー

全画面ビューでは、ウィンドウ上部に発言中の参加者の大きな画像が表示され、ウィンドウ下部に WebEx 参加者が表示されます（図 1-2 を参照）。全画面モードではプレゼンテーションは表示されません。

全画面モードに切り替えるには、デフォルト ビューのビデオ ウィンドウで [全画面（Full Screen）] ボタンをクリックします。

発言中の参加者のウィンドウにその他の TelePresence 参加者が表示されるように、Cisco TelePresence Server または MCU を設定できます。TelePresence Server でデフォルトで有効なアクティブ プレゼンスの例については、図 1-3 を参照してください。MCU は全画面レイアウトを送信します。

図 1-2　　Cisco WebEx 会議：全画面ビュー

図 1-3　　Cisco WebEx 会議：アクティブ プレゼンス モードの Cisco TelePresence Server 全画面表示

Cisco WebEx Enabled TelePresence の展開方法について

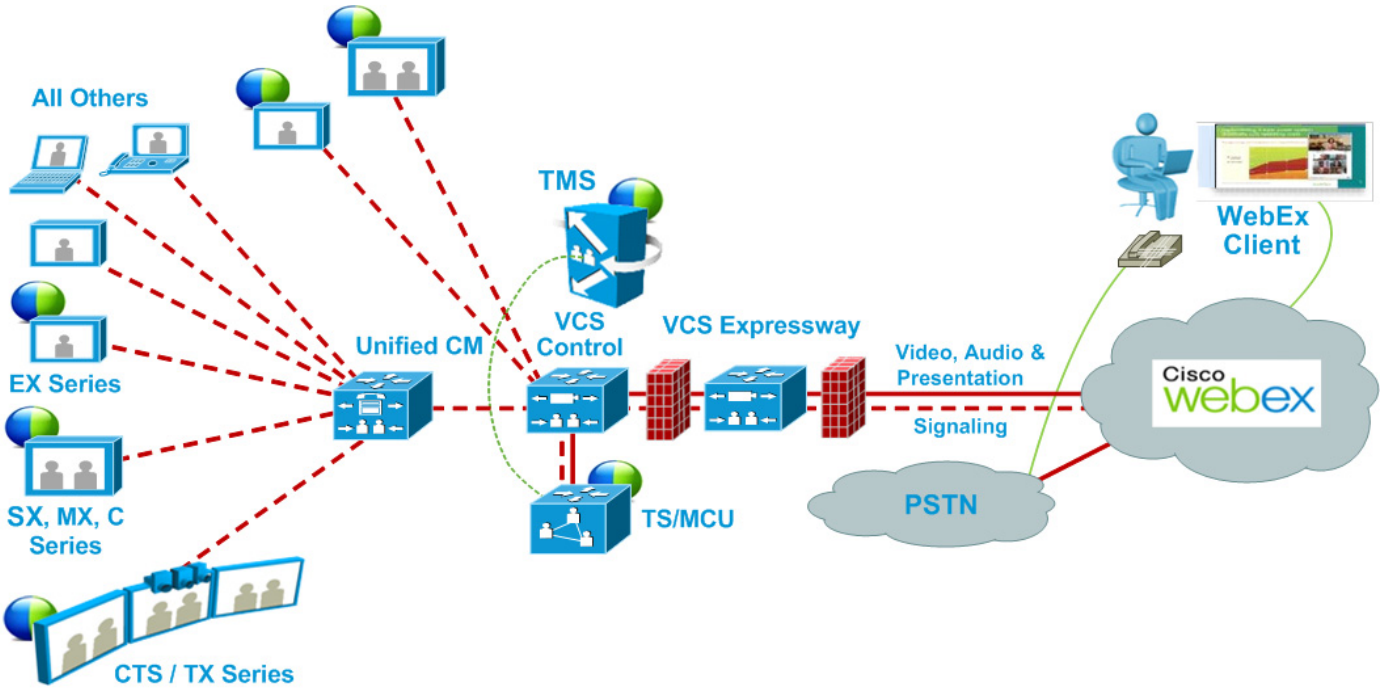
Cisco WebEx Enabled TelePresence には、3 つのネットワーク トポロジが考えられます。

- SIP ビデオ、プレゼンテーション、音声（1-6 ページ）
- SIP ビデオ、プレゼンテーション、PSTN 音声（1-7 ページ）：
  - Unified CM 登録ゲートウェイを使用する
  - Cisco VCS Control 登録ゲートウェイを使用する

SIP ビデオ、プレゼンテーション、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 1-4　　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



SIP ビデオ、プレゼンテーション、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 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 CM に登録された PSTN ゲートウェイを使用する：図 1-5 を参照してください。
- VCS に登録された PSTN ゲートウェイを使用する：図 1-6 を参照してください。

コメント　この展開タイプは、Cisco TelePresence Server ではサポートされません。

図 1-5　　ネットワーク トポロジ:Unified CM 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

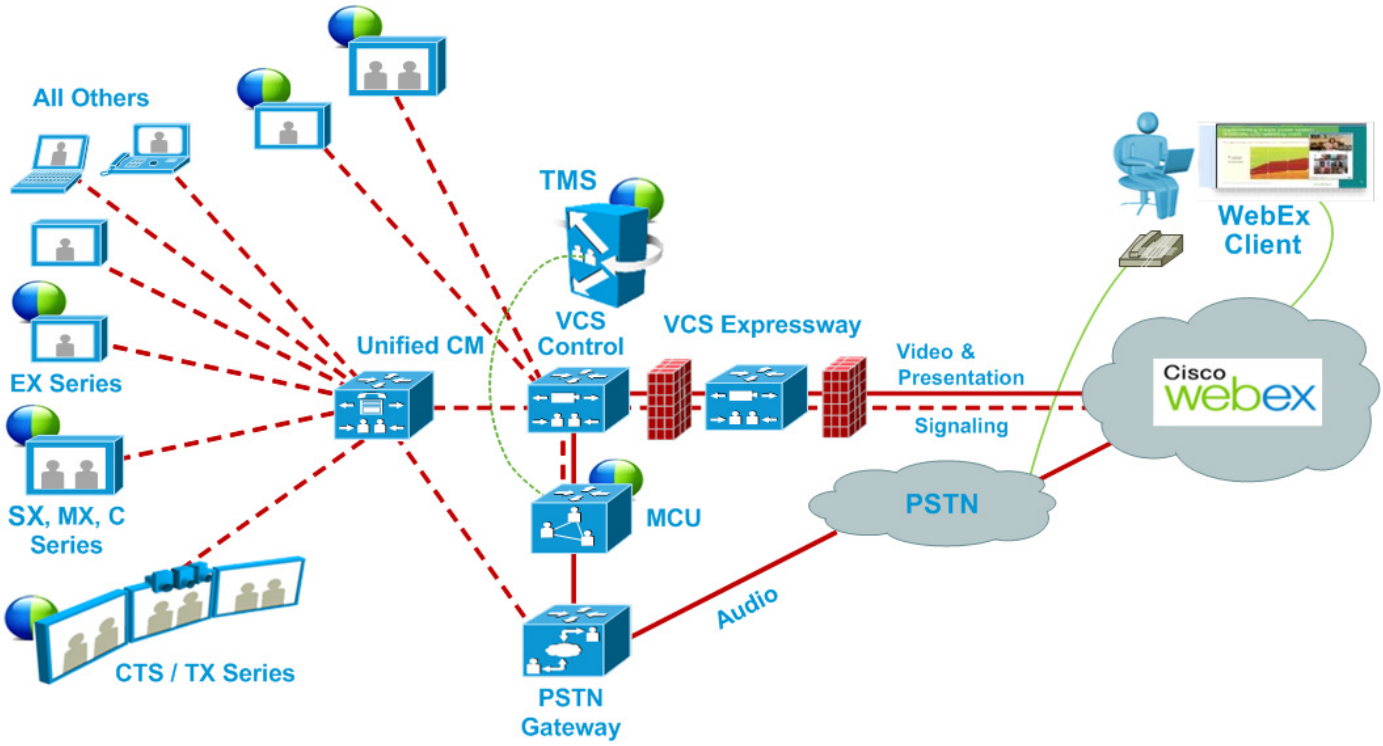
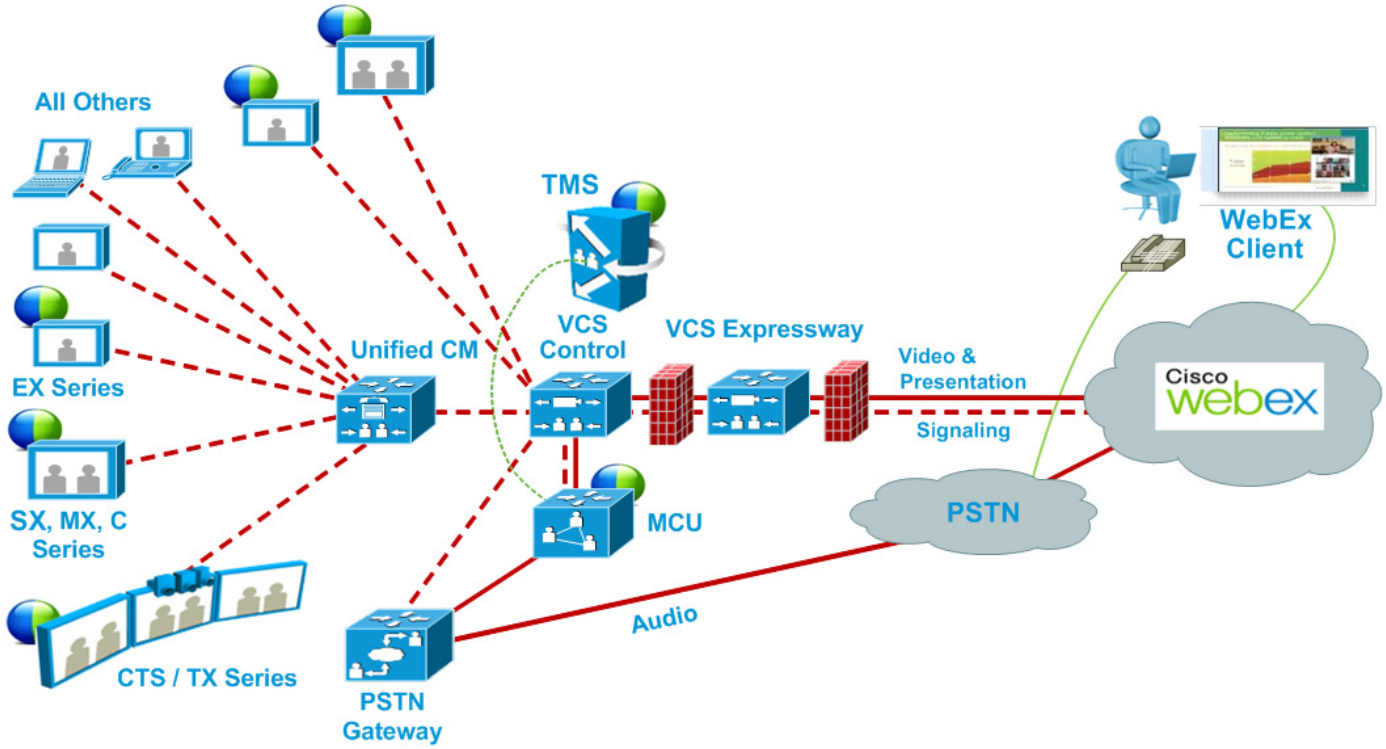


図 1-6　　ネットワーク トポロジ:VCS Control を使用した PSTN 音声の SIP ビデオおよびプレゼンテーション



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では、Cisco TMS が WebEx 対応会議を WebEx ホストの代わりに予約でき、会議参加者に配信される Cisco WebEx 会議情報を取得できます。Cisco TMS は、その後で、TelePresence Server/MCU に Cisco WebEx 会議の詳細をプッシュします。

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/TelePresence Server 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/TelePresence Server 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/TelePresence Server 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（1024x768）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。

プレゼンターが複数いる場合のプレゼンテーションの表示の詳細

プレゼンテーションを行う TelePresence ユーザのために、プレゼンターはビデオ ディスプレイ ケーブルをエンドポイントに接続し、（必要に応じて）エンドポイントのプレゼンテーション ボタンを押します。複数の TelePresence ユーザが同時にプレゼンテーションを行う場合、最後にプレゼンテーションを開始したエンドポイントが表示されます。ケーブルが抜かれたら、次のプレゼンターがプレゼンテーションを再び開始する必要があります。

プレゼンテーションを行う WebEx ユーザは、ボールを受け取りプレゼンテーションするコンテンツを選択します。WebEx ユーザがボールを受け取ることができない場合、ホストがボールをユーザに受け渡す必要があります。あるいは、ユーザがホスト キーを使用して新しいホストになることができます。

コメント　ホストがボールを受け渡すことや、ホスト キーを使用することなく、すべての WebEx 参加者がボールを受け取ることができるように、WebEx サイトをプロビジョニングできます。

会議参加者リスト

TelePresence 参加者リスト、つまり TelePresence Server（使用する場合）に現在接続されているエンドポイント名のリストが、TelePresence エンドポイント ディスプレイ デバイスに表示されます。MCU および特定のエンドポイント モデルではこの機能はサポートされていません。

ただし TelePresence 参加者リストは、WebEx ユーザに表示される参加者リストには表示されません。WebEx ユーザに対しては、他の WebEx 参加者と、会議のすべての TelePresence 参加者を表す 1 つの「TelePresence システム（TelePresence systems）」という参加者だけが表示されます。

WebEx Enabled TelePresence で使用されるポートとプロトコル

WebEx Enabled TelePresence 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。

表 1-1　WebEx Enabled TelePresence で使用されるポートとプロトコル

コンポーネント間の通信	使用するポートとプロトコル
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 TMSXE	TLS.443 を使用するエフェメラル ポート
VCS Expressway から WebEx クラウド	メディア用の TLS および UDP ポート 9000 および 9001

Cisco WebEx Enabled TelePresence スケジュールの流れについて

ここでは、次の機能を使用して Cisco WebEx Enabled TelePresence 会議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（1-11 ページ）
- Cisco Smart Scheduler を使用したスケジュール（1-13 ページ）
- Cisco WebEx Scheduling Mailbox を使用したスケジュール（1-15 ページ）

コメント　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、Microsoft Exchange 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。

Cisco WebEx and TelePresence Integration to Outlook を使用したスケジュール

図 1-7　Cisco WebEx and TelePresence Integration to Outlook でのスケジュールの流れ

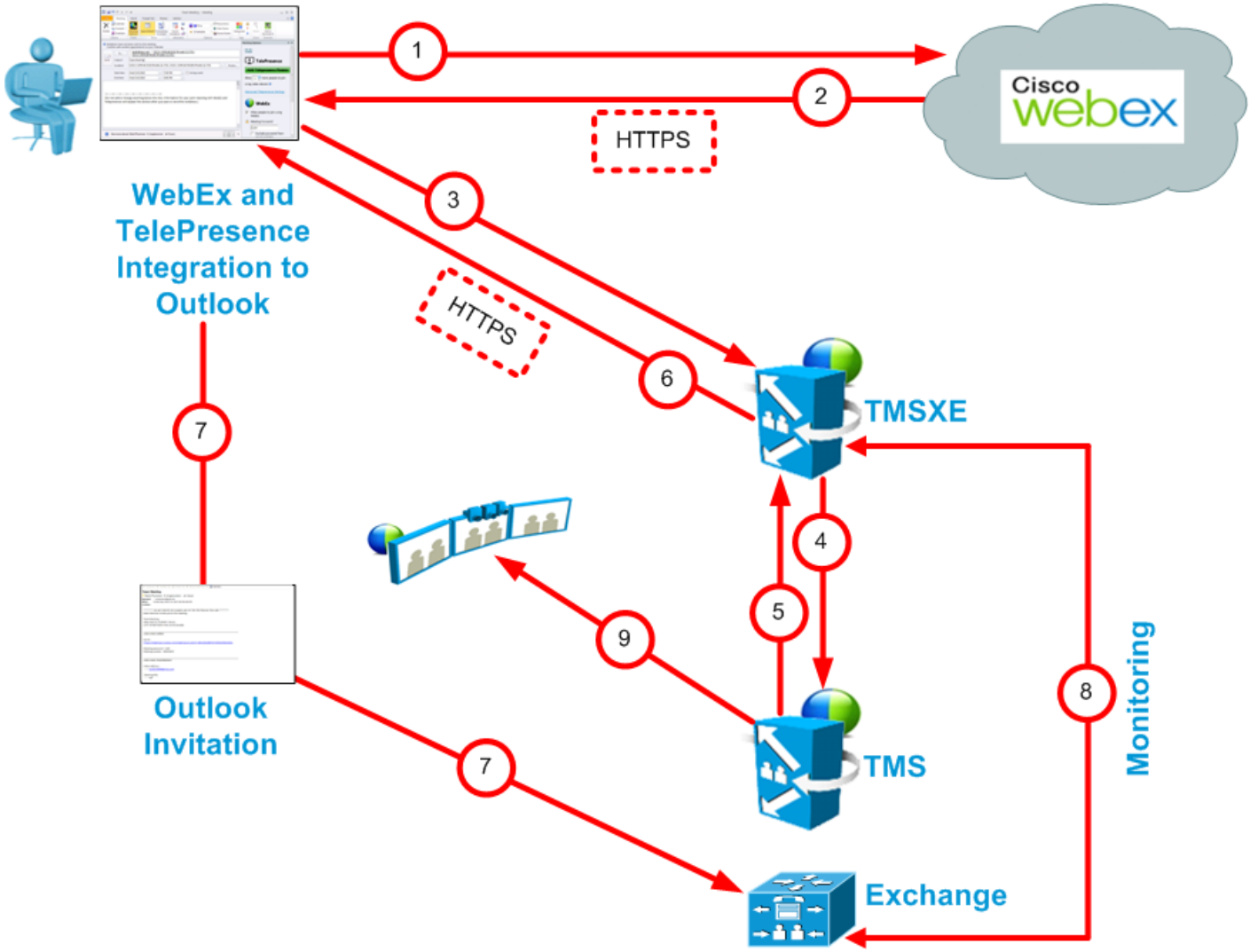


表 1-2　Cisco WebEx and TelePresence Integration to Outlook でのスケジュール手順

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

図 1-8　　Cisco WebEx Smart Scheduler でのスケジュールの流れ

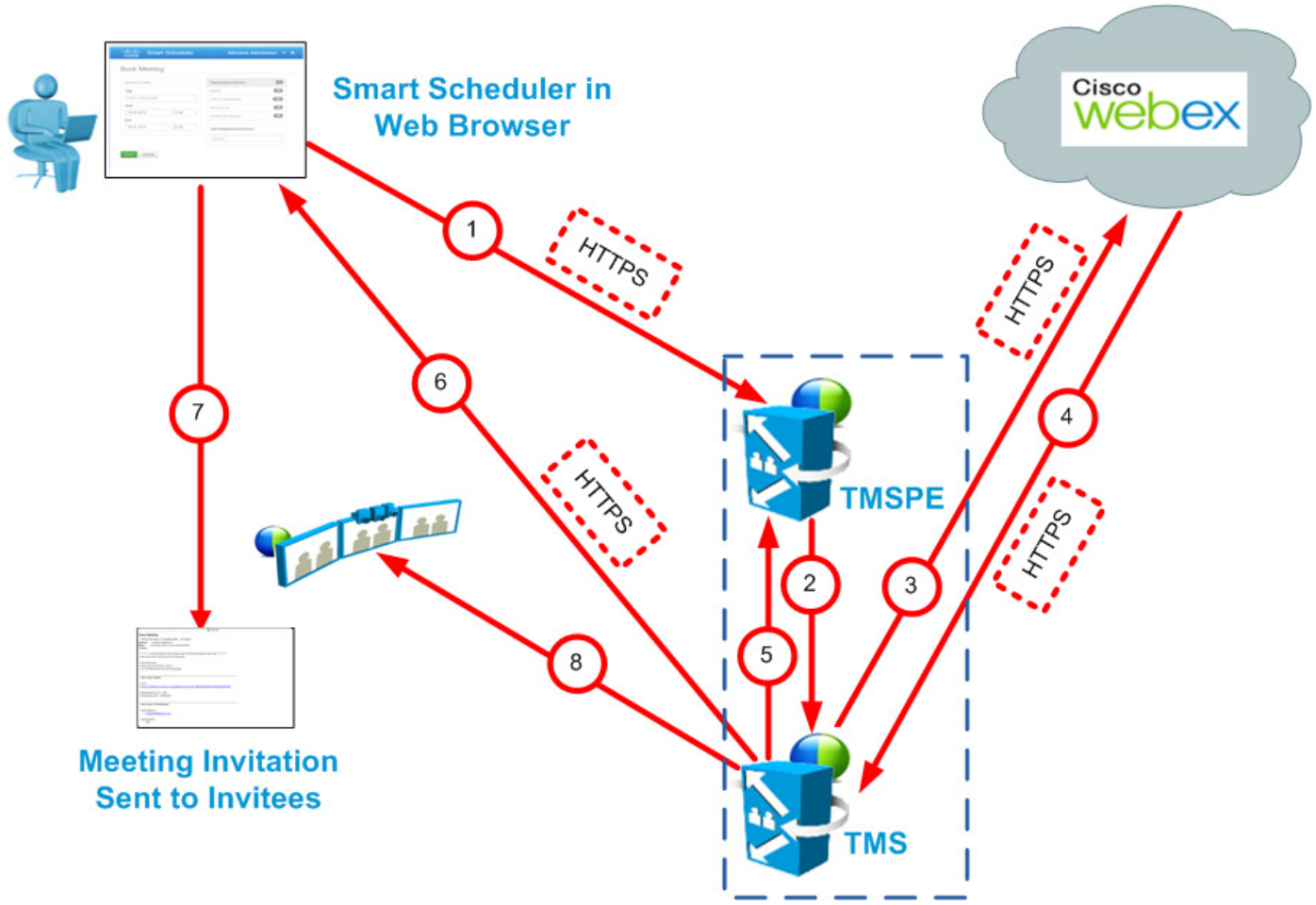


表 1-3　　Cisco Smart Scheduler でのスケジュール手順

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

図 1-9　　Cisco WebEx Scheduling Mailbox を使用したスケジュールの流れ

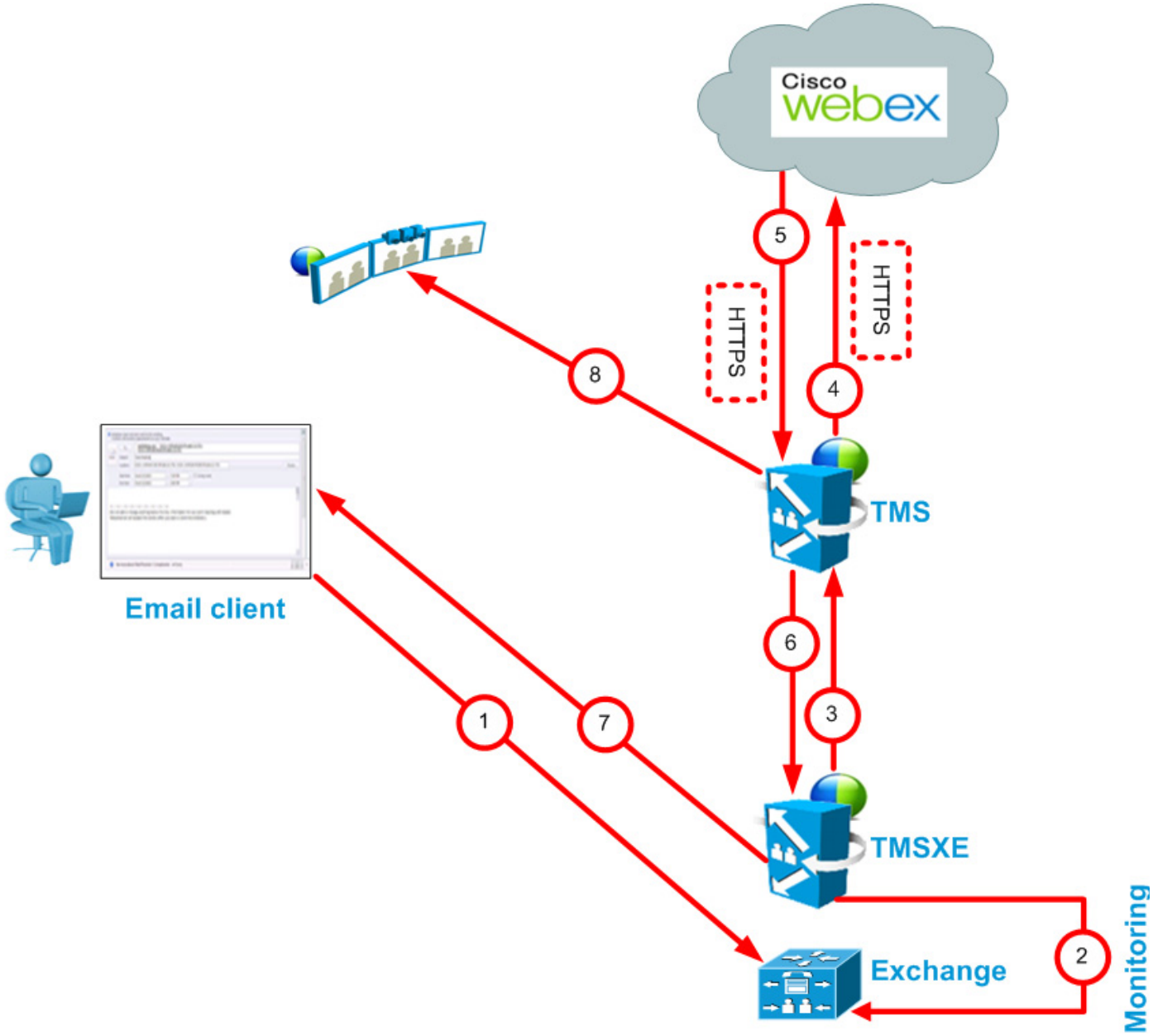


表 1-4　　Cisco WebEx Scheduling Mailbox を使用したスケジュール手順

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 Enabled 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。

Cisco WebEx Enabled TelePresence コール フローについて

ここでは、次の Cisco WebEx Enabled TelePresence 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（1-17 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（1-19 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（1-21 ページ）
- WebEx 音声（PSTN）コール フロー（1-23 ページ）

SIP 音声コール フロー

図 1-10　SIP 音声コール フロー

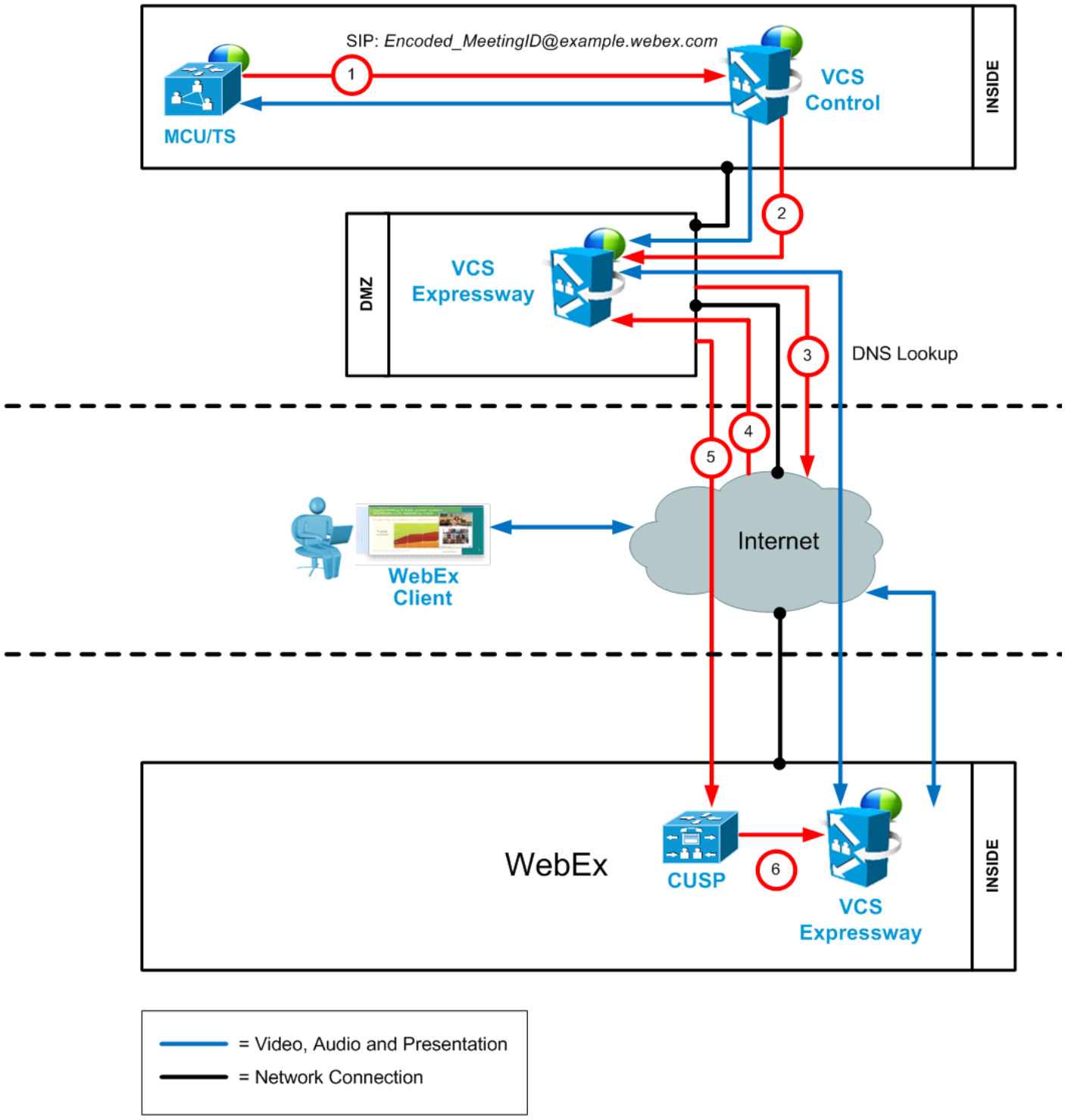


表 1-5　SIP 音声コール フローのステップ

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 VCS Control を介してルーティングされます。
2	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	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	VCS Expressway が 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）。 - 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 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 VCS Expressway 間で暗号化されます。 - MCU と顧客サイト内の 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

図 1-11　　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

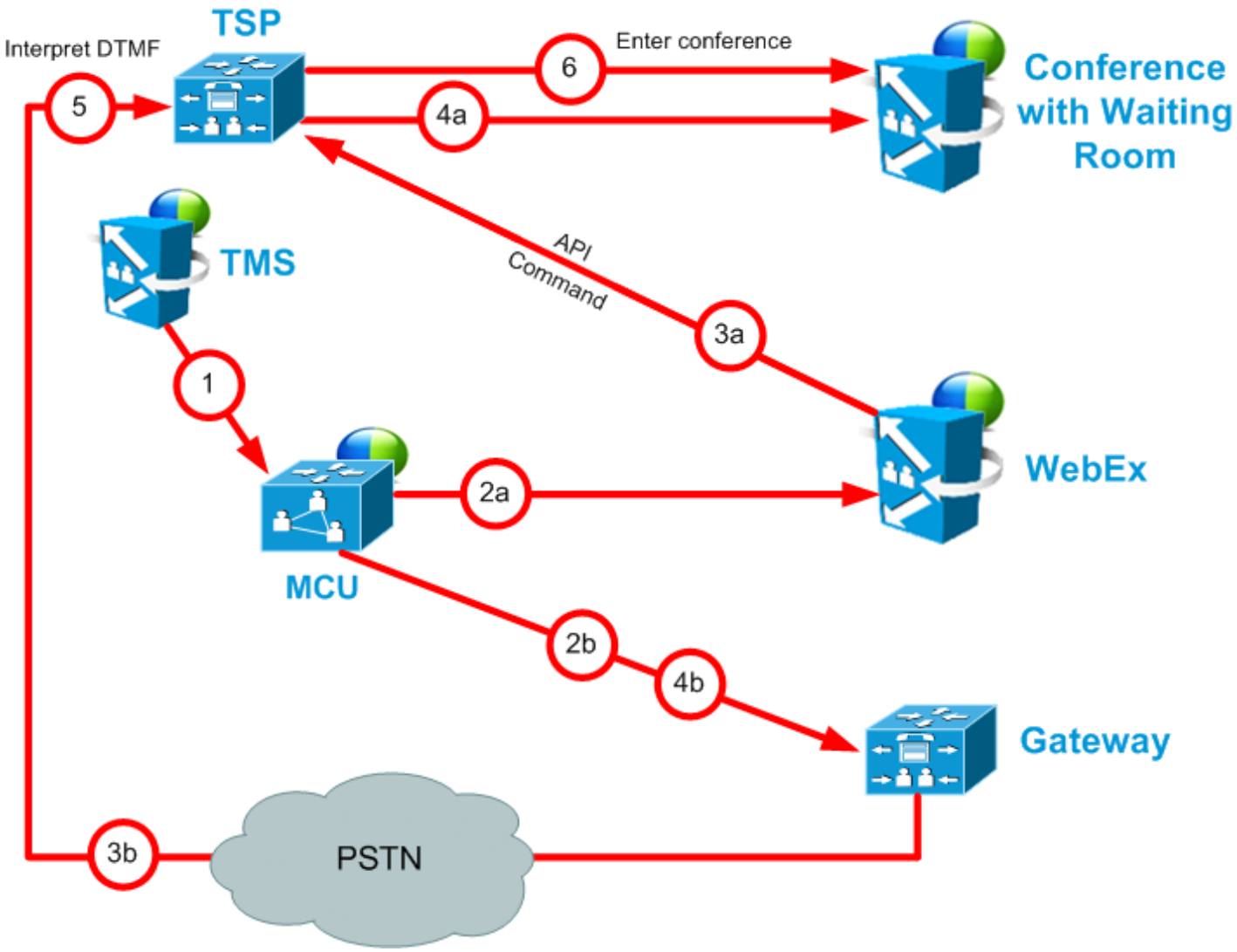


表 1-6　　待合室をアンロックする API コマンドを使用した TSP 音声コール フローのステップ

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、図 1-10 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

図 1-12　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

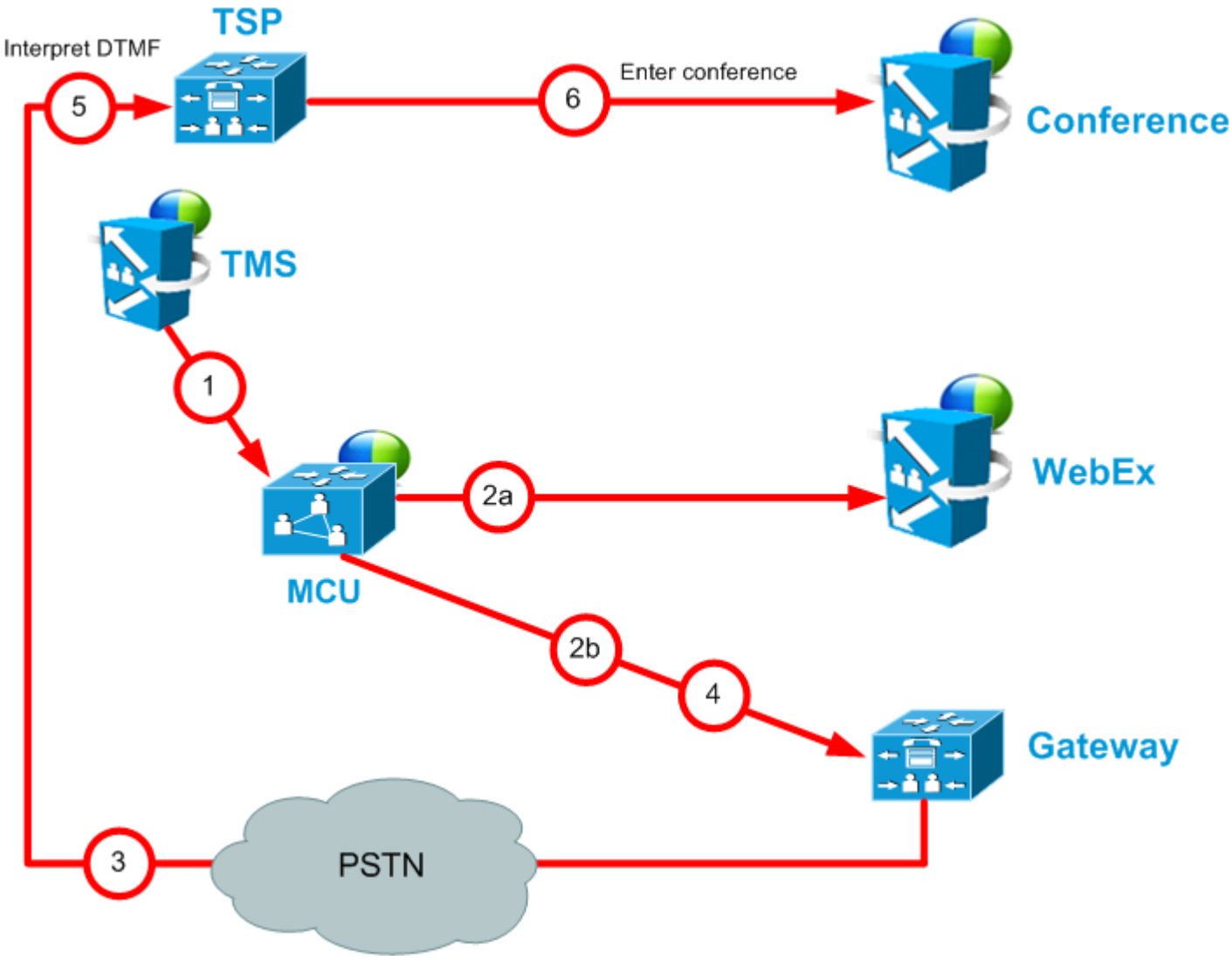


表 1-7　待合室および MCU/TelePresence Server をホストとして使用する TSP 音声コール フローのステップ

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、図 1-10 を参照してください）。

ステップ番号	説明
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。
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

図 1-13　　WebEx 音声（PSTN）コール フロー

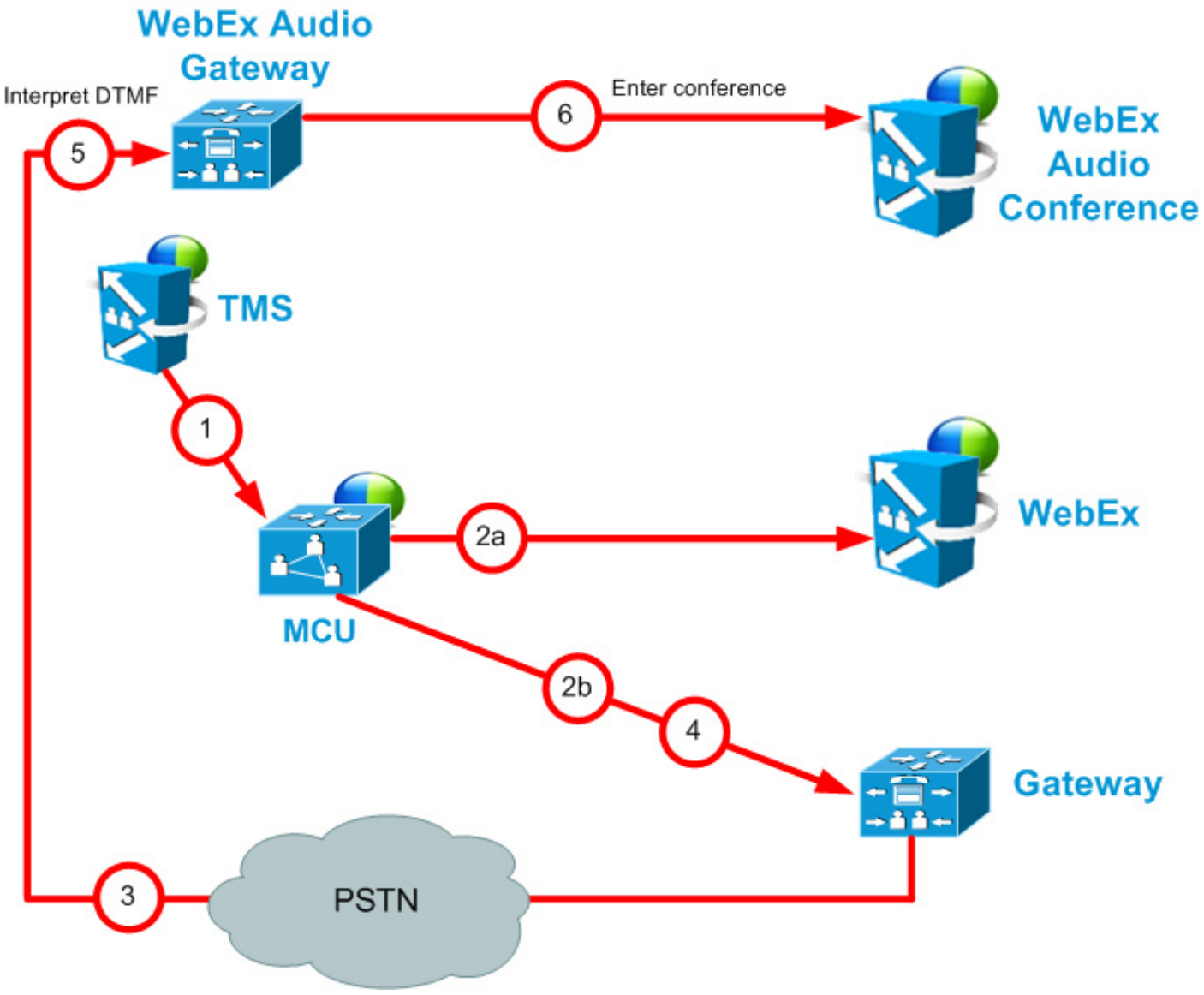
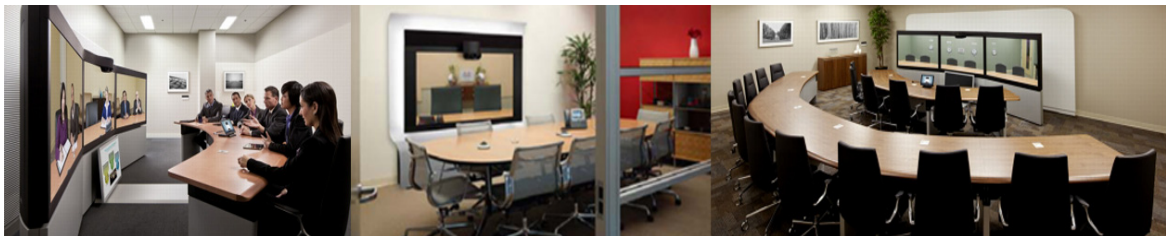


表 1-8　　WebEx 音声コール フローのステップ

ステップ番号	説明
1	TMS が MCU 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、図 1-10 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。

ステップ番号	説明
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。



CHAPTER 2

初回設定チェックリスト

改訂日：2013 年 12 月

目次

この章では、Cisco WebEx Enabled TelePresence を展開するために必要な項目と設定作業について説明します。次のような構成になっています。

- サーバおよびサイトのアクセス チェックリスト (2-1 ページ)
- 設定作業チェックリスト (2-3 ページ)

サーバおよびサイトのアクセス チェックリスト

表 2-1 に、Cisco WebEx Enabled TelePresence を初めて設定する前に、必要な情報を示します。

表 2-1　　必要な情報の確認

必要な情報	説明と入手先	✔
WebEx サイトの URL	Cisco WebEx サイトの URL。 **入手先**：Cisco WebEx アカウント チームから提供されます。 **例**：*https://example.webex.com/example* **詳細な手順**：Cisco TelePresence Management Suite の設定。	
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。 **入手先**：Cisco WebEx アカウント チームから提供されます。 **例**：“example.webex.com” **詳細な手順**：Cisco TelePresence Management Suite の設定	

表 2-1　必要な情報の確認

必要な情報	説明と入手先	✔
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。 **入手先**：Cisco WebEx アカウント チームから提供されます。 **例**：“https://example.webex.com/admin” **詳細な手順**：Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合	
Cisco WebEx 管理者ユーザ名	Cisco WebEx 管理者アカウント ユーザ名。 **入手先**：Cisco WebEx アカウント チームから提供されます。 **例**：“webexAdmin” **詳細な手順**：Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合	
（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。 **詳細な手順**：Cisco TMS でのシングル サインオンの設定	
VCS Expressway のクライアント/サーバ証明書	VCS Expressway と WebEx クラウド間のコール レッグを暗号化する必要があるため、SSL ハンドシェイクを実行するために有効なクライアント/サーバ証明書が必要です。これにより、セキュア シグナリングとメディアを実行できるようになります。 **詳細な手順**：VCS Expressway での WebEx 向けの新しい DNS ゾーンの作成およびCisco VCS Expressway の証明書の設定。	

設定作業チェックリスト

Cisco WebEx Enabled TelePresence 向けに Cisco TelePresence コンポーネントを設定する順序を選択できます。次に示す順序は参考用ですが、この機能を有効にするには、このチェックリストのすべての設定ステップを実行する必要があり、Cisco WebEx Site Administration を設定する前にこの機能と Cisco TelePresence を有効にする必要があります。

1. 会議ブリッジ
   - Cisco MCU（2-3 ページ）
   - Cisco TelePresence Server（2-4 ページ）
2. コール制御：
   - Cisco Video Communications Server（2-5 ページ）
   - Cisco Unified Communications Manager（2-5 ページ）
3. スケジューリング：
   - Cisco TelePresence Management Suite（2-6 ページ）
   - Cisco TelePresence Management Suite Extension for Microsoft Exchange（2-7 ページ）
   - Cisco TelePresence Management Suite Provisioning Extension（2-7 ページ）
4. 音声：
   - Cisco WebEx Enabled TelePresence の音声の設定（2-8 ページ）
5. WebEx サイト：
   - Cisco WebEx Site Administration（2-9 ページ）

Cisco MCU

表 2-2　チェックリスト：MCU での Cisco WebEx Enabled TelePresence 初回設定

第 3 章「Cisco MCU および TelePresence Server の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	**SIP** を設定します	SIP（3-2 ページ）	
ステップ 2	**コンテンツ モード**を設定します。	コンテンツ モード（3-2 ページ）	
ステップ 3	**ビデオおよびオーディオ コーデック**を設定します。	ビデオ コーデックとオーディオ コーデック（3-2 ページ）	

第 3 章「Cisco MCU および TelePresence Server の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 4	**自動コンテンツ ハンドオーバー**を設定します。	自動コンテンツ ハンドオーバー（3-3 ページ）	
ステップ 5	オプションの**推奨される設定**を行います。 • 自動的にコンテンツ チャネルを重要として設定 • 発信トランスコード コーデック • 適応型ゲイン制御 • 参加と退席の通知音 • 暗号化	MCU の推奨設定（3-3 ページ）	

Cisco TelePresence Server

表 2-3　チェックリスト：TelePresence Server での Cisco WebEx Enabled TelePresence 初回設定

第 3 章「Cisco MCU および TelePresence Server の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	SIP を設定します	SIP（3-6 ページ）	
ステップ 2	**ローカル管理モード**を設定します	ローカル管理モード（3-6 ページ）	
ステップ 1	**自動コンテンツ ハンドオーバー**を設定します。	自動コンテンツ ハンドオーバー（3-7 ページ）	
ステップ 2	オプションの**推奨される設定**を行います。 • 表示設定	表示設定（3-7 ページ）	

Cisco Video Communications Server

表 2-4　チェックリスト :Cisco Unified CM での Cisco WebEx Enabled TelePresence 初回設定

第 4 章「コール制御の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	**VCS Expressway で WebEx 向けの新しい DNS ゾーンを作成します** • 新しい DNS ゾーンを作成します • TLS 検証モードをオンにし、TLS 検証サブジェクト名を入力します。 • WebEx ドメインの検索ルールを設定します。	VCS Expressway での WebEx 向けの新しい DNS ゾーンの作成（4-3 ページ）	
ステップ 2	**有効なクライアント/サーバ証明書を設定します**	Cisco VCS Expressway の証明書の設定（5-1 ページ）	
ステップ 3	**暗号化が有効な MCU でのトラバーサル ゾーンを設定します**	暗号化が有効な MCU でのトラバーサル ゾーンの設定（4-4 ページ）	
ステップ 4	（Unified CM を使用して展開している場合）**Unified CM と VCS Control の間で SIP トランクを設定します。**	Unified CM と VCS Control 間の SIP トランクの設定（4-5 ページ）	

Cisco Unified Communications Manager

表 2-5　チェックリスト :Cisco Unified CM での Cisco WebEx Enabled TelePresence 初回設定

第 4 章「コール制御の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	**Unified CM と VCS Control の間で SIP トランクを設定します。**	Unified CM と VCS Control 間の SIP トランクの設定（4-5 ページ）	

Cisco TelePresence Management Suite

表 2-6　チェックリスト :Cisco TMS での Cisco WebEx Enabled TelePresence 初回設定

第 6 章「Cisco TelePresence Management Suite の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	Cisco TMS で WebEx 機能を有効にします。	Cisco TMS での Cisco WebEx 機能の設定（6-2 ページ）	
ステップ 2	Cisco TMS で WebEx ユーザを設定します。	Cisco TMS での WebEx ユーザの設定（6-4 ページ）	
ステップ 3	Cisco TMS で MCU のハイブリッド コンテンツ モードを設定します。	Cisco TMS での MCU のハイブリッド コンテンツ モードの設定（6-8 ページ）	

Cisco TelePresence Management Suite Extension for Microsoft Exchange

Microsoft Outlook を使用して WebEx Enabled TelePresence 会議のスケジュール機能を展開する場合は、次の手順を実行します。次のスケジュール オプションのいずれかまたは両方を設定できます。

- WebEx および TelePresence から Outlook
- WebEx Scheduling Mailbox

表 2-7　チェックリスト：Cisco TMSXE での Cisco WebEx Enabled TelePresence 初回設定

第 7 章「Cisco TelePresence Management Suite Extension for Microsoft Exchange の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	WebEx and TelePresence Integration to Microsoft Outlook を使用したスケジュールのために TMSXE を設定します。	WebEx and TelePresence Integration to Outlook のための Cisco TMSXE の設定（7-2 ページ）	
ステップ 2	WebEx Scheduling Mailbox を使用したスケジュールのために TMSXE を設定します。	WebEx Scheduling Mailbox のための Cisco TMSXE の設定（7-7 ページ）	

Cisco TelePresence Management Suite Provisioning Extension

Smart Scheduler を使用して Cisco WebEx Enabled TelePresence 会議のスケジュール機能を展開する場合は、次の手順を実行します。

表 2-8　チェックリスト：Cisco TMSPE での Cisco WebEx Enabled TelePresence 初回設定

	作業	**詳細な手順**	✔
ステップ 1	TMS に TelePresence Management Suite Provisioning Extension（TMSPE）をインストールして有効にします。	Cisco TelePresence Management Suite Provisioning Extension Deployment Guide。	
ステップ 2	TMSPE と Smart Scheduler の追加の前提条件と情報を確認します。	Cisco TelePresence Management Suite Provisioning Extension の設定（8-1 ページ）	

Cisco WebEx Enabled TelePresence の音声の設定

表 2-9　チェックリスト :Cisco WebEx Enabled TelePresence の音声の設定

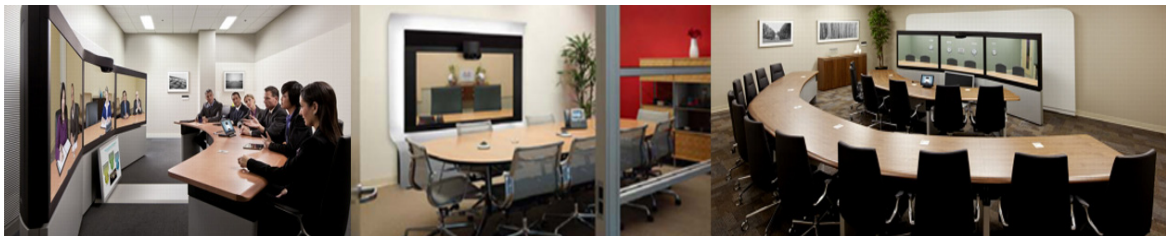
第 9 章「音声の設定」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	Cisco WebEx Enabled TelePresence の SIP 音声を設定します。 • SIP 音声を使用するように Cisco TMS で WebEx サイトを設定します • WebEx サイトでハイブリッド モードを有効にします。	Cisco WebEx Enabled TelePresence の SIP 音声の設定（9-2 ページ）	
ステップ 2	Cisco WebEx Enabled TelePresence の PSTN 音声を設定します。 • PSTN 音声を使用するように Cisco TMS で WebEx サイトを設定します • WebEx サイトでハイブリッド モードを有効にします（オプション） • PSTN コールが PSTN ゲートウェイをパススルーして WebEx に渡るように設定します	Cisco WebEx Enabled TelePresence の PSTN 音声の設定（9-3 ページ）	
ステップ 3	（必要に応じて）Cisco WebEx Enabled TelePresence の TSP 音声を設定します。 • MACC ドメイン インデックスおよびオープン TSP 会議室の WebEx を設定します • TSP ダイヤル文字列を設定します • 会議の開始方法を設定します • 会議主催者の TSP 音声を設定します	Cisco WebEx Enabled TelePresence の TSP 音声の設定（9-8 ページ）	

Cisco WebEx Site Administration

WebEx による WebEx Enabled TelePresence のサイトのプロビジョニングが完了したら、以下のステップに従います。

表 2-10　チェックリスト：Cisco WebEx Site Administration の初回設定

第 10 章「Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合」に進みます。			
	作業	**詳細な手順**	✔
ステップ 1	Cisco TelePresence Integration を有効にします（MC のみ）。	Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合	
ステップ 2	（推奨）TelePresence オプションを有効にします。 • カレンダー上の TelePresence のリスト • 会議ホストへの招待メールの送信 • フリーダイヤル電話番号の参加者への表示		
ステップ 3	Cisco TelePresence VoIP とビデオ接続を設定します。		
ステップ 4	Cisco TelePresence PRO：Meeting Center TelePresence セッション タイプを選択します。	Meeting Center TelePresence セッション タイプの割り当て	



CHAPTER 3

Cisco MCU および TelePresence Server の設定

改訂日：2014 年 7 月

コメント Cisco WebEx Enabled TelePresence の機能を使用するには、MCU ソフトウェア リリース 4.4 以降または TelePresence Server 3.0 以降を実行する必要があります。

目次

この章では、Cisco WebEx Enabled TelePresence 会議向けに MCU と TelePresence Server を設定する方法について説明します。次のような構成になっています。

- MCU の必須設定（3-2 ページ）
- MCU の推奨設定（3-3 ページ）
- TelePresence Server の必須設定（3-6 ページ）
- TelePresence Server の推奨設定（3-7 ページ）

はじめに

この章では、MCU と TelePresence Server の両方で、Cisco WebEx Enabled TelePresence 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。

導入に関して、MCU および TelePresence Server の両方を VCS に直接登録する必要があります。Unified CM にトランクすることはできません。

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。

コメント WebEx Enabled TelePresence 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 の必須設定

Cisco WebEx Enabled TelePresence に必要な MCU の設定を次に示します。

- SIP（3-2 ページ）
- コンテンツ モード（3-2 ページ）
- ビデオ コーデックとオーディオ コーデック（3-2 ページ）
- 自動コンテンツ ハンドオーバー（3-3 ページ）

MCU 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/ps12283/prod_release_notes_list.html

SIP

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/TelePresence Server、VCS Control、VCS Expressway、および WebEx クラウド間のコール レッグを相互接続することはできません。

コメント　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。

コンテンツ モード

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、TMS を使用して設定することを推奨します。

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、次の項を参照してください。

Cisco TMS での MCU のハイブリッド コンテンツ モードの設定（6-8 ページ）

ビデオ コーデックとオーディオ コーデック

WebEx では、ビデオとコンテンツに H.264、音声に G.711 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。

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。

ステップ 3　[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 4　[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 5　[詳細設定（Advanced Settings）] セクションの次の項目で [G.711] 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 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。

自動コンテンツ ハンドオーバー

Cisco WebEx Enabled TelePresence 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。

MCU で自動コンテンツ ハンドオーバーを有効にするには、次の手順を実行します。

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。

ステップ 3　[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 4　[コンテンツ（Content）] タブをクリックします。

ステップ 5　[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 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。

MCU の推奨設定

Cisco WebEx Enabled TelePresence で最適な結果を得るため、MCU で次の設定を行うことを推奨します。

- 自動的にコンテンツ チャネルを重要として設定（3-4 ページ）
- 発信トランスコード コーデック（3-4 ページ）
- 適応型ゲイン制御（3-4 ページ）
- 参加と退席の通知音（3-5 ページ）
- 暗号化（3-5 ページ）

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。

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

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。

発信トランスコード コーデックを H.264 に設定するには、次の手順を実行します。

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　[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。

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。

適応型ゲイン制御

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。

参加時の適応型ゲイン制御を有効に設定するには、次の手順を実行します。

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 [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。

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。

参加と退席の通知音

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。Cisco WebEx Enabled TelePresence 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。

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

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。

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 の必須設定

Cisco WebEx Enabled TelePresence に必要な TelePresence Server の設定を次に示します。

- SIP（3-6 ページ）
- ローカル管理モード（3-6 ページ）
- 自動コンテンツ ハンドオーバー（3-7 ページ）

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

コメント　TSP 音声のサポートには、サードパーティの相互運用キーを持つ TelePresence Server リリース 3.1 が必要です。

SIP

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。

コメント　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。

ローカル管理モード

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。動作モードを設定するには、以下の手順を実行します。

TelePresence Server でローカル管理モードを有効にするには、次の手順を実行します。

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

Cisco WebEx Enabled TelePresence 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。

TelePresence Server で自動コンテンツ ハンドオーバーを有効にするには、次の手順を実行します。

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。

TelePresence Server の推奨設定

Cisco WebEx Enabled TelePresence で最適な結果を得るため、TelePresence Server で次の設定を行うことを推奨します。

表示設定

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。

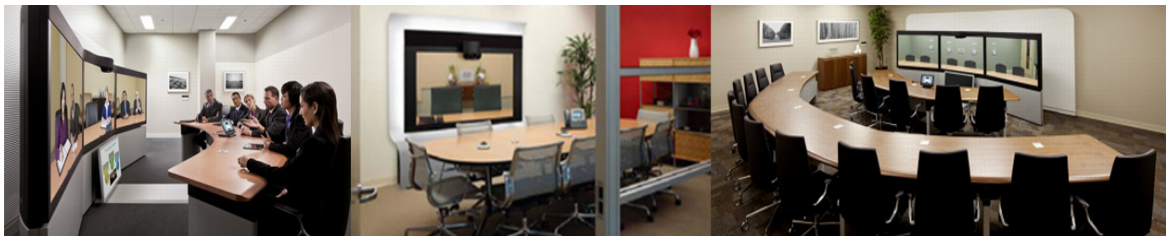
TelePresence Server で全画面表示を有効にするには、次の手順を実行します。

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。



CHAPTER 4

コール制御の設定

改訂日：2014 年 2 月

はじめに

この章では、Cisco WebEx Enabled TelePresence 会議のコール制御を設定する方法について説明します。

Cisco WebEx Enabled TelePresence 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。

3 通りのコール制御シナリオが考えられます。

- Cisco TelePresence VCS Control と Expressway

  エンドポイントは、VCS Control および/または Expressway のみに登録されます。
- Cisco Unified CM、VCS Control と Expressway あり

  エンドポイントは、Unified CM のみに登録されます。
- Cisco TelePresence VCS Control と Expressway、Unified CM あり

  エンドポイントは、VCS Control/Expressway および Unified CM に登録されます。

コメント コール制御ソリューションとして Unified CM を使用するには、エンドポイントが VCS Control と Expressway に登録されているかどうかに関係なく、WebEx と通信するために VCS Control と Expressway を導入する必要があります。

Cisco TelePresence Video Communication Server Control と Expressway の設定

ここでは、Cisco WebEx Enabled TelePresence で Cisco TelePresence Video Communication Server Control と Expressway を設定するために必要な手順を説明します。

ここでは、次の作業について説明します。

- 前提条件（4-2 ページ）
- VCS Expressway での WebEx 向けの新しい DNS ゾーンの作成（4-3 ページ）
- 暗号化が有効な MCU でのトラバーサル ゾーンの設定（4-4 ページ）

前提条件

Cisco TelePresence VCS 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（VCS）で、ファームウェア リリース X7.2.2 以降が稼動している必要があります。
- ネットワークのエンドポイントが、VCS Control または Expressway、あるいは Unified CM に登録されています。

コメント　エンドポイントが Unified CM に登録されている場合、Unified CM 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（4-4 ページ）を参照してください。

- Expressway にスタティック IP アドレスが割り当てられている必要があります
- 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。**
- 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。
- VCS Control がプライベート ネットワークに含まれています。
- VCS Expressway 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 1.1 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/en/US/docs/telepresence/infrastructure/vcs/admin_guide/Cisco_VCS_Administrator_Guide_X7-2.pdf

- VCS Control は SIP レジストラ/H.323 ゲートキーパーとして設定されます。

  Cisco WebEx Enabled TelePresence が機能できるようにするには、VCS Control を SIP レジストラとして設定し、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。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。

  VCS 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。VCS 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。

  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『Cisco TelePresence Video Communication Server Basic Configuration（Control with Expressway）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_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-2.pdf

- 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 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 H323 SRV レコードが必要です。これにより、TelePresence 参加者は VCS Expressway にルーティングできます。

VCS Expressway での WebEx 向けの新しい DNS ゾーンの作成

デフォルトでは、VCS ソリューションはローカル ドメインを処理し、非ローカル ドメイン宛てのコールを VCS Expressway にルーティングして、これらのコールを DNS ゾーン経由でインターネットにルーティングします。

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 VCS Expressway で設定する必要があります。

Cisco WebEx Enabled TelePresence 用に VCS Expressway を設定するには、次の手順を実行します。

ステップ 1　新しい DNS ゾーンを作成します。

a. [H.323] を [オフ（Off）] に設定します。

b. [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。

c. [TLS 検証モード（TLS Verify mode）] を有効にします。

d. [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。

e. [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（Protocol）]：[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。
https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-1.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 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。

注意　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、第 5 章「Cisco VCS Expressway の証明書の設定」を参照してください。

暗号化が有効な MCU でのトラバーサル ゾーンの設定

ここでは、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。

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。

ステップ 1　VCS Control から VCS Expressway への新しいトラバーサル クライアント ゾーンを設定します。

コメント　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　VCS Expressway で、前のステップで設定した 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 3　この新しい 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 4　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。

コメント　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、Cisco WebEx Enabled TelePresence 向けに Cisco Unified Communications Manager（Unified CM）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 CM だけに登録されている展開と、Unified CM と VCS Control/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。

- 前提条件（4-4 ページ）
- Unified CM と VCS Control 間の SIP トランクの設定（4-5 ページ）

前提条件

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

- Cisco Unified CM 8.6.2 または 9.1.1。
- ネットワーク上のエンドポイントは Unified CM に登録されています。

- 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て、VCS に登録されています。
- VCS Control がプライベート ネットワークに配備されています。
- MCU および TelePresence Server 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、1.3 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。
- DNS ゾーンが設定された VCS Expressway。

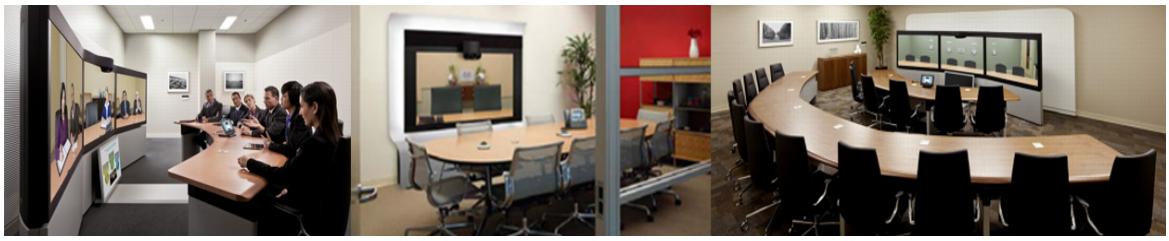
Unified CM と VCS Control 間の SIP トランクの設定

ここでは、Cisco TelePresence Video Communication Server（Cisco VCS）バージョン X7.2.1 以降と Cisco Unified Communications Manager（Unified CM）バージョン 6.1、7 または 8 が SIP トランクを介してインターワーキングするように設定する方法を説明します。

これは、Unified CM に登録されているエンドポイントが Cisco WebEx Enabled TelePresence 会議に参加し、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 CM 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。

設定手順の詳細については、次の URL にある『Cisco TelePresence Cisco Unified Communications Manager with Cisco VCS (SIP Trunk) Deployment Guide』を参照してください。

Cisco VCS and Unified CM Deployment Guide (Unified CM 8.6.x, 9.x and VCS X7.2).



CHAPTER 5

Cisco VCS Expressway の証明書の設定

改訂日：2014 年 4 月

はじめに

この章では、Cisco VCS Expressway で証明書を設定するためのベスト プラクティスについて説明します。

設定は 3 段階で行われます。

- 証明書署名要求（CSR）の生成
- VCS Expressway への SSL サーバ証明書のインストール
- VCS Expressway での信頼された CA リストの設定

VCS Expressway X7.2.2 および X8.1 の両方がサポートされます。それぞれの設定方法には重要な違いがあります。これらの違いは、以降の手順に記載されています。

注意 VCS Expressway X7.2.2 のスタティック NAT を使用しているお客様は、X8.1 にアップグレードしないことを強く推奨します。X8.1 でスタティック NAT を使用している場合は、「VCS Expressway X8.1 の暗号化の問題と回避策」の推奨回避策を参照してください。

VCS Expressway X8.1 の暗号化の問題と回避策

スタティック NAT を使用するときの VCS Expressway X8.1 の代理暗号化機能に問題があります。VCS Expressway X8.1 が SDP のメディア パーツにイーサネット 2 IP アドレスを使用するため、コールのメディア パーツが失敗します。（Caveat ID：CSCum90139）。X7.2.2 を実行する VCS Expressway でスタティック NAT を使用しているお客様は、メンテナンス リリースでこの問題が解決されるまで、X8.1 にアップグレードしないでください。

VCS Expressway X8.1 でスタティック NAT を使用している場合は、次のいずれかの回避策を推奨します。

- VCS Expressway を X7.2.2 にダウングレードする。
- スタティック NAT を使用しないように VCS Expressway X8.1 を再設定する。
- VCS Expressway ではなく VCS Control を使用して代理暗号化する。

代理暗号化に VCS Control を使用するには、次の手順を実行します。

ステップ 1　MCU で、すべての電話会議の暗号化を**オフ**にします。

ステップ 2　VCS Control で、専用の WebEx トラバーサル ゾーンを**強制暗号化**に変更します。

ステップ 3　VCS Expressway で、専用の WebEx DNS ゾーンを**暗号化自動**に変更します。

使用可能なビデオ

VCS Expressway 7.2.2 の設定手順全体については、次のビデオ シリーズでも例を挙げて説明されています。

Configuring Certificates on Cisco VCS Expressway for WebEx Enabled TelePresence

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。

コメント　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。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 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*
- 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

コメント　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。最新情報については、WebEx にお問い合わせください。

* 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、次の URL 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。

https://www.entrust.net/downloads/root_index.cfm

注意　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。

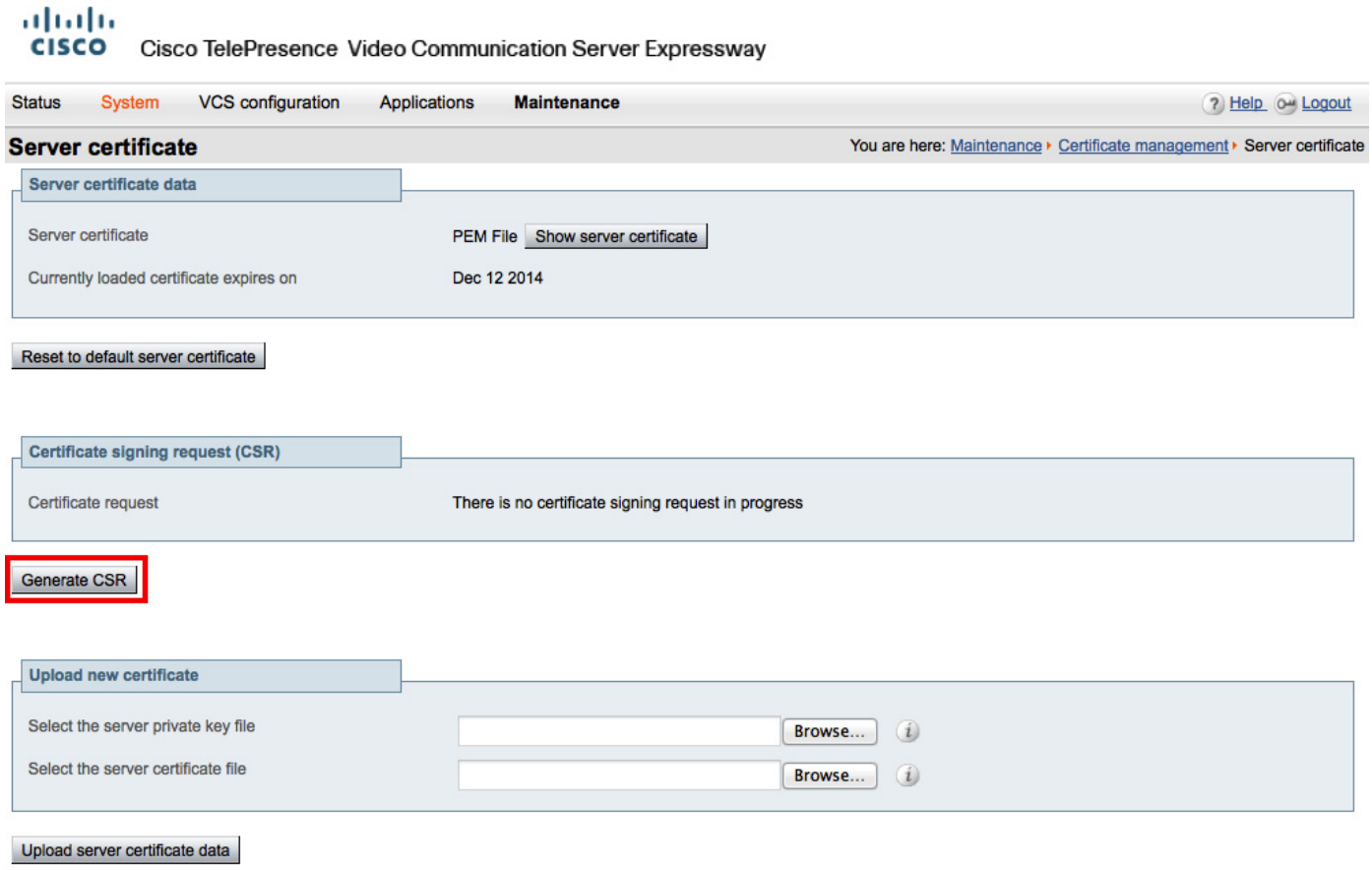
証明書署名要求（CSR）の生成

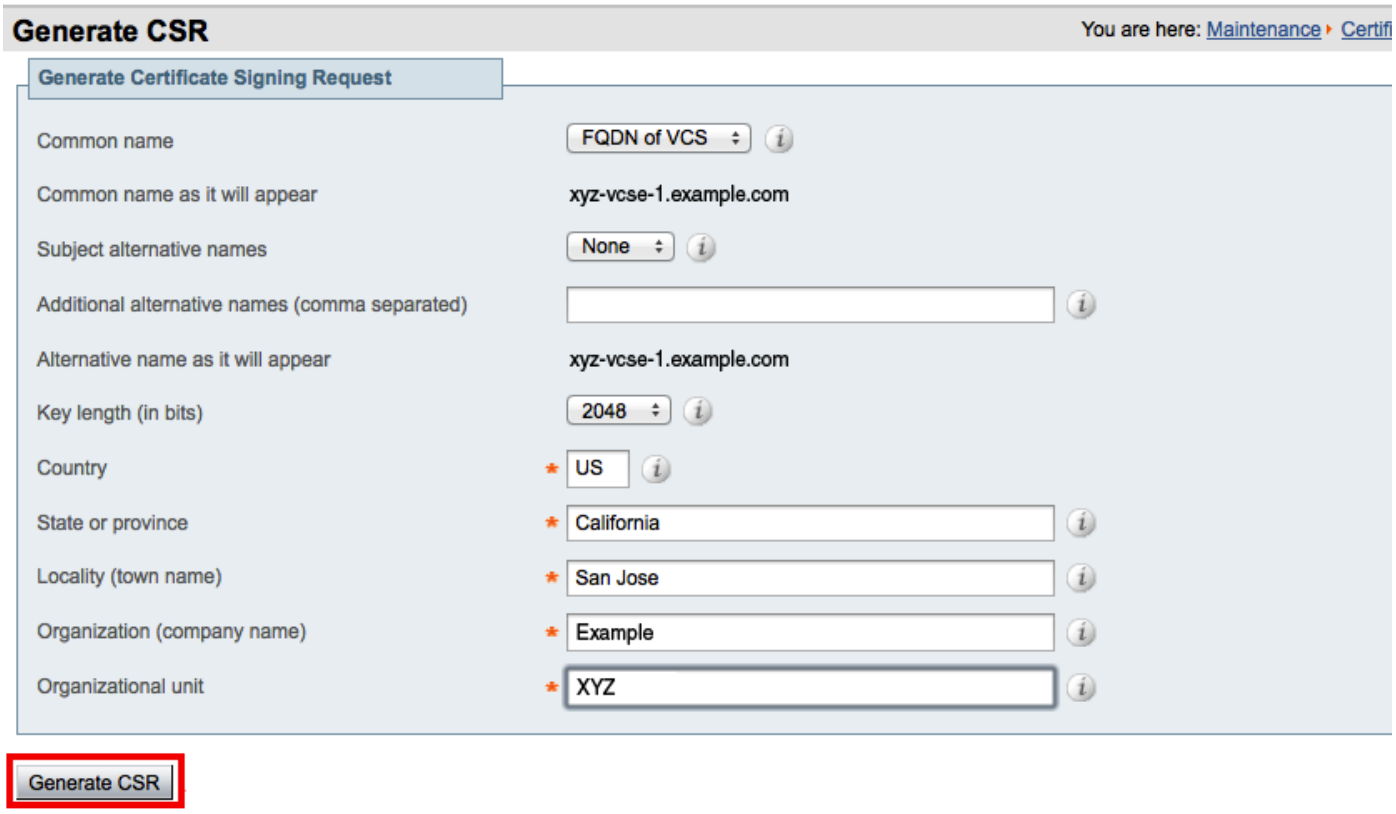
証明書署名要求を生成するには、次の手順を実行します。

ステップ 1　VCS Expressway で次の手順を実行します。

- X7.2.2 では、[メンテナンス（Maintenance）] > [証明書管理（Certificate management）] > [サーバ証明書（Server certificate）] の順に移動します。
- X8.1 では、[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）] の順に移動します。

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

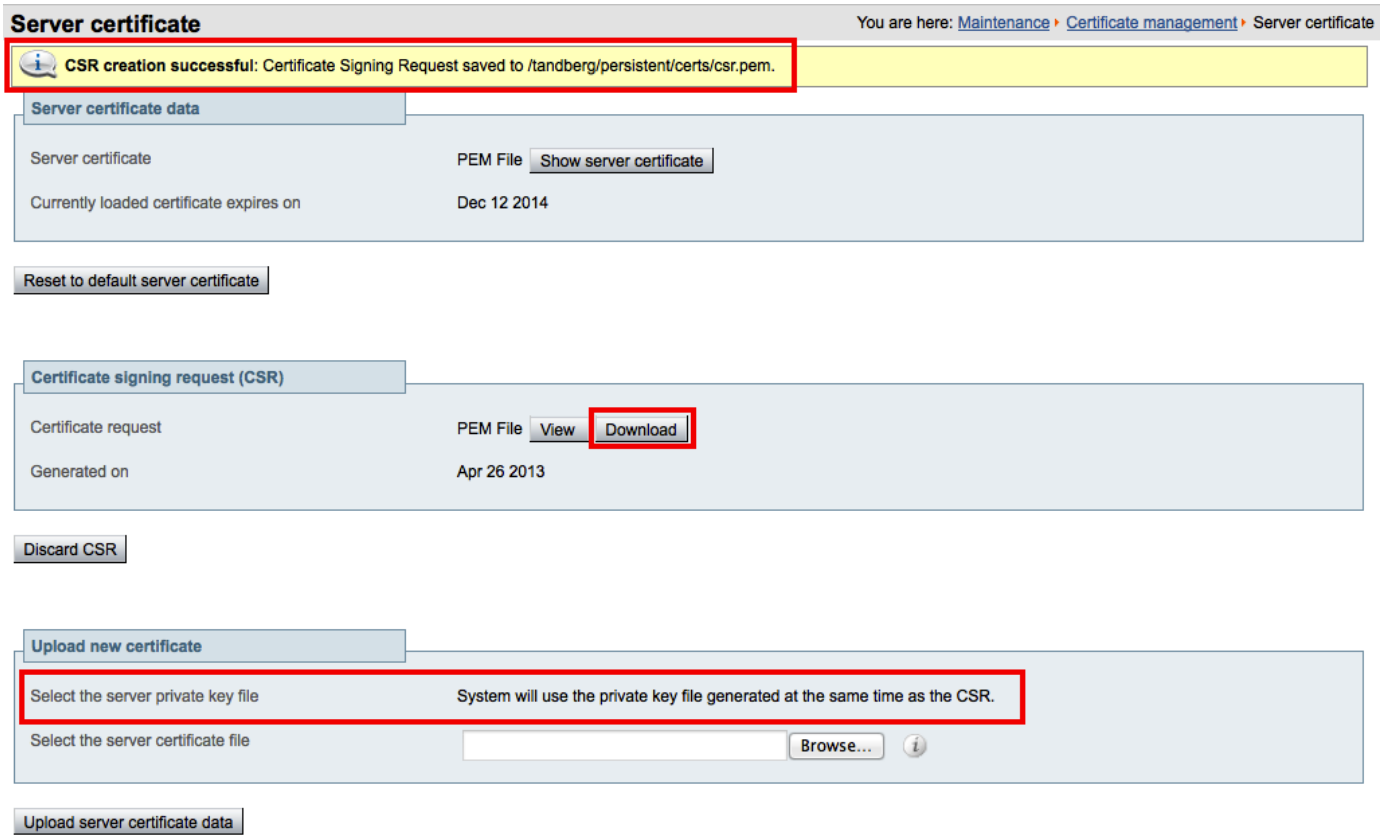

Cisco TelePresence Video Communication Server Expressway
Status
System
VCS configuration
Applications
Maintenance
Help
Logout
Server certificate
You are here: Maintenance ▸ Certificate management ▸ Server certificate
Server certificate data
Server certificate
PEM File
Show server certificate
Currently loaded certificate expires on
Dec 12 2014
Reset to default server certificate
Certificate signing request (CSR)
Certificate request
There is no certificate signing request in progress
Generate CSR
Upload new certificate
Select the server private key file
Browse...
Select the server certificate file
Browse...
Upload server certificate data



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。

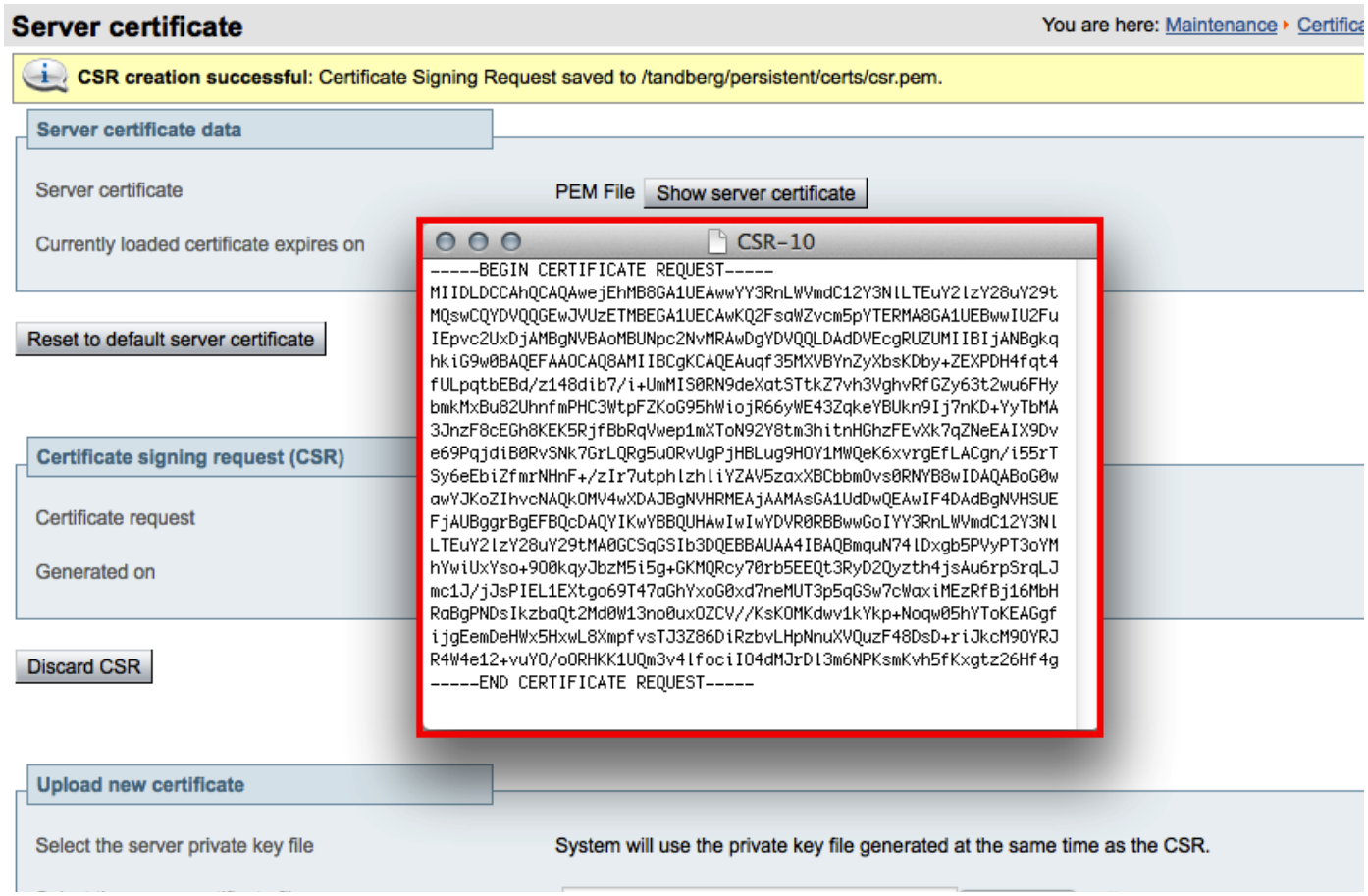
[CSRの作成（Generate CSR）] ボタンをクリックすると、[サーバ証明書（Server Certificate）] ページに、CSR の作成が成功したことを示すメッセージが表示されます。

コメント　秘密キーは CSR 作成プロセスで自動的に生成されます。CSR を廃棄するオプションをクリックしないでください。クリックすると CSR が再生成され、自動生成された秘密キーは [サーバ証明書（Server Certificate）] ページに表示されません。



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。

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（次に示します）。



ステップ 5　公開 CA に CSR を送信します。

コメント　重要: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、VCS Expressway にその証明書をインストールできます。

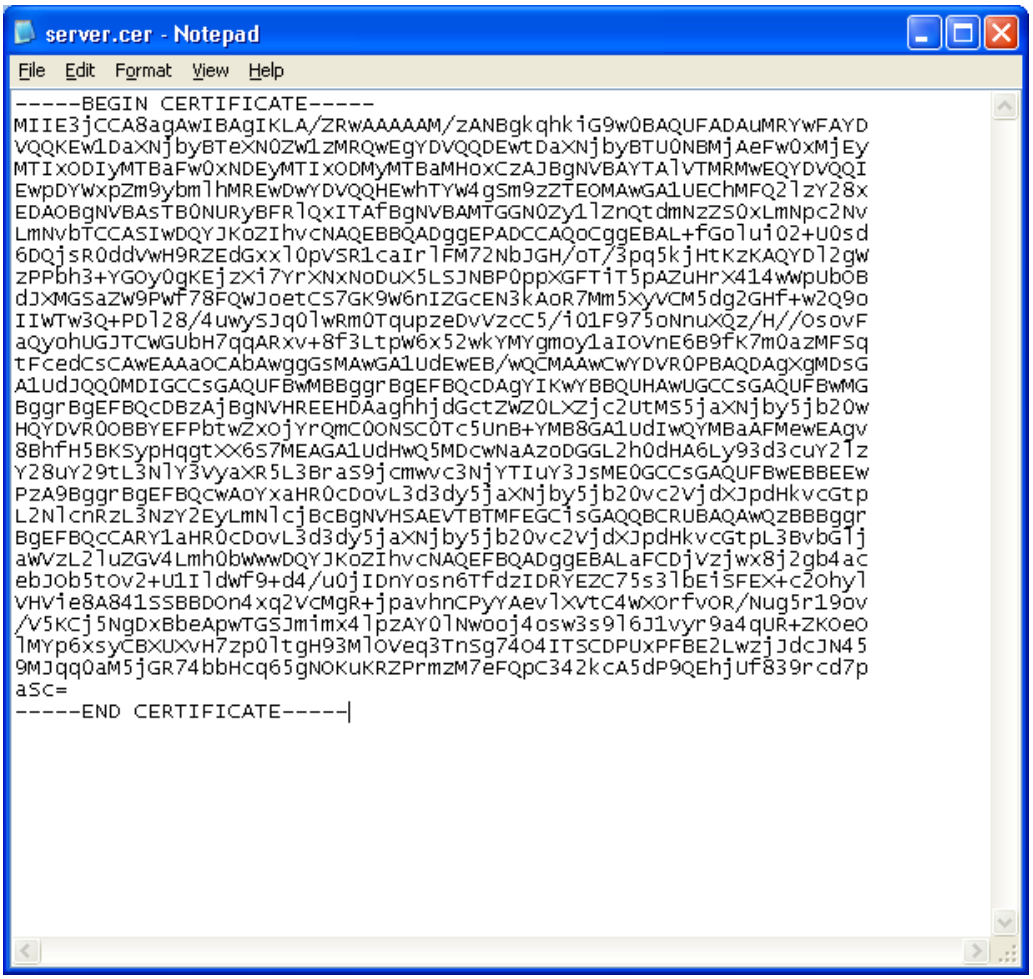
VCS Expressway への SSL サーバ証明書のインストール

コメント　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。

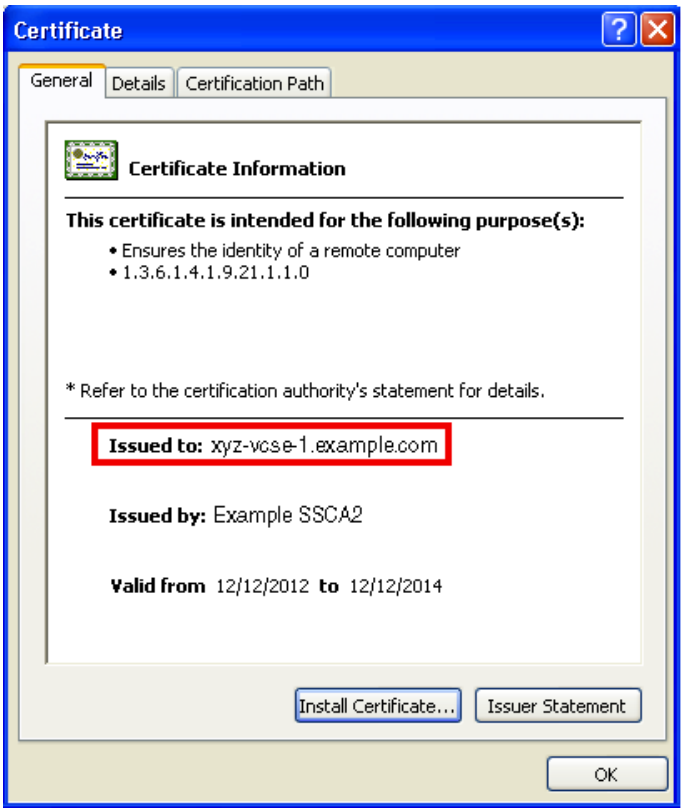
注意　サーバ証明書は、ルート CA 証明書または中間 CA 証明書とともにスタックすることはできません。

VCS Expressway に SSL サーバ証明書をインストールするには、次の手順を実行します。

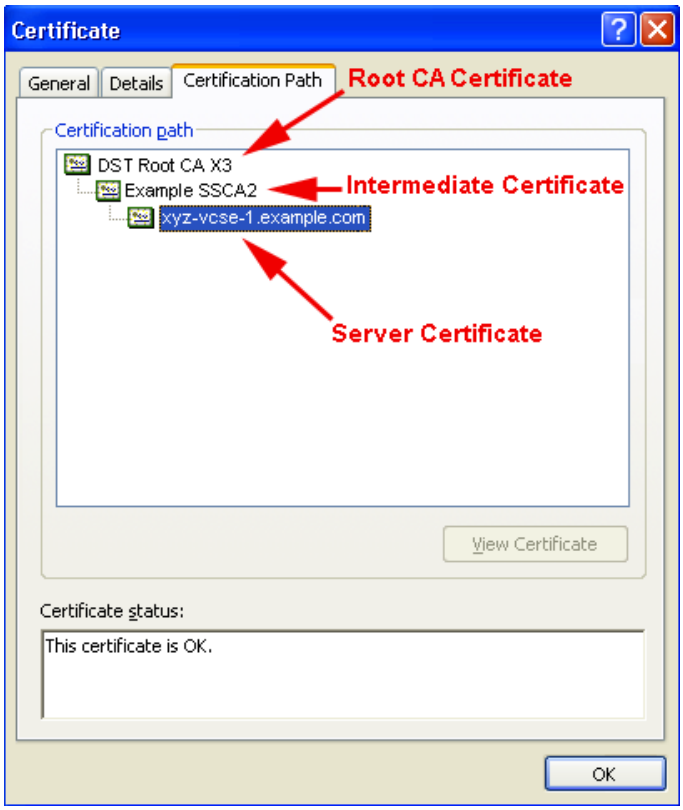
ステップ 1　(推奨) メモ帳などのテキスト エディタ アプリケーションでサーバ証明書を開き、1 つの証明書が表示されること (Begin Certificate と End Certificate で囲まれていること) を確認します。



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 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。



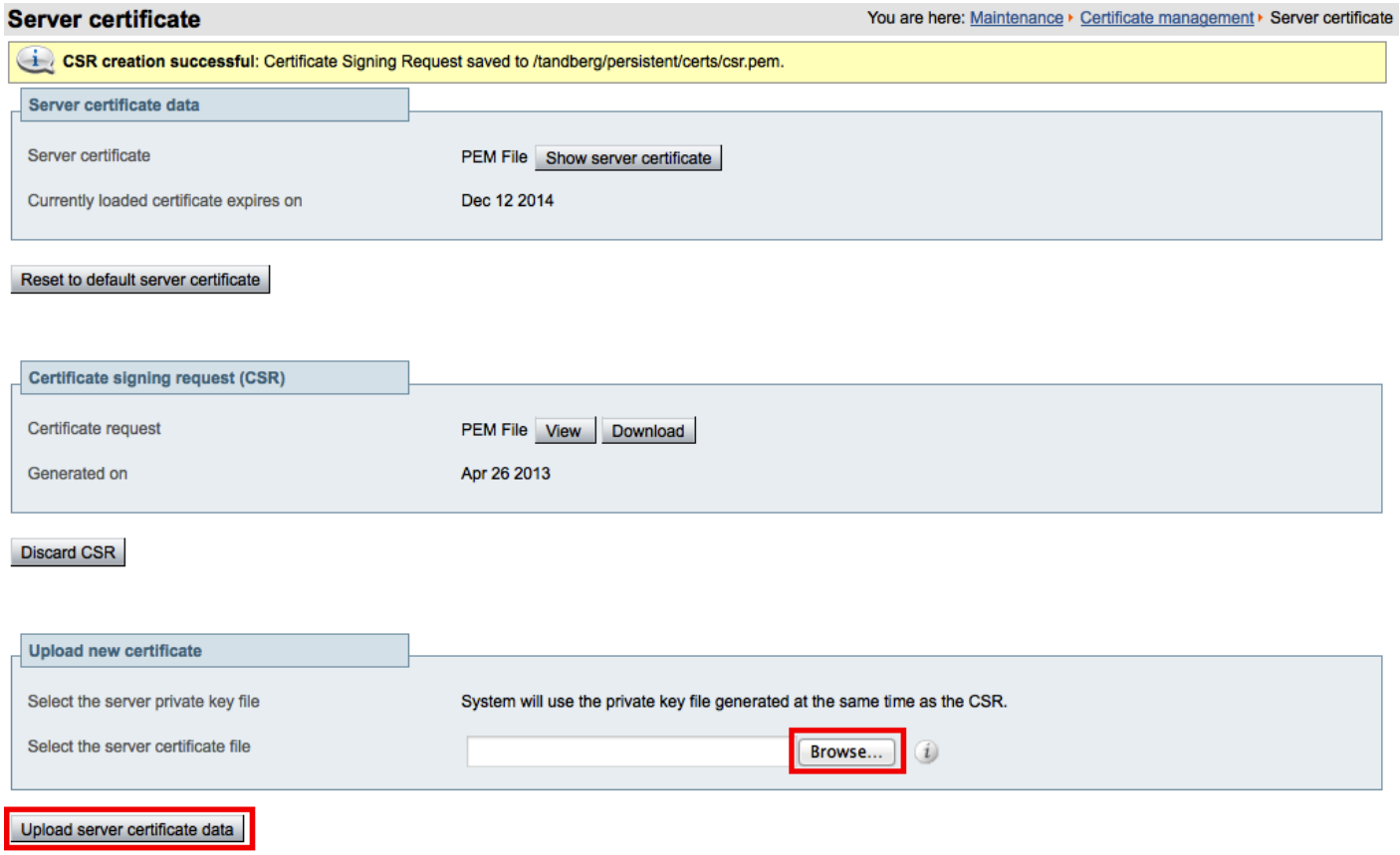
ステップ 2　VCS Expressway で次の手順を実行します。

- X7.2.2 では、[メンテナンス（Maintenance）] > [証明書管理（Certificate management）] > [サーバ証明書（Server certificate）] の順に移動します。
- X8.1 では、[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）] の順に移動します。

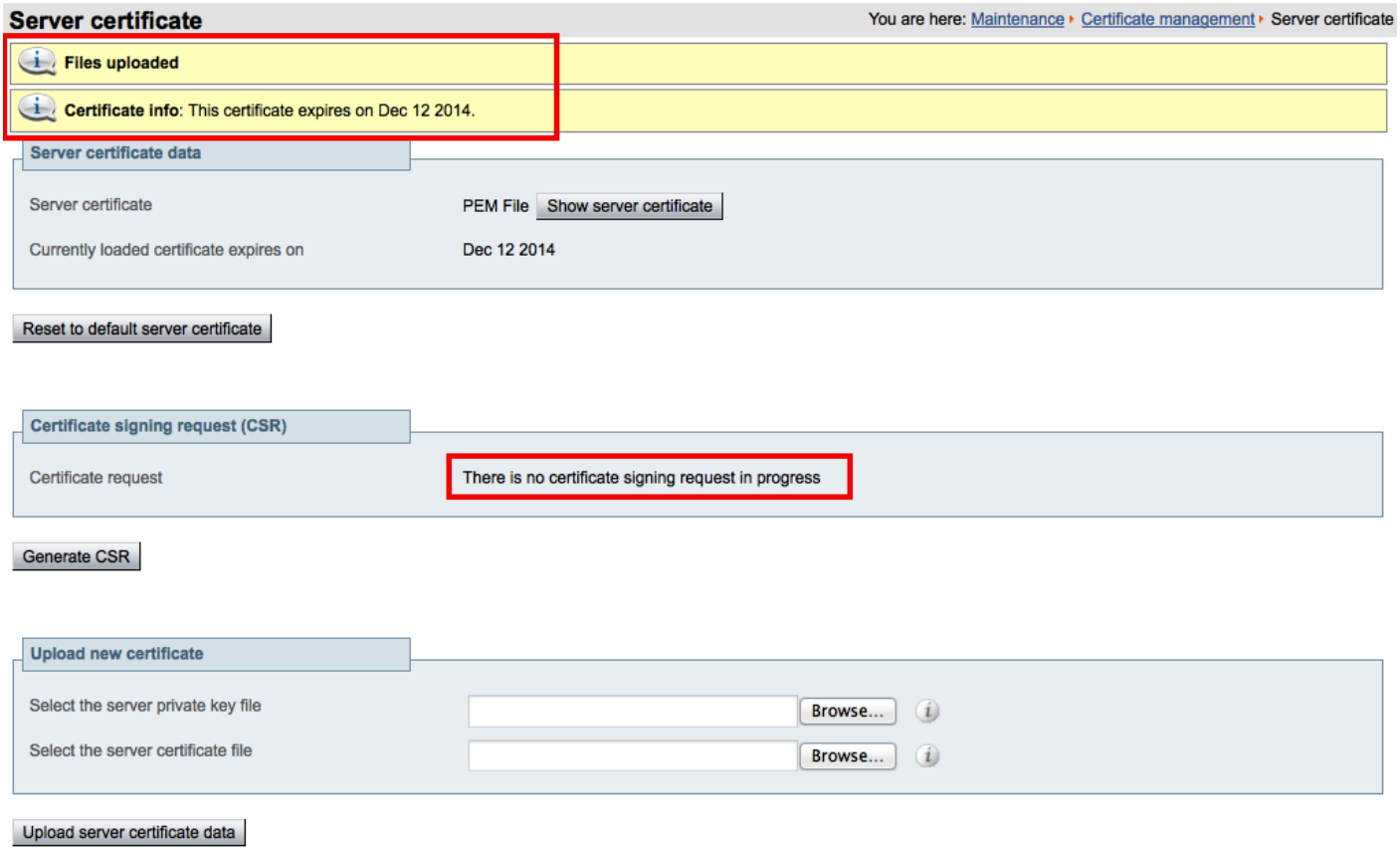
ステップ 3　[参照（Browse）] をクリックし、公開 CA から受信したサーバ証明書を選択し、[開く（Open）] をクリックします。

コメント　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。



VCS Expressway での信頼された CA 証明書リストの設定

ご使用の VCS Expressway 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。

VCS Expressway X7.2.2

VCS Expressway X7.2.2 のデフォルトの信頼された CA 証明書リストには、140 の証明書が含まれています。かなり高い確率で、サーバ証明書の発行元である公開ルート CA がデフォルトの信頼された CA 証明書リストにすでに含まれています。

VCS Expressway X7.2.2 の信頼された CA 証明書リストを設定する方法については、「VCS Expressway X7.2.2 での信頼された CA 証明書リストの設定」を参照してください。

X7.2.2 から X8.1 にアップグレードした VCS Expressway

X7.2.2 から X8.1 にアップグレードした VCS Expressway では、X7.2.2 の信頼された CA 証明書リストが維持されます。

X7.2.2 から X8.1 にアップグレードした VCS Expressway で信頼された CA 証明書リストを設定する方法については、「X7.2.2 から X8.1 にアップグレードした VCS Expressway での信頼された CA 証明書リストの設定」を参照してください。

VCS Expressway X8.1

新規にインストールした VCS Expressway X8.1 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、VCS Expressway 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。

新しくインストールした VCS Expressway X8.1 で信頼された CA 証明書リストを設定する方法については、「VCS Expressway X8.1 での信頼された CA 証明書リストの設定」を参照してください。

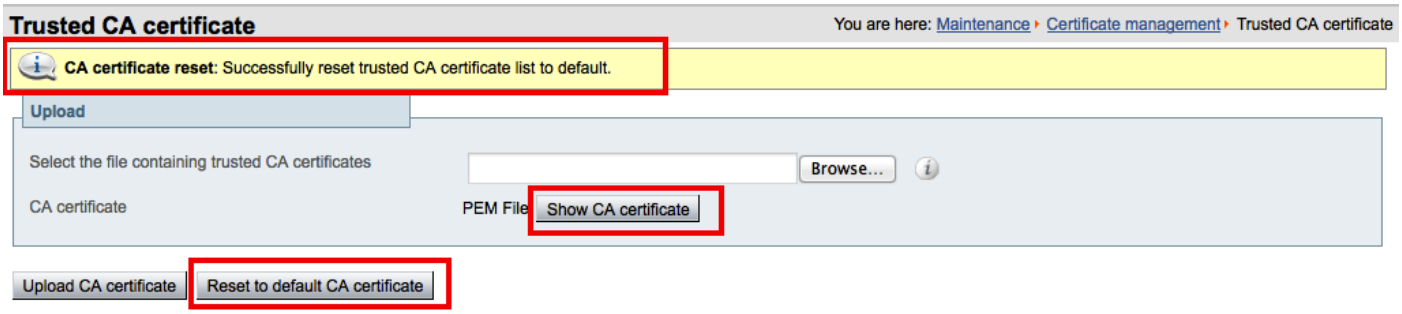
VCS Expressway X7.2.2 での信頼された CA 証明書リストの設定

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。

VCS Expressway X7.2.2 での信頼された CA 証明書リストのリセット

VCS Expressway X7.2.2 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。

ステップ 1　[メンテナンス（Maintenance）] > [証明書管理（Certificate management）] > [信頼されたCA証明書（Trusted CA certificate）] の順に進み、[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。



コメント　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）。

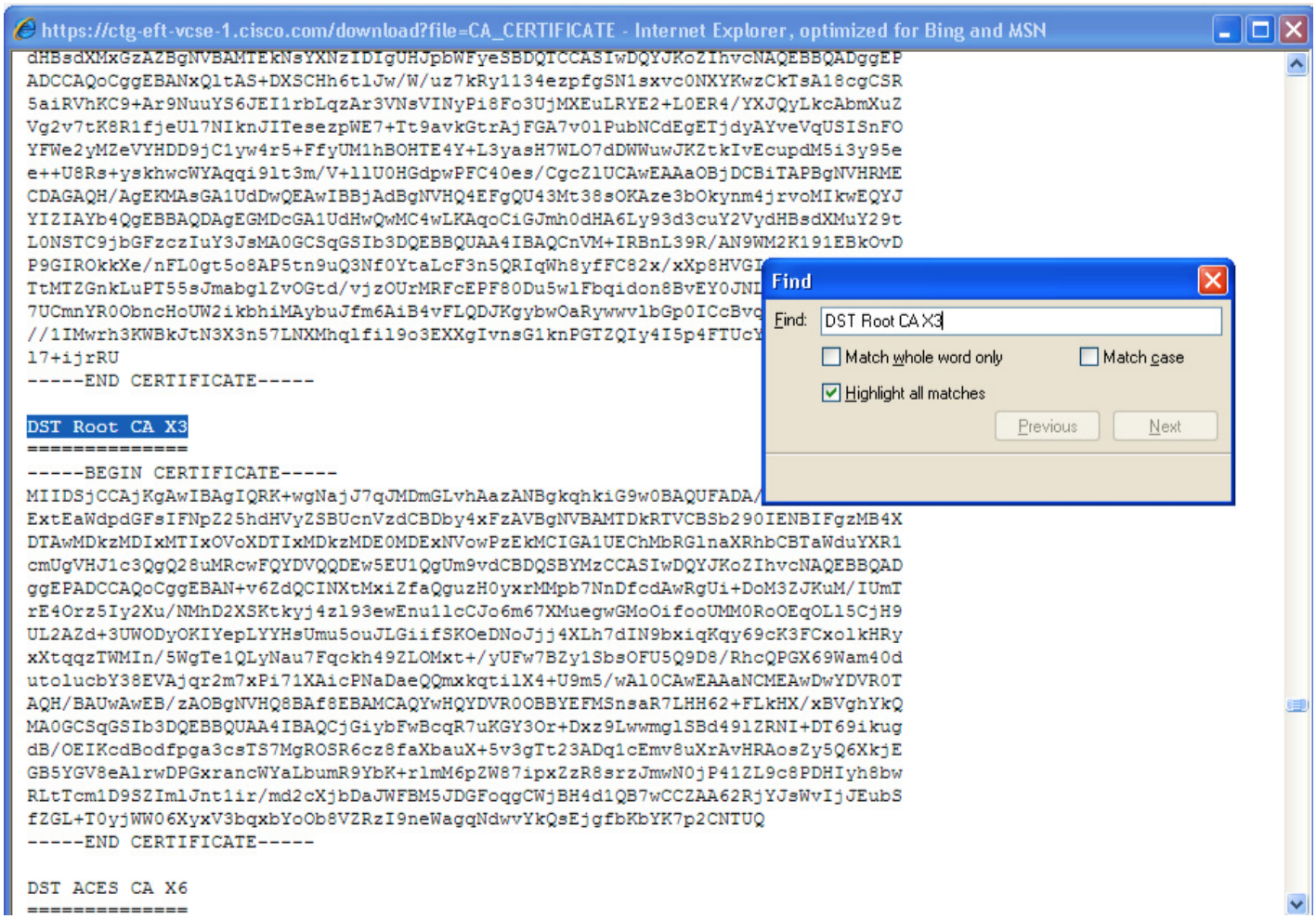
VCS Expressway のデフォルトの信頼された CA 証明書リストには、クラウドが示すサーバ証明書のパブリック ルート CA 証明書がすでに含まれています。WebEx クラウドのルート CA は、Cisco SSCA2 の中間 CA を含む DST ルート CA X3 です。

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、[CA 証明書を表示（Show CA certificate）] をクリックします。

この操作により、現在 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、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 である場合は、次のセクションに進みます。

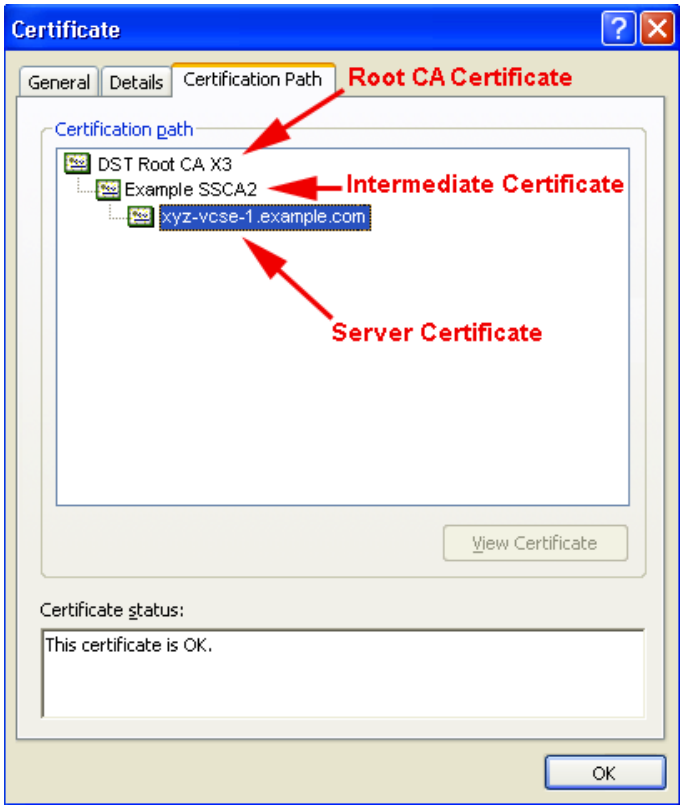
コメント　サーバ証明書の発行元である最上位ルート CA の証明書がデフォルトの信頼された CA 証明書リストに含まれていない場合は、次のセクションに詳細を説明する、中間 CA 証明書をスタックするための手順を使用して、追加する必要があります。

VCS Expressway X7.2.2 での信頼された CA 証明書リストへの中間 CA 証明書のスタック

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。

図 5-1　　.CER ファイル形式のサーバ証明書



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。

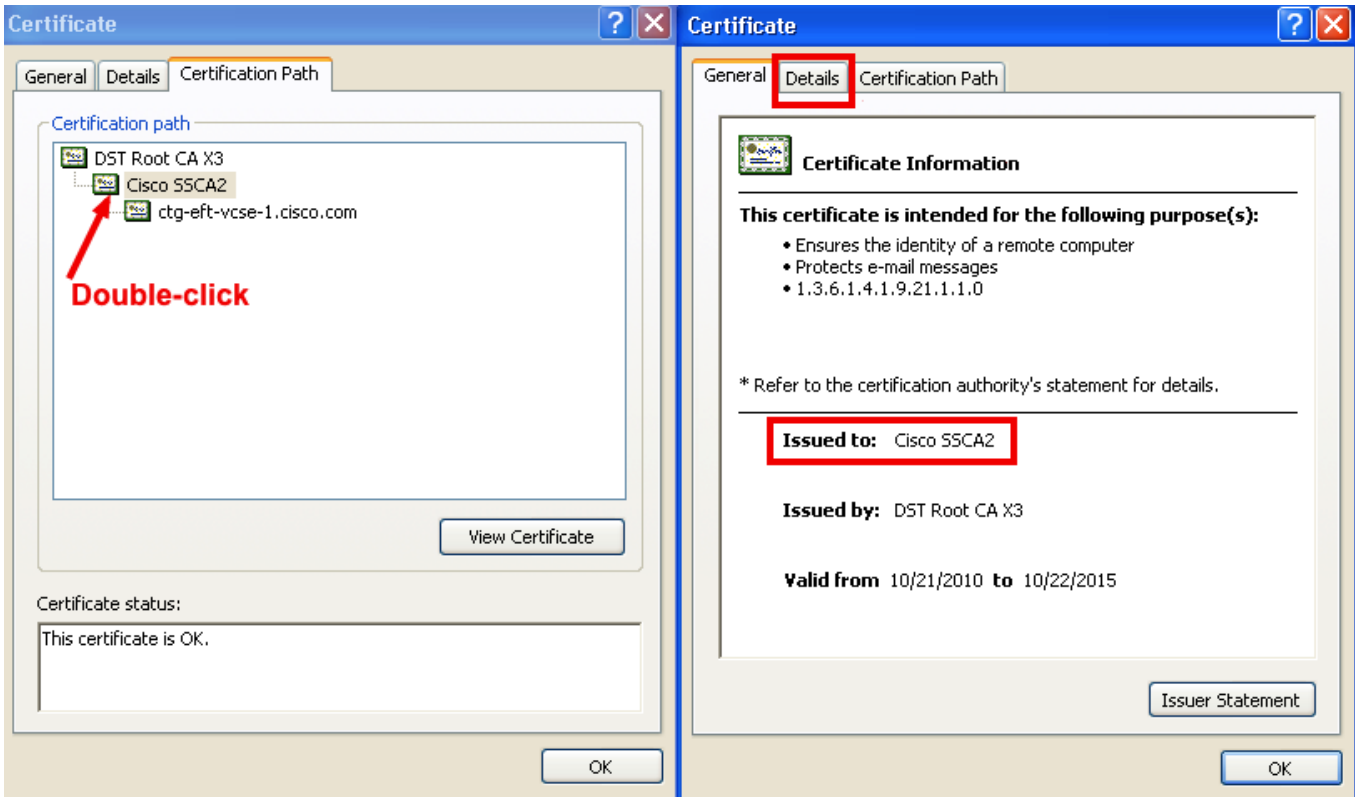
ステップ 1　サーバ証明書を .CER ファイルとして開きます（図 5-1 を参照）。

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。

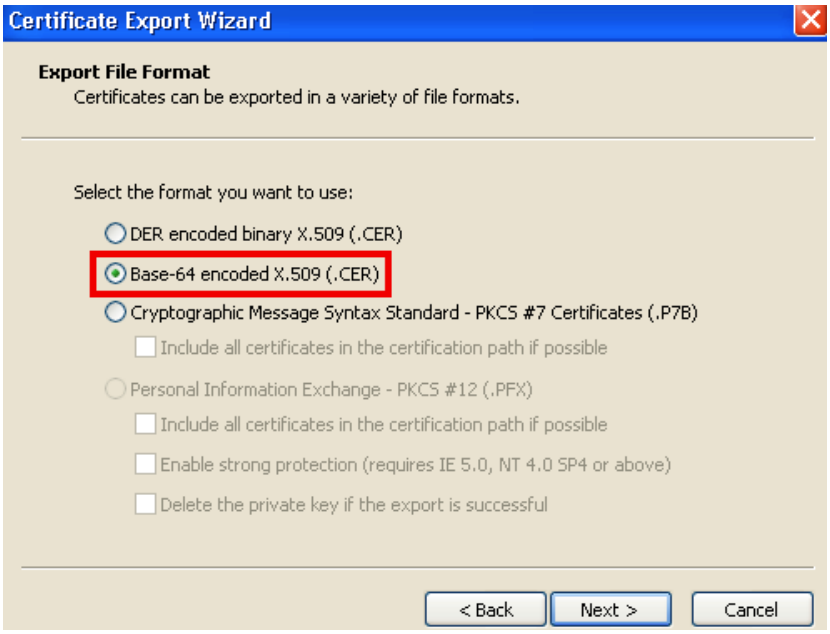
ステップ 4　[詳細（Details）] タブをクリックし、次に [ファイルにコピー...（Copy to File…）] をクリックします。



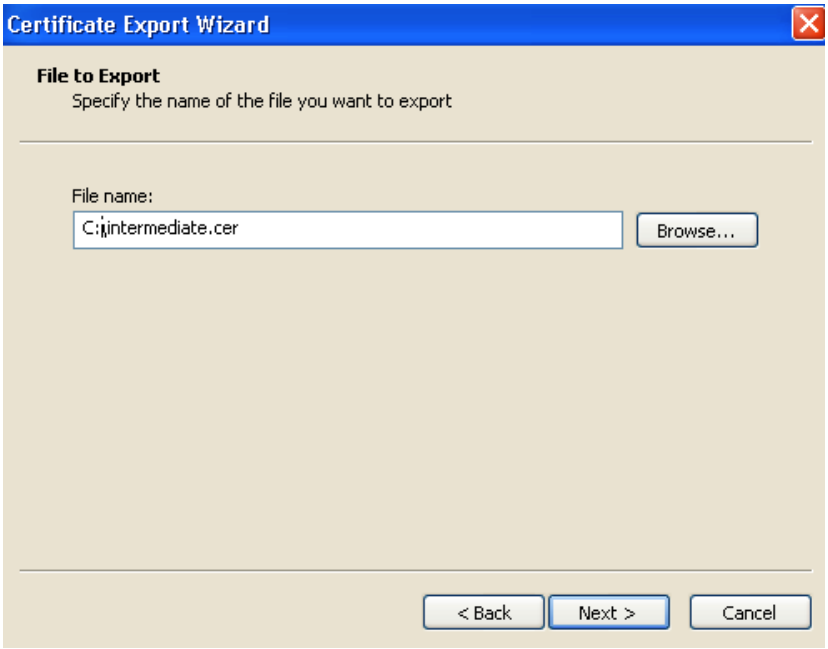
[証明書のエクスポートウィザードの開始(Welcome to the Certificate Export Wizard)] が表示されます。

ステップ 5　[次へ(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　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)] の順に進み、[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。

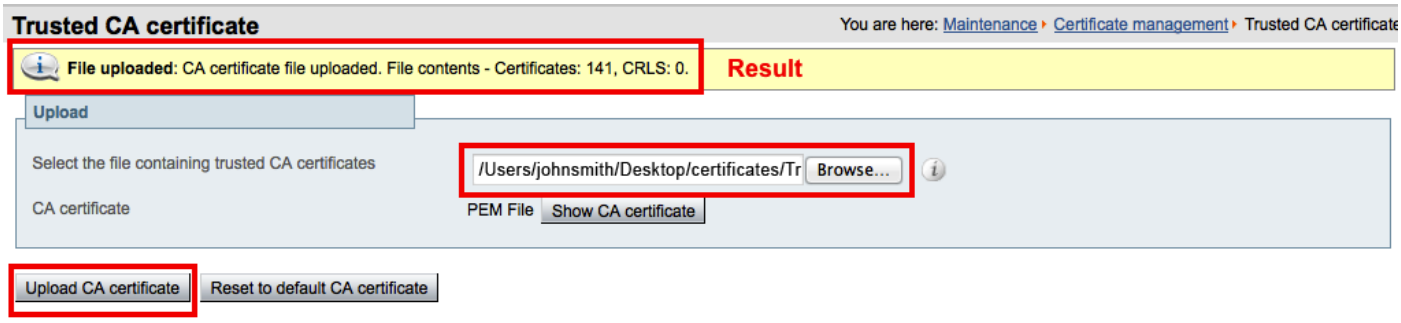
ステップ 12　ルート証明書の上に中間 CA 証明書を貼り付けます。

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。

コメント　ルート CA がデフォルトの信頼された CA リストに含まれていない場合は、中間 CA 証明書をスタックする手順に従います。

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。



VCS Expressway X7.2.2 での証明書の設定が完了しました。

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 (X7.2)』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

X7.2.2 から X8.1 にアップグレードした VCS Expressway での信頼された CA 証明書リストの設定

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。

X7.2.2 から X8.1 にアップグレードした VCS Expressway での信頼された CA 証明書リストのリセット

VCS Expressway X8.1 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。

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)] の順に進み、[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。

コメント　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)。

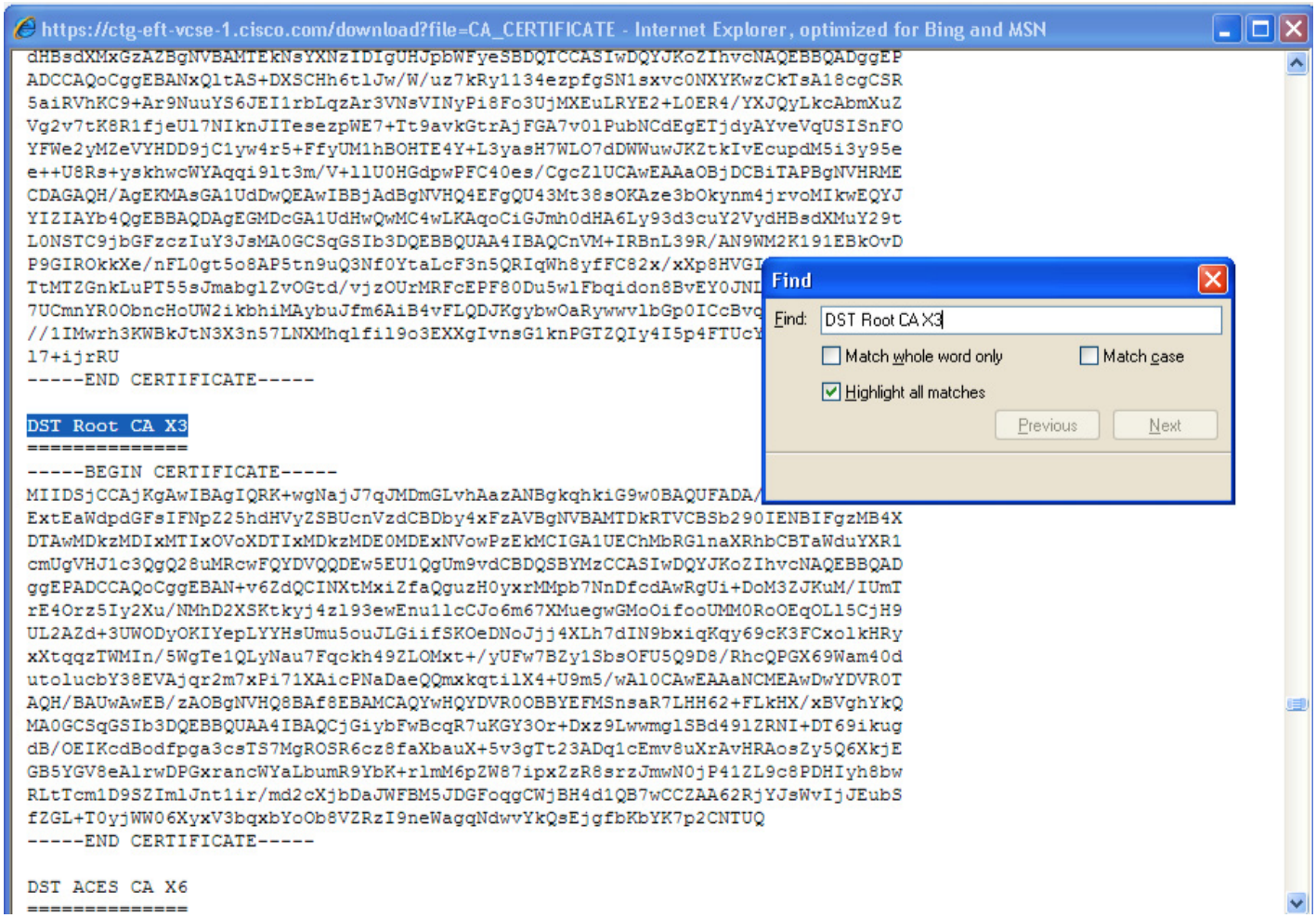
VCS Expressway のデフォルトの信頼された CA 証明書リストには、クラウドが示すサーバ証明書のパブリック ルート CA 証明書がすでに含まれています。WebEx クラウドのルート CA は、Cisco SSCA2 の中間 CA を含む DST ルート CA X3 です。

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 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、VCS Expressway での証明書の設定はこれで完了です。

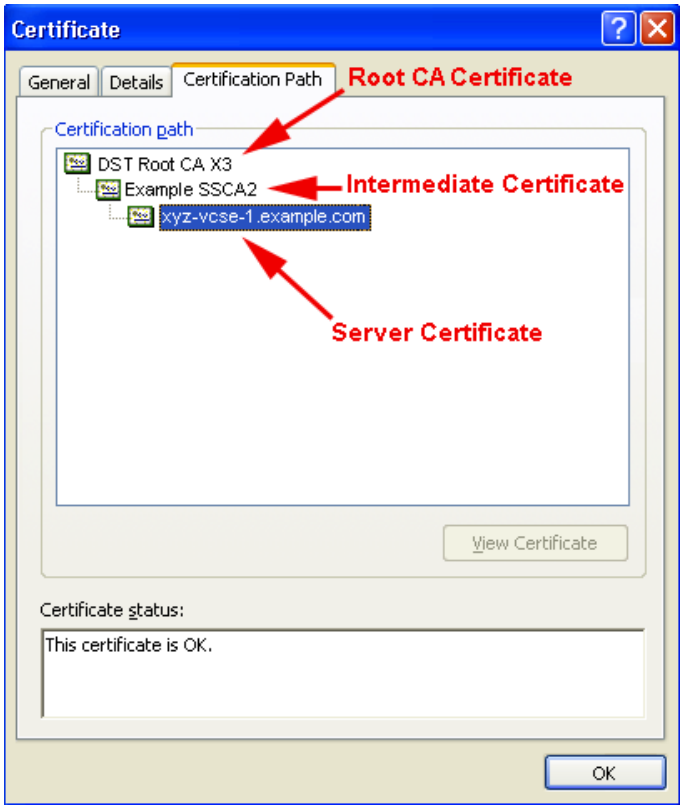
サーバ証明書の発行元が中間 CA である場合、またはサーバ証明書の発行元である最上位ルート CA の証明書が信頼された CA 証明書リストに含まれていない場合は、その証明書を信頼された CA 証明書リストに追加する必要があります。この手順については次の項で説明します。

VCS Expressway X8.1 への中間 CA 証明書の追加

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 証明書リストに追加する必要があります。

図 5-2　　.CER ファイル形式のサーバ証明書



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。

ステップ 1　サーバ証明書を .CER ファイルとして開きます（図 5-2 を参照）。

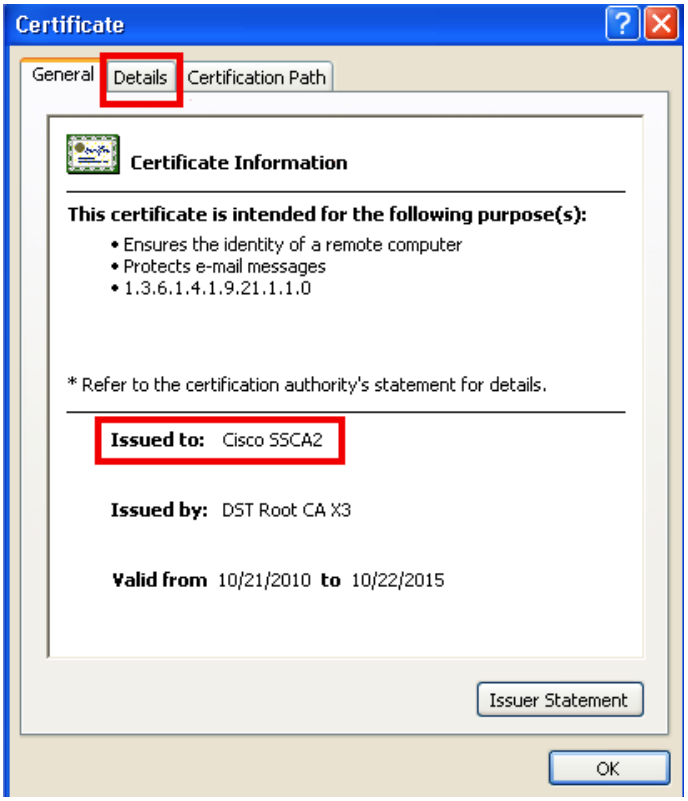
ステップ 2　[証明のパス（Certification Path）] タブをクリックします。

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。

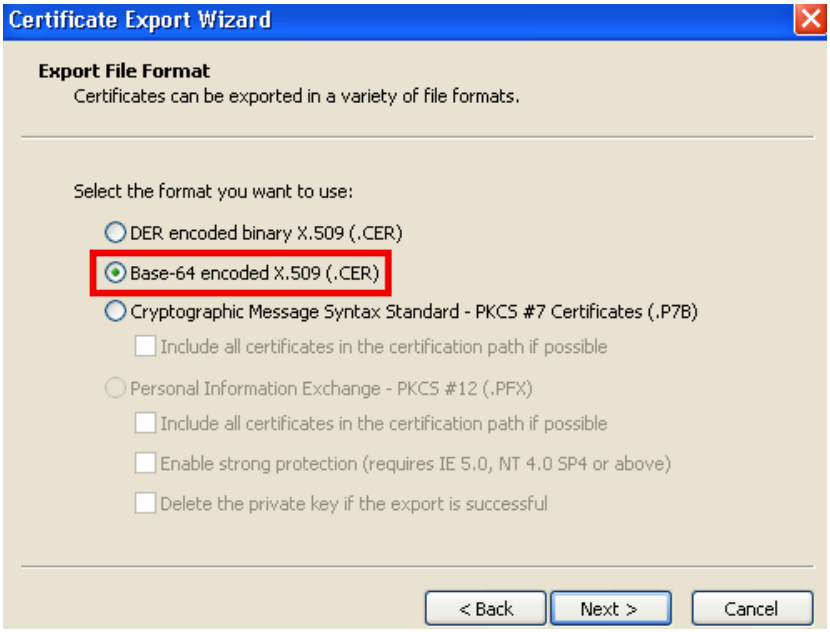
ステップ 5　[詳細（Details）] タブをクリックし、次に [ファイルにコピー...（Copy to File…）] をクリックします。



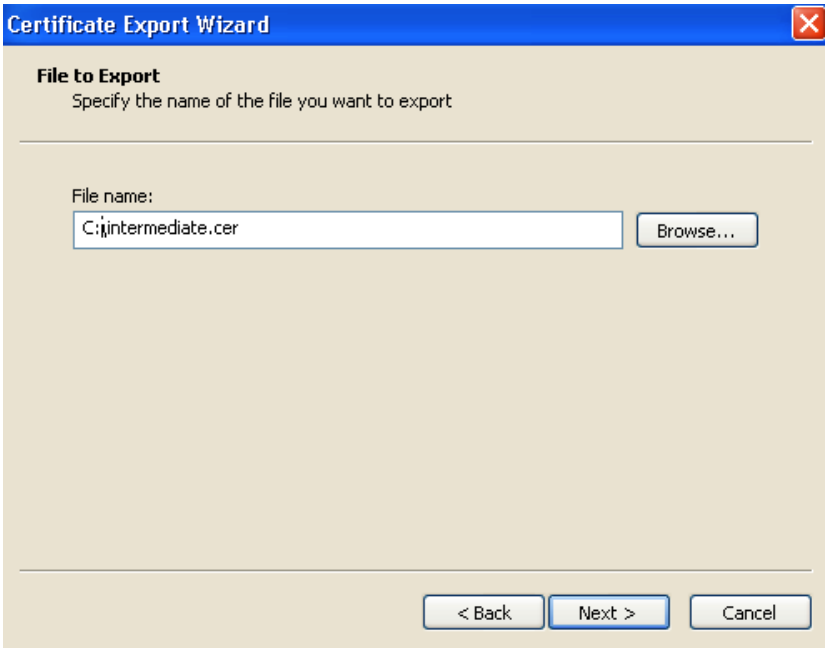
[証明書のエクスポートウィザードの開始(Welcome to the Certificate Export Wizard)] が表示されます。

ステップ 6　[次へ(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　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　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、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。

VCS Expressway X8.1 での証明書の設定が完了しました。

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

VCS Expressway X8.1 での信頼された CA 証明書リストの設定

新規インストールした VCS Expressway X8.1 では、信頼された CA 証明書リストに証明書がないため、次の 2 つの証明書を追加する必要があります。

- DST Root CA 証明書（WebEx クラウドのルート CA）
- サーバ証明書の発行元 CA の CA 証明書

VCS Expressway X8.1 への DST Root 証明書の追加

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）。

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

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　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 6　[参照（Browse）] をクリックし、ステップ 4 で保存した DST Root 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。

VCS Expressway X8.1 へのルート CA 証明書または中間 CA 証明書の追加

WebEx クラウドが VCS Expressway の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。

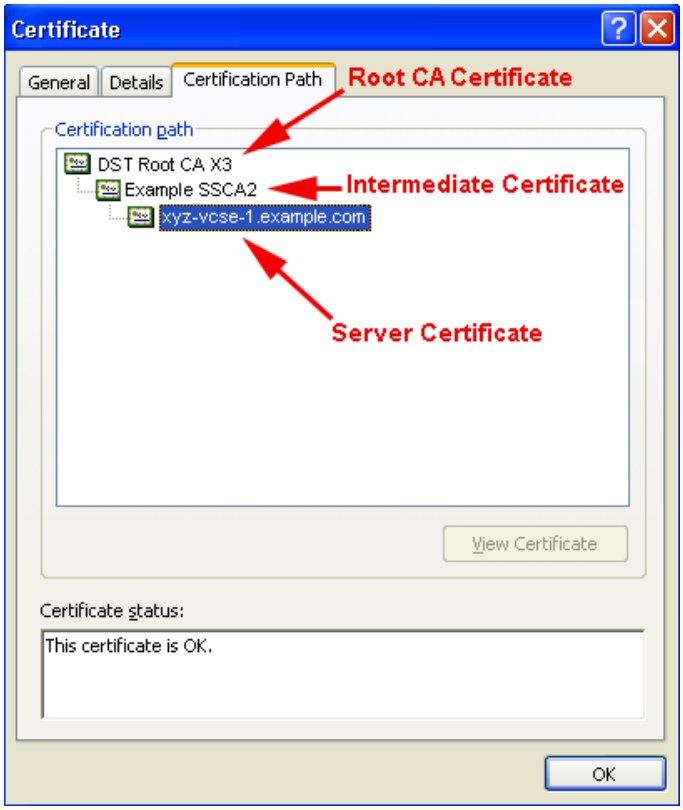
ロードする必要がある中間証明書またはルート証明書が公開 CA から提供されない場合、これらの証明書をサーバ証明書から取得できます。場合によっては、これは確実に正しい中間 CA 証明書をスタックできるより適切な方法です。

VCS Expressway X8.1 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。

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。（図 5-3 を参照）。

図 5-3　　.CER ファイル形式の中間 CA のサーバ証明書



コメント　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。

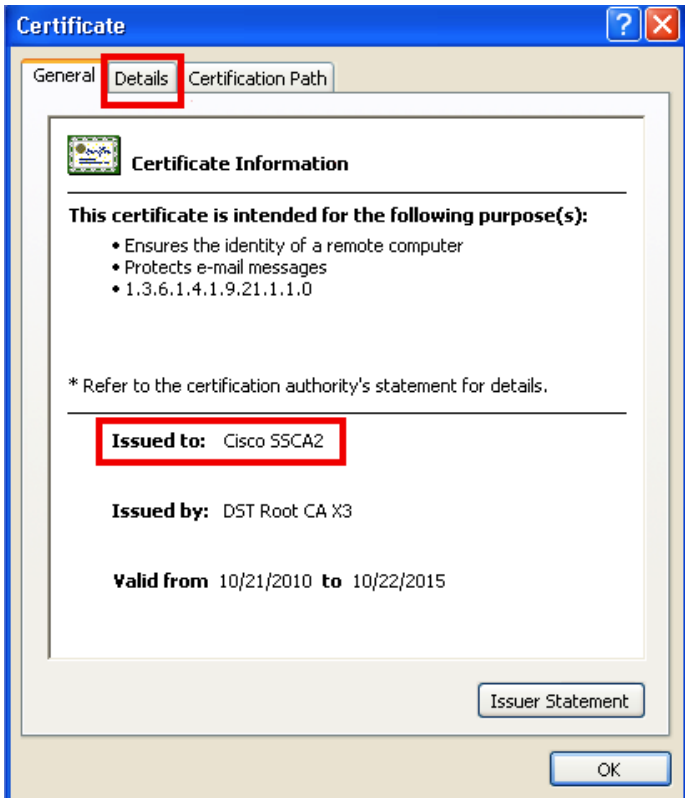
ステップ 3　CA 証明書を開きます。

- 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。

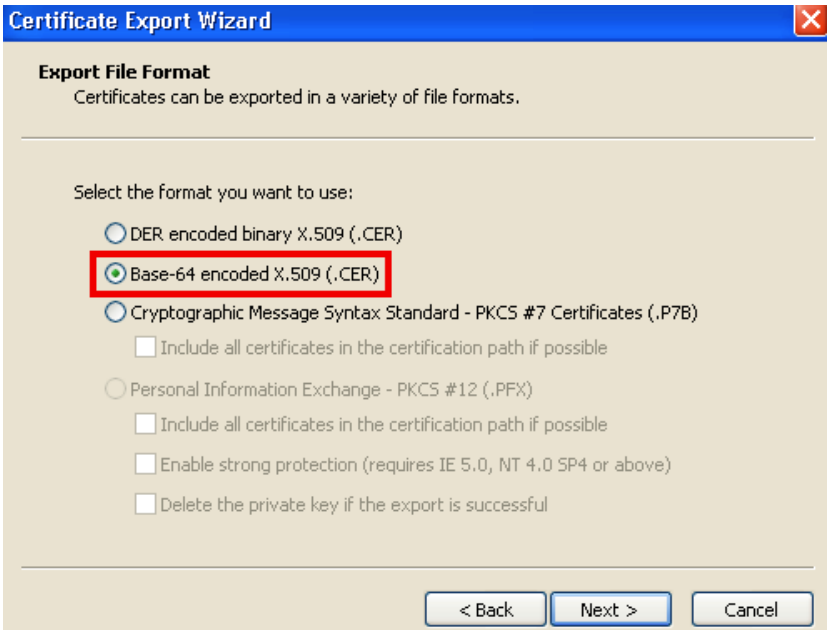
ステップ 5　[詳細（Details）] タブをクリックし、次に [ファイルにコピー...（Copy to File…）] をクリックします。



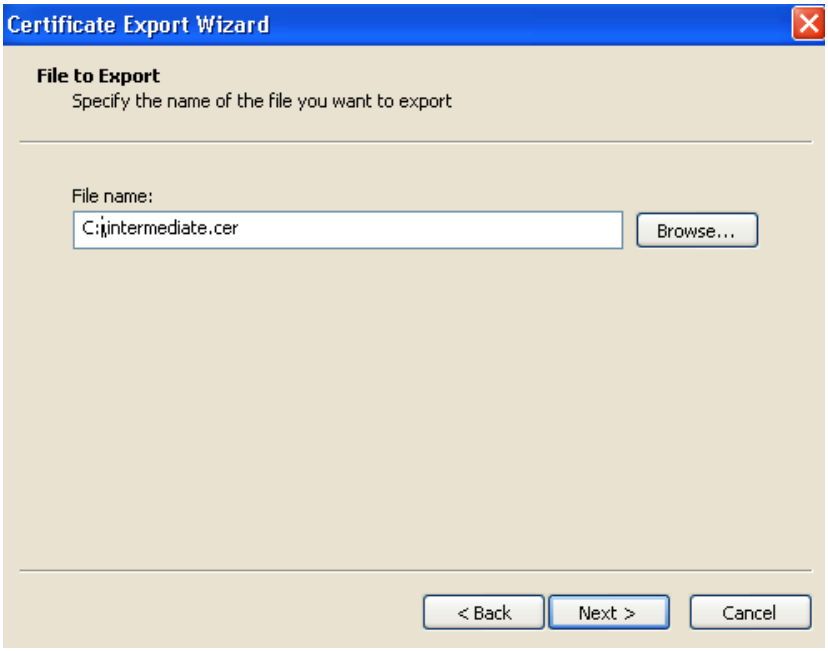
[証明書のエクスポートウィザードの開始(Welcome to the Certificate Export Wizard)] が表示されます。

ステップ 6　[次へ(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.pem** または **intermediate.pem**

ステップ 10　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。

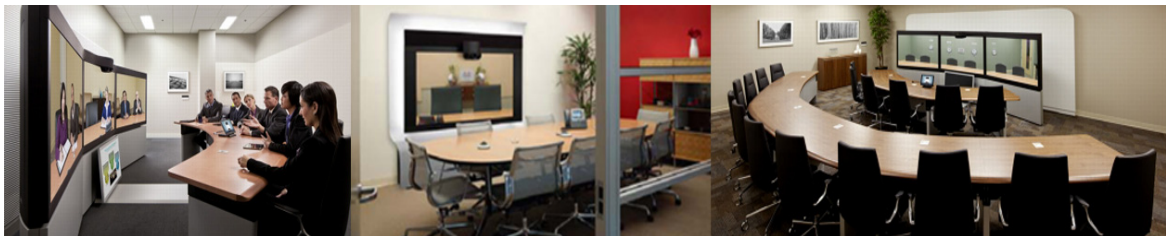
ステップ 11　[参照（Browse）] をクリックし、ルートまたは中間 CA 証明書を見つけ、[開く（Open）] をクリックします。

ステップ 12　[CA証明書の追加（Append CA certificate）] をクリックします。

VCS Expressway X8.1 での証明書の設定が完了しました。

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



CHAPTER 6

Cisco TelePresence Management Suite の設定

改訂日：2015 年 10 月

目次

この章では、Cisco WebEx Enabled TelePresence 会議用に Cisco TelePresence Management Suite（TMS）を設定する方法を説明します。次のような構成になっています。

- 前提条件（6-1 ページ）
- Cisco TMS での Cisco WebEx 機能の設定（6-2 ページ）
- Cisco TMS での WebEx ユーザの設定（6-4 ページ）
- Cisco TMS での MCU のハイブリッド コンテンツ モードの設定（6-8 ページ）
- Cisco TMS でのロビー画面の TelePresence Server の設定（6-8 ページ）
- Cisco TMS での会議の設定（6-9 ページ）
- Cisco TMS でのシングル サインオンの設定（6-12 ページ）
- TMS が WebEx ホスト代理としてスケジュールできる設定（6-19 ページ）

前提条件

- Cisco TMS ソフトウェア リリース 14.3.1 以降が必要です。
- 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 3.1 以降が必要です。

  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 1.1 以降が必要です。
- WebEx 機能を設定する前に、WebEx の統合オプション キーを Cisco TMS にインストールする必要があります。

コメント 複数の WebEx サイトがサポートされます。

- 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：Cisco WebEx Enabled TelePresence 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 TelePresence Management Suite の設定（6-1 ページ）を参照してください。

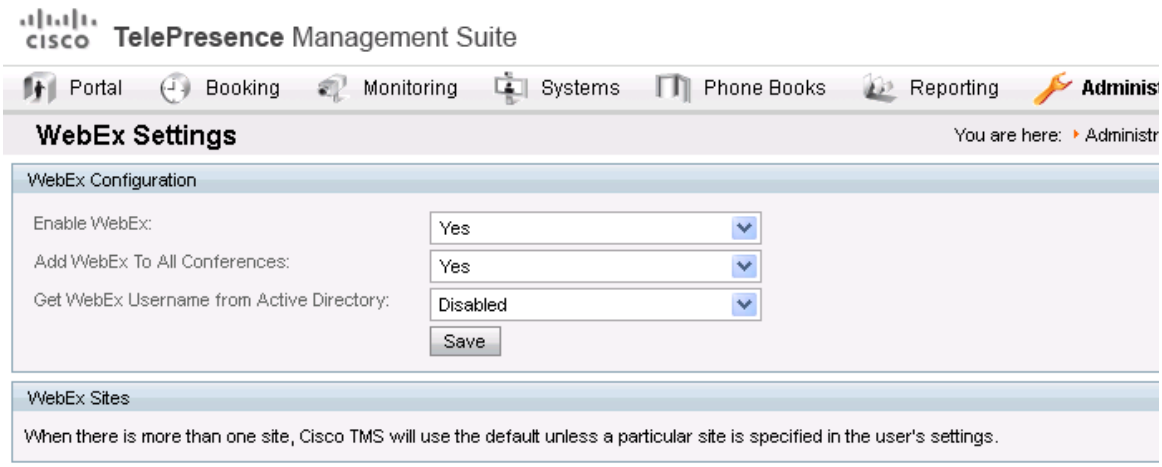
Cisco TMS での Cisco WebEx 機能の設定

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

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

[WebExの設定（WebEx Settings）] ページが表示されます。図 6-1を参照してください。

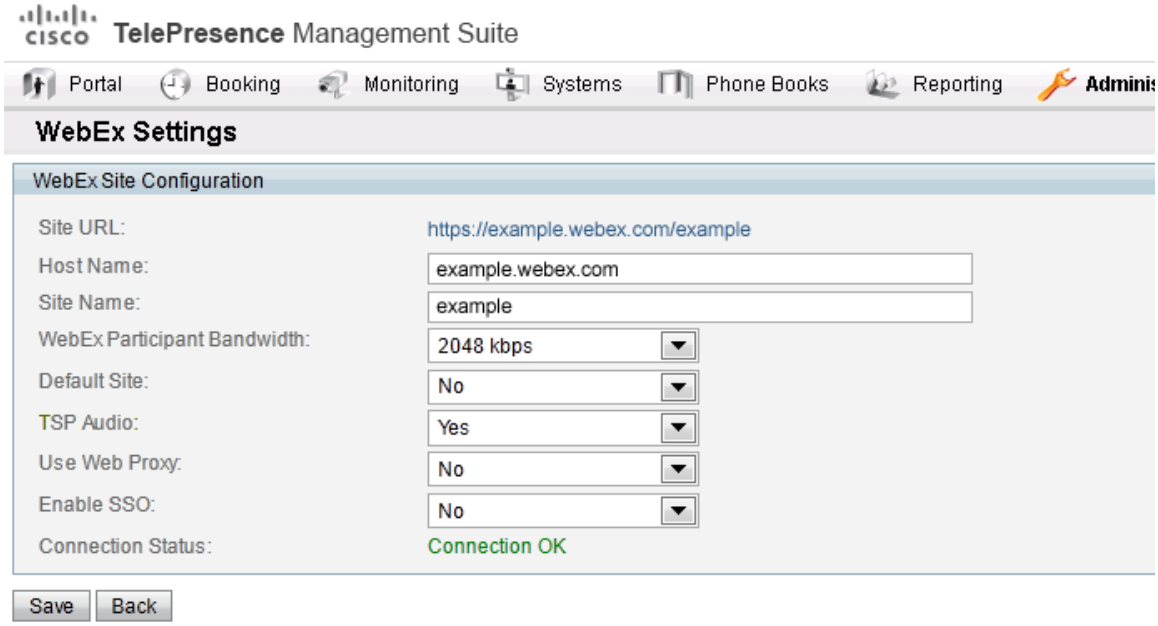
図 6-1　　Cisco TMS での WebEx の有効化



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 6-2を参照してください。

図 6-2　　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。

コメント　サイト URL の形式は **https://[HostName]/[SiteName]** でなければなりません。例：*https://example.webex.com/example*

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。

コメント　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。

コメント　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）] を [はい（Yes）] に設定します。

コメント　[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の設定（WebEx Configuration）]セクションで、次の手順を実行します。

a.　[WebEx有効（WebEx Enabled）] を [はい（Yes）] に設定します。

b. [すべての会議にWebExを追加(Add WebEx To All Conferences)] を [はい(Yes)] に設定します。

ステップ 10　[保存(Save)] をクリックします。

Cisco TMS での 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 対応の会議をスケジュールするには、Cisco TMS ユーザの次の情報が Cisco TMS ユーザ プロファイルに保存されている必要があります。

- 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

コメント　この WebEx サイトは、Cisco TMS での Cisco WebEx 機能の設定(6-2 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 ユーザの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 ユーザのプロファイルを編集する。

  詳細については、Cisco TMS での Cisco WebEx Enabled TelePresence ユーザの設定(6-6 ページ)を参照してください。

- 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（6-5 ページ）およびCisco TMS でのシングル サインオンの設定（6-12 ページ）を参照してください。

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。

ステップ 1　[管理ツール（Administrative Tools）] > [設定（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。

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。

[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 1　[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 2　[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 3　[保存(Save)] をクリックします。

詳細については、Cisco TMS の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 でのシングル サインオンの設定(6-12 ページ)を参照してください。

その他のフィールドは必須ではありませんが、他の Cisco TMS 機能に使用されます。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 WebEx Enabled TelePresence 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)] を有効に設定している場合(詳細についてはActive Directory からの自動ユーザ参照の設定(6-5 ページ)を参照)。
- 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 でのシングル サインオンの設定(6-12 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 WebEx Enabled TelePresence ユーザを設定するには、次の手順を実行します。

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。

コメント　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。

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。

コメント　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 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 での 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。

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

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)] 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。

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

ステップ 2　TelePresence Server 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)] 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 TelePresence Server に対してステップ 2 から 6 までを繰り返します。

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 Cisco WebEx Enabled TelePresence 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。

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

ステップ 2　MCU 名をクリックします。

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　[コンテンツモード(Content Mode)] を [ハイブリッド(Hybrid)] に設定し、[保存(Save)] をクリックします。

Cisco TMS でのロビー画面の TelePresence Server の設定

WebEx を使用した Cisco WebEx Enabled TelePresence 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。

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

ステップ 2　TelePresence Server 名をクリックします。

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、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 6-1 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、WebEx Enabled TelePresence 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 6-1　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	WebEx Enabled TelePresence 会議かどうか	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
×	×（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）
×	○	×	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）
×	○	○	×	WebEx 参加者のシルエット イメージ
×	○	○	○	WebEx 参加者のビデオ
○	×（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）
○	○	×	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）
○	○	○	×	WebEx 参加者のシルエット
○	○	○	○	WebEx 参加者のビデオ

Cisco TMS での会議の設定

ここでは、Cisco TMS で設定できる WebEx Enabled TelePresence 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。

デフォルトのセットアップ バッファとティアダウン バッファ

会議の TelePresence 部分がスケジュールされている時刻に開始および終了するように、デフォルトのセットアップ バッファとティアダウン バッファを設定しておくことを推奨します。

コメント　TMS を使用して会議をスケジュールするユーザは、必要に応じて会議ごとにセットアップ バッファとティアダウン バッファを変更できます。

Cisco TMS でデフォルトのセットアップ バッファとティアダウン バッファを設定するには、次の手順を実行します。

ステップ 1　[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] に進みます。

ステップ 2　[会議の作成（Conference Create）] セクションで次のように設定します。

- [デフォルトのセットアップ バッファ（Default Setup Buffer）] で [0] を選択します。
- [デフォルトのティアダウン バッファ（Default Tear Down Buffer）] で [0] を選択します。

ステップ 3　[保存（Save）] をクリックします。

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。

ステップ 1　[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] に進みます。

ステップ 2　[会議作成オプション（Conference Create Options）] セクションで次のオプションを設定します。

- [デフォルト画像モード（Default Picture Mode）] で、[分割表示（Continuous Presence）] を選択します。

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。

Cisco TMS で [会議接続/切断オプション（Conference Connection/Ending Options）] を設定するには、次の手順を実行します。

ステップ 1　[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] に進みます。

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

- [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。

コメント　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。

- [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。

  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

コメント　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。

- （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。
  - [メッセージのタイムアウト（秒）（Message Timeout (in seconds)）]：警告メッセージが表示される秒数。デフォルト設定：10 秒。
  - [終了X分前にメッセージを表示する（Show Message X Minutes Before End）]：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。

    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）。

コメント　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。

  - [会議延長のための連絡先（Contact Information to Extend Meetings）]：このフィールドでは、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　[保存（Save）] をクリックします。

Cisco TMS でのシングル 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。

コメント　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。

コメント　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。

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（6-2 ページ）を参照してください。

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（6-13 ページ）を参照してください。

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（6-17 ページ）を参照してください。

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（6-18 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。

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　証明書が .cer または .crt 形式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（6-18 ページ）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。

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（6-15 ページ）のステップ 10 のコマンドを使用して、PKCS#12 キーと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（6-18 ページ）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（6-15 ページ）のすべてのステップに従います。

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。

ステップ 1　OpenSSL を使用した証明書の生成（6-15 ページ）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（6-15 ページ）のステップ 8 を使用して、Base64 PEM エンコード バージョンの署名付き証明書を作成します。

ステップ 3　この署名付き証明書のファイル拡張子を .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（6-15 ページ）のステップ 10 のコマンドを使用して、PKCS#12 キーと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（6-18 ページ）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。

ステップ 1　OpenSSL を使用した証明書の生成（6-15 ページ）の手順を実行します。

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（6-18 ページ）で TMS に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。

1. 秘密キーを生成します。
2. 証明書署名要求（CSR）を生成します。
3. 認証局により CSR に署名してもらいます。
4. 署名証明書のファイル拡張子を .cer または .crt に変更し、WebEx Cloud Services チームに提供します。
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。
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。

OpenSSL を使用して証明書を生成するには、次の手順を実行します。

ステップ 1　Windows でコマンド プロンプトを開きます。

ステップ 2　openssl\bin インストール ディレクトリに移動します。

ステップ 3　次のコマンドを使用して秘密キーを生成します。

openssl genrsa -out tms-privatekey.pem 2048

ステップ 4　上記の秘密キーを使用して、証明書署名要求（CSR）を生成します。

openssl req -new -key tms-privatekey.pem -config openssl.cfg -out tms-certcsr.pem

ステップ 5　次の項目を含む、要求されたデータを入力します。

- 国
- 州または地域
- 組織名
- 組織ユニット
- 共通名（これは Cisco TMS のFQDN です）
- （任意）電子メール アドレス、パスワード、会社名

ステップ 6　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。
- OpenSSL を使用して証明書署名要求を自己署名するには、次のコマンドを使用します。**tms-certcsr.pem** は、PEM 形式での証明書署名要求です。**tms-certcsr.pem** は、PEM 形式での秘密キーです。**days** は、証明書の有効期間（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。
- 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 7　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。CA から署名証明書 **tms-cert.der** を受信します。

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、-----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 8　次の OpenSSL コマンドを使用して、署名付き証明書を .der から .pem に変換します。

openssl x509 -inform der -in tms-cert.cer -out tms-cert.pem

コメント　認証局が .pem 形式の署名証明書を提供する場合、このステップをスキップできます。

ステップ 9　この署名証明書のファイル拡張子を .cer または .crt に変更し、WebEx Cloud Services チームに提供します。

ステップ 10　ステップ 3 で作成した秘密キーと署名証明書 .pem を組み合わせます。

openssl pkcs12 -export -inkey tms-privatekey.pem -in tms-cert.pem -out tms-cert-key.p12 -name tms-cert-key

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。

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「WebEx サイトでのパートナー委任認証の有効化」セクション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（6-18 ページ）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

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。

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。

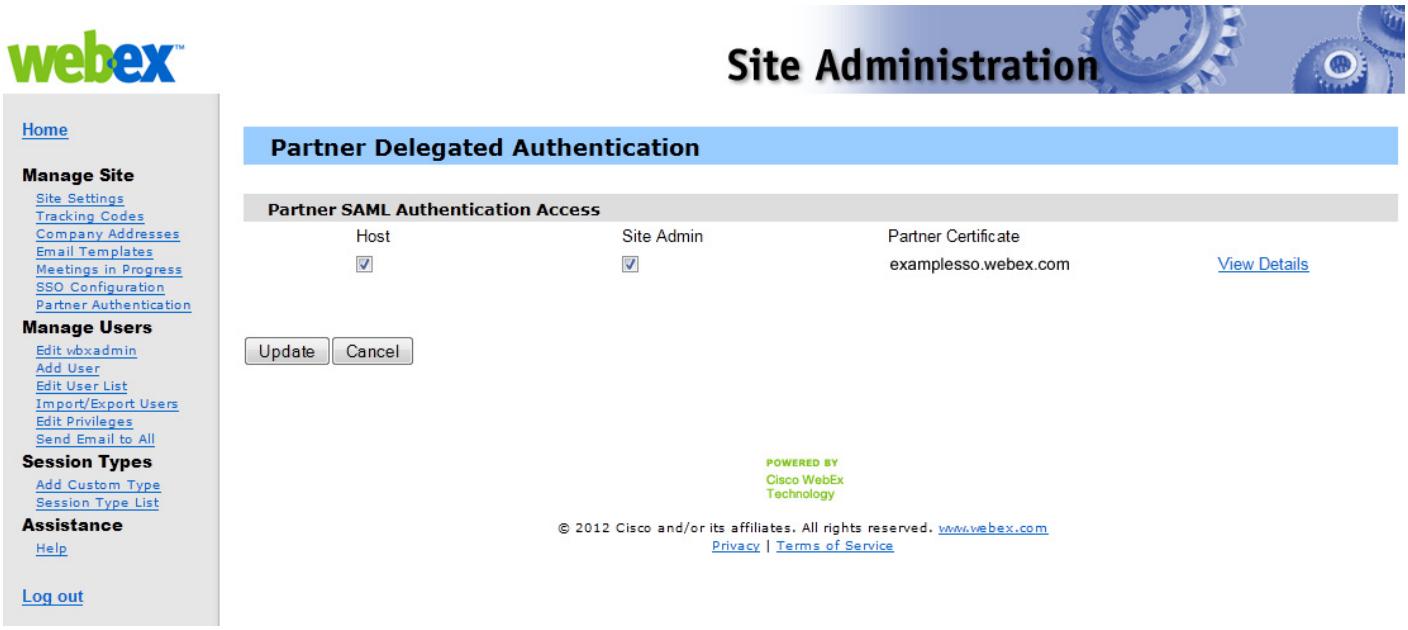
1. WebEx Cloud Services チームに対し、SAML 2.0 フェデレーション プロトコルに合わせて設定された TMS のパートナー証明書を追加すること要求します。
2. TMS の公開証明書を WebEx Cloud Services チームに提供します。ユーザの作成方法については、WebEx の証明書の生成（6-13 ページ）を参照してください。
3. WebEx Cloud Services チームから、このステップを完了したことが通知されたら、次の説明に従い、WebEx サイトの Site Administration のホスト アカウントと管理者アカウントの両方で、パートナー委任認証を有効にします。
4. 「Cisco TMS での SSO の有効化」に進みます。

WebEx サイトのパートナー委任認証を有効にするには、次の手順を実行します。

ステップ 1　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。

図 6-3　　WebEx 管理サイトでのパートナー委任認証



ステップ 2　[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

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

コメント　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（6-17 ページ）を参照してください。

Cisco TMS で SSO を有効にするには、次の手順を実行します。

ステップ 1　Cisco TMS にログインし、[管理ツール（Administrative Tools）] > [設定（Configuration）] > [WebExの設定（WebEx Settings）] の順に進みます。

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。

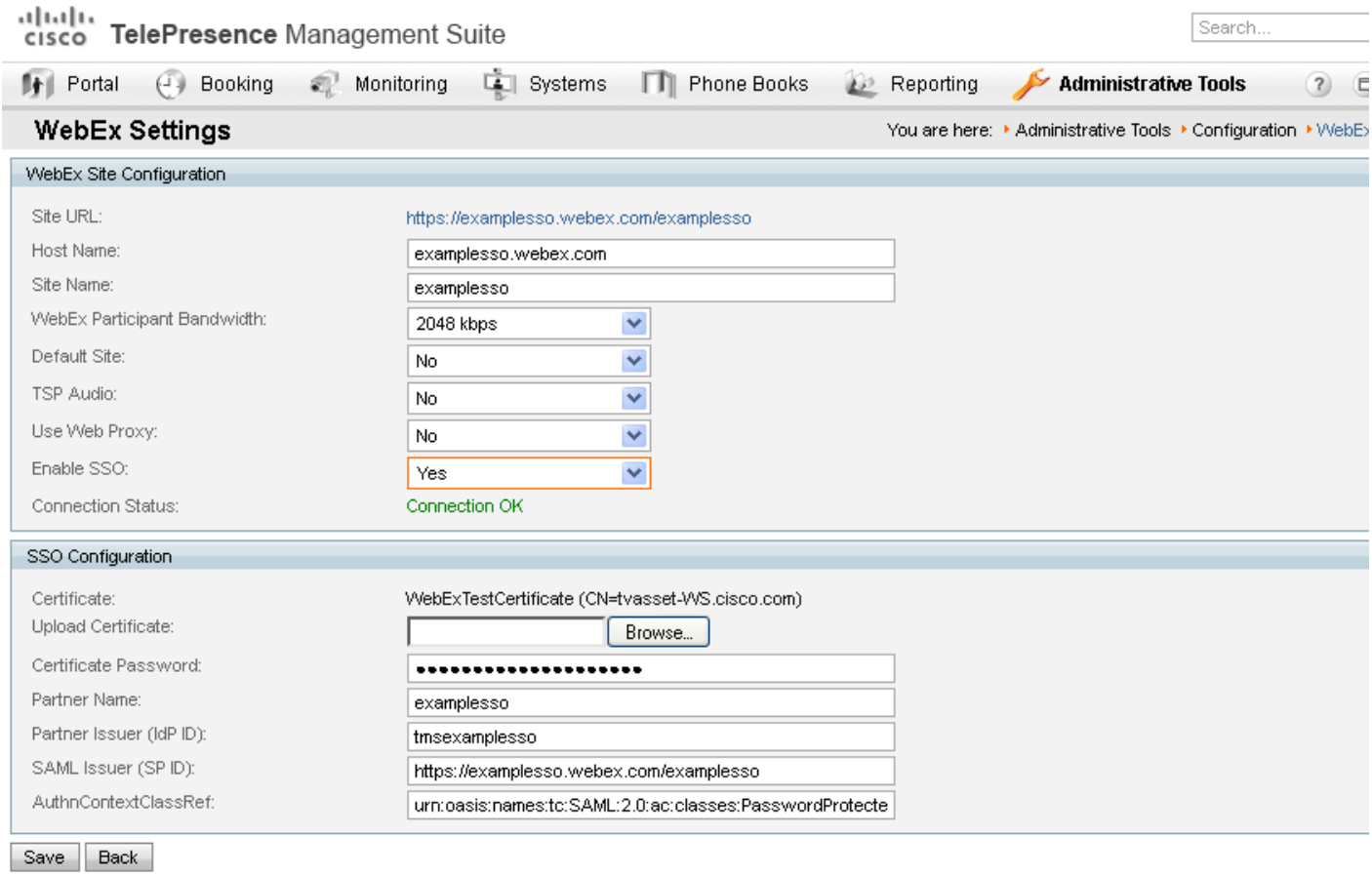
[SSO設定(SSO Configuration)] ペインが表示されます。

ステップ 4　[参照(Browse)] をクリックし、WebEx の証明書の生成(6-13 ページ)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 6-4　Cisco TMS の [WebExの設定(WebEx Settings)] の [SSO設定(SSO Configuration)]



TMS が WebEx ホスト代理としてスケジュールできる設定

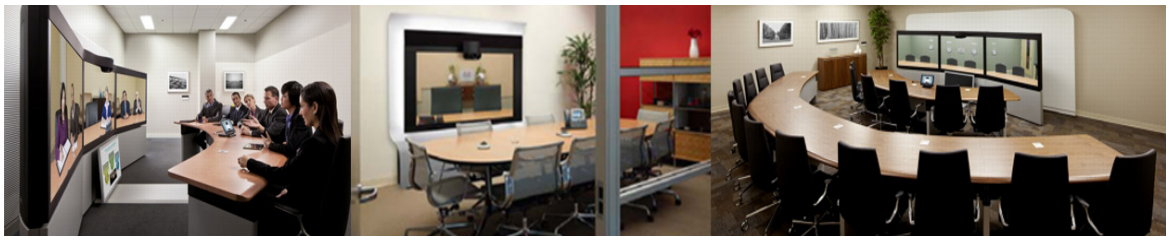
前の項では TMS での SSO の設定方法を中心に説明しましたが、WebEx サイト自体で SSO を設定することもできます。このため、WebEx Enabled TelePresence 会議のスケジュールでサポートされているすべての設定を理解しておくと便利です。

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。

1. WebEx サイトが SSO を使用せず、TMS では 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。

2. 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 サイトとのパートナー委任認証関係がある）
   - 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。
3. WebEx サイトが SSO を使用し、TMS で SSO が設定されている（WebEx サイトとのパートナー委任認証関係がある）
   - 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 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。



CHAPTER 7

Cisco TelePresence Management Suite Extension for Microsoft Exchange の設定

改訂日：2013 年 5 月

目次

この章では、WebEx and TelePresence Integration to Outlook と WebEx Scheduling Mailbox を使用して Cisco WebEx Enabled TelePresence 会議をスケジュールするために Cisco TelePresence Management Suite Extension for Microsoft Exchange（Cisco TMSXE）を設定する方法について説明します。次のような構成になっています。

- 前提条件（7-1 ページ）
- 展開のベスト プラクティス（7-2 ページ）
- TMSXE のスケジュール オプション（7-2 ページ）
- WebEx and TelePresence Integration to Outlook のための Cisco TMSXE の設定（7-2 ページ）
- WebEx Scheduling Mailbox のための Cisco TMSXE の設定（7-7 ページ）

前提条件

- Cisco TMSXE ソフトウェア リリース 3.1 以降が必要です。
- Cisco TMS ソフトウェア リリース 14.2 以降が必要です。
- Cisco WebEx Enabled TelePresence 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、社内の 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 のインストールと設定の詳細については、『Cisco TelePresence Management Suite Extension for Microsoft Exchange Installation Guide - Version 3.1.2』を参照してください。

TMSXE のスケジュール オプション

TMSXE では、スケジュールのオプションが 2 つあります。

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

  Microsoft Outlook で [WebEx会議オプション（WebEx Meeting Options）] パネルを使用して、会議に WebEx を追加します。

- WebEx Scheduling Mailbox の使用

  特別な招待先（WebEx メールボックス）を含めることによって、電子メール クライアントから WebEx を会議への招待状に直接追加します。

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 をインストールします。
- WebEx サイトと TMSXE 間の通信をセットアップします。

Cisco TMS Booking Service のインストール

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。

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。

コメント　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。

警告　**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：

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。

IIS7（Windows Server 2008）への公開ルート証明書のインストール

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）:

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。

ステップ 4　[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 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。

SSL サーバ証明書のインストール:

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 TMSXE 間の通信の設定

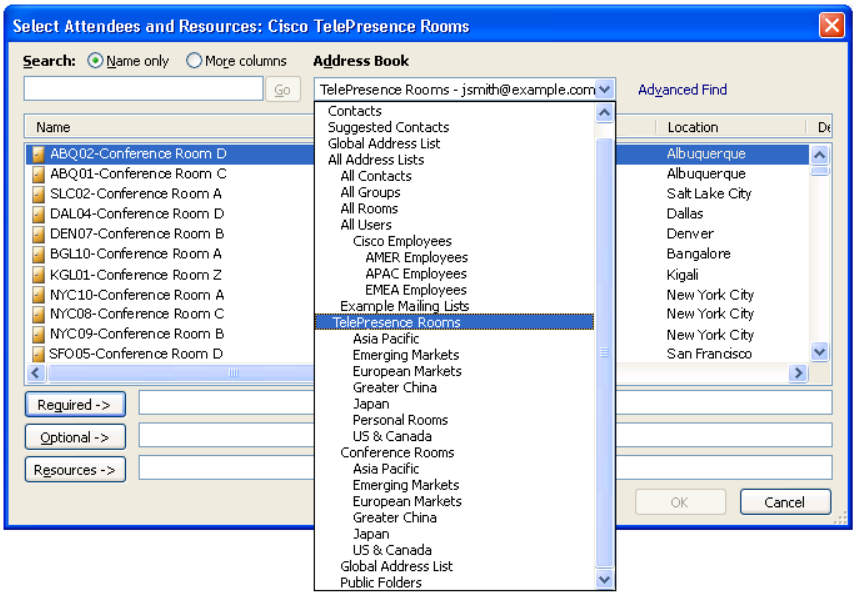
Cisco TelePresence Cisco WebEx の統合オプション（10-2 ページ）の手順に従ってください。

Outlook で TelePresence 会議室に表示されるロケーションの設定

Outlook で WebEx Enabled TelePresence 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（図 7-1、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（図 7-2、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。

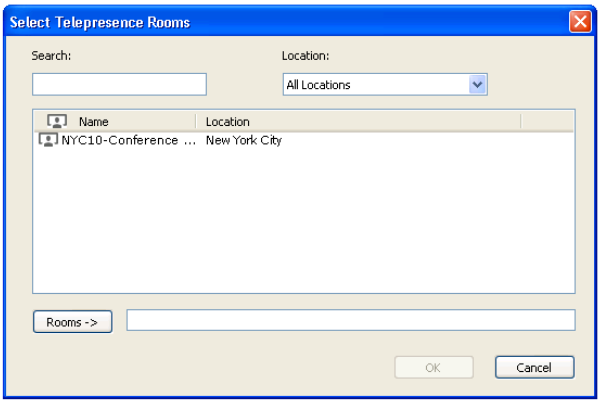
- [出席者とリソースの選択（Select Attendees and Resources）] - [アドレス帳（Address Book）] ウィンドウを表示するには、[会議（Meeting）] ウィンドウで [宛先...（To...）] ボタンをクリックします。

図 7-1　[出席者とリソースの選択(Select Attendees and Resources)] - [アドレス帳(Address Book)]



- [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。

図 7-2　テレプレゼンス会議室の選択(Select Telepresence Rooms)



[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、図 7-1 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。

Exchange の [アドレス帳(Address Book)] ドロップダウン メニューに表示される構造と階層(図 7-1)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、第 10 章「Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合」の「WebEx and TelePresence Integration to Outlook のインストール（10-6 ページ）」を参照してください。

WebEx Scheduling Mailbox のための Cisco TMSXE の設定

WebEx Scheduling Mailbox を使用したスケジュールのために Cisco TMSXE を設定するには、次の手順を実行する必要があります。

1. Microsoft Exchange で WebEx メールボックスを設定します。
2. WebEx メールボックスを Cisco TMSXE に追加します。

Microsoft Exchange で WebEx Scheduling Mailbox を設定します。

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。

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

Cisco TMSXE に WebEx メールボックスを追加するには、次の手順を実行します。

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。

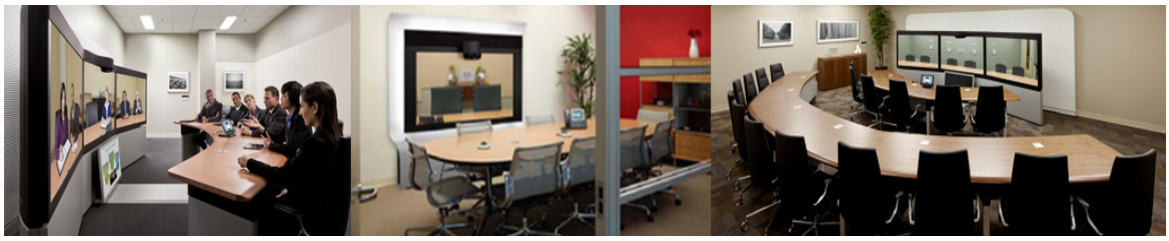
- Exchange 管理コンソールの [メールフローの設定（Mail Flow Settings）] または Powershell を使用して、必要に応じてメッセージ配信制限を強化します。

  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。



CHAPTER 8

Cisco TelePresence Management Suite Provisioning Extension の設定

改訂日：2013 年 11 月

目次

この章では、Smart Scheduler を使用して Cisco WebEx Enabled TelePresence 会議をスケジュールするために Cisco TelePresence Management Provisioning Extension（Cisco TMSPE）を設定する方法を説明します。次のような構成になっています。

- 前提条件（8-1 ページ）
- はじめに（8-2 ページ）
- Cisco TMSPE へのユーザ アクセス（8-2 ページ）
- Smart Scheduler のしくみ（8-3 ページ）
- 制限事項（8-4 ページ）

前提条件

- Cisco TMS ソフトウェア リリース 14.2 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 1.1 以降が 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。
  - 詳細については、『Cisco TelePresence Management Suite Provisioning Extension Deployment Guide』を参照してください。
- 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。

コメント　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。

TMS の設定については、「Cisco TelePresence Management Suite の設定」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。
  - Internet Explorer バージョン 9 以降
  - Mozilla Firefox バージョン 10 以降
  - Safari バージョン 6 以降
  - Chrome バージョン 24 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。

コメント　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/

例: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。

図 8-1　　Cisco TMS ポータル アイコン

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 へのアクセスは、Cisco TMS へのアクセスと同じです。

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。

コメント　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

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。
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。
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。

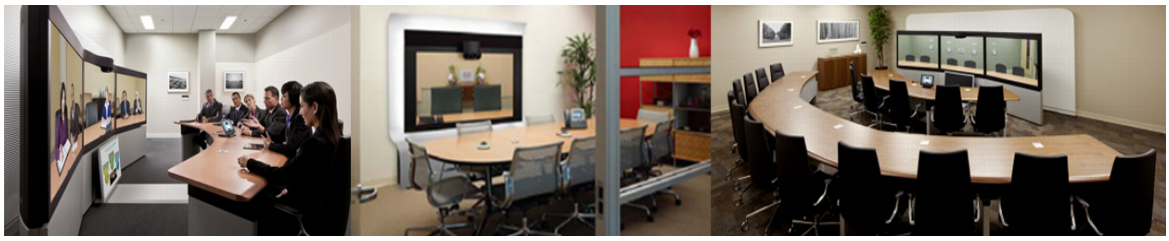
   Cisco TMSPE ユーザが Cisco TMS にまだ存在しない場合は、予約と同時にそれが作成されます。

4. 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。
- Smart Scheduler には、Cisco TMS スケジューリングでのセットアップおよびティアダウンバッファの使用との互換性がありません。これは、Cisco TelePresence Management Suite Extension Booking API の制限事項です。



CHAPTER 9

音声の設定

改訂日：2013 年 11 月

目次

この章では、Cisco WebEx Enabled TelePresence の音声を設定する方法について説明します。

次のセクションで音声機能の展開シナリオについて説明します。

- Cisco WebEx Enabled TelePresence の SIP 音声の設定（9-2 ページ）
- Cisco WebEx Enabled TelePresence の PSTN 音声の設定（9-3 ページ）
- Cisco WebEx Enabled TelePresence の TSP 音声の設定（9-8 ページ）

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。

- VCS Control/Expressway を設定する必要があります。

  詳細については、第 4 章「Cisco TelePresence Video Communication Server Control と Expressway の設定」を参照してください。
- Unified CM を使用する場合は、次の点を確認します。
  - Unified CM と Cisco VCS Control の間で SIP トランクを設定されていること。

  詳細については、Unified CM と VCS Control 間の SIP トランクの設定（4-5 ページ）を参照してください。
  - リージョンが G.711 に対応して設定されていること。
- PSTN 音声を設定する場合は、VCS または Unified CM 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 CM 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 CM 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。

コメント　現在、Cisco Conductor はサポートされていません。

Cisco WebEx Enabled TelePresence の SIP 音声の設定

ここでは、Cisco WebEx Enabled TelePresence の 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
- WebEx サイトでのハイブリッド音声の有効化（9-3 ページ）

コメント　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。

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。

[WebExの設定（WebEx Settings）] ページが表示されます。

ステップ 3　設定する 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）] ページが表示されます。

ステップ 4　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 5　[TSP音声（TSP Audio）] で [いいえ（No）] を選択します。

ステップ 6　[保存（Save）] をクリックします。

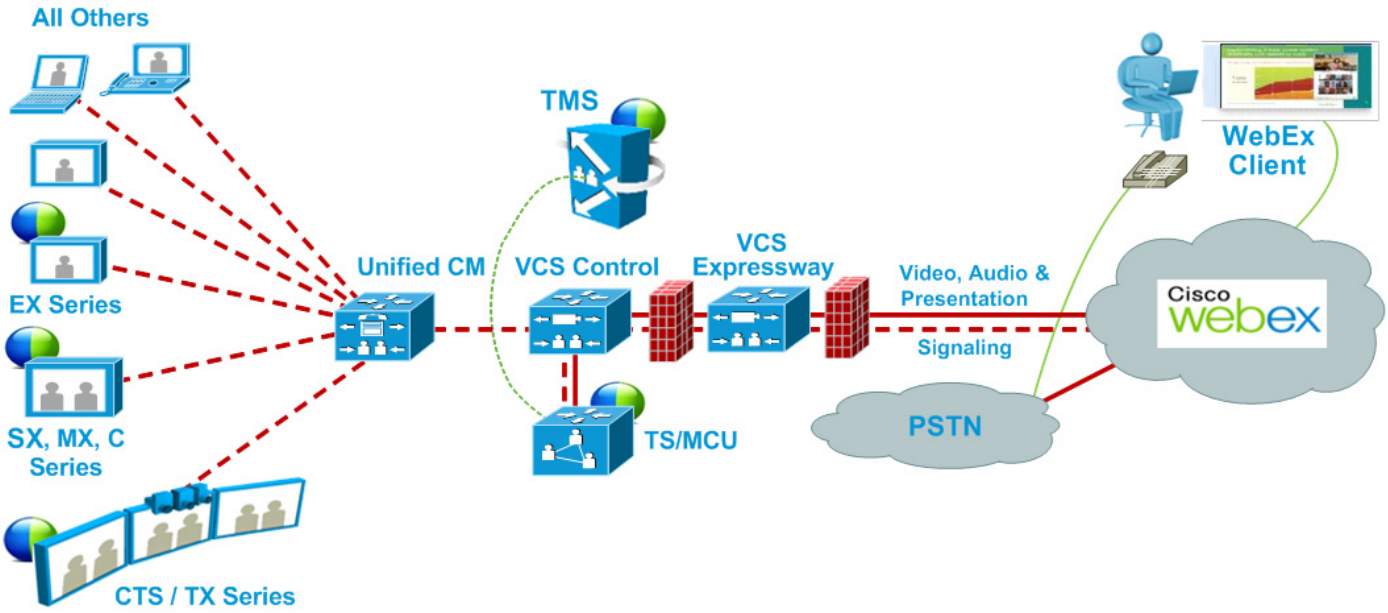
WebEx サイトでのハイブリッド音声の有効化

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://support.webex.com/MyAccountWeb/GPLWebForm.do

図 9-1　　Unified CM 登録エンドポイントを使用した SIP 音声機能の展開



Cisco WebEx Enabled TelePresence の PSTN 音声の設定

ここでは、Cisco WebEx Enabled TelePresence の 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
- WebEx サイトでのハイブリッド モードの有効化（9-4 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（9-4 ページ）

コメント　Cisco WebEx Enabled TelePresence 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 または Unified CM 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。

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。

[WebExの設定（WebEx Settings）] ページが表示されます。

ステップ 3　設定する 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）] ページが表示されます。

ステップ 4　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 5　[TSP音声（TSP Audio）] で [はい（Yes）] を選択します。

ステップ 6　[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 CM 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。

- 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（9-5 ページ）
- Unified CM 登録 PSTN ゲートウェイをパススルーする PSTN コールの設定（9-6 ページ）

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。

ステップ 1　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。

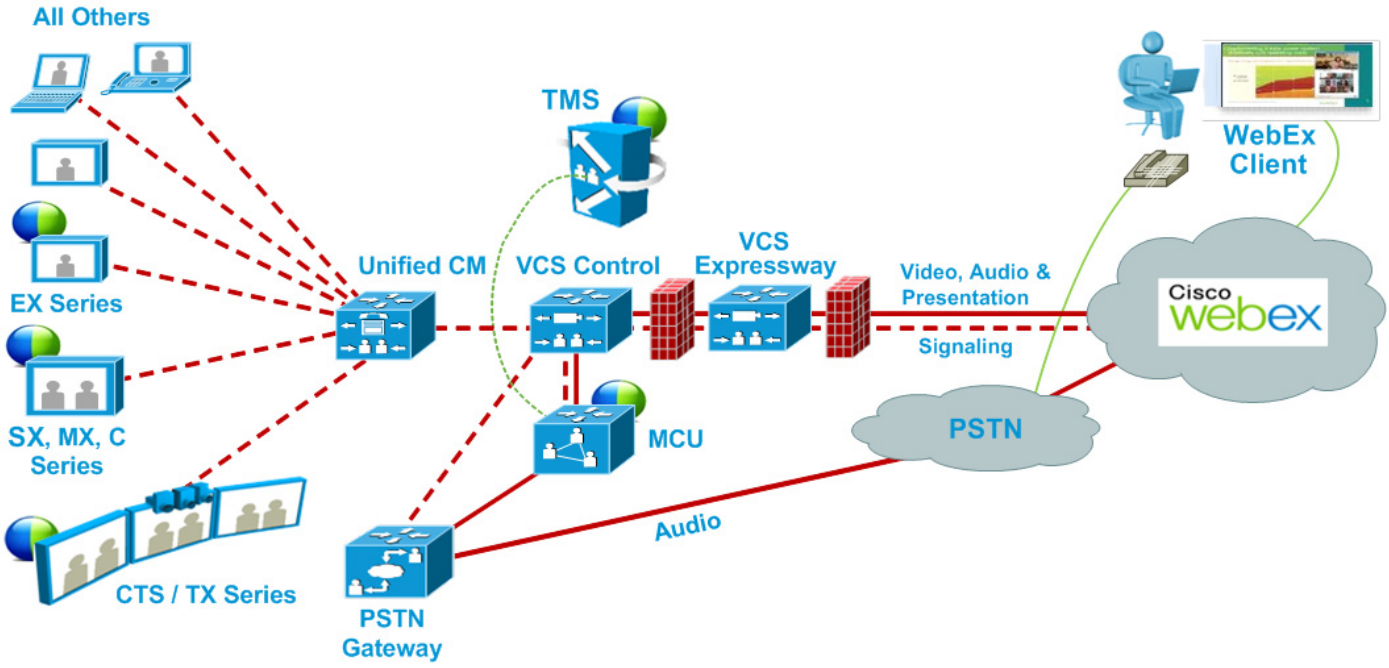
次の例では、**+14085551212@example.webex.com** が、正規表現パターン タイプを使用して **9#14085551212@example.webex.com** に変換されます。

- 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、次の『Cisco TelePresence Video Communication Server Basic Configuration（Control with Expressway）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_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-2.pdf

図 9-2　VCS 登録ゲートウェイと Unified CM 登録エンドポイントを使用した PSTN 音声機能の展開



ISDN ゲートウェイ用の VCS Control 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、VCS Control でインターワーキング設定を行う必要があります。

コメント　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 VCS Control を設定するには、次の手順を実行します。

ステップ 1　VCS Control にログインします。

ステップ 2　[VCS設定（VCS Configuration）] > [プロトコル（Protocols）] > [相互接続（Interworking）] に進みます。

ステップ 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。

コメント　この設定を保存するには、オプション キーが必要です。

Unified CM 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 CM 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。

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 CM 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 CM で、Unified CM 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。

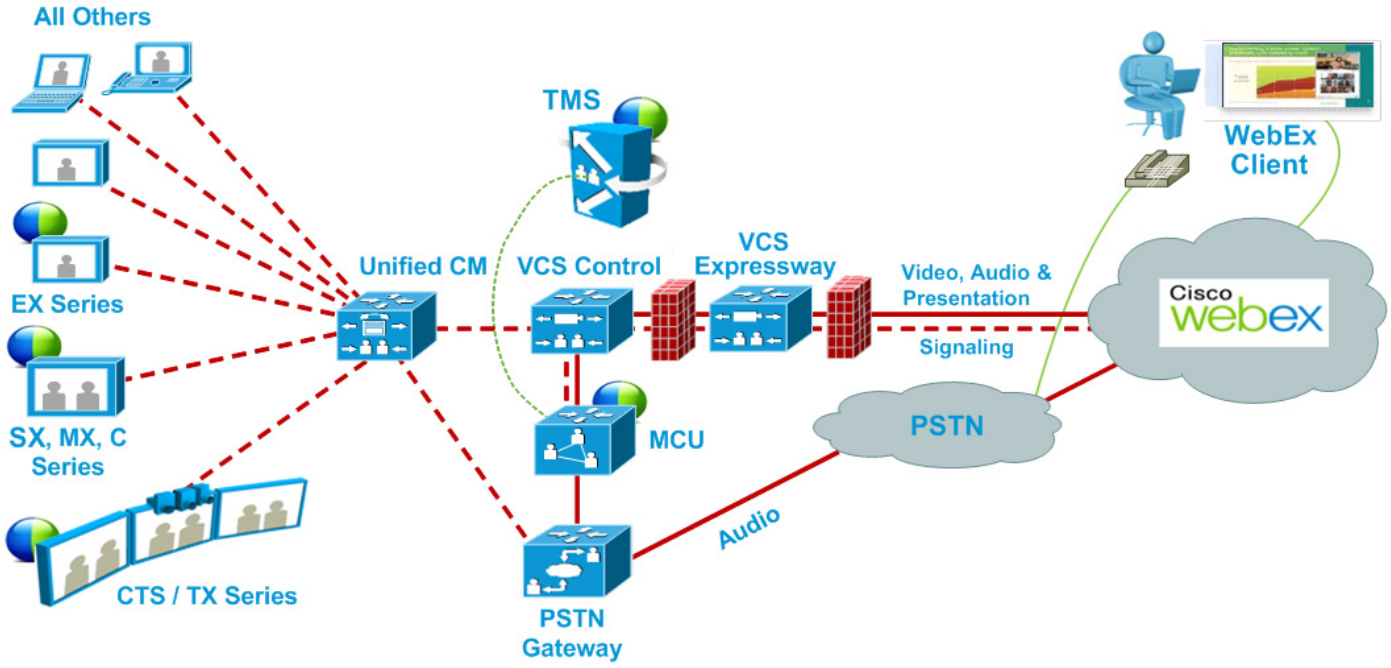
VCS での検索ルールの設定の詳細については、次の『Cisco TelePresence Video Communication Server Basic Configuration（Control with Expressway）Deployment Guide』を参照してください。

https://www.cisco.com/en/US/docs/telepresence/infrastructure/vcs/config_guide/Cisco_VCS_Basic_Configuration_Cisco_VCS_Control_with_Cisco_VCS_Expressway_Deployment_Guide_X7-2.pdf

Unified CM 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 CM 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

図 9-3　Unified CM 登録エンドポイントとゲートウェイを使用した PSTN 音声機能の展開



ISDN ゲートウェイ用の VCS Control 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、VCS Control でインターワーキング設定を行う必要があります。

コメント　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 VCS Control を設定するには、次の手順を実行します。

ステップ 1　VCS Control にログインします。

ステップ 2　[VCS設定（VCS Configuration）] > [プロトコル（Protocols）] > [相互接続（Interworking）] に進みます。

ステップ 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。

コメント　この設定を保存するには、オプション キーが必要です。

VCS と MCU/TelePresence Server の発信ダイヤル設定の確認

発信ダイヤルが正しく設定されていることを確認するには、次の手順を実行します。

ステップ 1　発信した直後に、VCS Control で [状態（Status）] > [履歴の検索（Search history）] の順に移動します。

ステップ 2　この発信が検索履歴に表示されているか確認します。

a. 発信がここに表示されなければ、MCU は発信していません。MCU で SIP/H323 ログを有効にします。もう一度発信し、SIP/H323 ロギングを停止して、ログをダウンロードします。

b. 発信がここに表示されたら、アクション ヘッダーの下でこの発信の表示をクリックします。詳細な検索履歴が表示されます。

ステップ 3　詳細な検索履歴の最初のサブ検索では、トランスフォームを表示する必要があります。この下に一覧表示される値は、トランスフォームが実行された後に呼び出す URI です。以降では、外部発信用のゾーン（通常は Unified CM）を指すサブ検索をする必要があります。ここに一覧表示されるエイリアスは、発信相手側にそのまま示されます。相手がこの形式の発信を期待していること（「+」文字などの相手側がサポートしていない文字がいずれも含まれないこと）を確認します。

ステップ 4　相手側の検索で「Found: False」と表示された場合は、原因を確認します。原因が「見つかりません（Not Found）」である場合は、発信相手は 404 を返送します。この場合は、次のことを確認します。

a. VCS が、発信相手が期待している URI を正確に渡していること

b. 発信相手が発信を許可するように設定されていること

Cisco WebEx Enabled TelePresence の TSP 音声の設定

Telephony Service Provider（TSP）音声機能を展開するには、PSTN 音声が必要です。「Cisco WebEx Enabled TelePresence の PSTN 音声の設定」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。

コメント　TSP プロバイダーはコールイン ユーザ マージをサポートする必要があります。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。

TSP 音声の設定には、次の 4 つの設定が必要です。

- MACC ドメイン インデックスおよびオープン TSP 会議室の WebEx の設定
- TSP ダイヤル文字列の設定
- 電話会議の開始方法の設定
- 会議主催者の TSP 音声の設定

詳細については、次のマニュアルを参照してください。

- TSP 音声の設定と会議の概要

コメント　TSP 音声を使用するには、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、MCU/TS が発信コールを実行できる必要があります。MCU/TS が発信できることを確認するには、セクション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（9-5 ページ）を参照してください。

MACC ドメイン インデックスおよびオープン TSP 会議室の WebEx の設定

WebEx Cloud Services がこれらの設定を行う必要があります。詳細については、WebEx Cloud Services にお問い合わせください。

TSP ダイヤル文字列の設定

TSP 音声を使用する会議中、TelePresence 機器は TSP パートナーのブリッジに発信し、メニュー階層を移動して電話会議に接続します。音声（IVR）プロンプトは、各 TSP プロバイダーによって異なります。その結果、DTMF のダイヤル文字列を作成する必要があります。

DTMF ダイヤル文字列

固定の DTMF ダイヤル文字列は、TSP 音声プロバイダーによって作成およびテストされ、Cisco WebEx クラウド サービスに提供される必要があります。その後、WebEx クラウド サービスが WebEx クラウドで WebEx サイト用にダイヤル文字列パラメータを設定します。次に、提供する必要があるシーケンスの例を示します。

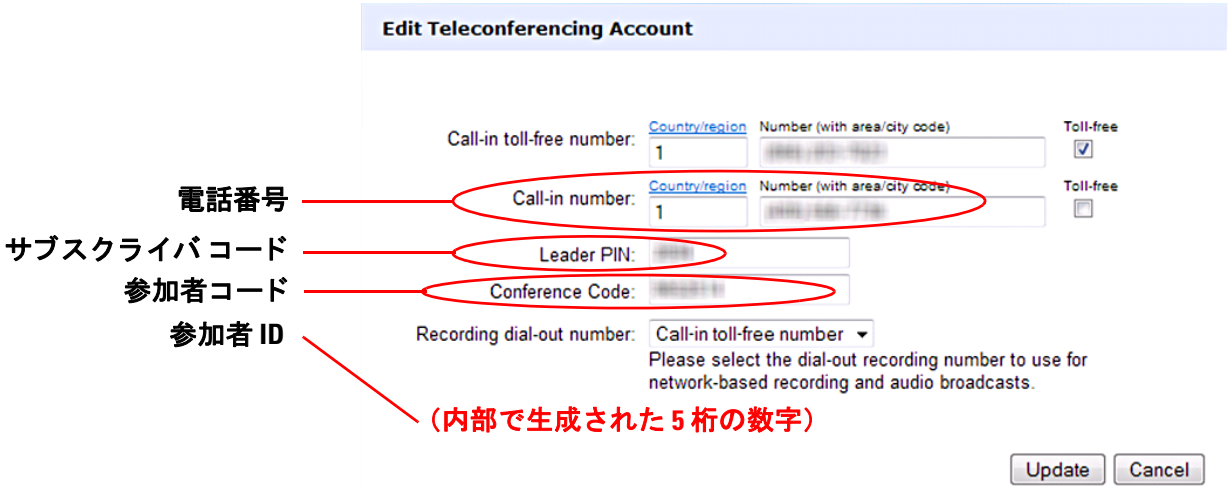
1. MCU/TelePresence Server が電話番号を発信します
2. 2 秒間、休止します
3. [参加者コード] DTMF 値（例：12345678）を入力します
4. # を入力します。
5. 6 秒間、休止します
6. # を入力します。
7. 25 秒間、休止します
8. #1 を入力します。
9. 1 秒間、休止します。
10. [参加者 ID] DTMF 値（例：44356）を入力します。

詳細については、Cisco WebEx クラウド サービスにお問い合わせください。

ダイヤル文字列に使用できる変数

TSP 音声プロバイダーにより作成され、WebEx Cloud Services により設定される DTMF ダイヤル文字列で使用できる変数を次に示します。

図 9-4　　WebEx ホスト アカウント/TSP 音声アカウント



電話会議の開始方法の設定

通常、TSP プロバイダーは WebEx ホストがコールするまで待った後で、電話会議を開始します。

ホストが（ホスト キーを入力して）ダイヤルインするまで、参加者は待合室で待機します。ホストが遅れたりダイヤルインしないで WebEx からロック解除したりした場合は、会議はロック解除されません。

待合室があるかどうかについては、TSP プロバイダーに問い合わせてください。待合室がある場合は、会議を確実に開く方法が 2 通りあります。

- **方法 1**：ホストとして会議に入室し、会議をロック解除する MCU/TelePresence Server 用の DTMF ダイヤル文字列を設定します。
  - WebEx クラウド サービスは TSP パートナーと連動して、適切な DTMF ダイヤル文字列を作成します。
  - WebEx ホストがすでに会議に入室している場合は、会議参加者に MCU/TelePresence Server の DTMF ダイヤル文字列が聞こえます。

コメント　DTMF ダイヤル文字列は、ホストとして会議に入室する MCU/TelePresence Server のダイヤル文字列を設定しているかどうかに関係なく、必要です。詳細については、WebEx Cloud Services にお問い合わせください。

- **方法 2**：WebEx TSP サーバが API コマンド **W2A_UpdateConference=2** を TSP パートナーのブリッジに送信し、会議をロック解除します。
  - 会議ロック解除コマンドを認識して正しく実行するために、TSP パートナーは TSP アダプタを再作成しなければならない場合があります。この API コマンドに対応しているかどうかについては、TSP プロバイダーにお問い合わせください。

TSP の統合方法が発信シナリオに与える影響

次の表に、一般的なシナリオと会議を開く方法による結果を示します。

表 9-1　　シナリオと TSP で使用する方法による結果

シナリオ	想定される結果	方法 1 を使用する場合	方法 2 を使用する場合
MCU/TelePresence Server が音声会議にコールする最初の発信者である場合	正常に参加	MCU/TelePresence Server は TSP 音声会議でホストの役割を担います。	MCU/TelePresence Server は音声会議でホストの役割を担いません。
MCU/TelePresence Server がダイヤルインする前に、1 人以上の参加者がすでに音声会議（待合室）に参加している場合。	正常に参加	MCU/TelePresence Server は TSP 音声会議でホストの役割を担います。	MCU/TelePresence Server は音声会議でホストの役割を担いません。
MCU/TelePresence Server がダイヤルインする前に、ホストがすでに音声会議に参加している場合。	正常に参加	音声会議にすでに参加しているユーザには、音声会議で「追加の」DTMF トーンが聞こえることがあります。これは、ホストのように動作する DTMF シーケンスに続く MCU/TelePresence Server です。	このような追加の DTMF トーンは聞こえません。
ホスト（MCU/TelePresence Server がダイヤルインする前にすでに音声会議に参加しているホスト）が、会議の進行中に切断する場合。	可変	音声会議が終了することがあります。TSP 実装によって異なります（終了しないこともあります）。会議退席時の WebEx GUI でのホストの選択（会議を継続するオプション）に応じて異なります。	方法 2 が使用されているため、パートナーは次のいずれかが発生するまで会議を継続する必要があります。 a. すべての参加者が会議を退席する、または b. TSP API が W2A_CloseConference を送信する
DTMF の障害	参加失敗		
MCU/TelePresence Server がダイヤルインする前にホストは WebEx 経由で会議に参加し、WebEx GUI を使用して会議をロックします。 （この場合 WebEx はホストによる会議のロックに従うことをすでに決定しています。）	参加失敗	MCU は参加できません。	MCU/TelePresence Server は参加できません。

会議主催者の TSP 音声の設定

TSP 音声を使用する WebEx Enabled TelePresence 会議をスケジュールする必要がある会議主催者は、WebEx サイトにログインし、TSP 音声を使用するよう自分のアカウントを設定する必要があります。これは 1 回限りの設定です。

前提条件

会議主催者には、TSP 音声サービス プロバイダーから提供される次の情報が必要です。

- コールイン番号（フリーダイヤル）
- コールイン番号
- ホスト アクセス コード
- 参加者アクセス コード

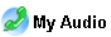
TSP 音声の設定

TSP 音声を設定するには、次の手順を実行します。

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　ページ上部の [My WebEx] をクリックします。 

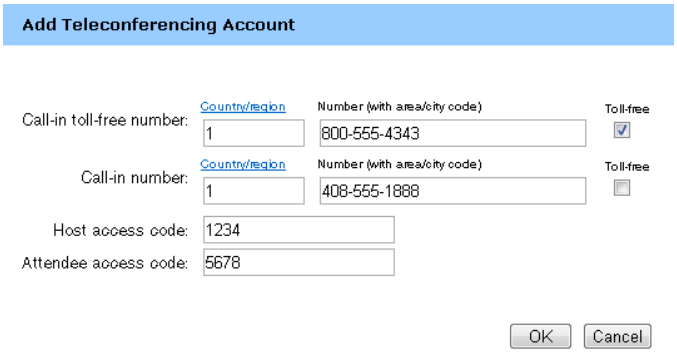
ステップ 3　WebEx アカウントのユーザ名とパスワードを入力し、[ログイン（Log In）] をクリックします。

ステップ 4　ページ左側の [マイオーディオ（My Audio）] をクリックします。 

ステップ 5　電話会議サービス アカウントのセクションで、[アカウントを追加（Add account）] をクリックします。

ステップ 6　[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、ホストおよび参加者の適切な電話番号とアクセス コードを入力します。

図 9-5　　[電話会議アカウントの追加（Add Teleconferencing Account）] ウィンドウ

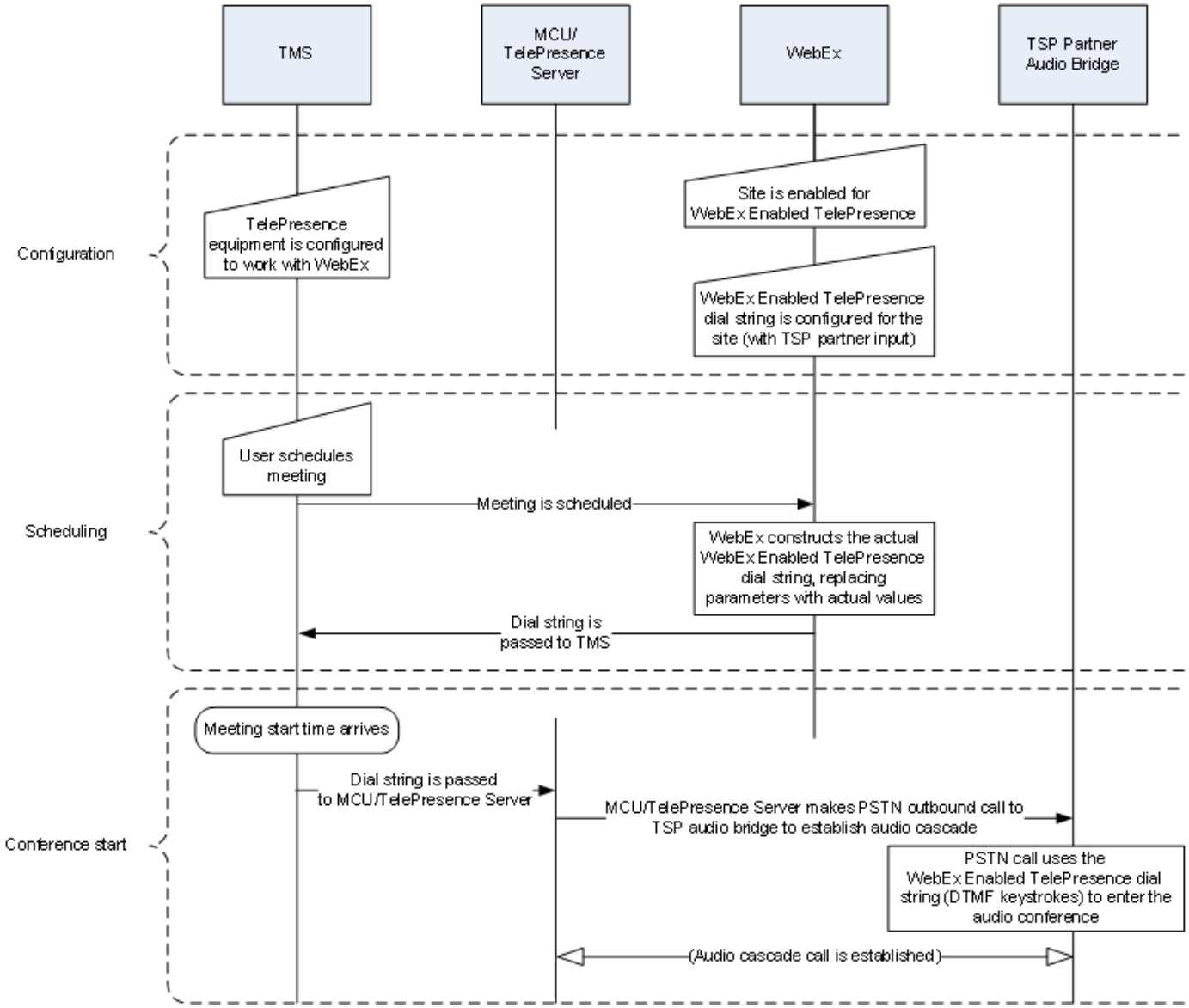


ステップ 7　[OK] をクリックします。

TSP 音声の設定と会議の概要

次の図は、TSP 音声向けに設定されるコンポーネントと、会議のスケジュール時および会議の開始時に実行される処理の概要を示しています。

図 9-6　TSP 音声の設定、スケジュール、および会議開始の流れ



TSP 会議のしくみ

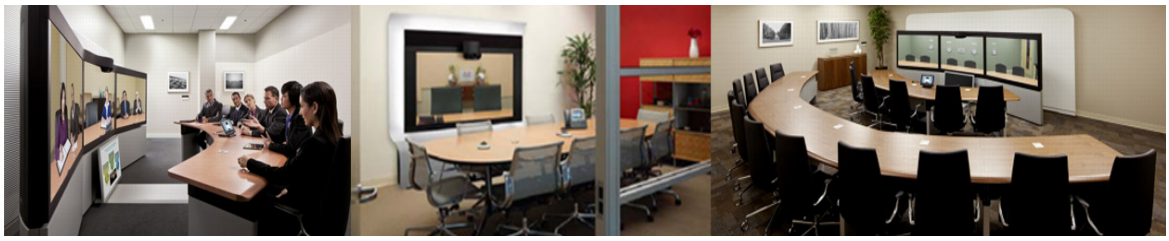
TSP 音声を使用する会議は、次のように実行されます。

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. スケジュールされた開始時刻に、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。

MCU または TelePresence Server がホストとしてダイヤルインする際の TSP 音声会議の動作

MCU/TelePresence Server は、どのような理由であっても最大再試行回数に達するまでリダイヤルを試行します。MCU/TelePresence Server がホストとして参加する場合、MCU/TelePresence Server がホストであるときにこのコールが何らかの理由で切断されると、TSP パートナーが音声会議を切断する（すべての参加者が切断される）可能性があることに注意してください。MCU/TelePresence Server はただちに再度ダイヤルインして音声会議を再確立しますが、参加者は再度コールインする必要があるかもしれません。「必要があるかもしれない」という表現を使っている理由は、これが TSP で設定可能であり、TSP プロバイダーによってその動作が異なる可能性があるためです。



CHAPTER 10

Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合

改訂日：2013 年 11 月

目次

この章では、Cisco WebEx Enabled TelePresence のために WebEx サイトを設定する方法について説明します。次のような構成になっています。

- Cisco WebEx Site Administration アカウントと Cisco TelePresence の統合（10-1 ページ）
- Meeting Center TelePresence セッション タイプの割り当て（10-3 ページ）
- ネットワーク ベースの WebEx Enabled TelePresence 会議の録画（10-6 ページ）
- WebEx and TelePresence Integration to Outlook のインストール（10-6 ページ）
- ユーザの WebEx アカウントのタイム ゾーンと言語の設定（10-8 ページ）
- ユーザの WebEx アカウントの TSP 音声の設定（10-9 ページ）

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。

- Cisco TelePresence Cisco WebEx の統合オプション（10-2 ページ）
- Meeting Center TelePresence セッション タイプの割り当て（10-3 ページ）

Cisco TelePresence Cisco WebEx の統合オプション

Cisco TelePresence を Cisco WebEx に統合するには、次の手順を実行します。

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。

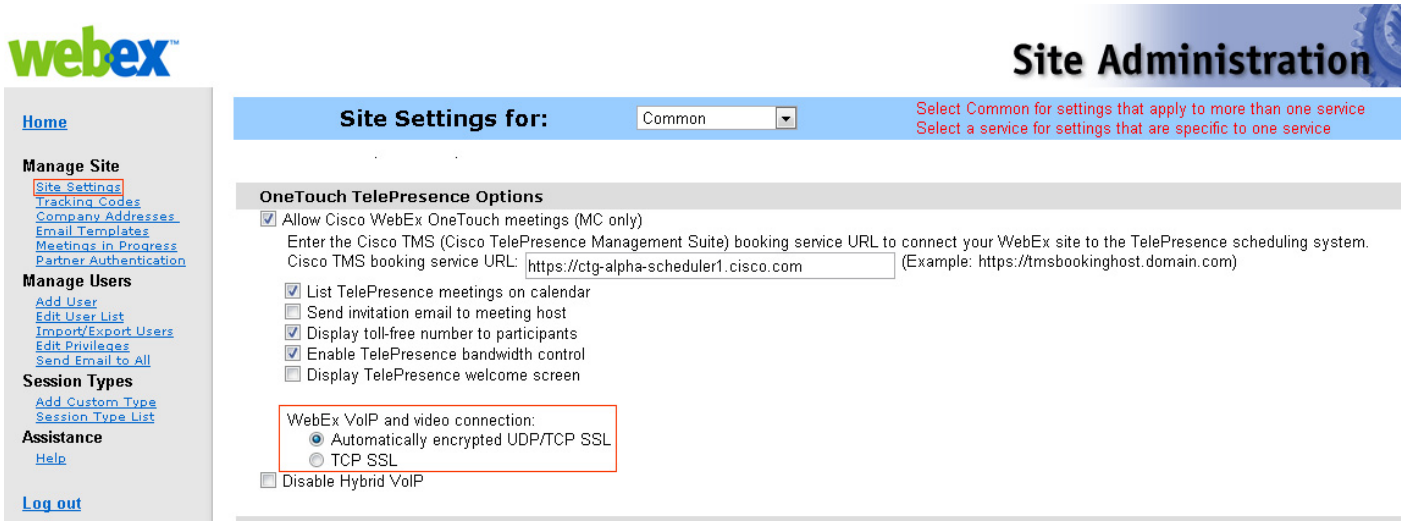
ログインするには、WebEx サイトの URL の後にスラッシュ（/）と「admin」を続けます。

例：*https://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　図 10-1 に示すように、[OneTouch TelePresence オプション（OneTouch TelePresence Options）] に達するまで下にスクロールします。

図 10-1　　Cisco WebEx 接続設定の設定



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 Cisco WebEx Enabled TelePresence 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。TMSXE の設定の詳細については、第 6 章「Cisco TelePresence Management Suite の設定」を参照してください。

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、スケジュール済み会議が Cisco WebEx カレンダーに表示されます。

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　[WebEx VoIP とビデオ接続（WebEx VOIP and video connection）] フィールドで、次のいずれかをクリックします。

- **自動暗号化 UDP/TCP SSL（Automatically encrypted UDP/TCP SSL）**：（推奨）TelePresence Server または MCU に UDP による Cisco TelePresence ゲートウェイへの接続を許可します。UDP 接続が許可されていない場合、TelePresence Server または MCU は TCP にフォールバックします。
- **TCP SSL**：SSL 接続で TCP 接続します。

これにより、Cisco WebEx クライアントとマルチメディア サーバ（VoIP とビデオ）間の接続方法を選択します。

ステップ 11　（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、WebEx 対応 TelePresence 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 12　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。

ステップ 13　Meeting Center TelePresence セッション タイプの割り当て 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（10-4 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（10-5 ページ）

カスタム セッション タイプのサポート

カスタム セッション タイプを作成できるようになりました。これにより、顧客は特定のユーザ グループに対して WebEx 機能を制限できます。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。

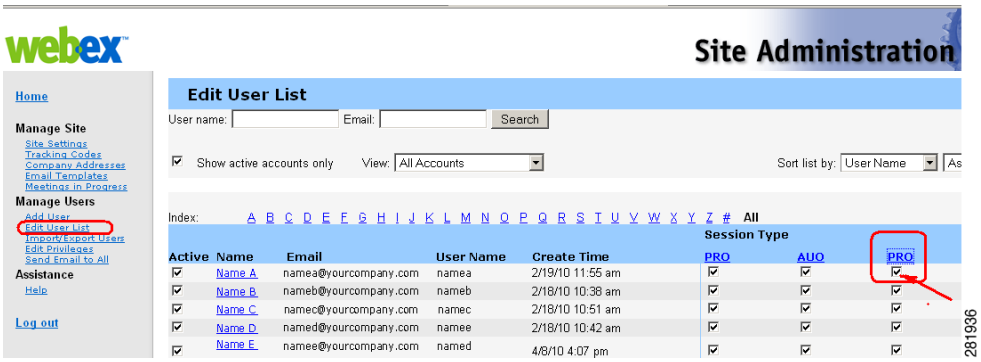
会議主催者が会議をスケジュールするときには、デフォルトの TelePresence セッション タイプが使用されます（これをカスタム セッション タイプに設定できます）。会議主催者が WebEx and TelePresence Integration to Outlook プラグインを使用して会議をスケジュールする場合、Site Administration レベルで設定されている他のカスタム セッション タイプを選択できます。WebEx サイト管理者は、特定のカスタム セッション タイプにアクセスできるユーザを決定できます。会議主催者が TMS、Smart Scheduler、または WebEx 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

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。図 10-2 に示すように [ユーザリストの編集（Edit User List）] 画面が表示されます。

図 10-2　WebEx Site Administration :[ユーザ リストの編集（Edit User List）]



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（図 10-2 に示すように、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。図 10-3 に示すように、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。

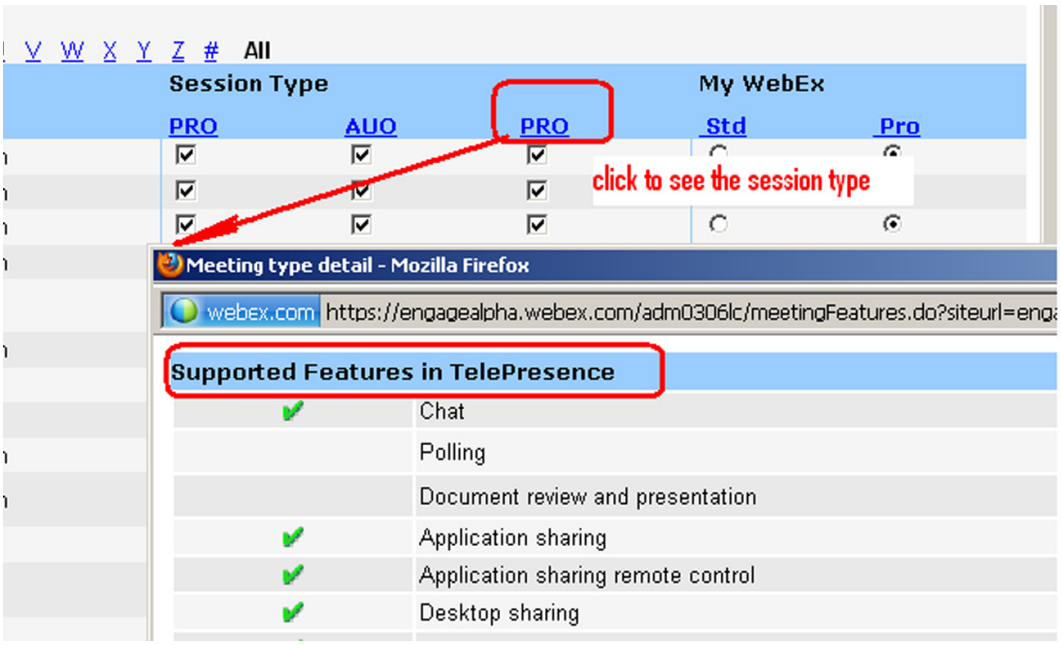
コメント　セッション タイプの列の数は、WebEx サイトでサポートされるセッション タイプの数に基づいて決まります。

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 WebEx Enabled TelePresence 向けに正しく設定されていません。

図 10-3　　TelePresence がサポートする機能



コメント　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。OneTouch 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 WebEx Enabled TelePresence 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。

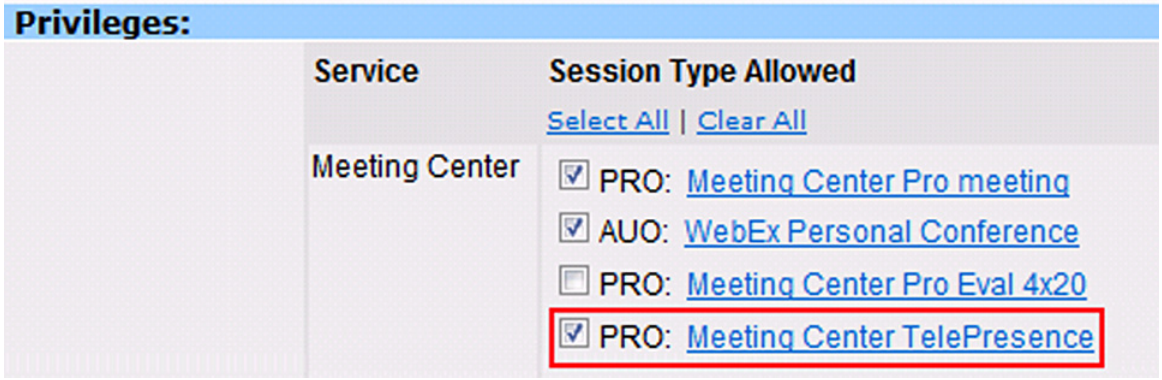
[ユーザの編集（Edit User）] 画面での Cisco TelePresence セッション タイプの追加

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。

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。図 10-4 に示すように、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。

図 10-4　　許可されているセッション タイプ



ステップ 3　必須作業です。図 10-4 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。

ヒント　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。

ネットワーク ベースの WebEx Enabled TelePresence 会議の録画

WebEx リリース T29 では、会議主催者が WebEx Enabled TelePresence 会議を録画できるようになりました。

- 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。
- 録画した会議を再生すると、WebEx と TelePresence 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。

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

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。

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

コメント　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。

WebEx 生産性向上ツールをインストールするには、ユーザが次の手順を実行する必要があります。

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。

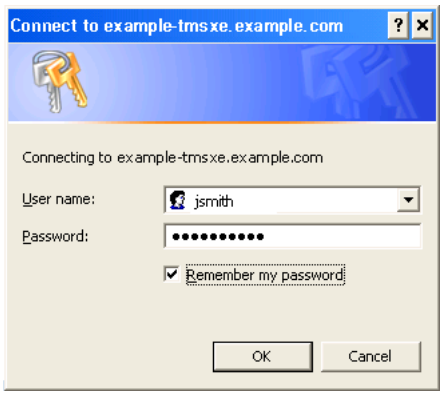
ステップ 8　インストール中に、WebEx サイトにログインする必要があります。

図 10-5　WebEx 生産性向上ツール ログイン

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。

ログイン後、WebEx 生産性向上ツールがサーバと通信して、TMSXE にログインするように求められます。

図 10-6　　TMSXE のログイン



ステップ 10　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 11　「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 12　[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 WebEx Enabled TelePresence 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。

WebEx アカウントの WebEx タイム ゾーンと優先言語を設定するには、ユーザが次の手順を実行する必要があります。

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。

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。ダウンロードを選択し、すぐにインストールする場合は、WebEx and TelePresence Integration to Outlook のインストール（10-6 ページ）のステップ 4 を参照してください

[My WebEx会議（My WebEx Meetings）] ページが表示されます。

ページ右隅に、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 4　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 5　[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、WebEx Enabled TelePresence 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 6　[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

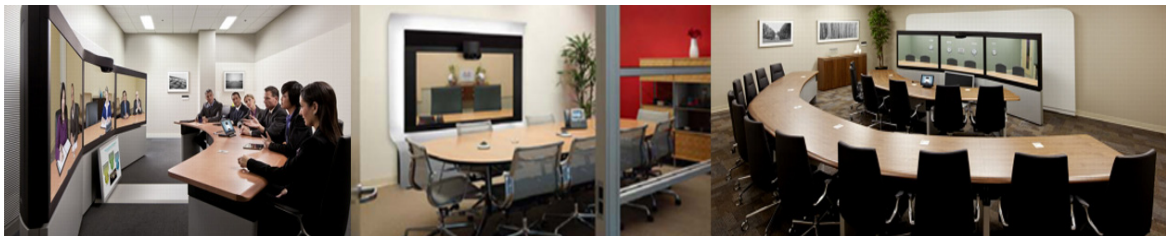
TSP 音声を使用する WebEx Enabled TelePresence 会議をスケジュールする必要がある会議主催者は、自分のアカウントに TSP 音声プロバイダー情報を追加する必要があります。

詳細については、会議主催者の TSP 音声の設定（9-12 ページ）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。

次の作業



CHAPTER 11

Cisco WebEx Enabled TelePresence 会議のスケジュール

改訂日：2013 年 11 月

目次

この章では、Cisco WebEx Enabled TelePresence 会議のスケジュール方法の背景情報、ヒント、および既知の問題について説明します。次のような構成になっています。

- はじめに（11-2 ページ）
- Cisco TMS での WebEx Enabled TelePresence 会議のスケジュール（11-3 ページ）
- WebEx Enabled TelePresence 会議についての情報、ヒント、既知の問題（11-5 ページ）

はじめに

この章では、TMS を使用して WebEx Enabled TelePresence 会議をスケジュールする方法の概要と、WebEx Enabled TelePresence 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。

WebEx Enabled TelePresence 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 WebEx Enabled TelePresence 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 WebEx Enabled TelePresence 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。

Cisco TMS での WebEx Enabled TelePresence 会議のスケジュール

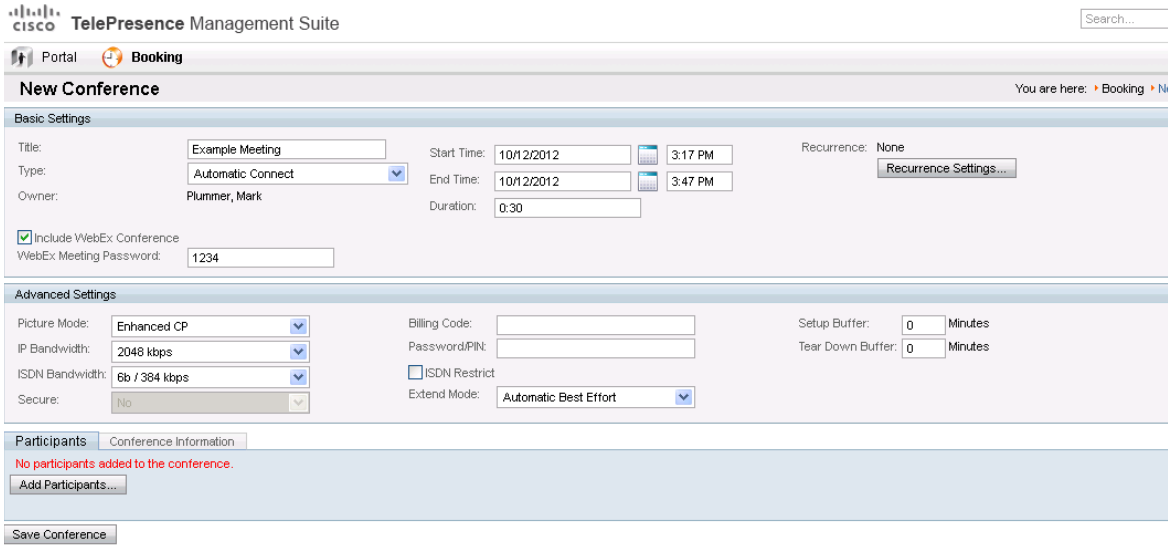
Cisco TMS で会議をスケジュールするときには、ユーザがネットワーク プロトコル、MCU、ゲートウェイを考慮する必要はありません。Cisco TMS により、これらのインフラストラクチャ選択と互換性チェックが自動的に行われます。上級ユーザは、必要に応じて、会議に選択された方法を調整できます。

Cisco WebEx Enabled TelePresence 会議をスケジュールするには、次の手順を実行します。

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。

図 11-1　　Cisco TMS の [新しい会議（New Conference）] ページ



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。
- [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。

コメント　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。

コメント　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。

コメント　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。

コメント　[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。

- 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。
- 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。
- 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 11　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 12　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。

- 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。
- 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 13　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 14　[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。このシステムに対して、次の操作が求められます。

- 自動コール開始がスケジュールされていない場合に、会議に接続する。
- まもなく有効期限が切れる場合、会議を延長する。

ステップ 15　[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 が要求の処理を完了できる場合:
  - 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。
  - また、Cisco TMS から確認の電子メールも送られ、そこにはすべての会議情報（WebEx およびビデオ ダイヤルイン情報など）が示され、Outlook（または互換の）カレンダーにイベントを保存するための ICS 添付ファイルも含まれます。ICS 添付ファイルを開き、カレンダーに保存します。
  - 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 つの電子メールを受け取ります。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 が予約要求の処理を完了できない場合:
  - [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。
  - 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。

ステップ 16　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。

Cisco WebEx Enabled TelePresence 会議エクスペリエンスについては、Cisco WebEx Enabled TelePresence エクスペリエンス（1-1 ページ）を参照してください。

WebEx Enabled TelePresence 会議についての情報、ヒント、既知の問題

ここでは、Cisco WebEx Enabled TelePresence 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。Cisco WebEx Enabled TelePresence ソリューション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 [デフォルト セットアップ バッファ（Default Setup Buffer）] 設定を使用することで、会議の早期開始がサポートされます。

コメント　Smart Scheduler、WebEx and TelePresence Integration to Outlook、および TMS Booking API を使用するその他のクライアントを使用する場合は、セットアップ（およびティアダウン）バッファがサポートされません。

- 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 TMS でその会議を変更してはなりません。

  後で TMS で元の会議を変更すると、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、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

- 会議の開始時に TelePresence または WebEx 参加者がいない場合でも、MCU/TelePresence Server は WebEx にコールします。
- 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 CM に登録されている場合、Unified CM 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。

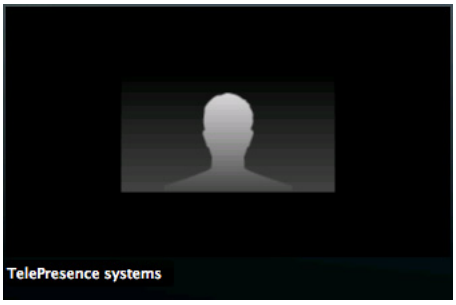
TMSXE

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

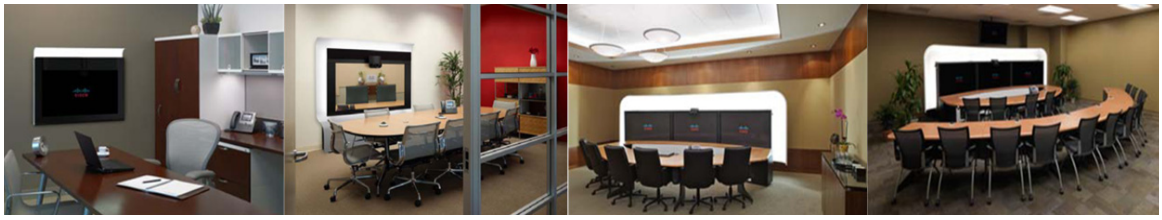
- 黒いシルエットは、WebEx ユーザがカメラをオンにしていないときや、WebEx クライアントを使用してビデオを送信するための十分な帯域幅がないときに、そのユーザを表します。
- WebEx Meeting Center では、TelePresence ユーザが発言中である場合および参加者リストの両方で、すべての TelePresence エンドポイントが「TelePresence システム（TelePresence systems）」という 1 つの WebEx 参加者として表示されます。
  - Meeting Center の全画面ビューでは、「TelePresence システム（TelePresence systems）」参加者は、図 2 に示すように黒色のシルエットとして表示されます。

図 2　　全画面ビューでの「TelePresence システム（TelePresence systems）」



- 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。

- Windows または Mac の WebEx Meeting Center クライアントを使用して参加する際、コンピュータのオーディオを使用する WebEx 参加者の音声品質が悪くなることがあります。シスコは、会議の音声会議番号を使用して電話機から発信することを推奨します。
- 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。
- ホスト以外のユーザが会議を開始できるのは、サイトで [ホストより前に参加（Join Before Host）] 機能が有効になっていて、その開始時刻がスケジュール時刻の 5/10/15 分前である場合だけです。それ以外の場合、ホスト以外のユーザは、ホストが会議を開始するまで待機する必要があります。
- 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。
- MCU と WebEx 間のリンク帯域幅は、最も低い帯域幅を使用する WebEx クライアントにより設定されます。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、リンクの帯域幅がすぐに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、すべての参加者の最大帯域幅は 360p に制限されます。その参加者が会議から退席したときに、他のすべての参加者がより大きい帯域幅（たとえば、720p）に対応している場合、すべての参加者の帯域幅が増加します。



CHAPTER 12

トラブルシューティング

改訂日：2013 年 10 月

目次

- 検証とテスト（12-1 ページ）
- トラブルシューティングのヒント（12-1 ページ）
- システム動作の管理（12-10 ページ）

検証とテスト

- Cisco WebEx サイト管理のオンラインヘルプ（12-1 ページ）

Cisco WebEx サイト管理のオンラインヘルプ

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。

ステップ 1 WebEx サイトの Site Administration 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://example.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、Cisco WebEx Enabled TelePresence 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。

- 会議のスケジュールに関する問題（12-2 ページ）
- 会議の開始または参加に関する問題（12-3 ページ）

- 会議の進行中に発生する問題（12-4 ページ）
- TSP 音声会議に関する問題（12-7 ページ）
- システム動作の管理（12-10 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。

会議が正しくスケジュールされなくなる一般的な問題を解決するには、表 12-1 のトラブルシューティング情報を参照してください。

表 12-1　　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、Meeting Center TelePresence セッション タイプの割り当て（10-3 ページ）を参照してください。
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。

表 12-1　会議のスケジュールに関する問題 （続き）

問題またはメッセージ	考えられる原因	推奨処置
([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 WebEx Enabled TelePresence 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。	Cisco WebEx Enabled TelePresence 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。
TelePresence スケジューリング システムで問題が発生しました。もう一度やり直してください。	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、表 12-2 のトラブルシューティング情報を参照してください。

表 12-2　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	会議はまだ開始されていません	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 会議は存在しません。 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。

表 12-2　会議の開始または参加に関する問題 （続き）

問題またはメッセージ	考えられる原因	推奨処置
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。
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	会議はまだ開始されていません。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 WebEx Enabled TelePresence 会議は 1 つだけです。

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、表 12-3 のトラブルシューティング情報を参照してください。

表 12-3　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	• -
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。
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。

表 12-3　会議の進行中に発生する問題 （続き）

問題またはメッセージ	考えられる原因	推奨処置
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。
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。
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。
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。

表 12-3　会議の進行中に発生する問題 （続き）

問題またはメッセージ	考えられる原因	推奨処置
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 参加者からのプレゼ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。
会議が自動的に拡張されません	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。

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、表 12-4 のトラブルシューティング情報を参照してください。

表 12-4　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)。 **コメント**　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)。 **コメント**　API を使用する方法ではこれは解決できません。
「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。

表 12-4　TSP 会議に関する問題 （続き）

問題またはメッセージ	考えられる原因	推奨処置
MCU/TelePresence Server がダイヤルできません。	PSTN コールが WebEx に PSTN ゲートウェイをパス スルーするように設定されていない可能性があります。 VCS からの発信ダイヤリングが正しく設定されていない可能性があります。	• PSTN ゲートウェイを WebEx にパススルーするようにコールを設定します。 • VCS と MCU/TelePresence Server の発信ダイヤル設定を確認します。
（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 A2W_RspCreateConference[NBRPhoneNumber] 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。	• 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。
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、表 12-5 のトラブルシューティング情報を参照してください。

表 12-5　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。 **コメント**　1 つのホストが一度に実行できる WebEx Enabled TelePresence 会議は 1 つだけです。

システム動作の管理

• Cisco WebEx ビデオ表示ウィンドウの管理（12-10 ページ）

Cisco WebEx ビデオ表示ウィンドウの管理

[Cisco WebEx ビデオ表示（Cisco WebEx video view）] パネルが開いている状態で、プレゼンテーション ケーブルを接続すると、ウィンドウ カスケード効果が発生することがあります。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、図 12-1 に示すようにビデオ表示ウィンドウを閉じます。

図 12-1　　カスケード表示された Cisco WebEx ビデオ表示ウィンドウ