Cisco Meeting Server

Cisco Meeting Server リリース 3.13

単一分割サーバー導入ガイド

2026 年 5 月 4 日

目次

新着情報

バージョン	変更内容（Change）
2026 年 5 月 4 日	バージョン 3.13 で更新。 ワンクリック SSO に関するコンテンツを追加しました。

1 はじめに

Cisco Meeting Server ソフトウェアは、Cisco Unified Computing Server（UCS）テクノロジに基づく特定のサーバー、または仕様ベースの VM サーバーでホストできます。本書では、Cisco Meeting ServerをMeeting Serverと呼びます。

注：Cisco Meeting Server ソフトウェアバージョン 3.0 以降は X シリーズサーバーをサポートしていません。

このガイドは、分割サーバー導入として導入された Meeting Server を対象としており、スケーラビリティやレジリエンスの要素は含まれていません。 サーバーは多くのコンポーネントで設定されています。図 1 を参照してください。

Meeting Server が統合された単一の導入では、参加者がシグナリングとメディアのために Call Bridge に直接ネットワークにアクセスしている場合、SIP アプリとウェブアプリの参加者の両方がミーティングに参加できます。 この導入は、すべての参加者が同じイントラネットまたはネットワーク内にいる場合に機能します。

ネットワーク境界外からミーティングに参加する参加者のサポートが必要な場合、**「スプリットサーバー導入」**と呼ばれるものが必要です。これは、NAT およびファイアウォールルールによる制限を克服するための追加コンポーネントが必要なためです。

Meeting Server は、この外部接続に対処するために、3 つの一般的な戦略をサポートします。Cisco Expressway ソリューション、サード パーティの SIP ファイアウォール トラバーサル ソリューション、および Meeting Server Edge 導入モデルです。

- **Cisco Expressway ソリューション**は、SIP 通話用のファイアウォール トラバーサル技術と、ウェブアプリ参加者向けの TURN サーバー機能を持つウェブプロキシを提供します。 Cisco Expressway は、Core および Edge インスタンスにさまざまな導入オプションを提供し、通話と電話会議のためのセキュリティエンクレーブをカバーするために構築されています。 Cisco Expressway ソリューションは、複数の Cisco コラボレーション テクノロジーに統合された Edge 戦略を提供します。
- **サードパーティの SIP ファイアウォール トラバーサル ソリューション**を利用できます。これらは、セッション ボーダー コントローラーなどの SIP 通話のネットワーク境界をトラバースする他の技術を提供します。 これらのテクノロジについては、このガイドでは特に扱いません。
- **Meeting Server Edge 導入モデル**は、Core と Edge の役割に分割された複数の Meeting Server インスタンスを使用して、ネットワーク外からのウェブアプリ参加者の接続を可能にします。 Meeting Server Edge 導入の価値は、ネットワーク外からの Web アプリ参加者に対し、Cisco Expressway でサポートされている以上の大容量接続を提供できることです。 Meeting Server Edge 導入モデルは、SIP ファイアウォール トラバーサルのニ

ーズに対応していません。SIP 通話のトラバーサルニーズは、Cisco Expressway または他の SIP 通話技術を使用して、個別に対応する必要があります。 典型的な Meeting Server Edge の導入では、SIP 通話に Cisco Expressway を使用し、ウェブアプリの参加者に Meeting Server Edge インスタンスを使用します。

導入モデルの選択は、組織のニーズに基づいて行う必要があります。 外部参加者への SIP 接続が必要な場合は、ファイアウォール トラバーサルに Cisco Expressway ソリューションを導入することをお勧めします。 ウェブアプリの接続性については、Expressway（大規模 OVA または CE1200）は中規模のウェブアプリ規模要件（つまり、800 コール以下）の導入に推奨されるソリューションです。Expressway（中規模 OVA）は小規模なウェブアプリスケール要件（200 コール以下など）の導入に推奨されるソリューションです。 バージョン 3.1 以降、より大きなウェブアプリのスケールが必要な導入では、Meeting Server Edge が推奨される導入モデルです。

注：Meeting Server Edge 導入では、Web Bridge 3 を使用して、このガイドに記載されている容量と機能をサポートする必要があります。 Web Bridge 2 を使用する既存の導入は、このガイドに従うために、Web Bridge 3 に移行する必要があります。

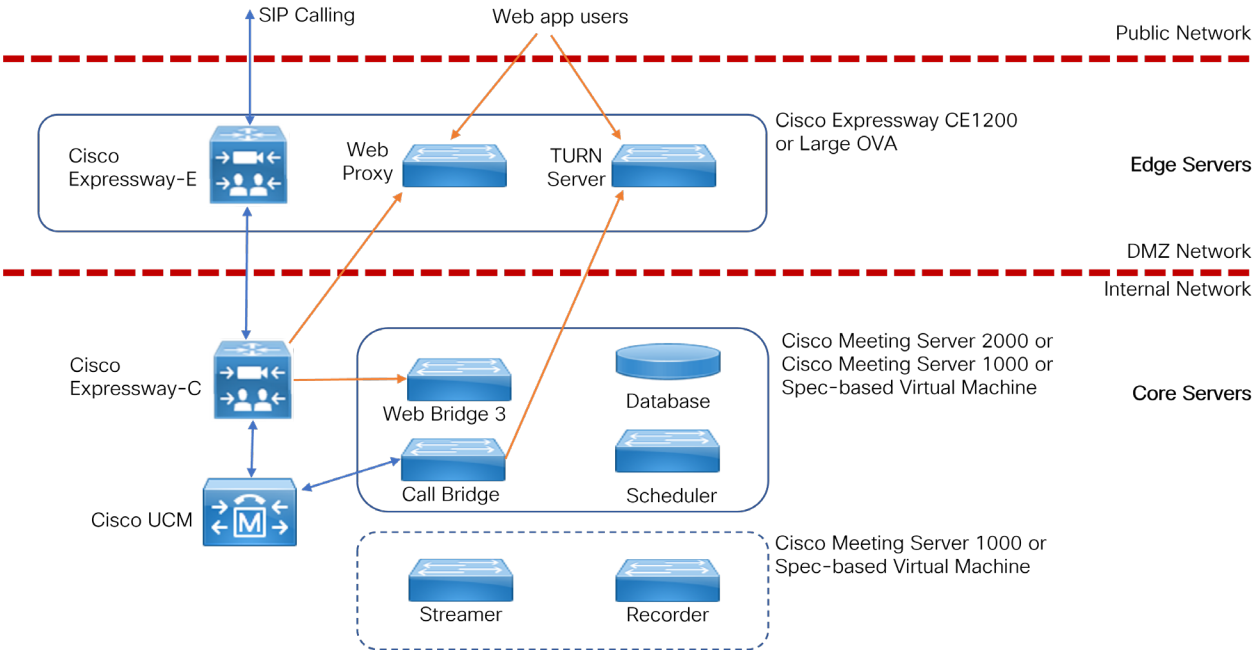
複数のサーバーに役割が分割されているため、これらの導入は**スプリットサーバー導入**と名付けられます。一部はネットワーク内で、一部は外部です。 Edge ロールは、組織外の接続をサポートするために、ネットワークのパブリックにアクセス可能な部分に存在し、Core ロールは、外部からすぐにアクセスできない内部ネットワークで動作します。 各ロールをさらに専門的なタスクに細分することもできます。 例えば、Meeting Server のレコーダーとストリーマのロールは、コアに導入されるオプション機能ですが、メインの Meeting Server とは別のサーバーに導入されます。

図 1 および 2 は、Cisco Expressway および Meeting Server Edge モデルを示します。

- 図 1 は、Cisco Expressway が SIP とウェブアプリの両方の接続を Edge で提供し、コアの Meeting Server が Call Bridge、Web Bridge、その他の Meeting Server サービスを提供することを示しています。
- 図 2 は、Meeting Server の Edge インスタンスとして DMZ にある Meeting Server が提供する TURN サービスと Web Bridge 3 機能を示しています。

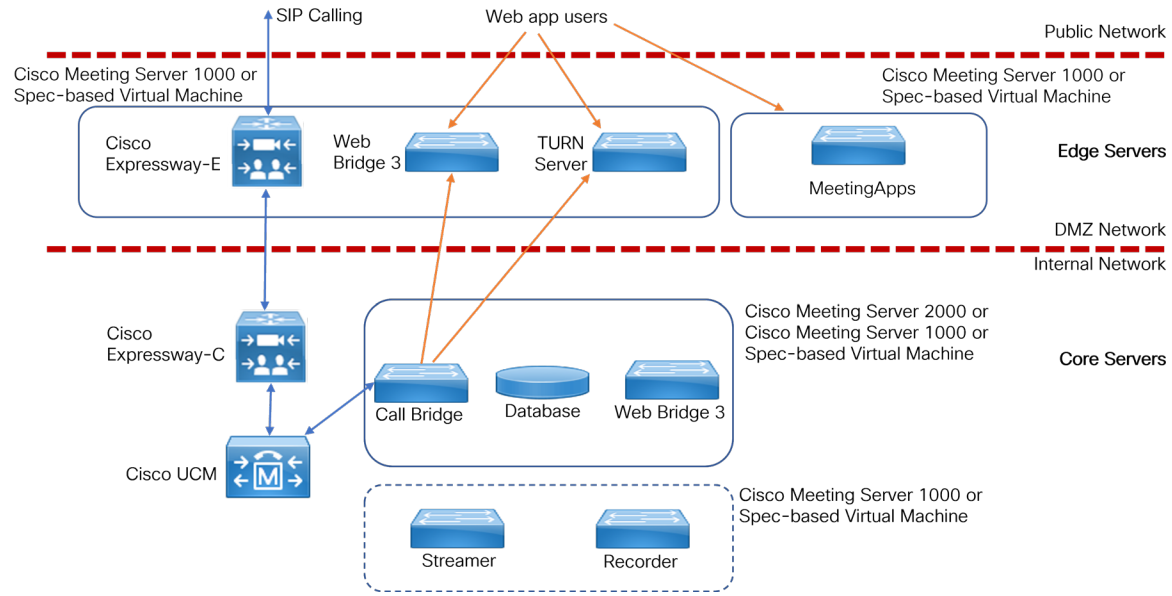
  注：Web Bridge 3 は Edge サーバーに移動しますが、内部参加者についてはコアでも引き続き操作できます。

図 1: Cisco Expressway を使用した分割サーバー導入



Edge サーバーとして使用する場合、Meeting Server は最小限必要なサービスのみで設定され、表面積を減らし、セキュリティ体制を改善します。 Edge インスタンスは、ウェブアプリユーザーに対して、インターネットに到達するために必要なサービスのみを実行します。Web Bridge は、クライアントに Web インターフェイスを提供します。TURN はメディアにファイアウォール トラバーサル技術を提供します。他のすべてがコア ネットワークで運用されている間、Edge はこれらの拡張機能をコアに提供し、一般に公開されないようにします。

図 2：Meeting Server Edge を使用した分割サーバー導入



1.1 Meeting Server の導入で Cisco Expressway-E を Edge デバイスとして使用する

Expressway（大規模 OVA または CE1200）は、中規模のウェブアプリのスケール要件を持つ導入（つまり、800 コール以下）に推奨されるソリューションです。 Expressway（中規模 OVA）は、小規模なウェブアプリスケール要件を持つ導入（つまり、200 コール以下）に推奨されるソリューションです。 しかし、より大きなウェブアプリスケールを必要とする展開では、バージョン 3.1 から、必須のソリューションとして Cisco Meeting Server ウェブエッジを推奨します。

Cisco Expressway ソフトウェアの Edge 機能は、Meeting Server の導入で Cisco Expressway-E を Edge デバイスとして使用できるように開発されました。 Cisco Expressway は、SIP ファイアウォール トラバーサル、ブラウザベースのウェブアプリを使用して Meeting Server 電話会議に参加する外部参加者をサポートするリバースウェブプロキシ、およびウェブアプリとリモートの Lync および Skype for Business クライアントのメディアトラバーサルをサポートする TURN サーバー機能を提供します。

さらに、Cisco Expressway-E を SIP レジストラとして使用して、SIP エンドポイントを登録したり、内部コール制御プラットフォーム（Cisco Unified Communications Manager または Cisco Expressway-C）に登録をプロキシすることもできます。

警告：Expressway ユーザーのための重要な注意点
Web Bridge 3 および Web App の導入は、Expressway バージョン X15.4 で検証済みです。 Web Bridge 3 は、それ以前の Expressway バージョンをサポートしていない場合があります。

注：Cisco Expressway-E は、オンプレミスの Microsoft インフラストラクチャとMeeting Serverの間で使用することはできません。 オンプレミスの Microsoft インフラストラクチャと Meeting Server の導入では、Meeting Serverは Microsoft Edge サーバーを使用して、Microsoft の組織内外への通話をトラバースする必要があります。

注：オンプレミスのMeeting Serverとオンプレミスの Microsoft Skype for Business インフラストラクチャの間のデュアルホーム電話会議を設定している場合、Meeting Serverは自動的に Skype for Business Edge の TURN サービスを使用します。

以下の表 1 は、これらの機能を実行するための Cisco Expressway-E のセットアップを説明する設定ドキュメントを示します。 表 2 以下では、リリースごとの機能の紹介を示しています。

表 1：Meeting Server のエッジデバイスとしての Cisco Expressway に関するドキュメント

Edge 機能	このガイドで説明されている設定
リモートブラウザベースの Meeting Server web app を接続する	Cisco Meeting Server 用 Cisco Expressway ウェブプロキシ 導入ガイド
リモートの Lync および Skype for Business クライアントを接続する	Cisco Expressway を使用した Cisco Meeting Server の導入ガイド
SIP レジストラまたは内部コール制御プラットフォームへの登録をプロキシする	Cisco Expressway-E および Expressway-C の基本設定 (X15.4)

表 2：Meeting Serverの Expressway エッジサポート

Cisco Expressway-E バージョン	Edge 機能	Meeting Server のバージョン
X15.4	Cisco Meeting Server web app をサポートしています。Cisco Meeting Server（X15.4）用 Cisco Expressway ウェブプロキシを参照してください	3.13

1.2 コアネットワークで Meeting Server と Cisco Expressway-C を使用する

ネットワークのエッジでの Cisco Expressway-E の導入に加えて、Cisco Expressway-C は Meeting Server と共にコアネットワークに導入することができます。 Meeting Server とオンプレミスの Microsoft Skype for Business インフラストラクチャの間に導入した場合、Cisco Expressway-C は IM&P とビデオの統合を提供できます。 さらに、Cisco Expressway-C は以下の機能を提供できます。

- SIP レジストラ
- H.323 ゲートキーパー
- Call Bridge グループが設定されている Meeting Server の導入における通話コントロール。これは、Meeting Server のノード全体で電話会議の負荷を分散します。

注: Cisco Meeting Server がネイバーゾーンを介して Expressway-E と統合されている場合、Expressway-E は Meeting Server ノード間で会議の負荷分散を行うための呼び出しを置き換えることができず、これはサポートされていない展開です。

表 3：Cisco Expressway-C および Meeting Server に関する追加ドキュメント

機能	このガイドで説明されている設定
クラスター化された Meeting Server の負荷を分散する通話コントロールデバイス	Cisco Meeting Server による Cisco Meeting Servers 間の通話のロードバランシング
SIP レジストラ	Cisco Expressway-E および Expressway-C 基本構成 (X15.4)
H.323 ゲートキーパー	Cisco Expressway-E および Expressway-C 基本構成 (X15.4)

1.2.1 Cisco Expressway H.323 ゲートウェイコンポーネントを使用する

Cisco Meeting Serverと Cisco Expressway で単一の Edge ソリューションを提供するという Cisco の目標に沿って、Cisco はMeeting Serverソフトウェアのバージョン 3.0 から H.323 ゲートウェイコンポーネントを削除しました。 顧客には、Cisco Expressway のより完成度の高い H.323 ゲートウェイコンポーネントに移行することをお勧めします。

Expressway-E または Expressway-C に登録された H.323 エンドポイントは、Expressway バージョン X8.10 以降から Cisco Meeting Server に通話する場合、リッチ メディア セッション (RMS) ライセンスを消費しません。

1.3 Meeting Server 展開で Meeting Server をエッジ デバイスとして使用する

Meeting Server の Edge 設計では、外部参加者が到達できる場所に Meeting Server の Edge インスタンスを導入する必要があります。 これは、DMZ またはパブリックネットワーク内に可能です。 このサーバーは信頼されていないトラフィックにさらされるため、必須のサービスのみが有効化されています。推奨される導入は、Edge インスタンスが NAT の背後にある DMZ または必要なトラフィックのみを許可する選択的なルールを持つファイアウォールに導入されることです。 DMZ の Edge サーバーは、コアに導入された Call Bridge サーバーによって到達可能である必要があります。 DMZ/イントラネットの境界は、必要なトラフィックのみを許可するアクセスコントロールすることを推奨します。

ウェブアプリクライアントの接続は、Call Bridge を TLS を使用して Web Bridge の C2W インターフェイスに発信接続させ、Web Bridge 機能のためにコアと Edge の間で安全なコントロールチャネルを確立することで実現します。 外部ブラウザ クライアントは、HTTPS を使用して Edge のWeb Bridgeに接続します。

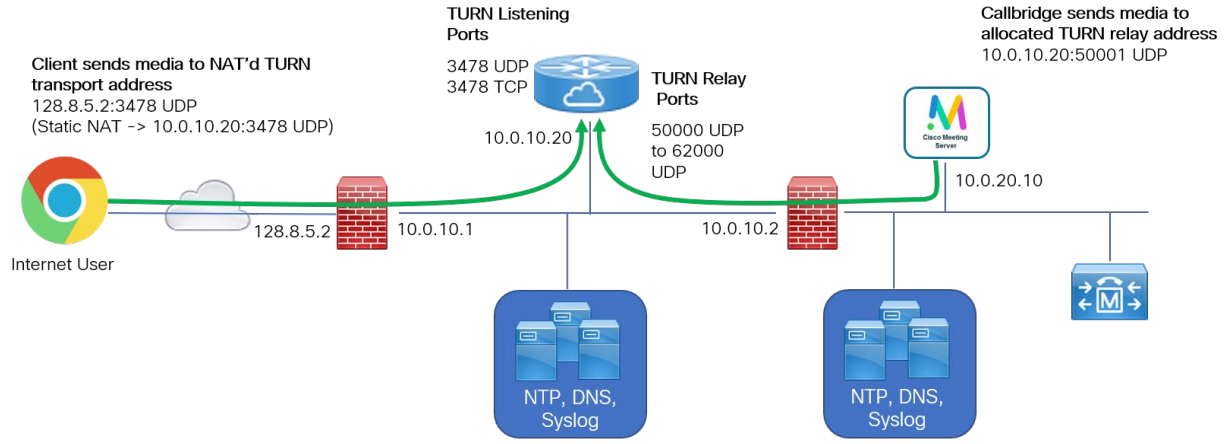
外部ウェブアプリクライアントのメディアトラフィックは、Meeting Serverの TURN サーバーを通じた TURN リレーセットアップを使用して処理されます。 Web Bridge に接続して確認されると、ウェブクライアントは TURN サーバーのリスニングポートに接続し、TURN サーバー

のインターフェイスで自分に割り当てられるリレー トランスポート アドレスをリクエストします。 ICE を使用して、クライアントと Call Bridge はこのリレーを介してお互いにトラフィックを送信できることを確認します。結果として得られたリレーにより、両当事者はネットワーク境界を越えてメディアを送受信できます。

外部クライアントによる TURN リレーセットアップの使用は、Edge サーバーが Meeting Server Edge の公開コールキャパシティを達成するための必要な導入戦略です。 他の組み合わせやシナリオでは、メディア接続が確立される場合がありますが、容量が減少し、メディア ルーティングが準最適になる可能性があるため、お勧めできません。

複雑さを軽減するために、このガイドではリモートクライアントがリレーを確立するシナリオのみを扱います。

図 3：Meeting Server Edge TURN サーバーの例



警告：Edge Meeting Serverは DMZ 内にある必要があり、異なる信頼レベルまたはセキュリティ領域を持つネットワークに直接接続しないでください。 TURN サーバーは、リレーの役割を実行するために 1 つのインタフェースのみを必要とします。

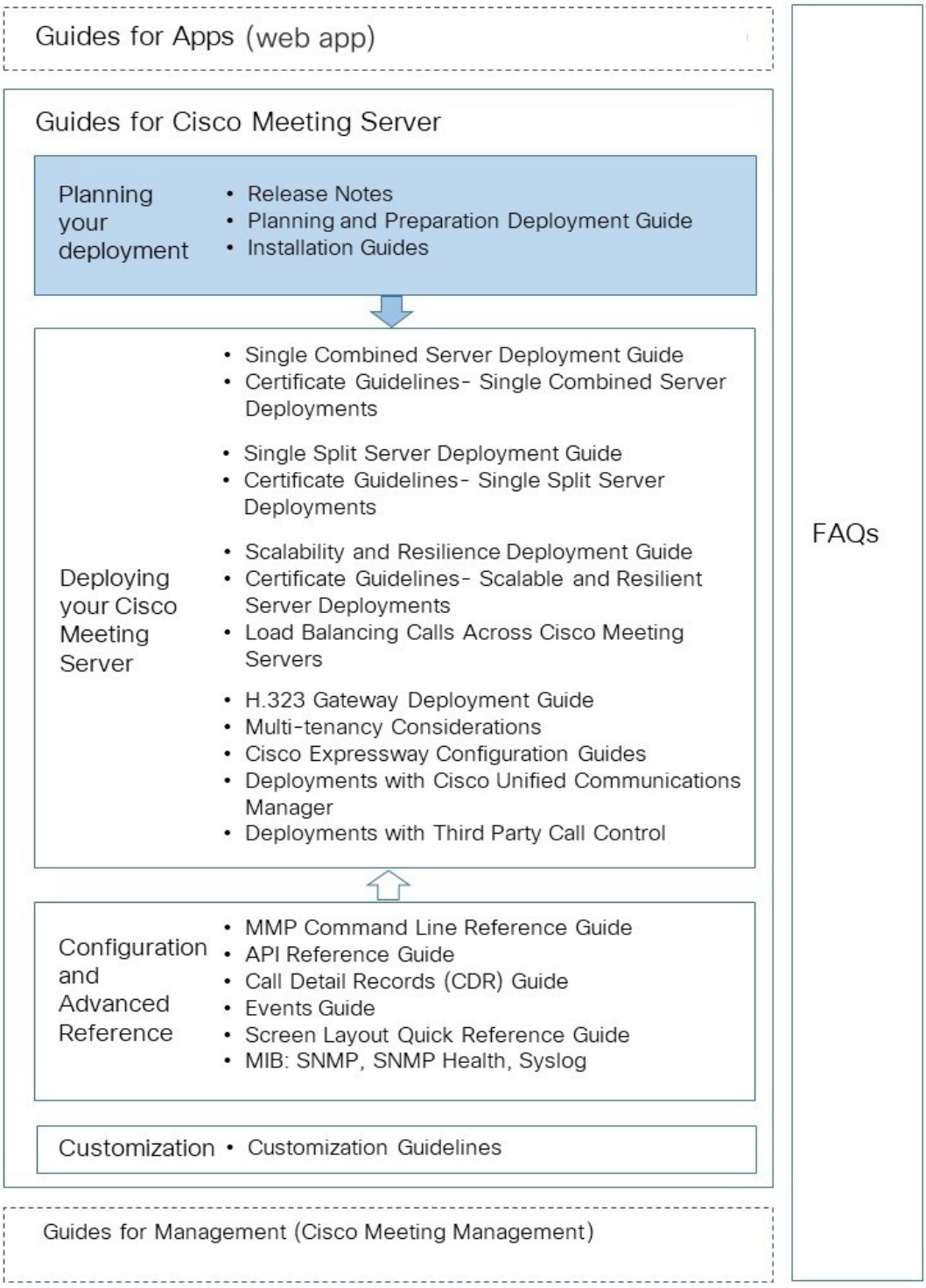
1.4 このガイドの使い方

この導入ガイドは、お使いのサーバーに適切な『設置ガイド』から続くものであり、インストールの説明はすでに完了していることを前提としています。 このガイドは、該当する『証明書ガイドライン』と併せて読み、活用してください。

Cisco Meeting Server ドキュメント には、この導入ガイドと証明書のガイドラインのほか、下図で示されている参照資料があります。

注：このガイドでは、coSpace をスペースと記載しています。

図 4：Meeting Server に関するガイドの概要



注：Cisco ユーザー用ドキュメントで使用しているアドレス範囲は、RFC 5737 で定義されているものです。これはドキュメント化のために明示的に予約されています。 Meeting Server のユーザーマニュアルに記載されている IP アドレスは、特に記載のない限り、お使いのネットワークでルーティング可能な正しい IP アドレスに置き換えてください。

1.4.1 コマンド

このドキュメントでは、コマンドは黒で表示され、指定どおりに入力する必要があります。括弧内に適切な値を入力します。 青で例を参照できます。これらは実際の導入に合わせて変更する必要があります。

1.5 Meeting Server を設定する

Cisco Meeting Server ソフトウェアには、プラットフォームとアプリケーションの 2 つのレイヤーがあります。

- **プラットフォーム** はメインボード管理プロセッサ (MMP) を通じて設定されます。 MMP は、低レベルのブートストラップ、およびコマンドライン インターフェイス経由の設定に使用されます。 例えば、MMP は Web Bridge、データベースクラスタリング、および他のさまざまなコンポーネントを有効にするために使用されます。
- **アプリケーション** は MMP プラットフォームで動作します。 アプリケーションレベルの管理（通話およびメディアの管理）は、Call Bridge の Web 管理インターフェイスまたは必要に応じてアプリケーション プログラミング インターフェイス（API）から実行できます。API は、トランスポートメカニズムとして HTTPS を使用し、導入で利用可能な非常に多数になる可能性のあるアクティブな通話とスペースを管理するために、スケーラブルに設計されています。

  バージョン 2.9 から、アプリケーションレベルの管理は、シングルおよびクラスタ Meeting Serverの両方で、 Call Bridge ウェブ管理インターフェイス からすべて行うことができます。

1.5.1 MMP と API インターフェース

表 4：異なる Meeting Server プラットフォーム上での MMP および API 用に設定されたネットワークインターフェース

プラットフォーム	MMP へのアクセス	Web 管理インターフェイスおよび API へのアクセス
Cisco Meeting Server 2000	ブレード 1 で Serial over LAN SoL 接続。 注： MMP にアクセスする前に、Fabric Interconnect モジュールのネットワーク設定を構成する必要があります。	MMP の構成中に作成されたインターフェイス A。 これは、Fabric Interconnect モジュールのポート 1 で構成されたアップリンクを介して外部ネットワークに接続される仮想接続です。 **注：**Cisco Meeting Server 2000 プラットフォームは複数のインターフェイスをサポートしていません（例えば、「ipv4 b| c	d」の設定はサポートされていません）。
Cisco Meeting Server Small およびその他の仮想化環境	仮想インターフェイス A	1 つのイーサネットインターフェイス (A) が作成されますが、さらに 3 つまで追加できます (B、C、D)。 Call Bridge Web 管理インターフェイスと API は、A-D イーサネットインターフェイスのいずれか 1 つで実行するように設定できます。

1.5.2 Meeting Server の設定を容易にする新しいツール

管理者が Meeting Server を設定および導入するのに役立つ以下のツールが利用できます。

- インストールアシスタントデモンストレーション、ラボ環境、または基本的なインストールの出発点として利用するための、シンプルな Cisco Meeting Server 環境の構築を容易にします。 バージョン 3.3 以降、Installation Assistant はスタンドアロンツールではなくなりました。 Meeting Management と統合されており、Meeting Management UI から使用できます。
- 「Cisco Meeting Management 経由で Cisco Meeting Server web app ユーザーをプロビジョニングする」は、バージョン 2.9 以降で利用できます。
- Meeting Server の Web インターフェイスを通じた API アクセス。 バージョン 2.9 以降、Meeting Server Web 管理インタフェースの **[設定（Configuration）]** タブから Meeting Server API にアクセスできます。 このガイドに記載されているいくつかの例が、API メソッドの POST および PUT から、ウェブ インターフェイスを通じた API アクセス の使用に変更されています。

インストール アシスタント ツール

インストールアシスタントを使用すると、デモンストレーション、ラボ環境向けに、または基本インストールの開始点として、単一の Cisco Meeting Server インストールの作成を簡素化できます。 このツールは、『Cisco Meeting Server 単一サーバー簡易導入ガイド』に記載されて

いるベストプラクティスの導入に基づいて、Meeting Server を設定します。 バージョン 3.3 以降、Meeting Management と統合され、セットアップに関する情報を収集し、その設定をサーバーにプッシュします。API、SFTP、または Meeting Server のコマンドライン インターフェイスにアクセスするためのユーティリティを使用する必要はありません。 Installation Assistant は Meeting Management UI から実行できます。 クライアントコンピュータ用のソフトウェア要件、ソフトウェアのインストールと実行の詳細、および Meeting Server の構成手順については、『ミーティング管理インストールガイド』を参照してください。

インストレーションアシスタントは、コールの受発信が可能な SIP MCU になるように Meeting Server を設定し、オプションで Cisco Meeting Server web app を有効にします。

インストールアシスタントは、空の、未設定の Meeting Server での使用を想定しています。 Meeting Server の管理ツールではなく、また既存の Meeting Server の再設定用のツールでもありません。 このツールは、Meeting Server 仮想マシンの設定専用です。 Cisco Meeting Server 2000 プラットフォームで使用することはできません。

Cisco Meeting Management を使用して Cisco Meeting Server web app のユーザーをプロビジョニングする

Meeting Server または Meeting Server クラスタに接続された Cisco Meeting Management は、Meeting Server API を使用する必要なく、LDAP 認証された Cisco Meeting Server web app ユーザーをプロビジョニングする機能を提供します。 この機能により、管理者はウェブアプリユーザーが使用して自分のスペースを作成できるスペーステンプレートを作成することもできます。

LDAP サーバーの Meeting Server クラスタへの接続、ユーザーインポートの追加方法、スペーステンプレートの作成方法、変更の確認とコミット、そして最後に LDAP 同期の実行についての情報については、『Cisco Meeting Management ユーザーガイド』を参照してください。

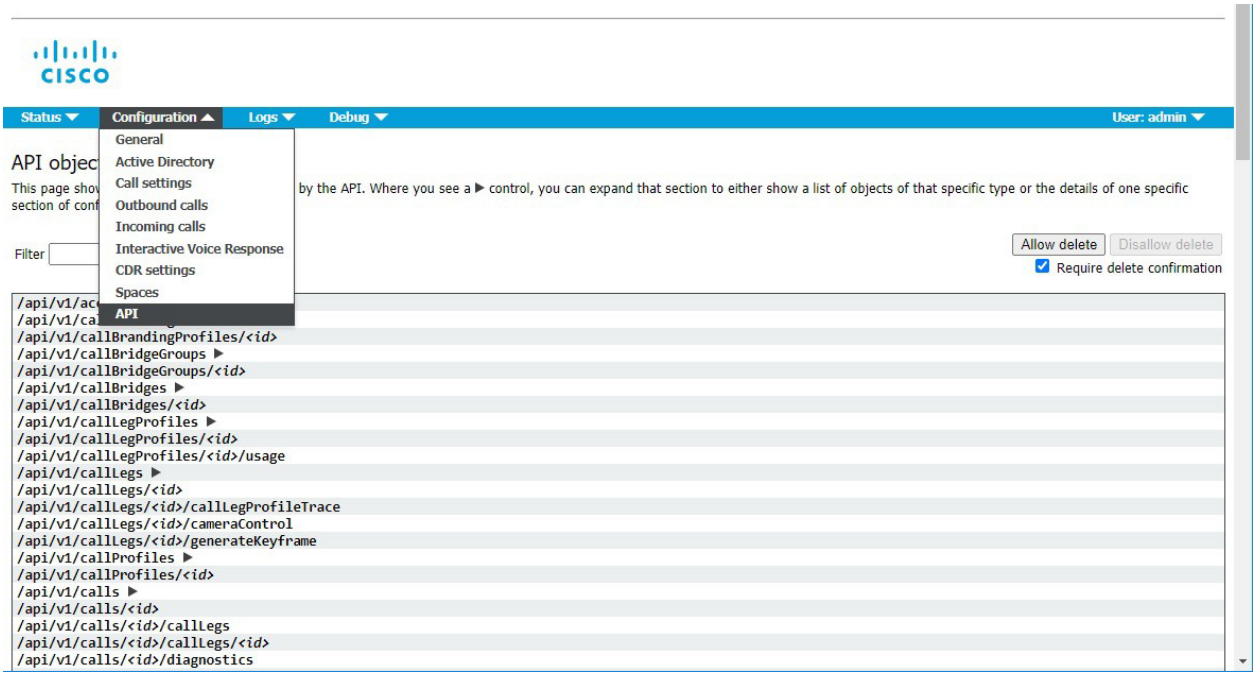
Web インターフェイスでの API アクセス

図 5で示されている通り、サードパーティアプリを必要とせずに Call Bridge API の使用を簡素化するために、バージョン 2.9 では、Meeting Server Web インターフェイスの［**設定（Configuration）**］タブ経由でアクセスできる Call Bridge API のユーザーインターフェイスが導入されました。

バージョン 3.3 で導入されたスケジューラ API はこのインターフェイス経由ではサポートされていません。 「スケジューラ API」を参照してください。

注：Web インターフェイス経由で API にアクセスするには、サードパーティ アプリケーションを使用する場合と同様に、Meeting Server の初期設定と MMP を使用した認証を行う必要があります。 詳細については、 MMP コマンドリファレンスガイド を参照してください。

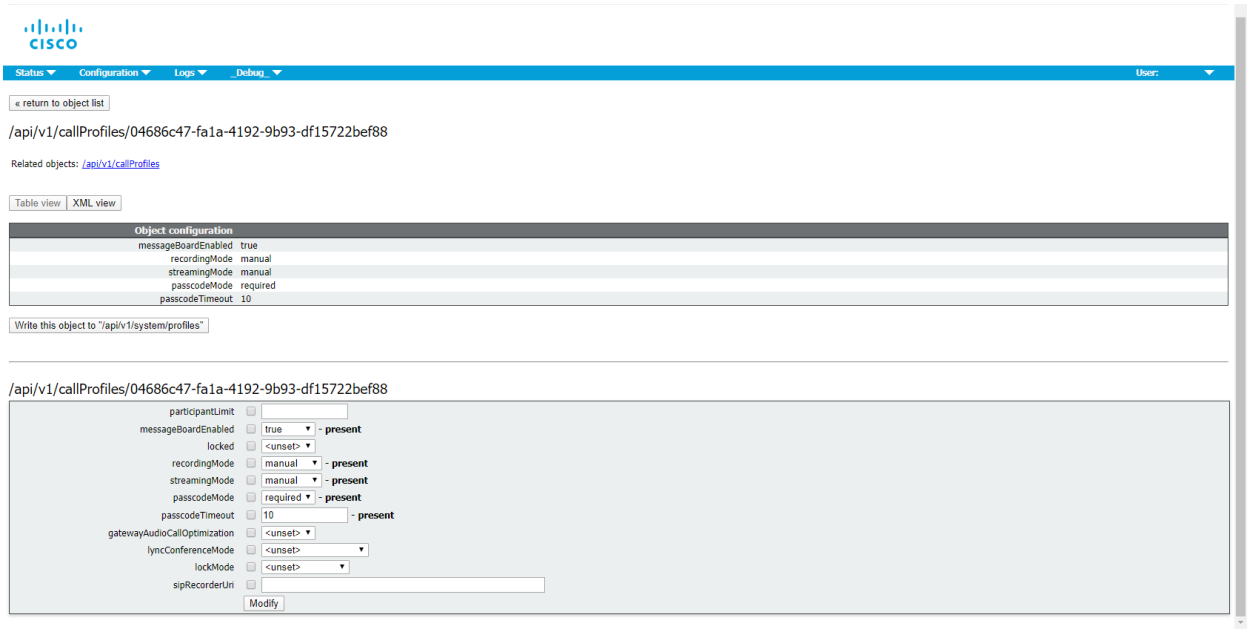
図 5：ミーMeeting Server Web インターフェイス経由で Call Bridge API にアクセスする



注： 設定済み API オブジェクトを削除したい場合は、画面の右側で [**削除を許可**] を選択します。 デフォルトでは削除は無効になっており、意図しない削除を防ぐため、[**削除の確認を要求する**] にチェックが入っています。

Web インタフェース経由で API を使用すると、より視覚的なアプローチで Meeting Server を設定するためのユーザーフレンドリーな方法が提供されます。 たとえば、 図 6 に示すチェックボックスとフィールドを使用して、callProfiles の設定を行うことができます。

図 6：Web インターフェイスで API アクセスを使用して callProfiles を設定する



1.6 Meeting Serverのライセンス

Cisco Meeting Server のセットアップを完了するにはライセンスが必要です。 Meeting Server は、Cisco Meeting Management 製品を通じたライセンス管理を必要とし、Cisco Smart Licensing をサポートしています。 3.4 リリース以降、Smart LicensingはMeeting Serverに必須です。 従来のライセンスのサポートは 3.4 以降のリリースで廃止されました。 顧客はスマート ライセンシングに移行することをお勧めします。

注： セキュリティ上の理由からミーティング管理を使用できない、またはインターネットに接続できない環境では、Cisco アカウントチームに連絡して別のライセンスオプションを入手してください。

この章では、ライセンス付き機能、スマートライセンス、およびスマートアカウントと仮想アカウントに関する情報について説明します。 ライセンスの詳細については、 このセクション を参照してください。

1.6.1 ライセンスが付与された機能

次の Meeting Server 機能にはライセンスが必要です:

- Call Bridge
- Call Bridge [暗号化サポートなし]
- カスタマイズ（カスタムレイアウト用）

- 録画またはストリーミング
- ミーティング参加者のスナップショット

機能ライセンスに加えて、ユーザーライセンスも購入する必要があります。ユーザーライセンスには 2 つの異なるタイプがあります。

- Personal Multiparty Plus (PMP Plus)
- Shared Multiparty Plus (SMP Plus)

詳細は マルチパーティライセンス を参照してください。

注：Cisco Meeting Management では、ライセンスなしでトライアルモードを 90 日間のフル機能で使用できます。

1.6.2 スマートライセンシング

Meeting Server のバージョン 3.0 では、Cisco Meeting Management バージョン 3.0（またはそれ以降）を使用する Cisco Meeting Server 上のスマートライセンシングのサポートを導入しました。 このソフトウェア ライセンス モデルへの移行、つまり従来の製品アクティベーション キー（PAK）ライセンスからスマートライセンシングへの移行により、ライセンスの購入、登録、ソフトウェア管理のユーザーエクスペリエンスが向上します。 また、Meeting Server を他の Cisco 製品のソフトウェアライセンシングに対するアプローチと整合させ、Cisco Smart Account（組織全体のライセンスを表示、保存、管理できる中央リポジトリ）を利用します。

注：Cisco スマート ライセンシング クラウド証明書は 2023 年 2 月に更新されます。更新後、スマート ライセンシング クラウドで直接、またはオンプレミスの Cisco Smart Software Manager（SSM）を介したすべての通信に影響が及びます。 2023 年 2 月より前に Meeting Management 3.6 にアップグレードすることをお勧めします。一眼レフ/PLR 顧客も、新しいライセンスの取得、手動同期の実行、または新しいコールブリッジの追加を行う場合、Meeting Management 3.6 にアップグレードする必要があります。

すべての新規ライセンス購入には、引き続き PAK コードが付与されます。参照用に保持しておきます。これは、Meeting Management が同期するスマートアカウントですべてのライセンスが利用できるためです。

詳細およびスマートアカウントの作成については、https://software.cisco.com に移動してスマートライセンシングを選択してください。

Meeting Server のライセンスの 3.0 以前のバージョンからの変更点：

- Cisco Meeting Management バージョン 3.0（またはそれ以降）はバージョン 3.0 で必須です。Meeting Management は Meeting Server ライセンスファイルを読み取り、製品の登録とスマートアカウント（セットアップされている場合）との対話を処理します。
- スマートアカウントの 1 セットの Meeting Server ライセンスで複数のクラスターのライセンスを取得できるようになり、3.0 以前の場合のように、個々の Meeting Server インスタンスにライセンスファイルをロードする必要がなくなりました。
- スマートライセンシングを含む Meeting Management は、クラスタごとに Call Bridge の数を追跡するため、R-CMS-K9 アクティベーション ライセンスの必要性を排除します。
- 既存のライセンスを持たない新規展開の場合：
    - 新しく購入したライセンスは、デフォルトで Smart が有効になっており、スマートアカウントを必要とする場合があります。ライセンスの詳細をミーティング管理に入力すると、スマートアカウントに保持されているものに対してライセンスの詳細が検証されます。
- 各 Call Bridge にローカルライセンスファイルがある既存の展開の場合：
    - Cisco Smart Software Manager（CSSM）ポータル を使用してスマートアカウントに移行し、既存のライセンスをスマートに変換するオプションを選択できます。
- SMP Plus および PMP Plus ライセンスの使用数が組み合わされて、日を超過使用数としてカウントされるかどうかが決定されます（いずれかのライセンスが期限切れの場合、1 日は使用資格の超過使用数とみなされます）。 他の機能ライセンス（例えば、録画またはカスタムレイアウト）については、個別に評価され、Meeting Management 経由で権限付与で有効化されます（ライセンスがスマートアカウントに存在すると想定）。

メモ：「超過」という用語は、ライセンス使用数が利用資格を上回る状況を表すのに使用されています。

注：Meeting Management はすべての 3.0 の導入に必要であるため、顧客が大規模な展開を行う場合、Meeting Management はアクティブなミーティング管理なしの新しいライセンスのみのモードで導入できます。

1.6.3 スマートアカウントとバーチャルアカウントの情報

スマートアカウントにはバーチャルアカウントを含めることができます。バーチャルアカウントを使えば、部門ごとなど、指定の指定ごとにライセンスを整理することができます。

Meeting Server および Meeting Management でスマートバーチャルアカウントを使用する際の注意事項は以下の通りです。

- 単一の Meeting Management に対する各 Meeting Server クラスタは、ユーザー定義のスマート バーチャル アカウントにリンクされている必要があります。
- 各バーチャルアカウントは、スマートライセンシングを処理するように設定された単一の Meeting Management サーバーのみに接続できます。
- 1 つの Meeting Management のみをスマートに設定します。スマートライセンシングの 2 つ目の冗長 Meeting Management を Smart に設定**しないでください。**ライセンス使用数の二重カウントが発生するため、お勧めしません。
- PMP Plus、SMP Plus、および録画/ストリーミングライセンスは、単一のバーチャルアカウント内の単一の Meeting Management インスタンスおよびスマートライセンシングを使用して、複数のクラスタにわたって共有できます。

ライセンスの詳細は、 追加のライセンス情報をご覧ください。

2 導入の一般的なコンセプト

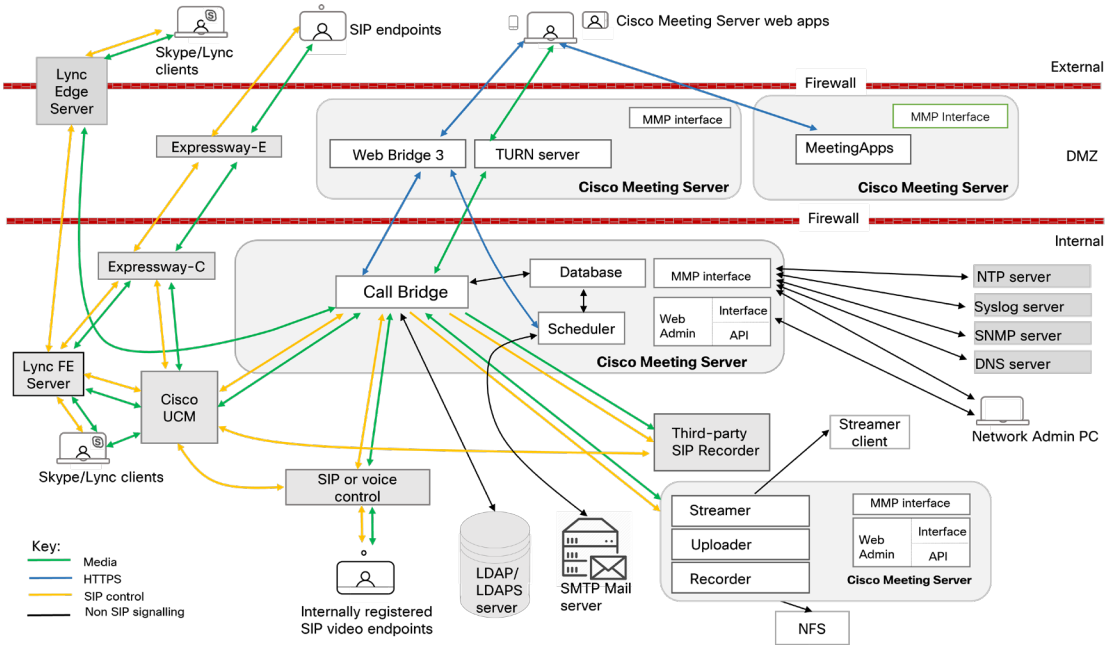
この章では、分割サーバー導入における Meeting Server の一般的な概念と導入について説明します。 図 7 は、DMZ 内の仮想 Meeting Server 上で有効になっている、TURN サーバー、MeetingApps、および Web Bridge 3 コンポーネントの典型的な Meeting Server Edge 導入を示しています。

注：コアとエッジサーバーの両方で同じバージョンのソフトウェアを実行する必要があります。

Expressway（大規模 OVA または CE1200）は、中規模のウェブアプリのスケール要件を持つ導入（つまり、800 コール以下）に推奨されるソリューションです。 Expressway（中規模 OVA）は、小規模なウェブアプリスケール要件を持つ導入（つまり、200 コール以下）に推奨されるソリューションです。 しかし、より大きなウェブアプリスケールを必要とする展開では、バージョン 3.1 から、必須のソリューションとして Cisco Meeting Server ウェブエッジを推奨します。

在宅勤務の需要が高まり、ウェブアプリのスケールが増大するにつれて、Cisco Meeting Server バージョン 3.1 がこの増大するウェブアプリのスケールにエッジサポートを提供するために開発およびテストされました。 図 7 は、Meeting Server のウェブエッジソリューションを導入し、より大規模なウェブアプリの導入に最適化する方法の例を示しています。

図 7: 分割サーバー展開での TURN サーバーコンポーネントを使用したMeeting Server展開の例



注：

- Meeting Server には、録画機能とストリーミング機能が含まれます。 機能を評価する場合にのみ、Call Bridge と同じサーバーでレコーダー/ストリーマを有効にします。これにより、通話が開始されてから 15 分後に接続が落ちます。 通常の導入では、レコーダー/ストリーマを Call Bridge とは別のサーバーで有効にします。 レコーダーとストリーマを同じMeeting Server上に導入する予定の場合、両方の使用に適したサーバーの規模を設定する必要があります。 録画とストリーミングの詳細については、 セクション 11を参照してください。

2.1 Web 管理（Web Admin）

Web 管理は、Meeting Server を設定するためのウェブベースのインタフェースです。

『Meeting Server インストールガイド』の説明に従って、HTTPS アクセス用に Web 管理インタフェースを設定した後、ウェブブラウザにサーバーのホスト名または IP アドレスを入力して、Web 管理インタフェースのログイン画面に到達します。 ウェブ管理インタフェースからアクセスできる設定の詳細は、 ウェブ管理インタフェース – 設定メニューオプション を参照してください。バージョン 2.9 以降、ウェブ管理インタフェースの [**設定**] タブから API にアクセスできます。

Web 管理は Meeting Server の管理者ウェブページを提供することに加えて、Web 管理 は Meeting Server の REST API のインタフェースも提供します。 REST API は、Postman または ChromePoster などの従来の REST ツールでアクセスできます。 バージョン 2.9 以降、ウェブ

管理者インタフェースに API Explorer インタフェースが含まれるようになりました。これにより、管理者は追加のツール/ソフトウェアなしで Meeting Server API を操作できます。 API リファレンスガイドは ここから参照できます。

2.2 Call Bridge

Call Bridge は電話会議接続をブリッジする Meeting Server 上のコンポーネントで、複数の参加者が Meeting Server または Lync AVMCUs で主催されるミーティングに参加できるようにします。 Call Bridge は音声とビデオのストリームを交換するため、参加者はお互いに顔を見たり聞いたりできます。 Call Bridge を動作させるにはライセンスが必要です。

2.3 データベース

Call Bridge は、スペースのメンバーやスペース内での最近のアクティビティなど、スペース情報を保存するデータベースの読み取りと書き込みを行います。 分割導入では、データベースはメイン コア インスタンスで実行されている Call Bridge によって自動的に作成され、管理されるため、ライセンスや設定は必要ありません。

2.4 Web Bridge 3 を設定する

Web Bridge 3 は、参加者がブラウザベースの Cisco ウェブアプリクライアントを使ってミーティングに参加できるようにするMeeting Server のコンポーネントです。 Web Bridge 3 は Cisco Meeting Server web app の参加者にウェブサーバーを提供し、Call Bridge および TURN サーバーコンポーネントと連携してクライアントをサポートします。

注: Web アプリを使用していない場合は、Web Bridge 3 を展開する必要がないため、このセクションをスキップできます。

2.5 Turn サーバー

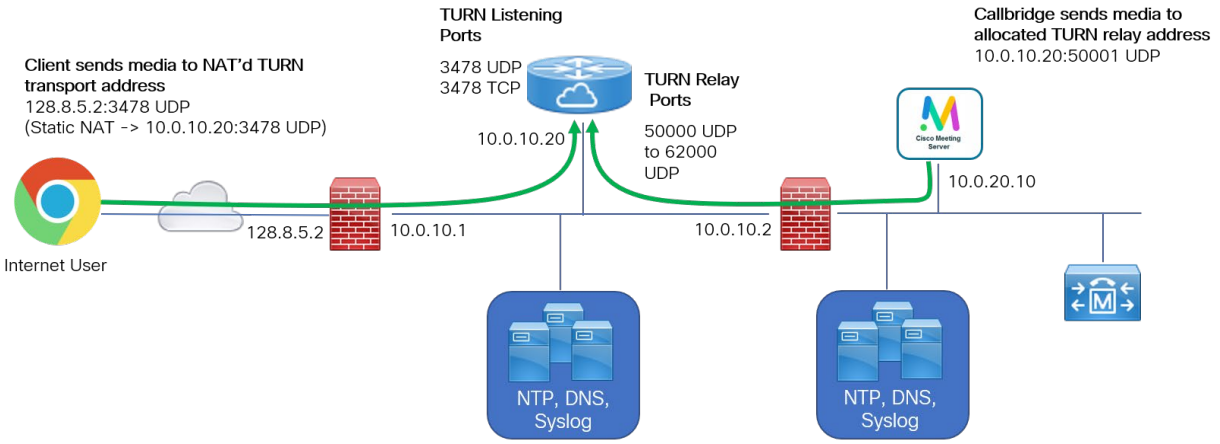
Meeting Serverの TURN Server コンポーネントは Cisco ウェブアプリのユーザーにファイアウォール トラバーサル技術を提供し、Meeting Server をファイアウォールまたは NAT の背後に導入することができます。TURN サーバーは TURN リレーを提供し、ファイアウォールまたは NAT 技術のために直接ルートがない場合に、ウェブアプリユーザーが Call Bridge でメディアを交換できるようにします。 TURN サーバの利用にはライセンスは必要ありません。

TURN Server の役割は、Meeting Server Edge 導入シナリオでMeeting Serverを使用して提供するか、Web Bridge プロキシに Expressway を使用している場合は Cisco Expressway により提供できます。 Meeting Server の導入では、TURN Server はウェブアプリクライアントにのみ使用されます。 Call Bridge を使用した SIP 通話では、TURN を使用しません。

TURN サーバーは、通話の両当事者が到達できるリレーポイントを提供することにより、エンドツーエンドで直接メディアを送信できない通話にファイアウォール トラバーサルを提供します。 通話のセットアップ中、ウェブアプリクライアントはリスニングポートで TURN サーバーに接続し、認証を行って、リレーを割り当てるよう要求します。 TURN サーバーは、このクライアント専用のリレートランスポートアドレスを割り当て、そのアドレスにメディアを転送するための別のポート番号をリッスンします。 リレーアドレスはリモートパーティに渡され、クライアント宛のメディアはこのリレーアドレスに送信するように指示されます。 リモート側がリレーアドレスに接続すると、TURN Server はリモート側が通話の側に到達するためのメディアを送信できるソースアドレスを学習します。 この交換により、両当事者が到達できるポイントが確立され、TURN Server は指定されたリレーに基づいて選択的に両方向にトラフィックを転送します。

ウェブ アプリ クライアントは TURN リスニング ポートに接続し、リモート参加者 (Call Bridge) はリレー ポートに接続します。 TURN に接続し、リレーをリクエストする（ロールを逆転させる）ように Call Bridge を設定することは可能ですが、ネットワークが Call Bridge と TURN サーバー間の UDP トラフィックを許可するように適切に設定されている限り、必要ではありません。

図 8: TURN Server のリレーの例



デフォルトでは、TURN Server は UDP をポート 3478 でリッスンします。 これは STUN トラフィックの業界標準であり、TURN Server リレーの割り当てを要求するクライアントによって使用されます。 TURN Server は、UDP STUN/TURN トラフィックをブロックする可能性があるネットワーク上のクライアントに対応するために、TCP ベースの接続を 2 番目のポートで待機することもできます。 この TCP ポートは通常、許可された HTTPS トラフィックをシャドウするためにポート 443 を使用するように設定されています。 クライアントが TCP を使用して TURN に接続すると、TURN Server は内部的に UDP へのトラフィックをインターワークし、UDP として Call Bridge に転送します。 Call Bridge は、メディアに TCP を使用しません。

TURN TCP を有効にする Meeting Server の構成オプションの名前は「tls」ですが、TURN TLS はMeeting Serverまたはウェブアプリでは使用されません。 ウェブアプリは TCP または UDP を使用し、Call Bridge は常に UDP を使用します（メディアは SRTP を使用して暗号化されます）。

TURN サーバーは、異なる信頼レベルまたはセキュリティエンクレーブにまたがるデバイスとして使用しないでください。 TURN サーバーは、ネットワークブリッジとしてではなく、トラフィックの共通のミーティングポイントとして機能します。

2.6 Meeting Server Edge

Meeting Server Edge または CMS Edge は、外部ウェブアプリ参加者の連絡先となる、DMZ または外部ネットワークに導入された限定された役割の Meeting Server インスタンスを説明するために使用されるラベルです。 1 つ以上のサービスが制限された Meeting Server のインスタンスが、「Edge」ロールとして DMZ または外部ネットワークに導入され、内部ネットワーク「Core」に導入された Meeting Server インスタンスと連携して機能します。CMS Edge では、Web Bridge 3 および TURN サービスのみが有効にするべきです。 この展開シナリオは、Cisco Expressway を外部ウェブアプリ参加者のプロキシおよび TURN Server として使用する代わりとなる大容量シナリオです。 Meeting Server Edge 導入モデルは、SIP ファイアウォール トラバーサルのニーズに対応していません。SIP 通話のトラバーサルニーズは、Cisco Expressway または他の SIP 通話技術を使用して、個別に対応する必要があります。 典型的な Meeting Server Edge の導入では、SIP 通話に Cisco Expressway を使用し、Cisco ウェブアプリの参加者に Meeting Server Edge 機能を使用します。

2.7 ミーティングの録画

3.0 以前は、Meeting Serverの内部レコーダーおよびストリーマコンポーネントは、Meeting Serverの内部 XMPP サーバーコンポーネントに依存していました。3.0 では、この XMPP サーバーは削除されます。 バージョン 3.0 では新しい内部レコーダーとストリーマーを導入し、どちらも SIP ベースです。

新しい内部レコーダーとストリーマコンポーネントとサードパーティへの発信
SIP レコーダーはすべて SIP URI を使用して設定されるため、録画またはストリーミングが開始されると、管理者が設定した SIP URI が呼び出されます。

Meeting Server上の内部 SIP レコーダーコンポーネントバージョン 3.0 以降は、ミーティングを録画し、録画をネットワークファイルシステム NFS などのドキュメントストレージに保存する機能を追加します。

ミーティングの録画の詳細については、次を参照してください。 セクション 11。

2.7.1 録画用ライセンスキー

録画には 1 つ以上のライセンスが必要です。 1 つの「録画」ライセンスは、1 つの同時ストリーミングまたは 1 つの録画をサポートします。既存の録画ライセンスはストリーミングを可能にします。 ライセンス要件については、Cisco の営業担当者またはパートナーにお問い合わせください。

2.8 ミーティングのストリーミング

内部 SIP ストリーマコンポーネント（バージョン 3.0 以降）は、スペースで開催されるミーティングをストリーミングする機能を、スペースで設定された RTMP URL に追加します。

この RTMP URL をリッスンするには、外部ストリーミングサーバーを設定する必要があります。 外部ストリーミングサーバーは、ユーザーにライブストリーミングを提供したり、後で再生するためにライブストリームを録画したりできます。

注：ストリーマコンポーネントは、RTMP 標準をサポートするサードパーティのストリーミングサーバーと連携するために、RTMP 標準をサポートしています。 Vbrick は正式にサポートされている外部ストリーミングサーバーですが、他のサーバーでもテストされています。

バージョン 3.1 では、内部 SIP ストリーマアプリケーションの RTMP サポートを RTMPS に拡張します。本質的には TLS 接続上の RTMP です。 これまでは、ストリーマと RTMP サーバー間のすべてのトラフィックは暗号化されていませんでした。3.1 RTMPS のサポートにより、このトラフィックを暗号化することができます。

既存の **tls** MMP コマンドが拡張され、オプションで RTMPS の TLS トラストの設定ができるようになりました。 このステップはオプションですが、推奨されています。 TLS 信頼が設定されていない場合、RTMPS 接続は安全ではありません。

2.8.1 ストリーミングのライセンスキー

ストリーミングには 1 つ以上のライセンスが必要です。 1 つの「録画」ライセンスは、1 つの同時ストリーミングまたは 1 つの録画をサポートします。既存の録画ライセンスはストリーミングを可能にします。 ライセンス要件については、Cisco の営業担当者またはパートナーにお問い合わせください。

2.9 ブランディング ファイルをローカルにホストする

ブランディングファイルの 1 セットは、Meeting Server上でローカルに保持できます。 ローカルでホストされているこれらのブランディングファイルは、Meeting Server が稼働状態になると Call Bridge と Web Bridge で利用できるようになり、ウェブサーバーの問題によりカスタ

マイズの適用が遅延するリスクを排除します。 画像と音声のプロンプトが、ミーティングサーバーソフトウェアに組み込まれた同等のファイルに置き換わります。起動時に、これらのブランディングファイルが検出され、デフォルトファイルの代わりに使用されます。 ローカルでホストされているブランディングファイルは、ウェブサーバーからのリモートブランディングによって上書きされます。

これらのローカルでホストされているファイルを変更するには、新しいバージョンのファイルをアップロードし、Call Bridge および Web Bridge を再起動するだけです。 ローカルでホストされているファイルを削除し、Call Bridge およびWeb Bridgeが再起動された後、Meeting Serverは組み込みの (米国英語) ブランディング ファイルを使用する状態に戻ります (ウェブ サーバーがブランディング ファイルを提供するようにセットアップされていない場合)。

注： 複数のブランディングファイルセットを使用する場合でも、外部ウェブサーバーを使用する必要があります。

ブランディングファイルをローカルでホストする方法の詳細は、 Cisco Meeting Server カスタマイズのガイドライン を参照してください。

2.10 オンスクリーンメッセージ

Meeting Serverは、Meeting Serverで主催されるミーティングの参加者に画面上にテキストメッセージを表示する機能を提供します。一度に 1 つのメッセージしか表示できません。 API を使用すると、メッセージが表示される期間を設定したり、新しいメッセージが表示されるまで永続的に表示したりすることができます。メッセージが設定されます。 **`messageText`、`messagePosition`、 `messageDuration` を使用します。**API オブジェクト **/呼び出し**のパラメータ。

SIP エンドポイントおよび Lync/Skype for Business クライアントのユーザーの場合、画面上のテキストメッセージがビデオペインに表示されます。 ビデオペインでのメッセージの位置は、上、中、下から選択できます。

画面上のメッセージはまた、導入で ActiveControl を使用している他のデバイス、例えば CE8.3 エンドポイント、およびクラスター内ではなく、通話メッセージ機能が有効になっている個々のMeeting Serverにも送信されます。 クラスタ内のMeeting Serverは、独自のメカニズムによるオンスクリーンメッセージングもサポートしています。

2.11 SIP トランクとルーティング

Meeting Serverは、SIP 通話コントロール、音声通話コントロール、および Lync フロントエンド (FE) サーバーの 1 つ以上から SIP トランクをセットアップする必要があります。 相互運

用のためにWeb Bridgeサービスを必要とするMeeting Serverに通話をルーティングするには、これらのデバイスでの通話ルーティング設定の変更が必要です。

2.12 Lync および Skype for Business のサポート

2.12.1 Lync および Skype for Business クライアントのサポート

Skype for Business クライアント、および Skype for Business サーバー、Lync 2010 または 2013 サーバーに接続されている Lync 2010 および Lync 2013 クライアントを使用できます。バージョン 2.6 から、Meeting Serverは Skype for Business 2019 をサポートしています。

Meeting Serverは以下を使用します。

- 2010 Lync Windows クライアントおよび 2011 Lync Mac クライアントで最大 1080p の RTV コーデック変換、
- 2013 Lync Windows クライアントおよび Skype for Business クライアントの H.264 コーデック。

異なるバージョンのクライアントが接続されている場合、Meeting Serverは RTV と H.264 の両方のストリームを提供します。

Lync 2010 および 2013 クライアントと Skype for Business クライアントはコンテンツを共有できます。 Meeting Serverはネイティブの Lync RDP からミーティングの他の参加者が使用するビデオ形式にコンテンツをトランスコードし、別のストリームとして送信します。 Lync および Skype for Business クライアントも RDP ストリーム経由でコンテンツを受信し、メインのビデオとは別に表示できます。

Lync FE サーバーは、Lync エンドポイントから発信されたコールを SIP ビデオ エンドポイントにルーティングする、つまり SIP ビデオ エンドポイント ドメイン内の宛先とのコールを Call Bridge にルーティングするように、信頼できる SIP トランクが必要です。

SIP コール制御では、SIP ビデオエンドポイントが Lync/Skype for Business クライアントに発信できるように、Lync/Skype for Business クライアントドメイン宛ての通話を Call Bridge にルートする設定を変更する必要があります。

ダイヤル プランは、これら 2 つのドメイン間の Lync/Skype for Business 通話を両方向にルーティングします。

Meeting Server には、ファイアウォールの外側にある Lync/Skype for Business クライアントがスペースに参加できるようにする Lync Edge のサポートが含まれています。

デュアルホーム会議機能は、Meeting Server と Lync AVMCU の通信方法を改善し、Lync/Skype for Business と Cisco Meeting Server web app のユーザーの両方にとってより豊

かなミーティングエクスペリエンスをもたらします。付録 E では、デュアルホーム電話会議について説明しています。

2.12.2 デュアルホーム会議のサポート

デュアルホーム電話会議では、電話会議のルックアップのために、Lync Edge サーバーの設定を Meeting Server で設定する必要があります。 すでにオンプレミス Lync 導入または Lync フェデレーション導入が Meeting Server 導入と連携している場合、Meeting Server で追加の設定は必要ありません。 これが新規の導入である場合、Lync Edge サーバーを使用するために Meeting Serverをセットアップする必要があります。第 8 章を参照してください。

Lync/Skype for Business ミーティングの参加者のエクスペリエンスを向上させる機能の詳細については、次を参照してください。

- Lync 参加者のミーティング体験の改善に関する FAQ、
- RDP サポートに関する FAQ、
- マルチプル ビデオ エンコーダのサポートに関する FAQ。

2.13 ウェブスケジューラ

スケジューラは、エンドユーザーがウェブアプリ経由でミーティングをスケジュールできるようにする Meeting Server コンポーネントです。 Meeting Server Small、Meeting Server 2000、および VM 上の Meeting Server でサポートされています。 スペックベースの VM プラットフォーム上の Meeting Server では、スケジューラコンポーネントを実行するために、追加で 4 GB の RAM が必要です。 Meeting Server Small および Meeting Server 2000 には、追加 RAM 要件はありません。スケジューラは、SMTP メールサーバーの設定により、メール通知の送信をサポートします。 メールサーバーの設定の詳細については、Cisco Meeting Server インストールガイドを参照してください。

1 つのスケジューラが 150,000 件のミーティングをサポートします。2 つまたは 3 つのスケジューラを追加してレジリエンスを提供できますが、定員は 150,000 件のスケジュールされたミーティングのままです。 スケジュール済みミーティングのデータはMeeting Server のデータベースに保存され、クラスター化およびシングルボックスデータベース導入の両方がサポートされています。

詳細については、「スケジューラ - 展開」を参照してください。

2.13.1 ウェブアプリの UI におけるスケジューラ

- ミーティングをスケジュールするためのユーザーインターフェイスがウェブアプリユーザーに表示されます。ただし、少なくとも 1 人のスケジューラが Web Bridge への接続を確立している必要があります。 スケジューラが有効になっていない場合、ウェブ アプリ

ユーザーにはミーティングをスケジュールするためのユーザー インターフェイスは表示されません。

- 管理者が Call Bridge /Web Bridge API 経由で Web Bridge を追加、削除、または変更しても、スケジューラが自動的にこれらの変更を認識することはありません。 そのため、スケジューラを再起動する必要があります。 同様に、スケジューラが無効になっている場合、Web Bridgeはスケジューラが予期せぬ理由でダウンしているのではなく、意図的に無効になっているとは気づきません。 スケジューラが管理者によって故意に無効にされた場合、ウェブブリッジを再起動して、スケジューリングのユーザーインターフェイスが表示されないようにすることをお勧めします。
- スケジューラが無効になっているか、または他の問題のためにダウンしている場合、Web Bridgeは別のスケジューラを使用します可能な場合。 そうでない場合は、ウェブアプリユーザーにエラーが表示されます。

2.14 ミーティングアプリ

ファイル共有やアンケートなどのウェブアプリ機能は、MeetingApps サービスで導入されます。MeetingApps は、他のサービスなしでスタンドアロンの Meeting Server ノードで設定する必要があります。 参加者が外部または内部ネットワークのどちらから参加しているかに応じて、MeetingApps を DMZ ネットワークまたは内部ネットワークで設定できます。

注：MeetingApps サービスは、Meeting Server 2000 では設定できません。MeetingApps は、Meeting Server の仕様ベースの仮想化導入でのみ設定することをお勧めします。 ただし、VM 導入でミーティングアプリと共に、Call Bridge または Web Bridge として、Meeting Server 2000 または Meeting ServerSmall を使用することができます。

内部および外部ネットワークから参加するウェブアプリ参加者がいるミーティングで MeetingApps がサポートする機能を有効にするには、MeetingApps を DMZ ネットワーク上に導入する必要があります。 MeetingApps にはパブリックにアクセス可能な IP アドレスを割り当てる必要があり、パブリックアクセス用に DMZ でファイアウォールポートを開く必要があります。

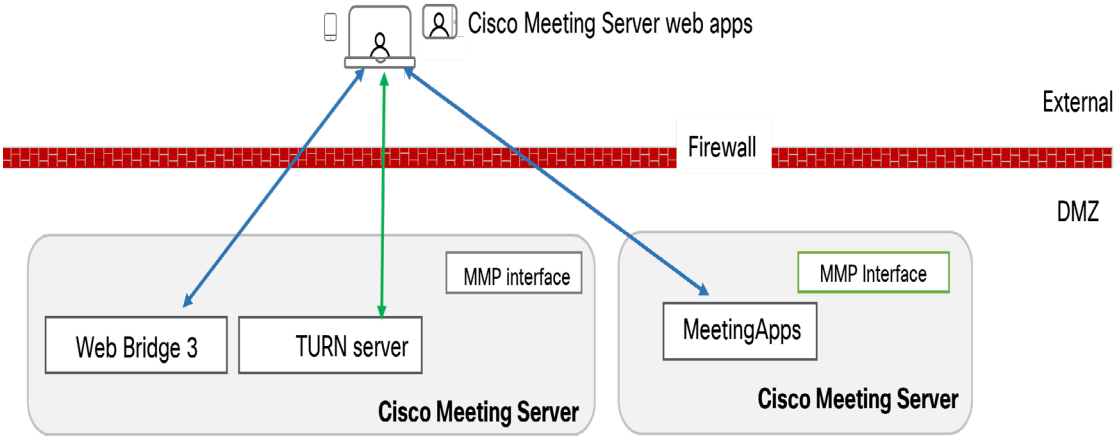
ファイル共有またはアンケートが内部のウェブアプリミーティングに参加する参加者のみに制限されている場合、MeetingApps はデータセンター内の任意の場所に展開できます。

MMP コマンド **`meetingapps`** を使用して、Meeting Server の VM 導入で MeetingApps を設定できます。

ある時点での MeetingApps のファイル保存容量は約 20 GB です。 最初にファイルが共有されてから 12 時間以内にファイルストアの容量を使い尽くす場合、ミーティングの参加者はファイルを共有できなくなります。 ファイルは 12 時間ごとに実行される内部タスクによって削除

されます。 ただし、管理者は手動でクリーンアップするオプションがあります。 MMP コマンド **meetingapps dbcleanup** を使用してファイルをクリーンアップします。 このコマンドを実行する前に MeetingApps サービスを無効にする必要があります。 このコマンドは、互換性の問題が原因でMeeting Server をアップグレードした後で、MeetingApps サービスでエラーが発生した場合にも使用できます。 そのため、Meeting Server のアップグレード後、MeetingApps サービスを有効にする前にこのコマンドを実行することを推奨します。

MeetingApps は、1 秒あたり最大 150 件の同時リクエストをサポートします。 これは、MeetingApps で毎秒最大 150 個のファイルのアップロードまたはダウンロードリクエストを処理できることを意味します。



ミーティングで共有されたファイルをアップロードまたはダウンロードするには、環境内の Web Bridge が MeetingApps と通信するように設定されている必要があります。

MeetingApps と Web Bridge 間の通信を安全にするために、MeetingApps の設定時にシークレットキーが生成されます。 MeetingApps のホスト名、ポート番号、生成された秘密鍵は、MMP コマンド **webbridge3 meetingapps add**を使用してウェブブリッジを設定するために提供する必要があります。 ウェブアプリユーザーがログインするたびに、Web Bridge は MeetingApps にユーザー認証のリクエストを送信します。

詳細は「MeetingApps を設定する」 を参照してください。

3 前提条件

3.1 ミーティングサーバーのインストールと設定の前提条件

この章では、Meeting Serverをインストールして設定する前に考慮しなければならないネットワーク設定の変更について説明します。一部の項目は事前に設定することができます。

3.1.1 DNS 設定

Meeting Serverはいくつかの DNS SRV および A レコードを必要とします。 完全な一覧については 付録 A を参照してください。特定のレコードは別の場所で言及されています。

3.1.2 セキュリティ証明書

TLS を使用するサービスの X.509 証明書とキーを生成し、インストールする必要があります。例えば、Call Bridge、Web 管理インターフェイス（Call Bridge のインターフェイス）、Web Bridge 3、TURN サーバー、ネットワークロードバランサ（使用する場合）などです。

分割導入のための『証明書ガイドライン』 には、Meeting Serverの MMP コマンドを使用して自己署名証明書を生成する方法など、証明書の背景情報と手順が記載されています。 これらの証明書は、ラボでの設定のテストに役立ちます。 しかし、本番環境では認証局 (CA) によって署名された証明書を使用することを 強く推奨します。

証明書に関連してこのガイドに記載されていた手順が削除され、証明書のガイドラインを参照する単一の手順に置き換えられました。

注：証明書に自己署名したものを使用する場合、サービスは信頼されていないという警告メッセージが表示される場合があります。 これらのメッセージが証明書を再発行し、信頼できる CA で署名してもらうのを避けるため、このコンポーネントにパブリックアクセスを希望しない限り、内部 CA を使用することができます。

3.1.3 ファイアウォールの設定

ファイアウォール上で開く必要があるポートのリストは 付録 B を参照してください。また、ファイアウォールルールの作成については セクション 15.6 を参照してください。

3.1.4 Syslog サーバ

Meeting Serverは Syslog 記録を作成します。この Syslog 記録はローカルに保存され、リモートロケーションに送信することもできます。 これらの記録は、Meeting Serverの内部ログページよりも詳細なログが含まれているため、トラブルシューティングの際に役立ちます。 内部

syslog メッセージは SFTP 経由でダウンロードできますが、Cisco はホストサーバー（Edge および Core）がデバッグ情報をリモート Syslog サーバーに送信するように設定することを推奨します。 両方の Meeting Servers が同じ Syslog サーバーを使用する必要があります。トラブルシューティングのために Syslog サーバーを使用する場合、両方の Meeting Server のログを確認してください。

メモ: Syslog サーバーは、UDP ではなく TCP を使用する必要があります。 Syslog サーバーが TCP を使用するように設定されていることを確認してください。

各Meeting Serverで以下の手順に従い、Syslog サーバーを定義します。

1. MMP に SSH でログインします。
2. 次のコマンドを入力します。 **`syslog server add <server address> [port]`** 例:

   ```
   syslog server add syslog01.example.com 514
   syslog server add 192.168.3.4 514
   ```

3. 次を入力して、Syslog サーバーを有効にします。

   ```
   syslog enable
   ```

4. 必要に応じて、Syslog サーバーに監査ログを送信する場合は、次の手順に従います。

   (監査ログ機能は、設定の変更と重要な低レベルイベントを記録します。 例えば、ウェブ管理者インターフェイスまたは API を経由してスペースのダイヤルプランまたは設定に加えられた変更は、このログファイルで追跡され、それぞれのソース IP アドレスと SSH ポートと共に変更を加えたユーザーの名前でタグ付けされます。 これにより、特に同時セッションにおいて、イベントの発生源を特定することが可能になります。 ファイルは SFTP 経由でも入手できます。)

   a. 監査ロールを持つユーザーを作成します。

      ```
      user add <username> (admin|crypto|audit|appadmin)
      user add audituser audit
      ```

   b. MMP からログアウトし、新しく作成したユーザー アカウントでログインし直します。

   c. 次のコマンドを入力します（このコマンドは監査の役割を持つユーザーのみが実行できます）。

      ```
      syslog audit add <servername>
      syslog audit add audit-server.example.org
      ```

注：通常、ローカルの Syslog ファイルは上書きされますが、**`syslog rotate <filename>`** と **`syslog audit rotate`** を使用して永久にシステムと監査ログファイルを保存できます。**`<filename>`** コマンド。 これらのファイルは SFTP 経由でもダウンロードできます。 MMP コマンドリファレンスを参照してください。

3.1.5 Network Time Protocol サーバー

1 つ以上のネットワークタイムプロトコル（NTP）サーバーを設定して、Meeting Serverコンポーネント間で時刻を同期します。

注：時間の共通ビューを共有することは様々な理由で重要です。証明書の有効性を確認する場合や、リプレイ攻撃を防ぐ場合などです。 また、ログ内のタイミングが一貫していることを確認します。

各Meeting Server上:

1. 必要に応じて、MMP に SSH で接続し、ログインします。
2. NTP サーバーをセットアップするには、次を入力します。

   ```
   ntp server add <domain name or IP address of NTP server>
   ```

設定済みの NTP サーバーの状況を確認するには、次のように入力します。 `ntp status`

MMP コマンドリファレンスで `ntp` コマンドの一覧を 参照してください。

3.1.6 通話詳細記録のサポート

Meeting Server は、サーバーに到達する新しい SIP 接続、または通話のアクティブ化または非アクティブ化など、主要な通話関連イベントに対して、内部で通話詳細レコード（CDR）を生成します。 これらの CDR をリモートシステムに送信して収集および分析するように設定できます。 Meeting Server 上にレコードを長期間保存するための規定はなく、Meeting Server 自体の CDR を参照する方法もありません。

単一の分割サーバー導入のコアサーバーは最大 4 つの CDR レシーバーをサポートするため、Meeting Management などの異なる管理ツールを導入したり、レジリエンスのために Meeting Management の複数のインスタンスを導入したりできます。

ミーティング管理を CDR 受信者として設定する方法の詳細は、『Cisco ミーティング管理管理ガイド』を参照してください。

Web 管理インターフェイスまたは API のいずれかを使用して、CDR 受信者の URI でコア Meeting Server を設定することができます。 Web 管理インターフェイスを使用している場合は、**[設定（Configuration）] > [CDR 設定（CDR settings）]** をクリックし、CDR 受信者の URI を入力します。 API を使用して CDR 受信者の URI を持つ Core Meeting Serverを設定する詳細については、『通話詳細記録ガイド』 または『API リファレンスガイド』 を参照してください。

3.1.7 ホスト名

Cisco は、各 Meeting Server に独自のホスト名を与えることを推奨しています。

1. 必要に応じて、MMP に SSH で接続し、ログインします。
2. タイプ：
   ```
   hostname <name>
   hostname london1
   ホスト名 mybox.example.com
   ```
3. タイプ：
   ```
   リブート
   ```

注： このコマンドを発行した後は再起動が必要です。

3.1.8 その他の要件

- LDAP サーバーにアクセスしてユーザーをインポートします。 これは Microsoft Active Directory (AD) サーバーまたは OpenLDAP サーバーのどちらかになります。

  ユーザーがウェブアプリを利用して Meeting Server に接続する場合、LDAP サーバーが必要です。 ユーザーアカウントは LDAP サーバーからインポートされます。 LDAP 設定で説明されているように、LDAP からフィールドをインポートすることでユーザー名を作成できます。 パスワードはミーティングサーバー上にキャッシュされません。LDAP サーバー上で集中的かつ安全に管理されます。 ウェブアプリが認証されると、LDAP サーバーへの呼び出しが行われます。

- Call Bridge でホストされている通話に到達するために使用するダイヤル プランを決定します。 ダイヤルプランは環境によって異なります。これは、発信する通話タイプが Lync、SIP（音声を含む）、ウェブアプリ通話のどれかによって決まります。 このダイヤルプランをデプロイする手順については、*「ダイヤルプランの構成 – 概要」* を参照してください。

- ソリューションをテストするために、次のうち 1 つ以上にアクセスします：Lync クライアント、SIP エンドポイント、SIP 電話、および/またはウェブアプリ（必要に応じて）。

- SIP 通話を発信する場合は、SIP コール制御プラットフォームにアクセスします。 「ダイヤルプランの構成 91 ページの「ダイヤル プランの設定 - SIP エンドポイント」 および「ダイヤル プランの設定 - Lync/Skype for Business」 では、Cisco VCS への SIP トランクを設定する方法について説明し、必要なダイヤル プラン設定の変更の概要を示します。 Cisco Unified Communications Manager (CUCM) への SIP トランク、Avaya CM および Polycom DMA の設定については、『コール制御による Cisco Meeting Server の導入』 ガイドを参照してください。このガイドに記載されていない他のコール制御デバイスを使用することもできます。

- Meeting Serverを音声導入と統合する場合、Meeting Serverは PBX に接続された音声通話コントロールデバイスに接続する必要があります。Meeting Serverを PBX に直接接続することはできません。
- Lync 環境で導入する場合、ダイヤルプラン設定の変更を行うために Lync フロントエンド (FE) サーバーへのアクセスが必要です。 必要な変更はこのドキュメントに記載されています。

3.1.9 仮想化展開のための具体的な前提条件

- 「Cisco Meeting Server仮想化デプロイメントのインストールガイド」で指定されているリソースを満たすホストサーバー。

3.2 Meeting Serverの Edge ハードウェア設定

Meeting Serverの Edge の役割は、単一のサーバーまたは複数のサーバーとして導入できます。この選択は、外部のウェブアプリ参加者に必要な同時呼び出し容量によって決まります。 参加者の大部分が外部の Web アプリ参加者であることが予想される場合は、シスコエッジ サーバーの容量がコア内の Call Bridge の容量と一致するかそれを超えるように展開することを推奨します。 Edge の容量が超過していても、Call Bridge のコア導入がサポートする数を超える参加者による接続はできないことに注意してください。 Edge は参加者に Web Bridge と TURN の能力を提供します。ただし、コアはウェブアプリの参加者に Call Bridge の能力を提供する必要があります。

3.2.1 エッジサーバーの設定

Edge サーバーロールでは、2 つの仮想マシンハードウェア設定がサポートされます。 これらの設定は、サポートされる最小ハードウェア要件と容量を定義します。

「小規模」Edge サーバー

1 x Cisco Meeting Server VM、サポート対象 Cisco ハードウェアのための次の仕様

- 4 GB RAM
- 4 vCPU
- 1Gbps ネットワークインタフェース

「大規模」Edge サーバー

1 x Cisco Meeting Server VM、サポート対象 Cisco ハードウェアのための次の仕様

- 8 GB RAM
- 16 vCPU
- 10Gbps ネットワークインターフェース

推奨プロセッサ仕様:

2.5GHz 以上で動作する Intel Xeon E5 2600 などのプロセッサ仕様を推奨します。 1 vCPU 対 1 物理 CPU を推奨します。

NIC 要件:

Cisco は、TURN Server に単一の NIC 設定を使用する分割サーバー導入をテストおよび検証しました。 そのため、バージョン 3.0 から、1 つのインターフェイスでのみ TURN Server のリスニングポートを設定することをお勧めします。

共存サポート:

Edge サーバーは他の VM と共存できます。 ただし、各 4 vCPU VM には 1 Gbps NIC 要件があり、16 vCPU には 10Gbps NIC 要件があります。 VM ホストは、すべてのアプリケーションに対して十分な NIC 容量を必要とします。

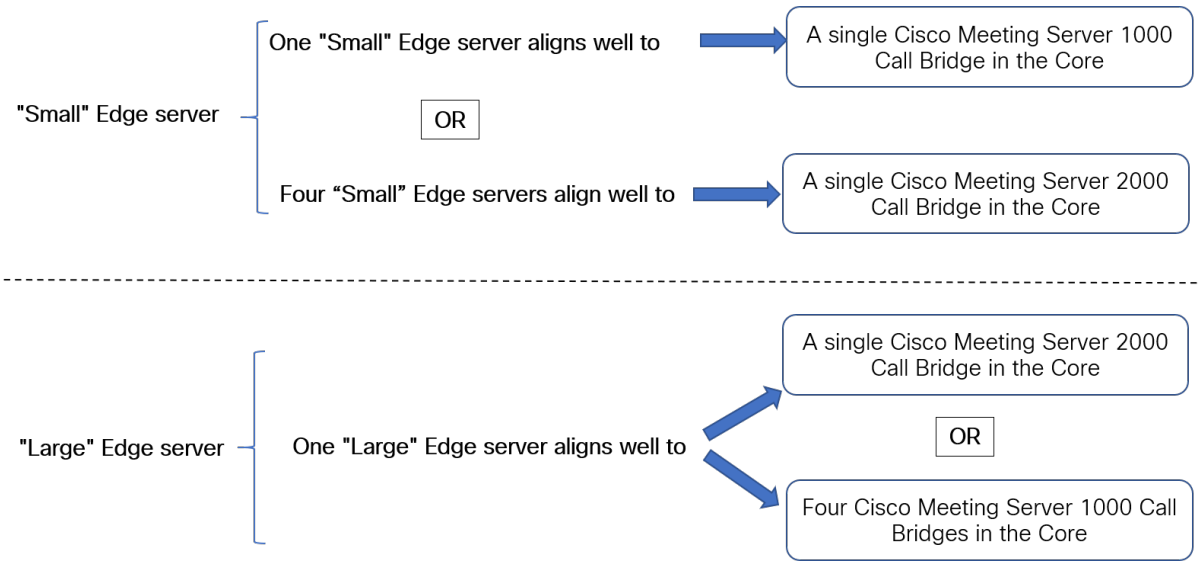
注：

- Meeting Server M5 以降のハードウェアは 10Gbps NIC をサポートします。
- CMS 2000 はMeeting Serverの Edge インスタンスとしては適していません。

表 5：Edge Server ウェブアプリのコールキャパシティ

通話のタイプ	小規模 Edge VM コールキャパシティ	大規模 Edge VM コールキャパシティ
フル HD コール 1080p30 ビデオ	100	350
HD 通話 720p30 ビデオ	175	700
SD 通話 448p30 ビデオ	250	1000
音声通話（G.711）	850	3000

2 台の Edge サーバー設定は、Call Bridge に Cisco Meeting Server アプライアンスを使用する場合に、Edge の容量とコア Call Bridge の容量を簡単に一致させる容量を提供します。



コア Call Bridge がサポートする Call Bridge コールキャパシティ、および使用されている Edge サーバーハードウェア設定を確認して、必要な Edge サーバーの数を決定します。

3.2.2 展開の考慮事項

- 同じ Call Bridge または Call Bridge グループにサービスを提供するすべてのエッジサーバーは、同じ性能、つまり、4 つの vCPU すべてまたは 16 個の vCPU であり、両方の混在ではないものにすることを推奨します。
- スケーラブルまたは復元力のある展開の場合、Call Bridge グループを設定することを推奨します。 これにより、TURN サーバーの一意のグループを各 Call Bridge グループに割り当てることができます。これは、ロード バランシングを支援し、TURN サーバーと Call Bridge の地理的位置を適切に維持するのに役立ちます。
- ウェブアプリが SIP スケール（クラスターごとに最大 24 Call Bridges）に一致するように、複数のエッジサーバーをサポートします。 ただし、Call Bridge グループは、グループごとに最大 10 台の Edge サーバーのみをサポートします。 10 台を超える Edge サーバーを必要とするスケーラブルまたはレジリエントな導入の場合、複数の Call Bridge グループが必要になります。
- Meeting Server の Edge ソリューションをサポートするために、TURN スケーラビリティモードを有効にする新しい MMP コマンド **`turn highcapacity-mode (enable|disable)`** が導入されました。 この設定はデフォルトでは有効になっています。

3.3 Meeting Server Edge のネットワーク計画

3.3.1 技術的な説明

Meeting Serverの Edge 設計では、外部参加者が到達できる Edge インスタンスを展開する必要があります。 これは、DMZ またはパブリックネットワーク内に可能です。 推奨される導入は、Edge インスタンスがNATまたは選択的なルールを持つファイアウォールの背後のDMZに導入されることです。 DMZ の Edge サーバーは、コアに導入された Call Bridge サーバーによって到達可能である必要があります。 DMZ/イントラネットの境界は、必要なトラフィックのみを許可するアクセスコントロールすることを推奨します。

ウェブアプリクライアントの接続は、Call Bridge を TLS を使用してWeb Bridge C2W インターフェイスに発信接続させ、Web Bridge 機能のコアとエッジ間のコントロールチャネルを確立することで実現します。 外部クライアントは、HTTPS を使用して Web Bridge のリスニングポートに接続します。

外部ウェブアプリ クライアントのメディア トラフィックは、TURN Server をリレーとして使用して処理されます。 認証されたウェブ クライアントは、TURN サーバーのリスニング ポートに接続し、TURN サーバーのインターフェイス上で自分に割り当てられるリレー トランスポート アドレスを要求します。クライアントと Call Bridge は、ICE を使用して、このリレーを介して相互にトラフィックを送信できること、そしてそれが最適なルートであるかどうかを確認します。 Call Bridge は、割り当てられたリレー アドレスにメディアをアウトバウンドで送信できます。このアドレスは、TURN Server によって外部クライアントに順方向に送信 (または「リレー」) されます。 クライアントからのトラフィックは TURN Server リスニング アドレスに送信され、リレー トランスポート アドレスをソースとして使用してリレーされ、Call Bridge に戻されます。 UDP ベースのメディアは、対称 UDP トラフィックを元の接続に戻すことを許可するファイアウォールによって、コアの Call Bridge に到達できます。

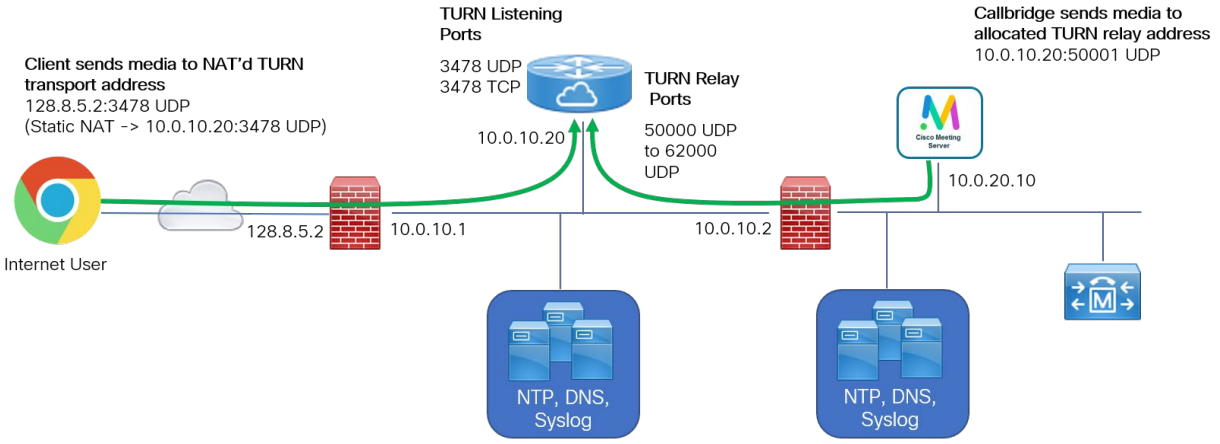
注： バージョン 3.0 以降、単一インターフェイスの TURN Server のリスニングポートを設定することをお勧めします。

外部クライアントによる TURN リレーセットアップの使用は、公開された通話キャパシティを達成するために、Edge サーバーに必要な導入モデルです。 他の組み合わせやシナリオでは、メディア接続は確立されますが、容量が減少し、メディア ルーティングが最適ではなくなる可能性があるため、推奨されません。

Meeting Server Edge の推奨導入は、外部ウェブアプリの参加者が TURN over UDP を使用して Edge インスタンスに接続し、Call Bridge が UDP 経由で TURN Relay に接続することが可能です。 この構成は、セキュリティとパフォーマンスのバランスをとるのに最適です。 制限的なクライアントネットワークとの互換性を向上させるために、2 番目の DMZ インターフェイスを追加して TURN を独自のインターフェイスに移動し、TURN over TCP 443 をサポート

するオプションのシナリオもカバーしています。 ネットワーク パスとサービス設定の他の組み合わせが技術的に実現可能である間、それらは他のセキュリティ リスク、容量への影響を招く可能性があるため、Cisco によって文書化されていないか、バリエーションを減らすためにこのガイドから除外されています。

図 9: UDP を使用した TURN のサンプルダイアグラム



3.3.2 ネットワーク計画

このセクションでは、DMZ ネットワークでMeeting Server Edge インスタンスを操作するためのネットワーク要件の概要を説明します。 使用される命名は、ネットワークに 3 つのセキュリティレベルがあることを想定しています。 インターネット、DMZ、イントラネット。 概要を説明するシナリオには、複数のMeeting Serverインスタンスと TCP フォールバックが含まれます。 宛先はロールに基づいてラベル付けされ、環境内で複数のアドレスにマッピングされる場合があります。

3.3.2.1 DMZからインターネットへの境界

DMZ はデフォルトで、承認されたトラフィックとサービスに対して、インターネットからの受信接続のみを受け入れる必要があります。 参加者がどこから接続するかわからないため、これらのサービスへの接続はすべてのソース IP から承認される必要があります。

注： DMZ ネットワークは、NAT かもしれません、または公共のインターネットから直接ルーティングできる場合があります。 この例では、DMZ が NAT であると想定しています。

ウェブアプリをサポートするには、ファイアウォールは、インターネットから、Web Bridge 3 サービスをホストするMeeting Serverの Edge サーバーのポート 443 への着信 TCP 接続を受け入れる必要があります。 HTTP リダイレクトを有効にする場合は、オプションで TCP ポー

ト 80 を有効にすることで、HTTP 接続を試みるユーザーが自動的に HTTPS にリダイレクトするようになります。 参加者は通話に HTTP を使用できません。このポートは HTTPS へのリダイレクトのみをサポートします。

メディアは UDP 経由で送信するのが最適ですが、インターネット上の通話参加者は UDP トラフィックをブロックするファイアウォールの背後にいる場合があるため、オプションの TCP フォールバックが提供されます。 メディアトラフィックの場合、ファイアウォールは TURN リスニングポート UDP 3478 で Edge サーバーへの着信接続を受け入れる必要があります。TCP を使用して TURN を有効にする場合、TURN サーバーはまた TCP 3478 および指定されたポートでリッスンします。 TCP 443 を使用して TURN を有効にする場合、TURN とWeb Bridge 3 がそれぞれ異なるインターフェイスでリッスンする 2 番目の DMZ IP インターフェイスがサーバーに必要です。

注：DMZ が NAT になっていて、複数の Edge サーバーを使用している場合、各 Edge サーバーは UDP トラフィックのイントラネットから直接アドレス指定できる必要があるため、NAT 設定で別の IP が必要です。

3.3.2.2 DMZ からインターネットへのトラフィックルール

説明	Direction	[ソースIP（Source IP）]	ソースプロトコル: ポート	ターゲット IP	ターゲットプロトコル: ポート
クライアントブラウザ HTTPS	着信	任意（Any）	TCP {未予約}	{WB3}	TCP 443
クライアントブラウザ（オプション）	着信	任意（Any）	TCP {未予約}	{WB3}	TCP 80
クライアント STUN/TURN	着信	任意（Any）	UDP {未予約}	{TURN}	UDP 3478
クライアント STUN/TURN TCP	着信	任意（Any）	TCP {未予約}	{TURN}	TCP 3478
クライアント STUN/TURN TCP 443（オプション）	着信	任意（Any）	TCP {未予約}	{TURN}	TCP 443
対称的なリターンのTURNトラフィック (通常は自動)	発信	{TURN}	UDP {3478}	任意（Any）	UDP {未予約}

注：

- {WB3} = Web Bridge 3 サーバーのリッスンインターフェイスのIPリスト
- {TURN} = TURN サーバーのリッスンインターフェイスのIPリスト
- TURN TCP 443 はオプションの導入です。 443 で TURN TCP を有効にする予定で、すでに Web Bridge 3 に TCP ポート 443 を使用している場合、別のインターフェース上にあるかどうかに関係なく、新しいMeeting Server Edge サーバーを導入する必要があります。
- ファイアウォールは、TURN Server リレーからのメディアのために、インターネットへの双方向または戻るUDPトラフィックを許可する必要があります。
- 複数の TURN Server を使用する場合、各 TURN Server はインターネットから個別にアドレス指定できる必要がある

3.3.2.3 イントラネットと DMZ の境界

デフォルトでは、イントラネットを保護するために、ファイアウォールはMeeting Server Edge サーバーインスタンスからイントラネットへの TCP 接続を許可しない必要があります。また、同じアドレス/ポートのペアで、すでに（そして最近）イントラネットからエッジボックスにUDPパケットが送信されていない限り、Meeting Server Edge サーバーからイントラネットに UDP パケットが送信されることを許可してはなりません。<DMZ IP>:50342 から <Intranet IP>:50131 へのパケットは、以前に <Intranet IP>:50131 から <DMZ IP>:50342 へのパケットがなかった場合を除き、ブロックされます。

ファイアウォールは、コアで動作する Call Bridge から C2W の待ち受けポート上の Meeting Server の Egde サーバーへの着信 TCP 接続を許可する必要があります。 また、コアで動作する Call Bridge からのインバウンド UDP パケットも許可する必要があります（つまり、ソース <any Core callridge IP>:< 32,768 to 65,535 >から接続先 <Edge CMS IP>:< 50,000 to 62,000 >)。 ファイアウォールはこれらの接続のリターン UDP トラフィックを許可する必要があります。

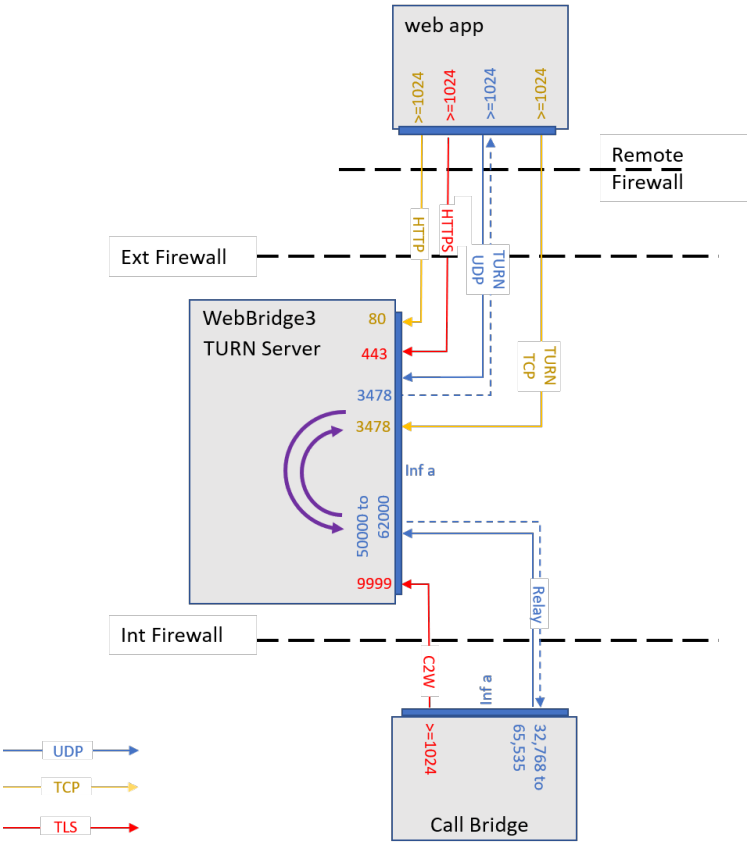
コア Call Bridge が Meeting Server の Edge ノードで直接ルーティング可能であることが望ましいですが、コア Meeting Server は DMZ サービスに対して NAT の背後にあり、外部クライアントによって割り当てられた TURN リレーを使用することができます。 コアのMeeting Serverは、TURNの待ち受けポートに接続する必要がありません。これは、外部クライアントによるリレーセットアップが両当事者にとって十分であるためです。 NAT を使用している場合、コールブリッジへのトラフィックは、ICE 接続テストでピア反射の候補と見なされます。

説明	Direction	[ソースIP（Source IP）]	ソースプロトコル:ポート	ターゲットIP	ターゲットプロトコル:ポート
Meeting Server C2W インタフェース	発信	{Call Bridge IPs}	TCP {未予約}	{WB3}	Web Bridge 3 C2W 待機ポート。 例えば、web ブリッジ 3 c2w リッスン a:9999 は TCP 9999 を使用します
Call Bridge メディア トラフィック	発信	{Call Bridge IPs}	UDP {32,768 to 65,535}	{TURN}	UDP {50,000 to 62,000}
対称的なリターン TURN トラフィック (通常は自動)	着信	{TURN}	UDP {50,000 to 62,000}	{Call Bridge IPs}	UDP {32,768 to 65,535}

注：

- {WB3} = Web Bridge 3 サーバーの IP リスト
- {TURN} = TURN サーバーの IP リスト
- Call Bridge = コア システムの Call Bridge サーバーの IP リスト
- ファイアウォールは、TURN サーバーリレーからのメディアのために、インターネットへの対称/リターン UDP トラフィックを許可する必要がある
- 単一インターフェイス上の TURN Server のリスニングポートを設定する必要があります。

図 10: TURN 3478 UDP または 3478 TCP を使用するウェブアプリ



3.3.2.4 管理およびプラットフォーム トラフィック

明確性を保つために、前のネットワーク要件のセクションでは、管理サービスとプラットフォームのニーズの要件についての説明は除外されました。 マネジメントとプラットフォームの要件はこのセクションで個別にカバーされます。 DMZ ネットワークのインフラストラクチャ サービスと管理ポリシーは組織によって異なるため、これらのトピックは、どのネットワーク境界を越えるかを説明するのではなく、Edge Meeting Server インスタンスに関連する用語で説明されます。 これらの概念をお客様の環境の詳細に適用してください。

Meeting Serverが TLS および証明書を適切に処理するには、Edge サーバーが NTP および DNS サービスにアクセスできる必要があります。 管理者はまた、SFTP および SSH を使用して、Meeting Serverソフトウェアを設定および更新する必要があります。 集中ログの Syslog はオプションですが、強く推奨されます。 これらのサービスは、既知のソースへのトラフィックの制限などの一般的なセキュリティ対策を遵守しながら、Edge の DMZ ネットワーク インターフェイスからアクセスできるように設定する必要があります。

3.3.2.5 Meeting Server Edge の管理トラフィック

説明	Direction	[ソースIP（Source IP）]	ソース Pro-to: Port	ターゲット IP	ターゲットプロトコル: ポート
NTP	発信	{WB3} または {TURN}	UDP 123	{NTP サーバー}	UDP 123
DNS	発信	{WB3} または {TURN}	UDP {unreserved}	{DNS サーバー}	UDP 53
Syslog	着信	{WB3} または {TURN}	TCP {unreserved}	{Syslog Server}	TCP 514*
アプリ管理 (SSH、SFTP)	着信	{イントラネット/管理 IP}	TCP {unreserved}	{WB3} または {TURN}	TCP 22

注：

- {WB3} = Web Bridge 3 サーバーの IP リスト
- {TURN} = TURN サーバーの IP リスト
- Syslog 接続先ポートは構成可能です
- 証明書の検証には、使用中の証明書で定義されている OSCP または CRL の宛先へのアウトバウンド接続が必要な場合があります
- Meeting Server仮想マシン (ESXi、Cisco CIMC インターフェイスなど) をホストするために使用されるサーバーハードウェアまたはハイパーバイザーを管理するために使用される他のサーバー管理テクノロジーは、ここに記載されていません。

3.3.3 Meeting Server ウェブエッジを導入する

以下の手順は、Meeting Server ウェブ Edge の導入方法の概要を説明します:

1. MMP 経由で Meeting Server エッジ上の TURN サーバーを設定します。
2. MMP 経由で Meeting Server エッジ上の Web Bridge 3 を設定します。
3. Web Bridge 3 を Call Bridge にリンクします（つまり、 callBridge パラメータを **設定 > API** の下で **/api/v1/turnServers** およびとします **/api/v1/webBridges** に追加し、Web Bridge 3 証明書の要件を確認します）。
4. 接続が正常に機能していることを確認します – これを行うには、ウェブアプリアドレス経由でログインして手動でテストするか、 **状況 > 全般** を見て **障害の状態**、および **最近のエラーと警告**を確認します。 (Web Bridge 3/TURN 接続失敗のメッセージは表示されないことに注意してください。)

5. 次のようにファイアウォール設定を追加します。
    a. Call Bridge は、API の「c2w://アドレス:ポート」で指定されたとおり、TCP 接続 Web Bridge3のc2w接続ポートに接続できる必要があります。つまり、 url フィールドにある /api/v1/webBridgesです。）
    b. Meeting Server のエッジの TURN リレー ポートは 50000 から 62000 までであるため、Call Bridge は UDP のポートに接続して、メディアを送信できる必要があります。
    c. 外部ウェブアプリ クライアントは、UDP 3478 で TURN Server に到達できる必要があります。TCP へのフォールバックが可能で、その場合のポートは「turn tls <port>」の設定に依存します。そのポートも開く必要があります。

4 MMP の設定

Meeting Serverのコンポーネントは MMP を使用して設定されます。 Meeting Serverの各インスタンスで設定が必要です。

4.1 MMP および Web 管理インターフェイスのユーザーアカウントを作成、管理する

『Cisco Meeting Server 設置ガイド』 に従って、各 Meeting Server に MMP 管理者ユーザーアカウントを作成しておく必要があります。それが済んでいれば、次の項に進みます。 同じアカウントがウェブ管理インターフェイスへのアクセスに使用されている。

（これらの MMP 管理者ユーザーアカウントがない場合は、導入に適した『設置ガイド』に記載されている緊急管理者復元手順を使用する必要があります。）

注： 追加の管理者ユーザーアカウントや他の役割を持つユーザーアカウントのセットアップを含む、すべての MMP コマンドについては、「MMP コマンドリファレンスガイド」を参照してください。

4.2 ソフトウェアをアップグレードする

数日前にソフトウェアをダウンロードした場合は、Cisco Web サイトで新しいバージョンが利用可能かどうかを確認し、利用可能であれば最新バージョンにアップグレードすることをお勧めします。

以下の手順は、すべてのタイプの導入に適用されます。

1. ミーティングサーバで実行されているソフトウェアバージョンを確認するには、サーバの MMP に SSH で接続し、ログインして次のように入力します。

   バージョン

2. Meeting Server をアップグレードする前に：

   a. 各サーバー上の現在の設定のバックアップを取ります。 バックアップをローカルサーバーに安全に保存します。 詳細については、MMP コマンドリファレンスガイド を参照してください。 アップグレードプロセス中に作成される自動バックアップファイルは使用しないでください。

   b. cms.lic および証明書ファイルをローカル サーバーに保存します。

   c. Web 管理インターフェイスを使用して、すべての呼び出し (SIP およびクライアント) が機能しており、障害状態がリストされていないことを確認します。

d. 導入にクラスター化されたデータベースがある場合、 **database cluster remove** コマンドを使用してノードのクラスターを解除します。

3. アップグレードするには、まず Cisco のウェブサイトから適切なソフトウェアファイルをダウンロードします。 この リンクをクリックし、ウェブページの右側の欄から適切なミーティングサーバーのタイプをクリックし、ダウンロードリンクと共に表示される手順に従ってください。
4. SFTP クライアントを使用して、Meeting Serverの MMP（メディア処理モジュール）に新しいソフトウェアイメージをアップロードします。 次に例を示します。

   ```
   sftp admin@10.1.124.10
   put upgrade.img
   ```

   10.1.x.y は IP アドレスまたはドメイン名です。
5. Core サーバーをアップグレードし、SSH 経由で MMP に接続し、次を入力します。

   upgrade

   サーバーが再起動し、ウェブ管理インターフェイスが利用できるようになるまで、約 10 から 12 分待ちます。
6. アップグレードが成功したことを確認するには、各サーバーの MMP に SSH で接続してログインし、次のコマンドを入力します。

   バージョン
7. Edge サーバーをアップグレードし、アップグレードが成功したことを確認します。

これでMeeting Server導入のアップグレードは完了です。 次のことを確認します。

- ダイヤル プランはそのままで、
- ウェブ管理インターフェイスとログファイルで障害が報告されないこと。

アップグレードの前にノードをクラスタ解除した場合、MMP コマンドを使用して、クラスタを戻します。

SIP およびウェブアプリ（サポートされている場合はWeb Bridge 3）を使用して接続できることを確認します。

ロールバック手順に関する注：サーバーのアップグレード後に予期せぬことが発生し、ダウングレードすることにした場合、前バージョンのソフトウェアリリースをアップロードして、**upgrade**と入力してください。 それから各サーバー上で MMP コマンド **factory_reset app** を使用します。 各サーバーが工場出荷時設定へのリセットから再起動したら、**backup rollback <name>** コマンドを使用して、サーバー上にバックアップ設定ファイルを復元します。 サーバーから作成されたバックアップファイルを復元すると、ライセンスファイルと証明書ファイルがサーバーと一致します。

4.3 Call Bridge リッスン インターフェイスの設定

Call Bridge サービスは、内部ネットワークのメインのMeeting Server インスタンスで実行する必要があります。 Call Bridge は、SIP プロキシ、Skype フロント エンド (FE) サーバーのようなピア、およびWeb Bridgeの C2W 接続との TLS 接続を確立するために使用されるキーと証明書のペアを必要とします。 ピア SIP プロキシが TLS (例: Skype for Business) を必要とする場合、証明書はピアによって信頼されている必要があります。

注： SIP および Skype 通話は、Cisco Expressway を使用してローカル ファイアウォールを通過できます。Call Bridge と Cisco Expressway 間の信頼を設定する必要があります。 Cisco Expressway は X8.9 以降を実行している必要があります。 詳細については、 Cisco Expressway Options with Cisco Meeting Serverおよび/または Microsoft インフラストラクチャ (Expressway X8.9.2) またはX8.10を実行している場合は、参照してください。 Cisco Meeting Server用 Cisco Expressway ウェブプロキシ (X8.10) および Cisco Expressway セッション 分類 導入ガイド(X8.10)。

コマンド **callbridge listen <interface>** を使用して、リッスンするインターフェイスを設定できます。 デフォルトでは、Call Bridge が最初のインターフェイス「a」でリッスンできるようにすることを推奨しています。

1. 証明書 ガイドラインの説明に従って、Call Bridge 証明書とキーを作成してアップロードします。
2. MMP にログインし、インターフェイス a でリッスンするように Call Bridge を設定します。

```
callbridge listen a
```

注： Call Bridge は、直接通信する必要がある SIP 参加者または SIP プロキシとの間に NAT を持たせないでください。 Call Bridge は、ファイアウォール トラバーサルまたは NAT の問題に対処するために、Cisco Expressway のようなファイアウォール トラバーサル ソリューションとペアリングできますが、しかし、それと SIP プロキシとの間の NAT を通過してはなりません。

3. Call Bridge が次のコマンドで使用する証明書を設定します。

   `callbridge certs <key file> <certificate file> <ca bundle>`

   例:

   `callbridge certs callbridge.key callbridge.crt ca-bundle.crt`

   証明書および CA が提供する証明書バンドルの使用に関する詳細は、証明書のガイドラインを参照してください。

4. 変更を適用するために、Call Bridge インターフェイスを再起動します。

   `callbridge restart`

4.4 HTTPS アクセスのためのウェブ管理インタフェースを設定する

ウェブ管理インターフェイスは、Call Bridge が実行されているMeeting Server インスタンスで必要ですが、Edge のMeeting Server インスタンスでは必要ありません。 攻撃対象領域を減らすには、Edge インスタンスでウェブ管理を実行しないことをお勧めします。

ウェブ管理インターフェイスは、Call Bridge のユーザー インターフェイスです。 (いずれかのインストールガイドに従い) ウェブ管理インターフェイスの証明書をセットアップしておく必要があります。 まだ行っていない場合は、今すぐ行ってください。

1. インストールは、ウェブ管理インタフェースがインタフェースのポート 443 を使用するように自動的にセットアップします。A. ただし、Web Bridgeは TCP ポート 443 も使用します。ウェブ管理インターフェイスと Web Bridgeが同じインターフェイスを使用する場合、ウェブ管理インターフェイスのポートを 445 などの非標準ポートに変更する必要があり、そのためには MMP コマンド **`webadmin listen <interface> <port>`** を使用します。
   次に例を示します。

   `webadmin listen a 445`

2. Web 管理インターフェースにアクセスできることを確認するには、Web ブラウザに以下を入力してください。 **`https://meetingserver.example.com:445`**

   機能する場合は、次のセクションに進みます。

3. ウェブ管理インターフェイスに到達できない場合:

   a. MMP にログインし、次を入力して出力を確認します。

```
webadmin
```

出力の最終行には、 **"webadmin running"** と表示されます。

b. 表示されない場合は、ウェブ管理インターフェイスの設定に問題があります。 次のように入力して、有効になっていることを確認します。

```
webadmin enable
```

c. **webadmin** コマンドの出力には、インストールした証明書の名前も含まれているはずです。例: webadmin.key および webadmin.crt。

注： 以前にアップロードした証明書と同じ名前を指定する必要があります。

これらが名前であると想定して、次を入力します。

```
pki match webadmin.key webadmin.crt
```

これにより、キーと証明書が一致することが確認されます。

d. それでも問題が解決しない場合は、証明書のガイドラインの説明に従ってトラブルシューティングを行ってください。

4.5 エッジサーバーインスタンスのステージング

外部ウェブアプリ参加者の Edge として Meeting Server を使用する場合は、この項を入力します。 Call Bridge に直接アクセスできないウェブアプリクライアントをサポートしていない場合、Meeting Server Edge は必要ないため、この項をスキップできます。

ミーティング サーバーの Edge インスタンスは、セキュリティの露出をできる限り最小限に抑えるために必要な最小限のサービスのみで構成する必要があります。 Edge サーバーインスタンスがロールを実行するには、Web Bridge 3 サービスと TURN サービスが有効になっている必要があります。 サーバーは、TLS 操作に必要なルックアップを行い、正確な時間を維持できるように、NTP および DNS クライアントを構成する必要があります。 オプションですが、中央のサーバーにログを送信するように syslog を構成することを推奨します。 導入の手順では、標準の TURN UDP 設定と、TCP 443 を使用するオプションの TURN 設定の両方をカバーします。

Web Bridgeと TURN を設定する前に、Edge 内のMeeting Serverインスタンスは、プラットフォームに関連する『インストールガイド』に従って導入され、完了している必要があります。

- サーバーの MMP インターフェイス (コンソールまたは SSH) へのセットアップアクセス
- ネットワークインターフェイスの IP 情報の設定
- サーバー上で DNS クライアントを設定しました

- サーバー上で NTP クライアントを設定しました
- 必要に応じて Syslog を設定しました

これらのタスクのヘルプについては、「設置ガイド」および「MMP コマンドリファレンス」を参照してください。

4.6 Web Bridge 3 を設定する

Web Bridge 3 は、ブラウザベースの Cisco Meeting Server web app の使用を有効にするために使用されます。 導入でウェブアプリの使用を有効にしない場合、Web Bridge サービスは必要ないため、この項をスキップできます。

- 内部ネットワークからウェブアプリクライアントをサポートする必要がある場合は、Core のメイン Meeting Server インスタンスで Web Bridge を設定し、この項の手順を完了する必要があります。
- ウェブアプリ用のプロキシおよび TURN Server として Cisco Expressway を使用している場合、コアのメインのMeeting Serverインスタンスで Web Bridgeを設定し、このセクションの手順を完了する必要があります。
- Edge Meeting Server モデルを使用している場合、Web ブリッジを Edge だけで実行するか、Edge とメインの内部Meeting Server インスタンスの両方で実行するかのオプションがあります。 内部サーバーでWeb Bridgeを有効にすると、クライアントは DMZ の Web Bridgeに接続しなくてもウェブアプリを使用できます。 Edge Meeting Server モデルを使用した導入では、DMZ と内部サーバーインスタンスの両方で Web Bridge を実行することを推奨します。 このセクションの手順を完了し、Edge インスタンスでWeb Bridgeを設定し、コアでメインのMeeting Serverインスタンスを設定します。

注： Core と Edge の両方でWeb Bridgeを実行するには、クライアントが、内部インスタンスまたは Edge インスタンス (必要に応じて) に同じWeb Bridgeのホスト名を解決する必要があります。これは通常「スプリットDNS」と呼ばれ、DNS サーバーは、クライアントが配置されている場所に基づいて、名前をアドレスに解決します。

警告：Expressway ユーザーのための重要な注意点
Web Bridge 3 および Web App の導入は、Expressway バージョン X15.4 で検証済みです。Web Bridge 3 は、それ以前の Expressway バージョンをサポートしていません。

注：ウェブアプリの詳細は、「Cisco Meeting Server web app の重要な情報」を参照してください。

4.6.1 Web Bridge 3 の設定に役立つ情報

以下は、ウェブアプリを使用できるように Web Bridge 3 を設定するのに役立つ情報です。

- 「Call Bridge to Web Bridge」プロトコル（C2W）は、Call Bridge と WebBridge3 間のリンクです。 間にコントロールチャネルを確立するのは、Call BridgeからWeb Bridgeへの発信接続です。 証明書は C2W 接続の認証とセキュリティ保護に使用されます。 C2W は Call Bridge 専用です。Web Bridge のトラフィックは、ユーザーや他のサービスによって使用されることはありません。
- C2W リスニングポートは、Call Bridge が HTTPS 接続を使用して Web Bridge に接続できるように、Web Bridge サーバー（**`webbridge3 c2w listen`** を使用）で定義されます。 使用するポート番号に既定値の設定はありませんが、このガイドでは例として 9999 を使用します。 この接続は証明書で保護する必要があります。
- 外部アクセスから C2W ポートを保護することを推奨します。Call Bridge からのみ到達可能である必要があります。
- Call Bridge は、連携するように設定された各 Web Bridge の C2W インターフェイスに一意に到達できる必要があります (C2W 接続では、Web Bridge 3 インスタンスごとに一意のホスト名または IP を使用する必要があります)。
- ウェブアプリクライアントは Web Bridge に到達するための単一のアドレスを持つため、複数の Web Bridge が使用される場合、DNS またはロード バランサ ソリューションを使用して、共有名を利用可能なウェブブリッジインスタンスに転送する必要があります。 クライアントから Web Bridge への接続は、通話以外のアクティビティではステートレスであり、セッションは単一の Web Bridge に留まる必要はありません。
- TLS 接続を確立するとき、両側は確認のために証明書を提示する必要があります。 Call Bridge は、 **`callbridge certs`** コマンドを使用して証明書セットを使用し、Web Bridgeは、 **`webbridge3 c2w certs`** コマンドを使用して証明書セットを使用します。
- Web Bridgeは、Web Bridgeの C2W トラストストアにある、または信頼ストアの **`webbridge3 c2w trust` で設定された証明書によって署名された `Call Bridge` とスケジューラの証明書を信頼します。** 特定の証明書の一致のみが許可されるように、この Web Bridge に接続する Call Bridge 証明書を含むバンドルを使用することをお勧めします（証明書ピニング）。
- Call Bridge は、Call Bridge の C2W トラストストアにある、または **`callbridge trust c2w`** で設定されたトラストストア内の証明書によって署名された Web Bridge の証明書を信頼します。 特定の証明書の一致のみが許可されるように、この Call Bridge が接続する

Web Bridge の証明書を含むバンドルを使用することをお勧めします（証明書ピニング）。

- スケジューラは、スケジューラの C2W トラストストアにある、またはコマンド **`scheduler c2w certs <key-file> <crt-fullchain-file>`**で設定された信頼ストアの証明書によって署名されたWeb Bridgeの証明書を信頼します。
- C2W または Call Bridge に使用される証明書に拡張キー使用法が定義されている場合、Call Bridge と Web Bridge の間の相互 TLS 認証交換を許可するために、使用法を有効にする必要があります。 拡張キー使用法が証明書に定義されている場合、Web Bridge 3 C2W 証明書には「サーバー認証」拡張キー使用法が含まれ、Call Bridge 証明書には「クライアント認証」拡張キー使用法が含まれる必要があります。 証明書で拡張キー使用法が定義されていない場合、すべての使用法が有効であると想定されます。
- C2W 接続は内部サービス間のみであるため、公的機関によって署名された証明書を明示的に使用する必要はありません。 MMP 内で作成された自己署名証明書を使用できます。
- Web Bridge C2W 証明書の SAN/CN は、Call Bridge API で Web Bridge3 を登録するために使用される c2w:// URL で使用される FQDN または IP アドレスと一致する必要があります。 これが一致しない場合、Call Bridge は TLS ネゴシエーションに失敗し、Web Bridgeが提示する証明書を拒否し、Web Bridgeとの接続に失敗します。

注： パブリック CA によって署名された証明書が必要な場合は、FQDN を使用する必要があります。 (パブリック CA は、IP アドレスを含む証明書に署名できません。) C2W アドレスで IP アドレスを使用する場合、C2W 接続はパブリック接続ではないため、独自の証明書を作成できます。パブリック CA を使用する必要はありません。

- Web Bridgeのリッスン インターフェイスに使用される証明書は、クライアントが信頼する認証局によって署名されている必要があります。これにより、クライアント接続時の証明書の警告が回避されます。 クライアントがWeb Bridgeに到達するために使用する FQDN は、クライアント接続時の証明書の警告を回避するために、証明書の CN または SAN リストにある必要があります。
- 証明書の一般的な情報については、導入に応じた 証明書のガイドライン を参照してください。

4.6.2 Web Bridge 3 サービスの有効化

Cisco Expressway プロキシを使用している場合、または Call Bridge に直接到達できるウェブアプリクライアントをサポートしている場合、Web Bridgeサービスはコアmeeting Serverインスタンスで有効になっている必要があります。 Meeting Serverの Edge 導入を使用する場合、

Web Bridge 3 はすべての Edge インスタンスで実行する必要があり、オプションで、Call Bridge が実行されているコア Meeting Server インスタンスでも実行できます。

Web Bridge 3 が実行される各Meeting Server インスタンスでこれらの手順を完了します。

1. MMP に SSH でログインします。
2. Web Bridgeがウェブ サーバーに使用するインターフェイスとポートを次のコマンドで設定します。

   webbridge3 https listen <interface>:<port>.

   最初のインターフェイスとポート 443 の使用を推奨します。 例:

   webbridge3 https listen a:443
3. Web Bridgeがウェブ サーバーに使用する HTTPS 証明書とキー ペアを次のコマンドで設定します。 **webbridge3 https certs <key file> <full certificate chain file>**。

   このコマンドは、証明書が完全な証明書チェーン (エンド エンティティ証明書で始まり、すべての中間署名認証局を含み、ルート証明書で終わる証明書バンドル) として定義されることを要求します。 例:

   webbridge3 https certs wb3-https.key wb3-https-fullchain.crt
4. コマンドを使用して、C2W 接続のインターフェイスとポートを設定します。

   webbridge3 c2w listen <interface>:<port>.

   最初のインターフェイスとデフォルトのサンプル ポート 9999 を使用することを推奨します。 例:

   webbridge3 c2w listen a:9999
5. C2W 接続証明書をコマンド **webbridge3 c2w certs** で設定します **<キーファイル><完全な証明書チェーンファイル>**。 例：

   webbridge3 c2w certs wb3-c2w.key wb3-c2w-fullchain.crt

   注： この証明書には、証明書の CN または SAN リストにある C2W インターフェイスの FQDN または IP アドレスが含まれている必要があります。 追加情報は、 Web Bridge 3 で使用する接続証明書を に設定するにはどうすればよいですか? も参照してください。

   ---
6. Web Bridge 3 の C2W トラストストアは、どの Call Bridge がこの Web Bridge に接続できるかを制御するように設定する必要があります。 信頼バンドルには、このWeb Bridgeに接続するすべての Call Bridge の Call Bridge 証明書、または Call Bridge 証明書に署名した CA の証明書が含まれている必要があります。 最大限のコントロールを行うために、署名機関の証明書ではなく、バンドル中の個々の Call Bridge 証明書 (証明書ピ

ニング) を使用することを推奨します。 Web Bridgeの c2w trust バンドルを次のコマンドで設定します: **webbridge3 c2w trust <certificate bundle>**

webbridge3 c2w trust wb3-c2w-trust-bundle.crt

7. http リダイレクトを有効にします。 これは任意ですが、エンドユーザーの使いやすさのために推奨されています

   webbridge3 http-redirect を有効にする

8. ウェブブリッジサービスを有効にする

   webbridge3 enable

Web Bridgeが実行される各Meeting Serverインスタンスに対して上記の手順を繰り返し、各インスタンスで使用される証明書またはキーペアが正しいことを確認します。

4.6.3 コールブリッジ C2W 接続の設定

C2W は、Call Bridge およびWeb Bridgeインスタンス間のコントロールインターフェイスであり、Web Bridgeが導入されている場合、Call Bridge で設定する必要があります。 Call Bridge の C2W 信頼バンドルには、この Call Bridge が接続するすべてのWeb Bridgeの C2W 証明書、またはWeb Bridgeの C2W 証明書に署名した証明書が含まれている必要があります。 最大限のコントロールを行うために、署名機関の証明書ではなく、バンドル中の個々の Web Bridge C2W 証明書（証明書ピニング）を使用することを推奨します。

1. Call Bridge を実行している内部Meeting Serverの MMP インターフェイスに接続します。
2. Call Bridge リッスン インターフェイスを設定する で実行した手順で、Call Bridge に証明書がすでに設定されている必要があります。 コマンド **callbridge** を実行して確認し、[キーファイル] と [証明書ファイル] の設定が設定されていることを確認します。 そうでない場合は、先に進む前に、 Call Bridge リスニングインターフェイスを設定する の手順を繰り返します。 Call Bridge は C2W 機能の証明書で設定する必要があります。
3. コマンド **callbridge trust c2w <certificate bundle file>** を使用して、Web Bridge インスタンスの C2W 証明書を含む証明書バンドルで Call Bridge の C2W トラストストアを設定します。 例:

   callbridge trust c2w c2w-callbrige-trust-store.crt

   注：対象範囲で制限されていない限り、Call Bridge は Meeting Server API で定義されているすべての Web Bridge への接続を試みます。

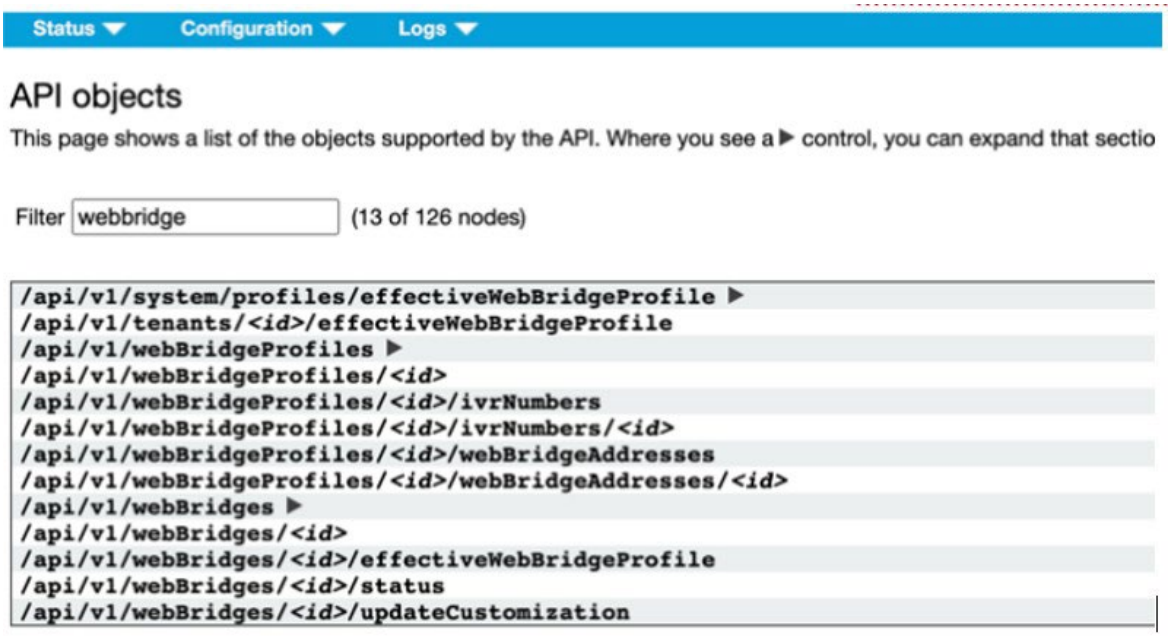
4. Call Bridge を再起動します

```
callbridge restart
```

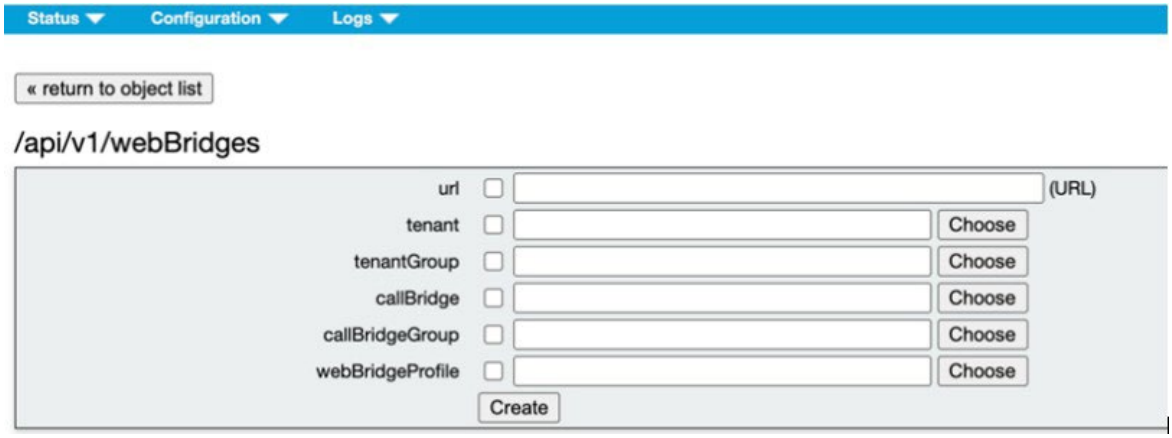
4.6.4 Web Bridge アドレスを使用して Call Bridge を設定する

Meeting Server API で Web Bridge のエントリを作成することで、Call Bridge が接続する各 Web Bridge（共存する Web Bridge を含む）の C2W アドレスを Call Bridge に通知する必要があります。 このガイドでは、Meeting Serverのウェブ管理インターフェースの API エクスプローラーを使用して、このタスクを完了する方法を説明します。

1. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）]** > [API] を選択します。
2. [フィルタ] ボックスに「 **webBridges** 」と入力し、リストビューをフィルタリングします。ここに示すように。



3. 表示されたリストから [**/api/v1/webBridges**] 行を見つけ、[▶] アイコンをクリックして導入します。
4. [Create new]をクリックして新しいWeb Bridgeオブジェクトを作成します。次のパラメータフィールドが次のように表示されます。



5. **url** フィールドには、*c2w://<Web Bridge FQDN>:<c2w port>* の形式で、追加する Web Bridge の C2W インターフェースの FQDN アドレスを入力します。 例:

   c2w://cmsedge1.company.com:9999

   注： ここで入力する FQDN は、Web Bridge 3 の C2W インターフェイスに割り当てられた証明書の CN または SAN 名のリストにあり、Web Bridgeの C2W インターフェイスの IP に解決する必要があります。 IP アドレスは、C2W 証明書が証明書の SAN または CN の IP アドレスを持つ場合にのみ使用できます。

6. 新しいWeb Bridgeエントリを保存するために **作成** をクリックします。

複数の Web Bridge がある場合は、上記の手順を繰り返し、Web Bridge の各インスタンスに対して 1 つの Web Bridge オブジェクトを作成します。

4.7 スケジューラ用のメールサーバーを設定する

このセクションでは、スケジューラコンポーネント用にメールサーバーを設定する手順について説明します。 ミーティングがスケジュール、キャンセル、または変更されると、メール通知が参加者に送信されます。 スケジューラは、SMTP メールサーバーの設定を介したメール通知の送信をサポートします。

サーバーアドレスとポートの構成、メールプロトコルの有効化、認証のためのユーザー名の設定は、次のスケジューラ MMP コマンドで指定します。

```
scheduler email server <hostname|address> <port>
scheduler email server none
scheduler email username <smtp username>
scheduler email protocol <smtp|smtps>
scheduler email auth <enable|disable>
scheduler email starttls <enable|disable>
```

サーバーアドレスが設定されていない場合、メールはスケジューラで設定されません。 スケジューラがメール招待を送信するには、少なくとも 1 つのメールサーバーを設定する必要があります。 メールは、ミーティングのスケジュールに使用されたスケジューラからではなく、任意のスケジューラから送信できます。 メールサーバーがダウンした場合、別のスケジューラがメールを送信します。

ミーティング サーバーが 5000 ミリ秒 (5 秒) 以内に Exchange 電子メール サーバーから応答を受信しない場合、スケジューラは要求を自動的に拒否します。

スケジューラは、次のタイプのメール設定をサポートしています。

1. SMTP
2. SMTP と認証済みログイン（Auth Login）
3. SMTP と STARTTLS
4. SMTP（認証ログインと STARTTLS 使用）
5. SMTPS （SMTP トランザクション全体のエンドツーエンド TLS 暗号化）
6. SMTPS（認証ログインあり）

メモ：Exchange Server 2016 CU22 - 15.1.2375.7 および Exchange Server 2019 CU11 - 15.2.986.5 の使用をお勧めします。

バージョン 3.4 から、ミーティングの招待状は共通のメールアドレスからすべての参加者に送信できます。 MMP コマンド **`scheduler email common-address <address@mail.domain> "<Display name>"`** で Meeting Server 上に共通のメールアドレスと表示名を設定します。 スケジューラが共通のメールアドレスから参加者にミーティング招待状を送信します。

共通メールアドレスが空の場合、スケジューラは開催者のメールアドレスから招待メールを送信します。

メモ：共通メールアドレスが設定されていない場合、SMTP サーバーによる認証では、MMP コマンド **`scheduler email username <smtp user-name>`** を使用してメールアドレスを設定する必要があります。 MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりにメールを送信できる適切な権限が必要です。

送信者を識別するために、表示名としてメールアドレスの他に開催者名を含めることもできます。 ウェブアプリを使用してミーティングがスケジュールされると、ウェブアプリはミーティングをスケジュールしているユーザーの名前を開催者の表示名としてスケジューラに送信します。 任意の名前を表示名として設定するには、オプションのパラメータ **`organizationDisplayName`** をスケジューラ API に含めることができます。

スケジューラが SMTP 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定ポートでリッスンするように設定します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. スケジューラを有効にします。

   scheduler enable

スケジューラが認証ログインを使用して SMTP 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコル用に指定されたポートでリッスンするように設定し、SMTP サーバーが認証ログインをサポートするようにし、認証用のユーザーアカウントを設定します。 MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりにメールを送信できる適切な権限が必要です。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

4. 認証に使用するユーザー名を設定してください。

   scheduler email username <username>

   パスワードを入力してください。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

5. スケジューラを有効にします。

   scheduler enable

スケジューラが SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートでリッスンするように設定し、STARTTLS を有効にします。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. STARTTLS オプションを有効にします。

   scheduler email starttls enable

4. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

5. スケジューラコンポーネントを有効にします。

   scheduler enable

スケジューラが Auth Login を使用した SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートでリッスンするように設定し、STARTTLS を有効にします。 さらに、SMTP サーバーを有効にしてログイン認

証をサポートし、認証に使用されるユーザーアカウントを設定し、STARTTLS を有効にします。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

4. 認証に使用するユーザー名を設定してください。

   scheduler email username <username> パスワードを入力してください。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

5. STARTTLS オプションを有効にします。

   scheduler email starttls enable

6. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

7. スケジューラコンポーネントを有効にします。

   scheduler enable

スケジューラが SMTPS 経由でメール通知を送信できるようにするには、特定のポートでエンドツーエンド SMTP 暗号化をサポートするようにメールサーバーを設定します。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. メールプロトコルを SMTPS 設定します。

   scheduler email protcol smtps

4. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

5. スケジューラコンポーネントが SMTPS を使用してメール設定を完了できるようにします。

   scheduler enable

スケジューラが Auth Login を使用した SMTPS 経由でメール通知を送信できるようにするには、特定のポートでエンドツーエンド SMTP 暗号化をサポートするようにメールサーバーを設定します。 さらに、SMTPS サーバーが Auth Login をサポートするようにし、認証に使用するユーザーアカウントを設定します。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

1. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

2. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

3. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

4. 認証に使用されるユーザーのユーザー名を設定します。

   scheduler email username <username>

   パスワードを入力します。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

5. メールプロトコルを SMTPS 設定します。

   scheduler email protcol smtps

6. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

7. スケジューラコンポーネントが Auth Login で SMTPS を使用してメール設定を完了できるようにします。

```
scheduler enable
```

4.7.1 スケジューラの詳細ログ

スケジューラは、ウェブブリッジ接続、メール通知、およびスケジューラ timedLogging MMP コマンドを使用した API の詳細なログを有効にするオプションをサポートしています。

timedLogging が有効ではない場合、Meeting Server は次の出力を表示します。

```
cms-vm> scheduler timedLogging
{
"webBridge": "0",
"api": "0",
"email": "0"
}
```

timedLogging オプションを有効にするには、次のコマンドを使用します。

```
scheduler timedLogging (webBridge|api|email) <time>
```

たとえば、

```
cms-vm> scheduler timedLogging webBridge 600
SUCCESS
```

time 変数は秒単位で表され、設定された継続時間の timedLogging を有効にします。

```
cms-vm> scheduler timedLogging
{
"webBridge": "594",
"api": "0",
"email": "0"
}
```

設定した継続時間が経過するか、特定の調査またはトラブルシューティングの手順が完了したら、SFTP を使用してログファイルをダウンロードします。

4.8 TURN Server の設定

TURN サーバーは、Call Bridge に直接到達できないウェブアプリユーザーにメディア トラバーサル サービスを提供するために使用されます。

- 導入でウェブアプリクライアントを使用していない場合は、この項をスキップできます。

- ウェブプロキシおよび TURN プロバイダとして Cisco Expressway を使用している場合、Cisco Meeting Server (X15.4) 用 Cisco Expressway ウェブプロキシの TURN サーバーと Call Bridge の設定方法についての指示を参照してください。
- Meeting Serverの Edge 展開を使用している場合、TURN Server は各 Edge インスタンスで設定されている必要があります。 この項の手順を完了して、TURN サービスを設定します。

以下のセクションを完了して、TURN Server を設定し、それを Call Bridge に追加します。

4.8.1 TURN サービスを有効にする

1. MMP に SSH でログインします。
2. TURN Server の短期資格情報モードを有効にします。 バージョン 3.1 で導入された短期間の資格情報は、以前使用されていた静的な TURN Server 資格情報に比べてセキュリティが大幅に向上します。 TURN 資格情報は、TURN Server でリレーをリクエストできるユーザーをコントロールするために使用され、TURN Server の使用を許可するために、通話のセットアップ中にウェブアプリ クライアントに自動的に与えられます。 Meeting Server Edge を使用するすべての導入で短期資格情報モードを有効にすることをお勧めします。 次のコマンドを入力して短期資格情報モードを有効にします:

   ```
   turn short_term_credentials_mode enable
   ```

3. 次のコマンドを使用して、TURN Server の短期資格情報機能の共有シークレットと領域を設定します。

   ```
   turn short_term_credentials <shared secret> <realm>
   ```

   この 2 つの値は任意の文字列で、パスワードのように扱われます。 これらの値は、Call Bridge 設定で TURN Server を定義する場合にも必要になります。 例:

   ```
   turn short_term_credentials mysharedsecret example.com
   ```

   警告：TURN Server のパスワードと資格情報は固有なものでなければなりません。 管理者のユーザー名またはパスワードを再使用しないでください。

4. TURN Server のリスニングインターフェイスが、インターネット/外部ネットワークに対して NAT の背後にある場合、TURN Server に、次のコマンドを使用して、TURN Server にマッピングするパブリック IP アドレスを設定します。

   ```
   turn public-ip <ip address>.
   ```

   お使いの TURN Server がパブリックなルーティング可能な IP アドレスを使用している場合、このステップをとばしてください。 例:

   ```
   turn public-ip 5.10.20.99.
   ```

5. 特定のインターフェイスでリッスンするように TURN Server を設定します。コマンド **turn listen <interface allowed list>** を使用します。 Web Bridge と共に最初のインターフェース「a」でリッスンするように TURN を設定する必要があります。 例:

   ```
   turn listen a
   ```

6. 3478でTURN TCPを有効にする場合、TURNサーバーが使用するべきTCPポートを設定してください。**turn tls <port|none>** command. 例:

   ```
   turn tls 3478
   ```

   この例では、TCP 3478 ポートを使用していることを想定しています。 TURN TCP を有効にしない場合は、この手順をスキップしてください。

7. TURN TCP を有効にする場合、使用する証明書とキーペアで TURN Server を設定する必要があります。 証明書は、Web Bridge の証明書に署名したのと同じ CA によって署名されている必要があります。 TURN TCP を有効にしない場合は、この手順をとばしてください。 TURN Server の証明書は、 **turn certs <key file> <certificate file>**コマンドで設定します。 **<ca cert>**. 例:

   ```
   turn certs turnCert.key turnCert.crt CAbundle.crt
   ```

   注：TURN サーバーで使用される証明書は、Web Bridge 3 証明書など、既存の証明書でもかまいません。

8. TURN Server を有効にする

   ```
   turn enable
   ```

複数の Edge Server インスタンスを使用する場合、各 Edge Meeting Server インスタンスに対して上記の TURN 設定手順を繰り返し、各インスタンスで使用される証明書/キーペアが正しいことを確認します。

4.8.2 TURN アドレスを使用して Call Bridge を設定する

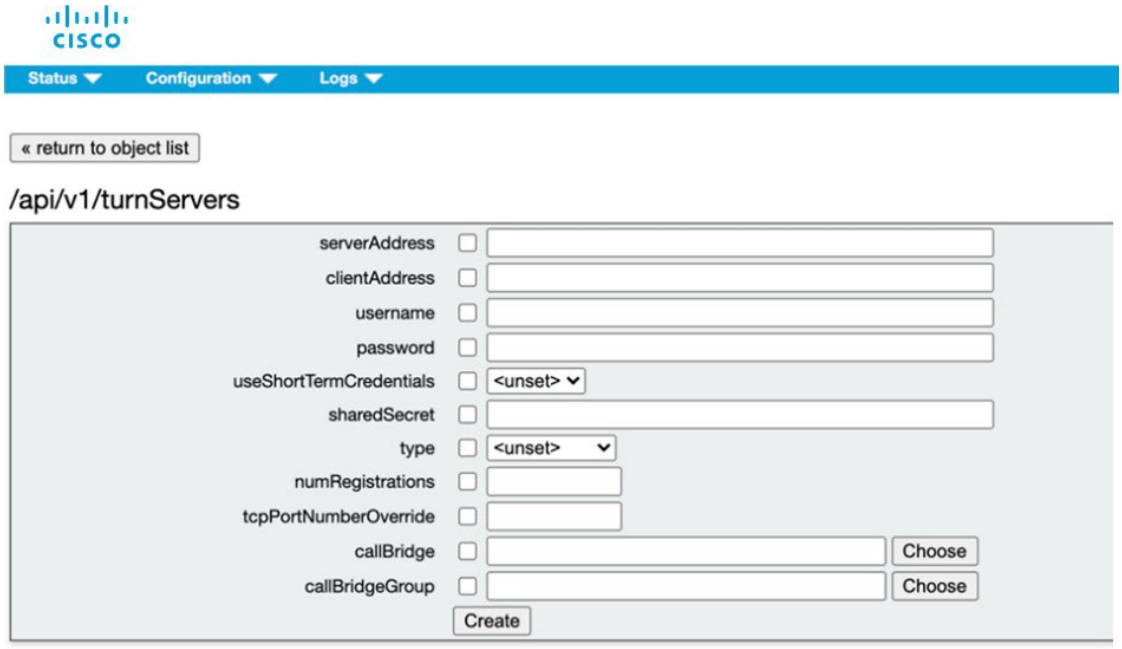
使用するには、利用可能な TURN Server の詳細を Call Bridge に設定する必要があります。これらの TURN 設定は、ウェブアプリの参加者と Skype for Business 通話フローにのみ使用されます。 Skype for Business サポートの構成の詳細については、「ダイヤル プランの構成 - Lync/Skype for Business の統合」セクションを参照してください。

Meeting Server API の各 TURN Server に対して **turnServers** エントリを作成することで、使用できる TURN Server を Call Bridge に知らせる必要があります。 このガイドでは、Meeting Serverのウェブ管理インターフェースの API エクスプローラーを使用して、このタスクを完了する方法を説明します。

1. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）]** > **[API]** を選択します。

2. [フィルター入力] ボックスに turn と入力し、次に示すようにリストビューをフィルタリングします:

3. 表示されたリストから [/api/v1/turnServers] 行を見つけ、[▶] アイコンをクリックして導入します。
4. [**新規作成**] をクリックして新しい turnServer オブジェクトを作成します。次のパラメータフィールドが表示されます:



5. 追加する TURN Server の以下のフィールドに入力します。

   serverAddress - Call Bridge が TURN Server のリスニングポートに接続する必要がある場合にのみ、TURN Server の IP アドレスまたは DNS 名を入力します。そうでない場合、Call Bridge が TURN と通信を試行しないように、ダミーのアドレスを指定します。サーバー - 例: nothing.local

clientAddress – 外部クライアントが TURN Server に到達するために使用する IP アドレスまたは DNS 名を入力します

注： TURN が NAT の場合、パブリック NAT アドレスを入力します。 例：128.8.5.2

useShortTermCredentials：前のセクションで短期証明書を使用するように TURN Server を設定した場合（推奨）、**true** に設定します。

共有シークレット – 前のセクションのステップ 3 で TURN Server を設定した際に使用した共有シークレット文字列を入力します。

type：このパラメータが設定されていない場合、デフォルトで「標準」になり、クライアントに UDP 3478 を使用し、TCP 443 にフォールバックして TURN サーバーに接続するよう指示します。 Meeting Server ウェブ Edge を展開する場合、このパラメータは「cms」に設定する必要があります。

tcpPortNumberOverride – 443 以外のポートで TURN TCP を設定した場合、turn tls コマンドで設定したポート番号を入力します。

注：この設定を使用すると、「serverAddress フィールドのダミー アドレスが原因で Call Bridge が TURN Server に接続できない」というステータスが生成される場合があります。これは既知の問題ですが、展開には影響しません。

---

6. **[作成]**をクリックして新しい TURN Server エントリを保存します。

複数の TURN Server がある場合は、上記の手順を繰り返し、各 TURN Server インスタンスの TURN Server オブジェクトを作成します。

4.9 MeetingApp の設定

Meeting Server 管理者は MeetingApps を設定して、ファイル共有やアンケートのようなウェブアプリ機能を有効にする必要があります。 ミーティング中にファイルを共有およびダウンロードできるのは、サインインしているウェブ アプリ ユーザーだけです。 調査機能の場合、ログインしたユーザーのみが調査を作成して開始することができます。 ただし、ゲストユーザーは調査にのみ参加できます。 スタンドアロンMeeting Server で MeetingApps サービスを設定することをお勧めします。

以下の設定手順に従ってください。

1. MMP に SSH でログインします。
2. MeetingApps が通信に使用するインターフェイスとポートを次のコマンドで設定します。

   `Meetingapps https リッスン<インターフェイス> <ポート>`

注：
- 構成されたポートは、内部および外部ネットワークの両方で到達可能である必要があります MeetingApp を導入する場所によって異なります。
- MeetingApps の到達可能性に関するトラブルシューティングについては、API **https://hostname/IP address:port/api/ping** を使用できます。

3. コマンド **meetingapps https certs <key-file> <crt-fullchain-file>** を使用して MeetingApp の証明書キーペアを設定します。

注： 公的に署名されたブラウザの信頼性のある CA 証明書の使用を推奨します。 内部 CA 署名付き証明書を使用する場合、CSR の生成と証明書の検証に関する情報については、『*Cisco Meeting Server リリース 証明書のガイドライン*』 を参照してください。

4. コマンドを使用して秘密鍵を生成します。

   meetingapps gensecret

   生成されたキーをコピーして、後ほど Web Bridge を設定します。 コマンドが実行されるたびに、新しい秘密鍵が生成され、Web Bridge は新しい鍵で設定される必要があります。

5. 次のコマンドを使用して、MeetingApps サービスを有効にします。

   meetingapps enable

6. MeetingApp に接続するように Web Bridge を設定する前に、次のコマンドを使用してすべての Web Bridge を無効にする必要があります。

   webbridge3 disable

7. セットアップされたすべての Web Bridge は MeetingApp と通信して、ミーティングで共有されるファイルをアップロードまたはダウンロードする必要があります。 次のコマンドを使用して、Web Bridge を MeetingApp に接続するよう設定します。

   webbridge3 meetingapps add <hostname> <port> <secretkey>

   Meeting Server 管理者は、MeetingApp の **hostname** と、**meetingapps gensecret** コマンドを使用して、先に生成した秘密鍵を提供する必要があります。

8. コマンドを使用してすべての Web Bridge を有効にします

   webbridge3 enable

4.10 MMP ユーザーの LDAP 認証

新しいldapオプションが、LDAP サーバーの詳細を設定するための user add MMP コマンドに追加されました。ディレクトリ検索パラメータ、TLS 設定、LDAP 認証の有効化または無効化を指定します。 Meeting Server の導入時に、LDAP ユーザーアカウントを持つ管理者およびウェブアプリユーザーは、LDAP 認証を使用してウェブ管理インターフェイス、SSH、SFTP、およびシリアルコンソールにログインできます。 LDAP 認証に失敗するとユーザーのログインが拒否されます。

注： Common Access Card (CAC) 導入の場合、CAC 認証は LDAP 認証およびローカル認証の両方より優先されます。

この機能では、LDAP 経由での MMP ユーザーのインポート、および既存のローカルユーザーから LDAP 認証ユーザーへの変換はサポートされていません。 管理者は LDAP ユーザを手動で事前設定する必要があります。MMP コマンド **user add** を使用して各ユーザを追加します。 ログイン名がローカルおよび LDAP ユーザーに対して一意であることを確認します。 LDAP ユーザーを追加するコマンドに、新しいオプション [**ldap**] が追加されます:

```
user add <username> (admin|crypto|audit|appadmin|api) [ldap]
```

メモ: ミーティングサーバー API は LDAP 認証によるユーザーへのアクセスをサポートしていません。

---

ldap オプションを使って追加されたユーザーの認証は LDAP サーバーが行います。 この場合、ローカルパスワードのルックアップは行われません。 ローカル ユーザーの場合、認証はローカル パスワード ルックアップのみを使用して行われます。 LDAP 認証はパスワードの変更をサポートしていません。

注：LDAP サーバーが利用できなくなった場合、または Meeting Server が LDAP サーバーに到達できない場合、LDAP ユーザーはログインできません。バックアップとして、MMP に少なくとも 1 人のローカル管理者ユーザーが設定されている必要があります。

Meeting Serverは、新しい **ldap** オプションを使用して、ホスト名/IPv4/IPV6 のいずれか 1 つとポートを使用して、Microsoft AD LDAP サーバーまたは Open LDAP サーバーの設定をサポートします。 この LDAP サーバーは、ウェブアプリのユーザー認証で使用されるものと同じものでもかまいません。 使用されている LDAP サーバーがサポートされているサーバータイプであること、そしてそれがMeeting Server用に別に設定されていることを確認してください。

詳細については、『MMP コマンドリファレンスガイド』 を参照してください。

5 LDAP 構成

ユーザーがウェブアプリを使って Meeting Server に接続する場合、LDAP サーバーが必要です（現在は Microsoft Active Directory、OpenLDAP または Oracle Internet Directory LDAP3、下記のメモを参照）。 Meeting Server が LDAP サーバーからユーザーアカウントをインポートします。

このセクションで説明するように、LDAP からフィールドをインポートすることでユーザー名を作成できます。 パスワードはMeeting Server上にキャッシュされません。ウェブアプリの認証時に LDAP サーバーへの呼び出しが行われるため、パスワードは LDAP サーバー上で一元的かつ安全に管理されます。

注： Meeting Serverで LDAP/AD 同期を設定する場合、LDAP/AD 属性を受け入れるフィールドでは、大文字と小文字を区別する形式で属性を入力する必要があります。 たとえば、ユーザー名のマッピングが属性 userPrincipalName を使用する場合、$userPrincipalName$ は同期に成功しますが、$UserPrincipalName$ は同期に失敗します。 各 LDAP 属性の大文字と小文字が正しく入力されていることを確認してください。

注： バージョン 2.1 から、Meeting Serverは Oracle Internet Directory (LDAP バージョン 3) をサポートします。 これは、Web 管理インターフェースではなく、API を通じて構成する必要があります。 ミーティングサーバーが Oracle Internet Directory をサポートするように設定する場合、ミーティングサーバーは LDAP 同期中の検索操作で LDAP ページングされた結果コントロールを使用すべきではありません。 **`/ldapServers`** に POST または **に `PUT /ldapServers/<ldap server id>`** リクエストパラメータ **`usePagedResults`** を false に設定します。

5.1 LDAP を使用する理由は何ですか?

LDAP を使った Meeting Server の設定は、環境をセットアップするための強力でスケーラブルな方法です。LDAP 構造内で組織の発信要件を定義することで、Meeting Server に必要な設定の量を最小限に抑えることができます。

サーバーはフィルター、ルール、およびテンプレートの概念を使用します。これにより、ユーザーを次のようなグループに分類できます。

- 人事部門の全員
- グレード11以上の職員

- 職名 = 'ディレクター'
- 姓が「B」で始まる人

5.2 Meeting Server の設定

この項の例では、Meeting Server の Web 管理インターフェイスを使用して、単一の LDAP サーバー（この場合は Active Directory）を設定する方法について説明します。 しかし、ミーティングサーバーは API 経由で設定可能な複数の LDAP サーバーをサポートしています。詳細は API リファレンス ガイドの LDAP メソッドセクションを参照してください。

Call Bridge のクラスタを設定する場合、API を使用するのが最も簡単な方法です。 ウェブ管理インターフェイス経由で複数の Call Bridge を設定する場合、それぞれが同一の設定になっている必要があります。

注： ウェブ管理インタフェースでは、1 つの LDAP サーバーのみ設定できます。

Active Directory と連携するようにMeeting Serverをセットアップするには、以下の手順に従ってください:

1. Web 管理インターフェイスにログインして、**設定** > Active Directoryに移動します。
2. 最初のセクションで LDAP サーバーへの接続を次のように設定します。
   - アドレス = LDAP サーバーのホスト名または IP アドレスです
   - ポート = 通常 636
   - ユーザー名 = 登録ユーザーの識別名 (DN) です。 この目的専用のユーザーを作成することもできます。
   - パスワード = 使用しているユーザー名のパスワード
   - 安全な接続 = 安全な接続を行うにはこのボックスにチェックを入れます。

     例:

     アドレス： `ldap.example.com`
     ポート： `636`
     ユーザー名： `cn=Fred Bloggs, cn=Users,OU=Sales,dc=YourCompany,dc=com`
     パスワード： `password`

     注： ユーザ名とパスワードの証明書に必要な権限の詳細は、 付録 F を参照してください。

注： Meeting Serverはセキュア LDAP をサポートしています。 デフォルトでは、LDAP サーバーは安全な通信のためにポート 636 で実行され、安全ではない通信のためにポート 389 で実行されます。 Meeting Server は両方をサポートしていますが、636 の使用をお勧めします。通信をセキュアなものにするためには、セキュア接続（上記参照）を選択する必要があります。ポート 636 の使用だけでは十分ではありません。

注：セキュアな接続を使用して、LDAP サーバーを設定する際、MMP の **tls ldap** コマンドを使用して、TLS 証明書検証が設定されるまで、接続は完全に安全ではありません。

3. インポートするユーザーのコントロールに使用するインポート設定を入力します。

- ベース識別名 = ユーザーをインポートする LDAP ツリー内のノード。 以下は、ユーザーをインポートするベース DN の賢明な選択です

  cn=Users,dc=sales,dc=YourCompany,dc=com

- フィルター = ユーザーの LDAP レコードの属性値を満たす必要があるフィルター式。フィルター フィールドの構文は rfc4515 で説明されています。

  ユーザーをメインデータベースにインポートするためのルールは、「メールアドレスを持つユーザーをインポートする」というのが妥当であり、これは次のフィルターで表されます:

  mail=*

  テスト目的で、指定ユーザ (例 fred.bloggs) と、メールアドレスが「test」で始まるテストユーザのグループをインポートする場合があります。例:

  (|(mail=fred.bloggs*)(mail=test*))

  1 人のユーザー (例: fred.bloggs) を除く全員をインポートする場合は、次の形式を使用します:

  (!(mail=fred.bloggs*))

  特定のグループに属するユーザーをインポートするために、memberOf属性でフィルタリングできます。 次に例を示します。

  memberOf=cn=apac,cn=Users,dc=Example,dc=com

  これにより、APAC グループのメンバーであるグループとユーザーの両方がインポートされます。 人々に制限する（そしてグループを省略する）には、次を使用します:

  (&(memberOf=cn=apac,cn=Users,dc=Example,dc=com)(objectClass=person))

拡張可能なマッチングルール (LDAP_MATCHING_RULE_IN_CHAIN / 1.2.840.113556.1.4.1941) を使用して、メンバーシップ階層 (指定されたグループの下) の任意のグループのメンバーシップでフィルタリングすることが可能です。例:

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=apac,cn=Users,dc=Example,
dc=com)(objectClass=person))
```

LDAP 設定に適用できるその他の良い例には、すべての Person と User を追加し、!

で定義されたものを除くフィルターが含まれます。

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))(!
(cn=Guest))(!(cn=krbtgt)))
```

上記と同じ条件を追加するフィルタ (krbtgt ユーザーを除く)。sAMAccountName を持っている場合にのみ追加します。

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))(!
(cn=Guest))(sAMAccountName=*))
```

上記と同じものを追加し (krbtgt ユーザーを含む)、sAMAccountName を持っている場合にのみ追加するフィルタ

```
(&(objectCategory=person)(objectClass=user)(!(cn=Administrator))(!
(cn=Guest))(!(cn=krbtgt))(sAMAccountName=*))
```

このフィルタは、(|(ツリー内の指定されたユーザーのみをインポートします

```
(&(objectCategory=person)(objectClass=user)(|(cn=accountname)
(cn=anotheraccountname)))
```

指定されたセキュリティグループのメンバーのみをインポートするためのGlobal Catalog クエリ（で示されます）=cn=xxxxx

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=groupname,cn=Users,
dc=example,dc=com)(objectClass=person))
```

4. フィールド マッピング式のセットアップ

   フィールドマッピング式は、Meeting Serverのユーザーレコードのフィールド値が、対応する LDAP レコードのフィールド値からどのように構築されるかを制御します。 現在、次のフィールドはこの方法で設定されます:

   - 表示名
   - ユーザー名
   - スペース名
   - スペース URI ユーザー部分 (つまり、URI からドメイン名を引いたもの)
   - スペース セカンダリ URI ユーザー部分 (スペース用のオプションの代替 URI)
   - スペース通話 ID (WebRTC クライアントのゲスト通話で使用するスペースの一意の ID)

フィールドマッピング式には、文字テキストと LDAP フィールド値の混在を含めることができます。次の通り：

$<LDAP フィールド名>$

一例として、表現

$sAMAccountName$@example.com

生成する:

fred@example.com

詳細は LDAP フィールドマッピングの詳細情報を参照してください。

注： インポートされる各ユーザーは、一意のユーザー ID (JID) を持つ必要があります。これは、「フィールドマッピング式」項のJIDフィールドを使用して構築されます。 **設定** > Active Directory。 有効な JID を構築するために、JID フィールドマッピング式で使用される LDAP 属性は、インポートされる各 LDAP レコードに存在する必要があります。 これらの属性を持つレコードのみがインポートされるように、JIDフィールドマッピング式で使用される各属性について、インポート設定のフィルターフィールドに'&'(AND)を使用してプレゼンスフィルター（つまり、(<attribute name>=*)の形式）を含めることを推奨します。

例えば、JID フィールドマッピング式が **$sAMAccountName$@company.com**であり、 次のメンバーであるユーザーをインポートするとします:グループ cn=Sales,cn=Users,dc=company,dc=com の場合、適切なインポート フィルタは次のようになります:

(&(memberOf=cn=Sales,cn=Users,dc=company,dc=com)(sAMAccountName=*))

---

5. Active Directory と同期するには、[**今すぐ同期**] を選択するか、適切な API 呼び出しを使用して同期を有効にしてください (『Cisco Meeting Server API リファレンスガイド』を参照してください)。

   注： LDAP サーバーのエントリが変更されると、手動で再同期する必要があります。

6. 同期の結果を確認するには、[**ステータス > ユーザー**] に移動します。

LDAP サーバーからのインポート時に OU 分離を使用するかどうかを選択できます。 Web 管理インターフェイスで、 [**設定** > Active Directory] に移動し、 **企業ディレクトリ設定** 項で **[検索者のOUに検索を制限]** を選択します。ユーザーアカウントの OU 内でのみ検索を有効にする。

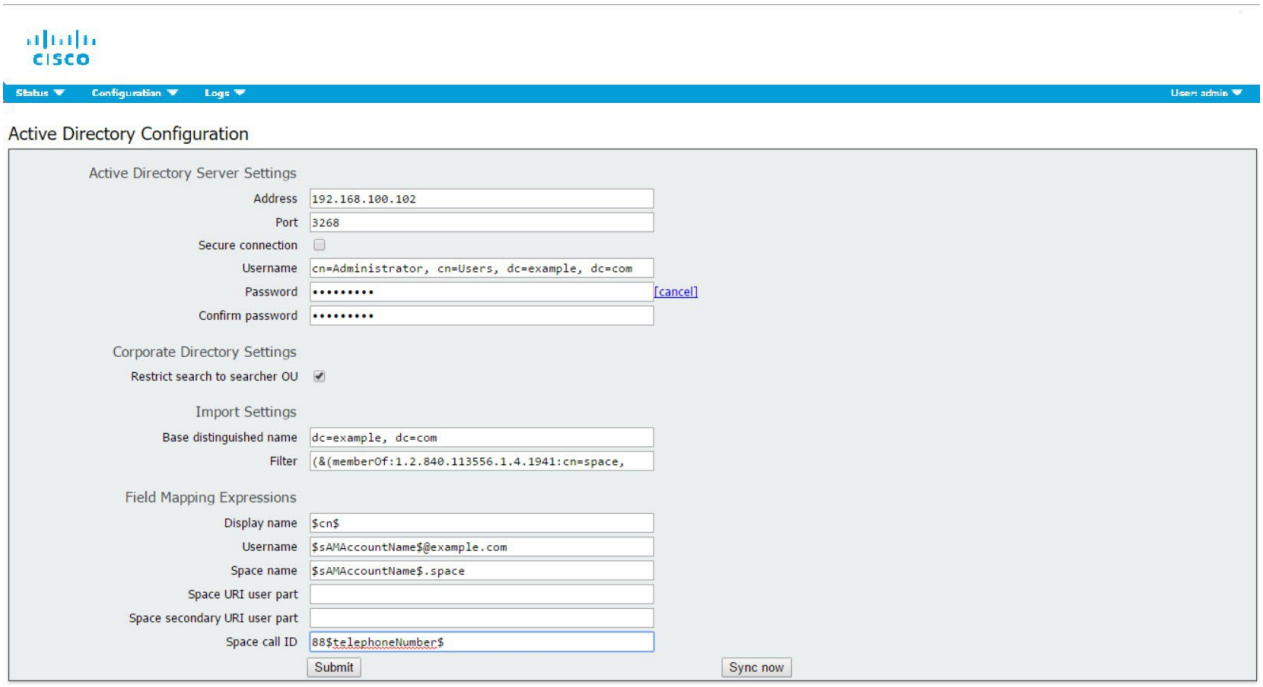
5.3 例

この例では、通常の電話番号の前の 88 プレフィックスを使用して、特定のユーザーグループとこのスペースの通話 ID にスペースを割り当てます。

1. LDAP 構造に「スペース」と呼ばれるグループを作成し、そのグループに必要なメンバーを割り当てます。

2. 拡張可能なマッチングルール (LDAP_MATCHING_RULE_ IN_CHAIN / 1.2.840.113556.1.4.1941) を使用する次のフィルターを使用して、「スペース」グループのメンバーであるすべてのユーザーを検索します。

```
(&(memberOf:1.2.840.113556.1.4.1941:=cn=space,cn=Users,dc=lync,
dc=example,dc=com)(objectClass=person))
```



3. 次に、次のディレクトリで特定のユーザーを同期します。

```
cn = Fred Blogs
TelePhoneNumber = 7655
sAMAccountName = fred.blogs
```

次のスペースが作成され、それは **状況 > ユーザー** ページで表示できます。

Name	ユーザー名
Fred Blogs	fred.blogs@example.com

次に示すスペースは、 **設定 > スペース** ページを参照してください。

Name	URI ユーザー部分
fred.blogs	`fred.blogs.space`

5.4 すべてのユーザースペースへの非メンバーアクセスにパスコード保護を適用する

LDAP 同期によりスペースが自動生成される場合、すべてパスコードなしで作成されます。デフォルトの **非メンバーアクセス** は `true` に設定されているため、既存の動作は変更されません。パスコードは必要なく、非メンバーも作成されたスペースにアクセスできます。

非メンバーアクセスを `[false]` に設定すると、会社はすべてのユーザースペースへのメンバー以外のアクセスに対してパスコード保護を強制することができます。

LDAP 同期の一環としてメンバーによる非メンバー アクセスの構成とパスコードの設定を必須にするには:

- `/ldapSources` に POST するか、 `/ldapSources/<ldap source id>` にリクエストパラメータ **非メンバーアクセス** を `false`に設定してPUTします。
- `nonMemberAccess` 設定を取得するには、on `/ldapSources/<ldap source id>` に `GET` を使用してください。

メモ: バージョン 2.4 (このパラメータが導入されたとき) より前に作成されたスペースは、LDAP 同期の影響を受けません。

---

6 ダイヤル プランの構成 - 概要

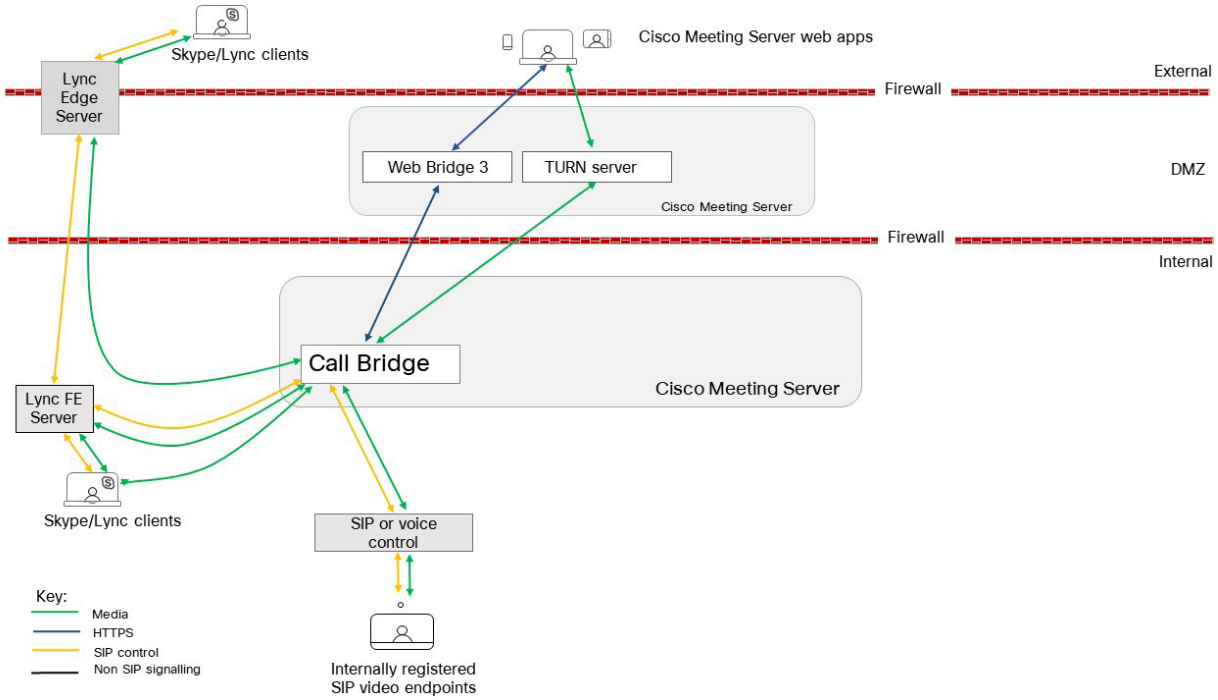
6.1 はじめに

Meeting Server を SIP、Lync、および音声環境に統合するには、SIP 通話コントロール、Lync FE サーバ、および音声通話コントロールからMeeting Server への接続をセットアップする必要があります。 Meeting Serverを必要とする通話を正しくルーティングするには、これらのデバイスで通話ルーティング設定を変更する必要があります。

図 11 は、SIP ビデオエンドポイント、Lync クライアント、および IP 電話が混在する会社の展開を想定しています。Meeting Serverは、Lync クライアントと SIP ビデオエンドポイントの間、および Lync クライアントと IP 電話の間の接続を可能にします。

SIP ビデオ エンドポイントは vc.example.com というドメインで設定され、Lync クライアントは example.com というドメインで設定されます。 必要に応じて例を変更する必要があります。

図 11: ダイヤル プラン構成の導入例



上の図に示すように、Lync FE サーバーには Meeting Server への信頼できる SIP トランクが必要です。これは、Lync クライアントから発信されたコールを Meeting Server スペース、Cisco Meeting Server web app ユーザー、さらに SIP ビデオエンドポイントにルーティング

するように構成されています。 サブドメイン vc.example.com（SIP ビデオエンドポイントの場合）および meetingserver.example.com（スペースの場合）は、Lync FE サーバーから Meeting Server にこのトランクを通じてルーティングする必要があります。

メモ: 別の組織で展開されている Office 365 またはオンプレミスの Lync への接続は、Cisco Expressway にルーティングする必要があります。 詳細については、 Expressway 導入ガイド を参照してください。

SIP コール制御プラットフォームでは、example.com ドメイン（Lync クライアントの場合）および meetingserver.example.com（スペースおよびウェブアプリの場合）への通話を Meeting Server にルーティングするように SIP トランクをセットアップする必要があります。

Meeting Server は、ドメイン example.com の通話を Lync FE サーバーに、サブドメイン vc.example.com の通話を SIP コール制御プラットフォームにルーティングするためのダイヤルプランを必要とします。

次のセクションでは、ミーティングサーバのウェブ管理インタフェースにある 2 つの設定ページについて説明します。これらの設定ページにより、ミーティングサーバが着信と発信を処理する方法が決まります。

この章に続いて、 第 7 章と 第 8 章 では、ソリューション全体の構成に関する手順を段階的に説明します。

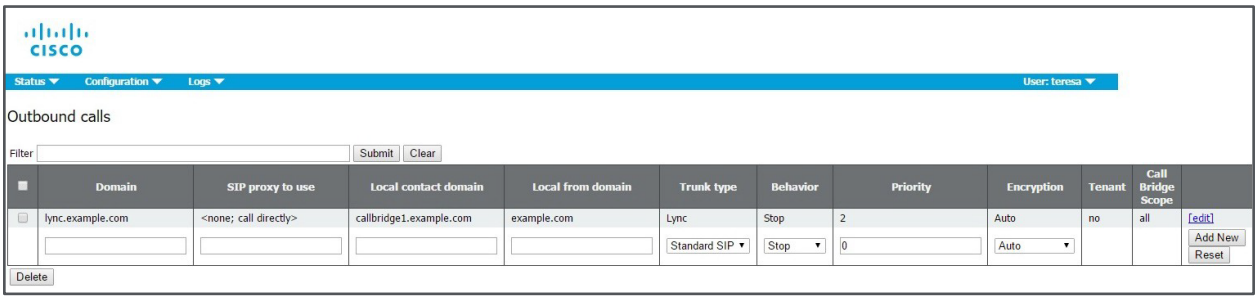
6.2 通話を管理するウェブ管理インターフェイス設定ページ

このセクションでは、各通話の処理方法を決定するためにミーティングサーバが使用するウェブ管理インタフェースの設定ページについて説明します。

ウェブ管理インターフェイスの 2 つの設定ページで、着信および発信通話に対するMeeting Serverの動作を制御します: **発信通話** と **着信通話**. [発信通話] ページでは、発信通話の処理方法を制御します。[着信] ページでは、着信を拒否するかどうかを指定します。 拒否ではなく一致して転送される場合、転送方法に関する情報が必要です。着信コールページには 2 つのテーブルがあります。1 つは一致/拒否を設定し、もう 1 つは転送設定をします。

6.2.1 アウトバウンドコールページ

[発信通話（Outbound Calls）] ページでは、ダイヤルプランルールの数を設定する適切なダイヤルプランを設定することができます。 ダイヤル変換を発信通話に適用して、発信通話のルーティングを制御できます。「ダイヤル変換」を参照してください。



ドメイン：ダイヤルプランルールを適用するために照合するドメイン、完全な値（例、「example.com」） または「ワイルドカード」（例：「*.com」のいずれかです）。

使用する SIP プロキシ：ダイヤル プランの各エントリ/ルールは、発信呼び出しのドメイン (以下を参照) と一致し、使用する SIP プロキシ (または直通呼び出しかどうか) を決定します。

ローカル連絡先ドメイン：は、このダイヤルプランルールを使用した通話の連絡先 URI に使用されるドメインです。

警告：Lync を使用している場合は、**ローカル連絡先ドメイン**を使用することをお勧めします。Lync を使用していない場合、SIP 通話フローでの予期せぬ問題を回避するために、 **ローカル連絡先ドメインの** フィールドを空にすることをお勧めします。

警告： 各 Lync ドメインに対して、アウトバウンドルールを作成する必要があります。このセクションで説明する手順に従ってください。 多くの Lync ドメインがある場合は、ワイルドカード ドメインを使用して送信ルールを作成することを検討してください。

ローカルからのドメイン：通話が発信者 ID/発信者 ID として使用するドメインです。

トランクタイプ：通常、ルールをセットアップして、発信を CiscoExpressway、Avaya Manager または Lync サーバなどのサードパーティ SIP コントロールデバイスにルーティングします。 そのため、現在設定できる SIP トランクには、標準 SIP、Avaya、Lync の 3 つのタイプがあります。

注：Meeting Server は一般的に Avaya PBX と共に使用されます。これらの通話は音声のみになります。 しかし、Meeting Serverは Avaya 製品 (ビデオをサポートする製品もあります) との相互運用性に関してこの制限を課しません。そのため、「avaya」の通話は、通話が音声のみであるという意味ではありません。

動作 および **優先度：**ダイヤルプランルールは [優先度] の値順に試されます。 ルールがマッチしたが、発信できない場合、他の優先順位の低いルールが試されます。 ルールの動作が [停止] の場合、以降のルールは使用されません。

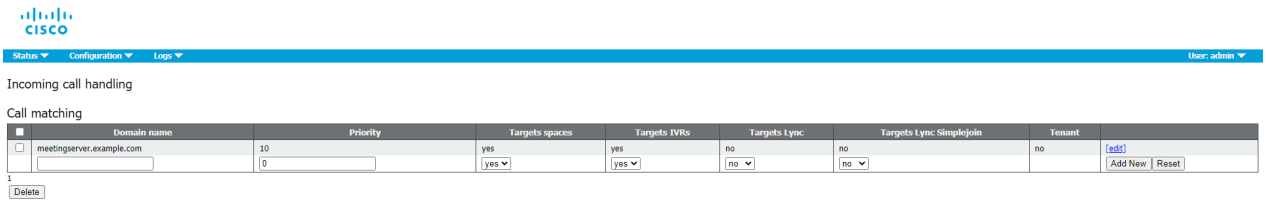
暗号化：以下から選択します: **自動**、 **暗号化**、 **非暗号化**。

警告：デフォルトの**[暗号化（Encryption）]** 動作モードは**[自動（Auto）]** です。 すべての「Lync」発信ダイヤルルールが明示的に **[暗号化（Encrypted）]** モードに設定されていることを確認し、TLS 接続試行が失敗した場合に、Call Bridge が非暗号化 TCP を使用しようとするのを防ぎます。

6.2.2 着信通話ページ: 通話の一致

着信ページの一番上の表は、コール マッチング テーブルです。 コールマッチングテーブルで定義されたルールは、Meeting Serverが着信 SIP 通話を処理する方法を管理します。 任意のドメインの Meeting Server にルーティングされた通話は、そのサーバーの IVR、ウェブアプリユーザー、または事前設定されたスペースに対してテストできます。

下記のコール マッチング ルールの例では、**meetingserver.example.com** ドメインをウェブアプリユーザーとスペースの両方にマッチさせることを試みます。



例えば、着信が **name.space@meetingserver.example.com** であり、 **name.space** という設定済みのスペースがある場合、通話はその名前のスペースにルーティングされます。

着信が予想されるすべてのドメインに対してルールを作成することをお勧めします。 一部のコール制御ソリューションでは、ドメインはサーバーの IP アドレスまたはホスト名である場合があります。 このような場合、最も優先順位の高いドメインがメイン ドメインになり、IP アドレスとホスト名のルールの優先順位が低くなります。

優先順位の値が高いルールが最初に照合されます。 複数のルールが同じ優先順位を持つ場合、ドメインのアルファベット順に基づいて一致が発生します。

ルールが実行されると、リストの下の方のルールは呼び出しで無視されます。

すべてのコール マッチング ルールが失敗した場合、次のセクションで説明されているように、次のテーブル (コール転送) が使用されます。

注意事項:

- スペースおよび/またはユーザーの照合は、@ の前の URI の部分でのみ行われます。
- 最も優先順位の高いスペースに一致するルールが、招待テキストの URI を形成するために使用されます。 個々の IP アドレスやホスト名ではなく、展開全体に対して最も高い優先順位のルールが適用されることが期待されます。

- ルールの [**ドメイン**] フィールドを空のままにしないでください。空欄にすると、Call Bridge が通話を拒否します。
- コール マッチング テーブルのルールでは、すべてのドメインが一致する結果となります。

6.2.3 通話転送

着信が [通話照合] テーブルのルールのいずれかに一致しない場合、通話は [着信の転送] テーブルに従って処理されます。 この表では、通話を完全に拒否するか、またはブリッジモードで通話を転送するか（例えば、Lync 電話会議に転送することなど）を決定するルールを定めることができます。 ルールを定義することで、通話を転送するかどうかを決定します。 特定の通話を「キャッチ」し、拒否することが適切な場合があります。

ルールは重複させることができ、[**ドメイン一致パターン（Domain matching pattern）**] にはワイルドカードを含めることができます。例：exa*.com。しかし、「*」を全てに一致する記号として使用しないでください。使用すると、呼び出しループが作成されます。 [**優先順位（Priority）**] の値を使用してルールを並べ替えます。番号が高いルールが最初に試されます。

通話を転送する場合は、[転送] ドメイン **を使用して宛先ドメインを書き換えることができます。** 指定したドメインへの新しい通話が作成されます。 [**発信者 ID**] の設定により、転送された通話で元の発信者 ID を保存するか、新しい ID を生成することができます。 選択 **パススルー** を使用して発信者 ID を保存するか、 **ダイヤルプランを使用して、**コールルーティング設定に従って新しい発信者 ID を生成します。

以下の着信転送ルールの例は、ドメイン lync.example.com の着信を転送し、ルーティングは着信ルーティング ルールによって決定されます。

Call forwarding

Domain matching pattern	Priority	Forward	Caller ID	Rewrite domain	Forwarding domain	
lync. example.com	50	forward	pass through	no		[edit]
	0	reject	use dial plan	no		Add New Reset

着信通話は、通話照合テーブルのどのルールにも一致しない場合、および着信転送テーブルのどの [**ドメイン一致パターン（Domain matching patterns）**] にも一致しない場合、終了されます。

6.3 ダイヤル変換

Dial Transforms は、発信ルールが有効になる前に発信通話に適用されます。 ダイヤル変換が適用されると、発信ダイヤルプランルールが変換された番号に適用されます。 ダイヤル変換は発信通話にのみ影響し、ゲートウェイの通話には影響しません。

変換には 3 つのステージがあります。

- 変換に適用する前処理の種類を定義する「種類」が適用されます。

- ロウ: 1 つのコンポーネントを生成します - $1
- ストリップ: ドット、ダッシュ、スペースを削除して 1 つのコンポーネントを生成します - $1
- 電話: 国際電話番号への変換に使用 - 2 つのコンポーネントを生成します $1 国コードと $2 番号

注： 電話の URI は、有効な国際ダイヤルコード (例、英国の 44、米国の 1) の後に次の電話番号の桁数が正確である場合に、純粋な数字列 (オプションのプレフィックス '+' が付き) として認識されます。

- コンポーネントは、ルールが有効かどうか確認するために、正規表現を使用して照合されます
- 出力文字列は、定義された変換に従ってコンポーネントから作成されます

例

例	タイプ	一致（Match）	変換
米国の番号については、「vcs1」を直接使用します	電話（Phone）	($1/01/)	$2@vcs1
英国の番号については、プレフィックスを追加し、「vcs2」を使用します	電話（Phone）	($1/44/)	90044$2@vcs2
7で始まるイギリスの番号には、プレフィックスとして「90044」を追加し、サフィックスとして「123@mobilevcs」を追加します	電話（Phone）	($1/44/)($2/^7/)	90044$2{}123@mobilevcs
認識されない全て数字の文字列には、サフィックスとして '@vcs3' を使用します	削除	($1/(\ d){6,}/)	$1@vcs3
+ を 00 に置換します	削除	($1/\+(\d)+/)	$1{/\+/00/}
(.*)@example.com などの英数字正規表現を置換し、と置換します \1.endpoint@vc.example.com	生	($1/(.*) @example.com/)	$1{/@example.com$/ .endpoint@vc.example.com/}

単一Meeting Server の場合、 **[設定] > [アウトバウンドコール]** ページをWeb 管理インターフェイスで使用して、ダイヤルした番号の変換方法を管理する。 一致式が指定されている場合、指定された変換式が適用されるかどうかは、正規表現により決定されます。

例えば、下のスクリーン ショットのダイヤル プランにより、発信の「+1」(米国) コールで 1 つの Call Bridge が使用され、+44 (英国) のコールで別のものが使用されるようになります。

7 ダイヤル プランの構成 - SIP エンドポイント

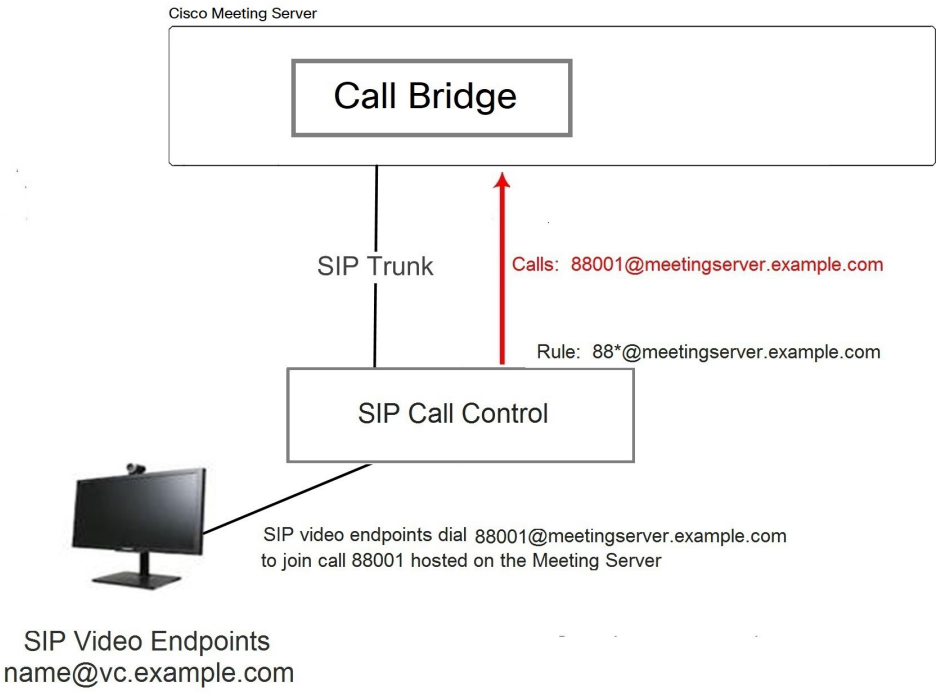
7.1 はじめに

この章では、SIP ビデオエンドポイントがMeeting Server で主催されているミーティングにダイヤルインするための設定について説明しています。 必要に応じて例を変更しながら、記載されている順番に手順を実行してください。

7.2 SIP ビデオエンドポイントが Meeting Server でホストされているミーティングにダイヤルする

この最初のステップでは、SIP ビデオエンドポイントを Meeting Server で主催されているミーティングに指向するために、コール制御デバイスと Meeting Server で必要な設定を検討します。

図 12: Meeting Serverがホストする通話に発信する SIP ビデオエンドポイントの例



7.2.1 SIP 通話コントロールの構成

この例では、SIP コール制御が Cisco VCS であると想定していますが、Cisco Unified Communications Manager を使用するなど、他のコール制御デバイスでも同様の手順が必要

です。「Cisco Meeting Server with Cisco Unified Communications Manager 導入ガイド」を参照してください。

1. VCS に管理者としてログインします。
2. ゾーンをセットアップして通話を Meeting Server にルーティングします。
   a. 次に進む **VCS 設定 > ゾーン > 新規**。
   b. 以下を使用してゾーンを作成します。
      - H.323 モード = オフ。
      - SIP モード = オン
      - SIP ポート = 5060 (5061) (TLS を使用する場合)
      - SIP トランスポート = TCP または TLS (必要に応じて)
      - SIP プロキシ登録の許可 = 許可
      - 認証ポリシー = 認証済みとして扱う
      - SIP 認証信頼モード = オフ
      - ピア 1 アドレス = Call Bridge の IP アドレス
3. 通話を Meeting Server にルーティングするための検索ルールを追加します。 たとえば、ドメイン **`meetingserver.example.com`**を使用してSIPエンドポイントの通話をMeeting Serverのミーティングにルーティングします。
   a. **VCS 設定 > ダイヤルプラン >検索ルールに移動します。**
   b. ルールに適切な名前を付けます。例えば **`Meeting Server への EP のルーティング`** など。
   c. 以下を設定します。
      - ソース = 任意
      - リクエストの認証が必要 = いいえ
      - モード = エイリアスパターンマッチ
      - パターンタイプ = Regex
      - パターン文字列 = **`.*@meetingserver.example.com`**
      - パターン動作 = そのままにする
      - 一致した場合 = 停止
      - ターゲット = Meeting Server用に作成したゾーン。

7.2.2 Meeting Server の設定

1. Meeting Server のWeb 管理インタフェースにログインします。
2. エンドポイントがダイヤルインするためのスペースをMeeting Server上に作成することもできます：
   a. **設定 > スペースへ進む**
   b. スペースを追加する方法:
      - Name =<string>、例： `Call 001`
      - URI =<user part of the URI>、例： `88001`

   または既存のスペースを使用してください。

注： スペースは API から作成または変更することもできます。 詳細については、 API リファレンス ガイドを参照してください。

---

3. Meeting Serverへの着信通話用のインバウンドダイヤルプランルールを追加してください。
   a. **[設定（Configuration）] > [着信コール（Inbound Calls）]** に移動し、次の詳細のダイヤルプランルールを追加します:
      - **ドメイン名** = <FQDN of the Meeting Server>、例 `meetingserver.example.com`
      - **スペースを対象とする** = **はい**
      - **IVRを対象とする** = **はい**
      - 任意の **ユーザ対象** = **はい**
      - **ターゲット** Lync = **はい** 注：これは後の セクション 8.1.2 で必要です

注: 管理インターフェース**の着信通話ページ**の詳細については、80 ページの「着信通話ページ: 通話の一致」を参照してください。

---

4. VCS 経由で SIP エンドポイントへの発信通話のための発信ダイヤルプランルールを追加します。
   a. **[設定（Configuration）] > [発信コール（Outbound Calls）]** に移動し、次の詳細のダイヤルプランルールを追加します。
      - **ドメイン** =<domain to match>例：`example.com` または `*.com`
      - **使用する SIP プロキシ** = <the IP address or FQDN of your VCS>
      - **ローカル連絡先ドメイン** =

メモ: ローカル連絡先ドメインのフィールドは、Lync へのトランクをセットアップしない限り、空白にしておきます (セクション 8.1.2 参照)。

- **ローカル送信ドメイン** = <FQDN of the Meeting Server>
- **トランクタイプ**=**標準** `SIP` です。

注: Web 管理インターフェイスの**発信通話ページ**の詳細については、86 ページ「の発信通話」を参照してください。

SIP ビデオエンドポイントは、ダイヤルすることで Meeting Server でホストされる 88001 の通話にダイヤルすることができます。 `88001@meetingserver.example.com`, ミーティングサーバーは SIP エンドポイントをコールアウトできます。

第 8 章の Lync のダイヤルプランの作成に移る前に、次のことを検討してください:

- メディア暗号化設定を設定するには、第 7.3 項を参照してください。
- Cisco CTS エンドポイントの TIP サポートを有効にするには、項 7.4 を参照してください。
- 自動音声応答(IVR)を設定するには、第 7.5 項を参照してください。

7.3 SIP 通話のメディア暗号化

Meeting Server は、Meeting Server との間で行われる、Lync 通話を含む SIP 接続のメディア暗号化をサポートしています。 これはウェブ管理インターフェイスの **設定 > 通話設定** ページで設定します。

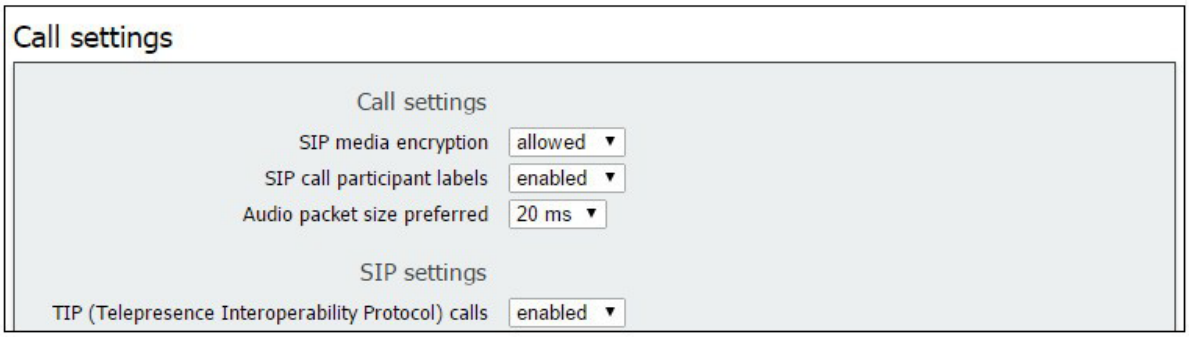
1. ウェブ管理インターフェイスにログインし、 **設定 > 通話設定**に移動します。
2. 適切な [**SIP メディア暗号化**] **設定** (許可する、 必須とする または **無効**)を選択します。
3. SIP、CMA (ウェブアプリ)、またはサーバーリフレクシブの帯域幅設定を変更します。
4. これらの変更をすでに進行中の SIP 通話に適用することを選択するには、ページの最後にある **[アクティブな通話に適用する]** ボタンをクリックするか、または今後の SIP 通話にこれらの変更を適用することを選択します [**送信**] ボタンをクリックします。

注: Web 管理インターフェースの **[設定] > [発信通話]** ページの [SIP 暗号化] フィールドでは、各 [発信通話]ルールの SIP 制御暗号化動作を設定できます。 これにより、コントロールとメディア暗号化の動作が分離され、メディア暗号化がない場合でも TLS コントロール接続を使用できます。API を使用して動作を設定することもできます。

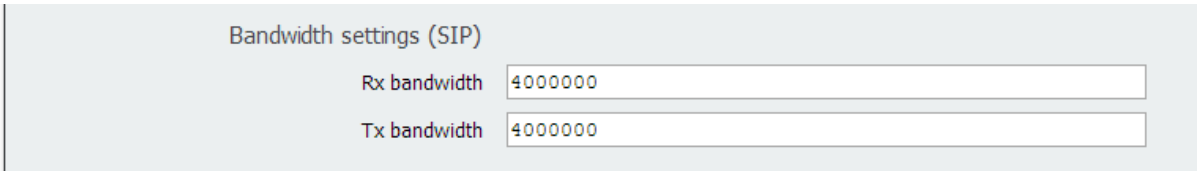
7.4 TIP サポートを有効にする

Cisco CTS 範囲のエンドポイントを使用する場合、TIP プロトコルサポートを選択する必要があります。 次の手順で有効にします。

1. ウェブ管理インターフェイスで **[設定 > 通話設定]** に移動し、SIP設定セクションでTIP (Telepresence Interoperability Protocol) を **有効にします。**



2. 両方の SIP 帯域幅設定を少なくとも 4000000 に設定してください。



3. **[送信（Submit）]** をクリックします。

7.5 IVR 設定

事前設定された通話に手動でルーティングするように、Interactive Voice Response (IVR) を設定できます。 着信通話は IVR にルーティングすることができます。ここで発信者は、参加する通話またはスペースの ID 番号を入力するように招待する、事前に録音されたボイス メッセージで挨拶されます。 ビデオ参加者にウェルカム スプラッシュ画面が表示されます。 ID を入力すると、ユーザーは適切な通話またはスペースにルーティングされるか、通話またはスペースに PIN がある場合は PIN の入力が求められます。 (発信者は 3 回目の間違ったコール ID の後に切断されます。)

IVR を使用する場合は、次の手順に従ってください:

1. ウェブ管理インターフェイスにログインして、 **設定 > 全般**に移動します。
2. [IVR] 項で次を設定します:
   - **IVR 数値 ID** = <numeric call ID that users call to reach the IVR>

- **ID によるスケジュール済み Lync 電話会議への参加**= 許可しないまたは許可する (ポリシーにより異なります)。

3. で **設定 >着信** 設定する **ターゲット IVR** = "yes" は、IVR への着信を照合します。
4. SIP コール制御で適切なルーティングを設定し、前の手順で設定した番号への通話が Meeting Server にルーティングされるようにします。

7.6 次のステップ

第 8 章 の手順に従い、ミーティングサーバを Lync 展開と統合するためのダイヤルプランを設定してください。

8 ダイヤルプランの構成 – Lync/Skype for Business の統合

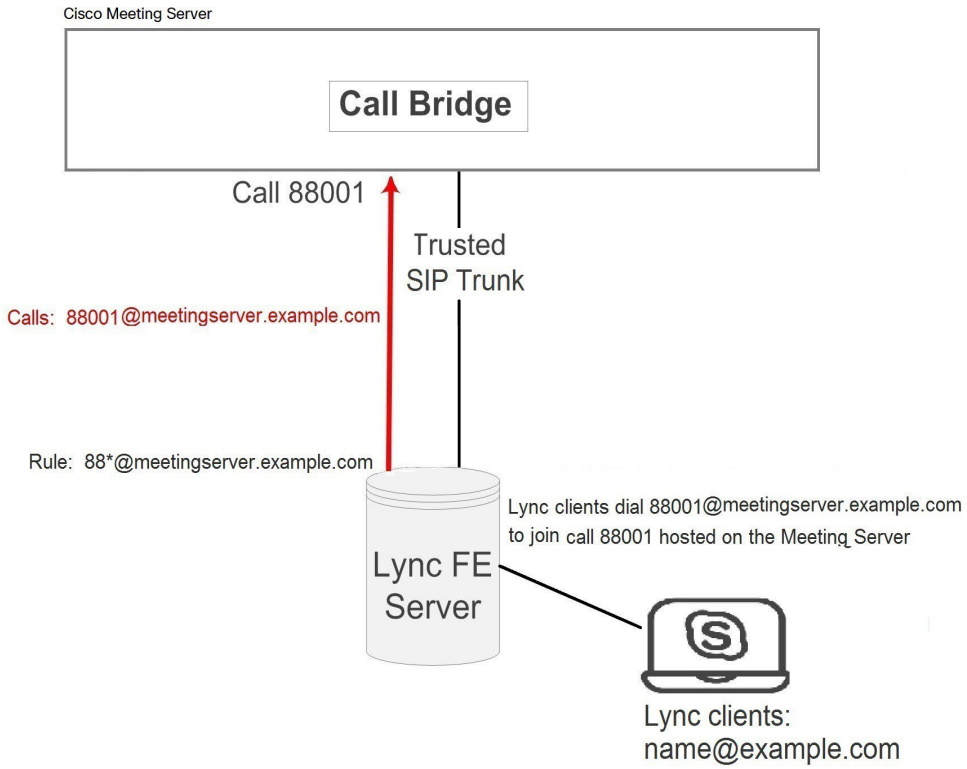
この章を通じて、Microsoft Lync という場合は、Microsoft Skype for Business を意味します。

注： Call Bridge と Lync Edge の統合では、Call Bridge 専用のログイン アカウントが必要です。 Call Bridge との間の Lync 通話ごとに、サーバーはそのアカウントを使用して、Lync Edge に TURN リソースを要求します。 その通話が切断されるまで、そのリソースは Lync の観点から「使用済み」と見なされます。 Lync では、ユーザーアカウントごとに最大 12 の TURN 割り当てのみが許可されます。したがって、1 回の登録では、最大 12 通のコールが可能です。

8.1 Meeting Server上の通話にダイヤルインする Lync クライアント

この項では、Lync エンドポイントがMeeting Server で主催されるミーティングに参加するために必要な設定について詳しく説明します。 セクション 7.2 で使用されたものと同じ呼び出し番号/URI を使用します。必要に応じて例を変更してください。

図 13: Meeting Serverが主催するミーティングに発信する Lync クライアントの例



8.1.1 Lync フロントエンド (FE) サーバーの設定

警告：のセクションでは、Lync FE サーバとMeeting Server間のスタティックルートの設定例を提供します。これはガイドラインにすぎず、必ずしもあなたが従うべき手順を示すものではありません。 お使いのサーバーに同等の機能を実装するための最良の方法については、お近くの Lync サーバー管理者に問い合わせることを強くお勧めします。

注：Lync FE サーバからのスタティックルートを設定する前に、Meeting Server に Lync FE サーバーから信頼される証明書がインストールされていることを確認してください。『証明書ガイドライン』に記載されています。

Lync クライアントからの通話を Meeting Server にルーティングするには、Meeting Server を指す Lync スタティックルートを追加します。 これには、Lync FE サーバの信頼できるアプリケーションとしてミーティングサーバを設定し、スタティックルートを追加することが含まれます。

1. Lync Server 管理シェルを開きます。

2. 信頼済みアプリケーションとしてMeeting Server を含む新しいアプリケーションプールを作成します。

   ```
   New-CsTrustedApplicationPool -Identity fqdn.meetingserver.com -
   ComputerFqdn fqdn.meetingserver.com -Registrar fqdn.lyncserver.com -site 1
   - RequiresReplication $false -ThrottleAsServer $true -TreatAsAuthenticated
   $true
   ```

   置換する

   - **fqdn.meetingserver.com** ミーティングサーバの FQDN を使用する場合、アイデンティティは Call Bridge の証明書で指定された CN である必要があります。
   - **fqdn.lyncserver.com** をあなたの Lync FE サーバまたは FE プールの FQDN として使用します。

3. Meeting Server を信頼できるアプリケーションとしてアプリケーションプールに追加します。

   ```
   New-CsTrustedApplication -ApplicationId meetingserver-application -
   TrustedApplicationPoolFqdn fqdn.meetingserver.com -ポート 5061
   ```

   置換する

   - **meetingserver-application** を任意の名前で
   - **fqdn.meetingserver.com** を Meeting Serverの FQDN に

4. Meeting Server と Lync FE サーバー間のスタティックルートを作成します。

   ```
   $x=New-CsStaticRoute -TLSRoute -Destination "fqdn.meetingserver.com" -
   MatchUri "meetingserver.example.com" -Port 5061 -UseDefaultCertificate
   $true
   ```

   置換する

   - **fqdn.meetingserver.com** をMeeting Serverの FQDN に
   - **meetingserver.example.com** あなたのMeeting Serverのすべての通話で使用されるドメインと一致するURI。

5. 新しいスタティック ルートを既存のスタティック ルートのコレクションに追加します。

   ```
   Set-CsStaticRoutingConfiguration -Identity global -Route @{Add=$x}
   ```

6. 任意。 静的ルートを有効にする前に、Lync 通話の既定の画面解像度を既定の VGA から HD720p に変更することを検討してください。 Lync で HD720p を有効にするには:

   ```
   Set-CsMediaConfiguration -MaxVideoRateAllowed Hd720p15M
   ```

7. 新しいスタティック ルートを有効にします。

   ```
   Enable-CsTopology
   ```

注： 新しい HD720p 設定に更新するには、ユーザーはいったんログアウトして、もう一度ログインする必要があります。他のすべての設定は自動的に行われ、数分以内に有効になります。

8.1.2 Meeting Server にダイヤルプランルールを追加する

1. Meeting Serverのウェブ管理インターフェイスにログインして、**設定 > 発信通話**
2. [発信通話（Outbound calls）] テーブルの一番下で、新しいダイヤルプランルールを作成します。
   a. **[ドメイン（Domain）]** フィールドで、Lync に送信する必要がある通話の照合を行う Lync ドメインを入力します。 例えば, **`example.com`**
   b. **フィールド** 使用する SIP プロキシで、発信に使用するプロキシデバイスのアドレス (IP アドレスまたは FQDN) を入力します。
      - このフィールドを空欄にしておくと、サーバーは **`_sipinternaltls._tcp.<yourlyncdomain>.com` を使用して、呼ばれたドメインの DNS SRV ルックアップを実行します。**
      - または、フロントエンドプール (または Lync SIP ドメイン) の IP アドレスまたは FQDN を入力すると、サーバーはまず、その定義されたドメインに対して DNS SRV ルックアップを実行します。 **`_sipinternaltls._tcp.<サーバアドレス>.com`**そして、SRV ルックアップが解決に失敗した場合に入力したホストの DNS A レコードルックアップを実行します。
      - または Lync FE サーバーの IP アドレスまたは FQDN を入力します
   c. **[ローカル連絡先ドメイン（Local Contact Domain）]** フィールドで、Meeting Server の FQDN を入力します。 次に例を示します。
      `meetingserver.example.com`

      注： Lync へのトランクをセットアップする場合にのみ、このフィールドを設定します。それ以外の場合は、空白にしておく必要があります。

   d. **ローカル [ドメイン]** フィールドに、通話の発信元とみなしたいドメイン (発信者 ID) を入力します。例: **`meetingserver.example.com`**

      注：[ローカルからのドメイン（Local From Domain）] を空のままにしておくと、発信者番号 ID に使用されるドメインは、デフォルトで [ローカル連絡先ドメイン（Local Contact Domain）] になります。

   e. **トランクタイプ** フィールドで、[**`Lync`**] を選択します

f. [**行動**] フィールドで [**停止**] または [**続行**] を選択します。このルールが接続された通話を結果としない場合に、次の発信ダイヤルプランルールが試行されるかどうかによります。

g. **[優先順位（Priority）]** フィールドで [優先順位レベル（Priority level）] を指定し、適用されるダイヤルプランルールの順序を決定します。 優先順位値の高いルールが最初に適用されます。

h. **暗号化** フィールドで [**自動**]、[**暗号化**] または [**未暗号化**] を選択します。このルールを通じて行われる通話の暗号化されたSIP制御トラフィックが強制されるかどうかによります。

i. **[新規追加（Add New）]** を選択します。

メモ：テナントと Call Bridge の範囲は、API を介してのみ設定できます。

完了すると、Lync 環境から Meeting Server に、および Meeting Server から Lync に発信できるようになります。

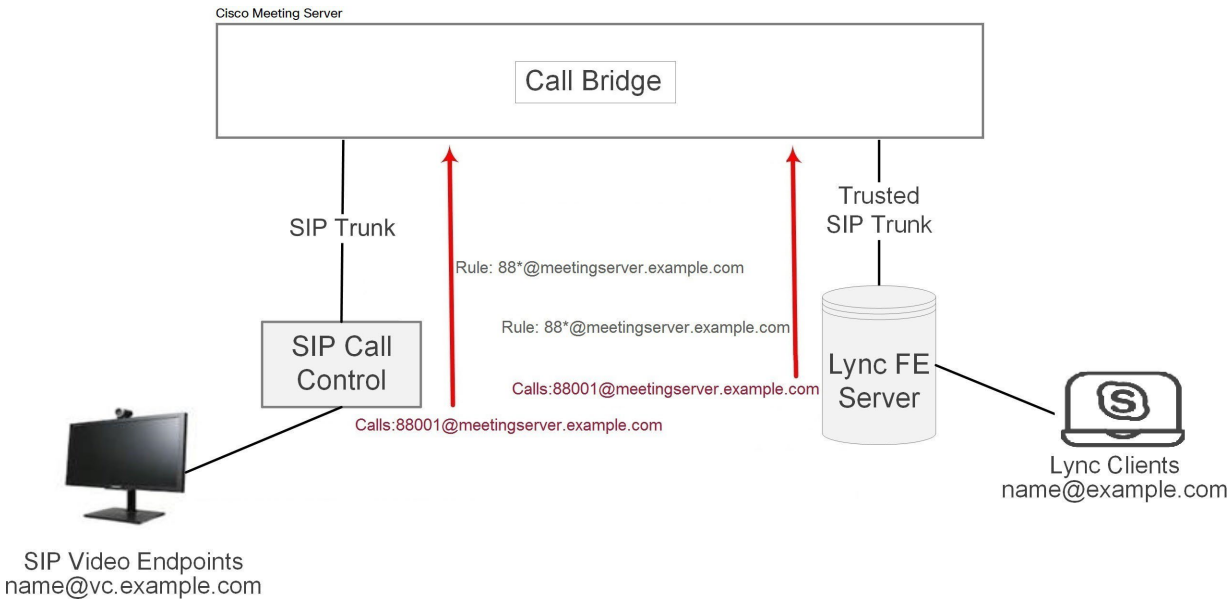
この例では、Lync クライアントは、 88001@example.com をダイヤルすることで、Meeting Serverでホストされている通話 88001 に接続できます。

8.2 SIP エンドポイントと Lync クライアントの統合

SIP エンドポイントがMeeting Serverスペースにダイヤルできるようにするには、セクション 7.2 の手順を実施します。Lync クライアントがMeeting Serverスペースにダイヤルできるようにするには、 セクション 8.1 を実施します。

これにより、SIP ビデオ エンドポイント ユーザーと Lync クライアントユーザーの両方が `<call_id>@meetingserver.example.com` をダイヤルすることで、同じ通話に参加できます。

図 14: Meeting Server が主催するミーティングに参加する SIP ビデオ エンドポイントと Lync クライアントの例

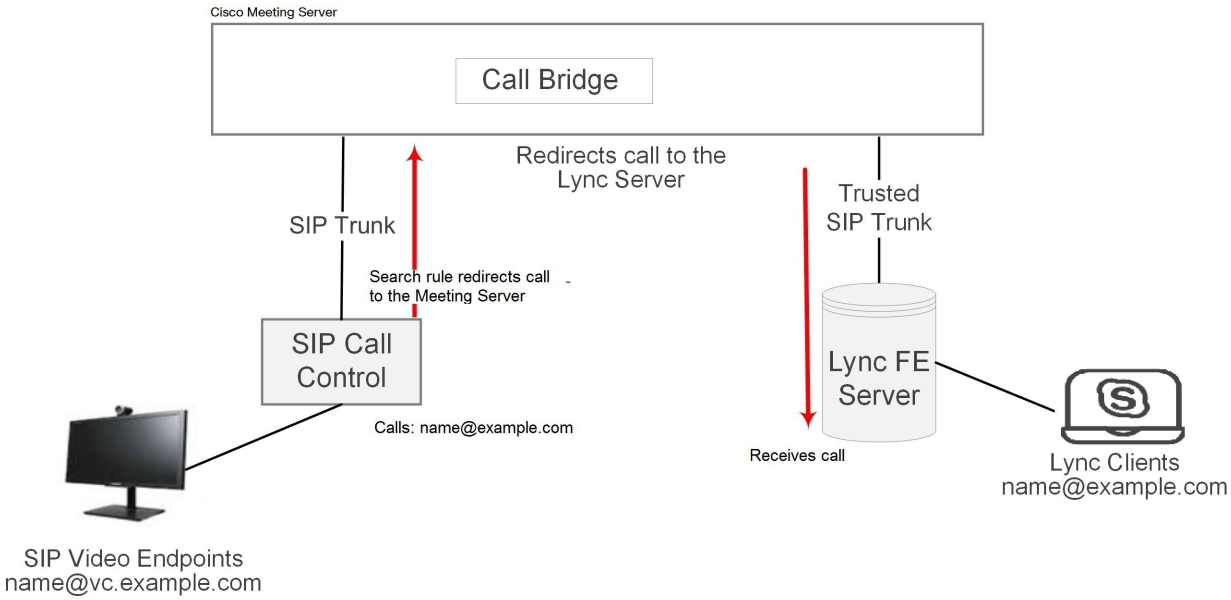


8.3 Lync クライアントと SIP ビデオエンドポイント間の通話を追加する

このセクションでは、2 つのダイヤルプラン設定のセクション (セクション 7.2 および セクション 8.1 で説明されている設定が完了していることを前提としています)。 例を拡張して、Lync および SIP ビデオエンドポイントが、ビデオと音声をトランスコードするゲートウェイとしてMeeting Server を使用して、通話でお互いに発信できるようにします (下図を参照)。

注：以前は、Meeting Serverから Cisco VCS への SIP トランクのセットアップにアウトバウンドコールページが使用されていました。 Lync 環境と SIP 環境の間の「ポイントツーポイントブリッジ」として機能するように Meeting Server を設定するには、このセクションで説明されているとおりに着信転送を設定し、Meeting Server から他の SIP コール制御デバイスへの SIP トランクをセットアップする必要があります。使用しているコール制御デバイス（Lync FE サーバー、Cisco VCS、CUCM、Avaya CM、Polycom DMA など)

図 15: 通話中の SIP ビデオ エンドポイントと Lync クライアントの例



今回の例：

- Lync ユーザーは **<name>@vc.example.com** にダイヤルして、SIP ビデオエンドポイントとの通話をセットアップできます (例: **meetingroom1@vc.example.com**)。
- SIP ビデオエンドポイントは、**<name>@example.com** にダイヤルして、Lync エンドポイントとの通話をセットアップできます（例：**roberta.smith@example.com**）。

必要に応じて例を修正してください。

8.3.1 Lync フロントエンドサーバーの構成

Lync クライアントに SIP ビデオエンドポイントの発信を許可するには:

- Lync スタティック ルートを追加し、Meeting Serverを指定します。このルートは、呼び出しをリダイレクトするためのものです。**@vc.example.com**。 セクション 8.1 に記載されているLyncスタティックルートの作成手順に従ってください。これにより、

Lyncクライアントからの通話がSIPビデオエンドポイントにルーティングされます。

8.3.2 VCS 設定

SIP ビデオ エンドポイントが Lync クライアントに発信することを許可するには:

- VCS (SIP コール制御デバイス) で検索ルールを追加して、サフィックスの通話をルーティングします。**@example.com** を Meeting Server にルーティングする

これにより、SIP ビデオ エンドポイント通話が Lync クライアントにルーティングされます。

8.3.3 Meeting Server の設定

Meeting Server に 2 つの転送ルールを作成します。1 つは SIP エンドポイントに通話を転送し、もう 1 つは Lync クライアントに通話を転送します。 次に、発信ダイヤルプランルールを 2 つ作成し、1 つは発信通話を SIP エンドポイントにルーティングし、もう 1 つは発信通話を Lync クライアントにルートするようにします。

1. ウェブ管理インターフェイスにログインして、**[設定（Configuration）] > [着信コール（Incoming Calls）]** に移動します。
2. [**着信の転送**] 項で、2 つの新しいルールを作成します:
   a. vc.example.com への着信に対して、着信の転送ルールを作成する
      - **ドメイン一致パターン** = **vc.exa*.com**
        ドメインマッチングパターンの任意の部分でワイルドカードを使用できますが、すべてに一致するものとして「*」を使用しないでください。そうすると呼び出しループが作成されます。
      - **優先順位** = <number>他の転送ルールが設定されていない場合は 0 を含め、任意の値を使用できます。 ルールが常に使用されるようにするには、設定したルールの中で最も高い優先順位を設定します。

        (ルールは優先順位に従ってチェックされます。優先順位の高いものから順に確認されます。 2 つのドメイン一致パターンが宛先ドメインに一致する場合、高い優先順位のルールが使用されます。)
      - **転送** = **転送**

        （「拒否」を選択した場合、ドメイン一致パターンに一致した通話は転送されずに切断されます。）
      - **発信者 ID** = **ダイヤルプランの使用** これは発信ダイヤルプランからのドメインを使用します。
      - **ドメインの書き換え** = **いいえ**
        通話は、呼び出されたドメインを使用して転送されます。

        (ここで [はい] を選択した場合、[**転送ドメイン**] フィールドを入力する必要があります。 元のドメインは、通話が転送される前に、 **転送ドメイン** に入力したドメインで置き換えられます。
      - **[新規追加（Add new）]** をクリックします。

   b. example.com への着信に対して、着信の転送ルールを作成する
      - **ドメイン一致パターン** = **exa*.com**
      - **優先順位**: <number>

- **転送** = **転送**
- **発信者番号通知** = **ダイヤルプランを使用**
- **ドメインの書き換え** = **いいえ**
- **[新規追加（Add new）]** をクリックします。

3. **[設定（Configuration）] >[アウトバウンドコール（Outbound calls）]** ページに移動して、2 つの新しいルールを作成します:
   a. SIPエンドポイントのドメインvc.example.comへの通話用のダイヤルプランを作成します。 セクション 7.2.2 のステップ 4 を繰り返します。
      - **[ドメイン（Domain）]** フィールドで、SIP エンドポイントに送信する必要がある通話の照合を行う SIP ドメインを入力します。 例えば、**vc.example.com**
      - **使用するSIPプロキシ** = <the IP address or FQDN of your VCS>
      - **ローカル連絡先ドメイン** =

        メモ：ローカル連絡先ドメインのフィールドは空欄にしておく必要があります。

      - **ローカル送信ドメイン** = <FQDN of the Meeting Server>
      - **トランクタイプ**=**標準 SIP** です。
      - **[新規追加（Add New）]** を選択します。
   b. Lync クライアントに対し、ドメイン example.com への発信に対するダイヤルプランルールを作成します。これは セクション 8.1.2 の繰り返しです。
      - **[ドメイン（Domain）]** フィールドで、Lync に送信する必要がある通話の照合を行う Lync ドメインを入力します。 例えば, **example.com**
      - **フィールド** 使用する SIP プロキシで、発信に使用するプロキシデバイスのアドレス (IP アドレスまたは FQDN) を入力します。
        - このフィールドを空欄にしておくと、サーバー**は _sipinternaltls._tcp.<yourlyncdomain>.com を使用して、呼ばれたドメインの DNS SRV ルックアップを実行します。**
        - または、フロントエンドプールの IP アドレスまたは FQDN (または Lync SIP ドメイン) を入力します。サーバーはまず、**_sipinternaltls._tcp.<yourlyncdomain>.com** を使用して定義されたドメインの DNS SRV ルックアップを実行し、SRV ルックアップが解決に失敗した場合は、入力されたホストの DNS A レコードを検索します。
        - または Lync FE サーバーの IP アドレスまたは FQDN を入力します

- **[ローカル連絡先ドメイン（Local Contact Domain）]** フィールドで、Meeting Server の FQDN を入力します。 次に例を示します。
  meetingserver.example.com

  注： Lync へのトランクをセットアップする場合にのみ、このフィールドを設定します。それ以外の場合は、空白にしておく必要があります。

- **ローカルからのドメイン** フィールドに、通話の発信元として表示するドメイン (発信者 ID) を入力します。これは Call Bridge の FQDN、例えば **meetingserver.example.com** になります。

  注：[ローカルからのドメイン（Local From Domain）] を空のままにしておくと、発信者番号 ID に使用されるドメインは、デフォルトで [ローカル連絡先ドメイン（Local Contact Domain）] になります。

- **トランクタイプ** フィールドで、[**Lync**] を選択します。
- [**行動**] フィールドで [**停止**] または [**続行**] を選択します。このルールが接続された通話を結果としない場合に、次の発信ダイヤルプランルールが試行されるかどうかによります。
- **[優先順位（Priority）]** フィールドで [優先順位レベル（Priority level）] を指定し、適用されるダイヤルプランルールの順序を決定します。 優先順位値の高いルールが最初に適用されます。
- **暗号化** フィールドで [**自動**]、[**暗号化**] または [**未暗号化**] を選択します。このルールを通じて行われる通話の暗号化されたSIP制御トラフィックが強制されるかどうかによります。
- **[新規追加（Add New）]** を選択します。

SIP ビデオ エンドポイントは、Lync クライアントに **<name>@example.com** をダイヤルすることで発信できます。また、Lync クライアントは、 **<endpoint>@vc.example.com** をダイヤルすることで SIP ビデオ エンドポイントに発信できます。

8.4 ウェブアプリを SIP および Lync クライアントと統合する

注： ウェブアプリユーザーは Lync ミーティングを呼び出すことができません。

Web アプリを使用するために Meeting Server を構成する手順については、 LDAP 構成のセクションを参照してください。

同じ LDAP 設定を使用して Lync アカウントとウェブアプリアカウントの両方を作成し、Meeting Serverを Lync ゲートウェイとして使用している場合、ユーザーが目的の Lync クライアントではなくウェブアプリクライアントを呼び出すときに問題が発生する可能性があります。 このような事態を防ぐには、以下で説明するように、着信のマッチングと着信の転送のルールをセットアップします。

例えば、Meeting Server に **fred@example.com** アカウントがあり、Lync FE サーバーに **fred@lync.example.com** アカウントがあるとします。 通話がMeeting Server に到達し、通話マッチングルールが設定されていない場合、Meeting Server はドメインを無視し、通話は Meeting Server の **fred@example.com** アカウントに転送されます。 Meeting Server はユーザー「fred」がローカルにいるかどうかを確認し、**fred@xxxx** 内の **xxxx**を無視します。

解決策は、着信コール ページで **コールマッチング** ルールを設定し、ローカルウェブアプリユーザーのドメインに一致するようにすること、そして **コール転送** ルールを使用して、Lync クライアントへのコールを転送することです。 **通話マッチング** ルールで、 **ドメイン名** フィールドを、Lync FE サーバーが使用するドメインとは異なるものに設定します。たとえば、**example.com などです。** **着信の転送** セクションの **ドメインマッチングパターン** フィールドに Lync ドメインを指定するルールを作成します。例：**lync.example.com**. **fred@example.com** への通話はウェブアプリのユーザーに届きますが、 **fred@lync.example.com** への通話はフレッドさんの Lync クライアントに転送されます。

8.5 Lync Edge サービスを使用した Lync の統合

Lync Edge サーバーを使用する NAT トラバーサルについては、この項の構成手順に従い、Meeting Serverで Lync Edge 設定を構成します。 これは、 デュアルホームド 会議システム をサポートする場合に必要です。あるいは、Meeting Serverではなく、Lync Edge が Lync 通話に対して TURN/ICE の役割を実行する場合に必要です。

8.5.1 Lync Edge の通話フロー

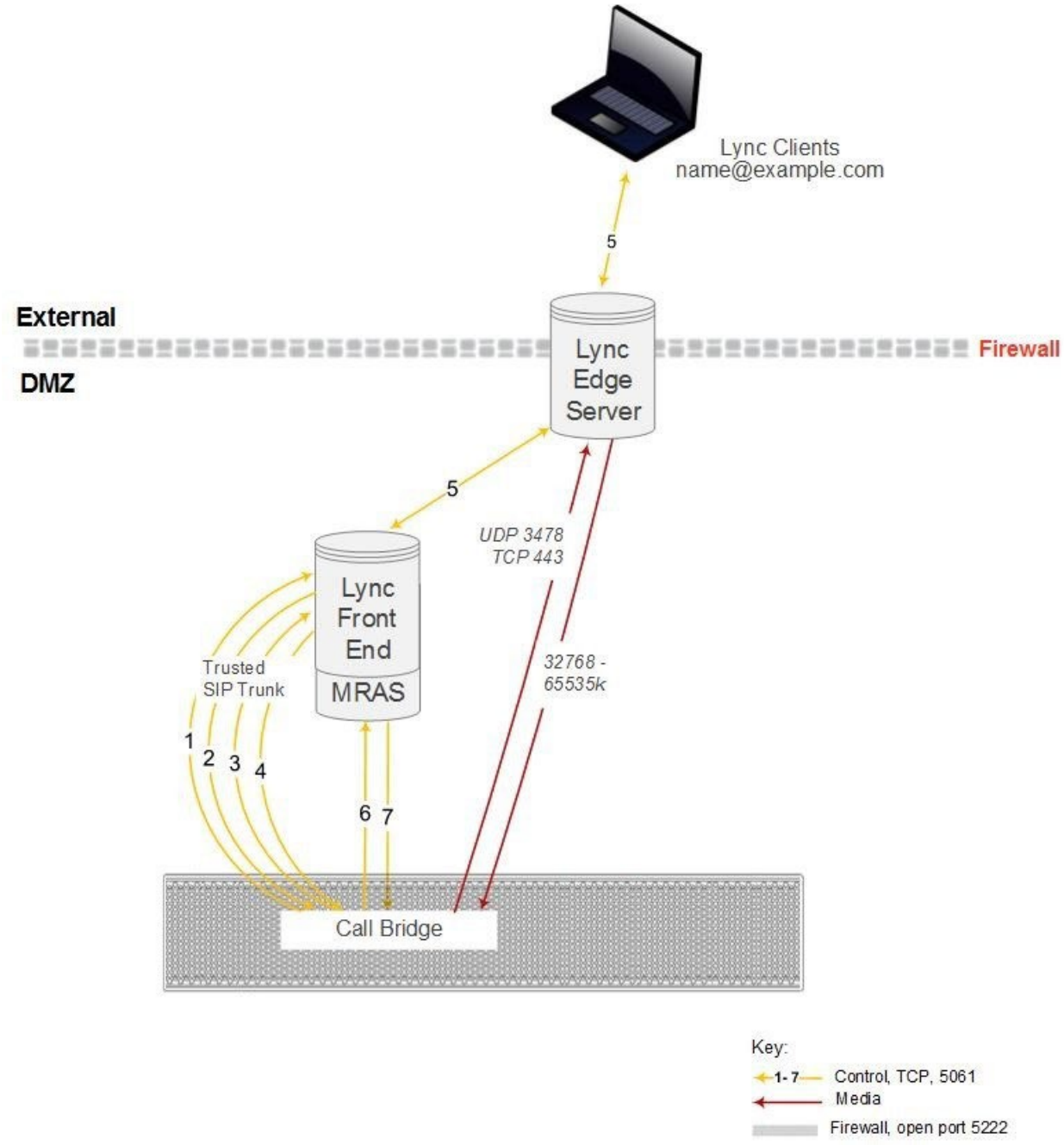
Meeting Serverから Lync Edge サーバーへの通話を確立するには (次の 図 16 を参照):

1. Call Bridge は、Lync FE サーバーへの「登録」SIP 通話を発信します。
2. 「登録」が承認されます。
3. Call Bridge は「サービス」を Lync FE サーバーに送信します。
4. FE サーバーは、メディア リレー認証サーバー (MRAS) の URI を返します。 (Lync Edge サーバーは MRAS として機能します。)
5. Lync クライアントが着信を受け取ります。

6. Call Bridge は、Lync FE サーバーに「サービス」メッセージを送信し、Lync Edge MRAS サービスを使用するための MRAS 資格情報を要求します。
7. Lync FE サーバーは、Call Bridge が使用する資格情報、UDP と TCP ポート、および MRAS URI を再度返します
8. Call Bridge は、DNS を使用してこの MRAS URI を解決し、Lync Edge サーバーへの直接 STUN メッセージの送信を開始します。
9. 通話メディアは、Call Bridge と Lync Edge の TURN サーバーの間を UDP ポート 3478 で直接流れ、上記の一時的な範囲のポートで Lync Edge サーバーから Call Bridge に返されます。

そのため、Call Bridge と Lync Edge サーバー間のメディアのために、ファイアウォールで次のポートを開く必要があります。UDP 3478 送信と 32768-65535 受信。

図 16: Call Bridge から Lync Edge サーバーへの通話フロー



8.5.2 Lync Edge を使用するためのミーティングサーバーの構成

Lync Edge サーバーを使用するには、Meeting Serverのウェブ管理インターフェイスにログインし、 **設定 > 全般** に移動して、Lync Edge 設定を設定します。 (Lync Edge サーバーが設定

されている場合、Lync 通話の TURN / ICE の役割を担うため、あるレベルでは、上記の TURN サーバー設定の代わりになります）。

また、Meeting Server Lync Server Edge 構成をセットアップするために、Lync ユーザークライアントアカウントを作成する必要があります。

これらの手順に従い、Lync Edge サーバーを使用するためにMeeting Server をセットアップします:

1. 適切な DNS レコードが設定されていることを確認してください。分割サーバー タイプの展開に必要な DNS レコードの一覧については、 付録 A を参照してください。

2. ディレクトリ内の他のユーザと同様に、LDAP ディレクトリ内に新しいユーザーを作成します。例えば、firstname="edge", second name = "user" です。

3. Lync FE サーバーのユーザマネージャーにログインし、前のステップで作成したユーザからLync クライアントユーザーを作成します。 他のユーザーと同じように、Lync を使用できるようにします。 上記の例の名前を使用して、**edge.user@lync.example.com** という名前のLync クライアントユーザーを作成します。

4. Meeting Serverのウェブ管理インタフェースにログインして、全般に **設定 > 一般**に移動します。 Lync FE サーバアドレス (またはこれを解決する主催者名) を入力して、Lync Edge 設定を設定します。 [ユーザ名] には、前の手順で作成した Lync クライアントのユーザ名を入力します。

5. 必要に応じて、[登録数] フィールドを完了してください。

   このフィールドは、1 つの登録済みデバイスに対して実行される同時通話の数を制限する Lync Edge サーバーの機能を克服します。 1 より大きい数字を入力することで、Call Bridge は指定された数の登録を行います。これにより、Meeting Serverが Lync Edge Server 経由で発信できる同時通話の数が増えます。

   1 より大きい数字を入力すると、Lync Edge ユーザー名の末尾に数字が追加され、そのユーザー名で登録されます。 例えば、ユーザー名を edge.user@lync.example.com として設定し、登録数を 3 に設定した場合、Edge サーバーで使用するためにLync 環境で次のユーザーを作成します：

   edge.user1@lync.example.com
   edge.user2@lync.example.com
   edge.user3@lync.example.com

   これにはいくらかの管理オーバーヘッドが必要です。しかし、それはLync Edge サーバーの制限によるものです。

   単一の登録のみを行うためには、[登録数] を空白のままにします。

   edge.user@lync.example.com.

注： Lync ユーザーのパスワードを入力する必要はありません。Lync FE サーバーが Call Bridge を信頼するためです。

Lync Edge の構成に関する注意事項:

- Meeting Server は、Lync Edge サーバー経由で到着するメディアを持つ外部の Lync クライアントからの Lync コンテンツ（RDP 経由で提供されるプレゼンテーション）をサポートします。 さらに、スペース (URI) は現在スペースにいる参加者の数に基づいて、使用中または利用可能としてレポートされるようになったため、お気に入りにスペースがある Lync クライアントはスペースの状況を確認できます。
- Lync AVMCU を使用している場合、Lync FE サーバーに登録するために、Lync エッジ設定を構成する必要があります。
- ウェブアプリは、Lync Edge サーバーが設定されている場合でも、Meeting Serverの TURN サーバーを使用し続けます。
- Lync Edge サーバーが構成されている場合、すべての Lync 通話は ICE 候補の収集と外部メディア接続にそのサーバーを使用します。 Lync Edge サーバーが設定されていないが、導入で Cisco Expressway が設定されている場合、Lync 通話は Expressway の設定された TURN サーバーによって処理されます。
- 通常の Lync Edge 導入では、Lync Edge サーバーの内部インターフェイスにはデフォルトゲートウェイが定義されません。外部インターフェイスのみにデフォルト ゲートウェイが定義されます。 Lync Edge サーバーの内部インターフェイスと同じローカルサブネット上にない場合、内部インターフェイスを使用して Meeting Server にパケットを正しくルーティングできるように、Lync Edge サーバーへの静的で永続的なネットワークルートを定義する必要があります。 静的で永続的なネットワークルートを Lync Edge サーバーに追加するには、CMD を開いて以下のコマンドを発行し、サンプルデータを実際の IP 情報で置き換えます。

  コマンド例:

  ```
  route add -p 10.255.200.0 mask 255.255.255.0 10.255.106.1
  ```

  この例では、10.255.200.0 のサブネット全体が 10.255.106.1、10.255.106.1は、Lync Edge サーバーの内部インターフェイスのサブネットのゲートウェイですのゲートウェイを経由してルーティングすることを許可するネットワーク ルートが追加されます。

  このルートの追加に失敗すると、Meeting Serverから Lync Edge サーバーに送信されたすべての STUN パケットが未回答になり、通話が失敗します。

8.6 Lync 直接フェデレーション

Meeting Server は、NAT が関与しないパブリック IP アドレスにCall Bridgeを置くことで、Microsoft Lync との直接フェデレーションをサポートします。これにより、Meeting Serverから Lync ドメインに直接、またはその逆に発信することができます。

着信通話を許可するには:

1. Meeting Serverの FQDN を指定する DNS SRV レコード _sipfederationtls._tcp.domain.com を作成します。 Call Bridgeはパブリック IP を持つ必要があり、NAT はこのシナリオではサポートされないため、この手順が必要です。

2. Meeting Serverの FQDN をパブリック IP アドレスに解決する DNS A レコードを追加します。

3. 以下の要件を満たす証明書と証明書バンドルを Meeting Server にアップロードします。

   a. 証明書は、CN として FQDN を持つ必要があります。または、SAN リストで証明書を使用する場合は、FQDN が SAN リストにもあることを確認します。 注：証明書に SAN リストが含まれている場合、Lync は CN フィールドを無視し、SAN リストのみを使用します。

   b. 証明書はパブリック CA によって署名されている必要があります。

   注： Lync FE サーバーによって信頼されているのと同じ認証局 (CA) を使用するように助言されます。 CA の詳細および Meeting Server と Lync の統合に関するサポートについては、Lync アドバイザに問い合わせてください。

   ---

   c. 証明書バンドルには、ルート CA の証明書と、チェーン中のすべての中間証明書が順番に含まれている必要があります。これにより、信頼のチェーンを確立できます。

   注： 証明書の詳細は、 Cisco ミーティング サーバー証明書のガイドラインの序論 を参照してください。

   ---

   d. 付録 B に記載されているとおりに、適切なファイアウォールポートを開きます。
   例: TCP 5061, UDP 3478, UDP 32768-65535, TCP 32768-65535

Meeting Serverからの発信通話の場合:

1. 発信ダイヤルルールを作成します。 **ドメイン** と **SIP プロキシ** のフィールドを空白のままにして、 **トランクタイプをLyncとして設定します。** また、適切な **ローカル連絡先ドメイン** および **ローカルからのドメイン** フィールドを設定します。

発信ダイヤルプランルールで個別のドメインを指定する場合、Lync 側で構成されたすべてのドメインが追加されていることを確認してください。 使用中のドメインは Lync Server トポロジービルダーから読み取ることができます。 追加のドメインが後で Lync に追加される場合、これらも発信ダイヤルプランルールに追加される必要があることに注意してください。

8.7 スケジュール済みの Lync ミーティングに直接または IVR 経由で発信する

Lync 導入の前提条件：この機能を使用するには、電話ダイヤルイン機能が有効な Lync 導入である必要があります。 Lync 導入では、1 つ以上のオンプレミス Lync FE サーバーを設定する必要があります。

注：オンプレミスの Lync FE サーバーは、Lync 導入が外部の Lync または Skype for Business クライアントをサポートしていない場合でも設定する必要があります。

Meeting Serverは、Lync 通話 ID を使用して通話に参加するための、WebRTC または SIP エンドポイントからスケジュールされた Lync ミーティングへの発信をサポートしています。Cisco ミーティングアプリのユーザーは、Lync クライアントによってのみ Lync ミーティングに追加されます。 この機能では、電話会議ルックアップ用に 1 つ以上の Lync FE サーバーが Meeting Server上で設定されている必要があります。 Web Admin インターフェイスの Lync Edge 設定から **設定 > 一般**で一つを設定し、APIを通じて一つ以上を設定することができます（それらを「lyncEdge」タイプのTURNサーバーとして作成します）。 これを行う方法については、「Lync Edge を使用するためのMeeting Server の設定」を参照してください。 プールに複数の FE サーバーがある場合、サーバー アドレスとしてプール FQDN を使用します。

注： Lync ミーティング解決のために、Meeting Serverは発信ルールではなく、Lync ミーティング ID と _sipinternaltls._tcp.lync-domain の DNS ルックアップを使用します。 DNS サーバーに DNS SRV レコード _ sipinternaltls._tcp.lync-domain を設定するか、DNS SRV レコードを使用しない場合は、コマンド **`dns app add rr` でMeeting Serverのレコードをセットアップします。`<DNS RR>`**. Dns app コマンドの使用に関する詳細は、『MMP コマンドライン リファレンス』を参照してください。分割タイプの導入に必要な DNS レコードのリストは、付録を参照してください。

Lync FE サーバーを設定し、次の 表 6 のタスクシーケンスに従います。

表 6: Lync FE サーバーを構成する一連のタスク

[順序 (Sequence)]	タスク	ウェブ管理インターフェイス上	API 経由
1	Lync 会議 ID の入力を許可するように Call Bridge IVR を設定する	ウェブ管理インタフェース経由で IVR をセットアップしている場合: **「構成」>「全般」**の IVR セクションで、**「ID によるスケジュールされた Lync 会議への参加」**を**許可に設定します。**	API を通じて IVR をセットアップしている場合: **`resolveLync 会議 ID` を設定する**設定された IVR に対して **`true`** に設定する
2	標準 SIP システムから Lync 会議 ID への直通ダイヤルを許可します。 注：既存の設定済みドメインを拡張して Lync 会議アクセスを許可するか、この目的のために新しくドメインを作成するかを選択できます。	**[設定（Configuration）] > [着信コール（Incoming calls）]** に移動します。そして、1 つ以上の設定されたコールマッチングドメインに対して、**[ターゲット Lync（Targets Lync）]** を **[yes]** に設定します。	設定**受信するダイアルプランルールで、`resolveToLync Conferences` tを `true` に設定します**
3	Web Bridgeの通話参加インターフェイス経由で Lync 会議 ID 入力を許可する	Web 管理インターフェース経由で Web Bridge をセットアップしている場合: **「構成」>「全般」**に移動し、Web ブリッジ設定セクションで**「ID によるスケジュールされた Lync 会議への参加」**が**許可されていることを確認します。**	API を通じてWeb Bridgeをセットアップしている場合: Web Bridgeで **resolveLync ConferenceIds** を **`true`** に設定します

通話が Lync 会議 ID と照合される場合、コールブリッジは最初に通話 ID がスペースに適用されないかどうかを確認し、適用されない場合、コールブリッジは Lync FE サーバを識別します。が設定されており、ID を解決する機能があると宣伝されています。 Call Bridge は Lync FE サーバにクエリを実行し、問題の通話 ID が Lync 会議に対応しているかどうかを判断します。対応している場合は、検索が成功したとみなされ、通話は Lync 通話に結合されます。 コール ID が Lync 会議に対応していると認識されない場合、それ以上の Lync FE サーバへのクエリは行われません。

注： 異なる Lync 導入にある複数の Lync FE サーバーの設定を追加すると、予期しない結果になる場合があります。 たとえば、異なる Lync 導入の複数の Lync 電話会議が同じコール ID を使用する場合、複数の Lync FE サーバーがルックアップに対して積極的に応答します。この場合、「最初」に成功した Lync の解決が使用されます。

注： Meeting Server経由で Lync に接続する各参加者は、Lync AVMCU での参加者の競合を避けるため、固有の「送信元」SIP アドレスが必要です。 PSTN ゲートウェイ経由で接続する電話参加者は、汎用の発信 callerID 情報のため、参加者の競合に遭遇するリスクが高くなります。 すべての電話参加者は、Meeting Serverの Dual Home ゲートウェイ経由ではなく、Lync PSTN 電話会議/仲介サーバー経由で Lync ミーティングに接続することをお勧めします。

スケジュールされた Lync ミーティングのために送信される招待状のテキストをカスタマイズして、ユーザーがMeeting Server経由で参加するために必要な詳細を含めることができます。これらの詳細は、カスタム フッター セクションに配置する必要があります。 例:'SIP/H.323 エンドポイントの場合は、 **join@example.com に発信し、上記の電話会議 ID を入力します。WebRTC については、join.example.com に移動して、上記の電話会議 ID を入力してください。」** この中の URI は、上記で設定したものと一致する必要があります。 詳細については、Microsoft のドキュメント https://technet.microsoft.com/en-us/library/gg398638.aspx を参照してください。

8.8 参加者を Lync 電話会議に接続するための Call Bridge モードを選択する

Meeting Server API を使用して、参加者を Lync 会議に接続するときの Call Bridge の動作を選択できます。 **リクエストパラメータ** lyncConferenceMode **が、`/callProfiles`** への POST 時または **`/callProfile/<call profile id>`** への PUT 時に追加されました。

同じ Call Bridge 上の通話を 1 つの会議に結合する場合は、 **`dualHomeCallBridge`** に設定します。 これにより、Call Bridge で 1 つの会議が開催され、Call Bridge が AVMCU ミーティングに発信します。

通話を 1 つの会議にまとめたくない場合は、 **ゲートウェイ** に設定します。 各 SIP 参加者は、関連付けられた AVMCU ミーティングへの発信を持つ自分の会議に参加します。

注： **`lyncConference Mode`** を ゲートウェイに設定して、デュアルホーム電話会議を無効にします。

9 Office 365 デュアルホームエクスペリエンスと OBTP スケジュール

9.1 概要

「OBTP (One Button To Push) スケジュールを使用した Office 365 デュアル ホーム エクスペリエンス」により、参加者は OBTP をサポートする Cisco エンドポイントを使用して Office 365 ミーティングに参加できます。

主催者は Skype for Business プラグインで Microsoft Outlook を使用してミーティングをスケジュールし、参加者、会議室 (OBTP 対応エンドポイントを含む)、およびミーティングの場所を追加します。

ミーティングに参加するには、OBTP 対応エンドポイントを使用する参加者はエンドポイントまたはタッチスクリーン上の OBTP ボタンを押すだけです。 Skype for Business クライアントは、通常どおりミーティングに参加するためのリンクをクリックします。

注： Office 365 を使用している場合、招待された OBTP 対応のエンドポイント、または Office 365 がインストールされている Skype for Business クライアントだけが Lync ミーティングに参加できます。Cisco エンドポイントはMeeting Server の IVR 経由で、手動でミーティングに参加することができません。 これは、任意の Cisco エンドポイントがMeeting Server IVR 経由で手動で参加できるオンプレミスの Lync 導入との主な違いです。

注： 「OBTP (One Button To Push) スケジュールによる Office 365 デュアルホーム体験」はバージョン 2.2 からサポートされており、Cisco TMS 15.5、および Cisco TMS XE 5.5 以降が必要です。

9.2 設定

注： この機能を使用するには、Office 365 と通信するために、Call Bridge を公共のインターネットに接続する必要があります。送信トラフィック用に、ファイアウォールの TCP ポート 443 を開く必要があります。

Office 365 ミーティングへの参加方法をセットアップするには、Meeting Serverのウェブ管理インターフェイスにログインして **[設定>着信]** に移動し、通話のマッチング **ルールで、Lync Simplejoinを対象とする** フィールドを **true** に設定します。 これにより、Office 365 招待で送信された Lync Simple Meet URL を解析する方法が Meeting Server に通知されます。

ミーティングだけでなく参加者にも発信できるようにするには、既存の発信ダイヤルプランルールを使用して発信通話をルーティングするか、新しい発信ダイヤルプランルールを作成します。

9.3 会議中の体験

「OBTP スケジュールを使用した Office 365 デュアル ホーム エクスペリエンス」は、双方向の音声、ビデオ、コンテンツ共有による「デュアル ホーム エクスペリエンス」を提供します。 Office 365 クライアントには、Lync AVMCU によって決定される使い慣れた電話会議中の体験があり、OBTP が有効なエンドポイントを使用する参加者は、Meeting Server によって決定されるビデオ会議エクスペリエンスになります。 全員に統合参加者リストが表示されます。

注： クライアントのコントロールは会議全体では機能しません。また、予期しない動作を引き起こす可能性があります。 例えば、Skype for Business クライアントが Meeting Server に接続されたエンドポイントをミュートする場合、エンドポイントはミュートされますが、ミュートされているという通知はエンドポイントに送信されません。エンドポイントは自分自身をミュート解除することはできません。 Skype for Business クライアントが Meeting Server に接続されているすべてのエンドポイントをミュートした後、ミュート解除すると、すべてのエンドポイントはミュート状態のままです。

注： 参加者のミュートやドロップなどの ActiveControl 機能は、ローカル Call Bridge の参加者にのみ影響し、Lync AVMCU の参加者には影響しません。

10 Web Bridge 3 の設定

このセクションでは、Call Bridge が Web Bridge 3 と通信するための設定を構成する方法について説明します。これにより、ウェブアプリのビデオコールとミーティングを使用できるようになります。

ウェブアプリをテストしている場合、Meeting Serverの初期設定が完了した後はいつでも、セクション 10.2 の手順をこの順番で実行してください。 ウェブアプリを使用していない場合は、この章をスキップしてください。

注： Cisco Expressway ウェブプロキシをWeb Bridgeに接続する必要がある導入の場合、Web Bridge証明書の SAN フィールドが、Web Bridgeに接続する Expressway-C で使用される A レコードが含まれていることを確認してください。そうしないと、接続に失敗します。 例えば、Expressway が join.example.com のWeb Bridgeに接続するように設定されている場合、A レコードがこの FQDN に対して存在している必要があり、Web Bridge証明書の SAN フィールドには join.example.com が含まれている必要があります。

10.1 Web Bridge 3 接続

表 7 にウェブアプリの接続に使用されるポートを示します。 項 10.1.1 では、ウェブアプリと Meeting Server のコンポーネント間の通話フローについて説明しています。

図 17: ウェブアプリのポートの使用状況

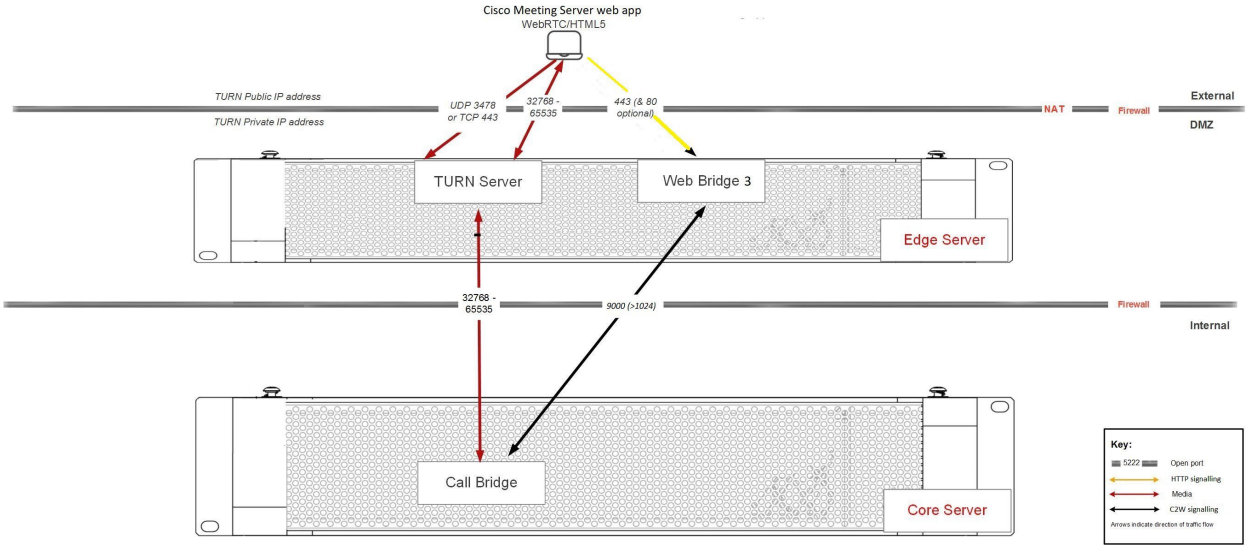


表 7: ウェブアプリの接続に必要なポート

コンポーネント	接続先	開く接続先ポート	トラフィック タイプ	コンポーネントに対するトラフィックの方向	追加情報
Web Bridge 3	web app	443 (メモ 1)	TCP (HTTPS)	着信 (Incoming)	
Web Bridge 3	web app	80	TCP (HTTP)	着信 (Incoming)	
Call Bridge	Web Bridge 3				開く接続先ポート：ユーザーにより設定可能。トラフィックタイプ：TCP (C2W) 、方向：発信

メモ 1：宛先ポートはWeb Bridge 3 https リスニング ポートに設定されているものである必要があります。

10.1.1 Web Bridge 3 のコールフロー

このセクションでは、ウェブアプリとMeeting Serverのコンポーネント間の通話フローについて説明します。

1. ウェブブラウザが HTTPS 接続を開きます。
2. ユーザーには **ミーティングに参加** (手順 3 を参照) または **ログイン** (手順 4 を参照)の選択が提示されます。
3. 「ミーティングに参加」が選択された場合、ユーザーは発信 ID/URI とパスコードを入力し、名前を設定するように求められます。
    a. 通話の詳細は、HTTPS 経由で Web Bridge 3 に送信されます。Web Bridge 3 は、通話の詳細を検証するために、C2W 接続を介して Call Bridge にクエリを実行します。
    b. 成功した場合、ユーザーはメディア設定を選択するように求められます。
    c. メディア設定を選択した後、通話の詳細と希望の名前が HTTPS 経由でWeb Bridge 3 に送信されます。C2W 経由で Call Bridge に転送されます。 Call Bridge は、ブラウザに返される通話アクセストークンで応答します。このトークンは、ブラウザが使用する TURN サーバーの詳細を示します。
    d. Call Bridge は、設定された TURN サーバーからの割り当てを要求します。
    e. ウェブアプリは、指定された TURN サーバーに割り当てを要求します。
    f. ブラウザがWeb Bridge 3 へのウェブソケット接続を開きます。この接続は、C2W 接続経由で Call Bridge に転送されます。 呼び出しアクセス トークンはこのウェブソケット経由で送信されます。

g. ブラウザと Call Bridge は、ローカル メディア IP アドレス/ポートおよびメディアリレー アドレス/ポートを含むウェブソケット上の SDP を交換します。

h. ICE ネゴシエーションは、すべてのブラウザメディア IP アドレス/ポートの組み合わせと、すべての Call Bridge アドレス/ポートの組み合わせの間で UDP パケットを送信し、TCP メディアリレーアドレス/ポートに TCP 接続を試みます。

i. ブラウザと Call Bridge の間のメディア転送には成功した最短メディア パスが使用され、これは直接、TURN UDP リレーを経由、または TURN サーバーが TCP ストリームと UDP の間でメディアパケットを変換する TURN TCP リレーを経由します。

4. **ログイン** が選択されている場合、ユーザーにはユーザー名とパスワードの入力が求められます。

   a. HTTPS 経由でウェブブリッジに送信され、成功した場合、ポータルアクセストークンを取得するためにコールブリッジに転送されます。

   b. ユーザーのポータルサイトに入ると、すべてのリクエストが HTTPS 経由で送信され、ポータル アクセス トークンがヘッダーとして送信されます。

   c. 通話参加リクエストが行われた場合、フローはステップ 3c 以降と同じですが、通話の詳細と希望する名前を送信して通話アクセストークンを取得する代わりに、ブラウザは代わりに通話の詳細とポータルアクセストークンを送信します。

役立つ情報: 呼び出しアクセストークンとポータルアクセストークンは似ていますが、異なります。 ポータル アクセス トークンは 24 時間有効で、これによりユーザー ポータルへのアクセスが許可されます。 通話アクセストークンは、ユーザーが通話に参加している間のみ有効で、通話に参加する場合にのみ使用されます。 ポータル アクセス トークンを入手する唯一の方法は、ユーザー名とパスワードを使ってログインすることです。 通話アクセス トークンは、ゲスト参加を行うか、またはユーザーが参加したいミーティングの詳細と共にポータル アクセス トークンを使用して取得できます。

10.2 Web Bridge 3 の設定

バージョン 3.0 以降、Web Bridgeごとではなく、共通の場所でWeb Bridgeの設定オプションを設定できます。すべてのWeb Bridge、または特定のグループのWeb Bridgeに同じ設定を適用できます。

/webBridgeProfiles API オブジェクトには、さまざまなWeb Bridge設定オプションが含まれています。 新しく定義されたWeb Bridgeのプロファイルは、個々の webBridge オブジェクト、または最上位のグローバルプロファイルまたはテナントに割り当てることができます。

Web Bridge 3 の設定に関する詳細は、 API リファレンスガイド のWeb BridgeとWeb Bridgeのプロファイルメソッドの項を参照してください。

10.2.1 Web Bridge プロファイルを作成して適用する方法の例

注：シングルスプリット導入では、Web Bridge 3 設定は Edge サーバーをポイントする必要があります。

開始する前に、Web Bridge 3 証明書をインストールし、Web Bridge 3 を設定していることを確認してください。 セクション 4.6 に詳述されているように。 その後、次の手順に従って操作してください:

1. Meeting Serverウェブ管理インターフェイスを使用して webBridgeProfile を作成するには:
   a. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）] > [API]** を選択します。
   b. API オブジェクトのリストで、**/api/v1/webBridgeProfiles** 後の ▶ をタップします。
   c. **[新規作成（Create new）]** をクリックします。
   d. **[name]** フィールドにこのウェブブリッジプロファイルに付けたい名前を設定します。
   e. **[resourceArchive]** フィールドに、このウェブブリッジプロファイルを使用するウェブブリッジのために Meeting Server が使用するべきカスタマイズ アーカイブ ファイルのアドレスを設定します。
   f. **[allowPasscodes]** フィールドを **[true]** または **[false]** に設定します。 このフィールドは、このWeb Bridgeプロファイルを使用するWeb Bridgeが、数値 ID/URI と組み合わされたパスコードで coSpace (および coSpace アクセス方法) のルックアップをユーザーに許可するかどうかを決定します。 このパラメータが指定されていない場合、デフォルトで **[true]** に設定されます。
   g. **[allowSecrets]** フィールドを **[true]** または **[false]** に設定します。 このフィールドは、このウェブブリッジプロファイルを使用するウェブブリッジが、数字の ID とシークレットのミーティング参加リンクを通じてユーザーが coSpaces（および coSpace のアクセス方法）にアクセスすることを許可するかどうかを決定します。このパラメータが指定されていない場合、デフォルトで **[true]** に設定されます。
   h. **userPortalEnabled** フィールドを **true** または **false に設定してください。** このフィールドでは、このウェブブリッジのプロファイルを使用するウェブブリッジのインデックスページにサインインタブを表示するかどうかを指定します。 このパラメータが指定されていない場合、デフォルトで **[true]** に設定されます。
   i. **allowUnauthenticatedGuests** フィールドを **true** または **false に設定してください。** **[true]** に設定した場合、このウェブブリッジのプロファイルを使用するウェブブリ

ッジのランディング画面からのゲストアクセスが許可されます。 False に設定すると、訪問者アクセスは、ユーザーがユーザーポータルにログインした後にのみ許可されます。 このパラメータが指定されていない場合、デフォルトで [true] に設定されます。

j. **resolveCoSpaceCallIds フィールドを true または false に設定してください。** このフィールドは、このウェブブリッジプロファイルを使用するウェブブリッジが、coSpace および coSpace アクセスメソッドコール ID を受け入れ、訪問者が cospace ミーティングに参加できるようにするかどうかを決定します。 このパラメータが指定されていない場合、デフォルトで [true] に設定されます。

k. **resolveCoSpaceUris フィールドを オフ、 domainSuggestionDisabled または domainSuggestionEnabled**に設定してください。 このフィールドは、このウェブブリッジが、coSpace および coSpace アクセス方式 SIP URI を、訪問者が cospace ミーティングに参加できるようにする目的で受け入れるかどうかを決定します。 [off] に設定すると、URI による参加は無効になります。 [domainSuggestionDisabled] に設定すると、URI による参加は有効になり、しかし、このウェブブリッジでは URI のドメインは自動補完または検証されません。 [domainSuggestionEnabled] に設定すると、URI による参加は有効になり、そして、このウェブブリッジで URI のドメインが自動補完され、検証されます。 このパラメータが指定されていない場合、デフォルトで [off] に設定されます。

l. **[作成（Create）]** をクリックします。

2. プロファイルを作成したら、その後、アドレスを追加できます。これは、ミーティングの招待を生成するためのWeb Bridge URIと、ウェブアプリのクロス起動URLです。

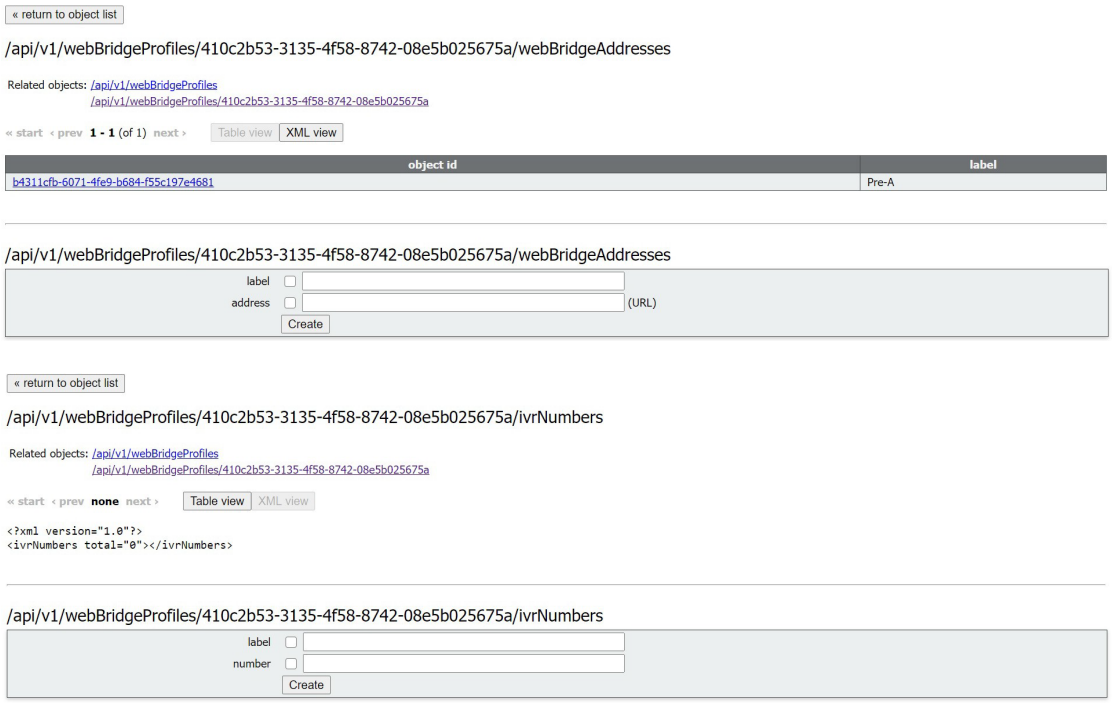
注：バージョン 3.1 以降、複数の IVR 番号とWeb Bridgeアドレスを指定できるようになりました。Web Bridgeプロファイルごとに最大 32 個の IVR 番号と最大 32 個のWeb Bridgeアドレスです。 これらは参加情報を表示する際、およびメール招待状を生成する際に使用されます。

この例では、Web BridgeのURIとIVR電話番号が次のようにwebBridgeProfileに適用されます。

a. API オブジェクトのリストで、**/api/v1/webBridgeProfiles** 後の ▶ をタップします。

b. [**表示または編集**] をクリックします。

c. 結果の"webBridgeProfile オブジェクト選択ウィンドウ"から、 **ステップ 1 で作成し、Web Bridge URI および IVR 番号を割り当てたい** webBridgeProfile **の** オブジェクト ID **を選択します。** Web Bridgeの **ラベル** および URL **アドレス** を入力し、必要に応じて IVR の **ラベル** および **番号** を入力します。



d. **[作成（Create）]** をクリックします。

3. 必要に応じて、新しく作成された webBridgeProfile の ID を次のいずれかまたはすべてに割り当てます。

   - 最上位 (グローバル) プロファイル (**/api/v1/system/profiles**)
   - テナント (**/api/v1/tenants/<*id*>**)
   - WebBridges (**/api/v1/webBridges/<*id*>**)

   この例では、更新された webBridgeProfile が次のように最上位 (グローバル) プロファイルに割り当てられます。

   a. API オブジェクトのリストで、**/api/v1/system/profiles** 後の ▶ をタップします。

   b. **[表示または編集]** をクリックします。

   c. パラメータを下にスクロールして **webBridgeProfile** を選択し、**[選択（Choose）]** をクリックします。

   d. 結果の"webBridgeProfile オブジェクト選択ウィンドウ"から、 **ステップ1で作成した、最上位のグローバルプロファイルに割り当てたいwebBridgeProfileの**オブジェクトIDを **選択** をクリックします。

   e. **[変更（Modify）]** をクリックします。

f. 新しく割り当てられた webBridgeProfile オブジェクト ID が、**オブジェクトの設定** の下に表示されます。

注：ウェブアプリの詳細は、「Cisco Meeting Server web app の重要な情報」を参照してください。

---

11 ミーティングの録画とストリーミング

3.0 以前は、Meeting Serverの内部レコーダーおよびストリーマコンポーネントは、Meeting Serverの内部 XMPP サーバーコンポーネントに依存していました。3.0 では、この XMPP サーバーは削除されます。 バージョン 3.0 では新しい内部レコーダーとストリーマーを導入し、どちらも SIP ベースです。

新しい内部レコーダーとストリーマコンポーネントとサードパーティへの発信
SIP レコーダーはすべて SIP URI を使用して設定されるため、録画またはストリーミングが開始されると、管理者が設定した SIP URI が呼び出されます。

11.1 新しい内部 SIP レコーダーとストリーマの機能の利点

- 新しいレコーダーとストリーマはレイアウトの変更をサポートしています。 レコーダー/ストリーマは、他の SIP 通話と同様の方法で、つまり callLegProfile 階層の defaultLayout パラメータまたは coSpace オブジェクトから、そのレイアウトを取得します。 callLeg のレイアウト パラメータを変更することもできます。
- カスタムレイアウトは、layoutTemplate パラメーターを使用して設定できます (カスタムレイアウトを実装するには、customizations ライセンスが必要です)。
- 最大解像度は、callLegProfiles および callLegs の qualityMain パラメータを使用して、コールレッグごとにコントロールできます。
- 以前の XMPP ストリーマは 720p 解像度のみをサポートしていましたが、新しいストリーマは最大 1080p の解像度をサポートし、3.0 では MMP コマンドを使用してストリーマの解像度を選択できるようになりました。 **`streamer sip resolution`**。
- callLegProfile の presentationViewingAllowed パラメーターの設定を変更することで、ストリーマ/レコーダーがプレゼンテーションを受信するかどうかを選択できます。
- 新しい MMP コマンド **レコーダー制限の導入によるスケーラビリティの向上**そして **ストリーマー制限**。

11.2 新しい内部 SIP レコーダーとストリーマーを実装する際の注意点

注：新しい内部 SIP レコーダーおよびストリーマサービスは、外部の録画またはストリーミングサービスとして使用できません。これらのサービスは、Meeting Server Call Bridge から渡される特定の SIP ヘッダーパラメータに依存しています。 Meeting Server Call Bridge以外の任意のソースからの通話が接続すると、レコーダー/ストリーマは特定の SIP ヘッダーを見つけられないため、通話を拒否します。

レコーダーの本番環境での使用で推奨される展開は、最小で 4 つの vCPU コアと 4 GB の RAM を備えた専用 VM で実行することです。 各録画タイプのパフォーマンスとリソース使用率を次の表に示します。

表 8: 内部 SIP レコーダーのパフォーマンスとリソース使用率

録画設定	vCPU あたりの録画数	1 回の録画で必要な RAM	時間あたりのディスクバジェット	最大同時録画
720p	2	0.5GB	1GB	40
1080p	1	1GB	2GB	20
オーディオ	16	100MB	150MB	100

注意すべき重要なポイント (新しい内部レコーダーコンポーネントにのみ適用されます):

- パフォーマンスは、vCPU を追加すると、最大でホストの物理コアの数まで直線的に増加します。

ストリーマを本番環境で使用する場合に推奨される展開は、最低 4 つの vCPU コアと 4 GB の RAM を備えた専用 VM で実行することです。 次の表は、推奨される 3 つの最小仕様とそれらが処理できるストリーム数を示しています。

表 9: 内部 SIP ストリーマの推奨仕様

vCPU の数	RAM	720p ストリーム数	1080p ストリームの数	音声のみのストリーム数
4	4GB	50	37	100
4	8GB	100	75	200
8	8GB	200	150	200

注意すべき重要なポイント (新しい内部ストリーマコンポーネントにのみ適用されます):

- vCPU の数は、物理コアの数を超過してはならない。
- vCPU を追加しても、サポートされる 720p ストリームの最大数は 200 です。
- サポートされる 1080p ストリームの最大数は、vCPU の追加に関係なく、150 です。
- サポートされる音声のみのストリームの最大数は、vCPU の追加に関係なく、200 です。

11.3 録画の概要

Meeting Server使用時にミーティングを録画するには 2 つの方法があります。

- サードパーティの外部 SIP レコーダー
- Meeting Serverの内部 SIP レコーダーコンポーネント

11.3.1 サードパーティの外部 SIP レコーダーのサポート

Cisco Meeting Server では、サードパーティの外部SIPレコーダーを設定できるため、録画が開始されると、管理者が設定したSIP URIが新しいCisco Meeting Server の内部SIPレコーダーコンポーネントと同じ方法で呼び出されます。

注： 外部のサードパーティ SIP レコーダーのサポートには、引き続きCisco Meeting Server の録画ライセンスが必要です。

サードパーティの外部 SIP レコーダー機能:

- レコーダーが BFCP をネゴシエートして別のビデオとコンテンツ ストリームを受信することを許可します。 これにより、録画の形式に関するより柔軟なオプションが提供されます。
- は、標準の SIP 通話の場合と同じ解像度をサポートします
- 標準 SIP 通話と同じ音声とビデオのコーデックをサポートします
- 既存のMeeting Server の内部レコーダーと同様に、SIP レコーダーから送信されたメディアコンテンツはすべて破棄されます。

注： SIP レコーダー機能は、TIP またはアクティブコントロールをサポートしていません。

11.3.2 Meeting Server 内部 SIP レコーダーコンポーネントのサポート

Meeting Server上の内部 SIP レコーダーコンポーネントバージョン 3.0 以降は、ミーティングを録画し、録画をネットワークファイルシステム NFS などのドキュメントストレージに保存する機能を追加します。

レコーダーは、電話会議を主催するサーバーとは別のMeeting Server上で有効にしてください。図 18 を参照してください。 レコーダーは、導入をテストする目的で、電話会議（ローカル）を主催している Call Bridge と同じ Meeting Server 上にのみ配置します。

可能な場合、レコーダーはターゲットファイルシステムと同じ物理的場所に導入し、低遅延と高ネットワーク帯域幅を確保することをお勧めします。 NFS は安全なネットワーク内に設置されることが想定されています。

注：録画の保存に使用するメカニズムによっては、レコーダー、アップローダ、ストレージシステムが通信できるように、外部ファイアウォールポートを開く必要がある場合があります。例: ポートマッパープロトコルのバージョン 2 または 3 を実行している NFS は、TCP または UDP ポート 2049 および 111 を使用します。

注： レコーダーまたはアップローダを使用する場合は、Meeting Serverでファイアウォールコンポーネントを使用しないでください。

注：ミーティングの録画が終了すると、録画は自動的に MP4 に変換されます。 変換されたファイルは、ドキュメントの保存/配信システム内に配置するのに適しています。例えば、ネットワーク ファイル システム（NFS）では、それらは NFS フォルダ spaces/<space ID> に保存され、テナントスペースは tenants/<tenant ID>/spaces/<space ID> に保存されます。

次の図は、許可されているさまざまな記録デプロイメントを示しています。

図 18: 録画のデプロイメントで許可されている: リモートモード

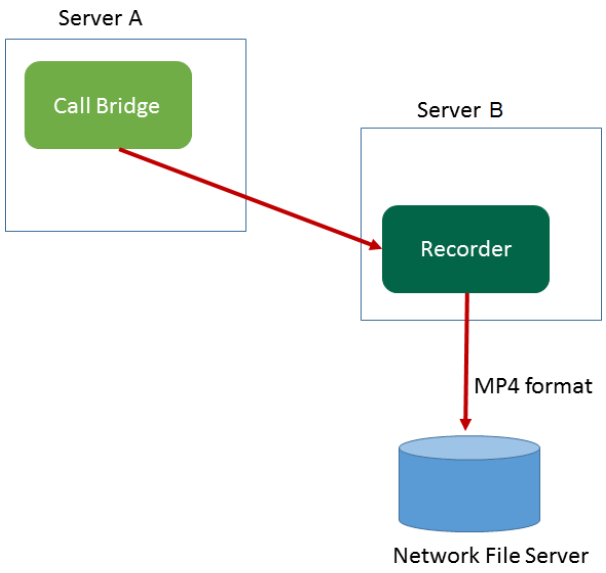
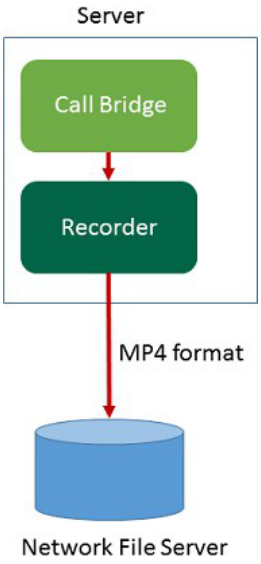


図 19: テスト目的のみで許可される録画のデプロイメント: ローカルモード



11.4 新しい内部 SIP レコーダー コンポーネントを VM サーバーに導入する例

注：録画を Windows 2008 R2 SP1 を実行している NFS サーバに保存する場合は、アクセス許可の問題を修正するための Windows ホットフィックスが必要です。https://support.microsoft.com/en-us/kb/2485529。 この修正を適用する前に、Microsoft Windows 管理者に問い合わせてください。

これは 2 段階のプロセスです。

- MMP 経由でミーティングサーバーレコーダーを設定する
- API を介してレコーダー URI を設定する

タスク 1: MMP 経由でMeeting Serverレコーダーを設定する

1. バージョン 3.0 にアップグレードします。
2. MMP に SSH で接続し、ログインしてレコーダーを設定します (MMP コマンド、**レコーダー** すべての利用可能なコマンドのリストを見るために。
3. **`recorder nfs <hostname/IP>:<directory>`** を入力し、NFS ロケーションを設定します。
4. **`recorder resolution <audio|720p|1080p>`** を入力し、目的の解像度に設定します（または通話の音声のみを録音します）。

5. MMP コマンド**recorder sip listen <interface> <tcp-port|none>** を使用して、レコーダーをリッスンするインターフェイスと、リッスンする SIP TCP および TLS ポートを設定します。 **<tls-port|none>**。 サービスを無効にするには、それぞれのポートを**なし** に設定します:
   a. たとえば、TCP ポートではなく、TLS ポートでのみリッスンする場合、次を入力します。 **recorder sip listen a none 6000を設定します**
   b. 設定したポートがデフォルトの TCP/TLS ポート（5060/5061）でない場合は、後で必要になるため、そのポート番号をメモしておいてください。

   注： デフォルトの SIP TCP/TLS ポート (5060/5061) でリッスンする場合、Call Bridge が同じインターフェイスでリッスンしていないことを確認する必要があります。そうしないと、ポートがクラッシュします。 対応するインターフェイスを削除し、MMP コマンド **callbridge listen none** を入力して、Call Bridge を無効にする必要があります。

6. オプションで、TLS が構成されている場合、使用する SIP TLS 証明書を構成します。
   a. MMP コマンド **recorder sip certs <key-file> <crt-file> [<crt- bundle>]** を入力します。

   注： SIP TLS 証明書がこのオプションで構成されていない場合、SIP TLS サービスは開始できないことに注意してください。

7. オプションで、TLS が構成されている場合、レコーダーの SIP の TLS 検証を次のように実行できます。
   a. MMP コマンド **tls sip trust [<crt-バンドル>]** を入力します。
   b. MMP コマンド **tls sip verify enable** を入力します。

   注： TLS 接続を安全なものにするために、TLS 検証を有効にすることをお勧めします。

8. 設定が正しいことを確認してください。MMP コマンド **recorder** を入力して設定を表示してください。
9. MMP コマンド **recorder enable** を入力してレコーダーサービスを有効にします。

タスク 2: API 経由でレコーダー URI を設定する

新しい SIP レコーダーが有効になると、Call Bridge で、 **sipRecorderUri** API パラメータを指定して、サードパーティの SIP レコーダーと同じように使用することができます。これは API コールプロファイルオブジェクトで指定されます。

希望する場合は、out バウンドダイヤルプランルールにマッピングするカスタム URI を構成することもできます (ドメインは自由に選択できます。例、「recording.com」)。**`sipRecorderUri`** で使用されるドメインをレコーダーにルーティングする方法を Meeting Server に指示する、outboundDialPlan ルールを設定する必要があります。 これにより、優先順位の値、暗号化などをコントロールできます。outboundDialPlan ルールの設定の詳細については、「ダイヤル プランの設定 - 概要」の章を参照してください。

注： 設定された URI のユーザー部分 ('@' 記号の前の部分) には特別な意味がありません。新しい内部 SIP レコーダー コンポーネントでは必須ですが、通常は何でもかまいません例: "recording@recorder.com". しかし、これはユーザー資格情報の URI のユーザー部分を使用する可能性があるサードパーティの SIP レコーダーには当てはまらない場合があります。 URI の重要な部分はドメイン部分です。

Meeting Server のWeb 管理インタフェースを使用して **`sipRecorderUri`** パラメータを設定するには:

1. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）] > [API]** を選択します。
2. API オブジェクトのリストで、**/api/v1/callProfiles** の後の ► をタップします。
3. 既存の通話プロファイルを設定または変更するには、必要な callProfile のオブジェクト ID を選択し、選択した URI を **sipRecorderUri** フィールドに入力します。

   注： 新しい SIP レコーダーを使用する場合、1 つの SIP URI のみを使用する必要があります。例、 recording@recorder.com 異なるプロファイルに異なるSIP URIを設定する必要はありません（違いはありません）。

   ---

4. まだ設定していない場合は、 **録画モード** フィールドを **手動** または **自動** (ミーティングの録画方法による)に設定します。
5. **[変更（Modify）]** をクリックします。

更新された callProfile は、必要に応じて、coSpace、テナント、またはトップレベル (グローバル) プロファイルに割り当てることができます。 この例では、更新された callProfile が次のようにグローバル レベルで割り当てられます。

1. Web 管理インターフェイスを使用して、**[設定（Configuration）] > [API]** の順に選択します。
   a. API オブジェクトのリストで、**/api/v1/system/profiles** 後の ► をタップします。
   b. [**表示または編集**] をクリックします。
   c. パラメータを **callProfile** まで下にスクロールし、[Choose] をクリックします。

d. 表示された「callProfile オブジェクト選択ウィンドウ」から、 **オブジェクト ID** を選択し、 **最上位のグローバルプロファイルに** 割り当てる callProfile を選択します。

e. **[変更（Modify）]** をクリックします。

f. 新しく割り当てられた callProfile オブジェクト ID が、 **[オブジェクトの構成]** の下に表示されます。

11.4.0.1 callProfile 構成例 (一致する発信ダイヤル プラン ルールを使用する場合):

この例では、 **上記の手順を使用して、**recordingModeは **自動** に、 sipRecorderUriは recording@recorder.com に設定されています。

Object configuration	
recordingMode	automatic
sipRecorderUri	recording@recorder.com

Meeting Server のWeb 管理インターフェイスから **[設定（Configuration）]** > **[発信通話（Outbound calls）]** を選択して、一致する発信ダイヤルプランルールを確認します。

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant	
	recorder.com	10.209.131.45		<use local contact domain>	Standard SIP	Stop	0	Unencrypted	no	[edit]
					Standard SIP	Stop	0	Auto		Add New Reset

デフォルトの標準ポート（5060/5061）とは異なる SIP TCP/TLS ポートを使用するように MMP レコーダーを設定した場合、sipRecorderUri フィールドまたは一致する発信ダイヤルプランルールを使用している場合はそのルールに追加します、以下に示すようにリスニングポートを指定しなければなりません。

	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption	Tenant	
	recorder.com	10.209.131.45:6000		<use local contact domain>	Standard SIP	Stop	0	Unencrypted	no	[edit]
					Standard SIP	Stop	0	Auto		Add New Reset

発信ダイヤルプランルールを使用している場合は、指定されたポートのサービスが暗号化タイプと一致していることを確認してください。例えば、SIP TLS ポートを使用している場合、**暗号化** モードを **暗号化**に設定します。

11.5 外部のサードパーティ SIP レコーダーの設定

- SIP レコーダーを指定します – /callProfile オブジェクトの sipRecorderUri API パラメーターを使用します。 設定されている場合、このURIは録画が有効な場合にダイヤルアウトするために使用されます。 設定されていない場合、Meeting Serverのレコーダーコンポーネント (/recorders で設定されている場合) が使用されます。

  a. Meeting Server のWeb 管理インタフェースを使用して、**[設定（Configuration）]** > **[API]** の順に選択します。

b. API オブジェクトのリストで、/callProfiles の後ろの ▸ をタップします。

c. 既存の通話プロファイルの **オブジェクト** ID をクリックするか、新しいプロファイルを作成する。

d. sipRecorderUri パラメータを設定します。

- API オブジェクト /callProfiles または /callProfiles/<call profile id>の recordingMode パラメータを使用して、ミーティングを録画できるかどうかを選択します。 このためのオプションは次のとおりです。
  - **自動** – ユーザーの介入なしで録画が行われます。録画ができない場合でもミーティングは行われます。
  - **手動** – ユーザーは DTMF を使用して手動で録画を開始および停止できます。
  - **無効** – どのユーザも録画できません。
- callLegProfiles の RecordingControlAllowed パラメーターを設定することで、どのユーザーが録画を開始および停止する権限を持つかを制御します。
- /dtmfProfiles に対して startRecording および stopRecording パラメータを使用します。/dtmfProfiles/<dtmf profile id> をマッピングするために、録音を開始および停止する DTMF トーンを使用します。

注： 追加の API オブジェクトについては、 Cisco Meeting Server API リファレンスガイドを参照してください。

11.6 レコーディングの状況を確認する

録画の状況を確認するには:

- Meeting Server のWeb 管理インタフェースを使用して、[**設定**（Configuration）] > [API] の順に選択します。
- API オブジェクトのリストで、/callLegs の後ろの ▸ をタップします。
- 既存のコールレッグ **のオブジェクト** ID をクリックしてください。

`callLegs/<call leg id>` で GET を実行します– **録音** の **ステータス** 出力は、この callLeg が録音されているか (**`true`**)、否か (**`false`**) を示します。

11.7 デュアルホーム会議の録画インジケータ

デュアルホーム電話会議の場合、録画は Lync/Skype エンドポイントで Microsoft 録画メソッドを使用して実行する必要があります。 デュアルホーム電話会議の録画に Cisco Meeting Server の使用はお勧めしません。

録画アイコンは、Meeting Server に接続している SIP 参加者に、Lync/Skype エンドポイントが Lync/Skype 側で電話会議を録画していることを示します。

Meeting Server は、ActiveControl 以外のエンドポイント用に作成されたビデオペインに録画アイコンを追加します。 表 10 は、デュアルホームド会議が録画されていることを示すために Meeting Serverが表示するアイコンを示しています。

表 10: 録画インジケータ

表示されるアイコン	説明
	ミーティングはMeeting Server経由で録画されています。
	ミーティングが Lync/Skype エンドポイントにより録画されています。
	ミーティングがMeeting Server経由、および Lync/Skype エンドポイント経由で録画されています。
	ミーティングは録画されていません (アイコンは表示されていません)。

注：ウェブアプリは独自のアイコンを使用して録画の状態を表示しますが、ローカルとリモートの録画を区別しません。 Meeting Server のアイコンがウェブ アプリのビデオ ペインにオーバーレイ表示されません。

11.8 Vbrick で録画する

注： この項は、Meeting Serverの内部レコーダーコンポーネントにのみ適用されます。

アップローダコンポーネントは、Meeting Server に設定された NFS 接続からビデオコンテンツマネージャ Vbrick に Meeting Server録画をアップロードするためのワークフローを簡素化します。 録画を手動でインポートする必要はありません。

アップローダ コンポーネントが設定され、有効になると、録画が NFS から Vbrick にプッシュされ、録画に所有者が割り当てられます。 Rev ポータルはビデオコンテンツに管理者が設定したセキュリティを適用し、ユーザーがアクセスできるのは、許可されたコンテンツのみです。所有者の Rev ポータルで録画が利用可能になると、Vbrick から所有者にメールが届きます。録画の所有者は Rev ポータルからビデオ コンテンツにアクセスし、必要に応じて編集して配信できます。

注： ファイルがスペースディレクトリ内の NFS 共有に追加される場合、ファイルは有効な録画であるかのように Vbrick にアップロードされます。 レコーダーだけが書き込みできるように、NFS 共有に権限を適用するように注意してください。

注：録画の保存に使用するメカニズムによっては、レコーダー、アップローダ、ストレージシステムが通信できるように、外部ファイアウォールポートを開く必要がある場合があります。最初の着信:

例：ポートマッパープロトコルのバージョン 2 または 3 を実行している NFS は、TCP または UDP ポート 2049 および 111 を使用します。

注：レコーダーまたはアップローダを使用する場合は、Meeting Serverでファイアウォールコンポーネントを使用しないでください。

11.8.1 ミーティングサーバーの前提条件

アップローダのインストール アップローダ コンポーネントは、レコーダー コンポーネントと同じサーバーにインストールすることも、別のサーバーにインストールすることもできます。レコーダーと同じサーバーにインストールされている場合、使用する vCPU をいくつか追加します。 別のサーバーで実行する場合、レコーダーと同じサーバー仕様、つまり最小 4 つの物理コアと 4GB の RAM を備えた専用 VM を使用します。

警告： アップローダは、電話会議を主催する Call Bridge とは別のMeeting Server 上で実行する必要があります。

NFS 共有への読み取りおよび書き込みアクセス権。 アップローダを実行している Meeting Server には、NFS の読み取りおよび書き込み権限が必要です。 アップロードが完了したときにアップローダが mp4 ファイルの名前を再書き込みできるようにするには、書き込み権限が必要です。

注： NFS が設定されているか、読み取り専用になっている場合、アップローダコンポーネントは同じビデオ録画を Vbrick にアップロードし続けます。 このエラーは、アップローダがファイルにアップロード完了のマークを付けることができないことが原因です。 これを回避するには、NFS が読み取り/書き込みアクセスを提供していることを確認してください。

Vbrick RevへのAPIアクセス Vbrick Revのユーザーの API アクセスを設定します。

Call Bridge への API アクセス。 Call Bridge を実行しているMeeting Server で、ユーザーの API アクセスを設定する。

トラストストア Vbrick Rev サーバーからの証明書チェーン、および Call Bridge のWeb 管理インターフェイスを実行しているMeeting Server を保存する。 アップローダは Vbrick Rev と Call Bridge の両方を信頼する必要があります。

ビデオ録画にアクセスできるユーザを決定します。アップロードされたビデオ録画へのアクセスは、すべてのユーザ、プライベート、スペース所有者とメンバーのみに設定できます。

ビデオ録画のデフォルト状態。 アップロード後すぐにビデオ録画を利用可能にするか (アクティブ)、またはビデオ録画の所有者が公開する必要があるか (非アクティブ) を決定します。

表 11: ポート要件

コンポーネント	接続先	開く接続先ポート
Call Bridge	NFS (バージョン 3)	2049
アップローダー	Call Bridge のWeb 管理	443 またはアップローダ設定で指定されたポート
アップローダー	Vbrick Rev サーバー	443 ビデオ アップロードおよび Vbrick Rev サーバーへの API アクセス

11.8.2 Vbrick と連携するようにミーティングサーバーを設定する

これらの手順は録画を保存するための NFS のセットアップが完了していることを前提としています。

1. アップローダを実行するMeeting Server の MMP への SSH 接続を確立します。 ログインします。
2. 新しい Vbrick インストールの場合、この手順は無視してください。 Vbrick インストールを再設定する場合、まずMeeting Server への Vbrick アクセスを無効にします。
   アップローダの無効化

3. アップローダが監視する NFS を指定します。
   uploader nfs <hostname/IP>:<directory>
4. アップローダが録画に関連するスペースをホストしているMeeting Server の名前などの録画情報を照会するMeeting Server を指定します。
   uploader cms host <hostname>
5. Call Bridge を実行しているMeeting Serverのウェブ管理ポートを指定します。 ポートが指定されていない場合、デフォルトでポート 443 になります。
   uploader cms port <port>
6. Call Bridge を実行しているMeeting Server上で API アクセスを持つユーザーを指定します。 パスワードは別に入力します。
   uploader cms user <username>
7. ステップ 6 で指定したユーザーのパスワードを設定します。次を入力します。
   uploader cms password
   パスワードの入力が求められます。
8. ルート CA の証明書のコピーを保持する証明書バンドル (crt-バンドル) を作成し、Call Bridgeを実行しているMeeting Server のWeb 管理用のチェーンにあるすべての中間証明書のコピーを保持します。
9. 手順 8 で作成した証明書バンドルをMeeting Server の信頼ストアに追加します。
   uploader cms trust <crt-bundle>
10. アップローダが接続するVbrick ホストとポートを設定します。
    uploader rev host <hostname>
    uploader rev port <port>

    注： 特に指定がない限り、ポートのデフォルトは 443 です。

11. ビデオ録画をアップロードするための API 権限を持つ Vbrick Rev ユーザーを追加します。
    uploader rev user <username>
12. ステップ 11 で指定したユーザーのパスワードを設定します。次を入力します。
    uploader rev password
    パスワードの入力が求められます。
13. ルート CA の証明書と Vbrick Rev サーバーのチェーンにあるすべての中間証明書のコピーを保持する証明書バンドル (crt-バンドル) を作成します。
14. 手順 13 で作成した証明書バンドルを Vbrick Rev の信頼ストアに追加します。
    uploader rev trust <crt-bundle>
15. ビデオ録画へのアクセスを設定します。
    uploader access <Private|Public|AllUsers>
16. 録画を表示または編集する権限をスペースのメンバーに付与します。
    uploader cospace_member_access <view|edit|none>

注： このステップでは、リスト中のメンバーが Vbrick のアカウントに関連付けられた有効なメール アドレスを持っている必要があります。 For example **user1@example.com**

17. 会議スペースの所有者がビデオ記録の単独の所有者であるかどうかを決定します。
    uploader recording_owned_by_ cospace_owner <true|false>

    注：また、このステップでは、ビデオ録画の所有者が Vbrick のアカウントに関連付けられた有効なメール アドレスを持っている必要があります。

18. 会議スペースの所有者が Vbrick リビジョンにリストされていない場合、代替所有者のユーザー名を設定します。 フォールバック所有者が指定されていない場合、MMP で設定されたユーザーがデフォルトで所有者になります。
    uploader fallback_owner <vbrick-user>
19. ビデオ録画へのコメントを有効にします。
    uploader comments enable
20. 録画のレーティングを有効にします。
    uploader ratings enable
21. ビデオ録画のダウンロード権限を設定します。
    uploader downloads enable
22. Vbrick Rev に最初にアップロードされたビデオ録画のデフォルト状態を設定します。
    uploader initial_state <active|inactive>
23. アップロード完了後に NFS から録画を削除するかどうかを決定する
    uploader delete_after_upload <true|false>
24. アップローダが Meeting Server にアクセスできるようにする
    アップローダの有効化

注: 録画が利用可能であることを示すメッセージがスペースに投稿されることを確認するには、messageBoardEnabled **を** true **に設定**します。

11.9 ミーティングのストリーミング

内部 SIP ストリーマコンポーネント（バージョン 3.0 以降）は、スペースで開催されるミーティングをストリーミングする機能を、スペースで設定された RTMP URL に追加します。

この RTMP URL をリッスンするには、外部ストリーミングサーバーを設定する必要があります。 外部ストリーミングサーバーは、ユーザーにライブストリーミングを提供したり、後で再生するためにライブストリームを録画したりできます。

注：ストリーマコンポーネントは、RTMP 標準をサポートするサードパーティのストリーミングサーバーと連携するために、RTMP 標準をサポートしています。 Vbrick は正式にサポートされている外部ストリーミングサーバーですが、他のサーバーでもテストされています。

注：ストリーマコンポーネントは、RTMP 標準をサポートするサードパーティのストリーミングサーバーと連携するために、RTMP 標準をサポートしています。 Vbrick は正式にサポートされている外部ストリーミングサーバーですが、他のサーバーでもテストされています。

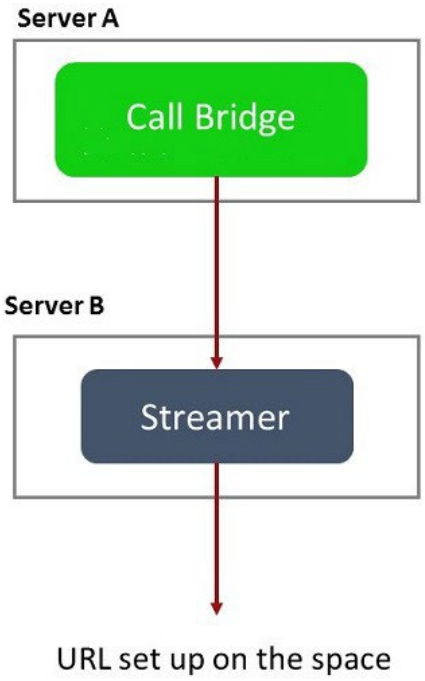
注：ストリーミングの宛先 RTMP URL がファイアウォールの外側にある場合は、ファイアウォールのポートを開く必要があります。

バージョン 3.1 では、内部 SIP ストリーマアプリケーションの RTMP サポートを RTMPS に拡張します。本質的には TLS 接続上の RTMP です。 これまでは、ストリーマと RTMP サーバー間のすべてのトラフィックは暗号化されていませんでした。3.1 RTMPS のサポートにより、このトラフィックを暗号化することができます。

既存の **tls** MMP コマンドが拡張され、オプションで RTMPS の TLS トラストの設定ができるようになりました。 このステップはオプションですが、推奨されています。 TLS 信頼が設定されていない場合、RTMPS 接続は安全ではありません。

次の図は、許可されているストリーマ導入を示しています。

図 20: ストリーミングで許可されている導入: リモートモード



テスト目的でのみ、ストリーマを Call Bridge と同じサーバー上に共存させることができます。これは 1 から 2 の同時ストリーミングをサポートします。

11.10 VM サーバーに新しい SIP ストリーマ コンポーネントを導入する

これは 2 段階のプロセスです。

- MMP 経由で Meeting Server ストリーマを設定する
- API 経由でストリーマー URI を設定する

タスク 1：MMP 経由でMeeting Serverのストリーマを設定する

1. バージョン 3.0 にアップグレードします。
2. MMP に SSH で接続し、ログインしてレコーダーを設定します (MMP コマンド、**`streamer help`** で、使用可能なすべてのコマンドのリストを表示します）。
3. MMP コマンド **`streamer sip listen <interface> <tcp-port|none>`** を使用して、ストリーマをリッスンするインターフェイスと、リッスンする SIP TCP および TLS ポートを設定します。**`<tls-port|none>`**。 サービスを無効にするには、それぞれのポートを **なし** に設定します:

a. たとえば、TCP ポートではなく、TLS ポートでのみリッスンする場合、次を入力します。**`streamer sip listen a none 6000`**

b. 設定したポートが既定の TCP/TLS ポート (5060/5061) ではない場合、後で必要になるため、メモしておいてください。

4. 必要に応じて、MMP コマンドを使用して、ストリーマが使用する(または通話の音声のみをストリーミングさせたい)最大解像度を設定することができます。 **`streamer sip resolution <audio|720p|1080p>`**です。指定しない場合、720pがデフォルトになります。

a. 例えば、1080p に設定したい場合、**`streamer sip resolution 1080p`** と入力します。

注：1080p を使用する場合は、送信 SIP 通話帯域幅を 3,500,000 ビット/秒に増やしてビデオ品質を最適化することをお勧めします。 これを行うには、Web 管理 UI で [Configuration] **に移動します。**[Call settings] **>帯域幅の設定** (SIP) および必要に応じて設定します。

---

5. オプションで、TLS が構成されている場合、使用する SIP TLS 証明書を構成します。

a. MMP コマンド **`streamer sip certs <key-file> <crt-file> [<crt- bundle>]`** を入力します。

注： SIP TLS 証明書がこのオプションで構成されていない場合、SIP TLS サービスは開始できないことに注意してください。

---

6. TLS が設定されている場合、オプションとして、以下のようにストリーマの SIP (または LDAP または RTMPS) の TLS 検証を実行できます。

a. MMP コマンド **`tls sip trust [<crt-バンドル>]`** を入力します。

b. MMP コマンド **`tls sip verify enable`** を入力します。

注： TLS 接続を安全なものにするために、TLS 検証を有効にすることをお勧めします。

---

7. 設定が正しいことを確認してください。設定を表示するには、MMP コマンド 'streamer' を入力します。

8. MMP コマンド **ストリーマ エネーブル** を入力してストリーマサービスを有効にします。

タスク 2：API 経由でストリーマ URI を設定する

新しい SIP ストリーマが有効になると、API コール プロファイル オブジェクトで指定された **`sipStreamerUri`** API パラメータを使用して、Call Bridge で設定して使用できます。

希望する場合は、'outboundDialPlan' ルールにマッピングするカスタム URI を設定することもできます (ドメインは自由に選択できます。例、「streaming.com」)。 **sipStreamerUri** で使用されるドメインをストリーマにルーティングする方法を Meeting Server に指示する、outboundDialPlan ルールを設定する必要があります。 これにより、優先順位の値、暗号化などを制御することができます。**/outboundDialPlanRules**の設定の詳細については、導入ガイドの「ダイヤル プランの設定 - 概要」の章を参照してください。

注：設定された URI のユーザー部分 ('@' 記号の前の部分) には特別な意味がありません。新しい内部 SIP ストリーマコンポーネントでは必須ですが、通常は何でもかまいません例: "streaming@streamer.com". URI の重要な部分はドメイン部分です。

Meeting Serverのウェブ管理インタフェースを使用して **sipStreamerUri** パラメータを設定するには:

1. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）] > [API]** を選択します。
2. API オブジェクトのリストで、/api/v1/callProfiles の後の ▶ をタップします。
3. 既存の通話プロファイルを設定または変更するには、必要な callProfile のオブジェクト ID を選択し、選択した URI を sipStreamerUri フィールドに記入します。

   注：新しい SIP ストリーマを使用する場合、1 つの SIP URI のみを使用する必要があります。例: streaming@streamer.com、異なるプロファイルで異なる SIP URI を持つ必要はありません。

   ---

4. まだ設定していない場合は、 **streamingMode** パラメータを **manual** または **自動**（ミーティングをどのようにストリーム配信するかによります）
5. **[変更（Modify）]** をクリックします。

更新された callProfile は、必要に応じて、coSpace、テナント、またはトップレベル (グローバル) プロファイルに割り当てることができます。 この例では、更新された callProfile が次のようにグローバル レベルで割り当てられます。

1. Web 管理インターフェイスを使用して、**[設定（Configuration）] > [API]** の順に選択します。
   a. API オブジェクトのリストで、/api/v1/system/profiles 後の ▶ をタップします。
   b. **[表示または編集]** をクリックします。
   c. パラメータを callProfile まで下にスクロールし、[Choose] をクリックします。

d. 表示された「callProfile オブジェクト選択ウィンドウ」から、 **オブジェクト ID** を選択し、 **最上位のグローバルプロファイルに** 割り当てる callProfile を選択します。

e. **[変更（Modify）]** をクリックします。

f. 新しく割り当てられた callProfile オブジェクト ID が、 **[オブジェクトの構成]** の下に表示されます。

ストリーミングを有効にする API の各 coSpace について、 **`streamUrl`** coSpace API フィールドに、ストリーミング先の RTMPS ストリーム URL を設定する必要があります (例: "rtmps://mystream.com/live/app"). これを構成するには:

1. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）]** > **[API]** を選択します。
2. API オブジェクトのリストで、**/api/v1/coSpaces** の後ろの ▶ をタップします。
3. 既存の共有スペースを設定または変更するには、必要な共有スペースのオブジェクト ID を選択します。**streamUrl** フィールドにストリーミング先の RTMPS ストリーム URL を入力します。
4. **[変更（Modify）]** をクリックします。

11.10.1 既知の制限事項

警告：ストリーム URL は SIP ヘッダーで送信されるため、ログイン資格情報を含むすべての RTMP ストリーム URL は、ログを記録する可能性のあるコールコントロールプロバイダに露出される可能性があることに注意してください。

12 Cisco Meeting Server web app のシングルサインオン（SSO）

この機能により、ウェブアプリユーザーは SSO プロバイダーを使用してログインし、ID を確認できます。

SSO は、ウェブアプリのユーザーが、ログインするたびにパスワードを入力する必要がないことを意味します。これは、例えば、OAuth、Gmailなどのアイデンティティプロバイダーとの単一のセッションを持つことができるためです。

これにより、ウェブアプリユーザーは異なる SSO プロバイダを使用して同じ Web Bridge にログインできます。

この SSO メカニズムでは、オープン標準で業界標準プロトコルとして広く使用されている SAML (Security Assertion Markup Language) 2.0 を使用しています。

注： 現在、Meeting Serverは SAML 2.0 プロトコルでの HTTP-POST バインディングのみをサポートしています。 これは、HTTP-POST AssertionConsumerService でのみメッセージを受け入れ、HTTP-POST バインディングが利用できない ID プロバイダを拒否することを意味します。

注： SSO ログインを有効にすると、LDAP ログインは使用できなくなります。

12.1 Meeting Server web app で使用する SSO を設定する

SSO を使用するには、ID プロバイダとMeeting Server (SAML 2.0 交換でサービスプロバイダと見なされる) で、以下に示すいくつかの設定が必要です。

タスク 1: ID プロバイダとMeeting Serverユーザ間のマッピング

Meeting Serverが ID プロバイダのユーザーを適切なユーザーにマッピングできるように、SSO 経由で認証されるすべてのユーザーに対し、authenticationId をセットアップする必要があります。 これは、標準 LDAP 同期プロセスの一部として実行できます。 このフィールドのコンテンツは、成功の応答でアイデンティティ プロバイダから渡されたカスタム パラメータに対して検証されます (タスク 2 を参照)。

各ユーザーに一意の識別子を選択することをお勧めします (例: $sAMAccountName$)。authenticationId の空の値は受け入れられません。

ldapSync の一部として authenticationId をセットアップするには、新しい ldapSync を作成するか、既存のものを変更します。

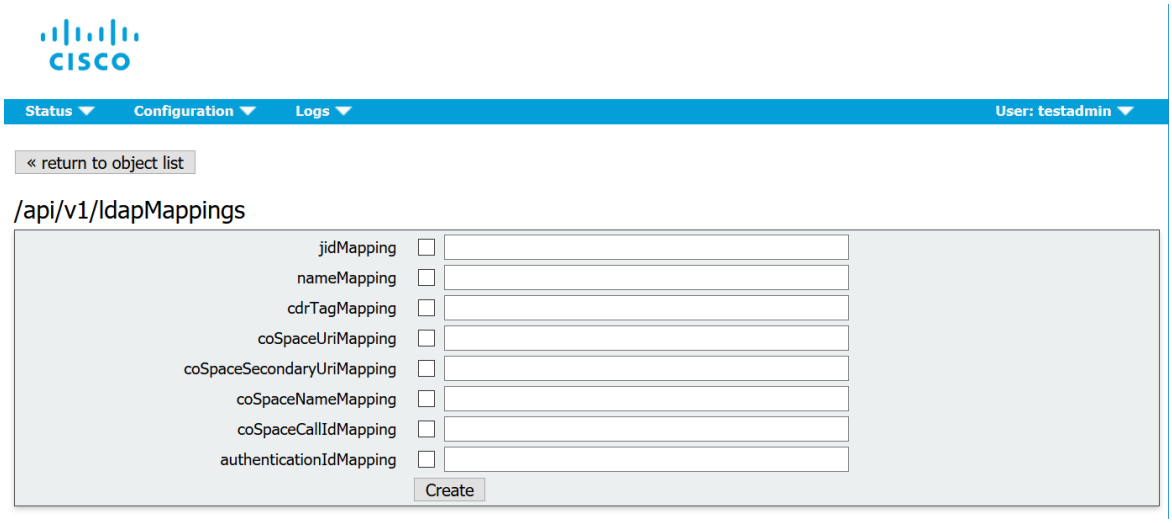
次に、ldapマッピングを作成/変更し、 **authenticationIdマッピング** パラメータに適切な値を入力する必要があります (例、$sAMAccountName$)。

Meeting Server のWeb 管理インタフェースを使用する:

a. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）]** > **[API]** を選択します。

b. API オブジェクトのリストで、**/api/v1/ldapMappings** の後ろの ▶ をタップします。

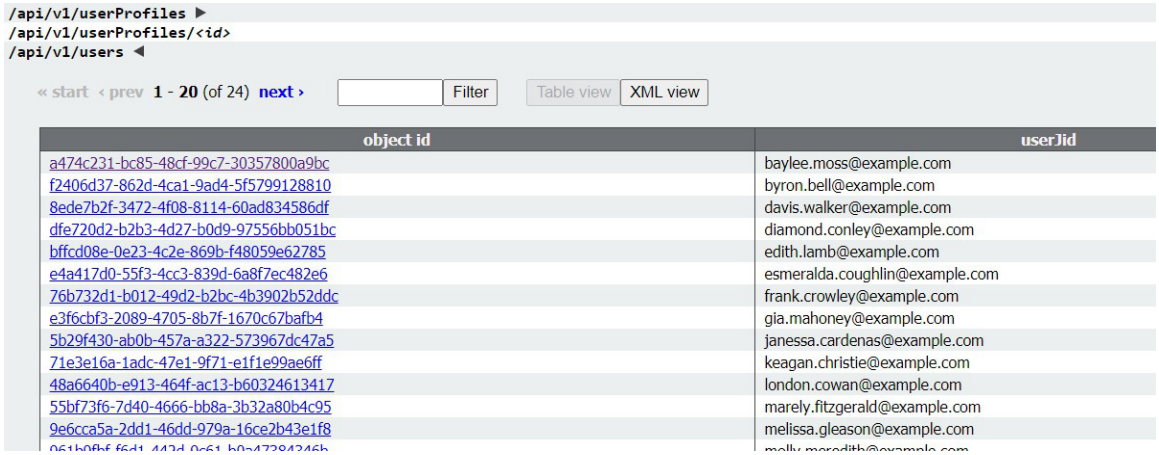
c. **[新規作成（Create new）]** をクリックするか、変更する既存の LDAP マッピングの ID を選択します。



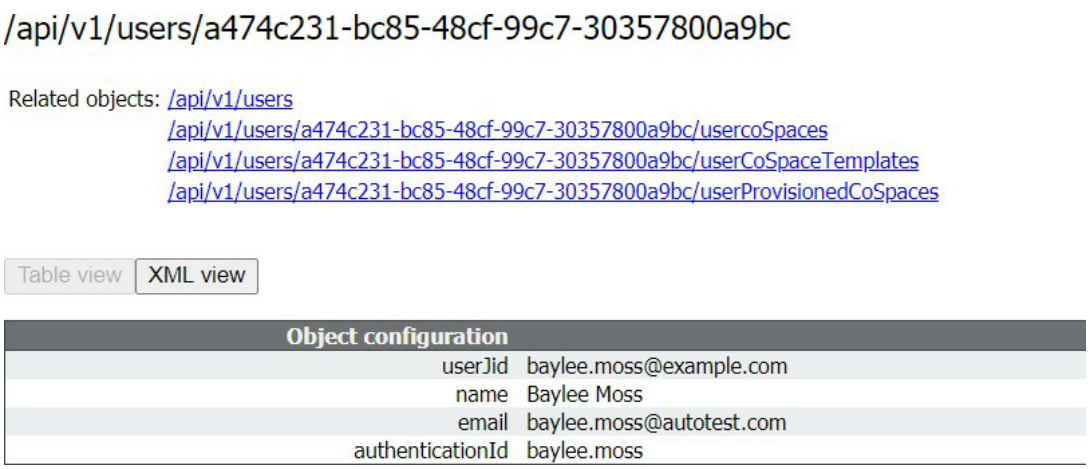
d. **authenticationIdMapping** パラメータに適切な値を入力します (例: $sAMAccountName$) を選択し、必要に応じて **[作成（Create）]** または **[変更（Modify）]** をクリックします。

e. Meeting Serverで変更を有効にするには、ldapSync をトリガーする必要があります。API オブジェクトのリストから、▶ **/api/v1/ldapSyncs** の後] をクリックしてオブジェクト ID を選択するか、 **新規作成** を選択します。 ldapSync が完了したら、Meeting Serverユーザーの 1 人を調べることで、プロセスが成功したことを確認できます。

f. まず、API オブジェクトのリストから、▶ **/api/v1/users** の後でタップして、次の例のようにユーザーのリストを表示します。



g. authenticationId をセットアップするユーザーの 1 人を選択します (場合によっては [フィルター] フィールドを使用します)。 ユーザーエントリには、次の例に示すように、ldapSync からの正しい値を持つ authenticationId フィールドが今は含まれるべきです。



タスク 2: ID プロバイダの構成

1. すべての ID プロバイダで、登録されているサービスプロバイダ (このインスタンスの場合はミーティングサーバー) を表すメタデータ xml ファイルをアップロードできます。一部の ID プロバイダーでは、最も重要な情報を設定できるため、プロセスが簡素化されます。 メタデータ xml ファイルの例は ここで確認できます。

   ID プロバイダにアップロードされるメタデータ xml ファイルに含まれる値:

   a. entityID – Web Bridge 3 アドレスです (例、https://<domain>:port)。 このアドレスは、ウェブアプリユーザーのブラウザから到達可能な有効な Web Bridge 3 アドレスである必要があります。

注： 展開に複数のWeb Bridge 3 がある場合、これは負荷分散されたアドレスである必要があります。

b. 「https://<domain>:<port>/api/auth/sso/idpResponse」形式に従い、entityId として定義されたWeb Bridge アドレスの HTTP-POST AssertionConsumerService。

c. 任意。 ID プロバイダが AuthnRequest 署名を確認するために使用する署名用の公開鍵。

d. 任意。 ID プロバイダが上記で提供されたアドレス経由でルーティング可能ないずれかのWeb Bridgeに送り返される情報を暗号化する際に使用する公開鍵です。

注：Meeting Server に送信するメッセージは、ID プロバイダによりレスポンスおよび/またはアサーションレベルで署名されている必要があります。 署名されていない通信は破棄されます。

2. 成功の応答で ID プロバイダから渡されたカスタム パラメータを設定する必要があります。 各ユーザーのコンテンツは、そのMeeting Serverユーザーの authenticationId として設定済みの値と一致する必要があります (例、$sAMAccountName$)。 通常、ID プロバイダは、サービスプロバイダエントリを作成する一環として、専用のフォームまたはダイアログを持ちます。 このパラメータには任意の名前を付けることができますが、「uid」など、覚えやすい名前を付けることをおすすめします (タスク 3 で名前が必要になります)。

タスク 3: SSO アーカイブ zip ファイルを作成する

1. Meeting Serverを設定するには、sso_ という名前のアーカイブ zip ファイルを作成する必要があります。<name>.zip を、その Meeting Server 上の Web Bridge 3 に設定する各 SSO 用に作成します。 "sso_"で始まり、その後に自分で選んだ意味のある名前を付ける必要があります。

   これらのファイルを含む zip アーカイブファイルを作成します。

   a. idp_config.xml – 管理者が ID プロバイダから受け取るファイルです。

   b. config.json – 含む:

      - supportedDomains (文字列の配列) – この ID プロバイダに対して認証されるMeeting Serverユーザーのすべてのドメインのリストです。 つまり、タスク 1 の例を使うと、supportedDomains には "example.com" という単一のエントリが含まれることになります。
      - authenticationIdMapping (文字列) – Meeting Server の authenticationIds に一致する、 タスク 2 の一部として設定された ID プロバイダの応答のパラメータ

(例、「uid」) の名前。 SSO のウェブアプリユーザーは、authenticationIds をセットアップする必要があります (タスク 1 を参照してください。)

- ssoServiceProviderAddress (文字列) – アイデンティティ プロバイダが応答を送信するアドレスです。これは タスク 2 の entityID で指定された Web Bridge 3 と一致します。

c. 任意です。sso_sign.key – ID プロバイダ側で設定された公開署名用の秘密鍵です。これは、Meeting Serverからの発信 AuthnRequest に署名するために使用され、アイデンティティプロバイダ側で公開鍵を使用して確認されます。

d. 任意です。sso_encrypt.key – ID プロバイダ側で設定された公開暗号化キーの秘密鍵です。 これは、アイデンティティプロバイダ側で公開鍵で暗号化されたメッセージをMeeting Server上で復号化するために使用されます。

注： ID プロバイダごとに異なる名前付き zip ファイルが必要です。

2. SSO ファイルを含むアーカイブ (zip) ファイルを作成します。

注： ファイルを圧縮する場合、SSO ファイルを含むフォルダは圧縮しないでください。これが行われると、フォルダの追加レイヤーが作成されます（zip 形式のファイル > フォルダ > SSO ファイル）。 代わりに、SSO ファイルをハイライトし、それらを右クリックして圧縮してください (または、zip アプリケーションを開き、ファイルをまとめて圧縮します)。 これにより、追加のフォルダ レイヤーを作成することなく、SSO ファイルを含む zip ファイルが作成されます (例: zip ファイル > SSO ファイル)。

タスク 4: SSO アーカイブ zip をアップロードする

SSO アーカイブの zip はアップロードされ、ローカルのWeb Bridge 3 でホストされる必要があります。

注： 次の手順で使用するコマンドは、コンソール/ターミナル環境 (コマンドプロンプトまたはターミナル) を対象としたものであり、WinSCP などの SFTP クライアントを対象としたものではありません。

1. この zip アーカイブをローカルでホストする、有効になっているWeb Bridge 3 を持つ各 Meeting Server について、
2. a. SFTP クライアントを MMP の IP アドレスに接続します。

   b. MMP 管理者ユーザーの資格情報を使用してログインします。

   c. zip ファイル **sso_<name>.zip**をアップロードしてください。 次に例を示します。

```
PUT sso_<name>.zip
```

d. SSH クライアントを MMP の IP アドレスに接続します。

e. MMP 管理者ユーザーの資格情報を使用してログインします。

f. Web Bridge 3 を再起動します。

```
webbridge3 restart
```

3. 新しい SSO アーカイブファイルは再起動後に反映されます。

注： ウェブアプリユーザーがログインすると、ウェブアプリアプリケーションで、ID プロバイダとのセッションとは別のセッションを持つことになります。 これは、同じユーザー名を入力した後に ID プロバイダ ではなく、Web アプリケーションからログアウトやサインアウトしても、Web アプリケーションに自動的に再許可されることを意味します。 ただし、ID プロバイダーからサインアウトする場合は、ウェブ アプリ アプリケーションからはサインアウトしないため、ウェブ アプリ アプリケーションからもサインアウトする必要があります。 このブラウザセッションで再度ログインできないようにするには、web app application と ID プロバイダーの両方からサインアウトする必要があります。

12.1.1 例 1 config.json ファイル

これは config.JSON ファイルの例です。

```
{
    "authenticationIdMapping" : "<parameter_from_task_2>",
    "ssoServiceProviderAddress" : "https://<domain>:<port>",
    "supportedDomains" : ["<domain1>","<domain2>"]
}
```

12.1.2 例 2：シンプルなサービスプロバイダのメタデータファイル。

これは、サービスプロバイダの簡単なメタデータファイルの例です。管理者は、<domain>および<port>をそれぞれの適切な値に変更する必要があります。

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https://<domain>:<port>" entityID="https://<domain>:<port>">
  <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://<domain>:<port>/api/auth/sso/idpResponse" index="0"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

12.1.3 例 3 総合的なサービスプロバイダー メタデータ ファイル。

これは、署名および暗号化キーの xml を含む包括的なメタデータ ファイルの例です。

注： 鍵は、使用パラメータ（「暗号化」または「署名」）に従って、対応する KeyDescriptor 要素の X509Certificate サブ要素に配置する必要があります。 「...」をキーのテキストコンテンツに置換する必要があります（例：ds:X509CertificateMIID**<omitted_key_ text>**+gb</ds:X509Certificate>）

注： 署名証明書を含める場合、AuthnRequestsSigned の値は「true」に設定されます (例 2 の簡単なメタデータファイルでは「false」に設定されています)。

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
ID="https://<domain>:<port>" entityID="https://<domain>:<port>">
  <md:SPSSODescriptor AuthnRequestsSigned="true" WantAssertionsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
         <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>...</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
    <md:AssertionConsumerService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://<domain>:<port>/api/auth/sso/idpResponse" index="0"/>
  </md:SPSSODescriptor>
</md:EntityDescriptor>
```

12.2 ワンクリックシングルサインオンの設定（ベータ版機能）

One Click Single Sign On（SSO）は、自動リダイレクトを有効にすることで、Cisco Meeting Server web app におけるシングルサインオン（SSO）の利用体験を向上させます。 デフォルトドメインが設定されている場合、ユーザはログイン時にユーザ名を手動で入力する必要がなくなります。

注：Cisco は、ベータ機能が将来完全にサポートされる機能になることを保証しません。 ベータ機能はフィードバックに基づいて変更される可能性があり、機能は今後変更されるか削除される可能性があります。

この機能を有効にするには、config.json ファイル内で新しい **isDefaultIdp** パラメーターを true に設定してください。 有効化されると、ミーティングサーバは **supportedDomains** 配列にリストされている最初のドメインをデフォルトドメインとして識別します。 その他の設定済みドメインには、Alternate SSO を使用して引き続きアクセスできます。

注意点:

- **デフォルトの動作：**config.json ファイルに **isDefaultIdp** パラメータを追加しない場合、サインインエクスペリエンスは変更されません。参加者は引き続き **[サインイン（Sign in）]** を選択し、username@domain 形式で資格情報を入力する必要があります。
- **UI インジケータ：デフォルトの IdP** が設定されている場合にのみ、「**SSO サインイン**」ラベルが表示され、ワンクリック SSO を利用できます。
- **複数のドメインの管理：**デフォルト ドメインを変更するには、管理者は **supportedDomains** リストの順序を変更して、優先するドメインが最初に表示されるようにする必要があります。
- **設定の競合：**デフォルトとして設定できる ID プロバイダ（isDefaultIdp: true）は 1 つのみです。 複数の ID プロバイダーがこのパラメータを true に設定して構成されている場合、システムはデフォルトでアルファベット順で最初の SSO 構成ファイルを使用します。

12.2.1 例：config.json ファイル

これは config.JSON ファイルの例です。

```
{
"authenticationIdMapping" : "<uid>",
"ssoServiceProviderAddress" : "https://<domain>:<port>",
"supportedDomains" : ["<domain1>","<domain2>"],
"isDefaultIdp": true
}
```

13 ActiveControl のサポート

Meeting Server は、主催された通話に対して ActiveControl をサポートしています。 CE 8.3+ ソフトウェアがインストールされた Cisco SX、MX または DX エンドポイントを使用する参加者の場合、ActiveControl によりミーティングの詳細を受け取り、ミーティング中にエンドポイント インターフェイスを使用していくつかの管理タスクを実行することができます。

13.1 Meeting Server の ActiveControl

Meeting Server は、ActiveControl が有効なエンドポイントへの次のミーティング情報の送信をサポートしています。

- 参加者リスト (参加者リストとも呼ばれます): 通話の参加者の名前と参加者の合計数を確認することができます。
- 発言中の参加者の音声アクティビティのインジケータ、
- 現在プレゼンテーションを行っている参加者を示すインジケータ、
- ミーティングが録画されているか、ストリーミングされているか、および通話中にセキュアではないエンドポイントが含まれているかどうかを示すインジケータ、
- すべての参加者に表示されるオンスクリーンメッセージ、

また、ActiveControl が有効なエンドポイントでこれらの管理タスクをサポートしています。

- エンドポイントに使用するレイアウトを選択し、
- ミーティングの他の参加者を切断します。

13.2 制約事項

- ActiveControl が有効な通話が、9.1 (2) より古い Unified CM バージョンの Unified CM トランクを通過する場合、通話は失敗する場合があります。 ActiveControl は、古い Unified CM トランク (Unified CM 8.x 以前) では有効にしないでください。
- ActiveControl は SIP のみの機能です。 H.323 インターワーキングシナリオはサポートされていません。

13.3 ActiveControl と iX プロトコルの概要

ActiveControl は、SIP セッション記述プロトコル (SDP) のアプリケーション回線として通知される iX プロトコルを使用します。 Meeting Server 自動的に ActiveControl をサポートしますが、この機能は無効にできます。セクション第 13.4 項を参照してください。 遠端ネットワー

クが不明であるか、iX プロトコルをサポートしないデバイスがあることがわかっている状況では、Meeting Server と他のコール制御またはビデオ会議デバイス間の SIP トランクで iX を無効にするのが最も安全です。 例：

- Unified CM 8.x 以前のシステムへの接続では、古い Unified CM システムは ActiveControl 対応デバイスからの発信を拒否します。 これらの通話の失敗を回避するには、ネットワーク内の Unified CM 8.x デバイスに向かうトランクで iX を無効のままにしておきます。 SIP プロキシ経由で 8.x デバイスに到達する場合、iX がプロキシへのトランクで無効になっていることを確認します。
- サードパーティネットワークへの接続用。 このような場合、サードパーティのネットワークが ActiveControl 対応デバイスからの呼び出しをどのように処理するかはわからず、処理システムによっては拒否される場合があります。 このような通話の失敗を避けるには、サードパーティネットワークへのすべてのトランクで iX を無効のままにします。
- 外部ネットワークに接続する、または内部で古い Unified CM バージョンに接続する、Cisco VCS 中心の導入用。 Cisco VCS X8.1 から、ゾーン フィルターをオンにして、外部ネットワークまたは古い Unified CM システムに送信される INVITE 要求の iX を無効にすることができます。 （デフォルトでは、このフィルターはオフになっています。）

13.4 SIP 通話内の UDT を無効にする

ActiveControl は、エンドポイントへの参加者リストの送信、通話中の他の参加者の切断、導入間の参加者リストなど、特定の機能に UDT トランスポートプロトコルを使用します。 UDT はデフォルトで有効になっています。 診断の目的で UDT を無効にすることができます。例えば、コールコントロールが UDT を使用しない場合で、これがコールコントロールがMeeting Serverからのコールを受けない原因であると考えられる場合です。

Meeting Server の Web 管理インターフェイスを使用して、**[設定（Configuration）]**>**[API]** の順に選択します。

1. API オブジェクトのリストで、/compatibilityProfiles の後の ► をタップします。
2. 既存の互換性プロファイルの object id をクリックするか、または新しい互換性プロファイルを作成します。
3. パラメータ sipUDT = false を設定します。 **[変更（Modify）]** をクリックします。
4. API オブジェクトのリストで、/system/profiles の後の ► をタップします。
5. **[表示または編集（View or edit）]** ボタンをクリックします。
6. **[選択（Choose）]** をクリックし、パラメータ compatibilityProfile の右側を選択します。上記のステップ 3 で作成した互換性プロファイルの **オブジェクト** ID を選択します。
7. **[変更（Modify）]** をクリックします。

13.5 Cisco Unified Communications Manager で iX サポートを有効にする

iX プロトコルのサポートは、Cisco Unified Communications Manager で一部の SIP プロファイルに対してデフォルトで無効になっています。 Unified CM で iX サポートを有効にするには、まず SIP プロファイルのサポートを設定し、それから SIP プロファイルを SIP トランクに適用します。

SIP プロファイルでの iX サポートの設定

1. **[デバイス（Device）] > [デバイス設定（Device Settings）] > [SIP プロファイル（SIP Profile）]** を選択します。 SIP プロファイルの検索と一覧表示ウィンドウが表示されます。
2. 次のいずれかを実行します。
   a. 新しい SIP プロファイルを追加するには、 **新規追加**をクリックします。
   b. 既存の SIP プロファイルを変更するには、検索条件を入力して **[検索（Find）]** をクリックします。 更新する SIP プロファイルの名前をクリックします。

   [SIP プロファイル設定] ウィンドウが表示されます。
3. **[iX アプリケーションメディアを許可（Allow iX Application Media）]** のチェックボックスを選択します。
4. 追加の設定変更を加えます。
5. [**保存**] をクリックします。

SIP トランクへの SIP プロファイルの適用

1. **[デバイス（Devce）] > [トランク（Trunk）]** を選択します。

   [トランクの検索と一覧表示] ウィンドウが表示されます。
2. 次のいずれかを実行します。
   a. 新しいトランクを追加するには、[**新規追加**] をクリックします。
   b. トランクを変更するには、検索条件を入力して、 **[検索]** をクリックします。 更新するトランクの名前をクリックします。

   [トランク設定] ウィンドウが表示されます。
3. [SIP プロファイル] ドロップダウンリストから、適切な SIP プロファイルを選択します。
4. [**保存**] をクリックします。
5. 既存のトランクを更新するには、**[設定の適用（Apply Config）]** をクリックして新しい設定を適用します。

13.6 Cisco VCS で iX をフィルタリングする

プロトコルをサポートしない近隣ゾーンの iX アプリケーション回線をフィルタリングするように Cisco VCS を設定するには、SIP UDP/IX フィルターモードの詳細設定オプションがオンに設定されているカスタムゾーンプロファイルでゾーンを設定する必要があります。

アドバンスト ゾーン プロファイルのオプション設定を更新するには、以下を行います。

1. 新しい近隣ゾーンを作成するか、または既存のゾーンを選択します（**[設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）]**）。
2. **[ゾーンプロファイル（Zone profile）]**の詳細設定のパラメータ項で、まだ選択されていない場合は、*[カスタム（Custom）]* を選択します。 ゾーンプロファイルの詳細設定オプションが表示されます。
3. **[SIP UDP/IX フィルタモード（SIP UDP/IX filter mode）]** ドロップダウンメニューから **[オン（On）]** を選択します。
4. [**保存**] をクリックします。

13.7 iX のトラブルシューティング

表 12: iX ヘッダーを含む通話の通話処理の概要

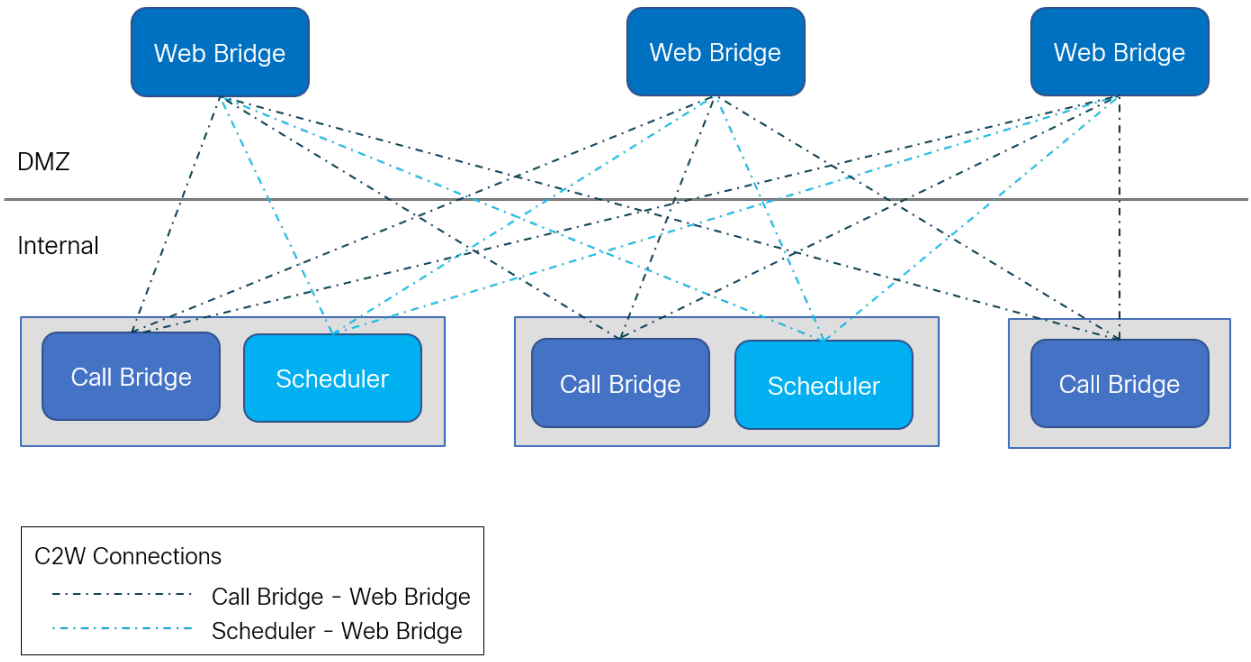
シナリオ	結果
Unified CM 8.x またはそれ以前	通話が失敗する
Unified CM 9.x 9.1(2) 以前	通話は正常に処理されるが、ActiveControl はなし
Unified CM 9.1(2)	通話は正常に処理され、ActiveControl もある
エンドポイント - iX および SDP 実装のサポートなし	エンドポイントが再起動する可能性があるか、通話が失敗する可能性がある

14 スケジューラ - 導入

スケジューラは、Meeting Server MMP を使用して、新しいコンポーネントとして導入されます。 スケジューラが有効になると、スケジューラはループバック インターフェイスを介して Call Bridge に API 要求を行います。 そのため、スケジューラは、Call Bridge もホストしている Meeting Server に導入する必要があります。 スケジューラがリモート Call Bridge を使用するように設定することはできません。

設定済みのWeb Bridgeのリストは、Call Bridge API を使用してスケジューラによって取得されます。 持続的な C2W 接続は、Call Bridge が各Web Bridgeへの C2W 接続を確立する方法と同様に、各Web Bridgeへ確立されます。 これはループバック インターフェイス経由で自動的に行われるため、スケジューラと Call Bridge 間の接続を有効にするために、明示的な設定は必要ありません。 同様に、C2W 接続はすべて自動ですが、スケジューラとWeb Bridgeの間で信頼バンドル を構成する必要があります。

注意：スケジューラは、クラスタ内のすべての Web Bridges への C2W 接続を確立できる必要があります。 大規模なデータベースを含む Call Bridge の導入では、サーバーを再起動する前にスケジューラを無効にし、データベースの同期が完了した後にのみ再度有効にします。これには最大 30 分かかります。



すべての Call Bridge と一緒にスケジューラを導入する必要はありません。 Meeting Server Small と VM 導入上の Meeting Server のスケジューラは、合わせて 150,000 のミーティングをサポートし、Meeting Server 2000 のスケジューラは 200,000 のミーティングをサポートし

ます。 2 つまたは 3 つのスケジューラを追加して、レジリエンスを提供できます。 スケジュール済みミーティングのデータはMeeting Server のデータベースに保存され、クラスター化およびシングルボックスデータベース導入の両方がサポートされています。

Call Bridge は、スケジューラからの API リクエストをユーザーの「スケジューラ」としてログ記録する場合があります。 これはログのみを目的としており、実際のアカウントではありません。 ビルトインアカウントはなく、スケジューラのユーザーは明示的にアカウントを作成する必要はありません。 スケジューラは、ループバック インターフェイス経由で Call Bridge API を使用し、自動的に API コマンドを発行する信頼できるソースになります。

14.1 スケジューラを導入する

スケジューラと Call Bridge の間の接続を有効にするために、明示的な設定は必要ありません。 これはループバック インターフェイスで自動的に行われます。 同様に、C2W 接続はすべて自動ですが、sスケジューラとWeb Bridgeの間で信頼関係バンドルを設定する必要があります。

1. C2W トラストを設定します。

   C2W は、スケジューラから各Web Bridgeに確立される TLS ベースの WebSocket 接続です。 各スケジューラは、クラスタ内の各Web Bridgeに接続できる必要があります。スケジューラは、この接続に使用されるクライアント証明書とキーの設定を要求します。これを行うには、証明書を作成し、SFTP 経由で Meeting Server にアップロードするか、**pki** MMP コマンドを使用して証明書を作成します。

   スケジューラが証明書を使用するように設定します。

   scheduler c2w certs <key-file> <crt- fullchain-file>

   次に例を示します。

   scheduler c2w certs scheduler_c2w.key scheduler.cer

   スケジューラは、接続する各Web Bridgeを信頼できる必要があります。 SFTP 経由で、各Web Bridgeの証明書を含む信頼バンドルをアップロードします。

   次のコマンドを使用して、スケジューラを設定します。

   scheduler c2w trust webbridge_bundle.cer

   Web Bridgeがスケジューラを信頼できることも必要です。 そのため、次のコマンドを使用して設定されたバンドルにスケジューラ証明書を含めることが重要です。

   webbridge3 c2w trust <crt-bundle>

   スケジューラと Call Bridge の両方に必要なすべての証明書は、<crt-bundle>.

2. （オプション）スケジューラの HTTPS インターフェースを設定します。

   スケジューラには独自の HTTPS インターフェイスがあり、これを有効にすると、スケジューラ API を使用してスケジューラ ミーティングを設定することができます。 ただし、Web Bridge は管理 API を使用してスケジューラと通信することはありません。 HTTPS サーバーの有効化は必須ではありませんが、診断およびトラブルシューティングの機能が提供されるため、有効にすることをお勧めします。

   次のコマンドを使用して、HTTPS サーバー リッスン インターフェイスを設定します。

   scheduler https listen <interface> <port>

   次に例を示します。

   scheduler https listen a 8443

   コマンド **scheduler https certs <key-file> <crt-fullchain-file>** を使用して、サーバーの証明書キーペアを設定します。例：

   scheduler https certs scheduler_https.key scheduler_https.cer

3. （オプション）メールサーバーを設定します。

   スケジューラは、SMTP メールサーバーの設定を介したメール通知の送信をサポートします。 ミーティングがスケジュール、キャンセル、または変更されると、メール通知が参加者に送信されます。

   サーバーアドレスとポートの構成、メールプロトコルの有効化、認証のためのユーザー名の設定は、次のスケジューラ MMP コマンドで指定します。

   ```
   scheduler email server <hostname|address> <port>
   scheduler email server none
   scheduler email username <smtp username>
   scheduler email protocol <smtp|smtps>
   scheduler email auth <enable|disable>
   scheduler email starttls <enable|disable>
   ```

   サーバーアドレスが設定されていない場合、メールはスケジューラで設定されません。スケジューラがメール招待を送信するには、少なくとも 1 つのメールサーバーを設定する必要があります。 メールは、ミーティングのスケジュールに使用されたスケジューラからではなく、任意のスケジューラから送信できます。 メールサーバーがダウンした場合、別のスケジューラがメールを送信します。

   ミーティング サーバーが 5000 ミリ秒 (5 秒) 以内に Exchange 電子メール サーバーから応答を受信しない場合、スケジューラは要求を自動的に拒否します。

スケジューラは、次のタイプのメール設定をサポートしています。

a. SMTP
b. SMTP と認証済みログイン（Auth Login）
c. SMTP と STARTTLS
d. SMTP（認証ログインと STARTTLS 使用）
e. SMTPS （SMTP トランザクション全体のエンドツーエンド TLS 暗号化）
f. SMTPS（認証ログインあり）

メモ：Exchange Server 2016 CU22 - 15.1.2375.7 および Exchange Server 2019 CU11 - 15.2.986.5 の使用をお勧めします。

バージョン 3.4 から、ミーティングの招待状は共通のメールアドレスからすべての参加者に送信できます。 MMP コマンド **`scheduler email common-address <address@mail.domain> "<Display name>"`** で Meeting Server 上に共通のメールアドレスと表示名を設定します。 スケジューラが共通のメールアドレスから参加者にミーティング招待状を送信します。

共通メールアドレスが空の場合、スケジューラは開催者のメールアドレスから招待メールを送信します。

注記： 共通の電子メールアドレスが設定されていない場合、SMTP サーバーによる認証には MMP コマンドを使用して電子メールアドレスを設定する必要があります。 **スケジューラメールのユーザー名 `<smtp ユーザー名>`**。 MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりにメールを送信できる適切な権限が必要です。

送信者を識別するために、表示名としてメールアドレスの他に開催者名を含めることもできます。 ウェブアプリを使用してミーティングがスケジュールされると、ウェブアプリはミーティングをスケジュールしているユーザーの名前を開催者の表示名としてスケジューラに送信します。 任意の名前を表示名として設定するには、オプションのパラメータ **`organizationDisplayName`** をスケジューラ API に含めることができます。

スケジューラが SMTP 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定ポートでリッスンするように設定します。

a. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

b. メールサーバーとポートを設定します。

   `scheduler email server <hostname|address> <port>`

たとえば、

```
scheduler email server exchange.example.com 25
scheduler email server 10.27.33.55 25
```

c. スケジューラを有効にします。

```
scheduler enable
```

スケジューラが認証ログインを使用して SMTP 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコル用に指定されたポートでリッスンするように設定し、SMTP サーバーが認証ログインをサポートするようにし、認証用のユーザーアカウントを設定します。 MMP で構成されたこのアカウントには、ウェブアプリユーザーの代わりにメールを送信できる適切な権限が必要です。

a. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

スケジュールを無効化

b. メールサーバーとポートを設定します。

```
scheduler email server <hostname|address> <port>
```

たとえば、

```
scheduler email server exchange.example.com 25
scheduler email server 10.27.33.55 25
```

c. [認証ログイン（Auth Login）] オプションを有効にします。

```
scheduler email auth enable
```

d. 認証に使用するユーザー名を設定してください。

```
scheduler email username <username>
```

パスワードを入力してください。

```
scheduler email username test@test.com
```

パスワードを入力してください：

パスワードを再度入力してください：

e. スケジューラを有効にします。

```
scheduler enable
```

スケジューラが SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートでリッスンするように設定し、STARTTLS を有効にします。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正

常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

a. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

b. メールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

c. STARTTLS オプションを有効にします。

   scheduler email starttls enable

d. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

e. スケジューラコンポーネントを有効にします。

   scheduler enable

スケジューラが Auth Login を使用した SMTP および STARTTLS 経由でメール通知を送信できるようにするには、メールサーバーが SMTP プロトコルの指定されたポートでリッスンするように設定し、STARTTLS を有効にします。 さらに、SMTP サーバーを有効にしてログイン認証をサポートし、認証に使用されるユーザーアカウントを設定し、STARTTLS を有効にします。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

a. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

b. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

c. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

d. 認証に使用するユーザー名を設定してください。

   scheduler email username <username>

   パスワードを入力してください。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください：

   パスワードを再度入力してください：

e. STARTTLS オプションを有効にします。

   scheduler email starttls enable

f. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

g. スケジューラコンポーネントを有効にします。

   scheduler enable

スケジューラが SMTPS 経由でメール通知を送信できるようにするには、特定のポートでエンドツーエンド SMTP 暗号化をサポートするようにメールサーバーを設定します。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信

頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

a. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

b. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

c. メールプロトコルを SMTPS 設定します。

   scheduler email protcol smtps

d. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

e. スケジューラコンポーネントが SMTPS を使用してメール設定を完了できるようにします。

   scheduler enable

スケジューラが Auth Login を使用した SMTPS 経由でメール通知を送信できるようにするには、特定のポートでエンドツーエンド SMTP 暗号化をサポートするようにメールサーバーを設定します。 さらに、SMTPS サーバーが Auth Login をサポートするようにし、認証に使用するユーザーアカウントを設定します。

TLS 接続を確立するための、メールサーバーとスケジューラ間の TLS ハンドシェイクによる証明書の交換が含まれます。 デフォルトでは、スケジューラはすべての証明書を信頼し、メールサーバーから送られてくる任意の証明書を受け入れることで TLS 接続を正常に確立するように設定されています。 しかし、スケジューラには特定の証明書を設定

するための追加オプションがあります。 このモードでは、スケジューラは設定された証明書のみを受け入れ、信頼します。

a. スケジューラが動作中の場合は、スケジューラコンポーネントを無効にします。

   スケジュールを無効化

b. 指定されたメールサーバーとポートを設定します。

   scheduler email server <hostname|address> <port>

   たとえば、

   ```
   scheduler email server exchange.example.com 25
   scheduler email server 10.27.33.55 25
   ```

c. [認証ログイン（Auth Login）] オプションを有効にします。

   scheduler email auth enable

d. 認証に使用されるユーザーのユーザー名を設定します。

   scheduler email username <username>

   パスワードを入力します。

   ```
   scheduler email username test@test.com
   ```

   パスワードを入力してください:

   もう一度パスワードを入力してください:

e. メールプロトコルを SMTPS 設定します。

   scheduler email protcol smtps

f. 特定の証明書を使用するには、まず証明書をインポートし、SFTP 経由で Meeting Server VM にアップロードします。 それから、次のコマンドを実行して証明書を設定します。

   scheduler email trust <cert or bundle name>

   設定された証明書は有効な証明書である必要があります。 たとえば、共通名または SAN 名がメールサーバーの FQDN と一致している必要があり、証明書が期限切れになっていない必要があります。 同様に、証明書が Certificate Authority によって発行された場合、またはチェーンに中間証明書がある場合、ルート CA 証明書、またはルート証明書、中間証明書 1、中間証明書 2 以降をこの順序で含む証明書バンドルを設定します。

g. スケジューラコンポーネントが Auth Login で SMTPS を使用してメール設定を完了できるようにします。

   scheduler enable

14.1.1 スケジューラの詳細ログ

スケジューラは、ウェブブリッジ接続、メール通知、およびスケジューラ timedLogging MMP コマンドを使用した API の詳細なログを有効にするオプションをサポートしています。

timedLogging が有効ではない場合、Meeting Server は次の出力を表示します。

```
cms-vm> scheduler timedLogging
{
"webBridge": "0",
"api": "0",
"email": "0"
}
```

timedLogging オプションのいずれかを有効にするには、次のコマンドを使用します。

スケジューラ timedLogging (webBridge|api|email) <時間>

例えば、

```
cms-vm> スケジューラ timedLogging webBridge 600
成功
```

time 変数は秒単位で表され、設定された継続時間の timedLogging を有効にします。

```
cms-vm> scheduler timedLogging
{
"webBridge": "594",
"api": "0",
"email": "0"
}
```

設定した継続時間が経過するか、特定の調査またはトラブルシューティングの手順が完了したら、SFTP を使用してログファイルをダウンロードします。

サーバーアドレスとポートの構成、メールプロトコルの有効化、認証のためのユーザー名の設定は、次のスケジューラ MMP コマンドで指定します。

```
scheduler email server <hostname|address> <port>
scheduler email server none
scheduler email username <smtp username>
scheduler email protocol <smtp|smtps>
```

```
scheduler email auth <enable|disable>
scheduler email starttls <enable|disable>
```

サーバーアドレスが設定されていない場合、メールはスケジューラで設定されません。スケジューラがメール招待を送信するには、少なくとも 1 つのメールサーバーを設定する必要があります。 メールは、ミーティングのスケジュールに使用されたスケジューラからではなく、任意のスケジューラから送信できます。 メールサーバーがダウンした場合、別のスケジューラがメールを送信します。

ミーティング サーバーが 5000 ミリ秒 (5 秒) 以内に Exchange 電子メール サーバーから応答を受信しない場合、スケジューラは要求を自動的に拒否します。

4. メールサーバーを設定したら、次のコマンドを使ってスケジューラを有効にします。

   ```
   scheduler enable
   ```

5. 次のコマンドを使用して、サービスの設定とステータスを確認します。

   ```
   scheduler status
   ```

   正常な構成のサンプル出力:

```
cms> scheduler status
ステータス：有効
実行中
起動時にデータベースが応答し、
HTTPS が設定されている
C2W が設定されました
メールサーバーが設定されました

スケジューラ アプリケーションのステータス:
{
     "status"："UP",
     "components"：{
```

```
        "c2w": {
            "status": "UP",
            "details": {
                "GUID": "dc06c10f-a220-42d8-b4eb-f9be3d07faf4",
                "webbridges": "webbridge1.mycompany.com:4443:CONNECTED,
webbridge1.mycompany.com:8443:CONNECTED,
webbridge3.mycompany.com:8443:CONNECTED"
            }
        },
        "db": {
            "status": "UP"
        },
        "mail": {
            "status": "UP",
            "details": {
                "location": "smtp.mycompany.com:25"
            }
        },
        "ping": {
            "status": "UP"
        }
    }
}
```

15 セキュリティに関するその他の考慮事項と QoS

この章では、X.509 証明書と公開鍵による認証に加えて、Meeting Serverで利用できるその他のセキュリティ機能について説明します。

注： この章に記載されているコマンドは、 MMP コマンドリファレンス ガイドにも記載されています。

15.1 共通アクセスカード（CAC）統合

Common Access カード (CAC) は、コンピュータ施設にアクセスするための認証トークンとして使用されます。 CAC には抽出できない秘密鍵が含まれていますが、カード上の暗号ハードウェアで使用してカード所有者の身元を証明することができます。

Meeting Server は、CAC を使用した SSH およびWeb 管理インタフェースへの管理ログインをサポートしています。 表 13 の MMP コマンドを使用して、あなたのデプロイメントのために CAC を設定します。

表 13: CAC ログインを設定する MMP コマンド

MMP コマンド	説明
`cac enable|disable [strict]`	すべてのパスワードベースのログインを削除するオプションのストリクトモードで CAC モードを有効/無効にします
`cac issuer <ca cert-bundle>`	CAC 証明書を確認するための信頼できる証明書バンドルを識別します
`cac ocsp certs <keyfile> <certificatefile>`	使用されている場合、OCSP サーバーとの TLS 通信のための証明書と秘密鍵を識別します
`cac ocsp responder <URL>`	OCSP サーバーの URL を識別します
`cac ocsp 有効化|無効化`	CAC OCSP 検証を有効/無効にします

15.2 Online Certificate Status Protocol (OCSP)

OCSP は、証明書の有効性と失効状況を確認するためのメカニズムです。 MMP は OCSP を使用して、ログインに使用された CAC が有効かどうか、特に失効していないかどうかを確認できます。

15.3 FIPS

FIPS 140-2 レベル 1 認定のソフトウェア暗号モジュールを有効にすると、暗号操作はこのモジュールを使用して実行され、暗号操作は FIPS 承認済み暗号アルゴリズムに制限されます。

表 14: FIPS を設定する MMP コマンド

MMP コマンド	説明
`fips enable|disable`	ネットワークトラフィックのすべての暗号化操作で FIPS-140-2 モード暗号化を有効または無効にします。 FIPS モードの有効化または無効化後は、再起動が必要です
`fips`	FIPS モードが有効かどうかを表示します
`FIPS テスト`	組み込みの FIPS テストを実行します

15.4 TLS 証明書の検証

リモート証明書が信頼できるものであることを確認するために、SIP および LDAP の相互認証を有効にすることができます。 有効にすると、Call Bridge は常にどちらの側で接続を開始したかに関係なく、リモート証明書を要求し、提示された証明書を、アップロードされ、サーバーに定義されている信頼ストアと比較します。

表 15: TLS を設定する MMP コマンド

MMP コマンド	説明
`tls <sip|ldap> trust <crt bundle>`	信頼できる認証局を定義します
`tls <sip|ldap> verify enable|disable|ocsp`	証明書の検証を有効/無効にするか、検証に OCSP を使用するかを指定します
`tls <sip|ldap>`	現在の構成を表示します

15.5 ユーザーコントロール

MMP 管理ユーザーは次のことができます。

- 別の管理ユーザーのパスワードをリセットする
- ユーザーのパスワードで繰り返し使用できる最大文字数を設定する - その他にも多くのユーザー パスワード ルールが追加されています
- IP アドレスで MMP アクセスを制限する
- 設定可能なアイドル期間の後に MMP アカウントを無効にする

15.6 ファイアウォールルール

MMP は、メディア インターフェイスと管理インターフェイスの両方に対して、簡単なファイアウォール ルールの作成をサポートします。 これは完全なスタンドアロン ファイアウォール ソリューションの代替を意図したものではないため、ここでは詳細を説明しません。

ファイアウォールルールは各インターフェイスに個別に指定する必要があります。 インターフェイスにファイアウォールルールを設定したら、必ずそのインターフェイスのファイアウォールを有効にしてください。 詳細と例については、 MMP コマンド リファレンス を参照してください。

警告：ファイアウォールの設定には、シリアルコンソールを使用することを推奨します。SSH を使用する場合、ルールのエラーにより SSH ポートがアクセス不能になるからです。 SSH を使用する必要がある場合は、ファイアウォールを有効にする前に、許可 **`ssh ルール`** が管理者インターフェースに対して作成されていることを確認してください。

15.7 DSCP

Meeting Server上の異なるトラフィックタイプに対して DSCP タギングを有効にできます(MMP コマンドリファレンス)を参照してください。

1. MMP にログインします。
2. 必要に応じて、**`dscp (4|6) <traffic type> (<DSCP value>|none)`** を使用して DSCP を設定します。 例: **`dscp 4 oa&m 0x22`** これは IPv4 の運用、管理、およびメンテナンスを設定します。
3. 代わりに、 **`dscp Assured (true|false)`** コマンドを使用して、「音声」および「マルチメディア」トラフィックタイプに対して保証または非保証 DSCP 値の使用を強制します。 例: **`dscp assured true`**

注： DSCP タグは、Meeting Serverから送信されるすべてのパケットにのみ適用されます。PC クライアント DSCP タギングの場合、グループポリシーを使用して希望の DSCP 値を定義する必要があります。これは Windows が制御し、通常のユーザーアカウントには DSCP を設定する権限がないためです。

15.8 SSH 指紋を確認する

初めて SSH または SFTP 経由で Meeting Server に接続する管理者は、ログインする前に Meeting Server にインストールされたキーの指紋を取得することで、Meeting Server がプロンプトするキーを確認することができます。

表 16: キーを取得する MMP コマンド

MMP コマンド	説明
ssh server_key リスト	出力には、Meeting Server ホスト内のすべての既存キーのサイズ、タイプ、フィンガープリントのキーのリストおよび以下のキーが表示されます。 • ssh_host_dsa_key.pub • ssh_host_ecdsa_key.pub • ssh_host_ed25519_key.pub • ssh_host_key.pub • ssh_host_rsa_key.pub

16 問題をトラブルシューティングするのに役立つ Cisco サポートの診断ツール

Syslog レコードを使用することに加えて (セクション 3.1.4) 展開の問題の診断を支援するために、Meeting Serverで以下の機能を利用できます。

- SIP トレース
- ログバンドル
- 特定のコールレッグのキーフレームを生成する
- 登録済みメディア モジュールの定期的なレポート

16.1 SIP トレース

Web管理者インタフェースの **[ログ] > [詳細トレース]** ページを使用して、追加のSIPトレースを有効にすることができます。 これらのログは、SIP エンドポイントの通話セットアップの失敗問題を調査する場合に役立ち、それ以外の場合は無効にする必要があります。 冗長ログが必要以上に長く有効になることを防ぐために、1 分、10 分、30 分、または 24 時間の選択後に自動的にオフになります。 トラブルシューティングの詳細については、Cisco ウェブサイトの「Meeting Serverのサポートに関する FAQ」を参照してください。

失敗したログイン試行の診断には以下が含まれます。

- ログインに関連するイベントログメッセージに含まれる遠端の IP アドレス。
- ユーザー名を除く失敗したログインおよびログイン セッションのタイムアウトに対して生成された監査メッセージ。 成功したログインに対しても生成されます。

16.2 ログバンドル

Meeting Serverは、Meeting Serverの様々なコンポーネントの構成と状態を含むログバンドルを生成することができます。 このログバンドルには、syslog および live.JSON ファイルが含まれます。 問題に関して Cisco サポートに連絡する際は、これらのファイルをご提供いただくと、早く分析ができます。

Meeting Serverのログバンドルは以下の方法で生成されます:

- Meeting Server 管理者は、MMP 管理者ユーザー資格情報を使用して、SFTP クライアントを MMP IP アドレスに接続すると、ログ バンドル ダウンロード プロセスを開始できます。 システムは、logbundle.tar.gz というファイル名でログバンドルを生成しダウンロードします。

- 代わりに、管理者は、**generate_logbundle** コマンドを使用してダウンロードプロセスを開始する前に、ログバンドルを生成できます。 generatedlogbundle.tar.gz という名前のログバンドルが生成されます。

コマンド/例	説明/メモ
generate_logbundle	それぞれの Meeting Server で generatedlogbundle.tar.gz というファイル名のログバンドルを生成します。 **注：** このコマンドが実行されるたびに、前に生成されたログバンドルが最新のログバンドルで置換されます。

以下の手順でログバンドルをダウンロードします。

1. SFTP クライアントを MMP の IP アドレスに接続します。
2. MMP 管理者ユーザーの資格情報を使用してログインします。
3. ログバンドルをダウンロードする場所でこれらのコマンドを実行します。
   a. **sftp get logbundle.tar.gz**
   b. **sftp get generatedlogbundle.tar.gz**
4. logbundle.tar.gz/generatedlogbundle.tar.gz ファイルをローカルフォルダにコピーします。
5. ファイル名を変更し、ファイル名の logbundle の箇所を変更し、ファイルを生成するサーバーを特定します。 これは複数サーバーの展開では重要です。
6. 名前を変更したファイルを分析のために Cisco サポート担当者に送信します。

log bundle.tar.gz の初期ファイルサイズは、1 KB です、SFTP 経由で転送した場合、サイズは、ファイル数とそのサイズに応じて大きくなります。

メモ：お使いのコンピューターと Meeting Server 間でネットワーク接続が遅いなどの原因で logbundle がダウンロードできない場合は、ログファイルと live.json ファイルをダウンロードして、Cisco サポートにご送信ください。

16.3 特定のコールレッグのキーフレームを生成する機能

generateKeyframe オブジェクトが /callLegs/<callleg id> に追加されました。 これはデバッグ機能です。Cisco サポートは、問題を診断する際に、この機能の使用をお願いする場合があります。

Web 管理インタフェースを使用して、[**設定** > API] を選択し、

1. API オブジェクトのリストで、/callLegs の後ろの ▶ をタップします。
2. コールレッグの **オブジェクト** ID をクリックします。
3. ページ上部にある **関連オブジェクトのリスト** で、 /callLegs/<callleg id>/generateKeyframe をクリックします。
4. [**作成（Create）**] をクリックします。

これにより、問題のコール レッグの発信ビデオ ストリームに新しいキーフレームが生成されます。

16.4 syslog に登録されたメディアモジュールを報告する

syslog では、15 分ごとにメッセージを出力することができるため、すべてのメディアモジュールが稼働しているかどうかを監視できます。

Meeting Server 2000 の例:

```
2020-08-06T13:21:39.316Z user.info cms2kapp host:server INFO : media module
status 1111111 (1111111/1111111) 7/7 (full media capacity)
```

17 追加のライセンス情報

Meeting Management はライセンスの目的で、Meeting Server 3.0 以降では必須です。 スマートライセンシングを使用している場合は、Cisco Smart Software Manager に接続する必要があります。 ローカル ライセンス ファイル (従来のライセンス モード) のサポートが廃止され、ライセンス予約が導入されました。

注：セキュリティ上の理由から Meeting Management を使用できない、またはインターネットに接続できない環境では、担当の Cisco アカウントチームに連絡して代替オプションを入手してください。

17.1 ライセンス

この章では以下の情報を確認できます:

- Meeting Server でのスマートライセンスの仕組み
- 期限切れライセンス機能の強制アクション
- ライセンス情報を取得する方法（Smart Licensing）
- Smart Licensing の登録プロセス
- ユーザーに Personal Multiparty ライセンスを指定する
- Cisco マルチパーティライセンスの割り当て方法
- Cisco Multiparty ライセンスの使用状況を確認する
- SMP Plus ライセンス使用量の計算
- Meeting Serverからライセンス使用状況のスナップショットを取得する
- ライセンスレポート

17.1.1 Meeting Server でのスマート ライセンスの仕組み - 概要

Meeting Server でライセンスが機能するには、Meeting Management が必須です。 Meeting Server と Meeting Management 間の信頼と相互作用により、Smart を使用したライセンス、または既存の顧客の場合はインストールされたライセンス ファイルの使用がサポートされます。この信頼されたリンクにより、Meeting Management は Meeting Server のライセンスを付与できるようになります。

注：Cisco Meeting Management を使ったスマートライセンシングの管理の詳細は、『Meeting Management 管理者ガイド』を参照してください。

スマートライセンシングを実装するためのワークフローの概要は以下の通りです。

1. Meeting Management をスマート ライセンシング バーチャル アカウントに登録します。
2. Meeting Server が最初に起動したとき、ライセンス状況の値は定義されていません。

   メモ：トライアルモードは、90 日間のフル機能の期間、ライセンスなしで使用できます。

3. Meeting Server は、スマートライセンシングを管理するためにセットアップされた Meeting Management インスタンスに最初に接続するときに、Meeting Server にライセンスが以前に適用されているかどうかを確認します。 有効になっていない場合、ライセンスの有効期限が 90 日後に設定されます。

   ライセンスの有効期限は Meeting Management に表示され、また付録 B.5 に示すように clusterLicensing API にも返されます。

   メモ：機能ライセンスの有効期限は、最大で 90 日後になります。

4. Meeting Management は、Meeting Server が準拠していることを確認するために必要なライセンスがあるかどうかを確認するために、クラスターの Meeting Server ライセンスの使用状況を照合し、スマートアカウントに日単位でレポートを行います。 スマートアカウントは Meeting Management に応答し、Meeting Server が準拠しているかどうかを示します。 Meeting Management では、有効期限を次のように適切に設定します。

   a. Meeting Management が、ライセンスが存在し、特定の機能の利用権限を下回っていることを確認した場合、有効期限は 90 日後に延長されます。

      注：Meeting Server が Meeting Management に接続せず、90 日間の使用状況データを送信しない場合、Meeting Server のライセンスは更新されず、期限切れになります。 ライセンスの有効期限が切れた場合の強制措置については、セクション 17.1.2 を参照してください。

   ライセンスの使用数が資格を超える場合、またはライセンスが見つからない場合、施行は次のように行われます。

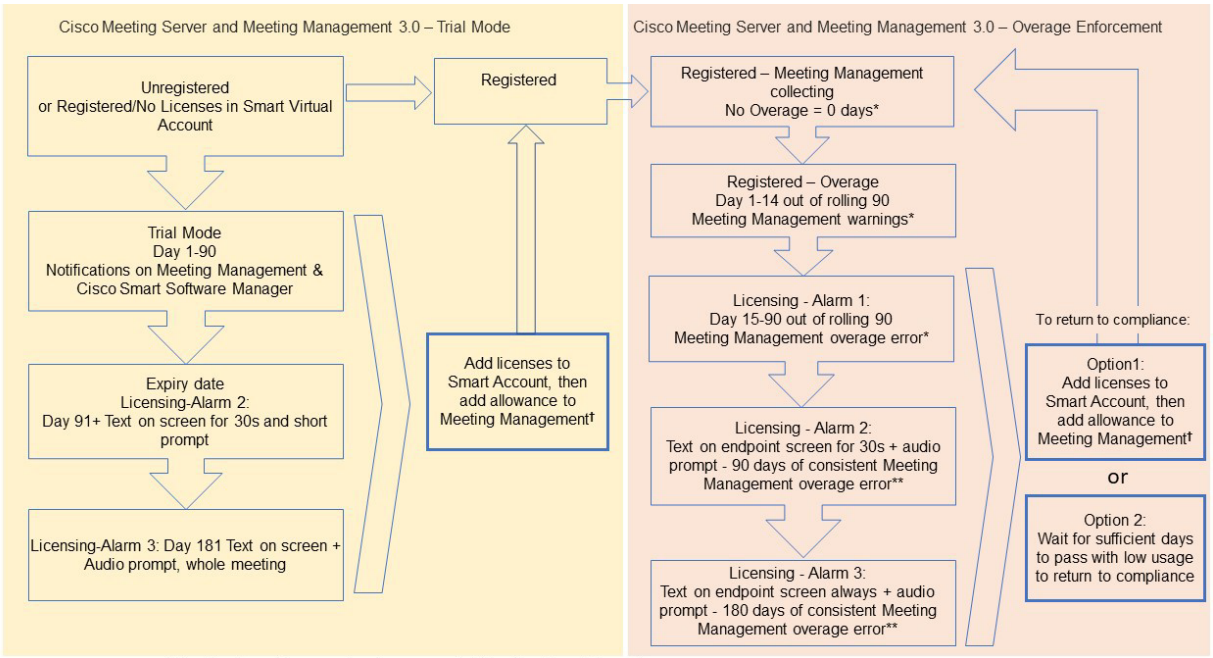
   b. Meeting Management が過去 90 日間のうち 15 日間未満が非準拠であると特定した場合、これを許可し、Meeting Server の有効期限日をその時点から 90 日後の将来にリセットします。 管理者は「ライセンスが不十分」を通知する視覚的な警告を受け取ります。

c. Meeting Management で過去 90 日間のうち 15 日間以上で準拠していないことが確認された場合、第 1 レベルの強制（アラーム 1）が発生します。つまり、Meeting Management インターフェイスに準拠していないことが通知されます。

d. 超過が続く場合、Meeting Management は 90 日のクロックをリセットしません。新しいライセンスを追加するための xx 日間のカウントダウンが表示されます。そうしないと、図 21 に示すように、ミーティングに参加するすべての参加者に対して、アラームレベル 2 と 3 が有効になります。

図 21 の左側にトライアルモードで最初に起動してから、右側に超過数の施行に至るまでの強制フローを示します。

図 21：Cisco Meeting Server および Cisco Meeting Management スマートライセンシングの強制フロー



17.1.2 期限切れライセンス機能の強制アクション

以前は、Meeting Server は再起動時にのみライセンスファイルを評価していました。 3.0 から、機能がライセンスされているかどうかの現在のステータスが動的に変更される可能性があります。これは、機能ライセンスの有効期限が切れている場合や（以前は再起動するまで確認できなかった場合）、または API が変更された場合などです。 Meeting Management で強制措置がスマートライセンシングで計算されます。

注：スマート ライセンシング ポータルを使用して、「不十分なライセンス」のメール通知を有効にできます。

ライセンス機能の有効期限が切れると、 表 17 に記載のアクションが行われます。

表 17：期限切れライセンスの強制アクション

機能	アクション
callBridge	有効期限が切れた場合：すべての参加者/すべてのミーティングのミーティングに参加するときに、視覚的なテキストメッセージが画面に 30 秒間表示され、音声プロンプトが再生されます。 （アラームレベル 2）
callBridgeNoEncryption	90 日以上前に期限切れになった場合、またはライセンスが存在しない場合：以前と同じですが、ビジュアルメッセージは永久的なものです。 音声プロンプトにより、「展開はライセンスに準拠していません。管理者に連絡してください」が再生されます。 （アラームレベル 3） ただし、暗号化されたコールは、ライセンスなし状態では処理されません。 メモ：上記のアクションを防ぐには、callBridge または callBridgeNoEncryption のみが必要です。
PMP/SMP	
customizations	有効期限が切れているか、存在しない場合、ミーティング中にカスタマイズ機能はアクティブになりません。
recording	有効期限が切れているか、出席していない場合、新しい録画を開始することはできません（サードパーティのレコーダーかどうかは関係ありません）。 このライセンスは録画とストリーミングを表すため、同じ制限がストリーミングにも適用されます。

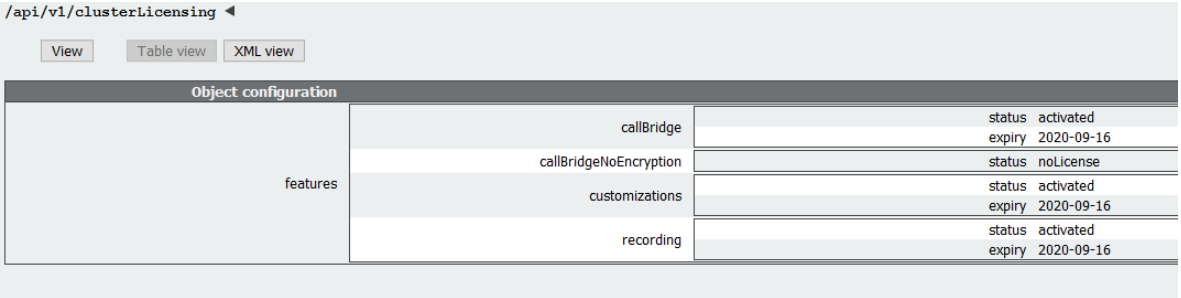
アラーム 2 および 3 をオフにするには、スマートアカウントにライセンスを追加するだけです。

17.1.3 ライセンス情報を取得する方法（Smart Licensing）

Meeting Server のウェブ管理インターフェイスを使用してクラスタのライセンス情報を取得するには、以下を行います。

1. Meeting Server のウェブ管理インタフェースにログインして **[設定（Configuration）] > [API]** を選択します。
2. API オブジェクトのリストで、**/api/v1/clusterLicensing** 後にタップします。
3. クラスターの現在のライセンス状況は、次の例のように表示されます。

図 22：clusterLicensing API - ライセンスステータス



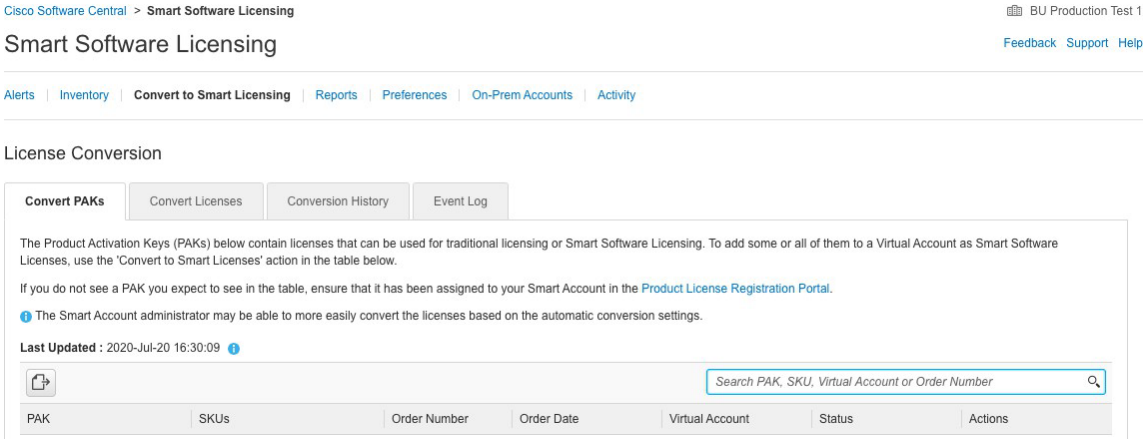
17.1.4 Smart Licensing の登録プロセス

Smart Licensing の有効化

1. Cisco Smart Software Manager（CSSM）ポータル にログインし、[Meeting Server ライセンスを持つバーチャルアカウント（Virtual Account with Meeting Server Licenses）] を選択します。
2. 登録トークンを生成します。
3. トークンをクリップボードにコピーします。
4. ライセンスレポートに使用する Meeting Management のインスタンスを開きます。
5. **設定** ページの **[ライセンス]** タブに移動します。
6. [**変更**] をクリックします。
7. **[スマートライセンシング（Smart Licensing）]** を選択し、**[保存（Save）]** を選択します。
8. **[登録（Register）]** をクリックします。
9. 登録トークンを貼り付けます（これにより、Meeting Management をスマート ライセンシング ポータルに接続できます）。
10. **[登録（Register）]** をクリックします。
11. 登録が済んだら、バーチャルアカウントにあるライセンス数を確認してください。
12. Meeting Management で、**[ライセンス（Licenses）]** ページに移動します。
13. バーチャルアカウントで所有するライセンスのライセンス情報を入力します。

    バーチャルアカウントに表示されていないライセンスがある場合は、[**ライセンスの変換**] タブを使用し、PAK で検索し、**[ライセンスの変換] を選択します。** 追加 図 23 に従います。（ライセンスが見つからない場合は、 licensing@cisco.com にメールを送信してケースを開きます。）

図 23：スマートライセンシングのライセンス変換



17.1.5 マルチパーティライセンス

17.1.5.1 パーソナル Multiparty Plus ライセンス

Personal Multiparty Plus（PMP Plus）は、頻繁にビデオミーティングを主催する特定のユーザーに割り当てられた指名主催者ライセンスを提供します。 これは、Cisco UWL Meeting を通じて購入できます。または Flex Meetings（PMP Plusを含む）。 Personal Multiparty Plus は、ビデオ会議のためのオールインワンのライセンス製品です。 これにより、ユーザーはあらゆるサイズの電話会議を開催できます（導入された Cisco Meeting Server ハードウェアの制限内）。 誰でもどのエンドポイントからでもミーティングに参加でき、このライセンスは最大 HD 1080p60 品質のビデオ、音声、コンテンツ共有に対応します。

メモ：Unified Communications Manager を使用すると、アドホック電話会議の開始者を識別することができます。PMP Plus ライセンスが割り当てられている場合は、それが電話会議で使用されます。

メモ：個人の PMP Plus ライセンスを使用するアクティブな通話数を確認するには、パラメータ **`callsActive`** を API オブジェクトで使用します。 **`/system/multipartyLicensing/activePersonalLicenses`**. 通常、2 つのコールをアクティブにできるため、1 つは開始、もう 1 つは終了とします。 通話が Call Bridge のクラスターで発生する場合、パラメータ **`weightedCallsActive`** を API オブジェクトで使用します。 **`/system/multipartyLicensing/activePersonalLicenses`** for each Call Bridge in the cluster. クラスター全体の **`weightedCallsActive`** の合計は、個人の PMP Plus ライセンスを使用するクラスター上の個別の通話数と一致します。 PMP Plus ライセンスの上限を超えた場合は、SMP Plus ライセンスが割り当てられます。 項 17.1.1 を参照してください。

17.1.5.2 Shared Multiparty Plus ライセンス

Shared Multiparty Plus（SMP Plus）は、まれにビデオミーティングを主催する複数のユーザーによって共有される同時ライセンスを提供します。 Shared Multiparty Plus は、PMP Plus 主催者ライセンスを持たないすべての従業員がビデオ会議にアクセスできるようにします。 これは、多くの従業員が共有する会議室システムを展開している顧客に最適です。 PMP Plus を持つユーザーまたは SMP Plus ライセンスを使用するユーザーは、同じように優れたエクスペリエンスを得ることができます。スペースでミーティングを主催したり、アドホック ミーティングを開始したり、今後のミーティングをスケジュールしたりできます。 各共有主催者ライセンスは、任意のサイズ (展開されたハードウェアの制限内) の 1 つの同時ビデオ ミーティングをサポートします。

メモ: 必要な SMP Plus ライセンスの数を確認するには、パラメータ **`callsWithoutPersonalLicense`** を使用します。API **`/system /multipartyLicensing`**. 通話が Call Bridge のクラスター上にある場合は、パラメータ **`weightedCallsWithoutPersonalLicense`** を API object **`/system/multipartyLicensing`** で使用します。> クラスター内の各 Call Bridge に対して。クラスター全体の **`weightedCallsWithoutPersonalLicense`** の合計は、SMP Plus ライセンスを必要とするクラスター上の個別の通話の数と一致します。

17.1.6 ユーザーに Personal Multiparty ライセンスを指定する

このプロセスでは、ユーザーが単一の LDAP ソースからインポートされる必要があります。詳細については、『ミーティング管理管理者ガイド』の「プロビジョニング - ユーザーのインポート」の章を参照してください。

17.1.6.1 特定のユーザーがライセンスを持っているかどうかを確認方法:

1. API オブジェクトのリストで、[**/users 回の後**] のをタップします。
    a. 特定のユーザーの**オブジェクト** ID を選択します
    b. このユーザーに関連付けられた userProfile の**オブジェクト** ID を特定する
2. API オブジェクトのリストで、[**/users 回の後**] のをタップします。
    a. 特定のユーザーの**オブジェクト** ID を選択します
    b. パラメータ hasLicenceの設定を確認してください。 **true** に設定すると、ステップ 1 で特定されたユーザーが Cisco Multiparty ユーザーライセンスに関連付けられます。 **false** に設定すると、ユーザーに Cisco Multiparty ユーザーライセンスは関連付けられません。

    注：userProfile が削除されると、ldapSource およびインポートされたユーザーの userProfile の設定が解除されます。

17.1.7 Cisco Multiparty ライセンスの割り当て方法

スペースでミーティングが開始されると、Cisco ライセンスがスペースに割り当てられます。Cisco Meeting Server により割り当てられるライセンスは、以下のルールにより決定されます。

- スペース所有者が定義されており、Cisco PMP Plus ライセンスが割り当てられている、Meeting Server からインポートされた LDAP ユーザーに対応する場合、その所有者のライセンスは、その人物が電話会議でアクティブであるかどうかに関係なく割り当てられます。
- ミーティングが Cisco Unified Communications Manager からのアドホックエスカレーションで作成された場合、Cisco Unified Communications Manager はミーティングをエスカレートするユーザーの GUID を提供します。 その GUID が、Meeting Server からインポートされた Cisco PMP Plus ライセンスを持つ LDAP ユーザーに対応する場合、そのユーザーのライセンスが割り当てられます。そうでない場合は、
- ミーティングが Cisco TMS バージョン 15.6 以降からスケジュールされた場合、TMS はミーティングの所有者に情報を提供します。 そのユーザーが、Cisco PMP Plus ライセンスが割り当てられたユーザー ID/メールアドレスで、Meeting Server からインポートされた LDAP ユーザーに対応する場合、そのユーザーのライセンスがミーティングに割り当てられます。そうでない場合は、次に、
- Cisco SMP Plus ライセンスが割り当てられている。

17.1.8 Cisco マルチパーティライセンスの使用状況の判定

マルチパーティライセンスの使用状況を表示するには、Meeting Management を使用することをお勧めします。 ただし、API は使用できます。

表 18 は、Multiparty ライセンスの消費量を決定するために使用できる API オブジェクトとパラメータの一覧です。

表 18: マルチパーティライセンスの使用に関連するオブジェクトとパラメータ

API オブジェクト	パラメータ	使用目的...
/system/license	個人用、共有	Cisco Meeting Server のコンポーネントが Multiparty ライセンスを持ち、アクティベートされているかどうかを判別します。 値は次のとおりです: noLicense、アクティブ化、猶予、期限切れ。 有効期限日と上限数も表示されます。

API オブジェクト	パラメータ	使用目的...
/system/multipartyLicensing	PersonalLicenseLimit、sharedLicenseLimit、personalLicenses、callsWithoutPersonalLicense、weightedCallsWithoutPersonalLicense	利用可能で使用中のライセンスの数を示します
/system/multipartyLicensing/activePersonalLicenses	CallsActive、weightedCallsActive	Personal Multiparty Plus ユーザーライセンスを使用しているアクティブなコール数を示します。
/userProfiles	hasLicense	ユーザーが Cisco Multiparty ユーザーライセンスに関連付けられているかどうかを示します。

Cisco Multiparty ライセンスをサポートするための、これらの追加のオブジェクトとフィールドの詳細については、『Cisco Meeting Server API リファレンスガイド』を参照してください。

17.1.9 SMP Plus ライセンス使用量の計算

次の特定のシナリオにおいて、ミーティングで使用される SMP Plus ライセンスは、フルライセンスの 1/6 に減らされます。

- 出席者がビデオを使用していない音声のみの電話会議
- Lync ゲートウェイ通話（Meeting Server が記録またはストリーミングを行っている場合を除く）
- ウェブアプリと 1 つの SIP エンドポイント、または 2 つのウェブアプリが関係する Meeting Server が録画またはストリーミング中の場合を除き、録画中またはストリーミング中は完全な電話会議と見なされ、SMP Plus ライセンスが消費されます。

フル SMP Plus ライセンスは、所有者のプロパティが未定義のスペースからインスタンス化された音声/ビデオ会議、PMP Plus ライセンスを持たないインポートされた LDAP ユーザーが所有、または PMP Plus ライセンスがすでに使用されているインポートされた LDAP ユーザーが所有する音声ビデオ会議です。これは参加者数に関係ありません。

メモ: ポイントツーポイント通話は次のように定義されます:

- Meeting Server 上に永久スペースがない
- レコーダーまたはストリーマを含めて 2 人未満の参加者
- Lync AVMCU で主催されている参加者がいない、

これには、Lync ゲートウェイ通話だけでなく、他のタイプの通話（ポイントツーポイント ウェブ アプリからウェブアプリ、ウェブアプリから SIP、および SIP から SIP）が含まれます。

17.1.10 Meeting Server からライセンス使用状況のスナップショットを取得する

管理者は Meeting Server からライセンスの使用状況を取得できます。 これらにはウェブ管理インターフェイスからはアクセスできません。代わりに、POSTMAN:

導入内の Meeting Server の主催者 ID を取得するには、**`/system/MPLicenseUsage/knownHosts`** で GET を使用します。 リストの最初のページ以外の主催者 ID を取得するために必要な場合は、オフセットと制限を指定します。

`/system/MPLicenseUsage` で GET を使用して、指定された主催者 ID を持つ Meeting Server の Call Bridge からライセンスの使用状況を取得します。 スナップショットの開始時刻と終了時刻を指定します。使用中のパーソナルライセンス数、使用中の音声のみ、ポイントツーポイント、または音声でもポイントツーポイントでもないライセンスの数、記録されている通話の数、ストリーミングされた通話の数に関する情報を提供します。

メモ: メモ:個人ライセンスと共有ライセンスは、通話がスパンする Call Bridge の数で正規化されます。

17.1.11 ライセンスレポート

Meeting Management には、過去 90 日間のライセンスレポート/使用情報があります。Cisco Smart Software Manager にはライセンスレポート情報も含まれます。 録画ライセンスの使用は同時に録画する会議の数を示し、同様にストリーミング ライセンスの使用は同時にストリーミングする会議の数を示します。

17.1.12 従来のライセンスファイル方式

このセクションは、従来のライセンス方法を使用している場合にのみ適用されます。 バージョン 3.4 から、従来のライセンスのサポートは廃止されました。 既存のローカルライセンスは、ライセンスの有効期限が切れるまで引き続きサポートされます。

17.1.12.1 従来のライセンス方法を使用して Cisco ユーザーライセンスを取得する

この項は、あなたがすでに Meeting Server に必要なライセンスを Cisco パートナーから購入しており、PAK コードを受け取っていることを前提としています。

これらの手順に従い、Cisco ライセンス登録ポータルサイトを使用して、Meeting Server の MAC アドレスに PAK コードを登録します。

1. サーバーの MMP にログインして Meeting Server の MAC アドレスを取得し、MMP コマンド **`iface a`** を入力します。

注： これは VM の MAC アドレスであり、VM がインストールされているサーバープラットフォームの MAC アドレスではありません。

2. Cisco ライセンス登録ポータルサイト を開き、Meeting Server の PAK コードと MAC アドレスを登録します。
3. PAK に R-CMS-K9 アクティベーション ライセンスがない場合、機能ライセンスに加えてこの PAK が必要になります。
4. ライセンスポータルからライセンスファイルの zip 圧縮されたコピーがメールで送信されます。 Zip ファイルを解凍し、結果として得られた xxxxx.lic ファイルの名前を **`cms.lic`**。
5. SFTP クライアントを使用して Meeting Server にログインし、 **`cms.lic`** ファイルを Meeting Server ファイルシステムにコピーする必要があります。
6. MMP コマンドを使用して Call Bridge を再起動する **`callbridge restart`**
7. Call Bridge を再起動したら、MMP コマンドを入力してライセンスのステータスを確認します。**`license`**

   アクティブ化された機能と有効期限が表示されます。

18 主催された電話会議の情報を取得する

Meeting Server で主催されている電話会議の情報を取得するための 2 つのメカニズムにより、API を頻繁にポーリングする必要性を減らします。通話詳細レコードとイベントです。

注：Cisco Meeting Managementを CDR（通話詳細記録）レシーバーおよびイベントクライアントとして設定し、API リクエスト、CDR、および Meeting Server イベント経由でアクティブなミーティングに関する情報を取得することができます。 詳細については、『管理者向け Meeting Management ユーザー ガイド』を参照してください。

18.1 コール詳細レコード（CDR）

Meeting Server は、サーバーに到達する新しい SIP 接続、または通話のアクティブ化または非アクティブ化など、主要な通話関連イベントに対して、内部で通話詳細レコード（CDR）を生成します。

サーバーはこれらのレコードを収集および分析するためにリモートシステムに送信するように設定することができます。 Meeting Server 上にレコードを長期間保存するための規定はなく、Meeting Server 自体の CDR を参照する方法もありません。

CDR システムは Meeting Server API と組み合わせて使用できます。コール ID とコールレッグ ID の値は 2 つのシステム間で一貫しているため、イベントと診断の相互参照が可能になります。

Meeting Serverは最大 4 つの CDR 受信者をサポートするため、Cisco Meeting Management など、異なる管理ツールまたは同じ管理ツールの複数のインスタンスを展開することができます。 詳細は、『Cisco Meeting Server 通話詳細記録ガイド』を参照してください。

18.2 イベント

Meeting Server は、Meeting Server 上で発生する変更をリアルタイムで「イベントクライアント」に通知することができます。 Meeting Server は、イベントのためのサーバーとして機能し、イベントクライアントは、例えば、ウェブベースの管理アプリケーションである場合があります。 Cisco Meeting Management はイベントクライアントとして機能します。

注： 独自のイベントクライアントを構築することができます。これは API クライアントの構築と似ています。 イベント クライアントは、HTTP および WebSocket ライブラリをサポートする必要があり、どちらも Python などの一般的なスクリプト言語で使用できます。 Meeting Serverのイベントポートはウェブ管理で設定したものと同じです。通常はインタフェース A の TCP ポート 443 です。

Meeting Server の API リソースを継続的にポーリングする代わりに、イベントクライアントはイベントリソースをサブスクライブして更新を受け取ることができます。 例えば、イベントクライアントとMeeting Server間の WebSocket 接続を確立した後、イベントクライアントはイベントリソース **`callRoster`** をサブスクライブすることができ、新しい参加者が参加したり、既存の参加者がレイアウトを変更したりしたときに知ることができます。

詳細については、『Cisco Meeting Server イベントガイド』を参照してください。

付録 A 展開に必要な DNS レコード

注： 外部 DNS サーバーで設定されていない、または上書きする必要がある値を返すように DNS リゾルバを設定することができます。外部 DNS サーバーに照会する代わりに返されるカスタム リソース レコード (RR) を設定することができます。 (クライアントは RR を利用できません。) 詳細は「MMP コマンドリファレンス」を参照してください。

注： 以下にレコードを定義する前に、Meeting Serverに A または SRV レコードが存在しないことを確認してください。

表 19: 展開に必要な DNS レコード

タイプ	例と説明
A / AAAA	**join.example.com** 解決先: Web Bridgeの IP アドレス。 説明： Meeting Serverがこのレコードを直接使用することはありません。しかし、エンドユーザーにWeb BridgeのIPアドレスに解決する FQDN をブラウザに入力するよう提供するのが一般的な方法です。この記録の形式に制限や要件はありません。
A / AAAA	**ukcore1.example.com** 解決先: Call Bridge の IP アドレス。 説明： Lync FE サーバが Call Bridge に接続するために使用します。
A / AAAA	**ukcoreadmin.example.com** **ukedgeadmin.example.com** 解決先: MMP インタフェースの IP アドレス 説明： このレコードは管理目的でのみ使用されます。システム管理者が各 MMP インターフェイスに対して覚えやすい FQDN を好む場合です。

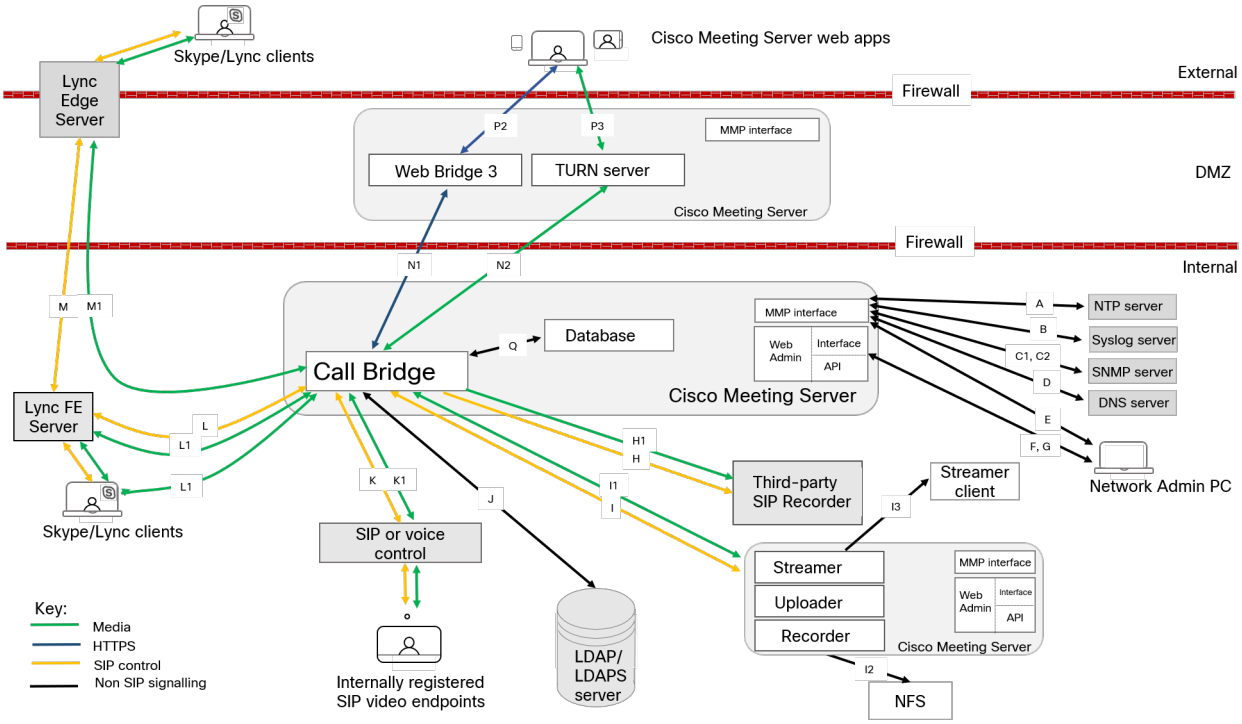
タイプ	例と説明
SRV(*)	**_sipinternaltls._tcp.<yourLyncdomain>** 解決先: Lync FE サーバまたは FE プールの A レコード。 説明： FE プールがある場合、プール内の個々の FE サーバーをポイントする複数の FE レコードを持つことができます。 Meeting Serverで Lync ミーティングを Lync ミーティング ID で解決する場合にも、このレコードが必要です。
A / AAAA	**fe.<yourLyncdomain>** 解決先: Lync FE サーバーの IP アドレス。 説明： 個々の FE サーバごとに 1 つのレコードが必要です。
SRV(*)	**_sipfederationtls._tcp.<yourSIPdomain>** 解決先: Call Bridge の FQDN。 説明： このレコードは Lync フェデレーションに必要です。
A	**callbridge.example.com** 解決先: Call Bridge の IP アドレス。 説明： Lync フェデレーションで必須。Call Bridge はパブリック IP アドレスを持つ必要があり、NAT はこのシナリオではサポートされません。

(*) SRV レコードは IP アドレスを直接解決しません。 SRV 要件を満たすために、関連する A または AAAA 名レコードを作成する必要があります。

付録 B 導入に必要なポート

以下の図は、分割サーバー導入におけるMeeting Server への接続とファイアウォールの場所を示します。 図の下の表を使用して、開くポートを特定します。

図 24：DMZ で TURN サーバーと Web Bridge 3 コンポーネントを使用する分割サーバー導入で開く必要があるポート



B.1 Meeting Server を設定する

Meeting Server の構成に使用するポートを表 20 に示します。

表 20: Meeting Server管理用のポート

code	接続先	開く接続先ポート	メソッド	トラフィック タイプ	Meeting Server に対するトラフィックの方向	追加情報
E	MMP	22	SSH	TCP	着信 (Incoming)	MMP への安全なログイン
F	API または Web 管理者	80	HTTP	TCP	着信 (Incoming)	MMP を通じて有効化/無効化されたポート

G	API または Web 管理者	443	HTTPS	TCP	着信（Incoming）	MMP を通じて構成可能なポート

B.2 サービスへの接続

さまざまなサービスをウェブアプリに接続するために使用されるポートを特定するために表 21 を使用します。

表 21: サービスに接続するために開くポート

code	コンポーネント	接続先	開く接続先ポート	トラフィック タイプ	コンポーネントに対するトラフィックの方向	追加情報
A	MMP	NTP サーバー	123	TCP または UDP	発信	
B	MMP	Syslog サーバー	514	TCP	発信	デフォルトのポート、MMP で別のポートを設定可能
C1	MMP	SNMP サーバー	161	UDP	着信（Incoming）	
C2	MMP	SNMP トラップ	162	TCP または UDP	発信	
D	MMP/Call Bridge/Web Bridge	DNS サーバー	53	TCP または UDP	発信	
	Call Bridge	CDR 受信デバイス		TCP	発信	Web 管理インターフェイスで CDR 受信者の URI を設定するか、/system/cdrReceivers/ のAPIオブジェクトを使用してAPI

B.3 Meeting Serverのコンポーネントを使用する

表 22 を使用して、Meeting Server のコンポーネントに接続するために使用するポートと、ファイアウォールを通して開く必要があるポートを特定します。

表 22: Meeting Serverコンポーネントを使用するために開くポート

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
H	Call Bridge	サードパーティ SIP レコーダー	5060	TCP（SIP）	発信	
			5060	UDP（SIP）		
			5061	TLS（SIP）		
H1	Call Bridge	サードパーティ SIP レコーダー		メディア	発信	サードパーティ SIP レコーダーにより決定されるポート
			32768-65535	UDP（STUN、RTP、BFCP）	着信（Incoming）	
I	Call Bridge	レコーダー/ストリーマ	5060	TCP（SIP）	発信	MMP を通じて構成可能なポート。 ローカルレコーダーの場合は、ループバック インターフェイスを使用します。例えば、lo:8443
			5061	TLS（SIP）		
			5060	TCP（SIP）	着信（Incoming）	
			5061	TLS（SIP）		
I1	Call Bridge	レコーダー/ストリーマ	32768-65535	メディア	発信	
			32768-65535	UDP（STUN、RTP、BFCP）	着信（Incoming）	
I2	レコーダ	ネットワークファイルサーバー NFS				MMP コマンドレコーダー nfs <host-name/IP<directory> を使用して、NFS 上のどこに録画を保存するかを指定します。
I3	ストリーマー	ストリーマ クライアント	1935	RTMP	発信	
J	Call Bridge	LDAP/LDAPS Active Directory	389/636（メモ 1）	TCP/TCP（SIP TLS）	発信	ウェブ管理インターフェイスを通じて設定可能なポート

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
K	Call Bridge	内部の登録済み SIP エンドポイントまたは音声コール制御	5060	UDP（SIP）/ TCP（SIP）	着信および発信	
			5061	TCP（SIP TLS）		
K1	Call Bridge	内部の登録済み SIP エンドポイントまたは音声コール制御	32768-65535	UDP（STUN、RTP、BFCP）	着信（Incoming）	
L	Call Bridge	Lync FE サーバー/ AVMCU	5061	TCP（SIP TLS）	着信および発信	
L1	Call Bridge	Lync クライアント、Lync FE サーバー/ AVMCU	1024-65535（メモ 2）	UDP（STUN、RTP）	発信	
			32768-65535	UDP（STUN、RTP）	着信（Incoming）	
			1024-65535（メモ 2）	TCP（RDP）	発信	
			32768-65535	TCP（RDP）	着信（Incoming）	
M	Call Bridge	Lync Edge サーバー	3478	UDP	発信	
			443	TCP	発信	
M1	Call Bridge	Lync Edge サーバー	32768-65535	UDP（STUN、RTP）	着信（Incoming）	
N1	Call Bridge	Web Bridge 3	9999	TCP（C2W）	双方向データフロー	注： C2W リスニング ポートは管理者によって定義されます
N2	Call Bridge	TURN サーバー	50000-62000（メモ 4）	UDP（RTP、STUN）	発信	ファイアウォールはリターン UDP トラフィックを許可する必要があります
P2	Web Bridge 3	Cisco Meeting Server web app	443	TCP (HTTPS)	着信および発信	HTTP 用のオプションポート 80 > HTTPS リダイレクト

code	コンポーネント	接続先	開く接続先ポート	トラフィックタイプ	コンポーネントに対するトラフィックの方向	追加情報
P3	TURN サーバー	Cisco Meeting Server web app	3478 (メモ 3) (メモ 4)	UDP（RTP、STUN）	着信（Incoming）	ファイアウォールはリターン UDP トラフィックを許可する必要があります
Q	Call Bridge	データベース				Meeting Server内部で、ファイアウォールのポートを開ける必要はありません

注：

メモ 1: この機能ではポート 636 (セキュア) および 389 (非セキュア) が一般的に使用されますが、ポートはウェブ管理インターフェイスから設定することができます。 同じことが 3268 および 3269 (非セキュアおよびセキュア) グローバル カタログ LDAP 要求にも適用されます。
メモ 2: 正確な範囲は Lync サーバーの構成により異なります。
メモ 3: 管理者はオプションで、TURN に対して 3478 TCP または別の TCP ポートを有効にすることができます。
注 4：TURN とメディアの範囲は、ウェブアプリが TURN リレーを割り当て、このガイドに記載されているように、Call Bridge が TURN リレーを作成しないことを想定しています。

B.4 ループバック上の開放ポート

表 23 に記載されているポートは、ループバック インターフェイスで開いています。

表 23: ループバックのポート

Port	使用法	注記
53	DNS	
123	NTP	
1234	HTTP	Cisco Meeting Server 2000 には適用されません
2829, 2830	サーバーからメディアへの内部接続	
3521	configd	
5432	postgres	
5060	SIP	常に開いている
5061	暗号化された SIP	証明書が Call Bridge に適用されている場合のみ
5070	BFCP	IPv6 のみ
8080	HTTP	常に開いている

Port	使用法	注記
8081	HTTP	Webadmin が有効な場合
3478	STUN	

付録 C Cisco Meeting Server プラットフォーム別のコールキャパシティ

表 24 以下では、後のソフトウェアバージョンにアップグレードすることで Meeting Server の最大コールキャパシティの詳細を示しています。 Call Bridge グループ内の負荷分散コールと比較して、単一またはクラスターの Meeting Server には異なる容量があることに注意してください。

表 24: クラスターと Call Bridge グループのミーティング サーバーの通話キャパシティ

Cisco Meeting Server プラットフォーム		Cisco Meeting Server Small M7（ノードあたり）	Cisco Meeting Server 2000 M6（ノードあたり）	Cisco Meeting Server Medium M8（ノードあたり）
個別の会議サーバーまたはクラスター内のミーティングサーバー（注 1、2、3、および 4） と Call Bridge グループの Meeting Server	1080p30 720p30 SD 音声通話	120 240 480 3000	648 1296 1875 3200	225 450 850 3000
	会議あたりサーバあたり HD 参加者数			
	web app のコールキャパシティ（内線通話と CMS Web Edge での外部通話）：			
	フル HD HD SD 音声通話	120 240 480 3000	648 1296 1875 1875	225 450 850 3000
Call Bridge グループのMeeting Server	サポートされているコール タイプ			
	読み込み制限	240,000	1,296,000	450,000

注意事項:

- クラスタあたり最大 24 個の Call Bridge ノード。8 個以上の Call Bridge ノードのクラスタ設計はシスコによる承認が必要です。詳細についてはシスコ サポートにお問い合わせください。

- Call Bridge グループが設定されていないクラスタ化された Cisco Meeting Server 2000 は、最大通話数の整数倍（たとえば、700 HD 通話の整数倍）をサポートします。
- クラスター内の Meeting Servers プラットフォームに応じて、クラスターあたり会議あたり最大 2600 人の参加者。
- 表 24 では、ビデオコールについては最大 2.5 Mbps-720p5 コンテンツ、音声コールについては G.711 のコールレートを想定しています。 他のコーデックおよび高いコンテンツ解像度/フレームレートを使用すると、容量が減ります。 ミーティングが複数の Call Bridge にまたがる場合、分散リンクが自動的に作成され、サーバーの呼び出しカウントとキャパシティに対してカウントされます。 読み込み制限値は H.264 のみに対するものです。
- クラスタでサポートされている通話セットアップレートは、SIP 通話で 1 秒あたり最大 40 通話、Cisco Meeting Server web app 通話で 1 秒あたり最大 20 通話です。
- クラスターあたり最大16,800 HD 同時通話（24 ノード x 700 HD 通話）は、SIP またはウェブアプリの通話に適用されます。
- 表 24 では、ビデオコールについては最大 2.5 Mbps-720p5 コンテンツ、音声コールについては G.711 のコールレートを想定しています。 他のコーデックおよび高いコンテンツ解像度/フレームレートを使用すると、容量が減ります。 ミーティングが複数の Call Bridge にまたがる場合、分散リンクが自動的に作成され、サーバーの呼び出しカウントとキャパシティに対してカウントされます。 読み込み制限値は H.264 のみに対するものです。
- Meeting Server 1000 M7 (Meeting Server Small) バリアントは、最大 94 個の vCPU と 128 GB の RAM をサポートします。

C.1 Cisco Meeting Server web app のコールキャパシティ

この項では、外線および混合通話に Web Bridge 3 とウェブアプリを使用した導入のコールキャパシティについて詳しく説明します。 （内線コールキャパシティについては、表 24 を参照してください。）

C.1.1 Cisco Meeting Server web app のコールキャパシティ - 外部コール

Expressway（大規模 OVA または CE1200）は、中規模のウェブアプリのスケール要件を持つ導入（つまり、800 コール以下）に推奨されるソリューションです。 Expressway（中規模 OVA）は、小規模なウェブアプリスケール要件を持つ導入（つまり、200 コール以下）に推奨されるソリューションです。 ただし、より大きなウェブアプリのスケールが必要な導入では、

バージョン 3.1 から、SIP 容量にスケールアップする必須のソリューションとして、Cisco Meeting Server ウェブエッジを推奨します（表 24を参照）。

外部発信では、クライアントが Cisco Expressway をリバースプロキシと TURN サーバーとして使用して、Web Bridgeと Call Bridge に到達します。

Expressway を使用してウェブアプリの通話をプロキシする場合、Expressway は、 表 25 に示すように、最大通話数制限をかけます。

注：Web Bridge 3 および Web App の導入は、Expressway バージョン X15.4 で検証済みです。Web Bridge 3 は、それ以前の Expressway バージョンをサポートしていません。

表 25：Cisco Meeting Server web app のコールキャパシティ - 外部コール

設定	コール タイプ	CE1200 プラットフォーム	大規模 OVA Expressway	中規模 OVA Expressway
Cisco Expressway あたり (X14.3 以降)	フル HD	150	150	50
	その他	200	200	50

Expressway 容量は、Expressway ペアをクラスタ化することで増やすことができます。Expressway ペアクラスタリングは最大 6 ノードまで可能で（4 はスケーリングに、2 は冗長性に使用されます）、合計コールキャパシティはシングルペアキャパシティの 4 倍になります。

メモ: Expressway クラスターの通話セットアップ レートは、Cisco Meeting Server web app の通話で 1 秒あたり 6 通話を超えてはなりません。

C.1.2 Cisco Meeting Server web app の容量 - 混合 (内部 + 外部) 通話

スタンドアロン導入とクラスター導入の両方で、組み合わせた内部と外部の通話使用をサポートできます。 内部と外部の参加者が混在する場合、ウェブアプリの合計容量は内線通話については付録 C に従いますが、外部から接続できる合計内の参加者数は表 25 の制限を受けます。

例えば、単一の大規模 OVA Expressway ペアを持つ単一のスタンドアロン Meeting Server 2000 は、1000 の音声のみのウェブアプリ コールの混在をサポートしますが、外部の参加者の数は、合計 1000 のうちの最大 200 に制限されます。

付録 D 暗号化されていない SIP メディア用のアクティベーションキー

Cisco Meeting Server Small、Cisco Meeting Server 2000、および VM ソフトウェアイメージについては、SIP メディア暗号化が有効になっているアクティベーションキー、または SIP メディア暗号化が無効になっている（暗号化されていない SIP メディア）アクティベーションキーのいずれかを選択して購入できます。 ソフトウェア PID R-CMS-K9 および R-CMS-2K-K9 の下で、暗号化または非暗号化オプションのいずれかを選択します。 メディアには、音声、ビデオ、コンテンツビデオ、および ActiveControl データが含まれます。

注： SIP メディア暗号化を無効にしてアクティベーション キーをアップロードしない限り、現在の Call Bridge アクティベーションは影響を受けません。

D.1 非暗号化 SIP メディア モード

「SIP メディア暗号化が無効」のアクティベーションキーが Meeting Server にアップロードされると、以下のことが起こります。

- Meeting Server と SIP デバイス間で送信されるメディアは暗号化されていません
- クラスタ化された Call Bridge 間の配信リンクを介して送信されるメディアは暗号化されていません
- コールシグナリングは暗号化されたままです
- プラットフォームを問わず、Meeting Server とウェブアプリ間の通話のメディアは暗号化されたままです
- 次の API オブジェクトで、 **sipMediaEncryption** パラメータが **許可しない** 以外に設定されている場合、エラーメッセージが返されます。

  / calls/ <call id>/ participants

  /calls/<call id>/callLegs

  /callLegs/<call leg id>

  /callLegProfiles および /callLegProfiles/<call leg profile id>

  /callLegs/<call leg id>/callLegProfileTrace

- エラーメッセージが表示されます、 **SIP メディア暗号化** フィールドが **設定**>Web **管理インタフェースの通話設定** ウェブページで、 **無効**以外に設定されている。

注： SIP メディア暗号化が無効になっている場合でも、必要に応じて sipControlEncryption パラメータを設定することで、発信通話で暗号化することができます。 **/アウトバウンドダイヤルプランルール。**

D.2 Call Bridge メディア モードの決定

Call Bridge が暗号化または非暗号化 SIP メディア使用のどちらを使用するかを決定するには、Web 管理インターフェイスを使用し、 **設定** を選択し、次に APIを選択します:

1. API オブジェクトのリストで、/api/v1/system/licensing 後の ► をタップします。

機能オブジェクト callBridgeNoEncryption のステータスが **アクティベート済み** に設定されている場合、非暗号化メディア用のアクティベーション キーが Call Bridge にロードされます。callBridgeNoEncryption のステータスに対する他の有効な設定は **ライセンスなし**、猶予期間、**または**期限切れです。

callBridgeNoEncryption にも、文字列形式の expiry フィールドがあります。

付録 E デュアルホーム電話会議

E.1 概要

デュアルホーム電話会議は、Lync でスケジュールされたミーティングおよび Lync のドラッグアンド ドロップ スタイルのミーティング（アドホックコールとも呼ばれる）で、Lync クライアントユーザーとウェブアプリユーザーの両方のユーザーエクスペリエンスも改善します。 Lync 参加者は、ドラッグアンドドロップを使用してウェブアプリユーザーを Lync ミーティングに追加でき、電話会議コントロールを使用してウェブアプリユーザーをミュートまたは切断できます。 Lync でスケジュールされた電話会議に参加するウェブアプリユーザーには、ウェブアプリユーザーからのビデオだけでなく、最大 5 人の Lync 参加者からのビデオが表示されます。 Lync ユーザーには、すべてのウェブアプリユーザーおよびミーティングの Lync ユーザーのビデオがギャラリー形式で表示されます。 Lync ユーザーとウェブアプリユーザーの両方が、ミーティングの参加者を組み合わせた完全なリストを受け取ります。

注： アドホックのデュアルホーム電話会議では、Lync/Skype for Business クライアントの [参加者の追加] ボタンは機能しません。 回避策として [今すぐミーティング（Meet Now）] ボタンを使用しないでください。これにより、Meeting Server と AVMCU 間のアクティブな通話が残ることになります。

Lync の参加者は、Meeting Server スペースに直接ダイヤルするか、またはドラッグアンドドロップを使用して Meeting Server スペースを Lync ミーティングに追加できます。 これらは、Lync ユーザーが参加したい Cisco Meeting Server スペースで大規模なミーティングが開催されている場合に便利です。 1 つ目のケースでは、複数の参加者で設定されたレイアウトを受信します。 Lync ミーティングに完全なスペースを追加すると、Lync ユーザーはスペース (主発言者) から 1 つのビデオ ストリームのみを受信し、完全に統合された参加者リストを受信しません。 通常どおり、Lync 参加者を追加できます。

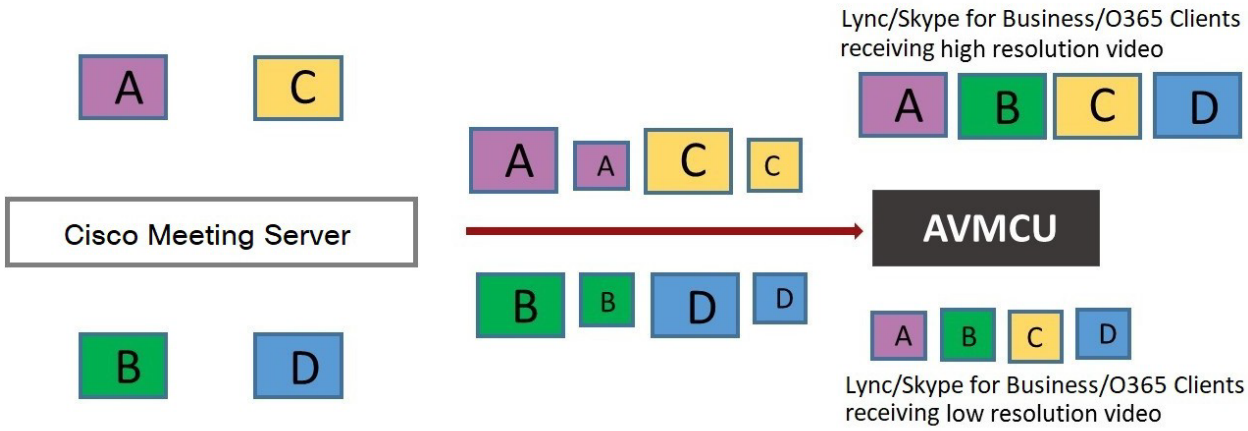
注：Expressway X8.11 を Meeting Server のエッジとして使用する場合、少なくとも一部の Microsoft トラフィックがクラスタ内の Meeting Server と Microsoft インフラストラクチャとの間で直接流れない限り（かつ Expressway を経由しない）、Meeting Server クラスタを持つデュアルホーム電話会議は現在サポートされていません。 デュアルホーミングは、スタンドアロン Meeting Server のエッジとして Expressway X8.11 でサポートされます。

E.2 デュアルホーム会議での一貫したミーティング エクスペリエンス

Meeting Server は、ビデオ参加者ごとに 2 つの H.264 ビデオストリームを AVMCU に送信します。高解像度ビデオストリームと低解像度ビデオストリームです。図 25 を参照してください。 Lync、Skype for Business、および O365 クライアントは高解像度をサポートし、高品質ビデオ ストリームをサブスクライブし、受信します。 帯域幅制限、ウィンドウ サイズ、レイアウト、CPU 性能、またはモバイル デバイスを使用しているために、より低い品質を選択するクライアントは、より低い品質のストリームをサブスクライブおよび受信し、ビデオ品質を低下させたり、他の参加者のビデオ エクスペリエンスを低下させたりしません。

注： SIP トランクの帯域幅は、2 つのビデオストリームを配信するのに十分に高く設定してください。 LAN には 8MB、WAN には 2.5MB を推奨します。

図 25: AVMCU へのデュアルメディアストリーム



注： Microsoft RTVideo を使用する端末ではこの機能から利益を得ることはありません。

E.2.1 ユーザーエクスペリエンスの要約

デュアル ホーム電話会議と RDP および複数のビデオ エンコーダーのサポートを組み合わせることで、Lync とウェブ アプリ ユーザーの両方によりリッチなミーティング エクスペリエンスを提供します。

- Lync クライアント ユーザーとウェブ アプリ ユーザーの両方に、使い慣れた画面レイアウトが表示されます。
- Lync クライアント ユーザーとウェブ アプリ ユーザーの両方は、接続している場所に関係なく、ミーティングのすべての参加者をまとめた完全なリストを受け取ります。
- Lync クライアントのユーザーには、SIP エンドポイントとウェブアプリからのビデオで非正方形のアスペクト比が表示されます。
- Lync クライアントのユーザーには、メインのビデオ領域ではなく、画面の別の領域にコンテンツが表示されます。
- Meeting Server は、Lync ミーティングの各参加者がサポートする最高品質のコーデックを使用してビデオを送信します。 これにより、参加者が複数の Lync クライアントバージョンを使用する場合に、ミーティングのすべての Lync クライアントユーザーのエクスペリエンスが最適化されます。
- Meeting Server は、高解像度ビデオストリームと低解像度ビデオストリームの 2 つの H.264 ビデオストリームをビデオ参加者ごとに AVMCU に送信します。これは、低解像度しかサポートできないクライアントがミーティングに参加した場合でも、高解像度をサポートするクライアントに対する高解像度体験を維持するためです。
- チャットは、スペースのウェブアプリユーザーとの Lync AVMCU 電話会議、およびウェブアプリユーザーと Lync クライアント間の直接通話で機能します。

注：ミーティング中に最高のユーザーエクスペリエンスを得るには、Lync 2013、Skype for Business 2015 以降を使用してください。これらのバージョンでは、複数のビデオストリームを Meeting Server に送信できます。 これにより、Meeting Server に接続しているエンドポイントまたはウェブアプリユーザーが複数の Lync 参加者を表示できます。 Lync 2010 は単一の最大発言者ストリームのみを提供します。最大発言者がすでに電話会議のMeeting Server側にいる場合、ウェブ アプリ ユーザーおよび SIP エンドポイント ユーザーは Lync 参加者を表示しません。

RDP および複数ビデオ エンコーダ サポートの詳細については、これらの FAQ を参照してください。

- RDP サポート、
- 複数のビデオ エンコーダのサポート。

E.3 デュアルホーム会議のミーティングコントロールをミュート/ミュート解除する

Meeting Server ソフトウェアのバージョン 2.4 では、以下のデュアルホーム電話会議でのミーティングコントロールのミュート/ミュート解除が改善されました。

- オンプレミスおよび Office 365 Lync/Skype for Business クライアント、
- エンドポイントユーザー、
- ウェブアプリユーザー。

注：この項では、Meeting Server の API を使用してミュートおよびミュート解除が有効になっていることを想定しています。

ミュート/ミュート解除:

- Lync クライアントは、デュアルホーム電話会議では自分自身と他の参加者を含め誰でもミュートおよびミュート解除できます。また、オーディエンスをミュートおよびミュート解除することもできます。
- すべてのエンドポイントユーザーは Lync クライアントをミュートできます。
- AVMCU の Lync 側のエンドポイントユーザーは、自分自身および他のエンドポイント（AVMCU に接続された Lync クライアント/エンドポイントまたは Meeting Server 側）をミュートおよびミュート解除できます。 バージョン 2.4 以前は、AVMCU の Meeting Server 側のエンドポイントユーザーのみが、自分自身と他のユーザーをミュートおよびミュート解除できました。
  - 非 ActiveControl エンドポイントの場合、Meeting Server はミュートおよびミュート解除するたびに DTMF キーシーケンスを送信し、エンドポイントへのメディアストリーム上にアイコンをオーバーレイして、エンドポイントがミュートまたはミュート解除されているかどうかを示します。
  - CE 9.2.1 以降のソフトウェアを実行している ActiveControl エンドポイントの場合、エンドポイントはアイコンとメッセージを処理します（Meeting Server はアイコンをオーバーレイしません）。
- ActiveControl エンドポイントがミュートされると、ローカルでの会話のプライバシーを確保するために、ローカルでミュート解除する必要があります。 たとえば、リモートの参加者が ActiveControl エンドポイントをミュートしてからミュート解除しようとすると、ActiveControl エンドポイントはローカルでミュート解除されるまで、自分自身をミュートし続けます。

- リモート参加者が ActiveControl 以外のエンドポイントのミュートを解除しようとすると、ActiveControl 以外のエンドポイントのミュートが解除されます。
- ウェブアプリユーザーと Cisco Meeting Management ユーザーは、Lync クライアントをミュートおよびミュート解除できます。 また、ミーティングのすべての参加者の正しいミュート状態も表示されます。

ミュート/ミュート解除ウェブアプリ ユーザー：

- ウェブアプリユーザーのローカルのミュートおよびミュート解除に関する情報は、デュアルホームの電話会議では Lync クライアントに渡されません。 しかし、Lync クライアントがウェブアプリのユーザーをリモートでミュートし、ウェブアプリがそれ自体をミュート解除する場合、Meeting Server は Lync クライアントにミュート解除について通知します。
- リモートの参加者がウェブ アプリ ユーザーのミュートを解除しようとすると、ウェブ アプリ ユーザーはローカルでミュートされたままになります。 注： 他の参加者は実際にはミュートされていますが、ミュートされていないように見えます。
- ウェブ アプリは独自のアイコンを使用してミュート/ミュート解除の状態を示します。Meeting Server のアイコンがウェブ アプリのビデオ ペインにオーバーレイ表示されません。

E.4 デュアルホームの Lync 機能の設定

すでにオンプレミス Lync 導入または Lync フェデレーション導入が Meeting Server 導入と連携している場合、Meeting Server で追加の設定は必要ありません。

これが新規の導入である場合、Meeting Server 上で Lync Edge 設定を設定していることを確認してください。セクション 8.5 を参照してください。

E.4.1 トラブルシューティング

ユーザーが IVR または「Lync」を解決するダイヤルプランルールを使用して Lync 電話会議に参加できない場合、最初に行うべきことは、「Lync Edge」設定がセットアップされていることを確認することです。Lync 電話会議を解決し、Edge サーバーを見つけるために同じメカニズムが使用されます。 Meeting Server は Lync FE サーバーにクエリを行い、これらの両方を見つける必要があります。

これに失敗した場合、電話会議 ID が見つからないというメッセージがイベントログに記録されます。

`lync 電話会議の解決: 電話会議 "1234" が見つかりません`

これは、電話会議が存在しないことを意味する場合もありますが、他の原因も考えられます。

SIP トラフィックのトレースが有効な場合、上記のメッセージがログに記録される直前に「SERVICE」メッセージが Lync FE サーバーに送信され、その応答に対して 200 OK が返されます。 このメッセージが正しい IP (Lync FE サーバーのものである必要があります) に送信されていることを確認してください。

このメッセージが送信されない場合（ログに表示されない場合）、Call Bridgeがどこに送信すべきかわからない可能性があります。これは、 **`_sipinternaltls._tcp.lyncdomain`** レコードのDNS SRV ルックアップを使用してLyncサーバーを見つけられないからです。 DNS トレースを有効にして再試行することでこれを確認する必要があります。 しかし、これは Lync Edge 設定が Meeting Server で設定されていない場合にも発生します。

サービスメッセージが送信されたものの、Lync サーバーが「403 未承認」と応答する場合、最も可能性の高い原因は、この Lync ドメインの発信ダイヤルプランルールのローカル連絡先ドメインが正しく設定されていないことです。 Meeting Server の FQDN に設定する必要があります。これは、Call Bridge の証明書の CN で提供される FQDN と同じである必要があります。

付録 F LDAP フィールド マッピングの詳細

このセクションでは、Meeting Server 用にセットアップする LDAP フィールドマッピングについての追加情報を提供します。

LDAP フィールド値の一部は、以下のように、sed に似た構文で置換できます。

$<LDAP フィールド名>|'/<regex>/<置換形式>/<オプション>'$

引数の説明

> **<option>** を g に指定すると、**<regex>** で **<replacement format>**、または空白にする場合は最初のみに一致
>
> の一部 **<regex>** を使用するためにタグをつけることができます。 **<replacement format>** には、それらを丸括弧でくくります。
>
> タグ付けされたマッチは、 **<replacement format>** で \x として参照でき、xは0から9までの数字です。マッチ0は全体マッチに対応し、マッチ1-9は1番目から9番目のタグ付けされた部分表現に対応します。
>
> 置換式の中の一重引用符は、バックスラッシュ文字自体と同様に、バックスラッシュでエスケープする必要があります
>
> 一重引用符、バックスラッシュ、または 0-9 の数字以外の任意の文字は、置換式のコンポーネントを区切るスラッシュの代わりに使用できます
>
> 式の中で区切り文字をリテラルとして使用する場合は、バックスラッシュでエスケープする必要があります。

一例として、以下はアドレスの形式を変換します:

firstname.lastname@test.example.com

次の形式に変換します:

firstname.lastname@example.com JIDたち

$mail|'/@test/@xmpp/'$

次の例では、ユーザーのフルネームからすべての小文字の「a」を削除することができます。

$cn|'/a//g'$

使用に理にかなった式のセットは次のとおりです。

氏名:	**cn**
JID:	**$mail|'/@test/'$**
space URI:	**$mail|'/@.*//'$.space**
space dial-in number:	**$ipPhone$**

注： LDAP サーバー資格情報は次のフィールドの読み取りに使用されます (セキュリティ上の理由から、これらの資格情報を使用して利用できるフィールドや権限を制限することもできます):

- メール
- objectGUID
- entryUUID
- nsuniqueid
- telephoneNumber
- mobile
- sn
- givenName

付録 G NAT の背後で TURN サーバーを使用する

TURN サーバーは NAT の背後に導入でき、NAT アドレスは MMP コマンド **`turn public-ip`** を使用して指定されます。 ただし、Interactive Connectivity Establishment (ICE) の仕組みにより、接続が常に機能することを保証するには、NAT の慎重な設定が必要です。

この付録では、ICE の動作原理について説明します。 以下の内容について説明しています。

- 候補を特定する方法、
- 接続性を確認する方法、
- TURN サーバーの前での NAT の影響、
- NAT が外部ウェブアプリユーザーに与える影響。

注： 両方のリレー候補が利用可能なパスにしか含まれていない場合、問題が発生する可能性があります。 これにはファイアウォールが正しく設定され、すべてのクライアントがビデオと音声を送受信できるようにする必要があります。

G.1 候補を特定する

ICE は、アドレスとポートの候補のリストを収集し、これらの候補のどのペアがメディアの交換を可能にするかを見つけることによって機能します。 複数のペアの候補がある場合、どのペアが使用されるかを決定するために、優先順位スキームが使用されます。

通常、3 つの候補が存在します。

1. ホスト候補
2. Server Reflexive Candidate
3. リレー候補

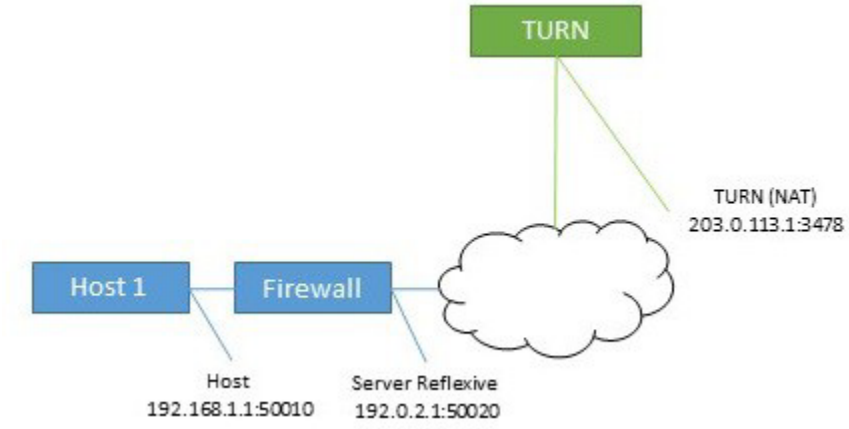
G.1.1 ホスト候補

最も単純な候補はホスト候補です。 これは、ホスト インターフェイスによって使用されるアドレスです。 これは多くの場合、ローカル ネットワーク上にあり、ルーティングできません。

G.1.2 Server Reflexive Candidate

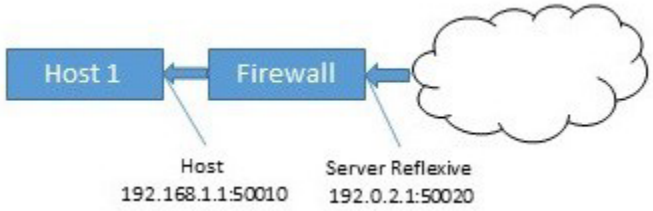
サーバー反射候補は、TURN サーバーが受信パケットが来ると見るアドレスです。 これを確認するために、ホストは TURN サーバーの定義されたポート（通常はポート 3478）にパケットを送信し、TURN サーバーはパケットの送信元に関する情報を返信します。

図 26: Server Reflexive Candidate



ホストが NAT を実行するファイアウォールの背後にいる場合、これはホスト候補とは異なります。 多くの場合、このポートとアドレスに送信されたパケットはホストに戻されます。

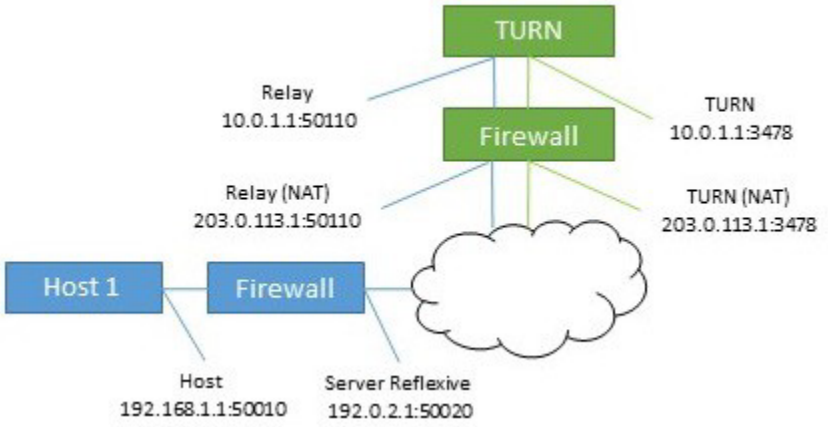
図 27: ファイアウォールの背後で NAT を実行するホストの影響



G.1.3 リレー候補

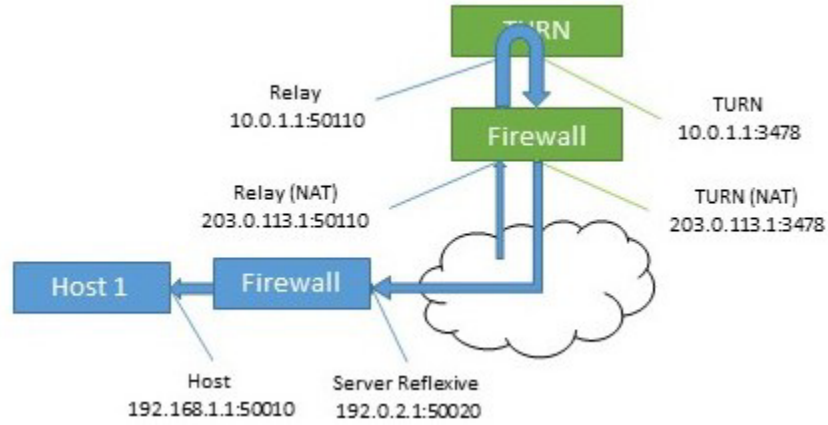
最終的な候補はリレーカンディデートです。 この候補は、ホストのリクエストに応じて TURN サーバーによって作成されます。 この候補者の中継アドレスは TURN サーバー インタフェース アドレスです。NAT が使用される場合、中継アドレスは NAT のアドレスに変更されます。

図 28: リレー候補者



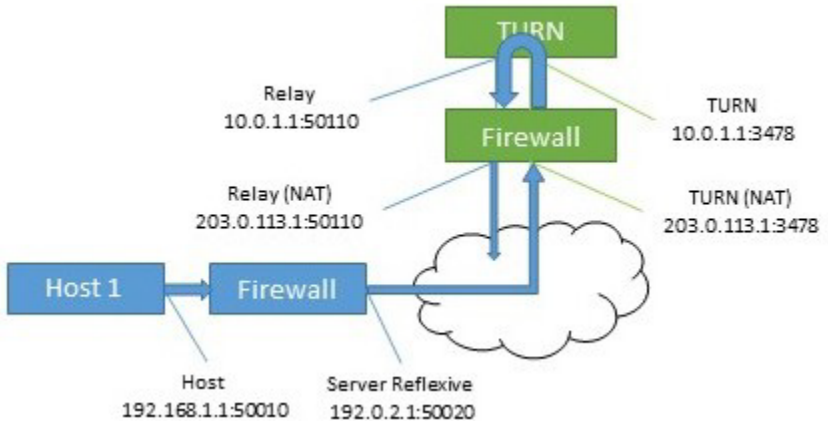
この中継アドレスに送信されたデータは、TURN サーバー経由でホストに返されます。

図 29：TURN サーバーがホストにリレーアドレスを返す



このリレー候補には 2 番目の用途があります。 また、遠端にパケットを送信するために、ホストが使用することもできます。 これは、他のパスが利用できない場合に発生します。 これらのパケットは TURN サーバーから送られてくることに注意してください。そのため、ファイアウォールによって書き換えられると、それらは NAT アドレスのみを取得します。

図 30: 遠端にパケットを送信するホスト



G.2 接続を確認しています

候補が特定されると、接続性チェックが行われます。 各ホストは、遠端のホスト、サーバー反射とリレーアドレスに直接接続しようとします。 また、リレーを使用して、同じ遠端候補への接続を試みます。

表 26：2 人のホストの候補（同じ TURN サーバーを使用）

ホスト	タイプ	Address:port
1	ホスト	192.168.1.1:50010
1	サーバーリフレクシブ	192.0.2.1:50020
1	リレー	203.0.113.1:50110
2	ホスト	172.16.1.1:50100
2	サーバーリフレクシブ	198.51.100.1:50040
2	リレー	203.0.113.1:50510

表 27: ホスト 1 によって形成された候補ペア

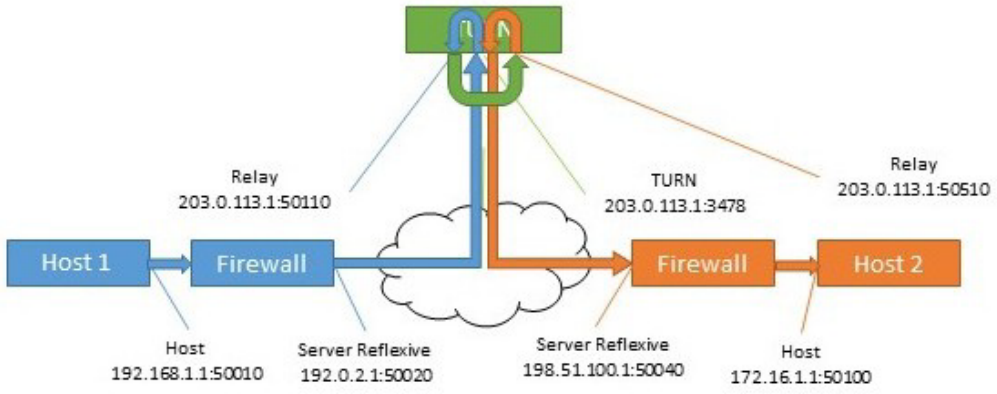
ソース（Source）	接続先タイプ	宛先アドレス
ホスト（192.168.1.1:50010）	ホスト	172.16.1.1:50100
ホスト（192.168.1.1:50010）	サーバーリフレクシブ	198.51.100.1:50040
ホスト（192.168.1.1:50010）	リレー	203.0.113.1:50510
リレー (10.0.1.1:50110)	ホスト	172.16.1.1:50100

ソース（Source）	接続先タイプ	宛先アドレス
リレー (10.0.1.1:50110)	サーバーリフレクシブ	198.51.100.1:50040
リレー (10.0.1.1:50110)	リレー	203.0.113.1:50510

通常、リレーアドレスはホストのネットワークアクセスが制限されている場合にのみ必要です。例えば、コーヒーショップやホテルのユーザーは、高番ポートにはアクセスできない場合があります。

両方のホストがアクセスを制限されている場合、両方のリレー候補を含むパスが形成されます。この場合、トラフィックは一方のリレー候補からもう一方のリレー候補に流れ込んでから、遠端に転送されます。

図 31: ホスト間のメディアパス（リレー間パスを使用、NATなし）



G.3 TURN サーバーの前の NAT

NAT が TURN サーバーの前に存在する場合、フローはより複雑になります。 リレー候補は、他のホスト候補の 1 つからトラフィックを受信することを期待しています。 パケットが TURN サーバーのインターフェイスから送信され、ファイアウォールによってリライトされない場合、未知のアドレスから送信されたように見えます。 これにより、接続性チェックの成功が妨げられ、他のパスが利用できない場合、メディアがたどるルートがなくなります。

図 32：ホスト間のメディアパス（リレー間パスを使用、NATあり）

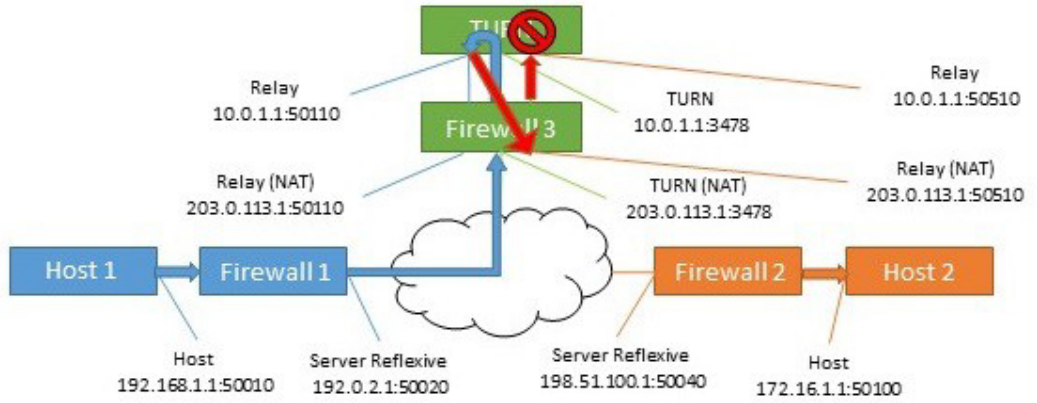


表 28：ホスト間のメディアパス（リレー間パスを使用、NATあり）

送信元アドレス (パケット単位)	Destination	宛先でのアクション
192.168.1.1:50010	203.0.113.1:3478 経由[ファイアウォール (Firewall)]	ファイアウォール 1 が送信元アドレスを書き直す
192.0.2.1:50020	203.0.113.1:3478	ファイアウォール 3 は宛先アドレスを書き換え、TURN サーバーに転送する
192.0.2.1:50020	10.0.1.1:3478	TURN サーバーは内部的にこれをこのソースのリレーアドレスにマッピングし、遠端のリレーに送信します。
10.0.1.1:50110	203.0.113.1:50510 ファイアウォール経由	Firewall 3 が宛先アドレスを書き換えます
10.0.1.1:50110	10.0.1.1:50510	TURN サーバーが予期せぬ送信元アドレスを検出し、トラフィックをドロップします。

これに対するソリューションは、ヘアピン NAT、ループバック NAT、または NAT リフレクションとして知られています。 この場合、トラフィックの送信元アドレスと宛先が書き換えられます。 この場合、ソースアドレスはファイアウォールのアドレスになります。これは、候補の 1 つと一致することを意味します。

表 29：ホスト間のメディアパス（リレー間パスを使用、ヘアピン NATあり）

送信元アドレス (パケット単位)	Destination	宛先でのアクション
192.168.1.1:50010	203.0.113.1:3478 ファイアウォール経由	ファイアウォール 1 が送信元アドレスを書き直す
192.0.2.1:50020	203.0.113.1:3478	ファイアウォール 3 は宛先アドレスを書き換え、TURN サーバーに転送します。
192.0.2.1:50020	10.0.1.1:3478	TURN サーバーは内部的にこれをこのソースのリレーアドレスにマッピングし、遠端のリレーに送信します。
10.0.1.1:50110	203.0.113.1:50510 ファイアウォール経由	Firewall 3 は送信元と送信先の両方のアドレスを書き換えます。
203.0.113.1:50110	10.0.1.1:50510	TURN サーバーは、リレーから指定されたホストへのトラフィックを内部的にマッピングします。
10.0.1.1:3478	198.51.100.1:50040 ファイアウォール経由	Firewall 3 が送信元アドレスを書き換えます。
203.0.113.1:3478	198.51.100.1:50040	Firewall 2 が送信先アドレスを書き換える。
203.0.113.1:3478	172.16.1.1:50100	最終目的地に到着します。

この機能を有効にする方法の詳細については、ファイアウォールのドキュメントを参照してください。

付録 H 待機型 Meeting Server を使用する

この付録の手順は、Cisco Meeting Server Small を含む仮想化環境に適用されます。

H.1 現在使用されている構成のバックアップ

1. OpenSSH または PuTTY などの SSH ユーティリティを使って、現在使用している Meeting Server への SSH 接続を確立します。
2. 次のコマンドを発行します:

   バックアップスナップショット<name>

   このバックアップには、IP アドレス、パスワード、および証明書が含まれ、それらは「という名前のファイルに保存されます<name>.bak. servername_date という形式の名前を使用することをお勧めします (例えば、test_server_2014_09_04)。

   バックアップの作成に成功すると、次のメッセージが返されます。

   ```
   cms> backup snapshot test_server_2014_09_04.bak ready for download
   ```
3. SFTP クライアント (例、WinSCP) を使用してバックアップファイルをダウンロードします。

注：Meeting Server は定期的に、例えば 1 日に 1 回バックアップすることをお勧めします。また、Meeting Server とスタンバイサーバーの外部にバックアップのコピーを保存することもお勧めします。

H.2 スタンバイサーバーにバックアップを転送する

スタンバイサーバーは常に起動しておくことを推奨します。

1. バックアップが作成された元のサーバーと異なる場合に備えて、すべての証明書と cms.lic ファイルをスタンバイサーバーからコピーします。 安全な場所に保管してください。
2. スタンバイサーバとの SFTP 接続を確立します。
3. 以前保存したバックアップファイルをスタンバイサーバーにアップロードします。
4. MMP バックアップ リスト コマンドを発行して、バックアップ ファイルが正常にアップロードされたことを確認します。 これにより、次のようなものが返されます。

   ```
   cms> backup list test_server_2014_09_
   ```
5. 次のコマンドを入力し、バックアップファイルからの復元を確認します:

   ```
   backup rollback <name>
   ```

これにより既存の設定が上書きされ、Meeting Server が再起動されます。 そのため、警告メッセージが表示されます。 確認では大文字と小文字が区別されます。大文字の **Y**を押す必要があります。そうしないと操作が中止されます。

注：ある導入タイプでバックアップを作成し、それをもう一方のタイプにロールバックすることはできません。例えば、仮想 Meeting Server 1000 から Meeting Server 2000へ、またはその逆です。

操作が成功すると次の値が返されます。

```
cms> backup list
Jul 23 09:42 test_2020_07_23
cms> backup rollback test_2020_07_23
WARNING!!!
This command will overwrite the existing system configuration
and result in a reboot of the system. This will cause
an interruption in service.

Are you sure you wish to proceed? (Y/n)
Successful backup extraction
Stopping Application monitor: app_monitor.
Rebooting system...
```

スマート ライセンシング ユーザーのみ対象：バックアップから復元するとき、IP アドレスと証明書を含むすべてが上書きされます。 したがって、バックアップが作成されたものとは別のサーバーに復元する場合、新しいサーバーで有効ではない証明書を手動でコピーする必要があります。

1. スタンバイ サーバーとの SFTP 接続を確立する
2. 必要に応じて:
   a. 証明書と秘密鍵を元に戻してください (復元されたバージョンがスタンバイサーバ上で有効ではない場合)。
   b. 次のコマンドを使用して、これらの証明書を対応するサービスに割り当てます。

      callbridge certs nameofkey nameofcertificate
      webbridge3 https certs nameofkey nameofcertificate

      webbridge3 c2w certs nameofkey nameofcertificate
      webadmin certs nameofkey nameofcertificate
      webbridge trust nameofcallbridgecertificate

c. 証明書を変更したサービスを再起動する

```
callbridge restart
webbridge3 restart
webadmin restart
```

新しいサーバーが完全に起動されると、完全に操作可能となり、元のサーバーのサービスを引き継ぎます。

付録 I ウェブ管理インタフェース – 設定メニューオプション

Call Bridge のWeb 管理インターフェイスにある [**設定**] タブでは、次のオプションを設定することができます。

- 全般
- Active Directory
- 通話設定
- 発信通話と着信通話
- CDR 設定
- スペース
- API

I.1 全般

を使用して[設定] >全般 ページ セットアップと設定:

- **TURN サーバー設定。** これらの設定を使用して、Call Bridge および外部クライアントによる TURN サーバーへのアクセスを許可します。 MMP コマンドを使用して、TURN サーバー自体を設定します。 MMP を設定する を参照してください。
- **Lync Edge 設定。** Call Bridge を Lync Edge と統合する場合は、これらの設定を使用します。 Lync Edge を使用するための Meeting Server の構成を参照してください。
- **IVR。** 音声自動応答 (IVR) を使用して事前設定された通話を手動でルーティングする場合、これらの設定を使用します。こうすることで、参加する通話またはスペースの ID 番号を入力するように促す事前に録音されたボイスメッセージで発信者が挨拶されます。 IVR 設定を参照してください。

I.2 Active Directory

ユーザーがウェブアプリを使って Meeting Server に接続するようにするには、LDAP サーバーが必要です。 Meeting Server が LDAP サーバーからユーザーアカウントをインポートします。

注：OpenLDAP および Oracle Internet Directory (LDAP バージョン 3) を使用できます。しかし、これは API 経由で設定する必要があります。ウェブ管理インタフェース経由では設定できません。

[設定（Configuration）] > [Active Directory] ページを使用して、Active Directory と連携するように Meeting Server をセットアップします。 LDAP 設定を参照してください。

I.3 通話設定

設定 > 通話設定ページで行うこと:

- SIP 通話 (Lync を含む) のメディア暗号化を許可する。
- SIP 通話で参加者ラベルのオーバーレイを表示するかどうかを指定します。
- 発信する音声パケットのサイズをミリ秒で指定します。10ms、20ms、または 40ms。
- TIP サポートを有効にします。 (Cisco CTS などのエンドポイントを使用する場合は、TIP サポートを有効にする必要があります。)
- プレゼンテーションビデオチャネルの操作を許可する **禁止** に設定された場合、コンテンツチャネルビデオまたは BFCP 機能は遠端にアドバタイズされません。
- プレゼンテーション ビデオ チャネル操作が SIP 通話に許可されている場合、この設定により、次のいずれかの Call Bridge の BFCP 動作が決定されます。
  - **サーバーロールのみ**–これは電話会議デバイスの通常のオプションであり、BFCP クライアントモードデバイス (SIP エンドポイントなど) での使用を想定しています。

    または
  - **サーバーとクライアントの役割**–このオプションを選択すると、リモート デバイスとの通話で、Call Bridge が BFCP クライアントまたは BFCP サーバー モードのいずれかで動作することができます。

  この設定により、リモートの電話会議主催デバイスとのプレゼンテーションビデオ共有が改善されます。
- 発信 SIP コールの Resource-プライオリティ ヘッダー フィールドの値を設定します。この設定により、Meeting Server に対し、帯域幅をプレゼンテーションに割り当てる優先順位を指定します。 これは、ネットワーク環境の帯域幅容量と、例えばHDをプッシュするイマーシブ システムがあるかどうかなど、他の要因によって異なります。
- SIP の UDP シグナリングを有効または無効にします。 次のいずれかに設定します:
  - **無効|有効** SIP over TCP を使用する場合、またはすべてのネットワークトラフィックを暗号化する必要がある場合に無効にします。

  - **有効な場合、単一アドレス** モードは 2.2 以前のバージョンでの SIP over UDP の動作に対応し、既定値になります。
  - 有効で、Call Bridge が複数のインターフェイスでリッスンするように設定されている場合は、**マルチアドレスモードを使用します。**
- Lync プレゼンスサポートを有効にします。 この設定では、この Call Bridge が Lync プレゼンスのサブスクライバに提供する接続先 URI に関する情報を提供する必要があるかどうかを決定します。
- Lync パケットペーシングモードは **デフォルト**のままにします。 Cisco サポートからの指示がない限り、設定を **遅延** に変更しないでください。

注： 各フィールドの詳細については、カーソルを合わせると各フィールドに表示されるテキストを使用するか、「ダイヤル プラン設定 - SIP エンドポイント」を参照してください。

[通話設定（Call settings）] ページでは、SIP、Cisco Meeting Server（ウェブアプリ）、Server Reflexive、Relay、VPN、Lync コンテンツの帯域幅設定を変更することもできます。設定は bps で測定されます。たとえば、2000000 は 2Mbps です。 少なくとも 64kbps を音声専用に割り当てます。720p30 通話には 2Mbps、1080p30 通話には約 3.5Mbps を推奨します。 60fps ではより多くの帯域幅が必要になります。

SIP メディア暗号化を許可したり、TIP サポートを有効にしたりする場合、帯域幅設定の一部を変更する必要がある場合があります。 3 スクリーン TIP コールの場合、 **通話設定** ページに表示される帯域幅の数値は自動的に 3 倍になるため、たとえば手動で 6Mbps に設定する必要はありません。 ただし、ほとんどの CTS 通話では通常、3 倍の 4Mbps を推奨しています。

I.4 発信通話と着信通話

[設定（Configuration）] > [発信コール（Outbound calls）] / [着信コール（Incoming calls）] ページを使用して、Meeting Server が各通話をどのように処理するかを決定します。

発信通話 ページでは、発信通話の処理方法を設定します。 **着信** ページでは、着信を拒否するか、照合および転送するかを指定します。 それらが一致して転送される場合、転送方法に関する情報が必要です。 **着信コール** ページには 2 つのテーブルがあります。1 つはマッチング/リジェクションを設定し、もう 1 つは転送動作を設定します。

これらのフィールドへの入力に関する詳細は、通話を処理する *Web 管理者インターフェイスの設定ページ* を参照してください。

I.5 CDR 設定

設定 > CDR 設定 ページをクリックして CDR 受信者の URI を入力します。

Meeting Server は、サーバーに到達する新しい SIP 接続、または通話のアクティブ化または非アクティブ化など、主要な通話関連イベントに対して、内部で通話詳細レコード（CDR）を生成します。 これらの CDR をリモートシステムに送信して収集および分析するように設定できます。 Meeting Server 上に長期のレコードを保存したり、Meeting Server 上の CDR を参照することはできません。

これらのフィールドへの入力方法の詳細は、「通話詳細記録サポート」および「通話詳細記録ガイド」を参照してください。

API を使用して、CDR 受信者の URI で Meeting Server を設定することもできます。 詳細については、 API リファレンス ガイドを参照してください。

I.6 スペース

[設定（Configuration）] > [スペース（Spaces）] ページを使用して、ダイヤルインする Meeting Server 上のスペースを作成します。 これにより、例えば、エンドポイントとウェブアプリがダイヤルインすることができます。

スペースを追加する方法:

- Name の例： `Call 001`
- URI の例： `88001`

このページでは、オプションで、セカンダリ URI ユーザーパート、コール ID、パスコード、デフォルトレイアウトも指定できます。

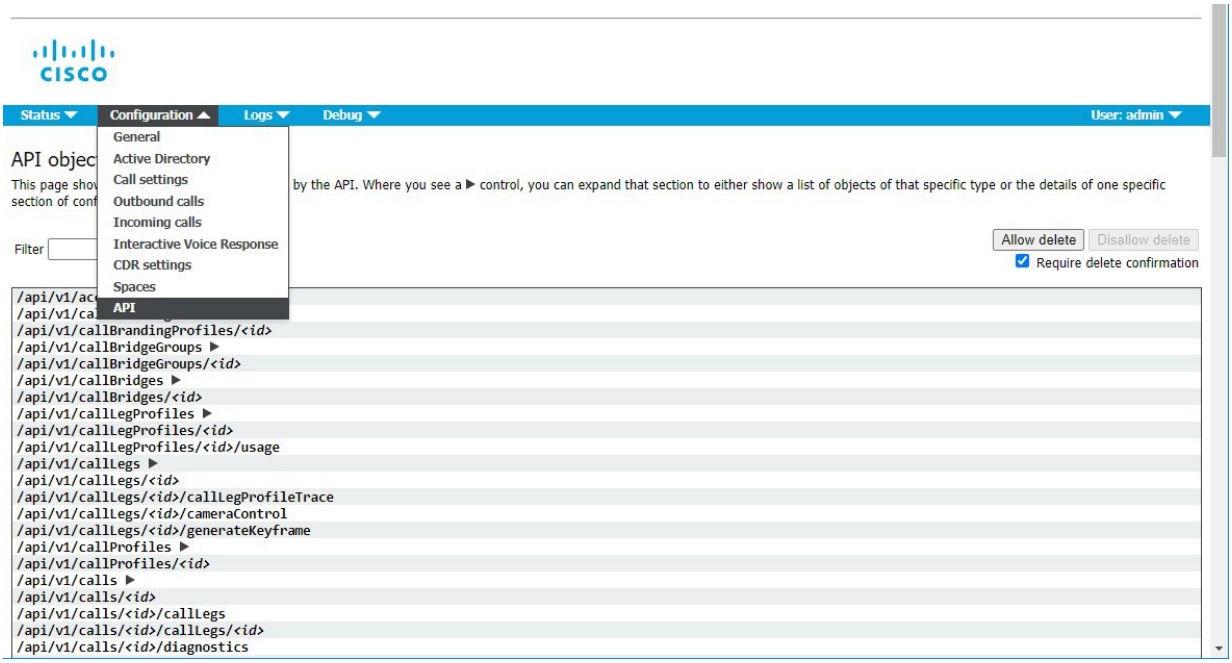
API を使用してスペースを作成することもできます。 詳細については、 API リファレンス ガイドを参照してください。

注： 通話 ID パラメーターは数値のみをサポートするため、数値で構成する必要があります。

I.7 API

バージョン 2.9 から、API には API メソッドおよびサードパーティアプリケーションではなく、Meeting Server のWeb 管理インターフェースを使用してアクセスできます。 Web 管理インターフェイスにログインした後、**[設定（Configuration）]** タブを選択し、[API] プルダウンリストから選択します。 図 33 を参照してください。

図 33：Meeting Server のウェブ管理インターフェイス経由で API にアクセスする



注：Web インターフェイスから API にアクセスするには、サードパーティアプリケーションを使用する場合と同様に、Meeting Server の初期設定と MMP を使用した認証を行う必要があります。

Cisco の法的情報

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

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

Cisco が採用している TCP ヘッダー圧縮機能は、UNIX オペレーティング システムの UCB（University of California, Berkeley）のパブリック ドメイン バージョンとして、UCB が開発したプログラムを採用したものです。 All rights reserved. Copyright © 1981, Regents of the University of California.

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

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

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

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

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

Cisco の商標または登録商標